



API Reference

# Amazon GuardDuty



**API Version 2017-11-28**

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

# Amazon GuardDuty: API Reference

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon's trademarks and trade dress may not be used in connection with any product or service that is not Amazon's, in any manner that is likely to cause confusion among customers, or in any manner that disparages or discredits Amazon. All other trademarks not owned by Amazon are the property of their respective owners, who may or may not be affiliated with, connected to, or sponsored by Amazon.

---

# Table of Contents

<b>Welcome</b> .....	<b>1</b>
<b>Actions</b> .....	<b>2</b>
AcceptAdministratorInvitation .....	5
Request Syntax .....	5
URI Request Parameters .....	5
Request Body .....	5
Response Syntax .....	6
Response Elements .....	6
Errors .....	6
See Also .....	6
AcceptInvitation .....	8
Request Syntax .....	8
URI Request Parameters .....	8
Request Body .....	8
Response Syntax .....	9
Response Elements .....	9
Errors .....	9
See Also .....	9
ArchiveFindings .....	11
Request Syntax .....	11
URI Request Parameters .....	11
Request Body .....	11
Response Syntax .....	12
Response Elements .....	12
Errors .....	12
See Also .....	12
CreateDetector .....	14
Request Syntax .....	14
URI Request Parameters .....	15
Request Body .....	15
Response Syntax .....	17
Response Elements .....	17
Errors .....	18
See Also .....	18

---

CreateFilter .....	19
Request Syntax .....	19
URI Request Parameters .....	19
Request Body .....	20
Response Syntax .....	25
Response Elements .....	25
Errors .....	26
See Also .....	26
CreateIPSet .....	27
Request Syntax .....	27
URI Request Parameters .....	27
Request Body .....	27
Response Syntax .....	29
Response Elements .....	29
Errors .....	30
See Also .....	30
CreateMalwareProtectionPlan .....	31
Request Syntax .....	31
URI Request Parameters .....	31
Request Body .....	31
Response Syntax .....	33
Response Elements .....	33
Errors .....	33
See Also .....	34
CreateMembers .....	35
Request Syntax .....	35
URI Request Parameters .....	36
Request Body .....	36
Response Syntax .....	36
Response Elements .....	37
Errors .....	37
See Also .....	37
CreatePublishingDestination .....	39
Request Syntax .....	39
URI Request Parameters .....	39
Request Body .....	39

---

Response Syntax .....	40
Response Elements .....	40
Errors .....	41
See Also .....	41
CreateSampleFindings .....	42
Request Syntax .....	42
URI Request Parameters .....	42
Request Body .....	42
Response Syntax .....	43
Response Elements .....	43
Errors .....	43
See Also .....	43
CreateThreatIntelSet .....	45
Request Syntax .....	45
URI Request Parameters .....	45
Request Body .....	45
Response Syntax .....	47
Response Elements .....	47
Errors .....	47
See Also .....	48
DeclineInvitations .....	49
Request Syntax .....	49
URI Request Parameters .....	49
Request Body .....	49
Response Syntax .....	49
Response Elements .....	50
Errors .....	50
See Also .....	51
DeleteDetector .....	52
Request Syntax .....	52
URI Request Parameters .....	52
Request Body .....	52
Response Syntax .....	52
Response Elements .....	52
Errors .....	52
See Also .....	53

---

DeleteFilter .....	54
Request Syntax .....	54
URI Request Parameters .....	54
Request Body .....	54
Response Syntax .....	54
Response Elements .....	54
Errors .....	54
See Also .....	55
DeleteInvitations .....	56
Request Syntax .....	56
URI Request Parameters .....	56
Request Body .....	56
Response Syntax .....	56
Response Elements .....	57
Errors .....	57
See Also .....	58
DeleteIPSet .....	59
Request Syntax .....	59
URI Request Parameters .....	59
Request Body .....	59
Response Syntax .....	59
Response Elements .....	59
Errors .....	60
See Also .....	60
DeleteMalwareProtectionPlan .....	61
Request Syntax .....	61
URI Request Parameters .....	61
Request Body .....	61
Response Syntax .....	61
Response Elements .....	61
Errors .....	61
See Also .....	62
DeleteMembers .....	63
Request Syntax .....	63
URI Request Parameters .....	63
Request Body .....	63

Response Syntax .....	64
Response Elements .....	64
Errors .....	64
See Also .....	65
DeletePublishingDestination .....	66
Request Syntax .....	66
URI Request Parameters .....	66
Request Body .....	66
Response Syntax .....	66
Response Elements .....	66
Errors .....	66
See Also .....	67
DeleteThreatIntelSet .....	68
Request Syntax .....	68
URI Request Parameters .....	68
Request Body .....	68
Response Syntax .....	68
Response Elements .....	68
Errors .....	68
See Also .....	69
DescribeMalwareScans .....	70
Request Syntax .....	70
URI Request Parameters .....	70
Request Body .....	71
Response Syntax .....	72
Response Elements .....	73
Errors .....	73
See Also .....	73
DescribeOrganizationConfiguration .....	75
Request Syntax .....	75
URI Request Parameters .....	75
Request Body .....	75
Response Syntax .....	76
Response Elements .....	77
Errors .....	78
See Also .....	79

DescribePublishingDestination .....	80
Request Syntax .....	80
URI Request Parameters .....	80
Request Body .....	80
Response Syntax .....	80
Response Elements .....	81
Errors .....	82
See Also .....	82
DisableOrganizationAdminAccount .....	83
Request Syntax .....	83
URI Request Parameters .....	83
Request Body .....	83
Response Syntax .....	83
Response Elements .....	83
Errors .....	84
See Also .....	84
DisassociateFromAdministratorAccount .....	85
Request Syntax .....	85
URI Request Parameters .....	85
Request Body .....	85
Response Syntax .....	85
Response Elements .....	85
Errors .....	86
See Also .....	86
DisassociateFromMasterAccount .....	87
Request Syntax .....	87
URI Request Parameters .....	87
Request Body .....	87
Response Syntax .....	87
Response Elements .....	87
Errors .....	88
See Also .....	88
DisassociateMembers .....	89
Request Syntax .....	89
URI Request Parameters .....	89
Request Body .....	90



Response Syntax .....	90
Response Elements .....	91
Errors .....	91
See Also .....	91
<b>EnableOrganizationAdminAccount .....</b>	<b>93</b>
Request Syntax .....	93
URI Request Parameters .....	93
Request Body .....	93
Response Syntax .....	93
Response Elements .....	93
Errors .....	94
See Also .....	94
<b>GetAdministratorAccount .....</b>	<b>95</b>
Request Syntax .....	95
URI Request Parameters .....	95
Request Body .....	95
Response Syntax .....	95
Response Elements .....	96
Errors .....	96
See Also .....	96
<b>GetCoverageStatistics .....</b>	<b>98</b>
Request Syntax .....	98
URI Request Parameters .....	98
Request Body .....	99
Response Syntax .....	99
Response Elements .....	99
Errors .....	100
See Also .....	100
<b>GetDetector .....</b>	<b>102</b>
Request Syntax .....	102
URI Request Parameters .....	102
Request Body .....	102
Response Syntax .....	102
Response Elements .....	104
Errors .....	105
See Also .....	105

---

GetFilter .....	107
Request Syntax .....	107
URI Request Parameters .....	107
Request Body .....	107
Response Syntax .....	107
Response Elements .....	108
Errors .....	109
See Also .....	110
GetFindings .....	111
Request Syntax .....	111
URI Request Parameters .....	111
Request Body .....	111
Response Syntax .....	112
Response Elements .....	129
Errors .....	130
See Also .....	130
GetFindingsStatistics .....	131
Request Syntax .....	131
URI Request Parameters .....	131
Request Body .....	132
Response Syntax .....	132
Response Elements .....	133
Errors .....	133
See Also .....	133
GetInvitationsCount .....	135
Request Syntax .....	135
URI Request Parameters .....	135
Request Body .....	135
Response Syntax .....	135
Response Elements .....	135
Errors .....	136
See Also .....	136
GetIPSet .....	137
Request Syntax .....	137
URI Request Parameters .....	137
Request Body .....	137

---

Response Syntax .....	137
Response Elements .....	138
Errors .....	139
See Also .....	139
<b>GetMalwareProtectionPlan .....</b>	<b>141</b>
Request Syntax .....	141
URI Request Parameters .....	141
Request Body .....	141
Response Syntax .....	141
Response Elements .....	142
Errors .....	143
See Also .....	144
<b>GetMalwareScanSettings .....</b>	<b>145</b>
Request Syntax .....	145
URI Request Parameters .....	145
Request Body .....	145
Response Syntax .....	145
Response Elements .....	146
Errors .....	146
See Also .....	147
<b>GetMasterAccount .....</b>	<b>148</b>
Request Syntax .....	148
URI Request Parameters .....	148
Request Body .....	148
Response Syntax .....	148
Response Elements .....	149
Errors .....	149
See Also .....	149
<b>GetMemberDetectors .....</b>	<b>151</b>
Request Syntax .....	151
URI Request Parameters .....	151
Request Body .....	151
Response Syntax .....	152
Response Elements .....	153
Errors .....	154
See Also .....	154

---

GetMembers .....	155
Request Syntax .....	155
URI Request Parameters .....	155
Request Body .....	155
Response Syntax .....	156
Response Elements .....	156
Errors .....	157
See Also .....	157
GetOrganizationStatistics .....	158
Request Syntax .....	158
URI Request Parameters .....	158
Request Body .....	158
Response Syntax .....	158
Response Elements .....	159
Errors .....	159
See Also .....	159
GetRemainingFreeTrialDays .....	161
Request Syntax .....	161
URI Request Parameters .....	161
Request Body .....	161
Response Syntax .....	162
Response Elements .....	163
Errors .....	163
See Also .....	164
GetThreatIntelSet .....	165
Request Syntax .....	165
URI Request Parameters .....	165
Request Body .....	165
Response Syntax .....	165
Response Elements .....	166
Errors .....	167
See Also .....	167
GetUsageStatistics .....	169
Request Syntax .....	169
URI Request Parameters .....	169
Request Body .....	170

---

Response Syntax .....	171
Response Elements .....	172
Errors .....	173
See Also .....	173
InviteMembers .....	175
Request Syntax .....	175
URI Request Parameters .....	176
Request Body .....	176
Response Syntax .....	177
Response Elements .....	177
Errors .....	177
See Also .....	178
ListCoverage .....	179
Request Syntax .....	179
URI Request Parameters .....	179
Request Body .....	180
Response Syntax .....	180
Response Elements .....	182
Errors .....	182
See Also .....	182
ListDetectors .....	184
Request Syntax .....	184
URI Request Parameters .....	184
Request Body .....	184
Response Syntax .....	184
Response Elements .....	185
Errors .....	185
See Also .....	185
ListFilters .....	187
Request Syntax .....	187
URI Request Parameters .....	187
Request Body .....	187
Response Syntax .....	187
Response Elements .....	188
Errors .....	188
See Also .....	189

---

ListFindings .....	190
Request Syntax .....	190
URI Request Parameters .....	190
Request Body .....	191
Response Syntax .....	193
Response Elements .....	194
Errors .....	194
See Also .....	195
ListInvitations .....	196
Request Syntax .....	196
URI Request Parameters .....	196
Request Body .....	196
Response Syntax .....	196
Response Elements .....	197
Errors .....	197
See Also .....	198
ListIPSets .....	199
Request Syntax .....	199
URI Request Parameters .....	199
Request Body .....	199
Response Syntax .....	199
Response Elements .....	200
Errors .....	200
See Also .....	201
ListMalwareProtectionPlans .....	202
Request Syntax .....	202
URI Request Parameters .....	202
Request Body .....	202
Response Syntax .....	202
Response Elements .....	202
Errors .....	203
See Also .....	203
ListMembers .....	205
Request Syntax .....	205
URI Request Parameters .....	205
Request Body .....	206

---

Response Syntax .....	206
Response Elements .....	206
Errors .....	207
See Also .....	207
ListOrganizationAdminAccounts .....	208
Request Syntax .....	208
URI Request Parameters .....	208
Request Body .....	208
Response Syntax .....	208
Response Elements .....	209
Errors .....	209
See Also .....	209
ListPublishingDestinations .....	211
Request Syntax .....	211
URI Request Parameters .....	211
Request Body .....	211
Response Syntax .....	211
Response Elements .....	212
Errors .....	212
See Also .....	213
ListTagsForResource .....	214
Request Syntax .....	214
URI Request Parameters .....	214
Request Body .....	214
Response Syntax .....	214
Response Elements .....	215
Errors .....	215
See Also .....	216
ListThreatIntelSets .....	217
Request Syntax .....	217
URI Request Parameters .....	217
Request Body .....	217
Response Syntax .....	218
Response Elements .....	218
Errors .....	218
See Also .....	219

StartMalwareScan .....	220
Request Syntax .....	220
URI Request Parameters .....	220
Request Body .....	220
Response Syntax .....	220
Response Elements .....	221
Errors .....	221
See Also .....	222
StartMonitoringMembers .....	223
Request Syntax .....	223
URI Request Parameters .....	223
Request Body .....	223
Response Syntax .....	224
Response Elements .....	224
Errors .....	224
See Also .....	225
StopMonitoringMembers .....	226
Request Syntax .....	226
URI Request Parameters .....	226
Request Body .....	226
Response Syntax .....	227
Response Elements .....	227
Errors .....	227
See Also .....	228
TagResource .....	229
Request Syntax .....	229
URI Request Parameters .....	229
Request Body .....	229
Response Syntax .....	230
Response Elements .....	230
Errors .....	230
See Also .....	230
UnarchiveFindings .....	232
Request Syntax .....	232
URI Request Parameters .....	232
Request Body .....	232



---

Response Syntax .....	233
Response Elements .....	233
Errors .....	233
See Also .....	233
UntagResource .....	235
Request Syntax .....	235
URI Request Parameters .....	235
Request Body .....	235
Response Syntax .....	235
Response Elements .....	236
Errors .....	236
See Also .....	236
UpdateDetector .....	238
Request Syntax .....	238
URI Request Parameters .....	239
Request Body .....	239
Response Syntax .....	240
Response Elements .....	240
Errors .....	240
See Also .....	241
UpdateFilter .....	242
Request Syntax .....	242
URI Request Parameters .....	242
Request Body .....	243
Response Syntax .....	244
Response Elements .....	244
Errors .....	244
See Also .....	245
UpdateFindingsFeedback .....	246
Request Syntax .....	246
URI Request Parameters .....	246
Request Body .....	246
Response Syntax .....	247
Response Elements .....	247
Errors .....	247
See Also .....	248

---

UpdateIPSet .....	249
Request Syntax .....	249
URI Request Parameters .....	249
Request Body .....	249
Response Syntax .....	250
Response Elements .....	250
Errors .....	250
See Also .....	251
UpdateMalwareProtectionPlan .....	252
Request Syntax .....	252
URI Request Parameters .....	252
Request Body .....	252
Response Syntax .....	253
Response Elements .....	253
Errors .....	253
See Also .....	254
UpdateMalwareScanSettings .....	255
Request Syntax .....	255
URI Request Parameters .....	255
Request Body .....	256
Response Syntax .....	256
Response Elements .....	256
Errors .....	256
See Also .....	257
UpdateMemberDetectors .....	258
Request Syntax .....	258
URI Request Parameters .....	259
Request Body .....	259
Response Syntax .....	260
Response Elements .....	260
Errors .....	260
See Also .....	261
UpdateOrganizationConfiguration .....	262
Request Syntax .....	262
URI Request Parameters .....	263
Request Body .....	263

---

Response Syntax .....	265
Response Elements .....	265
Errors .....	265
See Also .....	265
UpdatePublishingDestination .....	267
Request Syntax .....	267
URI Request Parameters .....	267
Request Body .....	267
Response Syntax .....	268
Response Elements .....	268
Errors .....	268
See Also .....	268
UpdateThreatIntelSet .....	270
Request Syntax .....	270
URI Request Parameters .....	270
Request Body .....	270
Response Syntax .....	271
Response Elements .....	271
Errors .....	271
See Also .....	272
<b>Data Types .....</b>	<b>273</b>
AccessControlList .....	280
Contents .....	280
See Also .....	280
AccessKeyDetails .....	281
Contents .....	281
See Also .....	281
AccountDetail .....	283
Contents .....	283
See Also .....	283
AccountFreeTrialInfo .....	284
Contents .....	284
See Also .....	284
AccountLevelPermissions .....	285
Contents .....	285
See Also .....	285

---

Action .....	286
Contents .....	286
See Also .....	287
AddonDetails .....	289
Contents .....	289
See Also .....	289
AdminAccount .....	290
Contents .....	290
See Also .....	290
Administrator .....	291
Contents .....	291
See Also .....	291
AgentDetails .....	293
Contents .....	293
See Also .....	293
Anomaly .....	294
Contents .....	294
See Also .....	294
AnomalyObject .....	295
Contents .....	295
See Also .....	295
AnomalyUnusual .....	297
Contents .....	297
See Also .....	297
AwsApiCallAction .....	298
Contents .....	298
See Also .....	299
BlockPublicAccess .....	300
Contents .....	300
See Also .....	300
BucketLevelPermissions .....	302
Contents .....	302
See Also .....	302
BucketPolicy .....	303
Contents .....	303
See Also .....	303

---

City .....	304
Contents .....	304
See Also .....	304
CloudTrailConfigurationResult .....	305
Contents .....	305
See Also .....	305
Condition .....	306
Contents .....	306
See Also .....	308
Container .....	309
Contents .....	309
See Also .....	310
ContainerInstanceDetails .....	311
Contents .....	311
See Also .....	311
Country .....	312
Contents .....	312
See Also .....	312
CoverageEc2InstanceDetails .....	313
Contents .....	313
See Also .....	314
CoverageEcsClusterDetails .....	315
Contents .....	315
See Also .....	315
CoverageEksClusterDetails .....	316
Contents .....	316
See Also .....	317
CoverageFilterCondition .....	318
Contents .....	318
See Also .....	318
CoverageFilterCriteria .....	319
Contents .....	319
See Also .....	319
CoverageFilterCriterion .....	320
Contents .....	320
See Also .....	320

---

CoverageResource .....	322
Contents .....	322
See Also .....	323
CoverageResourceDetails .....	324
Contents .....	324
See Also .....	324
CoverageSortCriteria .....	326
Contents .....	326
See Also .....	326
CoverageStatistics .....	328
Contents .....	328
See Also .....	328
CreateProtectedResource .....	329
Contents .....	329
See Also .....	329
CreateS3BucketResource .....	330
Contents .....	330
See Also .....	330
DataSourceConfigurations .....	331
Contents .....	331
See Also .....	331
DataSourceConfigurationsResult .....	332
Contents .....	332
See Also .....	333
DataSourceFreeTrial .....	334
Contents .....	334
See Also .....	334
DataSourcesFreeTrial .....	335
Contents .....	335
See Also .....	336
DefaultServerSideEncryption .....	337
Contents .....	337
See Also .....	337
Destination .....	338
Contents .....	338
See Also .....	338

DestinationProperties .....	340
Contents .....	340
See Also .....	340
Detection .....	341
Contents .....	341
See Also .....	341
DetectorAdditionalConfiguration .....	342
Contents .....	342
See Also .....	342
DetectorAdditionalConfigurationResult .....	343
Contents .....	343
See Also .....	343
DetectorFeatureConfiguration .....	345
Contents .....	345
See Also .....	346
DetectorFeatureConfigurationResult .....	347
Contents .....	347
See Also .....	348
DNSLogsConfigurationResult .....	349
Contents .....	349
See Also .....	349
DnsRequestAction .....	350
Contents .....	350
See Also .....	350
DomainDetails .....	352
Contents .....	352
See Also .....	352
EbsVolumeDetails .....	353
Contents .....	353
See Also .....	353
EbsVolumeScanDetails .....	354
Contents .....	354
See Also .....	355
EbsVolumesResult .....	356
Contents .....	356
See Also .....	356

---

EcsClusterDetails .....	357
Contents .....	357
See Also .....	358
EcsTaskDetails .....	359
Contents .....	359
See Also .....	360
EksClusterDetails .....	362
Contents .....	362
See Also .....	363
Evidence .....	364
Contents .....	364
See Also .....	364
FargateDetails .....	365
Contents .....	365
See Also .....	365
FilterCondition .....	367
Contents .....	367
See Also .....	367
FilterCriteria .....	369
Contents .....	369
See Also .....	369
FilterCriterion .....	370
Contents .....	370
See Also .....	370
Finding .....	372
Contents .....	372
See Also .....	374
FindingCriteria .....	376
Contents .....	376
See Also .....	376
FindingStatistics .....	377
Contents .....	377
See Also .....	377
FlowLogsConfigurationResult .....	378
Contents .....	378
See Also .....	378



FreeTrialFeatureConfigurationResult .....	379
Contents .....	379
See Also .....	379
GeoLocation .....	380
Contents .....	380
See Also .....	380
HighestSeverityThreatDetails .....	381
Contents .....	381
See Also .....	381
HostPath .....	382
Contents .....	382
See Also .....	382
IamInstanceProfile .....	383
Contents .....	383
See Also .....	383
ImpersonatedUser .....	384
Contents .....	384
See Also .....	384
InstanceDetails .....	385
Contents .....	385
See Also .....	387
Invitation .....	388
Contents .....	388
See Also .....	388
ItemPath .....	390
Contents .....	390
See Also .....	390
KubernetesApiCallAction .....	391
Contents .....	391
See Also .....	393
KubernetesAuditLogsConfiguration .....	394
Contents .....	394
See Also .....	394
KubernetesAuditLogsConfigurationResult .....	395
Contents .....	395
See Also .....	395

KubernetesConfiguration .....	396
Contents .....	396
See Also .....	396
KubernetesConfigurationResult .....	397
Contents .....	397
See Also .....	397
KubernetesDataSourceFreeTrial .....	398
Contents .....	398
See Also .....	398
KubernetesDetails .....	399
Contents .....	399
See Also .....	399
KubernetesPermissionCheckedDetails .....	400
Contents .....	400
See Also .....	400
KubernetesRoleBindingDetails .....	402
Contents .....	402
See Also .....	403
KubernetesRoleDetails .....	404
Contents .....	404
See Also .....	404
KubernetesUserDetails .....	405
Contents .....	405
See Also .....	406
KubernetesWorkloadDetails .....	407
Contents .....	407
See Also .....	408
LambdaDetails .....	410
Contents .....	410
See Also .....	411
LineageObject .....	412
Contents .....	412
See Also .....	413
LocalIpDetails .....	414
Contents .....	414
See Also .....	414

LocalPortDetails .....	415
Contents .....	415
See Also .....	415
LoginAttribute .....	416
Contents .....	416
See Also .....	416
MalwareProtectionConfiguration .....	418
Contents .....	418
See Also .....	418
MalwareProtectionConfigurationResult .....	419
Contents .....	419
See Also .....	419
MalwareProtectionDataSourceFreeTrial .....	420
Contents .....	420
See Also .....	420
MalwareProtectionPlanActions .....	421
Contents .....	421
See Also .....	421
MalwareProtectionPlanStatusReason .....	422
Contents .....	422
See Also .....	422
MalwareProtectionPlanSummary .....	423
Contents .....	423
See Also .....	423
MalwareProtectionPlanTaggingAction .....	424
Contents .....	424
See Also .....	424
MalwareScanDetails .....	425
Contents .....	425
See Also .....	425
Master .....	426
Contents .....	426
See Also .....	426
Member .....	428
Contents .....	428
See Also .....	429

MemberAdditionalConfiguration .....	430
Contents .....	430
See Also .....	430
MemberAdditionalConfigurationResult .....	431
Contents .....	431
See Also .....	431
MemberDataSourceConfiguration .....	433
Contents .....	433
See Also .....	433
MemberFeaturesConfiguration .....	435
Contents .....	435
See Also .....	435
MemberFeaturesConfigurationResult .....	437
Contents .....	437
See Also .....	438
NetworkConnectionAction .....	439
Contents .....	439
See Also .....	440
NetworkInterface .....	441
Contents .....	441
See Also .....	442
Observations .....	444
Contents .....	444
See Also .....	444
Organization .....	445
Contents .....	445
See Also .....	445
OrganizationAdditionalConfiguration .....	447
Contents .....	447
See Also .....	448
OrganizationAdditionalConfigurationResult .....	449
Contents .....	449
See Also .....	450
OrganizationDataSourceConfigurations .....	451
Contents .....	451
See Also .....	451

OrganizationDataSourceConfigurationsResult .....	452
Contents .....	452
See Also .....	452
OrganizationDetails .....	453
Contents .....	453
See Also .....	453
OrganizationEbsVolumes .....	454
Contents .....	454
See Also .....	454
OrganizationEbsVolumesResult .....	455
Contents .....	455
See Also .....	455
OrganizationFeatureConfiguration .....	456
Contents .....	456
See Also .....	457
OrganizationFeatureConfigurationResult .....	458
Contents .....	458
See Also .....	459
OrganizationFeatureStatistics .....	460
Contents .....	460
See Also .....	460
OrganizationFeatureStatisticsAdditionalConfiguration .....	462
Contents .....	462
See Also .....	462
OrganizationKubernetesAuditLogsConfiguration .....	463
Contents .....	463
See Also .....	463
OrganizationKubernetesAuditLogsConfigurationResult .....	464
Contents .....	464
See Also .....	464
OrganizationKubernetesConfiguration .....	465
Contents .....	465
See Also .....	465
OrganizationKubernetesConfigurationResult .....	466
Contents .....	466
See Also .....	466

OrganizationMalwareProtectionConfiguration .....	467
Contents .....	467
See Also .....	467
OrganizationMalwareProtectionConfigurationResult .....	468
Contents .....	468
See Also .....	468
OrganizationS3LogsConfiguration .....	469
Contents .....	469
See Also .....	469
OrganizationS3LogsConfigurationResult .....	470
Contents .....	470
See Also .....	470
OrganizationScanEc2InstanceWithFindings .....	471
Contents .....	471
See Also .....	471
OrganizationScanEc2InstanceWithFindingsResult .....	472
Contents .....	472
See Also .....	472
OrganizationStatistics .....	473
Contents .....	473
See Also .....	474
Owner .....	475
Contents .....	475
See Also .....	475
PermissionConfiguration .....	476
Contents .....	476
See Also .....	476
PortProbeAction .....	477
Contents .....	477
See Also .....	477
PortProbeDetail .....	478
Contents .....	478
See Also .....	478
PrivateIpAddressDetails .....	479
Contents .....	479
See Also .....	479

---

ProcessDetails .....	480
Contents .....	480
See Also .....	482
ProductCode .....	483
Contents .....	483
See Also .....	483
PublicAccess .....	484
Contents .....	484
See Also .....	484
RdsDbInstanceDetails .....	485
Contents .....	485
See Also .....	486
RdsDbUserDetails .....	487
Contents .....	487
See Also .....	488
RdsLoginAttemptAction .....	489
Contents .....	489
See Also .....	489
RemoteAccountDetails .....	490
Contents .....	490
See Also .....	490
RemotelpDetails .....	491
Contents .....	491
See Also .....	492
RemotePortDetails .....	493
Contents .....	493
See Also .....	493
Resource .....	494
Contents .....	494
See Also .....	496
ResourceDetails .....	497
Contents .....	497
See Also .....	497
RuntimeContext .....	498
Contents .....	498
See Also .....	502

---

RuntimeDetails .....	503
Contents .....	503
See Also .....	503
S3BucketDetail .....	504
Contents .....	504
See Also .....	505
S3LogsConfiguration .....	506
Contents .....	506
See Also .....	506
S3LogsConfigurationResult .....	507
Contents .....	507
See Also .....	507
S3ObjectDetail .....	508
Contents .....	508
See Also .....	509
Scan .....	510
Contents .....	510
See Also .....	513
ScanCondition .....	514
Contents .....	514
See Also .....	514
ScanConditionPair .....	515
Contents .....	515
See Also .....	515
ScanDetections .....	516
Contents .....	516
See Also .....	516
ScanEc2InstanceWithFindings .....	518
Contents .....	518
See Also .....	518
ScanEc2InstanceWithFindingsResult .....	519
Contents .....	519
See Also .....	519
ScanFilePath .....	520
Contents .....	520
See Also .....	520



---

ScannedItemCount .....	522
Contents .....	522
See Also .....	522
ScanResourceCriteria .....	523
Contents .....	523
See Also .....	523
ScanResultDetails .....	524
Contents .....	524
See Also .....	524
ScanThreatName .....	525
Contents .....	525
See Also .....	525
SecurityContext .....	527
Contents .....	527
See Also .....	527
SecurityGroup .....	528
Contents .....	528
See Also .....	528
Service .....	529
Contents .....	529
See Also .....	531
ServiceAdditionalInfo .....	533
Contents .....	533
See Also .....	533
SortCriteria .....	534
Contents .....	534
See Also .....	534
Tag .....	535
Contents .....	535
See Also .....	535
Threat .....	536
Contents .....	536
See Also .....	536
ThreatDetectedByName .....	537
Contents .....	537
See Also .....	537

ThreatIntelligenceDetail .....	539
Contents .....	539
See Also .....	539
ThreatsDetectedItemCount .....	540
Contents .....	540
See Also .....	540
Total .....	541
Contents .....	541
See Also .....	541
TriggerDetails .....	542
Contents .....	542
See Also .....	542
UnprocessedAccount .....	543
Contents .....	543
See Also .....	543
UnprocessedDataSourcesResult .....	544
Contents .....	544
See Also .....	544
UpdateProtectedResource .....	545
Contents .....	545
See Also .....	545
UpdateS3BucketResource .....	546
Contents .....	546
See Also .....	546
UsageAccountResult .....	547
Contents .....	547
See Also .....	547
UsageCriteria .....	548
Contents .....	548
See Also .....	549
UsageDataSourceResult .....	550
Contents .....	550
See Also .....	550
UsageFeatureResult .....	551
Contents .....	551
See Also .....	551

---

UsageResourceResult .....	552
Contents .....	552
See Also .....	552
UsageStatistics .....	553
Contents .....	553
See Also .....	554
UsageTopAccountResult .....	555
Contents .....	555
See Also .....	555
UsageTopAccountsResult .....	556
Contents .....	556
See Also .....	556
Volume .....	557
Contents .....	557
See Also .....	557
VolumeDetail .....	558
Contents .....	558
See Also .....	559
VolumeMount .....	560
Contents .....	560
See Also .....	560
VpcConfig .....	561
Contents .....	561
See Also .....	561
<b>Common Parameters .....</b>	<b>562</b>
<b>Common Errors .....</b>	<b>565</b>

# Welcome

Amazon GuardDuty is a continuous security monitoring service that analyzes and processes the following foundational data sources - VPC flow logs, AWS CloudTrail management event logs, CloudTrail S3 data event logs, EKS audit logs, DNS logs, Amazon EBS volume data, runtime activity belonging to container workloads, such as Amazon EKS, Amazon ECS (including AWS Fargate), and Amazon EC2 instances. It uses threat intelligence feeds, such as lists of malicious IPs and domains, and machine learning to identify unexpected, potentially unauthorized, and malicious activity within your AWS environment. This can include issues like escalations of privileges, uses of exposed credentials, or communication with malicious IPs, domains, or presence of malware on your Amazon EC2 instances and container workloads. For example, GuardDuty can detect compromised EC2 instances and container workloads serving malware, or mining bitcoin.

GuardDuty also monitors AWS account access behavior for signs of compromise, such as unauthorized infrastructure deployments like EC2 instances deployed in a Region that has never been used, or unusual API calls like a password policy change to reduce password strength.

GuardDuty informs you about the status of your AWS environment by producing security findings that you can view in the GuardDuty console or through Amazon EventBridge. For more information, see the [Amazon GuardDuty User Guide](#).

This document was last published on July 2, 2024.

# Actions

The following actions are supported:

- [AcceptAdministratorInvitation](#)
- [AcceptInvitation](#)
- [ArchiveFindings](#)
- [CreateDetector](#)
- [CreateFilter](#)
- [CreateIPSet](#)
- [CreateMalwareProtectionPlan](#)
- [CreateMembers](#)
- [CreatePublishingDestination](#)
- [CreateSampleFindings](#)
- [CreateThreatIntelSet](#)
- [DeclineInvitations](#)
- [DeleteDetector](#)
- [DeleteFilter](#)
- [DeleteInvitations](#)
- [DeleteIPSet](#)
- [DeleteMalwareProtectionPlan](#)
- [DeleteMembers](#)
- [DeletePublishingDestination](#)
- [DeleteThreatIntelSet](#)
- [DescribeMalwareScans](#)
- [DescribeOrganizationConfiguration](#)
- [DescribePublishingDestination](#)
- [DisableOrganizationAdminAccount](#)
- [DisassociateFromAdministratorAccount](#)
- [DisassociateFromMasterAccount](#)
- [DisassociateMembers](#)

- [EnableOrganizationAdminAccount](#)
- [GetAdministratorAccount](#)
- [GetCoverageStatistics](#)
- [GetDetector](#)
- [GetFilter](#)
- [GetFindings](#)
- [GetFindingsStatistics](#)
- [GetInvitationsCount](#)
- [GetIPSet](#)
- [GetMalwareProtectionPlan](#)
- [GetMalwareScanSettings](#)
- [GetMasterAccount](#)
- [GetMemberDetectors](#)
- [GetMembers](#)
- [GetOrganizationStatistics](#)
- [GetRemainingFreeTrialDays](#)
- [GetThreatIntelSet](#)
- [GetUsageStatistics](#)
- [InviteMembers](#)
- [ListCoverage](#)
- [ListDetectors](#)
- [ListFilters](#)
- [ListFindings](#)
- [ListInvitations](#)
- [ListIPSets](#)
- [ListMalwareProtectionPlans](#)
- [ListMembers](#)
- [ListOrganizationAdminAccounts](#)
- [ListPublishingDestinations](#)
- [ListTagsForResource](#)

- [ListThreatIntelSets](#)
- [StartMalwareScan](#)
- [StartMonitoringMembers](#)
- [StopMonitoringMembers](#)
- [TagResource](#)
- [UnarchiveFindings](#)
- [UntagResource](#)
- [UpdateDetector](#)
- [UpdateFilter](#)
- [UpdateFindingsFeedback](#)
- [UpdateIPSet](#)
- [UpdateMalwareProtectionPlan](#)
- [UpdateMalwareScanSettings](#)
- [UpdateMemberDetectors](#)
- [UpdateOrganizationConfiguration](#)
- [UpdatePublishingDestination](#)
- [UpdateThreatIntelSet](#)

# AcceptAdministratorInvitation

Accepts the invitation to be a member account and get monitored by a GuardDuty administrator account that sent the invitation.

## Request Syntax

```
POST /detector/detectorId/administrator HTTP/1.1  
Content-type: application/json
```

```
{  
  "administratorId": "string",  
  "invitationId": "string"  
}
```

## URI Request Parameters

The request uses the following URI parameters.

### detectorId

The unique ID of the detector of the GuardDuty member account.

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

## Request Body

The request accepts the following data in JSON format.

### administratorId

The account ID of the GuardDuty administrator account whose invitation you're accepting.

Type: String

Required: Yes

### invitationId

The value that is used to validate the administrator account to the member account.



Type: String

Required: Yes

## Response Syntax

```
HTTP/1.1 200
```

## Response Elements

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

## Errors

For information about the errors that are common to all actions, see [Common Errors](#).

### BadRequestException

A bad request exception object.

HTTP Status Code: 400

### InternalServerErrorException

An internal server error exception object.

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 v2](#)
- [AWS SDK for Java V2](#)

- [AWS SDK for JavaScript V3](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

# AcceptInvitation

*This action has been deprecated.*

Accepts the invitation to be monitored by a GuardDuty administrator account.

## Request Syntax

```
POST /detector/detectorId/master HTTP/1.1
Content-type: application/json
```

```
{
  "invitationId": "string",
  "masterId": "string"
}
```

## URI Request Parameters

The request uses the following URI parameters.

### detectorId

The unique ID of the detector of the GuardDuty member account.

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

## Request Body

The request accepts the following data in JSON format.

### invitationId

The value that is used to validate the administrator account to the member account.

Type: String

Required: Yes

### masterId

The account ID of the GuardDuty administrator account whose invitation you're accepting.

Type: String

Required: Yes

## Response Syntax

```
HTTP/1.1 200
```

## Response Elements

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

## Errors

For information about the errors that are common to all actions, see [Common Errors](#).

### BadRequestException

A bad request exception object.

HTTP Status Code: 400

### InternalServerErrorException

An internal server error exception object.

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 v2](#)
- [AWS SDK for Java V2](#)

- [AWS SDK for JavaScript V3](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

# ArchiveFindings

Archives GuardDuty findings that are specified by the list of finding IDs.

## Note

Only the administrator account can archive findings. Member accounts don't have permission to archive findings from their accounts.

## Request Syntax

```
POST /detector/detectorId/findings/archive HTTP/1.1
Content-type: application/json
```

```
{
  "findingIds": [ "string" ]
}
```

## URI Request Parameters

The request uses the following URI parameters.

### detectorId

The ID of the detector that specifies the GuardDuty service whose findings you want to archive.

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

## Request Body

The request accepts the following data in JSON format.

### findingIds

The IDs of the findings that you want to archive.

Type: Array of strings

Array Members: Minimum number of 0 items. Maximum number of 50 items.

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

## Response Syntax

```
HTTP/1.1 200
```

## Response Elements

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

## Errors

For information about the errors that are common to all actions, see [Common Errors](#).

### BadRequestException

A bad request exception object.

HTTP Status Code: 400

### InternalServerErrorException

An internal server error exception object.

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 v2](#)

- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)



# CreateDetector

Creates a single GuardDuty detector. A detector is a resource that represents the GuardDuty service. To start using GuardDuty, you must create a detector in each Region where you enable the service. You can have only one detector per account per Region. All data sources are enabled in a new detector by default.

- When you don't specify any features, with an exception to `RUNTIME_MONITORING`, all the optional features are enabled by default.
- When you specify some of the features, any feature that is not specified in the API call gets enabled by default, with an exception to `RUNTIME_MONITORING`.

Specifying both EKS Runtime Monitoring (`EKS_RUNTIME_MONITORING`) and Runtime Monitoring (`RUNTIME_MONITORING`) will cause an error. You can add only one of these two features because Runtime Monitoring already includes the threat detection for Amazon EKS resources. For more information, see [Runtime Monitoring](#).

There might be regional differences because some data sources might not be available in all the AWS Regions where GuardDuty is presently supported. For more information, see [Regions and endpoints](#).

## Request Syntax

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

{
  "clientToken": "string",
  "dataSources": {
    "kubernetes": {
      "auditLogs": {
        "enable": boolean
      }
    },
    "malwareProtection": {
      "scanEc2InstanceWithFindings": {
        "ebsVolumes": boolean
      }
    },
    "s3Logs": {
```

```
    "enable": boolean
  },
  "enable": boolean,
  "features": [
    {
      "additionalConfiguration": [
        {
          "name": "string",
          "status": "string"
        }
      ],
      "name": "string",
      "status": "string"
    }
  ],
  "findingPublishingFrequency": "string",
  "tags": {
    "string" : "string"
  }
}
```

## URI Request Parameters

The request does not use any URI parameters.

## Request Body

The request accepts the following data in JSON format.

### clientToken

The idempotency token for the create request.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 64.

Required: No

### dataSources

*This parameter has been deprecated.*

Describes which data sources will be enabled for the detector.

There might be regional differences because some data sources might not be available in all the AWS Regions where GuardDuty is presently supported. For more information, see [Regions and endpoints](#).

Type: [DataSourceConfigurations](#) object

Required: No

### **enable**

A Boolean value that specifies whether the detector is to be enabled.

Type: Boolean

Required: Yes

### **features**

A list of features that will be configured for the detector.

Type: Array of [DetectorFeatureConfiguration](#) objects

Required: No

### **findingPublishingFrequency**

A value that specifies how frequently updated findings are exported.

Type: String

Valid Values: FIFTEEN\_MINUTES | ONE\_HOUR | SIX\_HOURS

Required: No

### **tags**

The tags to be added to a new detector resource.

Type: String to string map

Map Entries: Maximum number of 200 items.

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

Key Pattern: `^(?!aws:)[a-zA-Z+-. _:/]+$`

Value Length Constraints: Maximum length of 256.

Required: No

## Response Syntax

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

{
  "detectorId": "string",
  "unprocessedDataSources": {
    "malwareProtection": {
      "scanEc2InstanceWithFindings": {
        "ebsVolumes": {
          "reason": "string",
          "status": "string"
        }
      },
      "serviceRole": "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.

### detectorId

The unique ID of the created detector.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 300.

### unprocessedDataSources

Specifies the data sources that couldn't be enabled when GuardDuty was enabled for the first time.

Type: [UnprocessedDataSourcesResult](#) object

## Errors

For information about the errors that are common to all actions, see [Common Errors](#).

### BadRequestException

A bad request exception object.

HTTP Status Code: 400

### InternalServerErrorException

An internal server error exception object.

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 v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

# CreateFilter

Creates a filter using the specified finding criteria. The maximum number of saved filters per AWS account per Region is 100. For more information, see [Quotas for GuardDuty](#).

## Request Syntax

```
POST /detector/detectorId/filter HTTP/1.1
Content-type: application/json
```

```
{
  "action": "string",
  "clientToken": "string",
  "description": "string",
  "findingCriteria": {
    "criterion": {
      "string" : {
        "eq": [ "string" ],
        "equals": [ "string" ],
        "greaterThan": number,
        "greaterThanOrEqualTo": number,
        "gt": number,
        "gte": number,
        "lessThan": number,
        "lessThanOrEqualTo": number,
        "lt": number,
        "lte": number,
        "neq": [ "string" ],
        "notEquals": [ "string" ]
      }
    }
  },
  "name": "string",
  "rank": number,
  "tags": {
    "string" : "string"
  }
}
```

## URI Request Parameters

The request uses the following URI parameters.

## detectorId

The ID of the detector belonging to the GuardDuty account that you want to create a filter for.

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

## Request Body

The request accepts the following data in JSON format.

### action

Specifies the action that is to be applied to the findings that match the filter.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 300.

Valid Values: NOOP | ARCHIVE

Required: No

### clientToken

The idempotency token for the create request.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 64.

Required: No

### description

The description of the filter. Valid characters include alphanumeric characters, and special characters such as hyphen, period, colon, underscore, parentheses ( { }, [ ], and ( )), forward slash, horizontal tab, vertical tab, newline, form feed, return, and whitespace.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 512.

Required: No

## findingCriteria

Represents the criteria to be used in the filter for querying findings.

You can only use the following attributes to query findings:

- accountId
- id
- region
- severity

To filter on the basis of severity, the API and AWS CLI use the following input list for the [FindingCriteria](#) condition:

- **Low:** ["1", "2", "3"]
- **Medium:** ["4", "5", "6"]
- **High:** ["7", "8", "9"]

For more information, see [Severity levels for GuardDuty findings](#).

- type
- updatedAt

Type: ISO 8601 string format: YYYY-MM-DDTHH:MM:SS.SSSZ or YYYY-MM-DDTHH:MM:SSZ depending on whether the value contains milliseconds.

- resource.accessKeyDetails.accessKeyId
- resource.accessKeyDetails.principalId
- resource.accessKeyDetails.userName
- resource.accessKeyDetails.userType
- resource.instanceDetails.iamInstanceProfile.id
- resource.instanceDetails.imageId
- resource.instanceDetails.instanceId
- resource.instanceDetails.tags.key
- resource.instanceDetails.tags.value
- resource.instanceDetails.networkInterfaces.ipv6Addresses
- resource.instanceDetails.networkInterfaces.privateIpAddresses.privateIpAddress
- resource.instanceDetails.networkInterfaces.publicDnsName



- resource.instanceDetails.networkInterfaces.publicIp
- resource.instanceDetails.networkInterfaces.securityGroups.groupId
- resource.instanceDetails.networkInterfaces.securityGroups.groupName
- resource.instanceDetails.networkInterfaces.subnetId
- resource.instanceDetails.networkInterfaces.vpcId
- resource.instanceDetails.outpostArn
- resource.resourceType
- resource.s3BucketDetails.publicAccess.effectivePermissions
- resource.s3BucketDetails.name
- resource.s3BucketDetails.tags.key
- resource.s3BucketDetails.tags.value
- resource.s3BucketDetails.type
- service.action.actionType
- service.action.awsApiCallAction.api
- service.action.awsApiCallAction.callerType
- service.action.awsApiCallAction.errorCode
- service.action.awsApiCallAction.remotelpDetails.city.cityName
- service.action.awsApiCallAction.remotelpDetails.country.countryName
- service.action.awsApiCallAction.remotelpDetails.ipAddressV4
- service.action.awsApiCallAction.remotelpDetails.ipAddressV6
- service.action.awsApiCallAction.remotelpDetails.organization.asn
- service.action.awsApiCallAction.remotelpDetails.organization.asnOrg
- service.action.awsApiCallAction.serviceName
- service.action.dnsRequestAction.domain
- service.action.dnsRequestAction.domainWithSuffix
- service.action.networkConnectionAction.blocked
- service.action.networkConnectionAction.connectionDirection
- service.action.networkConnectionAction.localPortDetails.port
- service.action.networkConnectionAction.protocol
- service.action.networkConnectionAction.remotelpDetails.city.cityName

- `service.action.networkConnectionAction.remoteIpDetails.country.countryName`
- `service.action.networkConnectionAction.remoteIpDetails.ipAddressV4`
- `service.action.networkConnectionAction.remoteIpDetails.ipAddressV6`
- `service.action.networkConnectionAction.remoteIpDetails.organization.asn`
- `service.action.networkConnectionAction.remoteIpDetails.organization.asnOrg`
- `service.action.networkConnectionAction.remotePortDetails.port`
- `service.action.awsApiCallAction.remoteAccountDetails.affiliated`
- `service.action.kubernetesApiCallAction.remoteIpDetails.ipAddressV4`
- `service.action.kubernetesApiCallAction.remoteIpDetails.ipAddressV6`
- `service.action.kubernetesApiCallAction.namespace`
- `service.action.kubernetesApiCallAction.remoteIpDetails.organization.asn`
- `service.action.kubernetesApiCallAction.requestUri`
- `service.action.kubernetesApiCallAction.statusCode`
- `service.action.networkConnectionAction.localIpDetails.ipAddressV4`
- `service.action.networkConnectionAction.localIpDetails.ipAddressV6`
- `service.action.networkConnectionAction.protocol`
- `service.action.awsApiCallAction.serviceName`
- `service.action.awsApiCallAction.remoteAccountDetails.accountId`
- `service.additionalInfo.threatListName`
- `service.resourceRole`
- `resource.eksClusterDetails.name`
- `resource.kubernetesDetails.kubernetesWorkloadDetails.name`
- `resource.kubernetesDetails.kubernetesWorkloadDetails.namespace`
- `resource.kubernetesDetails.kubernetesUserDetails.username`
- `resource.kubernetesDetails.kubernetesWorkloadDetails.containers.image`
- `resource.kubernetesDetails.kubernetesWorkloadDetails.containers.imagePrefix`
- `service.ebsVolumeScanDetails.scanId`
- `service.ebsVolumeScanDetails.scanDetections.threatDetectedByName.threatNames.name`
- `service.ebsVolumeScanDetails.scanDetections.threatDetectedByName.threatNames.severity`
- `service.ebsVolumeScanDetails.scanDetections.threatDetectedByName.threatNames.filePaths.hash`

- resource.ecsClusterDetails.name
- resource.ecsClusterDetails.taskDetails.containers.image
- resource.ecsClusterDetails.taskDetails.definitionArn
- resource.containerDetails.image
- resource.rdsDbInstanceDetails.dbInstanceIdentifier
- resource.rdsDbInstanceDetails.dbClusterIdentifier
- resource.rdsDbInstanceDetails.engine
- resource.rdsDbUserDetails.user
- resource.rdsDbInstanceDetails.tags.key
- resource.rdsDbInstanceDetails.tags.value
- service.runtimeDetails.process.executableSha256
- service.runtimeDetails.process.name
- service.runtimeDetails.process.name
- resource.lambdaDetails.functionName
- resource.lambdaDetails.functionArn
- resource.lambdaDetails.tags.key
- resource.lambdaDetails.tags.value

Type: [FindingCriteria](#) object

Required: Yes

### name

The name of the filter. Valid characters include period (.), underscore (\_), dash (-), and alphanumeric characters. A whitespace is considered to be an invalid character.

Type: String

Length Constraints: Minimum length of 3. Maximum length of 64.

Required: Yes

### rank

Specifies the position of the filter in the list of current filters. Also specifies the order in which this filter is applied to the findings.

Type: Integer

Valid Range: Minimum value of 1. Maximum value of 100.

Required: No

### tags

The tags to be added to a new filter resource.

Type: String to string map

Map Entries: Maximum number of 200 items.

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

Key Pattern:  $^(?!aws:)[a-zA-Z+--=._:/]+$

Value Length Constraints: Maximum length of 256.

Required: No

## Response Syntax

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

{
  "name": "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.

### name

The name of the successfully created filter.

Type: String

Length Constraints: Minimum length of 3. Maximum length of 64.

## Errors

For information about the errors that are common to all actions, see [Common Errors](#).

### **BadRequestException**

A bad request exception object.

HTTP Status Code: 400

### **InternalServerErrorException**

An internal server error exception object.

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 v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

# CreateIPSet

Creates a new IPSet, which is called a trusted IP list in the console user interface. An IPSet is a list of IP addresses that are trusted for secure communication with AWS infrastructure and applications. GuardDuty doesn't generate findings for IP addresses that are included in IPSets. Only users from the administrator account can use this operation.

## Request Syntax

```
POST /detector/detectorId/ipset HTTP/1.1
```

```
Content-type: application/json
```

```
{
  "activate": boolean,
  "clientToken": "string",
  "format": "string",
  "location": "string",
  "name": "string",
  "tags": {
    "string" : "string"
  }
}
```

## URI Request Parameters

The request uses the following URI parameters.

### detectorId

The unique ID of the detector of the GuardDuty account that you want to create an IPSet for.

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

## Request Body

The request accepts the following data in JSON format.

## activate

A Boolean value that indicates whether GuardDuty is to start using the uploaded IPSet.

Type: Boolean

Required: Yes

## clientToken

The idempotency token for the create request.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 64.

Required: No

## format

The format of the file that contains the IPSet.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 300.

Valid Values: TXT | STIX | OTX\_CSV | ALIEN\_VAULT | PROOF\_POINT | FIRE\_EYE

Required: Yes

## location

The URI of the file that contains the IPSet.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

## name

The user-friendly name to identify the IPSet.

Allowed characters are alphanumeric, whitespace, dash (-), and underscores (\_).

Type: String

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

### tags

The tags to be added to a new IP set resource.

Type: String to string map

Map Entries: Maximum number of 200 items.

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

Key Pattern:  $^(?!aws:)[a-zA-Z+-. _:/]+$

Value Length Constraints: Maximum length of 256.

Required: No

## Response Syntax

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

{
  "ipSetId": "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.

### ipSetId

The ID of the IPSet resource.

Type: String



## Errors

For information about the errors that are common to all actions, see [Common Errors](#).

### **BadRequestException**

A bad request exception object.

HTTP Status Code: 400

### **InternalServerErrorException**

An internal server error exception object.

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 v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

# CreateMalwareProtectionPlan

Creates a new Malware Protection plan for the protected resource.

When you create a Malware Protection plan, the AWS service terms for GuardDuty Malware Protection apply. For more information, see [AWS service terms for GuardDuty Malware Protection](#).

## Request Syntax

```
POST /malware-protection-plan HTTP/1.1
```

```
Content-type: application/json
```

```
{
  "actions": {
    "tagging": {
      "status": "string"
    }
  },
  "clientToken": "string",
  "protectedResource": {
    "s3Bucket": {
      "bucketName": "string",
      "objectPrefixes": [ "string" ]
    }
  },
  "role": "string",
  "tags": {
    "string" : "string"
  }
}
```

## URI Request Parameters

The request does not use any URI parameters.

## Request Body

The request accepts the following data in JSON format.

### actions

Information about whether the tags will be added to the S3 object after scanning.

Type: [MalwareProtectionPlanActions](#) object

Required: No

### [clientToken](#)

The idempotency token for the create request.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 64.

Required: No

### [protectedResource](#)

Information about the protected resource that is associated with the created Malware Protection plan. Presently, S3Bucket is the only supported protected resource.

Type: [CreateProtectedResource](#) object

Required: Yes

### [role](#)

IAM role with permissions required to scan and add tags to the associated protected resource.

Type: String

Required: Yes

### [tags](#)

Tags added to the Malware Protection plan resource.

Type: String to string map

Map Entries: Maximum number of 200 items.

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

Key Pattern: `^(?!aws:)[a-zA-Z+ -= . _ : / ] + $`

Value Length Constraints: Maximum length of 256.

Required: No

## Response Syntax

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

{
  "malwareProtectionPlanId": "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.

### [malwareProtectionPlanId](#)

A unique identifier associated with the Malware Protection plan resource.

Type: String

## Errors

For information about the errors that are common to all actions, see [Common Errors](#).

### **AccessDeniedException**

An access denied exception object.

HTTP Status Code: 403

### **BadRequestException**

A bad request exception object.

HTTP Status Code: 400

### **ConflictException**

A request conflict exception object.

HTTP Status Code: 409

## InternalServerErrorException

An internal server error exception object.

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 v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

# CreateMembers

Creates member accounts of the current AWS account by specifying a list of AWS account IDs. This step is a prerequisite for managing the associated member accounts either by invitation or through an organization.

As a delegated administrator, using `CreateMembers` will enable GuardDuty in the added member accounts, with the exception of the organization delegated administrator account. A delegated administrator must enable GuardDuty prior to being added as a member.

When you use `CreateMembers` as an AWS Organizations delegated administrator, GuardDuty applies your organization's auto-enable settings to the member accounts in this request, irrespective of the accounts being new or existing members. For more information about the existing auto-enable settings for your organization, see [DescribeOrganizationConfiguration](#).

If you disassociate a member account that was added by invitation, the member account details obtained from this API, including the associated email addresses, will be retained. This is done so that the delegated administrator can invoke the [InviteMembers](#) API without the need to invoke the `CreateMembers` API again. To remove the details associated with a member account, the delegated administrator must invoke the [DeleteMembers](#) API.

When the member accounts added through AWS Organizations are later disassociated, you (administrator) can't invite them by calling the `InviteMembers` API. You can create an association with these member accounts again only by calling the `CreateMembers` API.

## Request Syntax

```
POST /detector/detectorId/member HTTP/1.1
```

```
Content-type: application/json
```

```
{
  "accountDetails": [
    {
      "accountId": "string",
      "email": "string"
    }
  ]
}
```

## URI Request Parameters

The request uses the following URI parameters.

### [detectorId](#)

The unique ID of the detector of the GuardDuty account that you want to associate member accounts with.

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

## Request Body

The request accepts the following data in JSON format.

### [accountDetails](#)

A list of account ID and email address pairs of the accounts that you want to associate with the GuardDuty administrator account.

Type: Array of [AccountDetail](#) objects

Array Members: Minimum number of 1 item. Maximum number of 50 items.

Required: Yes

## Response Syntax

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

{
  "unprocessedAccounts": [
    {
      "accountId": "string",
      "result": "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.

### unprocessedAccounts

A list of objects that include the accountIds of the unprocessed accounts and a result string that explains why each was unprocessed.

Type: Array of [UnprocessedAccount](#) objects

Array Members: Minimum number of 0 items. Maximum number of 50 items.

## Errors

For information about the errors that are common to all actions, see [Common Errors](#).

### **BadRequestException**

A bad request exception object.

HTTP Status Code: 400

### **InternalServerErrorException**

An internal server error exception object.

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 v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

# CreatePublishingDestination

Creates a publishing destination to export findings to. The resource to export findings to must exist before you use this operation.

## Request Syntax

```
POST /detector/detectorId/publishingDestination HTTP/1.1
Content-type: application/json
```

```
{
  "clientToken": "string",
  "destinationProperties": {
    "destinationArn": "string",
    "kmsKeyArn": "string"
  },
  "destinationType": "string"
}
```

## URI Request Parameters

The request uses the following URI parameters.

### detectorId

The ID of the GuardDuty detector associated with the publishing destination.

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

## Request Body

The request accepts the following data in JSON format.

### clientToken

The idempotency token for the request.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 64.

Required: No

### destinationProperties

The properties of the publishing destination, including the ARNs for the destination and the KMS key used for encryption.

Type: [DestinationProperties](#) object

Required: Yes

### destinationType

The type of resource for the publishing destination. Currently only Amazon S3 buckets are supported.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 300.

Valid Values: S3

Required: Yes

## Response Syntax

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

{
  "destinationId": "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.

### destinationId

The ID of the publishing destination that is created.

Type: String

## Errors

For information about the errors that are common to all actions, see [Common Errors](#).

### **BadRequestException**

A bad request exception object.

HTTP Status Code: 400

### **InternalServerErrorException**

An internal server error exception object.

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 v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

# CreateSampleFindings

Generates sample findings of types specified by the list of finding types. If 'NULL' is specified for `findingTypes`, the API generates sample findings of all supported finding types.

## Request Syntax

```
POST /detector/detectorId/findings/create HTTP/1.1
Content-type: application/json

{
  "findingTypes": [ "string" ]
}
```

## URI Request Parameters

The request uses the following URI parameters.

### detectorId

The ID of the detector to create sample findings for.

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

## Request Body

The request accepts the following data in JSON format.

### findingTypes

The types of sample findings to generate.

Type: Array of strings

Array Members: Minimum number of 0 items. Maximum number of 50 items.

Length Constraints: Minimum length of 1. Maximum length of 50.

Required: No

## Response Syntax

```
HTTP/1.1 200
```

## Response Elements

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

## Errors

For information about the errors that are common to all actions, see [Common Errors](#).

### **BadRequestException**

A bad request exception object.

HTTP Status Code: 400

### **InternalServerErrorException**

An internal server error exception object.

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 v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)



# CreateThreatIntelSet

Creates a new ThreatIntelSet. ThreatIntelSets consist of known malicious IP addresses. GuardDuty generates findings based on ThreatIntelSets. Only users of the administrator account can use this operation.

## Request Syntax

```
POST /detector/detectorId/threatintelset HTTP/1.1
```

```
Content-type: application/json
```

```
{
  "activate": boolean,
  "clientToken": "string",
  "format": "string",
  "location": "string",
  "name": "string",
  "tags": {
    "string" : "string"
  }
}
```

## URI Request Parameters

The request uses the following URI parameters.

### detectorId

The unique ID of the detector of the GuardDuty account that you want to create a threatIntelSet for.

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

## Request Body

The request accepts the following data in JSON format.



## activate

A Boolean value that indicates whether GuardDuty is to start using the uploaded ThreatIntelSet.

Type: Boolean

Required: Yes

## clientToken

The idempotency token for the create request.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 64.

Required: No

## format

The format of the file that contains the ThreatIntelSet.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 300.

Valid Values: TXT | STIX | OTX\_CSV | ALIEN\_VAULT | PROOF\_POINT | FIRE\_EYE

Required: Yes

## location

The URI of the file that contains the ThreatIntelSet.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

## name

A user-friendly ThreatIntelSet name displayed in all findings that are generated by activity that involves IP addresses included in this ThreatIntelSet.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

## tags

The tags to be added to a new threat list resource.

Type: String to string map

Map Entries: Maximum number of 200 items.

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

Key Pattern:  $^(?!aws:)[a-zA-Z+ -= . _ : / ] + \$$

Value Length Constraints: Maximum length of 256.

Required: No

## Response Syntax

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

{
  "threatIntelSetId": "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.

### threatIntelSetId

The ID of the ThreatIntelSet resource.

Type: String

## Errors

For information about the errors that are common to all actions, see [Common Errors](#).

## **BadRequestException**

A bad request exception object.

HTTP Status Code: 400

## **InternalServerErrorException**

An internal server error exception object.

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 v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

# DeclineInvitations

Declines invitations sent to the current member account by AWS accounts specified by their account IDs.

## Request Syntax

```
POST /invitation/decline HTTP/1.1
Content-type: application/json

{
  "accountIds": [ "string" ]
}
```

## URI Request Parameters

The request does not use any URI parameters.

## Request Body

The request accepts the following data in JSON format.

### accountIds

A list of account IDs of the AWS accounts that sent invitations to the current member account that you want to decline invitations from.

Type: Array of strings

Array Members: Minimum number of 1 item. Maximum number of 50 items.

Length Constraints: Fixed length of 12.

Required: Yes

## Response Syntax

```
HTTP/1.1 200
```

```
Content-type: application/json
```

```
{
  "unprocessedAccounts": [
    {
      "accountId": "string",
      "result": "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.

### unprocessedAccounts

A list of objects that contain the unprocessed account and a result string that explains why it was unprocessed.

Type: Array of [UnprocessedAccount](#) objects

Array Members: Minimum number of 0 items. Maximum number of 50 items.

## Errors

For information about the errors that are common to all actions, see [Common Errors](#).

### **BadRequestException**

A bad request exception object.

HTTP Status Code: 400

### **InternalServerErrorException**

An internal server error exception object.

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 v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

# DeleteDetector

Deletes an Amazon GuardDuty detector that is specified by the detector ID.

## Request Syntax

```
DELETE /detector/detectorId HTTP/1.1
```

## URI Request Parameters

The request uses the following URI parameters.

### detectorId

The unique ID of the detector that you want to delete.

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

## Request Body

The request does not have a request body.

## Response Syntax

```
HTTP/1.1 200
```

## Response Elements

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

## Errors

For information about the errors that are common to all actions, see [Common Errors](#).

### BadRequestException

A bad request exception object.

HTTP Status Code: 400

## **InternalServerErrorException**

An internal server error exception object.

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 v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)



# DeleteFilter

Deletes the filter specified by the filter name.

## Request Syntax

```
DELETE /detector/detectorId/filter/filterName HTTP/1.1
```

## URI Request Parameters

The request uses the following URI parameters.

### detectorId

The unique ID of the detector that the filter is associated with.

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

### filterName

The name of the filter that you want to delete.

Required: Yes

## Request Body

The request does not have a request body.

## Response Syntax

```
HTTP/1.1 200
```

## Response Elements

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

## Errors

For information about the errors that are common to all actions, see [Common Errors](#).

## BadRequestException

A bad request exception object.

HTTP Status Code: 400

## InternalServerErrorException

An internal server error exception object.

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 v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

# DeleteInvitations

Deletes invitations sent to the current member account by AWS accounts specified by their account IDs.

## Request Syntax

```
POST /invitation/delete HTTP/1.1
Content-type: application/json

{
  "accountIds": [ "string" ]
}
```

## URI Request Parameters

The request does not use any URI parameters.

## Request Body

The request accepts the following data in JSON format.

### accountIds

A list of account IDs of the AWS accounts that sent invitations to the current member account that you want to delete invitations from.

Type: Array of strings

Array Members: Minimum number of 1 item. Maximum number of 50 items.

Length Constraints: Fixed length of 12.

Required: Yes

## Response Syntax

```
HTTP/1.1 200
```

```
Content-type: application/json
```

```
{
  "unprocessedAccounts": [
    {
      "accountId": "string",
      "result": "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.

### unprocessedAccounts

A list of objects that contain the unprocessed account and a result string that explains why it was unprocessed.

Type: Array of [UnprocessedAccount](#) objects

Array Members: Minimum number of 0 items. Maximum number of 50 items.

## Errors

For information about the errors that are common to all actions, see [Common Errors](#).

### **BadRequestException**

A bad request exception object.

HTTP Status Code: 400

### **InternalServerErrorException**

An internal server error exception object.

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 v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

# DeleteIPSet

Deletes the IPSet specified by the `ipSetId`. IPSets are called trusted IP lists in the console user interface.

## Request Syntax

```
DELETE /detector/detectorId/ipset/ipSetId HTTP/1.1
```

## URI Request Parameters

The request uses the following URI parameters.

### detectorId

The unique ID of the detector associated with the IPSet.

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

### ipSetId

The unique ID of the IPSet to delete.

Required: Yes

## Request Body

The request does not have a request body.

## Response Syntax

```
HTTP/1.1 200
```

## Response Elements

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

## Errors

For information about the errors that are common to all actions, see [Common Errors](#).

### BadRequestException

A bad request exception object.

HTTP Status Code: 400

### InternalServerErrorException

An internal server error exception object.

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 v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

# DeleteMalwareProtectionPlan

Deletes the Malware Protection plan ID associated with the Malware Protection plan resource. Use this API only when you no longer want to protect the resource associated with this Malware Protection plan ID.

## Request Syntax

```
DELETE /malware-protection-plan/malwareProtectionPlanId HTTP/1.1
```

## URI Request Parameters

The request uses the following URI parameters.

### malwareProtectionPlanId

A unique identifier associated with Malware Protection plan resource.

Required: Yes

## Request Body

The request does not have a request body.

## Response Syntax

```
HTTP/1.1 200
```

## Response Elements

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

## Errors

For information about the errors that are common to all actions, see [Common Errors](#).

### AccessDeniedException

An access denied exception object.



HTTP Status Code: 403

### **BadRequestException**

A bad request exception object.

HTTP Status Code: 400

### **InternalServerErrorException**

An internal server error exception object.

HTTP Status Code: 500

### **ResourceNotFoundException**

The requested resource can't be found.

HTTP Status Code: 404

## **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 v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

# DeleteMembers

Deletes GuardDuty member accounts (to the current GuardDuty administrator account) specified by the account IDs.

With `autoEnableOrganizationMembers` configuration for your organization set to ALL, you'll receive an error if you attempt to disable GuardDuty for a member account in your organization.

## Request Syntax

```
POST /detector/detectorId/member/delete HTTP/1.1
Content-type: application/json

{
  "accountIds": [ "string" ]
}
```

## URI Request Parameters

The request uses the following URI parameters.

### detectorId

The unique ID of the detector of the GuardDuty account whose members you want to delete.

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

## Request Body

The request accepts the following data in JSON format.

### accountIds

A list of account IDs of the GuardDuty member accounts that you want to delete.

Type: Array of strings

Array Members: Minimum number of 1 item. Maximum number of 50 items.

Length Constraints: Fixed length of 12.

Required: Yes

## Response Syntax

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

{
  "unprocessedAccounts": [
    {
      "accountId": "string",
      "result": "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.

### [unprocessedAccounts](#)

The accounts that could not be processed.

Type: Array of [UnprocessedAccount](#) objects

Array Members: Minimum number of 0 items. Maximum number of 50 items.

## Errors

For information about the errors that are common to all actions, see [Common Errors](#).

### BadRequestException

A bad request exception object.

HTTP Status Code: 400

## InternalServerErrorException

An internal server error exception object.

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 v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

# DeletePublishingDestination

Deletes the publishing definition with the specified `destinationId`.

## Request Syntax

```
DELETE /detector/detectorId/publishingDestination/destinationId HTTP/1.1
```

## URI Request Parameters

The request uses the following URI parameters.

### destinationId

The ID of the publishing destination to delete.

Required: Yes

### detectorId

The unique ID of the detector associated with the publishing destination to delete.

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

## Request Body

The request does not have a request body.

## Response Syntax

```
HTTP/1.1 200
```

## Response Elements

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

## Errors

For information about the errors that are common to all actions, see [Common Errors](#).

## **BadRequestException**

A bad request exception object.

HTTP Status Code: 400

## **InternalServerErrorException**

An internal server error exception object.

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 v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

# DeleteThreatIntelSet

Deletes the ThreatIntelSet specified by the ThreatIntelSet ID.

## Request Syntax

```
DELETE /detector/detectorId/threatintelset/threatIntelSetId HTTP/1.1
```

## URI Request Parameters

The request uses the following URI parameters.

### detectorId

The unique ID of the detector that the threatIntelSet is associated with.

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

### threatIntelSetId

The unique ID of the threatIntelSet that you want to delete.

Required: Yes

## Request Body

The request does not have a request body.

## Response Syntax

```
HTTP/1.1 200
```

## Response Elements

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

## Errors

For information about the errors that are common to all actions, see [Common Errors](#).

## BadRequestException

A bad request exception object.

HTTP Status Code: 400

## InternalServerErrorException

An internal server error exception object.

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 v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)



## DescribeMalwareScans

Returns a list of malware scans. Each member account can view the malware scans for their own accounts. An administrator can view the malware scans for all the member accounts.

There might be regional differences because some data sources might not be available in all the AWS Regions where GuardDuty is presently supported. For more information, see [Regions and endpoints](#).

### Request Syntax

```
POST /detector/detectorId/malware-scans HTTP/1.1
Content-type: application/json
```

```
{
  "filterCriteria": {
    "filterCriterion": [
      {
        "criterionKey": "string",
        "filterCondition": {
          "equalsValue": "string",
          "greaterThan": number,
          "lessThan": number
        }
      }
    ]
  },
  "maxResults": number,
  "nextToken": "string",
  "sortCriteria": {
    "attributeName": "string",
    "orderBy": "string"
  }
}
```

### URI Request Parameters

The request uses the following URI parameters.

#### [detectorId](#)

The unique ID of the detector that the request is associated with.

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

## Request Body

The request accepts the following data in JSON format.

### filterCriteria

Represents the criteria to be used in the filter for describing scan entries.

Type: [FilterCriteria](#) object

Required: No

### maxResults

You can use this parameter to indicate the maximum number of items that you want in the response. The default value is 50. The maximum value is 50.

Type: Integer

Valid Range: Minimum value of 1. Maximum value of 50.

Required: No

### nextToken

You can use this parameter when paginating results. Set the value of this parameter to null on your first call to the list action. For subsequent calls to the action, fill nextToken in the request with the value of NextToken from the previous response to continue listing data.

Type: String

Required: No

### sortCriteria

Represents the criteria used for sorting scan entries. The [attributeName](#) is required and it must be scanStartTime.

Type: [SortCriteria](#) object

Required: No

## Response Syntax

HTTP/1.1 200

Content-type: application/json

```
{
  "nextToken": "string",
  "scans": [
    {
      "accountId": "string",
      "adminDetectorId": "string",
      "attachedVolumes": [
        {
          "deviceName": "string",
          "encryptionType": "string",
          "kmsKeyArn": "string",
          "snapshotArn": "string",
          "volumeArn": "string",
          "volumeSizeInGB": number,
          "volumeType": "string"
        }
      ],
      "detectorId": "string",
      "failureReason": "string",
      "fileCount": number,
      "resourceDetails": {
        "instanceArn": "string"
      },
      "scanEndTime": number,
      "scanId": "string",
      "scanResultDetails": {
        "scanResult": "string"
      },
      "scanStartTime": number,
      "scanStatus": "string",
      "scanType": "string",
      "totalBytes": number,
      "triggerDetails": {
        "description": "string",
        "guardDutyFindingId": "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

The pagination parameter to be used on the next list operation to retrieve more items.

Type: String

### scans

Contains information about malware scans.

Type: Array of [Scan](#) objects

## Errors

For information about the errors that are common to all actions, see [Common Errors](#).

### **BadRequestException**

A bad request exception object.

HTTP Status Code: 400

### **InternalServerErrorException**

An internal server error exception object.

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 v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

# DescribeOrganizationConfiguration

Returns information about the account selected as the delegated administrator for GuardDuty.

There might be regional differences because some data sources might not be available in all the AWS Regions where GuardDuty is presently supported. For more information, see [Regions and endpoints](#).

## Request Syntax

```
GET /detector/detectorId/admin?maxResults=MaxResults&nextToken=NextToken HTTP/1.1
```

## URI Request Parameters

The request uses the following URI parameters.

### [detectorId](#)

The ID of the detector to retrieve information about the delegated administrator from.

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

### [MaxResults](#)

You can use this parameter to indicate the maximum number of items that you want in the response.

Valid Range: Minimum value of 1. Maximum value of 50.

### [NextToken](#)

You can use this parameter when paginating results. Set the value of this parameter to null on your first call to the list action. For subsequent calls to the action, fill `nextToken` in the request with the value of `NextToken` from the previous response to continue listing data.

## Request Body

The request does not have a request body.

## Response Syntax

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

{
  "autoEnable": boolean,
  "autoEnableOrganizationMembers": "string",
  "dataSources": {
    "kubernetes": {
      "auditLogs": {
        "autoEnable": boolean
      }
    },
    "malwareProtection": {
      "scanEc2InstanceWithFindings": {
        "ebsVolumes": {
          "autoEnable": boolean
        }
      }
    },
    "s3Logs": {
      "autoEnable": boolean
    }
  },
  "features": [
    {
      "additionalConfiguration": [
        {
          "autoEnable": "string",
          "name": "string"
        }
      ],
      "autoEnable": "string",
      "name": "string"
    }
  ],
  "memberAccountLimitReached": boolean,
  "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.

### autoEnable

*This parameter has been deprecated.*

Indicates whether GuardDuty is automatically enabled for accounts added to the organization.

Even though this is still supported, we recommend using `AutoEnableOrganizationMembers` to achieve the similar results.

Type: Boolean

### autoEnableOrganizationMembers

Indicates the auto-enablement configuration of GuardDuty or any of the corresponding protection plans for the member accounts in the organization.

- **NEW:** Indicates that when a new account joins the organization, they will have GuardDuty or any of the corresponding protection plans enabled automatically.
- **ALL:** Indicates that all accounts in the organization have GuardDuty and any of the corresponding protection plans enabled automatically. This includes NEW accounts that join the organization and accounts that may have been suspended or removed from the organization in GuardDuty.
- **NONE:** Indicates that GuardDuty or any of the corresponding protection plans will not be automatically enabled for any account in the organization. The administrator must manage GuardDuty for each account in the organization individually.

When you update the auto-enable setting from ALL or NEW to NONE, this action doesn't disable the corresponding option for your existing accounts. This configuration will apply to the new accounts that join the organization. After you update the auto-enable settings, no new account will have the corresponding option as enabled.

Type: String

Valid Values: NEW | ALL | NONE



## dataSources

*This parameter has been deprecated.*

Describes which data sources are enabled automatically for member accounts.

Type: [OrganizationDataSourceConfigurationsResult](#) object

## features

A list of features that are configured for this organization.

Type: Array of [OrganizationFeatureConfigurationResult](#) objects

## memberAccountLimitReached

Indicates whether the maximum number of allowed member accounts are already associated with the delegated administrator account for your organization.

Type: Boolean

## nextToken

The pagination parameter to be used on the next list operation to retrieve more items.

Type: String

## Errors

For information about the errors that are common to all actions, see [Common Errors](#).

### **BadRequestException**

A bad request exception object.

HTTP Status Code: 400

### **InternalServerErrorException**

An internal server error exception object.

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 v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

# DescribePublishingDestination

Returns information about the publishing destination specified by the provided `destinationId`.

## Request Syntax

```
GET /detector/detectorId/publishingDestination/destinationId HTTP/1.1
```

## URI Request Parameters

The request uses the following URI parameters.

### destinationId

The ID of the publishing destination to retrieve.

Required: Yes

### detectorId

The unique ID of the detector associated with the publishing destination to retrieve.

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

## Request Body

The request does not have a request body.

## Response Syntax

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

{
  "destinationId": "string",
  "destinationProperties": {
    "destinationArn": "string",
    "kmsKeyArn": "string"
  },
}
```

```
"destinationType": "string",  
"publishingFailureStartTimestamp": number,  
"status": "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.

### destinationId

The ID of the publishing destination.

Type: String

### destinationProperties

A `DestinationProperties` object that includes the `DestinationArn` and `KmsKeyArn` of the publishing destination.

Type: [DestinationProperties](#) object

### destinationType

The type of publishing destination. Currently, only Amazon S3 buckets are supported.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 300.

Valid Values: S3

### publishingFailureStartTimestamp

The time, in epoch millisecond format, at which GuardDuty was first unable to publish findings to the destination.

Type: Long

### status

The status of the publishing destination.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 300.

Valid Values: PENDING\_VERIFICATION | PUBLISHING |  
UNABLE\_TO\_PUBLISH\_FIX\_DESTINATION\_PROPERTY | STOPPED

## Errors

For information about the errors that are common to all actions, see [Common Errors](#).

### BadRequestException

A bad request exception object.

HTTP Status Code: 400

### InternalServerErrorException

An internal server error exception object.

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 v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

# DisableOrganizationAdminAccount

Removes the existing GuardDuty delegated administrator of the organization. Only the organization's management account can run this API operation.

## Request Syntax

```
POST /admin/disable HTTP/1.1
Content-type: application/json
```

```
{
  "adminAccountId": "string"
}
```

## URI Request Parameters

The request does not use any URI parameters.

## Request Body

The request accepts the following data in JSON format.

### adminAccountId

The AWS Account ID for the organizations account to be disabled as a GuardDuty delegated administrator.

Type: String

Required: Yes

## Response Syntax

```
HTTP/1.1 200
```

## Response Elements

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

## Errors

For information about the errors that are common to all actions, see [Common Errors](#).

### BadRequestException

A bad request exception object.

HTTP Status Code: 400

### InternalServerErrorException

An internal server error exception object.

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 v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

# DisassociateFromAdministratorAccount

Disassociates the current GuardDuty member account from its administrator account.

When you disassociate an invited member from a GuardDuty delegated administrator, the member account details obtained from the [CreateMembers](#) API, including the associated email addresses, are retained. This is done so that the delegated administrator can invoke the [InviteMembers](#) API without the need to invoke the CreateMembers API again. To remove the details associated with a member account, the delegated administrator must invoke the [DeleteMembers](#) API.

With `autoEnableOrganizationMembers` configuration for your organization set to ALL, you'll receive an error if you attempt to disable GuardDuty in a member account.

## Request Syntax

```
POST /detector/detectorId/administrator/disassociate HTTP/1.1
```

## URI Request Parameters

The request uses the following URI parameters.

### [detectorId](#)

The unique ID of the detector of the GuardDuty member account.

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

## Request Body

The request does not have a request body.

## Response Syntax

```
HTTP/1.1 200
```

## Response Elements

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



## Errors

For information about the errors that are common to all actions, see [Common Errors](#).

### **BadRequestException**

A bad request exception object.

HTTP Status Code: 400

### **InternalServerErrorException**

An internal server error exception object.

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 v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

# DisassociateFromMasterAccount

*This action has been deprecated.*

Disassociates the current GuardDuty member account from its administrator account.

When you disassociate an invited member from a GuardDuty delegated administrator, the member account details obtained from the [CreateMembers](#) API, including the associated email addresses, are retained. This is done so that the delegated administrator can invoke the [InviteMembers](#) API without the need to invoke the CreateMembers API again. To remove the details associated with a member account, the delegated administrator must invoke the [DeleteMembers](#) API.

## Request Syntax

```
POST /detector/detectorId/master/disassociate HTTP/1.1
```

## URI Request Parameters

The request uses the following URI parameters.

### [detectorId](#)

The unique ID of the detector of the GuardDuty member account.

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

## Request Body

The request does not have a request body.

## Response Syntax

```
HTTP/1.1 200
```

## Response Elements

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

## Errors

For information about the errors that are common to all actions, see [Common Errors](#).

### BadRequestException

A bad request exception object.

HTTP Status Code: 400

### InternalServerErrorException

An internal server error exception object.

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 v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

# DisassociateMembers

Disassociates GuardDuty member accounts (from the current administrator account) specified by the account IDs.

When you disassociate an invited member from a GuardDuty delegated administrator, the member account details obtained from the [CreateMembers](#) API, including the associated email addresses, are retained. This is done so that the delegated administrator can invoke the [InviteMembers](#) API without the need to invoke the CreateMembers API again. To remove the details associated with a member account, the delegated administrator must invoke the [DeleteMembers](#) API.

With `autoEnableOrganizationMembers` configuration for your organization set to ALL, you'll receive an error if you attempt to disassociate a member account before removing them from your organization.

If you disassociate a member account that was added by invitation, the member account details obtained from this API, including the associated email addresses, will be retained. This is done so that the delegated administrator can invoke the [InviteMembers](#) API without the need to invoke the CreateMembers API again. To remove the details associated with a member account, the delegated administrator must invoke the [DeleteMembers](#) API.

When the member accounts added through AWS Organizations are later disassociated, you (administrator) can't invite them by calling the InviteMembers API. You can create an association with these member accounts again only by calling the CreateMembers API.

## Request Syntax

```
POST /detector/detectorId/member/disassociate HTTP/1.1
```

```
Content-type: application/json
```

```
{
  "accountIds": [ "string" ]
}
```

## URI Request Parameters

The request uses the following URI parameters.

## detectorId

The unique ID of the detector of the GuardDuty account whose members you want to disassociate from the administrator account.

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

## Request Body

The request accepts the following data in JSON format.

### accountIds

A list of account IDs of the GuardDuty member accounts that you want to disassociate from the administrator account.

Type: Array of strings

Array Members: Minimum number of 1 item. Maximum number of 50 items.

Length Constraints: Fixed length of 12.

Required: Yes

## Response Syntax

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

```
{
  "unprocessedAccounts": [
    {
      "accountId": "string",
      "result": "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.

### unprocessedAccounts

A list of objects that contain the unprocessed account and a result string that explains why it was unprocessed.

Type: Array of [UnprocessedAccount](#) objects

Array Members: Minimum number of 0 items. Maximum number of 50 items.

## Errors

For information about the errors that are common to all actions, see [Common Errors](#).

### **BadRequestException**

A bad request exception object.

HTTP Status Code: 400

### **InternalServerErrorException**

An internal server error exception object.

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 v2](#)

- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

# EnableOrganizationAdminAccount

Designates an AWS account within the organization as your GuardDuty delegated administrator. Only the organization's management account can run this API operation.

## Request Syntax

```
POST /admin/enable HTTP/1.1
Content-type: application/json
```

```
{
  "adminAccountId": "string"
}
```

## URI Request Parameters

The request does not use any URI parameters.

## Request Body

The request accepts the following data in JSON format.

### [adminAccountId](#)

The AWS account ID for the organization account to be enabled as a GuardDuty delegated administrator.

Type: String

Required: Yes

## Response Syntax

```
HTTP/1.1 200
```

## Response Elements

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



## Errors

For information about the errors that are common to all actions, see [Common Errors](#).

### **BadRequestException**

A bad request exception object.

HTTP Status Code: 400

### **InternalServerErrorException**

An internal server error exception object.

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 v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

# GetAdministratorAccount

Provides the details of the GuardDuty administrator account associated with the current GuardDuty member account.

## Note

If the organization's management account or a delegated administrator runs this API, it will return success (HTTP 200) but no content.

## Request Syntax

```
GET /detector/detectorId/administrator HTTP/1.1
```

## URI Request Parameters

The request uses the following URI parameters.

### detectorId

The unique ID of the detector of the GuardDuty member account.

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

## Request Body

The request does not have a request body.

## Response Syntax

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

{
  "administrator": {
    "accountId": "string",
```

```
  "invitationId": "string",  
  "invitedAt": "string",  
  "relationshipStatus": "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.

### administrator

The administrator account details.

Type: [Administrator](#) object

## Errors

For information about the errors that are common to all actions, see [Common Errors](#).

### **BadRequestException**

A bad request exception object.

HTTP Status Code: 400

### **InternalServerErrorException**

An internal server error exception object.

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 v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

# GetCoverageStatistics

Retrieves aggregated statistics for your account. If you are a GuardDuty administrator, you can retrieve the statistics for all the resources associated with the active member accounts in your organization who have enabled Runtime Monitoring and have the GuardDuty security agent running on their resources.

## Request Syntax

```
POST /detector/detectorId/coverage/statistics HTTP/1.1
```

```
Content-type: application/json
```

```
{
  "filterCriteria": {
    "filterCriterion": [
      {
        "criterionKey": "string",
        "filterCondition": {
          "equals": [ "string" ],
          "notEquals": [ "string" ]
        }
      }
    ]
  },
  "statisticsType": [ "string" ]
}
```

## URI Request Parameters

The request uses the following URI parameters.

### detectorId

The unique ID of the GuardDuty detector associated to the coverage statistics.

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

## Request Body

The request accepts the following data in JSON format.

### filterCriteria

Represents the criteria used to filter the coverage statistics

Type: [CoverageFilterCriteria](#) object

Required: No

### statisticsType

Represents the statistics type used to aggregate the coverage details.

Type: Array of strings

Valid Values: COUNT\_BY\_RESOURCE\_TYPE | COUNT\_BY\_COVERAGE\_STATUS

Required: Yes

## Response Syntax

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

{
  "coverageStatistics": {
    "countByCoverageStatus": {
      "string" : number
    },
    "countByResourceType": {
      "string" : 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.

### coverageStatistics

Represents the count aggregated by the `statusCode` and `resourceType`.

Type: [CoverageStatistics](#) object

## Errors

For information about the errors that are common to all actions, see [Common Errors](#).

### BadRequestException

A bad request exception object.

HTTP Status Code: 400

### InternalServerErrorException

An internal server error exception object.

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 v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)





# GetDetector

Retrieves an Amazon GuardDuty detector specified by the detectorId.

There might be regional differences because some data sources might not be available in all the AWS Regions where GuardDuty is presently supported. For more information, see [Regions and endpoints](#).

## Request Syntax

```
GET /detector/detectorId HTTP/1.1
```

## URI Request Parameters

The request uses the following URI parameters.

### [detectorId](#)

The unique ID of the detector that you want to get.

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

## Request Body

The request does not have a request body.

## Response Syntax

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

```
{  
  "createdAt": "string",  
  "dataSources": {  
    "cloudTrail": {  
      "status": "string"  
    },  
    "dnsLogs": {  
      "status": "string"  
    }  
  }  
}
```

```
    },
    "flowLogs": {
      "status": "string"
    },
    "kubernetes": {
      "auditLogs": {
        "status": "string"
      }
    },
    "malwareProtection": {
      "scanEc2InstanceWithFindings": {
        "ebsVolumes": {
          "reason": "string",
          "status": "string"
        }
      },
      "serviceRole": "string"
    },
    "s3Logs": {
      "status": "string"
    }
  },
  "features": [
    {
      "additionalConfiguration": [
        {
          "name": "string",
          "status": "string",
          "updatedAt": number
        }
      ],
      "name": "string",
      "status": "string",
      "updatedAt": number
    }
  ],
  "findingPublishingFrequency": "string",
  "serviceRole": "string",
  "status": "string",
  "tags": {
    "string" : "string"
  },
  "updatedAt": "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.

### createdAt

The timestamp of when the detector was created.

Type: String

### dataSources

*This parameter has been deprecated.*

Describes which data sources are enabled for the detector.

Type: [DataSourceConfigurationsResult](#) object

### features

Describes the features that have been enabled for the detector.

Type: Array of [DetectorFeatureConfigurationResult](#) objects

### findingPublishingFrequency

The publishing frequency of the finding.

Type: String

Valid Values: FIFTEEN\_MINUTES | ONE\_HOUR | SIX\_HOURS

### serviceRole

The GuardDuty service role.

Type: String

### status

The detector status.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 300.

Valid Values: ENABLED | DISABLED

### tags

The tags of the detector resource.

Type: String to string map

Map Entries: Maximum number of 200 items.

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

Key Pattern: `^(?!aws:)[a-zA-Z+ -= . _ : / ]+$`

Value Length Constraints: Maximum length of 256.

### updatedAt

The last-updated timestamp for the detector.

Type: String

## Errors

For information about the errors that are common to all actions, see [Common Errors](#).

### **BadRequestException**

A bad request exception object.

HTTP Status Code: 400

### **InternalServerErrorException**

An internal server error exception object.

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 v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

# GetFilter

Returns the details of the filter specified by the filter name.

## Request Syntax

```
GET /detector/detectorId/filter/filterName HTTP/1.1
```

## URI Request Parameters

The request uses the following URI parameters.

### detectorId

The unique ID of the detector that the filter is associated with.

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

### filterName

The name of the filter you want to get.

Required: Yes

## Request Body

The request does not have a request body.

## Response Syntax

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

{
  "action": "string",
  "description": "string",
  "findingCriteria": {
    "criterion": {
```

```
    "string" : {
      "eq": [ "string" ],
      "equals": [ "string" ],
      "greaterThan": number,
      "greaterThanOrEqual": number,
      "gt": number,
      "gte": number,
      "lessThan": number,
      "lessThanOrEqual": number,
      "lt": number,
      "lte": number,
      "neq": [ "string" ],
      "notEquals": [ "string" ]
    }
  },
  "name": "string",
  "rank": number,
  "tags": {
    "string" : "string"
  }
}
```

## Response Elements

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

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

### action

Specifies the action that is to be applied to the findings that match the filter.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 300.

Valid Values: NOOP | ARCHIVE

### description

The description of the filter.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 512.

### findingCriteria

Represents the criteria to be used in the filter for querying findings.

Type: [FindingCriteria](#) object

#### name

The name of the filter.

Type: String

Length Constraints: Minimum length of 3. Maximum length of 64.

#### rank

Specifies the position of the filter in the list of current filters. Also specifies the order in which this filter is applied to the findings.

Type: Integer

Valid Range: Minimum value of 1. Maximum value of 100.

#### tags

The tags of the filter resource.

Type: String to string map

Map Entries: Maximum number of 200 items.

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

Key Pattern: `^(?!aws:)[a-zA-Z+ -= . _ : / ]+$`

Value Length Constraints: Maximum length of 256.

## Errors

For information about the errors that are common to all actions, see [Common Errors](#).

### **BadRequestException**

A bad request exception object.



HTTP Status Code: 400

## **InternalServerErrorException**

An internal server error exception object.

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 v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

# GetFindings

Describes Amazon GuardDuty findings specified by finding IDs.

## Request Syntax

```
POST /detector/detectorId/findings/get HTTP/1.1
Content-type: application/json
```

```
{
  "findingIds": [ "string" ],
  "sortCriteria": {
    "attributeName": "string",
    "orderBy": "string"
  }
}
```

## URI Request Parameters

The request uses the following URI parameters.

### detectorId

The ID of the detector that specifies the GuardDuty service whose findings you want to retrieve.

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

## Request Body

The request accepts the following data in JSON format.

### findingIds

The IDs of the findings that you want to retrieve.

Type: Array of strings

Array Members: Minimum number of 0 items. Maximum number of 50 items.

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

## [sortCriteria](#)

Represents the criteria used for sorting findings.

Type: [SortCriteria](#) object

Required: No

## Response Syntax

```
HTTP/1.1 200
```

```
Content-type: application/json
```

```
{
  "findings": [
    {
      "accountId": "string",
      "arn": "string",
      "confidence": number,
      "createdAt": "string",
      "description": "string",
      "id": "string",
      "partition": "string",
      "region": "string",
      "resource": {
        "accessKeyDetails": {
          "accessKeyId": "string",
          "principalId": "string",
          "userName": "string",
          "userType": "string"
        },
        "containerDetails": {
          "containerRuntime": "string",
          "id": "string",
          "image": "string",
          "imagePrefix": "string",
          "name": "string",
          "securityContext": {
            "allowPrivilegeEscalation": boolean,
            "privileged": boolean
          }
        }
      }
    }
  ]
}
```

```
    "volumeMounts": [
      {
        "mountPath": "string",
        "name": "string"
      }
    ],
  },
  "ebsVolumeDetails": {
    "scannedVolumeDetails": [
      {
        "deviceName": "string",
        "encryptionType": "string",
        "kmsKeyArn": "string",
        "snapshotArn": "string",
        "volumeArn": "string",
        "volumeSizeInGB": number,
        "volumeType": "string"
      }
    ],
    "skippedVolumeDetails": [
      {
        "deviceName": "string",
        "encryptionType": "string",
        "kmsKeyArn": "string",
        "snapshotArn": "string",
        "volumeArn": "string",
        "volumeSizeInGB": number,
        "volumeType": "string"
      }
    ]
  },
  "ecsClusterDetails": {
    "activeServicesCount": number,
    "arn": "string",
    "name": "string",
    "registeredContainerInstancesCount": number,
    "runningTasksCount": number,
    "status": "string",
    "tags": [
      {
        "key": "string",
        "value": "string"
      }
    ]
  },
],
```

```
"taskDetails": {
  "arn": "string",
  "containers": [
    {
      "containerRuntime": "string",
      "id": "string",
      "image": "string",
      "imagePrefix": "string",
      "name": "string",
      "securityContext": {
        "allowPrivilegeEscalation": boolean,
        "privileged": boolean
      },
      "volumeMounts": [
        {
          "mountPath": "string",
          "name": "string"
        }
      ]
    }
  ],
  "definitionArn": "string",
  "group": "string",
  "startedAt": number,
  "startedBy": "string",
  "tags": [
    {
      "key": "string",
      "value": "string"
    }
  ],
  "createdAt": number,
  "version": "string",
  "volumes": [
    {
      "hostPath": {
        "path": "string"
      },
      "name": "string"
    }
  ]
},
"eksClusterDetails": {
```

```
"arn": "string",
"createdAt": number,
"name": "string",
"status": "string",
"tags": [
  {
    "key": "string",
    "value": "string"
  }
],
"vpcId": "string"
},
"instanceDetails": {
  "availabilityZone": "string",
  "iamInstanceProfile": {
    "arn": "string",
    "id": "string"
  },
  "imageDescription": "string",
  "imageId": "string",
  "instanceId": "string",
  "instanceState": "string",
  "instanceType": "string",
  "launchTime": "string",
  "networkInterfaces": [
    {
      "ipv6Addresses": [ "string" ],
      "networkInterfaceId": "string",
      "privateDnsName": "string",
      "privateIpAddress": "string",
      "privateIpAddresses": [
        {
          "privateDnsName": "string",
          "privateIpAddress": "string"
        }
      ],
      "publicDnsName": "string",
      "publicIp": "string",
      "securityGroups": [
        {
          "groupId": "string",
          "groupName": "string"
        }
      ]
    }
  ],

```

```
        "subnetId": "string",
        "vpcId": "string"
    }
],
"outpostArn": "string",
"platform": "string",
"productCodes": [
    {
        "productCodeId": "string",
        "productCodeType": "string"
    }
],
"tags": [
    {
        "key": "string",
        "value": "string"
    }
]
},
"kubernetesDetails": {
    "kubernetesUserDetails": {
        "groups": [ "string" ],
        "impersonatedUser": {
            "groups": [ "string" ],
            "username": "string"
        },
        "sessionName": [ "string" ],
        "uid": "string",
        "username": "string"
    },
    "kubernetesWorkloadDetails": {
        "containers": [
            {
                "containerRuntime": "string",
                "id": "string",
                "image": "string",
                "imagePrefix": "string",
                "name": "string",
                "securityContext": {
                    "allowPrivilegeEscalation": boolean,
                    "privileged": boolean
                },
                "volumeMounts": [
                    {
```

```
        "mountPath": "string",
        "name": "string"
      }
    ]
  },
  "hostIPC": boolean,
  "hostNetwork": boolean,
  "hostPID": boolean,
  "name": "string",
  "namespace": "string",
  "serviceAccountName": "string",
  "type": "string",
  "uid": "string",
  "volumes": [
    {
      "hostPath": {
        "path": "string"
      },
      "name": "string"
    }
  ]
},
"lambdaDetails": {
  "description": "string",
  "functionArn": "string",
  "functionName": "string",
  "functionVersion": "string",
  "lastModifiedAt": number,
  "revisionId": "string",
  "role": "string",
  "tags": [
    {
      "key": "string",
      "value": "string"
    }
  ],
  "vpcConfig": {
    "securityGroups": [
      {
        "groupId": "string",
        "groupName": "string"
      }
    ]
  }
}
```



```
    ],
    "subnetIds": [ "string" ],
    "vpcId": "string"
  }
},
"rdsDbInstanceDetails": {
  "dbClusterIdentifier": "string",
  "dbInstanceArn": "string",
  "dbInstanceIdentifier": "string",
  "engine": "string",
  "engineVersion": "string",
  "tags": [
    {
      "key": "string",
      "value": "string"
    }
  ]
},
"rdsDbUserDetails": {
  "application": "string",
  "authMethod": "string",
  "database": "string",
  "ssl": "string",
  "user": "string"
},
"resourceType": "string",
"s3BucketDetails": [
  {
    "arn": "string",
    "createdAt": number,
    "defaultServerSideEncryption": {
      "encryptionType": "string",
      "kmsMasterKeyArn": "string"
    },
    "name": "string",
    "owner": {
      "id": "string"
    },
    "publicAccess": {
      "effectivePermission": "string",
      "permissionConfiguration": {
        "accountLevelPermissions": {
          "blockPublicAccess": {
            "blockPublicAcls": boolean,
```

```
        "blockPublicPolicy": boolean,
        "ignorePublicAcls": boolean,
        "restrictPublicBuckets": boolean
    }
},
"bucketLevelPermissions": {
    "accessControlList": {
        "allowsPublicReadAccess": boolean,
        "allowsPublicWriteAccess": boolean
    },
    "blockPublicAccess": {
        "blockPublicAcls": boolean,
        "blockPublicPolicy": boolean,
        "ignorePublicAcls": boolean,
        "restrictPublicBuckets": boolean
    },
    "bucketPolicy": {
        "allowsPublicReadAccess": boolean,
        "allowsPublicWriteAccess": boolean
    }
}
},
"s3ObjectDetails": [
    {
        "eTag": "string",
        "hash": "string",
        "key": "string",
        "objectArn": "string",
        "versionId": "string"
    }
],
"tags": [
    {
        "key": "string",
        "value": "string"
    }
],
"type": "string"
}
]
},
"schemaVersion": "string",
"service": {
```

```
"action": {
  "actionType": "string",
  "awsApiCallAction": {
    "affectedResources": {
      "string" : "string"
    },
    "api": "string",
    "callerType": "string",
    "domainDetails": {
      "domain": "string"
    },
    "errorCode": "string",
    "remoteAccountDetails": {
      "accountId": "string",
      "affiliated": boolean
    },
    "remoteIpDetails": {
      "city": {
        "cityName": "string"
      },
      "country": {
        "countryCode": "string",
        "countryName": "string"
      },
      "geoLocation": {
        "lat": number,
        "lon": number
      },
      "ipAddressV4": "string",
      "ipAddressV6": "string",
      "organization": {
        "asn": "string",
        "asnOrg": "string",
        "isp": "string",
        "org": "string"
      }
    },
    "serviceName": "string",
    "userAgent": "string"
  },
  "dnsRequestAction": {
    "blocked": boolean,
    "domain": "string",
    "domainWithSuffix": "string",
```

```
    "protocol": "string"
  },
  "kubernetesApiCallAction": {
    "namespace": "string",
    "parameters": "string",
    "remoteIpDetails": {
      "city": {
        "cityName": "string"
      },
      "country": {
        "countryCode": "string",
        "countryName": "string"
      },
      "geoLocation": {
        "lat": number,
        "lon": number
      },
      "ipAddressV4": "string",
      "ipAddressV6": "string",
      "organization": {
        "asn": "string",
        "asnOrg": "string",
        "isp": "string",
        "org": "string"
      }
    },
    "requestUri": "string",
    "resource": "string",
    "resourceName": "string",
    "sourceIps": [ "string" ],
    "statusCode": number,
    "subresource": "string",
    "userAgent": "string",
    "verb": "string"
  },
  "kubernetesPermissionCheckedDetails": {
    "allowed": boolean,
    "namespace": "string",
    "resource": "string",
    "verb": "string"
  },
  "kubernetesRoleBindingDetails": {
    "kind": "string",
    "name": "string",
```

```
    "roleRefKind": "string",
    "roleRefName": "string",
    "uid": "string"
  },
  "kubernetesRoleDetails": {
    "kind": "string",
    "name": "string",
    "uid": "string"
  },
  "networkConnectionAction": {
    "blocked": boolean,
    "connectionDirection": "string",
    "localIpDetails": {
      "ipAddressV4": "string",
      "ipAddressV6": "string"
    },
    "localPortDetails": {
      "port": number,
      "portName": "string"
    },
    "protocol": "string",
    "remoteIpDetails": {
      "city": {
        "cityName": "string"
      },
      "country": {
        "countryCode": "string",
        "countryName": "string"
      },
      "geoLocation": {
        "lat": number,
        "lon": number
      },
      "ipAddressV4": "string",
      "ipAddressV6": "string",
      "organization": {
        "asn": "string",
        "asnOrg": "string",
        "isp": "string",
        "org": "string"
      }
    },
    "remotePortDetails": {
      "port": number,
```

```
        "portName": "string"
    }
},
"portProbeAction": {
    "blocked": boolean,
    "portProbeDetails": [
        {
            "localIpDetails": {
                "ipAddressV4": "string",
                "ipAddressV6": "string"
            },
            "localPortDetails": {
                "port": number,
                "portName": "string"
            },
            "remoteIpDetails": {
                "city": {
                    "cityName": "string"
                },
                "country": {
                    "countryCode": "string",
                    "countryName": "string"
                },
                "geoLocation": {
                    "lat": number,
                    "lon": number
                },
                "ipAddressV4": "string",
                "ipAddressV6": "string",
                "organization": {
                    "asn": "string",
                    "asnOrg": "string",
                    "isp": "string",
                    "org": "string"
                }
            }
        }
    ]
},
"rdsLoginAttemptAction": {
    "LoginAttributes": [
        {
            "application": "string",
            "failedLoginAttempts": number,
```

```
        "successfulLoginAttempts": number,
        "user": "string"
    }
],
"remoteIpDetails": {
    "city": {
        "cityName": "string"
    },
    "country": {
        "countryCode": "string",
        "countryName": "string"
    },
    "geoLocation": {
        "lat": number,
        "lon": number
    },
    "ipAddressV4": "string",
    "ipAddressV6": "string",
    "organization": {
        "asn": "string",
        "asnOrg": "string",
        "isp": "string",
        "org": "string"
    }
}
}
},
"additionalInfo": {
    "type": "string",
    "value": "string"
},
"archived": boolean,
"count": number,
"detection": {
    "anomaly": {
        "profiles": {
            "string" : {
                "string" : [
                    {
                        "observations": {
                            "text": [ "string" ]
                        },
                        "profileSubtype": "string",
                        "profileType": "string"
                    }
                ]
            }
        }
    }
}
```

```

    }
  ]
}
},
"unusual": {
  "behavior": {
    "string" : {
      "string" : {
        "observations": {
          "text": [ "string" ]
        },
        "profileSubtype": "string",
        "profileType": "string"
      }
    }
  }
}
},
"detectorId": "string",
"ebsVolumeScanDetails": {
  "scanCompletedAt": number,
  "scanDetections": {
    "highestSeverityThreatDetails": {
      "count": number,
      "severity": "string",
      "threatName": "string"
    },
    "scannedItemCount": {
      "files": number,
      "totalGb": number,
      "volumes": number
    },
    "threatDetectedByName": {
      "itemCount": number,
      "shortened": boolean,
      "threatNames": [
        {
          "filePaths": [
            {
              "fileName": "string",
              "filePath": "string",
              "hash": "string",
              "volumeArn": "string"
            }
          ]
        }
      ]
    }
  }
}
}

```



```
        }
      ],
      "itemCount": number,
      "name": "string",
      "severity": "string"
    }
  ],
  "uniqueThreatNameCount": number
},
"threatsDetectedItemCount": {
  "files": number
}
},
"scanId": "string",
"scanStartedAt": number,
"scanType": "string",
"sources": [ "string " ],
"triggerFindingId": "string"
},
"eventFirstSeen": "string",
"eventLastSeen": "string",
"evidence": {
  "threatIntelligenceDetails": [
    {
      "threatFileSha256": "string",
      "threatListName": "string",
      "threatNames": [ "string " ]
    }
  ]
},
"featureName": "string",
"malwareScanDetails": {
  "threats": [
    {
      "itemPaths": [
        {
          "hash": "string",
          "nestedItemPath": "string"
        }
      ],
      "name": "string",
      "source": "string"
    }
  ]
}
```

```
},
  "resourceRole": "string",
  "runtimeDetails": {
    "context": {
      "addressFamily": "string",
      "commandLineExample": "string",
      "fileSystemType": "string",
      "flags": [ "string" ],
      "ianaProtocolNumber": number,
      "ldPreloadValue": "string",
      "libraryPath": "string",
      "memoryRegions": [ "string" ],
      "modifiedAt": number,
      "modifyingProcess": {
        "euid": number,
        "executablePath": "string",
        "executableSha256": "string",
        "lineage": [
          {
            "euid": number,
            "executablePath": "string",
            "name": "string",
            "namespacePid": number,
            "parentUuid": "string",
            "pid": number,
            "startTime": number,
            "userId": number,
            "uuid": "string"
          }
        ],
        "name": "string",
        "namespacePid": number,
        "parentUuid": "string",
        "pid": number,
        "pwd": "string",
        "startTime": number,
        "user": "string",
        "userId": number,
        "uuid": "string"
      },
      "moduleFilePath": "string",
      "moduleName": "string",
      "moduleSha256": "string",
      "mountSource": "string",
```

```
"mountTarget": "string",
"releaseAgentPath": "string",
"runcBinaryPath": "string",
"scriptPath": "string",
"serviceName": "string",
"shellHistoryFilePath": "string",
"socketPath": "string",
"targetProcess": {
  "euid": number,
  "executablePath": "string",
  "executableSha256": "string",
  "lineage": [
    {
      "euid": number,
      "executablePath": "string",
      "name": "string",
      "namespacePid": number,
      "parentUuid": "string",
      "pid": number,
      "startTime": number,
      "userId": number,
      "uuid": "string"
    }
  ],
  "name": "string",
  "namespacePid": number,
  "parentUuid": "string",
  "pid": number,
  "pwd": "string",
  "startTime": number,
  "user": "string",
  "userId": number,
  "uuid": "string"
},
"threatFilePath": "string",
"toolCategory": "string",
"toolName": "string"
},
"process": {
  "euid": number,
  "executablePath": "string",
  "executableSha256": "string",
  "lineage": [
    {
```

```
        "uuid": number,
        "executablePath": "string",
        "name": "string",
        "namespacePid": number,
        "parentUuid": "string",
        "pid": number,
        "startTime": number,
        "userId": number,
        "uuid": "string"
    }
],
"namespacePid": number,
"parentUuid": "string",
"pid": number,
"pwd": "string",
"startTime": number,
"user": "string",
"userId": number,
"uuid": "string"
}
},
"serviceName": "string",
"userFeedback": "string"
},
"severity": number,
"title": "string",
"type": "string",
"updatedAt": "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.

### findings

A list of findings.

Type: Array of [Finding](#) objects

Array Members: Minimum number of 0 items. Maximum number of 50 items.

## Errors

For information about the errors that are common to all actions, see [Common Errors](#).

### BadRequestException

A bad request exception object.

HTTP Status Code: 400

### InternalServerErrorException

An internal server error exception object.

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 v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

# GetFindingsStatistics

Lists Amazon GuardDuty findings statistics for the specified detector ID.

There might be regional differences because some flags might not be available in all the Regions where GuardDuty is currently supported. For more information, see [Regions and endpoints](#).

## Request Syntax

```
POST /detector/detectorId/findings/statistics HTTP/1.1
```

```
Content-type: application/json
```

```
{
  "findingCriteria": {
    "criterion": {
      "string" : {
        "eq": [ "string" ],
        "equals": [ "string" ],
        "greaterThan": number,
        "greaterThanOrEqual": number,
        "gt": number,
        "gte": number,
        "lessThan": number,
        "lessThanOrEqual": number,
        "lt": number,
        "lte": number,
        "neq": [ "string" ],
        "notEquals": [ "string" ]
      }
    }
  },
  "findingStatisticTypes": [ "string" ]
}
```

## URI Request Parameters

The request uses the following URI parameters.

### [detectorId](#)

The ID of the detector that specifies the GuardDuty service whose findings' statistics you want to retrieve.

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

## Request Body

The request accepts the following data in JSON format.

### findingCriteria

Represents the criteria that is used for querying findings.

Type: [FindingCriteria](#) object

Required: No

### findingStatisticTypes

The types of finding statistics to retrieve.

Type: Array of strings

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

Valid Values: COUNT\_BY\_SEVERITY

Required: Yes

## Response Syntax

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

{
  "findingStatistics": {
    "countBySeverity": {
      "string" : 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.

### [findingStatistics](#)

The finding statistics object.

Type: [FindingStatistics](#) object

## Errors

For information about the errors that are common to all actions, see [Common Errors](#).

### **BadRequestException**

A bad request exception object.

HTTP Status Code: 400

### **InternalServerErrorException**

An internal server error exception object.

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 v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript V3](#)



- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

# GetInvitationsCount

Returns the count of all GuardDuty membership invitations that were sent to the current member account except the currently accepted invitation.

## Request Syntax

```
GET /invitation/count HTTP/1.1
```

## URI Request Parameters

The request does not use any URI parameters.

## Request Body

The request does not have a request body.

## Response Syntax

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

{
  "invitationsCount": 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.

### [invitationsCount](#)

The number of received invitations.

Type: Integer

## Errors

For information about the errors that are common to all actions, see [Common Errors](#).

### **BadRequestException**

A bad request exception object.

HTTP Status Code: 400

### **InternalServerErrorException**

An internal server error exception object.

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 v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

# GetIPSet

Retrieves the IPSet specified by the `ipSetId`.

## Request Syntax

```
GET /detector/detectorId/ipset/ipSetId HTTP/1.1
```

## URI Request Parameters

The request uses the following URI parameters.

### detectorId

The unique ID of the detector that the IPSet is associated with.

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

### ipSetId

The unique ID of the IPSet to retrieve.

Required: Yes

## Request Body

The request does not have a request body.

## Response Syntax

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

{
  "format": "string",
  "location": "string",
  "name": "string",
  "status": "string",
```

```
"tags": {  
  "string" : "string"  
}  
}
```

## Response Elements

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

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

### format

The format of the file that contains the IPSet.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 300.

Valid Values: TXT | STIX | OTX\_CSV | ALIEN\_VAULT | PROOF\_POINT | FIRE\_EYE

### location

The URI of the file that contains the IPSet.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 300.

### name

The user-friendly name for the IPSet.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 300.

### status

The status of IPSet file that was uploaded.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 300.

Valid Values: INACTIVE | ACTIVATING | ACTIVE | DEACTIVATING | ERROR | DELETE\_PENDING | DELETED

## tags

The tags of the IPSet resource.

Type: String to string map

Map Entries: Maximum number of 200 items.

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

Key Pattern: `^(?!aws:)[a-zA-Z+-. _:/]+`

Value Length Constraints: Maximum length of 256.

## Errors

For information about the errors that are common to all actions, see [Common Errors](#).

### BadRequestException

A bad request exception object.

HTTP Status Code: 400

### InternalServerErrorException

An internal server error exception object.

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 v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

# GetMalwareProtectionPlan

Retrieves the Malware Protection plan details associated with a Malware Protection plan ID.

## Request Syntax

```
GET /malware-protection-plan/malwareProtectionPlanId HTTP/1.1
```

## URI Request Parameters

The request uses the following URI parameters.

### malwareProtectionPlanId

A unique identifier associated with Malware Protection plan resource.

Required: Yes

## Request Body

The request does not have a request body.

## Response Syntax

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

{
  "actions": {
    "tagging": {
      "status": "string"
    }
  },
  "arn": "string",
  "createdAt": number,
  "protectedResource": {
    "s3Bucket": {
      "bucketName": "string",
      "objectPrefixes": [ "string" ]
    }
  }
}
```



```
},
  "role": "string",
  "status": "string",
  "statusReasons": [
    {
      "code": "string",
      "message": "string"
    }
  ],
  "tags": {
    "string" : "string"
  }
}
```

## Response Elements

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

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

### actions

Information about whether the tags will be added to the S3 object after scanning.

Type: [MalwareProtectionPlanActions](#) object

### arn

Amazon Resource Name (ARN) of the protected resource.

Type: String

### createdAt

The timestamp when the Malware Protection plan resource was created.

Type: Timestamp

### protectedResource

Information about the protected resource that is associated with the created Malware Protection plan. Presently, S3Bucket is the only supported protected resource.

Type: [CreateProtectedResource](#) object

## role

IAM role that includes the permissions required to scan and add tags to the associated protected resource.

Type: String

## status

Malware Protection plan status.

Type: String

Valid Values: ACTIVE | WARNING | ERROR

## statusReasons

Information about the issue code and message associated to the status of your Malware Protection plan.

Type: Array of [MalwareProtectionPlanStatusReason](#) objects

Array Members: Minimum number of 0 items. Maximum number of 50 items.

## tags

Tags added to the Malware Protection plan resource.

Type: String to string map

Map Entries: Maximum number of 200 items.

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

Key Pattern: `^(?!aws:)[a-zA-Z+-._: /]+`

Value Length Constraints: Maximum length of 256.

## Errors

For information about the errors that are common to all actions, see [Common Errors](#).

### AccessDeniedException

An access denied exception object.

HTTP Status Code: 403

### **BadRequestException**

A bad request exception object.

HTTP Status Code: 400

### **InternalServerErrorException**

An internal server error exception object.

HTTP Status Code: 500

### **ResourceNotFoundException**

The requested resource can't be found.

HTTP Status Code: 404

## **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 v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

# GetMalwareScanSettings

Returns the details of the malware scan settings.

There might be regional differences because some data sources might not be available in all the AWS Regions where GuardDuty is presently supported. For more information, see [Regions and endpoints](#).

## Request Syntax

```
GET /detector/detectorId/malware-scan-settings HTTP/1.1
```

## URI Request Parameters

The request uses the following URI parameters.

### [detectorId](#)

The unique ID of the detector that the scan setting is associated with.

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

## Request Body

The request does not have a request body.

## Response Syntax

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

{
  "ebsSnapshotPreservation": "string",
  "scanResourceCriteria": {
    "exclude": {
      "string": {
        "mapEquals": [
```

```
    {
      "key": "string",
      "value": "string"
    }
  ]
},
"include": {
  "string": {
    "mapEquals": [
      {
        "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.

### [ebsSnapshotPreservation](#)

An enum value representing possible snapshot preservation settings.

Type: String

Valid Values: NO\_RETENTION | RETENTION\_WITH\_FINDING

### [scanResourceCriteria](#)

Represents the criteria to be used in the filter for scanning resources.

Type: [ScanResourceCriteria](#) object

## Errors

For information about the errors that are common to all actions, see [Common Errors](#).

## BadRequestException

A bad request exception object.

HTTP Status Code: 400

## InternalServerErrorException

An internal server error exception object.

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 v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

# GetMasterAccount

*This action has been deprecated.*

Provides the details for the GuardDuty administrator account associated with the current GuardDuty member account.

## Request Syntax

```
GET /detector/detectorId/master HTTP/1.1
```

## URI Request Parameters

The request uses the following URI parameters.

### detectorId

The unique ID of the detector of the GuardDuty member account.

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

## Request Body

The request does not have a request body.

## Response Syntax

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

{
  "master": {
    "accountId": "string",
    "invitationId": "string",
    "invitedAt": "string",
    "relationshipStatus": "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.

### master

The administrator account details.

Type: [Master](#) object

## Errors

For information about the errors that are common to all actions, see [Common Errors](#).

### **BadRequestException**

A bad request exception object.

HTTP Status Code: 400

### **InternalServerErrorException**

An internal server error exception object.

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 v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript V3](#)



- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

# GetMemberDetectors

Describes which data sources are enabled for the member account's detector.

There might be regional differences because some data sources might not be available in all the AWS Regions where GuardDuty is presently supported. For more information, see [Regions and endpoints](#).

## Request Syntax

```
POST /detector/detectorId/member/detector/get HTTP/1.1
Content-type: application/json

{
  "accountIds": [ "string" ]
}
```

## URI Request Parameters

The request uses the following URI parameters.

### [detectorId](#)

The detector ID for the administrator account.

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

## Request Body

The request accepts the following data in JSON format.

### [accountIds](#)

The account ID of the member account.

Type: Array of strings

Array Members: Minimum number of 1 item. Maximum number of 50 items.

Length Constraints: Fixed length of 12.

Required: Yes

## Response Syntax

HTTP/1.1 200

Content-type: application/json

```
{
  "members": [
    {
      "accountId": "string",
      "dataSources": {
        "cloudTrail": {
          "status": "string"
        },
        "dnsLogs": {
          "status": "string"
        },
        "flowLogs": {
          "status": "string"
        },
        "kubernetes": {
          "auditLogs": {
            "status": "string"
          }
        },
        "malwareProtection": {
          "scanEc2InstanceWithFindings": {
            "ebsVolumes": {
              "reason": "string",
              "status": "string"
            }
          },
          "serviceRole": "string"
        },
        "s3Logs": {
          "status": "string"
        }
      },
      "features": [
        {
```

```
    "additionalConfiguration": [
      {
        "name": "string",
        "status": "string",
        "updatedAt": number
      }
    ],
    "name": "string",
    "status": "string",
    "updatedAt": number
  }
]
}
],
"unprocessedAccounts": [
  {
    "accountId": "string",
    "result": "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.

### members

An object that describes which data sources are enabled for a member account.

Type: Array of [MemberDataSourceConfiguration](#) objects

Array Members: Minimum number of 1 item. Maximum number of 50 items.

### unprocessedAccounts

A list of member account IDs that were unable to be processed along with an explanation for why they were not processed.

Type: Array of [UnprocessedAccount](#) objects

Array Members: Minimum number of 0 items. Maximum number of 50 items.

## Errors

For information about the errors that are common to all actions, see [Common Errors](#).

### **BadRequestException**

A bad request exception object.

HTTP Status Code: 400

### **InternalServerErrorException**

An internal server error exception object.

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 v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

# GetMembers

Retrieves GuardDuty member accounts (of the current GuardDuty administrator account) specified by the account IDs.

## Request Syntax

```
POST /detector/detectorId/member/get HTTP/1.1
Content-type: application/json

{
  "accountIds": [ "string" ]
}
```

## URI Request Parameters

The request uses the following URI parameters.

### detectorId

The unique ID of the detector of the GuardDuty account whose members you want to retrieve.

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

## Request Body

The request accepts the following data in JSON format.

### accountIds

A list of account IDs of the GuardDuty member accounts that you want to describe.

Type: Array of strings

Array Members: Minimum number of 1 item. Maximum number of 50 items.

Length Constraints: Fixed length of 12.

Required: Yes

## Response Syntax

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

{
  "members": [
    {
      "accountId": "string",
      "administratorId": "string",
      "detectorId": "string",
      "email": "string",
      "invitedAt": "string",
      "masterId": "string",
      "relationshipStatus": "string",
      "updatedAt": "string"
    }
  ],
  "unprocessedAccounts": [
    {
      "accountId": "string",
      "result": "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.

### members

A list of members.

Type: Array of [Member](#) objects

Array Members: Minimum number of 0 items. Maximum number of 50 items.

### unprocessedAccounts

A list of objects that contain the unprocessed account and a result string that explains why it was unprocessed.

Type: Array of [UnprocessedAccount](#) objects

Array Members: Minimum number of 0 items. Maximum number of 50 items.

## Errors

For information about the errors that are common to all actions, see [Common Errors](#).

### BadRequestException

A bad request exception object.

HTTP Status Code: 400

### InternalServerErrorException

An internal server error exception object.

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 v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)



# GetOrganizationStatistics

Retrieves how many active member accounts have each feature enabled within GuardDuty. Only a delegated GuardDuty administrator of an organization can run this API.

When you create a new organization, it might take up to 24 hours to generate the statistics for the entire organization.

## Request Syntax

```
GET /organization/statistics HTTP/1.1
```

## URI Request Parameters

The request does not use any URI parameters.

## Request Body

The request does not have a request body.

## Response Syntax

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

{
  "organizationDetails": {
    "organizationStatistics": {
      "activeAccountsCount": number,
      "countByFeature": [
        {
          "additionalConfiguration": [
            {
              "enabledAccountsCount": number,
              "name": "string"
            }
          ],
          "enabledAccountsCount": number,
          "name": "string"
        }
      ],
    }
  },
}
```

```
    "enabledAccountsCount": number,
    "memberAccountsCount": number,
    "totalAccountsCount": number
  },
  "updatedAt": number
}
```

## Response Elements

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

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

### organizationDetails

Information about the statistics report for your organization.

Type: [OrganizationDetails](#) object

## Errors

For information about the errors that are common to all actions, see [Common Errors](#).

### **BadRequestException**

A bad request exception object.

HTTP Status Code: 400

### **InternalServerErrorException**

An internal server error exception object.

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 v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

# GetRemainingFreeTrialDays

Provides the number of days left for each data source used in the free trial period.

## Request Syntax

```
POST /detector/detectorId/freeTrial/daysRemaining HTTP/1.1
Content-type: application/json

{
  "accountIds": [ "string" ]
}
```

## URI Request Parameters

The request uses the following URI parameters.

### detectorId

The unique ID of the detector of the GuardDuty member account.

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

## Request Body

The request accepts the following data in JSON format.

### accountIds

A list of account identifiers of the GuardDuty member account.

Type: Array of strings

Array Members: Minimum number of 1 item. Maximum number of 50 items.

Length Constraints: Fixed length of 12.

Required: No

## Response Syntax

HTTP/1.1 200

Content-type: application/json

```
{
  "accounts": [
    {
      "accountId": "string",
      "dataSources": {
        "cloudTrail": {
          "freeTrialDaysRemaining": number
        },
        "dnsLogs": {
          "freeTrialDaysRemaining": number
        },
        "flowLogs": {
          "freeTrialDaysRemaining": number
        },
        "kubernetes": {
          "auditLogs": {
            "freeTrialDaysRemaining": number
          }
        },
        "malwareProtection": {
          "scanEc2InstanceWithFindings": {
            "freeTrialDaysRemaining": number
          }
        },
        "s3Logs": {
          "freeTrialDaysRemaining": number
        }
      },
      "features": [
        {
          "freeTrialDaysRemaining": number,
          "name": "string"
        }
      ]
    }
  ],
  "unprocessedAccounts": [
    {
```

```
    "accountId": "string",  
    "result": "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.

### accounts

The member accounts which were included in a request and were processed successfully.

Type: Array of [AccountFreeTrialInfo](#) objects

### unprocessedAccounts

The member account that was included in a request but for which the request could not be processed.

Type: Array of [UnprocessedAccount](#) objects

Array Members: Minimum number of 0 items. Maximum number of 50 items.

## Errors

For information about the errors that are common to all actions, see [Common Errors](#).

### **BadRequestException**

A bad request exception object.

HTTP Status Code: 400

### **InternalServerErrorException**

An internal server error exception object.

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 v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

# GetThreatIntelSet

Retrieves the ThreatIntelSet that is specified by the ThreatIntelSet ID.

## Request Syntax

```
GET /detector/detectorId/threatintelset/threatIntelSetId HTTP/1.1
```

## URI Request Parameters

The request uses the following URI parameters.

### detectorId

The unique ID of the detector that the threatIntelSet is associated with.

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

### threatIntelSetId

The unique ID of the threatIntelSet that you want to get.

Required: Yes

## Request Body

The request does not have a request body.

## Response Syntax

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

```
{
  "format": "string",
  "location": "string",
  "name": "string",
  "status": "string",
  "tags": {
```



```
    "string" : "string"  
  }  
}
```

## Response Elements

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

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

### format

The format of the threatIntelSet.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 300.

Valid Values: TXT | STIX | OTX\_CSV | ALIEN\_VAULT | PROOF\_POINT | FIRE\_EYE

### location

The URI of the file that contains the ThreatIntelSet.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 300.

### name

A user-friendly ThreatIntelSet name displayed in all findings that are generated by activity that involves IP addresses included in this ThreatIntelSet.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 300.

### status

The status of threatIntelSet file uploaded.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 300.

Valid Values: INACTIVE | ACTIVATING | ACTIVE | DEACTIVATING | ERROR | DELETE\_PENDING | DELETED

## tags

The tags of the threat list resource.

Type: String to string map

Map Entries: Maximum number of 200 items.

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

Key Pattern: `^(?!aws:)[a-zA-Z+-. _:/]+`

Value Length Constraints: Maximum length of 256.

## Errors

For information about the errors that are common to all actions, see [Common Errors](#).

### **BadRequestException**

A bad request exception object.

HTTP Status Code: 400

### **InternalServerErrorException**

An internal server error exception object.

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 v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

## GetUsageStatistics

Lists Amazon GuardDuty usage statistics over the last 30 days for the specified detector ID. For newly enabled detectors or data sources, the cost returned will include only the usage so far under 30 days. This may differ from the cost metrics in the console, which project usage over 30 days to provide a monthly cost estimate. For more information, see [Understanding How Usage Costs are Calculated](#).

### Request Syntax

```
POST /detector/detectorId/usage/statistics HTTP/1.1
Content-type: application/json
```

```
{
  "maxResults": number,
  "nextToken": "string",
  "unit": "string",
  "usageCriteria": {
    "accountIds": [ "string" ],
    "dataSources": [ "string" ],
    "features": [ "string" ],
    "resources": [ "string" ]
  },
  "usageStatisticsType": "string"
}
```

### URI Request Parameters

The request uses the following URI parameters.

#### detectorId

The ID of the detector that specifies the GuardDuty service whose usage statistics you want to retrieve.

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

## Request Body

The request accepts the following data in JSON format.

### maxResults

The maximum number of results to return in the response.

Type: Integer

Valid Range: Minimum value of 1. Maximum value of 50.

Required: No

### nextToken

A token to use for paginating results that are returned in the response. Set the value of this parameter to null for the first request to a list action. For subsequent calls, use the NextToken value returned from the previous request to continue listing results after the first page.

Type: String

Required: No

### unit

The currency unit you would like to view your usage statistics in. Current valid values are USD.

Type: String

Required: No

### usageCriteria

Represents the criteria used for querying usage.

Type: [UsageCriteria](#) object

Required: Yes

### usageStatisticsType

The type of usage statistics to retrieve.

Type: String

Valid Values: SUM\_BY\_ACCOUNT | SUM\_BY\_DATA\_SOURCE | SUM\_BY\_RESOURCE | TOP\_RESOURCES | SUM\_BY\_FEATURES | TOP\_ACCOUNTS\_BY\_FEATURE

Required: Yes

## Response Syntax

HTTP/1.1 200

Content-type: application/json

```
{
  "nextToken": "string",
  "usageStatistics": {
    "sumByAccount": [
      {
        "accountId": "string",
        "total": {
          "amount": "string",
          "unit": "string"
        }
      }
    ],
    "sumByDataSource": [
      {
        "dataSource": "string",
        "total": {
          "amount": "string",
          "unit": "string"
        }
      }
    ],
    "sumByFeature": [
      {
        "feature": "string",
        "total": {
          "amount": "string",
          "unit": "string"
        }
      }
    ]
  },
}
```

```
    "sumByResource": [
      {
        "resource": "string",
        "total": {
          "amount": "string",
          "unit": "string"
        }
      }
    ],
    "topAccountsByFeature": [
      {
        "accounts": [
          {
            "accountId": "string",
            "total": {
              "amount": "string",
              "unit": "string"
            }
          }
        ],
        "feature": "string"
      }
    ],
    "topResources": [
      {
        "resource": "string",
        "total": {
          "amount": "string",
          "unit": "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](#)

The pagination parameter to be used on the next list operation to retrieve more items.

Type: String

### usageStatistics

The usage statistics object. If a UsageStatisticType was provided, the objects representing other types will be null.

Type: [UsageStatistics](#) object

## Errors

For information about the errors that are common to all actions, see [Common Errors](#).

### **BadRequestException**

A bad request exception object.

HTTP Status Code: 400

### **InternalServerErrorException**

An internal server error exception object.

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 v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)





# InviteMembers

Invites AWS accounts to become members of an organization administered by the AWS account that invokes this API. If you are using AWS Organizations to manage your GuardDuty environment, this step is not needed. For more information, see [Managing accounts with organizations](#).

To invite AWS accounts, the first step is to ensure that GuardDuty has been enabled in the potential member accounts. You can now invoke this API to add accounts by invitation. The invited accounts can either accept or decline the invitation from their GuardDuty accounts. Each invited AWS account can choose to accept the invitation from only one AWS account. For more information, see [Managing GuardDuty accounts by invitation](#).

After the invite has been accepted and you choose to disassociate a member account (by using [DisassociateMembers](#)) from your account, the details of the member account obtained by invoking [CreateMembers](#), including the associated email addresses, will be retained. This is done so that you can invoke InviteMembers without the need to invoke [CreateMembers](#) again. To remove the details associated with a member account, you must also invoke [DeleteMembers](#).

If you disassociate a member account that was added by invitation, the member account details obtained from this API, including the associated email addresses, will be retained. This is done so that the delegated administrator can invoke the [InviteMembers](#) API without the need to invoke the CreateMembers API again. To remove the details associated with a member account, the delegated administrator must invoke the [DeleteMembers](#) API.

When the member accounts added through AWS Organizations are later disassociated, you (administrator) can't invite them by calling the InviteMembers API. You can create an association with these member accounts again only by calling the CreateMembers API.

## Request Syntax

```
POST /detector/detectorId/member/invite HTTP/1.1
```

```
Content-type: application/json
```

```
{
  "accountIds": [ "string" ],
  "disableEmailNotification": boolean,
  "message": "string"
}
```

## URI Request Parameters

The request uses the following URI parameters.

### detectorId

The unique ID of the detector of the GuardDuty account that you want to invite members with.

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

## Request Body

The request accepts the following data in JSON format.

### accountIds

A list of account IDs of the accounts that you want to invite to GuardDuty as members.

Type: Array of strings

Array Members: Minimum number of 1 item. Maximum number of 50 items.

Length Constraints: Fixed length of 12.

Required: Yes

### disableEmailNotification

A Boolean value that specifies whether you want to disable email notification to the accounts that you are inviting to GuardDuty as members.

Type: Boolean

Required: No

### message

The invitation message that you want to send to the accounts that you're inviting to GuardDuty as members.

Type: String

Required: No

## Response Syntax

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

{
  "unprocessedAccounts": [
    {
      "accountId": "string",
      "result": "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.

### unprocessedAccounts

A list of objects that contain the unprocessed account and a result string that explains why it was unprocessed.

Type: Array of [UnprocessedAccount](#) objects

Array Members: Minimum number of 0 items. Maximum number of 50 items.

## Errors

For information about the errors that are common to all actions, see [Common Errors](#).

### BadRequestException

A bad request exception object.

HTTP Status Code: 400

## InternalServerErrorException

An internal server error exception object.

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 v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

# ListCoverage

Lists coverage details for your GuardDuty account. If you're a GuardDuty administrator, you can retrieve all resources associated with the active member accounts in your organization.

Make sure the accounts have Runtime Monitoring enabled and GuardDuty agent running on their resources.

## Request Syntax

```
POST /detector/detectorId/coverage HTTP/1.1
```

```
Content-type: application/json
```

```
{
  "filterCriteria": {
    "filterCriterion": [
      {
        "criterionKey": "string",
        "filterCondition": {
          "equals": [ "string" ],
          "notEquals": [ "string" ]
        }
      }
    ]
  },
  "maxResults": number,
  "nextToken": "string",
  "sortCriteria": {
    "attributeName": "string",
    "orderBy": "string"
  }
}
```

## URI Request Parameters

The request uses the following URI parameters.

### detectorId

The unique ID of the detector whose coverage details you want to retrieve.

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

## Request Body

The request accepts the following data in JSON format.

### filterCriteria

Represents the criteria used to filter the coverage details.

Type: [CoverageFilterCriteria](#) object

Required: No

### maxResults

The maximum number of results to return in the response.

Type: Integer

Valid Range: Minimum value of 1. Maximum value of 50.

Required: No

### nextToken

A token to use for paginating results that are returned in the response. Set the value of this parameter to null for the first request to a list action. For subsequent calls, use the NextToken value returned from the previous request to continue listing results after the first page.

Type: String

Required: No

### sortCriteria

Represents the criteria used to sort the coverage details.

Type: [CoverageSortCriteria](#) object

Required: No

## Response Syntax

```
HTTP/1.1 200
```

Content-type: application/json

```
{
  "nextToken": "string",
  "resources": [
    {
      "accountId": "string",
      "coverageStatus": "string",
      "detectorId": "string",
      "issue": "string",
      "resourceDetails": {
        "ec2InstanceDetails": {
          "agentDetails": {
            "version": "string"
          },
          "clusterArn": "string",
          "instanceId": "string",
          "instanceType": "string",
          "managementType": "string"
        },
        "ecsClusterDetails": {
          "clusterName": "string",
          "containerInstanceDetails": {
            "compatibleContainerInstances": number,
            "coveredContainerInstances": number
          },
          "fargateDetails": {
            "issues": [ "string" ],
            "managementType": "string"
          }
        },
        "eksClusterDetails": {
          "addonDetails": {
            "addonStatus": "string",
            "addonVersion": "string"
          },
          "clusterName": "string",
          "compatibleNodes": number,
          "coveredNodes": number,
          "managementType": "string"
        },
        "resourceType": "string"
      },
      "resourceId": "string",
```



```
    "updatedAt": number
  }
]
}
```

## Response Elements

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

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

### [nextToken](#)

The pagination parameter to be used on the next list operation to retrieve more items.

Type: String

### [resources](#)

A list of resources and their attributes providing cluster details.

Type: Array of [CoverageResource](#) objects

## Errors

For information about the errors that are common to all actions, see [Common Errors](#).

### **BadRequestException**

A bad request exception object.

HTTP Status Code: 400

### **InternalServerErrorException**

An internal server error exception object.

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 v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

# ListDetectors

Lists detectorIds of all the existing Amazon GuardDuty detector resources.

## Request Syntax

```
GET /detector?maxResults=MaxResults&nextToken=NextToken HTTP/1.1
```

## URI Request Parameters

The request uses the following URI parameters.

### [MaxResults](#)

You can use this parameter to indicate the maximum number of items that you want in the response. The default value is 50. The maximum value is 50.

Valid Range: Minimum value of 1. Maximum value of 50.

### [NextToken](#)

You can use this parameter when paginating results. Set the value of this parameter to null on your first call to the list action. For subsequent calls to the action, fill nextToken in the request with the value of NextToken from the previous response to continue listing data.

## Request Body

The request does not have a request body.

## Response Syntax

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

{
  "detectorIds": [ "string" ],
  "nextToken": "string"
}
```

## Response Elements

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

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

### detectorIds

A list of detector IDs.

Type: Array of strings

Array Members: Minimum number of 0 items. Maximum number of 50 items.

Length Constraints: Minimum length of 1. Maximum length of 300.

### nextToken

The pagination parameter to be used on the next list operation to retrieve more items.

Type: String

## Errors

For information about the errors that are common to all actions, see [Common Errors](#).

### **BadRequestException**

A bad request exception object.

HTTP Status Code: 400

### **InternalServerErrorException**

An internal server error exception object.

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 v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

# ListFilters

Returns a paginated list of the current filters.

## Request Syntax

```
GET /detector/detectorId/filter?maxResults=MaxResults&nextToken=NextToken HTTP/1.1
```

## URI Request Parameters

The request uses the following URI parameters.

### [detectorId](#)

The unique ID of the detector that the filter is associated with.

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

### [MaxResults](#)

You can use this parameter to indicate the maximum number of items that you want in the response. The default value is 50. The maximum value is 50.

Valid Range: Minimum value of 1. Maximum value of 50.

### [NextToken](#)

You can use this parameter when paginating results. Set the value of this parameter to null on your first call to the list action. For subsequent calls to the action, fill nextToken in the request with the value of NextToken from the previous response to continue listing data.

## Request Body

The request does not have a request body.

## Response Syntax

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

```
{  
  "filterNames": [ "string" ],  
  "nextToken": "string"  
}
```

## Response Elements

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

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

### filterNames

A list of filter names.

Type: Array of strings

Array Members: Minimum number of 0 items. Maximum number of 50 items.

Length Constraints: Minimum length of 3. Maximum length of 64.

### nextToken

The pagination parameter to be used on the next list operation to retrieve more items.

Type: String

## Errors

For information about the errors that are common to all actions, see [Common Errors](#).

### **BadRequestException**

A bad request exception object.

HTTP Status Code: 400

### **InternalServerErrorException**

An internal server error exception object.

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 v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)



# ListFindings

Lists GuardDuty findings for the specified detector ID.

There might be regional differences because some flags might not be available in all the Regions where GuardDuty is currently supported. For more information, see [Regions and endpoints](#).

## Request Syntax

```
POST /detector/detectorId/findings HTTP/1.1
```

```
Content-type: application/json
```

```
{
  "findingCriteria": {
    "criterion": {
      "string": {
        "eq": [ "string" ],
        "equals": [ "string" ],
        "greaterThan": number,
        "greaterThanOrEqual": number,
        "gt": number,
        "gte": number,
        "lessThan": number,
        "lessThanOrEqual": number,
        "lt": number,
        "lte": number,
        "neq": [ "string" ],
        "notEquals": [ "string" ]
      }
    }
  },
  "maxResults": number,
  "nextToken": "string",
  "sortCriteria": {
    "attributeName": "string",
    "orderBy": "string"
  }
}
```

## URI Request Parameters

The request uses the following URI parameters.

## detectorId

The ID of the detector that specifies the GuardDuty service whose findings you want to list.

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

## Request Body

The request accepts the following data in JSON format.

### findingCriteria

Represents the criteria used for querying findings. Valid values include:

- JSON field name
- accountId
- region
- confidence
- id
- resource.accessKeyDetails.accessKeyId
- resource.accessKeyDetails.principalId
- resource.accessKeyDetails.userName
- resource.accessKeyDetails.userType
- resource.instanceDetails.iamInstanceProfile.id
- resource.instanceDetails.imageId
- resource.instanceDetails.instanceId
- resource.instanceDetails.networkInterfaces.ipv6Addresses
- resource.instanceDetails.networkInterfaces.privateIpAddresses.privateIpAddress
- resource.instanceDetails.networkInterfaces.publicDnsName
- resource.instanceDetails.networkInterfaces.publicIp
- resource.instanceDetails.networkInterfaces.securityGroups.groupId
- resource.instanceDetails.networkInterfaces.securityGroups.groupName
- resource.instanceDetails.networkInterfaces.subnetId

- resource.instanceDetails.networkInterfaces.vpcId
- resource.instanceDetails.tags.key
- resource.instanceDetails.tags.value
- resource.resourceType
- service.action.actionType
- service.action.awsApiCallAction.api
- service.action.awsApiCallAction.callerType
- service.action.awsApiCallAction.remotelpDetails.city.cityName
- service.action.awsApiCallAction.remotelpDetails.country.countryName
- service.action.awsApiCallAction.remotelpDetails.ipAddressV4
- service.action.awsApiCallAction.remotelpDetails.organization.asn
- service.action.awsApiCallAction.remotelpDetails.organization.asnOrg
- service.action.awsApiCallAction.serviceName
- service.action.dnsRequestAction.domain
- service.action.dnsRequestAction.domainWithSuffix
- service.action.networkConnectionAction.blocked
- service.action.networkConnectionAction.connectionDirection
- service.action.networkConnectionAction.localPortDetails.port
- service.action.networkConnectionAction.protocol
- service.action.networkConnectionAction.remotelpDetails.country.countryName
- service.action.networkConnectionAction.remotelpDetails.ipAddressV4
- service.action.networkConnectionAction.remotelpDetails.organization.asn
- service.action.networkConnectionAction.remotelpDetails.organization.asnOrg
- service.action.networkConnectionAction.remotePortDetails.port
- service.additionalInfo.threatListName
- service.archived

When this attribute is set to 'true', only archived findings are listed. When it's set to 'false', only unarchived findings are listed. When this attribute is not set, all existing findings are listed.

- service.resourceRole

- severity
- type
- updatedAt

Type: Timestamp in Unix Epoch millisecond format: 1486685375000

Type: [FindingCriteria](#) object

Required: No

### [maxResults](#)

You can use this parameter to indicate the maximum number of items you want in the response. The default value is 50. The maximum value is 50.

Type: Integer

Valid Range: Minimum value of 1. Maximum value of 50.

Required: No

### [nextToken](#)

You can use this parameter when paginating results. Set the value of this parameter to null on your first call to the list action. For subsequent calls to the action, fill nextToken in the request with the value of NextToken from the previous response to continue listing data.

Type: String

Required: No

### [sortCriteria](#)

Represents the criteria used for sorting findings.

Type: [SortCriteria](#) object

Required: No

## Response Syntax

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

```
{
  "findingIds": [ "string" ],
  "nextToken": "string"
}
```

## Response Elements

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

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

### findingIds

The IDs of the findings that you're listing.

Type: Array of strings

Array Members: Minimum number of 0 items. Maximum number of 50 items.

Length Constraints: Minimum length of 1. Maximum length of 300.

### nextToken

The pagination parameter to be used on the next list operation to retrieve more items.

Type: String

## Errors

For information about the errors that are common to all actions, see [Common Errors](#).

### **BadRequestException**

A bad request exception object.

HTTP Status Code: 400

### **InternalServerErrorException**

An internal server error exception object.

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 v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

# ListInvitations

Lists all GuardDuty membership invitations that were sent to the current AWS account.

## Request Syntax

```
GET /invitation?maxResults=MaxResults&nextToken=NextToken HTTP/1.1
```

## URI Request Parameters

The request uses the following URI parameters.

### [MaxResults](#)

You can use this parameter to indicate the maximum number of items that you want in the response. The default value is 50. The maximum value is 50.

Valid Range: Minimum value of 1. Maximum value of 50.

### [NextToken](#)

You can use this parameter when paginating results. Set the value of this parameter to null on your first call to the list action. For subsequent calls to the action, fill nextToken in the request with the value of NextToken from the previous response to continue listing data.

## Request Body

The request does not have a request body.

## Response Syntax

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

{
  "invitations": [
    {
      "accountId": "string",
      "invitationId": "string",
```

```
    "invitedAt": "string",  
    "relationshipStatus": "string"  
  }  
],  
"nextToken": "string"  
}
```

## Response Elements

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

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

### invitations

A list of invitation descriptions.

Type: Array of [Invitation](#) objects

Array Members: Minimum number of 0 items. Maximum number of 50 items.

### nextToken

The pagination parameter to be used on the next list operation to retrieve more items.

Type: String

## Errors

For information about the errors that are common to all actions, see [Common Errors](#).

### **BadRequestException**

A bad request exception object.

HTTP Status Code: 400

### **InternalServerErrorException**

An internal server error exception object.

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 v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

# ListIPSets

Lists the IPSets of the GuardDuty service specified by the detector ID. If you use this operation from a member account, the IPSets returned are the IPSets from the associated administrator account.

## Request Syntax

```
GET /detector/detectorId/ipset?maxResults=MaxResults&nextToken=NextToken HTTP/1.1
```

## URI Request Parameters

The request uses the following URI parameters.

### detectorId

The unique ID of the detector that the IPSet is associated with.

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

### MaxResults

You can use this parameter to indicate the maximum number of items you want in the response. The default value is 50. The maximum value is 50.

Valid Range: Minimum value of 1. Maximum value of 50.

### NextToken

You can use this parameter when paginating results. Set the value of this parameter to null on your first call to the list action. For subsequent calls to the action, fill nextToken in the request with the value of NextToken from the previous response to continue listing data.

## Request Body

The request does not have a request body.

## Response Syntax

```
HTTP/1.1 200
```

```
Content-type: application/json

{
  "ipSetIds": [ "string" ],
  "nextToken": "string"
}
```

## Response Elements

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

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

### ipSetIds

The IDs of the IPSet resources.

Type: Array of strings

Array Members: Minimum number of 0 items. Maximum number of 50 items.

### nextToken

The pagination parameter to be used on the next list operation to retrieve more items.

Type: String

## Errors

For information about the errors that are common to all actions, see [Common Errors](#).

### **BadRequestException**

A bad request exception object.

HTTP Status Code: 400

### **InternalServerErrorException**

An internal server error exception object.

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 v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

# ListMalwareProtectionPlans

Lists the Malware Protection plan IDs associated with the protected resources in your AWS account.

## Request Syntax

```
GET /malware-protection-plan?nextToken=NextToken HTTP/1.1
```

## URI Request Parameters

The request uses the following URI parameters.

### [NextToken](#)

You can use this parameter when paginating results. Set the value of this parameter to null on your first call to the list action. For subsequent calls to the action, fill nextToken in the request with the value of NextToken from the previous response to continue listing data.

## Request Body

The request does not have a request body.

## Response Syntax

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

{
  "malwareProtectionPlans": [
    {
      "malwareProtectionPlanId": "string"
    }
  ],
  "nextToken": "string"
}
```

## Response Elements

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

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

### malwareProtectionPlans

A list of unique identifiers associated with each Malware Protection plan.

Type: Array of [MalwareProtectionPlanSummary](#) objects

### nextToken

You can use this parameter when paginating results. Set the value of this parameter to null on your first call to the list action. For subsequent calls to the action, fill nextToken in the request with the value of NextToken from the previous response to continue listing data.

Type: String

## Errors

For information about the errors that are common to all actions, see [Common Errors](#).

### **AccessDeniedException**

An access denied exception object.

HTTP Status Code: 403

### **BadRequestException**

A bad request exception object.

HTTP Status Code: 400

### **InternalServerErrorException**

An internal server error exception object.

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 v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

# ListMembers

Lists details about all member accounts for the current GuardDuty administrator account.

## Request Syntax

```
GET /detector/detectorId/member?  
maxResults=MaxResults&nextToken=NextToken&onlyAssociated=OnlyAssociated HTTP/1.1
```

## URI Request Parameters

The request uses the following URI parameters.

### detectorId

The unique ID of the detector the member is associated with.

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

### MaxResults

You can use this parameter to indicate the maximum number of items you want in the response. The default value is 50. The maximum value is 50.

Valid Range: Minimum value of 1. Maximum value of 50.

### NextToken

You can use this parameter when paginating results. Set the value of this parameter to null on your first call to the list action. For subsequent calls to the action, fill nextToken in the request with the value of NextToken from the previous response to continue listing data.

### OnlyAssociated

Specifies whether to only return associated members or to return all members (including members who haven't been invited yet or have been disassociated). Member accounts must have been previously associated with the GuardDuty administrator account using [Create Members](#).



## Request Body

The request does not have a request body.

## Response Syntax

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

{
  "members": [
    {
      "accountId": "string",
      "administratorId": "string",
      "detectorId": "string",
      "email": "string",
      "invitedAt": "string",
      "masterId": "string",
      "relationshipStatus": "string",
      "updatedAt": "string"
    }
  ],
  "nextToken": "string"
}
```

## Response Elements

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

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

### members

A list of members.

#### Note

The values for `email` and `invitedAt` are available only if the member accounts are added by invitation.

Type: Array of [Member](#) objects

Array Members: Minimum number of 0 items. Maximum number of 50 items.

### nextToken

The pagination parameter to be used on the next list operation to retrieve more items.

Type: String

## Errors

For information about the errors that are common to all actions, see [Common Errors](#).

### **BadRequestException**

A bad request exception object.

HTTP Status Code: 400

### **InternalServerErrorException**

An internal server error exception object.

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 v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

# ListOrganizationAdminAccounts

Lists the accounts designated as GuardDuty delegated administrators. Only the organization's management account can run this API operation.

## Request Syntax

```
GET /admin?maxResults=MaxResults&nextToken=NextToken HTTP/1.1
```

## URI Request Parameters

The request uses the following URI parameters.

### MaxResults

The maximum number of results to return in the response.

Valid Range: Minimum value of 1. Maximum value of 50.

### NextToken

A token to use for paginating results that are returned in the response. Set the value of this parameter to null for the first request to a list action. For subsequent calls, use the NextToken value returned from the previous request to continue listing results after the first page.

## Request Body

The request does not have a request body.

## Response Syntax

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

{
  "adminAccounts": [
    {
      "adminAccountId": "string",
      "adminStatus": "string"
    }
  ],
}
```

```
"nextToken": "string"  
}
```

## Response Elements

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

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

### adminAccounts

A list of accounts configured as GuardDuty delegated administrators.

Type: Array of [AdminAccount](#) objects

Array Members: Minimum number of 0 items. Maximum number of 1 item.

### nextToken

The pagination parameter to be used on the next list operation to retrieve more items.

Type: String

## Errors

For information about the errors that are common to all actions, see [Common Errors](#).

### **BadRequestException**

A bad request exception object.

HTTP Status Code: 400

### **InternalServerErrorException**

An internal server error exception object.

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 v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

# ListPublishingDestinations

Returns a list of publishing destinations associated with the specified `detectorId`.

## Request Syntax

```
GET /detector/detectorId/publishingDestination?  
maxResults=MaxResults&nextToken=NextToken HTTP/1.1
```

## URI Request Parameters

The request uses the following URI parameters.

### detectorId

The ID of the detector to retrieve publishing destinations for.

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

### MaxResults

The maximum number of results to return in the response.

Valid Range: Minimum value of 1. Maximum value of 50.

### NextToken

A token to use for paginating results that are returned in the response. Set the value of this parameter to null for the first request to a list action. For subsequent calls, use the `NextToken` value returned from the previous request to continue listing results after the first page.

## Request Body

The request does not have a request body.

## Response Syntax

```
HTTP/1.1 200
```

```
Content-type: application/json

{
  "destinations": [
    {
      "destinationId": "string",
      "destinationType": "string",
      "status": "string"
    }
  ],
  "nextToken": "string"
}
```

## Response Elements

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

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

### destinations

A Destinations object that includes information about each publishing destination returned.

Type: Array of [Destination](#) objects

### nextToken

A token to use for paginating results that are returned in the response. Set the value of this parameter to null for the first request to a list action. For subsequent calls, use the NextToken value returned from the previous request to continue listing results after the first page.

Type: String

## Errors

For information about the errors that are common to all actions, see [Common Errors](#).

### **BadRequestException**

A bad request exception object.

HTTP Status Code: 400

## InternalServerErrorException

An internal server error exception object.

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 v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)



# ListTagsForResource

Lists tags for a resource. Tagging is currently supported for detectors, finding filters, IP sets, threat intel sets, and publishing destination, with a limit of 50 tags per resource. When invoked, this operation returns all assigned tags for a given resource.

## Request Syntax

```
GET /tags/resourceArn HTTP/1.1
```

## URI Request Parameters

The request uses the following URI parameters.

### resourceArn

The Amazon Resource Name (ARN) for the given GuardDuty resource.

Pattern: `^arn:[A-Za-z_.-]{1,20}:guardduty:[A-Za-z0-9_/.-]{0,63}:\d+:\detector/[A-Za-z0-9_/.-]{32,264}$`

Required: Yes

## Request Body

The request does not have a request body.

## Response Syntax

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

{
  "tags": {
    "string" : "string"
  }
}
```

## Response Elements

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

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

### tags

The tags associated with the resource.

Type: String to string map

Map Entries: Maximum number of 200 items.

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

Key Pattern: `^(?!aws:)[a-zA-Z+ -=._:/]+$`

Value Length Constraints: Maximum length of 256.

## Errors

For information about the errors that are common to all actions, see [Common Errors](#).

### **AccessDeniedException**

An access denied exception object.

HTTP Status Code: 403

### **BadRequestException**

A bad request exception object.

HTTP Status Code: 400

### **InternalServerErrorException**

An internal server error exception object.

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 v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

# ListThreatIntelSets

Lists the ThreatIntelSets of the GuardDuty service specified by the detector ID. If you use this operation from a member account, the ThreatIntelSets associated with the administrator account are returned.

## Request Syntax

```
GET /detector/detectorId/threatintelset?maxResults=MaxResults&nextToken=NextToken
HTTP/1.1
```

## URI Request Parameters

The request uses the following URI parameters.

### detectorId

The unique ID of the detector that the threatIntelSet is associated with.

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

### MaxResults

You can use this parameter to indicate the maximum number of items that you want in the response. The default value is 50. The maximum value is 50.

Valid Range: Minimum value of 1. Maximum value of 50.

### NextToken

You can use this parameter to paginate results in the response. Set the value of this parameter to null on your first call to the list action. For subsequent calls to the action, fill nextToken in the request with the value of NextToken from the previous response to continue listing data.

## Request Body

The request does not have a request body.

## Response Syntax

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

{
  "nextToken": "string",
  "threatIntelSetIds": [ "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

The pagination parameter to be used on the next list operation to retrieve more items.

Type: String

### threatIntelSetIds

The IDs of the ThreatIntelSet resources.

Type: Array of strings

Array Members: Minimum number of 0 items. Maximum number of 50 items.

## Errors

For information about the errors that are common to all actions, see [Common Errors](#).

### **BadRequestException**

A bad request exception object.

HTTP Status Code: 400

### **InternalServerErrorException**

An internal server error exception object.

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 v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

# StartMalwareScan

Initiates the malware scan. Invoking this API will automatically create the [Service-linked role](#) in the corresponding account.

When the malware scan starts, you can use the associated scan ID to track the status of the scan. For more information, see [DescribeMalwareScans](#).

## Request Syntax

```
POST /malware-scan/start HTTP/1.1
Content-type: application/json
```

```
{
  "resourceArn": "string"
}
```

## URI Request Parameters

The request does not use any URI parameters.

## Request Body

The request accepts the following data in JSON format.

### [resourceArn](#)

Amazon Resource Name (ARN) of the resource for which you invoked the API.

Type: String

Pattern: `^arn:[A-Za-z-]+:[A-Za-z0-9]+:[A-Za-z0-9-]+:\d+:(([A-Za-z0-9-]+)[:\V])?[A-Za-z0-9-]*$`

Required: Yes

## Response Syntax

```
HTTP/1.1 200
```

```
Content-type: application/json

{
  "scanId": "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.

### scanId

A unique identifier that gets generated when you invoke the API without any error. Each malware scan has a corresponding scan ID. Using this scan ID, you can monitor the status of your malware scan.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 200.

## Errors

For information about the errors that are common to all actions, see [Common Errors](#).

### **BadRequestException**

A bad request exception object.

HTTP Status Code: 400

### **ConflictException**

A request conflict exception object.

HTTP Status Code: 409

### **InternalServerErrorException**

An internal server error exception object.

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 v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

# StartMonitoringMembers

Turns on GuardDuty monitoring of the specified member accounts. Use this operation to restart monitoring of accounts that you stopped monitoring with the [StopMonitoringMembers](#) operation.

## Request Syntax

```
POST /detector/detectorId/member/start HTTP/1.1
Content-type: application/json

{
  "accountIds": [ "string" ]
}
```

## URI Request Parameters

The request uses the following URI parameters.

### [detectorId](#)

The unique ID of the detector of the GuardDuty administrator account associated with the member accounts to monitor.

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

## Request Body

The request accepts the following data in JSON format.

### [accountIds](#)

A list of account IDs of the GuardDuty member accounts to start monitoring.

Type: Array of strings

Array Members: Minimum number of 1 item. Maximum number of 50 items.

Length Constraints: Fixed length of 12.

Required: Yes

## Response Syntax

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

{
  "unprocessedAccounts": [
    {
      "accountId": "string",
      "result": "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.

### unprocessedAccounts

A list of objects that contain the unprocessed account and a result string that explains why it was unprocessed.

Type: Array of [UnprocessedAccount](#) objects

Array Members: Minimum number of 0 items. Maximum number of 50 items.

## Errors

For information about the errors that are common to all actions, see [Common Errors](#).

### BadRequestException

A bad request exception object.

HTTP Status Code: 400

## InternalServerErrorException

An internal server error exception object.

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 v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

# StopMonitoringMembers

Stops GuardDuty monitoring for the specified member accounts. Use the `StartMonitoringMembers` operation to restart monitoring for those accounts.

With `autoEnableOrganizationMembers` configuration for your organization set to ALL, you'll receive an error if you attempt to stop monitoring the member accounts in your organization.

## Request Syntax

```
POST /detector/detectorId/member/stop HTTP/1.1
Content-type: application/json

{
  "accountIds": [ "string" ]
}
```

## URI Request Parameters

The request uses the following URI parameters.

### detectorId

The unique ID of the detector associated with the GuardDuty administrator account that is monitoring member accounts.

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

## Request Body

The request accepts the following data in JSON format.

### accountIds

A list of account IDs for the member accounts to stop monitoring.

Type: Array of strings

Array Members: Minimum number of 1 item. Maximum number of 50 items.

Length Constraints: Fixed length of 12.

Required: Yes

## Response Syntax

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

{
  "unprocessedAccounts": [
    {
      "accountId": "string",
      "result": "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.

### unprocessedAccounts

A list of objects that contain an accountId for each account that could not be processed, and a result string that indicates why the account was not processed.

Type: Array of [UnprocessedAccount](#) objects

Array Members: Minimum number of 0 items. Maximum number of 50 items.

## Errors

For information about the errors that are common to all actions, see [Common Errors](#).

### **BadRequestException**

A bad request exception object.

HTTP Status Code: 400

## **InternalServerErrorException**

An internal server error exception object.

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 v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

# TagResource

Adds tags to a resource.

## Request Syntax

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

```
{
  "tags": {
    "string" : "string"
  }
}
```

## URI Request Parameters

The request uses the following URI parameters.

### resourceArn

The Amazon Resource Name (ARN) for the GuardDuty resource to apply a tag to.

Pattern: `^arn:[A-Za-z_.-]{1,20}:guardduty:[A-Za-z0-9_/.-]{0,63}:\d+:\detector/[A-Za-z0-9_/.-]{32,264}$`

Required: Yes

## Request Body

The request accepts the following data in JSON format.

### tags

The tags to be added to a resource.

Type: String to string map

Map Entries: Maximum number of 200 items.

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



Key Pattern: `^(?!aws:)[a-zA-Z+-._: /]+$`

Value Length Constraints: Maximum length of 256.

Required: Yes

## Response Syntax

```
HTTP/1.1 204
```

## Response Elements

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

## Errors

For information about the errors that are common to all actions, see [Common Errors](#).

### AccessDeniedException

An access denied exception object.

HTTP Status Code: 403

### BadRequestException

A bad request exception object.

HTTP Status Code: 400

### InternalServerErrorException

An internal server error exception object.

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 v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

# UnarchiveFindings

Unarchives GuardDuty findings specified by the `findingIds`.

## Request Syntax

```
POST /detector/detectorId/findings/unarchive HTTP/1.1
Content-type: application/json

{
  "findingIds": [ "string" ]
}
```

## URI Request Parameters

The request uses the following URI parameters.

### detectorId

The ID of the detector associated with the findings to unarchive.

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

## Request Body

The request accepts the following data in JSON format.

### findingIds

The IDs of the findings to unarchive.

Type: Array of strings

Array Members: Minimum number of 0 items. Maximum number of 50 items.

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

## Response Syntax

```
HTTP/1.1 200
```

## Response Elements

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

## Errors

For information about the errors that are common to all actions, see [Common Errors](#).

### **BadRequestException**

A bad request exception object.

HTTP Status Code: 400

### **InternalServerErrorException**

An internal server error exception object.

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 v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)



# UntagResource

Removes tags from a resource.

## Request Syntax

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

## URI Request Parameters

The request uses the following URI parameters.

### resourceArn

The Amazon Resource Name (ARN) for the resource to remove tags from.

Pattern: `^arn:[A-Za-z_.-]{1,20}:guardduty:[A-Za-z0-9_/.-]{0,63}:\d+:\detector/[A-Za-z0-9_/.-]{32,264}$`

Required: Yes

### TagKeys

The tag keys to remove from the resource.

Array Members: Minimum number of 1 item. Maximum number of 200 items.

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

Pattern: `^(?!aws:)[a-zA-Z+-. _:/]+$`

Required: Yes

## Request Body

The request does not have a request body.

## Response Syntax

```
HTTP/1.1 204
```

## Response Elements

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

## Errors

For information about the errors that are common to all actions, see [Common Errors](#).

### AccessDeniedException

An access denied exception object.

HTTP Status Code: 403

### BadRequestException

A bad request exception object.

HTTP Status Code: 400

### InternalServerErrorException

An internal server error exception object.

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 v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)





# UpdateDetector

Updates the GuardDuty detector specified by the detector ID.

Specifying both EKS Runtime Monitoring (EKS\_RUNTIME\_MONITORING) and Runtime Monitoring (RUNTIME\_MONITORING) will cause an error. You can add only one of these two features because Runtime Monitoring already includes the threat detection for Amazon EKS resources. For more information, see [Runtime Monitoring](#).

There might be regional differences because some data sources might not be available in all the AWS Regions where GuardDuty is presently supported. For more information, see [Regions and endpoints](#).

## Request Syntax

```
POST /detector/detectorId HTTP/1.1
Content-type: application/json

{
  "dataSources": {
    "kubernetes": {
      "auditLogs": {
        "enable": boolean
      }
    },
    "malwareProtection": {
      "scanEc2InstanceWithFindings": {
        "ebsVolumes": boolean
      }
    },
    "s3Logs": {
      "enable": boolean
    }
  },
  "enable": boolean,
  "features": [
    {
      "additionalConfiguration": [
        {
          "name": "string",
          "status": "string"
        }
      ]
    }
  ]
}
```

```
    ],  
    "name": "string",  
    "status": "string"  
  }  
],  
"findingPublishingFrequency": "string"  
}
```

## URI Request Parameters

The request uses the following URI parameters.

### detectorId

The unique ID of the detector to update.

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

## Request Body

The request accepts the following data in JSON format.

### dataSources

*This parameter has been deprecated.*

Describes which data sources will be updated.

There might be regional differences because some data sources might not be available in all the AWS Regions where GuardDuty is presently supported. For more information, see [Regions and endpoints](#).

Type: [DataSourceConfigurations](#) object

Required: No

### enable

Specifies whether the detector is enabled or not enabled.

Type: Boolean

Required: No

### features

Provides the features that will be updated for the detector.

Type: Array of [DetectorFeatureConfiguration](#) objects

Required: No

### findingPublishingFrequency

An enum value that specifies how frequently findings are exported, such as to CloudWatch Events.

Type: String

Valid Values: FIFTEEN\_MINUTES | ONE\_HOUR | SIX\_HOURS

Required: No

## Response Syntax

```
HTTP/1.1 200
```

## Response Elements

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

## Errors

For information about the errors that are common to all actions, see [Common Errors](#).

### **BadRequestException**

A bad request exception object.

HTTP Status Code: 400

### **InternalServerErrorException**

An internal server error exception object.

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 v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

# UpdateFilter

Updates the filter specified by the filter name.

## Request Syntax

```
POST /detector/detectorId/filter/filterName HTTP/1.1
Content-type: application/json
```

```
{
  "action": "string",
  "description": "string",
  "findingCriteria": {
    "criterion": {
      "string" : {
        "eq": [ "string" ],
        "equals": [ "string" ],
        "greaterThan": number,
        "greaterThanOrEqual": number,
        "gt": number,
        "gte": number,
        "lessThan": number,
        "lessThanOrEqual": number,
        "lt": number,
        "lte": number,
        "neq": [ "string" ],
        "notEquals": [ "string" ]
      }
    }
  },
  "rank": number
}
```

## URI Request Parameters

The request uses the following URI parameters.

### detectorId

The unique ID of the detector that specifies the GuardDuty service where you want to update a filter.

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

### filterName

The name of the filter.

Required: Yes

## Request Body

The request accepts the following data in JSON format.

### action

Specifies the action that is to be applied to the findings that match the filter.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 300.

Valid Values: NOOP | ARCHIVE

Required: No

### description

The description of the filter. Valid characters include alphanumeric characters, and special characters such as hyphen, period, colon, underscore, parentheses ( { }, [ ], and ( )), forward slash, horizontal tab, vertical tab, newline, form feed, return, and whitespace.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 512.

Required: No

### findingCriteria

Represents the criteria to be used in the filter for querying findings.

Type: [FindingCriteria](#) object

Required: No

## rank

Specifies the position of the filter in the list of current filters. Also specifies the order in which this filter is applied to the findings.

Type: Integer

Valid Range: Minimum value of 1. Maximum value of 100.

Required: No

## Response Syntax

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

{
  "name": "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.

### name

The name of the filter.

Type: String

Length Constraints: Minimum length of 3. Maximum length of 64.

## Errors

For information about the errors that are common to all actions, see [Common Errors](#).

### BadRequestException

A bad request exception object.

HTTP Status Code: 400

## **InternalServerErrorException**

An internal server error exception object.

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 v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)



# UpdateFindingsFeedback

Marks the specified GuardDuty findings as useful or not useful.

## Request Syntax

```
POST /detector/detectorId/findings/feedback HTTP/1.1
Content-type: application/json
```

```
{
  "comments": "string",
  "feedback": "string",
  "findingIds": [ "string" ]
}
```

## URI Request Parameters

The request uses the following URI parameters.

### detectorId

The ID of the detector associated with the findings to update feedback for.

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

## Request Body

The request accepts the following data in JSON format.

### comments

Additional feedback about the GuardDuty findings.

Type: String

Required: No

### feedback

The feedback for the finding.

Type: String

Valid Values: USEFUL | NOT\_USEFUL

Required: Yes

### findingIds

The IDs of the findings that you want to mark as useful or not useful.

Type: Array of strings

Array Members: Minimum number of 0 items. Maximum number of 50 items.

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

## Response Syntax

```
HTTP/1.1 200
```

## Response Elements

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

## Errors

For information about the errors that are common to all actions, see [Common Errors](#).

### BadRequestException

A bad request exception object.

HTTP Status Code: 400

### InternalServerErrorException

An internal server error exception object.

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 v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

# UpdateIPSet

Updates the IPSet specified by the IPSet ID.

## Request Syntax

```
POST /detector/detectorId/ipset/ipSetId HTTP/1.1
Content-type: application/json
```

```
{
  "activate": boolean,
  "location": "string",
  "name": "string"
}
```

## URI Request Parameters

The request uses the following URI parameters.

### detectorId

The detectorID that specifies the GuardDuty service whose IPSet you want to update.

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

### ipSetId

The unique ID that specifies the IPSet that you want to update.

Required: Yes

## Request Body

The request accepts the following data in JSON format.

### activate

The updated Boolean value that specifies whether the IPSet is active or not.

Type: Boolean

Required: No

### location

The updated URI of the file that contains the IPSet.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: No

### name

The unique ID that specifies the IPSet that you want to update.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: No

## Response Syntax

```
HTTP/1.1 200
```

## Response Elements

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

## Errors

For information about the errors that are common to all actions, see [Common Errors](#).

### **BadRequestException**

A bad request exception object.

HTTP Status Code: 400

### **InternalServerErrorException**

An internal server error exception object.

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 v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

# UpdateMalwareProtectionPlan

Updates an existing Malware Protection plan resource.

## Request Syntax

```
PATCH /malware-protection-plan/malwareProtectionPlanId HTTP/1.1  
Content-type: application/json
```

```
{  
  "actions": {  
    "tagging": {  
      "status": "string"  
    }  
  },  
  "protectedResource": {  
    "s3Bucket": {  
      "objectPrefixes": [ "string" ]  
    }  
  },  
  "role": "string"  
}
```

## URI Request Parameters

The request uses the following URI parameters.

### malwareProtectionPlanId

A unique identifier associated with the Malware Protection plan.

Required: Yes

## Request Body

The request accepts the following data in JSON format.

### actions

Information about whether the tags will be added to the S3 object after scanning.

Type: [MalwareProtectionPlanActions](#) object

Required: No

### [protectedResource](#)

Information about the protected resource that is associated with the created Malware Protection plan. Presently, S3Bucket is the only supported protected resource.

Type: [UpdateProtectedResource](#) object

Required: No

### [role](#)

IAM role with permissions required to scan and add tags to the associated protected resource.

Type: String

Required: No

## Response Syntax

```
HTTP/1.1 200
```

## Response Elements

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

## Errors

For information about the errors that are common to all actions, see [Common Errors](#).

### **AccessDeniedException**

An access denied exception object.

HTTP Status Code: 403

### **BadRequestException**

A bad request exception object.



HTTP Status Code: 400

### **InternalServerErrorException**

An internal server error exception object.

HTTP Status Code: 500

### **ResourceNotFoundException**

The requested resource can't be found.

HTTP Status Code: 404

## **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 v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

# UpdateMalwareScanSettings

Updates the malware scan settings.

There might be regional differences because some data sources might not be available in all the AWS Regions where GuardDuty is presently supported. For more information, see [Regions and endpoints](#).

## Request Syntax

```
POST /detector/detectorId/malware-scan-settings HTTP/1.1
```

```
Content-type: application/json
```

```
{
  "ebsSnapshotPreservation": "string",
  "scanResourceCriteria": {
    "exclude": {
      "string": {
        "mapEquals": [
          {
            "key": "string",
            "value": "string"
          }
        ]
      }
    },
    "include": {
      "string": {
        "mapEquals": [
          {
            "key": "string",
            "value": "string"
          }
        ]
      }
    }
  }
}
```

## URI Request Parameters

The request uses the following URI parameters.

## detectorId

The unique ID of the detector that specifies the GuardDuty service where you want to update scan settings.

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

## Request Body

The request accepts the following data in JSON format.

### ebsSnapshotPreservation

An enum value representing possible snapshot preservation settings.

Type: String

Valid Values: NO\_RETENTION | RETENTION\_WITH\_FINDING

Required: No

### scanResourceCriteria

Represents the criteria to be used in the filter for selecting resources to scan.

Type: [ScanResourceCriteria](#) object

Required: No

## Response Syntax

```
HTTP/1.1 200
```

## Response Elements

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

## Errors

For information about the errors that are common to all actions, see [Common Errors](#).

## BadRequestException

A bad request exception object.

HTTP Status Code: 400

## InternalServerErrorException

An internal server error exception object.

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 v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

## UpdateMemberDetectors

Contains information on member accounts to be updated.

Specifying both EKS Runtime Monitoring (EKS\_RUNTIME\_MONITORING) and Runtime Monitoring (RUNTIME\_MONITORING) will cause an error. You can add only one of these two features because Runtime Monitoring already includes the threat detection for Amazon EKS resources. For more information, see [Runtime Monitoring](#).

There might be regional differences because some data sources might not be available in all the AWS Regions where GuardDuty is presently supported. For more information, see [Regions and endpoints](#).

### Request Syntax

```
POST /detector/detectorId/member/detector/update HTTP/1.1
```

```
Content-type: application/json
```

```
{
  "accountIds": [ "string" ],
  "dataSources": {
    "kubernetes": {
      "auditLogs": {
        "enable": boolean
      }
    },
    "malwareProtection": {
      "scanEc2InstanceWithFindings": {
        "ebsVolumes": boolean
      }
    },
    "s3Logs": {
      "enable": boolean
    }
  },
  "features": [
    {
      "additionalConfiguration": [
        {
          "name": "string",
          "status": "string"
        }
      ]
    }
  ]
}
```

```
    ],  
    "name": "string",  
    "status": "string"  
  }  
]  
}
```

## URI Request Parameters

The request uses the following URI parameters.

### detectorId

The detector ID of the administrator account.

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

## Request Body

The request accepts the following data in JSON format.

### accountIds

A list of member account IDs to be updated.

Type: Array of strings

Array Members: Minimum number of 1 item. Maximum number of 50 items.

Length Constraints: Fixed length of 12.

Required: Yes

### dataSources

*This parameter has been deprecated.*

Describes which data sources will be updated.

Type: [DataSourceConfigurations](#) object

Required: No

## features

A list of features that will be updated for the specified member accounts.

Type: Array of [MemberFeaturesConfiguration](#) objects

Required: No

## Response Syntax

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

{
  "unprocessedAccounts": [
    {
      "accountId": "string",
      "result": "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.

### unprocessedAccounts

A list of member account IDs that were unable to be processed along with an explanation for why they were not processed.

Type: Array of [UnprocessedAccount](#) objects

Array Members: Minimum number of 0 items. Maximum number of 50 items.

## Errors

For information about the errors that are common to all actions, see [Common Errors](#).

## BadRequestException

A bad request exception object.

HTTP Status Code: 400

## InternalServerErrorException

An internal server error exception object.

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 v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)



# UpdateOrganizationConfiguration

Configures the delegated administrator account with the provided values. You must provide a value for either `autoEnableOrganizationMembers` or `autoEnable`, but not both.

Specifying both EKS Runtime Monitoring (EKS\_RUNTIME\_MONITORING) and Runtime Monitoring (RUNTIME\_MONITORING) will cause an error. You can add only one of these two features because Runtime Monitoring already includes the threat detection for Amazon EKS resources. For more information, see [Runtime Monitoring](#).

There might be regional differences because some data sources might not be available in all the AWS Regions where GuardDuty is presently supported. For more information, see [Regions and endpoints](#).

## Request Syntax

```
POST /detector/detectorId/admin HTTP/1.1
Content-type: application/json

{
  "autoEnable": boolean,
  "autoEnableOrganizationMembers": "string",
  "dataSources": {
    "kubernetes": {
      "auditLogs": {
        "autoEnable": boolean
      }
    },
    "malwareProtection": {
      "scanEc2InstanceWithFindings": {
        "ebsVolumes": {
          "autoEnable": boolean
        }
      }
    },
    "s3Logs": {
      "autoEnable": boolean
    }
  },
  "features": [
    {
```

```
    "additionalConfiguration": [  
      {  
        "autoEnable": "string",  
        "name": "string"  
      }  
    ],  
    "autoEnable": "string",  
    "name": "string"  
  }  
]
```

## URI Request Parameters

The request uses the following URI parameters.

### detectorId

The ID of the detector that configures the delegated administrator.

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

## Request Body

The request accepts the following data in JSON format.

### autoEnable

*This parameter has been deprecated.*

Represents whether or not to automatically enable member accounts in the organization.

Even though this is still supported, we recommend using `AutoEnableOrganizationMembers` to achieve the similar results. You must provide a value for either `autoEnableOrganizationMembers` or `autoEnable`.

Type: Boolean

Required: No

## autoEnableOrganizationMembers

Indicates the auto-enablement configuration of GuardDuty for the member accounts in the organization. You must provide a value for either `autoEnableOrganizationMembers` or `autoEnable`.

Use one of the following configuration values for `autoEnableOrganizationMembers`:

- **NEW**: Indicates that when a new account joins the organization, they will have GuardDuty enabled automatically.
- **ALL**: Indicates that all accounts in the organization have GuardDuty enabled automatically. This includes NEW accounts that join the organization and accounts that may have been suspended or removed from the organization in GuardDuty.

It may take up to 24 hours to update the configuration for all the member accounts.

- **NONE**: Indicates that GuardDuty will not be automatically enabled for any account in the organization. The administrator must manage GuardDuty for each account in the organization individually.

When you update the auto-enable setting from ALL or NEW to NONE, this action doesn't disable the corresponding option for your existing accounts. This configuration will apply to the new accounts that join the organization. After you update the auto-enable settings, no new account will have the corresponding option as enabled.

Type: String

Valid Values: NEW | ALL | NONE

Required: No

## dataSources

*This parameter has been deprecated.*

Describes which data sources will be updated.

Type: [OrganizationDataSourceConfigurations](#) object

Required: No

## features

A list of features that will be configured for the organization.

Type: Array of [OrganizationFeatureConfiguration](#) objects

Required: No

## Response Syntax

```
HTTP/1.1 200
```

## Response Elements

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

## Errors

For information about the errors that are common to all actions, see [Common Errors](#).

### BadRequestException

A bad request exception object.

HTTP Status Code: 400

### InternalServerErrorException

An internal server error exception object.

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 v2](#)
- [AWS SDK for Java V2](#)

- [AWS SDK for JavaScript V3](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

# UpdatePublishingDestination

Updates information about the publishing destination specified by the `destinationId`.

## Request Syntax

```
POST /detector/detectorId/publishingDestination/destinationId HTTP/1.1
Content-type: application/json
```

```
{
  "destinationProperties": {
    "destinationArn": "string",
    "kmsKeyArn": "string"
  }
}
```

## URI Request Parameters

The request uses the following URI parameters.

### destinationId

The ID of the publishing destination to update.

Required: Yes

### detectorId

The ID of the detector associated with the publishing destinations to update.

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

## Request Body

The request accepts the following data in JSON format.

### destinationProperties

A `DestinationProperties` object that includes the `DestinationArn` and `KmsKeyArn` of the publishing destination.

Type: [DestinationProperties](#) object

Required: No

## Response Syntax

```
HTTP/1.1 200
```

## Response Elements

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

## Errors

For information about the errors that are common to all actions, see [Common Errors](#).

### BadRequestException

A bad request exception object.

HTTP Status Code: 400

### InternalServerErrorException

An internal server error exception object.

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 v2](#)
- [AWS SDK for Java V2](#)

- [AWS SDK for JavaScript V3](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)



# UpdateThreatIntelSet

Updates the ThreatIntelSet specified by the ThreatIntelSet ID.

## Request Syntax

```
POST /detector/detectorId/threatintelset/threatIntelSetId HTTP/1.1
Content-type: application/json
```

```
{
  "activate": boolean,
  "location": "string",
  "name": "string"
}
```

## URI Request Parameters

The request uses the following URI parameters.

### detectorId

The detectorID that specifies the GuardDuty service whose ThreatIntelSet you want to update.

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

### threatIntelSetId

The unique ID that specifies the ThreatIntelSet that you want to update.

Required: Yes

## Request Body

The request accepts the following data in JSON format.

### activate

The updated Boolean value that specifies whether the ThreatIntelSet is active or not.

Type: Boolean

Required: No

### location

The updated URI of the file that contains the ThreatIntelSet.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: No

### name

The unique ID that specifies the ThreatIntelSet that you want to update.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: No

## Response Syntax

```
HTTP/1.1 200
```

## Response Elements

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

## Errors

For information about the errors that are common to all actions, see [Common Errors](#).

### **BadRequestException**

A bad request exception object.

HTTP Status Code: 400

### **InternalServerErrorException**

An internal server error exception object.

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 v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

# Data Types

The Amazon GuardDuty 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:

- [AccessControlList](#)
- [AccessKeyDetails](#)
- [AccountDetail](#)
- [AccountFreeTrialInfo](#)
- [AccountLevelPermissions](#)
- [Action](#)
- [AddonDetails](#)
- [AdminAccount](#)
- [Administrator](#)
- [AgentDetails](#)
- [Anomaly](#)
- [AnomalyObject](#)
- [AnomalyUnusual](#)
- [AwsApiCallAction](#)
- [BlockPublicAccess](#)
- [BucketLevelPermissions](#)
- [BucketPolicy](#)
- [City](#)
- [CloudTrailConfigurationResult](#)
- [Condition](#)

- [Container](#)
- [ContainerInstanceDetails](#)
- [Country](#)
- [CoverageEc2InstanceDetails](#)
- [CoverageEcsClusterDetails](#)
- [CoverageEksClusterDetails](#)
- [CoverageFilterCondition](#)
- [CoverageFilterCriteria](#)
- [CoverageFilterCriterion](#)
- [CoverageResource](#)
- [CoverageResourceDetails](#)
- [CoverageSortCriteria](#)
- [CoverageStatistics](#)
- [CreateProtectedResource](#)
- [CreateS3BucketResource](#)
- [DataSourceConfigurations](#)
- [DataSourceConfigurationsResult](#)
- [DataSourceFreeTrial](#)
- [DataSourcesFreeTrial](#)
- [DefaultServerSideEncryption](#)
- [Destination](#)
- [DestinationProperties](#)
- [Detection](#)
- [DetectorAdditionalConfiguration](#)
- [DetectorAdditionalConfigurationResult](#)
- [DetectorFeatureConfiguration](#)
- [DetectorFeatureConfigurationResult](#)
- [DNSLogsConfigurationResult](#)
- [DnsRequestAction](#)
- [DomainDetails](#)

- [EbsVolumeDetails](#)
- [EbsVolumeScanDetails](#)
- [EbsVolumesResult](#)
- [EcsClusterDetails](#)
- [EcsTaskDetails](#)
- [EksClusterDetails](#)
- [Evidence](#)
- [FargateDetails](#)
- [FilterCondition](#)
- [FilterCriteria](#)
- [FilterCriterion](#)
- [Finding](#)
- [FindingCriteria](#)
- [FindingStatistics](#)
- [FlowLogsConfigurationResult](#)
- [FreeTrialFeatureConfigurationResult](#)
- [GeoLocation](#)
- [HighestSeverityThreatDetails](#)
- [HostPath](#)
- [IamInstanceProfile](#)
- [ImpersonatedUser](#)
- [InstanceDetails](#)
- [Invitation](#)
- [ItemPath](#)
- [KubernetesApiCallAction](#)
- [KubernetesAuditLogsConfiguration](#)
- [KubernetesAuditLogsConfigurationResult](#)
- [KubernetesConfiguration](#)
- [KubernetesConfigurationResult](#)
- [KubernetesDataSourceFreeTrial](#)

- [KubernetesDetails](#)
- [KubernetesPermissionCheckedDetails](#)
- [KubernetesRoleBindingDetails](#)
- [KubernetesRoleDetails](#)
- [KubernetesUserDetails](#)
- [KubernetesWorkloadDetails](#)
- [LambdaDetails](#)
- [LineageObject](#)
- [LocalIpDetails](#)
- [LocalPortDetails](#)
- [LoginAttribute](#)
- [MalwareProtectionConfiguration](#)
- [MalwareProtectionConfigurationResult](#)
- [MalwareProtectionDataSourceFreeTrial](#)
- [MalwareProtectionPlanActions](#)
- [MalwareProtectionPlanStatusReason](#)
- [MalwareProtectionPlanSummary](#)
- [MalwareProtectionPlanTaggingAction](#)
- [MalwareScanDetails](#)
- [Master](#)
- [Member](#)
- [MemberAdditionalConfiguration](#)
- [MemberAdditionalConfigurationResult](#)
- [MemberDataSourceConfiguration](#)
- [MemberFeaturesConfiguration](#)
- [MemberFeaturesConfigurationResult](#)
- [NetworkConnectionAction](#)
- [NetworkInterface](#)
- [Observations](#)
- [Organization](#)

- [OrganizationAdditionalConfiguration](#)
- [OrganizationAdditionalConfigurationResult](#)
- [OrganizationDataSourceConfigurations](#)
- [OrganizationDataSourceConfigurationsResult](#)
- [OrganizationDetails](#)
- [OrganizationEbsVolumes](#)
- [OrganizationEbsVolumesResult](#)
- [OrganizationFeatureConfiguration](#)
- [OrganizationFeatureConfigurationResult](#)
- [OrganizationFeatureStatistics](#)
- [OrganizationFeatureStatisticsAdditionalConfiguration](#)
- [OrganizationKubernetesAuditLogsConfiguration](#)
- [OrganizationKubernetesAuditLogsConfigurationResult](#)
- [OrganizationKubernetesConfiguration](#)
- [OrganizationKubernetesConfigurationResult](#)
- [OrganizationMalwareProtectionConfiguration](#)
- [OrganizationMalwareProtectionConfigurationResult](#)
- [OrganizationS3LogsConfiguration](#)
- [OrganizationS3LogsConfigurationResult](#)
- [OrganizationScanEc2InstanceWithFindings](#)
- [OrganizationScanEc2InstanceWithFindingsResult](#)
- [OrganizationStatistics](#)
- [Owner](#)
- [PermissionConfiguration](#)
- [PortProbeAction](#)
- [PortProbeDetail](#)
- [PrivateIpAddressDetails](#)
- [ProcessDetails](#)
- [ProductCode](#)
- [PublicAccess](#)



- [RdsDbInstanceDetails](#)
- [RdsDbUserDetails](#)
- [RdsLoginAttemptAction](#)
- [RemoteAccountDetails](#)
- [RemoteIpDetails](#)
- [RemotePortDetails](#)
- [Resource](#)
- [ResourceDetails](#)
- [RuntimeContext](#)
- [RuntimeDetails](#)
- [S3BucketDetail](#)
- [S3LogsConfiguration](#)
- [S3LogsConfigurationResult](#)
- [S3ObjectDetail](#)
- [Scan](#)
- [ScanCondition](#)
- [ScanConditionPair](#)
- [ScanDetections](#)
- [ScanEc2InstanceWithFindings](#)
- [ScanEc2InstanceWithFindingsResult](#)
- [ScanFilePath](#)
- [ScannedItemCount](#)
- [ScanResourceCriteria](#)
- [ScanResultDetails](#)
- [ScanThreatName](#)
- [SecurityContext](#)
- [SecurityGroup](#)
- [Service](#)
- [ServiceAdditionalInfo](#)
- [SortCriteria](#)

- [Tag](#)
- [Threat](#)
- [ThreatDetectedByName](#)
- [ThreatIntelligenceDetail](#)
- [ThreatsDetectedItemCount](#)
- [Total](#)
- [TriggerDetails](#)
- [UnprocessedAccount](#)
- [UnprocessedDataSourcesResult](#)
- [UpdateProtectedResource](#)
- [UpdateS3BucketResource](#)
- [UsageAccountResult](#)
- [UsageCriteria](#)
- [UsageDataSourceResult](#)
- [UsageFeatureResult](#)
- [UsageResourceResult](#)
- [UsageStatistics](#)
- [UsageTopAccountResult](#)
- [UsageTopAccountsResult](#)
- [Volume](#)
- [VolumeDetail](#)
- [VolumeMount](#)
- [VpcConfig](#)

# AccessControlList

Contains information on the current access control policies for the bucket.

## Contents

### **allowsPublicReadAccess**

A value that indicates whether public read access for the bucket is enabled through an Access Control List (ACL).

Type: Boolean

Required: No

### **allowsPublicWriteAccess**

A value that indicates whether public write access for the bucket is enabled through an Access Control List (ACL).

Type: Boolean

Required: No

## See Also

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

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

# AccessKeyDetails

Contains information about the access keys.

## Contents

### **accessKeyId**

The access key ID of the user.

Type: String

Required: No

### **principalId**

The principal ID of the user.

Type: String

Required: No

### **userName**

The name of the user.

Type: String

Required: No

### **userType**

The type of the user.

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 Java V2](#)
- [AWS SDK for Ruby V3](#)

# AccountDetail

Contains information about the account.

## Contents

### accountId

The member account ID.

Type: String

Length Constraints: Fixed length of 12.

Required: Yes

### email

The email address of the member account.

Type: String

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

Required: Yes

## See Also

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

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

# AccountFreeTrialInfo

Provides details of the GuardDuty member account that uses a free trial service.

## Contents

### accountId

The account identifier of the GuardDuty member account.

Type: String

Required: No

### dataSources

*This member has been deprecated.*

Describes the data source enabled for the GuardDuty member account.

Type: [DataSourcesFreeTrial](#) object

Required: No

### features

A list of features enabled for the GuardDuty account.

Type: Array of [FreeTrialFeatureConfigurationResult](#) 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 Java V2](#)
- [AWS SDK for Ruby V3](#)

# AccountLevelPermissions

Contains information about the account level permissions on the S3 bucket.

## Contents

### **blockPublicAccess**

Describes the S3 Block Public Access settings of the bucket's parent account.

Type: [BlockPublicAccess](#) object

Required: No

## See Also

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

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)



# Action

Contains information about actions.

## Contents

### **actionType**

The GuardDuty finding activity type.

Type: String

Required: No

### **awsApiCallAction**

Information about the AWS\_API\_CALL action described in this finding.

Type: [AwsApiCallAction](#) object

Required: No

### **dnsRequestAction**

Information about the DNS\_REQUEST action described in this finding.

Type: [DnsRequestAction](#) object

Required: No

### **kubernetesApiCallAction**

Information about the Kubernetes API call action described in this finding.

Type: [KubernetesApiCallAction](#) object

Required: No

### **kubernetesPermissionCheckedDetails**

Information whether the user has the permission to use a specific Kubernetes API.

Type: [KubernetesPermissionCheckedDetails](#) object

Required: No

## **kubernetesRoleBindingDetails**

Information about the role binding that grants the permission defined in a Kubernetes role.

Type: [KubernetesRoleBindingDetails](#) object

Required: No

## **kubernetesRoleDetails**

Information about the Kubernetes role name and role type.

Type: [KubernetesRoleDetails](#) object

Required: No

## **networkConnectionAction**

Information about the NETWORK\_CONNECTION action described in this finding.

Type: [NetworkConnectionAction](#) object

Required: No

## **portProbeAction**

Information about the PORT\_PROBE action described in this finding.

Type: [PortProbeAction](#) object

Required: No

## **rdsLoginAttemptAction**

Information about RDS\_LOGIN\_ATTEMPT action described in this finding.

Type: [RdsLoginAttemptAction](#) object

Required: No

## **See Also**

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

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

# AddonDetails

Information about the installed EKS add-on (GuardDuty security agent).

## Contents

### **addonStatus**

Status of the installed EKS add-on.

Type: String

Required: No

### **addonVersion**

Version of the installed EKS add-on.

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 Java V2](#)
- [AWS SDK for Ruby V3](#)

# AdminAccount

The account within the organization specified as the GuardDuty delegated administrator.

## Contents

### adminAccountId

The AWS account ID for the account.

Type: String

Required: No

### adminStatus

Indicates whether the account is enabled as the delegated administrator.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 300.

Valid Values: ENABLED | DISABLE\_IN\_PROGRESS

Required: No

## See Also

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

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

# Administrator

Contains information about the administrator account and invitation.

## Contents

### **accountId**

The ID of the account used as the administrator account.

Type: String

Length Constraints: Fixed length of 12.

Required: No

### **invitationId**

The value that is used to validate the administrator account to the member account.

Type: String

Required: No

### **invitedAt**

The timestamp when the invitation was sent.

Type: String

Required: No

### **relationshipStatus**

The status of the relationship between the administrator and member accounts.

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 Java V2](#)
- [AWS SDK for Ruby V3](#)

# AgentDetails

Information about the installed GuardDuty security agent.

## Contents

### version

Version of the installed GuardDuty security agent.

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 Java V2](#)
- [AWS SDK for Ruby V3](#)



# Anomaly

Contains information about the anomalies.

## Contents

### profiles

Information about the types of profiles.

Type: String to string to array of [AnomalyObject](#) objects map map

Required: No

### unusual

Information about the behavior of the anomalies.

Type: [AnomalyUnusual](#) object

Required: No

## See Also

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

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

# AnomalyObject

Contains information about the unusual anomalies.

## Contents

### observations

The recorded value.

Type: [Observations](#) object

Required: No

### profileSubtype

The frequency of the anomaly.

Type: String

Valid Values: FREQUENT | INFREQUENT | UNSEEN | RARE

Required: No

### profileType

The type of behavior of the profile.

Type: String

Valid Values: FREQUENCY

Required: No

## See Also

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

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)



# AnomalyUnusual

Contains information about the behavior of the anomaly that is new to GuardDuty.

## Contents

### behavior

The behavior of the anomalous activity that caused GuardDuty to generate the finding.

Type: String to string to [AnomalyObject](#) object map map

Required: No

## See Also

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

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

# AwsApiCallAction

Contains information about the API action.

## Contents

### **affectedResources**

The details of the AWS account that made the API call. This field identifies the resources that were affected by this API call.

Type: String to string map

Required: No

### **api**

The AWS API name.

Type: String

Required: No

### **callerType**

The AWS API caller type.

Type: String

Required: No

### **domainDetails**

The domain information for the AWS API call.

Type: [DomainDetails](#) object

Required: No

### **errorCode**

The error code of the failed AWS API action.

Type: String

Required: No

## remoteAccountDetails

The details of the AWS account that made the API call. This field appears if the call was made from outside your account.

Type: [RemoteAccountDetails](#) object

Required: No

## remoteIpDetails

The remote IP information of the connection that initiated the AWS API call.

Type: [RemoteIpDetails](#) object

Required: No

## serviceName

The AWS service name whose API was invoked.

Type: String

Required: No

## userAgent

The agent through which the API request was made.

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 Java V2](#)
- [AWS SDK for Ruby V3](#)

# BlockPublicAccess

Contains information on how the bucket owner's S3 Block Public Access settings are being applied to the S3 bucket. See [S3 Block Public Access](#) for more information.

## Contents

### **blockPublicAcls**

Indicates if S3 Block Public Access is set to `BlockPublicAcls`.

Type: Boolean

Required: No

### **blockPublicPolicy**

Indicates if S3 Block Public Access is set to `BlockPublicPolicy`.

Type: Boolean

Required: No

### **ignorePublicAcls**

Indicates if S3 Block Public Access is set to `IgnorePublicAcls`.

Type: Boolean

Required: No

### **restrictPublicBuckets**

Indicates if S3 Block Public Access is set to `RestrictPublicBuckets`.

Type: Boolean

Required: No

## See Also

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

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)



# BucketLevelPermissions

Contains information about the bucket level permissions for the S3 bucket.

## Contents

### **accessControlList**

Contains information on how Access Control Policies are applied to the bucket.

Type: [AccessControlList](#) object

Required: No

### **blockPublicAccess**

Contains information on which account level S3 Block Public Access settings are applied to the S3 bucket.

Type: [BlockPublicAccess](#) object

Required: No

### **bucketPolicy**

Contains information on the bucket policies for the S3 bucket.

Type: [BucketPolicy](#) object

Required: No

## See Also

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

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

# BucketPolicy

Contains information on the current bucket policies for the S3 bucket.

## Contents

### **allowsPublicReadAccess**

A value that indicates whether public read access for the bucket is enabled through a bucket policy.

Type: Boolean

Required: No

### **allowsPublicWriteAccess**

A value that indicates whether public write access for the bucket is enabled through a bucket policy.

Type: Boolean

Required: No

## See Also

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

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

# City

Contains information about the city associated with the IP address.

## Contents

### cityName

The city name of the remote IP address.

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 Java V2](#)
- [AWS SDK for Ruby V3](#)

# CloudTrailConfigurationResult

Contains information on the status of CloudTrail as a data source for the detector.

## Contents

### status

Describes whether CloudTrail is enabled as a data source for the detector.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 300.

Valid Values: ENABLED | DISABLED

Required: Yes

## See Also

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

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

# Condition

Contains information about the condition.

## Contents

### eq

*This member has been deprecated.*

Represents the *equal* condition to be applied to a single field when querying for findings.

Type: Array of strings

Required: No

### equals

Represents an *equal* condition to be applied to a single field when querying for findings.

Type: Array of strings

Required: No

### greaterThan

Represents a *greater than* condition to be applied to a single field when querying for findings.

Type: Long

Required: No

### greaterThanOrEqualTo

Represents a *greater than or equal* condition to be applied to a single field when querying for findings.

Type: Long

Required: No

### gt

*This member has been deprecated.*

Represents a *greater than* condition to be applied to a single field when querying for findings.

Type: Integer

Required: No

### **gte**

*This member has been deprecated.*

Represents a *greater than or equal* condition to be applied to a single field when querying for findings.

Type: Integer

Required: No

### **lessThan**

Represents a *less than* condition to be applied to a single field when querying for findings.

Type: Long

Required: No

### **lessThanOrEqualTo**

Represents a *less than or equal* condition to be applied to a single field when querying for findings.

Type: Long

Required: No

### **lt**

*This member has been deprecated.*

Represents a *less than* condition to be applied to a single field when querying for findings.

Type: Integer

Required: No

### **lte**

*This member has been deprecated.*

Represents a *less than or equal* condition to be applied to a single field when querying for findings.

Type: Integer

Required: No

### **neq**

*This member has been deprecated.*

Represents the *not equal* condition to be applied to a single field when querying for findings.

Type: Array of strings

Required: No

### **notEquals**

Represents a *not equal* condition to be applied to a single field when querying for findings.

Type: Array of strings

Required: No

## **See Also**

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

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

# Container

Details of a container.

## Contents

### **containerRuntime**

The container runtime (such as, Docker or containerd) used to run the container.

Type: String

Required: No

### **id**

Container ID.

Type: String

Required: No

### **image**

Container image.

Type: String

Required: No

### **imagePrefix**

Part of the image name before the last slash. For example, imagePrefix for public.ecr.aws/amazonlinux/amazonlinux:latest would be public.ecr.aws/amazonlinux. If the image name is relative and does not have a slash, this field is empty.

Type: String

Required: No

### **name**

Container name.

Type: String



Required: No

### **securityContext**

Container security context.

Type: [SecurityContext](#) object

Required: No

### **volumeMounts**

Container volume mounts.

Type: Array of [VolumeMount](#) 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 Java V2](#)
- [AWS SDK for Ruby V3](#)

# ContainerInstanceDetails

Contains information about the Amazon EC2 instance that is running the Amazon ECS container.

## Contents

### **compatibleContainerInstances**

Represents total number of nodes in the Amazon ECS cluster.

Type: Long

Required: No

### **coveredContainerInstances**

Represents the nodes in the Amazon ECS cluster that has a HEALTHY coverage status.

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 Java V2](#)
- [AWS SDK for Ruby V3](#)

# Country

Contains information about the country where the remote IP address is located.

## Contents

### **countryCode**

The country code of the remote IP address.

Type: String

Required: No

### **countryName**

The country name of the remote IP address.

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 Java V2](#)
- [AWS SDK for Ruby V3](#)

# CoverageEc2InstanceDetails

Contains information about the Amazon EC2 instance runtime coverage details.

## Contents

### **agentDetails**

Information about the installed security agent.

Type: [AgentDetails](#) object

Required: No

### **clusterArn**

The cluster ARN of the Amazon ECS cluster running on the Amazon EC2 instance.

Type: String

Required: No

### **instanceId**

The Amazon EC2 instance ID.

Type: String

Required: No

### **instanceType**

The instance type of the Amazon EC2 instance.

Type: String

Required: No

### **managementType**

Indicates how the GuardDuty security agent is managed for this resource.

- `AUTO_MANAGED` indicates that GuardDuty deploys and manages updates for this resource.
- `MANUAL` indicates that you are responsible to deploy, update, and manage the GuardDuty security agent updates for this resource.

**Note**

The DISABLED status doesn't apply to Amazon EC2 instances and Amazon EKS clusters.

Type: String

Valid Values: AUTO\_MANAGED | MANUAL | DISABLED

Required: No

## See Also

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

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

# CoverageEcsClusterDetails

Contains information about Amazon ECS cluster runtime coverage details.

## Contents

### clusterName

The name of the Amazon ECS cluster.

Type: String

Required: No

### containerInstanceDetails

Information about the Amazon ECS container running on Amazon EC2 instance.

Type: [ContainerInstanceDetails](#) object

Required: No

### fargateDetails

Information about the Fargate details associated with the Amazon ECS cluster.

Type: [FargateDetails](#) object

Required: No

## See Also

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

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

# CoverageEksClusterDetails

Information about the EKS cluster that has a coverage status.

## Contents

### addonDetails

Information about the installed EKS add-on.

Type: [AddonDetails](#) object

Required: No

### clusterName

Name of the EKS cluster.

Type: String

Required: No

### compatibleNodes

Represents all the nodes within the EKS cluster in your account.

Type: Long

Required: No

### coveredNodes

Represents the nodes within the EKS cluster that have a HEALTHY coverage status.

Type: Long

Required: No

### managementType

Indicates how the Amazon EKS add-on GuardDuty agent is managed for this EKS cluster.

AUTO\_MANAGED indicates GuardDuty deploys and manages updates for this resource.

MANUAL indicates that you are responsible to deploy, update, and manage the Amazon EKS add-on GuardDuty agent for this resource.

Type: String

Valid Values: AUTO\_MANAGED | MANUAL | DISABLED

Required: No

## See Also

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

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)



# CoverageFilterCondition

Represents a condition that when matched will be added to the response of the operation.

## Contents

### **equals**

Represents an equal condition that is applied to a single field while retrieving the coverage details.

Type: Array of strings

Required: No

### **notEquals**

Represents a not equal condition that is applied to a single field while retrieving the coverage details.

Type: Array of strings

Required: No

## See Also

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

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

# CoverageFilterCriteria

Represents the criteria used in the filter.

## Contents

### filterCriterion

Represents a condition that when matched will be added to the response of the operation.

Type: Array of [CoverageFilterCriterion](#) objects

Array Members: Minimum number of 0 items. Maximum number of 50 items.

Required: No

## See Also

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

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

# CoverageFilterCriterion

Represents a condition that when matched will be added to the response of the operation.

## Contents

### critierionKey

An enum value representing possible filter fields.

#### Note

Replace the enum value CLUSTER\_NAME with EKS\_CLUSTER\_NAME. CLUSTER\_NAME has been deprecated.

Type: String

Valid Values: ACCOUNT\_ID | CLUSTER\_NAME | RESOURCE\_TYPE | COVERAGE\_STATUS | ADDON\_VERSION | MANAGEMENT\_TYPE | EKS\_CLUSTER\_NAME | ECS\_CLUSTER\_NAME | AGENT\_VERSION | INSTANCE\_ID | CLUSTER\_ARN

Required: No

### filterCondition

Contains information about the condition.

Type: [CoverageFilterCondition](#) object

Required: No

## See Also

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

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)



# CoverageResource

Information about the resource of the GuardDuty account.

## Contents

### **accountId**

The unique ID of the AWS account.

Type: String

Length Constraints: Fixed length of 12.

Required: No

### **coverageStatus**

Represents the status of the EKS cluster coverage.

Type: String

Valid Values: HEALTHY | UNHEALTHY

Required: No

### **detectorId**

The unique ID of the GuardDuty detector associated with the resource.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: No

### **issue**

Represents the reason why a coverage status was UNHEALTHY for the EKS cluster.

Type: String

Required: No

### **resourceDetails**

Information about the resource for which the coverage statistics are retrieved.

Type: [CoverageResourceDetails](#) object

Required: No

### **resourceId**

The unique ID of the resource.

Type: String

Required: No

### **updatedAt**

The timestamp at which the coverage details for the resource were last updated. This is in UTC format.

Type: Timestamp

Required: No

## **See Also**

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

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

# CoverageResourceDetails

Information about the resource for each individual EKS cluster.

## Contents

### ec2InstanceDetails

Information about the Amazon EC2 instance assessed for runtime coverage.

Type: [CoverageEc2InstanceDetails](#) object

Required: No

### ecsClusterDetails

Information about the Amazon ECS cluster that is assessed for runtime coverage.

Type: [CoverageEcsClusterDetails](#) object

Required: No

### eksClusterDetails

EKS cluster details involved in the coverage statistics.

Type: [CoverageEksClusterDetails](#) object

Required: No

### resourceType

The type of AWS resource.

Type: String

Valid Values: EKS | ECS | EC2

Required: No

## See Also

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

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)



# CoverageSortCriteria

Information about the sorting criteria used in the coverage statistics.

## Contents

### attributeName

Represents the field name used to sort the coverage details.

#### Note

Replace the enum value CLUSTER\_NAME with EKS\_CLUSTER\_NAME. CLUSTER\_NAME has been deprecated.

Type: String

Valid Values: ACCOUNT\_ID | CLUSTER\_NAME | COVERAGE\_STATUS | ISSUE | ADDON\_VERSION | UPDATED\_AT | EKS\_CLUSTER\_NAME | ECS\_CLUSTER\_NAME | INSTANCE\_ID

Required: No

### orderBy

The order in which the sorted findings are to be displayed.

Type: String

Valid Values: ASC | DESC

Required: No

## See Also

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

- [AWS SDK for C++](#)

- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

# CoverageStatistics

Information about the coverage statistics for a resource.

## Contents

### **countByCoverageStatus**

Represents coverage statistics for EKS clusters aggregated by coverage status.

Type: String to long map

Valid Keys: HEALTHY | UNHEALTHY

Required: No

### **countByResourceType**

Represents coverage statistics for EKS clusters aggregated by resource type.

Type: String to long map

Valid Keys: EKS | ECS | EC2

Required: No

## See Also

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

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

# CreateProtectedResource

Information about the protected resource that is associated with the created Malware Protection plan. Presently, S3Bucket is the only supported protected resource.

## Contents

### s3Bucket

Information about the protected S3 bucket resource.

Type: [CreateS3BucketResource](#) object

Required: No

## See Also

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

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

# CreateS3BucketResource

Information about the protected S3 bucket resource.

## Contents

### bucketName

Name of the S3 bucket.

Type: String

Required: No

### objectPrefixes

Information about the specified object prefixes. The S3 object will be scanned only if it belongs to any of the specified object prefixes.

Type: Array of strings

Array Members: Minimum number of 0 items. Maximum number of 5 items.

Required: No

## See Also

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

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

# DataSourceConfigurations

Contains information about which data sources are enabled.

## Contents

### kubernetes

Describes whether any Kubernetes logs are enabled as data sources.

Type: [KubernetesConfiguration](#) object

Required: No

### malwareProtection

Describes whether Malware Protection is enabled as a data source.

Type: [MalwareProtectionConfiguration](#) object

Required: No

### s3Logs

Describes whether S3 data event logs are enabled as a data source.

Type: [S3LogsConfiguration](#) object

Required: No

## See Also

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

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

# DataSourceConfigurationsResult

Contains information on the status of data sources for the detector.

## Contents

### cloudTrail

An object that contains information on the status of CloudTrail as a data source.

Type: [CloudTrailConfigurationResult](#) object

Required: Yes

### dnsLogs

An object that contains information on the status of DNS logs as a data source.

Type: [DNSLogsConfigurationResult](#) object

Required: Yes

### flowLogs

An object that contains information on the status of VPC flow logs as a data source.

Type: [FlowLogsConfigurationResult](#) object

Required: Yes

### s3Logs

An object that contains information on the status of S3 Data event logs as a data source.

Type: [S3LogsConfigurationResult](#) object

Required: Yes

### kubernetes

An object that contains information on the status of all Kubernetes data sources.

Type: [KubernetesConfigurationResult](#) object

Required: No

## malwareProtection

Describes the configuration of Malware Protection data sources.

Type: [MalwareProtectionConfigurationResult](#) object

Required: No

## See Also

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

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)



# DataSourceFreeTrial

Contains information about which data sources are enabled for the GuardDuty member account.

## Contents

### freeTrialDaysRemaining

A value that specifies the number of days left to use each enabled data source.

Type: Integer

Required: No

## See Also

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

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

# DataSourcesFreeTrial

Contains information about which data sources are enabled for the GuardDuty member account.

## Contents

### cloudTrail

Describes whether any AWS CloudTrail management event logs are enabled as data sources.

Type: [DataSourceFreeTrial](#) object

Required: No

### dnsLogs

Describes whether any DNS logs are enabled as data sources.

Type: [DataSourceFreeTrial](#) object

Required: No

### flowLogs

Describes whether any VPC Flow logs are enabled as data sources.

Type: [DataSourceFreeTrial](#) object

Required: No

### kubernetes

Describes whether any Kubernetes logs are enabled as data sources.

Type: [KubernetesDataSourceFreeTrial](#) object

Required: No

### malwareProtection

Describes whether Malware Protection is enabled as a data source.

Type: [MalwareProtectionDataSourceFreeTrial](#) object

Required: No

## s3Logs

Describes whether any S3 data event logs are enabled as data sources.

Type: [DataSourceFreeTrial](#) object

Required: No

## See Also

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

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

# DefaultServerSideEncryption

Contains information on the server side encryption method used in the S3 bucket. See [S3 Server-Side Encryption](#) for more information.

## Contents

### encryptionType

The type of encryption used for objects within the S3 bucket.

Type: String

Required: No

### kmsMasterKeyArn

The Amazon Resource Name (ARN) of the KMS encryption key. Only available if the bucket `EncryptionType` is `aws:kms`.

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 Java V2](#)
- [AWS SDK for Ruby V3](#)

# Destination

Contains information about the publishing destination, including the ID, type, and status.

## Contents

### **destinationId**

The unique ID of the publishing destination.

Type: String

Required: Yes

### **destinationType**

The type of resource used for the publishing destination. Currently, only Amazon S3 buckets are supported.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 300.

Valid Values: S3

Required: Yes

### **status**

The status of the publishing destination.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 300.

Valid Values: PENDING\_VERIFICATION | PUBLISHING | UNABLE\_TO\_PUBLISH\_FIX\_DESTINATION\_PROPERTY | STOPPED

Required: Yes

## See Also

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

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

# DestinationProperties

Contains the Amazon Resource Name (ARN) of the resource to publish to, such as an S3 bucket, and the ARN of the KMS key to use to encrypt published findings.

## Contents

### destinationArn

The ARN of the resource to publish to.

To specify an S3 bucket folder use the following format: `arn:aws:s3:::DOC-EXAMPLE-BUCKET/myFolder/`

Type: String

Required: No

### kmsKeyArn

The ARN of the KMS key to use for encryption.

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 Java V2](#)
- [AWS SDK for Ruby V3](#)

# Detection

Contains information about the detected behavior.

## Contents

### **anomaly**

The details about the anomalous activity that caused GuardDuty to generate the finding.

Type: [Anomaly](#) object

Required: No

## See Also

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

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)



# DetectorAdditionalConfiguration

Information about the additional configuration for a feature in your GuardDuty account.

## Contents

### name

Name of the additional configuration.

Type: String

Valid Values: EKS\_ADDON\_MANAGEMENT | ECS\_FARGATE\_AGENT\_MANAGEMENT | EC2\_AGENT\_MANAGEMENT

Required: No

### status

Status of the additional configuration.

Type: String

Valid Values: ENABLED | DISABLED

Required: No

## See Also

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

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

# DetectorAdditionalConfigurationResult

Information about the additional configuration.

## Contents

### name

Name of the additional configuration.

Type: String

Valid Values: EKS\_ADDON\_MANAGEMENT | ECS\_FARGATE\_AGENT\_MANAGEMENT | EC2\_AGENT\_MANAGEMENT

Required: No

### status

Status of the additional configuration.

Type: String

Valid Values: ENABLED | DISABLED

Required: No

### updatedAt

The timestamp at which the additional configuration was last updated. This is in UTC format.

Type: Timestamp

Required: No

## See Also

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

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)

- [AWS SDK for Ruby V3](#)

# DetectorFeatureConfiguration

Contains information about a GuardDuty feature.

Specifying both EKS Runtime Monitoring (EKS\_RUNTIME\_MONITORING) and Runtime Monitoring (RUNTIME\_MONITORING) will cause an error. You can add only one of these two features because Runtime Monitoring already includes the threat detection for Amazon EKS resources. For more information, see [Runtime Monitoring](#).

## Contents

### additionalConfiguration

Additional configuration for a resource.

Type: Array of [DetectorAdditionalConfiguration](#) objects

Required: No

### name

The name of the feature.

Type: String

Valid Values: S3\_DATA\_EVENTS | EKS\_AUDIT\_LOGS | EBS\_MALWARE\_PROTECTION  
| RDS\_LOGIN\_EVENTS | EKS\_RUNTIME\_MONITORING | LAMBDA\_NETWORK\_LOGS |  
RUNTIME\_MONITORING

Required: No

### status

The status of the feature.

Type: String

Valid Values: ENABLED | DISABLED

Required: No

## See Also

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

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

# DetectorFeatureConfigurationResult

Contains information about a GuardDuty feature.

Specifying both EKS Runtime Monitoring (EKS\_RUNTIME\_MONITORING) and Runtime Monitoring (RUNTIME\_MONITORING) will cause an error. You can add only one of these two features because Runtime Monitoring already includes the threat detection for Amazon EKS resources. For more information, see [Runtime Monitoring](#).

## Contents

### additionalConfiguration

Additional configuration for a resource.

Type: Array of [DetectorAdditionalConfigurationResult](#) objects

Required: No

### name

Indicates the name of the feature that can be enabled for the detector.

Type: String

Valid Values: FLOW\_LOGS | CLOUD\_TRAIL | DNS\_LOGS | S3\_DATA\_EVENTS  
| EKS\_AUDIT\_LOGS | EBS\_MALWARE\_PROTECTION | RDS\_LOGIN\_EVENTS |  
EKS\_RUNTIME\_MONITORING | LAMBDA\_NETWORK\_LOGS | RUNTIME\_MONITORING

Required: No

### status

Indicates the status of the feature that is enabled for the detector.

Type: String

Valid Values: ENABLED | DISABLED

Required: No

### updatedAt

The timestamp at which the feature object was updated.

Type: Timestamp

Required: No

## See Also

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

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

# DNSLogsConfigurationResult

Contains information on the status of DNS logs as a data source.

## Contents

### status

Denotes whether DNS logs is enabled as a data source.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 300.

Valid Values: ENABLED | DISABLED

Required: Yes

## See Also

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

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)



# DnsRequestAction

Contains information about the DNS\_REQUEST action described in this finding.

## Contents

### blocked

Indicates whether the targeted port is blocked.

Type: Boolean

Required: No

### domain

The domain information for the DNS query.

Type: String

Required: No

### domainWithSuffix

The second and top level domain involved in the activity that potentially prompted GuardDuty to generate this finding. For a list of top-level and second-level domains, see [public suffix list](#).

Type: String

Required: No

### protocol

The network connection protocol observed in the activity that prompted GuardDuty to generate the finding.

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 Java V2](#)
- [AWS SDK for Ruby V3](#)

# DomainDetails

Contains information about the domain.

## Contents

### domain

The domain information for the AWS API call.

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 Java V2](#)
- [AWS SDK for Ruby V3](#)

# EbsVolumeDetails

Contains list of scanned and skipped EBS volumes with details.

## Contents

### scannedVolumeDetails

List of EBS volumes that were scanned.

Type: Array of [VolumeDetail](#) objects

Required: No

### skippedVolumeDetails

List of EBS volumes that were skipped from the malware scan.

Type: Array of [VolumeDetail](#) 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 Java V2](#)
- [AWS SDK for Ruby V3](#)

# EbsVolumeScanDetails

Contains details from the malware scan that created a finding.

## Contents

### scanCompletedAt

Returns the completion date and time of the malware scan.

Type: Timestamp

Required: No

### scanDetections

Contains a complete view providing malware scan result details.

Type: [ScanDetections](#) object

Required: No

### scanId

Unique Id of the malware scan that generated the finding.

Type: String

Required: No

### scanStartedAt

Returns the start date and time of the malware scan.

Type: Timestamp

Required: No

### scanType

Specifies the scan type that invoked the malware scan.

Type: String

Valid Values: GUARDDUTY\_INITIATED | ON\_DEMAND

Required: No

### **sources**

Contains list of threat intelligence sources used to detect threats.

Type: Array of strings

Required: No

### **triggerFindingId**

GuardDuty finding ID that triggered a malware scan.

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 Java V2](#)
- [AWS SDK for Ruby V3](#)

# EbsVolumesResult

Describes the configuration of scanning EBS volumes as a data source.

## Contents

### reason

Specifies the reason why scanning EBS volumes (Malware Protection) was not enabled as a data source.

Type: String

Required: No

### status

Describes whether scanning EBS volumes is enabled as a data source.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 300.

Valid Values: ENABLED | DISABLED

Required: No

## See Also

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

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

# EcsClusterDetails

Contains information about the details of the ECS Cluster.

## Contents

### **activeServicesCount**

The number of services that are running on the cluster in an ACTIVE state.

Type: Integer

Required: No

### **arn**

The Amazon Resource Name (ARN) that identifies the cluster.

Type: String

Required: No

### **name**

The name of the ECS Cluster.

Type: String

Required: No

### **registeredContainerInstancesCount**

The number of container instances registered into the cluster.

Type: Integer

Required: No

### **runningTasksCount**

The number of tasks in the cluster that are in the RUNNING state.

Type: Integer

Required: No



**status**

The status of the ECS cluster.

Type: String

Required: No

**tags**

The tags of the ECS Cluster.

Type: Array of [Tag](#) objects

Required: No

**taskDetails**

Contains information about the details of the ECS Task.

Type: [EcsTaskDetails](#) object

Required: No

**See Also**

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

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

# EcsTaskDetails

Contains information about the task in an ECS cluster.

## Contents

### **arn**

The Amazon Resource Name (ARN) of the task.

Type: String

Required: No

### **containers**

The containers that's associated with the task.

Type: Array of [Container](#) objects

Required: No

### **definitionArn**

The ARN of the task definition that creates the task.

Type: String

Required: No

### **group**

The name of the task group that's associated with the task.

Type: String

Required: No

### **startedAt**

The Unix timestamp for the time when the task started.

Type: Timestamp

Required: No

**startedBy**

Contains the tag specified when a task is started.

Type: String

Required: No

**tags**

The tags of the ECS Task.

Type: Array of [Tag](#) objects

Required: No

**createdAt**

The Unix timestamp for the time when the task was created.

Type: Timestamp

Required: No

**version**

The version counter for the task.

Type: String

Required: No

**volumes**

The list of data volume definitions for the task.

Type: Array of [Volume](#) 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 Java V2](#)
- [AWS SDK for Ruby V3](#)

# EksClusterDetails

Details about the EKS cluster involved in a Kubernetes finding.

## Contents

### arn

EKS cluster ARN.

Type: String

Required: No

### createdAt

The timestamp when the EKS cluster was created.

Type: Timestamp

Required: No

### name

EKS cluster name.

Type: String

Required: No

### status

The EKS cluster status.

Type: String

Required: No

### tags

The EKS cluster tags.

Type: Array of [Tag](#) objects

Required: No

## **vpclId**

The VPC ID to which the EKS cluster is attached.

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 Java V2](#)
- [AWS SDK for Ruby V3](#)

# Evidence

Contains information about the reason that the finding was generated.

## Contents

### `threatIntelligenceDetails`

A list of threat intelligence details related to the evidence.

Type: Array of [ThreatIntelligenceDetail](#) 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 Java V2](#)
- [AWS SDK for Ruby V3](#)

# FargateDetails

Contains information about AWS Fargate details associated with an Amazon ECS cluster.

## Contents

### issues

Runtime coverage issues identified for the resource running on AWS Fargate.

Type: Array of strings

Array Members: Minimum number of 0 items. Maximum number of 50 items.

Required: No

### managementType

Indicates how the GuardDuty security agent is managed for this resource.

- `AUTO_MANAGED` indicates that GuardDuty deploys and manages updates for this resource.
- `DISABLED` indicates that the deployment of the GuardDuty security agent is disabled for this resource.

#### Note

The `MANUAL` status doesn't apply to the AWS Fargate (Amazon ECS only) workloads.

Type: String

Valid Values: `AUTO_MANAGED` | `MANUAL` | `DISABLED`

Required: No

## See Also

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

- [AWS SDK for C++](#)



- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

# FilterCondition

Contains information about the condition.

## Contents

### **equalsValue**

Represents an *equal* condition to be applied to a single field when querying for scan entries.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 200.

Required: No

### **greaterThan**

Represents a *greater than* condition to be applied to a single field when querying for scan entries.

Type: Long

Required: No

### **lessThan**

Represents a *less than* condition to be applied to a single field when querying for scan entries.

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 Java V2](#)
- [AWS SDK for Ruby V3](#)



# FilterCriteria

Represents the criteria to be used in the filter for describing scan entries.

## Contents

### filterCriterion

Represents a condition that when matched will be added to the response of the operation.

Type: Array of [FilterCriterion](#) objects

Array Members: Minimum number of 0 items. Maximum number of 1 item.

Required: No

## See Also

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

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

# FilterCriterion

Represents a condition that when matched will be added to the response of the operation. Irrespective of using any filter criteria, an administrator account can view the scan entries for all of its member accounts. However, each member account can view the scan entries only for their own account.

## Contents

### criteriaKey

An enum value representing possible scan properties to match with given scan entries.

#### Note

Replace the enum value CLUSTER\_NAME with EKS\_CLUSTER\_NAME. CLUSTER\_NAME has been deprecated.

Type: String

Valid Values: EC2\_INSTANCE\_ARN | SCAN\_ID | ACCOUNT\_ID | GUARDDUTY\_FINDING\_ID | SCAN\_START\_TIME | SCAN\_STATUS | SCAN\_TYPE

Required: No

### filterCondition

Contains information about the condition.

Type: [FilterCondition](#) object

Required: No

## See Also

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

- [AWS SDK for C++](#)

- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

# Finding

Contains information about the finding that is generated when abnormal or suspicious activity is detected.

## Contents

### **accountId**

The ID of the account in which the finding was generated.

Type: String

Required: Yes

### **arn**

The ARN of the finding.

Type: String

Required: Yes

### **createdAt**

The time and date when the finding was created.

Type: String

Required: Yes

### **id**

The ID of the finding.

Type: String

Required: Yes

### **region**

The Region where the finding was generated.

Type: String

Required: Yes

**resource**

Contains information about the AWS resource associated with the activity that prompted GuardDuty to generate a finding.

Type: [Resource](#) object

Required: Yes

**schemaVersion**

The version of the schema used for the finding.

Type: String

Required: Yes

**severity**

The severity of the finding.

Type: Double

Required: Yes

**type**

The type of finding.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 50.

Required: Yes

**updatedAt**

The time and date when the finding was last updated.

Type: String

Required: Yes

**confidence**

The confidence score for the finding.



Type: Double

Required: No

### **description**

The description of the finding.

Type: String

Required: No

### **partition**

The partition associated with the finding.

Type: String

Required: No

### **service**

Contains additional information about the generated finding.

Type: [Service](#) object

Required: No

### **title**

The title of the finding.

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 Java V2](#)
- [AWS SDK for Ruby V3](#)



# FindingCriteria

Contains information about the criteria used for querying findings.

## Contents

### criteron

Represents a map of finding properties that match specified conditions and values when querying findings.

Type: String to [Condition](#) object map

Required: No

## See Also

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

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

# FindingStatistics

Contains information about finding statistics.

## Contents

### countBySeverity

Represents a map of severity to count statistics for a set of findings.

Type: String to integer map

Required: No

## See Also

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

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

# FlowLogsConfigurationResult

Contains information on the status of VPC flow logs as a data source.

## Contents

### status

Denotes whether VPC flow logs is enabled as a data source.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 300.

Valid Values: ENABLED | DISABLED

Required: Yes

## See Also

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

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

# FreeTrialFeatureConfigurationResult

Contains information about the free trial period for a feature.

## Contents

### freeTrialDaysRemaining

The number of the remaining free trial days for the feature.

Type: Integer

Required: No

### name

The name of the feature for which the free trial is configured.

Type: String

Valid Values: FLOW\_LOGS | CLOUD\_TRAIL | DNS\_LOGS | S3\_DATA\_EVENTS  
| EKS\_AUDIT\_LOGS | EBS\_MALWARE\_PROTECTION | RDS\_LOGIN\_EVENTS  
| EKS\_RUNTIME\_MONITORING | LAMBDA\_NETWORK\_LOGS |  
FARGATE\_RUNTIME\_MONITORING | EC2\_RUNTIME\_MONITORING

Required: No

## See Also

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

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

# GeoLocation

Contains information about the location of the remote IP address.

## Contents

### lat

The latitude information of the remote IP address.

Type: Double

Required: No

### lon

The longitude information of the remote IP address.

Type: Double

Required: No

## See Also

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

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

# HighestSeverityThreatDetails

Contains details of the highest severity threat detected during scan and number of infected files.

## Contents

### count

Total number of infected files with the highest severity threat detected.

Type: Integer

Required: No

### severity

Severity level of the highest severity threat detected.

Type: String

Required: No

### threatName

Threat name of the highest severity threat detected as part of the malware scan.

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 Java V2](#)
- [AWS SDK for Ruby V3](#)



# HostPath

Represents a pre-existing file or directory on the host machine that the volume maps to.

## Contents

### path

Path of the file or directory on the host that the volume maps to.

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 Java V2](#)
- [AWS SDK for Ruby V3](#)

# IamInstanceProfile

Contains information about the EC2 instance profile.

## Contents

### arn

The profile ARN of the EC2 instance.

Type: String

Required: No

### id

The profile ID of the EC2 instance.

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 Java V2](#)
- [AWS SDK for Ruby V3](#)

# ImpersonatedUser

Contains information about the impersonated user.

## Contents

### groups

The group to which the user name belongs.

Type: Array of strings

Required: No

### username

Information about the username that was being impersonated.

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 Java V2](#)
- [AWS SDK for Ruby V3](#)

# InstanceDetails

Contains information about the details of an instance.

## Contents

### **availabilityZone**

The Availability Zone of the EC2 instance.

Type: String

Required: No

### **iamInstanceProfile**

The profile information of the EC2 instance.

Type: [IamInstanceProfile](#) object

Required: No

### **imageDescription**

The image description of the EC2 instance.

Type: String

Required: No

### **imageId**

The image ID of the EC2 instance.

Type: String

Required: No

### **instanceId**

The ID of the EC2 instance.

Type: String

Required: No

**instanceState**

The state of the EC2 instance.

Type: String

Required: No

**instanceType**

The type of the EC2 instance.

Type: String

Required: No

**launchTime**

The launch time of the EC2 instance.

Type: String

Required: No

**networkInterfaces**

The elastic network interface information of the EC2 instance.

Type: Array of [NetworkInterface](#) objects

Required: No

**outpostArn**

The Amazon Resource Name (ARN) of the AWS Outpost. Only applicable to AWS Outposts instances.

Type: String

Required: No

**platform**

The platform of the EC2 instance.

Type: String

Required: No

### **productCodes**

The product code of the EC2 instance.

Type: Array of [ProductCode](#) objects

Required: No

### **tags**

The tags of the EC2 instance.

Type: Array of [Tag](#) 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 Java V2](#)
- [AWS SDK for Ruby V3](#)

# Invitation

Contains information about the invitation to become a member account.

## Contents

### **accountId**

The ID of the account that the invitation was sent from.

Type: String

Length Constraints: Fixed length of 12.

Required: No

### **invitationId**

The ID of the invitation. This value is used to validate the inviter account to the member account.

Type: String

Required: No

### **invitedAt**

The timestamp when the invitation was sent.

Type: String

Required: No

### **relationshipStatus**

The status of the relationship between the inviter and invitee accounts.

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 Java V2](#)
- [AWS SDK for Ruby V3](#)



# ItemPath

Information about the nested item path and hash of the protected resource.

## Contents

### hash

The hash value of the infected resource.

Type: String

Required: No

### nestedItemPath

The nested item path where the infected file was found.

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 Java V2](#)
- [AWS SDK for Ruby V3](#)

# KubernetesApiCallAction

Information about the Kubernetes API call action described in this finding.

## Contents

### namespace

The name of the namespace where the Kubernetes API call action takes place.

Type: String

Required: No

### parameters

Parameters related to the Kubernetes API call action.

Type: String

Required: No

### remoteIpDetails

Contains information about the remote IP address of the connection.

Type: [RemoteIpDetails](#) object

Required: No

### requestUri

The Kubernetes API request URI.

Type: String

Required: No

### resource

The resource component in the Kubernetes API call action.

Type: String

Required: No

**resourceName**

The name of the resource in the Kubernetes API call action.

Type: String

Required: No

**sourceIps**

The IP of the Kubernetes API caller and the IPs of any proxies or load balancers between the caller and the API endpoint.

Type: Array of strings

Required: No

**statusCode**

The resulting HTTP response code of the Kubernetes API call action.

Type: Integer

Required: No

**subresource**

The name of the sub-resource in the Kubernetes API call action.

Type: String

Required: No

**userAgent**

The user agent of the caller of the Kubernetes API.

Type: String

Required: No

**verb**

The Kubernetes API request HTTP verb.

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 Java V2](#)
- [AWS SDK for Ruby V3](#)

# KubernetesAuditLogsConfiguration

Describes whether Kubernetes audit logs are enabled as a data source.

## Contents

### enable

The status of Kubernetes audit logs as a data source.

Type: Boolean

Required: Yes

## See Also

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

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

# KubernetesAuditLogsConfigurationResult

Describes whether Kubernetes audit logs are enabled as a data source.

## Contents

### status

A value that describes whether Kubernetes audit logs are enabled as a data source.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 300.

Valid Values: ENABLED | DISABLED

Required: Yes

## See Also

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

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

# KubernetesConfiguration

Describes whether any Kubernetes data sources are enabled.

## Contents

### auditLogs

The status of Kubernetes audit logs as a data source.

Type: [KubernetesAuditLogsConfiguration](#) object

Required: Yes

## See Also

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

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

# KubernetesConfigurationResult

Describes whether any Kubernetes logs will be enabled as a data source.

## Contents

### auditLogs

Describes whether Kubernetes audit logs are enabled as a data source.

Type: [KubernetesAuditLogsConfigurationResult](#) object

Required: Yes

## See Also

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

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)



# KubernetesDataSourceFreeTrial

Provides details about the Kubernetes resources when it is enabled as a data source.

## Contents

### auditLogs

Describes whether Kubernetes audit logs are enabled as a data source.

Type: [DataSourceFreeTrial](#) object

Required: No

## See Also

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

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

# KubernetesDetails

Details about Kubernetes resources such as a Kubernetes user or workload resource involved in a Kubernetes finding.

## Contents

### kubernetesUserDetails

Details about the Kubernetes user involved in a Kubernetes finding.

Type: [KubernetesUserDetails](#) object

Required: No

### kubernetesWorkloadDetails

Details about the Kubernetes workload involved in a Kubernetes finding.

Type: [KubernetesWorkloadDetails](#) object

Required: No

## See Also

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

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

# KubernetesPermissionCheckedDetails

Information about the Kubernetes API for which you check if you have permission to call.

## Contents

### allowed

Information whether the user has the permission to call the Kubernetes API.

Type: Boolean

Required: No

### namespace

The namespace where the Kubernetes API action will take place.

Type: String

Required: No

### resource

The Kubernetes resource with which your Kubernetes API call will interact.

Type: String

Required: No

### verb

The verb component of the Kubernetes API call. For example, when you check whether or not you have the permission to call the `CreatePod` API, the verb component will be `Create`.

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 Java V2](#)
- [AWS SDK for Ruby V3](#)

# KubernetesRoleBindingDetails

Contains information about the role binding that grants the permission defined in a Kubernetes role.

## Contents

### kind

The kind of the role. For role binding, this value will be `RoleBinding`.

Type: String

Required: No

### name

The name of the `RoleBinding`.

Type: String

Required: No

### roleRefKind

The type of the role being referenced. This could be either `Role` or `ClusterRole`.

Type: String

Required: No

### roleRefName

The name of the role being referenced. This must match the name of the `Role` or `ClusterRole` that you want to bind to.

Type: String

Required: No

### uid

The unique identifier of the role binding.

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 Java V2](#)
- [AWS SDK for Ruby V3](#)

# KubernetesRoleDetails

Information about the Kubernetes role name and role type.

## Contents

### kind

The kind of role. For this API, the value of kind will be Role.

Type: String

Required: No

### name

The name of the Kubernetes role.

Type: String

Required: No

### uid

The unique identifier of the Kubernetes role name.

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 Java V2](#)
- [AWS SDK for Ruby V3](#)

# KubernetesUserDetails

Details about the Kubernetes user involved in a Kubernetes finding.

## Contents

### groups

The groups that include the user who called the Kubernetes API.

Type: Array of strings

Required: No

### impersonatedUser

Information about the impersonated user.

Type: [ImpersonatedUser](#) object

Required: No

### sessionName

Entity that assumes the IAM role when Kubernetes RBAC permissions are assigned to that role.

Type: Array of strings

Required: No

### uid

The user ID of the user who called the Kubernetes API.

Type: String

Required: No

### username

The username of the user who called the Kubernetes API.

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 Java V2](#)
- [AWS SDK for Ruby V3](#)

# KubernetesWorkloadDetails

Details about the Kubernetes workload involved in a Kubernetes finding.

## Contents

### containers

Containers running as part of the Kubernetes workload.

Type: Array of [Container](#) objects

Required: No

### hostIPC

Whether the host IPC flag is enabled for the pods in the workload.

Type: Boolean

Required: No

### hostNetwork

Whether the hostNetwork flag is enabled for the pods included in the workload.

Type: Boolean

Required: No

### hostPID

Whether the host PID flag is enabled for the pods in the workload.

Type: Boolean

Required: No

### name

Kubernetes workload name.

Type: String

Required: No

## namespace

Kubernetes namespace that the workload is part of.

Type: String

Required: No

## serviceAccountName

The service account name that is associated with a Kubernetes workload.

Type: String

Required: No

## type

Kubernetes workload type (e.g. Pod, Deployment, etc.).

Type: String

Required: No

## uid

Kubernetes workload ID.

Type: String

Required: No

## volumes

Volumes used by the Kubernetes workload.

Type: Array of [Volume](#) 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 Java V2](#)
- [AWS SDK for Ruby V3](#)

# LambdaDetails

Information about the Lambda function involved in the finding.

## Contents

### **description**

Description of the Lambda function.

Type: String

Required: No

### **functionArn**

Amazon Resource Name (ARN) of the Lambda function.

Type: String

Required: No

### **functionName**

Name of the Lambda function.

Type: String

Required: No

### **functionVersion**

The version of the Lambda function.

Type: String

Required: No

### **lastModifiedAt**

The timestamp when the Lambda function was last modified. This field is in the UTC date string format (`2023-03-22T19:37:20.168Z`).

Type: Timestamp

Required: No

## revisionId

The revision ID of the Lambda function version.

Type: String

Required: No

## role

The execution role of the Lambda function.

Type: String

Required: No

## tags

A list of tags attached to this resource, listed in the format of key:value pair.

Type: Array of [Tag](#) objects

Required: No

## vpcConfig

Amazon Virtual Private Cloud configuration details associated with your Lambda function.

Type: [VpcConfig](#) object

Required: No

## See Also

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

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

# LineageObject

Information about the runtime process details.

## Contents

### **eid**

The effective user ID that was used to execute the process.

Type: Integer

Required: No

### **executablePath**

The absolute path of the process executable file.

Type: String

Required: No

### **name**

The name of the process.

Type: String

Required: No

### **namespacePid**

The process ID of the child process.

Type: Integer

Required: No

### **parentUid**

The unique ID of the parent process. This ID is assigned to the parent process by GuardDuty.

Type: String

Required: No

**pid**

The ID of the process.

Type: Integer

Required: No

**startTime**

The time when the process started. This is in UTC format.

Type: Timestamp

Required: No

**userId**

The user ID of the user that executed the process.

Type: Integer

Required: No

**uuid**

The unique ID assigned to the process by GuardDuty.

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 Java V2](#)
- [AWS SDK for Ruby V3](#)



# LocalIpDetails

Contains information about the local IP address of the connection.

## Contents

### ipAddressV4

The IPv4 local address of the connection.

Type: String

Required: No

### ipAddressV6

The IPv6 local address of the connection.

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 Java V2](#)
- [AWS SDK for Ruby V3](#)

# LocalPortDetails

Contains information about the port for the local connection.

## Contents

### port

The port number of the local connection.

Type: Integer

Required: No

### portName

The port name of the local connection.

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 Java V2](#)
- [AWS SDK for Ruby V3](#)

# LoginAttribute

Information about the login attempts.

## Contents

### **application**

Indicates the application name used to attempt log in.

Type: String

Required: No

### **failedLoginAttempts**

Represents the sum of failed (unsuccessful) login attempts made to establish a connection to the database instance.

Type: Integer

Required: No

### **successfulLoginAttempts**

Represents the sum of successful connections (a correct combination of login attributes) made to the database instance by the actor.

Type: Integer

Required: No

### **user**

Indicates the user name which attempted to log in.

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 Java V2](#)
- [AWS SDK for Ruby V3](#)

# MalwareProtectionConfiguration

Describes whether Malware Protection will be enabled as a data source.

## Contents

### scanEc2InstanceWithFindings

Describes the configuration of Malware Protection for EC2 instances with findings.

Type: [ScanEc2InstanceWithFindings](#) object

Required: No

## See Also

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

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

# MalwareProtectionConfigurationResult

An object that contains information on the status of all Malware Protection data sources.

## Contents

### scanEc2InstanceWithFindings

Describes the configuration of Malware Protection for EC2 instances with findings.

Type: [ScanEc2InstanceWithFindingsResult](#) object

Required: No

### serviceRole

The GuardDuty Malware Protection service role.

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 Java V2](#)
- [AWS SDK for Ruby V3](#)

# MalwareProtectionDataSourceFreeTrial

Provides details about Malware Protection when it is enabled as a data source.

## Contents

### scanEc2InstanceWithFindings

Describes whether Malware Protection for EC2 instances with findings is enabled as a data source.

Type: [DataSourceFreeTrial](#) object

Required: No

## See Also

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

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

# MalwareProtectionPlanActions

Information about whether the tags will be added to the S3 object after scanning.

## Contents

### tagging

Indicates whether the scanned S3 object will have tags about the scan result.

Type: [MalwareProtectionPlanTaggingAction](#) object

Required: No

## See Also

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

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)



# MalwareProtectionPlanStatusReason

Information about the issue code and message associated to the status of your Malware Protection plan.

## Contents

### code

Issue code.

Type: String

Required: No

### message

Issue message that specifies the reason. For information about potential troubleshooting steps, see [Troubleshooting Malware Protection for S3 status issues](#) in the *GuardDuty User Guide*.

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 Java V2](#)
- [AWS SDK for Ruby V3](#)

# MalwareProtectionPlanSummary

Information about the Malware Protection plan resource.

## Contents

### malwareProtectionPlanId

A unique identifier associated with Malware Protection plan.

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 Java V2](#)
- [AWS SDK for Ruby V3](#)

# MalwareProtectionPlanTaggingAction

Information about adding tags to the scanned S3 object after the scan result.

## Contents

### status

Indicates whether or not the tags will added.

Type: String

Valid Values: ENABLED | DISABLED

Required: No

## See Also

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

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

# MalwareScanDetails

Information about the malware scan that generated a GuardDuty finding.

## Contents

### threats

Information about the detected threats associated with the generated GuardDuty finding.

Type: Array of [Threat](#) 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 Java V2](#)
- [AWS SDK for Ruby V3](#)

# Master

Contains information about the administrator account and invitation.

## Contents

### **accountId**

The ID of the account used as the administrator account.

Type: String

Length Constraints: Fixed length of 12.

Required: No

### **invitationId**

The value used to validate the administrator account to the member account.

Type: String

Required: No

### **invitedAt**

The timestamp when the invitation was sent.

Type: String

Required: No

### **relationshipStatus**

The status of the relationship between the administrator and member accounts.

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 Java V2](#)
- [AWS SDK for Ruby V3](#)

# Member

Contains information about the member account.

## Contents

### **accountId**

The ID of the member account.

Type: String

Length Constraints: Fixed length of 12.

Required: Yes

### **email**

The email address of the member account.

Type: String

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

Required: Yes

### **masterId**

The administrator account ID.

Type: String

Required: Yes

### **relationshipStatus**

The status of the relationship between the member and the administrator.

Type: String

Required: Yes

### **updatedAt**

The last-updated timestamp of the member.

Type: String

Required: Yes

### **administratorId**

The administrator account ID.

Type: String

Required: No

### **detectorId**

The detector ID of the member account.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: No

### **invitedAt**

The timestamp when the invitation was sent.

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 Java V2](#)
- [AWS SDK for Ruby V3](#)



# MemberAdditionalConfiguration

Information about the additional configuration for the member account.

## Contents

### name

Name of the additional configuration.

Type: String

Valid Values: EKS\_ADDON\_MANAGEMENT | ECS\_FARGATE\_AGENT\_MANAGEMENT | EC2\_AGENT\_MANAGEMENT

Required: No

### status

Status of the additional configuration.

Type: String

Valid Values: ENABLED | DISABLED

Required: No

## See Also

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

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

# MemberAdditionalConfigurationResult

Information about the additional configuration for the member account.

## Contents

### name

Indicates the name of the additional configuration that is set for the member account.

Type: String

Valid Values: EKS\_ADDON\_MANAGEMENT | ECS\_FARGATE\_AGENT\_MANAGEMENT | EC2\_AGENT\_MANAGEMENT

Required: No

### status

Indicates the status of the additional configuration that is set for the member account.

Type: String

Valid Values: ENABLED | DISABLED

Required: No

### updatedAt

The timestamp at which the additional configuration was set for the member account. This is in UTC format.

Type: Timestamp

Required: No

## See Also

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

- [AWS SDK for C++](#)

- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

# MemberDataSourceConfiguration

Contains information on which data sources are enabled for a member account.

## Contents

### accountId

The account ID for the member account.

Type: String

Length Constraints: Fixed length of 12.

Required: Yes

### dataSources

*This member has been deprecated.*

Contains information on the status of data sources for the account.

Type: [DataSourceConfigurationsResult](#) object

Required: No

### features

Contains information about the status of the features for the member account.

Type: Array of [MemberFeaturesConfigurationResult](#) 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 Java V2](#)
- [AWS SDK for Ruby V3](#)



# MemberFeaturesConfiguration

Contains information about the features for the member account.

## Contents

### additionalConfiguration

Additional configuration of the feature for the member account.

Type: Array of [MemberAdditionalConfiguration](#) objects

Required: No

### name

The name of the feature.

Type: String

Valid Values: S3\_DATA\_EVENTS | EKS\_AUDIT\_LOGS | EBS\_MALWARE\_PROTECTION  
| RDS\_LOGIN\_EVENTS | EKS\_RUNTIME\_MONITORING | LAMBDA\_NETWORK\_LOGS |  
RUNTIME\_MONITORING

Required: No

### status

The status of the feature.

Type: String

Valid Values: ENABLED | DISABLED

Required: No

## See Also

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

- [AWS SDK for C++](#)

- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

# MemberFeaturesConfigurationResult

Contains information about the features for the member account.

## Contents

### **additionalConfiguration**

Indicates the additional configuration of the feature that is configured for the member account.

Type: Array of [MemberAdditionalConfigurationResult](#) objects

Required: No

### **name**

Indicates the name of the feature that is enabled for the detector.

Type: String

Valid Values: S3\_DATA\_EVENTS | EKS\_AUDIT\_LOGS | EBS\_MALWARE\_PROTECTION  
| RDS\_LOGIN\_EVENTS | EKS\_RUNTIME\_MONITORING | LAMBDA\_NETWORK\_LOGS |  
RUNTIME\_MONITORING

Required: No

### **status**

Indicates the status of the feature that is enabled for the detector.

Type: String

Valid Values: ENABLED | DISABLED

Required: No

### **updatedAt**

The timestamp at which the feature object was updated.

Type: Timestamp

Required: No



## See Also

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

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

# NetworkConnectionAction

Contains information about the NETWORK\_CONNECTION action described in the finding.

## Contents

### blocked

Indicates whether EC2 blocked the network connection to your instance.

Type: Boolean

Required: No

### connectionDirection

The network connection direction.

Type: String

Required: No

### localIpDetails

The local IP information of the connection.

Type: [LocalIpDetails](#) object

Required: No

### localPortDetails

The local port information of the connection.

Type: [LocalPortDetails](#) object

Required: No

### protocol

The network connection protocol.

Type: String

Required: No

## remoteIpDetails

The remote IP information of the connection.

Type: [RemoteIpDetails](#) object

Required: No

## remotePortDetails

The remote port information of the connection.

Type: [RemotePortDetails](#) object

Required: No

## See Also

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

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

# NetworkInterface

Contains information about the elastic network interface of the EC2 instance.

## Contents

### **ipv6Addresses**

A list of IPv6 addresses for the EC2 instance.

Type: Array of strings

Required: No

### **networkInterfaceId**

The ID of the network interface.

Type: String

Required: No

### **privateDnsName**

The private DNS name of the EC2 instance.

Type: String

Required: No

### **privateIpAddress**

The private IP address of the EC2 instance.

Type: String

Required: No

### **privateIpAddresses**

Other private IP address information of the EC2 instance.

Type: Array of [PrivateIpAddressDetails](#) objects

Required: No

**publicDnsName**

The public DNS name of the EC2 instance.

Type: String

Required: No

**publicIp**

The public IP address of the EC2 instance.

Type: String

Required: No

**securityGroups**

The security groups associated with the EC2 instance.

Type: Array of [SecurityGroup](#) objects

Required: No

**subnetId**

The subnet ID of the EC2 instance.

Type: String

Required: No

**vpcId**

The VPC ID of the EC2 instance.

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 Java V2](#)
- [AWS SDK for Ruby V3](#)

# Observations

Contains information about the observed behavior.

## Contents

### text

The text that was unusual.

Type: Array of strings

Required: No

## See Also

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

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

# Organization

Contains information about the ISP organization of the remote IP address.

## Contents

### asn

The Autonomous System Number (ASN) of the internet provider of the remote IP address.

Type: String

Required: No

### asnOrg

The organization that registered this ASN.

Type: String

Required: No

### isp

The ISP information for the internet provider.

Type: String

Required: No

### org

The name of the internet provider.

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 Java V2](#)
- [AWS SDK for Ruby V3](#)

# OrganizationAdditionalConfiguration

A list of additional configurations which will be configured for the organization.

## Contents

### **autoEnable**

The status of the additional configuration that will be configured for the organization. Use one of the following values to configure the feature status for the entire organization:

- **NEW:** Indicates that when a new account joins the organization, they will have the additional configuration enabled automatically.
- **ALL:** Indicates that all accounts in the organization have the additional configuration enabled automatically. This includes NEW accounts that join the organization and accounts that may have been suspended or removed from the organization in GuardDuty.

It may take up to 24 hours to update the configuration for all the member accounts.

- **NONE:** Indicates that the additional configuration will not be automatically enabled for any account in the organization. The administrator must manage the additional configuration for each account individually.

Type: String

Valid Values: NEW | NONE | ALL

Required: No

### **name**

The name of the additional configuration that will be configured for the organization.

Type: String

Valid Values: EKS\_ADDON\_MANAGEMENT | ECS\_FARGATE\_AGENT\_MANAGEMENT | EC2\_AGENT\_MANAGEMENT

Required: No

## See Also

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

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

# OrganizationAdditionalConfigurationResult

A list of additional configuration which will be configured for the organization.

## Contents

### autoEnable

Describes the status of the additional configuration that is configured for the member accounts within the organization. One of the following values is the status for the entire organization:

- **NEW:** Indicates that when a new account joins the organization, they will have the additional configuration enabled automatically.
- **ALL:** Indicates that all accounts in the organization have the additional configuration enabled automatically. This includes NEW accounts that join the organization and accounts that may have been suspended or removed from the organization in GuardDuty.

It may take up to 24 hours to update the configuration for all the member accounts.

- **NONE:** Indicates that the additional configuration will not be automatically enabled for any account in the organization. The administrator must manage the additional configuration for each account individually.

Type: String

Valid Values: NEW | NONE | ALL

Required: No

### name

The name of the additional configuration that is configured for the member accounts within the organization.

Type: String

Valid Values: EKS\_ADDON\_MANAGEMENT | ECS\_FARGATE\_AGENT\_MANAGEMENT | EC2\_AGENT\_MANAGEMENT

Required: No

## See Also

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

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

# OrganizationDataSourceConfigurations

An object that contains information on which data sources will be configured to be automatically enabled for new members within the organization.

## Contents

### kubernetes

Describes the configuration of Kubernetes data sources for new members of the organization.

Type: [OrganizationKubernetesConfiguration](#) object

Required: No

### malwareProtection

Describes the configuration of Malware Protection for new members of the organization.

Type: [OrganizationMalwareProtectionConfiguration](#) object

Required: No

### s3Logs

Describes whether S3 data event logs are enabled for new members of the organization.

Type: [OrganizationS3LogsConfiguration](#) object

Required: No

## See Also

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

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

# OrganizationDataSourceConfigurationsResult

An object that contains information on which data sources are automatically enabled for new members within the organization.

## Contents

### s3Logs

Describes whether S3 data event logs are enabled as a data source.

Type: [OrganizationS3LogsConfigurationResult](#) object

Required: Yes

### kubernetes

Describes the configuration of Kubernetes data sources.

Type: [OrganizationKubernetesConfigurationResult](#) object

Required: No

### malwareProtection

Describes the configuration of Malware Protection data source for an organization.

Type: [OrganizationMalwareProtectionConfigurationResult](#) object

Required: No

## See Also

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

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

# OrganizationDetails

Information about GuardDuty coverage statistics for members in your AWS organization.

## Contents

### **organizationStatistics**

Information about the GuardDuty coverage statistics for members in your AWS organization.

Type: [OrganizationStatistics](#) object

Required: No

### **updatedAt**

The timestamp at which the organization statistics was last updated. This is in UTC format.

Type: Timestamp

Required: No

## See Also

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

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)



# OrganizationEbsVolumes

Organization-wide EBS volumes scan configuration.

## Contents

### autoEnable

Whether scanning EBS volumes should be auto-enabled for new members joining the organization.

Type: Boolean

Required: No

## See Also

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

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

# OrganizationEbsVolumesResult

An object that contains information on the status of whether EBS volumes scanning will be enabled as a data source for an organization.

## Contents

### autoEnable

An object that contains the status of whether scanning EBS volumes should be auto-enabled for new members joining the organization.

Type: Boolean

Required: No

## See Also

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

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

# OrganizationFeatureConfiguration

A list of features which will be configured for the organization.

## Contents

### **additionalConfiguration**

The additional information that will be configured for the organization.

Type: Array of [OrganizationAdditionalConfiguration](#) objects

Required: No

### **autoEnable**

Describes the status of the feature that is configured for the member accounts within the organization. One of the following values is the status for the entire organization:

- **NEW**: Indicates that when a new account joins the organization, they will have the feature enabled automatically.
- **ALL**: Indicates that all accounts in the organization have the feature enabled automatically. This includes **NEW** accounts that join the organization and accounts that may have been suspended or removed from the organization in GuardDuty.

It may take up to 24 hours to update the configuration for all the member accounts.

- **NONE**: Indicates that the feature will not be automatically enabled for any account in the organization. The administrator must manage the feature for each account individually.

Type: String

Valid Values: **NEW** | **NONE** | **ALL**

Required: No

### **name**

The name of the feature that will be configured for the organization.

Type: String

Valid Values: **S3\_DATA\_EVENTS** | **EKS\_AUDIT\_LOGS** | **EBS\_MALWARE\_PROTECTION** | **RDS\_LOGIN\_EVENTS** | **EKS\_RUNTIME\_MONITORING** | **LAMBDA\_NETWORK\_LOGS** | **RUNTIME\_MONITORING**

Required: No

## See Also

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

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

# OrganizationFeatureConfigurationResult

A list of features which will be configured for the organization.

## Contents

### additionalConfiguration

The additional configuration that is configured for the member accounts within the organization.

Type: Array of [OrganizationAdditionalConfigurationResult](#) objects

Required: No

### autoEnable

Describes the status of the feature that is configured for the member accounts within the organization.

- **NEW:** Indicates that when a new account joins the organization, they will have the feature enabled automatically.
- **ALL:** Indicates that all accounts in the organization have the feature enabled automatically. This includes NEW accounts that join the organization and accounts that may have been suspended or removed from the organization in GuardDuty.
- **NONE:** Indicates that the feature will not be automatically enabled for any account in the organization. In this case, each account will be managed individually by the administrator.

Type: String

Valid Values: NEW | NONE | ALL

Required: No

### name

The name of the feature that is configured for the member accounts within the organization.

Type: String

Valid Values: S3\_DATA\_EVENTS | EKS\_AUDIT\_LOGS | EBS\_MALWARE\_PROTECTION | RDS\_LOGIN\_EVENTS | EKS\_RUNTIME\_MONITORING | LAMBDA\_NETWORK\_LOGS | RUNTIME\_MONITORING

Required: No

## See Also

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

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

# OrganizationFeatureStatistics

Information about the number of accounts that have enabled a specific feature.

## Contents

### **additionalConfiguration**

Name of the additional configuration.

Type: Array of [OrganizationFeatureStatisticsAdditionalConfiguration](#) objects

Required: No

### **enabledAccountsCount**

Total number of accounts that have enabled a specific feature.

Type: Integer

Required: No

### **name**

Name of the feature.

Type: String

Valid Values: S3\_DATA\_EVENTS | EKS\_AUDIT\_LOGS | EBS\_MALWARE\_PROTECTION  
| RDS\_LOGIN\_EVENTS | EKS\_RUNTIME\_MONITORING | LAMBDA\_NETWORK\_LOGS |  
RUNTIME\_MONITORING

Required: No

## See Also

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

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)





# OrganizationFeatureStatisticsAdditionalConfiguration

Information about the coverage statistic for the additional configuration of the feature.

## Contents

### **enabledAccountsCount**

Total number of accounts that have enabled the additional configuration.

Type: Integer

Required: No

### **name**

Name of the additional configuration within a feature.

Type: String

Valid Values: EKS\_ADDON\_MANAGEMENT | ECS\_FARGATE\_AGENT\_MANAGEMENT | EC2\_AGENT\_MANAGEMENT

Required: No

## See Also

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

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

# OrganizationKubernetesAuditLogsConfiguration

Organization-wide Kubernetes audit logs configuration.

## Contents

### autoEnable

A value that contains information on whether Kubernetes audit logs should be enabled automatically as a data source for the organization.

Type: Boolean

Required: Yes

## See Also

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

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

# OrganizationKubernetesAuditLogsConfigurationResult

The current configuration of Kubernetes audit logs as a data source for the organization.

## Contents

### autoEnable

Whether Kubernetes audit logs data source should be auto-enabled for new members joining the organization.

Type: Boolean

Required: Yes

## See Also

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

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

# OrganizationKubernetesConfiguration

Organization-wide Kubernetes data sources configurations.

## Contents

### auditLogs

Whether Kubernetes audit logs data source should be auto-enabled for new members joining the organization.

Type: [OrganizationKubernetesAuditLogsConfiguration](#) object

Required: Yes

## See Also

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

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

# OrganizationKubernetesConfigurationResult

The current configuration of all Kubernetes data sources for the organization.

## Contents

### auditLogs

The current configuration of Kubernetes audit logs as a data source for the organization.

Type: [OrganizationKubernetesAuditLogsConfigurationResult](#) object

Required: Yes

## See Also

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

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

# OrganizationMalwareProtectionConfiguration

Organization-wide Malware Protection configurations.

## Contents

### scanEc2InstanceWithFindings

Whether Malware Protection for EC2 instances with findings should be auto-enabled for new members joining the organization.

Type: [OrganizationScanEc2InstanceWithFindings](#) object

Required: No

## See Also

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

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

# OrganizationMalwareProtectionConfigurationResult

An object that contains information on the status of all Malware Protection data source for an organization.

## Contents

### scanEc2InstanceWithFindings

Describes the configuration for scanning EC2 instances with findings for an organization.

Type: [OrganizationScanEc2InstanceWithFindingsResult](#) object

Required: No

## See Also

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

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

# OrganizationS3LogsConfiguration

Describes whether S3 data event logs will be automatically enabled for new members of the organization.

## Contents

### autoEnable

A value that contains information on whether S3 data event logs will be enabled automatically as a data source for the organization.

Type: Boolean

Required: Yes

## See Also

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

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)



# OrganizationS3LogsConfigurationResult

The current configuration of S3 data event logs as a data source for the organization.

## Contents

### autoEnable

A value that describes whether S3 data event logs are automatically enabled for new members of the organization.

Type: Boolean

Required: Yes

## See Also

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

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

# OrganizationScanEc2InstanceWithFindings

Organization-wide EC2 instances with findings scan configuration.

## Contents

### ebsVolumes

Whether scanning EBS volumes should be auto-enabled for new members joining the organization.

Type: [OrganizationEbsVolumes](#) object

Required: No

## See Also

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

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

# OrganizationScanEc2InstanceWithFindingsResult

An object that contains information on the status of scanning EC2 instances with findings for an organization.

## Contents

### ebsVolumes

Describes the configuration for scanning EBS volumes for an organization.

Type: [OrganizationEbsVolumesResult](#) object

Required: No

## See Also

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

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

# OrganizationStatistics

Information about the coverage statistics of the features for the entire AWS organization.

When you create a new AWS organization, it might take up to 24 hours to generate the statistics summary for this organization.

## Contents

### **activeAccountsCount**

Total number of active accounts in your AWS organization that are associated with GuardDuty.

Type: Integer

Required: No

### **countByFeature**

Retrieves the coverage statistics for each feature.

Type: Array of [OrganizationFeatureStatistics](#) objects

Required: No

### **enabledAccountsCount**

Total number of accounts that have enabled GuardDuty.

Type: Integer

Required: No

### **memberAccountsCount**

Total number of accounts in your AWS organization that are associated with GuardDuty.

Type: Integer

Required: No

### **totalAccountsCount**

Total number of accounts in your AWS organization.

Type: Integer

Required: No

## See Also

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

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

## Owner

Contains information on the owner of the bucket.

## Contents

### id

The canonical user ID of the bucket owner. For information about locating your canonical user ID see [Finding Your Account Canonical User ID](#).

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 Java V2](#)
- [AWS SDK for Ruby V3](#)

# PermissionConfiguration

Contains information about how permissions are configured for the S3 bucket.

## Contents

### accountLevelPermissions

Contains information about the account level permissions on the S3 bucket.

Type: [AccountLevelPermissions](#) object

Required: No

### bucketLevelPermissions

Contains information about the bucket level permissions for the S3 bucket.

Type: [BucketLevelPermissions](#) object

Required: No

## See Also

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

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

# PortProbeAction

Contains information about the PORT\_PROBE action described in the finding.

## Contents

### blocked

Indicates whether EC2 blocked the port probe to the instance, such as with an ACL.

Type: Boolean

Required: No

### portProbeDetails

A list of objects related to port probe details.

Type: Array of [PortProbeDetail](#) 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 Java V2](#)
- [AWS SDK for Ruby V3](#)



# PortProbeDetail

Contains information about the port probe details.

## Contents

### localIpDetails

The local IP information of the connection.

Type: [LocalIpDetails](#) object

Required: No

### localPortDetails

The local port information of the connection.

Type: [LocalPortDetails](#) object

Required: No

### remoteIpDetails

The remote IP information of the connection.

Type: [RemoteIpDetails](#) object

Required: No

## See Also

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

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

# PrivateIpAddressDetails

Contains other private IP address information of the EC2 instance.

## Contents

### **privateDnsName**

The private DNS name of the EC2 instance.

Type: String

Required: No

### **privateIpAddress**

The private IP address of the EC2 instance.

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 Java V2](#)
- [AWS SDK for Ruby V3](#)

# ProcessDetails

Information about the observed process.

## Contents

### **eid**

The effective user ID of the user that executed the process.

Type: Integer

Required: No

### **executablePath**

The absolute path of the process executable file.

Type: String

Required: No

### **executableSha256**

The SHA256 hash of the process executable.

Type: String

Required: No

### **lineage**

Information about the process's lineage.

Type: Array of [LineageObject](#) objects

Required: No

### **name**

The name of the process.

Type: String

Required: No

**namespacePid**

The ID of the child process.

Type: Integer

Required: No

**parentUuid**

The unique ID of the parent process. This ID is assigned to the parent process by GuardDuty.

Type: String

Required: No

**pid**

The ID of the process.

Type: Integer

Required: No

**pwd**

The present working directory of the process.

Type: String

Required: No

**startTime**

The time when the process started. This is in UTC format.

Type: Timestamp

Required: No

**user**

The user that executed the process.

Type: String

Required: No

**userId**

The unique ID of the user that executed the process.

Type: Integer

Required: No

**uuid**

The unique ID assigned to the process by GuardDuty.

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 Java V2](#)
- [AWS SDK for Ruby V3](#)

# ProductCode

Contains information about the product code for the EC2 instance.

## Contents

### **productCodeId**

The product code information.

Type: String

Required: No

### **productCodeType**

The product code type.

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 Java V2](#)
- [AWS SDK for Ruby V3](#)

# PublicAccess

Describes the public access policies that apply to the S3 bucket.

## Contents

### **effectivePermission**

Describes the effective permission on this bucket after factoring all attached policies.

Type: String

Required: No

### **permissionConfiguration**

Contains information about how permissions are configured for the S3 bucket.

Type: [PermissionConfiguration](#) object

Required: No

## See Also

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

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

# RdsDbInstanceDetails

Contains information about the resource type RDSDBInstance involved in a GuardDuty finding.

## Contents

### **dbClusterIdentifier**

The identifier of the database cluster that contains the database instance ID involved in the finding.

Type: String

Required: No

### **dbInstanceArn**

The Amazon Resource Name (ARN) that identifies the database instance involved in the finding.

Type: String

Required: No

### **dbInstanceIdentifier**

The identifier associated to the database instance that was involved in the finding.

Type: String

Required: No

### **engine**

The database engine of the database instance involved in the finding.

Type: String

Required: No

### **engineVersion**

The version of the database engine that was involved in the finding.

Type: String

Required: No



## tags

Instance tag key-value pairs associated with the database instance ID.

Type: Array of [Tag](#) 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 Java V2](#)
- [AWS SDK for Ruby V3](#)

# RdsDbUserDetails

Contains information about the user and authentication details for a database instance involved in the finding.

## Contents

### **application**

The application name used in the anomalous login attempt.

Type: String

Required: No

### **authMethod**

The authentication method used by the user involved in the finding.

Type: String

Required: No

### **database**

The name of the database instance involved in the anomalous login attempt.

Type: String

Required: No

### **ssl**

The version of the Secure Socket Layer (SSL) used for the network.

Type: String

Required: No

### **user**

The user name used in the anomalous login attempt.

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 Java V2](#)
- [AWS SDK for Ruby V3](#)

# RdsLoginAttemptAction

Indicates that a login attempt was made to the potentially compromised database from a remote IP address.

## Contents

### LoginAttributes

Indicates the login attributes used in the login attempt.

Type: Array of [LoginAttribute](#) objects

Required: No

### remoteIpDetails

Contains information about the remote IP address of the connection.

Type: [RemoteIpDetails](#) object

Required: No

## See Also

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

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

# RemoteAccountDetails

Contains details about the remote AWS account that made the API call.

## Contents

### **accountId**

The AWS account ID of the remote API caller.

Type: String

Required: No

### **affiliated**

Details on whether the AWS account of the remote API caller is related to your GuardDuty environment. If this value is `True` the API caller is affiliated to your account in some way. If it is `False` the API caller is from outside your environment.

Type: Boolean

Required: No

## See Also

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

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

# RemoteIpDetails

Contains information about the remote IP address of the connection.

## Contents

### city

The city information of the remote IP address.

Type: [City](#) object

Required: No

### country

The country code of the remote IP address.

Type: [Country](#) object

Required: No

### geoLocation

The location information of the remote IP address.

Type: [GeoLocation](#) object

Required: No

### ipAddressV4

The IPv4 remote address of the connection.

Type: String

Required: No

### ipAddressV6

The IPv6 remote address of the connection.

Type: String

Required: No

## organization

The ISP organization information of the remote IP address.

Type: [Organization](#) object

Required: No

## See Also

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

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

# RemotePortDetails

Contains information about the remote port.

## Contents

### port

The port number of the remote connection.

Type: Integer

Required: No

### portName

The port name of the remote connection.

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 Java V2](#)
- [AWS SDK for Ruby V3](#)



## Resource

Contains information about the AWS resource associated with the activity that prompted GuardDuty to generate a finding.

### Contents

#### **accessKeyDetails**

The IAM access key details (user information) of a user that engaged in the activity that prompted GuardDuty to generate a finding.

Type: [AccessKeyDetails](#) object

Required: No

#### **containerDetails**

Details of a container.

Type: [Container](#) object

Required: No

#### **ebsVolumeDetails**

Contains list of scanned and skipped EBS volumes with details.

Type: [EbsVolumeDetails](#) object

Required: No

#### **ecsClusterDetails**

Contains information about the details of the ECS Cluster.

Type: [EcsClusterDetails](#) object

Required: No

#### **eksClusterDetails**

Details about the EKS cluster involved in a Kubernetes finding.

Type: [EksClusterDetails](#) object

Required: No

### **instanceDetails**

The information about the EC2 instance associated with the activity that prompted GuardDuty to generate a finding.

Type: [InstanceDetails](#) object

Required: No

### **kubernetesDetails**

Details about the Kubernetes user and workload involved in a Kubernetes finding.

Type: [KubernetesDetails](#) object

Required: No

### **lambdaDetails**

Contains information about the Lambda function that was involved in a finding.

Type: [LambdaDetails](#) object

Required: No

### **rdsDbInstanceDetails**

Contains information about the database instance to which an anomalous login attempt was made.

Type: [RdsDbInstanceDetails](#) object

Required: No

### **rdsDbUserDetails**

Contains information about the user details through which anomalous login attempt was made.

Type: [RdsDbUserDetails](#) object

Required: No

### **resourceType**

The type of AWS resource.

Type: String

Required: No

### **s3BucketDetails**

Contains information on the S3 bucket.

Type: Array of [S3BucketDetail](#) 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 Java V2](#)
- [AWS SDK for Ruby V3](#)

# ResourceDetails

Represents the resources that were scanned in the scan entry.

## Contents

### instanceArn

Instance ARN that was scanned in the scan entry.

Type: String

Pattern: `^arn:(aws|aws-cn|aws-us-gov):[a-z]+:[a-z]+(-[0-9]+|-[a-z]+)+:[0-9]{12}:[a-z\-\_+\/][a-zA-Z0-9]*$`

Required: No

## See Also

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

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

# RuntimeContext

Additional information about the suspicious activity.

## Contents

### addressFamily

Represents the communication protocol associated with the address. For example, the address family `AF_INET` is used for IP version of 4 protocol.

Type: String

Required: No

### commandLineExample

Example of the command line involved in the suspicious activity.

Type: String

Required: No

### fileSystemType

Represents the type of mounted fileSystem.

Type: String

Required: No

### flags

Represents options that control the behavior of a runtime operation or action. For example, a filesystem mount operation may contain a read-only flag.

Type: Array of strings

Required: No

### ianaProtocolNumber

Specifies a particular protocol within the address family. Usually there is a single protocol in address families. For example, the address family `AF_INET` only has the IP protocol.

Type: Integer

Required: No

### **ldPreloadValue**

The value of the LD\_PRELOAD environment variable.

Type: String

Required: No

### **libraryPath**

The path to the new library that was loaded.

Type: String

Required: No

### **memoryRegions**

Specifies the Region of a process's address space such as stack and heap.

Type: Array of strings

Required: No

### **modifiedAt**

The timestamp at which the process modified the current process. The timestamp is in UTC date string format.

Type: Timestamp

Required: No

### **modifyingProcess**

Information about the process that modified the current process. This is available for multiple finding types.

Type: [ProcessDetails](#) object

Required: No

**moduleFilePath**

The path to the module loaded into the kernel.

Type: String

Required: No

**moduleName**

The name of the module loaded into the kernel.

Type: String

Required: No

**moduleSha256**

The SHA256 hash of the module.

Type: String

Required: No

**mountSource**

The path on the host that is mounted by the container.

Type: String

Required: No

**mountTarget**

The path in the container that is mapped to the host directory.

Type: String

Required: No

**releaseAgentPath**

The path in the container that modified the release agent file.

Type: String

Required: No

## **runcBinaryPath**

The path to the leveraged `runc` implementation.

Type: String

Required: No

## **scriptPath**

The path to the script that was executed.

Type: String

Required: No

## **serviceName**

Name of the security service that has been potentially disabled.

Type: String

Required: No

## **shellHistoryFilePath**

The path to the modified shell history file.

Type: String

Required: No

## **socketPath**

The path to the docket socket that was accessed.

Type: String

Required: No

## **targetProcess**

Information about the process that had its memory overwritten by the current process.

Type: [ProcessDetails](#) object

Required: No



## threatFilePath

The suspicious file path for which the threat intelligence details were found.

Type: String

Required: No

## toolCategory

Category that the tool belongs to. Some of the examples are Backdoor Tool, Pentest Tool, Network Scanner, and Network Sniffer.

Type: String

Required: No

## toolName

Name of the potentially suspicious tool.

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 Java V2](#)
- [AWS SDK for Ruby V3](#)

# RuntimeDetails

Information about the process and any required context values for a specific finding.

## Contents

### context

Additional information about the suspicious activity.

Type: [RuntimeContext](#) object

Required: No

### process

Information about the observed process.

Type: [ProcessDetails](#) object

Required: No

## See Also

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

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

# S3BucketDetail

Contains information on the S3 bucket.

## Contents

### arn

The Amazon Resource Name (ARN) of the S3 bucket.

Type: String

Required: No

### createdAt

The date and time the bucket was created at.

Type: Timestamp

Required: No

### defaultServerSideEncryption

Describes the server side encryption method used in the S3 bucket.

Type: [DefaultServerSideEncryption](#) object

Required: No

### name

The name of the S3 bucket.

Type: String

Required: No

### owner

The owner of the S3 bucket.

Type: [Owner](#) object

Required: No

## publicAccess

Describes the public access policies that apply to the S3 bucket.

Type: [PublicAccess](#) object

Required: No

## s3ObjectDetails

Information about the S3 object that was scanned.

Type: Array of [S3ObjectDetail](#) objects

Required: No

## tags

All tags attached to the S3 bucket

Type: Array of [Tag](#) objects

Required: No

## type

Describes whether the bucket is a source or destination bucket.

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 Java V2](#)
- [AWS SDK for Ruby V3](#)

# S3LogsConfiguration

Describes whether S3 data event logs will be enabled as a data source.

## Contents

### enable

The status of S3 data event logs as a data source.

Type: Boolean

Required: Yes

## See Also

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

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

# S3LogsConfigurationResult

Describes whether S3 data event logs will be enabled as a data source.

## Contents

### status

A value that describes whether S3 data event logs are automatically enabled for new members of the organization.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 300.

Valid Values: ENABLED | DISABLED

Required: Yes

## See Also

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

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

# S3ObjectDetail

Information about the S3 object that was scanned

## Contents

### eTag

The entity tag is a hash of the S3 object. The ETag reflects changes only to the contents of an object, and not its metadata.

Type: String

Required: No

### hash

Hash of the threat detected in this finding.

Type: String

Required: No

### key

Key of the S3 object.

Type: String

Required: No

### objectArn

Amazon Resource Name (ARN) of the S3 object.

Type: String

Required: No

### versionId

Version ID of the object.

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 Java V2](#)
- [AWS SDK for Ruby V3](#)



# Scan

Contains information about a malware scan.

## Contents

### **accountId**

The ID for the account that belongs to the scan.

Type: String

Length Constraints: Fixed length of 12.

Required: No

### **adminDetectorId**

The unique detector ID of the administrator account that the request is associated with. Note that this value will be the same as the one used for `DetectorId` if the account is an administrator.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: No

### **attachedVolumes**

List of volumes that were attached to the original instance to be scanned.

Type: Array of [VolumeDetail](#) objects

Required: No

### **detectorId**

The unique ID of the detector that the request is associated with.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: No

**failureReason**

Represents the reason for FAILED scan status.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 200.

Required: No

**fileCount**

Represents the number of files that were scanned.

Type: Long

Valid Range: Minimum value of 0.

Required: No

**resourceDetails**

Represents the resources that were scanned in the scan entry.

Type: [ResourceDetails](#) object

Required: No

**scanEndTime**

The timestamp of when the scan was finished.

Type: Timestamp

Required: No

**scanId**

The unique scan ID associated with a scan entry.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 200.

Required: No

## scanResultDetails

Represents the result of the scan.

Type: [ScanResultDetails](#) object

Required: No

## scanStartTime

The timestamp of when the scan was triggered.

Type: Timestamp

Required: No

## scanStatus

An enum value representing possible scan statuses.

Type: String

Valid Values: RUNNING | COMPLETED | FAILED | SKIPPED

Required: No

## scanType

Specifies the scan type that invoked the malware scan.

Type: String

Valid Values: GUARDDUTY\_INITIATED | ON\_DEMAND

Required: No

## totalBytes

Represents total bytes that were scanned.

Type: Long

Valid Range: Minimum value of 0.

Required: No

## triggerDetails

Specifies the reason why the scan was initiated.

Type: [TriggerDetails](#) object

Required: No

## See Also

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

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

# ScanCondition

Contains information about the condition.

## Contents

### mapEquals

Represents an *mapEqual* condition to be applied to a single field when triggering for malware scan.

Type: Array of [ScanConditionPair](#) 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 Java V2](#)
- [AWS SDK for Ruby V3](#)

# ScanConditionPair

Represents the `key:value` pair to be matched against given resource property.

## Contents

### key

Represents the **key** in the map condition.

Type: String

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

Pattern: `^(?!aws:)[a-zA-Z+ -=._:/]+$`

Required: Yes

### value

Represents optional **value** in the map condition. If not specified, only the **key** will be matched.

Type: String

Length Constraints: 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 Java V2](#)
- [AWS SDK for Ruby V3](#)

# ScanDetections

Contains a complete view providing malware scan result details.

## Contents

### highestSeverityThreatDetails

Details of the highest severity threat detected during malware scan and number of infected files.

Type: [HighestSeverityThreatDetails](#) object

Required: No

### scannedItemCount

Total number of scanned files.

Type: [ScannedItemCount](#) object

Required: No

### threatDetectedByName

Contains details about identified threats organized by threat name.

Type: [ThreatDetectedByName](#) object

Required: No

### threatsDetectedItemCount

Total number of infected files.

Type: [ThreatsDetectedItemCount](#) object

Required: No

## See Also

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

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)



# ScanEc2InstanceWithFindings

Describes whether Malware Protection for EC2 instances with findings will be enabled as a data source.

## Contents

### ebsVolumes

Describes the configuration for scanning EBS volumes as data source.

Type: Boolean

Required: No

## See Also

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

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

# ScanEc2InstanceWithFindingsResult

An object that contains information on the status of whether Malware Protection for EC2 instances with findings will be enabled as a data source.

## Contents

### ebsVolumes

Describes the configuration of scanning EBS volumes as a data source.

Type: [EbsVolumesResult](#) object

Required: No

## See Also

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

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

# ScanFilePath

Contains details of infected file including name, file path and hash.

## Contents

### fileName

File name of the infected file.

Type: String

Required: No

### filePath

The file path of the infected file.

Type: String

Required: No

### hash

The hash value of the infected file.

Type: String

Required: No

### volumeArn

EBS volume ARN details of the infected file.

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 Java V2](#)
- [AWS SDK for Ruby V3](#)

# ScannedItemCount

Total number of scanned files.

## Contents

### files

Number of files scanned.

Type: Integer

Required: No

### totalGb

Total GB of files scanned for malware.

Type: Integer

Required: No

### volumes

Total number of scanned volumes.

Type: Integer

Required: No

## See Also

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

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

# ScanResourceCriteria

Contains information about criteria used to filter resources before triggering malware scan.

## Contents

### exclude

Represents condition that when matched will prevent a malware scan for a certain resource.

Type: String to [ScanCondition](#) object map

Valid Keys: EC2\_INSTANCE\_TAG

Required: No

### include

Represents condition that when matched will allow a malware scan for a certain resource.

Type: String to [ScanCondition](#) object map

Valid Keys: EC2\_INSTANCE\_TAG

Required: No

## See Also

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

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

# ScanResultDetails

Represents the result of the scan.

## Contents

### scanResult

An enum value representing possible scan results.

Type: String

Valid Values: CLEAN | INFECTED

Required: No

## See Also

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

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

# ScanThreatName

Contains files infected with the given threat providing details of malware name and severity.

## Contents

### filePaths

List of infected files in EBS volume with details.

Type: Array of [ScanFilePath](#) objects

Required: No

### itemCount

Total number of files infected with given threat.

Type: Integer

Required: No

### name

The name of the identified threat.

Type: String

Required: No

### severity

Severity of threat identified as part of the malware scan.

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 Java V2](#)
- [AWS SDK for Ruby V3](#)

# SecurityContext

Container security context.

## Contents

### **allowPrivilegeEscalation**

Whether or not a container or a Kubernetes pod is allowed to gain more privileges than its parent process.

Type: Boolean

Required: No

### **privileged**

Whether the container is privileged.

Type: Boolean

Required: No

## See Also

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

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

# SecurityGroup

Contains information about the security groups associated with the EC2 instance.

## Contents

### **groupId**

The security group ID of the EC2 instance.

Type: String

Required: No

### **groupName**

The security group name of the EC2 instance.

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 Java V2](#)
- [AWS SDK for Ruby V3](#)

# Service

Contains additional information about the generated finding.

## Contents

### action

Information about the activity that is described in a finding.

Type: [Action](#) object

Required: No

### additionalInfo

Contains additional information about the generated finding.

Type: [ServiceAdditionalInfo](#) object

Required: No

### archived

Indicates whether this finding is archived.

Type: Boolean

Required: No

### count

The total count of the occurrences of this finding type.

Type: Integer

Required: No

### detection

Contains information about the detected unusual behavior.

Type: [Detection](#) object

Required: No

**detectorId**

The detector ID for the GuardDuty service.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: No

**ebsVolumeScanDetails**

Returns details from the malware scan that created a finding.

Type: [EbsVolumeScanDetails](#) object

Required: No

**eventFirstSeen**

The first-seen timestamp of the activity that prompted GuardDuty to generate this finding.

Type: String

Required: No

**eventLastSeen**

The last-seen timestamp of the activity that prompted GuardDuty to generate this finding.

Type: String

Required: No

**evidence**

An evidence object associated with the service.

Type: [Evidence](#) object

Required: No

**featureName**

The name of the feature that generated a finding.

Type: String

Required: No

### **malwareScanDetails**

Returns details from the malware scan that generated a GuardDuty finding.

Type: [MalwareScanDetails](#) object

Required: No

### **resourceRole**

The resource role information for this finding.

Type: String

Required: No

### **runtimeDetails**

Information about the process and any required context values for a specific finding

Type: [RuntimeDetails](#) object

Required: No

### **serviceName**

The name of the AWS service (GuardDuty) that generated a finding.

Type: String

Required: No

### **userFeedback**

Feedback that was submitted about the finding.

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 Java V2](#)
- [AWS SDK for Ruby V3](#)

# ServiceAdditionalInfo

Additional information about the generated finding.

## Contents

### type

Describes the type of the additional information.

Type: String

Required: No

### value

This field specifies the value of the additional information.

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 Java V2](#)
- [AWS SDK for Ruby V3](#)



# SortCriteria

Contains information about the criteria used for sorting findings.

## Contents

### attributeName

Represents the finding attribute, such as `accountId`, that sorts the findings.

Type: String

Required: No

### orderBy

The order by which the sorted findings are to be displayed.

Type: String

Valid Values: ASC | DESC

Required: No

## See Also

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

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

# Tag

Contains information about a tag associated with the EC2 instance.

## Contents

### key

The EC2 instance tag key.

Type: String

Required: No

### value

The EC2 instance tag value.

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 Java V2](#)
- [AWS SDK for Ruby V3](#)

# Threat

Information about the detected threats associated with the generated finding.

## Contents

### itemPaths

Information about the nested item path and hash of the protected resource.

Type: Array of [ItemPath](#) objects

Required: No

### name

Name of the detected threat that caused GuardDuty to generate this finding.

Type: String

Required: No

### source

Source of the threat that generated this finding.

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 Java V2](#)
- [AWS SDK for Ruby V3](#)

# ThreatDetectedByName

Contains details about identified threats organized by threat name.

## Contents

### itemCount

Total number of infected files identified.

Type: Integer

Required: No

### shortened

Flag to determine if the finding contains every single infected file-path and/or every threat.

Type: Boolean

Required: No

### threatNames

List of identified threats with details, organized by threat name.

Type: Array of [ScanThreatName](#) objects

Required: No

### uniqueThreatNameCount

Total number of unique threats by name identified, as part of the malware scan.

Type: Integer

Required: No

## See Also

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

- [AWS SDK for C++](#)

- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

# ThreatIntelligenceDetail

An instance of a threat intelligence detail that constitutes evidence for the finding.

## Contents

### **threatFileSha256**

SHA256 of the file that generated the finding.

Type: String

Required: No

### **threatListName**

The name of the threat intelligence list that triggered the finding.

Type: String

Required: No

### **threatNames**

A list of names of the threats in the threat intelligence list that triggered the finding.

Type: Array of strings

Required: No

## See Also

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

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

# ThreatsDetectedItemCount

Contains total number of infected files.

## Contents

### files

Total number of infected files.

Type: Integer

Required: No

## See Also

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

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

# Total

Contains the total usage with the corresponding currency unit for that value.

## Contents

### amount

The total usage.

Type: String

Required: No

### unit

The currency unit that the amount is given in.

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 Java V2](#)
- [AWS SDK for Ruby V3](#)



# TriggerDetails

Represents the reason the scan was triggered.

## Contents

### description

The description of the scan trigger.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 200.

Required: No

### guardDutyFindingId

The ID of the GuardDuty finding that triggered the malware scan.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 200.

Required: No

## See Also

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

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

# UnprocessedAccount

Contains information about the accounts that weren't processed.

## Contents

### accountId

The AWS account ID.

Type: String

Length Constraints: Fixed length of 12.

Required: Yes

### result

A reason why the account hasn't been processed.

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 Java V2](#)
- [AWS SDK for Ruby V3](#)

# UnprocessedDataSourcesResult

Specifies the names of the data sources that couldn't be enabled.

## Contents

### malwareProtection

An object that contains information on the status of all Malware Protection data sources.

Type: [MalwareProtectionConfigurationResult](#) object

Required: No

## See Also

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

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

# UpdateProtectedResource

Information about the protected resource that is associated with the created Malware Protection plan. Presently, S3Bucket is the only supported protected resource.

## Contents

### s3Bucket

Information about the protected S3 bucket resource.

Type: [UpdateS3BucketResource](#) object

Required: No

## See Also

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

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

# UpdateS3BucketResource

Information about the protected S3 bucket resource.

## Contents

### objectPrefixes

Information about the specified object prefixes. The S3 object will be scanned only if it belongs to any of the specified object prefixes.

Type: Array of strings

Array Members: Minimum number of 0 items. Maximum number of 5 items.

Required: No

## See Also

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

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

# UsageAccountResult

Contains information on the total of usage based on account IDs.

## Contents

### accountId

The Account ID that generated usage.

Type: String

Length Constraints: Fixed length of 12.

Required: No

### total

Represents the total of usage for the Account ID.

Type: [Total](#) object

Required: No

## See Also

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

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

# UsageCriteria

Contains information about the criteria used to query usage statistics.

## Contents

### accountIds

The account IDs to aggregate usage statistics from.

Type: Array of strings

Array Members: Minimum number of 1 item. Maximum number of 50 items.

Length Constraints: Fixed length of 12.

Required: No

### dataSources

*This member has been deprecated.*

The data sources to aggregate usage statistics from.

Type: Array of strings

Valid Values: FLOW\_LOGS | CLOUD\_TRAIL | DNS\_LOGS | S3\_LOGS |  
KUBERNETES\_AUDIT\_LOGS | EC2\_MALWARE\_SCAN

Required: No

### features

The features to aggregate usage statistics from.

Type: Array of strings

Valid Values: FLOW\_LOGS | CLOUD\_TRAIL | DNS\_LOGS | S3\_DATA\_EVENTS  
| EKS\_AUDIT\_LOGS | EBS\_MALWARE\_PROTECTION | RDS\_LOGIN\_EVENTS  
| LAMBDA\_NETWORK\_LOGS | EKS\_RUNTIME\_MONITORING |  
FARGATE\_RUNTIME\_MONITORING | EC2\_RUNTIME\_MONITORING |  
RDS\_DBI\_PROTECTION\_PROVISIONED | RDS\_DBI\_PROTECTION\_SERVERLESS

Required: No

## resources

The resources to aggregate usage statistics from. Only accepts exact resource names.

Type: Array of strings

Required: No

## See Also

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

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)



# UsageDataSourceResult

Contains information on the result of usage based on data source type.

## Contents

### dataSource

The data source type that generated usage.

Type: String

Valid Values: FLOW\_LOGS | CLOUD\_TRAIL | DNS\_LOGS | S3\_LOGS | KUBERNETES\_AUDIT\_LOGS | EC2\_MALWARE\_SCAN

Required: No

### total

Represents the total of usage for the specified data source.

Type: [Total](#) object

Required: No

## See Also

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

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

# UsageFeatureResult

Contains information about the result of the total usage based on the feature.

## Contents

### feature

The feature that generated the usage cost.

Type: String

Valid Values: FLOW\_LOGS | CLOUD\_TRAIL | DNS\_LOGS | S3\_DATA\_EVENTS  
| EKS\_AUDIT\_LOGS | EBS\_MALWARE\_PROTECTION | RDS\_LOGIN\_EVENTS  
| LAMBDA\_NETWORK\_LOGS | EKS\_RUNTIME\_MONITORING |  
FARGATE\_RUNTIME\_MONITORING | EC2\_RUNTIME\_MONITORING |  
RDS\_DBI\_PROTECTION\_PROVISIONED | RDS\_DBI\_PROTECTION\_SERVERLESS

Required: No

### total

Contains the total usage with the corresponding currency unit for that value.

Type: [Total](#) object

Required: No

## See Also

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

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

# UsageResourceResult

Contains information on the sum of usage based on an AWS resource.

## Contents

### resource

The AWS resource that generated usage.

Type: String

Required: No

### total

Represents the sum total of usage for the specified resource type.

Type: [Total](#) object

Required: No

## See Also

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

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

# UsageStatistics

Contains the result of GuardDuty usage. If a `UsageStatisticType` is provided the result for other types will be null.

## Contents

### **sumByAccount**

The usage statistic sum organized by account ID.

Type: Array of [UsageAccountResult](#) objects

Required: No

### **sumByDataSource**

The usage statistic sum organized by on data source.

Type: Array of [UsageDataSourceResult](#) objects

Required: No

### **sumByFeature**

The usage statistic sum organized by feature.

Type: Array of [UsageFeatureResult](#) objects

Required: No

### **sumByResource**

The usage statistic sum organized by resource.

Type: Array of [UsageResourceResult](#) objects

Required: No

### **topAccountsByFeature**

Lists the top 50 accounts by feature that have generated the most GuardDuty usage, in the order from most to least expensive.

Currently, this doesn't support `RDS_LOGIN_EVENTS`.

Type: Array of [UsageTopAccountsResult](#) objects

Required: No

### **topResources**

Lists the top 50 resources that have generated the most GuardDuty usage, in order from most to least expensive.

Type: Array of [UsageResourceResult](#) 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 Java V2](#)
- [AWS SDK for Ruby V3](#)

# UsageTopAccountResult

Contains information on the total of usage based on the topmost 50 account IDs.

## Contents

### accountId

The unique account ID.

Type: String

Length Constraints: Fixed length of 12.

Required: No

### total

Contains the total usage with the corresponding currency unit for that value.

Type: [Total](#) object

Required: No

## See Also

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

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

# UsageTopAccountsResult

Information about the usage statistics, calculated by top accounts by feature.

## Contents

### accounts

The accounts that contributed to the total usage cost.

Type: Array of [UsageTopAccountResult](#) objects

Required: No

### feature

Features by which you can generate the usage statistics.

RDS\_LOGIN\_EVENTS is currently not supported with topAccountsByFeature.

Type: String

Valid Values: FLOW\_LOGS | CLOUD\_TRAIL | DNS\_LOGS | S3\_DATA\_EVENTS  
| EKS\_AUDIT\_LOGS | EBS\_MALWARE\_PROTECTION | RDS\_LOGIN\_EVENTS  
| LAMBDA\_NETWORK\_LOGS | EKS\_RUNTIME\_MONITORING |  
FARGATE\_RUNTIME\_MONITORING | EC2\_RUNTIME\_MONITORING |  
RDS\_DBI\_PROTECTION\_PROVISIONED | RDS\_DBI\_PROTECTION\_SERVERLESS

Required: No

## See Also

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

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

# Volume

Volume used by the Kubernetes workload.

## Contents

### hostPath

Represents a pre-existing file or directory on the host machine that the volume maps to.

Type: [HostPath](#) object

Required: No

### name

Volume name.

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 Java V2](#)
- [AWS SDK for Ruby V3](#)



# VolumeDetail

Contains EBS volume details.

## Contents

### **deviceName**

The device name for the EBS volume.

Type: String

Required: No

### **encryptionType**

EBS volume encryption type.

Type: String

Required: No

### **kmsKeyArn**

KMS key ARN used to encrypt the EBS volume.

Type: String

Required: No

### **snapshotArn**

Snapshot ARN of the EBS volume.

Type: String

Required: No

### **volumeArn**

EBS volume ARN information.

Type: String

Required: No

**volumeSizeInGB**

EBS volume size in GB.

Type: Integer

Required: No

**volumeType**

The EBS volume type.

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 Java V2](#)
- [AWS SDK for Ruby V3](#)

# VolumeMount

Container volume mount.

## Contents

### mountPath

Volume mount path.

Type: String

Required: No

### name

Volume mount name.

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 Java V2](#)
- [AWS SDK for Ruby V3](#)

# VpcConfig

Amazon Virtual Private Cloud configuration details associated with your Lambda function.

## Contents

### **securityGroups**

The identifier of the security group attached to the Lambda function.

Type: Array of [SecurityGroup](#) objects

Required: No

### **subnetIds**

The identifiers of the subnets that are associated with your Lambda function.

Type: Array of strings

Required: No

### **vpclId**

The identifier of the Amazon Virtual Private Cloud.

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 Java V2](#)
- [AWS SDK for Ruby V3](#)

# Common Parameters

The following list contains the parameters that all actions use for signing Signature Version 4 requests with a query string. Any action-specific parameters are listed in the topic for that action. For more information about Signature Version 4, see [Signing AWS API requests](#) in the *IAM User Guide*.

## Action

The action to be performed.

Type: string

Required: Yes

## Version

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

Type: string

Required: Yes

## X-Amz-Algorithm

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

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

Type: string

Valid Values: AWS4-HMAC-SHA256

Required: Conditional

## X-Amz-Credential

The credential scope value, which is a string that includes your access key, the date, the region you are targeting, the service you are requesting, and a termination string ("aws4\_request"). The value is expressed in the following format: *access\_key/YYYYMMDD/region/service/aws4\_request*.

For more information, see [Create a signed AWS API request](#) in the *IAM User Guide*.

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

Type: string

Required: Conditional

### **X-Amz-Date**

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

Condition: X-Amz-Date is optional for all requests; it can be used to override the date used for signing requests. If the Date header is specified in the ISO 8601 basic format, X-Amz-Date is not required. When X-Amz-Date is used, it always overrides the value of the Date header. For more information, see [Elements of an AWS API request signature](#) in the *IAM User Guide*.

Type: string

Required: Conditional

### **X-Amz-Security-Token**

The temporary security token that was obtained through a call to AWS Security Token Service (AWS STS). For a list of services that support temporary security credentials from AWS STS, see [AWS services that work with IAM](#) in the *IAM User Guide*.

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

Type: string

Required: Conditional

### **X-Amz-Signature**

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

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

Type: string

Required: Conditional

### **X-Amz-SignedHeaders**

Specifies all the HTTP headers that were included as part of the canonical request. For more information about specifying signed headers, see [Create a signed AWS API request](#) in the *IAM User Guide*.

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

Type: string

Required: Conditional

# Common Errors

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

## **AccessDeniedException**

You do not have sufficient access to perform this action.

HTTP Status Code: 403

## **ExpiredTokenException**

The security token included in the request is expired

HTTP Status Code: 403

## **IncompleteSignature**

The request signature does not conform to AWS standards.

HTTP Status Code: 403

## **InternalFailure**

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

HTTP Status Code: 500

## **MalformedHttpRequestException**

Problems with the request at the HTTP level, e.g. we can't decompress the body according to the decompression algorithm specified by the content-encoding.

HTTP Status Code: 400

## **NotAuthorized**

You do not have permission to perform this action.

HTTP Status Code: 401

## **OptInRequired**

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



HTTP Status Code: 403

### **RequestAbortedException**

Convenient exception that can be used when a request is aborted before a reply is sent back (e.g. client closed connection).

HTTP Status Code: 400

### **RequestEntityTooLargeException**

Problems with the request at the HTTP level. The request entity is too large.

HTTP Status Code: 413

### **RequestExpired**

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

HTTP Status Code: 400

### **RequestTimeoutException**

Problems with the request at the HTTP level. Reading the Request timed out.

HTTP Status Code: 408

### **ServiceUnavailable**

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

HTTP Status Code: 503

### **ThrottlingException**

The request was denied due to request throttling.

HTTP Status Code: 400

### **UnrecognizedClientException**

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

HTTP Status Code: 403

**UnknownOperationException**

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

HTTP Status Code: 404

**ValidationError**

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

HTTP Status Code: 400