aws

API Reference

Amazon CloudWatch Logs

API Version 2014-03-28

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon CloudWatch Logs: API Reference

Copyright © 2026 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

Welcome **1**
Actions **3**
AssociateKmsKey 8
Request Syntax 9
Request Parameters 9
Response Elements 11
Errors 11
Examples 11
See Also 13
AssociateSourceToS3TableIntegration 14
Request Syntax 14
Request Parameters 14
Response Syntax 15
Response Elements 15
Errors 15
See Also 16
CancelExportTask 17
Request Syntax 17
Request Parameters 17
Response Elements 17
Errors 17
Examples 18
See Also 19
CancelImportTask 20
Request Syntax 20
Request Parameters 20
Response Syntax 20
Response Elements 21
Errors 22
Examples 22
See Also 23
CreateDelivery 24
Request Syntax 24
Request Parameters 25

Response Syntax ... 26
Response Elements ... 27
Errors ... 27
See Also ... 28
CreateExportTask ... 30
Request Syntax ... 30
Request Parameters ... 31
Response Syntax ... 33
Response Elements ... 33
Errors ... 33
Examples ... 34
See Also ... 35
CreateImportTask ... 36
Request Syntax ... 37
Request Parameters ... 37
Response Syntax ... 38
Response Elements ... 38
Errors ... 39
Examples ... 40
See Also ... 40
CreateLogAnomalyDetector ... 42
Request Syntax ... 42
Request Parameters ... 43
Response Syntax ... 45
Response Elements ... 45
Errors ... 46
See Also ... 46
CreateLogGroup ... 48
Request Syntax ... 48
Request Parameters ... 49
Response Elements ... 51
Errors ... 51
Examples ... 52
See Also ... 52
CreateLogStream ... 54
Request Syntax ... 54

Request Parameters 54
Response Elements 55
Errors 55
Examples 56
See Also 56
CreateLookupTable 58
Request Syntax 58
Request Parameters 58
Response Syntax 60
Response Elements 60
Errors 61
See Also 62
CreateScheduledQuery 63
Request Syntax 63
Request Parameters 64
Response Syntax 67
Response Elements 68
Errors 68
See Also 69
DeleteAccountPolicy 71
Request Syntax 71
Request Parameters 71
Response Elements 72
Errors 72
See Also 73
DeleteDataProtectionPolicy 74
Request Syntax 74
Request Parameters 74
Response Elements 74
Errors 74
See Also 75
DeleteDelivery 76
Request Syntax 76
Request Parameters 76
Response Elements 76
Errors 76

See Also ... 77
DeleteDeliveryDestination ... 79
Request Syntax ... 79
Request Parameters ... 79
Response Elements ... 79
Errors ... 79
See Also ... 80
DeleteDeliveryDestinationPolicy ... 82
Request Syntax ... 82
Request Parameters ... 82
Response Elements ... 82
Errors ... 82
See Also ... 83
DeleteDeliverySource ... 84
Request Syntax ... 84
Request Parameters ... 84
Response Elements ... 84
Errors ... 84
See Also ... 85
DeleteDestination ... 87
Request Syntax ... 87
Request Parameters ... 87
Response Elements ... 87
Errors ... 87
Examples ... 88
See Also ... 89
DeleteIndexPolicy ... 90
Request Syntax ... 90
Request Parameters ... 90
Response Elements ... 91
Errors ... 91
See Also ... 91
DeleteIntegration ... 93
Request Syntax ... 93
Request Parameters ... 93
Response Elements ... 94

Errors ... 94
See Also ... 94
DeleteLogAnomalyDetector ... 96
Request Syntax ... 96
Request Parameters ... 96
Response Elements ... 96
Errors ... 96
See Also ... 97
DeleteLogGroup ... 98
Request Syntax ... 98
Request Parameters ... 98
Response Elements ... 98
Errors ... 98
Examples ... 99
See Also ... 100
DeleteLogStream ... 101
Request Syntax ... 101
Request Parameters ... 101
Response Elements ... 102
Errors ... 102
Examples ... 102
See Also ... 103
DeleteLookupTable ... 105
Request Syntax ... 105
Request Parameters ... 105
Response Elements ... 105
Errors ... 105
See Also ... 106
DeleteMetricFilter ... 107
Request Syntax ... 107
Request Parameters ... 107
Response Elements ... 108
Errors ... 108
Examples ... 108
See Also ... 109
DeleteQueryDefinition ... 110

Request Syntax ... 110
Request Parameters ... 110
Response Syntax ... 110
Response Elements ... 111
Errors ... 111
Examples ... 111
See Also ... 112
DeleteResourcePolicy ... 114
Request Syntax ... 114
Request Parameters ... 114
Response Elements ... 115
Errors ... 115
See Also ... 115
DeleteRetentionPolicy ... 117
Request Syntax ... 117
Request Parameters ... 117
Response Elements ... 117
Errors ... 117
Examples ... 118
See Also ... 119
DeleteScheduledQuery ... 120
Request Syntax ... 120
Request Parameters ... 120
Response Elements ... 120
Errors ... 120
See Also ... 121
DeleteSubscriptionFilter ... 123
Request Syntax ... 123
Request Parameters ... 123
Response Elements ... 124
Errors ... 124
Examples ... 124
See Also ... 125
DeleteSyslogConfiguration ... 126
Request Syntax ... 126
Request Parameters ... 126

Response Elements ... 126
Errors ... 127
Examples ... 128
See Also ... 128
DeleteTransformer ... 130
Request Syntax ... 130
Request Parameters ... 130
Response Elements ... 130
Errors ... 131
See Also ... 131
DescribeAccountPolicies ... 133
Request Syntax ... 133
Request Parameters ... 133
Response Syntax ... 134
Response Elements ... 135
Errors ... 135
See Also ... 136
DescribeConfigurationTemplates ... 137
Request Syntax ... 137
Request Parameters ... 137
Response Syntax ... 139
Response Elements ... 140
Errors ... 140
See Also ... 141
DescribeDeliveries ... 142
Request Syntax ... 142
Request Parameters ... 142
Response Syntax ... 143
Response Elements ... 143
Errors ... 144
See Also ... 144
DescribeDeliveryDestinations ... 146
Request Syntax ... 146
Request Parameters ... 146
Response Syntax ... 146
Response Elements ... 147

Errors ... 147
See Also ... 148
DescribeDeliverySources ... 149
Request Syntax ... 149
Request Parameters ... 149
Response Syntax ... 149
Response Elements ... 150
Errors ... 150
See Also ... 151
DescribeDestinations ... 152
Request Syntax ... 152
Request Parameters ... 152
Response Syntax ... 153
Response Elements ... 153
Errors ... 154
Examples ... 154
See Also ... 155
DescribeExportTasks ... 156
Request Syntax ... 156
Request Parameters ... 156
Response Syntax ... 157
Response Elements ... 158
Errors ... 158
Examples ... 158
See Also ... 160
DescribeFieldIndexes ... 162
Request Syntax ... 162
Request Parameters ... 162
Response Syntax ... 163
Response Elements ... 164
Errors ... 164
See Also ... 165
DescribeImportTaskBatches ... 166
Request Syntax ... 166
Request Parameters ... 166
Response Syntax ... 167

Response Elements ... 167
Errors ... 168
Examples ... 169
See Also ... 170
DescribeImportTasks ... 171
Request Syntax ... 171
Request Parameters ... 171
Response Syntax ... 172
Response Elements ... 173
Errors ... 173
Examples ... 174
See Also ... 175
DescribeIndexPolicies ... 176
Request Syntax ... 176
Request Parameters ... 176
Response Syntax ... 177
Response Elements ... 177
Errors ... 178
See Also ... 178
DescribeLogGroups ... 180
Request Syntax ... 180
Request Parameters ... 180
Response Syntax ... 184
Response Elements ... 184
Errors ... 185
Examples ... 185
See Also ... 187
DescribeLogStreams ... 188
Request Syntax ... 188
Request Parameters ... 188
Response Syntax ... 191
Response Elements ... 191
Errors ... 192
Examples ... 192
See Also ... 194
DescribeLookupTables ... 196

Request Syntax ... 196
Request Parameters ... 196
Response Syntax ... 197
Response Elements ... 197
Errors ... 198
See Also ... 198
DescribeMetricFilters ... 200
Request Syntax ... 200
Request Parameters ... 200
Response Syntax ... 202
Response Elements ... 202
Errors ... 203
Examples ... 203
See Also ... 204
DescribeQueries ... 206
Request Syntax ... 206
Request Parameters ... 206
Response Syntax ... 207
Response Elements ... 208
Errors ... 208
Examples ... 209
See Also ... 210
DescribeQueryDefinitions ... 212
Request Syntax ... 212
Request Parameters ... 212
Response Syntax ... 213
Response Elements ... 214
Errors ... 214
Examples ... 214
See Also ... 216
DescribeResourcePolicies ... 217
Request Syntax ... 217
Request Parameters ... 217
Response Syntax ... 218
Response Elements ... 218
Errors ... 219

See Also ... 219
DescribeSubscriptionFilters ... 220
Request Syntax ... 220
Request Parameters ... 220
Response Syntax ... 221
Response Elements ... 222
Errors ... 222
Examples ... 223
See Also ... 224
DisassociateKmsKey ... 225
Request Syntax ... 225
Request Parameters ... 225
Response Elements ... 226
Errors ... 227
Examples ... 227
See Also ... 228
DisassociateSourceFromS3TableIntegration ... 229
Request Syntax ... 229
Request Parameters ... 229
Response Syntax ... 229
Response Elements ... 229
Errors ... 230
See Also ... 231
FilterLogEvents ... 232
Request Syntax ... 233
Request Parameters ... 233
Response Syntax ... 237
Response Elements ... 238
Errors ... 238
Examples ... 239
See Also ... 243
GetDataProtectionPolicy ... 245
Request Syntax ... 245
Request Parameters ... 245
Response Syntax ... 245
Response Elements ... 245

Errors ... 246
See Also ... 247
GetDelivery ... 248
Request Syntax ... 248
Request Parameters ... 248
Response Syntax ... 248
Response Elements ... 249
Errors ... 249
See Also ... 250
GetDeliveryDestination ... 251
Request Syntax ... 251
Request Parameters ... 251
Response Syntax ... 251
Response Elements ... 252
Errors ... 252
See Also ... 253
GetDeliveryDestinationPolicy ... 254
Request Syntax ... 254
Request Parameters ... 254
Response Syntax ... 254
Response Elements ... 254
Errors ... 255
See Also ... 255
GetDeliverySource ... 257
Request Syntax ... 257
Request Parameters ... 257
Response Syntax ... 257
Response Elements ... 258
Errors ... 258
See Also ... 259
GetIntegration ... 260
Request Syntax ... 260
Request Parameters ... 260
Response Syntax ... 260
Response Elements ... 260
Errors ... 261

See Also ... 262
GetLogAnomalyDetector ... 263
Request Syntax ... 263
Request Parameters ... 263
Response Syntax ... 263
Response Elements ... 264
Errors ... 266
See Also ... 266
GetLogEvents ... 268
Request Syntax ... 269
Request Parameters ... 269
Response Syntax ... 272
Response Elements ... 272
Errors ... 273
Examples ... 273
See Also ... 275
GetLogFields ... 277
Request Syntax ... 277
Request Parameters ... 277
Response Syntax ... 277
Response Elements ... 278
Errors ... 278
See Also ... 279
GetLogGroupFields ... 280
Request Syntax ... 280
Request Parameters ... 280
Response Syntax ... 282
Response Elements ... 282
Errors ... 282
Examples ... 283
See Also ... 285
GetLogObject ... 286
Request Syntax ... 286
Request Parameters ... 286
Response Syntax ... 287
Response Elements ... 287

Errors ... 288
See Also ... 288
GetLogRecord ... 290
Request Syntax ... 290
Request Parameters ... 290
Response Syntax ... 291
Response Elements ... 291
Errors ... 291
Examples ... 292
See Also ... 293
GetLookupTable ... 294
Request Syntax ... 294
Request Parameters ... 294
Response Syntax ... 294
Response Elements ... 294
Errors ... 296
See Also ... 296
GetQueryResults ... 298
Request Syntax ... 298
Request Parameters ... 298
Response Syntax ... 299
Response Elements ... 300
Errors ... 301
Examples ... 302
See Also ... 304
GetScheduledQuery ... 305
Request Syntax ... 305
Request Parameters ... 305
Response Syntax ... 305
Response Elements ... 306
Errors ... 310
See Also ... 310
GetScheduledQueryHistory ... 312
Request Syntax ... 312
Request Parameters ... 312
Response Syntax ... 313

Response Elements ... 314
Errors ... 315
See Also ... 316
GetStorageTierPolicy ... 317
Response Syntax ... 317
Response Elements ... 317
Errors ... 317
See Also ... 318
GetTransformer ... 320
Request Syntax ... 320
Request Parameters ... 320
Response Syntax ... 320
Response Elements ... 324
Errors ... 325
See Also ... 325
ListAggregateLogGroupSummaries ... 327
Request Syntax ... 327
Request Parameters ... 327
Response Syntax ... 330
Response Elements ... 330
Errors ... 331
See Also ... 331
ListAnomalies ... 333
Request Syntax ... 333
Request Parameters ... 333
Response Syntax ... 334
Response Elements ... 335
Errors ... 336
Examples ... 336
See Also ... 344
ListIntegrations ... 346
Request Syntax ... 346
Request Parameters ... 346
Response Syntax ... 347
Response Elements ... 347
Errors ... 347

See Also ... 348
ListLogAnomalyDetectors ... 349
Request Syntax ... 349
Request Parameters ... 349
Response Syntax ... 350
Response Elements ... 350
Errors ... 351
See Also ... 351
ListLogGroups ... 353
Request Syntax ... 353
Request Parameters ... 353
Response Syntax ... 356
Response Elements ... 357
Errors ... 357
See Also ... 358
ListLogGroupsForQuery ... 359
Request Syntax ... 359
Request Parameters ... 359
Response Syntax ... 360
Response Elements ... 360
Errors ... 361
Examples ... 361
See Also ... 362
ListScheduledQueries ... 364
Request Syntax ... 364
Request Parameters ... 364
Response Syntax ... 365
Response Elements ... 366
Errors ... 366
See Also ... 367
ListSourcesForS3TableIntegration ... 368
Request Syntax ... 368
Request Parameters ... 368
Response Syntax ... 369
Response Elements ... 369
Errors ... 370

See Also ... 370
ListSyslogConfigurations ... 372
Request Syntax ... 372
Request Parameters ... 372
Response Syntax ... 373
Response Elements ... 373
Errors ... 374
Examples ... 375
See Also ... 376
ListTagsForResource ... 377
Request Syntax ... 377
Request Parameters ... 377
Response Syntax ... 377
Response Elements ... 378
Errors ... 378
See Also ... 379
ListTagsLogGroup ... 380
Request Syntax ... 380
Request Parameters ... 380
Response Syntax ... 380
Response Elements ... 381
Errors ... 381
See Also ... 382
PutAccountPolicy ... 383
Request Syntax ... 391
Request Parameters ... 391
Response Syntax ... 395
Response Elements ... 395
Errors ... 395
Examples ... 396
See Also ... 401
PutBearerTokenAuthentication ... 402
Request Syntax ... 402
Request Parameters ... 402
Response Elements ... 403
Errors ... 403

Examples ... 404
See Also ... 404
PutDataProtectionPolicy ... 406
Request Syntax ... 406
Request Parameters ... 406
Response Syntax ... 408
Response Elements ... 408
Errors ... 409
Examples ... 409
See Also ... 413
PutDeliveryDestination ... 414
Request Syntax ... 414
Request Parameters ... 415
Response Syntax ... 417
Response Elements ... 417
Errors ... 417
See Also ... 418
PutDeliveryDestinationPolicy ... 420
Request Syntax ... 420
Request Parameters ... 420
Response Syntax ... 421
Response Elements ... 421
Errors ... 421
Examples ... 422
See Also ... 423
PutDeliverySource ... 425
Request Syntax ... 425
Request Parameters ... 426
Response Syntax ... 429
Response Elements ... 429
Errors ... 430
See Also ... 431
PutDestination ... 432
Request Syntax ... 432
Request Parameters ... 432
Response Syntax ... 433

Response Elements ... 434
Errors ... 434
Examples ... 435
See Also ... 436
PutDestinationPolicy ... 437
Request Syntax ... 437
Request Parameters ... 437
Response Elements ... 438
Errors ... 438
Examples ... 439
See Also ... 439
PutIndexPolicy ... 441
Request Syntax ... 442
Request Parameters ... 442
Response Syntax ... 443
Response Elements ... 443
Errors ... 444
Examples ... 444
See Also ... 445
PutIntegration ... 446
Request Syntax ... 446
Request Parameters ... 446
Response Syntax ... 447
Response Elements ... 447
Errors ... 448
See Also ... 448
PutLogEvents ... 450
Request Syntax ... 451
Request Parameters ... 451
Response Syntax ... 453
Response Elements ... 453
Errors ... 454
Examples ... 455
See Also ... 456
PutLogGroupDeletionProtection ... 458
Request Syntax ... 458

Request Parameters ... 458
Response Elements ... 459
Errors ... 459
Examples ... 460
See Also ... 460
PutMetricFilter ... 462
Request Syntax ... 462
Request Parameters ... 463
Response Elements ... 465
Errors ... 465
Examples ... 466
See Also ... 467
PutQueryDefinition ... 468
Request Syntax ... 468
Request Parameters ... 468
Response Syntax ... 471
Response Elements ... 471
Errors ... 471
Examples ... 472
See Also ... 475
PutResourcePolicy ... 476
Request Syntax ... 476
Request Parameters ... 476
Response Syntax ... 478
Response Elements ... 478
Errors ... 479
See Also ... 479
PutRetentionPolicy ... 481
Request Syntax ... 481
Request Parameters ... 481
Response Elements ... 482
Errors ... 482
Examples ... 483
See Also ... 484
PutStorageTierPolicy ... 485
Request Syntax ... 485

Request Parameters ... 485
Response Syntax ... 485
Response Elements ... 485
Errors ... 486
See Also ... 487
PutSubscriptionFilter ... 488
Request Syntax ... 488
Request Parameters ... 489
Response Elements ... 492
Errors ... 492
Examples ... 493
See Also ... 493
PutSyslogConfiguration ... 495
Request Syntax ... 495
Request Parameters ... 495
Response Elements ... 495
Errors ... 496
Examples ... 497
See Also ... 497
PutTransformer ... 499
Request Syntax ... 499
Request Parameters ... 503
Response Elements ... 503
Errors ... 503
Examples ... 504
See Also ... 506
StartLiveTail ... 507
Request Syntax ... 508
Request Parameters ... 508
Response Syntax ... 510
Response Elements ... 511
Errors ... 511
See Also ... 512
StartQuery ... 513
Request Syntax ... 514
Request Parameters ... 514

Response Syntax ... 517
Response Elements ... 517
Errors ... 517
Examples ... 518
See Also ... 521
StopQuery ... 522
Request Syntax ... 522
Request Parameters ... 522
Response Syntax ... 522
Response Elements ... 522
Errors ... 523
Examples ... 523
See Also ... 524
TagLogGroup ... 526
Request Syntax ... 526
Request Parameters ... 526
Response Elements ... 527
Errors ... 527
Examples ... 528
See Also ... 528
TagResource ... 530
Request Syntax ... 530
Request Parameters ... 530
Response Elements ... 531
Errors ... 531
See Also ... 532
TestMetricFilter ... 533
Request Syntax ... 533
Request Parameters ... 533
Response Syntax ... 534
Response Elements ... 534
Errors ... 534
Examples ... 535
See Also ... 546
TestTransformer ... 548
Request Syntax ... 548

Request Parameters ... 551
Response Syntax ... 552
Response Elements ... 552
Errors ... 552
See Also ... 553
UntagLogGroup ... 554
Request Syntax ... 554
Request Parameters ... 554
Response Elements ... 555
Errors ... 555
Examples ... 555
See Also ... 556
UntagResource ... 557
Request Syntax ... 557
Request Parameters ... 557
Response Elements ... 558
Errors ... 558
See Also ... 558
UpdateAnomaly ... 560
Request Syntax ... 560
Request Parameters ... 560
Response Elements ... 562
Errors ... 562
See Also ... 563
UpdateDeliveryConfiguration ... 564
Request Syntax ... 564
Request Parameters ... 564
Response Elements ... 565
Errors ... 565
See Also ... 566
UpdateLogAnomalyDetector ... 568
Request Syntax ... 568
Request Parameters ... 568
Response Elements ... 569
Errors ... 569
See Also ... 570

UpdateLookupTable ... 571
Request Syntax ... 571
Request Parameters ... 571
Response Syntax ... 572
Response Elements ... 573
Errors ... 573
See Also ... 574
UpdateScheduledQuery ... 575
Request Syntax ... 575
Request Parameters ... 576
Response Syntax ... 579
Response Elements ... 580
Errors ... 583
See Also ... 584
Data Types ... 585
AccountPolicy ... 590
Contents ... 590
See Also ... 591
AddKeyEntry ... 592
Contents ... 592
See Also ... 592
AddKeys ... 594
Contents ... 594
See Also ... 594
AggregateLogGroupSummary ... 595
Contents ... 595
See Also ... 595
Anomaly ... 596
Contents ... 596
See Also ... 600
AnomalyDetector ... 601
Contents ... 601
See Also ... 603
ConfigurationTemplate ... 604
Contents ... 604
See Also ... 606

ConfigurationTemplateDeliveryConfigValues 608
Contents 608
See Also 609
CopyValue 610
Contents 610
See Also 610
CopyValueEntry 611
Contents 611
See Also 611
CSV 613
Contents 613
See Also 614
DataSource 615
Contents 615
See Also 615
DataSourceFilter 616
Contents 616
See Also 616
DateTimeConverter 617
Contents 617
See Also 618
DeleteKeys 620
Contents 620
See Also 620
Delivery 621
Contents 621
See Also 623
DeliveryDestination 624
Contents 624
See Also 626
DeliveryDestinationConfiguration 627
Contents 627
See Also 627
DeliverySource 628
Contents 628
See Also 631

DeliverySourceConfigurationSchema 632
Contents 632
See Also 633
Destination 634
Contents 634
See Also 635
DestinationConfiguration 636
Contents 636
See Also 636
Entity 637
Contents 637
See Also 638
ExportTask 639
Contents 639
See Also 641
ExportTaskExecutionInfo 642
Contents 642
See Also 642
ExportTaskStatus 643
Contents 643
See Also 643
FieldIndex 644
Contents 644
See Also 646
FieldsData 647
Contents 647
See Also 647
FilteredLogEvent 648
Contents 648
See Also 649
GetLogObjectResponseStream 650
Contents 650
See Also 650
Grok 651
Contents 651
See Also 651

GroupingIdentifier 653
Contents 653
See Also 653
Import 654
Contents 654
See Also 656
ImportBatch 657
Contents 657
See Also 657
ImportFilter 659
Contents 659
See Also 659
ImportStatistics 660
Contents 660
See Also 660
IndexPolicy 661
Contents 661
See Also 662
InputLogEvent 663
Contents 663
See Also 663
IntegrationDetails 664
Contents 664
See Also 664
IntegrationSummary 665
Contents 665
See Also 665
ListToMap 667
Contents 667
See Also 668
LiveTailSessionLogEvent 669
Contents 669
See Also 670
LiveTailSessionMetadata 671
Contents 671
See Also 671

LiveTailSessionStart 672
Contents 672
See Also 673
LiveTailSessionUpdate 675
Contents 675
See Also 675
LogEvent 676
Contents 676
See Also 676
LogFieldsListItem 677
Contents 677
See Also 677
LogFieldType 678
Contents 678
See Also 678
LogGroup 679
Contents 679
See Also 682
LogGroupField 683
Contents 683
See Also 683
LogGroupSummary 684
Contents 684
See Also 684
LogStream 686
Contents 686
See Also 688
LookupTable 689
Contents 689
See Also 690
LookupTableConfiguration 692
Contents 692
See Also 693
LowerCaseString 694
Contents 694
See Also 694

MetricFilter ... 695
Contents ... 695
See Also ... 697
MetricFilterMatchRecord ... 698
Contents ... 698
See Also ... 698
MetricTransformation ... 699
Contents ... 699
See Also ... 701
MoveKeyEntry ... 702
Contents ... 702
See Also ... 702
MoveKeys ... 704
Contents ... 704
See Also ... 704
OpenSearchApplication ... 705
Contents ... 705
See Also ... 706
OpenSearchCollection ... 707
Contents ... 707
See Also ... 707
OpenSearchDataAccessPolicy ... 709
Contents ... 709
See Also ... 709
OpenSearchDataSource ... 710
Contents ... 710
See Also ... 710
OpenSearchEncryptionPolicy ... 712
Contents ... 712
See Also ... 712
OpenSearchIntegrationDetails ... 713
Contents ... 713
See Also ... 715
OpenSearchLifecyclePolicy ... 716
Contents ... 716
See Also ... 716

OpenSearchNetworkPolicy 717
Contents 717
See Also 717
OpenSearchResourceConfig 718
Contents 718
See Also 719
OpenSearchResourceStatus 720
Contents 720
See Also 720
OpenSearchWorkspace 721
Contents 721
See Also 721
OutputLogEvent 722
Contents 722
See Also 722
ParseCloudfront 724
Contents 724
See Also 724
ParseJSON 725
Contents 725
See Also 725
ParseKeyValue 727
Contents 727
See Also 728
ParsePostgres 730
Contents 730
See Also 730
ParseRoute53 731
Contents 731
See Also 731
ParseToOCSF 732
Contents 732
See Also 733
ParseVPC 734
Contents 734
See Also 734

ParseWAF 735
Contents 735
See Also 735
PatternToken 736
Contents 736
See Also 737
Policy 738
Contents 738
See Also 738
Processor 739
Contents 739
See Also 743
QueryCompileError 744
Contents 744
See Also 744
QueryCompileErrorLocation 745
Contents 745
See Also 745
QueryDefinition 746
Contents 746
See Also 747
QueryInfo 749
Contents 749
See Also 751
QueryParameter 752
Contents 752
See Also 753
QueryStatistics 754
Contents 754
See Also 755
RecordField 756
Contents 756
See Also 756
RejectedEntityInfo 757
Contents 757
See Also 757

RejectedLogEventsInfo 758
Contents 758
See Also 758
RenameKeyEntry 759
Contents 759
See Also 759
RenameKeys 761
Contents 761
See Also 761
ResourceConfig 762
Contents 762
See Also 762
ResourcePolicy 763
Contents 763
See Also 764
ResultField 765
Contents 765
See Also 765
S3Configuration 766
Contents 766
See Also 767
S3DeliveryConfiguration 768
Contents 768
See Also 768
S3TableIntegrationSource 769
Contents 769
See Also 770
S3TablesIntegration 771
Contents 771
See Also 771
ScheduledQueryDestination 772
Contents 772
See Also 773
ScheduledQuerySummary 774
Contents 774
See Also 776

SearchedLogStream ... 777
Contents ... 777
See Also ... 777
SplitString ... 778
Contents ... 778
See Also ... 778
SplitStringEntry ... 779
Contents ... 779
See Also ... 779
StartLiveTailResponseStream ... 780
Contents ... 780
See Also ... 781
SubscriptionFilter ... 782
Contents ... 782
See Also ... 784
SubstituteString ... 785
Contents ... 785
See Also ... 785
SubstituteStringEntry ... 786
Contents ... 786
See Also ... 786
SuppressionPeriod ... 788
Contents ... 788
See Also ... 788
SyslogConfiguration ... 789
Contents ... 789
See Also ... 790
TagFilter ... 791
Contents ... 791
See Also ... 792
TransformedLogRecord ... 793
Contents ... 793
See Also ... 793
TriggerHistoryRecord ... 795
Contents ... 795
See Also ... 796

TrimString 797
Contents 797
See Also 797
TypeConverter 798
Contents 798
See Also 798
TypeConverterEntry 799
Contents 799
See Also 799
UpperCaseString 800
Contents 800
See Also 800
Common Parameters 801
Common Error Types 804

Welcome

You can use Amazon CloudWatch Logs to monitor, store, and access your log files from EC2 instances, AWS CloudTrail, and other sources. You can then retrieve the associated log data from CloudWatch Logs using the CloudWatch console. Alternatively, you can use CloudWatch Logs commands in the AWS CLI, CloudWatch Logs API, or CloudWatch Logs SDK.

For more information about CloudWatch Logs features, see the Amazon CloudWatch Logs User Guide.

You can use CloudWatch Logs to:

- **Monitor logs from EC2 instances in real time**: You can use CloudWatch Logs to monitor applications and systems using log data. For example, CloudWatch Logs can track the number of errors that occur in your application logs. Then, it can send you a notification whenever the rate of errors exceeds a threshold that you specify. CloudWatch Logs uses your log data for monitoring so no code changes are required. For example, you can monitor application logs for specific literal terms (such as "NullReferenceException"). You can also count the number of occurrences of a literal term at a particular position in log data (such as "404" status codes in an Apache access log). When the term you are searching for is found, CloudWatch Logs reports the data to a CloudWatch metric that you specify.
- **Monitor AWS CloudTrail logged events**: You can create alarms in CloudWatch and receive notifications of particular API activity as captured by CloudTrail. You can use the notification to perform troubleshooting.
- **Archive log data**: You can use CloudWatch Logs to store your log data in highly durable storage. You can change the log retention setting so that any log events earlier than this setting are automatically deleted. The CloudWatch Logs agent helps to quickly send both rotated and non-rotated log data off of a host and into the log service. You can then access the raw log data when you need it.

> **Note**
>
> CloudWatch Logs might log request contents for fields that aren't considered sensitive, such as API request parameters for CloudWatch Logs actions. This provides debugging information for failed API requests.

This document was last published on September 18, 2026.

Actions

The following actions are supported:

- AssociateKmsKey
- AssociateSourceToS3TableIntegration
- CancelExportTask
- CancelImportTask
- CreateDelivery
- CreateExportTask
- CreateImportTask
- CreateLogAnomalyDetector
- CreateLogGroup
- CreateLogStream
- CreateLookupTable
- CreateScheduledQuery
- DeleteAccountPolicy
- DeleteDataProtectionPolicy
- DeleteDelivery
- DeleteDeliveryDestination
- DeleteDeliveryDestinationPolicy
- DeleteDeliverySource
- DeleteDestination
- DeleteIndexPolicy
- DeleteIntegration
- DeleteLogAnomalyDetector
- DeleteLogGroup
- DeleteLogStream
- DeleteLookupTable
- DeleteMetricFilter
- DeleteQueryDefinition

- DeleteResourcePolicy
- DeleteRetentionPolicy
- DeleteScheduledQuery
- DeleteSubscriptionFilter
- DeleteSyslogConfiguration
- DeleteTransformer
- DescribeAccountPolicies
- DescribeConfigurationTemplates
- DescribeDeliveries
- DescribeDeliveryDestinations
- DescribeDeliverySources
- DescribeDestinations
- DescribeExportTasks
- DescribeFieldIndexes
- DescribeImportTaskBatches
- DescribeImportTasks
- DescribeIndexPolicies
- DescribeLogGroups
- DescribeLogStreams
- DescribeLookupTables
- DescribeMetricFilters
- DescribeQueries
- DescribeQueryDefinitions
- DescribeResourcePolicies
- DescribeSubscriptionFilters
- DisassociateKmsKey
- DisassociateSourceFromS3TableIntegration
- FilterLogEvents
- GetDataProtectionPolicy
- GetDelivery

- GetDeliveryDestination
- GetDeliveryDestinationPolicy
- GetDeliverySource
- GetIntegration
- GetLogAnomalyDetector
- GetLogEvents
- GetLogFields
- GetLogGroupFields
- GetLogObject
- GetLogRecord
- GetLookupTable
- GetQueryResults
- GetScheduledQuery
- GetScheduledQueryHistory
- GetStorageTierPolicy
- GetTransformer
- ListAggregateLogGroupSummaries
- ListAnomalies
- ListIntegrations
- ListLogAnomalyDetectors
- ListLogGroups
- ListLogGroupsForQuery
- ListScheduledQueries
- ListSourcesForS3TableIntegration
- ListSyslogConfigurations
- ListTagsForResource
- ListTagsLogGroup
- PutAccountPolicy
- PutBearerTokenAuthentication
- PutDataProtectionPolicy

- PutDeliveryDestination
- PutDeliveryDestinationPolicy
- PutDeliverySource
- PutDestination
- PutDestinationPolicy
- PutIndexPolicy
- PutIntegration
- PutLogEvents
- PutLogGroupDeletionProtection
- PutMetricFilter
- PutQueryDefinition
- PutResourcePolicy
- PutRetentionPolicy
- PutStorageTierPolicy
- PutSubscriptionFilter
- PutSyslogConfiguration
- PutTransformer
- StartLiveTail
- StartQuery
- StopQuery
- TagLogGroup
- TagResource
- TestMetricFilter
- TestTransformer
- UntagLogGroup
- UntagResource
- UpdateAnomaly
- UpdateDeliveryConfiguration
- UpdateLogAnomalyDetector
- UpdateLookupTable

- UpdateScheduledQuery

AssociateKmsKey

Associates the specified AWS KMS key with either one log group in the account, or with all stored CloudWatch Logs query insights results in the account.

When you use `AssociateKmsKey`, you specify either the `logGroupName` parameter or the `resourceIdentifier` parameter. You can't specify both of those parameters in the same operation.

- Specify the `logGroupName` parameter to cause log events ingested into that log group to be encrypted with that key. Only the log events ingested after the key is associated are encrypted with that key.

  Associating a KMS key with a log group overrides any existing associations between the log group and a KMS key. After a KMS key is associated with a log group, all newly ingested data for the log group is encrypted using the KMS key. This association is stored as long as the data encrypted with the KMS key is still within CloudWatch Logs. This enables CloudWatch Logs to decrypt this data whenever it is requested.

  Associating a key with a log group does not cause the results of queries of that log group to be encrypted with that key. To have query results encrypted with a AWS KMS key, you must use an `AssociateKmsKey` operation with the `resourceIdentifier` parameter that specifies a `query-result` resource.
- Specify the `resourceIdentifier` parameter with a `query-result` resource, to use that key to encrypt the stored results of all future StartQuery operations in the account. The response from a GetQueryResults operation will still return the query results in plain text.

  Even if you have not associated a key with your query results, the query results are encrypted when stored, using the default CloudWatch Logs method.

  If you run a query from a monitoring account that queries logs in a source account, the query results key from the monitoring account, if any, is used.

Important

If you delete the key that is used to encrypt log events or log group query results, then all the associated stored log events or query results that were encrypted with that key will be unencryptable and unusable.

Note

CloudWatch Logs supports only symmetric KMS keys. Do not associate an asymmetric KMS key with your log group or query results. For more information, see Using Symmetric and Asymmetric Keys.

It can take up to 5 minutes for this operation to take effect.

If you attempt to associate a KMS key with a log group but the KMS key does not exist or the KMS key is disabled, you receive an `InvalidParameterException` error.

Request Syntax

```
{
   "kmsKeyId": "string",
   "logGroupName": "string",
   "resourceIdentifier": "string"
}
```

Request Parameters

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

The request accepts the following data in JSON format.

kmsKeyId

The Amazon Resource Name (ARN) of the KMS key to use when encrypting log data. This must be a symmetric KMS key. For more information, see Amazon Resource Names and Using Symmetric and Asymmetric Keys.

Type: String

Length Constraints: Maximum length of 256.

Required: Yes

logGroupName

The name of the log group.

In your `AssociateKmsKey` operation, you must specify either the `resourceIdentifier` parameter or the `logGroup` parameter, but you can't specify both.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `[\.\-_/#A-Za-z0-9]+`

Required: No

resourceIdentifier

Specifies the target for this operation. You must specify one of the following:

- Specify the following ARN to have future GetQueryResults operations in this account encrypt the results with the specified AWS KMS key. Replace *REGION* and *ACCOUNT_ID* with your Region and account ID.

  `arn:aws:logs:REGION:ACCOUNT_ID:query-result:*`
- Specify the ARN of a log group to have CloudWatch Logs use the AWS KMS key to encrypt log events that are ingested and stored by that log group. The log group ARN must be in the following format. Replace *REGION* and *ACCOUNT_ID* with your Region and account ID.

  `arn:aws:logs:REGION:ACCOUNT_ID:log-group:LOG_GROUP_NAME`

In your `AssociateKmsKey` operation, you must specify either the `resourceIdentifier` parameter or the `logGroup` parameter, but you can't specify both.

Type: String

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

Pattern: `[\w+=/:,.@\-\*]*`

Required: No

Response Elements

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

Errors

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

InvalidParameterException

A parameter is specified incorrectly.

HTTP Status Code: 400

OperationAbortedException

Multiple concurrent requests to update the same resource were in conflict.

HTTP Status Code: 400

ResourceNotFoundException

The specified resource does not exist.

HTTP Status Code: 400

ServiceUnavailableException

The service cannot complete the request.

HTTP Status Code: 500

Examples

To associate a log group with aKMS key

The following example associates the specified log group with the specified KMS key.

Sample Request

```
POST / HTTP/1.1
Host: logs.<region>.<domain>
X-Amz-Date: <DATE>
```

```
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=content-
type;date;host;user-agent;x-amz-date;x-amz-target;x-amzn-requestid,
 Signature=<Signature>
User-Agent: <UserAgentString>
Accept: application/json
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Connection: Keep-Alive
X-Amz-Target: Logs_20140328.AssociateKmsKey
{
  "logGroupName": "my-log-group",
  "kmsKeyId": "arn:aws:kms:us-east-1:123456789012:key/abcd1234-a123-456a-a12b-
a123b456c789"
}
```

Sample Response

```
HTTP/1.1 200 OK
x-amzn-RequestId: <RequestId>
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Date: <Date>
```

To associate all future query results in this account with aKMS key

The following example associates all future CloudWatch Logs Insights query results with the specified KMS key.

Sample Request

```
POST / HTTP/1.1
Host: logs.<region>.<domain>
X-Amz-Date: <DATE>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=content-
type;date;host;user-agent;x-amz-date;x-amz-target;x-amzn-requestid,
 Signature=<Signature>
User-Agent: <UserAgentString>
Accept: application/json
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Connection: Keep-Alive
X-Amz-Target: Logs_20140328.AssociateKmsKey
```

```
{
  "resourceIdentifier": "arn:aws:logs:us-east-1:123456789012:query-result:*",
  "kmsKeyId": "arn:aws:kms:us-east-1:123456789012:key/abcd1234-a123-456a-a12b-
a123b456c789"
}
```

Sample Response

```
HTTP/1.1 200 OK
x-amzn-RequestId: <RequestId>
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Date: <Date>
```

See Also

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

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

AssociateSourceToS3TableIntegration

Associates a data source with an S3 Table Integration for query access in the 'logs' namespace. This enables querying log data using analytics engines that support Iceberg such as Amazon Athena, Amazon Redshift, and Apache Spark.

Request Syntax

```
{
   "dataSource": {
      "name": "string",
      "type": "string"
   },
   "integrationArn": "string"
}
```

Request Parameters

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

The request accepts the following data in JSON format.

dataSource

The data source to associate with the S3 Table Integration. Contains the name and type of the data source.

Type: DataSource object

Required: Yes

integrationArn

The Amazon Resource Name (ARN) of the S3 Table Integration to associate the data source with.

Type: String

Required: Yes

Response Syntax

```
{
   "identifier": "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.

identifier

The unique identifier for the association between the data source and S3 Table Integration.

Type: String

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

Errors

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

AccessDeniedException

You don't have sufficient permissions to perform this action.

HTTP Status Code: 400

InternalServerException

An internal server error occurred while processing the request. This exception is returned when the service encounters an unexpected condition that prevents it from fulfilling the request.

HTTP Status Code: 500

ResourceNotFoundException

The specified resource does not exist.

HTTP Status Code: 400

ThrottlingException

The request was throttled because of quota limits.

HTTP Status Code: 400

ValidationException

One of the parameters for the request is not valid.

HTTP Status Code: 400

See Also

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

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

CancelExportTask

Cancels the specified export task.

The task must be in the PENDING or RUNNING state.

Request Syntax

```
{
   "taskId": "string"
}
```

Request Parameters

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

The request accepts the following data in JSON format.

taskId

The ID of the export task.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Required: Yes

Response Elements

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

Errors

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

InvalidOperationException

The operation is not valid on the specified resource.

HTTP Status Code: 400

InvalidParameterException

A parameter is specified incorrectly.

HTTP Status Code: 400

ResourceNotFoundException

The specified resource does not exist.

HTTP Status Code: 400

ServiceUnavailableException

The service cannot complete the request.

HTTP Status Code: 500

Examples

To cancel an export task

The following example cancels the specified task.

Sample Request

```
POST / HTTP/1.1
Host: logs.<region>.<domain>
X-Amz-Date: <DATE>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=content-
type;date;host;user-agent;x-amz-date;x-amz-target;x-amzn-requestid,
 Signature=<Signature>
User-Agent: <UserAgentString>
Accept: application/json
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Connection: Keep-Alive
X-Amz-Target: Logs_20140328.CancelExportTask
{
  "taskId": "exampleTaskId"
}
```

Sample Response

```
HTTP/1.1 200 OK
x-amzn-RequestId: <RequestId>
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Date: <Date>
```

See Also

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

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

CancelImportTask

Cancels an active import task and stops importing data from the CloudTrail Lake Event Data Store.

Request Syntax

```
{
   "importId": "string"
}
```

Request Parameters

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

The request accepts the following data in JSON format.

importId

The ID of the import task to cancel.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

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

Required: Yes

Response Syntax

```
{
   "creationTime": number,
   "importId": "string",
   "importStatistics": {
      "bytesImported": number
   },
   "importStatus": "string",
   "lastUpdatedTime": 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.

creationTime

The timestamp when the import task was created, expressed as the number of milliseconds after Jan 1, 1970 00:00:00 UTC.

Type: Long

Valid Range: Minimum value of 0.

importId

The ID of the cancelled import task.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

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

importStatistics

Statistics about the import progress at the time of cancellation.

Type: ImportStatistics object

importStatus

The final status of the import task. This will be set to CANCELLED.

Type: String

Valid Values: `IN_PROGRESS | CANCELLED | COMPLETED | FAILED`

lastUpdatedTime

The timestamp when the import task was cancelled, expressed as the number of milliseconds after Jan 1, 1970 00:00:00 UTC.

Type: Long

Valid Range: Minimum value of 0.

Errors

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

AccessDeniedException

You don't have sufficient permissions to perform this action.

HTTP Status Code: 400

InvalidOperationException

The operation is not valid on the specified resource.

HTTP Status Code: 400

InvalidParameterException

A parameter is specified incorrectly.

HTTP Status Code: 400

ResourceNotFoundException

The specified resource does not exist.

HTTP Status Code: 400

ThrottlingException

The request was throttled because of quota limits.

HTTP Status Code: 400

Examples

To cancel an import task

The following example cancels an active import task and returns the final status.

Sample Request

```
POST / HTTP/1.1
          Host: logs.<region>.<domain>
```

```
          X-Amz-Target: Logs_20140328.CancelImportTask
          {
          "importId": "a1b2c3d4-e5f6-7890-abcd-ef1234567890"
          }
```

Sample Response

```
HTTP/1.1 200 OK
          {
          "importId": "a1b2c3d4-e5f6-7890-abcd-ef1234567890",
          "importStatistics": {
          "bytesImported": 524288
          },
          "importStatus": "CANCELLED",
          "creationTime": 1641168000000,
          "lastUpdatedTime": 1641175200000
          }
```

See Also

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

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

CreateDelivery

Creates a *delivery*. A delivery is a connection between a logical *delivery source* and a logical *delivery destination* that you have already created.

Only some AWS services support being configured as a delivery source using this operation. These services are listed as **Supported [V2 Permissions]** in the table at Enabling logging from AWS services.

A delivery destination can represent a log group in CloudWatch Logs, an Amazon S3 bucket, a delivery stream in Firehose, or X-Ray.

To configure logs delivery between a supported AWS service and a destination, you must do the following:

- Create a delivery source, which is a logical object that represents the resource that is actually sending the logs. For more information, see PutDeliverySource.
- Create a *delivery destination*, which is a logical object that represents the actual delivery destination. For more information, see PutDeliveryDestination.
- If you are delivering logs cross-account, you must use PutDeliveryDestinationPolicy in the destination account to assign an IAM policy to the destination. This policy allows delivery to that destination.
- Use `CreateDelivery` to create a *delivery* by pairing exactly one delivery source and one delivery destination.

You can configure a single delivery source to send logs to multiple destinations by creating multiple deliveries. You can also create multiple deliveries to configure multiple delivery sources to send logs to the same delivery destination.

To update an existing delivery configuration, use UpdateDeliveryConfiguration.

Request Syntax

```
{
   "deliveryDestinationArn": "string",
   "deliverySourceName": "string",
   "fieldDelimiter": "string",
   "recordFields": [ "string" ],
```

```
   "s3DeliveryConfiguration": {
      "enableHiveCompatiblePath": boolean,
      "suffixPath": "string"
   },
   "tags": {
      "string" : "string"
   }
}
```

Request Parameters

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

The request accepts the following data in JSON format.

deliveryDestinationArn

The ARN of the delivery destination to use for this delivery.

Type: String

Required: Yes

deliverySourceName

The name of the delivery source to use for this delivery.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 60.

Pattern: `[\w-]*`

Required: Yes

fieldDelimiter

The field delimiter to use between record fields when the final output format of a delivery is in `Plain`, `W3C`, or `Raw` format.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 5.

Required: No

recordFields

The list of record fields to be delivered to the destination, in order. If the delivery's log source has mandatory fields, they must be included in this list.

Type: Array of strings

Array Members: Minimum number of 0 items. Maximum number of 128 items.

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

Required: No

s3DeliveryConfiguration

This structure contains parameters that are valid only when the delivery's delivery destination is an S3 bucket.

Type: S3DeliveryConfiguration object

Required: No

tags

An optional list of key-value pairs to associate with the resource.

For more information about tagging, see Tagging AWS resources

Type: String to string map

Map Entries: Maximum number of 50 items.

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

Key Pattern: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]+)$`

Value Length Constraints: Maximum length of 256.

Value Pattern: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$`

Required: No

Response Syntax

```
{
```

```
   "delivery": {
      "arn": "string",
      "deliveryDestinationArn": "string",
      "deliveryDestinationType": "string",
      "deliverySourceName": "string",
      "fieldDelimiter": "string",
      "id": "string",
      "recordFields": [ "string" ],
      "s3DeliveryConfiguration": {
         "enableHiveCompatiblePath": boolean,
         "suffixPath": "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.

delivery

A structure that contains information about the delivery that you just created.

Type: Delivery object

Errors

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

AccessDeniedException

You don't have sufficient permissions to perform this action.

HTTP Status Code: 400

ConflictException

This operation attempted to create a resource that already exists.

HTTP Status Code: 400

ResourceNotFoundException

The specified resource does not exist.

HTTP Status Code: 400

ServiceQuotaExceededException

This request exceeds a service quota.

HTTP Status Code: 400

ServiceUnavailableException

The service cannot complete the request.

HTTP Status Code: 500

ThrottlingException

The request was throttled because of quota limits.

HTTP Status Code: 400

ValidationException

One of the parameters for the request is not valid.

HTTP Status Code: 400

See Also

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

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3

- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

CreateExportTask

Creates an export task so that you can efficiently export data from a log group to an Amazon S3 bucket. When you perform a `CreateExportTask` operation, you must use credentials that have permission to write to the S3 bucket that you specify as the destination.

Exporting log data to S3 buckets that are encrypted by AWS KMS is supported. Exporting log data to Amazon S3 buckets that have S3 Object Lock enabled with a retention period is also supported.

Exporting to S3 buckets that are encrypted with AES-256 is supported.

This is an asynchronous call. If all the required information is provided, this operation initiates an export task and responds with the ID of the task. After the task has started, you can use DescribeExportTasks to get the status of the export task. Each account can only have one active (`RUNNING` or `PENDING`) export task at a time. To cancel an export task, use CancelExportTask.

You can export logs from multiple log groups or multiple time ranges to the same S3 bucket. To separate log data for each export task, specify a prefix to be used as the Amazon S3 key prefix for all exported objects.

Note

We recommend that you don't regularly export to Amazon S3 as a way to continuously archive your logs. For that use case, we instead recommend that you use subscriptions. For more information about subscriptions, see Real-time processing of log data with subscriptions.

Note

Time-based sorting on chunks of log data inside an exported file is not guaranteed. You can sort the exported log field data by using Linux utilities.

Request Syntax

```
{
   "destination": "string",
```

```
    "destinationPrefix": "string",
    "from": number,
    "logGroupName": "string",
    "logStreamNamePrefix": "string",
    "taskName": "string",
    "to": number
}
```

Request Parameters

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

The request accepts the following data in JSON format.

destination

The name of S3 bucket for the exported log data. The bucket must be in the same AWS Region.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Required: Yes

destinationPrefix

The prefix used as the start of the key for every object exported. If you don't specify a value, the default is `exportedlogs`.

The length of this parameter must comply with the S3 object key name length limits. The object key name is a sequence of Unicode characters with UTF-8 encoding, and can be up to 1,024 bytes.

Type: String

Required: No

from

The start time of the range for the request, expressed as the number of milliseconds after `Jan 1, 1970 00:00:00` UTC. Events with a timestamp earlier than this time are not exported.

Type: Long

Valid Range: Minimum value of 0.

Required: Yes

logGroupName

The name of the log group.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `[\.\-_/#A-Za-z0-9]+`

Required: Yes

logStreamNamePrefix

Export only log streams that match the provided prefix. If you don't specify a value, no prefix filter is applied.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `[^:*]*`

Required: No

taskName

The name of the export task.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Required: No

to

The end time of the range for the request, expressed as the number of milliseconds after `Jan 1, 1970 00:00:00` UTC. Events with a timestamp later than this time are not exported.

You must specify a time that is not earlier than when this log group was created.

Type: Long

Valid Range: Minimum value of 0.

Required: Yes

Response Syntax

```
{
   "taskId": "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.

taskId

The ID of the export task.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Errors

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

InvalidParameterException

A parameter is specified incorrectly.

HTTP Status Code: 400

LimitExceededException

You have reached the maximum number of resources that can be created.

HTTP Status Code: 400

OperationAbortedException

Multiple concurrent requests to update the same resource were in conflict.

HTTP Status Code: 400

ResourceAlreadyExistsException

The specified resource already exists.

HTTP Status Code: 400

ResourceNotFoundException

The specified resource does not exist.

HTTP Status Code: 400

ServiceUnavailableException

The service cannot complete the request.

HTTP Status Code: 500

Examples

To create an export task

The following example creates an export task that exports data from a log group to an S3 bucket.

Sample Request

```
POST / HTTP/1.1
Host: logs.<region>.<domain>
X-Amz-Date: <DATE>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=content-
type;date;host;user-agent;x-amz-date;x-amz-target;x-amzn-requestid,
 Signature=<Signature>
User-Agent: <UserAgentString>
Accept: application/json
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Connection: Keep-Alive
X-Amz-Target: Logs_20140328.CreateExportTask
```

```
{
  "taskName": "my-task",
  "logGroupName": "my-log-group",
  "from": 1437584472382,
  "to": 1437584472833,
  "destination": "my-destination",
  "destinationPrefix": "my-prefix"
}
```

Sample Response

```
HTTP/1.1 200 OK
x-amzn-RequestId: <RequestId>
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Date: <Date>
{
  "taskId": "exampleTaskId"
}
```

See Also

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

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

CreateImportTask

Starts an import from a data source to CloudWatch Log and creates a managed log group as the destination for the imported data. Currently, CloudTrail Event Data Store is the only supported data source.

The import task must satisfy the following constraints:

- The specified source must be in an ACTIVE state.
- The API caller must have permissions to access the data in the provided source and to perform iam:PassRole on the provided import role which has the same permissions, as described below.
- The provided IAM role must trust the "cloudtrail.amazonaws.com" principal and have the following permissions:
  - cloudtrail:GetEventDataStoreData
  - logs:CreateLogGroup
  - logs:CreateLogStream
  - logs:PutResourcePolicy
  - (If source has an associated AWS KMS Key) kms:Decrypt
  - (If source has an associated AWS KMS Key) kms:GenerateDataKey

  Example IAM policy for provided import role:

```
[ { "Effect": "Allow", "Action": "iam:PassRole", "Resource":
"arn:aws:iam::123456789012:role/apiCallerCredentials",
"Condition": { "StringLike": { "iam:AssociatedResourceARN":
"arn:aws:logs:us-east-1:123456789012:log-group:aws/cloudtrail/
f1d45bff-d0e3-4868-b5d9-2eb678aa32fb:*" } } }, { "Effect": "Allow",
"Action": [ "cloudtrail:GetEventDataStoreData" ], "Resource":
[ "arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/
f1d45bff-d0e3-4868-b5d9-2eb678aa32fb" ] }, { "Effect": "Allow",
"Action": [ "logs:CreateImportTask", "logs:CreateLogGroup",
"logs:CreateLogStream", "logs:PutResourcePolicy" ], "Resource":
[ "arn:aws:logs:us-east-1:123456789012:log-group:/aws/cloudtrail/
*" ] }, { "Effect": "Allow", "Action": [ "kms:Decrypt",
"kms:GenerateDataKey" ], "Resource": [ "arn:aws:kms:us-
east-1:123456789012:key/12345678-1234-1234-1234-123456789012" ] } ]
```

- If the import source has a customer managed key, the "cloudtrail.amazonaws.com" principal needs permissions to perform kms:Decrypt and kms:GenerateDataKey.
- There can be no more than 3 active imports per account at a given time.
- The startEventTime must be less than or equal to endEventTime.
- The data being imported must be within the specified source's retention period.

Request Syntax

```
{
   "importFilter": {
      "endEventTime": number,
      "startEventTime": number
   },
   "importRoleArn": "string",
   "importSourceArn": "string"
}
```

Request Parameters

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

The request accepts the following data in JSON format.

importFilter

Optional filters to constrain the import by CloudTrail event time. Times are specified in Unix timestamp milliseconds. The range of data being imported must be within the specified source's retention period.

Type: ImportFilter object

Required: No

importRoleArn

The ARN of the IAM role that grants CloudWatch Logs permission to import from the CloudTrail Lake Event Data Store.

Type: String

Length Constraints: Minimum length of 1.

Required: Yes

importSourceArn

The ARN of the source to import from.

Type: String

Required: Yes

Response Syntax

```
{
   "creationTime": number,
   "importDestinationArn": "string",
   "importId": "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.

creationTime

The timestamp when the import task was created, expressed as the number of milliseconds after Jan 1, 1970 00:00:00 UTC.

Type: Long

Valid Range: Minimum value of 0.

importDestinationArn

The ARN of the CloudWatch Logs log group created as the destination for the imported events.

Type: String

importId

A unique identifier for the import task.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

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

Errors

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

AccessDeniedException

You don't have sufficient permissions to perform this action.

HTTP Status Code: 400

ConflictException

This operation attempted to create a resource that already exists.

HTTP Status Code: 400

InvalidOperationException

The operation is not valid on the specified resource.

HTTP Status Code: 400

InvalidParameterException

A parameter is specified incorrectly.

HTTP Status Code: 400

ResourceNotFoundException

The specified resource does not exist.

HTTP Status Code: 400

ThrottlingException

The request was throttled because of quota limits.

HTTP Status Code: 400

ValidationException

One of the parameters for the request is not valid.

HTTP Status Code: 400

Examples

To create an import task from CloudTrail Lake to CloudWatch Logs

The following example creates an import task with time-based filters.

Sample Request

```
POST / HTTP/1.1
          Host: logs.<region>.<domain>
          X-Amz-Target: Logs_20140328.CreateImportTask
          {
          "importSourceArn": "arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/
f1d45bff-d0e3-4868-b5d9-2eb678aa32fb",
          "importRoleArn": "arn:aws:iam::123456789012:role/CloudWatchLogsImportRole",
          "importFilter": {
          "startEventTime": 1640995200000,
          "endEventTime": 1641081600000
          }
          }
```

Sample Response

```
HTTP/1.1 200 OK
          {
          "importId": "a1b2c3d4-e5f6-7890-abcd-ef1234567890",
          "importDestinationArn": "arn:aws:logs:us-east-1:123456789012:log-group:aws/
cloudtrail/f1d45bff-d0e3-4868-b5d9-2eb678aa32fb",
          "creationTime": 1641168000000
          }
```

See Also

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

- AWS Command Line Interface V2
- AWS SDK for .NET V4

- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

CreateLogAnomalyDetector

Creates an *anomaly detector* that regularly scans one or more log groups and look for patterns and anomalies in the logs.

An anomaly detector can help surface issues by automatically discovering anomalies in your log event traffic. An anomaly detector uses machine learning algorithms to scan log events and find *patterns*. A pattern is a shared text structure that recurs among your log fields. Patterns provide a useful tool for analyzing large sets of logs because a large number of log events can often be compressed into a few patterns.

The anomaly detector uses pattern recognition to find `anomalies`, which are unusual log events. It uses the `evaluationFrequency` to compare current log events and patterns with trained baselines.

Fields within a pattern are called *tokens*. Fields that vary within a pattern, such as a request ID or timestamp, are referred to as *dynamic tokens* and represented by `<*>`.

The following is an example of a pattern:

```
[INFO] Request time: <*> ms
```

This pattern represents log events like `[INFO] Request time: 327 ms` and other similar log events that differ only by the number, in this csse 327. When the pattern is displayed, the different numbers are replaced by `<*>`

> **Note**
>
> Any parts of log events that are masked as sensitive data are not scanned for anomalies. For more information about masking sensitive data, see Help protect sensitive log data with masking.

Request Syntax

```
{
   "anomalyVisibilityTime": number,
   "detectorName": "string",
   "evaluationFrequency": "string",
   "filterPattern": "string",
```

```
   "kmsKeyId": "string",
   "logGroupArnList": [ "string" ],
   "tags": {
      "string" : "string"
   }
}
```

Request Parameters

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

The request accepts the following data in JSON format.

anomalyVisibilityTime

The number of days to have visibility on an anomaly. After this time period has elapsed for an anomaly, it will be automatically baselined and the anomaly detector will treat new occurrences of a similar anomaly as normal. Therefore, if you do not correct the cause of an anomaly during the time period specified in `anomalyVisibilityTime`, it will be considered normal going forward and will not be detected as an anomaly.

Type: Long

Valid Range: Minimum value of 7. Maximum value of 90.

Required: No

detectorName

A name for this anomaly detector.

Type: String

Length Constraints: Minimum length of 1.

Required: No

evaluationFrequency

Specifies how often the anomaly detector is to run and look for anomalies. Set this value according to the frequency that the log group receives new logs. For example, if the log group receives new log events every 10 minutes, then 15 minutes might be a good setting for `evaluationFrequency` .

Type: String

Valid Values: `ONE_MIN | FIVE_MIN | TEN_MIN | FIFTEEN_MIN | THIRTY_MIN | ONE_HOUR`

Required: No

filterPattern

You can use this parameter to limit the anomaly detection model to examine only log events that match the pattern you specify here. For more information, see Filter and Pattern Syntax.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 1024.

Required: No

kmsKeyId

Optionally assigns a AWS KMS key to secure this anomaly detector and its findings. If a key is assigned, the anomalies found and the model used by this detector are encrypted at rest with the key. If a key is assigned to an anomaly detector, a user must have permissions for both this key and for the anomaly detector to retrieve information about the anomalies that it finds.

Make sure the value provided is a valid AWS KMS key ARN. For more information about using a AWS KMS key and to see the required IAM policy, see Use a AWS KMS key with an anomaly detector.

Type: String

Length Constraints: Maximum length of 256.

Pattern: `^arn:aws[a-z\-]*:kms:[-a-z0-9]*:[0-9]*:key/[-a-z0-9]*$`

Required: No

logGroupArnList

An array containing the ARN of the log group that this anomaly detector will watch. You can specify only one log group ARN.

Type: Array of strings

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

Pattern: `[\w#+=/:,.@-]*`

Required: Yes

tags

An optional list of key-value pairs to associate with the resource.

For more information about tagging, see Tagging AWS resources

Type: String to string map

Map Entries: Maximum number of 50 items.

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

Key Pattern: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]+)$`

Value Length Constraints: Maximum length of 256.

Value Pattern: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$`

Required: No

Response Syntax

```
{
   "anomalyDetectorArn": "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.

anomalyDetectorArn

The ARN of the log anomaly detector that you just created.

Type: String

Length Constraints: Minimum length of 1.

Pattern: `[\w#+=/:,.@-]*`

Errors

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

InvalidParameterException

A parameter is specified incorrectly.

HTTP Status Code: 400

LimitExceededException

You have reached the maximum number of resources that can be created.

HTTP Status Code: 400

OperationAbortedException

Multiple concurrent requests to update the same resource were in conflict.

HTTP Status Code: 400

ResourceNotFoundException

The specified resource does not exist.

HTTP Status Code: 400

ServiceUnavailableException

The service cannot complete the request.

HTTP Status Code: 500

See Also

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

- AWS Command Line Interface V2
- AWS SDK for .NET V4

- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

CreateLogGroup

Creates a log group with the specified name. You can create up to 1,000,000 log groups per Region per account.

You must use the following guidelines when naming a log group:

- Log group names must be unique within a Region for an AWS account.
- Log group names can be between 1 and 512 characters long.
- Log group names consist of the following characters: a-z, A-Z, 0-9, '_' (underscore), '-' (hyphen), '/' (forward slash), '.' (period), and '#' (number sign)
- Log group names can't start with the string `aws/`

When you create a log group, by default the log events in the log group do not expire. To set a retention policy so that events expire and are deleted after a specified time, use PutRetentionPolicy.

If you associate an AWS KMS key with the log group, ingested data is encrypted using the KMS key. This association is stored as long as the data encrypted with the KMS key is still within CloudWatch Logs. This enables CloudWatch Logs to decrypt this data whenever it is requested.

If you attempt to associate a KMS key with the log group but the KMS key does not exist or the KMS key is disabled, you receive an `InvalidParameterException` error.

> **Important**
>
> CloudWatch Logs supports only symmetric KMS keys. Do not associate an asymmetric KMS key with your log group. For more information, see Using Symmetric and Asymmetric Keys.

Request Syntax

```
{
   "deletionProtectionEnabled": boolean,
   "kmsKeyId": "string",
   "logGroupClass": "string",
   "logGroupName": "string",
   "tags": {
```

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

Request Parameters

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

The request accepts the following data in JSON format.

deletionProtectionEnabled

Use this parameter to enable deletion protection for the new log group. When enabled on a log group, deletion protection blocks all deletion operations until it is explicitly disabled. By default log groups are created without deletion protection enabled.

Type: Boolean

Required: No

kmsKeyId

The Amazon Resource Name (ARN) of the KMS key to use when encrypting log data. For more information, see Amazon Resource Names.

Type: String

Length Constraints: Maximum length of 256.

Required: No

logGroupClass

Use this parameter to specify the log group class for this log group. There are three classes:

- The `Standard` log class supports all CloudWatch Logs features.
- The `Infrequent Access` log class supports a subset of CloudWatch Logs features and incurs lower costs.
- Use the `Delivery` log class only for delivering AWS Lambda logs to store in Amazon S3 or Amazon Data Firehose. Log events in log groups in the Delivery class are kept in CloudWatch Logs for only one day. This log class doesn't offer rich CloudWatch Logs capabilities such as CloudWatch Logs Insights queries.

If you omit this parameter, the default of `STANDARD` is used.

> **Important**
>
> The value of `logGroupClass` can't be changed after a log group is created.

For details about the features supported by each class, see Log classes

Type: String

Valid Values: `STANDARD | INFREQUENT_ACCESS | DELIVERY`

Required: No

logGroupName

A name for the log group.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `[\.\-_/#A-Za-z0-9]+`

Required: Yes

tags

The key-value pairs to use for the tags.

You can grant users access to certain log groups while preventing them from accessing other log groups. To do so, tag your groups and use IAM policies that refer to those tags. To assign tags when you create a log group, you must have either the `logs:TagResource` or `logs:TagLogGroup` permission. For more information about tagging, see Tagging AWS resources. For more information about using tags to control access, see Controlling access to Amazon Web Services resources using tags.

Type: String to string map

Map Entries: Maximum number of 50 items.

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

Key Pattern: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]+)$`

Value Length Constraints: Maximum length of 256.

Value Pattern: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$`

Required: No

Response Elements

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

Errors

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

InvalidParameterException

A parameter is specified incorrectly.

HTTP Status Code: 400

LimitExceededException

You have reached the maximum number of resources that can be created.

HTTP Status Code: 400

OperationAbortedException

Multiple concurrent requests to update the same resource were in conflict.

HTTP Status Code: 400

ResourceAlreadyExistsException

The specified resource already exists.

HTTP Status Code: 400

ServiceUnavailableException

The service cannot complete the request.

HTTP Status Code: 500

Examples

To create a log group

The following example creates a log group.

Sample Request

```
POST / HTTP/1.1
Host: logs.<region>.<domain>
X-Amz-Date: <DATE>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=content-
type;date;host;user-agent;x-amz-date;x-amz-target;x-amzn-requestid,
 Signature=<Signature>
User-Agent: <UserAgentString>
Accept: application/json
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Connection: Keep-Alive
X-Amz-Target: Logs_20140328.CreateLogGroup
{
  "logGroupName": "my-log-group",
  "kmsKeyId": "arn:aws:kms:us-east-1:123456789012:key/abcd1234-a123-456a-a12b-
a123b456c789"
}
```

Sample Response

```
HTTP/1.1 200 OK
x-amzn-RequestId: <RequestId>
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Date: <Date>
```

See Also

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

- AWS Command Line Interface V2
- AWS SDK for .NET V4

- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

CreateLogStream

Creates a log stream for the specified log group. A log stream is a sequence of log events that originate from a single source, such as an application instance or a resource that is being monitored.

There is no limit on the number of log streams that you can create for a log group. There is a limit of 50 TPS on `CreateLogStream` operations, after which transactions are throttled.

You must use the following guidelines when naming a log stream:

- Log stream names must be unique within the log group.
- Log stream names can be between 1 and 512 characters long.
- Don't use ':' (colon) or '*' (asterisk) characters.

Request Syntax

```
{
   "logGroupName": "string",
   "logStreamName": "string"
}
```

Request Parameters

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

The request accepts the following data in JSON format.

logGroupName

The name of the log group.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `[\.\-_/#A-Za-z0-9]+`

Required: Yes

logStreamName

The name of the log stream.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `[^:*]*`

Required: Yes

Response Elements

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

Errors

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

InvalidParameterException

A parameter is specified incorrectly.

HTTP Status Code: 400

ResourceAlreadyExistsException

The specified resource already exists.

HTTP Status Code: 400

ResourceNotFoundException

The specified resource does not exist.

HTTP Status Code: 400

ServiceUnavailableException

The service cannot complete the request.

HTTP Status Code: 500

Examples

To create a log stream

The following example creates a log stream for the specified log group.

Sample Request

```
POST / HTTP/1.1
Host: logs.<region>.<domain>
X-Amz-Date: <DATE>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=content-
type;date;host;user-agent;x-amz-date;x-amz-target;x-amzn-requestid,
 Signature=<Signature>
User-Agent: <UserAgentString>
Accept: application/json
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Connection: Keep-Alive
X-Amz-Target: Logs_20140328.CreateLogStream
{
  "logGroupName": "my-log-group",
  "logStreamName": "my-log-stream"
}
```

Sample Response

```
HTTP/1.1 200 OK
x-amzn-RequestId: <RequestId>
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Date: <Date>
```

See Also

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

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++

- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

CreateLookupTable

Creates a lookup table by uploading CSV data or from CloudWatch Logs query results. You can use lookup tables to enrich log data in CloudWatch Logs queries with reference data such as user details, application names, or error descriptions.

The table name must be unique within your account and Region. You must specify either `tableBody` or `queryId`, but not both. If you use `tableBody`, the CSV content must include a header row with column names, use UTF-8 encoding, and not exceed 10 MB.

Request Syntax

```
{
   "description": "string",
   "kmsKeyId": "string",
   "lookupTableName": "string",
   "queryId": "string",
   "tableBody": "string",
   "tags": {
      "string" : "string"
   }
}
```

Request Parameters

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

The request accepts the following data in JSON format.

description

A description of the lookup table. The description can be up to 1024 characters long.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 1024.

Required: No

kmsKeyId

The ARN of the AWS KMS key to use to encrypt the lookup table data. If you don't specify a key, the data is encrypted with an AWS-owned key.

Type: String

Length Constraints: Maximum length of 256.

Required: No

lookupTableName

The name of the lookup table. The name must be unique within your account and Region. The name can contain only alphanumeric characters and underscores, and can be up to 256 characters long.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `^[a-zA-Z0-9_]+$`

Required: Yes

queryId

The ID of a completed or cancelled CloudWatch Logs query whose results populate the lookup table. A cancelled query populates the table with the partial results that were available when the query was stopped.

You must specify either `tableBody` or `queryId`, but not both.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Required: No

tableBody

The CSV content of the lookup table. The first row must be a header row with column names. The content must use UTF-8 encoding and not exceed 10 MB.

You must specify either `tableBody` or `queryId`, but not both.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 10485760.

Required: No

tags

A list of key-value pairs to associate with the lookup table. You can associate as many as 50 tags with a lookup table. Tags can help you organize and categorize your resources.

Type: String to string map

Map Entries: Maximum number of 50 items.

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

Key Pattern: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]+)$`

Value Length Constraints: Maximum length of 256.

Value Pattern: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$`

Required: No

Response Syntax

```
{
   "createdAt": number,
   "lookupTableArn": "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 time when the lookup table was created, expressed as the number of milliseconds after `Jan 1, 1970 00:00:00 UTC`.

Type: Long

Valid Range: Minimum value of 0.

lookupTableArn

The ARN of the lookup table that was created.

Type: String

Errors

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

AccessDeniedException

You don't have sufficient permissions to perform this action.

HTTP Status Code: 400

InvalidParameterException

A parameter is specified incorrectly.

HTTP Status Code: 400

LimitExceededException

You have reached the maximum number of resources that can be created.

HTTP Status Code: 400

ResourceAlreadyExistsException

The specified resource already exists.

HTTP Status Code: 400

ServiceUnavailableException

The service cannot complete the request.

HTTP Status Code: 500

ValidationException

One of the parameters for the request is not valid.

HTTP Status Code: 400

See Also

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

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

CreateScheduledQuery

Creates a scheduled query that runs CloudWatch Logs Insights queries at regular intervals. Scheduled queries enable proactive monitoring by automatically executing queries to detect patterns and anomalies in your log data. Query results can be delivered to Amazon S3 for analysis or further processing.

Request Syntax

```
{
   "description": "string",
   "destinationConfiguration": {
      "lookupTableConfiguration": {
         "description": "string",
         "kmsKeyId": "string",
         "roleArn": "string",
         "tableName": "string",
         "tags": {
            "string" : "string"
         }
      },
      "s3Configuration": {
         "destinationIdentifier": "string",
         "kmsKeyId": "string",
         "ownerAccountId": "string",
         "roleArn": "string"
      }
   },
   "endTimeOffset": number,
   "executionRoleArn": "string",
   "logGroupIdentifiers": [ "string" ],
   "name": "string",
   "queryLanguage": "string",
   "queryString": "string",
   "scheduleEndTime": number,
   "scheduleExpression": "string",
   "scheduleStartTime": number,
   "startTimeOffset": number,
   "state": "string",
   "tags": {
      "string" : "string"
   },
```

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

Request Parameters

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

The request accepts the following data in JSON format.

description

An optional description for the scheduled query to help identify its purpose and functionality.

Type: String

Length Constraints: Maximum length of 1024.

Required: No

destinationConfiguration

Configuration for where to deliver query results. Supports Amazon S3 destinations for storing query output and lookup table destinations for automatically refreshing lookup tables with query results. You can configure one or both destination types.

Type: DestinationConfiguration object

Required: No

endTimeOffset

The time offset in seconds that defines the end of the lookback period for the query. Together with `startTimeOffset`, this determines the time window relative to the execution time over which the query runs.

Type: Long

Required: No

executionRoleArn

The ARN of the IAM role that grants permissions to execute the query and deliver results to the specified destination. The role must have permissions to read from the specified log groups and write to the destination.

Type: String

Length Constraints: Minimum length of 1.

Required: Yes

logGroupIdentifiers

An array of log group names or ARNs to query. You can specify between 1 and 50 log groups. Log groups can be identified by name or full ARN.

Type: Array of strings

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

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

Pattern: `[\w#+=/:,.@-]*`

Required: No

name

The name of the scheduled query. The name must be unique within your account and region. Length must be between 1 and 300 characters.

Type: String

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

Required: Yes

queryLanguage

The query language to use for the scheduled query. Valid values are `CWLI`, `PPL`, and `SQL`.

Type: String

Valid Values: `CWLI | SQL | PPL`

Required: Yes

queryString

The query string to execute. This is the same query syntax used in CloudWatch Logs Insights. Maximum length is 10,000 characters.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 10000.

Required: Yes

scheduleEndTime

The end time for the scheduled query in Unix epoch format. The query will stop executing after this time.

Type: Long

Valid Range: Minimum value of 0.

Required: No

scheduleExpression

A cron expression that defines when the scheduled query runs. The expression uses standard cron syntax and supports minute-level precision. Maximum length is 256 characters.

Type: String

Length Constraints: Maximum length of 256.

Required: Yes

scheduleStartTime

The start time for the scheduled query in Unix epoch format. The query will not execute before this time.

Type: Long

Valid Range: Minimum value of 0.

Required: No

startTimeOffset

The time offset in seconds that defines the lookback period for the query. This determines how far back in time the query searches from the execution time.

Type: Long

Required: No

state

The initial state of the scheduled query. Valid values are `ENABLED` and `DISABLED`. Default is `ENABLED`.

Type: String

Valid Values: `ENABLED | DISABLED`

Required: No

tags

Key-value pairs to associate with the scheduled query for resource management and cost allocation.

Type: String to string map

Map Entries: Maximum number of 50 items.

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

Key Pattern: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]+)$`

Value Length Constraints: Maximum length of 256.

Value Pattern: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$`

Required: No

timezone

The timezone for evaluating the schedule expression. This determines when the scheduled query executes relative to the specified timezone.

Type: String

Length Constraints: Minimum length of 1.

Required: No

Response Syntax

```
{
```

```
    "scheduledQueryArn": "string",
    "state": "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.

scheduledQueryArn

The ARN of the created scheduled query.

Type: String

state

The current state of the scheduled query.

Type: String

Valid Values: `ENABLED | DISABLED`

Errors

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

AccessDeniedException

You don't have sufficient permissions to perform this action.

HTTP Status Code: 400

ConflictException

This operation attempted to create a resource that already exists.

HTTP Status Code: 400

InternalServerException

An internal server error occurred while processing the request. This exception is returned when the service encounters an unexpected condition that prevents it from fulfilling the request.

HTTP Status Code: 500

ResourceNotFoundException

The specified resource does not exist.

HTTP Status Code: 400

ServiceQuotaExceededException

This request exceeds a service quota.

HTTP Status Code: 400

ThrottlingException

The request was throttled because of quota limits.

HTTP Status Code: 400

ValidationException

One of the parameters for the request is not valid.

HTTP Status Code: 400

See Also

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

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

DeleteAccountPolicy

Deletes a CloudWatch Logs account policy. This stops the account-wide policy from applying to log groups or data sources in the account. If you delete a data protection policy or subscription filter policy, any log-group level policies of those types remain in effect. This operation supports deletion of data source-based field index policies, including facet configurations, in addition to log group-based policies.

To use this operation, you must be signed on with the correct permissions depending on the type of policy that you are deleting.

- To delete a data protection policy, you must have the `logs:DeleteDataProtectionPolicy` and `logs:DeleteAccountPolicy` permissions.
- To delete a subscription filter policy, you must have the `logs:DeleteSubscriptionFilter` and `logs:DeleteAccountPolicy` permissions.
- To delete a transformer policy, you must have the `logs:DeleteTransformer` and `logs:DeleteAccountPolicy` permissions.
- To delete a field index policy, you must have the `logs:DeleteIndexPolicy` and `logs:DeleteAccountPolicy` permissions.

  If you delete a field index policy that included facet configurations, those facets will no longer be available for interactive exploration in the CloudWatch Logs Insights console. However, facet data is retained for up to 30 days.

If you delete a field index policy, the indexing of the log events that happened before you deleted the policy will still be used for up to 30 days to improve CloudWatch Logs Insights queries.

Request Syntax

```
{
   "policyName": "string",
   "policyType": "string"
}
```

Request Parameters

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

The request accepts the following data in JSON format.

policyName

The name of the policy to delete.

Type: String

Required: Yes

policyType

The type of policy to delete.

Type: String

Valid Values: `DATA_PROTECTION_POLICY | SUBSCRIPTION_FILTER_POLICY | FIELD_INDEX_POLICY | TRANSFORMER_POLICY | METRIC_EXTRACTION_POLICY`

Required: Yes

Response Elements

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

Errors

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

InvalidParameterException

A parameter is specified incorrectly.

HTTP Status Code: 400

OperationAbortedException

Multiple concurrent requests to update the same resource were in conflict.

HTTP Status Code: 400

ResourceNotFoundException

The specified resource does not exist.

HTTP Status Code: 400

ServiceUnavailableException

The service cannot complete the request.

HTTP Status Code: 500

See Also

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

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

DeleteDataProtectionPolicy

Deletes the data protection policy from the specified log group.

For more information about data protection policies, see PutDataProtectionPolicy.

Request Syntax

```
{
   "logGroupIdentifier": "string"
}
```

Request Parameters

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

The request accepts the following data in JSON format.

logGroupIdentifier

The name or ARN of the log group that you want to delete the data protection policy for.

Type: String

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

Pattern: `[\w#+=/:,.@-]*`

Required: Yes

Response Elements

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

Errors

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

InvalidParameterException

A parameter is specified incorrectly.

HTTP Status Code: 400

OperationAbortedException

Multiple concurrent requests to update the same resource were in conflict.

HTTP Status Code: 400

ResourceNotFoundException

The specified resource does not exist.

HTTP Status Code: 400

ServiceUnavailableException

The service cannot complete the request.

HTTP Status Code: 500

See Also

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

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

DeleteDelivery

Deletes a *delivery*. A delivery is a connection between a logical *delivery source* and a logical *delivery destination*. Deleting a delivery only deletes the connection between the delivery source and delivery destination. It does not delete the delivery destination or the delivery source.

Request Syntax

```
{
   "id": "string"
}
```

Request Parameters

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

The request accepts the following data in JSON format.

id

The unique ID of the delivery to delete. You can find the ID of a delivery with the DescribeDeliveries operation.

Type: String

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

Pattern: `^[0-9A-Za-z]+$`

Required: Yes

Response Elements

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

Errors

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

ConflictException

This operation attempted to create a resource that already exists.

HTTP Status Code: 400

ResourceNotFoundException

The specified resource does not exist.

HTTP Status Code: 400

ServiceQuotaExceededException

This request exceeds a service quota.

HTTP Status Code: 400

ServiceUnavailableException

The service cannot complete the request.

HTTP Status Code: 500

ThrottlingException

The request was throttled because of quota limits.

HTTP Status Code: 400

ValidationException

One of the parameters for the request is not valid.

HTTP Status Code: 400

See Also

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

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++

- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

DeleteDeliveryDestination

Deletes a *delivery destination*. A delivery is a connection between a logical *delivery source* and a logical *delivery destination*.

You can't delete a delivery destination if any current deliveries are associated with it. To find whether any deliveries are associated with this delivery destination, use the DescribeDeliveries operation and check the `deliveryDestinationArn` field in the results.

Request Syntax

```
{
   "name": "string"
}
```

Request Parameters

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

The request accepts the following data in JSON format.

name

The name of the delivery destination that you want to delete. You can find a list of delivery destination names by using the DescribeDeliveryDestinations operation.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 60.

Pattern: `[\w-]*`

Required: Yes

Response Elements

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

Errors

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

ConflictException

This operation attempted to create a resource that already exists.

HTTP Status Code: 400

ResourceNotFoundException

The specified resource does not exist.

HTTP Status Code: 400

ServiceQuotaExceededException

This request exceeds a service quota.

HTTP Status Code: 400

ServiceUnavailableException

The service cannot complete the request.

HTTP Status Code: 500

ThrottlingException

The request was throttled because of quota limits.

HTTP Status Code: 400

ValidationException

One of the parameters for the request is not valid.

HTTP Status Code: 400

See Also

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

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++

- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

DeleteDeliveryDestinationPolicy

Deletes a delivery destination policy. For more information about these policies, see PutDeliveryDestinationPolicy.

Request Syntax

```
{
   "deliveryDestinationName": "string"
}
```

Request Parameters

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

The request accepts the following data in JSON format.

deliveryDestinationName

The name of the delivery destination that you want to delete the policy for.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 60.

Pattern: `[\w-]*`

Required: Yes

Response Elements

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

Errors

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

ConflictException

This operation attempted to create a resource that already exists.

HTTP Status Code: 400

ResourceNotFoundException

The specified resource does not exist.

HTTP Status Code: 400

ServiceUnavailableException

The service cannot complete the request.

HTTP Status Code: 500

ValidationException

One of the parameters for the request is not valid.

HTTP Status Code: 400

See Also

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

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

DeleteDeliverySource

Deletes a *delivery source*. A delivery is a connection between a logical *delivery source* and a logical *delivery destination*.

You can't delete a delivery source if any current deliveries are associated with it. To find whether any deliveries are associated with this delivery source, use the DescribeDeliveries operation and check the `deliverySourceName` field in the results.

Request Syntax

```
{
   "name": "string"
}
```

Request Parameters

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

The request accepts the following data in JSON format.

name

The name of the delivery source that you want to delete.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 60.

Pattern: `[\w-]*`

Required: Yes

Response Elements

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

Errors

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

ConflictException

This operation attempted to create a resource that already exists.

HTTP Status Code: 400

ResourceNotFoundException

The specified resource does not exist.

HTTP Status Code: 400

ServiceQuotaExceededException

This request exceeds a service quota.

HTTP Status Code: 400

ServiceUnavailableException

The service cannot complete the request.

HTTP Status Code: 500

ThrottlingException

The request was throttled because of quota limits.

HTTP Status Code: 400

ValidationException

One of the parameters for the request is not valid.

HTTP Status Code: 400

See Also

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

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++

- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

DeleteDestination

Deletes the specified destination, and eventually disables all the subscription filters that publish to it. This operation does not delete the physical resource encapsulated by the destination.

Request Syntax

```
{
   "destinationName": "string"
}
```

Request Parameters

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

The request accepts the following data in JSON format.

destinationName

The name of the destination.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `[^:*]*`

Required: Yes

Response Elements

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

Errors

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

InvalidParameterException

A parameter is specified incorrectly.

HTTP Status Code: 400

OperationAbortedException

Multiple concurrent requests to update the same resource were in conflict.

HTTP Status Code: 400

ResourceNotFoundException

The specified resource does not exist.

HTTP Status Code: 400

ServiceUnavailableException

The service cannot complete the request.

HTTP Status Code: 500

Examples

To delete a destination

The following example deletes the specified destination.

Sample Request

```
POST / HTTP/1.1
Host: logs.<region>.<domain>
X-Amz-Date: <DATE>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=content-
type;date;host;user-agent;x-amz-date;x-amz-target;x-amzn-requestid,
 Signature=<Signature>
User-Agent: <UserAgentString>
Accept: application/json
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Connection: Keep-Alive
X-Amz-Target: Logs_20140328.DeleteDestination
{
  "destinationName": my-destination"
}
```

Sample Response

```
HTTP/1.1 200 OK
x-amzn-RequestId: <RequestId>
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Date: <Date>
```

See Also

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

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

DeleteIndexPolicy

Deletes a log-group level field index policy that was applied to a single log group. The indexing of the log events that happened before you delete the policy will still be used for as many as 30 days to improve CloudWatch Logs Insights queries.

If the deleted policy included facet configurations, those facets will no longer be available for interactive exploration in the CloudWatch Logs Insights console for this log group. However, facet data is retained for up to 30 days.

You can't use this operation to delete an account-level index policy. Instead, use DeleteAccountPolicy.

If you delete a log-group level field index policy and there is an account-level field index policy, in a few minutes the log group begins using that account-wide policy to index new incoming log events. This operation only affects log group-level policies, including any facet configurations, and preserves any data source-based account policies that may apply to the log group.

Request Syntax

```
{
   "logGroupIdentifier": "string"
}
```

Request Parameters

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

The request accepts the following data in JSON format.

logGroupIdentifier

The log group to delete the index policy for. You can specify either the name or the ARN of the log group.

Type: String

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

Pattern: `[\w#+=/:,.@-]*`

Required: Yes

Response Elements

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

Errors

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

InvalidParameterException

A parameter is specified incorrectly.

HTTP Status Code: 400

LimitExceededException

You have reached the maximum number of resources that can be created.

HTTP Status Code: 400

OperationAbortedException

Multiple concurrent requests to update the same resource were in conflict.

HTTP Status Code: 400

ResourceNotFoundException

The specified resource does not exist.

HTTP Status Code: 400

ServiceUnavailableException

The service cannot complete the request.

HTTP Status Code: 500

See Also

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

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

DeleteIntegration

Deletes the integration between CloudWatch Logs and OpenSearch Service. If your integration has active vended logs dashboards, you must specify `true` for the `force` parameter, otherwise the operation will fail. If you delete the integration by setting `force` to `true`, all your vended logs dashboards powered by OpenSearch Service will be deleted and the data that was on them will no longer be accessible.

Request Syntax

```
{
   "force": boolean,
   "integrationName": "string"
}
```

Request Parameters

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

The request accepts the following data in JSON format.

force

Specify `true` to force the deletion of the integration even if vended logs dashboards currently exist.

The default is `false`.

Type: Boolean

Required: No

integrationName

The name of the integration to delete. To find the name of your integration, use ListIntegrations.

Type: String

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

Pattern: `[\.\-_/#A-Za-z0-9]+`

Required: Yes

Response Elements

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

Errors

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

InvalidParameterException

A parameter is specified incorrectly.

HTTP Status Code: 400

ResourceNotFoundException

The specified resource does not exist.

HTTP Status Code: 400

ServiceUnavailableException

The service cannot complete the request.

HTTP Status Code: 500

ValidationException

One of the parameters for the request is not valid.

HTTP Status Code: 400

See Also

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

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++

- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

DeleteLogAnomalyDetector

Deletes the specified CloudWatch Logs anomaly detector.

Request Syntax

```
{
   "anomalyDetectorArn": "string"
}
```

Request Parameters

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

The request accepts the following data in JSON format.

anomalyDetectorArn

The ARN of the anomaly detector to delete. You can find the ARNs of log anomaly detectors in your account by using the ListLogAnomalyDetectors operation.

Type: String

Length Constraints: Minimum length of 1.

Pattern: `[\w#+=/:,.@-]*`

Required: Yes

Response Elements

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

Errors

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

InvalidParameterException

A parameter is specified incorrectly.

HTTP Status Code: 400

OperationAbortedException

Multiple concurrent requests to update the same resource were in conflict.

HTTP Status Code: 400

ResourceNotFoundException

The specified resource does not exist.

HTTP Status Code: 400

ServiceUnavailableException

The service cannot complete the request.

HTTP Status Code: 500

See Also

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

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

DeleteLogGroup

Deletes the specified log group and permanently deletes all the archived log events associated with the log group.

Request Syntax

```
{
   "logGroupName": "string"
}
```

Request Parameters

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

The request accepts the following data in JSON format.

logGroupName

The name of the log group.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `[\.\-_/#A-Za-z0-9]+`

Required: Yes

Response Elements

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

Errors

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

InvalidParameterException

A parameter is specified incorrectly.

HTTP Status Code: 400

OperationAbortedException

Multiple concurrent requests to update the same resource were in conflict.

HTTP Status Code: 400

ResourceNotFoundException

The specified resource does not exist.

HTTP Status Code: 400

ServiceUnavailableException

The service cannot complete the request.

HTTP Status Code: 500

ValidationException

One of the parameters for the request is not valid.

HTTP Status Code: 400

Examples

To delete a log group

The following example deletes the specified log group.

Sample Request

```
POST / HTTP/1.1
Host: logs.<region>.<domain>
X-Amz-Date: <DATE>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=content-
type;date;host;user-agent;x-amz-date;x-amz-target;x-amzn-requestid,
 Signature=<Signature>
User-Agent: <UserAgentString>
Accept: application/json
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Connection: Keep-Alive
```

```
X-Amz-Target: Logs_20140328.DeleteLogGroup
{
  "logGroupName": "my-log-group"
}
```

Sample Response

```
HTTP/1.1 200 OK
x-amzn-RequestId: <RequestId>
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Date: <Date>
```

See Also

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

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

DeleteLogStream

Deletes the specified log stream and permanently deletes all the archived log events associated with the log stream.

Request Syntax

```
{
   "logGroupName": "string",
   "logStreamName": "string"
}
```

Request Parameters

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

The request accepts the following data in JSON format.

logGroupName

The name of the log group.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `[\.\-_/#A-Za-z0-9]+`

Required: Yes

logStreamName

The name of the log stream.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `[^:*]*`

Required: Yes

Response Elements

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

Errors

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

InvalidParameterException

A parameter is specified incorrectly.

HTTP Status Code: 400

OperationAbortedException

Multiple concurrent requests to update the same resource were in conflict.

HTTP Status Code: 400

ResourceNotFoundException

The specified resource does not exist.

HTTP Status Code: 400

ServiceUnavailableException

The service cannot complete the request.

HTTP Status Code: 500

ValidationException

One of the parameters for the request is not valid.

HTTP Status Code: 400

Examples

To delete a log stream

The following example deletes the specified log stream.

Sample Request

```
POST / HTTP/1.1
Host: logs.<region>.<domain>
X-Amz-Date: <DATE>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=content-
type;date;host;user-agent;x-amz-date;x-amz-target;x-amzn-requestid,
 Signature=<Signature>
User-Agent: <UserAgentString>
Accept: application/json
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Connection: Keep-Alive
X-Amz-Target: Logs_20140328.DeleteLogStream
{
  "logGroupName": "my-log-group",
  "logStreamName": "my-log-stream"
}
```

Sample Response

```
HTTP/1.1 200 OK
x-amzn-RequestId: <RequestId>
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Date: <Date>
```

See Also

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

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin

- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

DeleteLookupTable

Deletes a lookup table permanently. This operation cannot be undone.

Queries that reference a deleted table will return an error. Before deleting a lookup table, review any saved queries or dashboards that may reference it.

Request Syntax

```
{
   "lookupTableArn": "string"
}
```

Request Parameters

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

The request accepts the following data in JSON format.

lookupTableArn

The ARN of the lookup table to delete.

Type: String

Required: Yes

Response Elements

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

Errors

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

AccessDeniedException

You don't have sufficient permissions to perform this action.

HTTP Status Code: 400

InvalidParameterException

A parameter is specified incorrectly.

HTTP Status Code: 400

ResourceNotFoundException

The specified resource does not exist.

HTTP Status Code: 400

ServiceUnavailableException

The service cannot complete the request.

HTTP Status Code: 500

See Also

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

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

DeleteMetricFilter

Deletes the specified metric filter.

Request Syntax

```
{
   "filterName": "string",
   "logGroupName": "string"
}
```

Request Parameters

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

The request accepts the following data in JSON format.

filterName

The name of the metric filter.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `[^:*]*`

Required: Yes

logGroupName

The name of the log group.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `[\.\-_/#A-Za-z0-9]+`

Required: Yes

Response Elements

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

Errors

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

InvalidParameterException

A parameter is specified incorrectly.

HTTP Status Code: 400

OperationAbortedException

Multiple concurrent requests to update the same resource were in conflict.

HTTP Status Code: 400

ResourceNotFoundException

The specified resource does not exist.

HTTP Status Code: 400

ServiceUnavailableException

The service cannot complete the request.

HTTP Status Code: 500

Examples

To delete a metric filter

The following example deletes the specified filter for the specified log group.

Sample Request

```
POST / HTTP/1.1
Host: logs.<region>.<domain>
X-Amz-Date: <DATE>
```

```
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=content-
type;date;host;user-agent;x-amz-date;x-amz-target;x-amzn-requestid,
 Signature=<Signature>
User-Agent: <UserAgentString>
Accept: application/json
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Connection: Keep-Alive
X-Amz-Target: Logs_20140328.DeleteMetricFilter
{
  "logGroupName": "my-log-group",
  "filterName": "my-metric-filter"
}
```

Sample Response

```
HTTP/1.1 200 OK
x-amzn-RequestId: <RequestId>
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Date: <Date>
```

See Also

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

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

DeleteQueryDefinition

Deletes a saved CloudWatch Logs Insights query definition. A query definition contains details about a saved CloudWatch Logs Insights query.

Each `DeleteQueryDefinition` operation can delete one query definition.

You must have the `logs:DeleteQueryDefinition` permission to be able to perform this operation.

Request Syntax

```
{
   "queryDefinitionId": "string"
}
```

Request Parameters

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

The request accepts the following data in JSON format.

queryDefinitionId

The ID of the query definition that you want to delete. You can use DescribeQueryDefinitions to retrieve the IDs of your saved query definitions.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Required: Yes

Response Syntax

```
{
   "success": boolean
}
```

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.

success

A value of TRUE indicates that the operation succeeded. FALSE indicates that the operation failed.

Type: Boolean

Errors

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

InvalidParameterException

A parameter is specified incorrectly.

HTTP Status Code: 400

ResourceNotFoundException

The specified resource does not exist.

HTTP Status Code: 400

ServiceUnavailableException

The service cannot complete the request.

HTTP Status Code: 500

Examples

Example

This example deletes a query definition.

Sample Request

```
POST / HTTP/1.1
Host: logs.<region>.<domain>
X-Amz-Date: <DATE>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=content-
type;date;host;user-agent;x-amz-date;x-amz-target;x-amzn-requestid,
 Signature=<Signature>
User-Agent: <UserAgentString>
Accept: application/json
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Connection: Keep-Alive
X-Amz-Target: Logs_20140328.DeleteQueryDefinition
{
   "queryDefinitionId": "123456ab-12ab-123a-789e-1234567890ab"
}
```

Sample Response

```
HTTP/1.1 200 OK
x-amzn-RequestId: <RequestId>
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Date: <Date>
{
   "success": True
}
```

See Also

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

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3

- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

DeleteResourcePolicy

Deletes a resource policy from this account. This revokes the access of the identities in that policy to put log events to this account.

Request Syntax

```
{
   "expectedRevisionId": "string",
   "policyName": "string",
   "resourceArn": "string"
}
```

Request Parameters

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

The request accepts the following data in JSON format.

expectedRevisionId

The expected revision ID of the resource policy. Required when deleting a resource-scoped policy to prevent concurrent modifications.

Type: String

Length Constraints: Minimum length of 1.

Required: No

policyName

The name of the policy to be revoked. This parameter is required.

Type: String

Required: No

resourceArn

The ARN of the CloudWatch Logs resource for which the resource policy needs to be deleted

Type: String

Required: No

Response Elements

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

Errors

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

InvalidParameterException

A parameter is specified incorrectly.

HTTP Status Code: 400

OperationAbortedException

Multiple concurrent requests to update the same resource were in conflict.

HTTP Status Code: 400

ResourceNotFoundException

The specified resource does not exist.

HTTP Status Code: 400

ServiceUnavailableException

The service cannot complete the request.

HTTP Status Code: 500

See Also

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

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++

- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

DeleteRetentionPolicy

Deletes the specified retention policy.

Log events do not expire if they belong to log groups without a retention policy.

Request Syntax

```
{
   "logGroupName": "string"
}
```

Request Parameters

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

The request accepts the following data in JSON format.

logGroupName

The name of the log group.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `[\.\-_/#A-Za-z0-9]+`

Required: Yes

Response Elements

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

Errors

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

InvalidParameterException

A parameter is specified incorrectly.

HTTP Status Code: 400

OperationAbortedException

Multiple concurrent requests to update the same resource were in conflict.

HTTP Status Code: 400

ResourceNotFoundException

The specified resource does not exist.

HTTP Status Code: 400

ServiceUnavailableException

The service cannot complete the request.

HTTP Status Code: 500

Examples

To delete a retention policy

The following example deletes the retention policy for the specified log group.

Sample Request

```
POST / HTTP/1.1
Host: logs.<region>.<domain>
X-Amz-Date: <DATE>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=content-
type;date;host;user-agent;x-amz-date;x-amz-target;x-amzn-requestid,
 Signature=<Signature>
User-Agent: <UserAgentString>
Accept: application/json
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Connection: Keep-Alive
X-Amz-Target: Logs_20140328.DeleteRetentionPolicy
{
  "logGroupName": "my-log-group"
}
```

Sample Response

```
HTTP/1.1 200 OK
x-amzn-RequestId: <RequestId>
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Date: <Date>
```

See Also

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

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

DeleteScheduledQuery

Deletes a scheduled query and stops all future executions. This operation also removes any configured actions and associated resources.

Request Syntax

```
{
   "identifier": "string"
}
```

Request Parameters

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

The request accepts the following data in JSON format.

identifier

The ARN or name of the scheduled query to delete.

Type: String

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

Required: Yes

Response Elements

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

Errors

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

AccessDeniedException

You don't have sufficient permissions to perform this action.

HTTP Status Code: 400

InternalServerException

An internal server error occurred while processing the request. This exception is returned when the service encounters an unexpected condition that prevents it from fulfilling the request.

HTTP Status Code: 500

ResourceNotFoundException

The specified resource does not exist.

HTTP Status Code: 400

ThrottlingException

The request was throttled because of quota limits.

HTTP Status Code: 400

ValidationException

One of the parameters for the request is not valid.

HTTP Status Code: 400

See Also

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

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

DeleteSubscriptionFilter

Deletes the specified subscription filter.

Request Syntax

```
{
   "filterName": "string",
   "logGroupName": "string"
}
```

Request Parameters

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

The request accepts the following data in JSON format.

filterName

The name of the subscription filter.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `[^:*]*`

Required: Yes

logGroupName

The name of the log group.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `[\.\-_/#A-Za-z0-9]+`

Required: Yes

Response Elements

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

Errors

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

InvalidParameterException

A parameter is specified incorrectly.

HTTP Status Code: 400

OperationAbortedException

Multiple concurrent requests to update the same resource were in conflict.

HTTP Status Code: 400

ResourceNotFoundException

The specified resource does not exist.

HTTP Status Code: 400

ServiceUnavailableException

The service cannot complete the request.

HTTP Status Code: 500

Examples

To delete a subscription filter

The following example deletes the specified subscription filter for the specified log group.

Sample Request

```
POST / HTTP/1.1
Host: logs.<region>.<domain>
X-Amz-Date: <DATE>
```

```
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=content-
type;date;host;user-agent;x-amz-date;x-amz-target;x-amzn-requestid,
 Signature=<Signature>
User-Agent: <UserAgentString>
Accept: application/json
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Connection: Keep-Alive
X-Amz-Target: Logs_20140328.DeleteSubscriptionFilter
{
  "logGroupName": "my-log-group",
  "filterName": "my-subscription-filter"
}
```

Sample Response

```
HTTP/1.1 200 OK
x-amzn-RequestId: <RequestId>
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Date: <Date>
```

See Also

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

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

DeleteSyslogConfiguration

Deletes a syslog configuration for a log group. After deletion, syslog data is no longer ingested through the specified VPC endpoint.

Request Syntax

```
{
   "logGroupIdentifier": "string",
   "vpcEndpointId": "string"
}
```

Request Parameters

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

The request accepts the following data in JSON format.

logGroupIdentifier

The name or ARN of the log group to remove the syslog configuration from.

Type: String

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

Pattern: `[\w#+=/:,.@-]*`

Required: Yes

vpcEndpointId

The ID of the VPC endpoint associated with the syslog configuration to delete.

Type: String

Pattern: `^vpce-[0-9a-f]{1,64}$`

Required: No

Response Elements

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

Errors

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

AccessDeniedException

You don't have sufficient permissions to perform this action.

HTTP Status Code: 400

InvalidOperationException

The operation is not valid on the specified resource.

HTTP Status Code: 400

InvalidParameterException

A parameter is specified incorrectly.

HTTP Status Code: 400

OperationAbortedException

Multiple concurrent requests to update the same resource were in conflict.

HTTP Status Code: 400

ResourceNotFoundException

The specified resource does not exist.

HTTP Status Code: 400

ServiceUnavailableException

The service cannot complete the request.

HTTP Status Code: 500

ThrottlingException

The request was throttled because of quota limits.

HTTP Status Code: 400

Examples

To delete a syslog configuration

The following example deletes the syslog configuration for the specified log group and VPC endpoint.

Sample Request

```
POST / HTTP/1.1
Host: logs.<region>.<domain>
X-Amz-Date: <DATE>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=content-
type;date;host;user-agent;x-amz-date;x-amz-target;x-amzn-requestid,
 Signature=<Signature>
User-Agent: <UserAgentString>
Accept: application/json
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Connection: Keep-Alive
X-Amz-Target: Logs_20140328.DeleteSyslogConfiguration
{
  "logGroupIdentifier": "arn:aws:logs:us-east-1:123456789012:log-group:my-syslog-
group",
  "vpcEndpointId": "vpce-0123456789abcdef0"
}
```

Sample Response

```
HTTP/1.1 200 OK
x-amzn-RequestId: <RequestId>
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Date: <Date>
```

See Also

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

- AWS Command Line Interface V2

- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

DeleteTransformer

Deletes the log transformer for the specified log group. As soon as you do this, the transformation of incoming log events according to that transformer stops. If this account has an account-level transformer that applies to this log group, the log group begins using that account-level transformer when this log-group level transformer is deleted.

After you delete a transformer, be sure to edit any metric filters or subscription filters that relied on the transformed versions of the log events.

Request Syntax

```
{
   "logGroupIdentifier": "string"
}
```

Request Parameters

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

The request accepts the following data in JSON format.

logGroupIdentifier

Specify either the name or ARN of the log group to delete the transformer for. If the log group is in a source account and you are using a monitoring account, you must use the log group ARN.

Type: String

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

Pattern: `[\w#+=/:,.@-]*`

Required: Yes

Response Elements

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

Errors

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

InvalidOperationException

The operation is not valid on the specified resource.

HTTP Status Code: 400

InvalidParameterException

A parameter is specified incorrectly.

HTTP Status Code: 400

OperationAbortedException

Multiple concurrent requests to update the same resource were in conflict.

HTTP Status Code: 400

ResourceNotFoundException

The specified resource does not exist.

HTTP Status Code: 400

ServiceUnavailableException

The service cannot complete the request.

HTTP Status Code: 500

See Also

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

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2

- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

DescribeAccountPolicies

Returns a list of all CloudWatch Logs account policies in the account.

To use this operation, you must be signed on with the correct permissions depending on the type of policy that you are retrieving information for.

- To see data protection policies, you must have the `logs:GetDataProtectionPolicy` and `logs:DescribeAccountPolicies` permissions.
- To see subscription filter policies, you must have the `logs:DescribeSubscriptionFilters` and `logs:DescribeAccountPolicies` permissions.
- To see transformer policies, you must have the `logs:GetTransformer` and `logs:DescribeAccountPolicies` permissions.
- To see field index policies, you must have the `logs:DescribeIndexPolicies` and `logs:DescribeAccountPolicies` permissions.

Request Syntax

```
{
   "accountIdentifiers": [ "string" ],
   "nextToken": "string",
   "policyName": "string",
   "policyType": "string"
}
```

Request Parameters

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

The request accepts the following data in JSON format.

accountIdentifiers

If you are using an account that is set up as a monitoring account for CloudWatch unified cross-account observability, you can use this to specify the account ID of a source account. If you do, the operation returns the account policy for the specified account. Currently, you can specify only one account ID in this parameter.

If you omit this parameter, only the policy in the current account is returned.

Type: Array of strings

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

Length Constraints: Fixed length of 12.

Pattern: `^\d{12}$`

Required: No

nextToken

The token for the next set of items to return. (You received this token from a previous call.)

Type: String

Length Constraints: Minimum length of 1.

Required: No

policyName

Use this parameter to limit the returned policies to only the policy with the name that you specify.

Type: String

Required: No

policyType

Use this parameter to limit the returned policies to only the policies that match the policy type that you specify.

Type: String

Valid Values: `DATA_PROTECTION_POLICY | SUBSCRIPTION_FILTER_POLICY | FIELD_INDEX_POLICY | TRANSFORMER_POLICY | METRIC_EXTRACTION_POLICY`

Required: Yes

Response Syntax

```
{
```

```
   "accountPolicies": [
      {
         "accountId": "string",
         "lastUpdatedTime": number,
         "policyDocument": "string",
         "policyName": "string",
         "policyType": "string",
         "scope": "string",
         "selectionCriteria": "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.

accountPolicies

An array of structures that contain information about the CloudWatch Logs account policies that match the specified filters.

Type: Array of AccountPolicy objects

nextToken

The token to use when requesting the next set of items. The token expires after 24 hours.

Type: String

Length Constraints: Minimum length of 1.

Errors

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

InvalidParameterException

A parameter is specified incorrectly.

HTTP Status Code: 400

OperationAbortedException

Multiple concurrent requests to update the same resource were in conflict.

HTTP Status Code: 400

ResourceNotFoundException

The specified resource does not exist.

HTTP Status Code: 400

ServiceUnavailableException

The service cannot complete the request.

HTTP Status Code: 500

See Also

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

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

DescribeConfigurationTemplates

Use this operation to return the valid and default values that are used when creating delivery sources, delivery destinations, and deliveries. For more information about deliveries, see CreateDelivery.

Request Syntax

```
{
   "deliveryDestinationTypes": [ "string" ],
   "limit": number,
   "logTypes": [ "string" ],
   "nextToken": "string",
   "resourceTypes": [ "string" ],
   "service": "string"
}
```

Request Parameters

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

The request accepts the following data in JSON format.

deliveryDestinationTypes

Use this parameter to filter the response to include only the configuration templates that apply to the delivery destination types that you specify here.

Type: Array of strings

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

Valid Values: `S3 | CWL | FH | XRAY`

Required: No

limit

Use this parameter to limit the number of configuration templates that are returned in the response.

Type: Integer

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

Required: No

logTypes

Use this parameter to filter the response to include only the configuration templates that apply to the log types that you specify here.

Type: Array of strings

Array Members: Minimum number of 1 item. Maximum number of 10 items.

Length Constraints: Minimum length of 1. Maximum length of 255.

Pattern: `[\w]*`

Required: No

nextToken

The token for the next set of items to return. The token expires after 24 hours.

Type: String

Length Constraints: Minimum length of 1.

Required: No

resourceTypes

Use this parameter to filter the response to include only the configuration templates that apply to the resource types that you specify here.

Type: Array of strings

Array Members: Minimum number of 1 item. Maximum number of 10 items.

Length Constraints: Minimum length of 1. Maximum length of 255.

Pattern: `[\w-_]*`

Required: No

service

Use this parameter to filter the response to include only the configuration templates that apply to the AWS service that you specify here.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 255.

Pattern: `[\w_-]*`

Required: No

Response Syntax

```
{
   "configurationTemplates": [
      {
         "allowedActionForAllowVendedLogsDeliveryForResource": "string",
         "allowedFieldDelimiters": [ "string" ],
         "allowedFields": [
            {
               "mandatory": boolean,
               "name": "string"
            }
         ],
         "allowedOutputFormats": [ "string" ],
         "allowedSuffixPathFields": [ "string" ],
         "defaultDeliveryConfigValues": {
            "fieldDelimiter": "string",
            "recordFields": [ "string" ],
            "s3DeliveryConfiguration": {
               "enableHiveCompatiblePath": boolean,
               "suffixPath": "string"
            }
         },
         "deliveryDestinationType": "string",
         "deliverySourceConfiguration": [
            {
               "defaultValue": "string",
               "keyName": "string",
               "maxValue": number,
               "minValue": number,
               "supportedValues": [ "string" ],
               "valueType": "string"
            }
         ],
         "logType": "string",
```

```
         "resourceType": "string",
         "s3TablesIntegration": {
            "datasourceName": "string",
            "datasourceType": "string"
         },
         "service": "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.

configurationTemplates

An array of objects, where each object describes one configuration template that matches the filters that you specified in the request.

Type: Array of ConfigurationTemplate objects

nextToken

The token for the next set of items to return. The token expires after 24 hours.

Type: String

Length Constraints: Minimum length of 1.

Errors

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

ResourceNotFoundException

The specified resource does not exist.

HTTP Status Code: 400

ServiceUnavailableException

The service cannot complete the request.

HTTP Status Code: 500

ThrottlingException

The request was throttled because of quota limits.

HTTP Status Code: 400

ValidationException

One of the parameters for the request is not valid.

HTTP Status Code: 400

See Also

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

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

DescribeDeliveries

Retrieves a list of the deliveries that have been created in the account.

A *delivery* is a connection between a *delivery source* and a *delivery destination*.

A delivery source represents an AWS resource that sends logs to an logs delivery destination. The destination can be CloudWatch Logs, Amazon S3, Firehose or X-Ray. Only some AWS services support being configured as a delivery source. These services are listed in Enable logging from AWS services.

Request Syntax

```
{
   "limit": number,
   "nextToken": "string"
}
```

Request Parameters

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

The request accepts the following data in JSON format.

limit

Optionally specify the maximum number of deliveries to return in the response.

Type: Integer

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

Required: No

nextToken

The token for the next set of items to return. The token expires after 24 hours.

Type: String

Length Constraints: Minimum length of 1.

Required: No

Response Syntax

```
{
   "deliveries": [
      {
         "arn": "string",
         "deliveryDestinationArn": "string",
         "deliveryDestinationType": "string",
         "deliverySourceName": "string",
         "fieldDelimiter": "string",
         "id": "string",
         "recordFields": [ "string" ],
         "s3DeliveryConfiguration": {
            "enableHiveCompatiblePath": boolean,
            "suffixPath": "string"
         },
         "tags": {
            "string" : "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.

deliveries

An array of structures. Each structure contains information about one delivery in the account.

Type: Array of Delivery objects

nextToken

The token for the next set of items to return. The token expires after 24 hours.

Type: String

Length Constraints: Minimum length of 1.

Errors

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

ServiceQuotaExceededException

This request exceeds a service quota.

HTTP Status Code: 400

ServiceUnavailableException

The service cannot complete the request.

HTTP Status Code: 500

ThrottlingException

The request was throttled because of quota limits.

HTTP Status Code: 400

ValidationException

One of the parameters for the request is not valid.

HTTP Status Code: 400

See Also

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

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3

- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

DescribeDeliveryDestinations

Retrieves a list of the delivery destinations that have been created in the account.

Request Syntax

```
{
   "limit": number,
   "nextToken": "string"
}
```

Request Parameters

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

The request accepts the following data in JSON format.

limit

Optionally specify the maximum number of delivery destinations to return in the response.

Type: Integer

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

Required: No

nextToken

The token for the next set of items to return. The token expires after 24 hours.

Type: String

Length Constraints: Minimum length of 1.

Required: No

Response Syntax

```
{
   "deliveryDestinations": [
      {
```

```
         "arn": "string",
         "deliveryDestinationConfiguration": {
            "destinationResourceArn": "string"
         },
         "deliveryDestinationType": "string",
         "name": "string",
         "outputFormat": "string",
         "tags": {
            "string" : "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.

deliveryDestinations

An array of structures. Each structure contains information about one delivery destination in the account.

Type: Array of DeliveryDestination objects

nextToken

The token for the next set of items to return. The token expires after 24 hours.

Type: String

Length Constraints: Minimum length of 1.

Errors

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

ServiceQuotaExceededException

This request exceeds a service quota.

HTTP Status Code: 400

ServiceUnavailableException

The service cannot complete the request.

HTTP Status Code: 500

ThrottlingException

The request was throttled because of quota limits.

HTTP Status Code: 400

ValidationException

One of the parameters for the request is not valid.

HTTP Status Code: 400

See Also

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

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

DescribeDeliverySources

Retrieves a list of the delivery sources that have been created in the account.

Request Syntax

```
{
   "limit": number,
   "nextToken": "string"
}
```

Request Parameters

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

The request accepts the following data in JSON format.

limit

Optionally specify the maximum number of delivery sources to return in the response.

Type: Integer

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

Required: No

nextToken

The token for the next set of items to return. The token expires after 24 hours.

Type: String

Length Constraints: Minimum length of 1.

Required: No

Response Syntax

```
{
   "deliverySources": [
```

```
      {
         "arn": "string",
         "deliverySourceConfiguration": {
            "string" : "string"
         },
         "logType": "string",
         "name": "string",
         "resourceArns": [ "string" ],
         "service": "string",
         "status": "string",
         "statusReason": "string",
         "tags": {
            "string" : "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.

deliverySources

An array of structures. Each structure contains information about one delivery source in the account.

Type: Array of DeliverySource objects

nextToken

The token for the next set of items to return. The token expires after 24 hours.

Type: String

Length Constraints: Minimum length of 1.

Errors

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

ServiceQuotaExceededException

This request exceeds a service quota.

HTTP Status Code: 400

ServiceUnavailableException

The service cannot complete the request.

HTTP Status Code: 500

ThrottlingException

The request was throttled because of quota limits.

HTTP Status Code: 400

ValidationException

One of the parameters for the request is not valid.

HTTP Status Code: 400

See Also

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

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

DescribeDestinations

Lists all your destinations. The results are ASCII-sorted by destination name.

Request Syntax

```
{
   "DestinationNamePrefix": "string",
   "limit": number,
   "nextToken": "string"
}
```

Request Parameters

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

The request accepts the following data in JSON format.

DestinationNamePrefix

The prefix to match. If you don't specify a value, no prefix filter is applied.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `[^:*]*`

Required: No

limit

The maximum number of items returned. If you don't specify a value, the default maximum value of 50 items is used.

Type: Integer

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

Required: No

nextToken

The token for the next set of items to return. (You received this token from a previous call.)

Type: String

Length Constraints: Minimum length of 1.

Required: No

Response Syntax

```
{
   "destinations": [
      {
         "accessPolicy": "string",
         "arn": "string",
         "creationTime": number,
         "destinationName": "string",
         "roleArn": "string",
         "targetArn": "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

The destinations.

Type: Array of Destination objects

nextToken

The token for the next set of items to return. The token expires after 24 hours.

Type: String

Length Constraints: Minimum length of 1.

Errors

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

InvalidParameterException

A parameter is specified incorrectly.

HTTP Status Code: 400

ServiceUnavailableException

The service cannot complete the request.

HTTP Status Code: 500

Examples

To list all destinations

The following example lists all the destinations for the account.

Sample Request

```
POST / HTTP/1.1
Host: logs.<region>.<domain>
X-Amz-Date: <DATE>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=content-
type;date;host;user-agent;x-amz-date;x-amz-target;x-amzn-requestid,
 Signature=<Signature>
User-Agent: <UserAgentString>
Accept: application/json
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Connection: Keep-Alive
X-Amz-Target: Logs_20140328.DescribeDestinations
{
  "destinationNamePrefix": "my-prefix"
}
```

Sample Response

```
HTTP/1.1 200 OK
```

```
x-amzn-RequestId: <RequestId>
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Date: <Date>
{
  "destination": [
    {
      "destinationName": "my-destination",
      "targetArn": "arn:aws:kinesis:us-east-1:123456789012:stream/my-kinesis-stream",
      "roleArn": "arn:aws:iam::123456789012:role/my-subscription-role",
      "arn": "arn:aws:logs:us-east-1:123456789012:destination:my-destination",
      "creationTime": 1437584472382
    }
  ]
}
```

See Also

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

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

DescribeExportTasks

Lists the specified export tasks. You can list all your export tasks or filter the results based on task ID or task status.

Request Syntax

```
{
   "limit": number,
   "nextToken": "string",
   "statusCode": "string",
   "taskId": "string"
}
```

Request Parameters

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

The request accepts the following data in JSON format.

limit

The maximum number of items returned. If you don't specify a value, the default is up to 50 items.

Type: Integer

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

Required: No

nextToken

The token for the next set of items to return. (You received this token from a previous call.)

Type: String

Length Constraints: Minimum length of 1.

Required: No

statusCode

The status code of the export task. Specifying a status code filters the results to zero or more export tasks.

Type: String

Valid Values: `CANCELLED | COMPLETED | FAILED | PENDING | PENDING_CANCEL | RUNNING`

Required: No

taskId

The ID of the export task. Specifying a task ID filters the results to one or zero export tasks.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Required: No

Response Syntax

```
{
   "exportTasks": [
      {
         "destination": "string",
         "destinationPrefix": "string",
         "executionInfo": {
            "completionTime": number,
            "creationTime": number
         },
         "from": number,
         "logGroupName": "string",
         "status": {
            "code": "string",
            "message": "string"
         },
         "taskId": "string",
         "taskName": "string",
         "to": number
      }
   ],
```

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

Response Elements

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

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

exportTasks

The export tasks.

Type: Array of ExportTask objects

nextToken

The token for the next set of items to return. The token expires after 24 hours.

Type: String

Length Constraints: Minimum length of 1.

Errors

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

InvalidParameterException

A parameter is specified incorrectly.

HTTP Status Code: 400

ServiceUnavailableException

The service cannot complete the request.

HTTP Status Code: 500

Examples

To list the export tasks that are complete

The following example lists the export tasks with the COMPLETE status.

Sample Request

```
POST / HTTP/1.1
Host: logs.<region>.<domain>
X-Amz-Date: <DATE>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=content-
type;date;host;user-agent;x-amz-date;x-amz-target;x-amzn-requestid,
 Signature=<Signature>
User-Agent: <UserAgentString>
Accept: application/json
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Connection: Keep-Alive
X-Amz-Target: Logs_20140328.DescribeExportTasks
{
  "statusCode": "COMPLETE"
}
```

Sample Response

```
HTTP/1.1 200 OK
x-amzn-RequestId: <RequestId>
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Date: <Date>
{
  "exportTasks": [
    {
      "taskId": "exampleTaskId",
      "taskName": "my-task-1",
      "logGroupName": "my-log-group",
      "from": 1437584472382,
      "to": 1437584472833,
      "destination": "my-destination",
      "destinationPrefix": "my-prefix",
      "status":
        {
          "code": "COMPLETE",
          "message": "Example message"
        },
      "executionInfo":
        {
          "creationTime": 1437584472856,
```

```
          "completionTime" : 1437584472986
        }
    },
    {
      "taskId": "exampleTaskId",
      "taskName": "my-task-2",
      "logGroupName": "my-log-group",
      "from": 1437584472382,
      "to": 1437584472833,
      "destination": "my-destination",
      "destinationPrefix": "my-prefix",
      "status":
        {
          "code": "COMPLETE",
          "message": "Example message"
        },
      "executionInfo":
        {
          "creationTime": 1437584472856,
          "completionTime" : 1437584472986
        }
    }
  ]
}
```

See Also

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

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)

- AWS SDK for Ruby V3

DescribeFieldIndexes

Returns a list of field indexes discovered in log data. By default, the response includes the `DEFAULT`, `CUSTOM`, and `INACTIVE` index categories. To return indexes from other categories, use the `indexCategories` parameter.

For more information about field index policies, see PutIndexPolicy.

Request Syntax

```
{
   "indexCategories": [ "string" ],
   "logGroupIdentifiers": [ "string" ],
   "nextToken": "string"
}
```

Request Parameters

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

The request accepts the following data in JSON format.

indexCategories

The index categories to return. The following values are supported:

- `DEFAULT`: Fields that CloudWatch Logs indexes by default. Examples include `@logStream` and `@data_format`.
- `CUSTOM`: Fields that you added manually to the field index policy. CloudWatch Logs always indexes these fields. These fields count toward the quota of 20 fields for each log group.
- `AUTO`: Fields that CloudWatch Logs indexes automatically based on your query patterns and usage. These fields do not count toward the field index quota. CloudWatch Logs might update these fields based on changes in your query patterns. To keep a field indexed permanently, add it to an account-level or log-group level field index policy.
- `INACTIVE`: Fields that CloudWatch Logs indexed before but does not index now. This happens if you remove a field from the field index policy or if CloudWatch Logs automatically selects a different field based on your queries.

If you omit this parameter, the response includes the `DEFAULT`, `CUSTOM`, and `INACTIVE` categories.

For more information about automatically indexed fields and using the AUTO category, see Automatically indexed fields.

Type: Array of strings

Array Members: Maximum number of 4 items.

Valid Values: `DEFAULT | CUSTOM | AUTO | INACTIVE`

Required: No

logGroupIdentifiers

An array containing the names or ARNs of the log groups that you want to retrieve field indexes for.

Type: Array of strings

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

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

Pattern: `[\w#+=/:,.@-]*`

Required: Yes

nextToken

The token for the next set of items to return. The token expires after 24 hours.

Type: String

Length Constraints: Minimum length of 1.

Required: No

Response Syntax

```
{
   "fieldIndexes": [
      {
         "fieldIndexName": "string",
         "firstEventTime": number,
```

```
            "indexCategory": "string",
            "lastEventTime": number,
            "lastScanTime": number,
            "logGroupIdentifier": "string",
            "type": "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.

fieldIndexes

An array containing the field index information.

Type: Array of FieldIndex objects

nextToken

The token for the next set of items to return. The token expires after 24 hours.

Type: String

Length Constraints: Minimum length of 1.

Errors

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

InvalidParameterException

A parameter is specified incorrectly.

HTTP Status Code: 400

LimitExceededException

You have reached the maximum number of resources that can be created.

HTTP Status Code: 400

OperationAbortedException

Multiple concurrent requests to update the same resource were in conflict.

HTTP Status Code: 400

ResourceNotFoundException

The specified resource does not exist.

HTTP Status Code: 400

ServiceUnavailableException

The service cannot complete the request.

HTTP Status Code: 500

See Also

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

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

DescribeImportTaskBatches

Gets detailed information about the individual batches within an import task, including their status and any error messages. For CloudTrail Event Data Store sources, a batch refers to a subset of stored events grouped by their eventTime.

Request Syntax

```
{
   "batchImportStatus": [ "string" ],
   "importId": "string",
   "limit": number,
   "nextToken": "string"
}
```

Request Parameters

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

The request accepts the following data in JSON format.

batchImportStatus

Optional filter to list import batches by their status. Accepts multiple status values: IN_PROGRESS, CANCELLED, COMPLETED and FAILED.

Type: Array of strings

Valid Values: `IN_PROGRESS | CANCELLED | COMPLETED | FAILED`

Required: No

importId

The ID of the import task to get batch information for.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

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

Required: Yes

limit

The maximum number of import batches to return in the response. Default: 10

Type: Integer

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

Required: No

nextToken

The pagination token for the next set of results.

Type: String

Length Constraints: Minimum length of 1.

Required: No

Response Syntax

```
{
   "importBatches": [
      {
         "batchId": "string",
         "errorMessage": "string",
         "status": "string"
      }
   ],
   "importId": "string",
   "importSourceArn": "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.

importBatches

The list of import batches that match the request filters.

Type: Array of ImportBatch objects

importId

The ID of the import task.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

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

importSourceArn

The ARN of the source being imported from.

Type: String

nextToken

The token to use when requesting the next set of results. Not present if there are no additional results to retrieve.

Type: String

Length Constraints: Minimum length of 1.

Errors

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

AccessDeniedException

You don't have sufficient permissions to perform this action.

HTTP Status Code: 400

InvalidOperationException

The operation is not valid on the specified resource.

HTTP Status Code: 400

InvalidParameterException

A parameter is specified incorrectly.

HTTP Status Code: 400

ResourceNotFoundException

The specified resource does not exist.

HTTP Status Code: 400

ThrottlingException

The request was throttled because of quota limits.

HTTP Status Code: 400

Examples

To describe import task batches

The following example retrieves batch-level details for an import task with status filtering.

Sample Request

```
POST / HTTP/1.1
          Host: logs.<region>.<domain>
          X-Amz-Target: Logs_20140328.DescribeImportTaskBatches
          {
          "importId": "a1b2c3d4-e5f6-7890-abcd-ef1234567890",
          "batchImportStatus": ["IN_PROGRESS", "COMPLETED"],
          "limit": 25,
          "nextToken": "eyJOZXh0VG9rZW4iOiJudWxsIiwiYm90b190cnVuY2F0ZV9hbW91bnQiOjF9"
          }
```

Sample Response

```
HTTP/1.1 200 OK
          {
          "importSourceArn": "arn:aws:cloudtrail:us-west-2:123456789012:eventdatastore/
f1d45bff-d0e3-4868-b5d9-2eb678aa32fb",
```

```
"importId": "a1b2c3d4-e5f6-7890-abcd-ef1234567890",
"importBatches": [
{
"batchId": "b1c2d3e4-f5g6-7890-hijk-lm1234567890",
"status": "COMPLETED"
},
{
"batchId": "c2d3e4f5-g6h7-8901-ijkl-mn2345678901",
"status": "IN_PROGRESS"
},
{
"batchId": "d3e4f5g6-h7i8-9012-jklm-no3456789012",
"status": "FAILED",
"errorMessage": "Access denied to CloudTrail event data store"
}
],
"nextToken": "eyJOZXh0VG9rZW4iOiJudWxsIiwiYm90b190cnVuY2F0ZV9hbW91bnQiOjJ9"
}
```


See Also

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

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

DescribeImportTasks

Lists and describes import tasks, with optional filtering by import status and source ARN.

Request Syntax

```
{
   "importId": "string",
   "importSourceArn": "string",
   "importStatus": "string",
   "limit": number,
   "nextToken": "string"
}
```

Request Parameters

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

The request accepts the following data in JSON format.

importId

Optional filter to describe a specific import task by its ID.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

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

Required: No

importSourceArn

Optional filter to list imports from a specific source

Type: String

Required: No

importStatus

Optional filter to list imports by their status. Valid values are IN_PROGRESS, CANCELLED, COMPLETED and FAILED.

Type: String

Valid Values: `IN_PROGRESS | CANCELLED | COMPLETED | FAILED`

Required: No

limit

The maximum number of import tasks to return in the response. Default: 50

Type: Integer

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

Required: No

nextToken

The pagination token for the next set of results.

Type: String

Length Constraints: Minimum length of 1.

Required: No

Response Syntax

```
{
   "imports": [
      {
         "creationTime": number,
         "errorMessage": "string",
         "importDestinationArn": "string",
         "importFilter": {
            "endEventTime": number,
            "startEventTime": number
         },
         "importId": "string",
         "importSourceArn": "string",
         "importStatistics": {
            "bytesImported": number
         },
```

```
            "importStatus": "string",
            "lastUpdatedTime": number
        }
    ],
    "nextToken": "string"
}
```

Response Elements

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

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

imports

The list of import tasks that match the request filters.

Type: Array of Import objects

nextToken

The token to use when requesting the next set of results. Not present if there are no additional results to retrieve.

Type: String

Length Constraints: Minimum length of 1.

Errors

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

AccessDeniedException

You don't have sufficient permissions to perform this action.

HTTP Status Code: 400

InvalidOperationException

The operation is not valid on the specified resource.

HTTP Status Code: 400

InvalidParameterException

A parameter is specified incorrectly.

HTTP Status Code: 400

ResourceNotFoundException

The specified resource does not exist.

HTTP Status Code: 400

ThrottlingException

The request was throttled because of quota limits.

HTTP Status Code: 400

Examples

To describe import tasks

The following example retrieves a list of import tasks with filters.

Sample Request

```
POST / HTTP/1.1
          Host: logs.<region>.<domain>
          X-Amz-Target: Logs_20140328.DescribeImportTasks
          {
          "importId": "a1b2c3d4-e5f6-7890-abcd-ef1234567890",
          "importStatus": "IN_PROGRESS",
          "importSourceArn": "arn:aws:cloudtrail:us-west-2:123456789012:eventdatastore/
f1d45bff-d0e3-4868-b5d9-2eb678aa32fb",
          "limit": 50,
          "nextToken": "eyJOZXh0VG9rZW4iOiJudWxsIiwiYm90b190cnVuY2F0ZV9hbW91bnQiOjF9"
          }
```

Sample Response

```
HTTP/1.1 200 OK
          {
          "imports": [
```

```
        {
        "importId": "a1b2c3d4-e5f6-7890-abcd-ef1234567890",
        "importSourceArn": "arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/
f1d45bff-d0e3-4868-b5d9-2eb678aa32fb",
        "importStatus": "IN_PROGRESS",
        "importDestinationArn": "arn:aws:logs:us-east-1:123456789012:log-group:aws/
cloudtrail/f1d45bff-d0e3-4868-b5d9-2eb678aa32fb",
        "importStatistics": {
        "bytesImported": 1048576
        },
        "importFilter": {
        "startEventTime": 1640995200000,
        "endEventTime": 1641081600000
        },
        "creationTime": 1641168000000,
        "lastUpdatedTime": 1641171600000
        }
        ],
        "nextToken": "eyJOZXh0VG9rZW4iOiJudWxsIiwiYm90b190cnVuY2F0ZV9hbW91bnQiOjJ9"
        }
```


See Also

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

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

DescribeIndexPolicies

Returns the field index policies of the specified log group. For more information about field index policies, see PutIndexPolicy.

If a specified log group has a log-group level index policy, that policy is returned by this operation.

If a specified log group doesn't have a log-group level index policy, but an account-wide index policy applies to it, that account-wide policy is returned by this operation.

To find information about only account-level policies, use DescribeAccountPolicies instead.

Request Syntax

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

Request Parameters

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

The request accepts the following data in JSON format.

logGroupIdentifiers

An array containing the name or ARN of the log group that you want to retrieve field index policies for.

Type: Array of strings

Array Members: Fixed number of 1 item.

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

Pattern: `[\w#+=/:,.@-]*`

Required: Yes

nextToken

The token for the next set of items to return. The token expires after 24 hours.

Type: String

Length Constraints: Minimum length of 1.

Required: No

Response Syntax

```
{
   "indexPolicies": [
      {
         "lastUpdateTime": number,
         "logGroupIdentifier": "string",
         "policyDocument": "string",
         "policyName": "string",
         "source": "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.

indexPolicies

An array containing the field index policies.

Type: Array of IndexPolicy objects

nextToken

The token for the next set of items to return. The token expires after 24 hours.

Type: String

Length Constraints: Minimum length of 1.

Errors

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

InvalidParameterException

A parameter is specified incorrectly.

HTTP Status Code: 400

LimitExceededException

You have reached the maximum number of resources that can be created.

HTTP Status Code: 400

OperationAbortedException

Multiple concurrent requests to update the same resource were in conflict.

HTTP Status Code: 400

ResourceNotFoundException

The specified resource does not exist.

HTTP Status Code: 400

ServiceUnavailableException

The service cannot complete the request.

HTTP Status Code: 500

See Also

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

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2

- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

DescribeLogGroups

Returns information about log groups, including data sources that ingest into each log group. You can return all your log groups or filter the results by prefix. The results are ASCII-sorted by log group name.

CloudWatch Logs doesn't support IAM policies that control access to the `DescribeLogGroups` action by using the `aws:ResourceTag/key-name` condition key. Other CloudWatch Logs actions do support the use of the `aws:ResourceTag/key-name` condition key to control access. For more information about using tags to control access, see Controlling access to Amazon Web Services resources using tags.

If you are using CloudWatch cross-account observability, you can use this operation in a monitoring account and view data from the linked source accounts. For more information, see CloudWatch cross-account observability.

Request Syntax

```
{
   "accountIdentifiers": [ "string" ],
   "includeLinkedAccounts": boolean,
   "limit": number,
   "logGroupClass": "string",
   "logGroupIdentifiers": [ "string" ],
   "logGroupNamePattern": "string",
   "logGroupNamePrefix": "string",
   "nextToken": "string"
}
```

Request Parameters

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

The request accepts the following data in JSON format.

accountIdentifiers

When `includeLinkedAccounts` is set to `true`, use this parameter to specify the list of accounts to search. You can specify as many as 20 account IDs in the array.

Type: Array of strings

Array Members: Minimum number of 0 items. Maximum number of 20 items.

Length Constraints: Fixed length of 12.

Pattern: `^\d{12}$`

Required: No

includeLinkedAccounts

If you are using a monitoring account, set this to `true` to have the operation return log groups in the accounts listed in `accountIdentifiers`.

If this parameter is set to `true` and `accountIdentifiers` contains a null value, the operation returns all log groups in the monitoring account and all log groups in all source accounts that are linked to the monitoring account.

The default for this parameter is `false`.

Type: Boolean

Required: No

limit

The maximum number of items returned. If you don't specify a value, the default is up to 50 items.

Type: Integer

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

Required: No

logGroupClass

Use this parameter to limit the results to only those log groups in the specified log group class. If you omit this parameter, log groups of all classes can be returned.

Specifies the log group class for this log group. There are three classes:

- The `Standard` log class supports all CloudWatch Logs features.
- The `Infrequent Access` log class supports a subset of CloudWatch Logs features and incurs lower costs.

- Use the `Delivery` log class only for delivering AWS Lambda logs to store in Amazon S3 or Amazon Data Firehose. Log events in log groups in the Delivery class are kept in CloudWatch Logs for only one day. This log class doesn't offer rich CloudWatch Logs capabilities such as CloudWatch Logs Insights queries.

For details about the features supported by each class, see Log classes

Type: String

Valid Values: `STANDARD | INFREQUENT_ACCESS | DELIVERY`

Required: No

logGroupIdentifiers

Use this array to filter the list of log groups returned. If you specify this parameter, the only other filter that you can choose to specify is `includeLinkedAccounts`.

If you are using this operation in a monitoring account, you can specify the ARNs of log groups in source accounts and in the monitoring account itself. If you are using this operation in an account that is not a cross-account monitoring account, you can specify only log group names in the same account as the operation.

Type: Array of strings

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

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

Pattern: `[\w#+=/:,.@-]*`

Required: No

logGroupNamePattern

If you specify a string for this parameter, the operation returns only log groups that have names that match the string based on a case-sensitive substring search. For example, if you specify `DataLogs`, log groups named `DataLogs`, `aws/DataLogs`, and `GroupDataLogs` would match, but `datalogs`, `Data/log/s` and `Groupdata` would not match.

If you specify `logGroupNamePattern` in your request, then only `arn`, `creationTime`, and `logGroupName` are included in the response.

> **Note**
>
> `logGroupNamePattern` and `logGroupNamePrefix` are mutually exclusive. Only one of these parameters can be passed.

Type: String

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

Pattern: `[\.\-_/#A-Za-z0-9]*`

Required: No

logGroupNamePrefix

The prefix to match.

> **Note**
>
> `logGroupNamePrefix` and `logGroupNamePattern` are mutually exclusive. Only one of these parameters can be passed.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `[\.\-_/#A-Za-z0-9]+`

Required: No

nextToken

The token for the next set of items to return. (You received this token from a previous call.)

Type: String

Length Constraints: Minimum length of 1.

Required: No

Response Syntax

```
{
   "logGroups": [
      {
         "arn": "string",
         "bearerTokenAuthenticationEnabled": boolean,
         "creationTime": number,
         "dataProtectionStatus": "string",
         "deletionProtectionEnabled": boolean,
         "inheritedProperties": [ "string" ],
         "kmsKeyId": "string",
         "logGroupArn": "string",
         "logGroupClass": "string",
         "logGroupName": "string",
         "metricFilterCount": number,
         "retentionInDays": number,
         "storedBytes": number
      }
   ],
   "nextToken": "string"
}
```

Response Elements

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

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

logGroups

An array of structures, where each structure contains the information about one log group.

Type: Array of LogGroup objects

nextToken

The token for the next set of items to return. The token expires after 24 hours.

Type: String

Length Constraints: Minimum length of 1.

Errors

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

InvalidParameterException

A parameter is specified incorrectly.

HTTP Status Code: 400

ServiceUnavailableException

The service cannot complete the request.

HTTP Status Code: 500

Examples

To list all log groups

The following example lists all your log groups.

Sample Request

```
POST / HTTP/1.1
Host: logs.<region>.<domain>
X-Amz-Date: <DATE>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=content-
type;date;host;user-agent;x-amz-date;x-amz-target;x-amzn-requestid,
 Signature=<Signature>
User-Agent: <UserAgentString>
Accept: application/json
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Connection: Keep-Alive
X-Amz-Target: Logs_20140328.DescribeLogGroups
```

Sample Response

```
HTTP/1.1 200 OK
x-amzn-RequestId: <RequestId>
```

```
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Date: <Date>
{
  "logGroups": [
    {
      "storageBytes": 1048576,
      "arn": "arn:aws:logs:us-east-1:123456789012:log-group:my-log-group-1:*",
      "creationTime": 1393545600000,
      "logGroupName": "my-log-group-1",
      "metricFilterCount": 0,
      "retentionInDays": 14,
      "kmsKeyId": "arn:aws:kms:us-east-1:123456789012:key/abcd1234-a123-456a-a12b-
a123b4cd56ef",
      "deletionProtectionEnabled": true
      "bearerTokenAuthenticationEnabled": true
    },
    {
      "storageBytes": 5242880,
      "arn": "arn:aws:logs:us-east-1:123456789012:log-group:my-log-group-2:*",
      "creationTime": 1396224000000,
      "logGroupName": "my-log-group-2",
      "metricFilterCount": 0,
      "retentionInDays": 30,
      "deletionProtectionEnabled": false
      "bearerTokenAuthenticationEnabled": false
    }
  ]
}
```

To list all of the log groups in a monitoring account and all linked source accounts that have logGroup in their name

The following example lists all of the log groups in a monitoring account and all linked source accounts that have `logGroup` in their name.

Sample Request

```
{
  "includeLinkedAccounts" : "true",
  "logGroupNamePattern": "logGroup"
}
```

Sample Response

```
{
  "logGroups": [
    {
      "arn": "arn:aws:logs:us-east-1:123456789012:log-group:monitoring-
logGroup-1234:*",
      "creationTime": 1393545600000,
      "logGroupName": "monitoring-logGroup-1234"
    },
    {
      "arn": "arn:aws:logs:us-east-1:012345678901:log-group:source-loggroup-5678:*",
      "creationTime": 1396224000000,
      "logGroupName": "source-loggroup-5678"
      }
  ]
}
```

See Also

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

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

DescribeLogStreams

Lists the log streams for the specified log group. You can list all the log streams or filter the results by prefix. You can also control how the results are ordered.

You can specify the log group to search by using either `logGroupIdentifier` or `logGroupName`. You must include one of these two parameters, but you can't include both.

This operation has a limit of 25 transactions per second, after which transactions are throttled.

If you are using CloudWatch cross-account observability, you can use this operation in a monitoring account and view data from the linked source accounts. For more information, see CloudWatch cross-account observability.

Request Syntax

```
{
   "descending": boolean,
   "limit": number,
   "logGroupIdentifier": "string",
   "logGroupName": "string",
   "logStreamNamePrefix": "string",
   "nextToken": "string",
   "orderBy": "string"
}
```

Request Parameters

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

The request accepts the following data in JSON format.

descending

If the value is true, results are returned in descending order. If the value is to false, results are returned in ascending order. The default value is false.

Type: Boolean

Required: No

limit

The maximum number of items returned. If you don't specify a value, the default is up to 50 items.

Type: Integer

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

Required: No

logGroupIdentifier

Specify either the name or ARN of the log group to view. If the log group is in a source account and you are using a monitoring account, you must use the log group ARN.

> **Note**
>
> You must include either `logGroupIdentifier` or `logGroupName`, but not both.

Type: String

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

Pattern: `[\w#+=/:,.@-]*`

Required: No

logGroupName

The name of the log group.

> **Note**
>
> You must include either `logGroupIdentifier` or `logGroupName`, but not both.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `[\.\-_/#A-Za-z0-9]+`

Required: No

logStreamNamePrefix

The prefix to match.

If `orderBy` is `LastEventTime`, you cannot specify this parameter.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `[^:*]*`

Required: No

nextToken

The token for the next set of items to return. (You received this token from a previous call.)

Type: String

Length Constraints: Minimum length of 1.

Required: No

orderBy

If the value is `LogStreamName`, the results are ordered by log stream name. If the value is `LastEventTime`, the results are ordered by the event time. The default value is `LogStreamName`.

If you order the results by event time, you cannot specify the `logStreamNamePrefix` parameter.

`lastEventTimestamp` represents the time of the most recent log event in the log stream in CloudWatch Logs. This number is expressed as the number of milliseconds after `Jan 1, 1970 00:00:00 UTC`. `lastEventTimestamp` updates on an eventual consistency basis. It typically updates in less than an hour from ingestion, but in rare situations might take longer.

Type: String

Valid Values: `LogStreamName | LastEventTime`

Required: No

Response Syntax

```
{
   "logStreams": [
      {
         "arn": "string",
         "creationTime": number,
         "firstEventTimestamp": number,
         "lastEventTimestamp": number,
         "lastIngestionTime": number,
         "logStreamName": "string",
         "storedBytes": number,
         "uploadSequenceToken": "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.

logStreams

The log streams.

Type: Array of LogStream objects

nextToken

The token for the next set of items to return. The token expires after 24 hours.

Type: String

Length Constraints: Minimum length of 1.

Errors

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

InvalidParameterException

A parameter is specified incorrectly.

HTTP Status Code: 400

ResourceNotFoundException

The specified resource does not exist.

HTTP Status Code: 400

ServiceUnavailableException

The service cannot complete the request.

HTTP Status Code: 500

Examples

To list the log streams for a log group

The following example lists the log streams associated with the specified log group.

Sample Request

```
POST / HTTP/1.1
Host: logs.<region>.<domain>
X-Amz-Date: <DATE>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=content-
type;date;host;user-agent;x-amz-date;x-amz-target;x-amzn-requestid,
 Signature=<Signature>
User-Agent: <UserAgentString>
Accept: application/json
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Connection: Keep-Alive
X-Amz-Target: Logs_20140328.DescribeLogStreams
{
  "logGroupName": "my-log-group"
```

```
}
```

Sample Response

```
HTTP/1.1 200 OK
x-amzn-RequestId: <RequestId>
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Date: <Date>
{
  "logStreams": [
    {
      "storedBytes": 0,
      "arn": "arn:aws:logs:us-east-1:123456789012:log-group:my-log-group-1:log-
stream:my-log-stream-1",
      "creationTime": 1393545600000,
      "firstEventTimestamp": 1393545600000,
      "lastEventTimestamp": 1393567800000,
      "lastIngestionTime": 1393589200000,
      "logStreamName": "my-log-stream-1"
    },
    {
      "storedBytes": 0,
      "arn": "arn:aws:logs:us-east-1:123456789012:log-group:my-log-group-2:log-
stream:my-log-stream-2",
      "creationTime": 1396224000000,
      "firstEventTimestamp": 1396224000000,
      "lastEventTimestamp": 1396235500000,
      "lastIngestionTime": 1396225560000,
      "logStreamName": "my-log-stream-2"
    }
  ]
}
```

Example

The following example lists the log streams associated with the specified log group.

Sample Request

```
{
  "logGroupIdentifier": "arn:aws:logs:us-east-1:123456789012:log-group:my-log-
group-1:dli"
```

```
}
```

Sample Response

```
{
  "logStreams": [
    {
      "storedBytes": 0,
      "arn": "arn:aws:logs:us-east-1:123456789012:log-group:my-log-group-1:log-
stream:my-
log-stream-1",
      "creationTime": 1393545600000,
      "firstEventTimestamp": 1393545600000,
      "lastEventTimestamp": 1393567800000,
      "lastIngestionTime": 1393589200000,
      "logStreamName": "my-log-stream-1"
      },
      {
      "storedBytes": 0,
      "arn": "arn:aws:logs:us-east-1:123456789012:log-group:my-log-group-2:log-
stream:my-
log-stream-2",
      "creationTime": 1396224000000,
      "firstEventTimestamp": 1396224000000,
      "lastEventTimestamp": 1396235500000,
      "lastIngestionTime": 1396225560000,
      "logStreamName": "my-log-stream-2"
      } ]
}
```

See Also

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

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2

- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

DescribeLookupTables

Retrieves metadata about lookup tables in your account. You can optionally filter the results by table name prefix. Results are sorted by table name in ascending order.

Request Syntax

```
{
   "lookupTableNamePrefix": "string",
   "maxResults": number,
   "nextToken": "string"
}
```

Request Parameters

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

The request accepts the following data in JSON format.

lookupTableNamePrefix

A prefix to filter lookup tables by name. Only tables whose names start with this prefix are returned. If you don't specify a prefix, all tables in the account and Region are returned.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `^[a-zA-Z0-9_]+$`

Required: No

maxResults

The maximum number of lookup tables to return in the response. The default value is 50 and the maximum value is 100.

Type: Integer

Valid Range: Maximum value of 100.

Required: No

nextToken

The token for the next set of items to return. (You received this token from a previous call.)

Type: String

Length Constraints: Minimum length of 1.

Required: No

Response Syntax

```
{
   "lookupTables": [
      {
         "description": "string",
         "kmsKeyId": "string",
         "lastUpdatedTime": number,
         "lookupTableArn": "string",
         "lookupTableName": "string",
         "recordsCount": number,
         "sizeBytes": number,
         "tableFields": [ "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.

lookupTables

An array of structures, where each structure contains metadata about one lookup table.

Type: Array of LookupTable objects

nextToken

The token to use when requesting the next set of items.

Type: String

Length Constraints: Minimum length of 1.

Errors

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

AccessDeniedException

You don't have sufficient permissions to perform this action.

HTTP Status Code: 400

InvalidParameterException

A parameter is specified incorrectly.

HTTP Status Code: 400

ResourceNotFoundException

The specified resource does not exist.

HTTP Status Code: 400

ServiceUnavailableException

The service cannot complete the request.

HTTP Status Code: 500

See Also

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

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2

- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

DescribeMetricFilters

Lists the specified metric filters. You can list all of the metric filters or filter the results by log name, prefix, metric name, or metric namespace. The results are ASCII-sorted by filter name.

Request Syntax

```
{
   "filterNamePrefix": "string",
   "limit": number,
   "logGroupName": "string",
   "metricName": "string",
   "metricNamespace": "string",
   "nextToken": "string"
}
```

Request Parameters

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

The request accepts the following data in JSON format.

filterNamePrefix

The prefix to match. CloudWatch Logs uses the value that you set here only if you also include the `logGroupName` parameter in your request.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `[^:*]*`

Required: No

limit

The maximum number of items returned. If you don't specify a value, the default is up to 50 items.

Type: Integer

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

Required: No

logGroupName

The name of the log group.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `[\.\-_/#A-Za-z0-9]+`

Required: No

metricName

Filters results to include only those with the specified metric name. If you include this parameter in your request, you must also include the `metricNamespace` parameter.

Type: String

Length Constraints: Maximum length of 255.

Pattern: `[^:*$]*`

Required: No

metricNamespace

Filters results to include only those in the specified namespace. If you include this parameter in your request, you must also include the `metricName` parameter.

Type: String

Length Constraints: Maximum length of 255.

Pattern: `[^:*$]*`

Required: No

nextToken

The token for the next set of items to return. (You received this token from a previous call.)

Type: String

Length Constraints: Minimum length of 1.

Required: No

Response Syntax

```
{
   "metricFilters": [
      {
         "applyOnTransformedLogs": boolean,
         "creationTime": number,
         "emitSystemFieldDimensions": [ "string" ],
         "fieldSelectionCriteria": "string",
         "filterName": "string",
         "filterPattern": "string",
         "logGroupName": "string",
         "metricTransformations": [
            {
               "defaultValue": number,
               "dimensions": {
                  "string" : "string"
               },
               "metricName": "string",
               "metricNamespace": "string",
               "metricValue": "string",
               "unit": "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.

metricFilters

The metric filters.

Type: Array of MetricFilter objects

nextToken

The token for the next set of items to return. The token expires after 24 hours.

Type: String

Length Constraints: Minimum length of 1.

Errors

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

InvalidParameterException

A parameter is specified incorrectly.

HTTP Status Code: 400

ResourceNotFoundException

The specified resource does not exist.

HTTP Status Code: 400

ServiceUnavailableException

The service cannot complete the request.

HTTP Status Code: 500

Examples

To list the metric filters for a log group

The following example lists the metric filters for the specified log group.

Sample Request

```
POST / HTTP/1.1
Host: logs.<region>.<domain>
X-Amz-Date: <DATE>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=content-
type;date;host;user-agent;x-amz-date;x-amz-target;x-amzn-requestid,
 Signature=<Signature>
```

```
User-Agent: <UserAgentString>
Accept: application/json
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Connection: Keep-Alive
X-Amz-Target: Logs_20140328.DescribeMetricFilters
{
  "logGroupName": "my-log-group"
}
```

Sample Response

```
HTTP/1.1 200 OK
x-amzn-RequestId: <RequestId>
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Date: <Date>
{
  "metricFilters": [
    {
      "applyOnTransformedLogs": true,
      "creationTime": 1396224000000,
      "filterName": "my-metric-filter",
      "filterPattern": "[ip, identity, user_id, timestamp, request, status_code,
 size]",
      "logGroupName": "my-log-group",
      "metricTransformations": [
        {
          "defaultValue": "0",
          "metricValue": "$size",
          "metricNamespace": "my-app",
          "metricName": "Volume"
         }
      ]
    }
  ]
}
```

See Also

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

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

DescribeQueries

Returns a list of CloudWatch Logs Insights queries that are scheduled, running, or have been run recently in this account. You can request all queries or limit it to queries of a specific log group or queries with a certain status.

This operation includes both interactive queries started directly by users and automated queries executed by scheduled query configurations. Scheduled query executions appear in the results alongside manually initiated queries, providing visibility into all query activity in your account.

Request Syntax

```
{
   "logGroupName": "string",
   "maxResults": number,
   "nextToken": "string",
   "queryLanguage": "string",
   "status": "string"
}
```

Request Parameters

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

The request accepts the following data in JSON format.

logGroupName

Limits the returned queries to only those for the specified log group.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `[\.\-_/#A-Za-z0-9]+`

Required: No

maxResults

Limits the number of returned queries to the specified number.

Type: Integer

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

Required: No

nextToken

The token for the next set of items to return. The token expires after 24 hours.

Type: String

Length Constraints: Minimum length of 1.

Required: No

queryLanguage

Limits the returned queries to only the queries that use the specified query language.

Type: String

Valid Values: `CWLI | SQL | PPL`

Required: No

status

Limits the returned queries to only those that have the specified status. Valid values are `Cancelled`, `Complete`, `Failed`, `Running`, and `Scheduled`.

Type: String

Valid Values: `Scheduled | Running | Complete | Failed | Cancelled | Timeout | Unknown`

Required: No

Response Syntax

```
{
   "nextToken": "string",
   "queries": [
```

```
      {
         "bytesScanned": number,
         "createTime": number,
         "logGroupName": "string",
         "queryDuration": number,
         "queryId": "string",
         "queryLanguage": "string",
         "queryString": "string",
         "status": "string",
         "userIdentity": "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 token for the next set of items to return. The token expires after 24 hours.

Type: String

Length Constraints: Minimum length of 1.

queries

The list of queries that match the request.

Type: Array of QueryInfo objects

Errors

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

InvalidParameterException

A parameter is specified incorrectly.

HTTP Status Code: 400

ResourceNotFoundException

The specified resource does not exist.

HTTP Status Code: 400

ServiceUnavailableException

The service cannot complete the request.

HTTP Status Code: 500

Examples

List the CloudWatch Logs Insights queries for a specific log group

The following example lists the successfully completed queries of the log group named `MyLogGroup`.

Sample Request

```
POST / HTTP/1.1
Host: logs.<region>.<domain>
X-Amz-Date: <DATE>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=content-
type;date;host;user-agent;x-amz-date;x-amz-target;x-amzn-requestid,
 Signature=<Signature>
User-Agent: <UserAgentString>
Accept: application/json
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Connection: Keep-Alive
X-Amz-Target: Logs_20140328.DescribeQueries
{
   "logGroupName": "MyLogGroup",
   "status": "Completed"
}
```

Sample Response

```
HTTP/1.1 200 OK
x-amzn-RequestId: <RequestId>
```

```
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Date: <Date>
{
    "nextToken": "string",
    "queries": [
        {
            "createTime": 1540923785,
            "logGroupName": "MyLogGroup",
            "queryId": "12ab3456-12ab-123a-789e-1234567890ab",
            "queryString": "filter @message like /Exception/ | stats count(*) as
 @exceptionCount by date_floor(@timestamp, 5m) | sort @exceptionCount desc",
            "status": "Completed",
            "queryDuration": 5200,
            "bytesScanned": 1048576.0,
            "userIdentity": "arn:aws:iam::123456789012:user/example-user"
        },
        {
            "createTime": 1540025601,
            "logGroupName": "MyLogGroup",
            "queryId": "98ab3456-12ab-123a-789e-1234567890ab",
            "queryString": "stats count(*) by eventSource, eventName, awsRegion",
            "status": "Running",
            "queryDuration": 1500,
            "bytesScanned": 524288.0,
            "userIdentity": "arn:aws:iam::123456789012:user/example-user"
        }
    ]
}
```

See Also

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

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3

- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

DescribeQueryDefinitions

This operation returns a paginated list of your saved CloudWatch Logs Insights query definitions. You can retrieve query definitions from the current account or from a source account that is linked to the current account.

You can use the `queryDefinitionNamePrefix` parameter to limit the results to only the query definitions that have names that start with a certain string.

Request Syntax

```
{
   "maxResults": number,
   "nextToken": "string",
   "queryDefinitionNamePrefix": "string",
   "queryLanguage": "string"
}
```

Request Parameters

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

The request accepts the following data in JSON format.

maxResults

Limits the number of returned query definitions to the specified number.

Type: Integer

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

Required: No

nextToken

The token for the next set of items to return. The token expires after 24 hours.

Type: String

Length Constraints: Minimum length of 1.

Required: No

queryDefinitionNamePrefix

Use this parameter to filter your results to only the query definitions that have names that start with the prefix you specify.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 255.

Required: No

queryLanguage

The query language used for this query. For more information about the query languages that CloudWatch Logs supports, see Supported query languages.

Type: String

Valid Values: `CWLI | SQL | PPL`

Required: No

Response Syntax

```
{
   "nextToken": "string",
   "queryDefinitions": [
      {
         "lastModified": number,
         "logGroupNames": [ "string" ],
         "name": "string",
         "parameters": [
            {
               "defaultValue": "string",
               "description": "string",
               "name": "string"
            }
         ],
         "queryDefinitionId": "string",
         "queryLanguage": "string",
         "queryString": "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 token for the next set of items to return. The token expires after 24 hours.

Type: String

Length Constraints: Minimum length of 1.

queryDefinitions

The list of query definitions that match your request.

Type: Array of QueryDefinition objects

Errors

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

InvalidParameterException

A parameter is specified incorrectly.

HTTP Status Code: 400

ServiceUnavailableException

The service cannot complete the request.

HTTP Status Code: 500

Examples

Example

This example retrieves a list of query definitions that have names that begin with `lambda`.

Sample Request

```
POST / HTTP/1.1
Host: logs.<region>.<domain>
X-Amz-Date: <DATE>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=content-
type;date;host;user-agent;x-amz-date;x-amz-target;x-amzn-requestid,
 Signature=<Signature>
User-Agent: <UserAgentString>
Accept: application/json
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Connection: Keep-Alive
X-Amz-Target: Logs_20140328.DescribeQueryDefinitions
{
   "queryDefinitionNamePrefix": "lambda",
   "maxResults": 2
}
```

Sample Response

```
HTTP/1.1 200 OK
x-amzn-RequestId: <RequestId>
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Date: <Date>
{
   "nextToken": "abdcefghijlkmn",
   "queryDefinitions": [
      {
         "lastModified": 1549321515,
         "logGroupNames": [ "VPC_Flow_Log1", "VPC_Flow_Log2" ],
         "name": "VPC-top15-packet-transfers",
         "queryDefinitionId": "123456ab-12ab-123a-789e-1234567890ab",
         "queryString": "stats sum(packets) as packetsTransferred by srcAddr, dstAddr |
 sort packetsTransferred  desc | limit 15",
         "parameters": []
      },
      {
         "lastModified": 1557321299,
         "name": "ErrorsByLevel",
         "queryDefinitionId": "456789ab-abcd-1234-789e-0987654321ab",
         "queryString": "fields @timestamp, @message | filter level = {{logLevel}}",
```

```
         "parameters": [
            {
               "name": "logLevel",
               "defaultValue": "ERROR",
               "description": "Log level to filter (ERROR, WARN, INFO, DEBUG)"
            }
         ]
      }
   ]
}
```

See Also

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

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

DescribeResourcePolicies

Lists the resource policies in this account.

Request Syntax

```
{
   "limit": number,
   "nextToken": "string",
   "policyScope": "string",
   "resourceArn": "string"
}
```

Request Parameters

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

The request accepts the following data in JSON format.

limit

The maximum number of resource policies to be displayed with one call of this API.

Type: Integer

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

Required: No

nextToken

The token for the next set of items to return. The token expires after 24 hours.

Type: String

Length Constraints: Minimum length of 1.

Required: No

policyScope

Specifies the scope of the resource policy. Valid values are ACCOUNT or RESOURCE. When not specified, defaults to ACCOUNT.

Type: String

Valid Values: ACCOUNT | RESOURCE

Required: No

resourceArn

The ARN of the CloudWatch Logs resource for which to query the resource policy.

Type: String

Required: No

Response Syntax

```
{
   "nextToken": "string",
   "resourcePolicies": [
      {
         "lastUpdatedTime": number,
         "policyDocument": "string",
         "policyName": "string",
         "policyScope": "string",
         "resourceArn": "string",
         "revisionId": "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 token for the next set of items to return. The token expires after 24 hours.

Type: String

Length Constraints: Minimum length of 1.

resourcePolicies

The resource policies that exist in this account.

Type: Array of ResourcePolicy objects

Errors

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

InvalidParameterException

A parameter is specified incorrectly.

HTTP Status Code: 400

ServiceUnavailableException

The service cannot complete the request.

HTTP Status Code: 500

See Also

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

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

DescribeSubscriptionFilters

Lists the subscription filters for the specified log group. You can list all the subscription filters or filter the results by prefix. The results are ASCII-sorted by filter name.

Request Syntax

```
{
   "filterNamePrefix": "string",
   "limit": number,
   "logGroupName": "string",
   "nextToken": "string"
}
```

Request Parameters

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

The request accepts the following data in JSON format.

filterNamePrefix

The prefix to match. If you don't specify a value, no prefix filter is applied.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `[^:*]*`

Required: No

limit

The maximum number of items returned. If you don't specify a value, the default is up to 50 items.

Type: Integer

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

Required: No

logGroupName

The name of the log group.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `[\.\-_/#A-Za-z0-9]+`

Required: Yes

nextToken

The token for the next set of items to return. (You received this token from a previous call.)

Type: String

Length Constraints: Minimum length of 1.

Required: No

Response Syntax

```
{
   "nextToken": "string",
   "subscriptionFilters": [
      {
         "applyOnTransformedLogs": boolean,
         "creationTime": number,
         "destinationArn": "string",
         "distribution": "string",
         "emitSystemFields": [ "string" ],
         "fieldSelectionCriteria": "string",
         "filterName": "string",
         "filterPattern": "string",
         "logGroupName": "string",
         "roleArn": "string"
      }
   ]
```

```
}
```

Response Elements

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

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

nextToken

The token for the next set of items to return. The token expires after 24 hours.

Type: String

Length Constraints: Minimum length of 1.

subscriptionFilters

The subscription filters.

Type: Array of SubscriptionFilter objects

Errors

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

InvalidParameterException

A parameter is specified incorrectly.

HTTP Status Code: 400

ResourceNotFoundException

The specified resource does not exist.

HTTP Status Code: 400

ServiceUnavailableException

The service cannot complete the request.

HTTP Status Code: 500

Examples

To list the subscription filters for a log group

The following example lists the subscription filters for the specified log group.

Sample Request

```
POST / HTTP/1.1
Host: logs.<region>.<domain>
X-Amz-Date: <DATE>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=content-
type;date;host;user-agent;x-amz-date;x-amz-target;x-amzn-requestid,
 Signature=<Signature>
User-Agent: <UserAgentString>
Accept: application/json
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Connection: Keep-Alive
X-Amz-Target: Logs_20140328.DescribeSubscriptionFilters
{
  "logGroupName": "my-log-group"
}
```

Sample Response

```
HTTP/1.1 200 OK
x-amzn-RequestId: <RequestId>
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Date: <Date>
{
  "subscriptionFilters": [
    {
      "creationTime": 1396224000000,
      "logGroupName": "my-log-group",
      "filterName": "my-subscription-ilter",
      "filterPattern": "[ip, identity, user_id, timestamp, request, status_code = 500,
 size]",
      "destinationArn": "arn:aws:kinesis:us-east-1:123456789012:stream/my-kinesis-
stream",
      "roleArn": "arn:aws:iam::123456789012:role/my-subscription-role"
    }
```

```
  ]
}
```

See Also

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

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

DisassociateKmsKey

Disassociates the specified AWS KMS key from the specified log group or from all CloudWatch Logs Insights query results in the account.

When you use `DisassociateKmsKey`, you specify either the `logGroupName` parameter or the `resourceIdentifier` parameter. You can't specify both of those parameters in the same operation.

- Specify the `logGroupName` parameter to stop using the AWS KMS key to encrypt future log events ingested and stored in the log group. Instead, they will be encrypted with the default CloudWatch Logs method. The log events that were ingested while the key was associated with the log group are still encrypted with that key. Therefore, CloudWatch Logs will need permissions for the key whenever that data is accessed.
- Specify the `resourceIdentifier` parameter with the `query-result` resource to stop using the AWS KMS key to encrypt the results of all future StartQuery operations in the account. They will instead be encrypted with the default CloudWatch Logs method. The results from queries that ran while the key was associated with the account are still encrypted with that key. Therefore, CloudWatch Logs will need permissions for the key whenever that data is accessed.

It can take up to 5 minutes for this operation to take effect.

Request Syntax

```
{
   "logGroupName": "string",
   "resourceIdentifier": "string"
}
```

Request Parameters

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

The request accepts the following data in JSON format.

logGroupName

The name of the log group.

In your `DisassociateKmsKey` operation, you must specify either the `resourceIdentifier` parameter or the `logGroup` parameter, but you can't specify both.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `[\.\-_/#A-Za-z0-9]+`

Required: No

resourceIdentifier

Specifies the target for this operation. You must specify one of the following:

- Specify the ARN of a log group to stop having CloudWatch Logs use the AWS KMS key to encrypt log events that are ingested and stored by that log group. After you run this operation, CloudWatch Logs encrypts ingested log events with the default CloudWatch Logs method. The log group ARN must be in the following format. Replace *REGION* and *ACCOUNT_ID* with your Region and account ID.

  `arn:aws:logs:`*`REGION`*`:`*`ACCOUNT_ID`*`:log-group:`*`LOG_GROUP_NAME`*

- Specify the following ARN to stop using this key to encrypt the results of future StartQuery operations in this account. Replace *REGION* and *ACCOUNT_ID* with your Region and account ID.

  `arn:aws:logs:`*`REGION`*`:`*`ACCOUNT_ID`*`:query-result:*`

In your `DisssociateKmsKey` operation, you must specify either the `resourceIdentifier` parameter or the `logGroup` parameter, but you can't specify both.

Type: String

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

Pattern: `[\w+=/:,.@\-\*]*`

Required: No

Response Elements

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

Errors

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

InvalidParameterException

A parameter is specified incorrectly.

HTTP Status Code: 400

OperationAbortedException

Multiple concurrent requests to update the same resource were in conflict.

HTTP Status Code: 400

ResourceNotFoundException

The specified resource does not exist.

HTTP Status Code: 400

ServiceUnavailableException

The service cannot complete the request.

HTTP Status Code: 500

Examples

To disassociate an KMS key from a log group

The following example disassociates the associated KMS key from the specified log group.

Sample Request

```
POST / HTTP/1.1
Host: logs.<region>.<domain>
X-Amz-Date: <DATE>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=content-
type;date;host;user-agent;x-amz-date;x-amz-target;x-amzn-requestid,
 Signature=<Signature>
User-Agent: <UserAgentString>
Accept: application/json
```

```
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Connection: Keep-Alive
X-Amz-Target: Logs_20140328.DisassociateKmsKey
{
  "logGroupName": "my-log-group",
}
```

Sample Response

```
HTTP/1.1 200 OK
x-amzn-RequestId: <RequestId>
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Date: <Date>
```

See Also

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

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

DisassociateSourceFromS3TableIntegration

Disassociates a data source from an S3 Table Integration, removing query access and deleting all associated data from the integration.

Request Syntax

```
{
   "identifier": "string"
}
```

Request Parameters

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

The request accepts the following data in JSON format.

identifier

The unique identifier of the association to remove between the data source and S3 Table Integration.

Type: String

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

Required: Yes

Response Syntax

```
{
   "identifier": "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.

identifier

The unique identifier of the association that was removed.

Type: String

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

Errors

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

AccessDeniedException

You don't have sufficient permissions to perform this action.

HTTP Status Code: 400

InternalServerException

An internal server error occurred while processing the request. This exception is returned when the service encounters an unexpected condition that prevents it from fulfilling the request.

HTTP Status Code: 500

ResourceNotFoundException

The specified resource does not exist.

HTTP Status Code: 400

ThrottlingException

The request was throttled because of quota limits.

HTTP Status Code: 400

ValidationException

One of the parameters for the request is not valid.

HTTP Status Code: 400

See Also

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

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

FilterLogEvents

Lists log events from the specified log group. You can list all the log events or filter the results using one or more of the following:

- A filter pattern
- A time range
- The log stream name, or a log stream name prefix that matches multiple log streams

You must have the `logs:FilterLogEvents` permission to perform this operation.

You can specify the log group to search by using either `logGroupIdentifier` or `logGroupName`. You must include one of these two parameters, but you can't include both.

`FilterLogEvents` is a paginated operation. Each page returned can contain up to 1 MB of log events or up to 10,000 log events. A returned page might only be partially full, or even empty. For example, if the result of a query would return 15,000 log events, the first page isn't guaranteed to have 10,000 log events even if they all fit into 1 MB.

Partially full or empty pages don't necessarily mean that pagination is finished. If the results include a `nextToken`, there might be more log events available. You can return these additional log events by providing the nextToken in a subsequent `FilterLogEvents` operation. If the results don't include a `nextToken`, then pagination is finished.

Specifying the `limit` parameter only guarantees that a single page doesn't return more log events than the specified limit, but it might return fewer events than the limit. This is the expected API behavior.

The returned log events are sorted by event timestamp, the timestamp when the event was ingested by CloudWatch Logs, and the ID of the `PutLogEvents` request. By default, the events are returned in ascending timestamp order (oldest first). To return events in descending timestamp order (newest first), set the `startFromHead` parameter to `false`.

If you are using CloudWatch cross-account observability, you can use this operation in a monitoring account and view data from the linked source accounts. For more information, see CloudWatch cross-account observability.

Note

If you are using log transformation, the `FilterLogEvents` operation returns only the original versions of log events, before they were transformed. To view the transformed versions, you must use a CloudWatch Logs query.

Request Syntax

```
{
   "endTime": number,
   "filterPattern": "string",
   "interleaved": boolean,
   "limit": number,
   "logGroupIdentifier": "string",
   "logGroupName": "string",
   "logStreamNamePrefix": "string",
   "logStreamNames": [ "string" ],
   "nextToken": "string",
   "startFromHead": boolean,
   "startTime": number,
   "unmask": boolean
}
```

Request Parameters

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

The request accepts the following data in JSON format.

endTime

The end of the time range, expressed as the number of milliseconds after `Jan 1, 1970 00:00:00` UTC. Events with a timestamp later than this time are not returned.

Type: Long

Valid Range: Minimum value of 0.

Required: No

filterPattern

The filter pattern to use. For more information, see Filter and Pattern Syntax.

If not provided, all the events are matched.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 1024.

Required: No

interleaved

This parameter has been deprecated.

If the value is true, the operation attempts to provide responses that contain events from multiple log streams within the log group, interleaved in a single response. If the value is false, all the matched log events in the first log stream are searched first, then those in the next log stream, and so on.

Important As of June 17, 2019, this parameter is ignored and the value is assumed to be true. The response from this operation always interleaves events from multiple log streams within a log group.

Type: Boolean

Required: No

limit

The maximum number of events to return. The default is 10,000 events.

Type: Integer

Valid Range: Minimum value of 1. Maximum value of 10000.

Required: No

logGroupIdentifier

Specify either the name or ARN of the log group to view log events from. If the log group is in a source account and you are using a monitoring account, you must use the log group ARN.

> **Note**
>
> You must include either `logGroupIdentifier` or `logGroupName`, but not both.

Type: String

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

Pattern: `[\w#+=/:,.@-]*`

Required: No

logGroupName

The name of the log group to search.

> **Note**
>
> You must include either `logGroupIdentifier` or `logGroupName`, but not both.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `[\.\-_/#A-Za-z0-9]+`

Required: No

logStreamNamePrefix

Filters the results to include only events from log streams that have names starting with this prefix.

If you specify a value for both `logStreamNamePrefix` and `logStreamNames`, the action returns an `InvalidParameterException` error.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `[^:*]*`

Required: No

logStreamNames

Filters the results to only logs from the log streams in this list.

If you specify a value for both `logStreamNames` and `logStreamNamePrefix`, the action returns an `InvalidParameterException` error.

Type: Array of strings

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

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `[^:*]*`

Required: No

nextToken

The token for the next set of events to return. (You received this token from a previous call.)

Type: String

Length Constraints: Minimum length of 1.

Required: No

startFromHead

If the value is true, the earliest log events are returned first. If the value is false, the latest log events are returned first. The default value is true.

The `startFromHead` parameter sets the sort direction on the first request. On subsequent requests, the `nextToken` determines the sort direction. To continue paginating in the same direction, provide the returned `nextToken`. If you provide both `nextToken` and `startFromHead`, the direction of the `nextToken` is used.

> **Note**
>
> Setting `startFromHead` to `false` is supported only when `startTime` is on or after `Jan 1, 2024 00:00:00` UTC. A request with `startFromHead` set to `false` and a `startTime` before this date returns an `InvalidParameterException`.

Type: Boolean

Required: No

startTime

The start of the time range, expressed as the number of milliseconds after `Jan 1, 1970 00:00:00` UTC. Events with a timestamp before this time are not returned.

> **Note**
>
> Set `startTime` explicitly to reduce the chances of empty pages in the response.

Type: Long

Valid Range: Minimum value of 0.

Required: No

unmask

Specify `true` to display the log event fields with all sensitive data unmasked and visible. The default is `false`.

To use this operation with this parameter, you must be signed into an account with the `logs:Unmask` permission.

Type: Boolean

Required: No

Response Syntax

```
{
   "events": [
      {
         "eventId": "string",
         "ingestionTime": number,
         "logStreamName": "string",
         "message": "string",
         "timestamp": number
      }
   ],
   "nextToken": "string",
```

```
   "searchedLogStreams": [
      {
         "logStreamName": "string",
         "searchedCompletely": boolean
      }
   ]
}
```

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.

events

The matched events.

Type: Array of FilteredLogEvent objects

nextToken

The token for the next set of items in the sorting direction specified by the `startFromHead` parameter in the first request. The token expires after 24 hours.

If the results don't include a `nextToken`, then pagination is finished.

Type: String

Length Constraints: Minimum length of 1.

searchedLogStreams

Important As of May 15, 2020, this parameter is no longer supported. This parameter returns an empty list.

Indicates which log streams have been searched and whether each has been searched completely.

Type: Array of SearchedLogStream objects

Errors

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

InvalidParameterException

A parameter is specified incorrectly.

HTTP Status Code: 400

ResourceNotFoundException

The specified resource does not exist.

HTTP Status Code: 400

ServiceUnavailableException

The service cannot complete the request.

HTTP Status Code: 500

Examples

To list the events in a log group that contain a pattern

The following example lists the events for the specified log group that contain ERROR.

Sample Request

```
POST / HTTP/1.1
Host: logs.<region>.<domain>
X-Amz-Date: <DATE>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=content-
type;date;host;user-agent;x-amz-date;x-amz-target;x-amzn-requestid,
 Signature=<Signature>
User-Agent: <UserAgentString>
Accept: application/json
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Connection: Keep-Alive
X-Amz-Target: Logs_20140328.FilterLogEvents
{
  "logGroupName": "my-log-group",
  "filterPattern": "ERROR"
}
```

Sample Response

```
HTTP/1.1 200 OK
x-amzn-RequestId: <RequestId>
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Date: <Date>
{
  "events": [
    {
      "ingestionTime": 1396035394997,
      "timestamp": 1396035378988,
      "message": "ERROR Event 1",
      "logStreamName": "my-log-stream-1",
      "eventId": "31132629274945519779805322857203735586714454643391594505"
    },
    {
      "ingestionTime": 1396035394997,
      "timestamp": 1396035378988,
      "message": "ERROR Event 2",
      "logStreamName": "my-log-stream-2",
      "eventId": "31132629274945519779805322857203735586814454643391594505"
    },
    {
      "ingestionTime": 1396035394997,
      "timestamp": 1396035378989,
      "message": "ERROR Event 3",
      "logStreamName": "my-log-stream-3"
      "eventId": "31132629274945519779805322857203735586824454643391594505"
    }
  ],
  "searchedLogStreams": [
    {
      "searchedCompletely": true,
      "logStreamName": "my-log-stream-1"
    },
    {
      "searchedCompletely": true,
      "logStreamName": "my-log-stream-2"
    },
    {
      "searchedCompletely": false,
      "logStreamName": "my-log-stream-3"
    },
```

```
  ],
  "nextToken": "ZNUEPl7FcQuXbIH4Swk9D9eFu2XBg-ijZIZlvzz4ea9zZRjw-
MMtQtvcoMdmq4T29K7Q6Y1e_KvyfpcT_f_tUw"
}
```

Example

The following example lists the events for the specified log group that contain ERROR.

Sample Request

```
{
  "logGroupIdentifier": "arn:aws:logs:us-east-1:123456789012:log-group:monitoring-
logGroup-1234:*",
  "filterPattern": "ERROR"
}
```

Sample Response

```
{
  "events": [
  {
      "ingestionTime": 1396035394997,
      "timestamp": 1396035378988,
      "message": "ERROR Event 1",
      "logStreamName": "my-log-stream-1",
      "eventId": "31132629274945519779805322857203735586714454643391594505"
  },
  {
     "ingestionTime": 1396035394997,
      "timestamp": 1396035378988,
      "message": "ERROR Event 2",
      "logStreamName": "my-log-stream-2",
      "eventId": "31132629274945519779805322857203735586814454643391594505"
  },
  {
      "ingestionTime": 1396035394997,
      "timestamp": 1396035378989,
      "message": "ERROR Event 3",
      "logStreamName": "my-log-stream-3"
      "eventId": "31132629274945519779805322857203735586824454643391594505"
   } ],
```

```
   "searchedLogStreams": [
   {
      "searchedCompletely": true,
      "logStreamName": "my-log-stream-1"
    },
    {
      "searchedCompletely": true,
      "logStreamName": "my-log-stream-2"
    },
    {
      "searchedCompletely": false,
      "logStreamName": "my-log-stream-3"
    }
    ],
    "nextToken": "ZNUEPl7FcQuXbIH4Swk9D9eFu2XBg-ijZIZlvzz4ea9zZRjw-
MMtQtvcoMdmq4T29K7Q6Y1e_KvyfpcT_f_tUw"
}
```

To list the most recent events in a log group in reverse order

The following example lists the most recent events for the specified log group that contain ERROR, returned in descending timestamp order (newest first).

Sample Request

```
POST / HTTP/1.1
Host: logs.<region>.<domain>
X-Amz-Date: <DATE>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=content-
type;date;host;user-agent;x-amz-date;x-amz-target;x-amzn-requestid,
 Signature=<Signature>
User-Agent: <UserAgentString>
Accept: application/json
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Connection: Keep-Alive
X-Amz-Target: Logs_20140328.FilterLogEvents
{
  "logGroupName": "my-log-group",
  "filterPattern": "ERROR",
  "startFromHead": false,
  "limit": 100
}
```

Sample Response

```
HTTP/1.1 200 OK
x-amzn-RequestId: <RequestId>
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Date: <Date>
{
  "events": [
    {
      "ingestionTime": 1396035394997,
      "timestamp": 1396035378989,
      "message": "ERROR Event 3",
      "logStreamName": "my-log-stream-3",
      "eventId": "31132629274945519779805322857203735586824454643391594505"
    },
    {
      "ingestionTime": 1396035394997,
      "timestamp": 1396035378988,
      "message": "ERROR Event 2",
      "logStreamName": "my-log-stream-2",
      "eventId": "31132629274945519779805322857203735586814454643391594505"
    },
    {
      "ingestionTime": 1396035394997,
      "timestamp": 1396035378988,
      "message": "ERROR Event 1",
      "logStreamName": "my-log-stream-1",
      "eventId": "31132629274945519779805322857203735586714454643391594505"
    }
  ],
  "nextToken": "eJxExampleTokenwjR"
}
```

See Also

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

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++

- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

GetDataProtectionPolicy

Returns information about a log group data protection policy.

Request Syntax

```
{
   "logGroupIdentifier": "string"
}
```

Request Parameters

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

The request accepts the following data in JSON format.

logGroupIdentifier

The name or ARN of the log group that contains the data protection policy that you want to see.

Type: String

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

Pattern: `[\w#+=/:,.@-]*`

Required: Yes

Response Syntax

```
{
   "lastUpdatedTime": number,
   "logGroupIdentifier": "string",
   "policyDocument": "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.

lastUpdatedTime

The date and time that this policy was most recently updated.

Type: Long

Valid Range: Minimum value of 0.

logGroupIdentifier

The log group name or ARN that you specified in your request.

Type: String

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

Pattern: `[\w#+=/:,.@-]*`

policyDocument

The data protection policy document for this log group.

Type: String

Errors

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

InvalidParameterException

A parameter is specified incorrectly.

HTTP Status Code: 400

OperationAbortedException

Multiple concurrent requests to update the same resource were in conflict.

HTTP Status Code: 400

ResourceNotFoundException

The specified resource does not exist.

HTTP Status Code: 400

ServiceUnavailableException

The service cannot complete the request.

HTTP Status Code: 500

See Also

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

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

GetDelivery

Returns complete information about one logical *delivery*. A delivery is a connection between a *delivery source* and a *delivery destination*.

A delivery source represents an AWS resource that sends logs to an logs delivery destination. The destination can be CloudWatch Logs, Amazon S3, or Firehose. Only some AWS services support being configured as a delivery source. These services are listed in Enable logging from AWS services.

You need to specify the delivery `id` in this operation. You can find the IDs of the deliveries in your account with the DescribeDeliveries operation.

Request Syntax

```
{
   "id": "string"
}
```

Request Parameters

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

The request accepts the following data in JSON format.

id

The ID of the delivery that you want to retrieve.

Type: String

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

Pattern: `^[0-9A-Za-z]+$`

Required: Yes

Response Syntax

```
{
```

```
   "delivery": {
      "arn": "string",
      "deliveryDestinationArn": "string",
      "deliveryDestinationType": "string",
      "deliverySourceName": "string",
      "fieldDelimiter": "string",
      "id": "string",
      "recordFields": [ "string" ],
      "s3DeliveryConfiguration": {
         "enableHiveCompatiblePath": boolean,
         "suffixPath": "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.

delivery

A structure that contains information about the delivery.

Type: Delivery object

Errors

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

ResourceNotFoundException

The specified resource does not exist.

HTTP Status Code: 400

ServiceQuotaExceededException

This request exceeds a service quota.

HTTP Status Code: 400

ServiceUnavailableException

The service cannot complete the request.

HTTP Status Code: 500

ThrottlingException

The request was throttled because of quota limits.

HTTP Status Code: 400

ValidationException

One of the parameters for the request is not valid.

HTTP Status Code: 400

See Also

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

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

GetDeliveryDestination

Retrieves complete information about one delivery destination.

Request Syntax

```
{
   "name": "string"
}
```

Request Parameters

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

The request accepts the following data in JSON format.

name

The name of the delivery destination that you want to retrieve.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 60.

Pattern: `[\w-]*`

Required: Yes

Response Syntax

```
{
   "deliveryDestination": {
      "arn": "string",
      "deliveryDestinationConfiguration": {
         "destinationResourceArn": "string"
      },
      "deliveryDestinationType": "string",
      "name": "string",
      "outputFormat": "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.

deliveryDestination

A structure containing information about the delivery destination.

Type: DeliveryDestination object

Errors

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

ResourceNotFoundException

The specified resource does not exist.

HTTP Status Code: 400

ServiceQuotaExceededException

This request exceeds a service quota.

HTTP Status Code: 400

ServiceUnavailableException

The service cannot complete the request.

HTTP Status Code: 500

ThrottlingException

The request was throttled because of quota limits.

HTTP Status Code: 400

ValidationException

One of the parameters for the request is not valid.

HTTP Status Code: 400

See Also

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

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

GetDeliveryDestinationPolicy

Retrieves the delivery destination policy assigned to the delivery destination that you specify. For more information about delivery destinations and their policies, see PutDeliveryDestinationPolicy.

Request Syntax

```
{
   "deliveryDestinationName": "string"
}
```

Request Parameters

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

The request accepts the following data in JSON format.

deliveryDestinationName

The name of the delivery destination that you want to retrieve the policy of.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 60.

Pattern: `[\w-]*`

Required: Yes

Response Syntax

```
{
   "policy": {
      "deliveryDestinationPolicy": "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.

policy

The IAM policy for this delivery destination.

Type: Policy object

Errors

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

ResourceNotFoundException

The specified resource does not exist.

HTTP Status Code: 400

ServiceUnavailableException

The service cannot complete the request.

HTTP Status Code: 500

ValidationException

One of the parameters for the request is not valid.

HTTP Status Code: 400

See Also

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

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3

- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

GetDeliverySource

Retrieves complete information about one delivery source.

Request Syntax

```
{
   "name": "string"
}
```

Request Parameters

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

The request accepts the following data in JSON format.

name

The name of the delivery source that you want to retrieve.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 60.

Pattern: `[\w-]*`

Required: Yes

Response Syntax

```
{
   "deliverySource": {
      "arn": "string",
      "deliverySourceConfiguration": {
         "string" : "string"
      },
      "logType": "string",
      "name": "string",
      "resourceArns": [ "string" ],
      "service": "string",
      "status": "string",
```

```
      "statusReason": "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.

deliverySource

A structure containing information about the delivery source.

Type: DeliverySource object

Errors

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

ResourceNotFoundException

The specified resource does not exist.

HTTP Status Code: 400

ServiceQuotaExceededException

This request exceeds a service quota.

HTTP Status Code: 400

ServiceUnavailableException

The service cannot complete the request.

HTTP Status Code: 500

ThrottlingException

The request was throttled because of quota limits.

HTTP Status Code: 400

ValidationException

One of the parameters for the request is not valid.

HTTP Status Code: 400

See Also

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

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

GetIntegration

Returns information about one integration between CloudWatch Logs and OpenSearch Service.

Request Syntax

```
{
   "integrationName": "string"
}
```

Request Parameters

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

The request accepts the following data in JSON format.

integrationName

The name of the integration that you want to find information about. To find the name of your integration, use ListIntegrations

Type: String

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

Pattern: `[\.\-_/#A-Za-z0-9]+`

Required: Yes

Response Syntax

```
{
   "integrationDetails": { ... },
   "integrationName": "string",
   "integrationStatus": "string",
   "integrationType": "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.

integrationDetails

A structure that contains information about the integration configuration. For an integration with OpenSearch Service, this includes information about OpenSearch Service resources such as the collection, the workspace, and policies.

Type: IntegrationDetails object

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

integrationName

The name of the integration.

Type: String

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

Pattern: `[\.\-_/#A-Za-z0-9]+`

integrationStatus

The current status of this integration.

Type: String

Valid Values: `PROVISIONING | ACTIVE | FAILED`

integrationType

The type of integration. Integrations with OpenSearch Service have the type `OPENSEARCH`.

Type: String

Valid Values: `OPENSEARCH`

Errors

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

InvalidParameterException

A parameter is specified incorrectly.

HTTP Status Code: 400

ResourceNotFoundException

The specified resource does not exist.

HTTP Status Code: 400

ServiceUnavailableException

The service cannot complete the request.

HTTP Status Code: 500

See Also

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

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

GetLogAnomalyDetector

Retrieves information about the log anomaly detector that you specify. The AWS KMS key ARN detected is valid.

Request Syntax

```
{
   "anomalyDetectorArn": "string"
}
```

Request Parameters

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

The request accepts the following data in JSON format.

anomalyDetectorArn

The ARN of the anomaly detector to retrieve information about. You can find the ARNs of log anomaly detectors in your account by using the ListLogAnomalyDetectors operation.

Type: String

Length Constraints: Minimum length of 1.

Pattern: `[\w#+=/:,.@-]*`

Required: Yes

Response Syntax

```
{
   "anomalyDetectorStatus": "string",
   "anomalyVisibilityTime": number,
   "creationTimeStamp": number,
   "detectorName": "string",
   "evaluationFrequency": "string",
   "filterPattern": "string",
   "kmsKeyId": "string",
```

```
    "lastModifiedTimeStamp": number,
    "logGroupArnList": [ "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.

anomalyDetectorStatus

Specifies whether the anomaly detector is currently active. To change its status, use the `enabled` parameter in the UpdateLogAnomalyDetector operation.

Type: String

Valid Values: `INITIALIZING | TRAINING | ANALYZING | FAILED | DELETED | PAUSED`

anomalyVisibilityTime

The number of days used as the life cycle of anomalies. After this time, anomalies are automatically baselined and the anomaly detector model will treat new occurrences of similar event as normal.

Type: Long

Valid Range: Minimum value of 7. Maximum value of 90.

creationTimeStamp

The date and time when this anomaly detector was created.

Type: Long

Valid Range: Minimum value of 0.

detectorName

The name of the log anomaly detector

Type: String

Length Constraints: Minimum length of 1.

evaluationFrequency

Specifies how often the anomaly detector runs and look for anomalies. Set this value according to the frequency that the log group receives new logs. For example, if the log group receives new log events every 10 minutes, then setting `evaluationFrequency` to `FIFTEEN_MIN` might be appropriate.

Type: String

Valid Values: `ONE_MIN | FIVE_MIN | TEN_MIN | FIFTEEN_MIN | THIRTY_MIN | ONE_HOUR`

filterPattern

A symbolic description of how CloudWatch Logs should interpret the data in each log event. For example, a log event can contain timestamps, IP addresses, strings, and so on. You use the filter pattern to specify what to look for in the log event message.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 1024.

kmsKeyId

The ARN of the AWS KMS key assigned to this anomaly detector, if any.

Type: String

Length Constraints: Maximum length of 256.

lastModifiedTimeStamp

The date and time when this anomaly detector was most recently modified.

Type: Long

Valid Range: Minimum value of 0.

logGroupArnList

An array of structures, where each structure contains the ARN of a log group associated with this anomaly detector.

Type: Array of strings

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

Pattern: `[\w#+=/:,.@-]*`

Errors

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

InvalidParameterException

A parameter is specified incorrectly.

HTTP Status Code: 400

OperationAbortedException

Multiple concurrent requests to update the same resource were in conflict.

HTTP Status Code: 400

ResourceNotFoundException

The specified resource does not exist.

HTTP Status Code: 400

ServiceUnavailableException

The service cannot complete the request.

HTTP Status Code: 500

See Also

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

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2

- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

GetLogEvents

Lists log events from the specified log stream. You can list all of the log events or filter using a time range.

`GetLogEvents` is a paginated operation. Each page returned can contain up to 1 MB of log events or up to 10,000 log events. A returned page might only be partially full, or even empty. For example, if the result of a query would return 15,000 log events, the first page isn't guaranteed to have 10,000 log events even if they all fit into 1 MB.

Partially full or empty pages don't necessarily mean that pagination is finished. As long as the `nextBackwardToken` or `nextForwardToken` returned is NOT equal to the `nextToken` that you passed into the API call, there might be more log events available. The token that you use depends on the direction you want to move in along the log stream. The returned tokens are never null.

> **Note**
>
> If you set `startFromHead` to `true` and you don't include `endTime` in your request, you can end up in a situation where the pagination doesn't terminate. This can happen when the new log events are being added to the target log streams faster than they are being read. This situation is a good use case for the CloudWatch Logs Live Tail feature.

If you are using CloudWatch cross-account observability, you can use this operation in a monitoring account and view data from the linked source accounts. For more information, see CloudWatch cross-account observability.

You can specify the log group to search by using either `logGroupIdentifier` or `logGroupName`. You must include one of these two parameters, but you can't include both.

> **Note**
>
> If you are using log transformation, the `GetLogEvents` operation returns only the original versions of log events, before they were transformed. To view the transformed versions, you must use a CloudWatch Logs query.

Request Syntax

```
{
   "endTime": number,
   "limit": number,
   "logGroupIdentifier": "string",
   "logGroupName": "string",
   "logStreamName": "string",
   "nextToken": "string",
   "startFromHead": boolean,
   "startTime": number,
   "unmask": boolean
}
```

Request Parameters

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

The request accepts the following data in JSON format.

endTime

The end of the time range, expressed as the number of milliseconds after `Jan 1, 1970 00:00:00` UTC. Events with a timestamp equal to or later than this time are not included.

Type: Long

Valid Range: Minimum value of 0.

Required: No

limit

The maximum number of log events returned. If you don't specify a limit, the default is as many log events as can fit in a response size of 1 MB (up to 10,000 log events).

Type: Integer

Valid Range: Minimum value of 1. Maximum value of 10000.

Required: No

logGroupIdentifier

Specify either the name or ARN of the log group to view events from. If the log group is in a source account and you are using a monitoring account, you must use the log group ARN.

> **Note**
>
> You must include either `logGroupIdentifier` or `logGroupName`, but not both.

Type: String

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

Pattern: `[\w#+=/:,.@-]*`

Required: No

logGroupName

The name of the log group.

> **Note**
>
> You must include either `logGroupIdentifier` or `logGroupName`, but not both.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `[\.\-_/#A-Za-z0-9]+`

Required: No

logStreamName

The name of the log stream.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `[^:*]*`

Required: Yes

nextToken

The token for the next set of items to return. (You received this token from a previous call.)

Type: String

Length Constraints: Minimum length of 1.

Required: No

startFromHead

If the value is true, the earliest log events are returned first. If the value is false, the latest log events are returned first. The default value is false.

If you are using a previous `nextForwardToken` value as the `nextToken` in this operation, you must specify `true` for `startFromHead`.

Type: Boolean

Required: No

startTime

The start of the time range, expressed as the number of milliseconds after `Jan 1, 1970 00:00:00 UTC`. Events with a timestamp equal to this time or later than this time are included. Events with a timestamp earlier than this time are not included.

> **Note**
>
> Set `startTime` explicitly to reduce the chances of empty pages in the response.

Type: Long

Valid Range: Minimum value of 0.

Required: No

unmask

Specify `true` to display the log event fields with all sensitive data unmasked and visible. The default is `false`.

To use this operation with this parameter, you must be signed into an account with the `logs:Unmask` permission.

Type: Boolean

Required: No

Response Syntax

```
{
   "events": [
      {
         "ingestionTime": number,
         "message": "string",
         "timestamp": number
      }
   ],
   "nextBackwardToken": "string",
   "nextForwardToken": "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.

events

The events.

Type: Array of OutputLogEvent objects

nextBackwardToken

The token for the next set of items in the backward direction. The token expires after 24 hours. This token is not null. If you have reached the end of the stream, it returns the same token you passed in.

Type: String

Length Constraints: Minimum length of 1.

nextForwardToken

The token for the next set of items in the forward direction. The token expires after 24 hours. If you have reached the end of the stream, it returns the same token you passed in.

Type: String

Length Constraints: Minimum length of 1.

Errors

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

InvalidParameterException

A parameter is specified incorrectly.

HTTP Status Code: 400

ResourceNotFoundException

The specified resource does not exist.

HTTP Status Code: 400

ServiceUnavailableException

The service cannot complete the request.

HTTP Status Code: 500

Examples

To list all the events for a log stream

The following example lists all events for the specified log stream.

Sample Request

```
POST / HTTP/1.1
Host: logs.<region>.<domain>
```

```
X-Amz-Date: <DATE>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=content-
type;date;host;user-agent;x-amz-date;x-amz-target;x-amzn-requestid,
 Signature=<Signature>
User-Agent: <UserAgentString>
Accept: application/json
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Connection: Keep-Alive
X-Amz-Target: Logs_20140328.GetLogEvents
{
  "logGroupName": "my-log-group",
  "logStreamName": "my-log-stream"
}
```

Sample Response

```
HTTP/1.1 200 OK
x-amzn-RequestId: <RequestId>
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Date: <Date>
{
  "events": [
    {
      "ingestionTime": 1396035394997,
      "timestamp": 1396035378988,
      "message": "Example event 1"
    },
    {
      "ingestionTime": 1396035394997,
      "timestamp": 1396035378988,
      "message": "Example event 2"
    },
    {
      "ingestionTime": 1396035394997,
      "timestamp": 1396035378989,
      "message": "Example event 3"
    }
  ],
  "nextBackwardToken": "b/31132629274945519779805322857203735586714454643391594505",
  "nextForwardToken": "f/31132629323784151764587387538205132201699397759403884544"
}
```

Example

The following example lists all events for the specified log stream.

Sample Request

```
{
  "logGroupIdentifier": "arn:aws:logs:us-east-1:123456789012:log-group:monitoring-
logGroup-1234:*",
  "logStreamName": "my-log-stream"
}
```

Sample Response

```
{
    "events": [
    {
      "ingestionTime": 1396035394997,
      "timestamp": 1396035378988,
      "message": "Example event 1"
    },
    {
      "ingestionTime": 1396035394997,
      "timestamp": 1396035378988,
      "message": "Example event 2"
    },
    {
      "ingestionTime": 1396035394997,
      "timestamp": 1396035378989,
      "message": "Example event 3"
    } ],
    "nextBackwardToken": "b/31132629274945519779805322857203735586714454643391594505",
    "nextForwardToken": "f/31132629323784151764587387538205132201699397759403884544"
}
```

See Also

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

- AWS Command Line Interface V2
- AWS SDK for .NET V4

- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

GetLogFields

Discovers available fields for a specific data source and type. The response includes any field modifications introduced through pipelines, such as new fields or changed field types.

Request Syntax

```
{
   "dataSourceName": "string",
   "dataSourceType": "string"
}
```

Request Parameters

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

The request accepts the following data in JSON format.

dataSourceName

The name of the data source to retrieve log fields for.

Type: String

Required: Yes

dataSourceType

The type of the data source to retrieve log fields for.

Type: String

Required: Yes

Response Syntax

```
{
   "logFields": [
      {
         "logFieldName": "string",
         "logFieldType": {
```

```
            "element": "LogFieldType",
            "fields": [
               "LogFieldsListItem"
            ],
            "type": "string"
         }
      }
   ]
}
```

Response Elements

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

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

logFields

The list of log fields for the specified data source, including field names and their data types.

Type: Array of LogFieldsListItem objects

Errors

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

InvalidParameterException

A parameter is specified incorrectly.

HTTP Status Code: 400

OperationAbortedException

Multiple concurrent requests to update the same resource were in conflict.

HTTP Status Code: 400

ResourceNotFoundException

The specified resource does not exist.

HTTP Status Code: 400

ServiceUnavailableException

The service cannot complete the request.

HTTP Status Code: 500

See Also

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

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

GetLogGroupFields

Returns a list of the fields that are included in log events in the specified log group. Includes the percentage of log events that contain each field. The search is limited to a time period that you specify.

This operation is used for discovering fields within log group events. For discovering fields across data sources, use the GetLogFields operation.

You can specify the log group to search by using either `logGroupIdentifier` or `logGroupName`. You must specify one of these parameters, but you can't specify both.

In the results, fields that start with @ are fields generated by CloudWatch Logs. For example, `@timestamp` is the timestamp of each log event. For more information about the fields that are generated by CloudWatch logs, see Supported Logs and Discovered Fields.

The response results are sorted by the frequency percentage, starting with the highest percentage.

If you are using CloudWatch cross-account observability, you can use this operation in a monitoring account and view data from the linked source accounts. For more information, see CloudWatch cross-account observability.

Request Syntax

```
{
   "logGroupIdentifier": "string",
   "logGroupName": "string",
   "time": number
}
```

Request Parameters

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

The request accepts the following data in JSON format.

logGroupIdentifier

Specify either the name or ARN of the log group to view. If the log group is in a source account and you are using a monitoring account, you must specify the ARN.

> **Note**
>
> You must include either `logGroupIdentifier` or `logGroupName`, but not both.

Type: String

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

Pattern: `[\w#+=/:,.@-]*`

Required: No

logGroupName

The name of the log group to search.

> **Note**
>
> You must include either `logGroupIdentifier` or `logGroupName`, but not both.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `[\.\-_/#A-Za-z0-9]+`

Required: No

time

The time to set as the center of the query. If you specify `time`, the 8 minutes before and 8 minutes after this time are searched. If you omit `time`, the most recent 15 minutes up to the current time are searched.

The `time` value is specified as epoch time, which is the number of seconds since `January 1, 1970, 00:00:00 UTC`.

Type: Long

Valid Range: Minimum value of 0.

Required: No

Response Syntax

```
{
   "logGroupFields": [
      {
         "name": "string",
         "percent": 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.

logGroupFields

The array of fields found in the query. Each object in the array contains the name of the field, along with the percentage of time it appeared in the log events that were queried.

Type: Array of LogGroupField objects

Errors

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

InvalidParameterException

A parameter is specified incorrectly.

HTTP Status Code: 400

LimitExceededException

You have reached the maximum number of resources that can be created.

HTTP Status Code: 400

ResourceNotFoundException

The specified resource does not exist.

HTTP Status Code: 400

ServiceUnavailableException

The service cannot complete the request.

HTTP Status Code: 500

Examples

Retrieve fields found in log events in a log group

The following example lists the log events and how often they occur in `MyLogGroup` for the 15 minutes before November 1, 2018, 00:00:00UTC.

Sample Request

```
POST / HTTP/1.1
Host: logs.<region>.<domain>
X-Amz-Date: <DATE>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=content-
type;date;host;user-agent;x-amz-date;x-amz-target;x-amzn-requestid,
 Signature=<Signature>
User-Agent: <UserAgentString>
Accept: application/json
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Connection: Keep-Alive
X-Amz-Target: Logs_20140328.GetLogGroupFields
{
   "logGroupName": "MyLogGroup",
   "time": 1541030400
}
```

Sample Response

```
HTTP/1.1 200 OK
x-amzn-RequestId: <RequestId>
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Date: <Date>
{
```

```
    "logGroupFields": [
        {
            "name": "@timestamp",
            "percent": 100
        },
        {
            "name": "@message",
            "percent": 100
        },
        {
            "name": "@logStream",
            "percent": 100
        },
        {
            "name": "type",
            "percent": 57
        },
        {
            "name": "duration",
            "percent": 13
        }
    ]
}
```

Example

The following example lists the log events and how often they occur in `MyLogGroup` for the 15 minutes before November 1, 2018, 00:00:00UTC.

Sample Request

```
{
  "logGroupIdentifier": "arn:aws:logs:us-east-1:123456789012:log-group:monitoring-
logGroup-1234:*",
  "time": 1541030400
}
```

Sample Response

```
{
    "logGroupFields": [
    {
```

```
         "name": "@timestamp",
         "percent": 100
    },
    {
      "name": "@message",
      "percent": 100
    },
    {
       "name": "@logStream",
       "percent": 100
    },
    {
       "name": "type",
       "percent": 57
    },
    {
       "name": "duration",
       "percent": 13
   }
] }
```

See Also

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

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

GetLogObject

Retrieves a large logging object (LLO) and streams it back. This API is used to fetch the content of large portions of log events that have been ingested through the PutOpenTelemetryLogs API. When log events contain fields that would cause the total event size to exceed 1MB, CloudWatch Logs automatically processes up to 10 fields, starting with the largest fields. Each field is truncated as needed to keep the total event size as close to 1MB as possible. The excess portions are stored as Large Log Objects (LLOs) and these fields are processed separately and LLO reference system fields (in the format `@ptr.$[path.to.field]`) are added. The path in the reference field reflects the original JSON structure where the large field was located. For example, this could be `@ptr.$['input']['message']`, `@ptr.$['AAA']['BBB']['CCC']['DDD']`, `@ptr.$['AAA']`, or any other path matching your log structure.

> **Note**
>
> The `GetLogObject` API routes requests using SDK host prefix injection. SDK versions released before April 1, 2026 route to `streaming-logs.`*`Region`*`.amazonaws.com`, which does not support VPC endpoints. SDK versions released on or after April 1, 2026 route to `stream-logs.`*`Region`*`.amazonaws.com`, which supports VPC endpoints. To set up a VPC endpoint for this API, see Creating a VPC endpoint for CloudWatch Logs .

Request Syntax

```
{
   "logObjectPointer": "string",
   "unmask": boolean
}
```

Request Parameters

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

The request accepts the following data in JSON format.

logObjectPointer

A pointer to the specific log object to retrieve. This is a required parameter that uniquely identifies the log object within CloudWatch Logs. The pointer is typically obtained from a previous query or filter operation.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Required: Yes

unmask

A boolean flag that indicates whether to unmask sensitive log data. When set to true, any masked or redacted data in the log object will be displayed in its original form. Default is false.

Type: Boolean

Required: No

Response Syntax

```
{
   "fieldStream": {
      "fields": {
         "data": blob
      },
      "InternalStreamingException": {
      }
   }
}
```

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.

fieldStream

A stream of structured log data returned by the GetLogObject operation. This stream contains log events with their associated metadata and extracted fields.

Type: GetLogObjectResponseStream object

Errors

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

AccessDeniedException

You don't have sufficient permissions to perform this action.

HTTP Status Code: 400

InvalidOperationException

The operation is not valid on the specified resource.

HTTP Status Code: 400

InvalidParameterException

A parameter is specified incorrectly.

HTTP Status Code: 400

LimitExceededException

You have reached the maximum number of resources that can be created.

HTTP Status Code: 400

ResourceNotFoundException

The specified resource does not exist.

HTTP Status Code: 400

See Also

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

- AWS Command Line Interface V2
- AWS SDK for .NET V4

- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

GetLogRecord

Retrieves all of the fields and values of a single log event. All fields are retrieved, even if the original query that produced the `logRecordPointer` retrieved only a subset of fields. Fields are returned as field name/field value pairs.

The full unparsed log event is returned within `@message`.

Request Syntax

```
{
   "logRecordPointer": "string",
   "unmask": boolean
}
```

Request Parameters

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

The request accepts the following data in JSON format.

logRecordPointer

The pointer corresponding to the log event record you want to retrieve. You get this from the response of a `GetQueryResults` operation. In that response, the value of the `@ptr` field for a log event is the value to use as `logRecordPointer` to retrieve that complete log event record.

Type: String

Required: Yes

unmask

Specify `true` to display the log event fields with all sensitive data unmasked and visible. The default is `false`.

To use this operation with this parameter, you must be signed into an account with the `logs:Unmask` permission.

Type: Boolean

Required: No

Response Syntax

```
{
   "logRecord": {
      "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.

logRecord

The requested log event, as a JSON string.

Type: String to string map

Errors

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

InvalidParameterException

A parameter is specified incorrectly.

HTTP Status Code: 400

LimitExceededException

You have reached the maximum number of resources that can be created.

HTTP Status Code: 400

ResourceNotFoundException

The specified resource does not exist.

HTTP Status Code: 400

ServiceUnavailableException

The service cannot complete the request.

HTTP Status Code: 500

Examples

To retrieve all fields for a specified log event

The following example retrieves the fields for a specified log event.

Sample Request

```
POST / HTTP/1.1
Host: logs.<region>.<domain>
X-Amz-Date: <DATE>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=content-
type;date;host;user-agent;x-amz-date;x-amz-target;x-amzn-requestid,
 Signature=<Signature>
User-Agent: <UserAgentString>
Accept: application/json
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Connection: Keep-Alive
X-Amz-Target: Logs_20140328.GetLogRecord
{
   "logRecordPointer": "123456789"
}
```

Sample Response

```
HTTP/1.1 200 OK
x-amzn-RequestId: <RequestId>
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Date: <Date>
{
   "logRecord": {
      "@timestamp" : "1536857812",
```

```
      "@message" : "123456789012 eni-1234567890abcde123 6 33 ACCEPT"
      "accountId" : "123456789012",
      "interfaceId" : "eni-1234567890abcde123",
      "protocol" : "6",
      "packets" : "33",
      "action" : "ACCEPT"
   }
}
```

See Also

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

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

GetLookupTable

Retrieves the full content of a lookup table, including the CSV data.

Request Syntax

```
{
   "lookupTableArn": "string"
}
```

Request Parameters

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

The request accepts the following data in JSON format.

lookupTableArn

The ARN of the lookup table to retrieve.

Type: String

Required: Yes

Response Syntax

```
{
   "description": "string",
   "kmsKeyId": "string",
   "lastUpdatedTime": number,
   "lookupTableArn": "string",
   "lookupTableName": "string",
   "sizeBytes": number,
   "tableBody": "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.

description

The description of the lookup table.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 1024.

kmsKeyId

The ARN of the AWS KMS key used to encrypt the lookup table data, if applicable.

Type: String

Length Constraints: Maximum length of 256.

lastUpdatedTime

The time when the lookup table was last updated, expressed as the number of milliseconds after `Jan 1, 1970 00:00:00 UTC`.

Type: Long

Valid Range: Minimum value of 0.

lookupTableArn

The ARN of the lookup table.

Type: String

lookupTableName

The name of the lookup table.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `^[a-zA-Z0-9_]+$`

sizeBytes

The size of the lookup table in bytes.

Type: Long

Valid Range: Minimum value of 0.

tableBody

The full CSV content of the lookup table.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 10485760.

Errors

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

AccessDeniedException

You don't have sufficient permissions to perform this action.

HTTP Status Code: 400

InvalidParameterException

A parameter is specified incorrectly.

HTTP Status Code: 400

ResourceNotFoundException

The specified resource does not exist.

HTTP Status Code: 400

ServiceUnavailableException

The service cannot complete the request.

HTTP Status Code: 500

See Also

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

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

GetQueryResults

Returns the results from the specified query.

Only the fields requested in the query are returned, along with a `@ptr` field, which is the identifier for the log record. You can use the value of `@ptr` in a GetLogRecord operation to get the full log record.

`GetQueryResults` does not start running a query. To run a query, use StartQuery. For more information about how long results of previous queries are available, see CloudWatch Logs quotas.

If the value of the `Status` field in the output is `Running`, this operation returns only partial results. If you see a value of `Scheduled` or `Running` for the status, you can retry the operation later to see the final results.

This operation is used both for retrieving results from interactive queries and from automated scheduled query executions. Scheduled queries use `GetQueryResults` internally to retrieve query results for processing and delivery to configured destinations.

You can retrieve up to 100,000 log event results from a query, if available, by using pagination. Use the `nextToken` returned in the response to request additional pages of results, with each page returning up to 10,000 log events. This is only supported for Logs Insights QL and is currently not supported for PPL and SQL query languages.

If you are using CloudWatch cross-account observability, you can use this operation in a monitoring account to start queries in linked source accounts. For more information, see CloudWatch cross-account observability.

Request Syntax

```
{
   "maxItems": number,
   "nextToken": "string",
   "queryId": "string"
}
```

Request Parameters

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

The request accepts the following data in JSON format.

maxItems

The maximum number of log events to return in the response. The maximum is 10,000 log events per request. You can retrieve up to 100,000 log event results from a query by paginating with the `nextToken`.

Type: Integer

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

Required: No

nextToken

The token for the next set of items to return. The token expires after 1 hour.

Type: String

Length Constraints: Maximum length of 1024.

Required: No

queryId

The ID number of the query.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Required: Yes

Response Syntax

```
{
   "encryptionKey": "string",
   "nextToken": "string",
   "queryLanguage": "string",
   "results": [
      [
         {
            "field": "string",
```

```
            "value": "string"
         }
      ]
   ],
   "statistics": {
      "bytesScanned": number,
      "estimatedBytesSkipped": number,
      "estimatedRecordsSkipped": number,
      "logGroupsScanned": number,
      "recordsMatched": number,
      "recordsScanned": number,
      "resultCount": 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.

encryptionKey

If you associated an AWS KMS key with the CloudWatch Logs Insights query results in this account, this field displays the ARN of the key that's used to encrypt the query results when StartQuery stores them.

Type: String

Length Constraints: Maximum length of 256.

nextToken

If there are more log events remaining in the results, the response includes a `nextToken`. You can use this token in a subsequent `GetQueryResults` request to get the next set of results. You can retrieve up to 100,000 log event results from a query by paginating with this token. This is only supported for Logs Insights QL and is currently not supported for PPL and SQL query languages.

Type: String

Length Constraints: Maximum length of 1024.

queryLanguage

The query language used for this query. For more information about the query languages that CloudWatch Logs supports, see Supported query languages.

Type: String

Valid Values: `CWLI | SQL | PPL`

results

The log events that matched the query criteria during the most recent time it ran.

The `results` value is an array of arrays. Each log event is one object in the top-level array. Each of these log event objects is an array of `field/value` pairs.

Type: Array of arrays of ResultField objects

statistics

Includes the number of log events scanned by the query, the number of log events that matched the query criteria, and the total number of bytes in the scanned log events. These values reflect the full raw results of the query.

Type: QueryStatistics object

status

The status of the most recent running of the query. Possible values are `Cancelled`, `Complete`, `Failed`, `Running`, `Scheduled`, `Timeout`, and `Unknown`.

Queries time out after 60 minutes of runtime. To avoid having your queries time out, reduce the time range being searched or partition your query into a number of queries.

Type: String

Valid Values: `Scheduled | Running | Complete | Failed | Cancelled | Timeout | Unknown`

Errors

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

InvalidParameterException

A parameter is specified incorrectly.

HTTP Status Code: 400

ResourceNotFoundException

The specified resource does not exist.

HTTP Status Code: 400

ServiceUnavailableException

The service cannot complete the request.

HTTP Status Code: 500

Examples

Get results from a recent query

The following returns the results from a specified query.

Sample Request

```
POST / HTTP/1.1
Host: logs.<region>.<domain>
X-Amz-Date: <DATE>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=content-
type;date;host;user-agent;x-amz-date;x-amz-target;x-amzn-requestid,
 Signature=<Signature>
User-Agent: <UserAgentString>
Accept: application/json
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Connection: Keep-Alive
X-Amz-Target: Logs_20140328.GetQueryResults
{
   "queryId": "12ab3456-12ab-123a-789e-1234567890ab",
   "maxItems": 1000,
   "nextToken": "eEXAMPLEtoken"
}
```

Sample Response

```
HTTP/1.1 200 OK
x-amzn-RequestId: <RequestId>
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Date: <Date>
{
    "results": [
        [
            {
                "field": "LogEvent1-field1-name",
                "value": "LogEvent1-field1-value"
            },
            {
                "field": "LogEvent1-field2-name",
                "value": "LogEvent1-field2-value"
            },
            ...
            {
                "field": "LogEvent1-fieldX-name",
                "value": "LogEvent1-fieldX-value"
            }
        ],
        [
            {
                "field": "LogEvent2-field1-name",
                "value": "LogEvent2-field1-value"
            },
            {
                "field": "LogEvent2-field2-name",
                "value": "LogEvent2-field2-value"
            },
            ...
            {
                "field": "LogEvent2-fieldX-name",
                "value": "LogEvent2-fieldX-value"
            }
        ],
        [
            {
                "field": "LogEventZ-field1-name",
                "value": "LogEventZ-field1-value"
            },
```

```
            {
                "field": "LogEventZ-field2-name",
                "value": "LogEventZ-field2-value"
            },
            ...
            {
                "field": "LogEventZ-fieldX-name",
                "value": "LogEventZ-fieldX-value"
            }
        ]
    ],
    "statistics": {
        "bytesScanned": 81349723,
        "recordsMatched": 360851,
        "recordsScanned": 610956
    },
    "status": "Complete",
    "nextToken": "eEXAMPLEtoken"
}
```

See Also

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

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

GetScheduledQuery

Retrieves details about a specific scheduled query, including its configuration, execution status, and metadata.

Request Syntax

```
{
   "identifier": "string"
}
```

Request Parameters

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

The request accepts the following data in JSON format.

identifier

The ARN or name of the scheduled query to retrieve.

Type: String

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

Required: Yes

Response Syntax

```
{
   "creationTime": number,
   "description": "string",
   "destinationConfiguration": {
      "lookupTableConfiguration": {
         "description": "string",
         "kmsKeyId": "string",
         "roleArn": "string",
         "tableName": "string",
         "tags": {
            "string" : "string"
         }
```

```
      },
      "s3Configuration": {
         "destinationIdentifier": "string",
         "kmsKeyId": "string",
         "ownerAccountId": "string",
         "roleArn": "string"
      }
   },
   "endTimeOffset": number,
   "executionRoleArn": "string",
   "lastExecutionStatus": "string",
   "lastTriggeredTime": number,
   "lastUpdatedTime": number,
   "logGroupIdentifiers": [ "string" ],
   "name": "string",
   "queryLanguage": "string",
   "queryString": "string",
   "scheduledQueryArn": "string",
   "scheduleEndTime": number,
   "scheduleExpression": "string",
   "scheduleStartTime": number,
   "scheduleType": "string",
   "startTimeOffset": number,
   "state": "string",
   "timezone": "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.

creationTime

The timestamp when the scheduled query was created.

Type: Long

Valid Range: Minimum value of 0.

description

The description of the scheduled query.

Type: String

Length Constraints: Maximum length of 1024.

destinationConfiguration

Configuration for where query results are delivered.

Type: DestinationConfiguration object

endTimeOffset

The time offset in seconds that defines the end of the lookback period for the query.

Type: Long

executionRoleArn

The ARN of the IAM role used to execute the query and deliver results.

Type: String

Length Constraints: Minimum length of 1.

lastExecutionStatus

The status of the most recent execution of the scheduled query.

Type: String

Valid Values: `Running | InvalidQuery | Complete | Failed | Timeout`

lastTriggeredTime

The timestamp when the scheduled query was last executed.

Type: Long

Valid Range: Minimum value of 0.

lastUpdatedTime

The timestamp when the scheduled query was last updated.

Type: Long

Valid Range: Minimum value of 0.

logGroupIdentifiers

The log groups queried by the scheduled query.

Type: Array of strings

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

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

Pattern: `[\w#+=/:,.@-]*`

name

The name of the scheduled query.

Type: String

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

queryLanguage

The query language used by the scheduled query.

Type: String

Valid Values: `CWLI | SQL | PPL`

queryString

The query string executed by the scheduled query.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 10000.

scheduledQueryArn

The ARN of the scheduled query.

Type: String

scheduleEndTime

The end time for the scheduled query in Unix epoch format.

Type: Long

Valid Range: Minimum value of 0.

scheduleExpression

The cron expression that defines when the scheduled query runs.

Type: String

Length Constraints: Maximum length of 256.

scheduleStartTime

The start time for the scheduled query in Unix epoch format.

Type: Long

Valid Range: Minimum value of 0.

scheduleType

The schedule type of the scheduled query. Valid values are `CUSTOMER_MANAGED` and `AWS_MANAGED`.

Type: String

Valid Values: `CUSTOMER_MANAGED | AWS_MANAGED`

startTimeOffset

The time offset in seconds that defines the lookback period for the query.

Type: Long

state

The current state of the scheduled query.

Type: String

Valid Values: `ENABLED | DISABLED`

timezone

The timezone used for evaluating the schedule expression.

Type: String

Length Constraints: Minimum length of 1.

Errors

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

AccessDeniedException

You don't have sufficient permissions to perform this action.

HTTP Status Code: 400

InternalServerException

An internal server error occurred while processing the request. This exception is returned when the service encounters an unexpected condition that prevents it from fulfilling the request.

HTTP Status Code: 500

ResourceNotFoundException

The specified resource does not exist.

HTTP Status Code: 400

ThrottlingException

The request was throttled because of quota limits.

HTTP Status Code: 400

ValidationException

One of the parameters for the request is not valid.

HTTP Status Code: 400

See Also

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

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++

- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

GetScheduledQueryHistory

Retrieves the execution history of a scheduled query within a specified time range, including query results and destination processing status.

Request Syntax

```
{
   "endTime": number,
   "executionStatuses": [ "string" ],
   "identifier": "string",
   "maxResults": number,
   "nextToken": "string",
   "startTime": number
}
```

Request Parameters

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

The request accepts the following data in JSON format.

endTime

The end time for the history query in Unix epoch format.

Type: Long

Valid Range: Minimum value of 0.

Required: Yes

executionStatuses

An array of execution statuses to filter the history results. Only executions with the specified statuses are returned.

Type: Array of strings

Valid Values: `Running | InvalidQuery | Complete | Failed | Timeout`

Required: No

identifier

The ARN or name of the scheduled query to retrieve history for.

Type: String

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

Required: Yes

maxResults

The maximum number of history records to return. Valid range is 1 to 1000.

Type: Integer

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

Required: No

nextToken

The token for the next set of items to return. The token expires after 24 hours.

Type: String

Length Constraints: Minimum length of 1.

Required: No

startTime

The start time for the history query in Unix epoch format.

Type: Long

Valid Range: Minimum value of 0.

Required: Yes

Response Syntax

```
{
```

```
   "name": "string",
   "nextToken": "string",
   "scheduledQueryArn": "string",
   "triggerHistory": [
      {
         "destinations": [
            {
               "destinationIdentifier": "string",
               "destinationType": "string",
               "errorMessage": "string",
               "processedIdentifier": "string",
               "status": "string"
            }
         ],
         "errorMessage": "string",
         "executionStatus": "string",
         "queryId": "string",
         "triggeredTimestamp": 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.

name

The name of the scheduled query.

Type: String

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

nextToken

The token for the next set of items to return. The token expires after 24 hours.

Type: String

Length Constraints: Minimum length of 1.

scheduledQueryArn

The ARN of the scheduled query.

Type: String

triggerHistory

An array of execution history records for the scheduled query.

Type: Array of TriggerHistoryRecord objects

Errors

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

AccessDeniedException

You don't have sufficient permissions to perform this action.

HTTP Status Code: 400

InternalServerException

An internal server error occurred while processing the request. This exception is returned when the service encounters an unexpected condition that prevents it from fulfilling the request.

HTTP Status Code: 500

ResourceNotFoundException

The specified resource does not exist.

HTTP Status Code: 400

ThrottlingException

The request was throttled because of quota limits.

HTTP Status Code: 400

ValidationException

One of the parameters for the request is not valid.

HTTP Status Code: 400

See Also

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

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

GetStorageTierPolicy

Returns the storage tier policy for the account.

Response Syntax

```
{
   "lastUpdatedTime": number,
   "storageTier": "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.

lastUpdatedTime

The time when the storage tier policy was last updated, expressed as the number of milliseconds after `January 1, 1970 00:00:00 UTC`.

Type: Long

Valid Range: Minimum value of 0.

storageTier

The current storage tier for the account.

Type: String

Valid Values: `STANDARD | INTELLIGENT_TIERING`

Errors

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

AccessDeniedException

You don't have sufficient permissions to perform this action.

HTTP Status Code: 400

InvalidParameterException

A parameter is specified incorrectly.

HTTP Status Code: 400

OperationAbortedException

Multiple concurrent requests to update the same resource were in conflict.

HTTP Status Code: 400

ResourceNotFoundException

The specified resource does not exist.

HTTP Status Code: 400

ServiceUnavailableException

The service cannot complete the request.

HTTP Status Code: 500

See Also

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

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

GetTransformer

Returns the information about the log transformer associated with this log group.

This operation returns data only for transformers created at the log group level. To get information for an account-level transformer, use DescribeAccountPolicies.

Request Syntax

```
{
   "logGroupIdentifier": "string"
}
```

Request Parameters

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

The request accepts the following data in JSON format.

logGroupIdentifier

Specify either the name or ARN of the log group to return transformer information for. If the log group is in a source account and you are using a monitoring account, you must use the log group ARN.

Type: String

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

Pattern: `[\w#+=/:,.@-]*`

Required: Yes

Response Syntax

```
{
   "creationTime": number,
   "lastModifiedTime": number,
   "logGroupIdentifier": "string",
   "transformerConfig": [
      {
```

```
      "addKeys": {
         "entries": [
            {
               "key": "string",
               "overwriteIfExists": boolean,
               "value": "string"
            }
         ]
      },
      "copyValue": {
         "entries": [
            {
               "overwriteIfExists": boolean,
               "source": "string",
               "target": "string"
            }
         ]
      },
      "csv": {
         "columns": [ "string" ],
         "delimiter": "string",
         "destination": "string",
         "quoteCharacter": "string",
         "source": "string"
      },
      "dateTimeConverter": {
         "locale": "string",
         "matchPatterns": [ "string" ],
         "source": "string",
         "sourceTimezone": "string",
         "target": "string",
         "targetFormat": "string",
         "targetTimezone": "string"
      },
      "deleteKeys": {
         "withKeys": [ "string" ]
      },
      "grok": {
         "match": "string",
         "source": "string"
      },
      "listToMap": {
         "flatten": boolean,
         "flattenedElement": "string",
```

```
            "key": "string",
            "source": "string",
            "target": "string",
            "valueKey": "string"
         },
         "lowerCaseString": {
            "withKeys": [ "string" ]
         },
         "moveKeys": {
            "entries": [
               {
                  "overwriteIfExists": boolean,
                  "source": "string",
                  "target": "string"
               }
            ]
         },
         "parseCloudfront": {
            "source": "string"
         },
         "parseJSON": {
            "destination": "string",
            "source": "string"
         },
         "parseKeyValue": {
            "destination": "string",
            "fieldDelimiter": "string",
            "keyPrefix": "string",
            "keyValueDelimiter": "string",
            "nonMatchValue": "string",
            "overwriteIfExists": boolean,
            "source": "string"
         },
         "parsePostgres": {
            "source": "string"
         },
         "parseRoute53": {
            "source": "string"
         },
         "parseToOCSF": {
            "eventSource": "string",
            "mappingVersion": "string",
            "ocsfVersion": "string",
            "source": "string"
```

```
         },
         "parseVPC": {
            "source": "string"
         },
         "parseWAF": {
            "source": "string"
         },
         "renameKeys": {
            "entries": [
               {
                  "key": "string",
                  "overwriteIfExists": boolean,
                  "renameTo": "string"
               }
            ]
         },
         "splitString": {
            "entries": [
               {
                  "delimiter": "string",
                  "source": "string"
               }
            ]
         },
         "substituteString": {
            "entries": [
               {
                  "from": "string",
                  "source": "string",
                  "to": "string"
               }
            ]
         },
         "trimString": {
            "withKeys": [ "string" ]
         },
         "typeConverter": {
            "entries": [
               {
                  "key": "string",
                  "type": "string"
               }
            ]
         },
```

```
         "upperCaseString": {
            "withKeys": [ "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.

creationTime

The creation time of the transformer, expressed as the number of milliseconds after Jan 1, 1970 00:00:00 UTC.

Type: Long

Valid Range: Minimum value of 0.

lastModifiedTime

The date and time when this transformer was most recently modified, expressed as the number of milliseconds after Jan 1, 1970 00:00:00 UTC.

Type: Long

Valid Range: Minimum value of 0.

logGroupIdentifier

The ARN of the log group that you specified in your request.

Type: String

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

Pattern: `[\w#+=/:,.@-]*`

transformerConfig

This sructure contains the configuration of the requested transformer.

Type: Array of Processor objects

Array Members: Minimum number of 1 item. Maximum number of 20 items.

Errors

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

InvalidOperationException

The operation is not valid on the specified resource.

HTTP Status Code: 400

InvalidParameterException

A parameter is specified incorrectly.

HTTP Status Code: 400

ResourceNotFoundException

The specified resource does not exist.

HTTP Status Code: 400

ServiceUnavailableException

The service cannot complete the request.

HTTP Status Code: 500

See Also

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

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2

- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

ListAggregateLogGroupSummaries

Returns an aggregate summary of all log groups in the Region grouped by specified data source characteristics. Supports optional filtering by log group class, name patterns, and data sources. If you perform this action in a monitoring account, you can also return aggregated summaries of log groups from source accounts that are linked to the monitoring account. For more information about using cross-account observability to set up monitoring accounts and source accounts, see CloudWatch cross-account observability.

The operation aggregates log groups by data source name and type and optionally format, providing counts of log groups that share these characteristics. The operation paginates results. By default, it returns up to 50 results and includes a token to retrieve more results.

Request Syntax

```
{
   "accountIdentifiers": [ "string" ],
   "dataSources": [
      {
         "name": "string",
         "type": "string"
      }
   ],
   "groupBy": "string",
   "includeLinkedAccounts": boolean,
   "limit": number,
   "logGroupClass": "string",
   "logGroupNamePattern": "string",
   "nextToken": "string"
}
```

Request Parameters

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

The request accepts the following data in JSON format.

accountIdentifiers

When `includeLinkedAccounts` is set to `true`, use this parameter to specify the list of accounts to search. You can specify as many as 20 account IDs in the array.

Type: Array of strings

Array Members: Minimum number of 0 items. Maximum number of 20 items.

Length Constraints: Fixed length of 12.

Pattern: `^\d{12}$`

Required: No

dataSources

Filters the results by data source characteristics to include only log groups associated with the specified data sources.

Type: Array of DataSourceFilter objects

Array Members: Minimum number of 1 item. Maximum number of 5 items.

Required: No

groupBy

Specifies how to group the log groups in the summary.

Type: String

Valid Values: `DATA_SOURCE_NAME_TYPE_AND_FORMAT | DATA_SOURCE_NAME_AND_TYPE`

Required: Yes

includeLinkedAccounts

If you are using a monitoring account, set this to `true` to have the operation return log groups in the accounts listed in `accountIdentifiers`.

If this parameter is set to `true` and `accountIdentifiers` contains a null value, the operation returns all log groups in the monitoring account and all log groups in all source accounts that are linked to the monitoring account.

The default for this parameter is `false`.

Type: Boolean

Required: No

limit

The maximum number of aggregated summaries to return. If you omit this parameter, the default is up to 50 aggregated summaries.

Type: Integer

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

Required: No

logGroupClass

Filters the results by log group class to include only log groups of the specified class.

Type: String

Valid Values: `STANDARD | INFREQUENT_ACCESS | DELIVERY`

Required: No

logGroupNamePattern

Use this parameter to limit the returned log groups to only those with names that match the pattern that you specify. This parameter is a regular expression that can match prefixes and substrings, and supports wildcard matching and matching multiple patterns, as in the following examples.

- Use ^ to match log group names by prefix.
- For a substring match, specify the string to match. All matches are case sensitive
- To match multiple patterns, separate them with a | as in the example `^/aws/lambda|discovery`

You can specify as many as five different regular expression patterns in this field, each of which must be between 3 and 24 characters. You can include the ^ symbol as many as five times, and include the | symbol as many as four times.

Type: String

Length Constraints: Minimum length of 3. Maximum length of 129.

Pattern: `(\^?[\.\-_\/#A-Za-z0-9]{3,24})(\|\^?[\.\-_\/#A-Za-z0-9]{3,24}){0,4}`

Required: No

nextToken

The token for the next set of items to return. The token expires after 24 hours.

Type: String

Length Constraints: Minimum length of 1.

Required: No

Response Syntax

```
{
   "aggregateLogGroupSummaries": [
      {
         "groupingIdentifiers": [
            {
               "key": "string",
               "value": "string"
            }
         ],
         "logGroupCount": number
      }
   ],
   "nextToken": "string"
}
```

Response Elements

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

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

aggregateLogGroupSummaries

The list of aggregate log group summaries grouped by the specified data source characteristics.

Type: Array of AggregateLogGroupSummary objects

nextToken

The token for the next set of items to return. The token expires after 24 hours.

Type: String

Length Constraints: Minimum length of 1.

Errors

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

InvalidParameterException

A parameter is specified incorrectly.

HTTP Status Code: 400

ServiceUnavailableException

The service cannot complete the request.

HTTP Status Code: 500

ValidationException

One of the parameters for the request is not valid.

HTTP Status Code: 400

See Also

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

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3

- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

ListAnomalies

Returns a list of anomalies that log anomaly detectors have found. For details about the structure format of each anomaly object that is returned, see the example in this section.

Request Syntax

```
{
   "anomalyDetectorArn": "string",
   "limit": number,
   "nextToken": "string",
   "suppressionState": "string"
}
```

Request Parameters

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

The request accepts the following data in JSON format.

anomalyDetectorArn

Use this to optionally limit the results to only the anomalies found by a certain anomaly detector.

Type: String

Length Constraints: Minimum length of 1.

Pattern: `[\w#+=/:,.@-]*`

Required: No

limit

The maximum number of items to return. If you don't specify a value, the default maximum value of 50 items is used.

Type: Integer

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

Required: No

nextToken

The token for the next set of items to return. The token expires after 24 hours.

Type: String

Length Constraints: Minimum length of 1.

Required: No

suppressionState

You can specify this parameter if you want to the operation to return only anomalies that are currently either suppressed or unsuppressed.

Type: String

Valid Values: SUPPRESSED | UNSUPPRESSED

Required: No

Response Syntax

```
{
   "anomalies": [
      {
         "active": boolean,
         "anomalyDetectorArn": "string",
         "anomalyId": "string",
         "description": "string",
         "firstSeen": number,
         "histogram": {
            "string" : number
         },
         "isPatternLevelSuppression": boolean,
         "lastSeen": number,
         "logGroupArnList": [ "string" ],
         "logSamples": [
            {
               "message": "string",
               "timestamp": number
            }
         ],
```

```
         "patternId": "string",
         "patternRegex": "string",
         "patternString": "string",
         "patternTokens": [
            {
               "dynamicTokenPosition": number,
               "enumerations": {
                  "string" : number
               },
               "inferredTokenName": "string",
               "isDynamic": boolean,
               "tokenString": "string"
            }
         ],
         "priority": "string",
         "state": "string",
         "suppressed": boolean,
         "suppressedDate": number,
         "suppressedUntil": number
      }
   ],
   "nextToken": "string"
}
```

Response Elements

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

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

anomalies

An array of structures, where each structure contains information about one anomaly that a log anomaly detector has found.

Type: Array of Anomaly objects

nextToken

The token for the next set of items to return. The token expires after 24 hours.

Type: String

Length Constraints: Minimum length of 1.

Errors

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

InvalidParameterException

A parameter is specified incorrectly.

HTTP Status Code: 400

OperationAbortedException

Multiple concurrent requests to update the same resource were in conflict.

HTTP Status Code: 400

ResourceNotFoundException

The specified resource does not exist.

HTTP Status Code: 400

ServiceUnavailableException

The service cannot complete the request.

HTTP Status Code: 500

Examples

To retrieve a list of anomalies found by logs anomaly detectors

This example illustrates one usage of ListAnomalies.

Sample Request

```
POST / HTTP/1.1
Host: logs.<region>.<domain>
X-Amz-Date: <DATE>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=content-
type;date;host;user-agent;x-amz-date;x-amz-target;x-amzn-requestid,
 Signature=<Signature>
User-Agent: <UserAgentString>
Accept: application/json
```

```
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Connection: Keep-Alive
X-Amz-Target: Logs_20140328.ListAnomalies
{
   "anomalyDetectorArn": "arn:aws:logs:us-west-1:123456789012:anomaly-
detector:EXAMPLE-1234-5678-abcd-111111111111",
   "limit": 50,
}
```

Sample Response

```
{
    "anomalies": [
        {
            "active": false,
            "anomalyDetectorArn": "arn:aws:logs:us-west-1:123456789012:anomaly-
detector:EXAMPLE-1234-5678-abcd-111111111111",
            "anomalyId": "EXAMPLE-529d-4e1e-bea9-123EXAMPLE",
            "description": "Count of ErrorCode: 200 at token: 9 deviated expected by:
 20.00%",
            "firstSeen": 1698488280000,
            "histogram": {
                "1698487995000": 2,
                "1698488285000": 4,
                "1698488295000": 1,
                "1698488300000": 1,
                "1698488305000": 4
            },
            "isPatternLevelSuppression": false,
            "lastSeen": 1698488580000,
            "logGroupArnList": [
                "arn:aws:logs:us-east-1:123456789012:log-group:/aws/lambda/my-log-
group-name"
            ],
            "logSamples": [
                {
                    "message": "2023-10-28T10:18:18.959Z\EXAMPLE-4e26-41d8-8b54-EXAMPLE
\tINFO\tResponse: 200 https://global.console.aws.amazon.com/EXAMPLEURL",
                    "timestamp": 1698488298959
                }
            ],
            "patternId": "EXAMPLE86827f77073836412345678",
```

```
            "patternRegex": ".*\\Q\t\\E.*\\Q\tINFO\tResponse: \\E.*\\Q https:\\E.*\\Q=\
\E.*\\Q=\\E.*\\Q=\\E.*\\Q\n\\E",
            "patternString": "<*>\t<*>\tINFO\tResponse: <*> https:<*>=<*>=<*>=<*>\n",
            "patternTokens": [
                {
                    "dynamicTokenPosition": 1,
                    "enumerations": {
                        "2023-10-28T10:18:08.420Z": 2,
                        "2023-10-28T10:18:18.959Z": 1,
                        "2023-10-28T10:18:20.260Z": 1,
                        "2023-10-28T10:18:25.440Z": 1,
                        "2023-10-28T10:18:27.508Z": 1
                    },
                    "isDynamic": true,
                    "tokenString": "<*>"
                },
                {
                    "dynamicTokenPosition": 0,
                    "enumerations": {},
                    "isDynamic": false,
                    "tokenString": "\t"
                },
                {
                    "dynamicTokenPosition": 2,
                    "enumerations": {
                        "4766bcdd-4e26-41d8-8b54-fa0ae43f6201": 6
                    },
                    "isDynamic": true,
                    "tokenString": "<*>"
                },
                {
                    "dynamicTokenPosition": 0,
                    "enumerations": {},
                    "isDynamic": false,
                    "tokenString": "\t"
                },
                {
                    "dynamicTokenPosition": 0,
                    "enumerations": {},
                    "isDynamic": false,
                    "tokenString": "INFO"
                },
                {
                    "dynamicTokenPosition": 0,
```

```
                    "enumerations": {},
                    "isDynamic": false,
                    "tokenString": "\t"
                },
                {
                    "dynamicTokenPosition": 0,
                    "enumerations": {},
                    "isDynamic": false,
                    "tokenString": "Response"
                },
                {
                    "dynamicTokenPosition": 0,
                    "enumerations": {},
                    "isDynamic": false,
                    "tokenString": ":"
                },
                {
                    "dynamicTokenPosition": 0,
                    "enumerations": {},
                    "isDynamic": false,
                    "tokenString": " "
                },
                {
                    "dynamicTokenPosition": 3,
                    "enumerations": {
                        "200": 6
                    },
                    "isDynamic": true,
                    "tokenString": "<*>"
                },
                {
                    "dynamicTokenPosition": 0,
                    "enumerations": {},
                    "isDynamic": false,
                    "tokenString": " "
                },
                {
                    "dynamicTokenPosition": 0,
                    "enumerations": {},
                    "isDynamic": false,
                    "tokenString": "https"
                },
                {
                    "dynamicTokenPosition": 0,
```

```
                    "enumerations": {},
                    "isDynamic": false,
                    "tokenString": ":"
                },
                {
                    "dynamicTokenPosition": 4,
                    "enumerations": {
                        "//global.console.aws.amazon.com/EXAMPLEURL": 1,
                        "//prod.EXAMPLEURL2": 5
                    },
                    "isDynamic": true,
                    "tokenString": "<*>"
                },
                {
                    "dynamicTokenPosition": 0,
                    "enumerations": {},
                    "isDynamic": false,
                    "tokenString": "="
                },
                {
                    "dynamicTokenPosition": 5,
                    "enumerations": {
                        "%40amzn%2Faws-ccx-regions-availability&majorVersion": 1,
                        "info&message": 5
                    },
                    "isDynamic": true,
                    "tokenString": "<*>"
                },
                {
                    "dynamicTokenPosition": 0,
                    "enumerations": {},
                    "isDynamic": false,
                    "tokenString": "="
                },
                {
                    "dynamicTokenPosition": 6,
                    "enumerations": {
                        "1&versionId": 1,
                        "checkForCookieConsent&payload": 3,
                        "geolocationLatency&payload": 1,
                        "uiMounted&payload": 1
                    },
                    "isDynamic": true,
                    "tokenString": "<*>"
```

```
                },
                {
                    "dynamicTokenPosition": 0,
                    "enumerations": {},
                    "isDynamic": false,
                    "tokenString": "="
                },
               {
                    "dynamicTokenPosition": 0,
                    "enumerations": {},
                    "isDynamic": false,
                    "tokenString": "\n"
                }
            ],
            "priority": "LOW",
            "state": "Active",
            "suppressed": false,
            "suppressedDate": 0,
            "suppressedUntil": 0
        },
        {
            "active": false,
            "anomalyDetectorArn": "arn:aws:logs:us-west-1:123456789012:anomaly-
detector:EXAMPLE-1234-5678-abcd-111111111111",
            "anomalyId": "EXAMPLE-09d4-4286-9cd3-EXAMPLE",
            "description": "Count of ErrorCode: 200 at token: 9 deviated expected by:
 95.12%",
            "firstSeen": 1698392040000,
            "histogram": {
                "1698392035000": 17,
                "1698392040000": 5
            },
            "isPatternLevelSuppression": true,
            "lastSeen": 1698392340000,
            "logGroupArnList": [
                "arn:aws:logs:us-east-1:123456789012:log-group:another-log-group"
            ],
            "logSamples": [
                {
                    "message": "2023-10-27T07:33:56.178Z\tb3c81837-
ead3-46ac-9334-68fa05453033\tINFO\tResponse: 200 https://EXAMPLE-URL-2",
                    "timestamp": 1698392036178
                }
            ],
```

```
            "patternId": "9f2e9e2844e41728651fb229351c90e0",
            "patternRegex": ".*\\Q\t\\E.*\\Q\tINFO\tResponse: \\E.*\\Q https:\\E.*\\Q\n
\\E",
            "patternString": "<*>\t<*>\tINFO\tResponse: <*> https:<*>\n",
            "patternTokens": [
                {
                    "dynamicTokenPosition": 1,
                    "enumerations": {
                        "2023-10-27T07:33:56.238Z": 1,
                        "2023-10-27T07:33:56.253Z": 1,
                        "2023-10-27T07:33:56.274Z": 1,
                        "2023-10-27T07:33:56.295Z": 1,
                        "2023-10-27T07:34:01.929Z": 1
                    },
                    "isDynamic": true,
                    "tokenString": "<*>"
                },
                {
                    "dynamicTokenPosition": 0,
                    "enumerations": {},
                    "isDynamic": false,
                    "tokenString": "\t"
                },
                {
                    "dynamicTokenPosition": 2,
                    "enumerations": {
                        "b3c81837-ead3-46ac-9334-68fa05453033": 22
                    },
                    "isDynamic": true,
                    "tokenString": "<*>"
                },
                {
                    "dynamicTokenPosition": 0,
                    "enumerations": {},
                    "isDynamic": false,
                    "tokenString": "\t"
                },
                {
                    "dynamicTokenPosition": 0,
                    "enumerations": {},
                    "isDynamic": false,
                    "tokenString": "INFO"
                },
                {
```

```
                    "dynamicTokenPosition": 0,
                    "enumerations": {},
                    "isDynamic": false,
                    "tokenString": "\t"
                },
                {
                    "dynamicTokenPosition": 0,
                    "enumerations": {},
                    "isDynamic": false,
                    "tokenString": "Response"
                },
                {
                    "dynamicTokenPosition": 0,
                    "enumerations": {},
                    "isDynamic": false,
                    "tokenString": ":"
                },
                {
                    "dynamicTokenPosition": 0,
                    "enumerations": {},
                    "isDynamic": false,
                    "tokenString": " "
                },
                {
                    "dynamicTokenPosition": 3,
                    "enumerations": {
                        "200": 22
                    },
                    "isDynamic": true,
                    "tokenString": "<*>"
                },
                {
                    "dynamicTokenPosition": 0,
                    "enumerations": {},
                    "isDynamic": false,
                    "tokenString": " "
                },
                {
                    "dynamicTokenPosition": 0,
                    "enumerations": {},
                    "isDynamic": false,
                    "tokenString": "https"
                },
                {
```

```
                "dynamicTokenPosition": 0,
                "enumerations": {},
                "isDynamic": false,
                "tokenString": ":"
            },
            {
                "dynamicTokenPosition": 4,
                "enumerations": {
                    "//EXAMPLE-URL-1": 12,
                    "//EXAMPLE-URL-2": 1,
                    "//EXAMPLE-URL-2": 6,
                    "//EXAMPLE-URL-3": 3
                },
                "isDynamic": true,
                "tokenString": "<*>"
            },
            {
                "dynamicTokenPosition": 0,
                "enumerations": {},
                "isDynamic": false,
                "tokenString": "\n"
            }
        ],
        "priority": "LOW",
        "state": "Active",
        "suppressed": true,
        "suppressedDate": 0,
        "suppressedUntil": 1702393208766
    },
```

See Also

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

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3

- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

ListIntegrations

Returns a list of integrations between CloudWatch Logs and other services in this account. Currently, only one integration can be created in an account, and this integration must be with OpenSearch Service.

Request Syntax

```
{
   "integrationNamePrefix": "string",
   "integrationStatus": "string",
   "integrationType": "string"
}
```

Request Parameters

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

The request accepts the following data in JSON format.

integrationNamePrefix

To limit the results to integrations that start with a certain name prefix, specify that name prefix here.

Type: String

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

Pattern: `[\.\-_/#A-Za-z0-9]+`

Required: No

integrationStatus

To limit the results to integrations with a certain status, specify that status here.

Type: String

Valid Values: `PROVISIONING | ACTIVE | FAILED`

Required: No

integrationType

To limit the results to integrations of a certain type, specify that type here.

Type: String

Valid Values: OPENSEARCH

Required: No

Response Syntax

```
{
   "integrationSummaries": [
      {
         "integrationName": "string",
         "integrationStatus": "string",
         "integrationType": "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.

integrationSummaries

An array, where each object in the array contains information about one CloudWatch Logs integration in this account.

Type: Array of IntegrationSummary objects

Errors

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

InvalidParameterException

A parameter is specified incorrectly.

HTTP Status Code: 400

ServiceUnavailableException

The service cannot complete the request.

HTTP Status Code: 500

See Also

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

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

ListLogAnomalyDetectors

Retrieves a list of the log anomaly detectors in the account.

Request Syntax

```
{
   "filterLogGroupArn": "string",
   "limit": number,
   "nextToken": "string"
}
```

Request Parameters

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

The request accepts the following data in JSON format.

filterLogGroupArn

Use this to optionally filter the results to only include anomaly detectors that are associated with the specified log group.

Type: String

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

Pattern: `[\w#+=/:,.@-]*`

Required: No

limit

The maximum number of items to return. If you don't specify a value, the default maximum value of 50 items is used.

Type: Integer

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

Required: No

nextToken

The token for the next set of items to return. The token expires after 24 hours.

Type: String

Length Constraints: Minimum length of 1.

Required: No

Response Syntax

```
{
   "anomalyDetectors": [
      {
         "anomalyDetectorArn": "string",
         "anomalyDetectorStatus": "string",
         "anomalyVisibilityTime": number,
         "creationTimeStamp": number,
         "detectorName": "string",
         "evaluationFrequency": "string",
         "filterPattern": "string",
         "kmsKeyId": "string",
         "lastModifiedTimeStamp": number,
         "logGroupArnList": [ "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.

anomalyDetectors

An array of structures, where each structure in the array contains information about one anomaly detector.

Type: Array of AnomalyDetector objects

nextToken

The token for the next set of items to return. The token expires after 24 hours.

Type: String

Length Constraints: Minimum length of 1.

Errors

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

InvalidParameterException

A parameter is specified incorrectly.

HTTP Status Code: 400

OperationAbortedException

Multiple concurrent requests to update the same resource were in conflict.

HTTP Status Code: 400

ResourceNotFoundException

The specified resource does not exist.

HTTP Status Code: 400

ServiceUnavailableException

The service cannot complete the request.

HTTP Status Code: 500

See Also

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

- AWS Command Line Interface V2
- AWS SDK for .NET V4

- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

ListLogGroups

Returns a list of log groups in the Region in your account. If you are performing this action in a monitoring account, you can choose to also return log groups from source accounts that are linked to the monitoring account. For more information about using cross-account observability to set up monitoring accounts and source accounts, see CloudWatch cross-account observability.

You can optionally filter the results by log group class, log group name pattern, field indexes, data sources, field index names, or log group tags. If you specify more than one filter type, the results include log groups that satisfy all filters.

This operation is paginated. By default, your first use of this operation returns 50 results, and includes a token to use in a subsequent operation to return more results.

Request Syntax

```
{
   "accountIdentifiers": [ "string" ],
   "dataSources": [
      {
         "name": "string",
         "type": "string"
      }
   ],
   "fieldIndexNames": [ "string" ],
   "includeLinkedAccounts": boolean,
   "limit": number,
   "logGroupClass": "string",
   "logGroupNamePattern": "string",
   "logGroupTags": [
      {
         "key": "string",
         "values": [ "string" ]
      }
   ],
   "nextToken": "string"
}
```

Request Parameters

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

The request accepts the following data in JSON format.

accountIdentifiers

When `includeLinkedAccounts` is set to `true`, use this parameter to specify the list of accounts to search. You can specify as many as 20 account IDs in the array.

Type: Array of strings

Array Members: Minimum number of 0 items. Maximum number of 20 items.

Length Constraints: Fixed length of 12.

Pattern: `^\d{12}$`

Required: No

dataSources

An array of data source filters to filter log groups by their associated data sources. You can filter by data source name, type, or both. Multiple filters within the same dimension are combined with OR logic, while filters across different dimensions are combined with AND logic.

Type: Array of DataSourceFilter objects

Array Members: Minimum number of 1 item. Maximum number of 5 items.

Required: No

fieldIndexNames

An array of field index names to filter log groups that have specific field indexes. Only log groups containing all specified field indexes are returned. You can specify 1 to 20 field index names, each with 1 to 512 characters.

Type: Array of strings

Array Members: Minimum number of 1 item. Maximum number of 20 items.

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `[\.\-_/#A-Za-z0-9]+`

Required: No

includeLinkedAccounts

If you are using a monitoring account, set this to `true` to have the operation return log groups in the accounts listed in `accountIdentifiers`.

If this parameter is set to `true` and `accountIdentifiers` contains a null value, the operation returns all log groups in the monitoring account and all log groups in all source accounts that are linked to the monitoring account.

The default for this parameter is `false`.

Type: Boolean

Required: No

limit

The maximum number of log groups to return. If you omit this parameter, the default is up to 50 log groups.

Type: Integer

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

Required: No

logGroupClass

Use this parameter to limit the results to only those log groups in the specified log group class. If you omit this parameter, log groups of all classes can be returned.

Type: String

Valid Values: `STANDARD | INFREQUENT_ACCESS | DELIVERY`

Required: No

logGroupNamePattern

Use this parameter to limit the returned log groups to only those with names that match the pattern that you specify. This parameter is a regular expression that can match prefixes and substrings, and supports wildcard matching and matching multiple patterns, as in the following examples.

- Use ^ to match log group names by prefix.

- For a substring match, specify the string to match. All matches are case sensitive
- To match multiple patterns, separate them with a | as in the example `^/aws/lambda|discovery`

You can specify as many as five different regular expression patterns in this field, each of which must be between 3 and 24 characters. You can include the ^ symbol as many as five times, and include the | symbol as many as four times.

Type: String

Length Constraints: Minimum length of 3. Maximum length of 129.

Pattern: `(\^?[\.\-_\/#A-Za-z0-9]{3,24})(\|\^?[\.\-_\/#A-Za-z0-9]{3,24}){0,4}`

Required: No

logGroupTags

An array of tag filters to return only log groups that have specific tags. Multiple filters are combined with AND logic.

Type: Array of TagFilter objects

Array Members: Minimum number of 1 item. Maximum number of 5 items.

Required: No

nextToken

The token for the next set of items to return. The token expires after 24 hours.

Type: String

Length Constraints: Minimum length of 1.

Required: No

Response Syntax

```
{
   "logGroups": [
      {
```

```
            "logGroupArn": "string",
            "logGroupClass": "string",
            "logGroupName": "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.

logGroups

An array of structures, where each structure contains the information about one log group.

Type: Array of LogGroupSummary objects

nextToken

The token for the next set of items to return. The token expires after 24 hours.

Type: String

Length Constraints: Minimum length of 1.

Errors

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

InvalidParameterException

A parameter is specified incorrectly.

HTTP Status Code: 400

ServiceUnavailableException

The service cannot complete the request.

HTTP Status Code: 500

See Also

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

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

ListLogGroupsForQuery

Returns a list of the log groups that were analyzed during a single CloudWatch Logs Insights query. This can be useful for queries that use log group name prefixes or the `filterIndex` command, because the log groups are dynamically selected in these cases.

For more information about field indexes, see Create field indexes to improve query performance and reduce costs.

Request Syntax

```
{
   "maxResults": number,
   "nextToken": "string",
   "queryId": "string"
}
```

Request Parameters

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

The request accepts the following data in JSON format.

maxResults

Limits the number of returned log groups to the specified number.

Type: Integer

Valid Range: Minimum value of 50. Maximum value of 500.

Required: No

nextToken

The token for the next set of items to return. The token expires after 24 hours.

Type: String

Length Constraints: Minimum length of 1.

Required: No

queryId

The ID of the query to use. This query ID is from the response to your StartQuery operation.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Required: Yes

Response Syntax

```
{
   "logGroupIdentifiers": [ "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.

logGroupIdentifiers

An array of the names and ARNs of the log groups that were processed in the query.

Type: Array of strings

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

Pattern: `[\w#+=/:,.@-]*`

nextToken

The token for the next set of items to return. The token expires after 24 hours.

Type: String

Length Constraints: Minimum length of 1.

Errors

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

AccessDeniedException

You don't have sufficient permissions to perform this action.

HTTP Status Code: 400

InvalidParameterException

A parameter is specified incorrectly.

HTTP Status Code: 400

ResourceNotFoundException

The specified resource does not exist.

HTTP Status Code: 400

ServiceUnavailableException

The service cannot complete the request.

HTTP Status Code: 500

Examples

To list the log groups that were analyzed during a specific query

The following examplereturns the log groups that were analyzed during the query with the `71bacb5a-30f1-4ed6-9959-2797EXAMPLE` ID.

Sample Request

```
POST / HTTP/1.1
Host: logs.<region>.<domain>
X-Amz-Date: <DATE>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=content-
type;date;host;user-agent;x-amz-date;x-amz-target;x-amzn-requestid,
 Signature=<Signature>
```

```
User-Agent: <UserAgentString>
Accept: application/json
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Connection: Keep-Alive
X-Amz-Target: Logs_20140328.ListLogGroupsForQuery
{
  "queryId": "71bacb5a-30f1-4ed6-9959-2797EXAMPLE"
}
```

Sample Response

```
HTTP/1.1 200 OK
x-amzn-RequestId: <RequestId>
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Date: <Date>
{
  "logGroupIdentifiers": [
    "arn:aws:logs:us-east-1:112233445566:log-group:/aws/lambda/applogs",
    "arn:aws:logs:us-east-1:112233445566:log-group:/aws/lambda/servicelogs",
    "arn:aws:logs:us-east-1:112233445566:log-group:/aws/lambda/errorlogs"
  ]
}
```

See Also

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

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)

- AWS SDK for Ruby V3

ListScheduledQueries

Lists all scheduled queries in your account and region. You can filter results by state to show only enabled or disabled queries.

Request Syntax

```
{
   "maxResults": number,
   "nextToken": "string",
   "scheduleType": "string",
   "state": "string"
}
```

Request Parameters

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

The request accepts the following data in JSON format.

maxResults

The maximum number of scheduled queries to return. Valid range is 1 to 1000.

Type: Integer

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

Required: No

nextToken

The token for the next set of items to return. The token expires after 24 hours.

Type: String

Length Constraints: Minimum length of 1.

Required: No

scheduleType

Filter scheduled queries by schedule type. Valid values are `CUSTOMER_MANAGED` and `AWS_MANAGED`. If not specified, scheduled queries of all schedule types are returned.

Type: String

Valid Values: `CUSTOMER_MANAGED | AWS_MANAGED`

Required: No

state

Filter scheduled queries by state. Valid values are `ENABLED` and `DISABLED`. If not specified, all scheduled queries are returned.

Type: String

Valid Values: `ENABLED | DISABLED`

Required: No

Response Syntax

```
{
   "nextToken": "string",
   "scheduledQueries": [
      {
         "creationTime": number,
         "destinationConfiguration": {
            "lookupTableConfiguration": {
               "description": "string",
               "kmsKeyId": "string",
               "roleArn": "string",
               "tableName": "string",
               "tags": {
                  "string" : "string"
               }
            },
            "s3Configuration": {
               "destinationIdentifier": "string",
               "kmsKeyId": "string",
               "ownerAccountId": "string",
               "roleArn": "string"
            }
         },
         "lastExecutionStatus": "string",
         "lastTriggeredTime": number,
         "lastUpdatedTime": number,
```

```
            "name": "string",
            "scheduledQueryArn": "string",
            "scheduleExpression": "string",
            "scheduleType": "string",
            "state": "string",
            "timezone": "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 token for the next set of items to return. The token expires after 24 hours.

Type: String

Length Constraints: Minimum length of 1.

scheduledQueries

An array of scheduled query summary information.

Type: Array of ScheduledQuerySummary objects

Errors

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

AccessDeniedException

You don't have sufficient permissions to perform this action.

HTTP Status Code: 400

InternalServerException

An internal server error occurred while processing the request. This exception is returned when the service encounters an unexpected condition that prevents it from fulfilling the request.

HTTP Status Code: 500

ThrottlingException

The request was throttled because of quota limits.

HTTP Status Code: 400

ValidationException

One of the parameters for the request is not valid.

HTTP Status Code: 400

See Also

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

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

ListSourcesForS3TableIntegration

Returns a list of data source associations for a specified S3 Table Integration, showing which data sources are currently associated for query access.

Request Syntax

```
{
   "integrationArn": "string",
   "maxResults": number,
   "nextToken": "string"
}
```

Request Parameters

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

The request accepts the following data in JSON format.

integrationArn

The Amazon Resource Name (ARN) of the S3 Table Integration to list associations for.

Type: String

Required: Yes

maxResults

The maximum number of associations to return in a single call. Valid range is 1 to 100.

Type: Integer

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

Required: No

nextToken

The token for the next set of items to return. The token expires after 24 hours.

Type: String

Length Constraints: Minimum length of 1.

Required: No

Response Syntax

```
{
   "nextToken": "string",
   "sources": [
      {
         "createdTimeStamp": number,
         "dataSource": {
            "name": "string",
            "type": "string"
         },
         "identifier": "string",
         "parentSourceIdentifier": "string",
         "status": "string",
         "statusReason": "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 token for the next set of items to return. The token expires after 24 hours.

Type: String

Length Constraints: Minimum length of 1.

sources

The list of data source associations for the specified S3 Table Integration.

Type: Array of S3TableIntegrationSource objects

Errors

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

AccessDeniedException

You don't have sufficient permissions to perform this action.

HTTP Status Code: 400

InternalServerException

An internal server error occurred while processing the request. This exception is returned when the service encounters an unexpected condition that prevents it from fulfilling the request.

HTTP Status Code: 500

ResourceNotFoundException

The specified resource does not exist.

HTTP Status Code: 400

ThrottlingException

The request was throttled because of quota limits.

HTTP Status Code: 400

ValidationException

One of the parameters for the request is not valid.

HTTP Status Code: 400

See Also

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

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++

- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

ListSyslogConfigurations

Returns a list of syslog configurations. You can optionally filter the results by log group or VPC endpoint.

Request Syntax

```
{
   "logGroupIdentifier": "string",
   "maxResults": number,
   "nextToken": "string",
   "vpcEndpointId": "string"
}
```

Request Parameters

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

The request accepts the following data in JSON format.

logGroupIdentifier

The name or ARN of the log group to filter syslog configurations for.

Type: String

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

Pattern: `[\w#+=/:,.@-]*`

Required: No

maxResults

The maximum number of syslog configurations to return in the response.

Type: Integer

Valid Range: Minimum value of 0. Maximum value of 50.

Required: No

nextToken

The token for the next set of items to return. You received this token from a previous call.

Type: String

Length Constraints: Minimum length of 1.

Required: No

vpcEndpointId

The ID of the VPC endpoint to filter syslog configurations for.

Type: String

Pattern: `^vpce-[0-9a-f]{1,64}$`

Required: No

Response Syntax

```
{
   "nextToken": "string",
   "syslogConfigurations": [
      {
         "createdAt": number,
         "logGroupArn": "string",
         "sourceType": "string",
         "vpcEndpointId": "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 token for the next set of items to return. The token expires after 24 hours.

Type: String

Length Constraints: Minimum length of 1.

syslogConfigurations

The list of syslog configurations.

Type: Array of SyslogConfiguration objects

Errors

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

AccessDeniedException

You don't have sufficient permissions to perform this action.

HTTP Status Code: 400

InvalidOperationException

The operation is not valid on the specified resource.

HTTP Status Code: 400

InvalidParameterException

A parameter is specified incorrectly.

HTTP Status Code: 400

ResourceNotFoundException

The specified resource does not exist.

HTTP Status Code: 400

ServiceUnavailableException

The service cannot complete the request.

HTTP Status Code: 500

ThrottlingException

The request was throttled because of quota limits.

HTTP Status Code: 400

Examples

To list syslog configurations

The following example lists the syslog configurations for the specified log group.

Sample Request

```
POST / HTTP/1.1
Host: logs.<region>.<domain>
X-Amz-Date: <DATE>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=content-
type;date;host;user-agent;x-amz-date;x-amz-target;x-amzn-requestid,
 Signature=<Signature>
User-Agent: <UserAgentString>
Accept: application/json
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Connection: Keep-Alive
X-Amz-Target: Logs_20140328.ListSyslogConfigurations
{
  "logGroupIdentifier": "arn:aws:logs:us-east-1:123456789012:log-group:my-syslog-group"
}
```

Sample Response

```
HTTP/1.1 200 OK
x-amzn-RequestId: <RequestId>
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Date: <Date>
{
  "syslogConfigurations": [
    {
      "logGroupArn": "arn:aws:logs:us-east-1:123456789012:log-group:my-syslog-group",
      "sourceType": "VPCE",
      "vpcEndpointId": "vpce-0123456789abcdef0",
      "createdAt": 1718000000000
    }
  ]
```

```
}
```

See Also

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

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

ListTagsForResource

Displays the tags associated with a CloudWatch Logs resource. Currently, log groups and destinations support tagging.

Request Syntax

```
{
   "resourceArn": "string"
}
```

Request Parameters

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

The request accepts the following data in JSON format.

resourceArn

The ARN of the resource that you want to view tags for.

The ARN format of a log group is `arn:aws:logs:Region:account-id:log-group:log-group-name`

The ARN format of a destination is `arn:aws:logs:Region:account-id:destination:destination-name`

For more information about ARN format, see CloudWatch Logs resources and operations.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 1011.

Pattern: `[\w+=/:,.@-]*`

Required: Yes

Response Syntax

```
{
```

```
   "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 list of tags associated with the requested resource.>

Type: String to string map

Map Entries: Maximum number of 50 items.

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

Key Pattern: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]+)$`

Value Length Constraints: Maximum length of 256.

Value Pattern: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$`

Errors

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

InvalidParameterException

A parameter is specified incorrectly.

HTTP Status Code: 400

ResourceNotFoundException

The specified resource does not exist.

HTTP Status Code: 400

ServiceUnavailableException

The service cannot complete the request.

HTTP Status Code: 500

See Also

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

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

ListTagsLogGroup

This action has been deprecated.

> **Important**
>
> The ListTagsLogGroup operation is on the path to deprecation. We recommend that you use ListTagsForResource instead.

Lists the tags for the specified log group.

Request Syntax

```
{
   "logGroupName": "string"
}
```

Request Parameters

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

The request accepts the following data in JSON format.

logGroupName

The name of the log group.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `[\.\-_/#A-Za-z0-9]+`

Required: Yes

Response Syntax

```
{
```

```
   "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 for the log group.

Type: String to string map

Map Entries: Maximum number of 50 items.

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

Key Pattern: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]+)$`

Value Length Constraints: Maximum length of 256.

Value Pattern: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$`

Errors

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

ResourceNotFoundException

The specified resource does not exist.

HTTP Status Code: 400

ServiceUnavailableException

The service cannot complete the request.

HTTP Status Code: 500

See Also

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

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

PutAccountPolicy

Creates an account-level data protection policy, subscription filter policy, field index policy, transformer policy, or metric extraction policy that applies to all log groups, a subset of log groups, or a data source name and type combination in the account.

> **Important**
>
> `PutAccountPolicy` is an account-wide administrative operation intended for CloudWatch Logs administrators. Because it affects all log groups (or a broad subset) in the account, you should grant `logs:PutAccountPolicy` permissions only to administrators who manage logging configuration across the account, not to application teams or individual log group owners.

Conflict resolution between account-level and log-group-level policies

When both an account-level policy and a log-group-level policy of the same type apply to a log group, the resolution depends on the policy type:

- *Data protection* — The two policies are cumulative. Any sensitive term specified in either the account-level or the log-group-level policy is masked.
- *Subscription filters* — Account-level and log-group-level subscription filters are additive. A log group can have up to 1 account-level and up to 2 log-group-level subscription filters.
- *Transformers* — A log-group-level transformer overrides the account-level transformer. If a log group has its own transformer, it ignores the account-level transformer policy.
- *Field index policies* — If a log group has its own field index policy (created with `PutIndexPolicy`), any account-level policy that uses `LogGroupNamePrefix` selection criteria or has no selection criteria is ignored for that log group. However, account-level policies that use `DataSourceName` and `DataSourceType` selection criteria still apply alongside the log-group-level policy.
- *Metric extraction policies* — Metric extraction policies are account-level only and have no log-group-level equivalent, so no conflict resolution applies.

For field index policies, you can configure indexed fields as *facets* to enable interactive exploration of your logs. Facets provide value distributions and counts for indexed fields in the CloudWatch

Logs Insights console without requiring query execution. For more information, see Use facets to group and explore logs.

To use this operation, you must be signed on with the correct permissions depending on the type of policy that you are creating.

- To create a data protection policy, you must have the `logs:PutDataProtectionPolicy` and `logs:PutAccountPolicy` permissions.
- To create a subscription filter policy, you must have the `logs:PutSubscriptionFilter` and `logs:PutAccountPolicy` permissions.
- To create a transformer policy, you must have the `logs:PutTransformer` and `logs:PutAccountPolicy` permissions.
- To create a field index policy, you must have the `logs:PutIndexPolicy` and `logs:PutAccountPolicy` permissions.
- To configure facets for field index policies, you must have the `logs:PutIndexPolicy` and `logs:PutAccountPolicy` permissions.
- To create a metric extraction policy, you must have the `logs:PutMetricExtractionPolicy` and `logs:PutAccountPolicy` permissions.

Data protection policy

A data protection policy can help safeguard sensitive data that's ingested by your log groups by auditing and masking the sensitive log data. Each account can have only one account-level data protection policy.

> **Important**
>
> Sensitive data is detected and masked when it is ingested into a log group. When you set a data protection policy, log events ingested into the log groups before that time are not masked.

If you use `PutAccountPolicy` to create a data protection policy for your whole account, it applies to both existing log groups and all log groups that are created later in this account. The account-level policy is applied to existing log groups with eventual consistency. It might take up to 5 minutes before sensitive data in existing log groups begins to be masked.

By default, when a user views a log event that includes masked data, the sensitive data is replaced by asterisks. A user who has the `logs:Unmask` permission can use a GetLogEvents or FilterLogEvents operation with the `unmask` parameter set to `true` to view the unmasked log events. Users with the `logs:Unmask` can also view unmasked data in the CloudWatch Logs console by running a CloudWatch Logs Insights query with the `unmask` query command.

For more information, including a list of types of data that can be audited and masked, see Protect sensitive log data with masking.

To use the `PutAccountPolicy` operation for a data protection policy, you must be signed on with the `logs:PutDataProtectionPolicy` and `logs:PutAccountPolicy` permissions.

The `PutAccountPolicy` operation applies to all log groups in the account. You can use PutDataProtectionPolicy to create a data protection policy that applies to just one log group. If a log group has its own data protection policy and the account also has an account-level data protection policy, then the two policies are cumulative. Any sensitive term specified in either policy is masked.

Subscription filter policy

A subscription filter policy sets up a real-time feed of log events from CloudWatch Logs to other AWS services. Account-level subscription filter policies apply to both existing log groups and log groups that are created later in this account. Supported destinations are Kinesis Data Streams, Firehose, and Lambda. When log events are sent to the receiving service, they are Base64 encoded and compressed with the GZIP format.

The following destinations are supported for subscription filters:

- An Kinesis Data Streams data stream in the same account as the subscription policy, for same-account delivery.
- An Firehose data stream in the same account as the subscription policy, for same-account delivery.
- A Lambda function in the same account as the subscription policy, for same-account delivery.
- A logical destination in a different account created with PutDestination, for cross-account delivery. Kinesis Data Streams and Firehose are supported as logical destinations.

Each account can have one account-level subscription filter policy per Region. If you are updating an existing filter, you must specify the correct name in `PolicyName`. To perform a

`PutAccountPolicy` subscription filter operation for any destination except a Lambda function, you must also have the `iam:PassRole` permission.

Transformer policy

Creates or updates a *log transformer policy* for your account. You use log transformers to transform log events into a different format, making them easier for you to process and analyze. You can also transform logs from different sources into standardized formats that contain relevant, source-specific information. After you have created a transformer, CloudWatch Logs performs this transformation at the time of log ingestion. You can then refer to the transformed versions of the logs during operations such as querying with CloudWatch Logs Insights or creating metric filters or subscription filters.

You can also use a transformer to copy metadata from metadata keys into the log events themselves. This metadata can include log group name, log stream name, account ID and Region.

A transformer for a log group is a series of processors, where each processor applies one type of transformation to the log events ingested into this log group. For more information about the available processors to use in a transformer, see Processors that you can use.

Having log events in standardized format enables visibility across your applications for your log analysis, reporting, and alarming needs. CloudWatch Logs provides transformation for common log types with out-of-the-box transformation templates for major AWS log sources such as VPC flow logs, Lambda, and Amazon RDS. You can use pre-built transformation templates or create custom transformation policies.

You can create transformers only for the log groups in the Standard log class.

You can have one account-level transformer policy that applies to all log groups in the account. Or you can create as many as 20 account-level transformer policies that are each scoped to a subset of log groups with the `selectionCriteria` parameter. If you have multiple account-level transformer policies with selection criteria, no two of them can use the same or overlapping log group name prefixes. For example, if you have one policy filtered to log groups that start with `my-log`, you can't have another transformer policy filtered to `my-logpprod` or `my-logging`.

You can also set up a transformer at the log-group level. For more information, see PutTransformer. If there is both a log-group level transformer created with `PutTransformer` and an account-level transformer that could apply to the same log group, the log group uses only the log-group level transformer. It ignores the account-level transformer.

Field index policy

You can use field index policies to create indexes on fields found in log events for a log group or data source name and type combination. Creating field indexes can help lower the scan volume for CloudWatch Logs Insights queries that reference those fields, because these queries attempt to skip the processing of log events that are known to not match the indexed field. Good fields to index are fields that you often need to query for and fields or values that match only a small fraction of the total log events. Common examples of indexes include request ID, session ID, user IDs, or instance IDs. For more information, see Create field indexes to improve query performance and reduce costs

To find the fields that are in your log group events, use the GetLogGroupFields operation. To find the fields for a data source use the GetLogFields operation.

For example, suppose you have created a field index for `requestId`. Then, any CloudWatch Logs Insights query on that log group that includes `requestId = value` or `requestId in [value, value, ...]` will attempt to process only the log events where the indexed field matches the specified value.

Matches of log events to the names of indexed fields are case-sensitive. For example, an indexed field of `RequestId` won't match a log event containing `requestId`.

You can have one account-level field index policy that applies to all log groups in the account. Or you can create as many as 20 account-level field index policies that are each scoped to a subset of log groups using `LogGroupNamePrefix` with the `selectionCriteria` parameter. You can have another 20 account-level field index policies using `DataSourceName` and `DataSourceType` for the `selectionCriteria` parameter. If you have multiple account-level index policies with `LogGroupNamePrefix` selection criteria, no two of them can use the same or overlapping log group name prefixes. For example, if you have one policy filtered to log groups that start with *my-log*, you can't have another field index policy filtered to *my-logpprod* or *my-logging*. Similarly, if you have multiple account-level index policies with `DataSourceName` and `DataSourceType` selection criteria, no two of them can use the same data source name and type combination. For example, if you have one policy filtered to the data source name `amazon_vpc` and data source type `flow` you cannot create another policy with this combination.

If you create an account-level field index policy in a monitoring account in cross-account observability, the policy is applied only to the monitoring account and not to any source accounts.

CloudWatch Logs provides default field indexes for all log groups in the Standard log class. Default field indexes are automatically available for the following fields:

- @logStream
- @aws.region
- @aws.account
- @source.log
- @data_source_name
- @data_source_type
- @data_format
- traceId
- severityText
- attributes.session.id

CloudWatch Logs provides default field indexes for certain data source name and type combinations as well. Default field indexes are automatically available for the following data source name and type combinations as identified in the following list:

amazon_vpc.flow

- action
- logStatus
- region
- flowDirection
- type

amazon_route53.resolver_query

- transport
- rcode

aws_waf.access

- action
- httpRequest.country

`aws_cloudtrail.data`, `aws_cloudtrail.management`

- `eventSource`
- `eventName`
- `awsRegion`
- `userAgent`
- `errorCode`
- `eventType`
- `managementEvent`
- `readOnly`
- `eventCategory`
- `requestId`

Default field indexes are in addition to any custom field indexes you define within your policy. Default field indexes are not counted towards your field index quota.

If you want to create a field index policy for a single log group, you can use PutIndexPolicy instead of `PutAccountPolicy`. If you do so, that log group will use that log-group level policy and any account-level policies that match at the data source level; any account-level policy that matches at the log group level (for example, no selection criteria or log group name prefix selection criteria) will be ignored.

Metric extraction policy

A metric extraction policy controls whether CloudWatch Metrics can be created through the Embedded Metrics Format (EMF) for log groups in your account. By default, EMF metric creation is enabled for all log groups. You can use metric extraction policies to disable EMF metric creation for your entire account or specific log groups.

When a policy disables EMF metric creation for a log group, log events in the EMF format are still ingested, but no CloudWatch Metrics are created from them.

> **Important**
>
> Creating a policy disables metrics for AWS features that use EMF to create metrics, such as CloudWatch Container Insights and CloudWatch Application Signals. To prevent turning

off those features by accident, we recommend that you exclude the underlying log-groups through a selection-criteria such as `LogGroupNamePrefix NOT IN ["/aws/containerinsights", "/aws/ecs/containerinsights", "/aws/application-signals/data"]`.

Each account can have either one account-level metric extraction policy that applies to all log groups, or up to 5 policies that are each scoped to a subset of log groups with the `selectionCriteria` parameter. The selection criteria supports filtering by `LogGroupName` and `LogGroupNamePrefix` using the operators `IN` and `NOT IN`. You can specify up to 50 values in each `IN` or `NOT IN` list.

The selection criteria can be specified in these formats:

```
LogGroupName IN ["log-group-1", "log-group-2"]
```

```
LogGroupNamePrefix NOT IN ["/aws/prefix1", "/aws/prefix2"]
```

If you have multiple account-level metric extraction policies with selection criteria, no two of them can have overlapping criteria. For example, if you have one policy with selection criteria `LogGroupNamePrefix IN ["my-log"]`, you can't have another metric extraction policy with selection criteria `LogGroupNamePrefix IN ["/my-log-prod"]` or `LogGroupNamePrefix IN ["/my-logging"]`, as the set of log groups matching these prefixes would be a subset of the log groups matching the first policy's prefix, creating an overlap.

When using `NOT IN`, only one policy with this operator is allowed per account.

When combining policies with `IN` and `NOT IN` operators, the overlap check ensures that policies don't have conflicting effects. Two policies with `IN` and `NOT IN` operators do not overlap if and only if every value in the `IN` policy is completely contained within some value in the `NOT IN` policy. For example:

- If you have a `NOT IN` policy for prefix `"/aws/lambda"`, you can create an `IN` policy for the exact log group name `"/aws/lambda/function1"` because the set of log groups matching `"/aws/lambda/function1"` is a subset of the log groups matching `"/aws/lambda"`.
- If you have a `NOT IN` policy for prefix `"/aws/lambda"`, you cannot create an `IN` policy for prefix `"/aws"` because the set of log groups matching `"/aws"` is not a subset of the log groups matching `"/aws/lambda"`.

Request Syntax

```
{
   "policyDocument": "string",
   "policyName": "string",
   "policyType": "string",
   "scope": "string",
   "selectionCriteria": "string"
}
```

Request Parameters

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

The request accepts the following data in JSON format.

policyDocument

Specify the policy, in JSON.

Data protection policy

A data protection policy must include two JSON blocks:

- The first block must include both a `DataIdentifer` array and an `Operation` property with an `Audit` action. The `DataIdentifer` array lists the types of sensitive data that you want to mask. For more information about the available options, see Types of data that you can mask.

  The `Operation` property with an `Audit` action is required to find the sensitive data terms. This `Audit` action must contain a `FindingsDestination` object. You can optionally use that `FindingsDestination` object to list one or more destinations to send audit findings to. If you specify destinations such as log groups, Firehose streams, and S3 buckets, they must already exist.
- The second block must include both a `DataIdentifer` array and an `Operation` property with an `Deidentify` action. The `DataIdentifer` array must exactly match the `DataIdentifer` array in the first block of the policy.

  The `Operation` property with the `Deidentify` action is what actually masks the data, and it must contain the `"MaskConfig": {}` object. The `"MaskConfig": {}` object must be empty.

For an example data protection policy, see the **Examples** section on this page.

> **Important**
>
> The contents of the two `DataIdentifer` arrays must match exactly.

In addition to the two JSON blocks, the `policyDocument` can also include `Name`, `Description`, and `Version` fields. The `Name` is different than the operation's `policyName` parameter, and is used as a dimension when CloudWatch Logs reports audit findings metrics to CloudWatch.

The JSON specified in `policyDocument` can be up to 30,720 characters long.

Subscription filter policy

A subscription filter policy can include the following attributes in a JSON block:

- **DestinationArn** The ARN of the destination to deliver log events to. Supported destinations are:
  - An Kinesis Data Streams data stream in the same account as the subscription policy, for same-account delivery.
  - An Firehose data stream in the same account as the subscription policy, for same-account delivery.
  - A Lambda function in the same account as the subscription policy, for same-account delivery.
  - A logical destination in a different account created with PutDestination, for cross-account delivery. Kinesis Data Streams and Firehose are supported as logical destinations.
- **RoleArn** The ARN of an IAM role that grants CloudWatch Logs permissions to deliver ingested log events to the destination stream. You don't need to provide the ARN when you are working with a logical destination for cross-account delivery.
- **FilterPattern** A filter pattern for subscribing to a filtered stream of log events.
- **Distribution** The method used to distribute log data to the destination. By default, log data is grouped by log stream, but the grouping can be set to `Random` for a more even distribution. This property is only applicable when the destination is an Kinesis Data Streams data stream.

Transformer policy

A transformer policy must include one JSON block with the array of processors and their configurations. For more information about available processors, see Processors that you can use.

Field index policy

A field index filter policy can include the following attribute in a JSON block:

- **Fields** The array of field indexes to create.
- **FieldsV2** The object of field indexes to create along with it's type.

It must contain at least one field index.

The following is an example of an index policy document that creates indexes with different types.

```
"policyDocument": "{ \"Fields\": [ \"TransactionId\" ], \"FieldsV2\":
{\"RequestId\": {\"type\": \"FIELD_INDEX\"}, \"APIName\": {\"type\":
\"FACET\"}, \"StatusCode\": {\"type\": \"FACET\"}}}"
```

You can use `FieldsV2` to specify the type for each field. Supported types are `FIELD_INDEX` and `FACET`. Field names within `Fields` and `FieldsV2` must be mutually exclusive.

Type: String

Required: Yes

policyName

A name for the policy. This must be unique within the account and cannot start with `aws/`.

Type: String

Required: Yes

policyType

The type of policy that you're creating or updating.

Type: String

Valid Values: `DATA_PROTECTION_POLICY | SUBSCRIPTION_FILTER_POLICY | FIELD_INDEX_POLICY | TRANSFORMER_POLICY | METRIC_EXTRACTION_POLICY`

Required: Yes

scope

Currently the only valid value for this parameter is ALL, which specifies that the data protection policy applies to all log groups in the account. If you omit this parameter, the default of ALL is used.

Type: String

Valid Values: ALL

Required: No

selectionCriteria

Use this parameter to apply the new policy to a subset of log groups in the account or a data source name and type combination.

Specifying selectionCriteria is valid only when you specify SUBSCRIPTION_FILTER_POLICY, FIELD_INDEX_POLICY or TRANSFORMER_POLICYfor policyType.

- If policyType is SUBSCRIPTION_FILTER_POLICY, the only supported selectionCriteria filter is LogGroupName NOT IN []
- If policyType is TRANSFORMER_POLICY, the only supported selectionCriteria filter is LogGroupNamePrefix
- If policyType is FIELD_INDEX_POLICY, the supported selectionCriteria filters are:
  - LogGroupNamePrefix
  - DataSourceName AND DataSourceType

  When you specify selectionCriteria for a field index policy you can use either LogGroupNamePrefix by itself or DataSourceName and DataSourceType together.

The selectionCriteria string can be up to 25KB in length. The length is determined by using its UTF-8 bytes.

Using the selectionCriteria parameter with SUBSCRIPTION_FILTER_POLICY is useful to help prevent infinite loops. For more information, see Log recursion prevention.

Type: String

Required: No

Response Syntax

```
{
   "accountPolicy": {
      "accountId": "string",
      "lastUpdatedTime": number,
      "policyDocument": "string",
      "policyName": "string",
      "policyType": "string",
      "scope": "string",
      "selectionCriteria": "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.

accountPolicy

The account policy that you created.

Type: AccountPolicy object

Errors

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

InvalidParameterException

A parameter is specified incorrectly.

HTTP Status Code: 400

LimitExceededException

You have reached the maximum number of resources that can be created.

HTTP Status Code: 400

OperationAbortedException

Multiple concurrent requests to update the same resource were in conflict.

HTTP Status Code: 400

ServiceUnavailableException

The service cannot complete the request.

HTTP Status Code: 500

Examples

To create a log transformer policy

The following example creates a log transformer that applies to log groups have names that start with `test-`

Sample Request

```
POST / HTTP/1.1
Host: logs.<region>.<domain>
X-Amz-Date: <DATE>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=content-
type;date;host;user-agent;x-amz-date;x-amz-target;x-amzn-requestid,
 Signature=<Signature>
User-Agent: <UserAgentString>
Accept: application/json
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Connection: Keep-Alive
X-Amz-Target: Logs_20140328.PutAccountPolicy
{
    "policyName": "ExamplePolicy",
    "policyType": "TRANSFORMER_POLICY",
    "policyDocument": [
        {
            "parseJSON": {}
        },
        {
            "addKeys": {
                "entries": [
```

```
                    {
                        "key": "metadata.transformed_in",
                        "value": "CloudWatchLogs"
                    }
                ]
            }
        },
        {
            "trimString": {
                "withKeys": [
                    "status"
                ]
            }
        },
        {
            "lowerCaseString": {
                "withKeys": [
                    "status"
                ]
            }
        }
    ],
 "selectionCriteria": 'LogGroupNamePrefix= "test-"'
}
```

To create a metric extraction policy

The following example creates a metric extraction policy that disables EMF metric creation for all log groups except Container Insights log groups.

Sample Request

```
POST / HTTP/1.1
Host: logs.<region>.<domain>
X-Amz-Date: <DATE>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=content-
type;date;host;user-agent;x-amz-date;x-amz-target;x-amzn-requestid,
 Signature=<Signature>
User-Agent: <UserAgentString>
Accept: application/json
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Connection: Keep-Alive
```

```
X-Amz-Target: Logs_20140328.PutAccountPolicy
{
    "policyName": "DisableEMFMetrics",
    "policyType": "METRIC_EXTRACTION_POLICY",
    "policyDocument": {
        "EmbeddedMetricFormat": {
            "Status": "Disabled"
        }
    },
    "selectionCriteria": 'LogGroupNamePrefix NOT IN ["/aws/containerinsights", "/aws/
ecs/containerinsights"]'
}
```

To create an account-wide data protection policy

The following example creates an account-wide log group data protection policy.

Sample Request

```
POST / HTTP/1.1
Host: logs.<region>.<domain>
X-Amz-Date: <DATE>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=content-
type;date;host;user-agent;x-amz-date;x-amz-target;x-amzn-requestid,
 Signature=<Signature>
User-Agent: <UserAgentString>
Accept: application/json
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Connection: Keep-Alive
X-Amz-Target: Logs_20140328.PutAccountPolicy
{
    "policyName": "my_global_data_protection_policy",
    "policyType": "GLOBAL",
    "policyDocument": {
        "Description": "test description",
        "Version": "2021-06-01",
        "Statement": [
            {
                "Sid": "audit-policy test",
                "DataIdentifier": [
                    "arn:aws:dataprotection::aws:data-identifier/EmailAddress",
                    "arn:aws:dataprotection::aws:data-identifier/DriversLicense-US"
```

```
                ],
                "Operation": {
                    "Audit": {
                        "FindingsDestination": {
                            "CloudWatchLogs": {
                                "LogGroup": "EXISTING_LOG_GROUP_IN_YOUR_ACCOUNT"
                            },
                            "Firehose": {
                                "DeliveryStream": "EXISTING_STREAM_IN_YOUR_ACCOUNT"
                            },
                            "S3": {
                                "Bucket": "EXISTING_BUCKET"
                            }
                        }
                    }
                }
            },
            {
            {
                "Sid": "redact-policy",
                "DataIdentifier": [
                    "arn:aws:dataprotection::aws:data-identifier/EmailAddress",
                    "arn:aws:dataprotection::aws:data-identifier/DriversLicense-US"
                ],
                "Operation": {
                    "Deidentify": {
                        "MaskConfig": {}
                    }
                }
            }
        ]
    }
}
```

To create an account-wide subscription filter policy

The following example creates an account-wide subscription filter policy that forwards log events containing the string ERROR to a Kinesis Data Streams stream. The policy applies to all log groups in the account except for `LogGroupToExclude1` and `LogGroupToExclude12`.

Sample Request

```
POST / HTTP/1.1
```

```
Host: logs.<region>.<domain>
X-Amz-Date: <DATE>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=content-
type;date;host;user-agent;x-amz-date;x-amz-target;x-amzn-requestid,
 Signature=<Signature>
User-Agent: <UserAgentString>
Accept: application/json
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Connection: Keep-Alive
X-Amz-Target: Logs_20140328.PutAccountPolicy
{
    "policyName": "ExamplePolicy",
    "policyType": "SUBSCRIPTION_FILTER_POLICY",
    "policyDocument": {
        "DestinationArn":"arn:aws:kinesis:region:111111111111:stream/TestStream",
        "RoleArn":"arn:aws:iam::111111111111:role/CWLtoKinesisRole",
        "FilterPattern": "ERROR",
        "Distribution": "Random"
    },
    "selectionCriteria": 'LogGroupName NOT IN ["LogGroupToExclude1",
 "LogGroupToExclude2"]'
}
```

To create an account-wide field index policy

The following example creates an account-wide field index policy for log groups with names that start with `lambda`.

Sample Request

```
POST / HTTP/1.1
Host: logs.<region>.<domain>
X-Amz-Date: <DATE>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=content-
type;date;host;user-agent;x-amz-date;x-amz-target;x-amzn-requestid,
 Signature=<Signature>
User-Agent: <UserAgentString>
Accept: application/json
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Connection: Keep-Alive
X-Amz-Target: Logs_20140328.PutAccountPolicy
```

```
{
    "policyDocument": {
        "Fields": ["RequestId", "TransactionId"]
     },
    "policyName": "LambdaIndexPolicy",
    "policyType" : "FIELD_INDEX_POLICY",
    "scope" : "ALL",
    "selectionCriteria": 'LogGroupNamePrefix="lambda"'
}
```

See Also

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

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

PutBearerTokenAuthentication

Enables or disables bearer token authentication for the specified log group. When enabled on a log group, bearer token authentication is enabled on operations until it is explicitly disabled.

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

Request Syntax

```
{
   "bearerTokenAuthenticationEnabled": boolean,
   "logGroupIdentifier": "string"
}
```

Request Parameters

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

The request accepts the following data in JSON format.

bearerTokenAuthenticationEnabled

Whether to enable bearer token authentication.

Type: Boolean

Required: Yes

Type: Boolean

Required: Yes

logGroupIdentifier

The name or ARN of the log group.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `[\.\-_/#A-Za-z0-9]+`

Required: Yes

Type: String

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

Pattern: `[\w#+=/:,.@-]*`

Required: Yes

Response Elements

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

Errors

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

AccessDeniedException

You don't have sufficient permissions to perform this action.

HTTP Status Code: 400

InvalidOperationException

The operation is not valid on the specified resource.

HTTP Status Code: 400

InvalidParameterException

A parameter is specified incorrectly.

HTTP Status Code: 400

OperationAbortedException

Multiple concurrent requests to update the same resource were in conflict.

HTTP Status Code: 400

ResourceNotFoundException

The specified resource does not exist.

HTTP Status Code: 400

ServiceUnavailableException

The service cannot complete the request.

HTTP Status Code: 500

Examples

Sample Request

This example illustrates one usage of PutBearerTokenAuthentication.

Sample Request

```
POST / HTTP/1.1
          Host: logs.<region>.<domain>
          X-Amz-Date: <DATE>
          Authorization: AWS4-HMAC-SHA256 Credential=<Credential>,
 SignedHeaders=content-type;date;host;user-agent;x-amz-date;x-amz-target;x-amzn-
requestid, Signature=<Signature>
          User-Agent: <UserAgentString>
          Accept: application/json
          Content-Type: application/x-amz-json-1.1
          Content-Length: <PayloadSizeBytes>
          Connection: Keep-Alive
          X-Amz-Target: Logs_20140328.PutBearerTokenAuthentication
          {
          "logGroupIdentifier": "my-log-group",
          "bearerTokenAuthenticationEnabled": true
          }
```

Sample Response

```
HTTP/1.1 200 OK
          x-amzn-RequestId: <RequestId>
          Content-Type: application/x-amz-json-1.1
          Content-Length: 0
          Date: <Date>
```

See Also

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

- AWS Command Line Interface V2

- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

PutDataProtectionPolicy

Creates a data protection policy for the specified log group. A data protection policy can help safeguard sensitive data that's ingested by the log group by auditing and masking the sensitive log data.

> **Important**
>
> Sensitive data is detected and masked when it is ingested into the log group. When you set a data protection policy, log events ingested into the log group before that time are not masked.

By default, when a user views a log event that includes masked data, the sensitive data is replaced by asterisks. A user who has the `logs:Unmask` permission can use a GetLogEvents or FilterLogEvents operation with the `unmask` parameter set to `true` to view the unmasked log events. Users with the `logs:Unmask` can also view unmasked data in the CloudWatch Logs console by running a CloudWatch Logs Insights query with the `unmask` query command.

For more information, including a list of types of data that can be audited and masked, see Protect sensitive log data with masking.

The `PutDataProtectionPolicy` operation applies to only the specified log group. You can also use PutAccountPolicy to create an account-level data protection policy that applies to all log groups in the account, including both existing log groups and log groups that are created level. If a log group has its own data protection policy and the account also has an account-level data protection policy, then the two policies are cumulative. Any sensitive term specified in either policy is masked.

Request Syntax

```
{
   "logGroupIdentifier": "string",
   "policyDocument": "string"
}
```

Request Parameters

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

The request accepts the following data in JSON format.

logGroupIdentifier

Specify either the log group name or log group ARN.

Type: String

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

Pattern: `[\w#+=/:,.@-]*`

Required: Yes

policyDocument

Specify the data protection policy, in JSON.

This policy must include two JSON blocks:

- The first block must include both a `DataIdentifer` array and an `Operation` property with an `Audit` action. The `DataIdentifer` array lists the types of sensitive data that you want to mask. For more information about the available options, see Types of data that you can mask.

  The `Operation` property with an `Audit` action is required to find the sensitive data terms. This `Audit` action must contain a `FindingsDestination` object. You can optionally use that `FindingsDestination` object to list one or more destinations to send audit findings to. If you specify destinations such as log groups, Firehose streams, and S3 buckets, they must already exist.
- The second block must include both a `DataIdentifer` array and an `Operation` property with an `Deidentify` action. The `DataIdentifer` array must exactly match the `DataIdentifer` array in the first block of the policy.

  The `Operation` property with the `Deidentify` action is what actually masks the data, and it must contain the `"MaskConfig": {}` object. The `"MaskConfig": {}` object must be empty.

For an example data protection policy, see the **Examples** section on this page.

> **Important**
>
> The contents of the two `DataIdentifer` arrays must match exactly.

In addition to the two JSON blocks, the `policyDocument` can also include `Name`, `Description`, and `Version` fields. The `Name` is used as a dimension when CloudWatch Logs reports audit findings metrics to CloudWatch.

The JSON specified in `policyDocument` can be up to 30,720 characters.

Type: String

Required: Yes

Response Syntax

```
{
   "lastUpdatedTime": number,
   "logGroupIdentifier": "string",
   "policyDocument": "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.

lastUpdatedTime

The date and time that this policy was most recently updated.

Type: Long

Valid Range: Minimum value of 0.

logGroupIdentifier

The log group name or ARN that you specified in your request.

Type: String

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

Pattern: `[\w#+=/:,.@-]*`

policyDocument

The data protection policy used for this log group.

Type: String

Errors

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

InvalidParameterException

A parameter is specified incorrectly.

HTTP Status Code: 400

LimitExceededException

You have reached the maximum number of resources that can be created.

HTTP Status Code: 400

OperationAbortedException

Multiple concurrent requests to update the same resource were in conflict.

HTTP Status Code: 400

ResourceNotFoundException

The specified resource does not exist.

HTTP Status Code: 400

ServiceUnavailableException

The service cannot complete the request.

HTTP Status Code: 500

Examples

To create a data protection policy

The following example creates a data protection policy in the log group.

Sample Request

```
POST / HTTP/1.1
Host: logs.<region>.<domain>
X-Amz-Date: <DATE>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=content-
type;date;host;user-agent;x-amz-date;x-amz-target;x-amzn-requestid,
 Signature=<Signature>
User-Agent: <UserAgentString>
Accept: application/json
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Connection: Keep-Alive
X-Amz-Target: Logs_20140328.PutDataProtectionPolicy
{
    "logGroupIdentifier": "my-log-group",
    "policyDocument": {
        "Name": "data-protection-policy",
        "Description": "test description",
        "Version": "2021-06-01",
        "Statement": [
            {
                "Sid": "audit-policy test",
                "DataIdentifier": [
                    "arn:aws:dataprotection::aws:data-identifier/EmailAddress",
                    "arn:aws:dataprotection::aws:data-identifier/DriversLicense-US"
                ],
                "Operation": {
                    "Audit": {
                        "FindingsDestination": {
                            "CloudWatchLogs": {
                                "LogGroup": "EXISTING_LOG_GROUP_IN_YOUR_ACCOUNT"
                            },
                            "Firehose": {
                                "DeliveryStream": "EXISTING_STREAM_IN_YOUR_ACCOUNT"
                            },
                            "S3": {
                                "Bucket": "EXISTING_BUCKET"
                            }
                        }
                    }
                }
            },
            {
```

```
                "Sid": "redact-policy",
                "DataIdentifier": [
                    "arn:aws:dataprotection::aws:data-identifier/EmailAddress",
                    "arn:aws:dataprotection::aws:data-identifier/DriversLicense-US"
                ],
                "Operation": {
                    "Deidentify": {
                        "MaskConfig": {}
                    }
                }
            }
        ]
    }
}
```

Sample Response

```
HTTP/1.1 200 OK
x-amzn-RequestId: <RequestId>
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Date: <Date>
```

To create a log transformer policy

The following example creates a log transformer policy in the account that applies to all log groups with names that start with `test-`.

Sample Request

```
POST / HTTP/1.1
Host: logs.<region>.<domain>
X-Amz-Date: <DATE>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=content-
type;date;host;user-agent;x-amz-date;x-amz-target;x-amzn-requestid,
 Signature=<Signature>
User-Agent: <UserAgentString>
Accept: application/json
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Connection: Keep-Alive
X-Amz-Target: Logs_20140328.PutDataProtectionPolicy
```

```
{
    "policyName": "ExampleTransformerPolicy",
    "policyType": "TRANSFORMER_POLICY",
    "selectionCriteria": 'LogGroupNamePrefix = "test-"'
    "policyDocument": [
        {
            "parseJSON": {}
        },
        {
            "addKeys": {
                "entries": [
                    {
                        "key": "metadata.transformed_in",
                        "value": "CloudWatchLogs"
                    }
                ]
            }
        },
        {
            "trimString": {
                "withKeys": [
                    "status"
                ]
            }
        },
        {
            "lowerCaseString": {
                "withKeys": [
                    "status"
                ]
            }
        }
    ]
        ]
    }
```

Sample Response

```
HTTP/1.1 200 OK
x-amzn-RequestId: <RequestId>
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Date: <Date>
```

To create a field index policy

The following example creates an account-level field index policy that is scoped to log groups that have names that begin with `test`. The policy indexed two fields in these log groups, `RequestId` and `TransactionId`

Sample Request

```
{
    "policyName": "my_indexing_account_policy",
    "policyType": "FIELD_INDEX_POLICY",
    "policyDocument": {
        "Fields": ["RequestId", "TransactionId"]
    },
    "selectionCriteria": 'LogGroupNamePrefix = "test"'
}
```

See Also

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

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

PutDeliveryDestination

Creates or updates a logical *delivery destination*. A delivery destination is an AWS resource that represents an AWS service that logs can be sent to. CloudWatch Logs, Amazon S3, and Firehose are supported as logs delivery destinations and X-Ray as the trace delivery destination.

To configure logs delivery between a supported AWS service and a destination, you must do the following:

- Create a delivery source, which is a logical object that represents the resource that is actually sending the logs. For more information, see PutDeliverySource.
- Use `PutDeliveryDestination` to create a *delivery destination* in the same account of the actual delivery destination. The delivery destination that you create is a logical object that represents the actual delivery destination.
- If you are delivering logs cross-account, you must use PutDeliveryDestinationPolicy in the destination account to assign an IAM policy to the destination. This policy allows delivery to that destination.
- Use `CreateDelivery` to create a *delivery* by pairing exactly one delivery source and one delivery destination. For more information, see CreateDelivery.

You can configure a single delivery source to send logs to multiple destinations by creating multiple deliveries. You can also create multiple deliveries to configure multiple delivery sources to send logs to the same delivery destination.

Only some AWS services support being configured as a delivery source. These services are listed as **Supported [V2 Permissions]** in the table at Enabling logging from AWS services.

If you use this operation to update an existing delivery destination, all the current delivery destination parameters are overwritten with the new parameter values that you specify.

Request Syntax

```
{
   "deliveryDestinationConfiguration": {
      "destinationResourceArn": "string"
   },
   "deliveryDestinationType": "string",
   "name": "string",
```

```
   "outputFormat": "string",
   "tags": {
      "string" : "string"
   }
}
```

Request Parameters

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

The request accepts the following data in JSON format.

deliveryDestinationConfiguration

A structure that contains the ARN of the AWS resource that will receive the logs.

> **Note**
>
> `deliveryDestinationConfiguration` is required for CloudWatch Logs, Amazon S3, Firehose log delivery destinations and not required for X-Ray trace delivery destinations. `deliveryDestinationType` is needed for X-Ray trace delivery destinations but not required for other logs delivery destinations.

Type: DeliveryDestinationConfiguration object

Required: No

deliveryDestinationType

The type of delivery destination. This parameter specifies the target service where log data will be delivered. Valid values include:

- `S3` - Amazon S3 for long-term storage and analytics
- `CWL` - CloudWatch Logs for centralized log management
- `FH` - Amazon Kinesis Data Firehose for real-time data streaming
- `XRAY` - AWS X-Ray for distributed tracing and application monitoring

The delivery destination type determines the format and configuration options available for log delivery.

Type: String

Valid Values: `S3 | CWL | FH | XRAY`

Required: No

name

A name for this delivery destination. This name must be unique for all delivery destinations in your account.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 60.

Pattern: `[\w-]*`

Required: Yes

outputFormat

The format for the logs that this delivery destination will receive.

Type: String

Valid Values: `json | plain | w3c | raw | parquet`

Required: No

tags

An optional list of key-value pairs to associate with the resource.

For more information about tagging, see Tagging AWS resources

Type: String to string map

Map Entries: Maximum number of 50 items.

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

Key Pattern: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]+)$`

Value Length Constraints: Maximum length of 256.

Value Pattern: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$`

Required: No

Response Syntax

```
{
   "deliveryDestination": {
      "arn": "string",
      "deliveryDestinationConfiguration": {
         "destinationResourceArn": "string"
      },
      "deliveryDestinationType": "string",
      "name": "string",
      "outputFormat": "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.

deliveryDestination

A structure containing information about the delivery destination that you just created or updated.

Type: DeliveryDestination object

Errors

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

ConflictException

This operation attempted to create a resource that already exists.

HTTP Status Code: 400

ResourceNotFoundException

The specified resource does not exist.

HTTP Status Code: 400

ServiceQuotaExceededException

This request exceeds a service quota.

HTTP Status Code: 400

ServiceUnavailableException

The service cannot complete the request.

HTTP Status Code: 500

ThrottlingException

The request was throttled because of quota limits.

HTTP Status Code: 400

ValidationException

One of the parameters for the request is not valid.

HTTP Status Code: 400

See Also

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

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin

- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

PutDeliveryDestinationPolicy

Creates and assigns an IAM policy that grants permissions to CloudWatch Logs to deliver logs cross-account to a specified destination in this account. To configure the delivery of logs from an AWS service in another account to a logs delivery destination in the current account, you must do the following:

- Create a delivery source, which is a logical object that represents the resource that is actually sending the logs. For more information, see PutDeliverySource.
- Create a *delivery destination*, which is a logical object that represents the actual delivery destination. For more information, see PutDeliveryDestination.
- Use this operation in the destination account to assign an IAM policy to the destination. This policy allows delivery to that destination.
- Create a *delivery* by pairing exactly one delivery source and one delivery destination. For more information, see CreateDelivery.

Only some AWS services support being configured as a delivery source. These services are listed as **Supported [V2 Permissions]** in the table at Enabling logging from AWS services.

The contents of the policy must include two statements. One statement enables general logs delivery, and the other allows delivery to the chosen destination. See the examples for the needed policies.

Request Syntax

```
{
   "deliveryDestinationName": "string",
   "deliveryDestinationPolicy": "string"
}
```

Request Parameters

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

The request accepts the following data in JSON format.

deliveryDestinationName

The name of the delivery destination to assign this policy to.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 60.

Pattern: `[\w-]*`

Required: Yes

deliveryDestinationPolicy

The contents of the policy.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 51200.

Required: Yes

Response Syntax

```
{
   "policy": {
      "deliveryDestinationPolicy": "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.

policy

The contents of the policy that you just created.

Type: Policy object

Errors

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

ConflictException

This operation attempted to create a resource that already exists.

HTTP Status Code: 400

ResourceNotFoundException

The specified resource does not exist.

HTTP Status Code: 400

ServiceUnavailableException

The service cannot complete the request.

HTTP Status Code: 500

ValidationException

One of the parameters for the request is not valid.

HTTP Status Code: 400

Examples

Policy to use with PutDeliveryDestination

The following example creates a policy that grants permission to CloudWatch Logs to deliver logs cross-account to a destination in the current account.

Sample Request

```
POST / HTTP/1.1
Host: logs.<region>.<domain>
X-Amz-Date: <DATE>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=content-
type;date;host;user-agent;x-amz-date;x-amz-target;x-amzn-requestid,
 Signature=<Signature>
User-Agent: <UserAgentString>
Accept: application/json
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
```

```
Connection: Keep-Alive
X-Amz-Target: Logs_20140328.PutDeliveryDestinationPolicy
{
   "deliveryDestinationName": "DeliveryDestinationName",
   "deliveryDestinationPolicy": "{
      "Version": "2012-10-17",
      "Statement": [
        {
          "Sid": "AllowLogDeliveryActions",
          "Effect": "Allow",
          "Principal": {
            "AWS": "arn:aws:iam::AccountID:root"
          },
          "Action": "logs:CreateDelivery",
          "Resource": [
            "arn:aws:logs:us-east-1:AccountID:delivery-source:*",
            "arn:aws:logs:us-east-1:AccountID:delivery:*",
            "arn:aws:logs:us-east-1:AccountID:delivery-destination:*"
          ]
        }
      ]
    }"
}
```

See Also

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

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

PutDeliverySource

Creates or updates a logical *delivery source*. A delivery source represents an AWS resource that sends logs to an logs delivery destination. The destination can be CloudWatch Logs, Amazon S3, Firehose or X-Ray for sending traces.

To configure logs delivery between a delivery destination and an AWS service that is supported as a delivery source, you must do the following:

- Use `PutDeliverySource` to create a delivery source, which is a logical object that represents the resource that is actually sending the logs.
- Use `PutDeliveryDestination` to create a *delivery destination*, which is a logical object that represents the actual delivery destination. For more information, see PutDeliveryDestination.
- If you are delivering logs cross-account, you must use PutDeliveryDestinationPolicy in the destination account to assign an IAM policy to the destination. This policy allows delivery to that destination.
- Use `CreateDelivery` to create a *delivery* by pairing exactly one delivery source and one delivery destination. For more information, see CreateDelivery.

You can configure a single delivery source to send logs to multiple destinations by creating multiple deliveries. You can also create multiple deliveries to configure multiple delivery sources to send logs to the same delivery destination.

Only some AWS services support being configured as a delivery source. These services are listed as **Supported [V2 Permissions]** in the table at Enabling logging from AWS services.

If you use this operation to update an existing delivery source, all the current delivery source parameters are overwritten with the new parameter values that you specify.

Request Syntax

```
{
   "deliverySourceConfiguration": {
      "string" : "string"
   },
   "logType": "string",
   "name": "string",
   "resourceArn": "string",
```

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

Request Parameters

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

The request accepts the following data in JSON format.

deliverySourceConfiguration

A map of key-value pairs to configure the delivery source. Both keys and values must be between 1 and 255 characters in length. For example, `{"samplingRate": "50"}`.

Type: String to string map

Key Length Constraints: Minimum length of 1. Maximum length of 255.

Value Length Constraints: Minimum length of 1. Maximum length of 255.

Required: No

logType

Defines the type of log that the source is sending.

- For Application Load Balancer, the valid values are `ALB_ACCESS_LOGS`, `ALB_CONNECTION_LOGS`, and `ALB_HEALTH_CHECK_LOGS`.
- For Amazon Bedrock Agents, the valid values are `APPLICATION_LOGS` and `EVENT_LOGS`.
- For Amazon Bedrock Knowledge Bases, the valid values are `APPLICATION_LOGS` and `TRACES`.
- For Amazon Bedrock AgentCore Runtime, the valid values are `APPLICATION_LOGS`, `USAGE_LOGS` and `TRACES`.
- For Amazon Bedrock AgentCore Tools, the valid values are `APPLICATION_LOGS`, `USAGE_LOGS` and `TRACES`.
- For Amazon Bedrock AgentCore Identity, the valid values are `APPLICATION_LOGS` and `TRACES`.
- For Amazon Bedrock AgentCore Memory, the valid values are `APPLICATION_LOGS` and `TRACES`.

- For Amazon Bedrock AgentCore Gateway, the valid values are APPLICATION_LOGS and TRACES.
- For Amazon Bedrock AgentCore Payments, the valid values are APPLICATION_LOGS and TRACES.
- For CloudFront, the valid value is ACCESS_LOGS.
- For DevOps Agent, the valid value is APPLICATION_LOGS.
- For Amazon CodeWhisperer, the valid value is EVENT_LOGS.
- For Elemental MediaPackage, the valid values are EGRESS_ACCESS_LOGS and INGRESS_ACCESS_LOGS.
- For Elemental MediaTailor, the valid values are AD_DECISION_SERVER_LOGS, MANIFEST_SERVICE_LOGS, and TRANSCODE_LOGS.
- For Amazon EKS Auto Mode, the valid values are AUTO_MODE_BLOCK_STORAGE_LOGS, AUTO_MODE_COMPUTE_LOGS, AUTO_MODE_IPAM_LOGS, and AUTO_MODE_LOAD_BALANCING_LOGS.
- For Amazon EKS Capability Logs, the valid values are EKS_CAPABILITY_ACK_LOGS, EKS_CAPABILITY_ARGOCD_APPLICATION_LOGS, EKS_CAPABILITY_ARGOCD_APPLICATIONSET_LOGS, EKS_CAPABILITY_ARGOCD_COMMITSERVER_LOGS, EKS_CAPABILITY_ARGOCD_REPOSERVER_LOGS, EKS_CAPABILITY_ARGOCD_SERVER_LOGS, and EKS_CAPABILITY_KRO_LOGS.
- For AWS Entity Resolution, the valid value is WORKFLOW_LOGS.
- For IAM Identity Center, the valid value is ERROR_LOGS.
- For Network Firewall Proxy, the valid values are ALERT_LOGS, ALLOW_LOGS, and DENY_LOGS.
- For Network Load Balancer, the valid value is NLB_ACCESS_LOGS.
- For AWS PCS, the valid values are PCS_SCHEDULER_LOGS, PCS_JOBCOMP_LOGS, and PCS_SCHEDULER_AUDIT_LOGS.
- For Quick, the valid values are AGENT_HOURS_LOGS, CHAT_LOGS, FEEDBACK_LOGS, and INDEX_USAGE_LOGS.
- For AWS RTB Fabric, the valid values is APPLICATION_LOGS.
- For Amazon Q, the valid values are EVENT_LOGS and SYNC_JOB_LOGS.
- For Amazon S3, the valid value is S3_SERVER_ACCESS_LOGS.
- For AWS Security Hub CSPM, the valid value is SECURITY_FINDING_LOGS.

- For AWS Security Hub, the valid value is `SECURITY_FINDING_LOGS`.
- For Amazon SES mail manager, the valid values are `APPLICATION_LOGS` and `TRAFFIC_POLICY_DEBUG_LOGS`.
- For Amazon WorkMail, the valid values are `ACCESS_CONTROL_LOGS`, `AUTHENTICATION_LOGS`, `WORKMAIL_AVAILABILITY_PROVIDER_LOGS`, `WORKMAIL_MAILBOX_ACCESS_LOGS`, and `WORKMAIL_PERSONAL_ACCESS_TOKEN_LOGS`.
- For Amazon VPC Route Server, the valid value is `EVENT_LOGS`.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 255.

Pattern: `[\w]*`

Required: Yes

name

A name for this delivery source. This name must be unique for all delivery sources in your account.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 60.

Pattern: `[\w-]*`

Required: Yes

resourceArn

The ARN of the AWS resource that is generating and sending logs. For example, `arn:aws:workmail:us-east-1:123456789012:organization/m-1234EXAMPLEabcd1234abcd1234abcd1234`

For the `SECURITY_FINDING_LOGS` logType, use a wildcard ARN for the hub resource. For AWS Security Hub CSPM, use `arn:aws:securityhub:us-east-1:111122223333:hub/*` and for AWS Security Hub, use `arn:aws:securityhub:us-east-1:111122223333:hubv2/*`

Type: String

Required: Yes

tags

An optional list of key-value pairs to associate with the resource.

For more information about tagging, see Tagging AWS resources

Type: String to string map

Map Entries: Maximum number of 50 items.

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

Key Pattern: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]+)$`

Value Length Constraints: Maximum length of 256.

Value Pattern: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$`

Required: No

Response Syntax

```
{
   "deliverySource": {
      "arn": "string",
      "deliverySourceConfiguration": {
         "string" : "string"
      },
      "logType": "string",
      "name": "string",
      "resourceArns": [ "string" ],
      "service": "string",
      "status": "string",
      "statusReason": "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.

deliverySource

A structure containing information about the delivery source that was just created or updated.

Type: DeliverySource object

Errors

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

ConflictException

This operation attempted to create a resource that already exists.

HTTP Status Code: 400

ResourceNotFoundException

The specified resource does not exist.

HTTP Status Code: 400

ServiceQuotaExceededException

This request exceeds a service quota.

HTTP Status Code: 400

ServiceUnavailableException

The service cannot complete the request.

HTTP Status Code: 500

ThrottlingException

The request was throttled because of quota limits.

HTTP Status Code: 400

ValidationException

One of the parameters for the request is not valid.

HTTP Status Code: 400

See Also

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

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

PutDestination

Creates or updates a destination. This operation is used only to create destinations for cross-account subscriptions.

A destination encapsulates a physical resource (such as an Amazon Kinesis stream). With a destination, you can subscribe to a real-time stream of log events for a different account, ingested using PutLogEvents.

Through an access policy, a destination controls what is written to it. By default, `PutDestination` does not set any access policy with the destination, which means a cross-account user cannot call PutSubscriptionFilter against this destination. To enable this, the destination owner must call PutDestinationPolicy after `PutDestination`.

To perform a `PutDestination` operation, you must also have the `iam:PassRole` permission.

Request Syntax

```
{
   "destinationName": "string",
   "roleArn": "string",
   "tags": {
      "string" : "string"
   },
   "targetArn": "string"
}
```

Request Parameters

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

The request accepts the following data in JSON format.

destinationName

A name for the destination.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `[^:*]*`

Required: Yes

roleArn

The ARN of an IAM role that grants CloudWatch Logs permissions to call the Amazon Kinesis `PutRecord` operation on the destination stream.

Type: String

Length Constraints: Minimum length of 1.

Required: Yes

tags

An optional list of key-value pairs to associate with the resource.

For more information about tagging, see Tagging AWS resources

Type: String to string map

Map Entries: Maximum number of 50 items.

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

Key Pattern: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]+)$`

Value Length Constraints: Maximum length of 256.

Value Pattern: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$`

Required: No

targetArn

The ARN of an Amazon Kinesis stream to which to deliver matching log events.

Type: String

Length Constraints: Minimum length of 1.

Required: Yes

Response Syntax

```
{
```

```
   "destination": {
      "accessPolicy": "string",
      "arn": "string",
      "creationTime": number,
      "destinationName": "string",
      "roleArn": "string",
      "targetArn": "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.

destination

The destination.

Type: Destination object

Errors

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

InvalidParameterException

A parameter is specified incorrectly.

HTTP Status Code: 400

OperationAbortedException

Multiple concurrent requests to update the same resource were in conflict.

HTTP Status Code: 400

ServiceUnavailableException

The service cannot complete the request.

HTTP Status Code: 500

Examples

To create or update a destination

The following example creates the specified destination.

Sample Request

```
POST / HTTP/1.1
Host: logs.<region>.<domain>
X-Amz-Date: <DATE>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=content-
type;date;host;user-agent;x-amz-date;x-amz-target;x-amzn-requestid,
 Signature=<Signature>
User-Agent: <UserAgentString>
Accept: application/json
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Connection: Keep-Alive
X-Amz-Target: Logs_20140328.PutDestination
{
  "destinationName": "my-destination",
  "targetArn": "arn:aws:kinesis:us-east-1:123456789012:stream/my-kinesis-stream",
  "roleArn": "arn:aws:iam::123456789012:role/my-subscription-role"
}
```

Sample Response

```
HTTP/1.1 200 OK
x-amzn-RequestId: <RequestId>
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Date: <Date>
{
  "destination": [
    {
      "destinationName": "my-destination",
      "targetArn": "arn:aws:kinesis:us-east-1:123456789012:stream/my-kinesis-stream",
      "roleArn": "arn:aws:iam::123456789012:role/my-subscription-role",
      "arn": "arn:aws:logs:us-east-1:123456789012:destination:my-destination",
      "creationTime": 1437584472382
    }
  ]
```

```
}
```

See Also

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

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

PutDestinationPolicy

Creates or updates an access policy associated with an existing destination. An access policy is an IAM policy document that is used to authorize claims to register a subscription filter against a given destination.

Request Syntax

```
{
   "accessPolicy": "string",
   "destinationName": "string",
   "forceUpdate": boolean
}
```

Request Parameters

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

The request accepts the following data in JSON format.

accessPolicy

An IAM policy document that authorizes cross-account users to deliver their log events to the associated destination. This can be up to 5120 bytes.

Type: String

Length Constraints: Minimum length of 1.

Required: Yes

destinationName

A name for an existing destination.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `[^:*]*`

Required: Yes

forceUpdate

Specify true if you are updating an existing destination policy to grant permission to an organization ID instead of granting permission to individual AWS accounts. Before you update a destination policy this way, you must first update the subscription filters in the accounts that send logs to this destination. If you do not, the subscription filters might stop working. By specifying `true` for `forceUpdate`, you are affirming that you have already updated the subscription filters. For more information, see Updating an existing cross-account subscription

If you omit this parameter, the default of `false` is used.

Type: Boolean

Required: No

Response Elements

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

Errors

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

InvalidParameterException

A parameter is specified incorrectly.

HTTP Status Code: 400

OperationAbortedException

Multiple concurrent requests to update the same resource were in conflict.

HTTP Status Code: 400

ServiceUnavailableException

The service cannot complete the request.

HTTP Status Code: 500

Examples

To create or update an access policy of a destination

The following example updates the access policy of the specified destination.

Sample Request

```
POST / HTTP/1.1
Host: logs.<region>.<domain>
X-Amz-Date: <DATE>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=content-
type;date;host;user-agent;x-amz-date;x-amz-target;x-amzn-requestid,
 Signature=<Signature>
User-Agent: <UserAgentString>
Accept: application/json
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Connection: Keep-Alive
X-Amz-Target: Logs_20140328.PutDestinationPolicy
{
  "destinationName": "my-destination",
  "accessPolicy": "{ \"Version\": \"2012-10-17\", \"Statement\": [{ \"Effect
\": \"Allow\", \"Principal\": { \"AWS\": \"111111111111\"}, \"Action
\": \"logs:PutSubscriptionFilter\",\"Resource\": \"arn:aws:logs:us-
east-1:123456789012:destination:my-destination\"}]}"
}
```

Sample Response

```
HTTP/1.1 200 OK
x-amzn-RequestId: <RequestId>
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Date: <Date>
```

See Also

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

- AWS Command Line Interface V2

- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

PutIndexPolicy

Creates or updates a *field index policy* for the specified log group. Only log groups in the Standard log class support field index policies. For more information about log classes, see Log classes.

You can use field index policies to create *field indexes* on fields found in log events in the log group. Creating field indexes speeds up and lowers the costs for CloudWatch Logs Insights queries that reference those field indexes, because these queries attempt to skip the processing of log events that are known to not match the indexed field. Good fields to index are fields that you often need to query for and fields or values that match only a small fraction of the total log events. Common examples of indexes include request ID, session ID, userID, and instance IDs. For more information, see Create field indexes to improve query performance and reduce costs.

You can configure indexed fields as *facets* to enable interactive exploration and filtering of your logs in the CloudWatch Logs Insights console. Facets allow you to view value distributions and counts for indexed fields without running queries. When you create a field index, you can optionally set it as a facet to enable this interactive analysis capability. For more information, see Use facets to group and explore logs.

To find the fields that are in your log group events, use the GetLogGroupFields operation.

For example, suppose you have created a field index for `requestId`. Then, any CloudWatch Logs Insights query on that log group that includes `requestId = value` or `requestId IN [value, value, ...]` will process fewer log events to reduce costs, and have improved performance.

CloudWatch Logs provides default field indexes for all log groups in the Standard log class. Default field indexes are automatically available for the following fields:

- `@logStream`
- `@aws.region`
- `@aws.account`
- `@source.log`
- `traceId`

Default field indexes are in addition to any custom field indexes you define within your policy. Default field indexes are not counted towards your field index quota.

Each index policy has the following quotas and restrictions:

- As many as 20 fields can be included in the policy.
- Each field name can include as many as 100 characters.

Matches of log events to the names of indexed fields are case-sensitive. For example, a field index of `RequestId` won't match a log event containing `requestId`.

Log group-level field index policies created with `PutIndexPolicy` override account-level field index policies created with PutAccountPolicy that apply to log groups. If you use `PutIndexPolicy` to create a field index policy for a log group, that log group uses only that policy for log group-level indexing, including any facet configurations. The log group ignores any account-wide field index policy that applies to log groups, but data source-based account policies may still apply.

Request Syntax

```
{
   "logGroupIdentifier": "string",
   "policyDocument": "string"
}
```

Request Parameters

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

The request accepts the following data in JSON format.

logGroupIdentifier

Specify either the log group name or log group ARN to apply this field index policy to. If you specify an ARN, use the format arn:aws:logs:*region*:*account-id*:log-group:*log_group_name* Don't include an * at the end.

Type: String

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

Pattern: `[\w#+=/:,.@-]*`

Required: Yes

policyDocument

The index policy document, in JSON format. The following is an example of an index policy document that creates indexes with different types.

```
"policyDocument": "{"Fields": [ "TransactionId" ], "FieldsV2":
{"RequestId": {"type": "FIELD_INDEX"}, "APIName": {"type": "FACET"},
"StatusCode": {"type": "FACET"}}}"
```

You can use `FieldsV2` to specify the type for each field. Supported types are `FIELD_INDEX` and `FACET`. Field names within `Fields` and `FieldsV2` must be mutually exclusive.

The policy document must include at least one field index. For more information about the fields that can be included and other restrictions, see Field index syntax and quotas.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 51200.

Required: Yes

Response Syntax

```
{
   "indexPolicy": {
      "lastUpdateTime": number,
      "logGroupIdentifier": "string",
      "policyDocument": "string",
      "policyName": "string",
      "source": "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.

indexPolicy

The index policy that you just created or updated.

Type: IndexPolicy object

Errors

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

InvalidParameterException

A parameter is specified incorrectly.

HTTP Status Code: 400

LimitExceededException

You have reached the maximum number of resources that can be created.

HTTP Status Code: 400

OperationAbortedException

Multiple concurrent requests to update the same resource were in conflict.

HTTP Status Code: 400

ResourceNotFoundException

The specified resource does not exist.

HTTP Status Code: 400

ServiceUnavailableException

The service cannot complete the request.

HTTP Status Code: 500

Examples

Create index policy for a log group

The following example creates an index policy that indexes two fields, `RequestId` and `TransactionId`.

Sample Request

```
{
    "logGroupIdentifier": "service-logs",
    "policyDocument": {
        "Fields": ["RequestId", "TransactionId"]
    }
}
```

See Also

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

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

PutIntegration

Creates an integration between CloudWatch Logs and another service in this account. Currently, only integrations with OpenSearch Service are supported, and currently you can have only one integration in your account.

Integrating with OpenSearch Service makes it possible for you to create curated vended logs dashboards, powered by OpenSearch Service analytics. For more information, see Vended log dashboards powered by Amazon OpenSearch Service.

You can use this operation only to create a new integration. You can't modify an existing integration.

Request Syntax

```
{
   "integrationName": "string",
   "integrationType": "string",
   "resourceConfig": { ... }
}
```

Request Parameters

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

The request accepts the following data in JSON format.

integrationName

A name for the integration.

Type: String

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

Pattern: `[\.\-_/#A-Za-z0-9]+`

Required: Yes

integrationType

The type of integration. Currently, the only supported type is `OPENSEARCH`.

Type: String

Valid Values: OPENSEARCH

Required: Yes

resourceConfig

A structure that contains configuration information for the integration that you are creating.

Type: ResourceConfig object

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

Required: Yes

Response Syntax

```
{
   "integrationName": "string",
   "integrationStatus": "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.

integrationName

The name of the integration that you just created.

Type: String

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

Pattern: `[\.\-_/#A-Za-z0-9]+`

integrationStatus

The status of the integration that you just created.

After you create an integration, it takes a few minutes to complete. During this time, you'll see the status as `PROVISIONING`.

Type: String

Valid Values: `PROVISIONING | ACTIVE | FAILED`

Errors

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

InvalidParameterException

A parameter is specified incorrectly.

HTTP Status Code: 400

LimitExceededException

You have reached the maximum number of resources that can be created.

HTTP Status Code: 400

ServiceUnavailableException

The service cannot complete the request.

HTTP Status Code: 500

ValidationException

One of the parameters for the request is not valid.

HTTP Status Code: 400

See Also

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

- AWS Command Line Interface V2
- AWS SDK for .NET V4

- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

PutLogEvents

Uploads a batch of log events to the specified log stream.

> **Important**
>
> The sequence token is now ignored in `PutLogEvents` actions. `PutLogEvents` actions are always accepted and never return `InvalidSequenceTokenException` or `DataAlreadyAcceptedException` even if the sequence token is not valid. You can use parallel `PutLogEvents` actions on the same log stream.

The batch of events must satisfy the following constraints:

- The maximum batch size is 1,048,576 bytes. This size is calculated as the sum of all event messages in UTF-8, plus 26 bytes for each log event.
- Events more than 2 hours in the future are rejected while processing remaining valid events.
- Events older than 14 days or preceding the log group's retention period are rejected while processing remaining valid events.
- The log events in the batch must be in chronological order by their timestamp. The timestamp is the time that the event occurred, expressed as the number of milliseconds after `Jan 1, 1970 00:00:00` UTC. (In AWS Tools for PowerShell and the AWS SDK for .NET, the timestamp is specified in .NET format: `yyyy-mm-ddThh:mm:ss`. For example, `2017-09-15T13:45:30`.)
- A batch of log events in a single request must be in a chronological order. Otherwise, the operation fails.
- Each log event can be no larger than 1 MB.
- The maximum number of log events in a batch is 10,000.
- For valid events (within 14 days in the past to 2 hours in future), the time span in a single batch cannot exceed 24 hours. Otherwise, the operation fails.

> **Important**
>
> The quota of five requests per second per log stream has been removed. Instead, `PutLogEvents` actions are throttled based on a per-second per-account quota. You can request an increase to the per-second throttling quota by using the Service Quotas service.

If a call to PutLogEvents returns "UnrecognizedClientException" the most likely cause is a non-valid AWS access key ID or secret key.

Request Syntax

```
{
   "entity": {
      "attributes": {
         "string" : "string"
      },
      "keyAttributes": {
         "string" : "string"
      }
   },
   "logEvents": [
      {
         "message": "string",
         "timestamp": number
      }
   ],
   "logGroupName": "string",
   "logStreamName": "string",
   "sequenceToken": "string"
}
```

Request Parameters

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

The request accepts the following data in JSON format.

entity

The entity associated with the log events.

Type: Entity object

Required: No

logEvents

The log events.

Type: Array of InputLogEvent objects

Array Members: Minimum number of 1 item. Maximum number of 10000 items.

Required: Yes

logGroupName

The name of the log group.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `[\.\-_/#A-Za-z0-9]+`

Required: Yes

logStreamName

The name of the log stream.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `[^:*]*`

Required: Yes

sequenceToken

The sequence token obtained from the response of the previous `PutLogEvents` call.

> **Important**
>
> The `sequenceToken` parameter is now ignored in `PutLogEvents` actions. `PutLogEvents` actions are now accepted and never return `InvalidSequenceTokenException` or `DataAlreadyAcceptedException` even if the sequence token is not valid.

Type: String

Length Constraints: Minimum length of 1.

Required: No

Response Syntax

```
{
   "nextSequenceToken": "string",
   "rejectedEntityInfo": {
      "errorType": "string"
   },
   "rejectedLogEventsInfo": {
      "expiredLogEventEndIndex": number,
      "tooNewLogEventStartIndex": number,
      "tooOldLogEventEndIndex": 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.

nextSequenceToken

The next sequence token.

> **Important**
>
> This field has been deprecated.
> The sequence token is now ignored in `PutLogEvents` actions. `PutLogEvents` actions are always accepted even if the sequence token is not valid. You can use parallel `PutLogEvents` actions on the same log stream and you do not need to wait for the response of a previous `PutLogEvents` action to obtain the `nextSequenceToken` value.

Type: String

Length Constraints: Minimum length of 1.

rejectedEntityInfo

Information about why the entity is rejected when calling `PutLogEvents`. Only returned when the entity is rejected.

> **Note**
>
> When the entity is rejected, the events may still be accepted.

Type: RejectedEntityInfo object

rejectedLogEventsInfo

The rejected events.

Type: RejectedLogEventsInfo object

Errors

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

DataAlreadyAcceptedException

The event was already logged.

> **Important**
>
> `PutLogEvents` actions are now always accepted and never return `DataAlreadyAcceptedException` regardless of whether a given batch of log events has already been accepted.

HTTP Status Code: 400

InvalidParameterException

A parameter is specified incorrectly.

HTTP Status Code: 400

InvalidSequenceTokenException

The sequence token is not valid. You can get the correct sequence token in the `expectedSequenceToken` field in the `InvalidSequenceTokenException` message.

> **Important**
>
> `PutLogEvents` actions are now always accepted and never return `InvalidSequenceTokenException` regardless of receiving an invalid sequence token.

HTTP Status Code: 400

ResourceNotFoundException

The specified resource does not exist.

HTTP Status Code: 400

ServiceUnavailableException

The service cannot complete the request.

HTTP Status Code: 500

UnrecognizedClientException

The most likely cause is an AWS access key ID or secret key that's not valid.

HTTP Status Code: 400

Examples

To upload log events into a log stream

The following example uploads the specified log events to the specified log stream.

Sample Request

```
POST / HTTP/1.1
Host: logs.<region>.<domain>
X-Amz-Date: <DATE>
```

```
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=content-
type;date;host;user-agent;x-amz-date;x-amz-target;x-amzn-requestid,
 Signature=<Signature>
User-Agent: <UserAgentString>
Accept: application/json
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Connection: Keep-Alive
X-Amz-Target: Logs_20140328.PutLogEvents
{
  "logGroupName": "my-log-group",
  "logStreamName": "my-log-stream",
  "logEvents": [
    {
      "timestamp": 1396035378988,
      "message": "Example event 1"
    },
    {
      "timestamp": 1396035378988,
      "message": "Example event 2"
    },
    {
      "timestamp": 1396035378989,
      "message": "Example event 3"
    }
  ]
}
```

Sample Response

```
HTTP/1.1 200 OK
x-amzn-RequestId: <RequestId>
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Date: <Date>
{
  "nextSequenceToken": "49536701251539826331025683274032969384950891766572122113"
}
```

See Also

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

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

PutLogGroupDeletionProtection

Enables or disables deletion protection for the specified log group. When enabled on a log group, deletion protection blocks all deletion operations until it is explicitly disabled.

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

Request Syntax

```
{
   "deletionProtectionEnabled": boolean,
   "logGroupIdentifier": "string"
}
```

Request Parameters

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

The request accepts the following data in JSON format.

deletionProtectionEnabled

Whether to enable deletion protection.

Type: Boolean

Required: Yes

Type: Boolean

Required: Yes

logGroupIdentifier

The name or ARN of the log group.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `[\.\-_/#A-Za-z0-9]+`

Required: Yes

Type: String

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

Pattern: `[\w#+=/:,.@-]*`

Required: Yes

Response Elements

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

Errors

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

AccessDeniedException

You don't have sufficient permissions to perform this action.

HTTP Status Code: 400

InvalidOperationException

The operation is not valid on the specified resource.

HTTP Status Code: 400

InvalidParameterException

A parameter is specified incorrectly.

HTTP Status Code: 400

OperationAbortedException

Multiple concurrent requests to update the same resource were in conflict.

HTTP Status Code: 400

ResourceNotFoundException

The specified resource does not exist.

HTTP Status Code: 400

ServiceUnavailableException

The service cannot complete the request.

HTTP Status Code: 500

Examples

Sample Request

This example illustrates one usage of PutLogGroupDeletionProtection.

Sample Request

```
POST / HTTP/1.1
Host: logs.<region>.<domain>
X-Amz-Date: <DATE>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=content-
type;date;host;user-agent;x-amz-date;x-amz-target;x-amzn-requestid,
 Signature=<Signature>
User-Agent: <UserAgentString>
Accept: application/json
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Connection: Keep-Alive
X-Amz-Target: Logs_20140328.PutLogGroupDeletionProtection
{
  "logGroupIdentifier": "my-log-group",
  "deletionProtectionEnabled": true
}
```

Sample Response

```
HTTP/1.1 200 OK
x-amzn-RequestId: <RequestId>
Content-Type: application/x-amz-json-1.1
Content-Length: 0
Date: <Date>
```

See Also

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

- AWS Command Line Interface V2

- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

PutMetricFilter

Creates or updates a metric filter and associates it with the specified log group. With metric filters, you can configure rules to extract metric data from log events ingested through PutLogEvents.

The maximum number of metric filters that can be associated with a log group is 100.

Using regular expressions in filter patterns is supported. For these filters, there is a quota of two regular expression patterns within a single filter pattern. There is also a quota of five regular expression patterns per log group. For more information about using regular expressions in filter patterns, see Filter pattern syntax for metric filters, subscription filters, filter log events, and Live Tail.

When you create a metric filter, you can also optionally assign a unit and dimensions to the metric that is created.

Important

Metrics extracted from log events are charged as custom metrics. To prevent unexpected high charges, do not specify high-cardinality fields such as `IPAddress` or `requestID` as dimensions. Each different value found for a dimension is treated as a separate metric and accrues charges as a separate custom metric.
CloudWatch Logs might disable a metric filter if it generates 1,000 different name/value pairs for your specified dimensions within one hour.
You can also set up a billing alarm to alert you if your charges are higher than expected. For more information, see Creating a Billing Alarm to Monitor Your Estimated AWS Charges.

Request Syntax

```
{
   "applyOnTransformedLogs": boolean,
   "emitSystemFieldDimensions": [ "string" ],
   "fieldSelectionCriteria": "string",
   "filterName": "string",
   "filterPattern": "string",
   "logGroupName": "string",
   "metricTransformations": [
      {
         "defaultValue": number,
```

```
         "dimensions": {
            "string" : "string"
         },
         "metricName": "string",
         "metricNamespace": "string",
         "metricValue": "string",
         "unit": "string"
      }
   ]
}
```

Request Parameters

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

The request accepts the following data in JSON format.

applyOnTransformedLogs

This parameter is valid only for log groups that have an active log transformer. For more information about log transformers, see PutTransformer.

If the log group uses either a log-group level or account-level transformer, and you specify `true`, the metric filter will be applied on the transformed version of the log events instead of the original ingested log events.

Type: Boolean

Required: No

emitSystemFieldDimensions

A list of system fields to emit as additional dimensions in the generated metrics. Valid values are `@aws.account` and `@aws.region`. These dimensions help identify the source of centralized log data and count toward the total dimension limit for metric filters.

Type: Array of strings

Required: No

fieldSelectionCriteria

A filter expression that specifies which log events should be processed by this metric filter based on system fields such as source account and source region. Uses selection criteria syntax

with operators like =, !=, AND, OR, IN, NOT IN. Example: `@aws.region = "us-east-1"` or `@aws.account IN ["123456789012", "987654321098"]`. Maximum length: 2000 characters.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 2000.

Required: No

filterName

A name for the metric filter.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `[^:*]*`

Required: Yes

filterPattern

A filter pattern for extracting metric data out of ingested log events.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 1024.

Required: Yes

logGroupName

The name of the log group.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `[\.\-_/#A-Za-z0-9]+`

Required: Yes

metricTransformations

A collection of information that defines how metric data gets emitted.

Type: Array of MetricTransformation objects

Array Members: Fixed number of 1 item.

Required: Yes

Response Elements

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

Errors

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

InvalidOperationException

The operation is not valid on the specified resource.

HTTP Status Code: 400

InvalidParameterException

A parameter is specified incorrectly.

HTTP Status Code: 400

LimitExceededException

You have reached the maximum number of resources that can be created.

HTTP Status Code: 400

OperationAbortedException

Multiple concurrent requests to update the same resource were in conflict.

HTTP Status Code: 400

ResourceNotFoundException

The specified resource does not exist.

HTTP Status Code: 400

ServiceUnavailableException

The service cannot complete the request.

HTTP Status Code: 500

Examples

To create or update a metric filter

The following example creates a metric filter for the specified log group.

Sample Request

```
POST / HTTP/1.1
Host: logs.<region>.<domain>
X-Amz-Date: <DATE>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=content-
type;date;host;user-agent;x-amz-date;x-amz-target;x-amzn-requestid,
 Signature=<Signature>
User-Agent: <UserAgentString>
Accept: application/json
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Connection: Keep-Alive
X-Amz-Target: Logs_20140328.PutMetricFilter
{
  "logGroupName": "my-log-group",
  "filterName": "my-metric-filter",
  "filterPattern": "[ip, identity, user_id, timestamp, request, status_code, size]",
  "metricTransformations": [
    {
      "defaultValue": "0",
      "metricValue": "$size",
      "metricNamespace": "MyApp",
      "metricName": "Volume",
      "dimensions": {"Request": "$request","UserId": "$user_id"},
      "unit": "Count"
    }
  ]
}
```

Sample Response

```
HTTP/1.1 200 OK
x-amzn-RequestId: <RequestId>
```

```
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Date: <Date>
```

See Also

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

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

PutQueryDefinition

Creates or updates a query definition for CloudWatch Logs Insights. For more information, see Analyzing Log Data with CloudWatch Logs Insights.

To update a query definition, specify its `queryDefinitionId` in your request. The values of `name`, `queryString`, and `logGroupNames` are changed to the values that you specify in your update operation. No current values are retained from the current query definition. For example, imagine updating a current query definition that includes log groups. If you don't specify the `logGroupNames` parameter in your update operation, the query definition changes to contain no log groups.

You must have the `logs:PutQueryDefinition` permission to be able to perform this operation.

Request Syntax

```
{
   "clientToken": "string",
   "logGroupNames": [ "string" ],
   "name": "string",
   "parameters": [
      {
         "defaultValue": "string",
         "description": "string",
         "name": "string"
      }
   ],
   "queryDefinitionId": "string",
   "queryLanguage": "string",
   "queryString": "string"
}
```

Request Parameters

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

The request accepts the following data in JSON format.

clientToken

Used as an idempotency token, to avoid returning an exception if the service receives the same request twice because of a network error.

Type: String

Length Constraints: Minimum length of 36. Maximum length of 128.

Pattern: `\S{36,128}`

Required: No

logGroupNames

Use this parameter to include specific log groups as part of your query definition. If your query uses the OpenSearch Service query language, you specify the log group names inside the `querystring` instead of here.

If you are updating an existing query definition for the Logs Insights QL or OpenSearch Service PPL and you omit this parameter, then the updated definition will contain no log groups.

Type: Array of strings

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `[\.\-_/#A-Za-z0-9]+`

Required: No

name

A name for the query definition. If you are saving numerous query definitions, we recommend that you name them. This way, you can find the ones you want by using the first part of the name as a filter in the `queryDefinitionNamePrefix` parameter of DescribeQueryDefinitions.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 255.

Required: Yes

parameters

Use this parameter to include specific query parameters as part of your query definition. Query parameters are supported only for Logs Insights QL queries. Query parameters allow you to use

placeholder variables in your query string that are substituted with values at execution time. Use the `{{parameterName}}` syntax in your query string to reference a parameter.

Type: Array of QueryParameter objects

Array Members: Maximum number of 20 items.

Required: No

queryDefinitionId

If you are updating a query definition, use this parameter to specify the ID of the query definition that you want to update. You can use DescribeQueryDefinitions to retrieve the IDs of your saved query definitions.

If you are creating a query definition, do not specify this parameter. CloudWatch generates a unique ID for the new query definition and include it in the response to this operation.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Required: No

queryLanguage

Specify the query language to use for this query. The options are Logs Insights QL, OpenSearch PPL, and OpenSearch SQL. For more information about the query languages that CloudWatch Logs supports, see Supported query languages.

Type: String

Valid Values: `CWLI | SQL | PPL`

Required: No

queryString

The query string to use for this definition. For more information, see CloudWatch Logs Insights Query Syntax.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 10000.

Required: Yes

Response Syntax

```
{
   "queryDefinitionId": "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.

queryDefinitionId

The ID of the query definition.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Errors

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

InvalidParameterException

A parameter is specified incorrectly.

HTTP Status Code: 400

LimitExceededException

You have reached the maximum number of resources that can be created.

HTTP Status Code: 400

ResourceNotFoundException

The specified resource does not exist.

HTTP Status Code: 400

ServiceUnavailableException

The service cannot complete the request.

HTTP Status Code: 500

Examples

Create a new query definition

This example creates a query definition.

Sample Request

```
POST / HTTP/1.1
Host: logs.<region>.<domain>
X-Amz-Date: <DATE>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=content-
type;date;host;user-agent;x-amz-date;x-amz-target;x-amzn-requestid,
 Signature=<Signature>
User-Agent: <UserAgentString>
Accept: application/json
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Connection: Keep-Alive
X-Amz-Target: Logs_20140328.PutQueryDefinition
{
   "querystring": "stats sum(packets) as packetsTransferred by srcAddr, dstAddr | sort
 packetsTransferred  desc | limit 15",
   "name": "VPC-top15-packet-transfers",
   "logGroupNames": [ "VPC_Flow_Log1", "VPC_Flow_Log2" ],
}
```

Sample Response

```
HTTP/1.1 200 OK
x-amzn-RequestId: <RequestId>
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Date: <Date>
```

```
{
   "queryDefinitionId": "123456ab-12ab-123a-789e-1234567890ab"
}
```

Update a query definition

This example updates the query definition that was created in the previous example. The query is changed to show the top 25 responses instead of the top 15, and the name of the query is changed to reflect this.

Sample Request

```
POST / HTTP/1.1
Host: logs.<region>.<domain>
X-Amz-Date: <DATE>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=content-
type;date;host;user-agent;x-amz-date;x-amz-target;x-amzn-requestid,
 Signature=<Signature>
User-Agent: <UserAgentString>
Accept: application/json
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Connection: Keep-Alive
X-Amz-Target: Logs_20140328.PutQueryDefinition
{
   "queryDefinitionId": "123456ab-12ab-123a-789e-1234567890ab",
   "querystring": "stats sum(packets) as packetsTransferred by srcAddr, dstAddr | sort
 packetsTransferred  desc | limit 25",
   "name": "VPC-top25-packet-transfers",
}
```

Sample Response

```
HTTP/1.1 200 OK
x-amzn-RequestId: <RequestId>
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Date: <Date>
{
   "success": True
}
```

Create a query definition with parameters

This example creates a parameterized query definition. The query string includes parameter placeholders that are substituted at execution time.

Sample Request

```
POST / HTTP/1.1
Host: logs.<region>.<domain>
X-Amz-Date: <DATE>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=content-
type;date;host;user-agent;x-amz-date;x-amz-target;x-amzn-requestid,
 Signature=<Signature>
User-Agent: <UserAgentString>
Accept: application/json
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Connection: Keep-Alive
X-Amz-Target: Logs_20140328.PutQueryDefinition
{
   "name": "ErrorsByLevel",
   "queryString": "fields @timestamp, @message | filter level = {{logLevel}}",
   "logGroupNames": [ "/aws/lambda/my-function" ],
   "parameters": [
      {
         "name": "logLevel",
         "defaultValue": "ERROR",
         "description": "Log level to filter (ERROR, WARN, INFO, DEBUG)"
      }
   ]
}
```

Sample Response

```
HTTP/1.1 200 OK
x-amzn-RequestId: <RequestId>
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Date: <Date>
{
   "queryDefinitionId": "12345678-1234-1234-1234-123456789012"
}
```

See Also

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

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

PutResourcePolicy

Creates or updates a resource policy allowing other AWS services to put log events to this account, such as Amazon Route 53. This API has the following restrictions:

- **Supported actions** - Policy only supports `logs:PutLogEvents` and `logs:CreateLogStream` actions
- **Supported principals** - Policy only applies when operations are invoked by AWS service principals (not IAM users, roles, or cross-account principals
- **Policy limits** - An account can have a maximum of 10 policies without resourceARN and one per LogGroup resourceARN

> **Important**
>
> Resource policies with actions invoked by non-AWS service principals (such as IAM users, roles, or other AWS accounts) will not be enforced. For access control involving these principals, use the IAM policies.

Request Syntax

```
{
   "expectedRevisionId": "string",
   "policyDocument": "string",
   "policyName": "string",
   "resourceArn": "string"
}
```

Request Parameters

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

The request accepts the following data in JSON format.

expectedRevisionId

The expected revision ID of the resource policy. Required when `resourceArn` is provided to prevent concurrent modifications. Use `null` when creating a resource policy for the first time.

Type: String

Length Constraints: Minimum length of 1.

Required: No

policyDocument

Details of the new policy, including the identity of the principal that is enabled to put logs to this account. This is formatted as a JSON string. This parameter is required.

The following example creates a resource policy enabling the Route 53 service to put DNS query logs in to the specified log group. Replace `"logArn"` with the ARN of your CloudWatch Logs resource, such as a log group or log stream.

CloudWatch Logs also supports aws:SourceArn and aws:SourceAccount condition context keys.

In the example resource policy, you would replace the value of `SourceArn` with the resource making the call from Route 53 to CloudWatch Logs. You would also replace the value of `SourceAccount` with the AWS account ID making that call.

```
{ "Version": "2012-10-17", "Statement": [ { "Sid":
"Route53LogsToCloudWatchLogs", "Effect": "Allow", "Principal":
{ "Service": [ "route53.amazonaws.com" ] }, "Action":
"logs:PutLogEvents", "Resource": "logArn", "Condition": { "ArnLike":
{ "aws:SourceArn": "myRoute53ResourceArn" }, "StringEquals":
{ "aws:SourceAccount": "myAwsAccountId" } } } ] }
```

Type: String

Length Constraints: Minimum length of 1. Maximum length of 51200.

Required: No

policyName

Name of the new policy. This parameter is required.

Type: String

Required: No

resourceArn

The ARN of the CloudWatch Logs resource to which the resource policy needs to be added or attached. Currently only supports LogGroup ARN.

Type: String

Required: No

Response Syntax

```
{
   "resourcePolicy": {
      "lastUpdatedTime": number,
      "policyDocument": "string",
      "policyName": "string",
      "policyScope": "string",
      "resourceArn": "string",
      "revisionId": "string"
   },
   "revisionId": "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.

resourcePolicy

The new policy.

Type: ResourcePolicy object

revisionId

The revision ID of the created or updated resource policy. Only returned for resource-scoped policies.

Type: String

Length Constraints: Minimum length of 1.

Errors

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

InvalidParameterException

A parameter is specified incorrectly.

HTTP Status Code: 400

LimitExceededException

You have reached the maximum number of resources that can be created.

HTTP Status Code: 400

OperationAbortedException

Multiple concurrent requests to update the same resource were in conflict.

HTTP Status Code: 400

ResourceNotFoundException

The specified resource does not exist.

HTTP Status Code: 400

ServiceUnavailableException

The service cannot complete the request.

HTTP Status Code: 500

See Also

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

- AWS Command Line Interface V2
- AWS SDK for .NET V4

- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

PutRetentionPolicy

Sets the retention of the specified log group. With a retention policy, you can configure the number of days for which to retain log events in the specified log group.

> **Note**
>
> CloudWatch Logs doesn't immediately delete log events when they reach their retention setting. It typically takes up to 72 hours after that before log events are deleted, but in rare situations might take longer.
> To illustrate, imagine that you change a log group to have a longer retention setting when it contains log events that are past the expiration date, but haven't been deleted. Those log events will take up to 72 hours to be deleted after the new retention date is reached. To make sure that log data is deleted permanently, keep a log group at its lower retention setting until 72 hours after the previous retention period ends. Alternatively, wait to change the retention setting until you confirm that the earlier log events are deleted.
> When log events reach their retention setting they are marked for deletion. After they are marked for deletion, they do not add to your archival storage costs anymore, even if they are not actually deleted until later. These log events marked for deletion are also not included when you use an API to retrieve the `storedBytes` value to see how many bytes a log group is storing.

Request Syntax

```
{
   "logGroupName": "string",
   "retentionInDays": number
}
```

Request Parameters

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

The request accepts the following data in JSON format.

logGroupName

The name of the log group.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `[\.\-_/#A-Za-z0-9]+`

Required: Yes

retentionInDays

The number of days to retain the log events in the specified log group. Possible values are: 1, 3, 5, 7, 14, 30, 60, 90, 120, 150, 180, 365, 400, 545, 731, 1096, 1827, 2192, 2557, 2922, 3288, and 3653.

To set a log group so that its log events do not expire, use DeleteRetentionPolicy.

Type: Integer

Required: Yes

Response Elements

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

Errors

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

InvalidParameterException

A parameter is specified incorrectly.

HTTP Status Code: 400

OperationAbortedException

Multiple concurrent requests to update the same resource were in conflict.

HTTP Status Code: 400

ResourceNotFoundException

The specified resource does not exist.

HTTP Status Code: 400

ServiceUnavailableException

The service cannot complete the request.

HTTP Status Code: 500

Examples

To create or update a retention policy for a log group

The following example creates a 30-day retention policy for the specified log group.

Sample Request

```
POST / HTTP/1.1
Host: logs.<region>.<domain>
X-Amz-Date: <DATE>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=content-
type;date;host;user-agent;x-amz-date;x-amz-target;x-amzn-requestid,
 Signature=<Signature>
User-Agent: <UserAgentString>
Accept: application/json
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Connection: Keep-Alive
X-Amz-Target: Logs_20140328.PutRetentionPolicy
{
  "logGroupName": "my-log-group",
  "retentionInDays": 30
}
```

Sample Response

```
HTTP/1.1 200 OK
x-amzn-RequestId: <RequestId>
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Date: <Date>
```

See Also

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

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

PutStorageTierPolicy

Sets the storage tier policy for the account. When you set the storage tier to `INTELLIGENT_TIERING`, the service automatically moves log data to the most cost-effective storage tier based on access frequency.

Request Syntax

```
{
   "storageTier": "string"
}
```

Request Parameters

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

The request accepts the following data in JSON format.

storageTier

The storage tier to set for the account. Use `INTELLIGENT_TIERING` to automatically optimize storage costs by moving log data to the appropriate tier based on access frequency.

Type: String

Valid Values: `STANDARD | INTELLIGENT_TIERING`

Required: Yes

Response Syntax

```
{
   "lastUpdatedTime": number,
   "storageTier": "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.

lastUpdatedTime

The time when the storage tier policy was last updated, expressed as the number of milliseconds after `January 1, 1970 00:00:00 UTC`.

Type: Long

Valid Range: Minimum value of 0.

storageTier

The storage tier for the account.

Type: String

Valid Values: `STANDARD | INTELLIGENT_TIERING`

Errors

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

AccessDeniedException

You don't have sufficient permissions to perform this action.

HTTP Status Code: 400

InvalidParameterException

A parameter is specified incorrectly.

HTTP Status Code: 400

OperationAbortedException

Multiple concurrent requests to update the same resource were in conflict.

HTTP Status Code: 400

ResourceNotFoundException

The specified resource does not exist.

HTTP Status Code: 400

ServiceUnavailableException

The service cannot complete the request.

HTTP Status Code: 500

See Also

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

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

PutSubscriptionFilter

Creates or updates a subscription filter and associates it with the specified log group. With subscription filters, you can subscribe to a real-time stream of log events ingested through PutLogEvents and have them delivered to a specific destination. When log events are sent to the receiving service, they are Base64 encoded and compressed with the GZIP format.

The following destinations are supported for subscription filters:

- An Amazon Kinesis data stream belonging to the same account as the subscription filter, for same-account delivery.
- A logical destination created with PutDestination that belongs to a different account, for cross-account delivery. We currently support Kinesis Data Streams and Firehose as logical destinations.
- An Amazon Kinesis Data Firehose delivery stream that belongs to the same account as the subscription filter, for same-account delivery.
- An AWS Lambda function that belongs to the same account as the subscription filter, for same-account delivery.

Each log group can have up to two subscription filters associated with it. If you are updating an existing filter, you must specify the correct name in `filterName`.

Using regular expressions in filter patterns is supported. For these filters, there is a quotas of quota of two regular expression patterns within a single filter pattern. There is also a quota of five regular expression patterns per log group. For more information about using regular expressions in filter patterns, see Filter pattern syntax for metric filters, subscription filters, filter log events, and Live Tail.

To perform a `PutSubscriptionFilter` operation for any destination except a Lambda function, you must also have the `iam:PassRole` permission.

Request Syntax

```
{
   "applyOnTransformedLogs": boolean,
   "destinationArn": "string",
   "distribution": "string",
   "emitSystemFields": [ "string" ],
```

```
    "fieldSelectionCriteria": "string",
    "filterName": "string",
    "filterPattern": "string",
    "logGroupName": "string",
    "roleArn": "string"
}
```

Request Parameters

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

The request accepts the following data in JSON format.

applyOnTransformedLogs

This parameter is valid only for log groups that have an active log transformer. For more information about log transformers, see PutTransformer.

If the log group uses either a log-group level or account-level transformer, and you specify `true`, the subscription filter will be applied on the transformed version of the log events instead of the original ingested log events.

Type: Boolean

Required: No

destinationArn

The ARN of the destination to deliver matching log events to. Currently, the supported destinations are:

- An Amazon Kinesis stream belonging to the same account as the subscription filter, for same-account delivery.
- A logical destination (specified using an ARN) belonging to a different account, for cross-account delivery.

  If you're setting up a cross-account subscription, the destination must have an IAM policy associated with it. The IAM policy must allow the sender to send logs to the destination. For more information, see PutDestinationPolicy.
- A Kinesis Data Firehose delivery stream belonging to the same account as the subscription filter, for same-account delivery.

- A Lambda function belonging to the same account as the subscription filter, for same-account delivery.

Type: String

Length Constraints: Minimum length of 1.

Required: Yes

distribution

The method used to distribute log data to the destination. By default, log data is grouped by log stream, but the grouping can be set to random for a more even distribution. This property is only applicable when the destination is an Amazon Kinesis data stream.

Type: String

Valid Values: `Random | ByLogStream`

Required: No

emitSystemFields

A list of system fields to include in the log events sent to the subscription destination. Valid values are `@aws.account`, `@aws.region`, and `@source.log`. These fields provide source information for centralized log data in the forwarded payload.

Type: Array of strings

Required: No

fieldSelectionCriteria

A filter expression that specifies which log events should be processed by this subscription filter based on system fields such as source account and source region. Uses selection criteria syntax with operators like `=`, `!=`, `AND`, `OR`, `IN`, `NOT IN`. Example: `@aws.region NOT IN ["cn-north-1"]` or `@aws.account = "123456789012" AND @aws.region = "us-east-1"`. Maximum length: 2000 characters.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 2000.

Required: No

filterName

A name for the subscription filter. If you are updating an existing filter, you must specify the correct name in `filterName`. To find the name of the filter currently associated with a log group, use DescribeSubscriptionFilters.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `[^:*]*`

Required: Yes

filterPattern

A filter pattern for subscribing to a filtered stream of log events.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 1024.

Required: Yes

logGroupName

The name of the log group.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `[\.\-_/#A-Za-z0-9]+`

Required: Yes

roleArn

The ARN of an IAM role that grants CloudWatch Logs permissions to deliver ingested log events to the destination stream. You don't need to provide the ARN when you are working with a logical destination for cross-account delivery.

Type: String

Length Constraints: Minimum length of 1.

Required: No

Response Elements

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

Errors

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

InvalidOperationException

The operation is not valid on the specified resource.

HTTP Status Code: 400

InvalidParameterException

A parameter is specified incorrectly.

HTTP Status Code: 400

LimitExceededException

You have reached the maximum number of resources that can be created.

HTTP Status Code: 400

OperationAbortedException

Multiple concurrent requests to update the same resource were in conflict.

HTTP Status Code: 400

ResourceNotFoundException

The specified resource does not exist.

HTTP Status Code: 400

ServiceUnavailableException

The service cannot complete the request.

HTTP Status Code: 500

Examples

To create or update a subscription filter

The following example creates a subscription filter.

Sample Request

```
POST / HTTP/1.1
Host: logs.<region>.<domain>
X-Amz-Date: <DATE>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=content-
type;date;host;user-agent;x-amz-date;x-amz-target;x-amzn-requestid,
 Signature=<Signature>
User-Agent: <UserAgentString>
Accept: application/json
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Connection: Keep-Alive
X-Amz-Target: Logs_20140328.PutSubscriptionFilter
{
  "logGroupName": "my-log-group",
  "filterName": "my-subscription-filter",
  "filterPattern": "[ip, identity, user_id, timestamp, request, status_code = 500,
 size]",
  "destinationArn": "arn:aws:kinesis:us-east-1:123456789012:stream/my-kinesis-stream",
  "roleArn": "arn:aws:iam::123456789012:role/my-subscription-role",
  "applyOnTransformedLogs" : true
}
```

Sample Response

```
HTTP/1.1 200 OK
x-amzn-RequestId: <RequestId>
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Date: <Date>
```

See Also

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

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

PutSyslogConfiguration

Creates or updates a syslog configuration for a log group. This enables ingestion of syslog data through the specified VPC endpoint into the log group.

Request Syntax

```
{
   "logGroupIdentifier": "string",
   "vpcEndpointId": "string"
}
```

Request Parameters

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

The request accepts the following data in JSON format.

logGroupIdentifier

The name or ARN of the log group to associate with the syslog configuration.

Type: String

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

Pattern: `[\w#+=/:,.@-]*`

Required: Yes

vpcEndpointId

The ID of the VPC endpoint to use for syslog ingestion.

Type: String

Pattern: `^vpce-[0-9a-f]{1,64}$`

Required: No

Response Elements

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

Errors

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

AccessDeniedException

You don't have sufficient permissions to perform this action.

HTTP Status Code: 400

InvalidOperationException

The operation is not valid on the specified resource.

HTTP Status Code: 400

InvalidParameterException

A parameter is specified incorrectly.

HTTP Status Code: 400

OperationAbortedException

Multiple concurrent requests to update the same resource were in conflict.

HTTP Status Code: 400

ResourceNotFoundException

The specified resource does not exist.

HTTP Status Code: 400

ServiceUnavailableException

The service cannot complete the request.

HTTP Status Code: 500

ThrottlingException

The request was throttled because of quota limits.

HTTP Status Code: 400

Examples

To create a syslog configuration

The following example creates a syslog configuration that enables syslog ingestion for the specified log group through a VPC endpoint.

Sample Request

```
POST / HTTP/1.1
Host: logs.<region>.<domain>
X-Amz-Date: <DATE>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=content-
type;date;host;user-agent;x-amz-date;x-amz-target;x-amzn-requestid,
 Signature=<Signature>
User-Agent: <UserAgentString>
Accept: application/json
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Connection: Keep-Alive
X-Amz-Target: Logs_20140328.PutSyslogConfiguration
{
  "logGroupIdentifier": "arn:aws:logs:us-east-1:123456789012:log-group:my-syslog-
group",
  "vpcEndpointId": "vpce-0123456789abcdef0"
}
```

Sample Response

```
HTTP/1.1 200 OK
x-amzn-RequestId: <RequestId>
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Date: <Date>
```

See Also

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

- AWS Command Line Interface V2

- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

PutTransformer

Creates or updates a *log transformer* for a single log group. You use log transformers to transform log events into a different format, making them easier for you to process and analyze. You can also transform logs from different sources into standardized formats that contains relevant, source-specific information.

After you have created a transformer, CloudWatch Logs performs the transformations at the time of log ingestion. You can then refer to the transformed versions of the logs during operations such as querying with CloudWatch Logs Insights or creating metric filters or subscription filers.

You can also use a transformer to copy metadata from metadata keys into the log events themselves. This metadata can include log group name, log stream name, account ID and Region.

A transformer for a log group is a series of processors, where each processor applies one type of transformation to the log events ingested into this log group. The processors work one after another, in the order that you list them, like a pipeline. For more information about the available processors to use in a transformer, see Processors that you can use.

Having log events in standardized format enables visibility across your applications for your log analysis, reporting, and alarming needs. CloudWatch Logs provides transformation for common log types with out-of-the-box transformation templates for major AWS log sources such as VPC flow logs, Lambda, and Amazon RDS. You can use pre-built transformation templates or create custom transformation policies.

You can create transformers only for the log groups in the Standard log class.

You can also set up a transformer at the account level. For more information, see PutAccountPolicy. If there is both a log-group level transformer created with `PutTransformer` and an account-level transformer that could apply to the same log group, the log group uses only the log-group level transformer. It ignores the account-level transformer.

Request Syntax

```
{
   "logGroupIdentifier": "string",
   "transformerConfig": [
      {
         "addKeys": {
            "entries": [
               {
```

```
                "key": "string",
                "overwriteIfExists": boolean,
                "value": "string"
             }
          ]
       },
       "copyValue": {
          "entries": [
             {
                "overwriteIfExists": boolean,
                "source": "string",
                "target": "string"
             }
          ]
       },
       "csv": {
          "columns": [ "string" ],
          "delimiter": "string",
          "destination": "string",
          "quoteCharacter": "string",
          "source": "string"
       },
       "dateTimeConverter": {
          "locale": "string",
          "matchPatterns": [ "string" ],
          "source": "string",
          "sourceTimezone": "string",
          "target": "string",
          "targetFormat": "string",
          "targetTimezone": "string"
       },
       "deleteKeys": {
          "withKeys": [ "string" ]
       },
       "grok": {
          "match": "string",
          "source": "string"
       },
       "listToMap": {
          "flatten": boolean,
          "flattenedElement": "string",
          "key": "string",
          "source": "string",
          "target": "string",
```

```
            "valueKey": "string"
         },
         "lowerCaseString": {
            "withKeys": [ "string" ]
         },
         "moveKeys": {
            "entries": [
               {
                  "overwriteIfExists": boolean,
                  "source": "string",
                  "target": "string"
               }
            ]
         },
         "parseCloudfront": {
            "source": "string"
         },
         "parseJSON": {
            "destination": "string",
            "source": "string"
         },
         "parseKeyValue": {
            "destination": "string",
            "fieldDelimiter": "string",
            "keyPrefix": "string",
            "keyValueDelimiter": "string",
            "nonMatchValue": "string",
            "overwriteIfExists": boolean,
            "source": "string"
         },
         "parsePostgres": {
            "source": "string"
         },
         "parseRoute53": {
            "source": "string"
         },
         "parseToOCSF": {
            "eventSource": "string",
            "mappingVersion": "string",
            "ocsfVersion": "string",
            "source": "string"
         },
         "parseVPC": {
            "source": "string"
```

```
      },
      "parseWAF": {
         "source": "string"
      },
      "renameKeys": {
         "entries": [
            {
               "key": "string",
               "overwriteIfExists": boolean,
               "renameTo": "string"
            }
         ]
      },
      "splitString": {
         "entries": [
            {
               "delimiter": "string",
               "source": "string"
            }
         ]
      },
      "substituteString": {
         "entries": [
            {
               "from": "string",
               "source": "string",
               "to": "string"
            }
         ]
      },
      "trimString": {
         "withKeys": [ "string" ]
      },
      "typeConverter": {
         "entries": [
            {
               "key": "string",
               "type": "string"
            }
         ]
      },
      "upperCaseString": {
         "withKeys": [ "string" ]
      }
```

```
        }
    ]
}
```

Request Parameters

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

The request accepts the following data in JSON format.

logGroupIdentifier

Specify either the name or ARN of the log group to create the transformer for.

Type: String

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

Pattern: `[\w#+=/:,.@-]*`

Required: Yes

transformerConfig

This structure contains the configuration of this log transformer. A log transformer is an array of processors, where each processor applies one type of transformation to the log events that are ingested.

Type: Array of Processor objects

Array Members: Minimum number of 1 item. Maximum number of 20 items.

Required: Yes

Response Elements

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

Errors

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

InvalidOperationException

The operation is not valid on the specified resource.

HTTP Status Code: 400

InvalidParameterException

A parameter is specified incorrectly.

HTTP Status Code: 400

LimitExceededException

You have reached the maximum number of resources that can be created.

HTTP Status Code: 400

OperationAbortedException

Multiple concurrent requests to update the same resource were in conflict.

HTTP Status Code: 400

ResourceNotFoundException

The specified resource does not exist.

HTTP Status Code: 400

ServiceUnavailableException

The service cannot complete the request.

HTTP Status Code: 500

Examples

To create a log transformer

The following example creates a log transformer for the specified log group.

Sample Request

```
POST / HTTP/1.1
Host: logs.<region>.<domain>
X-Amz-Date: <DATE>
```

```
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=content-
type;date;host;user-agent;x-amz-date;x-amz-target;x-amzn-requestid,
 Signature=<Signature>
User-Agent: <UserAgentString>
Accept: application/json
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Connection: Keep-Alive
X-Amz-Target: Logs_20140328.PutTransformer
{
    "logGroupIdentifier": "my-log-group-name",
    "transformerConfig": [
        {
            "parseJSON": {}
        },
        {
            "addKeys": {
                "entries": [
                    {
                        "key": "metadata.transformed_in",
                        "value": "CloudWatchLogs"
                    }
                ]
            }
        },
        {
            "trimString": {
                "withKeys": [
                    "status"
                ]
            }
        },
        {
            "lowerCaseString": {
                "withKeys": [
                    "status"
                ]
            }
        }
    ]
}
```

See Also

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

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

StartLiveTail

Starts a Live Tail streaming session for one or more log groups. A Live Tail session returns a stream of log events that have been recently ingested in the log groups. For more information, see Use Live Tail to view logs in near real time.

The response to this operation is a response stream, over which the server sends live log events and the client receives them.

The following objects are sent over the stream:

- A single LiveTailSessionStart object is sent at the start of the session.
- Every second, a LiveTailSessionUpdate object is sent. Each of these objects contains an array of the actual log events.

  If no new log events were ingested in the past second, the `LiveTailSessionUpdate` object will contain an empty array.

  The array of log events contained in a `LiveTailSessionUpdate` can include as many as 500 log events. If the number of log events matching the request exceeds 500 per second, the log events are sampled down to 500 log events to be included in each `LiveTailSessionUpdate` object.

  If your client consumes the log events slower than the server produces them, CloudWatch Logs buffers up to 10 `LiveTailSessionUpdate` events or 5000 log events, after which it starts dropping the oldest events.
- A SessionStreamingException object is returned if an unknown error occurs on the server side.
- A SessionTimeoutException object is returned when the session times out, after it has been kept open for three hours.

Note

The `StartLiveTail` API routes requests using SDK host prefix injection. SDK versions released before April 1, 2026 route to `streaming-logs.`*`Region`*`.amazonaws.com`, which does not support VPC endpoints. SDK versions released on or after April 1, 2026 route to `stream-logs.`*`Region`*`.amazonaws.com`, which supports VPC endpoints. To set up a VPC endpoint for this API, see Creating a VPC endpoint for CloudWatch Logs .

> **Important**
>
> You can end a session before it times out by closing the session stream or by closing the client that is receiving the stream. The session also ends if the established connection between the client and the server breaks.

For examples of using an SDK to start a Live Tail session, see Start a Live Tail session using an AWS SDK.

Request Syntax

```
{
   "logEventFilterPattern": "string",
   "logGroupIdentifiers": [ "string" ],
   "logStreamNamePrefixes": [ "string" ],
   "logStreamNames": [ "string" ]
}
```

Request Parameters

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

The request accepts the following data in JSON format.

logEventFilterPattern

An optional pattern to use to filter the results to include only log events that match the pattern. For example, a filter pattern of `error 404` causes only log events that include both `error` and `404` to be included in the Live Tail stream.

Regular expression filter patterns are supported.

For more information about filter pattern syntax, see Filter and Pattern Syntax.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 1024.

Required: No

logGroupIdentifiers

An array where each item in the array is a log group to include in the Live Tail session.

Specify each log group by its ARN.

If you specify an ARN, the ARN can't end with an asterisk (*).

> **Note**
>
> You can include up to 10 log groups.

Type: Array of strings

Array Members: Minimum number of 1 item. Maximum number of 10 items.

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

Pattern: `[\w#+=/:,.@-]*`

Required: Yes

logStreamNamePrefixes

If you specify this parameter, then only log events in the log streams that have names that start with the prefixes that you specify here are included in the Live Tail session.

If you specify this field, you can't also specify the `logStreamNames` field.

> **Note**
>
> You can specify this parameter only if you specify only one log group in `logGroupIdentifiers`.

Type: Array of strings

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

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `[^:*]*`

Required: No

logStreamNames

If you specify this parameter, then only log events in the log streams that you specify here are included in the Live Tail session.

If you specify this field, you can't also specify the `logStreamNamePrefixes` field.

> **Note**
>
> You can specify this parameter only if you specify only one log group in `logGroupIdentifiers`.

Type: Array of strings

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

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `[^:*]*`

Required: No

Response Syntax

```
{
   "responseStream": {
      "sessionStart": {
         "logEventFilterPattern": "string",
         "logGroupIdentifiers": [ "string" ],
         "logStreamNamePrefixes": [ "string" ],
         "logStreamNames": [ "string" ],
         "requestId": "string",
         "sessionId": "string"
      },
      "SessionStreamingException": {
      },
      "SessionTimeoutException": {
      },
      "sessionUpdate": {
```

```
         "sessionMetadata": {
            "sampled": boolean
         },
         "sessionResults": [
            {
               "ingestionTime": number,
               "logGroupIdentifier": "string",
               "logStreamName": "string",
               "message": "string",
               "timestamp": 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.

responseStream

An object that includes the stream returned by your request. It can include both log events and exceptions.

Type: StartLiveTailResponseStream object

Errors

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

AccessDeniedException

You don't have sufficient permissions to perform this action.

HTTP Status Code: 400

InvalidOperationException

The operation is not valid on the specified resource.

HTTP Status Code: 400

InvalidParameterException

A parameter is specified incorrectly.

HTTP Status Code: 400

LimitExceededException

You have reached the maximum number of resources that can be created.

HTTP Status Code: 400

ResourceNotFoundException

The specified resource does not exist.

HTTP Status Code: 400

See Also

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

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

StartQuery

Starts a query of one or more log groups or data sources using CloudWatch Logs Insights. You specify the log groups or data sources and time range to query and the query string to use. You can query up to 10 data sources in a single query.

For more information, see CloudWatch Logs Insights Query Syntax.

After you run a query using `StartQuery`, the query results are stored by CloudWatch Logs. You can use GetQueryResults to retrieve the results of a query, using the `queryId` that `StartQuery` returns.

Interactive queries started with `StartQuery` share concurrency limits with automated scheduled query executions. Both types of queries count toward the same regional concurrent query quota, so high scheduled query activity may affect the availability of concurrent slots for interactive queries.

Note

To specify the log groups to query, a `StartQuery` operation must include one of the following:

- Either exactly one of the following parameters: `logGroupName`, `logGroupNames`, or `logGroupIdentifiers`
- Or the `queryString` must include a SOURCE command to select log groups for the query. The SOURCE command can select log groups based on log group name prefix, account ID, and log class, or select data sources using dataSource syntax in LogsQL, PPL, and SQL. In LogsQL, the SOURCE command also supports filtering by log group tags.

  For more information about the SOURCE command, see SOURCE.

If you have associated a AWS KMS key with the query results in this account, then StartQuery uses that key to encrypt the results when it stores them. If no key is associated with query results, the query results are encrypted with the default CloudWatch Logs encryption method.

Queries time out after 60 minutes of runtime. If your queries are timing out, reduce the time range being searched or partition your query into a number of queries.

If you are using CloudWatch cross-account observability, you can use this operation in a monitoring account to start a query in a linked source account. For more information, see CloudWatch cross-

account observability. For a cross-account `StartQuery` operation, the query definition must be defined in the monitoring account.

You can have up to 100 concurrent CloudWatch Logs insights queries, including queries that have been added to dashboards.

Request Syntax

```
{
   "endTime": number,
   "limit": number,
   "logGroupIdentifiers": [ "string" ],
   "logGroupName": "string",
   "logGroupNames": [ "string" ],
   "queryLanguage": "string",
   "queryString": "string",
   "startTime": number
}
```

Request Parameters

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

The request accepts the following data in JSON format.

endTime

The end of the time range to query. The range is inclusive, so the specified end time is included in the query. Specified as epoch time, the number of seconds since `January 1, 1970, 00:00:00` UTC.

Type: Long

Valid Range: Minimum value of 0.

Required: Yes

limit

The maximum number of log events to return from the query. The maximum limit is 100,000. The maximum events returned in a single GetQueryResults API call is 10,000 log events per request. You can retrieve up to 100,000 log event results from a query by paginating with the

`nextToken`. 100,000 limit is only supported for Logs Insights QL and is currently not supported for PPL and SQL query languages.

Type: Integer

Valid Range: Minimum value of 1. Maximum value of 100000.

Required: No

logGroupIdentifiers

The list of log groups to query. You can include up to 50 log groups.

You can specify them by the log group name or ARN. If a log group that you're querying is in a source account and you're using a monitoring account, you must specify the ARN of the log group here. The query definition must also be defined in the monitoring account.

If you specify an ARN, use the format arn:aws:logs:*region*:*account-id*:log-group:*log_group_name* Don't include an * at the end.

A `StartQuery` operation must include exactly one of the following parameters: `logGroupName`, `logGroupNames`, or `logGroupIdentifiers`. The exception is queries using the OpenSearch Service SQL query language, where you specify the log group names inside the `querystring` instead of here.

Type: Array of strings

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

Pattern: `[\w#+=/:,.@-]*`

Required: No

logGroupName

The log group on which to perform the query.

> **Note**
>
> A `StartQuery` operation must include exactly one of the following parameters: `logGroupName`, `logGroupNames`, or `logGroupIdentifiers`. The exception is queries using the OpenSearch Service SQL query language, where you specify the log group names inside the `querystring` instead of here.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `[\.\-_/#A-Za-z0-9]+`

Required: No

logGroupNames

The list of log groups to be queried. You can include up to 50 log groups.

> **Note**
>
> A `StartQuery` operation must include exactly one of the following parameters: `logGroupName`, `logGroupNames`, or `logGroupIdentifiers`. The exception is queries using the OpenSearch Service SQL query language, where you specify the log group names inside the `querystring` instead of here.

Type: Array of strings

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `[\.\-_/#A-Za-z0-9]+`

Required: No

queryLanguage

Specify the query language to use for this query. The options are Logs Insights QL, OpenSearch PPL, and OpenSearch SQL. For more information about the query languages that CloudWatch Logs supports, see Supported query languages.

Type: String

Valid Values: `CWLI | SQL | PPL`

Required: No

queryString

The query string to use. For more information, see CloudWatch Logs Insights Query Syntax.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 10000.

Required: Yes

startTime

The beginning of the time range to query. The range is inclusive, so the specified start time is included in the query. Specified as epoch time, the number of seconds since `January 1, 1970, 00:00:00 UTC`.

Type: Long

Valid Range: Minimum value of 0.

Required: Yes

Response Syntax

```
{
   "queryId": "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.

queryId

The unique ID of the query.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Errors

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

InvalidParameterException

A parameter is specified incorrectly.

HTTP Status Code: 400

LimitExceededException

You have reached the maximum number of resources that can be created.

HTTP Status Code: 400

MalformedQueryException

The query string is not valid. Details about this error are displayed in a `QueryCompileError` object. For more information, see QueryCompileError.

For more information about valid query syntax, see CloudWatch Logs Insights Query Syntax.

queryCompileError

Reserved.

HTTP Status Code: 400

ResourceNotFoundException

The specified resource does not exist.

HTTP Status Code: 400

ServiceUnavailableException

The service cannot complete the request.

HTTP Status Code: 500

Examples

Example: Start a query

This example starts a query of three log groups, specifying the query string and start time. It also limits the results to the most recent 100 matching events.

Sample Request

```
POST / HTTP/1.1
```

```
Host: logs.<region>.<domain>
X-Amz-Date: <DATE>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=content-
type;date;host;user-agent;x-amz-date;x-amz-target;x-amzn-requestid,
 Signature=<Signature>
User-Agent: <UserAgentString>
Accept: application/json
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Connection: Keep-Alive
X-Amz-Target: Logs_20140328.StartQuery
{
    "limit": 100,
    "logGroupNames": [
        "LogGroupName1",
        "LogGroupName2",
        "LogGroupName3"
    ],
    "queryString": "stats count(*) by eventSource, eventName, awsRegion",
    "startTime": 1546300800,
    "endTime": 1546309800
}
```

Sample Response

```
HTTP/1.1 200 OK
x-amzn-RequestId: <RequestId>
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Date: <Date>
{
   "queryId": "12ab3456-12ab-123a-789e-1234567890ab"
}
```

Example: Start a query

This example starts a query for a log group ARN and specifies a query string. It also specifies the request start and end times.

Sample Request

```
{
```

```
    "limit": 100,
    "logGroupIdentifiers": [
        "arn:aws:logs:us-east-1:123456789012:log-group:monitoring-logGroup-1234"
     ],
    "queryString": "stats count(*) by eventSource, eventName, awsRegion",
    "startTime": 1546300800,
    "endTime": 1546309800
}
```

Sample Response

```
{
    "queryId": "12ab3456-12ab-123a-789e-1234567890ab"
}
```

Example: Start a query using field indexing and the source command

This example queries all log groups in the `111122223333` account that have log group names that start with `my-log`. It leverages field indexing so that only log groups and log events known to match the indexed field `transactionId` are processed. Only log events that include the value `tx-001` for the `transactionId` field will be returned.

Sample Request

```
POST / HTTP/1.1
Host: logs.<region>.<domain>
X-Amz-Date: <DATE>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=content-
type;date;host;user-agent;x-amz-date;x-amz-target;x-amzn-requestid,
 Signature=<Signature>
User-Agent: <UserAgentString>
Accept: application/json
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Connection: Keep-Alive
X-Amz-Target: Logs_20140328.StartQuery
{
 "queryString":
  "source logGroups(namePrefix: ['my-log'], accountIdentifiers: ['accountId' =
 '111122223333'])
 | filterIndex transactionId = 'tx-001'",
    "startTime": 1722704400000,
```

```
    "endTime": 1722705229849
}
```

See Also

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

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

StopQuery

Stops a CloudWatch Logs Insights query that is in progress. If the query has already ended, the operation returns an error indicating that the specified query is not running.

This operation can be used to cancel both interactive queries and individual scheduled query executions. When used with scheduled queries, `StopQuery` cancels only the specific execution identified by the query ID, not the scheduled query configuration itself.

Request Syntax

```
{
   "queryId": "string"
}
```

Request Parameters

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

The request accepts the following data in JSON format.

queryId

The ID number of the query to stop. To find this ID number, use `DescribeQueries`.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Required: Yes

Response Syntax

```
{
   "success": boolean
}
```

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.

success

This is true if the query was stopped by the `StopQuery` operation.

Type: Boolean

Errors

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

InvalidParameterException

A parameter is specified incorrectly.

HTTP Status Code: 400

ResourceNotFoundException

The specified resource does not exist.

HTTP Status Code: 400

ServiceUnavailableException

The service cannot complete the request.

HTTP Status Code: 500

Examples

Stop a query that is currently running

The following example stops the specified query, if it is currently running.

Sample Request

```
POST / HTTP/1.1
Host: logs.<region>.<domain>
X-Amz-Date: <DATE>
```

```
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=content-
type;date;host;user-agent;x-amz-date;x-amz-target;x-amzn-requestid,
 Signature=<Signature>
User-Agent: <UserAgentString>
Accept: application/json
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Connection: Keep-Alive
X-Amz-Target: Logs_20140328.StopQuery
{
   "queryId": "12ab3456-12ab-123a-789e-1234567890ab"
}
```

Sample Response

```
HTTP/1.1 200 OK
x-amzn-RequestId: <RequestId>
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Date: <Date>
{
   "success": True
}
```

See Also

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

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)

- AWS SDK for Ruby V3

TagLogGroup

> **Important**
>
> The TagLogGroup operation is on the path to deprecation. We recommend that you use TagResource instead.

Adds or updates the specified tags for the specified log group.

To list the tags for a log group, use ListTagsForResource. To remove tags, use UntagResource.

For more information about tags, see Tag Log Groups in Amazon CloudWatch Logs in the *Amazon CloudWatch Logs User Guide*.

CloudWatch Logs doesn't support IAM policies that prevent users from assigning specified tags to log groups using the `aws:Resource/key-name` or `aws:TagKeys` condition keys. For more information about using tags to control access, see Controlling access to Amazon Web Services resources using tags.

Request Syntax

```
{
   "logGroupName": "string",
   "tags": {
      "string" : "string"
   }
}
```

Request Parameters

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

The request accepts the following data in JSON format.

logGroupName

The name of the log group.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `[\.\-_/#A-Za-z0-9]+`

Required: Yes

tags

The key-value pairs to use for the tags.

Type: String to string map

Map Entries: Maximum number of 50 items.

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

Key Pattern: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]+)$`

Value Length Constraints: Maximum length of 256.

Value Pattern: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$`

Required: Yes

Response Elements

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

Errors

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

InvalidParameterException

A parameter is specified incorrectly.

HTTP Status Code: 400

ResourceNotFoundException

The specified resource does not exist.

HTTP Status Code: 400

Examples

To add tags for a log group

The following example adds the specified tags for the specified log group.

Sample Request

```
POST / HTTP/1.1
Host: logs.<region>.<domain>
X-Amz-Date: <DATE>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=content-
type;date;host;user-agent;x-amz-date;x-amz-target;x-amzn-requestid,
 Signature=<Signature>
User-Agent: <UserAgentString>
Accept: application/json
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Connection: Keep-Alive
X-Amz-Target: Logs_20140328.TagLogGroup
{
  "logGroupName": "my-log-group",
  "tags": {
      "Project": "A",
      "Environment": "test"
  }
}
```

Sample Response

```
HTTP/1.1 200 OK
x-amzn-RequestId: <RequestId>
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Date: <Date>
```

See Also

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

- AWS Command Line Interface V2

- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

TagResource

Assigns one or more tags (key-value pairs) to the specified CloudWatch Logs resource. Currently, the only CloudWatch Logs resources that can be tagged are log groups and destinations.

Tags can help you organize and categorize your resources. You can also use them to scope user permissions by granting a user permission to access or change only resources with certain tag values.

Tags don't have any semantic meaning to AWS and are interpreted strictly as strings of characters.

You can use the `TagResource` action with a resource that already has tags. If you specify a new tag key for the alarm, this tag is appended to the list of tags associated with the alarm. If you specify a tag key that is already associated with the alarm, the new tag value that you specify replaces the previous value for that tag.

You can associate as many as 50 tags with a CloudWatch Logs resource.

Request Syntax

```
{
   "resourceArn": "string",
   "tags": {
      "string" : "string"
   }
}
```

Request Parameters

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

The request accepts the following data in JSON format.

resourceArn

The ARN of the resource that you're adding tags to.

The ARN format of a log group is `arn:aws:logs:`*`Region`*`:`*`account-id`*`:log-group:`*`log-group-name`*

The ARN format of a destination is `arn:aws:logs:`*`Region`*`:`*`account-id`*`:destination:`*`destination-name`*

For more information about ARN format, see CloudWatch Logs resources and operations.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 1011.

Pattern: `[\w+=/:,.@-]*`

Required: Yes

tags

The list of key-value pairs to associate with the resource.

Type: String to string map

Map Entries: Maximum number of 50 items.

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

Key Pattern: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]+)$`

Value Length Constraints: Maximum length of 256.

Value Pattern: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$`

Required: Yes

Response Elements

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

Errors

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

InvalidParameterException

A parameter is specified incorrectly.

HTTP Status Code: 400

ResourceNotFoundException

The specified resource does not exist.

HTTP Status Code: 400

ServiceUnavailableException

The service cannot complete the request.

HTTP Status Code: 500

TooManyTagsException

A resource can have no more than 50 tags.

resourceName

The name of the resource.

HTTP Status Code: 400

See Also

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

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

TestMetricFilter

Tests the filter pattern of a metric filter against a sample of log event messages. You can use this operation to validate the correctness of a metric filter pattern.

Request Syntax

```
{
   "filterPattern": "string",
   "logEventMessages": [ "string" ]
}
```

Request Parameters

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

The request accepts the following data in JSON format.

filterPattern

A symbolic description of how CloudWatch Logs should interpret the data in each log event. For example, a log event can contain timestamps, IP addresses, strings, and so on. You use the filter pattern to specify what to look for in the log event message.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 1024.

Required: Yes

logEventMessages

The log event messages to test.

Type: Array of strings

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

Length Constraints: Minimum length of 1.

Required: Yes

Response Syntax

```
{
   "matches": [
      {
         "eventMessage": "string",
         "eventNumber": number,
         "extractedValues": {
            "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.

matches

The matched events.

Type: Array of MetricFilterMatchRecord objects

Errors

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

InvalidParameterException

A parameter is specified incorrectly.

HTTP Status Code: 400

ServiceUnavailableException

The service cannot complete the request.

HTTP Status Code: 500

Examples

To test a metric filter pattern on Apache access.log events

The following example tests the specified metric filter pattern.

Sample Request

```
POST / HTTP/1.1
Host: logs.<region>.<domain>
X-Amz-Date: <DATE>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=content-
type;date;host;user-agent;x-amz-date;x-amz-target;x-amzn-requestid,
 Signature=<Signature>
User-Agent: <UserAgentString>
Accept: application/json
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Connection: Keep-Alive
X-Amz-Target: Logs_20140328.TestMetricFilter
{
  "filterPattern": "[ip, identity, user_id, timestamp, request, status_code, size]",
  "logEventMessages": [
    "127.0.0.1 - frank [10/Oct/2000:13:25:15 -0700] \"GET /apache_pb.gif HTTP/1.0\" 200
 1534",
    "127.0.0.1 - frank [10/Oct/2000:13:35:22 -0700] \"GET /apache_pb.gif HTTP/1.0\" 500
 5324",
    "127.0.0.1 - frank [10/Oct/2000:13:50:35 -0700] \"GET /apache_pb.gif HTTP/1.0\" 200
 4355"
  ]
}
```

Sample Response

```
HTTP/1.1 200 OK
x-amzn-RequestId: <RequestId>
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Date: <Date>
{
  "matches": [
    {
      "eventNumber": 0,
```

```
      "eventMessage": "127.0.0.1 - frank [10/Oct/2000:13:25:15 -0700] \"GET /
apache_pb.gif HTTP/1.0\" 200 1534",
      "extractedValues": {
        "$status_code": "200",
        "$identity": "-",
        "$request": "GET /apache_pb.gif HTTP/1.0",
        "$size": "1534,",
        "$user_id": "frank",
        "$ip": "127.0.0.1",
        "$timestamp": "10/Oct/2000:13:25:15 -0700"
      }
    },
    {
      "eventNumber": 1,
      "eventMessage": "127.0.0.1 - frank [10/Oct/2000:13:35:22 -0700] \"GET /
apache_pb.gif HTTP/1.0\" 500 5324",
      "extractedValues": {
        "$status_code": "500",
        "$identity": "-",
        "$request": "GET /apache_pb.gif HTTP/1.0",
        "$size": "5324,",
        "$user_id": "frank",
        "$ip": "127.0.0.1",
        "$timestamp": "10/Oct/2000:13:35:22 -0700"
      }
    },
    {
      "eventNumber": 2,
      "eventMessage": "127.0.0.1 - frank [10/Oct/2000:13:50:35 -0700] \"GET /
apache_pb.gif HTTP/1.0\" 200 4355",
      "extractedValues": {
        "$status_code": "200",
        "$identity": "-",
        "$request": "GET /apache_pb.gif HTTP/1.0",
        "$size": "4355",
        "$user_id": "frank",
        "$ip": "127.0.0.1",
        "$timestamp": "10/Oct/2000:13:50:35 -0700"
      }
    }
  ]
}
```

To test a metric filter pattern on Apache access.log events without specifying all the fields

The following example tests the specified metric filter pattern.

Sample Request

```
POST / HTTP/1.1
Host: logs.<region>.<domain>
X-Amz-Date: <DATE>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=content-
type;date;host;user-agent;x-amz-date;x-amz-target;x-amzn-requestid,
 Signature=<Signature>
User-Agent: <UserAgentString>
Accept: application/json
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Connection: Keep-Alive
X-Amz-Target: Logs_20140328.TestMetricFilter
{
  "filterPattern": "[..., size]",
  "logEventMessages": [
    "127.0.0.1 - frank [10/Oct/2000:13:25:15 -0700] \"GET /apache_pb.gif HTTP/1.0\" 200
 1534",
    "127.0.0.1 - frank [10/Oct/2000:13:35:22 -0700] \"GET /apache_pb.gif HTTP/1.0\" 500
 5324",
    "127.0.0.1 - frank [10/Oct/2000:13:50:35 -0700] \"GET /apache_pb.gif HTTP/1.0\" 200
 4355"
  ]
}
```

Sample Response

```
HTTP/1.1 200 OK
x-amzn-RequestId: <RequestId>
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Date: <Date>
{
  "matches": [
    {
      "eventNumber": 0,
```

```
      "eventMessage": "127.0.0.1 - frank [10/Oct/2000:13:25:15 -0700] \"GET /
apache_pb.gif HTTP/1.0\" 200 1534",
      "extractedValues": {
        "$size": "1534",
        "$6": "200",
        "$4": "10/Oct/2000:13:25:15 -0700",
        "$5": "GET /apache_pb.gif HTTP/1.0",
        "$2": "-",
        "$3": "frank",
        "$1": "127.0.0.1"
      }
    },
    {
      "eventNumber": 1,
      "eventMessage": "127.0.0.1 - frank [10/Oct/2000:13:35:22 -0700] \"GET /
apache_pb.gif HTTP/1.0\" 500 5324",
      "extractedValues": {
        "$size": "5324",
        "$6": "500",
        "$4": "10/Oct/2000:13:35:22 -0700",
        "$5": "GET /apache_pb.gif HTTP/1.0",
        "$2": "-",
        "$3": "frank",
        "$1": "127.0.0.1"
      }
    },
    {
      "eventNumber": 2,
      "eventMessage": "127.0.0.1 - frank [10/Oct/2000:13:50:35 -0700] \"GET /
apache_pb.gif HTTP/1.0\" 200 4355",
      "extractedValues": {
        "$size": "4355",
        "$6": "200",
        "$4": "10/Oct/2000:13:50:35 -0700",
        "$5": "GET /apache_pb.gif HTTP/1.0",
        "$2": "-",
        "$3": "frank",
        "$1": "127.0.0.1"
      }
    }
  ]
}
```

To test a metric filter pattern on Apache access.log events without specifying any fields

The following example tests the specified metric filter pattern.

Sample Request

```
POST / HTTP/1.1
Host: logs.<region>.<domain>
X-Amz-Date: <DATE>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=content-
type;date;host;user-agent;x-amz-date;x-amz-target;x-amzn-requestid,
 Signature=<Signature>
User-Agent: <UserAgentString>
Accept: application/json
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Connection: Keep-Alive
X-Amz-Target: Logs_20140328.TestMetricFilter
{
  "filterPattern": "[]",
  "logEventMessages": [
    "127.0.0.1 - frank [10/Oct/2000:13:25:15 -0700] \"GET /apache_pb.gif HTTP/1.0\" 200
 1534",
    "127.0.0.1 - frank [10/Oct/2000:13:35:22 -0700] \"GET /apache_pb.gif HTTP/1.0\" 500
 5324",
    "127.0.0.1 - frank [10/Oct/2000:13:50:35 -0700] \"GET /apache_pb.gif HTTP/1.0\" 200
 4355"
  ]
}
```

Sample Response

```
HTTP/1.1 200 OK
x-amzn-RequestId: <RequestId>
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Date: <Date>
{
  "matches": [
    {
      "eventNumber": 0,
```

```
      "eventMessage": "127.0.0.1 - frank [10/Oct/2000:13:25:15 -0700] \"GET /
apache_pb.gif HTTP/1.0\" 200 1534",
      "extractedValues": {
        "$7": "1534",
        "$6": "200",
        "$4": "10/Oct/2000:13:25:15 -0700",
        "$5": "GET /apache_pb.gif HTTP/1.0",
        "$2": "-",
        "$3": "frank",
        "$1": "127.0.0.1"
      }
    },
    {
      "eventNumber": 1,
      "eventMessage": "127.0.0.1 - frank [10/Oct/2000:13:35:22 -0700] \"GET /
apache_pb.gif HTTP/1.0\" 500 5324",
      "extractedValues": {
        "$7": "5324",
        "$6": "500",
        "$4": "10/Oct/2000:13:35:22 -0700",
        "$5": "GET /apache_pb.gif HTTP/1.0",
        "$2": "-",
        "$3": "frank",
        "$1": "127.0.0.1"
      }
    },
    {
      "eventNumber": 2,
      "eventMessage": "127.0.0.1 - frank [10/Oct/2000:13:50:35 -0700] \"GET /
apache_pb.gif HTTP/1.0\" 200 4355",
      "extractedValues": {
        "$7": "4355",
        "$6": "200",
        "$4": "10/Oct/2000:13:50:35 -0700",
        "$5": "GET /apache_pb.gif HTTP/1.0",
        "$2": "-",
        "$3": "frank",
        "$1": "127.0.0.1"
      }
    }
  ]
}
```

To test a metric filter pattern that matches successful requests in Apache access.log events

The following example tests the specified metric filter pattern.

Sample Request

```
POST / HTTP/1.1
Host: logs.<region>.<domain>
X-Amz-Date: <DATE>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=content-
type;date;host;user-agent;x-amz-date;x-amz-target;x-amzn-requestid,
 Signature=<Signature>
User-Agent: <UserAgentString>
Accept: application/json
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Connection: Keep-Alive
X-Amz-Target: Logs_20140328.TestMetricFilter
{
  "filterPattern": "[..., status_code=200, size]",
  "logEventMessages": [
    "127.0.0.1 - frank [10/Oct/2000:13:25:15 -0700] \"GET /apache_pb.gif HTTP/1.0\" 200
 1534",
    "127.0.0.1 - frank [10/Oct/2000:13:35:22 -0700] \"GET /apache_pb.gif HTTP/1.0\" 500
 5324",
    "127.0.0.1 - frank [10/Oct/2000:13:50:35 -0700] \"GET /apache_pb.gif HTTP/1.0\" 200
 4355"
  ]
}
```

Sample Response

```
HTTP/1.1 200 OK
x-amzn-RequestId: <RequestId>
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Date: <Date>
{
  "matches": [
    {
      "eventNumber": 0,
```

```
      "eventMessage": "127.0.0.1 - frank [10/Oct/2000:13:25:15 -0700] \"GET /
apache_pb.gif HTTP/1.0\" 200 1534",
      "extractedValues": {
        "$status_code": "200",
        "$size": "1534",
        "$4": "10/Oct/2000:13:25:15 -0700",
        "$5": "GET /apache_pb.gif HTTP/1.0",
        "$2": "-",
        "$3": "frank",
        "$1": "127.0.0.1"
      }
    },
    {
      "eventNumber": 2,
      "eventMessage": "127.0.0.1 - frank [10/Oct/2000:13:50:35 -0700] \"GET /
apache_pb.gif HTTP/1.0\" 200 4355",
      "extractedValues": {
        "$status_code": "200",
        "$size": "4355",
        "$4": "10/Oct/2000:13:50:35 -0700",
        "$5": "GET /apache_pb.gif HTTP/1.0",
        "$2": "-",
        "$3": "frank",
        "$1": "127.0.0.1"
      }
    }
  ]
}
```

To test a metric filter pattern that matches 4XX response codes for HTML pages in Apache access.log events

The following example tests the specified metric filter pattern.

Sample Request

```
POST / HTTP/1.1
Host: logs.<region>.<domain>
X-Amz-Date: <DATE>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=content-
type;date;host;user-agent;x-amz-date;x-amz-target;x-amzn-requestid,
 Signature=<Signature>
User-Agent: <UserAgentString>
```

```
Accept: application/json
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Connection: Keep-Alive
X-Amz-Target: Logs_20140328.TestMetricFilter
{
  "filterPattern": "[..., request=*.html*, status_code=4*,]",
  "logEventMessages": [
    "127.0.0.1 - frank [10/Oct/2000:13:25:15 -0700] \"GET /index.html HTTP/1.0\" 404
 1534",
    "127.0.0.1 - frank [10/Oct/2000:13:35:22 -0700] \"GET /about-us/index.html
 HTTP/1.0\" 200 5324",
    "127.0.0.1 - frank [10/Oct/2000:13:50:35 -0700] \"GET /apache_pb.gif HTTP/1.0\" 404
 4355",
    "127.0.0.1 - frank [10/Oct/2000:13:25:15 -0700] \"GET /products/index.html
 HTTP/1.0\" 400 1534",
  ]
}
```

Sample Response

```
HTTP/1.1 200 OK
x-amzn-RequestId: <RequestId>
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Date: <Date>
{
  "matches": [
    {
      "eventNumber": 0,
      "eventMessage": "127.0.0.1 - frank [10/Oct/2000:13:25:15 -0700] \"GET /index.html
 HTTP/1.0\" 404 1534",
      "extractedValues": {
        "$status_code": "404",
        "$request": "GET /index.html HTTP/1.0",
        "$7": "1534",
        "$4": "10/Oct/2000:13:25:15 -0700",
        "$2": "-",
        "$3": "frank",
        "$1": "127.0.0.1"
      }
    },
    {
```

```
      "eventNumber": 3,
      "eventMessage": "127.0.0.1 - frank [10/Oct/2000:13:25:15 -0700] \"GET /products/
index.html HTTP/1.0\" 400 1534",
      "extractedValues": {
        "$status_code": "400",
        "$request": "GET /products/index.html HTTP/1.0",
        "$7": "1534",
        "$4": "10/Oct/2000:13:25:15 -0700",
        "$2": "-",
        "$3": "frank",
        "$1": "127.0.0.1"
      }
    }
  ]
}
```

To test a metric filter pattern that matches occurrences of "[ERROR]" in log events

The following example tests the specified metric filter pattern.

Sample Request

```
POST / HTTP/1.1
Host: logs.<region>.<domain>
X-Amz-Date: <DATE>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=content-
type;date;host;user-agent;x-amz-date;x-amz-target;x-amzn-requestid,
 Signature=<Signature>
User-Agent: <UserAgentString>
Accept: application/json
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Connection: Keep-Alive
X-Amz-Target: Logs_20140328.TestMetricFilter
{
  "filterPattern": "\"[ERROR]\"",
  "logEventMessages": [
    "02 May 2014 00:34:12,525 [INFO] Starting the application",
    "02 May 2014 00:35:14,245 [DEBUG] Database connection established",
    "02 May 2014 00:34:14,663 [INFO] Executing SQL Query",
    "02 May 2014 00:34:16,142 [ERROR] Unhanded exception: InvalidQueryException",
    "02 May 2014 00:34:16,224 [ERROR] Terminating the application"
  ]
```

```
}
```

Sample Response

```
HTTP/1.1 200 OK
x-amzn-RequestId: <RequestId>
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Date: <Date>
{
  "matches": [
    {
      "eventNumber": 3,
      "eventMessage": "02 May 2014 00:34:16,142 [ERROR] Unhanded exception:
 InvalidQueryException",
      "extractedValues": {}
    },
    {
      "eventNumber": 4,
      "eventMessage": "02 May 2014 00:34:16,224 [ERROR] Terminating the application",
      "extractedValues": {}
    }
  ]
}
```

To test a metric filter pattern that matches occurrences of "[ERROR]" and "Exception" in log events

The following example tests the specified metric filter pattern.

Sample Request

```
POST / HTTP/1.1
Host: logs.<region>.<domain>
X-Amz-Date: <DATE>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=content-
type;date;host;user-agent;x-amz-date;x-amz-target;x-amzn-requestid,
 Signature=<Signature>
User-Agent: <UserAgentString>
Accept: application/json
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
```

```
Connection: Keep-Alive
X-Amz-Target: Logs_20140328.TestMetricFilter
{
  "filterPattern": "\"[ERROR]\" Exception",
  "logEventMessages": [
    "02 May 2014 00:34:12,525 [INFO] Starting the application",
    "02 May 2014 00:35:14,245 [DEBUG] Database connection established",
    "02 May 2014 00:34:14,663 [INFO] Executing SQL Query",
    "02 May 2014 00:34:16,142 [ERROR] Unhanded exception: InvalidQueryException",
    "02 May 2014 00:34:16,224 [ERROR] Terminating the application"
  ]
}
```

Sample Response

```
HTTP/1.1 200 OK
x-amzn-RequestId: <RequestId>
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Date: <Date>
{
  "matches": [
    {
      "eventNumber": 3,
      "eventMessage": "02 May 2014 00:34:16,142 [ERROR] Unhanded exception:
 InvalidQueryException",
      "extractedValues": {}
    }
  ]
}
```

See Also

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

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2

- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

TestTransformer

Use this operation to test a log transformer. You enter the transformer configuration and a set of log events to test with. The operation responds with an array that includes the original log events and the transformed versions.

Request Syntax

```
{
   "logEventMessages": [ "string" ],
   "transformerConfig": [
      {
         "addKeys": {
            "entries": [
               {
                  "key": "string",
                  "overwriteIfExists": boolean,
                  "value": "string"
               }
            ]
         },
         "copyValue": {
            "entries": [
               {
                  "overwriteIfExists": boolean,
                  "source": "string",
                  "target": "string"
               }
            ]
         },
         "csv": {
            "columns": [ "string" ],
            "delimiter": "string",
            "destination": "string",
            "quoteCharacter": "string",
            "source": "string"
         },
         "dateTimeConverter": {
            "locale": "string",
            "matchPatterns": [ "string" ],
            "source": "string",
            "sourceTimezone": "string",
```

```
            "target": "string",
            "targetFormat": "string",
            "targetTimezone": "string"
         },
         "deleteKeys": {
            "withKeys": [ "string" ]
         },
         "grok": {
            "match": "string",
            "source": "string"
         },
         "listToMap": {
            "flatten": boolean,
            "flattenedElement": "string",
            "key": "string",
            "source": "string",
            "target": "string",
            "valueKey": "string"
         },
         "lowerCaseString": {
            "withKeys": [ "string" ]
         },
         "moveKeys": {
            "entries": [
               {
                  "overwriteIfExists": boolean,
                  "source": "string",
                  "target": "string"
               }
            ]
         },
         "parseCloudfront": {
            "source": "string"
         },
         "parseJSON": {
            "destination": "string",
            "source": "string"
         },
         "parseKeyValue": {
            "destination": "string",
            "fieldDelimiter": "string",
            "keyPrefix": "string",
            "keyValueDelimiter": "string",
            "nonMatchValue": "string",
```

```
            "overwriteIfExists": boolean,
            "source": "string"
         },
         "parsePostgres": {
            "source": "string"
         },
         "parseRoute53": {
            "source": "string"
         },
         "parseToOCSF": {
            "eventSource": "string",
            "mappingVersion": "string",
            "ocsfVersion": "string",
            "source": "string"
         },
         "parseVPC": {
            "source": "string"
         },
         "parseWAF": {
            "source": "string"
         },
         "renameKeys": {
            "entries": [
               {
                  "key": "string",
                  "overwriteIfExists": boolean,
                  "renameTo": "string"
               }
            ]
         },
         "splitString": {
            "entries": [
               {
                  "delimiter": "string",
                  "source": "string"
               }
            ]
         },
         "substituteString": {
            "entries": [
               {
                  "from": "string",
                  "source": "string",
                  "to": "string"
```

```
                }
             ]
          },
          "trimString": {
             "withKeys": [ "string" ]
          },
          "typeConverter": {
             "entries": [
                {
                   "key": "string",
                   "type": "string"
                }
             ]
          },
          "upperCaseString": {
             "withKeys": [ "string" ]
          }
       }
    ]
}
```

Request Parameters

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

The request accepts the following data in JSON format.

logEventMessages

An array of the raw log events that you want to use to test this transformer.

Type: Array of strings

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

Length Constraints: Minimum length of 1.

Required: Yes

transformerConfig

This structure contains the configuration of this log transformer that you want to test. A log transformer is an array of processors, where each processor applies one type of transformation to the log events that are ingested.

Type: Array of Processor objects

Array Members: Minimum number of 1 item. Maximum number of 20 items.

Required: Yes

Response Syntax

```
{
   "transformedLogs": [
      {
         "eventMessage": "string",
         "eventNumber": number,
         "transformedEventMessage": "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.

transformedLogs

An array where each member of the array includes both the original version and the transformed version of one of the log events that you input.

Type: Array of TransformedLogRecord objects

Errors

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

InvalidOperationException

The operation is not valid on the specified resource.

HTTP Status Code: 400

InvalidParameterException

A parameter is specified incorrectly.

HTTP Status Code: 400

ServiceUnavailableException

The service cannot complete the request.

HTTP Status Code: 500

See Also

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

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

UntagLogGroup

> **Important**
>
> The UntagLogGroup operation is on the path to deprecation. We recommend that you use UntagResource instead.

Removes the specified tags from the specified log group.

To list the tags for a log group, use ListTagsForResource. To add tags, use TagResource.

When using IAM policies to control tag management for CloudWatch Logs log groups, the condition keys `aws:Resource/key-name` and `aws:TagKeys` cannot be used to restrict which tags users can assign.

Request Syntax

```
{
   "logGroupName": "string",
   "tags": [ "string" ]
}
```

Request Parameters

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

The request accepts the following data in JSON format.

logGroupName

The name of the log group.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `[\.\-_/#A-Za-z0-9]+`

Required: Yes

tags

The tag keys. The corresponding tags are removed from the log group.

Type: Array of strings

Array Members: Minimum number of 1 item.

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

Pattern: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]+)$`

Required: Yes

Response Elements

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

Errors

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

ResourceNotFoundException

The specified resource does not exist.

HTTP Status Code: 400

Examples

To remove tags from a log group

The following example removes the specified tags for the specified log group.

Sample Request

```
POST / HTTP/1.1
Host: logs.<region>.<domain>
X-Amz-Date: <DATE>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=content-
type;date;host;user-agent;x-amz-date;x-amz-target;x-amzn-requestid,
 Signature=<Signature>
```

```
User-Agent: <UserAgentString>
Accept: application/json
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Connection: Keep-Alive
X-Amz-Target: Logs_20140328.UntagLogGroup
{
  "logGroupName": "my-log-group",
  "tags": {"Project", "Environment"}
}
```

Sample Response

```
HTTP/1.1 200 OK
x-amzn-RequestId: <RequestId>
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Date: <Date>
```

See Also

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

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

UntagResource

Removes one or more tags from the specified resource.

Request Syntax

```
{
   "resourceArn": "string",
   "tagKeys": [ "string" ]
}
```

Request Parameters

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

The request accepts the following data in JSON format.

resourceArn

The ARN of the CloudWatch Logs resource that you're removing tags from.

The ARN format of a log group is `arn:aws:logs:`*`Region`*`:`*`account-id`*`:log-group:`*`log-group-name`*

The ARN format of a destination is `arn:aws:logs:`*`Region`*`:`*`account-id`*`:destination:`*`destination-name`*

For more information about ARN format, see CloudWatch Logs resources and operations.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 1011.

Pattern: `[\w+=/:,.@-]*`

Required: Yes

tagKeys

The list of tag keys to remove from the resource.

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 128.

Pattern: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]+)$`

Required: Yes

Response Elements

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

Errors

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

InvalidParameterException

A parameter is specified incorrectly.

HTTP Status Code: 400

ResourceNotFoundException

The specified resource does not exist.

HTTP Status Code: 400

ServiceUnavailableException

The service cannot complete the request.

HTTP Status Code: 500

See Also

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

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++

- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

UpdateAnomaly

Use this operation to *suppress* anomaly detection for a specified anomaly or pattern. If you suppress an anomaly, CloudWatch Logs won't report new occurrences of that anomaly and won't update that anomaly with new data. If you suppress a pattern, CloudWatch Logs won't report any anomalies related to that pattern.

You must specify either `anomalyId` or `patternId`, but you can't specify both parameters in the same operation.

If you have previously used this operation to suppress detection of a pattern or anomaly, you can use it again to cause CloudWatch Logs to end the suppression. To do this, use this operation and specify the anomaly or pattern to stop suppressing, and omit the `suppressionType` and `suppressionPeriod` parameters.

Request Syntax

```
{
   "anomalyDetectorArn": "string",
   "anomalyId": "string",
   "baseline": boolean,
   "patternId": "string",
   "suppressionPeriod": {
      "suppressionUnit": "string",
      "value": number
   },
   "suppressionType": "string"
}
```

Request Parameters

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

The request accepts the following data in JSON format.

anomalyDetectorArn

The ARN of the anomaly detector that this operation is to act on.

Type: String

Length Constraints: Minimum length of 1.

Pattern: `[\w#+=/:,.@-]*`

Required: Yes

anomalyId

If you are suppressing or unsuppressing an anomaly, specify its unique ID here. You can find anomaly IDs by using the ListAnomalies operation.

Type: String

Length Constraints: Fixed length of 36.

Required: No

baseline

Set this to `true` to prevent CloudWatch Logs from displaying this behavior as an anomaly in the future. The behavior is then treated as baseline behavior. However, if similar but more severe occurrences of this behavior occur in the future, those will still be reported as anomalies.

The default is `false`

Type: Boolean

Required: No

patternId

If you are suppressing or unsuppressing an pattern, specify its unique ID here. You can find pattern IDs by using the ListAnomalies operation.

Type: String

Length Constraints: Fixed length of 32.

Required: No

suppressionPeriod

If you are temporarily suppressing an anomaly or pattern, use this structure to specify how long the suppression is to last.

Type: SuppressionPeriod object

Required: No

suppressionType

Use this to specify whether the suppression to be temporary or infinite. If you specify `LIMITED`, you must also specify a `suppressionPeriod`. If you specify `INFINITE`, any value for `suppressionPeriod` is ignored.

Type: String

Valid Values: `LIMITED | INFINITE`

Required: No

Response Elements

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

Errors

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

InvalidParameterException

A parameter is specified incorrectly.

HTTP Status Code: 400

OperationAbortedException

Multiple concurrent requests to update the same resource were in conflict.

HTTP Status Code: 400

ResourceNotFoundException

The specified resource does not exist.

HTTP Status Code: 400

ServiceUnavailableException

The service cannot complete the request.

HTTP Status Code: 500

See Also

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

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

UpdateDeliveryConfiguration

Use this operation to update the configuration of a delivery to change either the S3 path pattern or the format of the delivered logs. You can't use this operation to change the source or destination of the delivery.

Request Syntax

```
{
   "fieldDelimiter": "string",
   "id": "string",
   "recordFields": [ "string" ],
   "s3DeliveryConfiguration": {
      "enableHiveCompatiblePath": boolean,
      "suffixPath": "string"
   }
}
```

Request Parameters

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

The request accepts the following data in JSON format.

fieldDelimiter

The field delimiter to use between record fields when the final output format of a delivery is in `Plain`, `W3C`, or `Raw` format.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 5.

Required: No

id

The ID of the delivery to be updated by this request.

Type: String

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

Pattern: ^[0-9A-Za-z]+$

Required: Yes

recordFields

The list of record fields to be delivered to the destination, in order. If the delivery's log source has mandatory fields, they must be included in this list.

Type: Array of strings

Array Members: Minimum number of 0 items. Maximum number of 128 items.

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

Required: No

s3DeliveryConfiguration

This structure contains parameters that are valid only when the delivery's delivery destination is an S3 bucket.

Type: S3DeliveryConfiguration object

Required: No

Response Elements

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

Errors

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

AccessDeniedException

You don't have sufficient permissions to perform this action.

HTTP Status Code: 400

ConflictException

This operation attempted to create a resource that already exists.

HTTP Status Code: 400

ResourceNotFoundException

The specified resource does not exist.

HTTP Status Code: 400

ServiceUnavailableException

The service cannot complete the request.

HTTP Status Code: 500

ThrottlingException

The request was throttled because of quota limits.

HTTP Status Code: 400

ValidationException

One of the parameters for the request is not valid.

HTTP Status Code: 400

See Also

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

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

UpdateLogAnomalyDetector

Updates an existing log anomaly detector.

Request Syntax

```
{
   "anomalyDetectorArn": "string",
   "anomalyVisibilityTime": number,
   "enabled": boolean,
   "evaluationFrequency": "string",
   "filterPattern": "string"
}
```

Request Parameters

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

The request accepts the following data in JSON format.

anomalyDetectorArn

The ARN of the anomaly detector that you want to update.

Type: String

Length Constraints: Minimum length of 1.

Pattern: `[\w#+=/:,.@-]*`

Required: Yes

anomalyVisibilityTime

The number of days to use as the life cycle of anomalies. After this time, anomalies are automatically baselined and the anomaly detector model will treat new occurrences of similar event as normal. Therefore, if you do not correct the cause of an anomaly during this time, it will be considered normal going forward and will not be detected.

Type: Long

Valid Range: Minimum value of 7. Maximum value of 90.

Required: No

enabled

Use this parameter to pause or restart the anomaly detector.

Type: Boolean

Required: Yes

evaluationFrequency

Specifies how often the anomaly detector runs and look for anomalies. Set this value according to the frequency that the log group receives new logs. For example, if the log group receives new log events every 10 minutes, then setting `evaluationFrequency` to `FIFTEEN_MIN` might be appropriate.

Type: String

Valid Values: `ONE_MIN | FIVE_MIN | TEN_MIN | FIFTEEN_MIN | THIRTY_MIN | ONE_HOUR`

Required: No

filterPattern

A symbolic description of how CloudWatch Logs should interpret the data in each log event. For example, a log event can contain timestamps, IP addresses, strings, and so on. You use the filter pattern to specify what to look for in the log event message.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 1024.

Required: No

Response Elements

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

Errors

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

InvalidParameterException

A parameter is specified incorrectly.

HTTP Status Code: 400

OperationAbortedException

Multiple concurrent requests to update the same resource were in conflict.

HTTP Status Code: 400

ResourceNotFoundException

The specified resource does not exist.

HTTP Status Code: 400

ServiceUnavailableException

The service cannot complete the request.

HTTP Status Code: 500

See Also

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

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

UpdateLookupTable

Updates an existing lookup table by replacing all of its content with new CSV data or CloudWatch Logs query results. After the update completes, queries that use this table use the new data.

This is a full replacement operation. All existing content is replaced. You must specify either `tableBody` or `queryId`, but not both.

Request Syntax

```
{
   "description": "string",
   "kmsKeyId": "string",
   "lookupTableArn": "string",
   "queryId": "string",
   "tableBody": "string"
}
```

Request Parameters

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

The request accepts the following data in JSON format.

description

An updated description of the lookup table.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 1024.

Required: No

kmsKeyId

The ARN of the AWS KMS key to use to encrypt the lookup table data. You can use this parameter to add, update, or remove the KMS key. To remove the KMS key and use an AWS-owned key instead, specify an empty string.

Type: String

Length Constraints: Maximum length of 256.

Required: No

lookupTableArn

The ARN of the lookup table to update.

Type: String

Required: Yes

queryId

The ID of a completed or cancelled CloudWatch Logs query whose results replace the lookup table content. A cancelled query replaces the content with the partial results that were available when the query was stopped.

You must specify either `tableBody` or `queryId`, but not both.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Required: No

tableBody

The new CSV content to replace the existing data. The first row must be a header row with column names. The content must use UTF-8 encoding and not exceed 10 MB.

You must specify either `tableBody` or `queryId`, but not both.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 10485760.

Required: No

Response Syntax

```
{
   "lastUpdatedTime": number,
   "lookupTableArn": "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.

lastUpdatedTime

The time when the lookup table was last updated, expressed as the number of milliseconds after `Jan 1, 1970 00:00:00 UTC`.

Type: Long

Valid Range: Minimum value of 0.

lookupTableArn

The ARN of the lookup table that was updated.

Type: String

Errors

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

AccessDeniedException

You don't have sufficient permissions to perform this action.

HTTP Status Code: 400

InvalidParameterException

A parameter is specified incorrectly.

HTTP Status Code: 400

ResourceNotFoundException

The specified resource does not exist.

HTTP Status Code: 400

ServiceUnavailableException

The service cannot complete the request.

HTTP Status Code: 500

ValidationException

One of the parameters for the request is not valid.

HTTP Status Code: 400

See Also

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

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

UpdateScheduledQuery

Updates an existing scheduled query with new configuration. This operation uses PUT semantics, allowing modification of query parameters, schedule, and destinations.

Request Syntax

```
{
   "description": "string",
   "destinationConfiguration": {
      "lookupTableConfiguration": {
         "description": "string",
         "kmsKeyId": "string",
         "roleArn": "string",
         "tableName": "string",
         "tags": {
            "string" : "string"
         }
      },
      "s3Configuration": {
         "destinationIdentifier": "string",
         "kmsKeyId": "string",
         "ownerAccountId": "string",
         "roleArn": "string"
      }
   },
   "endTimeOffset": number,
   "executionRoleArn": "string",
   "identifier": "string",
   "logGroupIdentifiers": [ "string" ],
   "queryLanguage": "string",
   "queryString": "string",
   "scheduleEndTime": number,
   "scheduleExpression": "string",
   "scheduleStartTime": number,
   "startTimeOffset": number,
   "state": "string",
   "timezone": "string"
}
```

Request Parameters

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

The request accepts the following data in JSON format.

description

An updated description for the scheduled query.

Type: String

Length Constraints: Maximum length of 1024.

Required: No

destinationConfiguration

The updated configuration for where to deliver query results.

Type: DestinationConfiguration object

Required: No

endTimeOffset

The updated time offset in seconds that defines the end of the lookback period for the query.

Type: Long

Required: No

executionRoleArn

The updated ARN of the IAM role that grants permissions to execute the query and deliver results.

Type: String

Length Constraints: Minimum length of 1.

Required: Yes

identifier

The ARN or name of the scheduled query to update.

Type: String

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

Required: Yes

logGroupIdentifiers

The updated array of log group names or ARNs to query.

Type: Array of strings

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

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

Pattern: `[\w#+=/:,.@-]*`

Required: No

queryLanguage

The updated query language for the scheduled query.

Type: String

Valid Values: `CWLI | SQL | PPL`

Required: Yes

queryString

The updated query string to execute.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 10000.

Required: Yes

scheduleEndTime

The updated end time for the scheduled query in Unix epoch format.

Type: Long

Valid Range: Minimum value of 0.

Required: No

scheduleExpression

The updated cron expression that defines when the scheduled query runs.

Type: String

Length Constraints: Maximum length of 256.

Required: Yes

scheduleStartTime

The updated start time for the scheduled query in Unix epoch format.

Type: Long

Valid Range: Minimum value of 0.

Required: No

startTimeOffset

The updated time offset in seconds that defines the lookback period for the query.

Type: Long

Required: No

state

The updated state of the scheduled query.

Type: String

Valid Values: `ENABLED | DISABLED`

Required: No

timezone

The updated timezone for evaluating the schedule expression.

Type: String

Length Constraints: Minimum length of 1.

Required: No

Response Syntax

```
{
   "creationTime": number,
   "description": "string",
   "destinationConfiguration": {
      "lookupTableConfiguration": {
         "description": "string",
         "kmsKeyId": "string",
         "roleArn": "string",
         "tableName": "string",
         "tags": {
            "string" : "string"
         }
      },
      "s3Configuration": {
         "destinationIdentifier": "string",
         "kmsKeyId": "string",
         "ownerAccountId": "string",
         "roleArn": "string"
      }
   },
   "endTimeOffset": number,
   "executionRoleArn": "string",
   "lastExecutionStatus": "string",
   "lastTriggeredTime": number,
   "lastUpdatedTime": number,
   "logGroupIdentifiers": [ "string" ],
   "name": "string",
   "queryLanguage": "string",
   "queryString": "string",
   "scheduledQueryArn": "string",
   "scheduleEndTime": number,
   "scheduleExpression": "string",
   "scheduleStartTime": number,
   "scheduleType": "string",
   "startTimeOffset": number,
```

```
    "state": "string",
    "timezone": "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.

creationTime

The timestamp when the scheduled query was originally created.

Type: Long

Valid Range: Minimum value of 0.

description

The description of the updated scheduled query.

Type: String

Length Constraints: Maximum length of 1024.

destinationConfiguration

The destination configuration of the updated scheduled query.

Type: DestinationConfiguration object

endTimeOffset

The end time offset in seconds of the updated scheduled query.

Type: Long

executionRoleArn

The execution role ARN of the updated scheduled query.

Type: String

Length Constraints: Minimum length of 1.

lastExecutionStatus

The status of the most recent execution of the updated scheduled query.

Type: String

Valid Values: `Running | InvalidQuery | Complete | Failed | Timeout`

lastTriggeredTime

The timestamp when the updated scheduled query was last executed.

Type: Long

Valid Range: Minimum value of 0.

lastUpdatedTime

The timestamp when the scheduled query was last updated.

Type: Long

Valid Range: Minimum value of 0.

logGroupIdentifiers

The log groups queried by the updated scheduled query.

Type: Array of strings

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

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

Pattern: `[\w#+=/:,.@-]*`

name

The name of the updated scheduled query.

Type: String

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

queryLanguage

The query language of the updated scheduled query.

Type: String

Valid Values: `CWLI | SQL | PPL`

queryString

The query string of the updated scheduled query.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 10000.

scheduledQueryArn

The ARN of the updated scheduled query.

Type: String

scheduleEndTime

The end time of the updated scheduled query.

Type: Long

Valid Range: Minimum value of 0.

scheduleExpression

The cron expression of the updated scheduled query.

Type: String

Length Constraints: Maximum length of 256.

scheduleStartTime

The start time of the updated scheduled query.

Type: Long

Valid Range: Minimum value of 0.

scheduleType

The schedule type of the updated scheduled query.

Type: String

Valid Values: `CUSTOMER_MANAGED | AWS_MANAGED`

startTimeOffset

The time offset of the updated scheduled query.

Type: Long

state

The state of the updated scheduled query.

Type: String

Valid Values: `ENABLED | DISABLED`

timezone

The timezone of the updated scheduled query.

Type: String

Length Constraints: Minimum length of 1.

Errors

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

AccessDeniedException

You don't have sufficient permissions to perform this action.

HTTP Status Code: 400

ConflictException

This operation attempted to create a resource that already exists.

HTTP Status Code: 400

InternalServerException

An internal server error occurred while processing the request. This exception is returned when the service encounters an unexpected condition that prevents it from fulfilling the request.

HTTP Status Code: 500

ResourceNotFoundException

The specified resource does not exist.

HTTP Status Code: 400

ThrottlingException

The request was throttled because of quota limits.

HTTP Status Code: 400

ValidationException

One of the parameters for the request is not valid.

HTTP Status Code: 400

See Also

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

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby V3

Data Types

The Amazon CloudWatch Logs 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:

- AccountPolicy
- AddKeyEntry
- AddKeys
- AggregateLogGroupSummary
- Anomaly
- AnomalyDetector
- ConfigurationTemplate
- ConfigurationTemplateDeliveryConfigValues
- CopyValue
- CopyValueEntry
- CSV
- DataSource
- DataSourceFilter
- DateTimeConverter
- DeleteKeys
- Delivery
- DeliveryDestination
- DeliveryDestinationConfiguration
- DeliverySource
- DeliverySourceConfigurationSchema

- Destination
- DestinationConfiguration
- Entity
- ExportTask
- ExportTaskExecutionInfo
- ExportTaskStatus
- FieldIndex
- FieldsData
- FilteredLogEvent
- GetLogObjectResponseStream
- Grok
- GroupingIdentifier
- Import
- ImportBatch
- ImportFilter
- ImportStatistics
- IndexPolicy
- InputLogEvent
- IntegrationDetails
- IntegrationSummary
- ListToMap
- LiveTailSessionLogEvent
- LiveTailSessionMetadata
- LiveTailSessionStart
- LiveTailSessionUpdate
- LogEvent
- LogFieldsListItem
- LogFieldType
- LogGroup
- LogGroupField

- LogGroupSummary
- LogStream
- LookupTable
- LookupTableConfiguration
- LowerCaseString
- MetricFilter
- MetricFilterMatchRecord
- MetricTransformation
- MoveKeyEntry
- MoveKeys
- OpenSearchApplication
- OpenSearchCollection
- OpenSearchDataAccessPolicy
- OpenSearchDataSource
- OpenSearchEncryptionPolicy
- OpenSearchIntegrationDetails
- OpenSearchLifecyclePolicy
- OpenSearchNetworkPolicy
- OpenSearchResourceConfig
- OpenSearchResourceStatus
- OpenSearchWorkspace
- OutputLogEvent
- ParseCloudfront
- ParseJSON
- ParseKeyValue
- ParsePostgres
- ParseRoute53
- ParseToOCSF
- ParseVPC
- ParseWAF

- PatternToken
- Policy
- Processor
- QueryCompileError
- QueryCompileErrorLocation
- QueryDefinition
- QueryInfo
- QueryParameter
- QueryStatistics
- RecordField
- RejectedEntityInfo
- RejectedLogEventsInfo
- RenameKeyEntry
- RenameKeys
- ResourceConfig
- ResourcePolicy
- ResultField
- S3Configuration
- S3DeliveryConfiguration
- S3TableIntegrationSource
- S3TablesIntegration
- ScheduledQueryDestination
- ScheduledQuerySummary
- SearchedLogStream
- SplitString
- SplitStringEntry
- StartLiveTailResponseStream
- SubscriptionFilter
- SubstituteString
- SubstituteStringEntry

- SuppressionPeriod
- SyslogConfiguration
- TagFilter
- TransformedLogRecord
- TriggerHistoryRecord
- TrimString
- TypeConverter
- TypeConverterEntry
- UpperCaseString

AccountPolicy

A structure that contains information about one CloudWatch Logs account policy.

Contents

accountId

The AWS account ID that the policy applies to.

Type: String

Length Constraints: Fixed length of 12.

Pattern: `^\d{12}$`

Required: No

lastUpdatedTime

The date and time that this policy was most recently updated.

Type: Long

Valid Range: Minimum value of 0.

Required: No

policyDocument

The policy document for this account policy.

The JSON specified in `policyDocument` can be up to 30,720 characters.

Type: String

Required: No

policyName

The name of the account policy.

Type: String

Required: No

policyType

The type of policy for this account policy.

Type: String

Valid Values: `DATA_PROTECTION_POLICY | SUBSCRIPTION_FILTER_POLICY | FIELD_INDEX_POLICY | TRANSFORMER_POLICY | METRIC_EXTRACTION_POLICY`

Required: No

scope

The scope of the account policy.

Type: String

Valid Values: `ALL`

Required: No

selectionCriteria

The log group selection criteria that is used for this policy.

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

AddKeyEntry

This object defines one key that will be added with the addKeys processor.

Contents

key

The key of the new entry to be added to the log event

Type: String

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

Required: Yes

value

The value of the new entry to be added to the log event

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Required: Yes

overwriteIfExists

Specifies whether to overwrite the value if the key already exists in the log event. If you omit this, the default is `false`.

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

AddKeys

This processor adds new key-value pairs to the log event.

For more information about this processor including examples, see addKeys in the *CloudWatch Logs User Guide*.

Contents

entries

An array of objects, where each object contains the information about one key to add to the log event.

Type: Array of AddKeyEntry objects

Array Members: Minimum number of 1 item. Maximum number of 5 items.

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

AggregateLogGroupSummary

Contains an aggregate summary of log groups grouped by data source characteristics, including the count of log groups and their grouping identifiers.

Contents

groupingIdentifiers

An array of key-value pairs that identify the data source characteristics used to group the log groups.

The size and content of this array depends on the `groupBy` parameter specified in the request.

Type: Array of GroupingIdentifier objects

Required: No

logGroupCount

The number of log groups in this aggregate summary group.

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

Anomaly

This structure represents one anomaly that has been found by a logs anomaly detector.

For more information about patterns and anomalies, see CreateLogAnomalyDetector.

Contents

active

Specifies whether this anomaly is still ongoing.

Type: Boolean

Required: Yes

anomalyDetectorArn

The ARN of the anomaly detector that identified this anomaly.

Type: String

Length Constraints: Minimum length of 1.

Pattern: `[\w#+=/:,.@-]*`

Required: Yes

anomalyId

The unique ID that CloudWatch Logs assigned to this anomaly.

Type: String

Length Constraints: Fixed length of 36.

Required: Yes

description

A human-readable description of the anomaly. This description is generated by CloudWatch Logs.

Type: String

Length Constraints: Minimum length of 1.

Required: Yes

firstSeen

The date and time when the anomaly detector first saw this anomaly. It is specified as epoch time, which is the number of seconds since `January 1, 1970, 00:00:00 UTC`.

Type: Long

Valid Range: Minimum value of 0.

Required: Yes

histogram

A map showing times when the anomaly detector ran, and the number of occurrences of this anomaly that were detected at each of those runs. The times are specified in epoch time, which is the number of seconds since `January 1, 1970, 00:00:00 UTC`.

Type: String to long map

Key Length Constraints: Minimum length of 1.

Required: Yes

lastSeen

The date and time when the anomaly detector most recently saw this anomaly. It is specified as epoch time, which is the number of seconds since `January 1, 1970, 00:00:00 UTC`.

Type: Long

Valid Range: Minimum value of 0.

Required: Yes

logGroupArnList

An array of ARNS of the log groups that contained log events considered to be part of this anomaly.

Type: Array of strings

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

Pattern: `[\w#+=/:,.@-]*`

Required: Yes

logSamples

An array of sample log event messages that are considered to be part of this anomaly.

Type: Array of LogEvent objects

Required: Yes

patternId

The ID of the pattern used to help identify this anomaly.

Type: String

Length Constraints: Fixed length of 32.

Required: Yes

patternString

The pattern used to help identify this anomaly, in string format.

Type: String

Length Constraints: Minimum length of 1.

Required: Yes

patternTokens

An array of structures where each structure contains information about one token that makes up the pattern.

Type: Array of PatternToken objects

Required: Yes

state

Indicates the current state of this anomaly. If it is still being treated as an anomaly, the value is `Active`. If you have suppressed this anomaly by using the UpdateAnomaly operation, the value is `Suppressed`. If this behavior is now considered to be normal, the value is `Baseline`.

Type: String

Valid Values: `Active | Suppressed | Baseline`

Required: Yes

isPatternLevelSuppression

If this anomaly is suppressed, this field is `true` if the suppression is because the pattern is suppressed. If `false`, then only this particular anomaly is suppressed.

Type: Boolean

Required: No

patternRegex

The pattern used to help identify this anomaly, in regular expression format.

Type: String

Length Constraints: Minimum length of 1.

Required: No

priority

The priority level of this anomaly, as determined by CloudWatch Logs. Priority is computed based on log severity labels such as `FATAL` and `ERROR` and the amount of deviation from the baseline. Possible values are `HIGH`, `MEDIUM`, and `LOW`.

Type: String

Length Constraints: Minimum length of 1.

Required: No

suppressed

Indicates whether this anomaly is currently suppressed. To suppress an anomaly, use UpdateAnomaly.

Type: Boolean

Required: No

suppressedDate

If the anomaly is suppressed, this indicates when it was suppressed.

Type: Long

Valid Range: Minimum value of 0.

Required: No

suppressedUntil

If the anomaly is suppressed, this indicates when the suppression will end. If this value is `0`, the anomaly was suppressed with no expiration, with the `INFINITE` value.

Type: Long

Valid Range: Minimum value of 0.

Required: No

See Also

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

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

AnomalyDetector

Contains information about one anomaly detector in the account.

Contents

anomalyDetectorArn

The ARN of the anomaly detector.

Type: String

Length Constraints: Minimum length of 1.

Pattern: `[\w#+=/:,.@-]*`

Required: No

anomalyDetectorStatus

Specifies the current status of the anomaly detector. To pause an anomaly detector, use the `enabled` parameter in the UpdateLogAnomalyDetector operation.

Type: String

Valid Values: `INITIALIZING | TRAINING | ANALYZING | FAILED | DELETED | PAUSED`

Required: No

anomalyVisibilityTime

The number of days used as the life cycle of anomalies. After this time, anomalies are automatically baselined and the anomaly detector model will treat new occurrences of similar event as normal.

Type: Long

Valid Range: Minimum value of 7. Maximum value of 90.

Required: No

creationTimeStamp

The date and time when this anomaly detector was created.

Type: Long

Valid Range: Minimum value of 0.

Required: No

detectorName

The name of the anomaly detector.

Type: String

Length Constraints: Minimum length of 1.

Required: No

evaluationFrequency

Specifies how often the anomaly detector runs and look for anomalies.

Type: String

Valid Values: `ONE_MIN | FIVE_MIN | TEN_MIN | FIFTEEN_MIN | THIRTY_MIN | ONE_HOUR`

Required: No

filterPattern

A symbolic description of how CloudWatch Logs should interpret the data in each log event. For example, a log event can contain timestamps, IP addresses, strings, and so on. You use the filter pattern to specify what to look for in the log event message.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 1024.

Required: No

kmsKeyId

The ARN of the AWS KMS key assigned to this anomaly detector, if any.

Type: String

Length Constraints: Maximum length of 256.

Required: No

lastModifiedTimeStamp

The date and time when this anomaly detector was most recently modified.

Type: Long

Valid Range: Minimum value of 0.

Required: No

logGroupArnList

A list of the ARNs of the log groups that this anomaly detector watches.

Type: Array of strings

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

Pattern: `[\w#+=/:,.@-]*`

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

ConfigurationTemplate

A structure containing information about the deafult settings and available settings that you can use to configure a delivery or a delivery destination.

Contents

allowedActionForAllowVendedLogsDeliveryForResource

The action permissions that a caller needs to have to be able to successfully create a delivery source on the desired resource type when calling PutDeliverySource.

Type: String

Required: No

allowedFieldDelimiters

The valid values that a caller can use as field delimiters when calling CreateDelivery or UpdateDeliveryConfiguration on a delivery that delivers in `Plain`, `W3C`, or `Raw` format.

Type: Array of strings

Length Constraints: Minimum length of 0. Maximum length of 5.

Required: No

allowedFields

The allowed fields that a caller can use in the `recordFields` parameter of a CreateDelivery or UpdateDeliveryConfiguration operation.

Type: Array of RecordField objects

Required: No

allowedOutputFormats

The list of delivery destination output formats that are supported by this log source.

Type: Array of strings

Valid Values: `json | plain | w3c | raw | parquet`

Required: No

allowedSuffixPathFields

The list of variable fields that can be used in the suffix path of a delivery that delivers to an S3 bucket.

Type: Array of strings

Array Members: Minimum number of 0 items. Maximum number of 128 items.

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

Required: No

defaultDeliveryConfigValues

A mapping that displays the default value of each property within a delivery's configuration, if it is not specified in the request.

Type: ConfigurationTemplateDeliveryConfigValues object

Required: No

deliveryDestinationType

A string specifying which destination type this configuration template applies to.

Type: String

Valid Values: `S3 | CWL | FH | XRAY`

Required: No

deliverySourceConfiguration

The schema of the delivery source configuration that is available for this log type. Each element describes a configuration that can be set when calling PutDeliverySource, including the configuration name, type, and default value.

Type: Array of DeliverySourceConfigurationSchema objects

Required: No

logType

A string specifying which log type this configuration template applies to.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 255.

Pattern: `[\w]*`

Required: No

resourceType

A string specifying which resource type this configuration template applies to.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 255.

Pattern: `[\w-_]*`

Required: No

s3TablesIntegration

The S3 Tables integration configuration for this configuration template, including the datasource name and type.

Type: S3TablesIntegration object

Required: No

service

A string specifying which service this configuration template applies to. For more information about supported services see Enable logging from AWS services..

Type: String

Length Constraints: Minimum length of 1. Maximum length of 255.

Pattern: `[\w_-]*`

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

ConfigurationTemplateDeliveryConfigValues

This structure contains the default values that are used for each configuration parameter when you use CreateDelivery to create a deliver under the current service type, resource type, and log type.

Contents

fieldDelimiter

The default field delimiter that is used in a CreateDelivery operation when the field delimiter is not specified in that operation. The field delimiter is used only when the final output delivery is in `Plain`, `W3C`, or `Raw` format.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 5.

Required: No

recordFields

The default record fields that will be delivered when a list of record fields is not provided in a CreateDelivery operation.

Type: Array of strings

Array Members: Minimum number of 0 items. Maximum number of 128 items.

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

Required: No

s3DeliveryConfiguration

The delivery parameters that are used when you create a delivery to a delivery destination that is an S3 Bucket.

Type: S3DeliveryConfiguration 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

CopyValue

This processor copies values within a log event. You can also use this processor to add metadata to log events by copying the values of the following metadata keys into the log events: `@logGroupName`, `@logGroupStream`, `@accountId`, `@regionName`.

For more information about this processor including examples, see copyValue in the *CloudWatch Logs User Guide*.

Contents

entries

An array of `CopyValueEntry` objects, where each object contains the information about one field value to copy.

Type: Array of CopyValueEntry objects

Array Members: Minimum number of 1 item. Maximum number of 5 items.

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

CopyValueEntry

This object defines one value to be copied with the copyValue processor.

Contents

source

The key to copy.

Type: String

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

Required: Yes

target

The key of the field to copy the value to.

Type: String

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

Required: Yes

overwriteIfExists

Specifies whether to overwrite the value if the destination key already exists. If you omit this, the default is `false`.

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

CSV

The CSV processor parses comma-separated values (CSV) from the log events into columns.

For more information about this processor including examples, see csv in the *CloudWatch Logs User Guide*.

Contents

columns

An array of names to use for the columns in the transformed log event.

If you omit this, default column names (`[column_1, column_2 ...]`) are used.

Type: Array of strings

Array Members: Maximum number of 100 items.

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

Required: No

delimiter

The character used to separate each column in the original comma-separated value log event. If you omit this, the processor looks for the comma `,` character as the delimiter.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 2.

Required: No

destination

The path to the parent field to put transformed key value pairs under. If you omit this value, the key value pairs will be placed under the root node.

Type: String

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

Required: No

quoteCharacter

The character used used as a text qualifier for a single column of data. If you omit this, the double quotation mark " character is used.

Type: String

Length Constraints: Fixed length of 1.

Required: No

source

The path to the field in the log event that has the comma separated values to be parsed. If you omit this value, the whole log message is processed.

Type: String

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

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

DataSource

Represents a data source that categorizes logs by originating service and log type, providing service-based organization complementing traditional log groups.

Contents

name

The name of the data source.

Type: String

Required: Yes

type

The type of the data source.

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

DataSourceFilter

Filter criteria for data sources, used to specify which data sources to include in operations based on name and type.

Contents

name

The name pattern to filter data sources by.

Type: String

Required: Yes

type

The type pattern to filter data sources by.

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

DateTimeConverter

This processor converts a datetime string into a format that you specify.

For more information about this processor including examples, see datetimeConverter in the *CloudWatch Logs User Guide*.

Contents

matchPatterns

A list of patterns to match against the `source` field.

Type: Array of strings

Array Members: Minimum number of 1 item. Maximum number of 5 items.

Length Constraints: Minimum length of 1.

Required: Yes

source

The key to apply the date conversion to.

Type: String

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

Required: Yes

target

The JSON field to store the result in.

Type: String

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

Required: Yes

locale

The locale of the source field. If you omit this, the default of `locale.ROOT` is used.

Type: String

Length Constraints: Minimum length of 1.

Required: No

sourceTimezone

The time zone of the source field. If you omit this, the default used is the UTC zone.

Type: String

Length Constraints: Minimum length of 1.

Required: No

targetFormat

The datetime format to use for the converted data in the target field.

If you omit this, the default of `yyyy-MM-dd'T'HH:mm:ss.SSS'Z` is used.

Type: String

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

Required: No

targetTimezone

The time zone of the target field. If you omit this, the default used is the UTC zone.

Type: String

Length Constraints: Minimum length of 1.

Required: No

See Also

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

- AWS SDK for C++

- AWS SDK for Java V2
- AWS SDK for Ruby V3

DeleteKeys

This processor deletes entries from a log event. These entries are key-value pairs.

For more information about this processor including examples, see deleteKeys in the *CloudWatch Logs User Guide*.

Contents

withKeys

The list of keys to delete.

Type: Array of strings

Array Members: Minimum number of 1 item. Maximum number of 5 items.

Length Constraints: Minimum length of 1.

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

Delivery

This structure contains information about one *delivery* in your account.

A delivery is a connection between a logical *delivery source* and a logical *delivery destination*.

For more information, see CreateDelivery.

To update an existing delivery configuration, use UpdateDeliveryConfiguration.

Contents

arn

The Amazon Resource Name (ARN) that uniquely identifies this delivery.

Type: String

Required: No

deliveryDestinationArn

The ARN of the delivery destination that is associated with this delivery.

Type: String

Required: No

deliveryDestinationType

Displays whether the delivery destination associated with this delivery is CloudWatch Logs, Amazon S3, Firehose, or X-Ray.

Type: String

Valid Values: `S3 | CWL | FH | XRAY`

Required: No

deliverySourceName

The name of the delivery source that is associated with this delivery.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 60.

Pattern: `[\w-]*`

Required: No

fieldDelimiter

The field delimiter that is used between record fields when the final output format of a delivery is in `Plain`, `W3C`, or `Raw` format.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 5.

Required: No

id

The unique ID that identifies this delivery in your account.

Type: String

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

Pattern: `^[0-9A-Za-z]+$`

Required: No

recordFields

The record fields used in this delivery.

Type: Array of strings

Array Members: Minimum number of 0 items. Maximum number of 128 items.

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

Required: No

s3DeliveryConfiguration

This structure contains delivery configurations that apply only when the delivery destination resource is an S3 bucket.

Type: S3DeliveryConfiguration object

Required: No

tags

The tags that have been assigned to this delivery.

Type: String to string map

Map Entries: Maximum number of 50 items.

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

Key Pattern: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]+)$`

Value Length Constraints: Maximum length of 256.

Value Pattern: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$`

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

DeliveryDestination

This structure contains information about one *delivery destination* in your account. A delivery destination is an AWS resource that represents an AWS service that logs can be sent to. CloudWatch Logs, Amazon S3, Firehose, and X-Ray are supported as delivery destinations.

To configure logs delivery between a supported AWS service and a destination, you must do the following:

- Create a delivery source, which is a logical object that represents the resource that is actually sending the logs. For more information, see PutDeliverySource.
- Create a *delivery destination*, which is a logical object that represents the actual delivery destination.
- If you are delivering logs cross-account, you must use PutDeliveryDestinationPolicy in the destination account to assign an IAM policy to the destination. This policy allows delivery to that destination.
- Create a *delivery* by pairing exactly one delivery source and one delivery destination. For more information, see CreateDelivery.

You can configure a single delivery source to send logs to multiple destinations by creating multiple deliveries. You can also create multiple deliveries to configure multiple delivery sources to send logs to the same delivery destination.

Contents

arn

The Amazon Resource Name (ARN) that uniquely identifies this delivery destination.

Type: String

Required: No

deliveryDestinationConfiguration

A structure that contains the ARN of the AWS resource that will receive the logs.

Type: DeliveryDestinationConfiguration object

Required: No

deliveryDestinationType

Displays whether this delivery destination is CloudWatch Logs, Amazon S3, Firehose, or X-Ray.

Type: String

Valid Values: `S3 | CWL | FH | XRAY`

Required: No

name

The name of this delivery destination.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 60.

Pattern: `[\w-]*`

Required: No

outputFormat

The format of the logs that are sent to this delivery destination.

Type: String

Valid Values: `json | plain | w3c | raw | parquet`

Required: No

tags

The tags that have been assigned to this delivery destination.

Type: String to string map

Map Entries: Maximum number of 50 items.

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

Key Pattern: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]+)$`

Value Length Constraints: Maximum length of 256.

Value Pattern: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$`

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

DeliveryDestinationConfiguration

A structure that contains information about one logs delivery destination.

Contents

destinationResourceArn

The ARN of the AWS destination that this delivery destination represents. That AWS destination can be a log group in CloudWatch Logs, an Amazon S3 bucket, or a delivery stream in Firehose.

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

DeliverySource

This structure contains information about one *delivery source* in your account. A delivery source is an AWS resource that sends logs to an AWS destination. The destination can be CloudWatch Logs, Amazon S3, or Firehose.

Only some AWS services support being configured as a delivery source. These services are listed as **Supported [V2 Permissions]** in the table at Enabling logging from AWS services.

To configure logs delivery between a supported AWS service and a destination, you must do the following:

- Create a delivery source, which is a logical object that represents the resource that is actually sending the logs. For more information, see PutDeliverySource.
- Create a *delivery destination*, which is a logical object that represents the actual delivery destination. For more information, see PutDeliveryDestination.
- If you are delivering logs cross-account, you must use PutDeliveryDestinationPolicy in the destination account to assign an IAM policy to the destination. This policy allows delivery to that destination.
- Create a *delivery* by pairing exactly one delivery source and one delivery destination. For more information, see CreateDelivery.

You can configure a single delivery source to send logs to multiple destinations by creating multiple deliveries. You can also create multiple deliveries to configure multiple delivery sources to send logs to the same delivery destination.

Contents

arn

The Amazon Resource Name (ARN) that uniquely identifies this delivery source.

Type: String

Required: No

deliverySourceConfiguration

The map of key-value pairs that configure the delivery source.

Type: String to string map

Key Length Constraints: Minimum length of 1. Maximum length of 255.

Value Length Constraints: Minimum length of 1. Maximum length of 255.

Required: No

logType

The type of log that the source is sending. For valid values for this parameter, see the documentation for the source service.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 255.

Pattern: `[\w]*`

Required: No

name

The unique name of the delivery source.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 60.

Pattern: `[\w-]*`

Required: No

resourceArns

This array contains the ARN of the AWS resource that sends logs and is represented by this delivery source. Currently, only one ARN can be in the array.

Type: Array of strings

Required: No

service

The AWS service that is sending logs.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 255.

Pattern: `[\w_-]*`

Required: No

status

The status of the delivery source. A delivery source can have the status `ACTIVE` or `INACTIVE`. Note: This value is defined for selective log types.

Type: String

Valid Values: `ACTIVE | INACTIVE`

Required: No

statusReason

The reason for the status of the delivery source. A status reason of `RESOURCE_DELETED` indicates that the resource associated with the delivery source has been deleted. Note: This value is defined for selective log types.

Type: String

Valid Values: `RESOURCE_DELETED`

Required: No

tags

The tags that have been assigned to this delivery source.

Type: String to string map

Map Entries: Maximum number of 50 items.

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

Key Pattern: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]+)$`

Value Length Constraints: Maximum length of 256.

Value Pattern: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$`

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

DeliverySourceConfigurationSchema

A structure that describes a single configuration for a log type, including its name, value type, default value, and the range of supported values.

Contents

defaultValue

The default value of the configuration that is used when a value is not specified in a PutDeliverySource request.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Required: Yes

keyName

The name of the configuration.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Required: Yes

valueType

The data type of the configuration value. Valid values are `string`, `boolean`, `int`, `double`, and `long`.

Type: String

Valid Values: `string | boolean | int | double | long`

Required: Yes

maxValue

The maximum numeric value allowed for the configuration. This applies only when the `valueType` is a numeric type.

Type: Double

Required: No

minValue

The minimum numeric value allowed for the configuration. This applies only when the `valueType` is a numeric type.

Type: Double

Required: No

supportedValues

The list of allowed values for the configuration. Empty for free-form configuration.

Type: Array of strings

Length Constraints: Minimum length of 1. 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

Destination

Represents a cross-account destination that receives subscription log events.

Contents

accessPolicy

An IAM policy document that governs which AWS accounts can create subscription filters against this destination.

Type: String

Length Constraints: Minimum length of 1.

Required: No

arn

The ARN of this destination.

Type: String

Required: No

creationTime

The creation time of the destination, expressed as the number of milliseconds after Jan 1, 1970 00:00:00 UTC.

Type: Long

Valid Range: Minimum value of 0.

Required: No

destinationName

The name of the destination.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `[^:*]*`

Required: No

roleArn

A role for impersonation, used when delivering log events to the target.

Type: String

Length Constraints: Minimum length of 1.

Required: No

targetArn

The Amazon Resource Name (ARN) of the physical target where the log events are delivered (for example, a Kinesis stream).

Type: String

Length Constraints: Minimum length of 1.

Required: No

See Also

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

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

DestinationConfiguration

Configuration for where to deliver scheduled query results. Specifies the destination type and associated settings for result delivery.

Contents

lookupTableConfiguration

Configuration for delivering query results to a lookup table. The query results automatically populate or refresh the specified lookup table on each scheduled execution.

Type: LookupTableConfiguration object

Required: No

s3Configuration

Configuration for delivering query results to Amazon S3.

Type: S3Configuration 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

Entity

The entity associated with the log events in a `PutLogEvents` call.

Contents

attributes

Additional attributes of the entity that are not used to specify the identity of the entity. A list of key-value pairs.

For details about how to use the attributes, see How to add related information to telemetry in the *CloudWatch User Guide*.

Type: String to string map

Map Entries: Minimum number of 0 items. Maximum number of 10 items.

Key Length Constraints: Minimum length of 1. Maximum length of 256.

Value Length Constraints: Minimum length of 1. Maximum length of 512.

Required: No

keyAttributes

The attributes of the entity which identify the specific entity, as a list of key-value pairs. Entities with the same `keyAttributes` are considered to be the same entity.

There are five allowed attributes (key names): `Type`, `ResourceType`, `Identifier` `Name`, and `Environment`.

For details about how to use the key attributes, see How to add related information to telemetry in the *CloudWatch User Guide*.

Type: String to string map

Map Entries: Minimum number of 2 items. Maximum number of 4 items.

Key Length Constraints: Minimum length of 1. Maximum length of 32.

Value Length Constraints: Minimum length of 1. Maximum length of 512.

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

ExportTask

Represents an export task.

Contents

destination

The name of the S3 bucket to which the log data was exported.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Required: No

destinationPrefix

The prefix that was used as the start of Amazon S3 key for every object exported.

Type: String

Required: No

executionInfo

Execution information about the export task.

Type: ExportTaskExecutionInfo object

Required: No

from

The start time, expressed as the number of milliseconds after `Jan 1, 1970 00:00:00 UTC`. Events with a timestamp before this time are not exported.

Type: Long

Valid Range: Minimum value of 0.

Required: No

logGroupName

The name of the log group from which logs data was exported.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `[\.\-_/#A-Za-z0-9]+`

Required: No

status

The status of the export task.

Type: ExportTaskStatus object

Required: No

taskId

The ID of the export task.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Required: No

taskName

The name of the export task.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Required: No

to

The end time, expressed as the number of milliseconds after `Jan 1, 1970 00:00:00` UTC. Events with a timestamp later than this time are not exported.

Type: Long

Valid Range: Minimum value of 0.

Required: No

See Also

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

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

ExportTaskExecutionInfo

Represents the status of an export task.

Contents

completionTime

The completion time of the export task, expressed as the number of milliseconds after `Jan 1, 1970 00:00:00` UTC.

Type: Long

Valid Range: Minimum value of 0.

Required: No

creationTime

The creation time of the export task, expressed as the number of milliseconds after `Jan 1, 1970 00:00:00` UTC.

Type: Long

Valid Range: Minimum value of 0.

Required: No

See Also

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

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

ExportTaskStatus

Represents the status of an export task.

Contents

code

The status code of the export task.

Type: String

Valid Values: `CANCELLED | COMPLETED | FAILED | PENDING | PENDING_CANCEL | RUNNING`

Required: No

message

The status message related to the status code.

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

FieldIndex

This structure describes one log event field that is used as an index in at least one index policy in this account.

Contents

fieldIndexName

The string that this field index matches.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `[\.\-_/#A-Za-z0-9]+`

Required: No

firstEventTime

The time and date of the earliest log event that matches this field index, after the index policy that contains it was created.

Type: Long

Valid Range: Minimum value of 0.

Required: No

indexCategory

The category of the field index:

- `DEFAULT`: Fields that CloudWatch Logs indexes by default. Examples include `@logStream` and `@data_format`.
- `CUSTOM`: Fields that you added manually to the field index policy. CloudWatch Logs always indexes these fields. These fields count toward the quota of 20 fields for each log group.
- `AUTO`: Fields that CloudWatch Logs indexes automatically based on your query patterns and usage. These fields do not count toward the field index quota. CloudWatch Logs might update these fields based on changes in your query patterns. To keep a field indexed permanently, add it to an account-level or log-group level field index policy.

- `INACTIVE`: Fields that CloudWatch Logs indexed before but does not index now. This happens if you remove a field from the field index policy or if CloudWatch Logs automatically selects a different field based on your queries.

For more information about automatically indexed fields, see Automatically indexed fields.

Type: String

Valid Values: `DEFAULT | CUSTOM | AUTO | INACTIVE`

Required: No

lastEventTime

The time and date of the most recent log event that matches this field index.

Type: Long

Valid Range: Minimum value of 0.

Required: No

lastScanTime

The most recent time that CloudWatch Logs scanned ingested log events to search for this field index to improve the speed of future CloudWatch Logs Insights queries that search for this field index.

Type: Long

Valid Range: Minimum value of 0.

Required: No

logGroupIdentifier

If this field index appears in an index policy that applies only to a single log group, the ARN of that log group is displayed here.

Type: String

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

Pattern: `[\w#+=/:,.@-]*`

Required: No

type

The type of index. Specify `FACET` for facet-based indexing or `FIELD_INDEX` for field-based indexing. This determines how the field is indexed and can be queried.

Type: String

Valid Values: `FACET | FIELD_INDEX`

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

FieldsData

A structure containing the extracted fields from a log event. These fields are extracted based on the log format and can be used for structured querying and analysis.

Contents

data

The actual log data content returned in the streaming response. This contains the fields and values of the log event in a structured format that can be parsed and processed by the client.

Type: Base64-encoded binary data 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

FilteredLogEvent

Represents a matched event.

Contents

eventId

The ID of the event.

Type: String

Required: No

ingestionTime

The time the event was ingested, expressed as the number of milliseconds after `Jan 1, 1970 00:00:00 UTC`.

Type: Long

Valid Range: Minimum value of 0.

Required: No

logStreamName

The name of the log stream to which this event belongs.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `[^:*]*`

Required: No

message

The data contained in the log event.

Type: String

Length Constraints: Minimum length of 1.

Required: No

timestamp

The time the event occurred, expressed as the number of milliseconds after `Jan 1, 1970 00:00:00` UTC.

Type: Long

Valid Range: Minimum value of 0.

Required: No

See Also

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

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

GetLogObjectResponseStream

A stream of structured log data returned by the GetLogObject operation. This stream contains log events with their associated metadata and extracted fields.

Contents

fields

A structure containing the extracted fields from a log event. These fields are extracted based on the log format and can be used for structured querying and analysis.

Type: FieldsData object

Required: No

InternalStreamingException

An internal error occurred during the streaming of log data. This exception is thrown when there's an issue with the internal streaming mechanism used by the GetLogObject operation.

Type: Exception

HTTP Status Code:

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

Grok

This processor uses pattern matching to parse and structure unstructured data. This processor can also extract fields from log messages.

For more information about this processor including examples, see grok in the *CloudWatch Logs User Guide*.

Contents

match

The grok pattern to match against the log event. For a list of supported grok patterns, see Supported grok patterns.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Required: Yes

source

The path to the field in the log event that you want to parse. If you omit this value, the whole log message is parsed.

Type: String

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

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

GroupingIdentifier

A key-value pair that identifies how log groups are grouped in aggregate summaries.

Contents

key

The key that identifies the grouping characteristic. The format of the key uses dot notation. Examples are, `dataSource.Name`, `dataSource.Type`, and `dataSource.Format`.

Type: String

Required: No

value

The value associated with the grouping characteristic. Examples are `amazon_vpc`, `flow`, and `OCSF`.

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

Import

An import job to move data from CloudTrail Event Data Store to CloudWatch.

Contents

creationTime

The timestamp when the import task was created, expressed as the number of milliseconds after Jan 1, 1970 00:00:00 UTC.

Type: Long

Valid Range: Minimum value of 0.

Required: No

errorMessage

Error message related to any failed imports

Type: String

Required: No

importDestinationArn

The ARN of the managed CloudWatch Logs log group where the events are being imported to.

Type: String

Required: No

importFilter

The filter criteria used for this import task.

Type: ImportFilter object

Required: No

importId

The unique identifier of the import task.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

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

Required: No

importSourceArn

The ARN of the CloudTrail Lake Event Data Store being imported from.

Type: String

Required: No

importStatistics

Statistics about the import progress

Type: ImportStatistics object

Required: No

importStatus

The current status of the import task. Valid values are IN_PROGRESS, CANCELLED, COMPLETED and FAILED.

Type: String

Valid Values: `IN_PROGRESS | CANCELLED | COMPLETED | FAILED`

Required: No

lastUpdatedTime

The timestamp when the import task was last updated, expressed as the number of milliseconds after Jan 1, 1970 00:00:00 UTC.

Type: Long

Valid Range: Minimum value of 0.

Required: No

See Also

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

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

ImportBatch

A collection of events being imported to CloudWatch

Contents

batchId

The unique identifier of the import batch.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Required: Yes

status

The current status of the import batch. Valid values are IN_PROGRESS, CANCELLED, COMPLETED and FAILED.

Type: String

Valid Values: `IN_PROGRESS | CANCELLED | COMPLETED | FAILED`

Required: Yes

errorMessage

The error message if the batch failed to import. Only present when status is FAILED.

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

ImportFilter

The filter criteria used for import tasks

Contents

endEventTime

The end of the time range for events to import, expressed as the number of milliseconds after Jan 1, 1970 00:00:00 UTC.

Type: Long

Valid Range: Minimum value of 0.

Required: No

startEventTime

The start of the time range for events to import, expressed as the number of milliseconds after Jan 1, 1970 00:00:00 UTC.

Type: Long

Valid Range: Minimum value of 0.

Required: No

See Also

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

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

ImportStatistics

Statistics about the import progress

Contents

bytesImported

The total number of bytes that have been imported to the managed log group.

Type: Long

Valid Range: Minimum value of 0.

Required: No

See Also

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

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

IndexPolicy

This structure contains information about one field index policy in this account.

Contents

lastUpdateTime

The date and time that this index policy was most recently updated.

Type: Long

Valid Range: Minimum value of 0.

Required: No

logGroupIdentifier

The ARN of the log group that this index policy applies to.

Type: String

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

Pattern: `[\w#+=/:,.@-]*`

Required: No

policyDocument

The policy document for this index policy, in JSON format.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 51200.

Required: No

policyName

The name of this policy. Responses about log group-level field index policies don't have this field, because those policies don't have names.

Type: String

Required: No

source

This field indicates whether this is an account-level index policy or an index policy that applies only to a single log group.

Type: String

Valid Values: `ACCOUNT | LOG_GROUP`

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

InputLogEvent

Represents a log event, which is a record of activity that was recorded by the application or resource being monitored.

Contents

message

The raw event message. Each log event can be no larger than 1 MB.

Type: String

Length Constraints: Minimum length of 1.

Required: Yes

timestamp

The time the event occurred, expressed as the number of milliseconds after `Jan 1, 1970 00:00:00` UTC.

Type: Long

Valid Range: Minimum value of 0.

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

IntegrationDetails

This structure contains information about the integration configuration. For an integration with OpenSearch Service, this includes information about OpenSearch Service resources such as the collection, the workspace, and policies.

This structure is returned by a GetIntegration operation.

Contents

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

openSearchIntegrationDetails

This structure contains complete information about one integration between CloudWatch Logs and OpenSearch Service.

Type: OpenSearchIntegrationDetails 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

IntegrationSummary

This structure contains information about one CloudWatch Logs integration. This structure is returned by a ListIntegrations operation.

Contents

integrationName

The name of this integration.

Type: String

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

Pattern: `[\.\-_/#A-Za-z0-9]+`

Required: No

integrationStatus

The current status of this integration.

Type: String

Valid Values: `PROVISIONING | ACTIVE | FAILED`

Required: No

integrationType

The type of integration. Integrations with OpenSearch Service have the type `OPENSEARCH`.

Type: String

Valid Values: `OPENSEARCH`

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

ListToMap

This processor takes a list of objects that contain key fields, and converts them into a map of target keys.

For more information about this processor including examples, see listToMap in the *CloudWatch Logs User Guide*.

Contents

key

The key of the field to be extracted as keys in the generated map

Type: String

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

Required: Yes

source

The key in the log event that has a list of objects that will be converted to a map.

Type: String

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

Required: Yes

flatten

A Boolean value to indicate whether the list will be flattened into single items. Specify `true` to flatten the list. The default is `false`

Type: Boolean

Required: No

flattenedElement

If you set `flatten` to `true`, use `flattenedElement` to specify which element, `first` or `last`, to keep.

You must specify this parameter if `flatten` is `true`

Type: String

Valid Values: `first | last`

Required: No

target

The key of the field that will hold the generated map

Type: String

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

Required: No

valueKey

If this is specified, the values that you specify in this parameter will be extracted from the `source` objects and put into the values of the generated map. Otherwise, original objects in the source list will be put into the values of the generated map.

Type: String

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

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

LiveTailSessionLogEvent

This object contains the information for one log event returned in a Live Tail stream.

Contents

ingestionTime

The timestamp specifying when this log event was ingested into the log group.

Type: Long

Valid Range: Minimum value of 0.

Required: No

logGroupIdentifier

The name or ARN of the log group that ingested this log event.

Type: String

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

Pattern: `[\w#+=/:,.@-]*`

Required: No

logStreamName

The name of the log stream that ingested this log event.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `[^:*]*`

Required: No

message

The log event message text.

Type: String

Length Constraints: Minimum length of 1.

Required: No

timestamp

The timestamp specifying when this log event was created.

Type: Long

Valid Range: Minimum value of 0.

Required: No

See Also

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

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

LiveTailSessionMetadata

This object contains the metadata for one `LiveTailSessionUpdate` structure. It indicates whether that update includes only a sample of 500 log events out of a larger number of ingested log events, or if it contains all of the matching log events ingested during that second of time.

Contents

sampled

If this is `true`, then more than 500 log events matched the request for this update, and the `sessionResults` includes a sample of 500 of those events.

If this is `false`, then 500 or fewer log events matched the request for this update, so no sampling was necessary. In this case, the `sessionResults` array includes all log events that matched your request during this time.

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

LiveTailSessionStart

This object contains information about this Live Tail session, including the log groups included and the log stream filters, if any.

Contents

logEventFilterPattern

An optional pattern to filter the results to include only log events that match the pattern. For example, a filter pattern of `error 404` displays only log events that include both `error` and `404`.

For more information about filter pattern syntax, see Filter and Pattern Syntax.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 1024.

Required: No

logGroupIdentifiers

An array of the names and ARNs of the log groups included in this Live Tail session.

Type: Array of strings

Array Members: Minimum number of 1 item. Maximum number of 10 items.

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

Pattern: `[\w#+=/:,.@-]*`

Required: No

logStreamNamePrefixes

If your StartLiveTail operation request included a `logStreamNamePrefixes` parameter that filtered the session to only include log streams that have names that start with certain prefixes, these prefixes are listed here.

Type: Array of strings

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

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `[^:*]*`

Required: No

logStreamNames

If your StartLiveTail operation request included a `logStreamNames` parameter that filtered the session to only include certain log streams, these streams are listed here.

Type: Array of strings

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

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `[^:*]*`

Required: No

requestId

The unique ID generated by CloudWatch Logs to identify this Live Tail session request.

Type: String

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

Required: No

sessionId

The unique ID generated by CloudWatch Logs to identify this Live Tail session.

Type: String

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

Required: No

See Also

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

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

LiveTailSessionUpdate

This object contains the log events and metadata for a Live Tail session.

Contents

sessionMetadata

This object contains the session metadata for a Live Tail session.

Type: LiveTailSessionMetadata object

Required: No

sessionResults

An array, where each member of the array includes the information for one log event in the Live Tail session.

A `sessionResults` array can include as many as 500 log events. If the number of log events matching the request exceeds 500 per second, the log events are sampled down to 500 log events to be included in each `sessionUpdate` structure.

Type: Array of LiveTailSessionLogEvent 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

LogEvent

This structure contains the information for one sample log event that is associated with an anomaly found by a log anomaly detector.

Contents

message

The message content of the log event.

Type: String

Length Constraints: Minimum length of 1.

Required: No

timestamp

The time stamp of the log event.

Type: Long

Valid Range: Minimum value of 0.

Required: No

See Also

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

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

LogFieldsListItem

Represents a log field with its name and data type information for a specific data source.

Contents

logFieldName

The name of the log field.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Required: No

logFieldType

The data type information for the log field.

Type: LogFieldType 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

LogFieldType

Defines the data type structure for a log field, including the type, element information, and nested fields for complex types.

Contents

element

For array or collection types, specifies the element type information.

Type: LogFieldType object

Required: No

fields

For complex types, contains the nested field definitions.

Type: Array of LogFieldsListItem objects

Required: No

type

The data type of the log field.

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

LogGroup

Represents a log group.

Contents

arn

The Amazon Resource Name (ARN) of the log group. This version of the ARN includes a trailing `:*` after the log group name.

Use this version to refer to the ARN in IAM policies when specifying permissions for most API actions. The exception is when specifying permissions for TagResource, UntagResource, and ListTagsForResource. The permissions for those three actions require the ARN version that doesn't include a trailing `:*`.

Type: String

Required: No

bearerTokenAuthenticationEnabled

Indicates whether bearer token authentication is enabled for this log group. When enabled, bearer token authentication is allowed on operations until it is explicitly disabled.

Type: Boolean

Required: No

creationTime

The creation time of the log group, expressed as the number of milliseconds after Jan 1, 1970 00:00:00 UTC.

Type: Long

Valid Range: Minimum value of 0.

Required: No

dataProtectionStatus

Displays whether this log group has a protection policy, or whether it had one in the past. For more information, see PutDataProtectionPolicy.

Type: String

Valid Values: `ACTIVATED | DELETED | ARCHIVED | DISABLED`

Required: No

deletionProtectionEnabled

Indicates whether deletion protection is enabled for this log group. When enabled, deletion protection blocks all deletion operations until it is explicitly disabled.

Type: Boolean

Required: No

inheritedProperties

Displays all the properties that this log group has inherited from account-level settings.

Type: Array of strings

Valid Values: `ACCOUNT_DATA_PROTECTION`

Required: No

kmsKeyId

The Amazon Resource Name (ARN) of the AWS KMS key to use when encrypting log data.

Type: String

Length Constraints: Maximum length of 256.

Required: No

logGroupArn

The Amazon Resource Name (ARN) of the log group. This version of the ARN doesn't include a trailing `:*` after the log group name.

Use this version to refer to the ARN in the following situations:

- In the `logGroupIdentifier` input field in many CloudWatch Logs APIs.
- In the `resourceArn` field in tagging APIs
- In IAM policies, when specifying permissions for TagResource, UntagResource, and ListTagsForResource.

Type: String

Required: No

logGroupClass

This specifies the log group class for this log group. There are three classes:

- The `Standard` log class supports all CloudWatch Logs features.
- The `Infrequent Access` log class supports a subset of CloudWatch Logs features and incurs lower costs.
- Use the `Delivery` log class only for delivering AWS Lambda logs to store in Amazon S3 or Amazon Data Firehose. Log events in log groups in the Delivery class are kept in CloudWatch Logs for only one day. This log class doesn't offer rich CloudWatch Logs capabilities such as CloudWatch Logs Insights queries.

For details about the features supported by the Standard and Infrequent Access classes, see Log classes

Type: String

Valid Values: `STANDARD | INFREQUENT_ACCESS | DELIVERY`

Required: No

logGroupName

The name of the log group.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `[\.\-_/#A-Za-z0-9]+`

Required: No

metricFilterCount

The number of metric filters.

Type: Integer

Required: No

retentionInDays

The number of days to retain the log events in the specified log group. Possible values are: 1, 3, 5, 7, 14, 30, 60, 90, 120, 150, 180, 365, 400, 545, 731, 1096, 1827, 2192, 2557, 2922, 3288, and 3653.

To set a log group so that its log events do not expire, use DeleteRetentionPolicy.

Type: Integer

Required: No

storedBytes

The number of bytes stored.

Type: Long

Valid Range: Minimum value of 0.

Required: No

See Also

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

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

LogGroupField

The fields contained in log events found by a `GetLogGroupFields` operation, along with the percentage of queried log events in which each field appears.

Contents

name

The name of a log field.

Type: String

Required: No

percent

The percentage of log events queried that contained the field.

Type: Integer

Valid Range: Minimum value of 0. Maximum value of 100.

Required: No

See Also

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

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

LogGroupSummary

This structure contains information about one log group in your account.

Contents

logGroupArn

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

Type: String

Required: No

logGroupClass

The log group class for this log group. For details about the features supported by each log group class, see Log classes

Type: String

Valid Values: `STANDARD | INFREQUENT_ACCESS | DELIVERY`

Required: No

logGroupName

The name of the log group.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `[\.\-_/#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

LogStream

Represents a log stream, which is a sequence of log events from a single emitter of logs.

Contents

arn

The Amazon Resource Name (ARN) of the log stream.

Type: String

Required: No

creationTime

The creation time of the stream, expressed as the number of milliseconds after `Jan 1, 1970 00:00:00` UTC.

Type: Long

Valid Range: Minimum value of 0.

Required: No

firstEventTimestamp

The time of the first event, expressed as the number of milliseconds after `Jan 1, 1970 00:00:00` UTC.

Type: Long

Valid Range: Minimum value of 0.

Required: No

lastEventTimestamp

The time of the most recent log event in the log stream in CloudWatch Logs. This number is expressed as the number of milliseconds after `Jan 1, 1970 00:00:00` UTC. The `lastEventTime` value updates on an eventual consistency basis. It typically updates in less than an hour from ingestion, but in rare situations might take longer.

Type: Long

Valid Range: Minimum value of 0.

Required: No

lastIngestionTime

The ingestion time, expressed as the number of milliseconds after `Jan 1, 1970 00:00:00 UTC` The `lastIngestionTime` value updates on an eventual consistency basis. It typically updates in less than an hour after ingestion, but in rare situations might take longer.

Type: Long

Valid Range: Minimum value of 0.

Required: No

logStreamName

The name of the log stream.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `[^:*]*`

Required: No

storedBytes

This member has been deprecated.

The number of bytes stored.

Important: As of June 17, 2019, this parameter is no longer supported for log streams, and is always reported as zero. This change applies only to log streams. The `storedBytes` parameter for log groups is not affected.

Type: Long

Valid Range: Minimum value of 0.

Required: No

uploadSequenceToken

The sequence token.

> **Important**
>
> The sequence token is now ignored in `PutLogEvents` actions. `PutLogEvents` actions are always accepted regardless of receiving an invalid sequence token. You don't need to obtain `uploadSequenceToken` to use a `PutLogEvents` action.

Type: String

Length Constraints: Minimum length of 1.

Required: No

See Also

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

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

LookupTable

Contains metadata about a lookup table returned by `DescribeLookupTables`.

Contents

description

The description of the lookup table.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 1024.

Required: No

kmsKeyId

The ARN of the AWS KMS key used to encrypt the lookup table data, if applicable.

Type: String

Length Constraints: Maximum length of 256.

Required: No

lastUpdatedTime

The time when the lookup table was last updated, expressed as the number of milliseconds after `Jan 1, 1970 00:00:00 UTC`.

Type: Long

Valid Range: Minimum value of 0.

Required: No

lookupTableArn

The ARN of the lookup table.

Type: String

Required: No

lookupTableName

The name of the lookup table.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `^[a-zA-Z0-9_]+$`

Required: No

recordsCount

The number of data rows in the lookup table, excluding the header row.

Type: Long

Valid Range: Minimum value of 0.

Required: No

sizeBytes

The size of the lookup table in bytes.

Type: Long

Valid Range: Minimum value of 0.

Required: No

tableFields

The column headers from the first row of the CSV file.

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

LookupTableConfiguration

Configuration for a lookup table destination. Use it to automatically refresh a lookup table with query results on a schedule.

Contents

roleArn

The ARN of the IAM role that grants permissions to create or update the lookup table with query results.

Type: String

Length Constraints: Minimum length of 1.

Required: Yes

tableName

The name of the lookup table to create or update with query results. The name can contain only alphanumeric characters and underscores.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `^[a-zA-Z0-9_]+$`

Required: Yes

description

A description of the lookup table.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 1024.

Required: No

kmsKeyId

The ARN of the AWS KMS key to use to encrypt the lookup table data. If you don't specify a key, the data is encrypted with an AWS-owned key.

Type: String

Length Constraints: Maximum length of 256.

Required: No

tags

Key-value pairs to associate with the lookup table for resource management and cost allocation. The service applies tags only during initial table creation.

Type: String to string map

Map Entries: Maximum number of 50 items.

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

Key Pattern: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]+)$`

Value Length Constraints: Maximum length of 256.

Value Pattern: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$`

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

LowerCaseString

This processor converts a string to lowercase.

For more information about this processor including examples, see lowerCaseString in the *CloudWatch Logs User Guide*.

Contents

withKeys

The array caontaining the keys of the fields to convert to lowercase.

Type: Array of strings

Array Members: Minimum number of 1 item. Maximum number of 10 items.

Length Constraints: Minimum length of 1.

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

MetricFilter

Metric filters express how CloudWatch Logs would extract metric observations from ingested log events and transform them into metric data in a CloudWatch metric.

Contents

applyOnTransformedLogs

This parameter is valid only for log groups that have an active log transformer. For more information about log transformers, see PutTransformer.

If this value is `true`, the metric filter is applied on the transformed version of the log events instead of the original ingested log events.

Type: Boolean

Required: No

creationTime

The creation time of the metric filter, expressed as the number of milliseconds after `Jan 1, 1970 00:00:00 UTC`.

Type: Long

Valid Range: Minimum value of 0.

Required: No

emitSystemFieldDimensions

The list of system fields that are emitted as additional dimensions in the generated metrics. Returns the `emitSystemFieldDimensions` value if it was specified when the metric filter was created.

Type: Array of strings

Required: No

fieldSelectionCriteria

The filter expression that specifies which log events are processed by this metric filter based on system fields. Returns the `fieldSelectionCriteria` value if it was specified when the metric filter was created.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 2000.

Required: No

filterName

The name of the metric filter.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `[^:*]*`

Required: No

filterPattern

A symbolic description of how CloudWatch Logs should interpret the data in each log event. For example, a log event can contain timestamps, IP addresses, strings, and so on. You use the filter pattern to specify what to look for in the log event message.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 1024.

Required: No

logGroupName

The name of the log group.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `[\.\-_/#A-Za-z0-9]+`

Required: No

metricTransformations

The metric transformations.

Type: Array of MetricTransformation objects

Array Members: Fixed 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

MetricFilterMatchRecord

Represents a matched event.

Contents

eventMessage

The raw event data.

Type: String

Length Constraints: Minimum length of 1.

Required: No

eventNumber

The event number.

Type: Long

Required: No

extractedValues

The values extracted from the event data by the filter.

Type: String to string 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

MetricTransformation

Indicates how to transform ingested log events to metric data in a CloudWatch metric.

Contents

metricName

The name of the CloudWatch metric.

Type: String

Length Constraints: Maximum length of 255.

Pattern: `[^:*$]*`

Required: Yes

metricNamespace

A custom namespace to contain your metric in CloudWatch. Use namespaces to group together metrics that are similar. For more information, see Namespaces.

Type: String

Length Constraints: Maximum length of 255.

Pattern: `[^:*$]*`

Required: Yes

metricValue

The value to publish to the CloudWatch metric when a filter pattern matches a log event.

Type: String

Length Constraints: Maximum length of 100.

Required: Yes

defaultValue

(Optional) The value to emit when a filter pattern does not match a log event. This value can be null.

Type: Double

Required: No

dimensions

The fields to use as dimensions for the metric. One metric filter can include as many as three dimensions.

> **Important**
>
> Metrics extracted from log events are charged as custom metrics. To prevent unexpected high charges, do not specify high-cardinality fields such as `IPAddress` or `requestID` as dimensions. Each different value found for a dimension is treated as a separate metric and accrues charges as a separate custom metric.
> CloudWatch Logs disables a metric filter if it generates 1000 different name/value pairs for your specified dimensions within a certain amount of time. This helps to prevent accidental high charges.
> You can also set up a billing alarm to alert you if your charges are higher than expected. For more information, see Creating a Billing Alarm to Monitor Your Estimated AWS Charges.

Type: String to string map

Key Length Constraints: Maximum length of 255.

Value Length Constraints: Maximum length of 255.

Required: No

unit

The unit to assign to the metric. If you omit this, the unit is set as None.

Type: String

Valid Values: `Seconds | Microseconds | Milliseconds | Bytes | Kilobytes | Megabytes | Gigabytes | Terabytes | Bits | Kilobits | Megabits | Gigabits | Terabits | Percent | Count | Bytes/Second | Kilobytes/Second | Megabytes/Second | Gigabytes/Second | Terabytes/Second | Bits/Second |`

`Kilobits/Second | Megabits/Second | Gigabits/Second | Terabits/Second | Count/Second | None`

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

MoveKeyEntry

This object defines one key that will be moved with the moveKey processor.

Contents

source

The key to move.

Type: String

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

Required: Yes

target

The key to move to.

Type: String

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

Required: Yes

overwriteIfExists

Specifies whether to overwrite the value if the destination key already exists. If you omit this, the default is `false`.

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

MoveKeys

This processor moves a key from one field to another. The original key is deleted.

For more information about this processor including examples, see moveKeys in the *CloudWatch Logs User Guide*.

Contents

entries

An array of objects, where each object contains the information about one key to move.

Type: Array of MoveKeyEntry objects

Array Members: Minimum number of 1 item. Maximum number of 5 items.

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

OpenSearchApplication

This structure contains information about the OpenSearch Service application used for this integration. An OpenSearch Service application is the web application created by the integration with CloudWatch Logs. It hosts the vended logs dashboards.

Contents

applicationArn

The Amazon Resource Name (ARN) of the application.

Type: String

Required: No

applicationEndpoint

The endpoint of the application.

Type: String

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

Pattern: `^https://[\.\-_/#:A-Za-z0-9]+\.com$`

Required: No

applicationId

The ID of the application.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `[\.\-_/#A-Za-z0-9]+`

Required: No

status

This structure contains information about the status of this OpenSearch Service resource.

Type: OpenSearchResourceStatus 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

OpenSearchCollection

This structure contains information about the OpenSearch Service collection used for this integration. An OpenSearch Service collection is a logical grouping of one or more indexes that represent an analytics workload. For more information, see Creating and managing OpenSearch Service Serverless collections.

Contents

collectionArn

The ARN of the collection.

Type: String

Required: No

collectionEndpoint

The endpoint of the collection.

Type: String

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

Pattern: `^https://[\.\-_/#:A-Za-z0-9]+\.com$`

Required: No

status

This structure contains information about the status of this OpenSearch Service resource.

Type: OpenSearchResourceStatus 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

OpenSearchDataAccessPolicy

This structure contains information about the OpenSearch Service data access policy used for this integration. The access policy defines the access controls for the collection. This data access policy was automatically created as part of the integration setup. For more information about OpenSearch Service data access policies, see Data access control for Amazon OpenSearch Serverless in the OpenSearch Service Developer Guide.

Contents

policyName

The name of the data access policy.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `[\.\-_/#A-Za-z0-9]+`

Required: No

status

This structure contains information about the status of this OpenSearch Service resource.

Type: OpenSearchResourceStatus 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

OpenSearchDataSource

This structure contains information about the OpenSearch Service data source used for this integration. This data source was created as part of the integration setup. An OpenSearch Service data source defines the source and destination for OpenSearch Service queries. It includes the role required to execute queries and write to collections.

For more information about OpenSearch Service data sources , see Creating OpenSearch Service data source integrations with Amazon S3.

Contents

dataSourceName

The name of the OpenSearch Service data source.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `[\.\-_/#A-Za-z0-9]+`

Required: No

status

This structure contains information about the status of this OpenSearch Service resource.

Type: OpenSearchResourceStatus 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

OpenSearchEncryptionPolicy

This structure contains information about the OpenSearch Service encryption policy used for this integration. The encryption policy was created automatically when you created the integration. For more information, see Encryption policies in the OpenSearch Service Developer Guide.

Contents

policyName

The name of the encryption policy.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `[\.\-_/#A-Za-z0-9]+`

Required: No

status

This structure contains information about the status of this OpenSearch Service resource.

Type: OpenSearchResourceStatus 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

OpenSearchIntegrationDetails

This structure contains complete information about one CloudWatch Logs integration. This structure is returned by a GetIntegration operation.

Contents

accessPolicy

This structure contains information about the OpenSearch Service data access policy used for this integration. The access policy defines the access controls for the collection. This data access policy was automatically created as part of the integration setup. For more information about OpenSearch Service data access policies, see Data access control for Amazon OpenSearch Serverless in the OpenSearch Service Developer Guide.

Type: OpenSearchDataAccessPolicy object

Required: No

application

This structure contains information about the OpenSearch Service application used for this integration. An OpenSearch Service application is the web application that was created by the integration with CloudWatch Logs. It hosts the vended logs dashboards.

Type: OpenSearchApplication object

Required: No

collection

This structure contains information about the OpenSearch Service collection used for this integration. This collection was created as part of the integration setup. An OpenSearch Service collection is a logical grouping of one or more indexes that represent an analytics workload. For more information, see Creating and managing OpenSearch Service Serverless collections.

Type: OpenSearchCollection object

Required: No

dataSource

This structure contains information about the OpenSearch Service data source used for this integration. This data source was created as part of the integration setup. An OpenSearch

Service data source defines the source and destination for OpenSearch Service queries. It includes the role required to execute queries and write to collections.

For more information about OpenSearch Service data sources , see Creating OpenSearch Service data source integrations with Amazon S3.

Type: OpenSearchDataSource object

Required: No

encryptionPolicy

This structure contains information about the OpenSearch Service encryption policy used for this integration. The encryption policy was created automatically when you created the integration. For more information, see Encryption policies in the OpenSearch Service Developer Guide.

Type: OpenSearchEncryptionPolicy object

Required: No

lifecyclePolicy

This structure contains information about the OpenSearch Service data lifecycle policy used for this integration. The lifecycle policy determines the lifespan of the data in the collection. It was automatically created as part of the integration setup.

For more information, see Using data lifecycle policies with OpenSearch Service Serverless in the OpenSearch Service Developer Guide.

Type: OpenSearchLifecyclePolicy object

Required: No

networkPolicy

This structure contains information about the OpenSearch Service network policy used for this integration. The network policy assigns network access settings to collections. For more information, see Network policies in the OpenSearch Service Developer Guide.

Type: OpenSearchNetworkPolicy object

Required: No

workspace

This structure contains information about the OpenSearch Service workspace used for this integration. An OpenSearch Service workspace is the collection of dashboards along with other OpenSearch Service tools. This workspace was created automatically as part of the integration setup. For more information, see Centralized OpenSearch user interface (Dashboards) with OpenSearch Service.

Type: OpenSearchWorkspace 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

OpenSearchLifecyclePolicy

This structure contains information about the OpenSearch Service data lifecycle policy used for this integration. The lifecycle policy determines the lifespan of the data in the collection. It was automatically created as part of the integration setup.

For more information, see Using data lifecycle policies with OpenSearch Service Serverless in the OpenSearch Service Developer Guide.

Contents

policyName

The name of the lifecycle policy.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `[\.\-_/#A-Za-z0-9]+`

Required: No

status

This structure contains information about the status of this OpenSearch Service resource.

Type: OpenSearchResourceStatus 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

OpenSearchNetworkPolicy

This structure contains information about the OpenSearch Service network policy used for this integration. The network policy assigns network access settings to collections. For more information, see Network policies in the OpenSearch Service Developer Guide.

Contents

policyName

The name of the network policy.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `[\.\-_/#A-Za-z0-9]+`

Required: No

status

This structure contains information about the status of this OpenSearch Service resource.

Type: OpenSearchResourceStatus 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

OpenSearchResourceConfig

This structure contains configuration details about an integration between CloudWatch Logs and OpenSearch Service.

Contents

dashboardViewerPrincipals

Specify the ARNs of IAM roles and IAM users who you want to grant permission to for viewing the dashboards.

> **Important**
>
> In addition to specifying these users here, you must also grant them the **CloudWatchOpenSearchDashboardAccess** IAM policy. For more information, see IAM policies for users.

Type: Array of strings

Required: Yes

dataSourceRoleArn

Specify the ARN of an IAM role that CloudWatch Logs will use to create the integration. This role must have the permissions necessary to access the OpenSearch Service collection to be able to create the dashboards. For more information about the permissions needed, see Permissions that the integration needs in the CloudWatch Logs User Guide.

Type: String

Required: Yes

retentionDays

Specify how many days that you want the data derived by OpenSearch Service to be retained in the index that the dashboard refers to. This also sets the maximum time period that you can choose when viewing data in the dashboard. Choosing a longer time frame will incur additional costs.

Type: Integer

Valid Range: Minimum value of 1. Maximum value of 30.

Required: Yes

applicationArn

If you want to use an existing OpenSearch Service application for your integration with OpenSearch Service, specify it here. If you omit this, a new application will be created.

Type: String

Required: No

kmsKeyArn

To have the vended dashboard data encrypted with AWS KMS instead of the CloudWatch Logs default encryption method, specify the ARN of the AWS KMS key that you want to use.

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

OpenSearchResourceStatus

This structure contains information about the status of an OpenSearch Service resource.

Contents

status

The current status of this resource.

Type: String

Valid Values: `ACTIVE | NOT_FOUND | ERROR`

Required: No

statusMessage

A message with additional information about the status of this resource.

Type: String

Length Constraints: Minimum length of 1.

Required: No

See Also

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

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

OpenSearchWorkspace

This structure contains information about the OpenSearch Service workspace used for this integration. An OpenSearch Service workspace is the collection of dashboards along with other OpenSearch Service tools. This workspace was created automatically as part of the integration setup. For more information, see Centralized OpenSearch user interface (Dashboards) with OpenSearch Service.

Contents

status

This structure contains information about the status of an OpenSearch Service resource.

Type: OpenSearchResourceStatus object

Required: No

workspaceId

The ID of this workspace.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `[\.\-_/#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

OutputLogEvent

Represents a log event.

Contents

ingestionTime

The time the event was ingested, expressed as the number of milliseconds after `Jan 1, 1970 00:00:00` UTC.

Type: Long

Valid Range: Minimum value of 0.

Required: No

message

The data contained in the log event.

Type: String

Length Constraints: Minimum length of 1.

Required: No

timestamp

The time the event occurred, expressed as the number of milliseconds after `Jan 1, 1970 00:00:00` UTC.

Type: Long

Valid Range: Minimum value of 0.

Required: No

See Also

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

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

ParseCloudfront

This processor parses CloudFront vended logs, extract fields, and convert them into JSON format. Encoded field values are decoded. Values that are integers and doubles are treated as such. For more information about this processor including examples, see parseCloudfront

For more information about CloudFront log format, see Configure and use standard logs (access logs).

If you use this processor, it must be the first processor in your transformer.

Contents

source

Omit this parameter and the whole log message will be processed by this processor. No other value than `@message` is allowed for `source`.

Type: String

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

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

ParseJSON

This processor parses log events that are in JSON format. It can extract JSON key-value pairs and place them under a destination that you specify.

Additionally, because you must have at least one parse-type processor in a transformer, you can use `ParseJSON` as that processor for JSON-format logs, so that you can also apply other processors, such as mutate processors, to these logs.

For more information about this processor including examples, see parseJSON in the *CloudWatch Logs User Guide*.

Contents

destination

The location to put the parsed key value pair into. If you omit this parameter, it is placed under the root node.

Type: String

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

Required: No

source

Path to the field in the log event that will be parsed. Use dot notation to access child fields. For example, `store.book`

Type: String

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

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

ParseKeyValue

This processor parses a specified field in the original log event into key-value pairs.

For more information about this processor including examples, see parseKeyValue in the *CloudWatch Logs User Guide*.

Contents

destination

The destination field to put the extracted key-value pairs into

Type: String

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

Required: No

fieldDelimiter

The field delimiter string that is used between key-value pairs in the original log events. If you omit this, the ampersand & character is used.

Type: String

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

Required: No

keyPrefix

If you want to add a prefix to all transformed keys, specify it here.

Type: String

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

Required: No

keyValueDelimiter

The delimiter string to use between the key and value in each pair in the transformed log event.

If you omit this, the equal = character is used.

Type: String

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

Required: No

nonMatchValue

A value to insert into the value field in the result, when a key-value pair is not successfully split.

Type: String

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

Required: No

overwriteIfExists

Specifies whether to overwrite the value if the destination key already exists. If you omit this, the default is `false`.

Type: Boolean

Required: No

source

Path to the field in the log event that will be parsed. Use dot notation to access child fields. For example, `store.book`

Type: String

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

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

ParsePostgres

Use this processor to parse RDS for PostgreSQL vended logs, extract fields, and and convert them into a JSON format. This processor always processes the entire log event message. For more information about this processor including examples, see parsePostGres.

For more information about RDS for PostgreSQL log format, see RDS for PostgreSQL database log filesTCP flag sequence.

> **Important**
>
> If you use this processor, it must be the first processor in your transformer.

Contents

source

Omit this parameter and the whole log message will be processed by this processor. No other value than `@message` is allowed for `source`.

Type: String

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

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

ParseRoute53

Use this processor to parse Route 53 vended logs, extract fields, and and convert them into a JSON format. This processor always processes the entire log event message. For more information about this processor including examples, see parseRoute53.

Important

If you use this processor, it must be the first processor in your transformer.

Contents

source

Omit this parameter and the whole log message will be processed by this processor. No other value than `@message` is allowed for `source`.

Type: String

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

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

ParseToOCSF

This processor converts logs into Open Cybersecurity Schema Framework (OCSF) events.

For more information about this processor including examples, see parseToOCSF in the *CloudWatch Logs User Guide*.

Contents

eventSource

Specify the service or process that produces the log events that will be converted with this processor.

Type: String

Valid Values: `CloudTrail | Route53Resolver | VPCFlow | EKSAudit | AWSWAF`

Required: Yes

ocsfVersion

Specify which version of the OCSF schema to use for the transformed log events.

Type: String

Valid Values: `V1.1 | V1.5`

Required: Yes

mappingVersion

The version of the OCSF mapping to use for parsing log data.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 10.

Pattern: `^\d+\.\d+(\.\d+)?$`

Required: No

source

The path to the field in the log event that you want to parse. If you omit this value, the whole log message is parsed.

Type: String

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

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

ParseVPC

Use this processor to parse Amazon VPC vended logs, extract fields, and and convert them into a JSON format. This processor always processes the entire log event message.

This processor doesn't support custom log formats, such as NAT gateway logs. For more information about custom log formats in Amazon VPC, see parseVPC For more information about this processor including examples, see parseVPC.

> **Important**
>
> If you use this processor, it must be the first processor in your transformer.

Contents

source

Omit this parameter and the whole log message will be processed by this processor. No other value than `@message` is allowed for `source`.

Type: String

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

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

ParseWAF

Use this processor to parse AWS WAF vended logs, extract fields, and and convert them into a JSON format. This processor always processes the entire log event message. For more information about this processor including examples, see parseWAF.

For more information about AWS WAF log format, see Log examples for web ACL traffic.

> **Important**
>
> If you use this processor, it must be the first processor in your transformer.

Contents

source

Omit this parameter and the whole log message will be processed by this processor. No other value than `@message` is allowed for `source`.

Type: String

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

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

PatternToken

A structure that contains information about one pattern token related to an anomaly.

For more information about patterns and tokens, see CreateLogAnomalyDetector.

Contents

dynamicTokenPosition

For a dynamic token, this indicates where in the pattern that this token appears, related to other dynamic tokens. The dynamic token that appears first has a value of 1, the one that appears second is 2, and so on.

Type: Integer

Required: No

enumerations

Contains the values found for a dynamic token, and the number of times each value was found.

Type: String to long map

Key Length Constraints: Minimum length of 1.

Required: No

inferredTokenName

A name that CloudWatch Logs assigned to this dynamic token to make the pattern more readable. The string part of the `inferredTokenName` gives you a clearer idea of the content of this token. The number part of the `inferredTokenName` shows where in the pattern this token appears, compared to other dynamic tokens. CloudWatch Logs assigns the string part of the name based on analyzing the content of the log events that contain it.

For example, an inferred token name of `IPAddress-3` means that the token represents an IP address, and this token is the third dynamic token in the pattern.

Type: String

Length Constraints: Minimum length of 1.

Required: No

isDynamic

Specifies whether this is a dynamic token.

Type: Boolean

Required: No

tokenString

The string represented by this token. If this is a dynamic token, the value will be <*>

Type: String

Length Constraints: Minimum length of 1.

Required: No

See Also

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

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

Policy

A structure that contains information about one delivery destination policy.

Contents

deliveryDestinationPolicy

The contents of the delivery destination policy.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 51200.

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

Processor

This structure contains the information about one processor in a log transformer.

Contents

addKeys

Use this parameter to include the addKeys processor in your transformer.

Type: AddKeys object

Required: No

copyValue

Use this parameter to include the copyValue processor in your transformer.

Type: CopyValue object

Required: No

csv

Use this parameter to include the CSV processor in your transformer.

Type: CSV object

Required: No

dateTimeConverter

Use this parameter to include the datetimeConverter processor in your transformer.

Type: DateTimeConverter object

Required: No

deleteKeys

Use this parameter to include the deleteKeys processor in your transformer.

Type: DeleteKeys object

Required: No

grok

Use this parameter to include the grok processor in your transformer.

Type: Grok object

Required: No

listToMap

Use this parameter to include the listToMap processor in your transformer.

Type: ListToMap object

Required: No

lowerCaseString

Use this parameter to include the lowerCaseString processor in your transformer.

Type: LowerCaseString object

Required: No

moveKeys

Use this parameter to include the moveKeys processor in your transformer.

Type: MoveKeys object

Required: No

parseCloudfront

Use this parameter to include the parseCloudfront processor in your transformer.

If you use this processor, it must be the first processor in your transformer.

Type: ParseCloudfront object

Required: No

parseJSON

Use this parameter to include the parseJSON processor in your transformer.

Type: ParseJSON object

Required: No

parseKeyValue

Use this parameter to include the parseKeyValue processor in your transformer.

Type: ParseKeyValue object

Required: No

parsePostgres

Use this parameter to include the parsePostGres processor in your transformer.

If you use this processor, it must be the first processor in your transformer.

Type: ParsePostgres object

Required: No

parseRoute53

Use this parameter to include the parseRoute53 processor in your transformer.

If you use this processor, it must be the first processor in your transformer.

Type: ParseRoute53 object

Required: No

parseToOCSF

Use this parameter to convert logs into Open Cybersecurity Schema (OCSF) format.

Type: ParseToOCSF object

Required: No

parseVPC

Use this parameter to include the parseVPC processor in your transformer.

If you use this processor, it must be the first processor in your transformer.

Type: ParseVPC object

Required: No

parseWAF

Use this parameter to include the parseWAF processor in your transformer.

If you use this processor, it must be the first processor in your transformer.

Type: ParseWAF object

Required: No

renameKeys

Use this parameter to include the renameKeys processor in your transformer.

Type: RenameKeys object

Required: No

splitString

Use this parameter to include the splitString processor in your transformer.

Type: SplitString object

Required: No

substituteString

Use this parameter to include the substituteString processor in your transformer.

Type: SubstituteString object

Required: No

trimString

Use this parameter to include the trimString processor in your transformer.

Type: TrimString object

Required: No

typeConverter

Use this parameter to include the typeConverter processor in your transformer.

Type: TypeConverter object

Required: No

upperCaseString

Use this parameter to include the upperCaseString processor in your transformer.

Type: UpperCaseString 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

QueryCompileError

Reserved.

Contents

location

Reserved.

Type: QueryCompileErrorLocation object

Required: No

message

Reserved.

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

QueryCompileErrorLocation

Reserved.

Contents

endCharOffset

Reserved.

Type: Integer

Required: No

startCharOffset

Reserved.

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

QueryDefinition

This structure contains details about a saved CloudWatch Logs Insights query definition.

Contents

lastModified

The date that the query definition was most recently modified.

Type: Long

Valid Range: Minimum value of 0.

Required: No

logGroupNames

If this query definition contains a list of log groups that it is limited to, that list appears here.

Type: Array of strings

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `[\.\-_/#A-Za-z0-9]+`

Required: No

name

The name of the query definition.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 255.

Required: No

parameters

If this query definition contains a list of query parameters that define placeholder variables for the query string, that list appears here.

Type: Array of QueryParameter objects

Array Members: Maximum number of 20 items.

Required: No

queryDefinitionId

The unique ID of the query definition.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Required: No

queryLanguage

The query language used for this query. For more information about the query languages that CloudWatch Logs supports, see Supported query languages.

Type: String

Valid Values: `CWLI | SQL | PPL`

Required: No

queryString

The query string to use for this definition. For more information, see CloudWatch Logs Insights Query Syntax.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 10000.

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

QueryInfo

Information about one CloudWatch Logs Insights query that matches the request in a `DescribeQueries` operation.

Contents

bytesScanned

The total number of bytes scanned by the query. This indicates the cost associated with the query.

Type: Double

Required: No

createTime

The date and time that this query was created.

Type: Long

Valid Range: Minimum value of 0.

Required: No

logGroupName

The name of the log group scanned by this query.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `[\.\-_/#A-Za-z0-9]+`

Required: No

queryDuration

The duration in milliseconds that the query took to execute.

Type: Long

Required: No

queryId

The unique ID number of this query.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Required: No

queryLanguage

The query language used for this query. For more information about the query languages that CloudWatch Logs supports, see Supported query languages.

Type: String

Valid Values: `CWLI | SQL | PPL`

Required: No

queryString

The query string used in this query.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 10000.

Required: No

status

The status of this query. Possible values are `Cancelled`, `Complete`, `Failed`, `Running`, `Scheduled`, and `Unknown`.

Type: String

Valid Values: `Scheduled | Running | Complete | Failed | Cancelled | Timeout | Unknown`

Required: No

userIdentity

The ARN of the user who ran the query.

Type: String

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

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

QueryParameter

This structure defines a query parameter for a saved CloudWatch Logs Insights query definition. Query parameters are supported only for Logs Insights QL queries. They are placeholder variables that you can reference in a query string using the `{{parameterName}}` syntax. Each parameter can include a default value and a description.

Contents

name

The name of the query parameter. A query parameter name must start with a letter or underscore, and contain only letters, digits, and underscores.

Type: String

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

Pattern: `^[a-zA-Z_][a-zA-Z0-9_]*`

Required: Yes

defaultValue

The default value to use for this query parameter if no value is supplied at execution time.

Type: String

Length Constraints: Maximum length of 1024.

Required: No

description

A description of the query parameter that explains its purpose or expected values.

Type: String

Length Constraints: Maximum length of 512.

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

QueryStatistics

Contains the number of log events scanned by the query, the number of log events that matched the query criteria, and the total number of bytes in the log events that were scanned.

If the query involved log groups that have field index policies, the estimated number of skipped log events and the total bytes of those skipped log events are included. Using field indexes to skip log events in queries reduces scan volume and improves performance. For more information, see Create field indexes to improve query performance and reduce scan volume.

Contents

bytesScanned

The total number of bytes in the log events scanned during the query.

Type: Double

Required: No

estimatedBytesSkipped

An estimate of the number of bytes in the log events that were skipped when processing this query, because the query contained an indexed field. Skipping these entries lowers query costs and improves the query performance time. For more information about field indexes, see PutIndexPolicy.

Type: Double

Required: No

estimatedRecordsSkipped

An estimate of the number of log events that were skipped when processing this query, because the query contained an indexed field. Skipping these entries lowers query costs and improves the query performance time. For more information about field indexes, see PutIndexPolicy.

Type: Double

Required: No

logGroupsScanned

The number of log groups that were scanned by this query.

Type: Double

Required: No

recordsMatched

The number of log events that matched the query string.

Type: Double

Required: No

recordsScanned

The total number of log events scanned during the query.

Type: Double

Required: No

resultCount

The number of rows in the final query result set. This value represents the total number of output rows across all pages. For queries that include post-aggregation filters (such as `stats count(*) by field | filter count > threshold`), this value might be less than `recordsMatched`. It reflects only the rows that survived all operations in the query.

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

RecordField

A structure that represents a valid record field header and whether it is mandatory.

Contents

mandatory

If this is `true`, the record field must be present in the `recordFields` parameter provided to a CreateDelivery or UpdateDeliveryConfiguration operation.

Type: Boolean

Required: No

name

The name to use when specifying this record field in a CreateDelivery or UpdateDeliveryConfiguration operation.

Type: String

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

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

RejectedEntityInfo

If an entity is rejected when a `PutLogEvents` request was made, this includes details about the reason for the rejection.

Contents

errorType

The type of error that caused the rejection of the entity when calling `PutLogEvents`.

Type: String

Valid Values: `InvalidEntity | InvalidTypeValue | InvalidKeyAttributes | InvalidAttributes | EntitySizeTooLarge | UnsupportedLogGroupType | MissingRequiredFields`

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

RejectedLogEventsInfo

Represents the rejected events.

Contents

expiredLogEventEndIndex

The expired log events.

Type: Integer

Required: No

tooNewLogEventStartIndex

The index of the first log event that is too new. This field is inclusive.

Type: Integer

Required: No

tooOldLogEventEndIndex

The index of the last log event that is too old. This field is exclusive.

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

RenameKeyEntry

This object defines one key that will be renamed with the renameKey processor.

Contents

key

The key to rename

Type: String

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

Required: Yes

renameTo

The string to use for the new key name

Type: String

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

Required: Yes

overwriteIfExists

Specifies whether to overwrite the existing value if the destination key already exists. The default is `false`

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

RenameKeys

Use this processor to rename keys in a log event.

For more information about this processor including examples, see renameKeys in the *CloudWatch Logs User Guide*.

Contents

entries

An array of `RenameKeyEntry` objects, where each object contains the information about a single key to rename.

Type: Array of RenameKeyEntry objects

Array Members: Minimum number of 1 item. Maximum number of 5 items.

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

ResourceConfig

This structure contains configuration details about an integration between CloudWatch Logs and another entity.

Contents

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

openSearchResourceConfig

This structure contains configuration details about an integration between CloudWatch Logs and OpenSearch Service.

Type: OpenSearchResourceConfig 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

ResourcePolicy

A policy enabling one or more entities to put logs to a log group in this account.

Contents

lastUpdatedTime

Timestamp showing when this policy was last updated, expressed as the number of milliseconds after `Jan 1, 1970 00:00:00 UTC`.

Type: Long

Valid Range: Minimum value of 0.

Required: No

policyDocument

The details of the policy.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 51200.

Required: No

policyName

The name of the resource policy.

Type: String

Required: No

policyScope

Specifies scope of the resource policy. Valid values are ACCOUNT or RESOURCE.

Type: String

Valid Values: `ACCOUNT | RESOURCE`

Required: No

resourceArn

The ARN of the CloudWatch Logs resource to which the resource policy is attached. Only populated for resource-scoped policies.

Type: String

Required: No

revisionId

The revision ID of the resource policy. Only populated for resource-scoped policies.

Type: String

Length Constraints: Minimum length of 1.

Required: No

See Also

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

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

ResultField

Contains one field from one log event returned by a CloudWatch Logs Insights query, along with the value of that field.

For more information about the fields that are generated by CloudWatch logs, see Supported Logs and Discovered Fields.

Contents

field

The log event field.

Type: String

Required: No

value

The value of this field.

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

S3Configuration

Configuration for Amazon S3 destination where scheduled query results are delivered.

Contents

destinationIdentifier

The Amazon S3 URI where query results are delivered. Must be a valid S3 URI format.

Type: String

Length Constraints: Maximum length of 1024.

Pattern: `s3://[a-z0-9][\.\-a-z0-9]{1,61}[a-z0-9](/.*)?`

Required: Yes

roleArn

The ARN of the IAM role that grants permissions to write query results to the specified Amazon S3 destination.

Type: String

Length Constraints: Minimum length of 1.

Required: Yes

kmsKeyId

The Amazon Resource Name (ARN) of the KMS encryption key. Must belong to the same AWS Region as the destination Amazon S3 bucket.

Type: String

Length Constraints: Maximum length of 256.

Required: No

ownerAccountId

The AWS accountId for the bucket owning account.

Type: String

Length Constraints: Fixed length of 12.

Pattern: ^\d{12}$

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

S3DeliveryConfiguration

This structure contains delivery configurations that apply only when the delivery destination resource is an S3 bucket.

Contents

enableHiveCompatiblePath

This parameter causes the S3 objects that contain delivered logs to use a prefix structure that allows for integration with Apache Hive.

Type: Boolean

Required: No

suffixPath

This string allows re-configuring the S3 object prefix to contain either static or variable sections. The valid variables to use in the suffix path vary by log type. To find the values supported for the suffix path for each log type, use the DescribeConfigurationTemplates operation and check the `allowedSuffixPathFields` field in the response. For more information about how the destination prefix, suffix path, and Hive-compatible setting determine the Amazon S3 object key, see Amazon S3 object key for V2 deliveries.

Type: String

Length Constraints: Minimum length of 1. 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

S3TableIntegrationSource

Represents a data source association with an S3 Table Integration, including its status and metadata.

Contents

createdTimeStamp

The timestamp when the data source association was created.

Type: Long

Valid Range: Minimum value of 0.

Required: No

dataSource

The data source associated with the S3 Table Integration.

Type: DataSource object

Required: No

identifier

The unique identifier for this data source association.

Type: String

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

Required: No

parentSourceIdentifier

The identifier of the parent data source for this association.

Type: String

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

Required: No

status

The current status of the data source association.

Type: String

Valid Values: `ACTIVE | UNHEALTHY | FAILED | DATA_SOURCE_DELETE_IN_PROGRESS`

Required: No

statusReason

Additional information about the status of the data source association.

Type: String

Length Constraints: Minimum length of 1.

Required: No

See Also

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

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

S3TablesIntegration

Contains information about the S3 Tables integration configuration for a configuration template.

Contents

datasourceName

The name of the S3 Tables datasource.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Required: No

datasourceType

The type of the S3 Tables datasource.

Type: String

Length Constraints: Minimum length of 1. 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

ScheduledQueryDestination

Information about a destination where scheduled query results are processed, including processing status and any error messages.

Contents

destinationIdentifier

The identifier for the destination where results are delivered.

Type: String

Required: No

destinationType

The type of destination for query results.

Type: String

Valid Values: `S3 | LOOKUP_TABLE`

Required: No

errorMessage

Error message if destination processing failed.

Type: String

Required: No

processedIdentifier

The identifier of the processed result at the destination.

Type: String

Required: No

status

The processing status of the destination delivery.

Type: String

Valid Values: `IN_PROGRESS | CLIENT_ERROR | FAILED | COMPLETE`

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

ScheduledQuerySummary

Summary information about a scheduled query, including basic configuration and execution status.

Contents

creationTime

The timestamp when the scheduled query was created.

Type: Long

Valid Range: Minimum value of 0.

Required: No

destinationConfiguration

Configuration for where query results are delivered.

Type: DestinationConfiguration object

Required: No

lastExecutionStatus

The status of the most recent execution.

Type: String

Valid Values: `Running | InvalidQuery | Complete | Failed | Timeout`

Required: No

lastTriggeredTime

The timestamp when the scheduled query was last executed.

Type: Long

Valid Range: Minimum value of 0.

Required: No

lastUpdatedTime

The timestamp when the scheduled query was last updated.

Type: Long

Valid Range: Minimum value of 0.

Required: No

name

The name of the scheduled query.

Type: String

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

Required: No

scheduledQueryArn

The ARN of the scheduled query.

Type: String

Required: No

scheduleExpression

The cron expression that defines when the scheduled query runs.

Type: String

Length Constraints: Maximum length of 256.

Required: No

scheduleType

The schedule type of the scheduled query. Valid values are `CUSTOMER_MANAGED` and `AWS_MANAGED`.

Type: String

Valid Values: `CUSTOMER_MANAGED | AWS_MANAGED`

Required: No

state

The current state of the scheduled query.

Type: String

Valid Values: `ENABLED | DISABLED`

Required: No

timezone

The timezone used for evaluating the schedule expression.

Type: String

Length Constraints: Minimum length of 1.

Required: No

See Also

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

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

SearchedLogStream

Represents the search status of a log stream.

Contents

logStreamName

The name of the log stream.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `[^:*]*`

Required: No

searchedCompletely

Indicates whether all the events in this log stream were searched.

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

SplitString

Use this processor to split a field into an array of strings using a delimiting character.

For more information about this processor including examples, see splitString in the *CloudWatch Logs User Guide*.

Contents

entries

An array of `SplitStringEntry` objects, where each object contains the information about one field to split.

Type: Array of SplitStringEntry objects

Array Members: Minimum number of 1 item. Maximum number of 10 items.

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

SplitStringEntry

This object defines one log field that will be split with the splitString processor.

Contents

delimiter

The separator characters to split the string entry on.

Type: String

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

Required: Yes

source

The key of the field to split.

Type: String

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

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

StartLiveTailResponseStream

This object includes the stream returned by your StartLiveTail request.

Contents

sessionStart

This object contains information about this Live Tail session, including the log groups included and the log stream filters, if any.

Type: LiveTailSessionStart object

Required: No

SessionStreamingException

This exception is returned if an unknown error occurs.

Type: Exception

HTTP Status Code:

Required: No

SessionTimeoutException

This exception is returned in the stream when the Live Tail session times out. Live Tail sessions time out after three hours.

Type: Exception

HTTP Status Code:

Required: No

sessionUpdate

This object contains the log events and session metadata.

Type: LiveTailSessionUpdate 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

SubscriptionFilter

Represents a subscription filter.

Contents

applyOnTransformedLogs

This parameter is valid only for log groups that have an active log transformer. For more information about log transformers, see PutTransformer.

If this value is `true`, the subscription filter is applied on the transformed version of the log events instead of the original ingested log events.

Type: Boolean

Required: No

creationTime

The creation time of the subscription filter, expressed as the number of milliseconds after `Jan 1, 1970 00:00:00` UTC.

Type: Long

Valid Range: Minimum value of 0.

Required: No

destinationArn

The Amazon Resource Name (ARN) of the destination.

Type: String

Length Constraints: Minimum length of 1.

Required: No

distribution

The method used to distribute log data to the destination, which can be either random or grouped by log stream.

Type: String

Valid Values: `Random | ByLogStream`

Required: No

emitSystemFields

The list of system fields that are included in the log events sent to the subscription destination. Returns the `emitSystemFields` value if it was specified when the subscription filter was created.

Type: Array of strings

Required: No

fieldSelectionCriteria

The filter expression that specifies which log events are processed by this subscription filter based on system fields. Returns the `fieldSelectionCriteria` value if it was specified when the subscription filter was created.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 2000.

Required: No

filterName

The name of the subscription filter.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `[^:*]*`

Required: No

filterPattern

A symbolic description of how CloudWatch Logs should interpret the data in each log event. For example, a log event can contain timestamps, IP addresses, strings, and so on. You use the filter pattern to specify what to look for in the log event message.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 1024.

Required: No

logGroupName

The name of the log group.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `[\.\-_/#A-Za-z0-9]+`

Required: No

roleArn

Type: String

Length Constraints: Minimum length of 1.

Required: No

See Also

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

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

SubstituteString

This processor matches a key's value against a regular expression and replaces all matches with a replacement string.

For more information about this processor including examples, see substituteString in the *CloudWatch Logs User Guide*.

Contents

entries

An array of objects, where each object contains the information about one key to match and replace.

Type: Array of SubstituteStringEntry objects

Array Members: Minimum number of 1 item. Maximum number of 10 items.

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

SubstituteStringEntry

This object defines one log field key that will be replaced using the substituteString processor.

Contents

from

The regular expression string to be replaced. Special regex characters such as [and] must be escaped using \\ when using double quotes and with \ when using single quotes. For more information, see Class Pattern on the Oracle web site.

Type: String

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

Required: Yes

source

The key to modify

Type: String

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

Required: Yes

to

The string to be substituted for each match of `from`

Type: String

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

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

SuppressionPeriod

If you are suppressing an anomaly temporariliy, this structure defines how long the suppression period is to be.

Contents

suppressionUnit

Specifies whether the value of `value` is in seconds, minutes, or hours.

Type: String

Valid Values: `SECONDS | MINUTES | HOURS`

Required: No

value

Specifies the number of seconds, minutes or hours to suppress this anomaly. There is no maximum.

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

SyslogConfiguration

Contains information about a syslog configuration associated with a log group.

Contents

createdAt

The time when the syslog configuration was created, expressed as the number of milliseconds after `Jan 1, 1970 00:00:00 UTC`.

Type: Long

Valid Range: Minimum value of 0.

Required: No

logGroupArn

The ARN of the log group associated with this syslog configuration.

Type: String

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

Pattern: `[\w#+=/:,.@-]*`

Required: No

sourceType

The source type for the syslog configuration.

Type: String

Valid Values: `VPCE`

Required: No

vpcEndpointId

The ID of the VPC endpoint used for syslog ingestion.

Type: String

Pattern: `^vpce-[0-9a-f]{1,64}$`

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

TagFilter

A tag filter that specifies a tag key and optional tag values for filtering log groups by tags.

Contents

key

The tag key to filter on.

Type: String

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

Pattern: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]+)$`

Required: Yes

values

An optional list of tag values to filter on.

- If you specify a filter that contains more than one value for a key, the response returns log groups that match any of the specified values for that key.
- If you don't specify values, the response returns all log groups that are tagged with that key, with any or no value.
- Use `*` for wildcard matching. For example, `prod*` matches values that start with `prod`.
- Use `!` as a prefix for negation. For example, `!prod` matches values that are not `prod`.
- Exact matching and negation are case-sensitive. Wildcard matching is case-insensitive.

Type: Array of strings

Array Members: Minimum number of 0 items. Maximum number of 5 items.

Length Constraints: Minimum length of 0. Maximum length of 259.

Pattern: `^!?\*?([\p{L}\p{Z}\p{N}_.:/=+\-@]*)\*?$`

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

TransformedLogRecord

This structure contains information for one log event that has been processed by a log transformer.

Contents

eventMessage

The original log event message before it was transformed.

Type: String

Length Constraints: Minimum length of 1.

Required: No

eventNumber

The event number.

Type: Long

Required: No

transformedEventMessage

The log event message after being transformed.

Type: String

Length Constraints: Minimum length of 1.

Required: No

See Also

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

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

TriggerHistoryRecord

A record of a scheduled query execution, including execution status, timestamp, and destination processing results.

Contents

destinations

Information about destination processing for this query execution.

Type: Array of ScheduledQueryDestination objects

Required: No

errorMessage

Error message if the query execution failed.

Type: String

Required: No

executionStatus

The execution status of the scheduled query run.

Type: String

Valid Values: `Running | InvalidQuery | Complete | Failed | Timeout`

Required: No

queryId

The unique identifier for this query execution.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Required: No

triggeredTimestamp

The timestamp when the scheduled query execution was triggered.

Type: Long

Valid Range: Minimum value of 0.

Required: No

See Also

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

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

TrimString

Use this processor to remove leading and trailing whitespace.

For more information about this processor including examples, see trimString in the *CloudWatch Logs User Guide*.

Contents

withKeys

The array containing the keys of the fields to trim.

Type: Array of strings

Array Members: Minimum number of 1 item. Maximum number of 10 items.

Length Constraints: Minimum length of 1.

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

TypeConverter

Use this processor to convert a value type associated with the specified key to the specified type. It's a casting processor that changes the types of the specified fields. Values can be converted into one of the following datatypes: `integer`, `double`, `string` and `boolean`.

For more information about this processor including examples, see trimString in the *CloudWatch Logs User Guide*.

Contents

entries

An array of `TypeConverterEntry` objects, where each object contains the information about one field to change the type of.

Type: Array of TypeConverterEntry objects

Array Members: Minimum number of 1 item. Maximum number of 5 items.

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

TypeConverterEntry

This object defines one value type that will be converted using the typeConverter processor.

Contents

key

The key with the value that is to be converted to a different type.

Type: String

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

Required: Yes

type

The type to convert the field value to. Valid values are `integer`, `double`, `string` and `boolean`.

Type: String

Valid Values: `boolean | integer | double | 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

UpperCaseString

This processor converts a string field to uppercase.

For more information about this processor including examples, see upperCaseString in the *CloudWatch Logs User Guide*.

Contents

withKeys

The array of containing the keys of the field to convert to uppercase.

Type: Array of strings

Array Members: Minimum number of 1 item. Maximum number of 10 items.

Length Constraints: Minimum length of 1.

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

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*.

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 Error Types

This section lists common error types that this AWS service may return. Not all services return all error types listed here. For errors specific to an API action for this service, see the topic for that API action.

AccessDeniedException

You don't have permission to perform this action. Verify that your IAM policy includes the required permissions.

HTTP Status Code: 403

ExpiredTokenException

The security token included in the request has expired. Request a new security token and try again.

HTTP Status Code: 403

IncompleteSignature

The request signature doesn't conform to AWS standards. Verify that you're using valid AWS credentials and that your request is properly formatted. If you're using an SDK, ensure it's up to date.

HTTP Status Code: 403

InternalFailure

The request can't be processed right now because of an internal server issue. Try again later. If the problem persists, contact AWS Support.

HTTP Status Code: 500

MalformedHttpRequestException

The request body can't be processed. This typically happens when the request body can't be decompressed using the specified content encoding algorithm. Verify that the content encoding header matches the compression format used.

HTTP Status Code: 400

NotAuthorized

You don't have permissions to perform this action. Verify that your IAM policy includes the required permissions.

HTTP Status Code: 401

OptInRequired

Your AWS account needs a subscription for this service. Verify that you've enabled the service in your account.

HTTP Status Code: 403

RequestAbortedException

The request was aborted before a response could be returned. This typically happens when the client closes the connection.

HTTP Status Code: 400

RequestEntityTooLargeException

The request entity is too large. Reduce the size of the request body and try again.

HTTP Status Code: 413

RequestTimeoutException

The request timed out. The server didn't receive the complete request within the expected time frame. Try again.

HTTP Status Code: 408

ServiceUnavailable

The service is temporarily unavailable. Try again later.

HTTP Status Code: 503

ThrottlingException

Your request rate is too high. The AWS SDKs automatically retry requests that receive this exception. Reduce the frequency of requests.

HTTP Status Code: 400

UnknownOperationException

The action or operation isn't recognized. Verify that the action name is spelled correctly and that it's supported by the API version you're using.

HTTP Status Code: 404

UnrecognizedClientException

The X.509 certificate or AWS access key ID you provided doesn't exist in our records. Verify that you're using valid credentials and that they haven't expired.

HTTP Status Code: 403

ValidationError

The input doesn't meet the required format or constraints. Check that all required parameters are included and that values are valid.

HTTP Status Code: 400