開發人員指南

Amazon OpenSearch 服務

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

Amazon OpenSearch 服務: 開發人員指南

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

Amazon 的商標和商業外觀不得用於任何非 Amazon 的產品或服務，也不能以任何可能造成客戶混淆、任何貶低或使 Amazon 名譽受損的方式使用 Amazon 的商標和商業外觀。所有其他非 Amazon 擁有的商標均為其各自擁有者的財產，這些擁有者可能附屬於 Amazon，或與 Amazon 有合作關係，亦或受到 Amazon 贊助。

Table of Contents

什麼是 Amazon OpenSearch 服務？ 1
Amazon OpenSearch 服務的特點 1
使用情況 3
Amazon OpenSearch 無服務器 3
Amazon OpenSearch 攝入 3
支援的版本 3
定價 4
開始使用 4
相關服務 5
設定 7
註冊一個 AWS 帳戶 7
建立具有管理存取權的使用者 7
授予許可 8
授與程式設計存取權 9
設定 AWS CLI 10
開啟 主控台 11
開始使用 12
步驟 1：建立網域 12
步驟 2：上傳資料以編製索引 13
選項 1：上傳單一文件 14
選項 2：上傳多個文件 14
步驟 3：搜尋文件 15
從命令列搜尋文件 15
使用 OpenSearch儀表板搜尋文件 16
步驟 4：刪除網域 17
後續步驟 17
Amazon OpenSearch 攝入 18
重要概念 19
優勢 20
限制 21
支援的資料預留程式版本 21
調整管線 22
定價 23
支援 AWS 區域 23

配額 23
設定角色和使用者 24
管理角色 25
管線角色 26
擷取角色 28
授與管道對網域的存取權 29
授予管道對集合的存取權 33
OpenSearch擷取得 40
教學課程：將資料擷取至網域 41
教學課程：將資料擷取至集合 49
管線特徵概觀 56
持久緩衝 57
分割 58
鏈接 59
無效字母佇列 60
索引管理 62
電子nd-to-end 確認 65
源背壓 66
建立管道 66
必要條件和必要角色 67
必要許可 67
指定管線版本 69
指定擷取路徑 69
建立管道 70
追蹤管道建立的狀態 73
使用藍圖建立管道 74
檢視配管 76
更新管道 79
考量事項 79
必要許可 80
更新管道 80
管道更新的藍色/綠色部署 81
停用和啟動管道 82
停用和啟動管道 82
停用管道 82
啟動管道 83

刪除配管 84
支持的插件和選項 85
支持的插件 85
無狀態處理器與可狀態處理器 87
組態需求和限制 87
使用管道整合 92
建構擷取端點 93
建立擷取角色 93
Amazon DynamoDB 95
Amazon DocumentDB 108
匯流雲卡夫卡 121
Amazon MSK 130
Amazon S3 137
Amazon Security Lake 146
Fluent Bit 149
Fluentd 150
OpenTelemetry 收藏家 152
自我管理的 Kafka 154
自我管理 OpenSearch 161
後續步驟 168
在網域和系列之間移轉資料 168
限制 169
OpenSearch 服務作為來源 169
指定多個 OpenSearch 服務網域接收器 171
將資料移轉至 OpenSearch 無伺服器 VPC 集合 172
使用 AWS SDK 管理管道 172
Python 172
OpenSearch擷取中的安全性 176
設定管線的 VPC 存取 177
身分和存取權管理 181
使用 CloudTrail 進行監控 188
標記管線 191
必要許可 192
處理標籤 (主控台) 192
處理標籤 (AWS CLI) 193
記錄和監控 193

監控管道日誌 ... 194
監控管道指標 ... 195
最佳實務 ... 222
一般最佳實務 ... 223
建議的 CloudWatch 鬧鐘 ... 223
Amazon OpenSearch 無服務器 ... 229
優勢 ... 229
什麼是 Amazon OpenSearch 無伺服器？ ... 230
OpenSearch 無伺服器使用案例 ... 230
開始使用 ... 231
運作方式 ... 231
選擇集合類型 ... 233
OpenSearch 無伺服器的定價 ... 234
支援 AWS 區域 ... 234
限制 ... 234
比較 OpenSearch 服務與 OpenSearch 無伺服器 ... 235
開始使用 OpenSearch 無伺服器 ... 238
步驟 1：設定許可 ... 238
步驟 2：建立集合 ... 239
步驟 3：上傳並搜尋資料 ... 240
步驟 4：刪除集合 ... 241
後續步驟 ... 242
建立和管理集合 ... 242
建立、列出和刪除集合 ... 242
使用向量搜尋集合 ... 251
使用資料生命週期原 ... 258
使用 AWS SDK 管理集合 ... 264
使用建立集合 CloudFormation ... 276
管理容量限制 ... 278
進行容量設定 ... 279
容量限制上限 ... 279
監控容量用量 ... 280
將資料擷取至集合 ... 280
所需的最低許可 ... 281
OpenSearch 攝入 ... 281
Fluent Bit ... 282

Amazon 數據 Firehose 282
Go 283
Java 285
JavaScript 287
Logstash 289
Python 291
Ruby 293
其他客戶 294
OpenSearch 無伺服器的安全性 295
加密政策 297
網路政策 297
資料存取政策 298
IAM 和 SAML 身分驗證 299
基礎架構安全 300
開始使用安全功能 300
身分和存取權管理 313
加密 323
網路存取 332
資料存取控制 342
VPC 端點 352
SAML認證 359
法規遵循驗證 368
標記集合 369
必要許可 370
處理標籤 (主控台) 370
使用標籤 (AWS CLI) 370
支援的操作和外掛程式 371
支援的 OpenSearch API 作業和權限 371
支持的 OpenSearch 插件 376
監控 OpenSearch 無伺服器 377
使用監控 CloudWatch 378
使用監控 CloudTrail 382
使用監控 EventBridge 385
建立和管理網域 389
建立 OpenSearch 服務網域 389
建立 OpenSearch 服務網域 (主控台) 389

建立 OpenSearch 服務網域 (AWS CLI) ... 394
建立 OpenSearch 服務網域 (AWS SDKs) ... 396
建立 OpenSearch 服務網域 (AWS CloudFormation) ... 396
設定存取政策 ... 396
進階叢集設定 ... 396
組態變更 ... 397
通常會導致藍/綠部署的變更 ... 398
通常不會導致藍/綠部署的變更 ... 399
判斷變更是否會導致藍/綠部署 ... 399
啟動和追蹤組態變更 ... 403
組態變更的階段 ... 406
藍/綠部署的效能影響 ... 408
組態變更的費用 ... 408
對驗證錯誤進行疑難排解 ... 408
服務軟體更新 ... 412
可選更新與必要更新 ... 413
補丁更新 ... 414
考量事項 ... 414
開始更新 ... 414
離峰窗 ... 417
監控更新 ... 418
網域不符合更新條件時， ... 418
離峰窗 ... 419
離峰服務軟體更新 ... 420
離峰自動調諧最佳化 ... 421
啟用離峰期 ... 421
設定自訂離峰時段 ... 422
檢視排程動作 ... 422
重排作業 ... 424
從自動調整維護時段移轉 ... 426
通知 ... 427
開始使用通知 ... 427
通知嚴重性 ... 428
樣品 EventBridge 事件 ... 428
設定多可用區域網域 ... 429
異地同步備份含待機 ... 429

異地同步備份 (不含 ... 431
可用區域中斷 ... 434
VPC支持 ... 436
VPC與公共領域 ... 436
限制 ... 437
架構 ... 437
建立索引快照 ... 443
必要條件 ... 444
註冊手動快照儲存庫 ... 447
手動拍攝快照 ... 452
還原快照 ... 453
刪除手動快照 ... 455
使用快照管理自動化快照 ... 455
使用索引狀態管理自動化快照 ... 457
使用 Curator 進行快照 ... 457
升級網域 ... 458
支援的升級路徑 ... 458
開始升級 (主控台) ... 461
開始升級 (CLI) ... 461
開始升級 (SDK) ... 462
對驗證失敗進行故障排除 ... 463
升級疑難排解 ... 463
使用快照來遷移資料 ... 465
建立自訂端點 ... 471
新網域的自訂端點 ... 472
現有網域的自訂端點 ... 472
後續步驟 ... 473
自動調校 ... 473
變更類型 ... 474
啟用或停用自動調整 ... 475
排程自動調整增強功 ... 475
監視自動調整變更 ... 476
標記網域 ... 476
標記範例 ... 477
處理標籤 (主控台) ... 478
處理標籤 (AWS CLI) ... 478

使用標籤 (AWS SDK) ... 480
執行管理動作 ... 481
重新啟動節點上的 OpenSearch 處理序 ... 481
重新啟動資料節點 ... 482
重新啟動節點上的儀表板或 Kibana 處理序 ... 482
限制 ... 482
使用直接查詢 ... 484
定價 ... 484
限制 ... 485
建議 ... 485
配額 ... 486
支援地區 ... 486
建立資料來源 ... 486
必要條件 ... 487
設定新的直接查詢資料來源 ... 487
對應 AWS Glue Data Catalog 角色 (如果在建立資料來源之後啟用了精細的存取控制) ... 491
後續步驟 ... 492
配置資料來源 ... 492
設定存取控制 ... 492
熱門 AWS 記錄類型的設定整合 ... 492
將資料匯出至 Amazon S3 的參考指南 ... 493
使用查詢工作台創建星火表 ... 494
加速查詢 ... 494
跳過索引 ... 494
具體化視觀表 ... 495
覆蓋索引 ... 497
查詢資料 ... 498
SQL ... 498
PPL ... 499
建議 ... 499
管理資料來源 ... 499
使用 CloudWatch 指標資料來源監控 ... 499
啟用和停用資料來源 ... 501
使用 AWS 預算監控 ... 502
刪除資料來源 ... 502
監控網域 ... 503

監控叢集指標 504
檢視量度 CloudWatch 504
解譯服務中的健康圖表 OpenSearch 505
叢集指標 506
專用主節點指標 512
EBS體積指標 513
執行個體指標 515
UltraWarm 度量 524
冷儲存指標 529
OR1度量 530
提醒指標 531
異常偵測指標 532
非同步搜尋指標 533
自動調整指標 535
異地同步備份含備用量度 536
時間點量度 538
SQL度量 539
k-NN 指標 540
跨叢集搜尋指標 542
跨叢集複寫指標 543
Learning to Rank 指標 544
Piped Processing Language 指標 545
監控日誌 546
啟用日誌發佈 (主控台) 547
啟用日誌發佈 (AWS CLI) 549
啟用記錄發佈 (AWS SDKs) 551
啟用日誌發佈 (CloudFormation) 551
設定搜尋要求慢速記錄閾值 553
設置碎片緩慢日誌閾值 554
測試慢速記錄 554
檢視日誌 555
監控稽核日誌 555
限制 556
啟用稽核日誌 556
啟用稽核記錄 AWS CLI 558
使用組態 API 啟用稽核日誌記錄 558

稽核日誌層和類別 558
稽核日誌設定 560
稽核日誌範例 563
使用 REST API 設定稽核日誌 566
監控事件 567
服務軟體更新事件 568
自動調整事件 575
叢集運作狀態事件 579
VPC 端點事件 592
節點淘汰事件 594
降級的節點淘汰事件 596
網域錯誤事件 598
教學課程：偵聽服 OpenSearch 務事件 600
教學課程：傳送可用更新的 SNS 提醒 602
使用 CloudTrail 進行監控 604
亞馬遜OpenSearch服務信息 CloudTrail 383
了解 Amazon Amazon Ser OpenSearch vice 日誌檔案項目 384
安全 608
資料保護 608
靜態加密 609
N ode-to-node 加密技術 613
身分和存取權管理 613
政策的類型 614
提出和簽署 OpenSearch 服務請求 621
當政策衝突時 622
政策元素參考 623
進階選項與API考量 628
設定存取政策 631
其他範例政策 631
API 許可參考 631
AWS 受管理政策 631
預防跨服務混淆代理人 638
精細定義存取控制 639
更大的局面：精細的訪問控制和 OpenSearch 服務安全 640
重要概念 644
關於主要使用者 644

啟用精細存取控制 ... 645
以主要使用者身分存取 OpenSearch 儀表板 ... 648
管理許可 ... 650
建議的組態 ... 655
限制 ... 658
修改主要使用者 ... 659
其他主要使用者 ... 659
手動快照 ... 661
整合 ... 661
REST API 差異 ... 662
教學課程：使用 Cognito 身分驗證進行精細存取控制 ... 663
教學課程：內部使用者資料庫和基本身分驗證 ... 668
法規遵循驗證 ... 671
恢復能力 ... 672
JSON網絡令牌 ... 672
考量事項 ... 672
修改網域存取政策 ... 673
設定JWT驗證和授權 ... 673
使用 a JWT 發送測試請求 ... 674
基礎架構安全 ... 675
使用 OpenSearch 服務管理的端VPC點 ... 676
SAML OpenSearch 儀表板的驗證 ... 680
SAML組態概觀 ... 680
考量事項 ... 681
SAMLVPC網域驗證 ... 681
修改網域存取政策 ... 681
設定 SP 或 IdP 啟動的身分驗證 ... 683
同時設定 SP 和 IdP 啟動的身分驗證 ... 689
設定SAML驗證 (AWS CLI) ... 689
配置SAML身份驗證（配置API） ... 689
SAML疑難排 ... 690
停用SAML驗證 ... 692
用於儀表板的 Amazon Cognito 份 OpenSearch ... 693
先決條件 ... 694
設定網域以使用 Amazon Cognito 身分驗證 ... 696
允許已經過身分驗證的角色 ... 700

設定身分提供者 ... 701
(選用) 設定精細分級的存取 ... 701
(選用) 自訂登入頁面 ... 702
(選用) 設定進階安全性 ... 702
測試 ... 702
配額 ... 703
常見的設定問題 ... 703
停用儀表板的 Amazon Cognito 份驗證 OpenSearch ... 707
刪除針對儀表板使用 Amazon Cognito 身份驗證的 OpenSearch 網域 ... 707
使用服務連結角色 ... 707
VPC 網域建立角色 ... 708
集合建立角色 ... 711
管道建立角色 ... 713
範本程式碼 ... 716
Elasticsearch 用戶端相容性 ... 716
壓縮 HTTP 請求 ... 717
啟用 gzip 壓縮 ... 717
必要標頭 ... 718
範本程式碼 (Python 3) ... 718
使用 AWS SDK ... 719
Java ... 719
Python ... 731
節點 ... 733
建立資料索引 ... 737
索引的命名限制 ... 737
縮減回應大小 ... 738
索引轉碼器 ... 739
將串流資料載入 OpenSearch 服務 ... 740
從 OpenSearch 擷取載入串流資料 ... 741
從 Amazon S3 載入串流資料 ... 741
從 Amazon Kinesis Data Streams 中載入串流資料 ... 746
從 Amazon DynamoDB 中載入串流資料 ... 750
從 Amazon 數據防 Firehose 件加載流數據 ... 753
從 Amazon 加載流數據 CloudWatch ... 754
從 AWS IoT中載入串流資料 ... 754
使用 Logstash 載入資料 ... 754

組態 ... 754
搜尋資料 ... 757
URI搜尋 ... 757
要求主體搜尋 ... 759
增加欄位 ... 760
搜尋結果反白呈現 ... 761
伯爵 API ... 763
對搜尋結果進行分頁 ... 763
時間點 ... 764
from和size參數 ... 764
儀表板查詢語言 ... 764
自訂套件 ... 766
套件許可要求 ... 767
將套件上傳至 Amazon S3 ... 767
匯入和關聯套件 ... 768
使用套件搭配 OpenSearch ... 768
更新套件 ... 773
字典的手動索引更新 ... 776
解除關聯並移除套件 ... 778
SQL 支援 ... 779
範例呼叫 ... 780
備註和差異 ... 780
SQL Workbench ... 781
SQL CLI ... 674
JDBC 驅動程式 ... 781
ODBC 驅動程式 ... 783
k-NN 搜尋 ... 783
k-NN 入門 ... 785
k-NN 差異、調校和限制 ... 787
跨叢集搜尋 ... 787
限制 ... 788
跨叢集搜尋先決條件 ... 789
跨叢集搜尋定價 ... 789
設定連線 ... 789
移除連線 ... 790
設定安全性和範例演練 ... 791

OpenSearch 儀表板 ... 796
Learning to Rank ... 796
Learning to Rank 入門 ... 797
Learning to Rank API ... 818
非同步搜尋 ... 824
搜尋呼叫範例 ... 824
非同步搜尋許可 ... 826
非同步搜尋設定 ... 826
跨叢集搜尋 ... 827
UltraWarm ... 828
時間點 ... 829
考量事項 ... 829
創建一個坑 ... 830
時間點權限 ... 831
進地坑設置 ... 832
跨叢集搜尋 ... 832
UltraWarm ... 832
语义搜索 ... 832
並行區段搜尋 ... 833
自然語言查詢產生 ... 833
必要條件 ... 833
開始使用 ... 834
設定許可 ... 834
組態自動化 ... 835
OpenSearch 儀表板 ... 836
控制 OpenSearch 儀表板的存取 ... 836
使用 Proxy 從 OpenSearch 儀表板存取 OpenSearch 服務 ... 837
設定 OpenSearch 儀表板以使用地WMS圖伺服器 ... 840
將本機儀表板伺服器連線至 OpenSearch 服務 ... 841
管理 OpenSearch 儀表板中的索引 ... 843
額外功能 ... 843
管理索引 ... 845
UltraWarm 儲存 ... 845
必要條件 ... 846
UltraWarm 儲存需求和效能考量 ... 848
UltraWarm 定價 ... 848

啟用 UltraWarm 849
將索引遷移到 UltraWarm 存儲 851
自動化遷移 854
遷移調整 854
取消遷移 855
列出熱索引和暖索引 855
將暖索引傳回熱儲存區 855
從快照還原暖索引 855
暖索引的手動快照 857
將暖索引遷移到冷儲存 858
禁用 UltraWarm 858
冷儲存 858
必要條件 859
冷儲存要求和效能考量 860
冷儲存定價 860
啟用冷儲存 861
管理 OpenSearch 儀表板中的冷索引 863
將索引遷移至冷儲存 863
自動移轉至冷儲存 864
取消遷移至冷儲存 864
列出冷索引 865
將冷索引遷移至暖儲存 868
從快照中還原冷索引 870
取消從冷儲存遷移至暖儲存 870
更新冷索引中繼資料 871
刪除冷索引 871
停用冷儲存 871
OR1儲存 872
限制 872
調整以獲得更好的擷取輸送量 873
OpenSearch 最佳化執行個體與非 OpenSearch 優化執行個體有何 873
與 UltraWarm儲存空間OR1有何不同 873
使用OR1實例 874
索引狀態管理 875
建立 ISM 政策。 876
範例政策 876

ISM 範本 880
差異 881
教學課程：自動化 ISM 程序 882
索引彙總 886
建立索引彙總任務 887
索引轉換 888
建立索引轉換任務 888
跨叢集複寫 889
限制 890
必要條件 891
許可需求 891
設定跨叢集連線 892
開始複寫 893
確認複寫 893
暫停和繼續複寫 895
停止複寫 895
自動追蹤 896
升級連線的網域 897
遠端重新索引 897
必要條件 898
重新索引 OpenSearch 服務互聯網域之間的數據 898
當遠端網域位於 VPC 中時重新建立資料索引 900
重新索引非OpenSearch 服務網域之間的資料 904
重新索引大型資料集 904
遠端重新索引設定 906
資料串流 906
資料串流入門 907
監控資料 910
提醒 910
提醒許可 911
提醒入門 911
通知 911
差異 912
異常偵測 914
..... 914
教學課程：使用異常偵測來偵測高 CPU 使用率 917

機器學習 920
用於連接器 AWS 服務 920
必要條件 920
建立 OpenSearch 服務連接器 923
外部平台的連接器 925
必要條件 926
建立 OpenSearch 服務連接器 928
CloudFormation 模板集成 930
必要條件 931
Amazon SageMaker 模板 932
Amazon 基岩模板 933
不支援的 ML 共享資源 934
流程框架插件 934
在 OpenSearch 服務中建立 ML 連接器 934
設定許可 941
安全性分析 943
安全性分析元件和概念 943
記錄檔類型 943
偵測器 944
規則 944
問題清單 944
Alerts (提醒) 944
探索安全性分析 944
設定許可 946
故障診斷 948
沒有這樣的索引錯誤 948
可觀測性 949
利用事件分析探索您的資料 949
建立視覺化效果 951
利用 Trace Analytics 進行深入分析 952
Trace Analytics 953
必要條件 954
OpenTelemetry 收集器範例組態 954
OpenSearch 擷取範例組態 955
瀏覽追蹤資料 956
Piped Processing Language 958

... 958
最佳實務 ... 960
監控和提醒 ... 960
設定 CloudWatch 鬧鐘 ... 960
啟用日誌發佈 ... 960
碎片策略 ... 961
確定碎片和資料節點計數 ... 961
避免儲存扭曲 ... 962
穩定性 ... 962
保持最新 OpenSearch ... 962
改善快照效能 ... 963
啟用專用主節點 ... 963
在多個可用區域中進行部署 ... 963
控制擷取流量和緩衝 ... 964
建立搜尋工作負載的映射 ... 964
使用索引範本 ... 965
使用索引狀態管理功能來管理索引 ... 966
移除未使用的索引 ... 966
使用多個網域實現高可用性 ... 966
效能 ... 966
最佳化批量請求大小和壓縮 ... 966
減少批量請求回應的大小 ... 967
調校重新整理間隔 ... 967
啟用自動調整 ... 967
安全 ... 968
啟用精細存取控制 ... 968
部署網域 VPC ... 968
套用限制性存取政策 ... 968
啟用靜態加密 ... 968
啟用 node-to-node 加密 ... 969
使用監視器 AWS Security Hub ... 969
成本最佳化 ... 969
使用最新一代執行個體類型 ... 969
使用最新的 Amazon EBS gp3 卷 ... 969
使用 UltraWarm 和冷存儲時間序列日誌數據 ... 970
檢閱預留執行個體的建議 ... 970

調整網域大小 970
計算儲存需求 970
選擇碎片數 972
選擇執行個體類型並進行測試 973
PB 規模 974
專用主節點 976
選擇專用主節點數目 977
選擇專用主節點的執行個體類型 978
建議的 CloudWatch 鬧鐘 979
您可能會考慮的其他警示 983
一般參考 986
支援的執行個體類型 986
最新一代執行個體類型 986
上一代執行個體類型 999
各引擎版本的功能 1002
依引擎版本分類的外掛程式 1006
可選插件 1009
受支援的操作 1009
顯著的API差異 1010
OpenSearch 版本 2.13 1012
OpenSearch 版本 1015
OpenSearch 第二版 1016
OpenSearch 版本 2.7 1018
OpenSearch 版本 2.5 1019
OpenSearch 第二版本 1021
OpenSearch 版本 1.3 1023
OpenSearch 版本 1.2 1024
OpenSearch 最新版本 1026
OpenSearch 1.0 版本 1027
Elasticsearch 7.10 版 1029
Elasticsearch 7.9 版 1031
Elasticsearch 7.8 版 1032
Elasticsearch 7.7 版 1034
Elasticsearch 7.4 版 1035
Elasticsearch 7.1 版 1037
Elasticsearch 6.8 版 1038

Elasticsearch 6.7 版 1039
Elasticsearch 6.5 版 1041
Elasticsearch 6.4 版 1042
Elasticsearch 6.3 版 1044
Elasticsearch 6.2 版 1045
Elasticsearch 6.0 版 1046
Elasticsearch 5.6 版 1048
Elasticsearch 5.5 版 1049
Elasticsearch 5.3 版 1050
Elasticsearch 5.1 版 1052
Elasticsearch 2.3 版 1053
Elasticsearch 1.5 版 1054
配額 1055
UltraWarm 儲存配額 1055
EBS磁碟區大小配額 1056
網路配額 1063
碎片大小配額 1069
Java 處理序配額 1070
網域政策配額 1070
預留執行個體 1070
購買預留執行個體 (主控台) 1071
購買預留執行個體 (AWS CLI) 1072
購買預留執行個體 (AWS 開發套件) 1074
檢查成本 1076
其他受支援的資源 1076
教學課程 1078
建立和搜尋文件 1078
先決條件 1078
將文件新增至索引 1079
建立自動產生的 ID 1080
使用 POST 命令更新文件 1081
執行大量動作 1082
搜尋文件 1083
相關資源 1084
移轉至OpenSearch服務 1085
建立並上傳快照 1085

建立網域 ... 1086
提供許可以存取 S3 儲存貯體。 ... 1087
還原快照 ... 1089
建立搜尋應用程式 ... 1092
必要條件 ... 1093
步驟 1：索引範例資料 ... 1093
步驟 2：建立和部署 Lambda 函數 ... 1094
步驟 3：在 API Gateway 中建立 API ... 1096
步驟 4：(選用) 修改網域存取政策 ... 1099
映射 Lambda 角色 (如果使用精細存取控制) ... 1100
步驟 5：測試 Web 應用程式 ... 1100
後續步驟 ... 1102
視覺化支援呼叫 ... 1102
步驟 1：設定先決條件 ... 1103
步驟 2：複製範本程式碼 ... 1104
(選用) 步驟 3：索引範例資料 ... 1109
步驟 4：分析和視覺化您的資料 ... 1110
步驟 5：清除資源和後續步驟 ... 1114
Amazon OpenSearch Service 重新命名 ... 1115
新的 API 版本 ... 1115
已重新命名的執行個體類型 ... 1116
存取政策變更 ... 1116
IAM 政策 ... 1116
SCP 政策 ... 1116
新資源類型 ... 1117
Kibana 已更名為 OpenSearch Dashboards ... 1118
已重新命名的 CloudWatch 指標 ... 1118
「帳單和成本管理」主控台的變更 ... 1119
新事件格式 ... 1120
什麼保持不變？ ... 1120
開始使用：將您的網域升級至 OpenSearch 1.x ... 1120
故障診斷 ... 1122
無法存取 OpenSearch 儀表板 ... 1122
無法存取 VPC 網域 ... 1122
叢集處於唯讀狀態 ... 1122
紅色叢集狀態 ... 1123

紅色叢集的自動修復 1125
從持續繁重的處理負載中復原 1125
黃色叢集狀態 1127
ClusterBlockException 1127
缺少可用儲存空間 1127
高 JVM 記憶體壓力 1127
在待命狀態下移轉至異地同步備份 1128
在從不待命的網域移轉至待命狀態的網域期間建立索引、索引範本或 ISM 原則 948
資料複本數量不正確 1128
JVM OutOfMemoryError 1128
叢集節點失敗 1129
超出最大碎片限制 1130
網域卡在處理狀態 1130
低 EBS 爆量餘額 1130
無法啟用稽核日誌 1131
無法關閉索引 1131
用戶端授權檢查 1131
請求調節 1131
無法對節點執行 SSH 1132
「無效的物件存放區類別」快照錯誤 1132
無效主機標頭 1132
無效的 M3 執行個體類型 1132
啟用後熱查詢停止工作 UltraWarm 1133
升級後無法降級 1133
需要所有 AWS 區域的網域摘要 1133
使用 OpenSearch 儀表板時出錯瀏覽器 1134
節點碎片和儲存扭曲 1134
索引碎片和儲存扭曲 1135
在選取 VPC 存取後未經授權的操作 1135
在建立 VPC 網域後載入停滯 1136
拒絕對 OpenSearch API 的要求 1136
無法從 Alpine Linux 連線 1137
搜尋背壓要求太多 1137
使用開發套件時發生憑證錯誤 1137
文件歷史紀錄 1139
舊版更新 1169

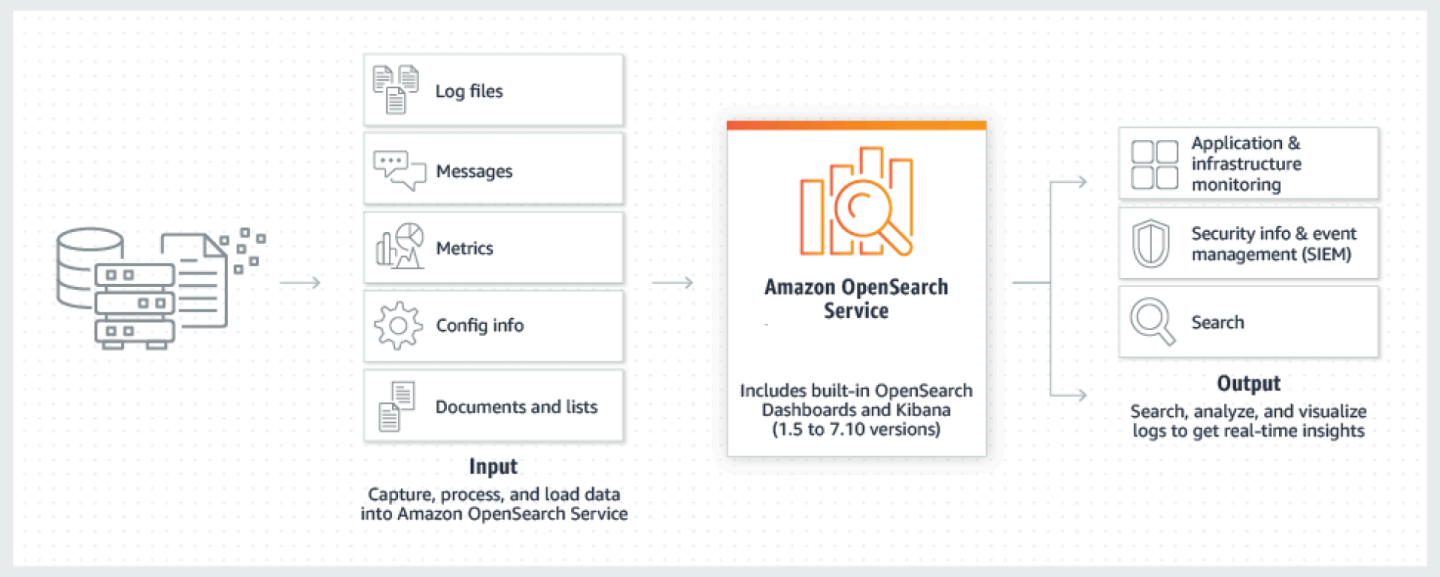
AWS 詞彙表 1172
..... mclxxiii

什麼是 Amazon OpenSearch 服務？

Amazon Ser OpenSearch vice 是一種受管服務，可讓您輕鬆部署、操作 OpenSearch 和擴展 AWS 雲端。Amazon OpenSearch 服務支持 OpenSearch 和傳統的彈性搜索OSS（最高 7.10，軟件的最終開源版本）。在您建立叢集時，您可選擇要使用的搜尋引擎。

OpenSearch是完全開放原始碼的搜尋和分析引擎，適用於日誌分析、即時應用程式監控和點擊流分析等使用案例。如需詳細資訊，請參閱OpenSearch 文件。

Amazon OpenSearch 服務會為您的 OpenSearch 叢集佈建所有資源並啟動它。它也會自動偵測並取代故障的 OpenSearch 服務節點，減少與自我管理基礎架構相關的額外負荷。您可以透過單一API呼叫或在主控台中按幾下滑鼠來擴展叢集。



若要開始使用 OpenSearch 服務，您需要建立一個 OpenSearch 服務網域，該網域等同於 OpenSearch 叢集。叢集中的每個EC2執行個體都充當一個 OpenSearch 服務節點。

您可以使用 OpenSearch Service 主控台在幾分鐘內設定和設定網域。如果您偏好以程式設計方式存取，可以使用 AWS CLI，該 AWS SDKs，或地形。

Amazon OpenSearch 服務的特點

OpenSearch 服務包括以下功能：

擴展

- 多種稱為執行個體類型的組態CPU、記憶體和儲存容量，包括符合成本效益的 Graviton 執行個體

- 多達 3 PB 的連接儲存空間
- 符合成本效益UltraWarm和冷儲存的唯讀資料

安全性

- AWS Identity and Access Management (IAM) 存取控制
- 與 Amazon VPC 和VPC安全群組輕鬆整合
- 靜態資料加密與 node-to-node 加密
- 適用於儀表板的 Amazon Cognito、HTTP基本或身SAML份驗證 OpenSearch
- 索引層級、文件層級，以及欄位層級安全
- 稽核日誌
- Dashboards 多租用

穩定性

- 適用於您資源的多個地理位置，也稱為區域和可用區域
- 在相同的兩個或三個可用區域之間配置節點 AWS 區域，稱為異地同步備份
- 卸載叢集管理任務用的專用主節點
- 備份和還原 OpenSearch 服務網域的自動快照

彈性

- SQL支援與商業智慧 (BI) 應用程式整合
- 自訂套件以改善搜尋結果

與熱門服務整合

- 使用 OpenSearch 儀表板進行資料
- 與 Amazon CloudWatch 整合以監控 OpenSearch 服務網域指標和設定警示
- 整合 AWS CloudTrail 用於稽核對 OpenSearch 服務網域的組態API呼叫
- 與 Amazon S3、亞 Amazon Kinesis 和亞 Amazon DynamoDB 整合，以便將串流資料載入服務 OpenSearch
- SNS當您的資料超過特定閾值時，Amazon 發出警示

何時使用 OpenSearch 與 Amazon OpenSearch 服務

使用下表協助您決定佈建的 Amazon OpenSearch 服務或自我管理 OpenSearch 是否適合您。

OpenSearch	Amazon OpenSearch 服務
• 您的組織願意並擁有具備正確技能的人員來手動監控和維護自我佈建的叢集。 • 您需要對程式碼進行完整的編譯層級控制。 • 您的組織偏好或獨特地使用開放原始碼軟體。 • 您有一個多雲端策略，需要不是特定於廠商的技術。 • 您的團隊能夠解決任何關鍵的生產問題。 • 您希望可以根據需要靈活使用，修改和擴展產品。 • 您希望在新功能發布後立即訪問它們。	• 您不想手動管理、監控和維護基礎結構。 • 您想要以簡單的方式來管理不斷成長的分析成本，方法是將資料分層到各個儲存層，並利用 Amazon S3 的耐用性和低成本。 • 您想利用與其他的集成的優勢 AWS 服務 例如，Amazon DocumentDB (與 MongoDB 相容性)、、和. IAM CloudWatch CloudFormation • 您希望輕鬆獲得協助 AWS Support 用於預防性維護和生產問題期間。 • 您想要利用自我修復、主動式維護、恢復和備份等功能。

Amazon OpenSearch 無服務器

Amazon OpenSearch 無伺服器是適用於 Amazon OpenSearch 服務的隨需、auto 擴展、無伺服器組態。無伺服器可免除佈建、設定和調整叢集的作業複雜性。 OpenSearch 如需詳細資訊，請參閱Amazon OpenSearch 無服務器。

Amazon OpenSearch 攝入

Amazon OpenSearch 擷取是由資料準備器提供支援的全受管資料收集器，可將即時日誌和追蹤資料傳送至 Amazon OpenSearch 服務網域和 OpenSearch 無伺服器集合。它可讓您篩選、豐富、轉換、標準化和彙總資料，以便進行下游分析和視覺化。如需詳細資訊，請參閱 Amazon OpenSearch 擷取。

彈性搜尋的 OpenSearch 支援版本

OpenSearch 服務目前支援下列 OpenSearch 版本：

- 2.15、2.13、2.11、2.9、2.7、2.5、二、三、一、一、

OpenSearch 服務也支援下列舊版彈性搜尋OSS版本：

- 7.10, 7.9, 7.8, 7.7, 7.4, 7.1
- 6.8、6.7、6.5、6.4、6.3、6.2、6.0
- 5.6、5.5、5.3、5.1
- 2.3
- 1.5

如需詳細資訊，請參閱the section called “受支援的操作”、the section called “各引擎版本的功能”及the section called “依引擎版本分類的外掛程式”。

如果您啟動新的 OpenSearch Service 專案，我們強烈建議您選擇最新的支援 OpenSearch 版本。如果您的現有網域使用較舊的 Elasticsearch 版本，您可以選擇保留網域或遷移您的資料。如需詳細資訊，請參閱the section called “升級網域”。

Amazon OpenSearch 服務的定價

對於 OpenSearch Service，您需支付執行個體每小時的使用費，以及連接至執行個體之任何EBS儲存磁碟區的累計大小。EC2標準 AWS 數據傳輸費用也適用。

不過，存在值得注意的某些資料傳輸例外狀況。如果網域使用多個可用區域，則 OpenSearch 服務不會針對可用區域之間的流量計費。在碎片分配和重新平衡期間，網域內會發生重大的資料傳輸。 OpenSearch 服務既不是米，也沒有賬單這種交通。同樣地， OpenSearch 服務不會收取 UltraWarm/冷節點和 Amazon S3 之間的資料傳輸費用。

如需完整的定價詳細資訊，請參閱 Amazon OpenSearch 服務定價。如需組態變更所產生費用的變動的資訊，請參閱the section called “組態變更的費用”。

開始使用 Amazon OpenSearch 服務

要開始使用，請註冊一個 AWS 帳戶如果你還沒有一個。使用帳戶設定完成後，請完成 Amazon OpenSearch 服務的入門教學。如果您需要更多資訊，同時要了解該服務，請參閱以下簡介主題：

- 建立網域
- 妥善調整工作負載網域大小

- 使用網域存取政策或精細定義存取控制來控制網域的存取
- 手動或從其他索引資料 AWS 服務
- 使用OpenSearch 儀表板搜尋資料並建立視覺效果

如需從自我管理 OpenSearch 叢集移轉至 OpenSearch Service 的相關資訊，請參閱the section called “移轉至OpenSearch服務”。

相關服務

OpenSearch 服務通常與以下服務一起使用：

Amazon CloudWatch

OpenSearch 服務網域會自動傳送指標，以 CloudWatch 便您監控網域健康狀況和效能。如需詳細資訊，請參閱使用 Amazon 監控 OpenSearch 叢集指標 CloudWatch。

CloudWatch 日誌也可以朝另一個方向發展。您可以配置 CloudWatch 日誌以將數據流式傳輸到 OpenSearch 服務進行分析。如需進一步了解，請參閱 the section called “從 Amazon 加載流數據 CloudWatch”。

AWS CloudTrail

使用 AWS CloudTrail 取得您帳戶之 OpenSearch 服務設定API呼叫和相關事件的歷史記錄。如需詳細資訊，請參閱使用來監控 Amazon Amazon Ser OpenSearch vice API 呼叫 AWS CloudTrail。

Amazon Kinesis

Kinesis 是一項受管服務，可即時處理大規模的串流資料。如需詳細資訊，請參閱 the section called “從 Amazon Kinesis Data Streams 中載入串流資料” 和 the section called “從 Amazon 數據防 Firehose 件加載流數據”。

Amazon Simple Storage Service (Amazon S3)

Amazon Simple Storage Service (Amazon S3) 為網際網路提供儲存服務。本指南提供與 Simple Storage Service (Amazon S3) 整合的 Lambda 範本程式碼。如需詳細資訊，請參閱the section called “從 Amazon S3 載入串流資料”。

AWS IAM

AWS Identity and Access Management (IAM) 是可用來管理服務網域存取權的 Web OpenSearch 服務。如需詳細資訊，請參閱the section called “身分和存取權管理”。

AWS Lambda

AWS Lambda 是一種運算服務，可讓您執行程式碼，而無需佈建或管理伺服器。本指南提供從 DynamoDB、Simple Storage Service (Amazon S3) 和 Kinesis 中串流資料的 Lambda 範本程式碼。如需詳細資訊，請參閱the section called “將串流資料載入 OpenSearch 服務”。

Amazon DynamoDB

Amazon DynamoDB 是全受管的無SQL資料庫服務，可提供快速且可預測的效能以及無縫的可擴展性。若要進一步瞭解將資料串流至 OpenSearch 服務，請參閱the section called “從 Amazon DynamoDB 中載入串流資料”。

Amazon QuickSight

您可以使用 Amazon QuickSight 儀表板將 OpenSearch 服務中的資料視覺化。有關更多信息，請參閱 Amazon 用 QuickSight 戶指南 QuickSight中的與 Amazon 搭配使用 Amazon OpenSearch 服務。

> **Note**
>
> OpenSearch 包括來自彈性搜索 BV 和其他源代碼的某些 APACHE 許可的彈性搜索代碼。Elasticsearch B.V. 不是該其他原始程式碼的來源。ELASTICSEARCH是彈性搜索 B.V. 的註冊商標

設置 Amazon OpenSearch 服務

主題

- 註冊一個 AWS 帳戶
- 建立具有管理存取權的使用者
- 授予許可
- 安裝和配置 AWS CLI
- 開啟 主控台

註冊一個 AWS 帳戶

如果您沒有 AWS 帳戶，請完成下列步驟來建立一個步驟。

若要註冊成為 AWS 帳戶

1. 打開https://portal.aws.amazon.com/billing/註冊。
2. 請遵循線上指示進行。

   部分註冊程序需接收來電，並在電話鍵盤輸入驗證碼。

   當您註冊一個 AWS 帳戶，一個 AWS 帳戶根使用者已建立。根使用者可以存取所有 AWS 服務 和帳戶中的資源。作為安全最佳實務，請將管理存取權指派給使用者，並且僅使用根使用者來執行需要根使用者存取權的任務。

AWS 註冊過程完成後，會向您發送確認電子郵件。您可以隨時前往 https://aws.amazon.com/並選擇「我的帳戶」，檢視目前的帳戶活動並管理您的帳戶。

建立具有管理存取權的使用者

在您註冊一個 AWS 帳戶，保護您的 AWS 帳戶根使用者，啟用 AWS IAM Identity Center，並建立系統管理使用者，這樣您就不會將 root 使用者用於日常工作。

保護您的 AWS 帳戶根使用者

1. 登入 AWS Management Console通過選擇 Root 用戶並輸入您的帳戶所有者 AWS 帳戶 電子郵件地址。在下一頁中，輸入您的密碼。

如需使用 root 使用者登入的說明，請參閱以 root 使用者身分登入 AWS 登入 使用者指南。

2. 為您的 root 使用者開啟多因素驗證 (MFA)。

   如需指示，請參閱為您的MFA裝置啟用虛擬裝置 AWS 帳戶 使用者指南中的 root IAM 使用者 (主控台)。

建立具有管理存取權的使用者

1. 啟用IAM身分識別中心。

   如需指示，請參閱啟用 AWS IAM Identity Center 中的 AWS IAM Identity Center 使用者指南。

2. 在IAM身分識別中心中，將管理存取權授與使用者。

   若要取得有關使用 IAM Identity Center 目錄 做為您的身分識別來源，請參閱以預設值設定使用者存取 IAM Identity Center 目錄 中的 AWS IAM Identity Center 使用者指南。

以具有管理存取權的使用者身分登入

- 若要使用您的 IAM Identity Center 使用者登入URL，請使用建立IAM身分識別中心使用者時傳送至您電子郵件地址的登入資訊。

  如需使用IAM身分識別中心使用者登入的說明，請參閱登入 AWS 存取入口網站 AWS 登入 使用者指南。

指派存取權給其他使用者

1. 在 IAM Identity Center 中，建立遵循套用最低權限權限的最佳作法的權限集。

   如需指示，請參閱 AWS IAM Identity Center 使用者指南。

2. 將使用者指派至群組，然後對該群組指派單一登入存取權。

   如需指示，請參閱新增群組 AWS IAM Identity Center 使用者指南。

授予許可

在生產環境中，建議您使用更精細的原則。若要進一步了解存取管理，請參閱的存取管理 AWS 《IAM 使用者指南》中的資源。

若要提供存取權，請新增權限至您的使用者、群組或角色：

- 中的使用者和群組 AWS IAM Identity Center:

  建立權限合集。遵循中建立權限集中的指示 AWS IAM Identity Center 使用者指南。
- IAM透過身分識別提供者管理的使用者：

  建立聯合身分的角色。請遵循《使用指南》中的〈為第三方身分識別提供IAM者 (同盟) 建立角色〉中的指示進行。
- IAM使用者：
  - 建立您的使用者可擔任的角色。請按照《用戶指南》中的「為IAM用戶創建角色」中的IAM說明進行操作。
  - (不建議) 將政策直接附加至使用者，或將使用者新增至使用者群組。請遵循《使用指南》中的「向使用者 (主控台) 新增權限」IAM 中的指示進行。

授與程式設計存取權

如果用戶想要與之互動，則需要以程式設計方式存取 AWS 的之外 AWS Management Console。 授與程式設計存取權的方式取決於存取的使用者類型 AWS.

若要授與使用者程式設計存取權，請選擇下列其中一個選項。

哪個使用者需要程式設計存取權？	到	By
人力身分 (在IAM身分識別中心管理的使用者)	使用臨時登入資料來簽署程式設計要求 AWS CLI, AWS SDKs，或 AWS APIs.	請依照您要使用的介面所提供的指示操作。 • 對於 AWS CLI，請參閱配置 AWS CLI 若要使用 AWS IAM Identity Center 中的 AWS Command Line Interface 使用者指南。 • 用於 AWS SDKs、工具和 AWS APIs，請參閱IAM身分識別中心驗證 AWS SDKs和工具參考指南。

哪個使用者需要程式設計存取權？	到	By
IAM	使用臨時登入資料來簽署程式設計要求 AWS CLI, AWS SDKs，或 AWS APIs.	遵循使用臨時登入資料中的指示 AWS《IAM使用者指南》中的資源。
IAM	(不建議使用) 使用長期認證來簽署程式設計要求 AWS CLI, AWS SDKs，或 AWS APIs.	請依照您要使用的介面所提供的指示操作。 • 對於 AWS CLI，請參閱「使用使用IAM者認證進行驗證」AWS Command Line Interface 使用者指南。 • 用於 AWS SDKs和工具，請參閱使用長期認證進行身份驗證 AWS SDKs和工具參考指南。 • 用於 AWS APIs，請參閱《使用指南》中的〈管理使IAM用IAM者的存取金鑰〉。

安裝和配置 AWS CLI

如果您要使用 OpenSearch 服務APIs，則必須安裝最新版本的 AWS Command Line Interface (AWS CLI). 你不需要 AWS CLI 從主控台使用 OpenSearch Service，您可以按照中的CLI步驟在不使用開始使用 Amazon OpenSearch 服務.

若要設定 AWS CLI

1. 若要安裝最新版本的 AWS CLI 如需 macOS、Linux 或視窗，請參閱安裝或更新最新版本的 AWS CLI.
2. 若要設定 AWS CLI 並安全設置您的訪問 AWS 服務，包括 OpenSearch 服務，請參閱快速配置`aws configure`。
3. 若要驗證設定，請在 DataBrew 命令提示字元中輸入下列命令。

```
aws opensearch help
```

AWS CLI 指令使用預設 AWS 區域 從您的配置中，除非您使用參數或配置文件進行設置。若要設定 AWS 區域 使用參數，您可以將`--region`參數添加到每個命令中。

若要設定 AWS 區域 使用配置文件，首先在`~/.aws/config`文件或文件中添加一個命名的配置`%UserProfile%/.aws/config`文件（適用於 Microsoft Windows）。依照 [已命名] 設定檔中的步驟執行 AWS CLI。 接下來，設置 AWS 區域 以及使用類似於下列範例中的指令的其他設定。

```
[profile opensearch]
aws_access_key_id = ACCESS-KEY-ID-OF-IAM-USER
aws_secret_access_key = SECRET-ACCESS-KEY-ID-OF-IAM-USER
region = us-east-1
output = text
```

開啟 主控台

本節中大部分的主控台導向主題都是從 Service 主控台開始。OpenSearch 如果您尚未登入 AWS 帳戶，請登入，然後開啟 OpenSearch Service 主控台並繼續下一節以繼續開始使用 OpenSearch 服務。

開始使用 Amazon OpenSearch 服務

本教學說明如何使用 Amazon OpenSearch 服務建立和設定測試網域。 OpenSearch 服務網域是叢集的代名詞 OpenSearch 。網域是指具有您指定之設定、執行個體類型、執行個體計數和儲存資源的叢集。

本教學課程將引導您完成基本步驟，以快速啟動並執行 OpenSearch Service 網域。如需更詳細的資訊，請參閱建立和管理網域和本指南內的其他主題。如需從自我管理 OpenSearch 叢集移轉至 OpenSearch Service 的相關資訊，請參閱the section called “移轉至OpenSearch服務”。

您可以使用 OpenSearch Service 主控台來完成本教學課程中的步驟， AWS CLI，或 AWS SDK。有關安裝和設置的信息 AWS CLI，請參閱 AWS Command Line Interface 用戶指南。

步驟 1：創建一個 Amazon OpenSearch 服務域

> **Important**
>
> 這是設定測試 Amazon OpenSearch 服務網域的簡明教學課程。請勿使用此程序來建立生產網域。如需相同程序的完整版本，請參閱建立和管理網域。

OpenSearch 服務網域是叢集的代名詞 OpenSearch 。網域是指具有您指定之設定、執行個體類型、執行個體計數和儲存資源的叢集。您可以使用主控台建立 OpenSearch 服務網域 AWS CLI，或 AWS SDKs.

使用主控台建立 OpenSearch 服務網域

1. 移至https://aws.amazon.com並選擇 [登入主控台]。
2. 在分析下，選擇 Amazon OpenSearch 服務。
3. 選擇 Create domain (建立網域)。
4. 提供網域名稱。本教學課程中的範例使用名稱 movies。
5. 對於網域建立方法，請選擇 [標準建立]。

> **Note**
>
> 若要使用最佳做法快速設定生產網域，您可以選擇 [輕鬆建立]。對於本教程的開發和測試目的，我們將使用標準創建。

6. 對於範本，請選擇開發/測試。
7. 對於部署選項，請選擇有待命的網域。
8. 對於 Version (版本)，選擇最新版本。
9. 目前，請忽略 [資料節點]、[暖和冷資料儲存]、[專用主節點]、[快照組態] 和 [自訂端點] 區段。
10. 為了保持本教學課程的簡易性，請使用公有存取網域。在 Network (網路) 中，選擇 Public access (公有存取)。
11. 在細微的存取控制設定中，保持選取 [啟用精細存取控制] 核取方塊。選取 [建立主要使用者] 並提供使用者名稱和密碼。
12. 目前，請忽略身份SAML驗證和 Amazon Cognito 身份驗證區段。
13. 對於 Access policy (存取政策)，選擇 Only use fine-grained access control (僅使用精細存取控制)。在本教學課程中，精細存取控制會處理驗證，而非網域存取政策。
14. 忽略其他設定，並選擇 Create (建立)。新網域通常需要 15-30 分鐘才能初始化，但視組態而定，可能需要更長的時間。網域初始化後，選擇網域以打開其組態窗格。記下 General information (一般資訊) 下的網域端點 (例如，`https://search-my-domain.us-east-1.es.amazonaws.com`)，下一步會用到。

下一個:將資料上傳至 OpenSearch 服務網域以進行索引

步驟 2：將數據上傳到 Amazon OpenSearch 服務以進行索引

> **Important**
>
> 這是一個簡潔的教程，用於將少量測試數據上傳到 Amazon OpenSearch 服務。如需有關在生產網域中上傳資料的詳細資訊，請參閱建立資料索引。

您可以使用命令列或大多數程式設計語言，將資料上傳到 OpenSearch Service 網域。

下面的示例請求使用 curl（一個通用的HTTP客戶端）簡潔和方便。如果您的存取原則指定IAM使用者或角色，像 curl 這樣的用戶端就無法執行要求簽署。若要順利完成此程序，您必須使用具有主要使用者名稱和密碼的精細存取控制，就像您在步驟 1 中設定的那樣。

您可以在 Windows 中安裝 curl，並在命令提示中使用它，但我們建議使用像 Cygwin 或 Windows Subsystem for Linux 之類的工具。macOS 和大部分 Linux 發行版本均預先安裝有 curl。

選項 1：上傳單一文件

執行以下命令，將單一文件加入到 movies 網域：

```
curl -XPUT -u 'master-user:master-user-password' 'domain-endpoint/movies/_doc/1' -d
 '{"director": "Burton, Tim", "genre": ["Comedy","Sci-Fi"], "year": 1996, "actor":
 ["Jack Nicholson","Pierce Brosnan","Sarah Jessica Parker"], "title": "Mars Attacks!"}'
 -H 'Content-Type: application/json'
```

在命令中，提供您在步驟 1 中建立的使用者名稱和密碼。

如需此命令的詳細說明，以及如何向 OpenSearch Service 發出已簽署要求，請參閱建立資料索引。

選項 2：上傳多個文件

將包含多個文件的JSON檔案上載至 OpenSearch 服務網域

1. 建立稱為 `bulk_movies.json` 的本機檔案。將以下內容貼到檔案中，並新增結尾新行：

```
{ "index" : { "_index": "movies", "_id" : "2" } }
{"director": "Frankenheimer, John", "genre": ["Drama", "Mystery", "Thriller",
 "Crime"], "year": 1962, "actor": ["Lansbury, Angela", "Sinatra, Frank", "Leigh,
 Janet", "Harvey, Laurence", "Silva, Henry", "Frees, Paul", "Gregory, James",
 "Bissell, Whit", "McGiver, John", "Parrish, Leslie", "Edwards, James", "Flowers,
 Bess", "Dhiegh, Khigh", "Payne, Julie", "Kleeb, Helen", "Gray, Joe", "Nalder,
 Reggie", "Stevens, Bert", "Masters, Michael", "Lowell, Tom"], "title": "The
 Manchurian Candidate"}
{ "index" : { "_index": "movies", "_id" : "3" } }
{"director": "Baird, Stuart", "genre": ["Action", "Crime", "Thriller"], "year":
 1998, "actor": ["Downey Jr., Robert", "Jones, Tommy Lee", "Snipes, Wesley",
 "Pantoliano, Joe", "Jacob, Ir\u00e8ne", "Nelligan, Kate", "Roebuck, Daniel",
 "Malahide, Patrick", "Richardson, LaTanya", "Wood, Tom", "Kosik, Thomas",
 "Stellate, Nick", "Minkoff, Robert", "Brown, Spitfire", "Foster, Reese",
 "Spielbauer, Bruce", "Mukherji, Kevin", "Cray, Ed", "Fordham, David", "Jett,
 Charlie"], "title": "U.S. Marshals"}
{ "index" : { "_index": "movies", "_id" : "4" } }
{"director": "Ray, Nicholas", "genre": ["Drama", "Romance"], "year": 1955, "actor":
 ["Hopper, Dennis", "Wood, Natalie", "Dean, James", "Mineo, Sal", "Backus, Jim",
 "Platt, Edward", "Ray, Nicholas", "Hopper, William", "Allen, Corey", "Birch,
 Paul", "Hudson, Rochelle", "Doran, Ann", "Hicks, Chuck", "Leigh, Nelson",
 "Williams, Robert", "Wessel, Dick", "Bryar, Paul", "Sessions, Almira", "McMahon,
 David", "Peters Jr., House"], "title": "Rebel Without a Cause"}
```

2. 在儲存檔案的本機目錄中執行下列命令，以將其上傳到 movies 網域：

```
curl -XPOST -u 'master-user:master-user-password' 'domain-endpoint/movies/_bulk' --
data-binary @bulk_movies.json -H 'Content-Type: application/x-ndjson'
```

如需有關大量檔案格式的詳細資訊，請參閱建立資料索引。

下一步：搜尋文件

步驟 3：在 Amazon OpenSearch 服務中搜索文檔

若要搜尋 Amazon OpenSearch 服務網域中的文件，請使用 OpenSearch 搜尋API。或者，您可以使用OpenSearch 儀表板來搜尋網域中的文件。

從命令列搜尋文件

執行以下命令搜尋影片網域的 mars 這個字：

```
curl -XGET -u 'master-user:master-user-password' 'domain-endpoint/movies/_search?
q=mars&pretty=true'
```

如果已在先前頁面中使用大量資料，則請嘗試改成搜尋 rebel。

您應該會看到類似以下的回應：

```
{
  "took" : 5,
  "timed_out" : false,
  "_shards" : {
    "total" : 5,
    "successful" : 5,
    "skipped" : 0,
    "failed" : 0
  },
  "hits" : {
    "total" : {
      "value" : 1,
      "relation" : "eq"
    },
```

```
    "max_score" : 0.2876821,
    "hits" : [
      {
        "_index" : "movies",
        "_type" : "_doc",
        "_id" : "1",
        "_score" : 0.2876821,
        "_source" : {
          "director" : "Burton, Tim",
          "genre" : [
            "Comedy",
            "Sci-Fi"
          ],
          "year" : 1996,
          "actor" : [
            "Jack Nicholson",
            "Pierce Brosnan",
            "Sarah Jessica Parker"
          ],
          "title" : "Mars Attacks!"
        }
      }
    ]
  }
}
```

使用 OpenSearch儀表板搜尋文件

OpenSearch 儀表板是一種流行的開源可視化工具，旨在使用 OpenSearch。它提供了一個很有幫助的使用者介面，供您搜尋和監控您的索引。

使用儀表板從 OpenSearch 服務網域搜尋文件

1. 導覽至您網域URL的 OpenSearch 儀表板。您可以URL在 OpenSearch 服務主控台的網域儀表板上找到。格式URL如下：

   ```
   domain-endpoint/_dashboards/
   ```

2. 使用您的主要使用者名稱和密碼登入。
3. 若要使用 Dashboards，您需要建立至少一個索引模式。Dashboards 使用這些模式來識別您要分析的索引。開啟左側導覽面板，選擇 Stack Management (堆疊管理)，選擇 Index Patterns (索引模式)，然後選擇 Create index pattern (建立索引模式)。對於本教學課程，輸入 movies。

4. 選擇 Next step (下一步)，然後選擇 Create index pattern (建立索引模式)。建立模式之後，您可以檢視各種文件欄位，例如 `actor` 和 `director`。
5. 返回 Index Patterns (索引模式) 頁面，並確認將 `movies` 設為預設值。如果不是，請選擇模式並選擇星形圖示以使其成為預設值。
6. 若要開始搜尋您的資料，請再次開啟左側導覽面板，然後選擇 Discover (探索)。
7. 如果上傳了單一文件，則在搜尋列中輸入 mars，或者如果上傳了多份文件，則輸入 rebel，然後按 Enter 鍵。您可以嘗試搜尋其他用語，例如演員或導演姓名。

下一步：刪除網域

步驟 4：刪除 Amazon OpenSearch 服務域

由於本教學課程的 movies 網域是用於測試目的，因此請確保在完成試驗後將其刪除，以避免產生任何費用。

從主控台刪除 OpenSearch 服務網域

1. 登錄到 Amazon 服 OpenSearch 務控制台。
2. 在 Domains (網域) 中，選取 movies 網域。
3. 選擇 Delete (刪除)，並確認刪除。

後續步驟

您現在已知道如何建立網域和索引資料，您可能想要嘗試以下一些練習：

- 進一步了解建立網域的進階選項。如需詳細資訊，請參閱建立和管理網域。
- 探索如何管理網域中的索引。如需詳細資訊，請參閱管理索引。
- 嘗試使用 Amazon OpenSearch 服務的教程之一。如需詳細資訊，請參閱教學課程。

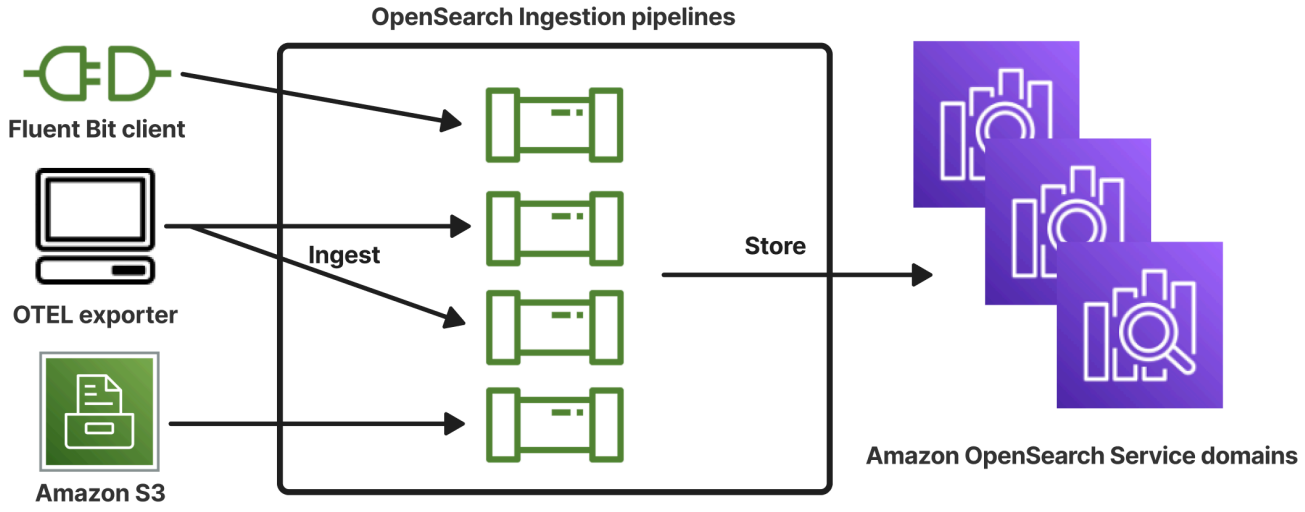
Amazon OpenSearch 攝入

Amazon OpenSearch 擷取是全受管的無伺服器資料收集器，可將即時日誌、指標和追蹤資料傳送至 Amazon OpenSearch 服務網域和無 OpenSearch 伺服器集合。

透過 OpenSearch 擷取，您不再需要使用第三方解決方案 (例如 Logstash 或 Jaeger)，將資料導入您 OpenSearch 的服務網域和無伺服器集合。 OpenSearch 您可以將資料生產者設定為將資料傳送至 OpenSearch 擷取。然後，它會自動將資料傳送至您指定的網域或集合。您也可以將 OpenSearch 擷取設定為在傳送資料之前轉換資料。

此外，透過 OpenSearch 擷取，您不必擔心佈建伺服器、管理和修補軟體，或擴展伺服器叢集的問題。您可以直接在中佈建擷取管線 AWS Management Console，而 OpenSearch 擷取會負責管理和擴展它們。

OpenSearch 攝入是 Amazon OpenSearch 服務的一個子集。它由 Data Prepper 提供支援，這是一個開放原始碼資料收集器，可篩選、豐富、轉換、標準化和彙總資料，以進行下游分析和視覺化。



主題

- 重要概念
- OpenSearch 攝入的好處
- 限制
- 支援的資料預留程式版本
- 調整管線
- OpenSearch 擷取定價
- 支援 AWS 區域

- OpenSearch 擷取配額
- 在 Amazon OpenSearch 擷取中設定角色和使用者
- Amazon OpenSearch 攝入門
- Amazon OpenSearch 擷取中的管道功能概觀
- 建立 Amazon OpenSearch 擷取管道
- 檢視亞馬遜OpenSearch擷取管道
- 更新 Amazon OpenSearch 擷取管道
- 停止和啟動亞馬遜OpenSearch擷取管道
- 刪除亞馬遜OpenSearch擷取管道
- Amazon OpenSearch 擷取管道支援的外掛程式和選項
- 使用 Amazon OpenSearch 擷取管道整合
- 使用 Amazon OpenSearch 擷取在網域和集合之間移轉資料
- 使用AWS軟體開發套件與亞馬遜OpenSearch擷取互動
- 亞馬遜OpenSearch攝入中的安全性
- 標記亞馬遜OpenSearch導入管道
- 使用亞馬遜記錄和監控亞馬遜OpenSearch攝取 CloudWatch
- Amazon OpenSearch 擷取的最佳實務

重要概念

當您開始使用 OpenSearch 擷取時，您可以從瞭解下列概念中獲益：

管道

從 OpenSearch 擷取的觀點來看，管線是指您在 OpenSearch Service 中建立的單一佈建資料收集器。您可以將其視為整個 YAML 組態檔案，其中包含一或多個子管線。如需建立擷取管線的步驟，請參閱the section called “建立管道”。

分管道

您可以在 YAML 組態檔案中定義子管線。每個子管線都是源，緩衝區，零個或多個處理器以及一個或多個接收器的組合。您可以在單一 YAML 檔案中定義多個子管線，每個子管線都有唯一的來源、處理器和接收器。若要協助監視 CloudWatch 及其他服務，建議您指定與其所有子管線不同的管線名稱。

您可以在單一 YAML 檔案中將多個子管線串連在一起，這樣一個子管線的來源就是另一個子管線，而且其接收器是第三個子管線。如需範例，請參閱the section called “OpenTelemetry 收藏家”。

來源

子管線的輸入元件。它定義了管道消耗記錄的機制。來源可以透過 HTTPS 接收事件，或從外部端點 (例如 Amazon S3) 讀取事件來使用事件。有兩種類型的源：基於推送和基於拉取。以推送為基礎的來源 (例如 HTTP 和 oTel 記錄) 會將記錄串流至擷取端點。提取式來源，例如 oTel 追蹤和 S3，可從來源提取資料。

Processors

在將記錄發佈到接收器之前，可以將記錄過濾、轉換和豐富成所需格式的中繼處理單元。處理器是管線的選用元件。如果您未定義處理器，則會以來源中定義的格式發佈記錄。您可以擁有多個處理器。配管會依照您定義的順序執行處理器。

接收

子管線的輸出元件。它定義了子管線將記錄發佈到的一個或多個目的地。 OpenSearch 擷取支援 OpenSearch 服務網域做為接收器。它還支持子管道作為接收器。這表示您可以將單一 OpenSearch 擷取管線 (YAML 檔案) 中的多個子管線串接在一起。自我管理 OpenSearch 叢集不支援做為接收器。

緩衝區

處理器的一部分，充當源和水槽之間的層。您無法在管道中手動配置緩衝區。 OpenSearch 擷取會使用預設的緩衝區組態。

路由

處理器的一部分，允許管線作者僅將符合特定條件的事件傳送到不同的接收器。

有效的子管線定義必須包含來源和接收器。如需有關每個配管元素的詳細資訊，請參閱組態參照。

OpenSearch 攝入的好處

OpenSearch 擷取具有下列主要優點：

- 無需手動管理自我佈建的管道。
- 根據您定義的容量限制自動擴展管道。
- 利用安全性和錯誤修補程式，讓您的管道保持最新狀態。
- 提供將管線連接到虛擬私有雲 (VPC) 的選項，以獲得額外的安全性。

- 允許您停止和啟動管道以控制成本。
- 提供熱門使用案例的管線組態藍圖，協助您更快速地啟動並執行。
- 可讓您透過各種 AWS SDK 和 OpenSearch 擷取 API，以程式設計方式與管道互動。
- 支援 Amazon 中的效能監控 CloudWatch 和 CloudWatch 日誌中的錯誤記錄。

限制

OpenSearch 擷取有下列限制：

- 您只能將資料擷取至執行 OpenSearch 1.0 或更新版本的網域，或彈性搜尋 6.8 或更新版本的網域。如果您使用 oTel 追蹤來源，我們建議您使用 Elasticsearch 7.9 或更新版本，以便您可以使用儀表板外掛程式OpenSearch 。
- 如果管線正在寫入 VPC 內的 OpenSearch Service 網域，則必須在與該網域相同 AWS 區域 的管道中建立管線。
- 您只能在管線定義中配置單一資料來源。
- 您無法將自我管理 OpenSearch 叢集指定為接收器。
- 您無法將自訂端點指定為接收器。您仍然可以寫入已啟用自訂端點的網域，但必須指定其標準端點。
- 您無法將選擇加入區域內的資源指定為來源或接收器。
- 您可以在配管組態中包含的參數有一些限制。如需詳細資訊，請參閱 the section called “組態需求和限制”。

支援的資料預留程式版本

OpenSearch 擷取目前支援下列主要版本的資料準備器：

- 2.x

建立管線時，請使用必要的`version`選項來指定要使用的主要資料準備器版本。例如，`version: "2"`. OpenSearch 擷取會擷取該主要版本的最新受支援次要版本，並使用該版本佈建管道。如需詳細資訊，請參閱 the section called “指定管線版本”。

目前， OpenSearch 擷取管道是使用 2.7 版的資料準備器佈建。如需詳細資訊，請參閱 2.7 版本說明。如需每個「資料預留程式」版本中的功能和錯誤修正的相關資訊，請參閱「發行版本」頁面。OpenSearch 擷取不支援特定主要版本的每個次要版本。

當您更新管線的 YAML 組態檔案時，如果支援新的次要版本的資料準備器， OpenSearch 擷取會自動將管線升級至管線組態中指定的主要版本的最新受支援次要版本。例如，您可能已`version: "2"`在管線組態中，而 OpenSearch 擷取最初佈建了 2.6.0 版的管道。新增對版本 2.7.0 的支援並變更管線組態時， OpenSearch 擷取會將管道升級至 2.7.0 版。此過程可讓您的管道保持最新狀態，並獲得最新的錯誤修復和性能改進。 OpenSearch 除非您在管線組態中手動變更`version`選項，否則擷取無法更新管道的主要版本。如需詳細資訊，請參閱 the section called “更新管道”。

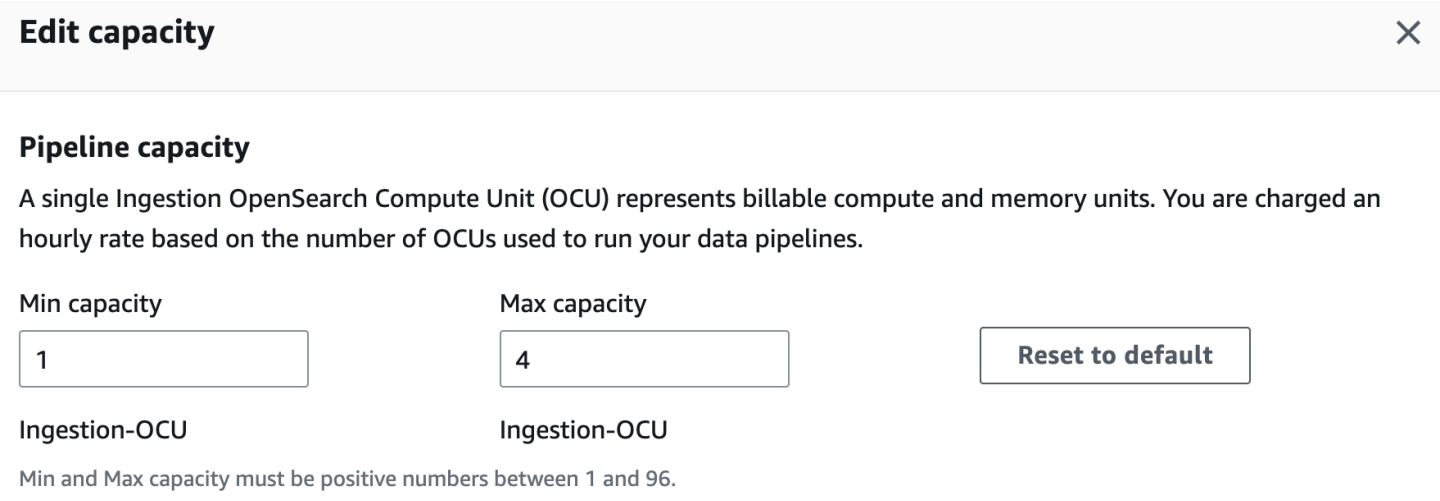
調整管線

您不需要自行佈建和管理管道容量。 OpenSearch 擷取會根據您指定的最小和最大擷取 OpenSearch 運算單元 (擷取 OCU)，自動根據您估計的工作負載擴展管道容量。

每個擷取的 OCU 都是大約 8 GiB 記憶體和 2 個 vCPUs 的組合。您可以指定管線的最小和最大 OCU 值， OpenSearch 擷取會根據這些限制自動擴展管線容量。

您可以指定下列值：

- 最小容量 — 管道可以將容量降低到這個擷取 OCU 數目。指定的最小容量也是配管的起始容量。
- 最大容量 — 管道可將容量增加到這個擷取 OCU 數目。



請確定管線的最大容量足以處理工作負載峰值，並且最小容量足夠低，以便在管線不忙碌時將成本降至最低。 OpenSearch 擷取會根據您的設定自動調整管線的擷取 OCU 數目，以處理擷取工作負載。在任何特定時間，您只需為管道正在積極使用的擷取 OCU 付費。

分配給您的 OpenSearch 擷取管道的容量會根據管道的處理需求和用戶端應用程式產生的負載來擴展和縮減。當容量受到限制時， OpenSearch 擷取會透過配置更多運算單元 (記憶體的 GiB) 來擴展。當您的管道正在處理較小的工作負載，或完全不處理資料時，它可以縮減到設定的最小擷取 OCU。

您至少可以指定 1 個擷取 OCU、無狀態管線最多 96 個擷取 OCU，以及可設定狀態管線的最多 48 個擷取 OCU。對於以推送為基礎的來源，我們建議至少 2 個擷取 OCU。啟用持續緩衝時，您可以指定至少 2 個，最多 384 個擷取 OCU。

指定具有單一來源、簡單 grok 模式和接收器的標準記錄管線，每個運算單元每秒最多可支援 2 MiB。對於具有多個處理器的更複雜的日誌管道，每個運算單元可能支援較少的擷取負載。根據管道容量和資源使用率， OpenSearch 擷取擴展程序會啟動。

為了確保高可用性，擷取 OCU 會分散在可用區域 (AZ) 之間。AZ 的數量取決於您指定的最小容量。

例如，如果您指定至少 2 個運算單位，則在任何指定時間使用中的擷取 OCU 都會平均分佈在 2 個 AZ 上。如果您指定至少 3 個或更多個運算單位，擷取 OCU 會平均分佈在 3 個 AZ 上。建議您至少佈建兩個擷取 OCU，以確保擷取管線的 99.9% 可用性。

當管道位於`Create failed`、`Creating`和`Stopped`狀態時，您不會針對擷取 OCU 付費。`Deleting`

如需設定和擷取管線容量設定的指示，請參閱the section called “建立管道”。

OpenSearch 擷取定價

在任何特定時間，無論是否有資料流經管線，您都只需支付配置給管線的擷取 OCU 數量付費。OpenSearch 擷取可根據使用情況擴展或縮減管道容量，立即容納您的工作負載。

如需完整的定價詳細資訊，請參閱 Amazon OpenSearch 服務定價。

支援 AWS 區域

OpenSearch 您可以在中使用 AWS 區域 該 OpenSearch 服務的子集中提供擷取。如需支援區域的清單，請參閱 AWS 一般參考. OpenSearch

OpenSearch 擷取配額

如需 OpenSearch 擷取資源的預設配額清單，請參閱 Amazon OpenSearch 服務配額。

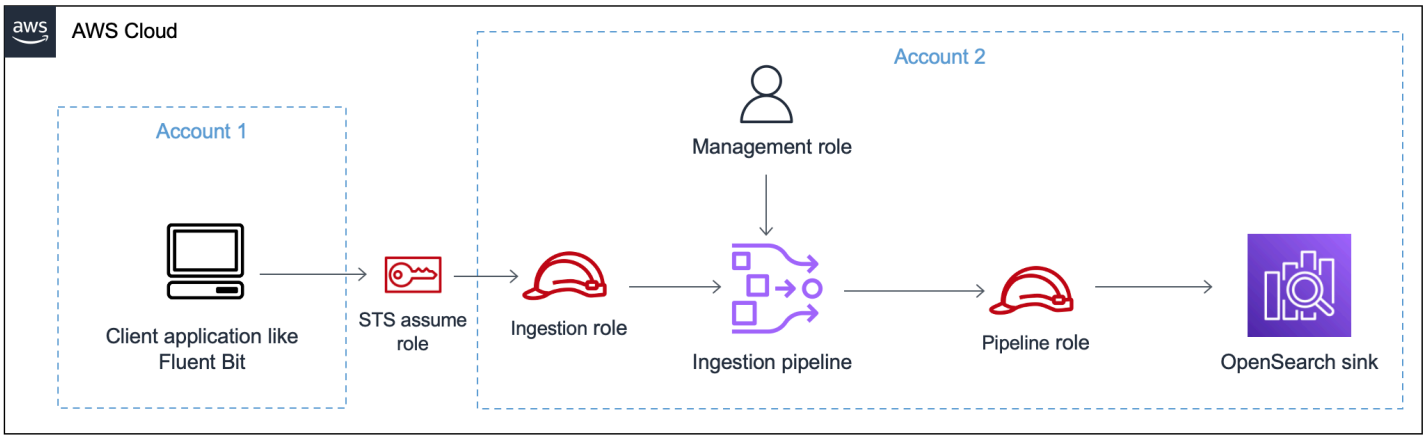
在 Amazon OpenSearch 擷取中設定角色和使用者

Amazon OpenSearch Intection 使用各種許可模型和IAM角色，以允許來源應用程式寫入管道，並允許管道寫入接收器。在開始擷取資料之前，您需要根據使用案例建立具有特定權限的一或多個IAM角色。

至少需要下列角色才能設定成功的管道。

名稱	描述
管理角色	管理管道的任何主體 (通常是「管道管理員」) 都需要管理存取權，其中包括`osis:CreatePipeline` 和等權限`osis:UpdatePipeline` 。這些權限可讓使用者管理管道，但不一定要將資料寫入管道。
管線角色	您在管線YAML組態中指定的管線角色提供了必要的權限，讓管線寫入網域或集合接收器以及從提取式來源讀取。如需詳細資訊，請參閱下列主題： • the section called “授與管道對網域的存取權” • the section called “授予管道對集合的存取權”
擷取角色	擷取角色包含管線資源的`osis:Ingest` 權限。此權限允許以推送為基礎的來源將資料內嵌到管線中。

下圖示範典型的管道設定，其中 Amazon S3 或 Fluent Bit 等資料來源正在寫入不同帳戶中的管道。在此情況下，用戶端必須擔任擷取角色才能存取管線。如需詳細資訊，請參閱the section called “跨帳戶擷取”。



如需簡單的設定指南，請參閱the section called “教學課程：將資料擷取至網域”。

主題

- the section called “管理角色”
- the section called “擷取角色”
- the section called “管線角色”
- the section called “跨帳戶擷取”

管理角色

除了建立和修改管線所需的基本`osis:*`權限之外，您還需要管線角色資源的`iam:PassRole`權限。任何接 AWS 服務 受角色的人都必須使用此權限。 OpenSearch 每次需要將資料寫入接收器時，擷取都會擔任該角色。這有助於管理員確保只有核准的使用者可以使用授與權限的角色來設定 OpenSearch 擷取。如需詳細資訊，請參閱授與使用者將角色傳遞給 AWS 服務.

如果您使用的是 AWS Management Console (使用藍圖並稍後檢查管線)，則需要下列權限才能建立和更新管道：

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Resource":"*",
         "Action":[
            "osis:CreatePipeline",
            "osis:GetPipelineBlueprint",
            "osis:ListPipelineBlueprints",
            "osis:GetPipeline",
            "osis:ListPipelines",
            "osis:GetPipelineChangeProgress",
            "osis:ValidatePipeline",
            "osis:UpdatePipeline"
         ]
      },
      {
         "Resource":[
            "arn:aws:iam::your-account-id:role/pipeline-role"
         ],
         "Effect":"Allow",
         "Action":[
            "iam:PassRole"
```

```
            ]
        }
    ]
}
```

如果您使用的是 AWS CLI (未預先驗證管道或使用藍圖)，則需要下列權限才能建立和更新管道：

```
{
    "Version":"2012-10-17",
    "Statement":[
        {
            "Effect":"Allow",
            "Resource":"*",
            "Action":[
                "osis:CreatePipeline",
                "osis:UpdatePipeline"
            ]
        },
        {
            "Resource":[
                "arn:aws:iam::your-account-id:role/pipeline-role"
            ],
            "Effect":"Allow",
            "Action":[
                "iam:PassRole"
            ]
        }
    ]
}
```

管線角色

管道需要某些權限才能寫入其接收器。這些權限取決於接收器是 OpenSearch 服務網域還是 OpenSearch 無伺服器集合。

此外，管道可能需要從來源應用程式提取權限 (如果來源是提取式外掛程式)，以及寫入 S3 無效字母佇列的權限 (如果已設定)。

主題

- 寫入網域接收器
- 寫入收藏水槽

- 寫入無效字母佇列

寫入網域接收器

OpenSearch 擷取管線需要寫入設定為接收器的 OpenSearch Service 網域的權限。這些權限包括描述網域並向其傳送HTTP要求的功能。

為了讓管道具有寫入接收器的必要權限，請先建立具有所需權限的 AWS Identity and Access Management (IAM) 角色。這些權限對於公用和VPC管線來說是相同的。然後，在網域存取原則中指定管線角色，以便網域可以接受來自管線的寫入要求。

最後，將角色指定ARN為配管組態中 sts_role_arn 選項的值：

```
version: "2"
source:
  http:
    ...
processor:
  ...
sink:
  - opensearch:
      ...
      aws:
        sts_role_arn: arn:aws:iam::your-account-id:role/pipeline-role
```

如需完成上述每個步驟的指示，請參閱允許管道存取網域。

寫入收藏水槽

OpenSearch 擷取管線需要權限，才能寫入設定為其接收器的 OpenSearch 無伺服器集合。這些權限包括描述集合並向其傳送HTTP要求的功能。

首先，建立具有對所有資源 (*) `aoss:BatchGetCollection` 權限的IAM角色。然後，將此角色包含在資料存取原則中，並提供建立索引、更新索引、描述索引和寫入集合中文件的權限。最後，將角色指定ARN為配管組態中 sts_role_arn 選項的值。

如需完成上述每個步驟的指示，請參閱允許管道存取集合。

寫入無效字母佇列

如果將管線設定為寫入無效字母佇列 (DLQ)，則必須在組態中包含該`sts_role_arn`選項。DLQ此角色中包含的權限可讓管道存取您指定為DLQ事件目的地的 S3 儲存貯體。

您必須`sts_role_arn`在所有配管元件中使用相同的配管元件。因此，您必須將個別的權限原則附加至提供DLQ存取權的管線角色。至少必須允許角色對值區資源`S3:PutObject`執行動作：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "WriteToS3DLQ",
      "Effect": "Allow",
      "Action": "s3:PutObject",
      "Resource": "arn:aws:s3:::my-dlq-bucket/*"
    }
  ]
}
```

然後，您可以在管線的DLQ組態中指定角色：

```
  ...
  sink:
    opensearch:
      dlq:
        s3:
          bucket: "my-dlq-bucket"
          key_path_prefix: "dlq-files"
          region: "us-west-2"
          sts_role_arn: "arn:aws:iam::your-account-id:role/pipeline-role"
```

擷取角色

OpenSearch 擷取目前支援的所有來源外掛程式 (S3 除外) 都使用以推送為基礎的架構。這表示來源應用程式會將資料推送至管線，而不是從來源提取資料的管線。

因此，您必須授與來源應用程式所需的權限，才能將資料 OpenSearch 擷取至 Intection 管線。簽署請求的角色至少必須獲得`osis:Ingest`動作的權限，以允許其將資料傳送至管線。公用端點和VPC管線端點需要相同的權限。

下列範例原則可讓相關聯的主體將資料內嵌至名為`my-pipeline`的單一管線：

```
{
  "Version": "2012-10-17",
```

```
  "Statement": [
    {
      "Sid": "PermitsWriteAccessToPipeline",
      "Effect": "Allow",
      "Action": "osis:Ingest",
      "Resource": "arn:aws:osis:region:your-account-id:pipeline/pipeline-name"
    }
  ]
}
```

如需詳細資訊，請參閱the section called “使用管道整合”。

跨帳戶擷取

您可能需要將資料從不同的管道內嵌 AWS 帳戶，例如應用程式帳戶。若要設定跨帳戶擷取，請在與管道相同的帳戶內定義擷取角色，並在擷取角色和應用程式帳戶之間建立信任關係：

```
{
  "Version": "2012-10-17",
  "Statement": [{
     "Effect": "Allow",
     "Principal": {
       "AWS": "arn:aws:iam::external-account-id:root"
      },
     "Action": "sts:AssumeRole"
  }]
}
```

然後，將您的應用程式設定為擔任擷取角色。應用程式帳戶必須授與管線帳戶中擷取角色的應用程式角色AssumeRole權限。

如需詳細步驟和IAM原則範例，請參閱the section called “提供跨帳戶擷取存取”。

授予 Amazon OpenSearch 擷取管道對網域的存取權

Amazon OpenSearch 擷取管道需要權限才能寫入設定為接收器的 OpenSearch 服務網域。若要提供存取權，您可以設定具有限制性權限原則的 AWS Identity and Access Management (IAM) 角色，以限制對管線傳送資料之網域的存取。例如，您可能想要將擷取管道限制為僅支援其使用案例所需的網域和索引。

在管線組態中指定角色之前，必須先設定適當的信任關係，然後授與其網域存取原則中網域的存取權。

主題

- 步驟 1：建立管線角色
- 步驟 2：在網域存取原則中包含管線角色
- 步驟 3：對應管線角色 (僅適用於使用精細存取控制的網域)
- 步驟 4：指定管線組態中的角色

步驟 1：建立管線角色

您在管線組態的 sts_role_arn 參數中指定的角色必須具有附加的權限原則，允許其將資料傳送至網域接收器。它還必須具有允許 OpenSearch 擷取擔任角色的信任關係。如需有關如何將原則附加至角色的指示，請參閱IAM使用指南中的新增IAM身分識別權限。

下列範例原則示範您可以在管線組態的 sts_role_arn 角色中為其寫入單一網域提供的最低權限：

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "es:DescribeDomain",
            "Resource": "arn:aws:es:*:your-account-id:domain/*"
        },
        {
            "Effect": "Allow",
            "Action": "es:ESHttp*",
            "Resource": "arn:aws:es:*:your-account-id:domain/domain-name/*"
        }
    ]
}
```

如果您打算重複使用角色來寫入多個網域，您可以將網域名稱取代為萬用字元 (*)，以使原則更廣泛。

角色必須具有下列信任關係，以允許 OpenSearch 擷取擔任管線角色：

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
```

```
        "Principal":{
           "Service":"osis-pipelines.amazonaws.com"
        },
        "Action":"sts:AssumeRole"
      }
   ]
}
```

此外，我們建議您在原則中加入aws:SourceAccount和aws:SourceArn條件索引鍵，以保護自己免於混淆的副問題。來源帳戶是管線的擁有者。

例如，您可以將下列條件區塊新增至政策：

```
"Condition": {
    "StringEquals": {
        "aws:SourceAccount": "your-account-id"
    },
    "ArnLike": {
        "aws:SourceArn": "arn:aws:osis:region:your-account-id:pipeline/*"
    }
}
```

步驟 2：在網域存取原則中包含管線角色

為了讓管線將資料寫入網域，網域必須具有允許 sts_role_arn 管線角色存取該原則的網域層級存取原則。

下列範例網域存取原則允許您在上一個步驟中建立的名為pipeline-role的管線角色將資料寫入名為的網域ingestion-domain：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::your-account-id:role/pipeline-role"
      },
      "Action": ["es:DescribeDomain", "es:ESHttp*"],
      "Resource": "arn:aws:es:region:your-account-id:domain/domain-name/*"
    }
  ]
```

```
}
```

步驟 3：對應管線角色 (僅適用於使用精細存取控制的網域)

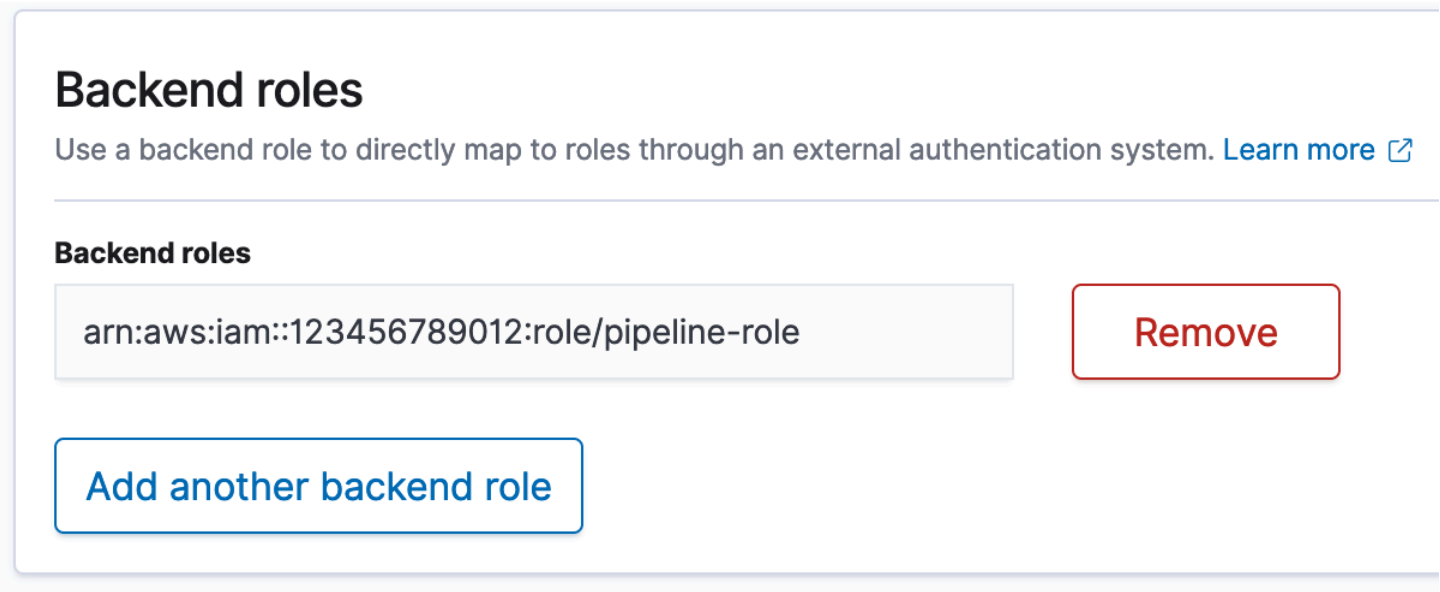
如果您的網域使用精細的存取控制來進行驗證，您需要採取額外的步驟來提供管道存取網域。這些步驟會根據您的網域組態而有所不同：

案例 1：不同的主要角色和管道角色 — 如果您使用 IAM Amazon Resource Name (ARN) 作為主要使用者，且該名稱與管道角色 (`sts_role_arn`) 不同，則需要將管道角色對應至 OpenSearch`all_access`後端角色。這基本上會將管線角色新增為額外的主要使用者。如需詳細資訊，請參閱其他主要使用者。

案例 2：內部使用者資料庫中的主要使用者 — 如果您的網域使用內部使用者資料庫中的主要使用者，並針對 OpenSearch 儀表板使用HTTP基本驗證，則無法將主要使用者名稱和密碼直接傳遞至管線組態。相反地，您需要將管線角色 (`sts_role_arn`) 對應至後 OpenSearch`all_access`端角色。這基本上會將管線角色新增為額外的主要使用者。如需詳細資訊，請參閱其他主要使用者。

案例 3：相同的主要角色和管線角色 (不常見) — 如果您以主要使用者IAMARN身分使用，而且與您ARN用作管線角色 (`sts_role_arn`) 相同，則不需要採取任何進一步的動作。管線具有寫入網域所需的權限。這種情況並不常見，因為大多數環境都使用管理員角色或其他角色做為主要角色。

下圖顯示如何將管線角色對應至後端角色：



步驟 4：指定管線組態中的角色

若要成功建立管線，您必須將在步驟 1 中建立的管線角色指定為配管組態中的 sts_role_arn 參數。管線會擔任此角色，以便簽署要求至 OpenSearch 服務網域接收器。

在`sts_role_arn`欄位中，指定ARNIAM管線角色的：

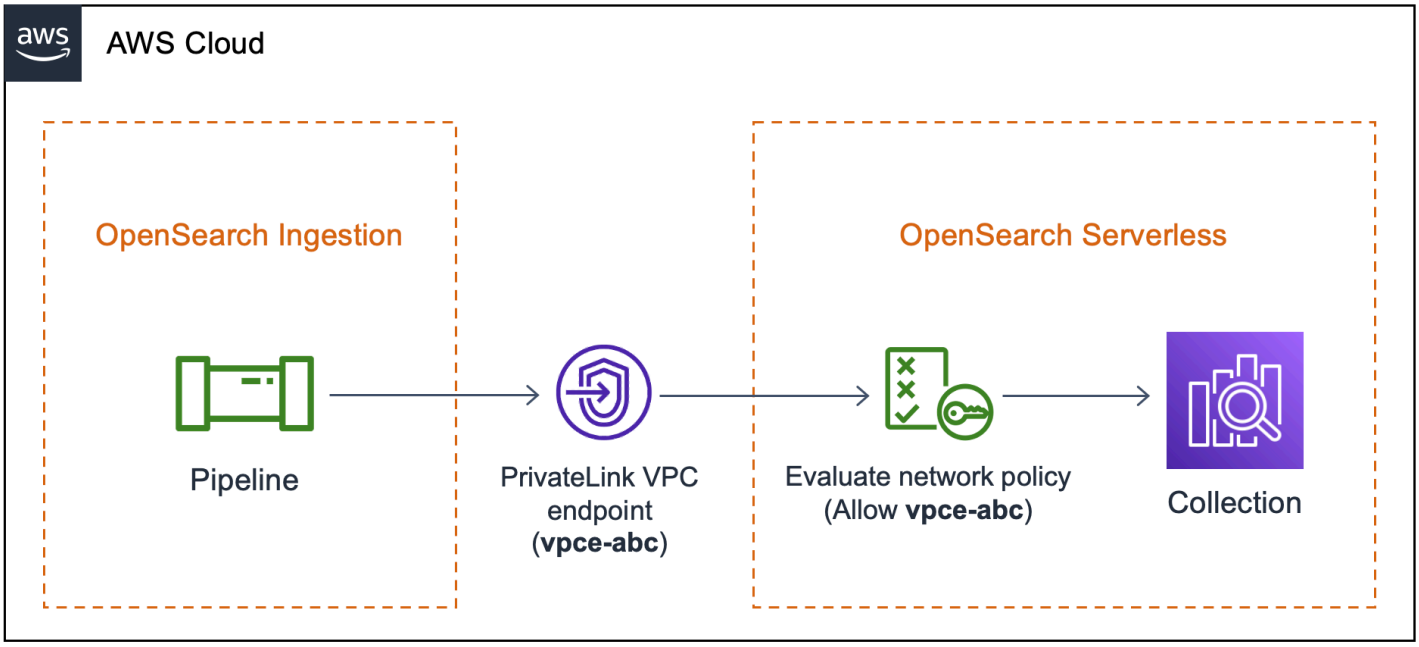
```
version: "2"
log-pipeline:
  source:
    http:
      path: "/${pipelineName}/logs"
  processor:
    - grok:
        match:
          log: [ "%{COMMONAPACHELOG}" ]
  sink:
    - opensearch:
        hosts: [ "https://search-domain-name.us-east-1.es.amazonaws.com" ]
        index: "my-index"
        aws:
          region: "region"
          sts_role_arn: "arn:aws:iam::your-account-id:role/pipeline-role"
```

如需必要和不受支援參數的完整參考，請參閱〈〉the section called “支持的插件和選項”。

授與 Amazon OpenSearch 擷取管道對集合的存取權

Amazon OpenSearch 擷取管道可以寫入 OpenSearch 無伺服器公開收集或VPC集合。若要提供對集合的存取權，您可以設定具有授與集合存取權的權限原則的 AWS Identity and Access Management (IAM) 管線角色。在管線組態中指定角色之前，必須先使用適當的信任關係對其進行設定，然後透過資料存取原則授與其資料存取權限。

在管道建立期間， OpenSearch 擷取會在管 AWS PrivateLink 線和 OpenSearch 無伺服器集合之間建立連線。來自管線的所有流量都會經過此VPC端點，並路由至集合。若要存取集合，必須透過網路存取原則授與端點存取集合的存取權。



主題

- 提供對管道的網路存取
- 步驟 1：建立管線角色
- 步驟 2：建立集合
- 步驟 3：建立管道

提供對管道的網路存取

您在 OpenSearch 無伺服器中建立的每個集合至少都有一個與其相關聯的網路存取原則。網路存取原則會決定集合是否可透過網際網路從公用網路存取，或是否必須以私密方式存取。如需有關網路原則的詳細資訊，請參閱the section called “網路存取”。

在網路存取原則中，您只能指定 OpenSearch 無伺服器管理VPC的端點。如需詳細資訊，請參閱the section called “VPC 端點”。 OpenSearch 不過，為了讓管線寫入集合，原則也必須授與存取權給 Intection 在管線和集合之間自動建立的VPC端點。因此，當您建立具有 OpenSearch 無伺服器收集接收器的管線時，必須使用此`network_policy_name`選項提供相關聯網路原則的名稱。

例如：

```
...
sink:
   - opensearch:
```

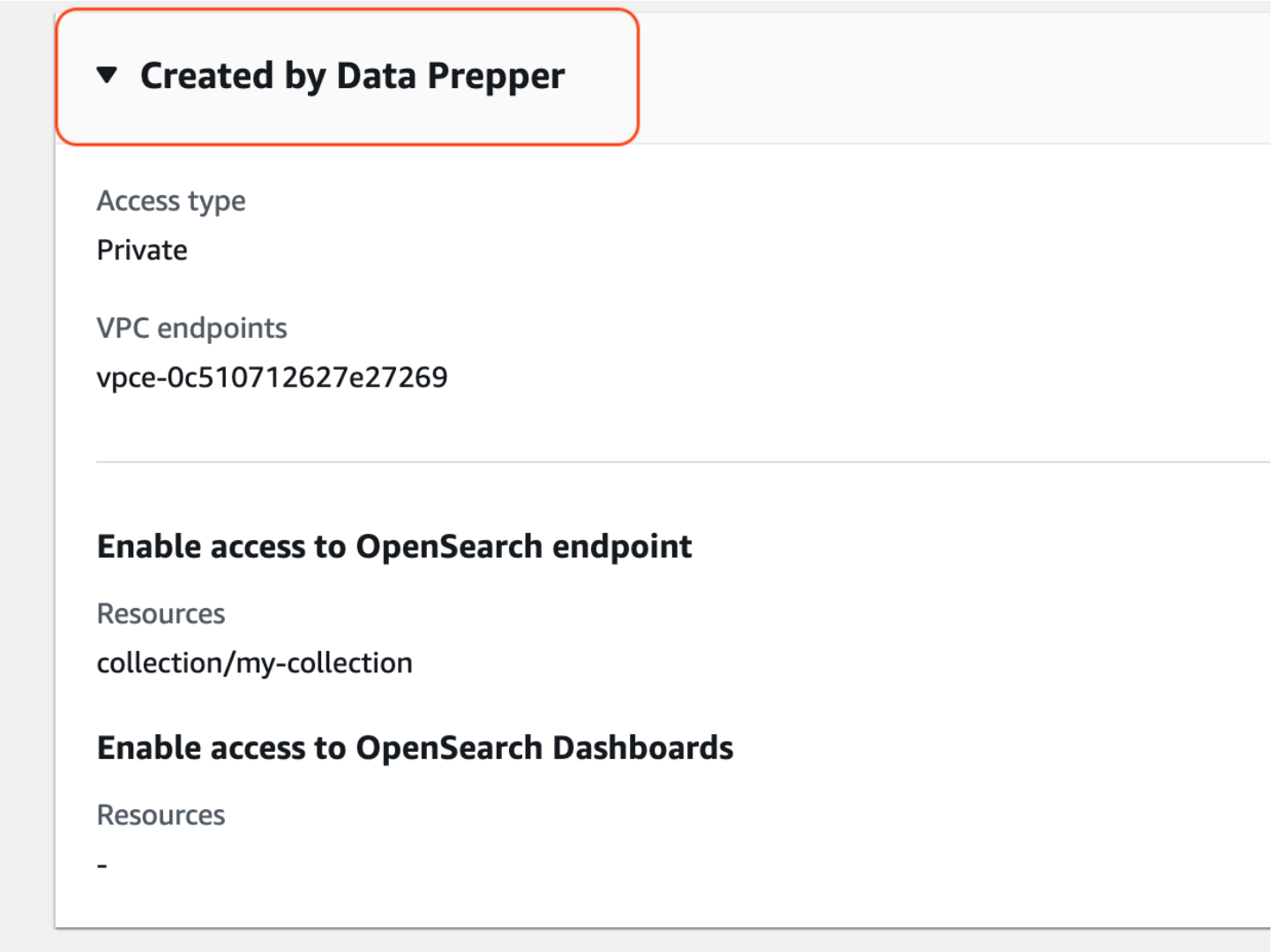
```
        hosts: [ "https://collection-id.region.aoss.amazonaws.com" ]
        index: "my-index"
         aws:
           serverless: true
           serverless_options:
             network_policy_name: "network-policy-name"
```

在管線建立期間，OpenSearch 擷取會檢查指定的網路原則是否存在。如果它不存在，OpenSearch 擷取會建立它。如果確實存在，OpenSearch 擷取會透過向其新增規則來更新它。此規則會授與對連接管線和集合之VPC端點的存取權。

例如：

```
{
   "Rules":[
      {
         "Resource":[
            "collection/my-collection"
         ],
         "ResourceType":"collection"
      }
   ],
   "SourceVPCEs":[
      "vpce-0c510712627e27269" # The ID of the VPC endpoint that OpenSearch Ingestion
 creates between the pipeline and collection
   ],
   "Description":"Created by Data Prepper"
}
```

在主控台中，OpenSearch 擷取新增至網路原則的任何規則都會命名為「由資料準備器建立」：



> **Note**
>
> 一般而言，指定集合的公開存取權限的規則會覆寫指定私人存取權的規則。因此，如果原則已經設定了公開存取權， OpenSearch 擷取新增的這個新規則並不會實際變更原則的行為。如需詳細資訊，請參閱the section called “政策優先順序”。

如果您停止或刪除管線， OpenSearch 擷取會刪除管線和集合之間的VPC端點。它也會修改網路策略，將VPC端點從允許的端點清單中移除。如果您重新啟動管道，它會重新建立VPC端點，並使用端點 ID 重新更新網路政策。

步驟 1：建立管線角色

您在管線組態的 sts_role_arn 參數中指定的角色必須具有附加的權限原則，允許其將資料傳送至收集接收器。它還必須具有允許 OpenSearch 擷取擔任角色的信任關係。如需有關如何將原則附加至角色的指示，請參閱IAM使用指南中的新增IAM身分識別權限。

下列範例原則示範您可以在管線組態的 sts_role_arn 角色中為其寫入集合提供的最低權限：

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Statement1",
            "Effect": "Allow",
            "Action": [
                "aoss:APIAccessAll",
                "aoss:BatchGetCollection",
                "aoss:CreateSecurityPolicy",
                "aoss:GetSecurityPolicy",
                "aoss:UpdateSecurityPolicy"
            ],
            "Resource": "*"
        }
    ]
}
```

角色必須具有下列信任關係，以允許 OpenSearch 擷取假設它：

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "osis-pipelines.amazonaws.com"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

步驟 2：建立集合

使用下列設定建立 OpenSearch 無伺服器集合。如需建立集合的指示，請參閱the section called “建立集合”。

資料存取政策

為集合建立資料存取原則，以授與管線角色所需的權限。例如：

```
[
  {
    "Rules": [
      {
        "Resource": [
          "index/collection-name/*"
        ],
        "Permission": [
          "aoss:CreateIndex",
          "aoss:UpdateIndex",
          "aoss:DescribeIndex",
          "aoss:WriteDocument"
        ],
        "ResourceType": "index"
      }
    ],
    "Principal": [
      "arn:aws:iam::account-id:role/pipeline-role"
    ],
    "Description": "Pipeline role access"
  }
]
```

> **Note**
>
> 在`Principal`元素中，指定您在上一個步驟中建立的管道角色的 Amazon 資源名稱 (ARN)。

網路存取政策

建立集合的網路存取原則。您可以將資料內嵌到公開集合或集VPC合中。例如，下列原則提供對單一 OpenSearch 無伺服器管理VPC端點的存取權：

```
[
   {
      "Description":"Rule 1",
      "Rules":[
         {
            "ResourceType":"collection",
            "Resource":[
               "collection/collection-name"
            ]
         }
      ],
      "AllowFromPublic": false,
      "SourceVPCEs":[
         "vpce-050f79086ee71ac05"
      ]
   }
]
```

> **Important**
>
> 您必須在管線組態的`network_policy_name`選項內指定網路原則的名稱。在管道建立時，OpenSearch 擷取會更新此網路原則，以允許存取管道和集合之間自動建立的VPC端點。如需管線組態範例，請參閱步驟 3。如需詳細資訊，請參閱the section called “提供對管道的網路存取”。

步驟 3：建立管道

最後，建立一個管道，您可以在其中指定管線角色和集合詳細資訊。管線會擔任此角色，以便將要求簽署至 OpenSearch 無伺服器收集接收器。

請確定執行下列操作：

- 針對此`hosts`選項，指定您在步驟 2 中建立的集合的端點。
- 針對該`sts_role_arn`選項，指定您在步驟 1 中建立的管道角色的 Amazon 資源名稱 (ARN)。
- 將`serverless`選項設定為`true`。
- 將選`network_policy_name`項設定為附加至集合的網路原則名稱。 OpenSearch 擷取會自動更新此網路原則，以允許從管線和集合之間建立的網路原則進行存取。VPC如需詳細資訊，請參閱the section called “提供對管道的網路存取”。

```
version: "2"
log-pipeline:
  source:
    http:
        path: "/log/ingest"
  processor:
    - date:
        from_time_received: true
        destination: "@timestamp"
  sink:
    - opensearch:
        hosts: [ "https://collection-id.region.aoss.amazonaws.com" ]
        index: "my-index"
        aws:
          serverless: true
          serverless_options:
            network_policy_name: "network-policy-name" # If the policy doesn't exist, a
 new policy is created.
          region: "us-east-1"
          sts_role_arn: "arn:aws:iam::account-id:role/pipeline-role"
```

如需必要和不受支援參數的完整參考，請參閱〈〉the section called “支持的插件和選項”。

Amazon OpenSearch 攝入門

Amazon OpenSearch 擷取支援將資料擷取到受管OpenSearch服務網域和OpenSearch無伺服器集合。下列教學課程會帶您逐步了解每個使用案例的基本步驟，並且執行。

> **Note**
>
> 如果您未設定正確的權限，管線建立將會失敗。在建立管道之前，請參閱以the section called “設定角色和使用者”進一步瞭解所需角色。

主題

- 教學課程：使用 Amazon OpenSearch 擷取將資料導入網域
- 教學課程：使用 Amazon OpenSearch 擷取將資料擷取到集合

教學課程：使用 Amazon OpenSearch 擷取將資料導入網域

本教學說明如何使用 Amazon OpenSearch 擷取設定簡單管道，並將資料擷取至 Amazon OpenSearch 服務網域。管線是 OpenSearch 擷取佈建和管理的資源。您可以使用管道來篩選、豐富、轉換、標準化和彙總資料，以便在 OpenSearch Service 中進行下游分析和視覺化。

本教程將引導您完成基本步驟，以快速啟動和運行管道。如需詳細資訊，請參閱the section called “建立管道”。

在本教學課程中，您會完成下列步驟：

1. 建立管線角色。
2. 建立網域。
3. 建立管線。
4. 擷取一些範例資料。

在教學課程中，您將建立下列資源：

- 一個名為的管道 `ingestion-pipeline`
- 管道將寫入的名稱`ingestion-domain`網域
- 為了寫入網域`PipelineRole`，管道將假定為了寫入網域的IAM角色

所需的許可

若要完成本教學課程，您必須擁有正確的IAM權限。您的使用者或角色必須具有以下最低權限的附加以身分識別為基礎的原則。這些權限可讓您建立管線角色 (`iam:Create`)、建立或修改網域 (`es:*`)，以及使用管線 (`osis:*`)。

此外，管線角色資源需要`iam:PassRole`權限。此權限可讓您將管線角色傳遞給 OpenSearch 擷取，以便將資料寫入網域。

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Resource":"*",
```

```
        "Action":[
           "osis:*",
           "iam:Create*",
           "es:*"
        ]
     },
     {
        "Resource":[
           "arn:aws:iam::your-account-id:role/PipelineRole"
        ],
        "Effect":"Allow",
        "Action":[
           "iam:PassRole"
        ]
     }
   ]
}
```

步驟 1：建立管線角色

首先，建立管線為了存取 OpenSearch 服務網域接收器而假設的角色。您將在本教學課程稍後的管線設定中包含此角色。

若要建立管線角色

1. 在開啟 AWS Identity and Access Management 主控台https://console.aws.amazon.com/iamv2/。
2. 選擇 [原則]，然後選擇 [建立原則]。
3. 在本教學課程中，您會將資料擷取到名為的網域中`ingestion-domain`，您將在下一個步驟中建立該網域。選取下列原則JSON並貼到編輯器中。更換為您`{your-account-id}`的帳戶 ID，並視需要修改「地區」。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "es:DescribeDomain",
            "Resource": "arn:aws:es:us-east-1:your-account-id:domain/ingestion-
domain"
        },
        {
            "Effect": "Allow",
```

```
            "Action": "es:ESHttp*",
            "Resource": "arn:aws:es:us-east-1:your-account-id:domain/ingestion-
domain/*"
        }
    ]
}
```

如果您想要將資料寫入現有網域，請以您的網域名稱取代`ingestion-domain`。

> **Note**
>
> 為了在本教程中簡單起見，我們使用了相當廣泛的訪問策略。但是，在生產環境中，我們建議您對管道角色套用限制更嚴格的存取原則。如需提供最低必要權限的範例原則，請參閱the section called “授與管道對網域的存取權”。

4. 選擇 [下一步]，選擇 [下一步]，然後命名原則管線原則。
5. 選擇 建立政策。
6. 接下來，建立角色並將原則附加至該角色。選擇 Roles (角色)，然後選擇 Create role (建立角色)。
7. 選擇 [自訂信任原則]，然後將下列原則貼到編輯器中：

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Principal":{
            "Service":"osis-pipelines.amazonaws.com"
         },
         "Action":"sts:AssumeRole"
      }
   ]
}
```

8. 選擇 Next (下一步)。然後搜尋並選取管線原則 (您剛建立的)。
9. 選擇 [下一步] 並命名角色PipelineRole。
10. 選擇建立角色。

請記住角色的 Amazon 資源名稱 (ARN) (例如，`arn:aws:iam::your-account-id:role/PipelineRole`)。當您建立管道時，您將需要它。

步驟 2：建立網域

接下來，建立一個名為將資料擷取`ingestion-domain`到的網域。

導覽至https://console.aws.amazon.com/aos/家中的 Amazon OpenSearch 服務主控台，並建立符合下列需求的網域：

- 正在執行 OpenSearch 1.0 或更新版本，或彈性搜尋 7.4 或更新版本
- 使用公共訪問
- 不使用細粒度的訪問控制

> **Note**
>
> 這些要求是為了確保在本教程中的簡單性。在生產環境中，您可以設定具有VPC存取權和/或使用精細存取控制的網域。若要使用精細的存取控制，請參閱對應管線角色。

網域必須具有授與權限的存取原則`PipelineRole`，這是您在上一個步驟中建立的權限。管線將扮演此角色 (在管線組態中名為 sts_role_arn)，以便將資料傳送至服務網域接收器。 OpenSearch

請確定網域具有下列網域層級存取原則，這些原則會授與網域的`PipelineRole`存取權。使用您自己的地區和帳戶 ID 取代：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::your-account-id:role/PipelineRole"
      },
      "Action": "es:*",
      "Resource": "arn:aws:es:us-east-1:your-account-id:domain/ingestion-domain/*"
    }
  ]
}
```

如需建立網域層級存取原則的詳細資訊，請參閱以資源為基礎的存取原則。

如果您已經建立了網域，請修改其現有存取原則，將上述權限提供給`PipelineRole`。

> **Note**
>
> 記住網域端點 (例如，`https://search-ingestion-domain.us-east-1.es.amazonaws.com`)。您將在下一步中使用它來配置管道。

步驟 3：建立管道

現在您擁有具有適當存取權限的網域和角色，您可以建立管道。

建立管道

1. 在 Amazon OpenSearch 服務主控台內，從左側導覽窗格中選擇管道。
2. 選擇 Create pipeline (建立管道)。
3. 選取空白管線，然後選擇選取藍圖。
4. 命名管線擷取管線，並將容量設定保留為其預設值。
5. 在本教程中，您將創建一個簡單的子管道，稱為`log-pipeline`使用 Http 源插件。此外掛程式接受JSON陣列格式的記錄資料。您將指定單一 OpenSearch Service 網域做為接收器，並將所有資料擷取到`application_logs`索引中。

   在「管線組態」下，將下列YAML組態貼到編輯器中：

```
version: "2"
log-pipeline:
  source:
    http:
      path: "/${pipelineName}/test_ingestion_path"
  processor:
    - date:
        from_time_received: true
        destination: "@timestamp"
  sink:
    - opensearch:
        hosts: [ "https://search-ingestion-domain.us-east-1.es.amazonaws.com" ]
        index: "application_logs"
        aws:
          sts_role_arn: "arn:aws:iam::your-account-id:role/PipelineRole"
          region: "us-east-1"
```

> **Note**
>
> `path`此選項會指定擷取的URI路徑。此選項對於以提取為基礎的來源是必需的。如需詳細資訊，請參閱the section called “指定擷取路徑”。

6. 以您在上一節中建立 (或修改) 之網域的端點取代。`hosts` URL將`sts_role_arn`參數取代為ARN的`PipelineRole`。
7. 選擇驗證管線，並確定驗證成功。
8. 為了簡化本教學課程，請設定管線的公用存取權。在 Network (網路) 中，選擇 Public access (公有存取)。

   如需有關配置VPC存取權的資訊，請參閱the section called “設定管線的 VPC 存取”。
9. 保持日誌發佈啟用狀態，以防您在完成本教學課程時遇到任何問題。如需詳細資訊，請參閱the section called “監控管道日誌”。

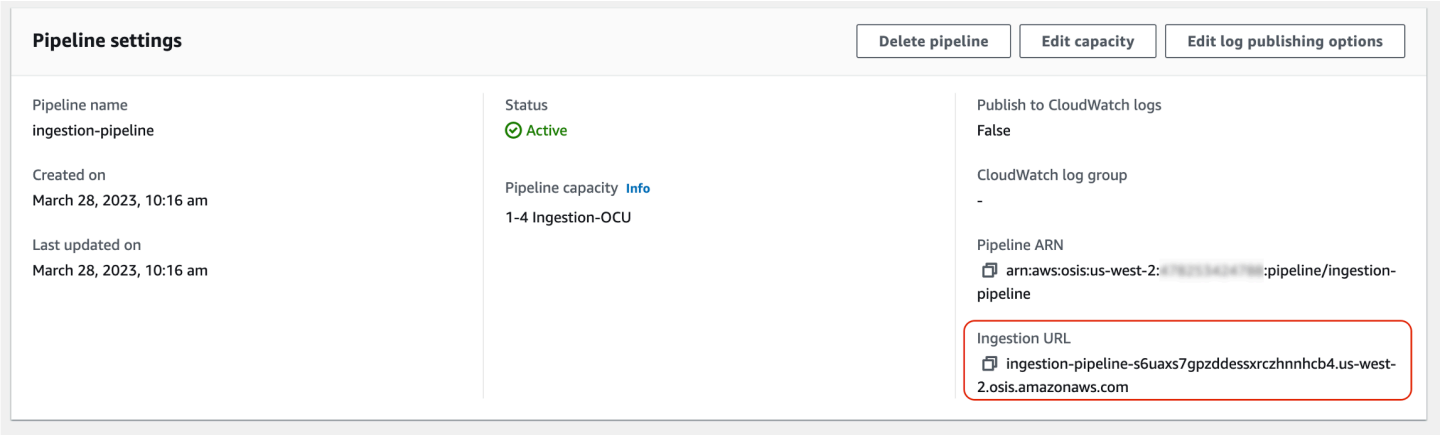
   指定下列記錄群組名稱：`/aws/vendedlogs/OpenSearchIngestion/ingestion-pipeline/audit-logs`
10. 選擇 Next (下一步)。檢閱管線組態，然後選擇「建立管線」。管道需要 5-10 分鐘才能成為活動狀態。

步驟 4：擷取一些範例資料

當管道狀態為時`Active`，您就可以開始將資料擷取到其中。您必須使用簽名版本 4 將所有HTTP請求簽署到管道。使用郵遞員或 awscurl 等HTTP工具將一些數據發送到管道。就像將資料直接索引到網域一樣，將資料導入管道一律需要IAM角色或IAM存取金鑰和秘密金鑰。

> **Note**
>
> 簽署要求的主體必須具有`osis:Ingest`IAM權限。

首先，URL從「管道設定」 頁面取得擷取：



然後，擷取一些範例資料。下列要求會使用 awscurl 將單一記錄檔傳送至索引application_logs：

```
awscurl --service osis --region us-east-1 \
    -X POST \
    -H "Content-Type: application/json" \
    -d
 '[{"time":"2014-08-11T11:40:13+00:00","remote_addr":"122.226.223.69","status":"404","request":
 http://www.k2proxy.com//hello.html HTTP/1.1","http_user_agent":"Mozilla/4.0
 (compatible; WOW64; SLCC2;)"}]' \
    https://pipeline-endpoint.us-east-1.osis.amazonaws.com/log-pipeline/
test_ingestion_path
```

您應該會看到200 OK回應。如果您收到驗證錯誤，可能是因為您從不同的帳戶擷取資料，而不是管道所在。請參閱 the section called “修正權限問題”。

現在，查詢索application_logs引以確保您的日誌項目已成功導入：

```
awscurl --service es --region us-east-1 \
     -X GET \
     https://search-ingestion-domain.us-east-1.es.amazonaws.com/application_logs/
_search | json_pp
```

範例回應：

```
{
   "took":984,
   "timed_out":false,
   "_shards":{
      "total":1,
```

```
      "successful":5,
      "skipped":0,
      "failed":0
   },
   "hits":{
      "total":{
         "value":1,
         "relation":"eq"
      },
      "max_score":1.0,
      "hits":[
         {
            "_index":"application_logs",
            "_type":"_doc",
            "_id":"z6VY_IMBRpceX-DU6V4O",
            "_score":1.0,
            "_source":{
               "time":"2014-08-11T11:40:13+00:00",
               "remote_addr":"122.226.223.69",
               "status":"404",
               "request":"GET http://www.k2proxy.com//hello.html HTTP/1.1",
               "http_user_agent":"Mozilla/4.0 (compatible; WOW64; SLCC2;)",
               "@timestamp":"2022-10-21T21:00:25.502Z"
            }
         }
      ]
   }
}
```


修正權限問題

如果您遵循教學課程中的步驟，但在嘗試擷取資料時仍然看到驗證錯誤，可能是因為寫入管線的角色與管線本身 AWS 帳戶 不同。在這種情況下，您需要建立並擔任特別可讓您擷取資料的角色。如需說明，請參閱 the section called “提供跨帳戶擷取存取”。

相關資源

本教學課程介紹了擷取單一文件的簡單使用案例。HTTP在生產環境中，您將設定用戶端應用程式 (例如 Fluent Bit、Kubernetes 或 OpenTelemetry 收集器)，以便將資料傳送至一或多個管線。您的管道可能會比本教學課程中的簡單範例更複雜。

若要開始設定用戶端和擷取資料，請參閱下列資源：

- 建立和管理管道
- 設定用戶端以將資料傳送至 OpenSearch 擷取
- 資料預留程式文件

教學課程：使用 Amazon OpenSearch 擷取將資料擷取到集合

本教學說明如何使用 Amazon OpenSearch 擷取設定簡單管道，並將資料擷取至 Amazon OpenSearch 無伺服器集合。管線是 OpenSearch 擷取佈建和管理的資源。您可以使用管道來篩選、豐富、轉換、標準化和彙總資料，以便在 OpenSearch Service 中進行下游分析和視覺化。

如需示範如何將資料內嵌至已佈建 OpenSearch 服務網域的教學課程，請參閱the section called “教學課程：將資料擷取至網域”。

在本教學課程中，您會完成下列步驟：

1. 建立管線角色。
2. 建立集合。
3. 建立管線。
4. 擷取一些範例資料。

在教學課程中，您將建立下列資源：

- 一個名為的管道 `ingestion-pipeline-serverless`
- 一個名為管`ingestion-collection`道將寫入的集合
- 為了寫入集合`PipelineRole`，管道將承擔的IAM角色

所需的許可

若要完成本教學課程，您必須擁有正確的IAM權限。您的使用者或角色必須具有以下最低權限的附加以身分識別為基礎的原則。這些權限可讓您建立管線角色 (`iam:Create*`)、建立或修改集合 (`aoss:*`)，以及使用管線 (`osis:*`)。

此外，管線角色資源需要`iam:PassRole`權限。此權限可讓您將管線角色傳遞給 OpenSearch 擷取，以便將資料寫入集合。

```
{
```

```
    "Version":"2012-10-17",
    "Statement":[
       {
          "Effect":"Allow",
          "Resource":"*",
          "Action":[
             "osis:*",
             "iam:Create*",
             "aoss:*"
          ]
       },
       {
          "Resource":[
             "arn:aws:iam::your-account-id:role/PipelineRole"
          ],
          "Effect":"Allow",
          "Action":[
             "iam:PassRole"
          ]
       }
    ]
}
```

步驟 1：建立管線角色

首先，建立管道為了存取 OpenSearch 無伺服器收集接收器而假設的角色。您將在本教學課程稍後的管線設定中包含此角色。

若要建立管線角色

1. 在開啟 AWS Identity and Access Management 主控台https://console.aws.amazon.com/iamv2/。
2. 選擇 [原則]，然後選擇 [建立原則]。
3. 選取下列原則JSON並貼到編輯器中。相應地修改集合ARN和名稱。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "aoss:BatchGetCollection",
        "aoss:APIAccessAll"
      ],
```

```
      "Effect": "Allow",
      "Resource": "arn:aws:aoss:us-east-1:your-account-id:collection/collection-id"
    },
    {
      "Action": [
        "aoss:CreateSecurityPolicy",
        "aoss:GetSecurityPolicy",
        "aoss:UpdateSecurityPolicy"
      ],
      "Effect": "Allow",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aoss:collection": "collection-name"
        }
      }
    }
  ]
}
```

4. 選擇 [下一步]，選擇 [下一步]，然後命名原則collection-pipeline-policy。
5. 選擇 建立政策。
6. 接下來，建立角色並將原則附加至該角色。選擇 Roles (角色)，然後選擇 Create role (建立角色)。
7. 選擇 [自訂信任原則]，然後將下列原則貼到編輯器中：

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Principal":{
            "Service":"osis-pipelines.amazonaws.com"
         },
         "Action":"sts:AssumeRole"
      }
   ]
}
```

8. 選擇 Next (下一步)。然後搜索並選擇 collection-pipeline-policy（您剛剛創建的）。
9. 選擇 [下一步] 並命名角色PipelineRole。
10. 選擇建立角色。

請記住角色的 Amazon 資源名稱 (ARN) (例如，`arn:aws:iam::your-account-id:role/PipelineRole`)。當您建立管道時，您將需要它。

步驟 2：建立集合

接下來，創建一個集合以將數據導入其中。我們將命名集合`ingestion-collection`。

1. 導航到https://console.aws.amazon.com/aos/家中的 Amazon OpenSearch 服務控制台。
2. 從左側導覽列中選擇「商品系列」，然後選擇「建立
3. 為集合擷取集合命名。
4. 在「安全性」中選擇「標準建立」
5. 在 [網路存取設定] 下，將存取類型變更為 [公用]。
6. 將其他所有設定保留為預設值，然後選擇 Next (下一步)。
7. 現在，設定集合的資料存取政策。對於定義方法，請選擇下列原則JSON並貼到編輯器中。這項政策做了兩件事：

   - 允許管線角色寫入集合。
   - 可讓您從集合中讀取。稍後，在您將一些範例資料導入管線之後，您將查詢集合，以確保資料已成功擷取並寫入索引。

```
[
  {
    "Rules": [
      {
        "Resource": [
          "index/ingestion-collection/*"
        ],
        "Permission": [
          "aoss:CreateIndex",
          "aoss:UpdateIndex",
          "aoss:DescribeIndex",
          "aoss:ReadDocument",
          "aoss:WriteDocument"
        ],
        "ResourceType": "index"
      }
    ],
    "Principal": [
      "arn:aws:iam::your-account-id:role/PipelineRole",
      "arn:aws:iam::your-account-id:role/Admin"
```

```
    ],
    "Description": "Rule 1"
  }
]
```

8. 取代`Principal`元素。第一個主體應該指定您建立的管線角色。第二個應該指定一個用戶或角色，以便稍後用於查詢集合。
9. 選擇 Next (下一步)。命名存取原則 pipeline-domain-access，然後再次選擇 [下一步]。
10. 檢閱集合組態，然後選擇 Submit (提交)。

當集合處於作用中狀態時，請記下「 OpenSearch 端點」(Endpoint) 下的端點 (例如，`https://{collection-id}.us-east-1.aoss.amazonaws.com`)。當您建立管道時，您將需要它。

步驟 3：建立管道

現在您已經擁有了具有適當存取權限的集合和角色，您可以建立管線。

建立管道

1. 在 Amazon OpenSearch 服務主控台內，從左側導覽窗格中選擇管道。
2. 選擇 Create pipeline (建立管道)。
3. 選取空白管線，然後選擇選取藍圖。
4. 命名管線無伺服器擷取，並將容量設定保留為其預設值。
5. 在本教程中，我們將創建一個簡單的子管道，稱`log-pipeline`為使用HTTP源插件。該插件接受數JSON組格式的日誌數據。我們將指定單一 OpenSearch 無伺服器集合做為接收器，並將所有資料擷取到索引中`my_logs`。

   在「管線組態」下，將下列YAML組態貼到編輯器中：

```
version: "2"
log-pipeline:
  source:
    http:
      path: "/${pipelineName}/test_ingestion_path"
  processor:
    - date:
        from_time_received: true
        destination: "@timestamp"
```

```
sink:
  - opensearch:
      hosts: [ "https://collection-id.us-east-1.aoss.amazonaws.com" ]
      index: "my_logs"
      aws:
        sts_role_arn: "arn:aws:iam::your-account-id:role/PipelineRole"
        region: "us-east-1"
        serverless: true
```

6. 將其取hostsURL代為您在上一節中建立的集合的端點。將sts_role_arn參數取代為ARN的PipelineRole。(可選) 修改region.
7. 選擇驗證管線，並確定驗證成功。
8. 為了簡化本教學課程，我們將設定管線的公用存取權限。在 Network (網路) 中，選擇 Public access (公有存取)。

   如需有關配置VPC存取權的資訊，請參閱the section called “設定管線的 VPC 存取”。
9. 保持日誌發佈啟用狀態，以防您在完成本教學課程時遇到任何問題。如需詳細資訊，請參閱the section called “監控管道日誌”。

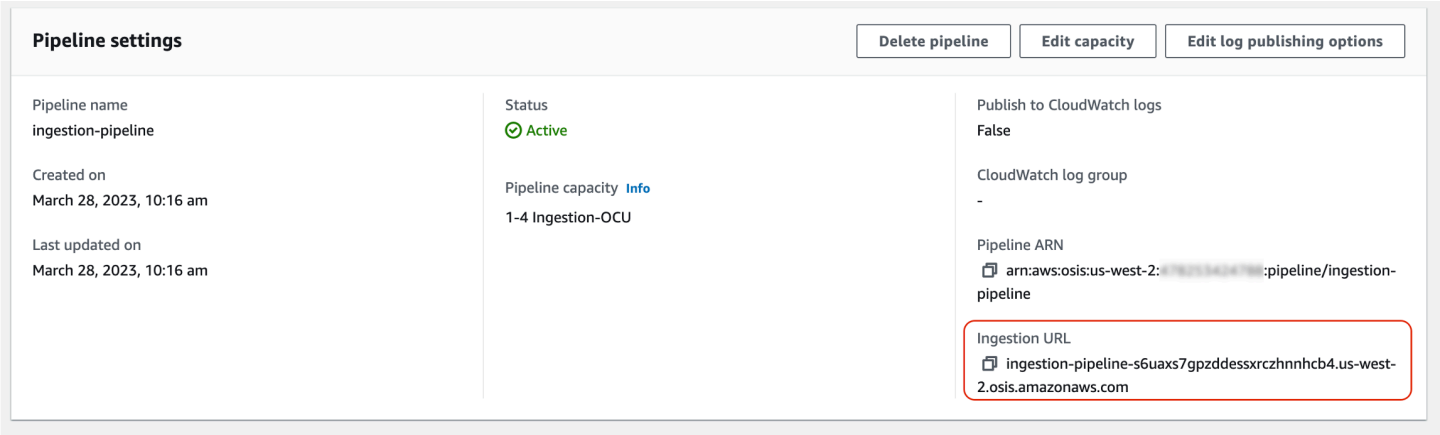
   指定下列記錄群組名稱：/aws/vendedlogs/OpenSearchIngestion/serverless-ingestion/audit-logs
10. 選擇 Next (下一步)。檢閱管線組態，然後選擇「建立管線」。管道需要 5-10 分鐘才能成為活動狀態。

步驟 4：擷取一些範例資料

當管道狀態為時Active，您就可以開始將資料擷取到其中。您必須使用「簽名版本 4」將所有HTTP請求簽署到管道。使用郵遞員或 awscurl 等HTTP工具將一些數據發送到管道。與將資料直接索引至集合一樣，將資料擷取到管道中始終需要IAM角色或IAM存取金鑰和秘密金鑰。

> **Note**
>
> 簽署要求的主體必須具有osis:IngestIAM權限。

首先，URL從「管道設定」 頁面取得擷取：



然後，擷取一些範例資料。下列範例要求會使用 awscurl 將單一記錄檔傳送至索引my_logs：

```
awscurl --service osis --region us-east-1 \
    -X POST \
    -H "Content-Type: application/json" \
    -d
 '[{"time":"2014-08-11T11:40:13+00:00","remote_addr":"122.226.223.69","status":"404","request":
 http://www.k2proxy.com//hello.html HTTP/1.1","http_user_agent":"Mozilla/4.0
 (compatible; WOW64; SLCC2;)"}]' \
    https://pipeline-endpoint.us-east-1.osis.amazonaws.com/log-pipeline/
test_ingestion_path
```

您應該會看到200 OK回應。

現在，查詢索my_logs引以確保記錄項目已成功擷取：

```
awscurl --service aoss --region us-east-1 \
     -X GET \
     https://collection-id.us-east-1.aoss.amazonaws.com/my_logs/_search | json_pp
```

範例回應：

```
{
   "took":348,
   "timed_out":false,
   "_shards":{
      "total":0,
      "successful":0,
      "skipped":0,
      "failed":0
   },
```

```
    "hits":{
       "total":{
          "value":1,
          "relation":"eq"
       },
       "max_score":1.0,
       "hits":[
          {
             "_index":"my_logs",
             "_id":"1%3A0%3ARJgDvIcBTy5m12xrKE-y",
             "_score":1.0,
             "_source":{
                "time":"2014-08-11T11:40:13+00:00",
                "remote_addr":"122.226.223.69",
                "status":"404",
                "request":"GET http://www.k2proxy.com//hello.html HTTP/1.1",
                "http_user_agent":"Mozilla/4.0 (compatible; WOW64; SLCC2;)",
                "@timestamp":"2023-04-26T05:22:16.204Z"
             }
          }
       ]
    }
}
```

相關資源

本教學課程介紹了擷取單一文件的簡單使用案例。HTTP在生產環境中，您將設定用戶端應用程式 (例如 Fluent Bit、Kubernetes 或 OpenTelemetry 收集器)，以便將資料傳送至一或多個管線。您的管道可能會比本教學課程中的簡單範例更複雜。

若要開始設定用戶端和擷取資料，請參閱下列資源：

- 建立和管理管道
- 設定用戶端以將資料傳送至 OpenSearch 擷取
- 資料預留程式文件

Amazon OpenSearch 擷取中的管道功能概觀

Amazon OpenSearch 擷取佈建管道，其中包含一個來源、一個緩衝區、零個或多個處理器，以及一或多個接收器。擷取管線由資料準備程式作為資料引擎提供支援。如需配管各種元件的概觀，請參閱the section called “重要概念”。

以下各節提供 Amazon OpenSearch 擷取中一些最常用功能的概觀。

> **Note**
>
> 這不是可用於配管的特徵的詳盡清單。如需所有可用管線功能的完整文件，請參閱資料準備程式文件。請注意，「 OpenSearch 擷取」會對您可以使用的外掛程式和選項設置一些限制。如需詳細資訊，請參閱the section called “支持的插件和選項”。

主題

- 持久緩衝
- 分割
- 鏈接
- 無效字母佇列
- 索引管理
- 電子nd-to-end 確認
- 源背壓

持久緩衝

持續性緩衝區會將您的資料儲存在跨多個可用區域的磁碟型緩衝區中，以增加資料的耐久性。您可以使用持續緩衝來擷取所有支援的以推送為基礎的來源的資料，而不需要設定獨立緩衝區。這些包括HTTP日誌，跟踪和指標的 OpenTelemetry 來源。

若要啟用持續性緩衝，請在建立或更新管線時選擇「啟用持續緩衝區」。如需詳細資訊，請參閱the section called “建立管道”。 OpenSearch 擷取會根據您為管線指定的擷取 OpenSearch 運算單位 (擷取 OCUs)，自動判斷所需的緩衝容量。

如果您為管線啟用持續性緩衝，則來源的要求承載大小上限為 1 MB，HTTP來源則為 OpenTelemetry 4 MB。如果您未啟用持續性緩衝，最大承載大小為 20 MB。您無法修改要求承載上限。

依預設，管道會使用 a AWS 擁有的金鑰 來加密緩衝區資料。這些管道不需要管線角色的任何其他權限。或者，您可以指定客戶管理的金鑰，並將下列IAM權限新增至管道角色：

```
{
    "Version": "2012-10-17",
    "Statement": [
```

```
        {
            "Sid": "KeyAccess",
            "Effect": "Allow",
            "Action": [
              "kms:Decrypt",
              "kms:GenerateDataKeyWithoutPlaintext"
            ],
            "Resource": "arn:aws:kms:{region}:{aws-account-
id}:key/1234abcd-12ab-34cd-56ef-1234567890ab"
        }
    ]
}
```

如需更多資訊，請參閱 AWS Key Management Service 開發人員指南中的客戶受管金鑰。

> **Note**
>
> 如果您停用持續性緩衝，您的管道將會更新為完全在記憶體內緩衝上執行。

分割

您可以設定 OpenSearch 擷取管線，將內送事件分割為子管線，讓您可以在相同的內送事件上執行不同類型的處理。

下列範例配管會將傳入事件分割為兩個子配管。每個子管道都使用自己的處理器來豐富和操作數據，然後將數據發送到不同的 OpenSearch 索引。

```
version: "2"
log-pipeline:
  source:
    http:
    ...
  sink:
    - pipeline:
        name: "logs_enriched_one_pipeline"
    - pipeline:
        name: "logs_enriched_two_pipeline"

logs_enriched_one_pipeline:
  source:
    log-pipeline
```

```
  processor:
   ...
  sink:
    - opensearch:
        # Provide a domain or collection endpoint
        # Enable the 'serverless' flag if the sink is an OpenSearch Serverless
 collection
        aws:
          ...
        index: "enriched_one_logs"

logs_enriched_two_pipeline:
  source:
    log-pipeline
  processor:
   ...
  sink:
    - opensearch:
        # Provide a domain or collection endpoint
        # Enable the 'serverless' flag if the sink is an OpenSearch Serverless
 collection
        aws:
          ...
          index: "enriched_two_logs"
```

鏈接

您可以將多個子管線鏈結在一起，以便在區塊中執行資料處理和擴充。換句話說，您可以在一個子管道中使用某些處理能力來豐富傳入的事件，然後將其發送到另一個子管道以使用不同的處理器進行額外的豐富，最後將其發送到接收器。 OpenSearch

在下列範例中，`log_pipeline`子管線會使用一組處理器來豐富傳入的記錄事件，然後將事件傳送至名為的 OpenSearch 索引。`enriched_logs`管線會將相同的事件傳送至`log_advanced_pipeline`子管線，子管線會處理該事件，並將其傳送至名為`enriched_advanced_logs`的不同 OpenSearch 索引。

```
version: "2"
log-pipeline:
  source:
    http:
    ...
  processor:
```

```
    ...
  sink:
    - opensearch:
        # Provide a domain or collection endpoint
        # Enable the 'serverless' flag if the sink is an OpenSearch Serverless
 collection
        aws:
          ...
          index: "enriched_logs"
    - pipeline:
        name: "log_advanced_pipeline"

log_advanced_pipeline:
  source:
    log-pipeline
  processor:
   ...
  sink:
    - opensearch:
        # Provide a domain or collection endpoint
        # Enable the 'serverless' flag if the sink is an OpenSearch Serverless
 collection
        aws:
          ...
          index: "enriched_advanced_logs"
```

無效字母佇列

無效字母佇列 (DLQs) 是管線無法寫入接收器之事件的目的地。在 OpenSearch 擷取中，您必須指定具有適當寫入許可的 Amazon S3 儲存貯體做為. DLQ 您可以將DLQ組態新增至管線中的每個接收器。當管道遇到寫入錯誤時，會在設定的 S3 儲存貯體中建立DLQ物件。DLQ物件以失敗事JSON件的陣列形式存在於檔案中。

當符合下列任一條件DLQ時，管線會將事件寫入：

- 對`max_retries`於 OpenSearch 水槽已經用盡。 OpenSearch 此選項至少需要 16 個擷取。
- 由於錯誤狀況，接收器拒絕事件。

組態

若要設定子管線的無效字母佇列，請在接收器組態中指定`dlq`選項：`opensearch`

```
apache-log-pipeline:
  ...
  sink:
    opensearch:
      dlq:
        s3:
          bucket: "my-dlq-bucket"
          key_path_prefix: "dlq-files"
          region: "us-west-2"
          sts_role_arn: "arn:aws:iam::123456789012:role/dlq-role"
```

寫入此 S3 的檔案DLQ將具有下列命名模式：

```
dlq-v${version}-${pipelineName}-${pluginId}-${timestampIso8601}-${uniqueId}
```

如需詳細資訊，請參閱無效字母佇列 () DLQ。

如需設定`sts_role_arn`角色的指示，請參閱the section called “寫入無效字母佇列”。

範例

請考慮下面的示例DLQ文件：

```
dlq-v2-apache-log-pipeline-opensearch-2023-04-05T15:26:19.152938Z-e7eb675a-
f558-4048-8566-dac15a4f8343
```

以下是無法寫入接收器並傳送至 DLQ S3 儲存貯體以進行進一步分析的資料範例：

```
Record_0
pluginId            "opensearch"
pluginName          "opensearch"
pipelineName        "apache-log-pipeline"
failedData
index    "logs"
indexId   null
status    0
message  "Number of retries reached the limit of max retries (configured value 15)"
document
log      "sample log"
timestamp     "2023-04-14T10:36:01.070Z"
```

```
Record_1
pluginId            "opensearch"
pluginName          "opensearch"
pipelineName        "apache-log-pipeline"
failedData
index               "logs"
indexId   null
status    0
message  "Number of retries reached the limit of max retries (configured value 15)"
document
log                 "another sample log"
timestamp           "2023-04-14T10:36:01.071Z"
```

索引管理

Amazon OpenSearch 擷取具有許多索引管理功能，包括下列功能。

建立索引

您可以在管線接收器中指定索引名稱，而 OpenSearch 擷取會在佈建管線時建立索引。如果索引已存在，管線會使用它來索引傳入事件。如果您停止並重新啟動管道，或者更新其YAML組態，則管道會嘗試建立新索引 (如果尚未存在)。管線永遠無法刪除索引。

下列範例接收器會在佈建管線時建立兩個索引：

```
sink:
  - opensearch:
      index: apache_logs
  - opensearch:
      index: nginx_logs
```

產生索引名稱和模式

您可以使用傳入事件欄位中的變數來產生動態索引名稱。在接收器配置中，使用格式`string${}`向字符串插值發出信號，並使用JSON指針從事件中提取字段。的選項`index_type`為`custom`或`management_disabled`。由`custom`於 OpenSearch 網域和`management_disabled` OpenSearch 無伺服器集合的`index_type`預設值為，因此可以將其保留為未設定。

例如，下列管線會從傳入事件中選取`metadataType`欄位來產生索引名稱。

```
pipeline:
  ...
  sink:
    opensearch:
      index: "metadata-${metadataType}"
```

下列組態會持續每天或每小時產生一個新索引。

```
pipeline:
  ...
  sink:
    opensearch:
      index: "metadata-${metadataType}-%{yyyy.MM.dd}"

pipeline:
  ...
  sink:
    opensearch:
      index: "metadata-${metadataType}-%{yyyy.MM.dd.HH}"
```

索引名稱也可以是具有日期時間模式作為後綴的純字符串，例如。`my-index-%{yyyy.MM.dd}`當接收器將資料傳送至時間時 OpenSearch，它會以時間取代日期UTC時間模式，並為每天建立新索引，例如。`my-index-2022.01.25`如需詳細資訊，請參閱DateTimeFormatter類別。

此索引名稱也可以是格式化字串 (有無論是否有日期-時間模式尾碼)，例如。`my-${index}-name`當接收器將數據發送到時 OpenSearch，它將替換為正在處理的事件中的值的`"${index}"`部分。如果格式為`"${index1/index2/index3}"`，則會以事件中`index1/index2/index3`的值取代欄位。

產生文件 IDs

管線可以在將文件編入索引時產生文件 ID OpenSearch。它可以從傳入事件IDs中的欄位推斷這些文件。

此範例使用來自傳入事件的`uuid`欄位來產生文件 ID。

```
pipeline:
  ...
  sink:
    opensearch:
      index_type: custom
```

```
      index: "metadata-${metadataType}-%{yyyy.MM.dd}"
      document_id_field: "uuid"
```

在下列範例中，「新增項目」處理器會合併欄位uuid和來other_field自傳入事件的欄位，以產生文件 ID。

此create動作可確保IDs不會覆寫相同的文件。管道丟棄重複的文檔，沒有任何重試或DLQ事件。對於使用此動作的管道作者來說，這是一個合理的期望，因為目標是避免更新現有文件。

```
pipeline:
  ...
  processor:
   - add_entries:
      entries:
        - key: "my_doc_id_field"
          format: "${uuid}-${other_field}"
  sink:
    - opensearch:
       ...
       action: "create"
       document_id_field: "my_doc_id_field"
```

您可能想要將事件的文件 ID 設定為子物件中的欄位。在下列範例中，接 OpenSearch 收器外掛程式會使用子物件info/id來產生文件 ID。

```
sink:
  - opensearch:
       ...
       document_id_field: info/id
```

鑑於下列事件，管線會產生_id欄位設定為的文件json001：

```
{
   "fieldA":"arbitrary value",
   "info":{
      "id":"json001",
      "fieldA":"xyz",
      "fieldB":"def"
   }
}
```

產生路由 IDs

您可以使用接收 OpenSearch 器外掛程式中的`routing_field`選項，將文件路由屬性的值 (`_routing`) 設定為來自傳入事件的值。

路由支持JSON指針語法，因此嵌套字段也可用，而不僅僅是頂級字段。

```
sink:
  - opensearch:
      ...
      routing_field: metadata/id
      document_id_field: id
```

鑑於下列事件，外掛程式會產生`_routing`欄位設定為的文件`abcd`：

```
{
   "id":"123",
   "metadata":{
      "id":"abcd",
      "fieldA":"valueA"
   },
   "fieldB":"valueB"
}
```

如需建立管線可在索引建立期間使用之索引範本的指示，請參閱索引範本。

電子nd-to-end 確認

OpenSearch 擷取可使end-to-end用確認來追蹤資料從來源到接收器的傳遞，以確保資料的持久性和可靠性。目前，只有 S3 來源外掛程式支援 end-to-end 確認。

透過 end-to-end 確認，管線來源外掛程式會建立確認集來監視一批事件。當這些事件成功發送到接收器時，它會收到正確的確認，或者當任何事件無法發送到他們的接收器時，會收到負面的確認。

如果管線元件發生故障或損毀，或者來源無法接收確認，則來源會逾時並採取必要的動作，例如重試或記錄失敗。如果管線配置了多個接收器或多個子管線，則只有在將事件傳送至所有子管線中的所有接收器之後，才會傳送事件層級確認。如果接收器已DLQ設定， end-to-end 確認也會追蹤寫入. DLQ

若要啟用 end-to-end 確認，請在來源組態中包含`acknowledgments`選項：

```
s3-pipeline:
```

```
  source:
    s3:
      acknowledgments: true
...
```

源背壓

當管道忙於處理資料時，或者接收器暫時關閉或擷取資料速度緩慢時，可能會遇到背壓。 OpenSearch 根據管道使用的來源外掛程式，擷取有不同的處理背壓方式。

HTTP來源

使用HTTP來源外掛程式的管道會根據哪個管線元件擁擠而有不同的方式處理背壓：

- 緩衝區 — 當緩衝區已滿時，管道會開始將HTTP狀態REQUEST_TIMEOUT傳回錯誤碼 408 回來源端點。隨著緩衝區被釋放，管道再次開始處理HTTP事件。
- 來源執行緒 — 當所有HTTP來源執行緒都忙於執行要求，且未處理的要求佇列大小已超過允許的要求數目上限時，管道會開始將HTTP狀態TOO_MANY_REQUESTS傳回錯誤碼 429 回來源端點。當要求佇列低於允許的最大佇列大小時，管線會再次開始處理要求。

OTel來源

當使用 OpenTelemetry 來源 (OTel記錄檔、OTel指標和OTel追蹤) 的管道的緩衝區已滿時，管道會開始將HTTP狀態REQUEST_TIMEOUT傳回來源端點，錯誤碼為 408。隨著緩衝區被釋放，管道再次開始處理事件。

S3 來源

當具有 S3 來源的管道的緩衝區已滿時，管道會停止處理SQS通知。釋放緩衝區後，管道會再次開始處理通知。

如果接收器關閉或無法擷取資料，且已啟用來源的 end-to-end 確認，則管線會停止處理SQS通知，直到收到來自所有接收器的成功確認為止。

建立 Amazon OpenSearch 擷取管道

管道是 Amazon OpenSearch Intetion 用來將資料從其來源 (資料來源) 移至接收器 (資料傳送位置) 的機制。在 OpenSearch 擷取中，接收器永遠是單一 Amazon OpenSearch 服務網域，而資料來源可能是 Amazon S3、Fluent Bit 或 OpenTelemetry 收集器等用戶端。

如需詳細資訊，請參閱 OpenSearch 文件中的管道。

主題

- 必要條件和必要角色
- 必要許可
- 指定管線版本
- 指定擷取路徑
- 建立管道
- 追蹤管道建立的狀態
- 使用藍圖建立管道

必要條件和必要角色

若要建立 OpenSearch 擷取管線，您必須具備下列資源：

- OpenSearch 擷取將承擔寫入接收器的IAM角色。您將在管線組態ARN中包含此角色。
- 作為接收器的 OpenSearch 服務網域或 OpenSearch 無伺服器集合。如果您要寫入網域，則該網域必須執行 OpenSearch 1.0 或更新版本，或是彈性搜尋 7.4 或更新版本。接收器必須具有授與IAM管線角色適當權限的存取原則。

如需建立這些資源的指示，請參閱下列主題：

- the section called “授與管道對網域的存取權”
- the section called “授予管道對集合的存取權”

> **Note**
>
> 如果您要寫入使用精細存取控制的網域，您需要完成額外的步驟。請參閱 the section called “步驟 3：對應管線角色 (僅適用於使用精細存取控制的網域)”。

必要許可

OpenSearch 擷取會使用下列IAM權限來建立管道：

- `osis:CreatePipeline`— 建立管線。
- `osis:ValidatePipeline`-檢查配管組態是否有效。
- `iam:PassRole`— 將管線角色傳遞至 OpenSearch 擷取，以便將資料寫入網域。此權限必須位於管線角色資源 (您為管線組態中的`sts_role_arn`選項指定的資源) 上，或僅限於`*`您計劃在每個管線中使用不同的角色時。ARN

例如，下列原則授與建立管道的權限：

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Resource":"*",
         "Action":[
            "osis:CreatePipeline",
            "osis:ListPipelineBlueprints",
            "osis:ValidatePipeline"
         ]
      },
      {
         "Resource":[
            "arn:aws:iam::your-account-id:role/pipeline-role"
         ],
         "Effect":"Allow",
         "Action":[
            "iam:PassRole"
         ]
      }
   ]
}
```

OpenSearch 擷取也包含稱為的權限`osis:Ingest`，這是使用簽章版本 4 傳送已簽署要求至管線所需的權限。如需詳細資訊，請參閱the section called “建立擷取角色”。

> **Note**
>
> 此外，第一個在帳戶中建立管道的使用者必須具有`iam:CreateServiceLinkedRole`動作的權限。如需詳細資訊，請參閱管線角色資源。

如需有關每個權限的詳細資訊，請參閱服務授權參考中用於 OpenSearch 擷取的動作、資源和條件金鑰。

指定管線版本

設定管線時，您必須指定管線將執行的主要資料預留程式版本。若要指定版本，請在管線組態中包含`version`選項：

```
version: "2"
log-pipeline:
  source:
    ...
```

當您選擇建立時， OpenSearch 擷取會決定您指定之主要版本的最新可用次要版本，並以該版本佈建管道。例如，如果您指定`version: "2"`，且最新支援的資料預留器版本為 2.1.1，則 OpenSearch 擷取會以 2.1.1 版佈建管道。我們不會公開顯示您的管道正在執行的次要版本。

若要在有新的主要資料預留程式版本可供使用時升級管線，請編輯管線組態並指定新版本。您無法將管道降級為較早的版本。

> **Note**
>
> OpenSearch 擷取不會立即支援新版本的資料預留器，一旦推出。新版本可公開使用到「 OpenSearch 擷取」支援時，會有一些延遲。此外， OpenSearch 擷取可能完全不支援某些主要或次要版本。如需完整清單，請參閱the section called “支援的資料預留程式版本”。

每當您對啟動藍/綠部署的管道進行變更時， OpenSearch 擷取都可以將其升級到管道檔案中目前設定的主要版本的最新次要版本。YAML如需詳細資訊，請參閱the section called “管道更新的藍色/綠色部署”。 OpenSearch 除非您在管道組態中明確更新`version`選項，否則擷取無法變更管道的主要版本。

指定擷取路徑

對於OTel追蹤和OTel指標等提取式來源， OpenSearch 擷取需要來源組態中的其他`path`選項。路徑是字串，例如`/log/ingest`，代表擷取的URI路徑。此路徑定義URI用於將資料傳送至管線的路徑。

例如，假設您為名為的擷取管線指定下列項目子管線：`logs`

```
entry-pipeline:
```

```
  source:
    http:
      path: "/my/test_path"
```

將資料內嵌到管線時，必須在用戶端組態中指定下列端點：`https://logs-abcdefgh.us-west-2.osis.amazonaws.com/my/test_path`。

路徑必須以斜線 (/) 開頭，且可以包含特殊字元 '-'、'_'、' 。 ' ，和'/'，以及${pipelineName}佔位符。如果使用 ${pipelineName} (例如path: "/${pipelineName}/test_path")，則變數會被相關子配管的名稱取代。在這個例子中，它將是`https://logs.us-west-2.osis.amazonaws.com/entry-pipeline/test_path`。

建立管道

本節說明如何使 OpenSearch 用服 OpenSearch 務主控台和. AWS CLI

主控台

建立管道

1. 在https://console.aws.amazon.com/aos/家中登錄 Amazon OpenSearch 服務控制台。
2. 在左側導覽窗格中選擇「管線」，然後選擇「建立管線」
3. 選取空白管線，或選擇組態藍圖。藍圖包含適用於各種常見使用案例的預先設定檔YAML和JSON組態檔案。如需詳細資訊，請參閱the section called “使用藍圖建立管道”。

   選擇選取藍圖。
4. 輸入管道的名稱。
5. (選擇性) 選擇「啟用持續緩衝區」。持續性緩衝區會將您的資料儲存在多個磁碟型緩衝區中。AZs 如需詳細資訊，請參閱持續性緩衝。如果您啟用持續性緩衝區，請選取 AWS Key Management Service 要加密緩衝區資料的金鑰。
6. 在擷取 OpenSearch 運算單元 (OCUs) 中設定最小和最大管線容量。如需詳細資訊，請參閱the section called “調整管線”。
7. 在「管線組態」下，以YAML格式提供管線組態。如果您使用藍圖，則組態已預先填入，但您必須進行一些修改。

   單一配管組態檔案可以包含 1-10 個子配管。每個子管線都是單一來源、零個或多個處理器以及單一接收器的組合。對於 OpenSearch 擷取，接收器必須始終是 OpenSearch 服務網域。如需支援選項的清單，請參閱the section called “支持的插件和選項”。

> **Note**
>
> 您必須將`sts_role_arn`選項包括在每個子配管中。管線會採用中定義的角色，`sts_role_arn`將要求簽署至網域。如需詳細資訊，請參閱the section called “授與管道對網域的存取權”。

下列範例設定檔使用HTTP來源和 Grok 外掛程式來處理非結構化記錄資料，並將其傳送至 OpenSearch 服務網域。子管線被命名`log-pipeline`為。

```
version: "2"
log-pipeline:
  source:
    http:
      path: "/log/ingest"
  processor:
    - grok:
        match:
          log: [ '%{COMMONAPACHELOG}' ]
    - date:
        from_time_received: true
        destination: "@timestamp"
  sink:
    - opensearch:
        hosts: [ "https://search-my-domain.us-east-1.es.amazonaws.com" ]
        index: "apache_logs"
        aws:
          sts_role_arn: "arn:aws:iam::123456789012:role/{pipeline-role}"
          region: "us-east-1"
```

您可以建立自己的管線組態，或選擇 [上傳檔案] 並匯入自我管理的資料預留程式管線的現有組態。或者，您可以使用組態藍圖。

8. 設定管線後，選擇驗證管線以確認您的組態正確無誤。如果驗證失敗，請修正錯誤並重新執行驗證。
9. 在 [網路組態] 下，選擇 [VPC存取] 或 [公用存取]。如果選擇 Public access (公開存取)，請跳到下一步驟。如果您選擇VPC存取權，請進行下列設定：

設定	描述
端點管理	選擇是要自行建立VPC端點，還是要讓 OpenSearch 擷取為您建立端點。端點管理預設為由 OpenSearch 擷取管理的端點。
VPC	選擇您要使用的虛擬私有雲 (VPC) ID。VPC和管線必須是相同的 AWS 區域。
子網	選擇一或多個子網路。 OpenSearch 服務會在子網路中放置VPC端點和彈性網路介面。
安全群組	選擇一個或多個VPC安全群組，讓所需的應用程式在管線公開的連接埠 (80 或 443) 和通訊協定 (HTTP或HTTPs) 上連接埠進 OpenSearch 入擷取管線。
VPC貼附選項	如果您的來源是自我管理的端點，請將您的管道附加到VPC. 選擇提供的預設CIDR選項之一，或使用自訂選項CIDR。

如需詳細資訊，請參閱the section called “設定管線的 VPC 存取”。

10. (選擇性) 在標籤下，將一或多個標籤 (鍵值配對) 新增至管線。如需詳細資訊，請參閱the section called “標記管線”。
11. (選擇性) 在日誌發佈選項下，開啟 Amazon CloudWatch 日誌的管道日誌發佈功能。建議您啟用記錄發佈，以便更輕鬆地疑難排解管線問題。如需詳細資訊，請參閱the section called “監控管道日誌”。
12. 選擇 Next (下一步)。
13. 檢閱管線組態，然後選擇「建立」。

OpenSearch 擷取會執行非同步處理程序來建置管線。管道狀態為後`Active`，您就可以開始擷取資料。

AWS CLI

建立管線命令接受管線組態做為字串或 .yaml 檔案。如果您將配置作為字符串提供，則每個新行都必須使用轉義`\n`。例如 `"log-pipeline:\n source:\n http:\n processor:\n - grok:\n ...`

下列範例指令會建立具有下列組態的管線：

- 最少 4 次攝入OCUs，最多 10 次攝入 OCUs
- 在虛擬私有雲中佈建 (VPC)
- 已啟用記錄發佈

```
aws osis create-pipeline \
  --pipeline-name my-pipeline \
  --min-units 4 \
  --max-units 10 \
  --log-publishing-options
 IsLoggingEnabled=true,CloudWatchLogDestination={LogGroup="MyLogGroup"} \
  --vpc-options
 SecurityGroupIds={sg-12345678,sg-9012345},SubnetIds=subnet-1212234567834asdf \
  --pipeline-configuration-body "file://pipeline-config.yaml"
```

OpenSearch 擷取會執行非同步處理程序來建置管線。管道狀態為後`Active`，您就可以開始擷取資料。若要檢查管線的狀態，請使用GetPipeline指令。

OpenSearch 攝入 API

若要使用 OpenSearch 擷取建立 OpenSearch 擷取管線API，請呼叫作業。CreatePipeline

成功建立管道後，您可以設定用戶端並開始將資料擷取到您的 OpenSearch 服務網域。如需詳細資訊，請參閱the section called “使用管道整合”。

追蹤管道建立的狀態

您可以在 OpenSearch 擷取佈建管道時追蹤管道的狀態，並準備擷取資料。

主控台

在您初始建立管道之後，它會經過多個階段，因為 OpenSearch 擷取準備擷取資料。若要檢視管線建立的各個階段，請選擇管線名稱以查看其「管線設定」 頁面。在狀態下，選擇檢視詳細資料。

管道會先經過下列階段，才能擷取資料：

- 驗證 — 驗證管線組態。當此階段完成時，所有驗證都已成功。
- 建立環境 — 準備和佈建資源。當此階段完成時，就會建立新的管線環境。

- 部署管線 — 部署管線。當此階段完成時，管線已成功部署。
- 檢查管道健康狀況 — 檢查管道的健康狀況。當這個階段完成時，所有健康狀態檢查都已通過。
- 啟用流量 — 讓管道能夠擷取資料。完成此階段後，您就可以開始將資料擷取到管線中。

CLI

使用get-pipeline-change-progress指令來檢查管線的狀態。下列 AWS CLI 要求會檢查名為的管線狀態`my-pipeline`：

```
aws osis get-pipeline-change-progress \
    --pipeline-name my-pipeline
```

回應：

```
{
   "ChangeProgressStatuses": {
      "ChangeProgressStages": [
         {
            "Description": "Validating pipeline configuration",
            "LastUpdated": 1.671055851E9,
            "Name": "VALIDATION",
            "Status": "PENDING"
         }
      ],
      "StartTime": 1.671055851E9,
      "Status": "PROCESSING",
      "TotalNumberOfStages": 5
   }
}
```

OpenSearch 攝入 API

若要使用 OpenSearch 擷取追蹤管線建立的狀態API，請呼叫GetPipelineChangeProgress作業。

使用藍圖建立管道

您可以使用組態藍圖，而不是從頭開始建立管線定義，而是針對追蹤分析或 Apache 記錄等常見擷取案例的預先設定YAML範本。組態藍圖可協助您輕鬆佈建管線，而不必從頭開始編寫組態。

主控台

使用管線藍圖

1. 在https://console.aws.amazon.com/aos/家中登錄 Amazon OpenSearch 服務控制台。
2. 在左側導覽窗格中選擇「管線」，然後選擇「建立管線」
3. 從使用案例清單中選取藍圖，然後選擇選取藍圖。配管組態會根據您選取的使用案例填入子配管。
4. 檢閱註解文字，以引導您完成藍圖的設定。

> **Important**
> 管線藍圖不是有效的。您需要進行一些修改，例如提供 AWS 區域 和用於驗證ARN的角色，否則管線驗證將會失敗。

CLI

若要使用取得所有可用藍圖的清單 AWS CLI，請傳送list-pipeline-blueprints要求。

```
aws osis list-pipeline-blueprints
```

要求會傳回所有可用藍圖的清單。

若要取得有關特定藍圖的更多詳細資訊，請使用以下get-pipeline-blueprint命令：

```
aws osis get-pipeline-blueprint --blueprint-name AWS-ApacheLogPipeline
```

此要求會傳回 Apache 記錄管線藍圖的內容：

```
{
   "Blueprint":{
      "PipelineConfigurationBody":"###\n  # Limitations: https://docs.aws.amazon.com/
opensearch-service/latest/ingestion/ingestion.html#ingestion-limitations\n###\n###\n
 # apache-log-pipeline:\n    # This pipeline receives logs via http (e.g. FluentBit),
 extracts important values from the logs by matching\n    # the value in the 'log' key
 against the grok common Apache log pattern. The grokked logs are then sent\n    # to
 OpenSearch to an index named 'logs'\n###\n\nversion: \"2\"\napache-log-pipeline:\n
 source:\n    http:\n      # Provide the path for ingestion. ${pipelineName} will be
 replaced with pipeline name configured for this pipeline.\n      # In this case it
```

```
 would be \"/apache-log-pipeline/logs\". This will be the FluentBit output URI value.
\n      path: \"/${pipelineName}/logs\"\n  processor:\n    - grok:\n        match:\n
         log: [ \"%{COMMONAPACHELOG_DATATYPED}\" ]\n  sink:\n    - opensearch:\n
   # Provide an AWS OpenSearch Service domain endpoint\n        # hosts: [ \"https://
search-mydomain-1a2a3a4a5a6a7a8a9a0a9a8a7a.us-east-1.es.amazonaws.com\" ]\n
 aws:\n          # Provide a Role ARN with access to the domain. This role should have
 a trust relationship with osis-pipelines.amazonaws.com\n          # sts_role_arn:
 \"arn:aws:iam::123456789012:role/Example-Role\"\n          # Provide the region of the
 domain.\n          # region: \"us-east-1\"\n          # Enable the 'serverless' flag
 if the sink is an Amazon OpenSearch Serverless collection\n          # serverless:
 true\n        index: \"logs\"\n        # Enable the S3 DLQ to capture any failed
 requests in an S3 bucket\n        # dlq:\n          # s3:\n            # Provide an
 S3 bucket\n            # bucket: \"your-dlq-bucket-name\"\n            # Provide a key
 path prefix for the failed requests\n            # key_path_prefix: \"${pipelineName}/
logs/dlq\"\n            # Provide the region of the bucket.\n            # region:
 \"us-east-1\"\n            # Provide a Role ARN with access to the bucket. This role
 should have a trust relationship with osis-pipelines.amazonaws.com\n            #
 sts_role_arn: \"arn:aws:iam::123456789012:role/Example-Role\"\n",
      "BlueprintName":"AWS-ApacheLogPipeline"
   }
}
```

OpenSearch 攝入 API

若要使用 OpenSearch 擷取取得管線藍圖的相關資訊API，請使用ListPipelineBlueprints和GetPipelineBlueprint作業。

檢視亞馬遜OpenSearch擷取管道

您可以使用AWS Management Console、或OpenSearch擷取 API 檢視有關 Amazon 擷取管道的AWS CLI詳細資料。OpenSearch

主控台

檢視管道

1. 登入 Amazon Ser OpenSearch vice 主控台，網址為 https://console.aws.amazon.com/aos/home。
2. 在左側導覽窗格中選擇「管道」。
3. (選擇性) 若要檢視具有特定狀態的配管，請選擇「任何狀態」(Any status) 並選取要篩選依據的狀態。

配管可能為下列狀態：

- `Creating`— 正在建立配管。
- `Active`— 管線處於作用中狀態並準備擷取資料。
- `Updating`— 正在更新管線。
- `Deleting`正在刪除配管。
- `Create failed`— 無法建立配管。
- `Update failed`— 無法更新管線。
- `Starting`— 管道正在啟動。
- `Start failed`— 管道無法啟動。
- `Stopping`— 正在停止管線。
- `Stopped`— 管道已停止，且可以隨時重新啟動。

當管道位於`Create failed`、`Creating`和`Stopped`狀態時，您不會針對擷取 OCU 付費。`Deleting`

CLI

若要使用檢視管線AWS CLI，請傳送清單管線要求：

```
aws osis list-pipelines
```

該請求返回所有現有管道的列表：

```
{
    "NextToken": null,
    "Pipelines": [
        {,
            "CreatedAt": 1.671055851E9,
            "LastUpdatedAt": 1.671055851E9,
            "MaxUnits": 4,
            "MinUnits": 2,
            "PipelineArn": "arn:aws:osis:us-west-2:123456789012:pipeline/log-pipeline",
            "PipelineName": "log-pipeline",
            "Status": "ACTIVE",
            "StatusReason": {
                "Description": "The pipeline is ready to ingest data."
```

```
            }
        },
            "CreatedAt": 1.671055851E9,
            "LastUpdatedAt": 1.671055851E9,
            "MaxUnits": 2,
            "MinUnits": 8,
            "PipelineArn": "arn:aws:osis:us-west-2:123456789012:pipeline/another-
pipeline",
            "PipelineName": "another-pipeline",
            "Status": "CREATING",
            "StatusReason": {
                "Description": "The pipeline is being created. It is not able to ingest
 data."
            }
        }
    ]
}
```

若要取得單一管線的相關資訊，請使用 get-pipeline 指令：

```
aws osis get-pipeline --pipeline-name "my-pipeline"
```

要求會傳回指定管線的組態資訊：

```
{
    "Pipeline": {
        "PipelineName": "my-pipeline",
        "PipelineArn": "arn:aws:osis:us-east-1:123456789012:pipeline/my-pipeline",
        "MinUnits": 9,
        "MaxUnits": 10,
        "Status": "ACTIVE",
        "StatusReason": {
            "Description": "The pipeline is ready to ingest data."
        },
        "PipelineConfigurationBody": "log-pipeline:\n source:\n http:\n processor:\n
 - grok:\n match:\nlog: [ '%{COMMONAPACHELOG}' ]\n - date:\n from_time_received: true
\n destination: \"@timestamp\"\n  sink:\n - opensearch:\n hosts: [ \"https://search-
mdp-performance-test-duxkb4qnycd63rpy6svmvyvfpi.us-east-1.es.amazonaws.com\" ]\n index:
 \"apache_logs\"\n aws_sts_role_arn: \"arn:aws:iam::123456789012:role/my-domain-role
\"\n  aws_region: \"us-east-1\"\n  aws_sigv4: true",,
        "CreatedAt": "2022-10-01T15:28:05+00:00",
        "LastUpdatedAt": "2022-10-21T21:41:08+00:00",
        "IngestEndpointUrls": [
```

```
            "my-pipeline-123456789012.us-east-1.osis.amazonaws.com"
        ]
    }
}
```

OpenSearch擷取 API

若要使用OpenSearch擷取 API 檢視OpenSearch擷取管道，請呼叫ListPipelines和GetPipeline作業。

更新 Amazon OpenSearch 擷取管道

您可以使用 AWS Management Console、或 OpenSearch 擷取 API 更新 Amazon OpenSearch 擷取管道。 AWS CLI OpenSearch 當您更新管線的 YAML 組態時，擷取會啟動藍/綠部署。如需詳細資訊，請參閱 the section called “管道更新的藍色/綠色部署”。

主題

- 考量事項
- 必要許可
- 更新管道
- 管道更新的藍色/綠色部署

考量事項

更新管線時，請考慮下列事項：

- 您可以編輯管線的容量限制、記錄發佈選項和 YAML 組態。您無法編輯其名稱或網路設定。
- 如果管線寫入 VPC 網域接收器，則在建立管線後，您無法返回並將接收器變更為不同的 VPC 網域。您必須使用新的接收器刪除並重新建立配管。您仍然可以將接收器從 VPC 網域切換到公用網域、從公用網域切換到 VPC 網域，或從公用網域切換到另一個公用網域。
- 您可以隨時在公用 OpenSearch 服務網域和無伺服器集合之間切換管線接收 OpenSearch 器。
- 當您更新管線的 YAML 組態時， OpenSearch 擷取會初始化藍/綠部署。如需詳細資訊，請參閱 the section called “管道更新的藍色/綠色部署”。
- 當您更新管線的 YAML 組態時， OpenSearch 擷取會自動將管線升級至管線組態中指定之主要資料預留程式的最新受支援次要版本。此過程可讓您的管道保持最新狀態，並獲得最新的錯誤修復和性能改進。

- 您仍然可以在管道停止時對管道進行更新。

必要許可

OpenSearch 擷取會使用下列 IAM 許可更新管道：

- `osis:UpdatePipeline`— 更新管道。
- `osis:ValidatePipeline`-檢查配管組態是否有效。
- `iam:PassRole`— 將管線角色傳遞至 OpenSearch 擷取，以便將資料寫入網域。只有在更新管線 YAML 組態時才需要此權限，而不是在修改其他設定 (例如記錄發佈或容量限制) 時才需要此權限。

例如，下列原則授與更新管線的權限：

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Resource":"*",
         "Action":[
            "osis:UpdatePipeline",
            "osis:ValidatePipeline"
         ]
      },
      {
         "Resource":[
            "arn:aws:iam::{your-account-id}:role/{pipeline-role}"
         ],
         "Effect":"Allow",
         "Action":[
            "iam:PassRole"
         ]
      }
   ]
}
```

更新管道

您可以使用 AWS Management Console、或 OpenSearch 擷取 API 更新 Amazon OpenSearch 擷取管道。 AWS CLI

主控台

更新配管

1. 登錄到 Amazon OpenSearch 服務控制台 https://console.aws.amazon.com/aos/home.
2. 在左側導覽窗格中選擇「管道」。
3. 選擇管線以開啟其設定。您可以編輯管線的容量限制、記錄發佈選項和 YAML 組態。您無法編輯其名稱或網路設定。
4. 修改完成後，請選擇 Save (儲存)。

CLI

若要使用更新管線 AWS CLI，請傳送更新管線要求。下列範例請求會上傳新的組態檔案，並更新容量下限和最大容量值：

```
aws osis update-pipeline \
  --pipeline-name "my-pipeline" \
  --pipline-configuration-body "file://new-pipeline-config.yaml" \
  --min-units 11 \
  --max-units 18
```

OpenSearch 擷取 API

若要使用 OpenSearch 擷取 API 更新 OpenSearch 擷取管線，請呼叫作業。UpdatePipeline

管道更新的藍色/綠色部署

OpenSearch 當您更新管線的 YAML 組態時，擷取會啟動藍/綠部署程序。

藍/綠是指為管線更新建立新環境，並在這些更新完成後將流量路由傳送至新環境的做法。實務可在萬一部署到新環境不成功時將停機時間減至最小並維護原始環境。藍/綠部署本身不會對效能造成任何影響，但是如果管線組態以改變效能的方式發生變更，效能可能會改變。

OpenSearch 擷取會在藍/綠部署期間封鎖 auto-scaling 模。在舊管道重新導向至新管道之前，您仍會繼續支付流量的費用。重新導向流量後，您只需支付新管道的費用。您不需要同時支付兩個管道的費用。

當您更新管線的 YAML 組態檔案時， OpenSearch 擷取可以自動將管線升級至管線組態中指定之主要資料預留程式的最新受支援次要版本。例如，您可能已`version: "2"`在管線組態中，

而 OpenSearch 擷取最初佈建了 2.1.0 版的管道。新增對版本 2.1.1 的支援並變更管線組態時，OpenSearch 擷取會將管道升級至 2.1.1 版。

此過程可讓您的管道保持最新狀態，並獲得最新的錯誤修復和性能改進。 OpenSearch 除非您在管線組態中手動變更`version`選項，否則擷取無法更新管道的主要版本。

停止和啟動亞馬遜OpenSearch擷取管道

停用和啟動 Amazon OpenSearch 擷取管道可協助您管理開發和測試環境的成本。您可以暫時停用管道，而非每次使用管道時，設定和卸除管道。

主題

- 停用和啟動OpenSearch擷取管道
- 停止OpenSearch擷取管線
- 啟動OpenSearch擷取管線

停用和啟動OpenSearch擷取管道

您可以在不需要將資料內嵌到管道的期間停止管道。一旦您需要管道，即可隨時重新啟動管道。啟動和停用可簡化用於下列操作之管道的設定和卸除程序：開發、測試或不需要連續可用性的類似活動。

管道停用時，您無須支付任何擷取 OCU 小時數的費用。您仍然可以更新已停止的管道，它們會收到自動次要版本更新和安全性修補程式。

如果您需要保持管道執行中，但它具有的容量超過所需，請勿使用啟動和停用。如果您的管道成本太高或不是很繁忙，請考慮降低管道的最大容量限制。如需詳細資訊，請參閱the section called “調整管線”。

停止OpenSearch擷取管線

若要使用 OpenSearch Ingestion 管線或執行管理，請始終從使用中的管線開始，然後停止管線，然後再次啟動管線。管道停用時，您無須支付擷取 OCU 小時數的費用。

主控台

停用管道

1. 登入 Amazon Ser OpenSearch vice 主控台，網址為 https://console.aws.amazon.com/aos/home。

2. 在導覽窗格中，選擇管道，然後選擇管道。您可以從這個頁面執行停用操作，或導覽至欲停用管道的詳細資訊頁面。
3. 在「動作」 中選擇「停止管線」。

   如果管道無法停用和啟動管道，則無法使用停用管道動作。

AWS CLI

若要使用停用管道AWS CLI，請搭配下列參數呼叫 stop-pipeline 命令：

- `--pipeline-name`— 管道名稱。

Example

```
aws osis stop-pipeline --pipeline-name my-pipeline
```

OpenSearch擷取 API

若要使用OpenSearch擷取 API 停用管道，請搭配下列參數呼叫StopPipeline操作：

- `PipelineName`— 管道名稱。

啟動OpenSearch擷取管線

您一律會啟動OpenSearch擷取管道，從已處於停用狀態的管道開始。管道會保留其組態設定，例如容量限制、網路設定和記錄發佈選項。

重新啟動管道通常需要幾分鐘的時間。

主控台

啟動管道

1. 登入 Amazon Ser OpenSearch vice 主控台，網址為 https://console.aws.amazon.com/aos/home。
2. 在導覽窗格中，選擇管道，然後選擇管道。您可以從這個頁面執行啟動操作，或導覽至欲啟動管道的詳細資訊頁面。
3. 對於「動作」，選擇「啟動管線」

AWS CLI

若要使用啟動管道AWS CLI，請搭配下列參數呼叫 start-管道：

- `--pipeline-name`— 管道名稱。

Example

```
aws osis start-pipeline --pipeline-name my-pipeline
```

OpenSearch擷取 API

若要使用OpenSearch擷取 API 啟動OpenSearch擷取管線，請使用下列參數呼叫StartPipeline作業：

- `PipelineName`— 管道名稱。

刪除亞馬遜OpenSearch擷取管道

您可以使用AWS Management Console、或OpenSearch擷取 API 刪除 Amazon OpenSearch 擷取管道。AWS CLI狀態為`Creating`或時，您無法刪除管道`Updating`。

主控台

刪除管道

1. 登入 Amazon OpenSearch 服務主控台，網址為 https://console.aws.amazon.com/aos/home。
2. 在左側導覽窗格中選擇「管道」。
3. 選擇您要刪除的管道，然後選擇刪除。
4. 確認刪除，然後選擇 Delete (刪除)。

CLI

若要使用刪除管線AWS CLI，請傳送刪除管線要求：

```
aws osis delete-pipeline --pipeline-name "my-pipeline"
```

OpenSearch擷取 API

若要使用OpenSearch擷取 API 刪除OpenSearch擷取管線，請使用下列參數呼叫DeletePipeline作業：

- `PipelineName`— 名稱。

Amazon OpenSearch 擷取管道支援的外掛程式和選項

相較於開放原始碼資料準備器，Amazon OpenSearch 擷取支援來源、處理器和接收器的子集。此外，OpenSearch 擷取對每個支援外掛程式的可用選項也有一些限制。下列各節說明 OpenSearch 擷取支援的外掛程式和相關選項。

> **Note**
>
> OpenSearch 擷取不支援任何緩衝區外掛程式，因為它會自動設定預設緩衝區。如果您在管線組態中包含緩衝區，則會收到驗證錯誤。

主題

- 支持的插件
- 無狀態處理器與可狀態處理器
- 組態需求和限制

支持的插件

OpenSearch 擷取支援下列資料預留器外掛程式：

資料來源：

- Amazon DocumentDB
- DynamoDB
- OpenSearch

- HTTP
- Kafka
- OTel日誌
- OTel度量
- OTel跟踪
- S3

處理器：

- Aggregate
- 異常探測器
- CSV
- 日期
- 解壓
- 解剖
- 掉落事件
- IP 地理位址
- Grok
- 關鍵值
- 映射到列表
- 變異事件（系列處理器）
- 變異字符串（系列處理器）
- 混淆
- OTel度量
- OTel追蹤群組
- OTel跟踪
- 解析離子
- 剖析 JSON
- 剖析 XML
- 選取項目
- 服務地圖
- 跟踪對等轉發
- 截斷
- 使用者代理

水槽：

- OpenSearch(支援 OpenSearch 服務、 OpenSearch 無伺服器及彈性搜尋 6.8 或更新版本)
- S3

接收編解碼器：

- 阿夫羅
- NDJSON
- JSON
- 木地板

無狀態處理器與可狀態處理器

無狀態處理器執行諸如轉換和篩選之類的操作，而有狀態處理器則執行諸如彙總之類的操作，這會記住上一次運行的結果。 OpenSearch 擷取支援可設定狀態的處理器彙總和服務對應。所有其他支援的處理器都是無狀態的。

對於僅包含無狀態處理器的管道，最大容量限制為 96 擷取OCUs。如果管線包含任何可設定狀態的處理器，則最大容量限制為 48 擷取OCUs。不過，如果管線已啟用持續性緩衝，則只有無狀態處理器的最大擷取最多可達 384；如果管線OCUs包含任何可設定狀態的處理器，OCUs則最多可以有 192 個擷取。如需詳細資訊，請參閱the section called “調整管線”。

只有無狀態nd-to-end 處理器才支援 E 確認。如需詳細資訊，請參閱the section called “電子nd-to-end 確認”。

組態需求和限制

除非下面另有指定，否則在 OpenSearch Intection 管道中允許上述支援外掛程式的「資料預留程式」組態參考中描述的所有選項。下列各節說明 OpenSearch 擷取對特定外掛程式選項所造成的限制。

> **Note**
>
> OpenSearch 擷取不支援任何緩衝區外掛程式，因為它會自動設定預設緩衝區。如果您在管線組態中包含緩衝區，則會收到驗證錯誤。

許多選項都是透過 OpenSearch 擷取在內部設定和管理，例如`authentication`和`acm_certificate_arn`。如果手動變更，其他選項 (例如`thread_count`和`request_timeout`) 會影響效能。因此，這些值會在內部設定，以確保管線的最佳效能。

最後，某些選項無法傳遞給 OpenSearch 擷取，例如`ism_policy_file`和`sink_template`，因為在開放原始碼資料預留器中執行時，它們是本機檔案。不支援這些值。

主題

- 一般配管選項
- 格羅克處理器
- HTTP來源
- OpenSearch 水槽
- OTel指標來源、OTel追蹤來源和OTel記錄來源
- OTel追蹤群組處理器
- OTel追蹤處理器
- 服務對應處理器
- S3 來源

一般配管選項

下列一般管道選項由 OpenSearch 擷取設定，管線組態中不支援：

- `workers`
- `delay`

格羅克處理器

不支援下列 Grom 處理器選項：

- `patterns_directories`
- `patterns_files_glob`

HTTP來源

HTTP源插件具有以下要求和約束：

- 該path選項是必需的。路徑是字串，例如`/log/ingest`，代表記錄擷取的URI路徑。此路徑定義URI用於將資料傳送至管線的路徑。例如：`https://log-pipeline.us-west-2.osis.amazonaws.com/log/ingest`。路徑必須以斜線 (/) 開頭，且可以包含特殊字元'-'、'_'、'。'，和'/'，以及${pipelineName}佔位符。
- 下列HTTP來源選項由 OpenSearch 擷取設定，管線組態中不支援：
  - `port`

- ssl
- ssl_key_file
- ssl_certificate_file
- aws_region
- authentication
- unauthenticated_health_check
- use_acm_certificate_for_ssl
- thread_count
- request_timeout
- max_connection_count
- max_pending_requests
- health_check_service
- acm_private_key_password
- acm_certificate_timeout_millis
- acm_certificate_arn

OpenSearch 水槽

接OpenSearch收器外掛程式具有下列需求和限制。

- 此選aws項為必要選項，且必須包含下列選項：
  - sts_role_arn
  - region
  - hosts
  - serverless(如果接收器是 OpenSearch 無伺服器集合)
- sts_role_arn此選項必須為YAML定義檔案中的每個接收器指向相同的角色。
- hosts此選項必須指定 OpenSearch 服務網域端點或 OpenSearch 無伺服器集合端點。您無法為網域指定自訂端點；它必須是標準端點。
- 如果此選hosts項是無伺服器收集端點，則必須將serverless選項設定為true。此外，如果您的YAML定義檔案包含選index_type項，則必須將其設定為management_disabled，否則驗證會失敗。
- 不支援下列選項：

- `username`
- `password`
- `cert`
- `proxy`
- `dlq_file`-如果您想要將失敗的事件卸載到無效字母佇列 (DLQ)，則必須使用`dlq`選項並指定 S3 儲存貯體。
- `ism_policy_file`
- `socket_timeout`
- `template_file`
- `insecure`
- `bulk_size`

OTel指標來源、OTel追蹤來源和OTel記錄來源

OTel指標來源、OTel追蹤來源和OTel記錄來源外掛程式具有下列需求和限制：

- 該`path`選項是必需的。路徑是字串，例如`/log/ingest`，代表記錄擷取的URI路徑。此路徑定義URI用於將資料傳送至管線的路徑。例如：`https://log-pipeline.us-west-2.osis.amazonaws.com/log/ingest`。路徑必須以斜線 (/) 開頭，且可以包含特殊字元'-'、'_'、'。'，和'/'，以及`${pipelineName}`佔位符。
- 下列選項由 OpenSearch 擷取設定，管線組態不支援：
  - `port`
  - `ssl`
  - `sslKeyFile`
  - `sslKeyCertChainFile`
  - `authentication`
  - `unauthenticated_health_check`
  - `useAcmCertForSSL`
  - `unframed_requests`
  - `proto_reflection_service`
  - `thread_count`
  - `request_timeout`

- max_connection_count
- acmPrivateKeyPassword
- acmCertIssueTimeOutMillis
- health_check_service
- acmCertificateArn
- awsRegion

OTel追蹤群組處理器

OTel追蹤群組處理器具有下列需求和限制：

- 此選aws項為必要選項，且必須包含下列選項：
  - sts_role_arn
  - region
  - hosts
- 此選sts_role_arn項會指定與您在接 OpenSearch 收器組態中指定的管線角色相同的角色。
- 不支援usernamepasswordcert、、和insecure選項。
- 此選aws_sigv4項為必要選項，且必須設定為 true。
- 不支援serverless接 OpenSearch 收器外掛程式中的選項。Otel 追蹤群組處理器目前無法與 OpenSearch 無伺服器集合搭配使用。
- 管線組態主體內的otel_trace_group處理器數目不能超過 8。

OTel追蹤處理器

OTel追蹤處理器具有下列需求和限制：

- trace_flush_interval選項的值不能超過 300 秒。

服務對應處理器

服務對應處理器具有下列需求和限制：

- window_duration選項的值不能超過 300 秒。

S3 來源

S3 來源外掛程式具有下列要求和限制：

- 此選`aws`項為必要選項，且必須包含`region`和`sts_role_arn`選項。
- `records_to_accumulate`選項的值不能超過 200。
- `maximum_messages`選項的值不能超過 10。
- 如果指定`disable_bucket_ownership_validation`此選項，則必須將選項設定為 false。
- 如果已指定，則必須將`input_serialization`選項設定為`parquet`。

使用 Amazon OpenSearch 擷取管道整合

為了成功地將資料 OpenSearch 導入 Amazon Intection 管道，您必須將用戶端應用程式 (來源) 設定為將資料傳送到管道端點。您的來源可能是用戶端，例如 Fluent Bit 日誌、 OpenTelemetry收集器或簡單的 S3 儲存貯體。每個客戶端的確切配置不同。

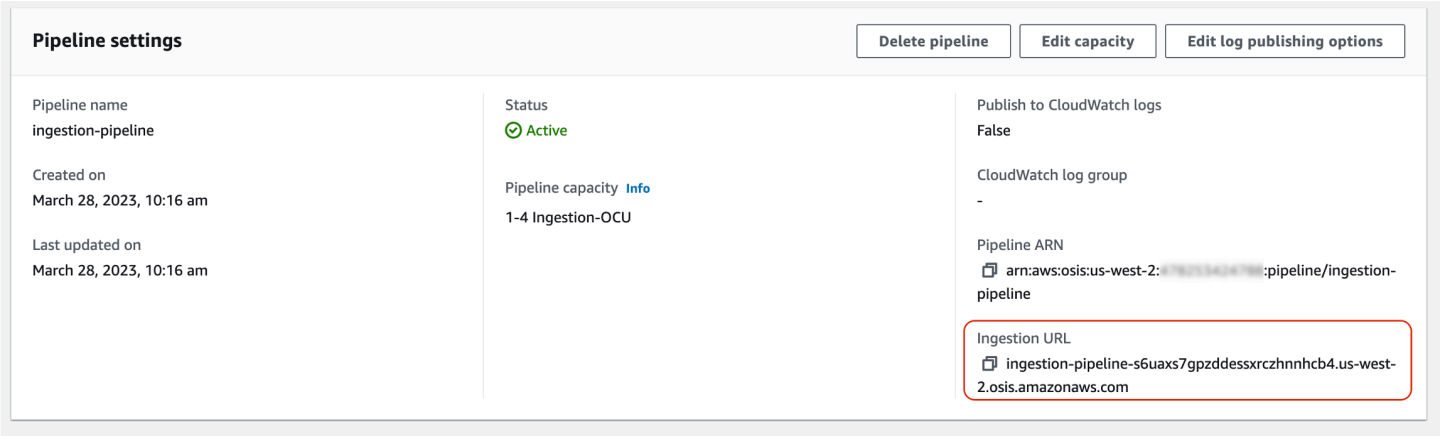
來源組態期間的重要差異 (與直接傳送資料至 OpenSearch 服務網域或 OpenSearch 無伺服器集合相比) 是 AWS 服務名稱 (`osis`) 和主機端點 (必須是管線端點)。

主題

- 建構擷取端點
- 建立擷取角色
- 將 OpenSearch 擷取管道與 Amazon DynamoDB 使用
- 使用 OpenSearch 擷取管道搭配 Amazon DocumentDB
- 使用與融 OpenSearch 合雲卡夫卡的攝入管道
- 搭配使用 OpenSearch 擷取管線 Amazon Managed Streaming for Apache Kafka
- 搭配 Amazon S3 使用 OpenSearch 擷取管道
- 使用帶有 Amazon 安全湖的 OpenSearch 擷取管道
- 使用具有流利位 OpenSearch 元的擷取管線
- 搭配 Fluentd 使用 OpenSearch 擷取管線
- 搭 OpenTelemetry 配收集器使用 OpenSearch 擷取管線
- 使用 OpenSearch 擷取管線與卡夫卡
- 搭配使用 OpenSearch 擷取管線 OpenSearch
- 後續步驟

建構擷取端點

為了將資料導入管道，請將其傳送至擷取端點。若要尋找擷取URL，請瀏覽至「管線設定」 頁面並複製擷URL取：



若要為OTel追蹤和OTel指標等提取式來源建構完整擷取端點，請將管線組態的擷取路徑新增至擷取。URL

例如，假設您的管線組態具有下列擷取路徑：

```
entry-pipeline:
  source:
    http:
      path: "/my/test_path"
```

您在用戶端組態中指定的完整擷取端點將採用下列格式：`https://ingestion-pipeline-abcdefg.us-west-2.osis.amazonaws.com/my/test_path`

如需詳細資訊，請參閱the section called “指定擷取路徑”。

建立擷取角色

所有對 OpenSearch 擷取的要求都必須使用簽名版本 4 簽署。至少，簽署請求的角色必須獲得`osis:Ingest`動作的權限，這允許其將資料傳送至 OpenSearch 擷取管線。

例如，下列 AWS Identity and Access Management (IAM) 原則允許對應的角色將資料傳送至單一管線：

```
{
```

```
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "osis:Ingest",
      "Resource": "arn:aws:osis:us-east-1:{account-id}:pipeline/pipeline-name"
    }
  ]
}
```

> **Note**
>
> 若要將角色用於所有管線，請以萬用字`Resource`元 (*) 取代元素ARN中的。

提供跨帳戶擷取存取

> **Note**
>
> 您只能為公有管道提供跨帳戶擷取存取權，而不VPC能為管線提供。

您可能需要將資料從不同的管道內嵌到管道中 AWS 帳戶，例如存放來源應用程式的帳戶。如果寫入管線的主體與管線本身的帳戶不同，您需要設定主體以信任另一個IAM角色，才能將資料內嵌到管線中。

設定跨帳戶擷取權限

1. 在管道內建立具有`osis:Ingest`權限的擷取角色 (AWS 帳戶 如前一節所述)。如需指示，請參閱建立IAM角色。
2. 將信任原則附加至擷取角色，讓其他帳戶中的主體可以假設這個角色：

```
{
  "Version": "2012-10-17",
  "Statement": [{
     "Effect": "Allow",
     "Principal": {
       "AWS": "arn:aws:iam::{external-account-id}:root"
      },
     "Action": "sts:AssumeRole"
  }]
```

```
}
```

3. 在另一個帳戶中，設定您的用戶端應用程式 (例如 Fluent Bit) 以擔任擷取角色。為了使此功能運作，應用程式帳戶必須將權限授與應用程式使用者或角色，才能擔任擷取角色。

   下列範例以身分識別為基礎的原則允許`ingestion-role`從管線帳戶假設附加的主參與者：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "sts:AssumeRole",
      "Resource": "arn:aws:iam::{account-id}:role/ingestion-role"
    }
  ]
}
```

然後，用戶端應用程式可以使用該AssumeRole作業來假設資料，`ingestion-role`並將資料擷取至關聯的管線。

將 OpenSearch 擷取管道與 Amazon DynamoDB 使用

您可以將 OpenSearch 擷取管道與 DynamoDB 搭配使用，將 DynamoDB 表格事件 (例如建立、更新和刪除) 串流至 Amazon OpenSearch 服務網域和集合。 OpenSearch 擷取管道整合了變更資料擷取 (CDC) 基礎架構，以提供高規模、低延遲的方式來持續從 DynamoDB 表格串流資料。

您可以透過兩種方式使用 DynamoDB 做為處理資料的來源，無論是否有完整的初始快照。

完整初始快照是 DynamoDB 使用point-in-time 復原 (PITR) 功能所採用的資料表備份。DynamoDB 此快照上傳到 Amazon S3。從那裡， OpenSearch 擷取管線會將其傳送到網域中的一個索引，或將其分割為網域中的多個索引。為了保持 DynamoDB 中的資料 OpenSearch 一致性，管線會將 DynamoDB 表中的所有建立、更新和刪除事件與儲存在索引中的文件同步。 OpenSearch

使用完整初始快照時，擷取管道會先 OpenSearch 擷取快照，然後開始從 DynamoDB Streams 讀取資料。它最終可以追趕並維持 DynamoDB 和. 之間近乎即時的資料一致性。 OpenSearch選擇此選項時，您必須在表格上同時啟用PITR和 DynamoDB 串流。

您也可以使用與 DynamoDB 的 OpenSearch 擷取整合，在沒有快照的情況下串流事件。如果您已經擁有其他機制的完整快照，或者您只想從 DynamoDB 資料表中 DynamoDB Streams 目前的事件，請選擇此選項。選擇此選項時，您只需要在表格上啟用 DynamoDB 串流即可。

如需有關此整合的詳細資訊，請參閱Amazon DynamoDB 開發人員指南中的 DynamoDB 與 Amazon OpenSearch 服務零ETL整合。

主題

- 必要條件
- 步驟 1：設定管線角色
- 步驟 2：建立管道
- 資料一致性
- 對映資料類型
- 限制
- 建議 CloudWatch DynamoDB 示

必要條件

若要設定管線，您必須啟用 DynamoDB 串流的 DynamoDB 表格。您的串流應該使用`NEW_IMAGE`串流檢視類型。不過，`NEW_AND_OLD_IMAGES`如果此串流檢視類型符合您的使用案例， OpenSearch 擷取管線也可以串流事件。

如果您使用的是快照，您也必須在資料表上啟用 point-in-time 復原功能。如需詳細資訊，請參閱 Amazon DynamoDB 開發人員指南中的建立表格、啟用 point-in-time 復原和啟用串流。

步驟 1：設定管線角色

設定 DynamoDB 表之後，請設定要在管線組態中使用的管線角色，並在角色中新增下列 DynamoDB 權限：

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "allowRunExportJob",
            "Effect": "Allow",
            "Action": [
                "dynamodb:DescribeTable",
                "dynamodb:DescribeContinuousBackups",
                "dynamodb:ExportTableToPointInTime"
            ],
            "Resource": [
                "arn:aws:dynamodb:us-east-1:{account-id}:table/my-table"
```

```
            ]
        },
        {
            "Sid": "allowCheckExportjob",
            "Effect": "Allow",
            "Action": [
                "dynamodb:DescribeExport"
            ],
            "Resource": [
                "arn:aws:dynamodb:us-east-1:{account-id}:table/my-table/export/*"
            ]
        },
        {
            "Sid": "allowReadFromStream",
            "Effect": "Allow",
            "Action": [
                "dynamodb:DescribeStream",
                "dynamodb:GetRecords",
                "dynamodb:GetShardIterator"
            ],
            "Resource": [
                "arn:aws:dynamodb:us-east-1:{account-id}:table/my-table/stream/*"
            ]
        },
        {
            "Sid": "allowReadAndWriteToS3ForExport",
            "Effect": "Allow",
            "Action": [
                "s3:GetObject",
                "s3:AbortMultipartUpload",
                "s3:PutObject",
                "s3:PutObjectAcl"
            ],
            "Resource": [
                "arn:aws:s3:::my-bucket/{exportPath}/*"
            ]
        }
    ]
}
```

您也可以使用 AWS KMS 客戶管理的金鑰來加密匯出資料檔案。若要解密匯出的物件，`s3_sse_kms_key_id`請以下列格式在管線的匯出組態中指定金鑰 ID：`arn:aws:kms:us-west-2:{account-id}:key/my-key-id`下列原則包含使用客戶管理金鑰的必要權限：

```
{
    "Sid": "allowUseOfCustomManagedKey",
    "Effect": "Allow",
    "Action": [
        "kms:GenerateDataKey",
        "kms:Decrypt"
    ],
    "Resource": arn:aws:kms:us-west-2:{account-id}:key/my-key-id
}
```

步驟 2：建立管道

然後，您可以如下所示設定 OpenSearch 擷取管道，該管道會將 DynamoDB 指定為來源。此範例管道會從`table-a`PITR快照擷取資料，接著是 DynamoDB Streams 中的事件。的開始位置`LATEST`表示管道應該從 DynamoDB Streams 讀取最新資料。

```
version: "2"
cdc-pipeline:
  source:
    dynamodb:
      tables:
      - table_arn: "arn:aws:dynamodb:us-west-2:{account-id}:table/table-a"
        export:
          s3_bucket: "my-bucket"
          s3_prefix: "export/"
        stream:
          start_position: "LATEST"
      aws:
        region: "us-west-2"
        sts_role_arn: "arn:aws:iam::{account-id}:role/pipeline-role"
  sink:
  - opensearch:
      hosts: ["https://search-mydomain.us-east-1.es.amazonaws.com"]
      index: "${getMetadata(\"table_name\")}"
      index_type: custom
      normalize_index: true
      document_id: "${getMetadata(\"primary_key\")}"
      action: "${getMetadata(\"opensearch_action\")}"
      document_version: "${getMetadata(\"document_version\")}"
      document_version_type: "external"
```

您可以使用預先設定的 DynamoDB 藍圖來建立此管道。如需詳細資訊，請參閱the section called “使用藍圖建立管道”。

資料一致性

OpenSearch 擷取支援確 end-to-end 認，以確保資料耐久性。管道讀取快照或串流時，會動態建立分割區以進行 parallel 處理。管道會在擷取 OpenSearch 網域或集合中的所有記錄後收到確認後，將分割區標示為完整。

如果您想要內嵌至 OpenSearch 無伺服器搜尋集合，可以在管道中產生文件 ID。如果您想要導入 OpenSearch 無伺服器時間序列集合，請注意，管線不會產生文件 ID。

OpenSearch 擷取管線也會將傳入的事件動作對應至對應的大量索引動作，以協助擷取文件。這樣可以保持資料一致，以便 DynamoDB 中的每個資料變更都會與中的對應文件變更協調。 OpenSearch

對映資料類型

OpenSearch 服務會動態地將每個傳入文件中的資料類型對應至 DynamoDB 中的對應資料類型。下表顯示了 OpenSearch 服務如何自動映射各種數據類型。

資料類型	OpenSearch	DynamoDB
Number	OpenSearch 自動對應數值資料。如果數字是整數，則將其 OpenSearch 映射為長值。如果數字是分數，則將其 OpenSearch 映射為浮點值。 OpenSearch 根據第一個發送的文檔動態映射各種屬性。如果 DynamoDB 中的相同屬性混合了資料類型 (例如整數和小數)，則對應可能會失敗。 例如，如果您的第一個文件具有整數的屬性，而稍後的文件具有與小數編號相同的屬性，則 OpenSearch 無法內嵌第二個文件。在這些情況下，您應該提供明確的對應範本，如下所示： `{ "template": {`	支援數字。

資料類型	OpenSearch	DynamoDB

	``
	  "mappings": {
	  "properties": {
	  "MixedNumberAttribute": {
	  "type": "float"
	  }
	  }
	  }
	  }
	}
	``
	如果您需要雙精度，請使用字符串類型的字段映射。中沒有支持 38 位精度的等效數字類型 OpenSearch。	

數字, 集合	OpenSearch 自動將數字集合映射到長值或浮點值的數組中。與標量數一樣，這取決於攝入的第一個數字是整數還是小數。您可以使用與對映純量字串相同的方式，為數字集提供對映。	DynamoDB 支援代表一組數字的類型。

資料類型	OpenSearch	DynamoDB
字串	OpenSearch 自動將字串值對應為文字。在某些情況下 (例如列舉值)，您可以對應至關鍵字類型。 下列範例顯示如何將名為的 DynamoDB 屬性對應`PartType`至關鍵字。OpenSearch `{ "template": { "mappings": { "properties": { "PartType": { "type": "keyword" } } } } }`	支援字串。
字符串集	OpenSearch 自動將字符串集映射到字符串數組中。您可以使用與對映純量字串相同的方式，為字串集提供對應。	DynamoDB 支援代表字串集合的類型。

資料類型	OpenSearch	DynamoDB
二進位	OpenSearch 自動將二進位資料對應為文字。您可以提供一個映射，將這些字段寫入為中的二進制字段 OpenSearch。 下列範例顯示如何將名為的 DynamoDB 屬性對應`ImageData` 至 OpenSearch 二進位欄位。 `{ "template": { "mappings": { "properties": { "ImageData": { "type": "binary" } } } } }`	DynamoDB 進位類型屬性。
二進制集	OpenSearch 自動將二進制集映射到二進制數據的數組作為文本。您可以使用與對映純量二進位相同的方式，為數字集提供對應。	DynamoDB 支援代表二進位值集合的類型。
Boolean	OpenSearch 將 DynamoDB 布林型別對應至布 OpenSearch 林型別。	DynamoDB 林型別屬性。
Null	OpenSearch 可以擷取具有 DynamoDB 空值類型的文件。它將值保存為文檔中的空值。此類型沒有對應，且此欄位無法編製索引或搜尋。 如果空類型使用相同的屬性名稱，然後稍後變更為不同類型 (例如 string)，則會為第一個非空值 OpenSearch 建立動態對應。後續的值仍然 DynamoDB 是空值。	支援空類型屬性。

資料類型	OpenSearch	DynamoDB
Map	OpenSearch 將 DynamoDB 會將屬性對應至巢狀欄位。相同的對映適用於巢狀欄位中。 下列範例會將巢狀欄位中的字串對應至中的關鍵字類型 OpenSearch： `{ "template": { "mappings": { "properties": { "AdditionalDescriptions": { "properties": { "PartType": { "type": "keyword" } } } } } } }`	支援對應類型屬性。
清單	OpenSearch 根據清單中的內容，為 DynamoDB 清單提供不同的結果。 當清單包含所有相同類型的純量類型時 (例如，所有字串的清單)，則會將清單 OpenSearch 內嵌為該類型的陣列。這適用於字符串，數字，布爾和空類型。每種類型的限制都與該類型的標量的限制相同。 您也可以使用與用於地圖相同的對映來提供對映清單的對映。 您無法提供混合類型的清單。	支援清單類型屬性。

資料類型	OpenSearch	DynamoDB
設定	OpenSearch 根據集合中的內容，為 DynamoDB 集提供不同的結果。 當一個集合包含所有相同類型的標量類型（例如，一組所有字符串），然後將該集合 OpenSearch 內嵌為該類型的數組。這適用於字符串，數字，布爾和空類型。每種類型的限制都與該類型的標量的限制相同。 您也可以使用與用於地圖相同的對映來提供對映集的對映。 您無法提供一組混合類型。	DynamoDB 支援代表集合的類型。

建議您在 OpenSearch 擷取管線中設定無效字母佇列 (DLQ)。如果您已設定佇列， OpenSearch Service 會將由於動態對應失敗而無法擷取的所有失敗文件傳送至佇列。

如果自動對映失敗，您可以在管線組態`template_content`中使用`template_type`和來定義明確的對應規則。或者，您可以在啟動管道之前，直接在搜尋網域或集合中建立對應範本。

限制

為 DynamoDB 設定 OpenSearch 擷取管線時，請考慮下列限制：

- 與 DynamoDB 的 OpenSearch 擷取整合目前不支援跨區域擷取。您的 DynamoDB 資料表和 OpenSearch 擷取管道必須位於相同的資料表中。 AWS 區域
- 您的 DynamoDB 資料表和 OpenSearch 擷取管道必須位於相同的資料表中。 AWS 帳戶
- OpenSearch 擷取管線僅支援一個 DynamoDB 表做為其來源。
- DynamoDB Streams 最多只能將資料儲存在記錄中，最多可儲存 24 小時。如果從大型資料表的初始快照擷取需要 24 小時或更長時間，則會有一些初始資料遺失。若要減少此資料遺失，請預估資料表的大小，並設定 OpenSearch 擷取管線的適當運算單元。

建議 CloudWatch DynamoDB 示

建議您使用下列 CloudWatch 指標來監控擷取管線的效能。這些量度可協助您識別從匯出中處理的資料量、從串流處理的事件數量、處理匯出和串流事件時的錯誤，以及寫入目標的文件數量。您可以設定 CloudWatch 警示，以便在其中一個量度超過指定值超過指定的時間長度時執行動作。

指標	描述
`dynamodb-pipeline.BlockingBuffer.bufferUsage.value`	指示正在使用多少緩衝區。
`dynamodb-pipeline.dynamodb.activeExportS3ObjectConsumers.value`	顯示主動處理匯出之 OCUs Amazon S3 物件的物件總數。
`dynamodb-pipeline.dynamodb.bytesProcessed.count`	從 DynamoDB 來源處理的位元組計數。
`dynamodb-pipeline.dynamodb.changeEventsProcessed.count`	從 DynamoDB 串流處理的變更事件數目。
`dynamodb-pipeline.dynamodb.changeEventsProcessingErrors.count`	從 DynamoDB 處理的變更事件所產生的錯誤數目。
`dynamodb-pipeline.dynamodb.exportJobFailure.count`	失敗的匯出工作提交嘗試次數。
`dynamodb-pipeline.dynamodb.exportJobSuccess.count`	已成功提交的匯出工作數目。
`dynamodb-pipeline.dynamodb.exportRecordsProcessed.count`	從匯出處理的記錄總數。
`dynamodb-pipeline.dynamodb.exportRecordsTotal.count`	從 DynamoDB 匯出的記錄總數，對於追蹤資料匯出量而言至關重要。
`dynamodb-pipeline.dynamodb.exportS3ObjectsProcessed.count`	已從 Amazon S3 成功處理的匯出資料檔案總數。

指標	描述
dynamodb-pipeline.opensearch.bulkBadRequestErrors.count	由於格式錯誤的請求而導致批量請求期間的錯誤計數。
dynamodb-pipeline.opensearch.bulkRequestLatency.avg	大量寫入要求的平均延遲時間 OpenSearch。
dynamodb-pipeline.opensearch.bulkRequestNotFoundErrors.count	因找不到目標資料而失敗的大量要求數目。
dynamodb-pipeline.opensearch.bulkRequestNumberOfRetries.count	OpenSearch 擷取管線寫入 OpenSearch叢集的重試次數。
dynamodb-pipeline.opensearch.bulkRequestSizeBytes.sum	發出的所有大量請求的總大小（以字節為單位）OpenSearch。
dynamodb-pipeline.opensearch.documentErrors.count	將文件傳送至時發生的錯誤數 OpenSearch。導致錯誤的文件將被發送到DLQ。
dynamodb-pipeline.opensearch.documentsSuccess.count	成功寫入 OpenSearch 叢集或集合的文件數目。
dynamodb-pipeline.opensearch.documentsSuccessFirstAttempt.count	第一次嘗試時成功編製 OpenSearch 索引的文件數目。
dynamodb-pipeline.opensearch.documentsVersionConflictErrors.count	因處理期間文件中的版本衝突而導致的錯誤計數。
dynamodb-pipeline.opensearch.PipelineLatency.avg	透過從來源讀取以寫 OpenSearch 入目的地來處理資料的擷取管線平均延遲。
dynamodb-pipeline.opensearch.PipelineLatency.max	透過從來源讀取到寫 OpenSearch 入目的地來處理資料的擷取管線延遲上限。

指標	描述
dynamodb-pipeline.opensearch.recordsIn.count	成功攝入 OpenSearch的記錄計數。此指標對於跟踪正在處理和存儲的數據量至關重要。
dynamodb-pipeline.opensearch.s3.dlqS3RecordsFailed.count	無法寫入的記錄數DLQ。
dynamodb-pipeline.opensearch.s3.dlqS3RecordsSuccess.count	寫入的記錄數DLQ。
dynamodb-pipeline.opensearch.s3.dlqS3RequestLatency.count	Amazon S3 無效字母佇列請求的延遲測量計數。
dynamodb-pipeline.opensearch.s3.dlqS3RequestLatency.sum	Amazon S3 無效字母佇列的所有請求總延遲
dynamodb-pipeline.opensearch.s3.dlqS3RequestSizeBytes.sum	對 Amazon S3 無效字母佇列發出的所有請求的總大小 (以位元組為單位)。
dynamodb-pipeline.recordsProcessed.count	管道中處理的記錄總數，這是整體輸送量的關鍵指標。
dynamodb.changeEventsProcessed.count	沒有從 DynamoDB 串流收集任何記錄。這可能是因為資料表上沒有活動、匯出正在進行中，或是存取 DynamoDB 串流發生問題。
dynamodb.exportJobFailure.count	嘗試觸發匯出至 S3 失敗。
line.opensearch.bulkRequestInvalidInputErrors.count	由於輸入無效 OpenSearch 而導致的批量請求錯誤計數，這對於監視數據質量和操作問題至關重要。
opensearch.EndToEndLatency.avg	端對端位置高於從 DynamoDB 串流讀取時所需的值。這可能是因為 OpenSearch 叢集規模不足，或是 DynamoDB 表格上WCU輸送OCU量太低的最大管線容量所致。此端對端延遲在匯出後會很高，並且會隨著時間的推移而減少，因為它可以追溯到最新的 DynamoDB 串流。

使用 OpenSearch 擷取管道搭配 Amazon DocumentDB

您可以將 OpenSearch 擷取管道與 Amazon DocumentDB 搭配使用，將文件變更 (例如建立、更新和刪除) 串流至 Amazon OpenSearch 服務網域和集合。 OpenSearch 擷取管道可利用變更資料擷取 (CDC) 機制 (如果 Amazon DocumentDB 叢集上有的話)，或者API輪詢提供高規模、低延遲的方式來持續從 Amazon DocumentDB 叢集串流資料。

您可以透過兩種方式使用 Amazon DocumentDB 做為處理資料的來源，無論是否有完整的初始快照。

完整的初始快照是整個 Amazon DocumentDB 集合的大量查詢。Amazon DocumentDB 將此快照上傳到 Amazon S3。從那裡， OpenSearch 擷取管線會將其傳送到網域中的一個索引，或將其分割為網域中的多個索引。為了保持 Amazon DocumentDB 中的資料和 OpenSearch 一致性，管道會將 Amazon DocumentDB 集合中的所有建立、更新和刪除事件與儲存在索引中的文件同步。 OpenSearch

當您使用完整的初始快照時， OpenSearch 擷取管道會先擷取快照，然後開始從 Amazon DocumentDB 變更串流讀取資料。它最終趕上並維持 Amazon DocumentDB 和. 之間的近乎即時的資料一致性。 OpenSearch

您也可以使用 Amazon DocumentDB 的 OpenSearch 擷取整合，在不使用快照的情況下串流事件。如果您已經擁有來自某些其他機制的完整快照，或者只是想要使用變更串流從 Amazon DocumentDB 集合串流目前的事件，請選擇此選項。

使用這兩個選項時，如果在管道中設定中啟用串流，則必須在 Amazon DocumentDB 集合上啟用變更串流。如果您只使用完整載入或匯出，則不需要啟用變更串流。

必要條件

建立 OpenSearch 擷取管道之前，請執行下列步驟：

1. 依照 Amazon DocumentDB 開發人員指南中的建立 Amazon DocumentDB 叢集中的步驟，建立具有讀取資料權限的 Amazon DocumentDB 叢集。如果您使用CDC基礎設施，請確保將 Amazon DocumentDB 叢集設定為發佈變更串流。
2. TLS在您的 Amazon DocumentDB 叢集上啟用。
3. 設定要與 OpenSearch 擷取搭配使用的私人位址空間。VPC CIDR
4. 使用設定您的 Amazon DocumentDB 叢集上的身份驗證。 AWS Secrets Manager按照自動輪替 Amazon DocumentDB 的密碼中的步驟啟用密碼輪替。如需詳細資訊，請參閱 Amazon DocumentDB 中使用以角色為基礎的存取控制和安全性進行資料庫存取。
5. 如果您使用變更串流訂閱 Amazon DocumentDB 收集上的資料變更，請使用參數將保留期延長至最多 7 天，以避免資料遺失。`change_stream_log_retention_duration`根據預設，在記錄事

件之後，變更串流事件會儲存 3 小時，因此時間不足以容納大型集合。如要修改串流保留期間的變更，請參閱修改變串流記錄保留期間。

6. 建立 OpenSearch 服務網域或 OpenSearch 無伺服器集合。如需詳細資訊，請參閱建立 OpenSearch 服務網域和建立集合。
7. 將資源型政策附加至您的網域，或將資料存取原則附加至您的集合。這些存取政策允許 OpenSearch 擷取將資料從 Amazon DocumentDB 叢集寫入您的網域或集合。

   下列範例網域存取原則允許您在下一個步驟中建立的管線角色將資料寫入網域。確保您使用自己`resource`的更新ARN。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::{pipeline-account-id}:role/pipeline-role"
      },
      "Action": [
        "es:DescribeDomain",
        "es:ESHttp*"
      ],
      "Resource": [
        "arn:aws:es:{region}:{account-id}:domain/domain-name"
      ]
    }
  ]
}
```

   若要建立具有正確權限的IAM角色，以存取集合或網域的寫入資料，請參閱網域的必要權限和集合的必要權限。

步驟 1：設定管線角色

設定 Amazon DocumentDB 管道先決條件之後，請設定要在管道組態中使用的管道角色，並在該角色中新增以下 Amazon DocumentDB 許可：

```
{
    "Version": "2012-10-17",
    "Statement": [
```

```
        {
            "Sid": "allowS3ListObjectAccess",
            "Effect": "Allow",
            "Action": [
                "s3:ListBucket"
            ],
            "Resource": [
                "arn:aws:s3:::{s3_bucket}"
            ],
            "Condition": {
                "StringLike": {
                    "s3:prefix": "{s3_prefix}/*"
                }
            }
        },
        {
            "Sid": "allowReadAndWriteToS3ForExportStream",
            "Effect": "Allow",
            "Action": [
                "s3:PutObject",
                "s3:GetObject",
                "s3:DeleteObject"
            ],
            "Resource": [
                "arn:aws:s3:::{s3_bucket}/{s3_prefix}/*"
            ]
        },
        {
            "Sid": "SecretsManagerReadAccess",
            "Effect": "Allow",
            "Action": [
                "secretsmanager:GetSecretValue"
            ],
            "Resource": ["arn:aws:secretsmanager:{region}:{account-id}:secret:secret-
name"]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:AttachNetworkInterface",
                "ec2:CreateNetworkInterface",
                "ec2:CreateNetworkInterfacePermission",
                "ec2:DeleteNetworkInterface",
                "ec2:DeleteNetworkInterfacePermission",
```

```
                "ec2:DetachNetworkInterface",
                "ec2:DescribeNetworkInterfaces"
            ],
            "Resource": [
                "arn:aws:ec2:*:{account-id}:network-interface/*",
                "arn:aws:ec2:*:{account-id}:subnet/*",
                "arn:aws:ec2:*:{account-id}:security-group/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeDhcpOptions",
                "ec2:DescribeRouteTables",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcs",
                "ec2:Describe*"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTags"
            ],
            "Resource": "arn:aws:ec2:*:*:network-interface/*",
            "Condition": {
               "StringEquals":
                    {
                        "aws:RequestTag/OSISManaged": "true"
                    }
            }
        }
    ]
}
```

您必須對用於建立 OpenSearch 擷取管道的IAM角色提供上述 Amazon EC2 許可，因為管道使用這些許可在您VPC的網路界面中建立和刪除網路界面。管道只能透過此網路界面存取 Amazon DocumentDB 叢集。

步驟 2：建立管道

然後，您可以設定如下所示的 OpenSearch 擷取管道，該管道會將 Amazon DocumentDB 指定為來源。請注意，若要填入索引名稱，`getMetadata`函數會使用*`documentdb_collection`*做為中繼資料索引鍵。如果您想在不使用該`getMetadata`方法的情況下使用不同的索引名稱，則可以使用配置`index: "`*`my_index_name`*`"`。

```
version: "2"
documentdb-pipeline:
  source:
    documentdb:
      acknowledgments: true
      host: "https://docdb-cluster-id.us-east-1.docdb.amazonaws.com"
      port: 27017
      authentication:
        username: ${aws_secrets:secret:username}
        password: ${aws_secrets:secret:password}
      aws:
        sts_role_arn: "arn:aws:iam::{account-id}:role/pipeline-role"
      s3_bucket: "bucket-name"
      s3_region: "bucket-region"
      s3_prefix: "path" #optional path for storing the temporary data
      collections:
        - collection: "dbname.collection"
          export: true
          stream: true
  sink:
  - opensearch:
      hosts: ["https://search-mydomain.us-east-1.es.amazonaws.com"]
      index: "${getMetadata(\"documentdb_collection\")}"
      index_type: custom
      document_id: "${getMetadata(\"primary_key\")}"
      action: "${getMetadata(\"opensearch_action\")}"
      document_version: "${getMetadata(\"document_version\")}"
      document_version_type: "external"
extension:
  aws:
    secrets:
      secret:
        secret_id: "my-docdb-secret"
        region: "us-east-1"
        sts_role_arn: "arn:aws:iam::{account-id}:role/pipeline-role"
```

```
        refresh_interval: PT1H
```

您可以使用預先設定的 Amazon DocumentDB 藍圖來建立此管道。如需詳細資訊，請參閱the section called “使用藍圖建立管道”。

如果您使用建立管道，您還必須將管道附加到您VPC的，才能使用 Amazon DocumentDB 做為來源。AWS Management Console 若要這麼做，請找到 [網路設定] 區段，選取 [連接至] VPC 核取方塊，然後CIDR從提供的預設選項中選擇您的選項，或選取您自己的選項。您可以使用 CIDR「RFC1918 年最佳目前作法」中定義的私人位址空間中的任何位址空間。

若要提供自訂CIDR，請從下拉式功能表中選取「其他」。若要避免 OpenSearch 擷取和 Amazon DocumentDB 之間的 IP 地址發生衝突，請確保 Amazon DocumentDB 與用於擷取的VPCCIDR不同。CIDR OpenSearch

如需詳細資訊，請參閱設定管線的VPC存取權限。

資料一致性

管道會持續輪詢或接收來自 Amazon DocumentDB 叢集的變更，並更新索引中的對應文件，以確保資料一致性。 OpenSearch

OpenSearch 擷取支援確 end-to-end 認，以確保資料耐久性。管道讀取快照或串流時，會動態建立分割區以進行 parallel 處理。管道會在擷取 OpenSearch 網域或集合中的所有記錄後收到確認後，將分割區標示為完整。

如果您想要導入 OpenSearch 無伺服器搜尋集合，可以在管道中產生文件 ID。如果您想要內嵌至 OpenSearch 無伺服器時間序列集合，請注意，管線不會產生文件 ID，因此您必須在管線接收器組態`document_id: "${getMetadata(\"primary_key\")}"`中省略。

OpenSearch 擷取管線也會將傳入的事件動作對應至對應的大量索引動作，以協助擷取文件。這樣可以保持資料一致，以便 Amazon DocumentDB 中的每個資料變更都能與中的對應文件變更協調。OpenSearch

對映資料類型

OpenSearch 服務會將每個傳入文件中的資料類型動態對應至 Amazon DocumentDB 中的對應資料類型。下表顯示了 OpenSearch 服務如何自動映射各種數據類型。

資料類型	OpenSearch	Amazon DocumentDB
Integer	OpenSearch 自動將 Amazon DocumentDB 整數值映射到 OpenSearch 整數。 OpenSearch 根據第一個傳送的文件動態對應欄位。如果您在 Amazon DocumentDB 中混合使用相同屬性的資料類型，則自動對應可能會失敗。 例如，如果您的第一個文件具有 long 屬性，而稍後的文件具有與整數相同的屬性，則 OpenSearch 無法內嵌第二個文件。在這些情況下，您應該提供一個明確的映射模板，以選擇最靈活的數字類型，如下所示： `{ "template": { "mappings": { "properties": { "MixedNumberField": { "type": "float" } } } } }`	Amazon DocumentDB 支持整數。
Long	OpenSearch 自動將 Amazon DocumentDB 長值映射到 OpenSearch多頭。 OpenSearch 根據第一個傳送的文件動態對應欄位。如果您在 Amazon DocumentDB 中混合使用相同屬性的資料類型，則自動對應可能會失敗。	Amazon DocumentDB 支持多頭。

資料類型	OpenSearch	Amazon DocumentDB
	例如，如果您的第一個文件具有 long 屬性，而稍後的文件具有與整數相同的屬性，則 OpenSearch 無法內嵌第二個文件。在這些情況下，您應該提供一個明確的映射模板，以選擇最靈活的數字類型，如下所示： `{ "template": { "mappings": { "properties": { "MixedNumberField": { "type": "float" } } } } }`	
字串	OpenSearch 自動將字串值對應為文字。在某些情況下 (例如列舉值)，您可以對應至關鍵字類型。 下面的示例演示了如何將 Amazon DocumentDB 屬性映射`PartType`到一個 OpenSearch 關鍵字。 `{ "template": { "mappings": { "properties": { "PartType": { "type": "keyword" } } } } }`	Amazon DocumentDB 支持字符串。

資料類型	OpenSearch	Amazon DocumentDB
Double	OpenSearch 自動將 Amazon DocumentDB 雙值映射到 OpenSearch雙倍。 OpenSearch 根據第一個傳送的文件動態對應欄位。如果您在 Amazon DocumentDB 中混合使用相同屬性的資料類型，則自動對應可能會失敗。 例如，如果您的第一個文件具有 long 屬性，而稍後的文件具有與整數相同的屬性，則 OpenSearch 無法內嵌第二個文件。在這些情況下，您應該提供一個明確的映射模板，以選擇最靈活的數字類型，如下所示： `{ "template": { "mappings": { "properties": { "MixedNumberField": { "type": "float" } } } } }`	Amazon DocumentDB 支持雙打。

資料類型	OpenSearch	Amazon DocumentDB
日期	依預設，日期對應至中的整數 OpenSearch。您可以定義自訂對應範本，將日期對應至 OpenSearch 日期。 `{ "template": { "mappings": { "properties": { "myDateField": { "type": "date", "format": "epoch_second" } } } } }`	Amazon DocumentDB 支持日期。
時間戳記	依預設，時間戳記會對應至中的整數 OpenSearch。您可以定義自訂對應範本，將日期對應至 OpenSearch日期。 `{ "template": { "mappings": { "properties": { "myTimestampField": { "type": "date", "format": "epoch_second" } } } } }`	Amazon DocumentDB 支持時間戳。
Boolean	OpenSearch Amazon DocumentDB 布爾類型映射到一個 OpenSearch 布爾類型。	Amazon DocumentDB 支持布爾類型屬性。

資料類型	OpenSearch	Amazon DocumentDB
Decimal (小數)	OpenSearch 將 Amazon DocumentDB 映射到嵌套字段的屬性。相同的對映適用於巢狀欄位。 下列範例會將巢狀欄位中的字串對應至中的關鍵字類型 OpenSearch： `{ "template": { "mappings": { "properties": { "myDecimalField": { "type": "double" } } } } }` 使用此自定義映射，您可以查詢和聚合具有雙級精度的字段。原始值會保留文 OpenSearch件`_source`屬性中的完整精確度。如果沒有此對映，則依預設 OpenSearch 會使用文字。	Amazon DocumentDB 支持小數。
規則運算式	正則表達式類型創建嵌套字段。這些包括`<myFieldName>.pattern`和`<myFieldName>.options`.	Amazon DocumentDB 支持正則表達式。

資料類型	OpenSearch	Amazon DocumentDB
二進位資料	OpenSearch 自動將 Amazon DocumentDB 二進制數據映射到 OpenSearch文本。您可以提供一個映射，將這些字段寫入為中的二進制字段 OpenSearch。 下列範例顯示如何將名為的 Amazon DocumentDB 欄位對應`imageData` 至 OpenSearch 二進位欄位。 `{ "template": { "mappings": { "properties": { "imageData": { "type": "binary" } } } } }`	Amazon DocumentDB 支持二進制數據字段。
ObjectId	具有 objectId 映射到 OpenSearch 文本字段類型的字段。該值將是的字串表示 objectId。	Amazon DocumentDB 支持。objectIds
Null	OpenSearch 可以使用 Amazon DocumentDB 空類型導入文檔。它將值保存為文檔中的空值。此類型沒有對應，且此欄位無法編製索引或搜尋。 如果空類型使用相同的屬性名稱，然後稍後變更為不同類型 (例如 string)，則會為第一個非空值 OpenSearch 建立動態對應。後續值仍然可以是 Amazon DocumentDB 空值。	Amazon DocumentDB 支持空類型字段。

資料類型	OpenSearch	Amazon DocumentDB
未定義	OpenSearch 可以使用 Amazon DocumentDB 未定義類型導入文檔。它將值保存為文檔中的空值。此類型沒有對應，且此欄位無法編製索引或搜尋。 如果未定義的類型使用相同的欄位名稱，之後又變更為不同類型 (例如字串)，則會為第一個非未定義值 OpenSearch 建立動態對應。後續值仍然可以是 Amazon DocumentDB 未定義的值。	Amazon DocumentDB 支持未定義的類型字段。
MinKey	OpenSearch 可以使用 Amazon Document minKey DB 類型導入文檔。它將值保存為文檔中的空值。此類型沒有對應，且此欄位無法編製索引或搜尋。 如果 minKey 類型使用相同的欄位名稱，之後又變更為不同類型 (例如字串)，則會為第一個非minKey 值 OpenSearch 建立動態對應。後續值仍然可以是 Amazon DocumentDB minKey 值。	Amazon DocumentDB 支持minKey 類型字段。
MaxKey	OpenSearch 可以使用 Amazon Document maxKey DB 類型導入文檔。它將值保存為文檔中的空值。此類型沒有對應，且此欄位無法編製索引或搜尋。 如果 maxKey 類型使用相同的欄位名稱，之後又變更為不同類型 (例如字串)，則會為第一個非maxKey 值 OpenSearch 建立動態對應。後續值仍然可以是 Amazon DocumentDB maxKey 值。	Amazon DocumentDB 支持maxKey 類型字段。

建議您在 OpenSearch 擷取管線中設定無效字母佇列 (DLQ)。如果您已設定佇列， OpenSearch Service 會將由於動態對應失敗而無法擷取的所有失敗文件傳送至佇列。

如果自動對映失敗，您可以在管線組態`template_content`中使用 `template_type` and 來定義明確的對應規則。或者，您可以在啟動管道之前，直接在搜尋網域或集合中建立對應範本。

限制

為 Amazon DocumentDB 設定 OpenSearch 擷取管道時，請考慮下列限制：

- 與 Amazon DocumentDB 的 OpenSearch 擷取整合目前不支援跨區域擷取。您的 Amazon DocumentDB 叢集和 OpenSearch 擷取管道必須位於相同。 AWS 區域
- 與 Amazon DocumentDB 的 OpenSearch 擷取整合目前不支援跨帳戶擷取。您的 Amazon DocumentDB 叢集和 OpenSearch 擷取管道必須位於相同。 AWS 帳戶
- OpenSearch 擷取管道僅支援一個 Amazon DocumentDB 叢集做為其來源。
- 與 Amazon 文件資料庫的 OpenSearch 擷取整合特別支援 Amazon DocumentDB 執行個體型叢集。它不支援 Amazon DocumentDB 彈性叢集。
- OpenSearch 擷取整合僅支援 AWS Secrets Manager 做為 Amazon DocumentDB 叢集的身分驗證機制。
- 您無法更新現有管線組態，以便從不同的資料庫或集合擷取資料。相反地，您必須建立新的管線。

使用與融 OpenSearch 合雲卡夫卡的攝入管道

您可以使用 OpenSearch 擷取管道將資料從 Confluent 雲端 Kafka 叢集串流到 Amazon OpenSearch 服務網域和無伺服器集合。 OpenSearch OpenSearch 擷取支援公用和私人網路組態，將資料從 Confluent Cloud Kafka 叢集串流到由 OpenSearch 服務或無伺服器管理的網域或集合。 OpenSearch

連接到統一雲公共卡夫卡集群

您可以使用 OpenSearch 擷取管線從 Confluent Cloud Kafka 叢集遷移資料，並具有公用設定，這表示網域DNS名稱可以公開解析。若要這麼做，請將 Confluent Cloud 公用 Kafka 叢集設定為來源，並將 OpenSearch 服務或 OpenSearch 無伺服器設定為目的地的 OpenSearch 擷取管道。這會將您的串流資料從自我管理的來源叢集處理到 AWS管理的目的地網域或集合。

必要條件

建立 OpenSearch 擷取管道之前，請執行下列步驟：

1. 創建一個融合雲卡夫卡集群作為源。叢集應包含您要擷取至 OpenSearch 服務的資料。
2. 建立您要將資料移轉至其中的 OpenSearch 服務網域或 OpenSearch 無伺服器集合。如需詳細資訊，請參閱建立 OpenSearch 服務網域和建立集合。

3. 設置身份驗證您的協流雲卡夫卡群集與. AWS Secrets Manager按照旋轉密碼中的步驟啟用AWS Secrets Manager 密碼輪換。
4. 將資源型政策附加至您的網域，或將資料存取原則附加至您的集合。這些存取原則可讓 OpenSearch 擷取將資料從自我管理的叢集寫入您的網域或集合。

   下列範例網域存取原則允許您在下一個步驟中建立的管線角色將資料寫入網域。確保您使用自己`resource`的更新ARN。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::{pipeline-account-id}:role/pipeline-role"
      },
      "Action": [
        "es:DescribeDomain",
        "es:ESHttp*"
      ],
      "Resource": [
        "arn:aws:es:{region}:{account-id}:domain/domain-name"
      ]
    }
  ]
}
```

   若要建立具有正確權限的IAM角色，以存取集合或網域的寫入資料，請參閱網域的必要權限和集合的必要權限。

步驟 1：設定管線角色

設定 Confluent Cloud Kafka 叢集管線先決條件之後，請設定要在管線組態中使用的管線角色，並新增寫入 OpenSearch 服務網域或 OpenSearch 無伺服器集合的權限，以及從 Secrets Manager 讀取密碼的權限。

管理網路介面需要下列權限：

```
{
    "Version": "2012-10-17",
    "Statement": [
```

```
        {
            "Effect": "Allow",
            "Action": [
                "ec2:AttachNetworkInterface",
                "ec2:CreateNetworkInterface",
                "ec2:CreateNetworkInterfacePermission",
                "ec2:DeleteNetworkInterface",
                "ec2:DeleteNetworkInterfacePermission",
                "ec2:DetachNetworkInterface",
                "ec2:DescribeNetworkInterfaces"
            ],
            "Resource": [
                "arn:aws:ec2:*:{account-id}:network-interface/*",
                "arn:aws:ec2:*:{account-id}:subnet/*",
                "arn:aws:ec2:*:{account-id}:security-group/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeDhcpOptions",
                "ec2:DescribeRouteTables",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcs",
                "ec2:Describe*"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [ "ec2:CreateTags" ],
            "Resource": "arn:aws:ec2:*:*:network-interface/*",
            "Condition": {
               "StringEquals": { "aws:RequestTag/OSISManaged": "true" }
            }
        }
    ]
}
```

以下是從 AWS Secrets Manager 服務讀取密碼所需的權限：

```
{
```

```
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "SecretsManagerReadAccess",
            "Effect": "Allow",
            "Action": ["secretsmanager:GetSecretValue"],
            "Resource": ["arn:aws:secretsmanager:<region:<account-id>:secret:<,secret-
name>"]
        }
    ]
}
```

寫入 Amazon OpenSearch 服務域需要以下許可：

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::{your-account-id}:role/{pipeline-role}"
      },
      "Action": ["es:DescribeDomain", "es:ESHttp*"],
      "Resource": "arn:aws:es:{region}:{your-account-id}:domain/{domain-name}/*"
    }
  ]
}
```

步驟 2：建立管道

然後，您可以配置如下所示的 OpenSearch 擷取管道，該管道會將您的 Confluent Cloud Kafka 指定為來源。

您可以指定多個 OpenSearch 服務網域做為資料的目的地。此功能可讓傳入資料進行條件式路由或複寫至多個 OpenSearch Service 網域。

您也可以將資料從來源 Confluent Kafka 叢集遷移到無伺服器集合 OpenSearch 。VPC請務必在管線組態中提供網路存取原則。您可以使用 Confluent 模式註冊表來定義一個 Confluent 模式。

```
version: "2"
kafka-pipeline:
  source:
    kafka:
      encryption:
```

```
        type: "ssl"
      topics:
        - name: "topic-name"
          group_id: "group-id"
      bootstrap_servers:
        - "bootstrap-server.us-west-2.aws.private.confluent.cloud:9092"
      authentication:
        sasl:
          plain:
            username: ${aws_secrets:confluent-kafka-secret:username}
            password: ${aws_secrets:confluent-kafka-secret:password}
      schema:
        type: confluent
        registry_url: https://my-registry.us-west-2.aws.confluent.cloud
        api_key: "${{aws_secrets:schema-secret:schema_registry_api_key}}"
        api_secret: "${{aws_secrets:schema-secret:schema_registry_api_secret}}"
        basic_auth_credentials_source: "USER_INFO"
  sink:
  - opensearch:
      hosts: ["https://search-mydomain.us-west-2.es.amazonaws.com"]
      aws:
          sts_role_arn: "arn:aws:iam::{account-id}:role/pipeline-role"
          region: "us-west-2"
      index: "confluent-index"
extension:
  aws:
    secrets:
      confluent-kafka-secret:
        secret_id: "my-kafka-secret"
        region: "us-west-2"
        sts_role_arn: "arn:aws:iam::{account-id}:role/pipeline-role"
      schema-secret:
        secret_id: "my-self-managed-kafka-schema"
        region: "us-west-2"
        sts_role_arn: "arn:aws:iam::{account-id}:role/pipeline-role"
```

您可以使用預先設定的藍圖來建立此管道。如需詳細資訊，請參閱the section called “使用藍圖建立管道”。

連接到一致雲卡夫卡集群 VPC

您也可以使用 OpenSearch 擷取管線，將資料從在. VPC 若要這麼做，請將 Confluent Cloud Kafka 叢集設定為來源，並將 OpenSearch 服務或 OpenSearch 無伺服器設定為目的地的 OpenSearch 擷取

管線。這會將您的串流資料從 Confluent Cloud Kafka 來源叢集處理至 AWS受管理的目的地網域或集合。

OpenSearch 擷取支援在 Confluent 中所有支援的網路模式中設定的結合雲端 Kafka 叢集。OpenSearch 擷取中支援下列網路組態模式作為來源：

- AWS VPC凝視
- AWS PrivateLink 適用於專用叢集
- AWS PrivateLink 適用於企業叢集
- AWS Transit Gateway

必要條件

建立 OpenSearch 擷取管道之前，請執行下列步驟：

1. 使用包含要導入服務的數據的VPC網絡配置創建 Confluent Cloud Kafka 集群。 OpenSearch
2. 建立您要將資料移轉至其中的 OpenSearch 服務網域或 OpenSearch 無伺服器集合。如需詳細資訊，請參閱建立 OpenSearch 服務網域和建立集合。
3. 設置身份驗證您的協流雲卡夫卡群集與. AWS Secrets Manager按照旋轉密碼中的步驟啟用AWS Secrets Manager 密碼輪換。
4. 獲取VPC可以訪問自我管理卡夫卡的 ID。選擇VPCCIDR要由 OpenSearch 擷取使用的。

> **Note**
>
> 如果您使用建立管道，您還必須將 OpenSearch 擷取管道附加到您的，才能使用自我管理的 Kafka。 AWS Management Console VPC若要這麼做，請找到 [網路組態] 區段，選取 [連接至] VPC 核取方塊，然後CIDR從提供的預設選項中選擇您的選項，或選取您自己的選項。您可以使用 CIDR「RFC1918 最新最佳作法」中定義的私人位址空間中的任何位址空間。若要提供自訂CIDR，請從下拉式功能表中選取「其他」。若要避免 OpenSearch 擷取與自我管理之間的 IP 位址發生衝突 OpenSearch，請確定自我管理 OpenSearch VPCCIDR與擷取的CIDR不同。 OpenSearch

5. 將資源型政策附加至您的網域，或將資料存取原則附加至您的集合。這些存取原則可讓 OpenSearch 擷取將資料從自我管理的叢集寫入您的網域或集合。

> **Note**
>
> 如果您使用連 AWS PrivateLink 接您的協流雲卡夫卡，您將需要配置選項。VPC DHCPDNS應啟用主機名稱和DNS解析度。

下列範例網域存取原則允許您在下一個步驟中建立的管線角色將資料寫入網域。確保您使用自己`resource`的更新ARN。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::{pipeline-account-id}:role/pipeline-role"
      },
      "Action": [
        "es:DescribeDomain",
        "es:ESHttp*"
      ],
      "Resource": [
        "arn:aws:es:{region}:{account-id}:domain/domain-name"
      ]
    }
  ]
}
```

若要建立具有正確權限的IAM角色，以存取集合或網域的寫入資料，請參閱網域的必要權限和集合的必要權限。

步驟 1：設定管線角色

設定管線必要條件後，請設定要在管線組態中使用的管線角色，並在角色中新增下列權限：

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "SecretsManagerReadAccess",
```

```
            "Effect": "Allow",
            "Action": [
                "secretsmanager:GetSecretValue"
            ],
            "Resource": ["arn:aws:secretsmanager:{region}:{account-id}:secret:secret-
name"]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:AttachNetworkInterface",
                "ec2:CreateNetworkInterface",
                "ec2:CreateNetworkInterfacePermission",
                "ec2:DeleteNetworkInterface",
                "ec2:DeleteNetworkInterfacePermission",
                "ec2:DetachNetworkInterface",
                "ec2:DescribeNetworkInterfaces"
            ],
            "Resource": [
                "arn:aws:ec2:*:{account-id}:network-interface/*",
                "arn:aws:ec2:*:{account-id}:subnet/*",
                "arn:aws:ec2:*:{account-id}:security-group/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeDhcpOptions",
                "ec2:DescribeRouteTables",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcs",
                "ec2:Describe*"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTags"
            ],
            "Resource": "arn:aws:ec2:*:*:network-interface/*",
            "Condition": {
               "StringEquals":
```

```
                    {
                        "aws:RequestTag/OSISManaged": "true"
                    }
            }
        }
    ]
}
```

您必須對用於建立 OpenSearch 擷取管道的IAM角色提供上述 Amazon EC2 許可，因為管道使用這些許可在您VPC的網路界面中建立和刪除網路界面。管線只能透過此網路介面存取 Kafka 叢集。

步驟 2：建立管道

然後，您可以配置如下所示的 OpenSearch 擷取管道，該管道將 Kafka 指定為來源。

您可以指定多個 OpenSearch 服務網域做為資料的目的地。此功能可讓傳入資料進行條件式路由或複寫至多個 OpenSearch Service 網域。

您也可以將資料從來源 Confluent Kafka 叢集遷移到無伺服器集合 OpenSearch 。VPC請務必在管線組態中提供網路存取原則。您可以使用 Confluent 模式註冊表來定義一個 Confluent 模式。

```
 version: "2"
kafka-pipeline:
  source:
    kafka:
      encryption:
        type: "ssl"
      topics:
        - name: "topic-name"
          group_id: "group-id"
      bootstrap_servers:
        - "bootstrap-server.us-west-2.aws.private.confluent.cloud:9092"
      authentication:
        sasl:
          plain:
            username: ${aws_secrets:confluent-kafka-secret:username}
            password: ${aws_secrets:confluent-kafka-secret:password}
      schema:
        type: confluent
        registry_url: https://my-registry.us-west-2.aws.confluent.cloud
        api_key: "${{aws_secrets:schema-secret:schema_registry_api_key}}"
        api_secret: "${{aws_secrets:schema-secret:schema_registry_api_secret}}"
        basic_auth_credentials_source: "USER_INFO"
```

```
  sink:
  - opensearch:
      hosts: ["https://search-mydomain.us-west-2.es.amazonaws.com"]
      aws:
          sts_role_arn: "arn:aws:iam::{account-id}:role/pipeline-role"
          region: "us-west-2"
      index: "confluent-index"
extension:
  aws:
    secrets:
      confluent-kafka-secret:
        secret_id: "my-kafka-secret"
        region: "us-west-2"
        sts_role_arn: "arn:aws:iam::{account-id}:role/pipeline-role"
      schema-secret:
        secret_id: "my-self-managed-kafka-schema"
        region: "us-west-2"
        sts_role_arn: "arn:aws:iam::{account-id}:role/pipeline-role"
```

您可以使用預先設定的藍圖來建立此管道。如需詳細資訊，請參閱the section called “使用藍圖建立管道”。

搭配使用 OpenSearch 擷取管線 Amazon Managed Streaming for Apache Kafka

您可以使用 Kafka 外掛程式，將 Apache Kafka (AmazonMSK) 的 Amazon 受管串流中的資料擷取到您的擷取管道中。 OpenSearch 透過 AmazonMSK，您可以建置和執行使用 Apache Kafka 處理串流資料的應用程式。 OpenSearch 攝入用 AWS PrivateLink 於連接到 Amazon MSK。您可以從 Amazon MSK 和 Amazon MSK 無伺服器叢集擷取資料。這兩個程序之間的唯一差別是您在設定管道之前必須採取的先決步驟。

主題

- Amazon MSK 前提
- Amazon MSK 無伺服器先決條件
- 步驟 1：設定管線角色
- 步驟 2：建立管道
- 步驟 3：（可選）使用 AWS Glue 模式註冊表
- 步驟 4：(選擇性) 為 Amazon MSK 管道設定建議的運算單元 (OCUs)

Amazon MSK 前提

建立 OpenSearch 擷取管道之前，請執行下列步驟：

1. 按照 Amazon 的 Apache Kafka 受管串流開發人員指南中的建立叢集中的步驟，建立 Amazon MSK 佈建的叢集。對於「代理**t3**類型」，請選擇類型以外的任何選項，因為「 OpenSearch 擷取」不支援這些選項。
2. 叢集處於 [作用中] 狀態之後，請依照開啟多重VPC連線中的步驟執行。
3. 依照將叢集原則附加至叢集中的步驟，根據您的MSK叢集和管線是否在相同的情況下，附加下列其中一個原則 AWS 帳戶。此政策允許 OpenSearch 擷取建立與 Amazon MSK 叢集的 AWS PrivateLink 連線，並從 Kafka 主題讀取資料。確保您使用自己`resource`的更新ARN。

   當您的叢集和管線位於相同時，下列原則適用 AWS 帳戶：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "osis.amazonaws.com"
      },
      "Action": [
        "kafka:CreateVpcConnection",
        "kafka:DescribeClusterV2"
      ],
      "Resource": "arn:aws:kafka:us-east-1:{account-id}:cluster/cluster-name/cluster-
id"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "osis-pipelines.amazonaws.com"
      },
      "Action": [
        "kafka:CreateVpcConnection",
        "kafka:GetBootstrapBrokers",
        "kafka:DescribeClusterV2"
      ],
      "Resource": "arn:aws:kafka:us-east-1:{account-id}:cluster/cluster-name/cluster-
id"
    }
```

```
  ]
}
```

如果您的 Amazon MSK 叢集與管道 AWS 帳戶 不同，請改為附加以下政策。請注意，只有佈建的 Amazon 叢集才能進行跨帳戶存取，而不能使用 Amazon MSK 無伺服器MSK叢集。的ARN AWS `principal`應該是您提供給 pipleine YAML 配置的相同管道角色：ARN

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "osis.amazonaws.com"
      },
      "Action": [
        "kafka:CreateVpcConnection",
        "kafka:DescribeClusterV2"
      ],
      "Resource": "arn:aws:kafka:us-east-1:{msk-account-id}:cluster/cluster-
name/cluster-id"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "osis-pipelines.amazonaws.com"
      },
      "Action": [
        "kafka:CreateVpcConnection",
        "kafka:GetBootstrapBrokers",
        "kafka:DescribeClusterV2"
      ],
      "Resource": "arn:aws:kafka:us-east-1:{msk-account-id}:cluster/cluster-
name/cluster-id"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::{pipeline-account-id}:role/pipeline-role"
      },
      "Action": [
        "kafka-cluster:*",
        "kafka:*"
```

```
      ],
      "Resource": [
        "arn:aws:kafka:us-east-1:{msk-account-id}:cluster/cluster-name/cluster-id",
        "arn:aws:kafka:us-east-1:{msk-account-id}:topic/cluster-name/cluster-id/*",
        "arn:aws:kafka:us-east-1:{msk-account-id}:group/cluster-name/*"
      ]
    }
  ]
}
```

4. 依照建立主題中的步驟建立 Kafka 主題。確保它*BootstrapServerString*是私有端點（單一VPC）引導程序之一URLs。的值`--replication-factor`應該是`2`或`3`，根據 Amazon MSK 叢集擁有的區域數量而定。的值至少`--partitions`應該是`10`。
5. 按照產生和消耗數據中的步驟生成和消耗數據。同樣，確保這*BootstrapServerString*是您的私有端點（單一VPC）引導程序之一URLs。

Amazon MSK 無伺服器先決條件

建立 OpenSearch 擷取管道之前，請執行下列步驟：

1. 按照 Amazon MSK Ap ache Kafka 受管串流開發人員指南中的建立MSK無伺服器叢集中的步驟，建立 Amazon 無伺服器叢集。
2. 叢集處於作用中狀態之後，請遵循將叢集原則連結至叢集中的MSK步驟，以附加下列原則。確保您使用自己`resource`的更新ARN。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "osis.amazonaws.com"
      },
      "Action": [
        "kafka:CreateVpcConnection",
        "kafka:DescribeClusterV2"
      ],
      "Resource": "arn:aws:kafka:us-east-1:{account-id}:cluster/cluster-name/cluster-
id"
    },
    {
```

```
        "Effect": "Allow",
        "Principal": {
          "Service": "osis-pipelines.amazonaws.com"
        },
        "Action": [
          "kafka:CreateVpcConnection",
          "kafka:GetBootstrapBrokers",
          "kafka:DescribeClusterV2"
        ],
        "Resource": "arn:aws:kafka:us-east-1:{account-id}:cluster/cluster-name/cluster-
id"
      }
    ]
}
```

此政策允許 OpenSearch 擷取建立與 Amazon MSK 無伺服器叢集的 AWS PrivateLink 連線，並從 Kafka 主題讀取資料。當您的叢集和管道處於相同狀態時 AWS 帳戶，此政策必須為真，因為 Amazon MSK 無伺服器不支援跨帳戶存取。

3. 依照建立主題中的步驟建立 Kafka 主題。確保這*BootstrapServerString*是您的簡單身份驗證和安全層（SASL）IAM引導程序之一URLs。的值`--replication-factor`應該是2或3，根據 Amazon MSK 無伺服器叢集所擁有的區域數目而定。的值至少`--partitions`應該是10。
4. 按照產生和消耗數據中的步驟生成和消耗數據。同樣，請確保這*BootstrapServerString*是您的簡單身份驗證和安全層（SASL）IAM引導程序之一URLs。

步驟 1：設定管線角色

設定 Amazon MSK 或無伺服器叢集之後，請在管道組態中使用的管道角色中新增以下 Kafka 許可：

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "kafka-cluster:Connect",
                "kafka-cluster:AlterCluster",
                "kafka-cluster:DescribeCluster",
                "kafka:DescribeClusterV2",
                "kafka:GetBootstrapBrokers"
            ],
```

```
            "Resource": [
                "arn:aws:kafka:us-east-1:{account-id}:cluster/cluster-name/cluster-id"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "kafka-cluster:*Topic*",
                "kafka-cluster:ReadData"
            ],
            "Resource": [
                "arn:aws:kafka:us-east-1:{account-id}:topic/cluster-name/cluster-
id/topic-name"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "kafka-cluster:AlterGroup",
                "kafka-cluster:DescribeGroup"
            ],
            "Resource": [
                "arn:aws:kafka:us-east-1:{account-id}:group/cluster-name/*"
            ]
        }
    ]
}
```

步驟 2：建立管道

然後，您可以設定如下所示的 OpenSearch 擷取管線，該管道會將 Kafka 指定為來源：

```
version: "2"
log-pipeline:
  source:
    kafka:
      acknowledgements: true
      topics:
      - name: "topic-name"
        group_id: "group-id"
      aws:
        msk:
          arn: "arn:aws:kafka:{region}:{account-id}:cluster/cluster-name/cluster-id"
```

```
        region: "us-west-2"
        sts_role_arn: "arn:aws:iam::{account-id}:role/pipeline-role"
  processor:
  - grok:
      match:
        message:
        - "%{COMMONAPACHELOG}"
  - date:
      destination: "@timestamp"
      from_time_received: true
  sink:
  - opensearch:
      hosts: ["https://search-domain-endpoint.us-east-1.es.amazonaws.com"]
      index: "index_name"
      aws_sts_role_arn: "arn:aws:iam::{account-id}:role/pipeline-role"
      aws_region: "us-east-1"
      aws_sigv4: true
```

您可以使用預先設定的 Amazon MSK 藍圖來建立此管道。如需詳細資訊，請參閱the section called “使用藍圖建立管道”。

步驟 3：（可選）使用 AWS Glue 模式註冊表

將 OpenSearch 擷取與 Amazon 搭配使用時MSK，可以針對架 AWS Glue 構登錄中託管的結構描述使用AVRO資料格式。使用結AWS Glue 構描述登錄，您可以集中探索、控制和發展資料串流結構描述。

若要使用此選項，請在管線組態type中啟用結構描述：

```
schema:
  type: "aws_glue"
```

您還必須在管道角色中提供 AWS Glue 讀取存取權限。您可以使用稱為的 AWS 受管理策略AWSGlueSchemaRegistryReadonlyAccess。此外，您的登錄檔必須 AWS 帳戶 與 OpenSearch 擷取管道位於相同的區域。

步驟 4：(選擇性) 為 Amazon MSK 管道設定建議的運算單元 (OCUs)

每個運算單元每個主題都有一個取用者。經紀人平衡這些消費者對於給定主題之間的分區。但是，當分區數量大於消費者數量時，Amazon 會在每個消費者上MSK託管多個分區。 OpenSearch 擷取具有內建的 auto 調整功能，可根據管道中的CPU使用量或擱置記錄數量來擴展或縮減。

若要取得最佳效能，請將您的分割區分散到多個運算單元以進行 parallel 處 如果主題有大量的分割區 (例如，超過 96 個，這是OCUs每個管線的最大值)，我們建議您將管道設定為 1—96 OCUs。這是因為它會根據需要自動擴展。如果主題的分割區數目很少 (例如，小於 96)，請將最大運算單元保持與分割區數目相同。

當管線有多個主題時，請選擇分割區數目最多的主題作為配置最大計算單位的參照。透過將具有新集合的另一個管道新增OCUs至相同主題和用戶群組，您可以幾乎線性地擴展輸送量。

搭配 Amazon S3 使用 OpenSearch 擷取管道

透過 OpenSearch 擷取，您可以使用 Amazon S3 做為來源或目的地。當您使用 Amazon S3 做為來源時，您會將資料傳送到 OpenSearch 擷取管道。使用 Amazon S3 做為目的地時，您可以從 OpenSearch 擷取管道將資料寫入一或多個 S3 儲存貯體。

主題

- Amazon S3 作為來源
- Amazon S3 作為目的地
- Amazon S3 跨賬戶作為來源

Amazon S3 作為來源

您可以透過兩種方式使用 Amazon S3 做為處理資料的來源 — 透過 S3 SQS 處理和排程掃描。

當您需要在檔案寫入 S3 之後進行近乎即時的掃描時，請使用 S3 SQS 處理。您可以設定 Amazon S3 儲存貯體，隨時在儲存貯體中存放或修改物件時引發事件。使用一次性或週期性排程掃描來批次處理 S3 儲存貯體中的資料。

主題

- 必要條件
- 步驟 1：設定管線角色
- 步驟 2：建立管道

必要條件

若要使用 Amazon S3 做為排程掃描或 S3 SQS 處理的 OpenSearch 擷取管道來源，請先建立 S3 儲存貯體。

> **Note**
>
> 如果在 OpenSearch 擷取管道中用作來源的 S3 儲存貯體位於不同的儲存貯體 AWS 帳戶，您還需要在儲存貯體上啟用跨帳戶讀取權限。這可讓管線讀取和處理資料。若要啟用跨帳戶許可，請參閱 Amazon S3 使用者指南中的儲存貯體擁有者授予跨帳戶儲存貯體許可。
> 如果您的 S3 儲存貯體位於多個帳戶中，請使用`bucket_owners`地圖。如需範例，請參閱 OpenSearch文件中的跨帳戶 S3 存取。

若要設定 S3-SQS 處理，您還需要執行下列步驟：

1. 創建一個 Amazon SQS 隊列。
2. 在 S3 儲存貯體上啟用事件通知，並將SQS佇列作為目的地。

步驟 1：設定管線角色

與其他將資料推送至管道的來源外掛程式不同，S3 來源外掛程式具有以讀取為基礎的架構，其中管道會從來源擷取資料。

因此，為了讓管道從 S3 讀取，您必須在管道的 S3 來源組態中指定一個角色，該角色可同時存取 S3 儲存貯體和 Amazon SQS 佇列。管線將扮演此角色，以便從佇列讀取資料。

> **Note**
>
> 您在 S3 來源組態中指定的角色必須是管道角色。因此，您的管道角色必須包含兩個不同的許可政策 — 一個用於寫入接收器，另一個用於從 S3 來源提取。您必須`sts_role_arn`在所有配管元件中使用相同的配管元件。

下列範例政策顯示使用 S3 作為來源所需的權限：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action":[
          "s3:ListBucket",
          "s3:GetBucketLocation",
```

```
            "s3:GetObject"
        ],
        "Resource": "arn:aws:s3:::my-bucket/*"
    },
    {
        "Effect":"Allow",
        "Action":"s3:ListAllMyBuckets",
        "Resource":"arn:aws:s3:::*"
    },
    {
        "Effect": "Allow",
        "Action": [
          "sqs:DeleteMessage",
          "sqs:ReceiveMessage",
          "sqs:ChangeMessageVisibility"
        ],
        "Resource": "arn:aws:sqs:us-west-2:{account-id}:MyS3EventSqsQueue"
    }
  ]
}
```

您必須將這些權限附加到您在 S3 來源外掛程式組態中的`sts_role_arn`選項中指定的IAM角色：

```
version: "2"
source:
  s3:
    ...
    aws:
      ...
      sts_role_arn: arn:aws:iam::{account-id}:role/pipeline-role
processor:
  ...
sink:
  - opensearch:
      ...
```

步驟 2：建立管道

設定許可後，您可以根據 Amazon S3 使用案例設定 OpenSearch 擷取管道。

S3-SQS 處理

若要設定 S3 SQS 處理，請設定管道以將 S3 指定為來源並設定 Amazon SQS 通知：

```
version: "2"
s3-pipeline:
  source:
    s3:
      notification_type: "sqs"
      codec:
        newline: null
      sqs:
        queue_url: "https://sqs.us-east-1.amazonaws.com/{account-id}/ingestion-queue"
      compression: "none"
      aws:
        region: "us-east-1"
        # IAM role that the pipeline assumes to read data from the queue. This role
 must be the same as the pipeline role.
        sts_role_arn: "arn:aws:iam::{account-id}:role/pipeline-role"
  processor:
  - grok:
      match:
        message:
        - "%{COMMONAPACHELOG}"
  - date:
      destination: "@timestamp"
      from_time_received: true
  sink:
  - opensearch:
      hosts: ["https://search-domain-endpoint.us-east-1.es.amazonaws.com"]
      index: "index-name"
      aws:
        # IAM role that the pipeline assumes to access the domain sink
        sts_role_arn: "arn:aws:iam::{account-id}:role/pipeline-role"
        region: "us-east-1"
```

如果您在 Amazon S3 上處理小型檔案時發現CPU使用率低，請考慮修改`workers`選項的值來增加輸送量。如需詳細資訊，請參閱 S3 外掛程式組態選項。

預約掃瞄

若要設定排程掃描，請使用適用於所有 S3 儲存貯體的掃描層級或儲存貯體層級的排程來設定管道。儲存貯體層級排程或掃描間隔組態一律會覆寫掃描層級組態。

您可以使用一次性掃描 (非常適合資料移轉) 或週期性掃描 (非常適合批次處理) 來設定排程掃描。

若要將管道設定為從 Amazon S3 讀取，請使用預先設定的 Amazon S3 藍圖。您可以編輯管線組態的scan部分，以符合您的排程需求。如需詳細資訊，請參閱the section called “使用藍圖建立管道”。

一次性掃描

一次性預約掃瞄會執行一次。在YAML配置中，您可以使用start_time和end_time來指定何時掃描值區中的物件。或者，您也可range以使用指定要掃描值區中物件的相對於目前時間的時間間隔。

例如，設定為PT4H掃瞄過去四小時內建立的所有檔案的範圍。若要將一次性掃描設定為第二次執行，您必須停止並重新啟動管線。如果您未設定範圍，則還必須更新開始和結束時間。

下列組態會針對這些值區中的所有值區和所有物件設定一次性掃描：

```
version: "2"
log-pipeline:
  source:
    s3:
      codec:
        csv:
      compression: "none"
      aws:
        region: "us-east-1"
        sts_role_arn: "arn:aws:iam::{account-id}:role/pipeline-role"
      acknowledgments: true
      scan:
        buckets:
          - bucket:
              name: my-bucket-1
              filter:
                include_prefix:
                  - Objects1/
                exclude_suffix:
                  - .jpeg
                  - .png
          - bucket:
              name: my-bucket-2
              key_prefix:
                include:
                  - Objects2/
                exclude_suffix:
                  - .jpeg
                  - .png
      delete_s3_objects_on_read: false
```

```
  processor:
    - date:
        destination: "@timestamp"
        from_time_received: true
  sink:
    - opensearch:
        hosts: ["https://search-domain-endpoint.us-east-1.es.amazonaws.com"]
        index: "index-name"
        aws:
          sts_role_arn: "arn:aws:iam::{account-id}:role/pipeline-role"
          region: "us-east-1"
        dlq:
          s3:
            bucket: "my-bucket-1"
            region: "us-east-1"
            sts_role_arn: "arn:aws:iam::{account-id}:role/pipeline-role"
```

下列組態設定在指定時間範圍內對所有儲存貯體進行一次性掃描。這表示 S3 只會處理建立時間落在此視窗內的物件。

```
scan:
  start_time: 2023-01-21T18:00:00.000Z
  end_time: 2023-04-21T18:00:00.000Z
  buckets:
    - bucket:
        name: my-bucket-1
        filter:
          include:
            - Objects1/
          exclude_suffix:
            - .jpeg
            - .png
    - bucket:
        name: my-bucket-2
        filter:
          include:
            - Objects2/
          exclude_suffix:
            - .jpeg
            - .png
```

下列組態會在掃描層級和儲存貯體層級設定一次性掃描。儲存貯體層級的開始和結束時間會覆寫掃描層級的開始和結束時間。

```
scan:
  start_time: 2023-01-21T18:00:00.000Z
  end_time: 2023-04-21T18:00:00.000Z
  buckets:
    - bucket:
        start_time: 2023-01-21T18:00:00.000Z
        end_time: 2023-04-21T18:00:00.000Z
        name: my-bucket-1
        filter:
          include:
            - Objects1/
          exclude_suffix:
            - .jpeg
            - .png
    - bucket:
        start_time: 2023-01-21T18:00:00.000Z
        end_time: 2023-04-21T18:00:00.000Z
        name: my-bucket-2
        filter:
          include:
            - Objects2/
          exclude_suffix:
            - .jpeg
            - .png
```

停止管線會移除在停止之前管線掃描哪些物件的任何預先存在的參照。如果單一掃描管線停止，它會在啟動後再次掃描所有物件，即使它們已經被掃描也是如此。如果您需要停止單一掃描管線，建議您先變更時間範圍，然後再次啟動管道。

如果您需要依照開始時間和結束時間篩選物件，停止和啟動管線是唯一的選擇。如果您不需要依照開始時間和結束時間進行篩選，您可以依名稱篩選物件。按名稱翻轉不需要您停止並啟動管道。要做到這一點，使用`include_prefix`和`exclude_suffix`。

週期性掃描

週期性排程掃描會以定期排程的間隔執行指定的 S3 儲存貯體掃描。您只能在掃描層級設定這些間隔，因為不支援個別儲存貯體層級組態。

在您的YAML組態中，會`interval`指定週期性掃描的頻率，且可以介於 30 秒到 365 天之間。這些掃描中的第一個掃描始終會在您建立管道時進行。定`count`義掃描執行個體的總數。

下列組態會設定週期性掃描，掃描間隔延遲 12 小時：

```
scan:
  scheduling:
    interval: PT12H
    count: 4
  buckets:
    - bucket:
        name: my-bucket-1
        filter:
          include:
            - Objects1/
          exclude_suffix:
            - .jpeg
            - .png
    - bucket:
        name: my-bucket-2
        filter:
          include:
            - Objects2/
          exclude_suffix:
            - .jpeg
            - .png
```

Amazon S3 作為目的地

若要將資料從 OpenSearch 擷取管道寫入 S3 儲存貯體，請使用預先設定的 S3 藍圖建立具有 S3 接收器的管道。此管道會將選擇性資料路由到接 OpenSearch 收器，並同時傳送所有資料以在 S3 中存檔。如需詳細資訊，請參閱the section called “使用藍圖建立管道”。

建立 S3 接收器時，您可以從各種接收器轉碼器指定偏好的格式。例如，如果您想要以欄式格式寫入資料，請選擇「鑲木地板」或「Avro」轉碼器。如果您偏好以列為基礎的格式，請選擇JSON或 ND-JSON。若要在指定結構定義中將資料寫入 S3，您也可以使用 Avro 格式在接收器轉碼器中定義內嵌結構描述。

下列範例會定義 S3 接收器中的內嵌結構描述：

```
- s3:
  codec:
    parquet:
      schema: >
        {
           "type" : "record",
           "namespace" : "org.vpcFlowLog.examples",
```

```
            "name" : "VpcFlowLog",
            "fields" : [
              { "name" : "version", "type" : "string"},
              { "name" : "srcport", "type": "int"},
              { "name" : "dstport", "type": "int"},
              { "name" : "start", "type": "int"},
              { "name" : "end", "type": "int"},
              { "name" : "protocol", "type": "int"},
              { "name" : "packets", "type": "int"},
              { "name" : "bytes", "type": "int"},
              { "name" : "action", "type": "string"},
              { "name" : "logStatus", "type" : "string"}
            ]
          }
```

定義此結構描述時，請指定可能存在於管道傳送給接收器的不同事件類型中的所有索引鍵的超集合。

例如，如果事件可能遺失索引鍵，請在結構描述中加入該索引鍵並加入`null`值。空值聲明允許模式處理非統一數據（其中一些事件具有這些鍵，而其他事件則沒有）。當傳入事件確實存在這些鍵時，它們的值會寫入接收器。

此結構描述定義充當篩選器，只允許將已定義的索引鍵傳送至接收器，並從傳入事件中卸除未定義的索引鍵。

您也可以在接收器`exclude_keys`中使用`include_keys`和來篩選路由到其他接收器的資料。這兩個篩選器是互斥的，因此您一次只能在結構描述中使用一個篩選器。此外，您不能在使用者定義的結構描述中使用它們。

若要使用此類篩選器建立管道，請使用預先設定的接收器篩選器藍圖。如需詳細資訊，請參閱the section called “使用藍圖建立管道”。

Amazon S3 跨賬戶作為來源

您可以授與 Amazon S3 跨帳戶的存取權，以便 OpenSearch 擷取管道可以存取另一個帳戶中的 S3 儲存貯體作為來源。若要啟用跨帳戶存取，請參閱 Amazon S3 使用者指南中的儲存貯體擁有者授予跨帳戶儲存貯體許可。授與存取權後，請確保管線角色具有必要的權限。

然後，您可以使用建立YAML組態，`bucket_owners`以啟用跨帳戶存取 Amazon S3 儲存貯體做為來源：

```
s3-pipeline:
```

```
source:
 s3:
  notification_type: "sqs"
  codec:
   csv:
    delimiter: ","
    quote_character: "\""
    detect_header: True
  sqs:
   queue_url: "https://sqs.ap-northeast-1.amazonaws.com/401447383613/test-s3-queue"
  bucket_owners:
   my-bucket-01: 123456789012
   my-bucket-02: 999999999999
  compression: "gzip"
```

使用帶有 Amazon 安全湖的 OpenSearch 擷取管道

您可以使用 S3 來源外掛程式將資料從 Amazon 安全湖導入您的 OpenSearch 擷取管道。Security Lake 會自動將來自 AWS 環境、內部部署環境和 SaaS 提供者的安全性資料集中到專門建置的資料湖。您可以建立將資料從 Security Lake 複製到 OpenSearch 擷取管線的訂閱，然後將其寫入您的 OpenSearch 服務網域或 OpenSearch 無伺服器集合。

若要將管線設定為從安全湖讀取，請使用預先設定的安全湖藍圖。該藍圖包括用於從 Security Lake 導入開放網絡安全架構框架（OCSF）實木複合地板文件的默認配置。如需詳細資訊，請參閱the section called “使用藍圖建立管道”。

主題

- 必要條件
- 步驟 1：設定管線角色
- 步驟 2：建立管道

必要條件

建立 OpenSearch 擷取管道之前，請執行下列步驟：

- 啟用安全湖泊。
- 在安全湖中建立訂閱者。
  - 選擇您要內嵌到管道中的來源。

- 若為訂閱者認證，請新增您 AWS 帳戶 要建立管線之位置的 ID。對於外部 ID，請指定`OpenSearchIngestion-{accountid}`。
- 對於資料存取方法，請選擇 S3。
- 如需通知詳細資訊，請選擇SQS佇列。

當您建立訂閱者時，Security Lake 會自動建立兩個內嵌許可政策 — 一個適用於 S3，另一個用於。SQS原則採用下列格式：`AmazonSecurityLake-{12345}-S3`和`AmazonSecurityLake-{12345}-SQS`。若要允許管道存取訂閱者來源，您必須將必要權限與管線角色建立關聯。

步驟 1：設定管線角色

在中建立新的權限原則，IAM該原則僅結合 Security Lake 自動建立的兩個原則中的必要權限。下列範例原則顯示 OpenSearch 擷取管線從多個 Security Lake 來源讀取資料所需的最低權限：

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action":[
            "s3:GetObject"
         ],
         "Resource":[
            "arn:aws:s3:::aws-security-data-lake-{region}-abcde/aws/
LAMBDA_EXECUTION/1.0/*",
            "arn:aws:s3:::aws-security-data-lake-{region}-abcde/aws/S3_DATA/1.0/*",
            "arn:aws:s3:::aws-security-data-lake-{region}-abcde/aws/VPC_FLOW/1.0/*",
            "arn:aws:s3:::aws-security-data-lake-{region}-abcde/aws/ROUTE53/1.0/*",
            "arn:aws:s3:::aws-security-data-lake-{region}-abcde/aws/SH_FINDINGS/1.0/*"
         ]
      },
      {
         "Effect":"Allow",
         "Action":[
            "sqs:ReceiveMessage",
            "sqs:DeleteMessage"
         ],
         "Resource":[
            "arn:aws:sqs:{region}:{account-id}:AmazonSecurityLake-abcde-Main-Queue"
         ]
```

```
      }
    ]
}
```

> **Important**
>
> 安全湖不會為您管理管道角色原則。如果您從 Security Lake 訂閱新增或移除來源，則必須手動更新原則。Security Lake 會為每個記錄來源建立磁碟分割，因此您必須手動新增或移除管線角色中的權限。

您必須將這些權限附加到您IAM在 S3 來源外掛程式組態下的`sts_role_arn`選項中指定的角色`sqs`。

```
version: "2"
source:
  s3:
    ...
    sqs:
      queue_url: "https://sqs.{region}.amazonaws.com/{account-id}/
AmazonSecurityLake-abcde-Main-Queue"
    aws:
      ...
      sts_role_arn: arn:aws:iam::{account-id}:role/pipeline-role
processor:
  ...
sink:
  - opensearch:
      ...
```

步驟 2：建立管道

將權限新增至管線角色後，請使用預先設定的 Security Lake 藍圖來建立管線。如需詳細資訊，請參閱the section called “使用藍圖建立管道”。

您必須在`s3`來源組態中指定`queue_url`選項，也就是URL要讀取的 Amazon SQS 佇列。若要格式化URL，請在訂閱者組態中找到訂閱端點，然後變更`arn:aws:`為`https://`。例如：`https://sqs.{region}.amazonaws.com/{account-id}/AmazonSecurityLake-abdcef-Main-Queue`。

您`sts_role_arn`在 S3 來源組態中指定ARN的必須是管道角色。

使用具有流利位 OpenSearch 元的擷取管線

此範例 Fluent Bit 組態檔案會將記錄資料從 Fluent Bit 傳送至 OpenSearch 擷取管線。如需有關擷取記錄檔資料的詳細資訊，請參閱資料準備器文件中的記錄分析。

注意下列事項：

- 該host值必須是您的管道端點。例如：*pipeline-endpoint*.us-east-1.osis.amazonaws.com。
- aws_service 值必須為 osis。
- 此aws_role_arn值是用戶端承擔並用於簽章版本 4 驗證ARN的 AWS IAM角色。

```
[INPUT]
  name                  tail
  refresh_interval      5
  path                  /var/log/test.log
  read_from_head        true

[OUTPUT]
  Name http
  Match *
  Host pipeline-endpoint.us-east-1.osis.amazonaws.com
  Port 443
  URI /log/ingest
  Format json
  aws_auth true
  aws_region us-east-1
  aws_service osis
  aws_role_arn arn:aws:iam::{account-id}:role/ingestion-role
  Log_Level trace
  tls On
```

然後，您可以設定如下所示的 OpenSearch 擷取管道，其HTTP作為來源：

```
version: "2"
unaggregated-log-pipeline:
  source:
    http:
      path: "/log/ingest"
  processor:
    - grok:
```

```
        match:
          log:
            - "%{TIMESTAMP_ISO8601:timestamp} %{NOTSPACE:network_node}
 %{NOTSPACE:network_host} %{IPORHOST:source_ip}:%{NUMBER:source_port:int} ->
 %{IPORHOST:destination_ip}:%{NUMBER:destination_port:int} %{GREEDYDATA:details}"
    - grok:
        match:
          details:
            - "'%{NOTSPACE:http_method} %{NOTSPACE:http_uri}' %{NOTSPACE:protocol}"
            - "TLS%{NOTSPACE:tls_version} %{GREEDYDATA:encryption}"
            - "%{NUMBER:status_code:int} %{NUMBER:response_size:int}"
    - delete_entries:
        with_keys: ["details", "log"]

  sink:
    - opensearch:
        hosts: ["https://search-domain-endpoint.us-east-1.es.amazonaws.com"]
        index: "index_name"
        index_type: custom
        bulk_size: 20
        aws:
          # IAM role that the pipeline assumes to access the domain sink
          sts_role_arn: "arn:aws:iam::{account-id}:role/pipeline-role"
          region: "us-east-1"
```

搭配 Fluentd 使用 OpenSearch 擷取管線

Fluentd 是一個開放原始碼的資料收集生態系統，可提供不同SDKs的語言和子專案，例如 Fluent Bit。此範例 Fluentd 設定檔會將記錄資料從 Fluentd 傳送至擷取管線。 OpenSearch 如需有關擷取記錄檔資料的詳細資訊，請參閱資料準備器文件中的記錄分析。

注意下列事項：

- 該`endpoint`值必須是您的管道端點。例如：*`pipeline-endpoint`*`.us-east-1.osis.amazonaws.com/apache-log-pipeline/logs`。
- `aws_service` 值必須為 `osis`。
- 此`aws_role_arn`值是用戶端承擔並用於簽章版本 4 驗證ARN的 AWS IAM角色。

```
<source>
  @type tail
  path logs/sample.log
```

```
  path_key log
  tag apache
  <parse>
    @type none
  </parse>
</source>

<filter apache>
  @type record_transformer
  <record>
    log ${record["message"]}
  </record>
</filter>

<filter apache>
  @type record_transformer
  remove_keys message
</filter>

<match apache>
  @type http
  endpoint pipeline-endpoint.us-east-1.osis.amazonaws.com/apache-log-pipeline/logs
  json_array true

  <auth>
    method aws_sigv4
    aws_service osis
    aws_region us-east-1
    aws_role_arn arn:aws:iam::{account-id}:role/ingestion-role
  </auth>

  <format>
    @type json
  </format>

  <buffer>
    flush_interval 1s
  </buffer>
</match>
```

然後，您可以設定如下所示的 OpenSearch 擷取管道，其HTTP作為來源：

```
version: "2"
```

```
apache-log-pipeline:
  source:
    http:
      path: "/${pipelineName}/logs"
  processor:
    - grok:
        match:
          log:
            - "%{TIMESTAMP_ISO8601:timestamp} %{NOTSPACE:network_node}
 %{NOTSPACE:network_host} %{IPORHOST:source_ip}:%{NUMBER:source_port:int} ->
 %{IPORHOST:destination_ip}:%{NUMBER:destination_port:int} %{GREEDYDATA:details}"
  sink:
    - opensearch:
        hosts: ["https://search-domain-endpoint.us-east-1.es.amazonaws.com"]
        index: "index_name"
        aws_sts_role_arn: "arn:aws:iam::{account-id}:role/pipeline-role"
        aws_region: "us-east-1"
        aws_sigv4: true
```

搭 OpenTelemetry 配收集器使用 OpenSearch 擷取管線

此範例OpenTelemetry 組態檔案會從 OpenTelemetry收集器匯出追蹤資料，並將其傳送至 OpenSearch 擷取管線。如需有關擷取追蹤資料的詳細資訊，請參閱資料準備器文件中的追蹤分析。

注意下列事項：

- 該`endpoint`值必須包含您的管道端點。例如：`https://pipeline-endpoint.us-east-1.osis.amazonaws.com`。
- `service` 值必須為 `osis`。
- OTLP/HTTP匯出器的`compression`選項必須與管線 OpenTelemetry 來源上的`compression`選項相符。

```
extensions:
  sigv4auth:
    region: "us-east-1"
    service: "osis"

receivers:
  jaeger:
    protocols:
      grpc:
```

```
exporters:
  otlphttp:
    traces_endpoint: "https://pipeline-endpoint.us-east-1.osis.amazonaws.com/v1/traces"
    auth:
      authenticator: sigv4auth
    compression: none

service:
  extensions: [sigv4auth]
  pipelines:
    traces:
      receivers: [jaeger]
      exporters: [otlphttp]
```

然後，您可以設定如下所示的 OpenSearch 擷取管線，將 OTeltrace 外掛程式指定為來源：

```
version: "2"
otel-trace-pipeline:
  source:
    otel_trace_source:
      path: "/v1/traces"
  processor:
    - trace_peer_forwarder:
  sink:
    - pipeline:
        name: "trace-pipeline"
    - pipeline:
        name: "service-map-pipeline"
trace-pipeline:
  source:
    pipeline:
      name: "otel-trace-pipeline"
  processor:
    - otel_traces:
  sink:
    - opensearch:
        hosts: ["https://search-domain-endpoint.us-east-1.es.amazonaws.com"]
        index_type: trace-analytics-raw
        aws:
          # IAM role that OpenSearch Ingestion assumes to access the domain sink
          sts_role_arn: "arn:aws:iam::{account-id}:role/pipeline-role"
          region: "us-east-1"
```

```
service-map-pipeline:
  source:
    pipeline:
      name: "otel-trace-pipeline"
  processor:
    - service_map:
  sink:
    - opensearch:
        hosts: ["https://search-domain-endpoint.us-east-1.es.amazonaws.com"]
        index_type: trace-analytics-service-map
        aws:
          # IAM role that the pipeline assumes to access the domain sink
          sts_role_arn: "arn:aws:iam::{account-id}:role/pipeline-role"
          region: "us-east-1"
```

如需其他管道範例，請參閱預先設定的追蹤分析藍圖。如需詳細資訊，請參閱the section called “使用藍圖建立管道”。

使用 OpenSearch 擷取管線與卡夫卡

您可以使用具有自我管理 Kafka 的 OpenSearch 擷取管道，將資料串流至 Amazon OpenSearch 服務網域和無伺服器集合。 OpenSearch OpenSearch 擷取支援公用和私人網路組態，將資料從自我管理的 Kafka 串流到由 OpenSearch 服務或無伺服器管理的網域或集合。 OpenSearch

連接到公共卡夫卡集群

您可以使用 OpenSearch 擷取管道從具有公用設定的自我管理 Kafka 叢集遷移資料，這表示網域DNS名稱可以公開解析。若要這麼做，請以自我管理的 Kafka 作為來源設定 OpenSearch 擷取管道，並將 OpenSearch 服務或 OpenSearch 無伺服器設定為目的地。這會將您的串流資料從自我管理的來源叢集處理到 AWS管理的目的地網域或集合。

必要條件

建立 OpenSearch 擷取管道之前，請執行下列步驟：

1. 使用公用網路組態建立自我管理的 Kafka 叢集。叢集應包含您要擷取至 OpenSearch 服務的資料。
2. 建立您要將資料移轉至其中的 OpenSearch 服務網域或 OpenSearch 無伺服器集合。如需詳細資訊，請參閱建立 OpenSearch 服務網域和建立集合。
3. 在您的自我管理叢集上使用 AWS Secrets Manager. 按照旋轉密碼中的步驟啟用AWS Secrets Manager 密碼輪換。

4. 將資源型政策附加至您的網域，或將資料存取原則附加至您的集合。這些存取原則可讓 OpenSearch 擷取將資料從自我管理的叢集寫入您的網域或集合。

   下列範例網域存取原則允許您在下一個步驟中建立的管線角色將資料寫入網域。確保您使用自己`resource`的更新ARN。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::{pipeline-account-id}:role/pipeline-role"
      },
      "Action": [
        "es:DescribeDomain",
        "es:ESHttp*"
      ],
      "Resource": [
        "arn:aws:es:{region}:{account-id}:domain/domain-name"
      ]
    }
  ]
}
```

   若要建立具有正確權限的IAM角色，以存取集合或網域的寫入資料，請參閱網域的必要權限和集合的必要權限。

步驟 1：設定管線角色

設定 Kafka 管線必要條件之後，請設定要在管線組態中使用的管線角色，並新增寫入 OpenSearch 服務網域或 OpenSearch 無伺服器集合的權限，以及從 Secrets Manager 讀取密碼的權限。

步驟 2：建立管道

然後，您可以配置如下所示的 OpenSearch 擷取管道，該管道將 Kafka 指定為來源。

您可以指定多個 OpenSearch 服務網域做為資料的目的地。此功能可讓傳入資料進行條件式路由或複寫至多個 OpenSearch Service 網域。

您也可以將資料從來源 Confluent Kafka 叢集遷移到無伺服器集合 OpenSearch 。VPC請務必在管線組態中提供網路存取原則。您可以使用 Confluent 模式註冊表來定義一個 Confluent 模式。

```
version: "2"
kafka-pipeline:
  source:
    kafka:
      encryption:
        type: "ssl"
      topics:
        - name: "topic-name"
          group_id: "group-id"
      bootstrap_servers:
        - "bootstrap-server.us-west-2.aws.private.confluent.cloud:9092"
      authentication:
        sasl:
          plain:
            username: ${aws_secrets:confluent-kafka-secret:username}
            password: ${aws_secrets:confluent-kafka-secret:password}
      schema:
        type: confluent
        registry_url: https://my-registry.us-west-2.aws.confluent.cloud
        api_key: "${{aws_secrets:schema-secret:schema_registry_api_key}}"
        api_secret: "${{aws_secrets:schema-secret:schema_registry_api_secret}}"
        basic_auth_credentials_source: "USER_INFO"
  sink:
  - opensearch:
      hosts: ["https://search-mydomain.us-west-2.es.amazonaws.com"]
      aws:
          sts_role_arn: "arn:aws:iam::{account-id}:role/pipeline-role"
          region: "us-west-2"
      index: "confluent-index"
extension:
  aws:
    secrets:
      confluent-kafka-secret:
        secret_id: "my-kafka-secret"
        region: "us-west-2"
        sts_role_arn: "arn:aws:iam::{account-id}:role/pipeline-role"
      schema-secret:
        secret_id: "my-self-managed-kafka-schema"
        region: "us-west-2"
        sts_role_arn: "arn:aws:iam::{account-id}:role/pipeline-role"
```

您可以使用預先設定的藍圖來建立此管道。如需詳細資訊，請參閱the section called “使用藍圖建立管道”。

連接到卡夫卡集群 VPC

您也可以使用 OpenSearch 擷取管線，將資料從在. VPC 若要這麼做，請以自我管理的 Kafka 作為來源設定 OpenSearch 擷取管道，並將 OpenSearch 服務或 OpenSearch 無伺服器設定為目的地。這會將您的串流資料從自我管理的來源叢集處理到 AWS管理的目的地網域或集合。

必要條件

建立 OpenSearch 擷取管道之前，請執行下列步驟：

1. 使用VPC網路組態建立自我管理的 Kafka 叢集，其中包含您要擷取至服務的資料。 OpenSearch
2. 建立您要將資料移轉至其中的 OpenSearch 服務網域或 OpenSearch 無伺服器集合。如需詳細資訊，請參閱建立 OpenSearch 服務網域和建立集合。
3. 在您的自我管理叢集上使用 AWS Secrets Manager. 按照旋轉密碼中的步驟啟用AWS Secrets Manager 密碼輪換。
4. 獲取VPC可以訪問自我管理卡夫卡的 ID。選擇VPCCIDR要由 OpenSearch 擷取使用的。

> **Note**
>
> 如果您使用建立管道，您還必須將 OpenSearch 擷取管道附加到您的，才能使用自我管理的 Kafka。 AWS Management Console VPC若要這麼做，請找到 [網路設定] 區段，選取 [連接至] VPC 核取方塊，然後CIDR從提供的預設選項中選擇您的選項，或選取您自己的選項。您可以使用 CIDR「RFC1918 最新最佳作法」中定義的私人位址空間中的任何位址空間。若要提供自訂CIDR，請從下拉式功能表中選取「其他」。若要避免 OpenSearch 擷取與自我管理之間的 IP 位址發生衝突 OpenSearch，請確定自我管理 OpenSearch VPCCIDR與擷取的CIDR不同。 OpenSearch

5. 將資源型政策附加至您的網域，或將資料存取原則附加至您的集合。這些存取原則可讓 OpenSearch 擷取將資料從自我管理的叢集寫入您的網域或集合。

   下列範例網域存取原則允許您在下一個步驟中建立的管線角色將資料寫入網域。確保您使用自己`resource`的更新ARN。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
```

```
          "AWS": "arn:aws:iam::{pipeline-account-id}:role/pipeline-role"
        },
        "Action": [
          "es:DescribeDomain",
          "es:ESHttp*"
        ],
        "Resource": [
          "arn:aws:es:{region}:{account-id}:domain/domain-name"
        ]
      }
    ]
  }
```

若要建立具有正確權限的IAM角色，以存取集合或網域的寫入資料，請參閱網域的必要權限和集合的必要權限。

步驟 1：設定管線角色

設定管線必要條件後，請設定要在管線組態中使用的管線角色，並在角色中新增下列權限：

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "SecretsManagerReadAccess",
            "Effect": "Allow",
            "Action": [
                "secretsmanager:GetSecretValue"
            ],
            "Resource": ["arn:aws:secretsmanager:{region}:{account-id}:secret:secret-
name"]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:AttachNetworkInterface",
                "ec2:CreateNetworkInterface",
                "ec2:CreateNetworkInterfacePermission",
                "ec2:DeleteNetworkInterface",
                "ec2:DeleteNetworkInterfacePermission",
                "ec2:DetachNetworkInterface",
                "ec2:DescribeNetworkInterfaces"
```

```
            ],
            "Resource": [
                "arn:aws:ec2:*:{account-id}:network-interface/*",
                "arn:aws:ec2:*:{account-id}:subnet/*",
                "arn:aws:ec2:*:{account-id}:security-group/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeDhcpOptions",
                "ec2:DescribeRouteTables",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcs",
                "ec2:Describe*"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTags"
            ],
            "Resource": "arn:aws:ec2:*:*:network-interface/*",
            "Condition": {
               "StringEquals":
                    {
                        "aws:RequestTag/OSISManaged": "true"
                    }
            }
        }
    ]
}
```

您必須對用於建立 OpenSearch 擷取管道的IAM角色提供上述 Amazon EC2 許可，因為管道使用這些許可在您VPC的網路界面中建立和刪除網路界面。管線只能透過此網路介面存取 Kafka 叢集。

步驟 2：建立管道

然後，您可以配置如下所示的 OpenSearch 擷取管道，該管道將 Kafka 指定為來源。

您可以指定多個 OpenSearch 服務網域做為資料的目的地。此功能可讓傳入資料進行條件式路由或複寫至多個 OpenSearch Service 網域。

您也可以將資料從來源 Confluent Kafka 叢集遷移到無伺服器集合 OpenSearch 。VPC請務必在管線組態中提供網路存取原則。您可以使用 Confluent 模式註冊表來定義一個 Confluent 模式。

```
 version: "2"
kafka-pipeline:
  source:
    kafka:
      encryption:
        type: "ssl"
      topics:
        - name: "topic-name"
          group_id: "group-id"
      bootstrap_servers:
        - "bootstrap-server.us-west-2.aws.private.confluent.cloud:9092"
      authentication:
        sasl:
          plain:
            username: ${aws_secrets:confluent-kafka-secret:username}
            password: ${aws_secrets:confluent-kafka-secret:password}
      schema:
        type: confluent
        registry_url: https://my-registry.us-west-2.aws.confluent.cloud
        api_key: "${{aws_secrets:schema-secret:schema_registry_api_key}}"
        api_secret: "${{aws_secrets:schema-secret:schema_registry_api_secret}}"
        basic_auth_credentials_source: "USER_INFO"
  sink:
  - opensearch:
      hosts: ["https://search-mydomain.us-west-2.es.amazonaws.com"]
      aws:
          sts_role_arn: "arn:aws:iam::{account-id}:role/pipeline-role"
          region: "us-west-2"
      index: "confluent-index"
extension:
  aws:
    secrets:
      confluent-kafka-secret:
        secret_id: "my-kafka-secret"
        region: "us-west-2"
        sts_role_arn: "arn:aws:iam::{account-id}:role/pipeline-role"
      schema-secret:
        secret_id: "my-self-managed-kafka-schema"
        region: "us-west-2"
        sts_role_arn: "arn:aws:iam::{account-id}:role/pipeline-role"
```

您可以使用預先設定的藍圖來建立此管道。如需詳細資訊，請參閱the section called “使用藍圖建立管道”。

搭配使用 OpenSearch 擷取管線 OpenSearch

您可以使用具有自我管理 OpenSearch 或 Elasticsearch 的 OpenSearch 擷取管道，將資料遷移到 Amazon OpenSearch 服務網域和無伺服器集合。 OpenSearch OpenSearch 擷取支援公用和私人網路組態，以便從自我管理 OpenSearch 和 Elasticsearch 移轉資料。

公用 OpenSearch叢集的連線能力

您可以使用 OpenSearch 擷取管道從具有公用組態的自我管理 OpenSearch 或 Elasticsearch 叢集遷移資料，這表示可以公開解析網域DNS名稱。若要這麼做，請以自我管理 OpenSearch 或 Elasticsearch 做為來源設定 OpenSearch 擷取管道，將「服務」或「 OpenSearch 無伺 OpenSearch 服器」設定為目的地。如此可有效地將您的資料從自我管理的來源叢集移轉至受管 AWS理的目的地網域或集合。

必要條件

建立 OpenSearch 擷取管道之前，請執行下列步驟：

1. 建立包含您要移轉之資料的自我管理 OpenSearch 或 Elastisearch 叢集，並設定公用名稱。DNS
2. 建立您要將資料移轉至其中的 OpenSearch 服務網域或 OpenSearch 無伺服器集合。如需詳細資訊，請參閱建立 OpenSearch 服務網域和建立集合。
3. 在您的自我管理叢集上使用 AWS Secrets Manager. 按照旋轉密碼中的步驟啟用AWS Secrets Manager 密碼輪換。
4. 將資源型政策附加至您的網域，或將資料存取原則附加至您的集合。這些存取原則可讓 OpenSearch 擷取將資料從自我管理的叢集寫入您的網域或集合。

   下列範例網域存取原則允許您在下一個步驟中建立的管線角色將資料寫入網域。確保您使用自己`resource`的更新ARN。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::{pipeline-account-id}:role/pipeline-role"
      },
      "Action": [
```

```
        "es:DescribeDomain",
        "es:ESHttp*"
      ],
      "Resource": [
        "arn:aws:es:{region}:{account-id}:domain/domain-name"
      ]
    }
  ]
}
```

若要建立具有正確權限的IAM角色，以存取集合或網域的寫入資料，請參閱網域的必要權限和集合的必要權限。

步驟 1：設定管線角色

設定 OpenSearch 管線必要條件之後，請設定要在管線組態中使用的管線角色，並新增寫入 OpenSearch 服務網域或 OpenSearch 無伺服器集合的權限，以及從 Secrets Manager 讀取密碼的權限。

步驟 2：建立管道

然後，您可以設定如下所示的 OpenSearch 擷取管道，該管道會指定 OpenSearch 為來源。

您可以指定多個 OpenSearch 服務網域做為資料的目的地。此功能可讓傳入資料進行條件式路由或複寫至多個 OpenSearch Service 網域。

您也可以將資料從來源 OpenSearch 或 Elasticsearch 叢集移轉至 OpenSearch 無伺服器VPC集合。請務必在管線組態中提供網路存取原則。

```
version: "2"
opensearch-migration-pipeline:
  source:
    opensearch:
      acknowledgments: true
      host: [ "https://my-self-managed-cluster-name:9200" ]
      indices:
        include:
          - index_name_regex: "include-.*"
        exclude:
          - index_name_regex: '\..*'
      authentication:
        username: ${aws_secrets:secret:username}
```

```
        password: ${aws_secrets:secret:password}
        scheduling:
           interval: "PT2H"
           index_read_count: 3
           start_time: "2023-06-02T22:01:30.00Z"
  sink:
  - opensearch:
      hosts: ["https://search-mydomain.us-east-1.es.amazonaws.com"]
      aws:
          sts_role_arn: "arn:aws:iam::{account-id}:role/pipeline-role"
          region: "us-east-1"
          #Uncomment the following lines if your destination is an OpenSearch
 Serverless collection
          #serverless: true
          # serverless_options:
          #     network_policy_name: "network-policy-name"
      index: "${getMetadata(\"opensearch-index\")}"
      document_id: "${getMetadata(\"opensearch-document_id\")}"
      enable_request_compression: true
      dlq:
        s3:
          bucket: "bucket-name"
          key_path_prefix: "apache-log-pipeline/logs/dlq"
          region: "us-east-1"
          sts_role_arn: "arn:aws:iam::{account-id}:role/pipeline-role"
extension:
  aws:
    secrets:
      secret:
        secret_id: "my-opensearch-secret"
        region: "us-east-1"
        sts_role_arn: "arn:aws:iam::{account-id}:role/pipeline-role"
        refresh_interval: PT1H
```

您可以使用預先設定的藍圖來建立此管道。如需詳細資訊，請參閱the section called “使用藍圖建立管道”。

連線至 OpenSearch 叢集 VPC

您也可以使用 OpenSearch 擷取管道，將資料從在. OpenSearch VPC 若要這麼做，請以自我管理 OpenSearch 或 Elasticsearch 做為來源設定 OpenSearch 擷取管道，將「服務」或「 OpenSearch 無伺 OpenSearch 服器」設定為目的地。如此可有效地將您的資料從自我管理的來源叢集移轉至受管 AWS理的目的地網域或集合。

必要條件

建立 OpenSearch 擷取管道之前，請執行下列步驟：

1. 使用包含要移轉之資料的VPC網路組態來建立自我管理 OpenSearch 或 Elastisearch 叢集。
2. 建立您要將資料移轉至其中的 OpenSearch 服務網域或 OpenSearch 無伺服器集合。如需詳細資訊，請參閱建立 OpenSearch 服務網域和建立集合。
3. 在您的自我管理叢集上使用 AWS Secrets Manager. 按照旋轉密碼中的步驟啟用AWS Secrets Manager 密碼輪換。
4. 取得VPC可存取自我管理 OpenSearch 或彈性搜尋的識別碼。選擇VPCCIDR要由 OpenSearch 擷取使用的。

> **Note**
>
> 如果您使用建立管道，您還必須將 OpenSearch 擷取管道附加至您VPC的，才能使用自我管理 OpenSearch 或 Elasticsearch。 AWS Management Console 若要這麼做，請找到 [網路組態] 區段，選取 [連接至] VPC 核取方塊，然後CIDR從提供的預設選項中選擇您的選項，或選取您自己的選項。您可以使用 CIDR「RFC1918 最新最佳作法」中定義的私人位址空間中的任何位址空間。
> 若要提供自訂CIDR，請從下拉式功能表中選取「其他」。若要避免 OpenSearch 擷取與自我管理之間的 IP 位址發生衝突 OpenSearch，請確定自我管理 OpenSearch VPCCIDR與擷取的CIDR不同。 OpenSearch

5. 將資源型政策附加至您的網域，或將資料存取原則附加至您的集合。這些存取原則可讓 OpenSearch 擷取將資料從自我管理的叢集寫入您的網域或集合。

   下列範例網域存取原則允許您在下一個步驟中建立的管線角色將資料寫入網域。確保您使用自己`resource`的更新ARN。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::{pipeline-account-id}:role/pipeline-role"
      },
      "Action": [
        "es:DescribeDomain",
```

```
          "es:ESHttp*"
        ],
        "Resource": [
          "arn:aws:es:{region}:{account-id}:domain/domain-name"
        ]
      }
    ]
  }
```

若要建立具有正確權限的IAM角色，以存取集合或網域的寫入資料，請參閱網域的必要權限和集合的必要權限。

步驟 1：設定管線角色

設定管線必要條件後，請設定要在管線組態中使用的管線角色，並在角色中新增下列權限：

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "SecretsManagerReadAccess",
            "Effect": "Allow",
            "Action": [
                "secretsmanager:GetSecretValue"
            ],
            "Resource": ["arn:aws:secretsmanager:{region}:{account-id}:secret:secret-
name"]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:AttachNetworkInterface",
                "ec2:CreateNetworkInterface",
                "ec2:CreateNetworkInterfacePermission",
                "ec2:DeleteNetworkInterface",
                "ec2:DeleteNetworkInterfacePermission",
                "ec2:DetachNetworkInterface",
                "ec2:DescribeNetworkInterfaces"
            ],
            "Resource": [
                "arn:aws:ec2:*:{account-id}:network-interface/*",
                "arn:aws:ec2:*:{account-id}:subnet/*",
```

```
                "arn:aws:ec2:*:{account-id}:security-group/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeDhcpOptions",
                "ec2:DescribeRouteTables",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcs",
                "ec2:Describe*"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTags"
            ],
            "Resource": "arn:aws:ec2:*:*:network-interface/*",
            "Condition": {
               "StringEquals":
                    {
                        "aws:RequestTag/OSISManaged": "true"
                    }
            }
        }
    ]
}
```

您必須對用於建立 OpenSearch 擷取管道的IAM角色提供上述 Amazon EC2 許可，因為管道使用這些許可在您VPC的網路界面中建立和刪除網路界面。管線只能透過此網路介面存取 OpenSearch 叢集。

步驟 2：建立管道

然後，您可以設定如下所示的 OpenSearch 擷取管道，該管道會指定 OpenSearch 為來源。

您可以指定多個 OpenSearch 服務網域做為資料的目的地。此功能可讓傳入資料進行條件式路由或複寫至多個 OpenSearch Service 網域。

您也可以將資料從來源 OpenSearch 或 Elasticsearch 叢集移轉至 OpenSearch 無伺服器VPC集合。請務必在管線組態中提供網路存取原則。

```
version: "2"
opensearch-migration-pipeline:
  source:
    opensearch:
      acknowledgments: true
      host: [ "https://my-self-managed-cluster-name:9200" ]
      indices:
        include:
          - index_name_regex: "include-.*"
        exclude:
          - index_name_regex: '\..*'
      authentication:
        username: ${aws_secrets:secret:username}
        password: ${aws_secrets:secret:password}
        scheduling:
           interval: "PT2H"
           index_read_count: 3
           start_time: "2023-06-02T22:01:30.00Z"
  sink:
  - opensearch:
      hosts: ["https://search-mydomain.us-east-1.es.amazonaws.com"]
      aws:
          sts_role_arn: "arn:aws:iam::{account-id}:role/pipeline-role"
          region: "us-east-1"
          #Uncomment the following lines if your destination is an OpenSearch
 Serverless collection
          #serverless: true
          # serverless_options:
          #     network_policy_name: "network-policy-name"
      index: "${getMetadata(\"opensearch-index\")}"
      document_id: "${getMetadata(\"opensearch-document_id\")}"
      enable_request_compression: true
      dlq:
        s3:
          bucket: "bucket-name"
          key_path_prefix: "apache-log-pipeline/logs/dlq"
          region: "us-east-1"
          sts_role_arn: "arn:aws:iam::{account-id}:role/pipeline-role"
extension:
  aws:
    secrets:
      secret:
        secret_id: "my-opensearch-secret"
```

```
        region: "us-east-1"
        sts_role_arn: "arn:aws:iam::{account-id}:role/pipeline-role"
        refresh_interval: PT1H
```

您可以使用預先設定的藍圖來建立此管道。如需詳細資訊，請參閱the section called “使用藍圖建立管道”。

後續步驟

將資料匯出至管線之後，您可以從設定為管線接收器的 OpenSearch Service 網域進行查詢。下列資源可協助您開始使用：

- 可觀測性
- the section called “Trace Analytics”
- the section called “Piped Processing Language”

使用 Amazon OpenSearch 擷取在網域和集合之間移轉資料

您可以使用 OpenSearch 擷取管道在 Amazon OpenSearch 服務網域或 OpenSearch 無伺服器 VPC 集合之間移轉資料。若要這麼做，您必須設定管線，在其中將一個網域或集合設定為來源，並將另一個網域或集合設定為接收器。這可以有效地將您的資料從一個網域或集合遷移到另一個網域或集合。

若要移轉資料，您必須具備下列資源：

- 來源 OpenSearch 服務網域或 OpenSearch 無伺服器 VPC 集合。此網域或集合包含您要移轉的資料。如果您使用的是網域，該網域必須執行 1.0 或更新 OpenSearch 版本，或是版本 7.4 或更新版本。網域也必須具有授與管線角色適當權限的存取原則。
- 您要將資料移轉至的個別網域或 VPC 集合。此網域或集合將充當管線接收器。
- OpenSearch 擷取將用來讀取和寫入您的集合或網域的管線角色。您可以在管道組態中包含此角色的 Amazon 資源名稱 (ARN)。如需詳細資訊，請參閱下列資源：
  - the section called “授與管道對網域的存取權”
  - the section called “授予管道對集合的存取權”

主題

- 限制
- OpenSearch 服務作為來源

- 指定多個 OpenSearch 服務網域接收器
- 將資料移轉至 OpenSearch 無伺服器 VPC 集合

限制

當您將 OpenSearch 服務網域或 OpenSearch 無伺服器集合指定為接收器時，會套用下列限制：

- 管線無法寫入多個 VPC 網域。
- 您只能在使用 VPC 存取的 OpenSearch 無伺服器集合之間移轉資料，或從中移轉資料。不支援公開收藏。
- 您無法在單一管線組態中指定 VPC 和公用網域的組合。
- 在單一配管組態中，您最多可以有 20 個非管線接收器。
- 您可以在單一配管組態中指定最多三 AWS 區域 個不同的接收器。
- 如果任何接收器關閉時間過長，或者沒有佈建足夠的容量來接收傳入資料，則具有多個接收器的管線可能會隨著時間的推移而降低處理速度。

OpenSearch 服務作為來源

您指定為來源的網域或集合，就是資料移轉來源的地方。

在 IAM 中建立管道角色

若要建立 OpenSearch 擷取管道，您必須先建立管線角色，以授與網域或集合之間的讀取和寫入存取權限。若要這麼做，請執行下列步驟：

1. 在 IAM 中建立新的許可政策以附加到管道角色。確保您允許從源讀取並寫入接收器的權限。如需為 OpenSearch 服務網域設定 IAM 管道許可的詳細資訊，請參閱the section called “授與管道對網域的存取權”和the section called “授予管道對集合的存取權”。
2. 在管線角色中指定下列要從來源讀取的權限：

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action":"es:ESHttpGet",
         "Resource":[
```

```
            "arn:aws:es:us-east-1:{account-id}:domain/{domain-name}/",
            "arn:aws:es:us-east-1:{account-id}:domain/{domain-name}/_cat/indices",
            "arn:aws:es:us-east-1:{account-id}:domain/{domain-name}/_search",
            "arn:aws:es:us-east-1:{account-id}:domain/{domain-name}/_search/scroll",
            "arn:aws:es:us-east-1:{account-id}:domain/{domain-name}/*/_search"
         ]
      },
      {
         "Effect":"Allow",
         "Action":"es:ESHttpPost",
         "Resource":[
            "arn:aws:es:us-east-1:{account-id}:domain/{domain-name}/*/_search/
point_in_time",
            "arn:aws:es:us-east-1:{account-id}:domain/{domain-name}/*/_search/scroll"
         ]
      },
      {
         "Effect":"Allow",
         "Action":"es:ESHttpDelete",
         "Resource":[
            "arn:aws:es:us-east-1:{account-id}:domain/{domain-name}/_search/
point_in_time",
            "arn:aws:es:us-east-1:{account-id}:domain/{domain-name}/_search/scroll"
         ]
      }
   ]
}
```

建立管線

將原則連結至管線角色後，請使用AWSOpenSearchDataMigrationPipeline移轉藍圖建立管線。此藍圖包括用於在 OpenSearch 服務網域或集合之間移轉資料的預設組態。如需詳細資訊，請參閱 the section called “使用藍圖建立管道”。

> **Note**
>
> OpenSearch 擷取會使用您的來源網域版本和散佈來決定要使用哪種機制進行移轉。某些版本支持該`point_in_time`選項。 OpenSearch 無伺服器會使用`search_after`此選項，因為它不支援`point_in_time`或`scroll`.

新索引可能正在遷移過程中建立，或者在移轉進行中時，文件可能正在更新。因此，您可能需要對網域索引資料執行單次掃描或多次掃描，以取得新的或更新的資料。

透過`interval`在管線組態中配置`index_read_count`和來指定要執行的掃描數。下列範例顯示如何執行多個掃描：

```
scheduling:
    interval: "PT2H"
    index_read_count: 3
    start_time: "2023-06-02T22:01:30.00Z"
```

OpenSearch 擷取會使用下列組態來確保將資料寫入相同的索引，並維護相同的文件 ID：

```
index: "${getMetadata(\"opensearch-index\")}"
document_id: "${getMetadata(\"opensearch-document_id\")}"
```

指定多個 OpenSearch 服務網域接收器

您可以指定多個公用 OpenSearch 服務網域做為資料的目的地。您可以使用此功能執行條件式路由，或將傳入資料複製到多個 OpenSearch Service 網域中。您最多可以指定 10 個不同的公用 OpenSearch 服務網域做為接收器。

在下列範例中，傳入資料會有條件地路由到不同的 OpenSearch Service 網域：

```
...
  route:
    - 2xx_status: "/response >= 200 and /response < 300"
    - 5xx_status: "/response >= 500 and /response < 600"
  sink:
    - opensearch:
        hosts: [ "https://search-response-2xx.us-east-1.es.amazonaws.com" ]
        aws:
          sts_role_arn: "arn:aws:iam::123456789012:role/Example-Role"
          region: "us-east-1"
        index: "response-2xx"
        routes:
          - 2xx_status
    - opensearch:
        hosts: [ "https://search-response-5xx.us-east-1.es.amazonaws.com" ]
        aws:
          sts_role_arn: "arn:aws:iam::123456789012:role/Example-Role"
          region: "us-east-1"
```

```
        index: "response-5xx"
        routes:
          - 5xx_status
```

將資料移轉至 OpenSearch 無伺服器 VPC 集合

您可以使用 OpenSearch 擷取將資料從來源 OpenSearch 服務網域或 OpenSearch 無伺服器集合移轉至 VPC 收集接收器。您必須在管線組態中提供網路存取原則。如需將資料擷取至 OpenSearch 無伺服器 VPC 集合的詳細資訊，請參閱。the section called “教學課程：將資料擷取至集合”

若要將資料移轉至 VPC 集合

1. 建立 OpenSearch 無伺服器集合。如需說明，請參閱the section called “教學課程：將資料擷取至集合”。
2. 為集合建立網路原則，以指定對集合端點和儀表板端點的 VPC 存取權。如需說明，請參閱the section called “網路存取”。
3. 如果您還沒有管線角色，請建立管線角色。如需說明，請參閱the section called “管線角色”。
4. 建立管線。如需說明，請參閱 the section called “使用藍圖建立管道”。

使用AWS軟體開發套件與亞馬遜OpenSearch擷取互動

本節包含如何使用AWS開發套件與 Amazon OpenSearch 擷取互動的範例。程式碼範例示範如何建立網域和管線，然後將資料擷取至管線。

主題

- Python

Python

下列範例指令碼使AWS SDK for Python (Boto3)用建立 IAM 管道角色、要寫入資料的網域，以及用來擷取資料的管道。然後，它會使用 `requests` HTTP 程式庫將範例記錄檔內嵌到管線中。

若要安裝所需的相依性，請執行下列命令：

```
pip install boto3
pip install botocore
pip install requests
pip install requests-auth-aws-sigv4
```

在指令碼中，以您的 ID 取代存取原則中的帳號 AWS 帳戶 ID。您也可以選擇性地修改 region。

```
import boto3
import botocore
from botocore.config import Config
import requests
from requests_auth_aws_sigv4 import AWSSigV4
import time

# Build the client using the default credential configuration.
# You can use the CLI and run 'aws configure' to set access key, secret
# key, and default region.

my_config = Config(
    # Optionally lets you specify a Region other than your default.
    region_name='us-east-1'
)

opensearch = boto3.client('opensearch', config=my_config)
iam = boto3.client('iam', config=my_config)
osis = boto3.client('osis', config=my_config)

domainName = 'test-domain'  # The name of the domain
pipelineName = 'test-pipeline' # The name of the pipeline

def createPipelineRole(iam, domainName):
    """Creates the pipeline role"""
    response = iam.create_policy(
        PolicyName='pipeline-policy',
        PolicyDocument=f'{{\"Version\":\"2012-10-17\",\"Statement\":[{{\"Effect
\":\"Allow\",\"Action\":\"es:DescribeDomain\",\"Resource\":\"arn:aws:es:us-
east-1:123456789012:domain\/{domainName}\"}},{{\"Effect\":\"Allow\",\"Action\":
\"es:ESHttp*\",\"Resource\":\"arn:aws:es:us-east-1:123456789012:domain\/{domainName}\/*
\"}}]}}'
    )
    policyarn = response['Policy']['Arn']

    response = iam.create_role(
        RoleName='PipelineRole',
        AssumeRolePolicyDocument='{\"Version\":\"2012-10-17\",\"Statement\":[{\"Effect
\":\"Allow\",\"Principal\":{\"Service\":\"osis-pipelines.amazonaws.com\"},\"Action\":
\"sts:AssumeRole\"}]}'
    )
    rolename=response['Role']['RoleName']
```

```
    response = iam.attach_role_policy(
        RoleName=rolename,
        PolicyArn=policyarn
    )

    print('Creating pipeline role...')
    time.sleep(10)
    print('Role created: ' + rolename)

def createDomain(opensearch, domainName):
    """Creates a domain to ingest data into"""
    response = opensearch.create_domain(
        DomainName=domainName,
        EngineVersion='OpenSearch_2.3',
        ClusterConfig={
            'InstanceType': 't2.small.search',
            'InstanceCount': 5,
            'DedicatedMasterEnabled': True,
            'DedicatedMasterType': 't2.small.search',
            'DedicatedMasterCount': 3
        },
        # Many instance types require EBS storage.
        EBSOptions={
            'EBSEnabled': True,
            'VolumeType': 'gp2',
            'VolumeSize': 10
        },
        AccessPolicies=f'{{\"Version\":\"2012-10-17\",\"Statement\":[{{\"Effect\":
\"Allow\",\"Principal\":{{\"AWS\":\"arn:aws:iam::123456789012:role\/PipelineRole
\"}},\"Action\":\"es:*\",\"Resource\":\"arn:aws:es:us-east-1:123456789012:domain\/
{domainName}\/*\"}}]}}',
        NodeToNodeEncryptionOptions={
            'Enabled': True
        }
    )
    return(response)

def waitForDomainProcessing(opensearch, domainName):
    """Waits for the domain to be active"""
    try:
        response = opensearch.describe_domain(
            DomainName=domainName
        )
```

```
        # Every 30 seconds, check whether the domain is processing.
        while 'Endpoint' not in response['DomainStatus']:
            print('Creating domain...')
            time.sleep(60)
            response = opensearch.describe_domain(
                DomainName=domainName)

        # Once we exit the loop, the domain is ready for ingestion.
        endpoint = response['DomainStatus']['Endpoint']
        print('Domain endpoint ready to receive data: ' + endpoint)
        createPipeline(osis, endpoint)

    except botocore.exceptions.ClientError as error:
        if error.response['Error']['Code'] == 'ResourceNotFoundException':
            print('Domain not found.')
        else:
            raise error

def createPipeline(osis, endpoint):
    """Creates a pipeline using the domain and pipeline role"""
    try:
        definition = f'version: \"2\"\nlog-pipeline:\n  source:\n    http:\n      path:
 \"/${{pipelineName}}/logs\"\n  processor:\n    - date:\n        from_time_received:
 true\n        destination: \"@timestamp\"\n  sink:\n    - opensearch:\n        hosts:
 [ \"https://{endpoint}\" ]\n        index: \"application_logs\"\n        aws:\n
     sts_role_arn: \"arn:aws:iam::123456789012:role/PipelineRole\"\n          region:
 \"us-east-1\"'
        response = osis.create_pipeline(
            PipelineName=pipelineName,
            MinUnits=4,
            MaxUnits=9,
            PipelineConfigurationBody=definition
        )

        response = osis.get_pipeline(
                PipelineName=pipelineName
        )

        # Every 30 seconds, check whether the pipeline is active.
        while response['Pipeline']['Status'] == 'CREATING':
            print('Creating pipeline...')
            time.sleep(30)
            response = osis.get_pipeline(
                PipelineName=pipelineName)
```

```
        # Once we exit the loop, the pipeline is ready for ingestion.
        ingestionEndpoint = response['Pipeline']['IngestEndpointUrls'][0]
        print('Pipeline ready to ingest data at endpoint: ' + ingestionEndpoint)
        ingestData(ingestionEndpoint)

    except botocore.exceptions.ClientError as error:
        if error.response['Error']['Code'] == 'ResourceAlreadyExistsException':
            print('Pipeline already exists.')
            response = osis.get_pipeline(
                PipelineName=pipelineName
            )
            ingestionEndpoint = response['Pipeline']['IngestEndpointUrls'][0]
            ingestData(ingestionEndpoint)
        else:
            raise error


def ingestData(ingestionEndpoint):
    """Ingests a sample log file into the pipeline"""
    endpoint = 'https://' + ingestionEndpoint
    r = requests.request('POST', f'{endpoint}/log-pipeline/logs',

 data='[{"time":"2014-08-11T11:40:13+00:00","remote_addr":"122.226.223.69","status":"404","requ
 http://www.k2proxy.com//hello.html HTTP/1.1","http_user_agent":"Mozilla/4.0
 (compatible; WOW64; SLCC2;)"}]',
    auth=AWSSigV4('osis'))
    print('Ingesting sample log file into pipeline')
    print('Response: ' + r.text)

def main():
    createPipelineRole(iam, domainName)
    createDomain(opensearch, domainName)
    waitForDomainProcessing(opensearch, domainName)

if __name__ == "__main__":
    main()
```

亞馬遜OpenSearch攝入中的安全性

雲端安全是 AWS 最重視的一環。身為 AWS 客戶的您，將能從資料中心和網路架構的建置中獲益，以滿足組織最為敏感的安全要求。

安全是 AWS 與您共同的責任。共同的責任模型 將此描述為雲端 本身 的安全和雲端內部的安全：

- 雲端本身的安全：AWS 負責保護在 AWS Cloud 中執行 AWS 服務的基礎設施。AWS 也提供您可安全使用的服務。在 AWS 合規計劃中，第三方稽核員會定期測試並驗證我們的安全功效。
- 雲端內部的安全：您的責任取決於所使用的 AWS 服務。您也必須對其他因素負責，包括資料的機密性、您公司的要求和適用法律和法規。

本文件有助於您了解如何在使用資料OpenSearch擷取時套用共同責任模型。下列主題將示範如何設定OpenSearch擷取以符合您的安全和合規目標。您也會了解如何使用其他AWS服務來協助監控並保護OpenSearch資源。

主題

- 為 Amazon OpenSearch 擷取管道設定 VPC 存取
- 適用於 Amazon OpenSearch 擷 Identity and Access Management
- 使用記錄亞馬遜OpenSearch擷取 API 呼叫 AWS CloudTrail

為 Amazon OpenSearch 擷取管道設定 VPC 存取

您可以使用界面 VPC 端點存取 Amazon OpenSearch 擷取管道。VPC 是一種虛擬網路，專用於您 AWS 帳戶的. 它在邏輯上與 AWS 雲端中的其他虛擬網路隔離。透過 VPC 端點存取管道可在 VPC 內的 OpenSearch 擷取與其他服務之間進行安全通訊，而不需要網際網路閘道、NAT 裝置或 VPN 連線。所有流量都安全地保留在 AWS 雲中。

OpenSearch 擷取透過建立由技術提供支援的介面端點來建立此私人連線。 AWS PrivateLink我們會在您在管道建立期間指定的每個子網路中建立端點網路介面。這些是由請求者管理的網路介面，可做為輸入管道的流量的進入點。 OpenSearch 您也可以選擇自行建立和管理介面端點。

使用 VPC 可讓您在 VPC 邊界內強制執行資料流通過 OpenSearch 擷取管道，而不是透過公用網際網路。不在 VPC 內的管道會透過公開端點和網際網路傳送和接收資料。

具有 VPC 存取權的管道可以寫入公用或 VPC OpenSearch 服務網域，以及公用或 VPC OpenSearch 無伺服器集合。

主題

- 考量事項
- 限制

- 必要條件
- 設定管線的 VPC 存取
- 自我管理的 VPC 端點
- VPC 存取適用的服務連結角色

考量事項

為管線設定 VPC 存取時，請考慮下列事項。

- 管道不需要與其接收器位於相同的 VPC 中。您也不需要在兩個 VPC 之間建立連線。 OpenSearch 攝入需要為您連接它們的照顧。
- 您只能為管線指定一個 VPC。
- 與公用管線不同，VPC 管線必須與寫入的網域或集合接收器位於相同 AWS 區域 的位置。
- 您可以選擇將管道部署到 VPC 的一個、兩個或三個子網路中。子網路分佈在您的擷取 OpenSearch 運算單元 (OCU) 部署在相同的可用區域中。
- 如果您只在一個子網路中部署管線，且可用區域停止運作，您將無法擷取資料。為確保高可用性，建議您使用兩個或三個子網路來設定管線。
- 指定安全性群組是選擇性的。如果您未提供安全性群組， OpenSearch 擷取會使用 VPC 中指定的預設安全性群組。

限制

具有 VPC 存取權的管線具有下列限制。

- 建立管道之後，您無法變更管道的網路組態。如果您在 VPC 中啟動管道，則以後無法將其更改為公共端點，反之亦然。
- 您可以使用介面 VPC 端點或公用端點來啟動管線，但不能同時執行這兩種作業。建立配管時，您必須選擇其中一個。
- 佈建具有 VPC 存取權的管道後，您無法將其移至其他 VPC，也無法變更其子網路或安全性群組設定。
- 如果您的管線寫入使用 VPC 存取的網域或集合接收器，則在建立管線之後，您無法稍後返回並變更接收器 (VPC 或 public)。您必須使用新的接收器刪除並重新建立配管。您仍然可以從公共接收器切換到具有 VPC 訪問權限的接收器。
- 您無法提供對 VPC 管道的跨帳戶擷取存取權。

必要條件

您必須先執行下列動作，才能佈建具有 VPC 存取權的管線：

- 建立 VPC

  若要建立 VPC，您可以使用 Amazon VPC 主控台、 AWS CLI 或其中一個開發套件 AWS 。如需詳細資訊，請參閱 Amazon VPC 使用者指南中的使用 VPC。如果您已有 VPC，則可以略過此步驟。

- 預留 IP 地址

  OpenSearch 擷取會在您在管線建立期間指定的每個子網路中放置一個 elastic network interface。每個網路界面都與 IP 地址關聯。您必須為每個子網路為網路介面保留一個 IP 位址。

設定管線的 VPC 存取

您可以在 OpenSearch 服務主控台中為管線啟用 VPC 存取，或使用 AWS CLI.

主控台

您可以在管線建立期間設定 VPC 存取。在 [網路] 下，選擇 [VPC 存取] 並設定下列設定：

設定	描述
端點管理	選擇是要自行建立 VPC 端點，還是要讓 OpenSearch 擷取為您建立這些端點。
VPC	選擇您想使用的虛擬私有雲端 (VPC) ID。VPC 和管線必須在相同 AWS 區域的位置。
子網	選擇一或多個子網路。 OpenSearch 服務會在子網路中放置 VPC 端點和彈性網路介面。
安全群組	選擇一或多個 VPC 安全性群組，以允許所需的應用程式在管線公開的連接埠 (80 或 443) 和通訊協定 (HTTP 或 HTTPS) 上連接到 OpenSearch 擷取管線。
VPC 附件選項	如果您的來源是自我管理的端點，請將管道連接到 VPC。選擇其中一個提供的預設 CIDR 選項，或使用自訂 CIDR。

CLI

若要使用設定 VPC 存取 AWS CLI，請指定`--vpc-options`參數：

```
aws osis create-pipeline \
  --pipeline-name vpc-pipeline \
  --min-units 4 \
  --max-units 10 \
  --vpc-options
 SecurityGroupIds={sg-12345678,sg-9012345},SubnetIds=subnet-1212234567834asdf \
  --pipeline-configuration-body "file://pipeline-config.yaml"
```

自我管理的 VPC 端點

建立管道時，您可以使用端點管理來建立具有自我管理端點或服務管理端點的管道。端點管理是選用的，預設為由 OpenSearch 擷取管理的端點。

若要在中建立具有自我管理 VPC 端點的管道 AWS Management Console，請參閱使用 OpenSearch Service 主控台建立管道。若要在中建立具有自我管理 VPC 端點的管線 AWS CLI，您可以使用建立管線命令中的`--vpc-options`參數：

```
--vpc-options SubnetIds=subnet-abcdef01234567890,VpcEndpointManagement=CUSTOMER
```

當您指定端點服務時，您可以自行建立管道的端點。若要尋找您的端點服務，請使用 get-pipeline 指令，該命令會傳回類似下列內容的回應：

```
"vpcEndpointService" : "com.amazonaws.osis.us-east-1.pipeline-
id-1234567890abcdef1234567890",
"vpcEndpoints" : [
  {
    "vpcId" : "vpc-1234567890abcdef0",
    "vpcOptions" : {
      "subnetIds" : [ "subnet-abcdef01234567890", "subnet-021345abcdef6789" ],
      "vpcEndpointManagement" : "CUSTOMER"
    }
  }
```

使用來`vpcEndpointService`自回應的來建立具有 AWS Management Console 或 AWS CLI的 VPC 端點。

如果您使用自我管理的 VPC 端點，則必須在 VPC `enableDnsHostnames` 中啟用 DNS 屬性`enableDnsSupport`。請注意，如果您的管道具有已停止並重新啟動的自我管理端點，則必須在帳戶中重新建立 VPC 端點。

VPC 存取適用的服務連結角色

服務連結角色是一個唯一的 IAM 角色類型，它將許可委派給服務，以便服務可代表您建立和管理資源。如果您選擇服務管理的 VPC 端點， OpenSearch 擷取需要一個服務連結角色 (稱為)，AWSServiceRoleForAmazonOpenSearchIngestionService才能存取您的 VPC、建立管線端點，以及將網路介面放置在 VPC 子網路中。

如果您選擇自我管理的 VPC 端點， OpenSearch 擷取需要名為的服務連結角色。AWSServiceRoleForOpensearchIngestionSelfManagedVpce如需這些角色、其權限以及如何刪除這些角色的詳細資訊，請參閱the section called “管道建立角色”。

OpenSearch 當您建立擷取管線時，擷取會自動建立角色。若要成功建立此自動建立，在帳戶中建立第一個管道的使用者必須具有`iam:CreateServiceLinkedRole`動作的權限。如需進一步了解，請參閱 IAM 使用者指南中的服務連結角色許可。建立角色後，您可以在 AWS Identity and Access Management (IAM) 主控台中檢視該角色。

適用於 Amazon OpenSearch 擷 Identity and Access Management

AWS Identity and Access Management (IAM) 可協助系統管理員安全地控制 AWS 資源存取權。 AWS 服務 IAM管理員控制哪些人可以驗證 (登入) 和授權 (具有權限) 以使用 OpenSearch 擷取資源。IAM是您 AWS 服務 可以免費使用的。

主題

- 擷取以身分識別為基礎的原則 OpenSearch
- OpenSearch 擷取的原則動作
- OpenSearch 擷取的原則資源
- Amazon OpenSearch 擷取的政策條件金鑰
- ABAC與 OpenSearch 攝入
- 搭配 OpenSearch 擷取使用臨時登入資料
- 用 OpenSearch 於擷取的服務連結角色
- 擷取以身分識別為基礎的原則範例 OpenSearch

擷取以身分識別為基礎的原則 OpenSearch

支援身分型政策：是

以身分識別為基礎的原則是您可以附加至身分識別 (例如使用者、使用IAM者群組或角色) 的JSON權限原則文件。這些政策可控制身分在何種條件下能對哪些資源執行哪些動作。若要瞭解如何建立以身分識別為基礎的策略，請參閱《IAM使用指南》中的〈建立IAM策略〉。

使用以IAM身分識別為基礎的策略，您可以指定允許或拒絕的動作和資源，以及允許或拒絕動作的條件。您無法在身分型政策中指定主體，因為這會套用至連接的使用者或角色。若要瞭解可在JSON策略中使用的所有元素，請參閱《使用IAM者指南》中的IAMJSON策略元素參考資料。

擷取以身分識別為基礎的原則範例 OpenSearch

若要檢視 OpenSearch 擷取以身分識別為基礎的原則範例，請參閱。the section called “身分型政策範例”

OpenSearch 擷取的原則動作

支援政策動作：是

JSON策略`Action`元素描述了您可以用來允許或拒絕策略中存取的動作。策略動作通常與關聯 AWS API操作具有相同的名稱。有一些例外情況，例如沒有匹配API操作的僅限權限的操作。也有一些作業需要政策中的多個動作。這些額外的動作稱為相依動作。

政策會使用動作來授予執行相關聯動作的許可。

OpenSearch 擷取中的原則動作會在動作之前使用下列前置詞：

```
osis
```

若要在單一陳述式中指定多個動作，請用逗號分隔。

```
"Action": [
      "osis:action1",
      "osis:action2"
         ]
```

您可以使用萬用字元 (*) 來指定多個動作。例如，若要指定開頭是 `List` 文字的所有動作，請包含以下動作：

```
"Action": "osis:List*"
```

若要檢視 OpenSearch 擷取以身分識別為基礎的原則範例，請參閱。 無伺服器的身分識別原則範例 OpenSearch

OpenSearch 擷取的原則資源

支援政策資源：是

管理員可以使用 AWS JSON策略來指定誰可以存取什麼內容。也就是說，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

ResourceJSON原則元素會指定要套用動作的一或多個物件。陳述式必須包含 Resource 或 NotResource 元素。最佳做法是使用其 Amazon 資源名稱 (ARN) 指定資源。您可以針對支援特定資源類型的動作 (稱為資源層級許可) 來這麼做。

對於不支援資源層級許可的動作 (例如列出操作)，請使用萬用字元 (*) 來表示陳述式適用於所有資源。

```
"Resource": "*"
```

Amazon OpenSearch 擷取的政策條件金鑰

支援服務特定政策條件金鑰：否

管理員可以使用 AWS JSON策略來指定誰可以存取什麼內容。也就是說，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

Condition 元素 (或 Condition 區塊) 可讓您指定使陳述式生效的條件。Condition 元素是選用項目。您可以建立使用條件運算子的條件運算式 (例如等於或小於)，來比對政策中的條件和請求中的值。

若您在陳述式中指定多個 Condition 元素，或是在單一 Condition 元素中指定多個索引鍵， AWS 會使用邏輯 AND 操作評估他們。如果您為單一條件索引鍵指定多個值，請使用邏輯OR運算來 AWS 評估條件。必須符合所有條件，才會授與陳述式的許可。

您也可以在指定條件時使用預留位置變數。例如，只有在IAM使用者名稱標記資源時，您才可以授與IAM使用者存取資源的權限。如需詳細資訊，請參閱《IAM使用指南》中的IAM政策元素：變數和標籤。

AWS 支援全域條件金鑰和服務特定條件金鑰。若要查看所有 AWS 全域條件索引鍵，請參閱《使用指南》中的AWS 全域條件內IAM容索引鍵。

若要查看 OpenSearch 擷取條件金鑰清單，請參閱服務授權參考中的 Amazon OpenSearch 擷取的條件金鑰。若要了解可以使用條件金鑰的動作和資源，請參閱 Amazon OpenSearch 擷取定義的動作。

ABAC與 OpenSearch 攝入

支援 ABAC (策略中的標籤): 是

以屬性為基礎的存取控制 (ABAC) 是一種授權策略，可根據屬性定義權限。在中 AWS，這些屬性稱為標籤。您可以將標籤附加至IAM實體 (使用者或角色) 和許多 AWS 資源。標記實體和資源是的第一步ABAC。然後，您可以設計ABAC策略，以便在主參與者的標籤與他們嘗試存取的資源上的標籤相符時允許作業。

ABAC在快速成長的環境中很有幫助，並且有助於原則管理變得繁瑣的情況。

如需根據標籤控制存取，請使用 `aws:ResourceTag/key-name`、`aws:RequestTag/key-name` 或 `aws:TagKeys` 條件索引鍵，在政策的條件元素中，提供標籤資訊。

如果服務支援每個資源類型的全部三個條件金鑰，則對該服務而言，值為 Yes。如果服務僅支援某些資源類型的全部三個條件金鑰，則值為 Partial。

如需有關的詳細資訊ABAC，請參閱什麼是ABAC？ 在《IAM使用者指南》中。若要檢視包含設定步驟的自學課程ABAC，請參閱《使用指南》中的〈使用以屬性為基礎的存取控制 (ABAC) IAM 〉。

如需標記 OpenSearch 擷取資源的詳細資訊，請參閱the section called “標記管線”。

搭配 OpenSearch 擷取使用臨時登入資料

支援臨時憑證：是

當您使用臨時憑據登錄時，某些 AWS 服務 不起作用。如需其他資訊，包括哪些 AWS 服務 與臨時登入資料搭配使用 AWS 服務 ，請參閱《IAM使用指南》IAM中的使用方式。

如果您使用除了使用者名稱和密碼以外的任何方法登入，則您正在 AWS Management Console 使用臨時認證。例如，當您 AWS 使用公司的單一登入 (SSO) 連結存取時，該程序會自動建立臨時認證。當您以使用者身分登入主控台，然後切換角色時，也會自動建立臨時憑證。如需有關切換角色的詳細資訊，請參閱《IAM使用者指南》中的〈切換到角色 (主控台)〉。

您可以使用 AWS CLI 或手動建立臨時認證 AWS API。然後，您可以使用這些臨時登入資料來存取 AWS。 AWS 建議您動態產生臨時登入資料，而不是使用長期存取金鑰。如需詳細資訊，請參閱IAM。

用 OpenSearch 於擷取的服務連結角色

支援服務連結角色：是

服務連結角色是一種連結至. AWS 服務服務可以擔任代表您執行動作的角色。服務連結角色會顯示在您的中， AWS 帳戶 且屬於服務所有。IAM管理員可以檢視 (但無法編輯服務連結角色) 的權限。

OpenSearch 擷取會使用稱為的服務連結角色。`AWSServiceRoleForAmazonOpenSearchIngestionService`名`AWSServiceRoleForOpensearc`的服務連結角色也適用於具有自我管理VPC端點的管道。如需有關建立和管理 OpenSearch 擷取服務連結角色的詳細資訊，請參閱。the section called “管道建立角色”

擷取以身分識別為基礎的原則範例 OpenSearch

根據預設，使用者和角色沒有建立或修改 OpenSearch 擷取資源的權限。他們也無法使用 AWS Management Console、 AWS Command Line Interface (AWS CLI) 或執行工作 AWS API。若要授與使用者對所需資源執行動作的權限，IAM管理員可以建立IAM策略。然後，系統管理員可以將IAM原則新增至角色，使用者可以擔任這些角色。

若要瞭解如何使用這些範例原則文件來建立以IAM身分識別為基礎的JSON策略，請參閱使用指南中的IAM建立IAM策略。

如需 Amazon OpenSearch Intetion 定義的動作和資源類型的詳細資訊，包括每種資源類型的格式，請參閱服務授權參考中針對 Amazon OpenSearch 擷取的動作、資源和條件金鑰。ARNs

主題

- 政策最佳實務
- 在主 OpenSearch 控台中使用擷取
- 管理 OpenSearch 擷取管線
- 將資料導入擷取管線 OpenSearch

政策最佳實務

身分型政策相當強大。他們決定是否有人可以在您的帳戶中建立、存取或刪除 OpenSearch 擷取資源。這些動作可能會讓您的 AWS 帳戶產生費用。當您建立或編輯身分型政策時，請遵循下列準則及建議事項：

以身分識別為基礎的政策會決定某人是否可以在您的帳戶中建立、存取或刪除 OpenSearch 擷取資源。這些動作可能會讓您的 AWS 帳戶產生費用。當您建立或編輯身分型政策時，請遵循下列準則及建議事項：

- 開始使用 AWS 受管原則並邁向最低權限權限 — 若要開始授與使用者和工作負載的權限，請使用可授與許多常見使用案例權限的AWS 受管理原則。它們在您的 AWS 帳戶. 建議您透過定義特定於您使用案例的 AWS 客戶管理政策，進一步降低使用權限。如需詳細資訊，請參閱AWS 《IAM使用指南》中針對工作職能的AWS 受管理策略或受管理的策略。

- 套用最低權限權限 — 當您使用原則設定權限時，IAM只授與執行工作所需的權限。為實現此目的，您可以定義在特定條件下可以對特定資源採取的動作，這也稱為最低權限許可。如需有關使用套用權限IAM的詳細資訊，請參閱《使用指南》IAM中的IAM《策略與權限》。
- 使用IAM策略中的條件進一步限制存取 — 您可以在策略中新增條件，以限制對動作和資源的存取。例如，您可以撰寫政策條件，以指定必須使用傳送所有要求SSL。您也可以使用條件來授與對服務動作的存取權 (如透過特定) 使用這些動作 AWS 服務，例如 AWS CloudFormation。如需詳細資訊，請參閱《IAM使用指南》中的IAMJSON策略元素：條件。
- 使用 IAM Access Analyzer 驗證您的原IAM則，以確保安全和功能性的權限 — IAM Access Analyzer 會驗證新的和現有的原則，以便原則遵循IAM原則語言 (JSON) 和IAM最佳做法。IAMAccess Analyzer 提供超過 100 項原則檢查和可採取動作的建議，協助您撰寫安全且功能正常的原則。如需詳細資訊，請參閱IAM使IAM用指南中的存取分析器原則驗證。
- 需要多因素驗證 (MFA) — 如果您的案例需要使IAM用者或 root 使用者 AWS 帳戶，請開啟以取得額外MFA的安全性。若要在呼叫API作業MFA時需要，請在原則中新增MFA條件。如需詳細資訊，請參閱《IAM使用指南》中的 < 設定MFA受保護的API存取 >。

如需有關中最佳作法的詳細資訊IAM，請參閱《IAM使用指南》IAM中的「安全性最佳作法」。

在主 OpenSearch 控台中使用擷取

若要在 OpenSearch 服務主控台中存取 OpenSearch 擷取，您必須擁有最少一組權限。這些權限必須允許您列出並檢視 AWS 帳戶中 OpenSearch 擷取資源的詳細資料。如果您建立的以身分識別為基礎的原則，而該原則的限制性比最低所需權限更嚴格，則主控台將無法如預期用於具有該原則的實體 (例如IAM角色) 運作。

您不需要為只對 AWS CLI 或撥打電話的使用者允許最低主控台權限 AWS API。而是只允許存取與您嘗試執行之API作業相符的動作。

下列原則可讓使用者在 OpenSearch 服務主控台中存取 OpenSearch 擷取：

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Resource": "*",
            "Effect": "Allow",
            "Action": [
                "osis:ListPipelines",
                "osis:GetPipeline",
                "osis:ListPipelineBlueprints",
```

```
                "osis:GetPipelineBlueprint",
                "osis:GetPipelineChangeProgress"
            ]
        }
    ]
}
```

或者，您可以使用the section called “AmazonOpenSearchIngestionReadOnlyAccess” AWS 受管理的策略，該策略會授與. OpenSearch AWS 帳戶

管理 OpenSearch 擷取管線

此政策是允許使用者管理和管理 Amazon OpenSearch 擷取管道的「管道管理」政策範例。使用者可以建立、檢視和刪除管線。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Resource": "arn:aws:osis:region:123456789012:pipeline/*",
            "Action": [
                "osis:CreatePipeline",
                "osis:DeletePipeline",
                "osis:UpdatePipeline",
                "osis:ValidatePipeline",
                "osis:StartPipeline",
                "osis:StopPipeline"
            ],
            "Effect": "Allow"
        },
        {
            "Resource": "*",
            "Action": [
                "osis:ListPipelines",
                "osis:GetPipeline",
                "osis:ListPipelineBlueprints",
                "osis:GetPipelineBlueprint",
                "osis:GetPipelineChangeProgress"
            ],
            "Effect": "Allow"
        }
    ]
}
```

將資料導入擷取管線 OpenSearch

此範例政策可讓使用者或其他實體將資料擷取到其帳戶中的 Amazon OpenSearch 擷取管道。使用者無法修改管線。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Resource": "arn:aws:osis:region:123456789012:pipeline/*",
            "Action": [
                "osis:Ingest"
            ],
            "Effect": "Allow"
        }
    ]
}
```

使用記錄亞馬遜OpenSearch擷取 API 呼叫 AWS CloudTrail

Amazon OpenSearch In擷取已與整合AWS CloudTrail，這項服務可提供由使用者、角色或「OpenSearch擷取為」中AWS服務所採取之動作的記錄。

CloudTrail將的所有 API 呼叫OpenSearch擷取為事件。擷取的呼叫包括來自 OpenSearch Service 主控台的「OpenSearch擷取」區段的呼叫，以及對OpenSearch擷取 API 操作進行的程式碼呼叫。

若您建立追蹤，便可將CloudTrail事件持續交付至 Amazon S3 儲存貯體，包括用於OpenSearch擷取的事件。如果您不設定追蹤記錄，仍然可以透過 CloudTrail 主控台中的 Event history (事件歷史記錄) 檢視最新的事件。

您可以使用收集的資訊來CloudTrail判斷向OpenSearch擷取的請求，以及發出請求的 IP 地址、提出請求的對象、提出請求的時間，以及其他詳細資訊。

若要進一步了解 CloudTrail，請參閱 AWS CloudTrail 使用者指南。

OpenSearch擷取資訊 CloudTrail

當您建立帳戶時，系統會在您的 AWS 帳戶 中啟用 CloudTrail。當活動發生時，系統便OpenSearch會將該活動記錄至事件，並將其他AWS服務CloudTrail事件記錄到事件歷史記錄中。您可以檢視、搜尋和下載 AWS 帳戶 的最新事件。如需詳細資訊，請參閱使用 CloudTrail 事件歷史記錄檢視事件。

若要持續記錄您的事件AWS 帳戶，包括用於OpenSearch擷取的事件，請建立追蹤。線索能CloudTrail將日誌檔案交付至 Amazon S3 儲存貯體。依預設，當您在主控台中建立追蹤時，該追蹤會套用至所有的 AWS 區域。

該追蹤會記錄來自 AWS 分割區中所有區域的事件，並將日誌檔案交付到您指定的 Amazon S3 儲存貯體。此外，您可以設定其他 AWS 服務，以進一步分析和處理 CloudTrail 日誌中所收集的事件資料。如需詳細資訊，請參閱下列內容：

- 建立追蹤的概觀
- CloudTrail 支援的服務和整合
- 設定 CloudTrail 的 Amazon SNS 通知
- 接收多個區域的 CloudTrail 日誌檔案及接收多個帳戶的 CloudTrail 日誌檔案

所有OpenSearch擷取動作均由記錄，CloudTrail並記錄在OpenSearch擷取 API 參考資料中。例如，對 `CreateCollection`、`ListCollections` 及 `DeleteCollection` 動作發出的呼叫會在 CloudTrail 日誌檔案中產生項目。

每一筆事件或日誌項目都會包含產生請求者的資訊。身分資訊可協助您判斷：

- 該請求是否透過根或 AWS Identity and Access Management (IAM) 使用者憑證來提出。
- 提出該請求時，是否使用了特定角色或聯合身分使用者的暫時安全憑證。
- 該請求是否由另一項 AWS 服務提出。

如需詳細資訊，請參閱 CloudTrail userIdentity 元素。

了解日誌OpenSearch檔案項目

追蹤是一種組態，能讓事件以日誌檔案的形式交付到您指定的 Amazon S3 儲存貯體。CloudTrail 日誌檔案包含一個或多個日誌項目。

事件代表來自任何來源的單一請求。其中包含了請求的動作、動作的日期和時間、請求參數等相關資訊。CloudTrail 日誌檔案並非依公有 API 呼叫追蹤記錄的堆疊排序，因此不會以任何特定順序出現。

以下範例顯示的是展示 `DeletePipeline` 動作的 CloudTrail 日誌項目。

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
```

```
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn":"arn:aws:iam::123456789012:user/test-user",
        "accountId": "123456789012",
        "accessKeyId": "access-key",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AIDACKCEVSQ6C2EXAMPLE",
                "arn": "arn:aws:iam::123456789012:role/Admin",
                "accountId": "123456789012",
                "userName": "Admin"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-04-21T16:48:33Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-04-21T16:49:22Z",
    "eventSource": "osis.amazonaws.com",
    "eventName": "UpdatePipeline",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "123.456.789.012",
    "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/112.0.0.0 Safari/537.36",
    "requestParameters": {
        "pipelineName": "my-pipeline",
        "pipelineConfigurationBody": "version: \"2\"\nlog-pipeline:\n  source:\n
 http:\n        path: \"/test/logs\"\n  processor:\n    - grok:\n        match:\n
        log: [ '%{COMMONAPACHELOG}' ]\n    - date:\n        from_time_received: true
\n        destination: \"@timestamp\"\n  sink:\n    - opensearch:\n        hosts:
 [ \"https://search-b5zd22mwxhggheqpj5ftslgyle.us-west-2.es.amazonaws.com\" ]\n
  index: \"apache_logs2\"\n        aws_sts_role_arn: \"arn:aws:iam::709387180454:role/
canary-bootstrap-OsisRole-J1BARLD26QKN\"\n        aws_region: \"us-west-2\"\n
 aws_sigv4: true\n"
    },
    "responseElements": {
        "pipeline": {
            "pipelineName": "my-pipeline",sourceIPAddress
            "pipelineArn": "arn:aws:osis:us-west-2:123456789012:pipeline/my-pipeline",
            "minUnits": 1,
            "maxUnits": 1,
            "status": "UPDATING",
```

```
            "statusReason": {
                "description": "An update was triggered for the pipeline. It is still
 available to ingest data."
            },
            "pipelineConfigurationBody": "version: \"2\"\nlog-pipeline:\n  source:\n
    http:\n        path: \"/test/logs\"\n  processor:\n    - grok:\n        match:
\n          log: [ '%{COMMONAPACHELOG}' ]\n    - date:\n        from_time_received:
 true\n        destination: \"@timestamp\"\n  sink:\n    - opensearch:\n        hosts:
 [ \"https://search-b5zd22mwxhggheqpj5ftslgyle.us-west-2.es.amazonaws.com\" ]\n
  index: \"apache_logs2\"\n        aws_sts_role_arn: \"arn:aws:iam::709387180454:role/
canary-bootstrap-OsisRole-J1BARLD26QKN\"\n        aws_region: \"us-west-2\"\n
 aws_sigv4: true\n",
            "createdAt": "Mar 29, 2023 1:03:44 PM",
            "lastUpdatedAt": "Apr 21, 2023 9:49:21 AM",
            "ingestEndpointUrls": [
                "my-pipeline-tu33ldsgdltgv7x7tjqiudvf7m.us-west-2.osis.amazonaws.com"
            ]
        }
    },
    "requestID": "12345678-1234-1234-1234-987654321098",
    "eventID": "12345678-1234-1234-1234-987654321098",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "709387180454",
    "eventCategory": "Management",
    "tlsDetails": {
        "tlsVersion": "TLSv1.2",
        "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
        "clientProvidedHostHeader": "osis.us-west-2.amazonaws.com"
    },
    "sessionCredentialFromConsole": "true"
}
```


標記亞馬遜OpenSearch導入管道

標籤可讓您將任意資訊指派給 Amazon OpenSearch Ings管道，以便對該資訊進行分類和篩選。標籤是您或 AWS 指派給 AWS 資源的中繼資料標籤。每個標籤皆包含鍵與值。對於您指派的標籤，您可以定義鍵與值。例如，您可以將鍵定義為 `stage`，將資源的值定義為 `test`。

標籤可協助您執行以下操作：

- 識別和組織您的 AWS 資源。許多 AWS 服務支援標記，因此您可以對來自不同服務的資源指派相同的標籤，指出資源是相關的。例如，您可以將指派給 Amazon Ser OpenSearch vice 網域的相同標籤指派給您的OpenSearch擷取管道。
- 追蹤您的 AWS 成本。您可以在 AWS Billing and Cost Management 儀表板上啟用這些標籤。AWS 會使用標籤分類您的成本，並交付每月成本配置報告給您。如需詳細資訊，請參閱《AWS Billing 使用者指南》中的使用成本分配標籤。
- 使用基於屬性的訪問控制限制對管道的訪問。如需詳細資訊，請參閱 IAM 使用者指南中的根據標籤金鑰控制存取權限。

在OpenSearch擷取中，主要資源是管線。您可以使用 OpenSearch Service 主控台、、AWS CLI、、、、、、、、OpenSearch、、、、、、、、、、、、、、、、、、、、、、、、移除管線中的標籤。AWS

主題

- 必要許可
- 處理標籤 (主控台)
- 處理標籤 (AWS CLI)

必要許可

OpenSearch擷取會使用下列 AWS Identity and Access Management Access Analyzer (IAM) 許可來標記管線：

- `osis:TagResource`
- `osis:ListTagsForResource`
- `osis:UntagResource`

如需有關每個權限的詳細資訊，請參閱 Service 授權參考中的適用於OpenSearch擷取的動作、資源及條件金鑰。

處理標籤 (主控台)

主控台是標記管線的最簡單方法。

建立標籤

1. 登入 Amazon Ser OpenSearch vice 主控台，網址為 https://console.aws.amazon.com/aos/home。
2. 在左側導覽窗格中選擇 [擷取]。
3. 選取您想要新增標籤的配管，然後前往「標籤」(Tags) 標籤。
4. 選擇 Manage (管理) 和 Add new tag (新增標籤)。
5. 輸入標籤索引鍵和選用的值。
6. 選擇 儲存 。

若要刪除標籤，請按照同樣的步驟進行，然後在 Manage tags (管理標籤) 頁面上選擇 Remove (移除)。

如需使用主控台處理標籤的詳細資訊，請參閱 《AWS 管理主控台入門指南》中的標籤編輯器。

處理標籤 (AWS CLI)

若要使用標記管線AWS CLI，請傳送`TagResource`請求：

```
aws osis tag-resource
  --arn arn:aws:osis:us-east-1:123456789012:pipeline/my-pipeline
  --tags Key=service,Value=osis Key=source,Value=otel
```

使用以下`UntagResource`指令從管線移除標籤：

```
aws osis untag-resource
  --arn arn:aws:osis:us-east-1:123456789012:pipeline/my-pipeline
  --tag-keys service
```

使用`ListTagsForResource`命令檢視管線的現有效率地址：

```
aws osis list-tags-for-resource
  --arn arn:aws:osis:us-east-1:123456789012:pipeline/my-pipeline
```

使用亞馬遜記錄和監控亞馬遜OpenSearch攝取 CloudWatch

亞馬遜OpenSearch擷取將指標和日誌發佈到亞馬遜CloudWatch。

主題

- 監控管道日誌
- 監控管道指標

監控管道日誌

您可以啟用 Amazon OpenSearch 擷取管道的記錄功能，以公開管道操作和擷取活動期間引發的錯誤和警告訊息。OpenSearch擷取會將所有日誌發佈到 Amazon CloudWatch 日誌。CloudWatch日誌可監控日誌檔案中的資訊，並在達到特定閾值時通知您。您也可以將日誌資料存檔在高耐用性的儲存空間。如需詳細資訊，請參閱 Amazon CloudWatch 日誌使用者指南。

來自OpenSearch擷取的記錄可能表示要求處理失敗、從來源到接收器的驗證錯誤，以及其他有助於疑難排解的警告。OpenSearch擷取會針對其記錄檔使用`INFO`、`WARN`、`ERROR`和`FATAL`的記錄層級。我們建議您啟用所有管線的記錄檔發佈。

必要許可

若要讓OpenSearch擷取將日誌傳送到日CloudWatch誌，您必須以具有特定許可的使用者身分登入。

您需要下列CloudWatch記錄檔權限才能建立和更新記錄傳遞資源：

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Resource": "*",
            "Action": [
                "logs:CreateLogDelivery",
                "logs:PutResourcePolicy",
                "logs:UpdateLogDelivery",
                "logs:DeleteLogDelivery",
                "logs:DescribeResourcePolicies",
                "logs:GetLogDelivery",
                "logs:ListLogDeliveries"
            ]
        }
    ]
}
```

啟用日誌發佈

您可以在現有管道上啟用記錄發佈，或在建立管線時啟用記錄檔發佈。如需在管線建立期間啟用記錄發佈的步驟，請參閱the section called “建立管道”。

主控台

若要在現有管道上啟用日誌發佈

1. 登入 Amazon Ser OpenSearch vice 主控台，網址為 https://console.aws.amazon.com/aos/home。
2. 在左側導覽窗格中選擇 [擷取]，然後選取您要啟用記錄的管道。
3. 選擇 [編輯記錄發佈選項]。
4. 選取「發佈至CloudWatch記錄檔」。
5. 建立新日誌群組，或選取現有日誌群組。建議您將名稱格式化為路徑，例如`/aws/vendedlogs/OpenSearchIngestion/pipeline-name/audit-logs`。此格式可讓您更輕鬆地將CloudWatch存取原則套用至特定路徑 (例如) 下的所有記錄群組授與權限`/aws/vendedlogs/OpenSearchService/OpenSearchIngestion`。

   > **Important**
   > 您必須在記錄群組名稱`vendedlogs`中包含前置詞，否則建立會失敗。

6. 選擇 儲存 。

CLI

若要使用啟用日誌發佈AWS CLI，請傳送以下請求：

```
aws osis update-pipeline \
  --pipeline-name my-pipeline \
  --log-publishing-options  IsLoggingEnabled=true,CloudWatchLogDestination={LogGroup="/
aws/vendedlogs/OpenSearchIngestion/pipeline-name"}
```

監控管道指標

您可以使用 Amazon 監控 Amazon Data 監控 OpenSearch Amazon Data 監控 Amazon Data 監控 Amazon CloudWatch Data 監控 Amazon Data 監控 Amazon Data 監控 Amazon Data 監控 Amazon

Data 監控 Amazon Data 監控 Amazon Data 監控 Amazon 這些統計資料會保留 15 個月，以便您存取歷史資訊，並更清楚 Web 應用程式或服務的執行效能。您也可以設定留意特定閾值的警示，當滿足這些閾值時傳送通知或採取動作。如需詳細資訊，請參閱 Amazon CloudWatch 使用者指南。

OpenSearch擷取主控台會根據每個管道的原始資料顯示一系列圖形。CloudWatch

OpenSearch擷取會從大多數支援的外掛程式報告量度。如果某些插件下面沒有自己的表格，則表示它們不會報告任何插件特定的指標。管道指標會在AWS/OSIS命名空間中發佈。

主題

- 常用指標
- 緩衝指標
- 簽名 V4 度量
- 界限阻塞緩衝區指標
- Otel 追蹤來源指標
- 歐特爾度量來源指標
- HTTP 指標
- S3 指標
- 彙總指標
- 日期指標
- 怪物指標
- Otel 追蹤原始指標
- Otel 追蹤群組指標
- 服務對應可設定狀態度量
- OpenSearch 指標
- 系統和計量指標

常用指標

以下是所有處理器和接收器通用的指標。

*########################## < ##### >< #### >< metric_name >#*例如，名為的子管線my-pipeline和日期處理器的recordsIn.count指標的完整名稱。my-pipeline.date.recordsIn.count

公制字尾	描述
recordsIn.count	記錄輸入至管線元件。此指標適用於處理器和接收器。 相關統計資料：總和 尺寸:PipelineName
recordsOut.count	管線元件的記錄輸出。此指標適用於處理器和來源。 相關統計資料：總和 尺寸:PipelineName
timeElapsed.count	執行配管元件期間記錄的資料點計數。此指標適用於處理器和接收器。 相關統計資料：總和 尺寸:PipelineName
timeElapsed.sum	執行管線元件期間經過的總時間。此測量結果適用於處理器和接收器，以毫秒為單位。 相關統計資料：總和 尺寸:PipelineName
timeElapsed.max	管線元件執行期間所經過的時間上限。此測量結果適用於處理器和接收器，以毫秒為單位。 相關統計資料：上限 尺寸:PipelineName

緩衝指標

下列測量結果適用於OpenSearch擷取為所有管線自動設定的預設「有界封鎖」緩衝區。

########################## < ##### > < ##### >#例如，名為的子管線的recordsWritten.count度量完整名稱my-pipeline為。my-pipeline.BlockingBuffer.recordsWritten.count

公制字尾	描述
recordsWritten.count	寫入緩衝區的記錄數。 相關統計資料：總和 尺寸:PipelineName
recordsRead.count	從緩衝區讀取的記錄數。 相關統計資料：總和 尺寸:PipelineName
recordsInFlight.value	從緩衝區讀取的未勾選記錄數。 相關統計數字：平均 尺寸:PipelineName
recordsInBuffer.value	目前在緩衝區中的記錄數。 相關統計數字：平均 尺寸:PipelineName
recordsProcessed.count	從緩衝區讀取並由管線處理的記錄數。 相關統計資料：總和 尺寸:PipelineName
recordsWriteFailed.count	管道無法寫入接收器的記錄數。 相關統計資料：總和 尺寸:PipelineName

公制字尾	描述
writeTimeElapsed.count	寫入緩衝區時記錄的資料點計數。 相關統計資料：總和 尺寸:PipelineName
writeTimeElapsed.sum	寫入緩衝區時經過的總時間，以毫秒為單位。 相關統計資料：總和 尺寸:PipelineName
writeTimeElapsed.max	寫入緩衝區時經過的時間上限，以毫秒為單位。 相關統計資料：上限 尺寸:PipelineName
writeTimeouts.count	寫入緩衝區逾時的計數。 相關統計資料：總和 尺寸:PipelineName
readTimeElapsed.count	從緩衝區讀取時記錄的資料點計數。 相關統計資料：總和 尺寸:PipelineName
readTimeElapsed.sum	從緩衝區讀取時經過的總時間，以毫秒為單位。 相關統計資料：總和 尺寸:PipelineName
readTimeElapsed.max	從緩衝區讀取時經過的時間上限，以毫秒為單位。 相關統計資料：上限 尺寸:PipelineName

公制字尾	描述
checkpointTimeElapsed.count	檢查點時記錄的資料點計數。 相關統計資料：總和 尺寸:PipelineName
checkpointTimeElapsed.sum	檢查點時經過的總時間，以毫秒為單位。 相關統計資料：總和 尺寸:PipelineName
checkpointTimeElapsed.max	檢查點所經過的時間上限，以毫秒為單位。 相關統計資料：上限 尺寸:PipelineName

簽名 V4 度量

下列量度適用於管線的擷取端點，並與來源外掛程式 (httpotel_trace、和otel_metrics) 產生關聯。對擷取端點的所有要求都必須使用簽章版本 4 簽署。這些指標可協助您在連線至管道時識別授權問題，或確認您已成功驗證。

每個量度都以子管線名稱和作為前綴。osis_sigv4_auth例如：*sub_pipeline_name*.osis_sigv4_auth.httpAuthSuccess.count。

公制字尾	描述
httpAuthSuccess.count	對管線的成功簽章 V4 要求數目。 相關統計資料：總和 尺寸:PipelineName
httpAuthFailure.count	對管線發出失敗的簽章 V4 要求數目。 相關統計資料：總和

公制字尾	描述
	尺寸:PipelineName
`httpAuthServerError.count`	傳回伺服器錯誤之管線的簽章 V4 要求數目。 相關統計資料：總和 尺寸:PipelineName

界限阻塞緩衝區指標

下列測量結果適用於有界封鎖緩衝區。每個量度都以子管線名稱和作為前綴。`BlockingBuffer`例如：*`sub_pipeline_name`*`.BlockingBuffer.bufferUsage.value`。

公制字尾	描述
`bufferUsage.value`	`buffer_size` 根據緩衝區中記錄數目的使用百分比。`buffer_size` 代表寫入緩衝區的記錄數目上限，以及尚未檢查的進行中記錄。 相關統計數字：平均 尺寸:PipelineName

Otel 追蹤來源指標

下列指標適用於 oTel 追蹤來源。每個量度都以子管線名稱和作為前綴。`otel_trace_source`例如：*`sub_pipeline_name`*`.otel_trace_source.requestTimeouts.count`。

公制字尾	描述
`requestTimeouts.count`	逾時的請求數。 相關統計資料：總和 尺寸:PipelineName
`requestsReceived.count`	外掛程式接收的請求數。

公制字尾	描述
	相關統計資料：總和 尺寸:PipelineName
successRequests.count	外掛程式成功處理的請求數。 相關統計資料：總和 尺寸:PipelineName
badRequests.count	外掛程式所處理之格式無效的要求數目。 相關統計資料：總和 尺寸:PipelineName
requestsTooLarge.count	要求數目，其內容中的跨度數目大於緩衝區容量。 相關統計資料：總和 尺寸:PipelineName
internalServerError.count	具有自訂例外狀況類型的外掛程式所處理的要求數目。 相關統計資料：總和 尺寸:PipelineName
requestProcessDuration.count	外掛程式處理要求時所記錄的資料點計數。 相關統計資料：總和 尺寸:PipelineName
requestProcessDuration.sum	外掛程式處理要求的總延遲時間，以毫秒為單位。 相關統計資料：總和 尺寸:PipelineName

公制字尾	描述
requestProcessDuration.max	外掛程式處理要求的最大延遲時間，以毫秒為單位。 相關統計資料：上限 尺寸:PipelineName
payloadSize.count	傳入要求的承載大小分佈計數，以位元組為單位。 相關統計資料：總和 尺寸:PipelineName
payloadSize.sum	傳入要求的裝載大小總分佈 (以位元組為單位)。 相關統計資料：總和 尺寸:PipelineName
payloadSize.max	傳入要求的裝載大小上限分配 (以位元組為單位)。 相關統計資料：上限 尺寸:PipelineName

歐特爾度量來源指標

下列指標適用於 oTel 指標來源。每個量度都以子管線名稱和作為前綴。otel_metrics_source例如：*sub_pipeline_name*.otel_metrics_source.requestTimeouts.count。

公制字尾	描述
requestTimeouts.count	逾時的請求總數。 相關統計資料：總和 尺寸:PipelineName
requestsReceived.count	外掛程式接收的請求總數。

公制字尾	描述
	相關統計資料：總和 尺寸:PipelineName
successRequests.count	外掛程式已成功處理的要求數目 (200 個回應狀態碼)。 相關統計資料：總和 尺寸:PipelineName
requestProcessDuration.count	外掛程式處理要求的延遲計數，以秒為單位。 相關統計資料：總和 尺寸:PipelineName
requestProcessDuration.sum	外掛程式處理要求的總延遲時間，以毫秒為單位。 相關統計資料：總和 尺寸:PipelineName
requestProcessDuration.max	外掛程式處理要求的最大延遲時間，以毫秒為單位。 相關統計資料：上限 尺寸:PipelineName
payloadSize.count	傳入要求的承載大小分佈計數，以位元組為單位。 相關統計資料：總和 尺寸:PipelineName
payloadSize.sum	傳入要求的裝載大小總分佈 (以位元組為單位)。 相關統計資料：總和 尺寸:PipelineName

公制字尾	描述
payloadSize.max	傳入要求的裝載大小上限分配 (以位元組為單位)。 相關統計資料：上限 尺寸:PipelineName

HTTP 指標

下列指標適用於 HTTP 來源。每個量度都以子管線名稱和作為前綴。http例如：*sub_pipeline_name*.http.requestsReceived.count。

公制字尾	描述
requestsReceived.count	/log/ingest 端點接收的請求數。 相關統計資料：總和 尺寸:PipelineName
requestsRejected.count	外掛程式拒絕的要求數 (429 回應狀態碼)。 相關統計資料：總和 尺寸:PipelineName
successRequests.count	外掛程式已成功處理的要求數目 (200 個回應狀態碼)。 相關統計資料：總和 尺寸:PipelineName
badRequests.count	外掛程式處理含有無效內容類型或格式 (400 回應狀態碼) 的要求數目。 相關統計資料：總和 尺寸:PipelineName
requestTimeouts.count	HTTP 來源伺服器中逾時的要求數目 (415 回應狀態碼)。

公制字尾	描述
	相關統計資料：總和 尺寸:PipelineName
requestsTooLarge.count	內容中事件大小大於緩衝區容量的要求數目 (413 回應狀態碼)。 相關統計資料：總和 尺寸:PipelineName
internalServerError.count	具有自訂例外狀況類型的外掛程式所處理的要求數目 (500 個回應狀態碼)。 相關統計資料：總和 尺寸:PipelineName
requestProcessDuration.count	外掛程式處理要求的延遲計數，以秒為單位。 相關統計資料：總和 尺寸:PipelineName
requestProcessDuration.sum	外掛程式處理要求的總延遲時間，以毫秒為單位。 相關統計資料：總和 尺寸:PipelineName
requestProcessDuration.max	外掛程式處理要求的最大延遲時間，以毫秒為單位。 相關統計資料：上限 尺寸:PipelineName
payloadSize.count	傳入要求的承載大小分佈計數，以位元組為單位。 相關統計資料：總和 尺寸:PipelineName

公制字尾	描述
payloadSize.sum	傳入要求的裝載大小總分佈 (以位元組為單位)。 相關統計資料：總和 尺寸:PipelineName
payloadSize.max	傳入要求的裝載大小上限分配 (以位元組為單位)。 相關統計資料：上限 尺寸:PipelineName

S3 指標

下列指標適用於 S3 來源。每個量度都以子管線名稱和作為前綴。s3例如：*sub_pipeline_name*.s3.s3ObjectsFailed.count。

公制字尾	描述
s3ObjectsFailed.count	外掛程式無法讀取的 S3 物件總數。 相關統計資料：總和 尺寸:PipelineName
s3ObjectsNotFound.count	外掛程式因 S3 發Not Found生錯誤而無法讀取的 S3 物件數目。這些量度也會計入s3ObjectsFailed 量度。 相關統計資料：總和 尺寸:PipelineName
s3ObjectsAccessDenied.count	外掛程式因 S3 發Forbidden 生Access Denied或錯誤而無法讀取的 S3 物件數目。這些量度也會計入s3ObjectsFailed 量度。 相關統計資料：總和

公制字尾	描述
	尺寸:PipelineName
s3ObjectReadTimeElapsed.count	外掛程式針對 S3 物件執行 GET 要求、剖析物件，以及將事件寫入緩衝區所花費的時間。 相關統計資料：總和 尺寸:PipelineName
s3ObjectReadTimeElapsed.sum	外掛程式針對 S3 物件執行 GET 要求、剖析物件，以及將事件寫入緩衝區所花費的總時間，以毫秒為單位。 相關統計資料：總和 尺寸:PipelineName
s3ObjectReadTimeElapsed.max	外掛程式針對 S3 物件執行 GET 要求、剖析物件並將事件寫入緩衝區所花費的時間上限 (以毫秒為單位)。 相關統計資料：上限 尺寸:PipelineName
s3ObjectSizeBytes.count	S3 物件大小的分佈計數，以位元組為單位。 相關統計資料：總和 尺寸:PipelineName
s3ObjectSizeBytes.sum	S3 物件大小的總分佈，以位元組為單位。 相關統計資料：總和 尺寸:PipelineName
s3ObjectSizeBytes.max	S3 物件大小的最大分佈，以位元組為單位。 相關統計資料：上限 尺寸:PipelineName

公制字尾	描述
s3ObjectProcessedBytes.count	外掛程式所處理的 S3 物件分佈計數，以位元組為單位。 相關統計資料：總和 尺寸:PipelineName
s3ObjectProcessedBytes.sum	外掛程式處理的 S3 物件總分佈，以位元組為單位。 相關統計資料：總和 尺寸:PipelineName
s3ObjectProcessedBytes.max	外掛程式所處理 S3 物件的最大分佈，以位元組為單位。 相關統計資料：上限 尺寸:PipelineName
s3ObjectsEvents.count	外掛程式收到的 S3 事件分佈計數。 相關統計資料：總和 尺寸:PipelineName
s3ObjectsEvents.sum	外掛程式收到的 S3 事件總分佈。 相關統計資料：總和 尺寸:PipelineName
s3ObjectsEvents.max	外掛程式收到的 S3 事件的最大分佈。 相關統計資料：上限 尺寸:PipelineName

公制字尾	描述
sqsMessageDelay.count	S3 會將建立物件的事件時間記錄到完全剖析物件時所記錄的資料點計數。 相關統計資料：總和 尺寸:PipelineName
sqsMessageDelay.sum	S3 記錄建立物件的事件時間到完全剖析之間的總時間 (以毫秒為單位)。 相關統計資料：總和 尺寸:PipelineName
sqsMessageDelay.max	S3 記錄建立物件的事件時間到完全剖析之間的時間上限 (以毫秒為單位)。 相關統計資料：上限 尺寸:PipelineName
s3ObjectsSucceeded.count	外掛程式成功讀取的 S3 物件數目。 相關統計資料：總和 尺寸:PipelineName
sqsMessagesReceived.count	外掛程式從佇列接收的 Amazon SQS 訊息數目。 相關統計資料：總和 尺寸:PipelineName
sqsMessagesDeleted.count	外掛程式從佇列中刪除的 Amazon SQS 訊息數目。 相關統計資料：總和 尺寸:PipelineName

公制字尾	描述
sqsMessagesFailed.count	外掛程式無法剖析的 Amazon SQS 訊息數目。 相關統計資料：總和 尺寸:PipelineName

彙總指標

下列量度適用於彙總處理器。每個量度都以子管線名稱和作為前綴。aggregate例如：*sub_pipeline_name*.aggregate.actionHandleEventsOut.count。

公制字尾	描述
actionHandleEvents Out.count	handleEvent 呼叫已設定動作所傳回的事件數目。 相關統計資料：總和 尺寸:PipelineName
actionHandleEvents Dropped.count	handleEvent 呼叫已設定動作所傳回的事件數目。 相關統計資料：總和 尺寸:PipelineName
actionHandleEvents ProcessingErrors.count	handleEvent 針對已設定動作進行的呼叫次數，導致錯誤。 相關統計資料：總和 尺寸:PipelineName
actionConcludeGrou pEventsOut.count	concludeGroup 呼叫已設定動作所傳回的事件數目。 相關統計資料：總和 尺寸:PipelineName

公制字尾	描述
actionConcludeGroupEventsDropped.count	condludeGroup 呼叫已設定動作時尚未傳回的事件數目。 相關統計資料：總和 尺寸:PipelineName
actionConcludeGroupEventsProcessingErrors.count	concludeGroup 針對已設定動作進行的呼叫次數，導致錯誤。 相關統計資料：總和 尺寸:PipelineName
currentAggregateGroups.value	目前群組數。當群組結束時，此量規會減少，而且當事件起始建立新群組時，此量規會增加。 相關統計數字：平均 尺寸:PipelineName

日期指標

下列量度適用於日期處理器。每個量度都以子管線名稱和作為前綴。date例如：*sub_pipeline_name*.date.dateProcessingMatchSuccess.count。

公制字尾	描述
dateProcessingMatchSuccess.count	至少一個與match組態選項指定模式相符的記錄數。 相關統計資料：總和 尺寸:PipelineName
dateProcessingMatchFailure.count	與match組態選項中指定的任何模式不符的記錄數目。 相關統計資料：總和

公制字尾	描述
	尺寸:PipelineName

怪物指標

下列指標適用於 Grok 處理器。每個量度都以子管線名稱和作為前綴。grok例如：*sub_pipeline_name*.grok.grokProcessingMatch.count。

公制字尾	描述
grokProcessingMatch.count	從match組態選項中找到至少一個模式相符的記錄數。 相關統計資料：總和 尺寸:PipelineName
grokProcessingMismatch.count	與match組態選項中指定的任何模式不符的記錄數目。 相關統計資料：總和 尺寸:PipelineName
grokProcessingErrors.count	記錄處理錯誤的數目。 相關統計資料：總和 尺寸:PipelineName
grokProcessingTimeouts.count	比對時逾時的記錄數。 相關統計資料：總和 尺寸:PipelineName
grokProcessingTime.count	個別記錄與match組態選項中的模式比對時所記錄的資料點計數。 相關統計資料：總和 尺寸:PipelineName

公制字尾	描述
grokProcessingTime.sum	每個個別記錄與match組態選項中的模式比對所花費的總時間量 (以毫秒為單位)。 相關統計資料：總和 尺寸:PipelineName
grokProcessingTime.max	每個個別記錄與match組態選項中的模式比對所花費的時間上限 (以毫秒為單位)。 相關統計資料：上限 尺寸:PipelineName

Otel 追蹤原始指標

下列指標適用於 oTel 追蹤原始處理器。每個量度都以子管線名稱和作為前綴。otel_trace_raw例如：*sub_pipeline_name*.otel_trace_raw.traceGroupCacheCount.value。

公制字尾	描述
traceGroupCacheCount.value	追蹤群組快取中的追蹤群組數目。 相關統計資料：總和 尺寸:PipelineName
spanSetCount.value	範圍集合中的範圍集合數目。 相關統計資料：總和 尺寸:PipelineName

Otel 追蹤群組指標

下列指標適用於 oTel 追蹤群組處理器。每個量度都以子管線名稱和作為前綴。otel_trace_group例如：*sub_pipeline_name*.otel_trace_group.recordsInMissingTraceGroup.count。

公制字尾	描述
recordsInMissingTraceGroup.count	遺失追蹤群組欄位的輸入記錄數目。 相關統計資料：總和 尺寸:PipelineName
recordsOutFixedTraceGroup.count	成功填入追蹤群組欄位的出口記錄數目。 相關統計資料：總和 尺寸:PipelineName
recordsOutMissingTraceGroup.count	遺失追蹤群組欄位的輸出記錄數目。 相關統計資料：總和 尺寸:PipelineName

服務對應可設定狀態度量

下列指標適用於服務對應狀態處理器。每個量度都以子管線名稱和作為前綴。service-map-stateful例如：*sub_pipeline_name*.service-map-stateful.spansDbSize.count。

公制字尾	描述
spansDbSize.value	在目前和之前的視窗持續時間內，MapDB 中跨越的記憶體內位元組大小。 相關統計數字：平均 尺寸:PipelineName

公制字尾	描述
traceGroupDbSize.value	在目前和之前的視窗持續時間內，MapDB 中追蹤群組的記憶體內位元組大小。 相關統計數字：平均 尺寸:PipelineName
spansDbCount.value	目前和之前視窗持續時間之間的 MapDB 中的跨距計數。 相關統計資料：總和 尺寸:PipelineName
traceGroupDbCount.value	目前和先前視窗持續時間中 MapDB 中追蹤群組的計數。 相關統計資料：總和 尺寸:PipelineName
relationshipCount.value	在目前和之前的視窗持續時間中儲存的關係計數。 相關統計資料：總和 尺寸:PipelineName

OpenSearch 指標

下列量度適用於接OpenSearch收器。每個量度都以子管線名稱和作為前綴。opensearch例如：*sub_pipeline_name*.opensearch.bulkRequestErrors.count。

公制字尾	描述
bulkRequestErrors.count	傳送大量要求時發生的錯誤總數。 相關統計資料：總和 尺寸:PipelineName

公制字尾	描述
documentsSuccess.count	透過大量要求成功傳送至OpenSearch服務的文件數目，包括重試。 相關統計資料：總和 尺寸:PipelineName
documentsSuccessFirstAttempt.count	第一次嘗試時透過大量要求成功傳送至OpenSearch服務的文件數目。 相關統計資料：總和 尺寸:PipelineName
documentErrors.count	大量請求傳送失敗的文件數目。 相關統計資料：總和 尺寸:PipelineName
bulkRequestFailed.count	失敗的批次要求數。 相關統計資料：總和 尺寸:PipelineName
bulkRequestNumberOfRetries.count	失敗的大量要求重試次數。 相關統計資料：總和 尺寸:PipelineName
bulkBadRequestErrors.count	傳送大量要求時遇到的Bad Request錯誤數目。 相關統計資料：總和 尺寸:PipelineName

公制字尾	描述
bulkRequestNotAllowedErrors.count	傳送大量要求時遇到的Request Not Allowed錯誤數目。 相關統計資料：總和 尺寸:PipelineName
bulkRequestInvalidInputErrors.count	傳送大量要求時遇到的Invalid Input錯誤數目。 相關統計資料：總和 尺寸:PipelineName
bulkRequestNotFoundErrors.count	傳送大量要求時遇到的Request Not Found錯誤數目。 相關統計資料：總和 尺寸:PipelineName
bulkRequestTimeoutErrors.count	傳送大量要求時遇到的Request Timeout錯誤數目。 相關統計資料：總和 尺寸:PipelineName
bulkRequestServerErrors.count	傳送大量要求時遇到的Server Error錯誤數目。 相關統計資料：總和 尺寸:PipelineName
bulkRequestSizeBytes.count	大量要求的裝載大小分佈計數，以位元組為單位。 相關統計資料：總和 尺寸:PipelineName

公制字尾	描述
bulkRequestSizeBytes.sum	大量要求的裝載大小總分佈，以位元組為單位。 相關統計資料：總和 尺寸:PipelineName
bulkRequestSizeBytes.max	批量請求的有效負載大小的最大分佈，以字節為單位。 相關統計資料：上限 尺寸:PipelineName
bulkRequestLatency.count	傳送要求至外掛程式時所記錄的資料點計數，包括重試。 相關統計資料：總和 尺寸:PipelineName
bulkRequestLatency.sum	傳送至外掛程式的要求總延遲 (包括重試)，以毫秒為單位。 相關統計資料：總和 尺寸:PipelineName
bulkRequestLatency.max	傳送至外掛程式的要求 (包括重試) 的最大延遲時間 (以毫秒為單位)。 相關統計資料：上限 尺寸:PipelineName
s3.dlqS3RecordsSuccess.count	成功傳送至 S3 無效字母佇列的記錄數。 相關統計資料：總和 尺寸:PipelineName

公制字尾	描述
s3.dlqS3RecordsFailed.count	無法傳送至 S3 無效字母佇列的資源數目。 相關統計資料：總和 尺寸:PipelineName
s3.dlqS3RequestSuccess.count	S3 無效字母佇列的成功要求數目。 相關統計資料：總和 尺寸:PipelineName
s3.dlqS3RequestFailed.count	S3 無效字母佇列的失敗要求數目。 相關統計資料：總和 尺寸:PipelineName
s3.dlqS3RequestLatency.count	請求傳送至 S3 無效字母佇列時所記錄的資料點計數，包括重試。 相關統計資料：總和 尺寸:PipelineName
s3.dlqS3RequestLatency.sum	傳送至 S3 無效字母佇列的請求總延遲 (包括重試)，以毫秒為單位。 相關統計資料：總和 尺寸:PipelineName
s3.dlqS3RequestLatency.max	傳送至 S3 無效字母佇列的要求延遲上限 (包括重試)，以毫秒為單位。 相關統計資料：上限 尺寸:PipelineName

公制字尾	描述
s3.dlqS3RequestSizeBytes.count	S3 無效字母佇列要求的有效負載大小分配計數，以位元組為單位。 相關統計資料：總和 尺寸:PipelineName
s3.dlqS3RequestSizeBytes.sum	S3 無效字母佇列要求的有效負載大小總分佈，以位元組為單位。 相關統計資料：總和 尺寸:PipelineName
s3.dlqS3RequestSizeBytes.max	S3 無效字母佇列的要求有效負載大小的最大分配，以位元組為單位。 相關統計資料：上限 尺寸:PipelineName

系統和計量指標

下列指標適用於整個OpenSearch擷取系統。這些指標不會加上任何字首。

指標	描述
system.cpu.usage.value	所有資料節點的可用 CPU 使用率百分比。 相關統計數字：平均 尺寸:PipelineName ,area, id
system.cpu.count.value	所有資料節點的 CPU 使用總量。 相關統計數字：平均 尺寸:PipelineName ,area, id

指標	描述
jvm.memory.max.value	可用於記憶體管理的記憶體容量上限，以位元組為單位。 相關統計數字：平均 尺寸:PipelineName ,area, id
jvm.memory.used.value	使用的記憶體總量，以位元組為單位。 相關統計數字：平均 尺寸：PipelineName area，id，
jvm.memory.committed.value	認可供使用的記憶體容量，以位元組為單位。 相關統計數字：平均 尺寸:PipelineName ,area, id
computeUnits	管線正在使用的擷取OpenSearch運算單元 (擷取 OCU) 數目。 相關統計：最大，總和，平均 尺寸:PipelineName

Amazon OpenSearch 擷取的最佳實務

本主題提供建立和管理 Amazon OpenSearch 擷取管道的最佳實務，並包含適用於許多使用案例的一般準則。每個工作負載都是獨一無二的，具有獨特的特性，因此沒有任何一個通用建議適合每個使用案例。

主題

- 一般最佳實務
- 建議的 CloudWatch 鬧鐘

一般最佳實務

下列一般最佳作法適用於建立和管理管線。

- 若要確保高可用性，請使用兩個或三個子網路設定VPC管線。如果您只在一個子網路中部署管線，且可用區域停止運作，您將無法擷取資料。
- 在每個管道中，我們建議將子配管數限制在 5 條或更少。
- 如果您使用 S3 來源外掛程式，請使用大小適中的 S3 檔案以獲得最佳效能。
- 如果您使用 S3 來源外掛程式，請為 S3 儲存貯體中每 0.25 GB 的檔案大小新增 30 秒的額外可見性逾時，以獲得最佳效能。
- 在管線配置中包含無效字母 queue (DLQ)，以便卸載失敗的事件並使其可供分析使用。如果您的接收器因不正確的對應或其他問題而拒絕資料，您可以將資料路由到，以便疑難排解並修正問題。DLQ

建議的 CloudWatch 鬧鐘

CloudWatch 當量度在一段時間內超過 CloudWatch 指定值時，警示會執行動作。例如，您可能想要 AWS 如果您的叢集健康狀態超過一分鐘，`red`請傳送電子郵件給您。本節包含 Amazon OpenSearch 擷取的一些建議警示，以及如何回應這些警示。

如需設定警示的詳細資訊，請參閱 Amazon CloudWatch 使用者指南中的建立 Amazon CloudWatch 警示。

警示	問題
`computeUnits` 最大值 = 設定`maxUnits`為 15 分鐘，連續 3 次	管線已達到最大容量，可能需要`maxUnits`更新。增加管道的最大容量
`opensearch.documentErrors.count` 總和 = 1 分鐘，連續 1 次的*`{sub_pipeline_name}`* `.opensear`	管線無法寫入接收 OpenSearch 器。檢查管線權限，並確認網域或集合狀況良好。如果已配置，您也可以檢查無效字母 queue (DLQ) 是否有失敗的事件。

警示	問題
ch.recordsIn.count 總和	
bulkRequestLatency.max 最大值為 > = x，表示 1 分鐘，連續 1 次	管道正在將資料傳送至接 OpenSearch 收器的高延遲時間。這可能是由於水槽尺寸過小或分片策略不佳，這導致水槽落後。持續的高延遲可能會影響管道效能，並可能導致用戶端的背壓。
httpAuthFailure.count 總和 >= 1 對於 1 分鐘，連續 1 次	擷取要求未經過驗證。確認所有用戶端都已正確啟用簽章版本 4 驗證。
system.cpu.usage.value 在 15 分鐘內平均大於等於 80%，連續 3 次	持續的高CPU使用率可能會有問題。考慮增加管線的最大容量。
bufferUsage.value 在 15 分鐘內平均大於等於 80%，連續 3 次	持續的高緩衝區使用率可能會有問題。考慮增加管線的最大容量。

您可能會考慮的其他警示

請考慮根據您經常使用的 Amazon OpenSearch 擷取功能設定下列警示。

警示	問題
dynamodb.exportJobFailure.count 總和 1	嘗試觸發匯出到 Amazon S3 失敗。
opensearch.EndtoEn	高EndtoEndLatency 於從 DynamoDB 串流讀取時所需的值。這可能是由於規模不足的 OpenSearch 叢集或最大管線OCU容量造成的，而對

警示	問題
dLatency.avg 平均值超過 15 分鐘，連續 4 次	於 DynamoDB 表上的WCU輸送量而言太低。 EndtoEndLatency 匯出後會較高，但會隨著時間的推移而減少，因為它可以追溯到最新的 DynamoDB 串流。
dynamodb.changeEventsProcessed.count 總和 == 0 表示 X 分鐘	沒有從 DynamoDB 串流收集任何記錄。這可能是由於表格上沒有任何活動，或者存取 DynamoDB 串流發生問題。
opensearch.s3.dlqS3RecordsSuccess.count 總和 >= opensearch.documentSuccess.count 總和 1 分鐘，連續 1 次	傳送的記錄數目DLQ比接收 OpenSearch 器更多。檢閱接 OpenSearch 收器外掛程式指標，以調查並判斷根本原因。
grok.grokProcessingTimeouts.count 總和 =recordsIn. 計數 1 分鐘的總和，連續 5 次	當 Grok 處理器嘗試模式匹配時，所有數據都會超時。這可能會影響效能並降低管道速度。請考慮調整您的模式以減少逾時。
grok.grokProcessingErrors.count 總和 >= 1 對於 1 分鐘，連續 1 次	Grok 處理器無法將模式與管道中的數據匹配，從而導致錯誤。查看您的數據和 Grok 插件配置，以確保預期模式匹配。

警示	問題
`grok.grok Processing Mismatch .count` 總和 =recordsIn. 計數 1 分鐘的總和，連續 5 次	Grok 處理器無法將模式與管道中的資料進行比對。查看您的數據和 Grok 插件配置，以確保預期模式匹配。
`date.date Processing MatchFailure.count` 總和 =recordsIn. 計數總和 1 分鐘，連續 5 次	日期處理器無法將任何模式與管線中的資料相符。檢閱您的資料和 Date 外掛程式設定，以確保預期的模式。
`s3.s3ObjectsFailed .count` 總和 >= 1 對於 1 分鐘，連續 1 次	之所以發生這個問題，是因為 S3 物件不存在，或管道的權限不足。確定`s3ObjectsNotFound.count` 和`s3ObjectsAccessDenied.count` 指標以確定根本原因。確認 S3 物件存在和/或更新許可。
`s3.sqsMessagesFailed.count` 總和 >= 1 對於 1 分鐘，連續 1 次	S3 插件無法處理 Amazon SQS 消息。如果您已在SQS佇列中DLQ啟用，請檢閱失敗的訊息。佇列可能正在接收管線嘗試處理的無效資料。
`http.badRequests.count` 總和 >= 1 對於 1 分鐘，連續 1 次	用戶端傳送錯誤的要求。確認所有用戶端都傳送適當的裝載。
`http.requestsTooLarge.count` 總和 >= 1 對於 1 分鐘，連續 1 次	來自HTTP來源外掛程式的要求包含太多資料，這超出了緩衝區容量。調整用戶端的批次大小。

警示	問題
`http.internalServerError.count` 總和 >= 0 表示 1 分鐘，連續 1 次	來HTTP源外掛程式在接收事件時遇到問題。
`http.requestTimeouts.count` 總和 >= 0 表示 1 分鐘，連續 1 次	來源逾時可能是管線佈建不足的結果。考慮增加管道`maxUnits`以處理額外的工作負載。
`otel_trace.badRequests.count` 總和 >= 1 對於 1 分鐘，連續 1 次	用戶端傳送錯誤的要求。確認所有用戶端都傳送適當的裝載。
`otel_trace.requestsTooLarge.count` 總和 >= 1 對於 1 分鐘，連續 1 次	來自 Otel 跟踪源插件的請求包含太多數據，這超出了緩衝區容量。調整用戶端的批次大小。
`otel_trace.internalServerError.count` 總和 >= 0 表示 1 分鐘，連續 1 次	Otel 跟踪源插件無法接收事件。
`otel_trace.requestTimeouts.count` 總和 >= 0 表示 1 分鐘，連續 1 次	來源逾時可能是管線佈建不足的結果。考慮增加管道`maxUnits`以處理額外的工作負載。

警示	問題
otel_metrics.requestTimeouts.count 總和 >= 0 表示 1 分鐘，連續 1 次	來源逾時可能是管線佈建不足的結果。考慮增加管道maxUnits以處理額外的工作負載。

Amazon OpenSearch 無服務器

Amazon OpenSearch 無伺服器是適用於 Amazon OpenSearch 服務的隨需 auto-scaling 配置。OpenSearch 無伺服器集合是根據應用程式需求調整運算容量的 OpenSearch 叢集。這與您手動管理容量的 OpenSearch 服務佈建的 OpenSearch 網域形成鮮明對比。

OpenSearch 無伺服器為罕見、間歇性或無法預測的工作負載提供簡單、具成本效益的選項。它可自動調整運算容量以符合應用程式用量，因此具有成本效益。

OpenSearch 無伺 OpenSearch 服器集合具有與佈建的服務網域所使用的相同類型的高容量、分散式和高可用性儲存磁碟區。

OpenSearch 無伺服器集合一律會加密。您可以選擇加密金鑰，但無法停用加密。如需詳細資訊，請參閱 the section called “加密”。

主題

- 優勢
- 什麼是 Amazon OpenSearch 無伺服器？
- 開始使用 Amazon OpenSearch 無伺服器
- 建立和管理 Amazon OpenSearch 無伺服器集合
- 管理 Amazon OpenSearch 無伺服器的容量限制
- 將資料導入 Amazon OpenSearch 無伺服器集合
- Amazon OpenSearch 無伺服器中的安全性概觀
- 標記 Amazon OpenSearch 無伺服器集合
- Amazon OpenSearch 無伺服器支援的操作和外掛程式
- 監控 Amazon OpenSearch 無伺服器

優勢

OpenSearch 無伺服器具有下列優點：

- 比佈建更簡單 — OpenSearch 無伺服器消除了管理 OpenSearch 叢集和容量的複雜性。它會自動調整叢集的大小並進行調校，負責碎片和索引生命週期管理。它還管理服務軟件更新和 OpenSearch版本升級。所有更新和升級都屬於非中斷式。

- 符合成本效益 — 使用 OpenSearch 無伺服器時，您只需為耗用的資源付費。如此就不需要為尖峰工作負載預先佈建和過度佈建。
- 高可用性 — OpenSearch 無伺服器透過備援支援生產工作負載，以防止可用區域中斷和基礎架構故障。
- 可擴充 — OpenSearch 無伺服器會自動擴展資源，以維持一致的快速資料擷取率和查詢回應時間。

什麼是 Amazon OpenSearch 無伺服器？

Amazon OpenSearch 無伺服器是 Amazon OpenSearch 服務的隨需無伺服器組態。無伺服器可免除佈建、設定和調整叢集的作業複雜性。 OpenSearch對於不想自行管理叢集的組織或沒有專門資源或專業知識來操作大型 OpenSearch 叢集的組織而言，這是一個不錯的選擇。使用 OpenSearch 無伺服器，您可以輕鬆搜尋和分析大量資料，而不必擔心基礎架構和資料管理問題。

OpenSearch 無伺服器集合是一組共同運作以支援特定工作負載或使用案例的 OpenSearch索引。集合比需要手動佈建的自我管理 OpenSearch 叢集更容易使用。

集合具有與佈建的 OpenSearch 服務網域所使用的相同類型的高容量、分散式和高可用性的儲存磁碟區，但是由於不需要手動設定和調整，因此可移除較多複雜性。資料會在集合中傳輸過程中加密。OpenSearch 無伺服器也支援 OpenSearch 儀表板，提供用於分析資料的直覺式介面。

無伺服器集合目前執行 2.0. OpenSearch x 版。隨著新版本發布， OpenSearch Serverless 將自動升級您的系列以使用新功能，錯誤修復和性能改進。

主題

- OpenSearch 無伺服器使用案例
- 開始使用
- 運作方式
- 選擇集合類型
- OpenSearch 無伺服器的定價
- 支援 AWS 區域
- 限制
- 比較 OpenSearch 服務與 OpenSearch 無伺服器

OpenSearch 無伺服器使用案例

OpenSearch 無伺服器支援兩種主要使用案例：

- 日誌分析：日誌分析區段專注於分析大量半結構化、機器產生的時間序列資料，以提供操作和使用者行為洞察。
- 全文檢索搜尋：全文檢索搜尋區段強化內部網路中的應用程式 (內容管理系統、法律文件) 以及面向網際網路的應用程式，例如電子商務網站內容搜尋。

建立集合時，您可以選擇上述其中一種使用案例。如需詳細資訊，請參閱 the section called “選擇集合類型”。

開始使用

若要開始使用 OpenSearch 無伺服器，請使用 OpenSearch 服務主控台、或其中一個 AWS SDK 建立一或多個集合。 AWS CLI如需協助您快速建立和執行集合的教學課程，請參閱 the section called “開始使用 OpenSearch 無伺服器”。

OpenSearch 無伺服器支援與 OpenSearch 開放原始碼套件相同的擷取和查詢 API 作業，因此您可以繼續使用現有的用戶端和應用程式。您的用戶端必須與 OpenSearch 2.x 相容，才能使用 OpenSearch 無伺服器。如需詳細資訊，請參閱 the section called “將資料擷取至集合”。

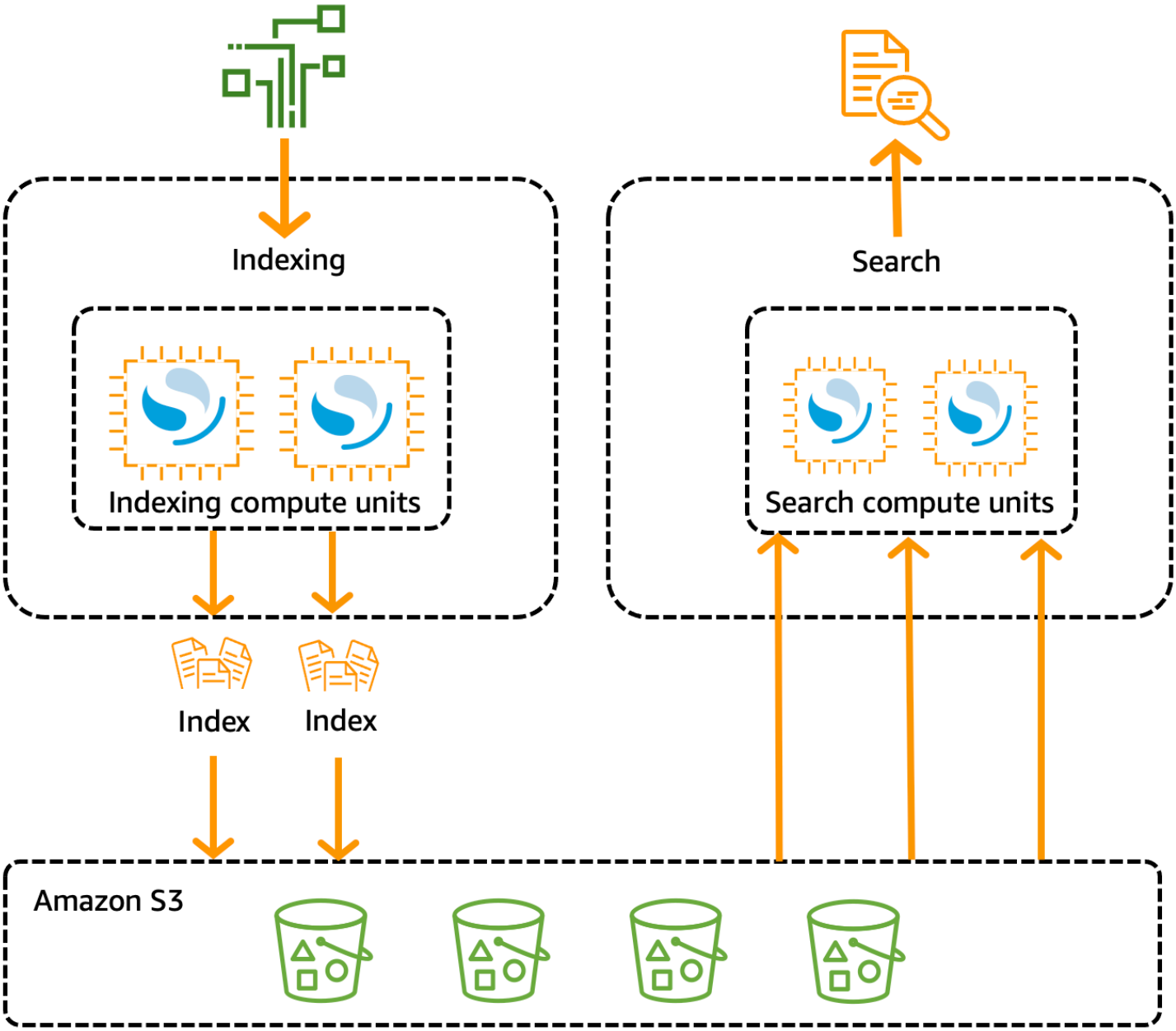
運作方式

傳統 OpenSearch 叢集有一組執行個體，可同時執行索引和搜尋作業，而索引儲存與運算容量緊密結合。相較之下， OpenSearch 無伺服器使用雲端原生架構，將索引 (擷取) 元件與搜尋 (查詢) 元件分開，而 Amazon S3 則是索引的主要資料儲存。

此分開的架構可讓您獨立擴展搜尋和索引編製功能，並且獨立於 S3 中的索引資料。該架構也會隔離擷取和查詢操作，以便同時執行這兩項操作，而不會爭用資源。

當您將資料寫入集合時， OpenSearch 無伺服器會將其散佈至索引運算單元。索引編製運算單元會擷取傳入資料，並將索引移至 S3。當您對收集資料執行搜尋時， OpenSearch Serverless 會將要求路由傳送至保留所查詢資料的搜尋運算單位。搜尋運算單元會直接從 S3 下載索引資料 (如果尚未在本機快取資料)、執行搜尋操作並執行彙總。

下圖說明了此分開的架構：



OpenSearch 用於資料擷取、搜尋和查詢的無伺服器運算容量是以 OpenSearch 運算單位 (OCU) 來衡量。每個 OCU 都是 6 GiB 記憶體和對應虛擬 CPU (vCPU) 的組合，並會建立 Amazon S3 的資料管道。每個 OCU 都包含足夠的暫時性熱儲存，可容納 120 GiB 的索引資料。

當您建立第一個集合時， OpenSearch 無伺服器會實體化兩個 OCU，一個用於索引，另一個用於搜尋。為確保高可用性，它也會啟動另一個可用區域中的待命節點集。基於開發和測試目的，您可以停用集合的 [啟用備援] 設定，這樣可以消除兩個待命複本，而且只建立兩個 OCU。依預設，會啟用備援作用中複本，這表示帳戶中的第一個集合總共會實例化四個 OCU。

即使在任何集合端點上沒有任何活動，這些 OCU 也會存在。所有後續的集合都會共用這些 OCU。當您在相同帳戶中建立其他集合時， OpenSearch Serverless 只會根據您指定的容量限制，視需要新增額外的 OCU 以供搜尋和擷取，以支援集合。容量會隨著運算用量的減少而縮減。

如需有關這些 OCU 如何計費的資訊，請參閱 the section called “ OpenSearch 無伺服器的定價”。

選擇集合類型

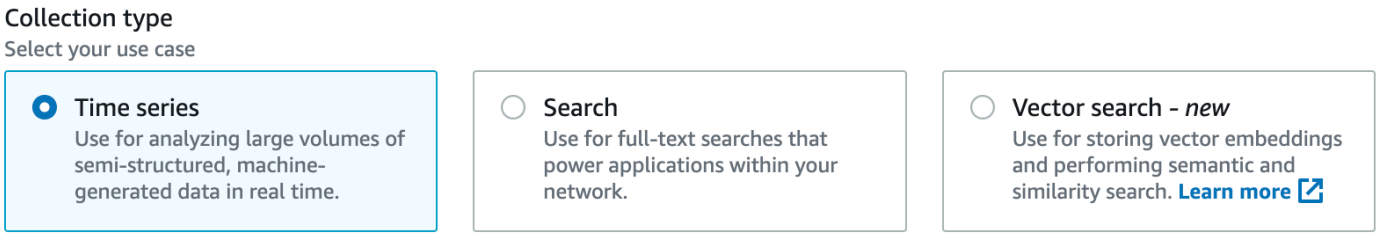
OpenSearch 無伺服器支援三種主要集合類型：

時間序列：日誌分析區段專注於即時分析大量半結構化、機器產生的資料，以提供操作、安全、使用者行為和商業洞察。

搜尋：支援內部網路中的應用程式 (內容管理系統、法律文件) 以及面向網際網路之應用程式的全文檢索搜尋，例如電子商務網站搜尋和內容搜尋。

向量搜尋 — 對向量嵌入進行語意搜尋，可簡化向量資料管理，並支援機器學習 (ML) 擴增搜尋體驗和生成 AI 應用程式，例如聊天機器人、個人助理和詐騙偵測。

您可以在第一次建立集合時選擇集合類型：



您選擇的集合類型取決於您計劃擷取至集合的資料類型，以及計劃的查詢方式。您無法在建立後變更集合類型。

集合類型有以下顯著差異：

- 對於搜索和矢量搜索集合，所有數據都存儲在熱存儲中，以確保快速查詢響應時間。時間序列集合使用熱儲存和暖儲存組合，其中最新的資料會保留在熱儲存中，以優化更頻繁存取資料的查詢回應時間。
- 對於時間序列和向量搜尋集合，您無法依據自訂文件 ID 編製索引，也無法依 upsert 要求進行更新。此操作保留給搜尋使用案例。您可以改用文件 ID 更新。如需詳細資訊，請參閱 the section called “支援的 OpenSearch API 作業和權限”。
- 對於搜尋和時間序列集合，您不能使用 k-nN 類型索引。

OpenSearch 無伺服器的定價

在 OpenSearch 無伺服器中，您需支付下列元件的費用：

- 資料擷取運算
- 搜尋和查詢運算
- 保留在 Amazon S3 中的儲存

OCU 按小時計費，精細程度為每秒。在帳單中，您會看到以 OCU 小時為單位的運算項目，其中包含資料擷取標籤和搜尋標籤。您也需按月支付存放在 Amazon S3 中的資料的費用。使用 OpenSearch 儀表板不會向您收取費用。

當您建立集合並啟用備援的主動複本時，您需支付至少 2 個 OCU [0.5 OCU x 2] 的擷取費用，以及搜尋 1 個 OCU [0.5 OCU x 2] 的費用。如果停用冗餘作用中複本，則帳戶中的第一個收集至少需支付 1 OCU [0.5 OCU x 2] 的費用。所有後續的集合可以共用這些 OCU。

OpenSearch 無伺服器會根據支援集合所需的運算能力和儲存裝置，以 1 個 OCU 為增量，新增額外的 OCU。您可以為您的帳戶設定 OCU 數量上限，以控制成本。

> **Note**
>
> 具有唯一性的系列 AWS KMS keys 無法與其他系列共用 OCU。

OpenSearch 無伺服器嘗試使用所需的最低資源來解決不斷變化的工作負載。在任何給定時間佈建的 OCU 數量可能會有所不同，而且不準確。隨著時間的推移， OpenSearch 無伺服器使用的演算法將持續改善，以便更有效地減少系統使用量。

如需完整的定價詳細資訊，請參閱 Amazon OpenSearch 服務定價。

支援 AWS 區域

OpenSearch AWS 區域 該服務的子集中提供無伺 OpenSearch 服器。如需支援區域的清單，請參閱 AWS 一般參考. OpenSearch

限制

OpenSearch 無伺服器有下列限制：

- 部分 OpenSearch API 作業不受支援。請參閱the section called “支援的 OpenSearch API 作業和權限”。
- 部分 OpenSearch 外掛程式不受支援。請參閱the section called “支持的 OpenSearch 插件”。
- 目前無法將您的資料從受管理的 OpenSearch 服務網域自動移轉至無伺服器集合。您必須將資料從網域重新索引至集合。
- 不支援集合的跨帳戶存取權。您無法在加密或資料存取政策中包含其他帳戶的集合。
- 不支援自訂 OpenSearch 外掛程式。
- 您無法建立或還原 OpenSearch 無伺服器集合的快照。
- 不支援跨區域搜尋和複寫。
- 您可以在單一帳戶和區域中擁有的無伺服器資源數量有限制。請參閱OpenSearch 無伺服器配額。
- 向量搜尋集合中索引的重新整理間隔約為 60 秒。搜尋和時間序列集合中索引的重新整理間隔約為 10 秒。
- 碎片數量、間隔數和重新整理間隔不可修改，且由 OpenSearch 無伺服器處理。分片策略基於收集類型和流量。例如，時間序列集合會根據寫入流量瓶頸來調整主要碎片。
- 支援最高 2.1 OpenSearch 版本的空間圖徵。

比較 OpenSearch 服務與 OpenSearch 無伺服器

在 OpenSearch 無伺服器中，某些概念和功能與佈建之 OpenSearch 服務網域的對應功能不同。例如，一個重要的差異是 OpenSearch 無伺服器沒有叢集或節點的概念。

下表說明 OpenSearch 無伺服器中的重要功能和概念與佈建的 OpenSearch 服務網域中的對等功能有何不同。

功能	OpenSearch 服務	OpenSearch 無伺服器
網域與集合比較	索引保留在網域中，這些網域是預先佈建的 OpenSearch 叢集。 如需詳細資訊，請參閱 建立和管理網域。	索引會保留在集合中，這些是代表特定工作負載或使用案例的索引邏輯分組。 如需詳細資訊，請參閱 the section called “建立、列出和刪除集合”。
節點類型和容量管理	您可以使用符合成本和效能規格的節點類型來建置叢集。您	OpenSearch 無伺服器會根據您的容量使用量，為您的帳戶自動擴展和佈建額外的運算單位。

功能	OpenSearch 服務	OpenSearch 無伺服器
	必須計算自己的儲存要求，並選擇網域的執行個體類型。 如需詳細資訊，請參閱 the section called “調整網域大小”。	如需詳細資訊，請參閱 the section called “管理容量限制”。
帳單	您需對於每小時 EC2 執行個體的使用，以及連接到執行個體的任何 EBS 儲存磁碟區的累積大小支付費用。 如需詳細資訊，請參閱 the section called “定價”。	我們會向您收取資料擷取運算、搜尋和查詢運算以及保留在 S3 中的儲存的費用 (以 OCU 小時計算)。 如需詳細資訊，請參閱 the section called “ OpenSearch 無伺服器的定價”。
加密	網域的靜態加密是選擇性。 如需詳細資訊，請參閱 the section called “靜態加密”。	集合需要靜態加密。 如需詳細資訊，請參閱 the section called “加密”。
資料存取控制	網域內資料的存取權由 IAM 政策和精細存取控制決定。	集合內的資料存取權由資料存取政策決定。
支援的 OpenSearch 作業	OpenSearch 服務支援所有 OpenSearch API 作業的子集。 如需詳細資訊，請參閱 the section called “受支援的操作”。	OpenSearch 無伺服器支援不同的 OpenSearch API 作業子集。 如需詳細資訊，請參閱 the section called “支援的操作和外掛程式”。
Dashboards 登入	使用使用者名稱和密碼登入。 如需詳細資訊，請參閱 the section called “以主要使用者身分存取 OpenSearch 儀表板”。	如果您已登入 AWS 主控台並瀏覽至控制面板 URL，就會自動登入。 如需詳細資訊，請參閱 the section called “存取 OpenSearch 儀表板”。

功能	OpenSearch 服務	OpenSearch 無伺服器
API	使用 OpenSearch 服務 API 作業以程式設計方式與OpenSearch 服務互動。	使用 OpenSearch 無伺服器 API 作業，以程式設計方式與OpenSearch 無伺服器互動。
網路存取	網域的網路設定會套用至網域端點以及 OpenSearch 儀表板端點。兩者的網路存取緊密結合。	網域端點和 OpenSearch 儀表板端點的網路設定會分離。您可以選擇不設定 OpenSearch 儀表板的網路存取權。 如需詳細資訊，請參閱 the section called “網路存取”。
簽署請求	使用 OpenSearch 高階和低階 REST 用戶端來簽署要求。將服務名稱指定為 `es`。	目前， OpenSearch 無伺服器支援 OpenSearch 服務支援的用戶端子集。 簽署請求時，請將服務名稱指定為 `aoss`。需要有 `x-amz-content-sha256` 標頭。如需詳細資訊，請參閱 the section called “其他客戶”。
OpenSearch 版本升級	當新版本的可用時，您可以手動升級您 OpenSearch的網域。您有責任確保您的網域符合升級要求，並且已解決任何突破性變更。	OpenSearch 無伺服器會自動將您的系列升級至新 OpenSearch 版本。一旦有新版本可用，不一定需要升級。
服務軟體更新	您可以在服務軟體更新可用時，手動將更新套用至您的網域。	OpenSearch 無伺服器會自動更新您的系列，以使用最新的錯誤修正、功能和效能改進。
VPC 存取	您可以在 VPC 中佈建您的網域。 您也可以建立其他OpenSearch 服務管理的 VPC 端點來存取網域。	您可以為您的帳戶建立一或多個OpenSearch 無伺服器管理的 VPC 端點。然後，請將這些端點包含在網路政策中。

功能	OpenSearch 服務	OpenSearch 無伺服器
SAML 身分驗證	您可以針對每個網域啟用 SAML 身分驗證。 如需詳細資訊，請參閱 the section called “SAML OpenSearch 儀表板的驗證”。	您可以在帳戶層級設定一個或多個 SAML 提供者，然後在資料存取政策中包含相關聯的使用者和群組 ID。 如需詳細資訊，請參閱 the section called “SAML認證”。
Transport Layer Security (TLS)	OpenSearch 服務支援 TLS 1.2，但建議您使用 TLS 1.3。	OpenSearch 無伺服器支援 TLS 1.2，但建議您使用 TLS 1.3。

開始使用 Amazon OpenSearch 無伺服器

本教學將引導您完成基本步驟，以快速啟動並執行 Amazon OpenSearch 無伺服器搜尋集合。搜尋集合可讓您為內部網路和網際網路對向應用程式 (例如電子商務網站搜尋和內容搜尋) 中的應用程式提供支援。

若要瞭解如何使用向量搜尋集合，請參閱the section called “使用向量搜尋集合”。如需使用集合的更多詳細資訊，請參閱本指南中的the section called “建立、列出和刪除集合”和其他主題。

在本教學課程中，您會完成下列步驟：

1. 設定許可
2. 建立集合
3. 上傳並搜尋資料
4. 刪除集合

步驟 1：設定許可

若要完成本教學課程並一般使用 OpenSearch 無伺服器，您必須擁有正確的 IAM 許可。在本教學課程中，您將建立集合、上傳並搜尋資料，然後刪除該集合。

使用者或角色必須連接身分型政策，該政策包含以下最低許可：

```
{
```

```
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "aoss:CreateCollection",
        "aoss:ListCollections",
        "aoss:BatchGetCollection",
        "aoss:DeleteCollection",
        "aoss:CreateAccessPolicy",
        "aoss:ListAccessPolicies",
        "aoss:UpdateAccessPolicy",
        "aoss:CreateSecurityPolicy",
        "aoss:GetSecurityPolicy",
        "aoss:UpdateSecurityPolicy",
        "iam:ListUsers",
        "iam:ListRoles"
      ],
      "Effect": "Allow",
      "Resource": "*"
    }
  ]
}
```

如需 OpenSearch 無伺服器 IAM 許可的詳細資訊，請參閱the section called “身分和存取權管理”。

步驟 2：建立集合

集合是一組 OpenSearch 索引，可協同運作以支援特定工作負載或使用案例。

建立 OpenSearch 無伺服器集合

1. 在以下位置打開 Amazon OpenSearch 服務控制台 https://console.aws.amazon.com/aos/home。
2. 在左側導覽窗格中選擇 Collections (集合)，然後選擇 Create collection (建立集合)。
3. 將集合命名為 movies。
4. 對於集合類型，選擇 Search (搜尋)。如需詳細資訊，請參閱選擇集合類型。
5. 在「安全性」中選擇「標準建立」
6. 在「加密」下選取「使用」 AWS 擁有的金鑰。這是 OpenSearch 無伺服 AWS KMS key 器將用來加密您的資料。
7. 在 Network (網路) 下，設定集合的網路設定。

   - 對於存取類型，選取 Public (公用)。

- 對於資源類型，請選擇 [啟用 OpenSearch 端點存取] 和 [啟用 OpenSearch 儀表板存取]。由於您將使用 OpenSearch 儀表板上傳和搜尋資料，因此您必須同時啟用兩者。

8. 選擇下一步。
9. 對於 Configure data access (設定資料存取)，請設定集合的存取設定。資料存取政策讓使用者和角色可以存取集合中的資料。在本教學課程中，我們將為單一使用者提供為 movies 集合中資料編製索引和進行搜尋所需的許可。

   建立可存取 movies 集合的單一規則。將規則命名為 Movies collection access (電影集合存取)。
10. 選擇 [新增主體、IAM 使用者和角色]，然後選取用來登入 OpenSearch 儀表板和索引資料的使用者或角色。選擇儲存。
11. 在 Index permissions (索引許可) 下，選取所有許可。
12. 選擇下一步。
13. 對於存取政策設定，請選擇 Create a new data access policy (建立新的資料存取政策) 並命名政策 movies。
14. 選擇下一步。
15. 檢閱集合設定，然後選擇 Submit (提交)。等待幾分鐘，讓收集狀態變成 `Active`。

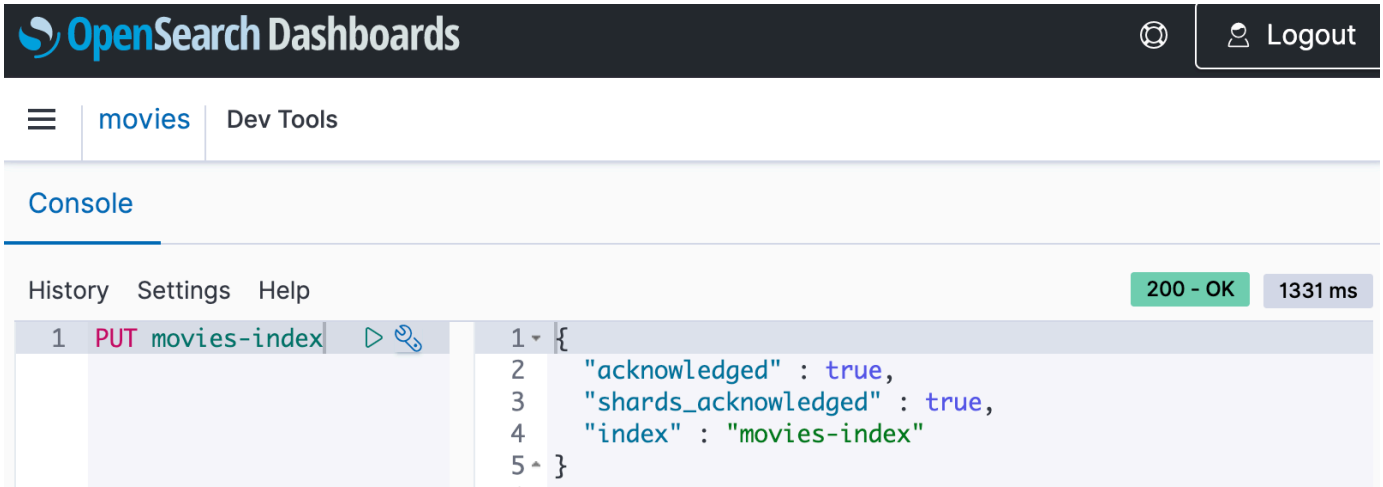
步驟 3：上傳並搜尋資料

您可以使用郵遞員或 cURL 將資料上傳至 OpenSearch 無伺服器集合。為了簡潔起見，這些示例使用 OpenSearch 儀表板控制台中的開發工具。

為 movies 集合中的資料編製索引和進行搜尋

1. 在左側導覽窗格中選擇 Collections (集合)，然後選擇 movies 集合以開啟其詳細資訊頁面。
2. 選擇集合的 OpenSearch 儀表板 URL。URL 採用的格式為 `https://dashboards.{region}.aoss.amazonaws.com/_login/?collectionId={collection-id}`。
3. 在 OpenSearch 儀表板中，開啟左側導覽窗格，然後選擇 [開發工具]。
4. 若要建立名為 movies-index 的單一索引，請傳送以下請求：

```
PUT movies-index
```



5. 若要將單一文件的索引編製為 movies-index，請傳送以下請求：

```
PUT movies-index/_doc/1
{
  "title": "Shawshank Redemption",
  "genre": "Drama",
  "year": 1994
}
```

6. 要搜索 OpenSearch 儀表板中的數據，您需要配置至少一個索引模式。 OpenSearch 使用這些模式來識別您要分析的索引。開啟左側導覽窗格，依序選擇 Stack Management (堆疊管理)、Index Patterns (索引模式)，然後選擇 Create index pattern (建立索引模式)。對於本教學課程，輸入 movies。
7. 選擇 Next step (下一步)，然後選擇 Create index pattern (建立索引模式)。建立模式之後，您可以檢視各種文件欄位，例如 `title` 和 `genre`。
8. 若要開始搜尋資料，請再次開啟左側導覽窗格，然後選擇 Discover (探索)，或使用開發工具中的搜尋 API。

步驟 4：刪除集合

movies 集合用於測試目的，因此請確保在完成實驗後將其刪除。

若要刪除 OpenSearch 無伺服器集合

1. 返回 Amazon OpenSearch 服務控制台。
2. 在左側導覽窗格中選擇 Collections (集合)，然後選擇 movies 集合。

3. 選擇 Delete (刪除)，並確認刪除。

後續步驟

您現在已知道如何建立集合並為資料編製索引，您可能想要嘗試以下一些練習：

- 查看用於建立集合的更多進階選項。如需詳細資訊，請參閱 the section called “建立、列出和刪除集合”。
- 了解如何設定安全政策以大規模管理集合安全性。如需詳細資訊，請參閱 the section called “ OpenSearch 無伺服器的安全性”。
- 探索將資料的索引編製為集合的其他方法。如需更多詳細資訊，請參閱 the section called “將資料擷取至集合”。

建立和管理 Amazon OpenSearch 無伺服器集合

您可以使 OpenSearch 用主控台、AWS CLI和 API、AWS開發套件和. AWS CloudFormation

主題

- 建立、列出和刪除 Amazon OpenSearch 無伺服器集合
- 使用向量搜尋集合
- 搭配 Amazon OpenSearch 無伺服器使用資料生命週期政策
- 使用開AWS發套件與 Amazon OpenSearch 無伺服器互動
- 使用建AWS CloudFormation立亞馬遜OpenSearch無伺服器集合

建立、列出和刪除 Amazon OpenSearch 無伺服器集合

Amazon OpenSearch 無伺服器中的集合是由代表分析工作負載的一或多個索引組成的邏輯分組。OpenSearch 服務會自動管理和調整集合，需要最少的手動輸入。

主題

- 必要許可
- 建立集合
- 存取 OpenSearch 儀表板
- 檢視集合

- 刪除集合

必要許可

OpenSearch 無伺服器會使用下列 AWS Identity and Access Management (IAM) 許可來建立和管理集合。您可以指定 IAM 條件，將使用者限制在特定集合內。

- `aoss:CreateCollection` ：建立集合。
- `aoss:ListCollections` ：列出目前帳戶中的集合。
- `aoss:BatchGetCollection` ：取得有關一個或多個集合的詳細資訊。
- `aoss:UpdateCollection` ：修改集合。
- `aoss:DeleteCollection` ：刪除集合。

下列身分型存取政策範例提供使用者管理名為 Logs 的單一集合所需的最低許可：

```
[
   {
      "Sid":"Allows managing logs collections",
      "Effect":"Allow",
      "Action":[
         "aoss:CreateCollection",
         "aoss:ListCollections",
         "aoss:BatchGetCollection",
         "aoss:UpdateCollection",
         "aoss:DeleteCollection",
         "aoss:CreateAccessPolicy",
         "aoss:CreateSecurityPolicy"
      ],
      "Resource":"*",
      "Condition":{
         "StringEquals":{
            "aoss:collection":"Logs"
         }
      }
   }
]
```

需要加密、網路和資料存取政策，才能讓集合正常運作，因此要將 `aoss:CreateAccessPolicy` 和 `aoss:CreateSecurityPolicy` 包含在內。如需詳細資訊，請參閱 the section called “身分和存取權管理”。

> **Note**
>
> 如果您要在帳戶中建立第一個集合，您也需要 `iam:CreateServiceLinkedRole` 許可。如需詳細資訊，請參閱 the section called “集合建立角色”。

建立集合

您可以使用主控台或建 AWS CLI 立無伺服器集合。這些步驟涵蓋如何建立搜尋或時間序列集合。若要建立向量搜尋集合，請參閱the section called “使用向量搜尋集合”。

建立集合 (主控台)

使用主控台建立集合

1. 導航到 Amazon OpenSearch 服務控制台 https://console.aws.amazon.com/aos/home/.
2. 展開左側導覽窗格中的 Serverless (無伺服器)，然後選擇 Collections (集合)。
3. 選擇 Create collection (建立集合)。
4. 提供集合的名稱和描述。名稱必須符合下列條件：
   - 對於您的帳戶而言是唯一的， AWS 區域
   - 開頭為小寫字母
   - 包含 3 到 32 個之間字元數
   - 只能包含小寫字母 a-z、數字 0-9 和連字號 (-)
5. 選擇集合類型：
   - 搜尋：支援內部網路中的應用程式以及面向網際網路之應用程式的全文檢索搜尋。所有搜尋資料均存放在熱儲存中，以確保快速的查詢回應時間。
   - Time series (時間序列)：著重於分析大量半結構化、機器產生之資料的日誌分析區段。至少 24 小時的資料會儲存在熱索引中，其餘資料會保留在暖儲存區中。
   - 向量搜尋 — 可簡化向量資料管理的向量嵌入的語義搜尋。支援機器學習 (ML) 擴增搜尋體驗和生成 AI 應用程式，例如聊天機器人、個人助理和詐騙偵測。

如需詳細資訊，請參閱 the section called “選擇集合類型”。

6. 在 [部署類型] 下，選擇集合的備援設定。根據預設，每個集合都建立具有冗餘，這表示索引和搜尋 OpenSearch Compute Units (OCU) 每個集合在不同的可用區域中都有自己的待命複本。基於開發和測試目的，您可以選擇停用備援，如此可將集合中的 OCU 數量減少為兩個。如需詳細資訊，請參閱 the section called “運作方式”。
7. 在「加密」下，選擇用來加密資料的 AWS KMS 金鑰。 OpenSearch 如果您輸入的集合名稱符合加密原則中定義的模式，則無伺服器會通知您。您可以選擇保留此相符項目，也可以使用唯一的加密設定進行覆寫。如需詳細資訊，請參閱 the section called “加密”。
8. 在 Network access settings (網路存取設定) 下，設定集合的網路存取。
   - 對於存取類型，請選取公用或私人。然後，指定哪些 VPC 端點 AWS 服務 可以存取集合。
     - 要存取的 VPC 端點 — 指定一或多個允許透過存取的 VPC 端點。若要建立 VPC 端點，請參閱 the section called “VPC 端點”。
     - AWS 服務 私人存取 — 選取一或多個支援的服務以允許存取。
   - 對於資源類型，請選取集合是否可透過其OpenSearch端點存取 (透過 curl、Postter 等進行 API 呼叫)、透過OpenSearch 儀表板端點存取 (以使用視覺效果並透過主控台進行 API 呼叫)，或透過兩者進行存取。

   > **Note**
   >
   > AWS 服務 私人存取僅適用於 OpenSearch端點，而不適用於 OpenSearch 儀表板端點。

   OpenSearch 如果您輸入的集合名稱符合網路原則中定義的模式，則無伺服器會通知您。您可以選擇保留此相符項目，也可以使用自訂網路設定進行覆寫。如需詳細資訊，請參閱 the section called “網路存取”。
9. (選用) 將一個或多個標籤新增至集合。如需詳細資訊，請參閱 the section called “標記集合”。
10. 選擇下一步。
11. 設定集合的資料存取規則，以定義可存取集合中資料的使用者。針對您建立的每個規則，執行下列步驟：
    - 選擇 Add principals (新增主體)，然後選取要向其提供資料存取權的一個或多個 IAM 角色或 SAML 使用者和群組。

- 在 Grant permissions (授予許可)下選取別名、範本和索引許可，以授予關聯的主體。如需完整的許可及其允許之存取的完整清單，請參閱 the section called “支援的 OpenSearch API 作業和權限”。

OpenSearch 如果您輸入的集合名稱與資料存取原則中定義的模式相符，則無伺服器會通知您。您可以選擇保留此相符項目，也可以使用唯一的資料存取設定進行覆寫。如需詳細資訊，請參閱 the section called “資料存取控制”。

12. 選擇下一步。
13. 在 Data access policy settings (資料存取政策設定) 下，選擇如何處理您剛建立的規則。您可以使用它們來建立新的資料存取政策，或將其新增至現有政策。
14. 檢閱集合組態，然後選擇 Submit (提交)。

`Creating`當「 OpenSearch 無伺服器」建立集合時，收集狀態會變更為。

建立集合 (CLI)

使用建立集合之前 AWS CLI，您必須擁有一個加密原則，其資源模式符合所需的集合名稱。例如，如果您計劃將集合命名為 logs-application，則可以建立如下所示的加密政策：

```
aws opensearchserverless create-security-policy \
  --name logs-policy \
  --type encryption --policy "{\"Rules\":[{\"ResourceType\":\"collection\",\"Resource
\":[\"collection\/logs-application\"]}],\"AWSOwnedKey\":true}"
```

如果您計劃將政策用於其他集合，則可以使規則的範圍更廣泛，例如 `collection/logs*` 或 `collection/*`。

您也需要以網路政策的形式設定集合的網路設定。使用先前的 logs-application 範例，您可建立下列網路政策：

```
aws opensearchserverless create-security-policy \
  --name logs-policy \
  --type network --policy "[{\"Description\":\"Public access for logs collection
\",\"Rules\":[{\"ResourceType\":\"dashboard\",\"Resource\":[\"collection\/logs-
application\"]},{\"ResourceType\":\"collection\",\"Resource\":[\"collection\/logs-
application\"]}],\"AllowFromPublic\":true}]"
```

> **Note**
> 您可以在建立集合之後建立網路政策，但建議您事先執行此操作。

若要建立系列，請傳送CreateCollection要求：

```
aws opensearchserverless create-collection --name "logs-application" --type SEARCH --
description "A collection for storing log data"
```

對於 type，指定 SEARCH 或 TIMESERIES。如需詳細資訊，請參閱 the section called “選擇集合類型”。

回應範例

```
{
    "createCollectionDetail": {
        "id": "07tjusf2h91cunochc",
        "name": "books",
        "description":"A collection for storing log data",
        "status": "CREATING",
        "type": "SEARCH",
        "kmsKeyArn": "auto",
        "arn": "arn:aws:aoss:us-east-1:123456789012:collection/07tjusf2h91cunochc",
        "createdDate": 1665952577473
    }
}
```

如果您未在請求中指定集合類型，即會預設為 TIMESERIES。如果您的集合使用 AWS 擁有的金鑰加密，則 kmsKeyArn 是 auto 而不是 ARN。

> **Important**
> 建立集合後，除非該集合符合資料存取政策，否則您將無法存取它。如需建立資料存取政策的說明，請參閱 the section called “資料存取控制”。

存取 OpenSearch 儀表板

使用建立商品系列後 AWS Management Console，您可以導覽至該系列的 OpenSearch 儀表板 URL。您可以在左側導覽窗格中選擇「商品系列」，然後選取商品系列以開啟其詳細資訊頁面，以尋找儀表板 URL。URL 採用的格式為 `https://dashboards.us-east-1.aoss.amazonaws.com/_login/?collectionId=07tjusf2h91cunochc`。導航到 URL 後，您將自動登錄到儀表板。

如果您已經有可用的 OpenSearch 儀表板 URL，但不在 AWS Management Console，從瀏覽器呼叫儀表板 URL 將重新導向到控制台。輸入 AWS 認證後，您將自動登入儀表板。如需存取 SAML 集合的相關資訊，請參閱使用 SAML 存取 OpenSearch 儀表板。

OpenSearch 儀表板主控台逾時為一小時，無法設定。

> **Note**
>
> 2023 年 5 月 10 日，為 OpenSearch 儀表板 OpenSearch 引入了一個通用的全球端點。您現在可以在具有採用格式的 URL 瀏覽器中導覽至「 OpenSearch 儀表板」`https://dashboards.us-east-1.aoss.amazonaws.com/_login/?collectionId=07tjusf2h91cunochc`。為了確保回溯相容性，我們將繼續以該格式支援現有集合特定 OpenSearch 儀表板端點`https://07tjusf2h91cunochc.us-east-1.aoss.amazonaws.com/_dashboards`。

檢視集合

您可以在 Amazon OpenSearch 服務主控台的「集合」索引標籤 AWS 帳戶 上檢視現有的商品系列。

若要列出系列及其 ID，請傳送ListCollections請求。

```
aws opensearchserverless list-collections
```

回應範例

```
{
   "collectionSummaries":[
      {
         "arn":"arn:aws:aoss:us-east-1:123456789012:collection/07tjusf2h91cunochc",
         "id":"07tjusf2h91cunochc",
         "name":"my-collection",
```

```
            "status":"CREATING"
        }
    ]
}
```

若要限制搜尋結果，請使用集合篩選條件。此請求會篩選對處於 ACTIVE 狀態之集合的回應：

```
aws opensearchserverless list-collections --collection-filters '{ "status": "ACTIVE" }'
```

若要取得有關一或多個集合 (包括 OpenSearch 端點和 OpenSearch 儀表板端點) 的更多詳細資訊，請傳送BatchGetCollection要求：

```
aws opensearchserverless batch-get-collection --ids ["07tjusf2h91cunochc",
 "1iu5usc4rame"]
```

> **Note**
>
> 您可以在請求中包含 `--names` 或 `--ids`，但不能同時包含兩者。

回應範例

```
{
   "collectionDetails":[
      {
         "id": "07tjusf2h91cunochc",
         "name": "my-collection",
         "status": "ACTIVE",
         "type": "SEARCH",
         "description": "",
         "arn": "arn:aws:aoss:us-east-1:123456789012:collection/07tjusf2h91cunochc",
         "kmsKeyArn": "arn:aws:kms:us-
east-1:123456789012:key/1234abcd-12ab-34cd-56ef-1234567890ab",
         "createdDate": 1667446262828,
         "lastModifiedDate": 1667446300769,
         "collectionEndpoint": "https://07tjusf2h91cunochc.us-
east-1.aoss.amazonaws.com",
         "dashboardEndpoint": "https://07tjusf2h91cunochc.us-east-1.aoss.amazonaws.com/
_dashboards"
      },
      {
```

```
         "id": "178ukvtg3i82dvopdid",
         "name": "another-collection",
         "status": "ACTIVE",
         "type": "TIMESERIES",
         "description": "",
         "arn": "arn:aws:aoss:us-east-1:123456789012:collection/178ukvtg3i82dvopdid",
         "kmsKeyArn": "arn:aws:kms:us-
east-1:123456789012:key/1234abcd-12ab-34cd-56ef-1234567890ab",
         "createdDate": 1667446262828,
         "lastModifiedDate": 1667446300769,
         "collectionEndpoint": "https://178ukvtg3i82dvopdid.us-
east-1.aoss.amazonaws.com",
         "dashboardEndpoint": "https://178ukvtg3i82dvopdid.us-
east-1.aoss.amazonaws.com/_dashboards"
      }
   ],
   "collectionErrorDetails":[]
}
```

刪除集合

刪除集合會刪除集合中的所有資料和索引。刪除集合後，您將無法復原集合。

使用主控台刪除集合

1. 從 Amazon OpenSearch 服務主控台的「集合」面板中，選取要刪除的集合。
2. 選擇 Delete (刪除)，並確認刪除。

若要使用刪除集合 AWS CLI，請傳送DeleteCollection要求：

```
aws opensearchserverless delete-collection --id 07tjusf2h91cunochc
```

回應範例

```
{
   "deleteCollectionDetail":{
      "id":"07tjusf2h91cunochc",
      "name":"my-collection",
      "status":"DELETING"
   }
}
```

使用向量搜尋集合

OpenSearch 無伺服器中的向量搜尋集合類型提供可擴充且高效能的相似性搜尋功能。您可以輕鬆建置現代機器學習 (ML) 擴增搜尋體驗和生成人工智慧 (AI) 應用程式，而無需管理基礎向量資料庫基礎架構。

向量搜尋系列的使用案例包括影像搜尋、文件搜尋、音樂擷取、產品推薦、影片搜尋、位置型搜尋、詐騙偵測和異常偵測。

由於 OpenSearch 無伺服器的向量引擎是由中的 k 最近鄰點 (k-nN) 搜尋功能提供支援 OpenSearch，因此您可以在無伺服器環境的簡易性下獲得相同的功能。此引擎支援 k-NN OpenSearch API 作業。透過這些作業，您可以利用全文檢索搜尋、進階篩選、彙總、地理空間查詢、巢狀查詢以加快資料擷取速度，以及增強的搜尋結果。

向量引擎提供距離度量，例如歐幾里得距離、餘弦相似度和點積相似度，並且可容納 16,000 個維度。您可以為中繼資料儲存具有各種資料類型的欄位，例如數字、布林值、日期、關鍵字和地理點。您還可以將帶有文本的字段存儲為描述性信息，以向存儲的向量添加更多上下文。分配數據類型可降低複雜性，提高可維護性，並避免數據重複，版本兼容性挑戰和許可問題。

開始使用向量搜尋集合

在本教學課程中，您將完成下列步驟，以即時儲存、搜尋和擷取向量嵌入：

1. 設定許可
2. 建立集合
3. 上傳並搜尋資料
4. 刪除集合

步驟 1：設定許可

若要完成本教學課程 (以及一般使用 OpenSearch 無伺服器)，您必須擁有正確的 AWS Identity and Access Management (IAM) 許可。在本教學課程中，您會建立系列、上傳和搜尋資料，然後刪除系列。

使用者或角色必須連接身分型政策，該政策包含以下最低許可：

```
{
  "Version": "2012-10-17",
```

```
  "Statement": [
    {
      "Action": [
        "aoss:CreateCollection",
        "aoss:ListCollections",
        "aoss:BatchGetCollection",
        "aoss:DeleteCollection",
        "aoss:CreateAccessPolicy",
        "aoss:ListAccessPolicies",
        "aoss:UpdateAccessPolicy",
        "aoss:CreateSecurityPolicy",
        "iam:ListUsers",
        "iam:ListRoles"
      ],
      "Effect": "Allow",
      "Resource": "*"
    }
  ]
}
```

如需 OpenSearch 無伺服器 IAM 許可的詳細資訊，請參閱the section called “身分和存取權管理”。

步驟 2：建立集合

集合是一組 OpenSearch 索引，可協同運作以支援特定工作負載或使用案例。

若要建立 OpenSearch 無伺服器集合

1. 在以下位置打開 Amazon OpenSearch 服務控制台 https://console.aws.amazon.com/aos/home。
2. 在左側導覽窗格中選擇 Collections (集合)，然後選擇 Create collection (建立集合)。
3. 命名收集房屋。
4. 對於集合類型，請選擇向量搜尋。如需詳細資訊，請參閱 the section called “選擇集合類型”。
5. 在 [部署類型] 下，清除 [啟用備援 (主動複本)]。這會在開發或測試模式中建立集合，並將集合中的 OpenSearch 運算單元 (OCU) 數量減少為兩個。如果您要在此自學課程中建立生產環境，請保持選取勾選方塊。
6. 在 [安全性] 下，選取 [輕鬆建立] 以簡化安全性設定。預設情況下，向量引擎中的所有資料都會在傳輸過程中和靜態時進行加密。向量引擎支援精細的 IAM 許可，因此您可以定義誰可以建立、更新和刪除加密、網路、集合和索引。
7. 選擇下一步。
8. 檢閱集合設定，然後選擇 Submit (提交)。等待幾分鐘，讓收集狀態變成 `Active`。

步驟 3：上傳並搜尋資料

索引是具有通用數據模式的文檔集合，它為您提供了一種存儲，搜索和檢索向量嵌入和其他字段的方法。您可以使用 OpenSearch 儀表板中的開發工具主控台或 HTTP 工具 (例如郵遞員或 aw scurl)，建立資料並將其上傳至 OpenSearch 無伺服器集合中的索引。本教學課程使用開發工具。

為 movies 集合中的資料編製索引和進行搜尋

1. 若要為新集合建立單一索引，請在 Dev Tools 主控台中傳送下列要求。默認情況下，這將創建一個帶有`nmslib`引擎和歐幾里得距離的索引。

```
PUT housing-index
{
   "settings": {
      "index.knn": true
   },
   "mappings": {
      "properties": {
         "housing-vector": {
            "type": "knn_vector",
            "dimension": 3
         },
         "title": {
            "type": "text"
         },
         "price": {
            "type": "long"
         },
         "location": {
            "type": "geo_point"
         }
      }
   }
}
```

2. 要索引單個文檔到住房索引，發送以下請求：

```
POST housing-index/_doc
{
  "housing-vector": [
    10,
    20,
    30
```

```
  ],
  "title": "2 bedroom in downtown Seattle",
  "price": "2800",
  "location": "47.71, 122.00"
}
```

3. 若要搜尋與索引中類似的屬性，請傳送下列查詢：

```
GET housing-index/_search
{
    "size": 5,
    "query": {
        "knn": {
            "housing-vector": {
                "vector": [
                    10,
                    20,
                    30
                ],
                "k": 5
            }
        }
    }
}
```

步驟 4：刪除集合

因為住房集合是用於測試目的，請確保在完成實驗後將其刪除。

若要刪除 OpenSearch 無伺服器集合

1. 返回 Amazon OpenSearch 服務控制台。
2. 在左側導覽窗格中選擇「集合」，然後選取屬性集合。
3. 選擇刪除並確認刪除。

篩選搜尋

您可以使用過濾器來優化語義搜索結果。若要建立索引並對文件執行篩選搜尋，請使用下列指示取代上一個教學課程中的「上載」和「搜尋資料」。其他步驟保持不變。如需有關篩選器的詳細資訊，請參閱 K-NN 使用篩選器搜尋。

為 movies 集合中的資料編製索引和進行搜尋

1. 若要為集合建立單一索引，請在 Dev Tools 主控台中傳送下列要求：

```
PUT housing-index-filtered
{
  "settings": {
    "index.knn": true
  },
  "mappings": {
    "properties": {
      "housing-vector": {
        "type": "knn_vector",
        "dimension": 3,
        "method": {
          "engine": "faiss",
          "name": "hnsw"
        }
      },
      "title": {
        "type": "text"
      },
      "price": {
        "type": "long"
      },
      "location": {
        "type": "geo_point"
      }
    }
  }
}
```

2. 若要將單一文件編入索引 housing-index-filtered，請傳送下列要求：

```
POST housing-index-filtered/_doc
{
  "housing-vector": [
    10,
    20,
    30
  ],
  "title": "2 bedroom in downtown Seattle",
  "price": "2800",
```

```
  "location": "47.71, 122.00"
}
```

3. 要以指定價格並在地理位置的指定距離內搜索西雅圖的公寓數據，請發送以下請求：

```
GET housing-index-filtered/_search
{
  "size": 5,
  "query": {
    "knn": {
      "housing-vector": {
        "vector": [
          0.1,
          0.2,
          0.3
        ],
        "k": 5,
        "filter": {
          "bool": {
            "must": [
              {
                "query_string": {
                  "query": "Find me 2 bedroom apartment in Seattle under $3000 ",
                  "fields": [
                    "title"
                  ]
                }
              },
              {
                "range": {
                  "price": {
                    "lte": 3000
                  }
                }
              },
              {
                "geo_distance": {
                  "distance": "100miles",
                  "location": {
                    "lat": 48,
                    "lon": 121
                  }
                }
              }
```

```
            ]
          }
        }
      }
    }
  }
}
```

十億規模的工作

向量搜尋集合支援具有數十億向量的工作負載。您不需要為縮放目的重新索引，因為 auto 縮放可以為您執行此操作。如果您有數百萬個具有大量維度的向量 (或更多)，且需要 200 個以上的 OCU，請連絡 Sup AWS port 部門，以提高您帳戶的最大 OpenSearch 運算單位 (OCU)。

限制

向量搜尋集合有下列限制：

- 向量搜尋集合不支援阿帕奇尼的 ANN 引擎。
- 矢量搜索集合僅支持使用 Faiss 的 HNSW 算法，不支持 IVF 和 IVFQ。
- 向量搜尋集合不支援暖機、統計資料和模型訓練 API 作業。
- 向量搜尋集合不支援內嵌或儲存的指令碼。
- 向量搜尋集合中無法使用索引計數資訊。 AWS Management Console
- 向量搜尋集合上索引的重新整理間隔為 60 秒。

後續步驟

現在您已經知道如何建立向量搜尋集合和索引資料，您可能想要嘗試下列其中一些練習：

- 使用 OpenSearch Python 用戶端來處理向量搜尋集合。請參閱上的此自學課程GitHub。
- 您可以使用 OpenSearch Java 客戶端來處理矢量搜索集合。請參閱上的此自學課程GitHub。
- 設置 LangChain 為用 OpenSearch 作矢量存儲。 LangChain 是一個開放原始碼架構，用於開發採用語言模型的應用程式。如需詳細資訊，請參閱LangChain 文件。

搭配 Amazon OpenSearch 無伺服器使用資料生命週期政策

Amazon OpenSearch 無伺服器時間序列收集的資料生命週期政策決定了該集合中資料的壽命。OpenSearch 無伺服器會在您設定的期間內保留資料。

您可以為您的每個時間序列集合的每個索引設定個別的資料生命週期原則AWS 帳戶。 OpenSearch 無伺服器至少會在您在原則中設定的保留期間內，將文件保留在索引中。然後，它會盡最大努力自動刪除它們，通常在 48 小時或保留期的 10% 內（以較長者為準）。

只有時間序列集合支援資料生命週期原則。搜尋或向量搜尋集合不支援它們。

主題

- 資料生命週期原
- 必要許可
- 政策優先順序
- 政策語法
- 建立資料生命週期原則 (AWS CLI)
- 檢視資料生命週期原
- 更新資料生命週期原
- 刪除資料生命週期原

資料生命週期原

在資料生命週期原則中，您可以指定一系列規則。資料生命週期原則可讓您管理與符合這些規則的索引或集合相關聯的資料保留期間。這些規則會定義索引或索引群組中資料的保留期間。每個規則都包含資源類型 (`index`)、保留期間以及套用保留期間的資源 (索引) 清單。

您可以使用下列其中一種格式來定義保留期間：

- `"MinIndexRetention": "24h"`— OpenSearch 無伺服器會保留指定期間內的索引資料 (以小時或天為單位)。您可以將此期間設定`24h`為從到`3650d`。
- `"NoMinIndexRetention": true`— OpenSearch 無伺服器會無限期保留索引資料。

在下列範例原則中，第一個規則會指定集合中所有索引的保留期為 15 天`marketing`。第二個規則會指定`finance`集合`log`中以開頭的所有索引名稱都沒有設定保留期間，而且會無限期保留。

```
{
   "lifeCyclePolicyDetail": {
      "type": "retention",
      "name": "my-policy",
      "policyVersion": "MTY4ODI0NTM2OTk1N18x",
      "policy": {
         "Rules": [
            {
            "ResourceType":"index",
            "Resource":[
               "index/marketing/*"
            ],
            "MinIndexRetention": "15d"
         },
         {
            "ResourceType":"index",
            "Resource":[
               "index/finance/log*"
            ],
            "NoMinIndexRetention": true
         }
         ]
      },
      "createdDate": 1688245369957,
      "lastModifiedDate": 1688245369957
   }
}
```

在下列範例原則規則中， OpenSearch Serverless 會無限期地保留帳戶內所有集合的所有索引中的資料。

```
{
   "Rules": [
      {
         "ResourceType": "index",
         "Resource": [
            "index/*/*"
         ]
      }
   ],
   "NoMinIndexRetention": true
}
```

必要許可

OpenSearch 無伺服器的生命週期政策使用下列 AWS Identity and Access Management (IAM) 許可。您可以指定 IAM 條件，將使用者限制在與特定集合和索引相關聯的資料生命週期政策。

- `aoss:CreateLifecyclePolicy`— 建立資料生命週期原則。
- `aoss:ListLifecyclePolicies`— 列出目前帳戶中的所有資料生命週期政策。
- `aoss:BatchGetLifecyclePolicy`— 檢視與帳號或策略名稱相關聯的資料生命週期策略。
- `aoss:BatchGetEffectiveLifecyclePolicy`— 檢視指定資源的資料生命週期政策 (`index`是唯一受支援的資源)。
- `aoss:UpdateLifecyclePolicy`— 修改指定的資料生命週期原則，並變更其保留設定或資源。
- `aoss:DeleteLifecyclePolicy`— 刪除資料生命週期原則。

下列身分型存取原則可讓使用者檢視所有資料生命週期策略，並使用資源模式更新策略：`collection/application-logs`

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "aoss:UpdateLifecyclePolicy"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aoss:collection": "application-logs"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "aoss:ListLifecyclePolicies",
                "aoss:BatchGetLifecyclePolicy"
            ],
            "Resource": "*"
        }
    ]
```

```
}
```

政策優先順序

在某些情況下，資料生命週期原則規則可能會在策略內部或跨策略重疊。發生這種情況時，具有更特定資源名稱或索引模式的規則會覆寫具有較一般資源名稱或模式的規則，這兩個規則通用的任何索引。

例如，在下列原則中，索引會套用兩個規則`index/sales/logstash`。在此情況下，第二個規則優先順序，因為`index/sales/log*`是最長的相符項目`index/sales/logstash`。因此， OpenSearch 無伺服器不會設定索引的保留期間。

```
{
      "Rules":[
         {
            "ResourceType":"index",
            "Resource":[
               "index/sales/*",
            ],
            "MinIndexRetention": "15d"
         },
         {
            "ResourceType":"index",
            "Resource":[
               "index/sales/log*",
            ],
            "NoMinIndexRetention": true
         }
      ]
   }
```

政策語法

提供一個或多個規則。這些規則會定義 OpenSearch 無伺服器索引的資料生命週期設定。

每個規則都包含下列元素。您可以`NoMinIndexRetention`在每個規則中提供`MinIndexRetention`或，但不能同時提供兩者。

Element	描述
Resource Type (資源類型)	該規則適用的資源類型。資料生命週期原則唯一支援的選項是`index`。

Element	描述
Resource	資源名稱和/或模式的清單。模式由前綴和萬用字元 (*) 組成，可讓相關聯的權限套用至多個資源。例如：index/*<collection-name|pattern>* /*<index-name|pattern>* 。
MinIndexRetention	在索引中保留文件的最短期間 (以天 (dh) 或小時 () 為單位。下界是24h，上限是3650d。
NoMinIndexRetention	如果true， OpenSearch 無伺服器會無限期保留文件。

下列是一些範例：

```
{
  "Rules": [
    {
      "ResourceType": "index",
      "Resource": [
        "index/autoparts-inventory/*"
      ],
      "MinIndexRetention": "20d"
    },
    {
      "ResourceType": "index",
      "Resource": [
        "index/auto*/gear"
      ],
      "MinIndexRetention": "24h"
    },
    {
      "ResourceType": "index",
      "Resource": [
        "index/autoparts-inventory/tires"
      ],
      "NoMinIndexRetention": true
    }
  ]
}
```

建立資料生命週期原則 (AWS CLI)

若要使用 OpenSearch 無伺服器 API 作業建立資料生命週期原則，請使用指CreateLifecyclePolicy令。此命令接受內嵌政策和 .json 檔案。內嵌政策必須編碼為 JSON 逸出字串。

下列要求會建立資料生命週期原則：

```
aws opensearchserverless create-lifecycle-policy \
    --name my-policy \
    --type retention \
    --policy "{\"Rules\":[{\"ResourceType\":\"index\",\"Resource\":[\"index/autoparts-
inventory/*\"],\"MinIndexRetention\": \"81d\"},{\"ResourceType\":\"index\",\"Resource
\":[\"index/sales/orders*\"],\"NoMinIndexRetention\":true}]}"
```

若要在 JSON 檔案中提供政策，請使用 `--policy file://my-policy.json` 格式

檢視資料生命週期原

在建立集合之前，您可能想要預覽帳戶中現有的資料生命週期政策，以查看哪個資源模式具有符合您集合名稱的資源模式。以下ListLifecyclePolicies請求列出您帳戶中的所有資料生命週期政策：

```
aws opensearchserverless list-lifecycle-policies --type retention
```

請求會傳回所有已設定資料生命週期原則的相關資訊 若要檢視在一個特定策略中定義的特徵碼規則，請在回應中的`lifecyclePolicySummaries`元素內容中尋找原則資訊。請注意此原則`type`的`name`和，並在BatchGetLifecyclePolicy要求中使用這些屬性，以接收含下列原則詳細資訊的回應：

```
{
    "lifecyclePolicySummaries": [
        {
            "type": "retention",
            "name": "my-policy",
            "policyVersion": "MTY2MzY5MTY1MDA3Ml8x",
            "createdDate": 1663691650072,
            "lastModifiedDate": 1663691650072
        }
    ]
}
```

若要將結果限制為包含特定集合或索引的策略，您可以包含資源篩選器：

```
aws opensearchserverless list-lifecycle-policies --type retention --resources
 "index/autoparts-inventory/*"
```

若要檢視有關特定原則的詳細資訊，請使用BatchGetLifecyclePolicy命令。

更新資料生命週期原

當您修改資料生命週期原則時，所有關聯的集合都會受到影響。若要在 OpenSearch 無伺服器主控台中更新資料生命週期原則，請展開資料生命週期原則，選取要修改的原則，然後選擇編輯。進行變更，然後選擇 Save (儲存)。

若要使用 OpenSearch 無伺服器 API 更新資料生命週期原則，請使用指UpdateLifecyclePolicy令。您必須在請求中包含政策版本。您可以使用 `ListLifecyclePolicies` 或 `BatchGetLifecyclePolicy` 命令擷取政策版本。將最新的政策版本納入其中，可確保您不會意外覆寫其他人所做的變更。

下列要求會使用新的原則 JSON 文件來更新資料生命週期原則：

```
aws opensearchserverless update-lifecycle-policy \
    --name my-policy \
    --type retention \
    --policy-version MTY2MzY5MTY1MDA3Ml8x \
    --policy file://my-new-policy.json
```

在您更新原則與強制執行新保留期間之間，可能會有幾分鐘的延遲時間。

刪除資料生命週期原

當您刪除資料生命週期原則時，它不會再套用至任何相符的索引。若要刪除 OpenSearch 無伺服器主控台中的原則，請選取該原則，然後選擇刪除。

您也可以使用以下DeleteLifecyclePolicy命令：

```
aws opensearchserverless delete-lifecycle-policy --name my-policy --type retention
```

使用開AWS發套件與 Amazon OpenSearch 無伺服器互動

本節包含如何使用AWS開發套件與 Amazon OpenSearch 無伺服器互動的範例。這些程式碼範例顯示如何建立安全政策和集合，以及如何查詢集合。

> **Note**
>
> 我們目前正在建置這些程式碼範例。如果你想提供一個代碼示例（Java，Go 等），請直接在GitHub存儲庫中打開一個提取請求。

主題

- Python
- JavaScript

Python

下列範例指令碼會使用 Python 的 AWS SDK for Python (Boto3) 以及 opensearch-py 用戶端，來建立加密、網路和資料存取政策、建立相符的集合，以及為某些範例資料編製索引。

若要安裝所需的相依性，請執行下列命令：

```
pip install opensearch-py
pip install boto3
pip install botocore
pip install requests-aws4auth
```

在指令碼中，將 `Principal` 元素取代為簽署請求的使用者或角色的 Amazon Resource Name (ARN)。您也可以選擇性地修改 `region`。

```
from opensearchpy import OpenSearch, RequestsHttpConnection
from requests_aws4auth import AWS4Auth
import boto3
import botocore
import time

# Build the client using the default credential configuration.
# You can use the CLI and run 'aws configure' to set access key, secret
# key, and default region.

client = boto3.client('opensearchserverless')
service = 'aoss'
region = 'us-east-1'
credentials = boto3.Session().get_credentials()
awsauth = AWS4Auth(credentials.access_key, credentials.secret_key,
```

```
                    region, service, session_token=credentials.token)


def createEncryptionPolicy(client):
    """Creates an encryption policy that matches all collections beginning with tv-"""
    try:
        response = client.create_security_policy(
            description='Encryption policy for TV collections',
            name='tv-policy',
            policy="""
                {
                    \"Rules\":[
                        {
                            \"ResourceType\":\"collection\",
                            \"Resource\":[
                                \"collection\/tv-*\"
                            ]
                        }
                    ],
                    \"AWSOwnedKey\":true
                }
                """,
            type='encryption'
        )
        print('\nEncryption policy created:')
        print(response)
    except botocore.exceptions.ClientError as error:
        if error.response['Error']['Code'] == 'ConflictException':
            print(
                '[ConflictException] The policy name or rules conflict with an existing
 policy.')
        else:
            raise error


def createNetworkPolicy(client):
    """Creates a network policy that matches all collections beginning with tv-"""
    try:
        response = client.create_security_policy(
            description='Network policy for TV collections',
            name='tv-policy',
            policy="""
                [{
                    \"Description\":\"Public access for TV collection\",
```

```
                    \"Rules\":[
                        {
                            \"ResourceType\":\"dashboard\",
                            \"Resource\":[\"collection\/tv-*\"]
                        },
                        {
                            \"ResourceType\":\"collection\",
                            \"Resource\":[\"collection\/tv-*\"]
                        }
                    ],
                    \"AllowFromPublic\":true
                }]
                """,
            type='network'
        )
        print('\nNetwork policy created:')
        print(response)
    except botocore.exceptions.ClientError as error:
        if error.response['Error']['Code'] == 'ConflictException':
            print(
                '[ConflictException] A network policy with this name already exists.')
        else:
            raise error


def createAccessPolicy(client):
    """Creates a data access policy that matches all collections beginning with tv-"""
    try:
        response = client.create_access_policy(
            description='Data access policy for TV collections',
            name='tv-policy',
            policy="""
                [{
                    \"Rules\":[
                        {
                            \"Resource\":[
                                \"index\/tv-*\/*\"
                            ],
                            \"Permission\":[
                                \"aoss:CreateIndex\",
                                \"aoss:DeleteIndex\",
                                \"aoss:UpdateIndex\",
                                \"aoss:DescribeIndex\",
                                \"aoss:ReadDocument\",
```

```
                                \"aoss:WriteDocument\"
                            ],
                            \"ResourceType\": \"index\"
                        },
                        {
                            \"Resource\":[
                                \"collection\/tv-*\"
                            ],
                            \"Permission\":[
                                \"aoss:CreateCollectionItems\"
                            ],
                            \"ResourceType\": \"collection\"
                        }
                    ],
                    \"Principal\":[
                        \"arn:aws:iam::123456789012:role\/Admin\"
                    ]
                }]
                """,
            type='data'
        )
        print('\nAccess policy created:')
        print(response)
    except botocore.exceptions.ClientError as error:
        if error.response['Error']['Code'] == 'ConflictException':
            print(
                '[ConflictException] An access policy with this name already exists.')
        else:
            raise error


def createCollection(client):
    """Creates a collection"""
    try:
        response = client.create_collection(
            name='tv-sitcoms',
            type='SEARCH'
        )
        return(response)
    except botocore.exceptions.ClientError as error:
        if error.response['Error']['Code'] == 'ConflictException':
            print(
                '[ConflictException] A collection with this name already exists. Try
 another name.')
```

```
        else:
            raise error


def waitForCollectionCreation(client):
    """Waits for the collection to become active"""
    response = client.batch_get_collection(
        names=['tv-sitcoms'])
    # Periodically check collection status
    while (response['collectionDetails'][0]['status']) == 'CREATING':
        print('Creating collection...')
        time.sleep(30)
        response = client.batch_get_collection(
            names=['tv-sitcoms'])
    print('\nCollection successfully created:')
    print(response["collectionDetails"])
    # Extract the collection endpoint from the response
    host = (response['collectionDetails'][0]['collectionEndpoint'])
    final_host = host.replace("https://", "")
    indexData(final_host)


def indexData(host):
    """Create an index and add some sample data"""
    # Build the OpenSearch client
    client = OpenSearch(
        hosts=[{'host': host, 'port': 443}],
        http_auth=awsauth,
        use_ssl=True,
        verify_certs=True,
        connection_class=RequestsHttpConnection,
        timeout=300
    )
    # It can take up to a minute for data access rules to be enforced
    time.sleep(45)

    # Create index
    response = client.indices.create('sitcoms-eighties')
    print('\nCreating index:')
    print(response)

    # Add a document to the index.
    response = client.index(
        index='sitcoms-eighties',
```

```
        body={
            'title': 'Seinfeld',
            'creator': 'Larry David',
            'year': 1989
        },
        id='1',
    )
    print('\nDocument added:')
    print(response)


def main():
    createEncryptionPolicy(client)
    createNetworkPolicy(client)
    createAccessPolicy(client)
    createCollection(client)
    waitForCollectionCreation(client)


if __name__ == "__main__":
    main()
```

JavaScript

下列範例指令碼使用 Node.js JavaScript 中的 SDK，以及用於的 opensearch-js 用戶端來建立加密 JavaScript、網路和資料存取原則、建立相符的集合、建立索引，以及為某些範例資料建立索引。

若要安裝所需的相依性，請執行下列命令：

```
npm i aws-sdk
npm i aws4
npm i @opensearch-project/opensearch
```

在指令碼中，將 `Principal` 元素取代為簽署請求的使用者或角色的 Amazon Resource Name (ARN)。您也可以選擇性地修改 `region`。

```
var AWS = require('aws-sdk');
var aws4 = require('aws4');
var {
    Client,
    Connection
} = require("@opensearch-project/opensearch");
var {
```

```
    OpenSearchServerlessClient,
    CreateSecurityPolicyCommand,
    CreateAccessPolicyCommand,
    CreateCollectionCommand,
    BatchGetCollectionCommand
} = require("@aws-sdk/client-opensearchserverless");
var client = new OpenSearchServerlessClient();

async function execute() {
    await createEncryptionPolicy(client)
    await createNetworkPolicy(client)
    await createAccessPolicy(client)
    await createCollection(client)
    await waitForCollectionCreation(client)
}

async function createEncryptionPolicy(client) {
    // Creates an encryption policy that matches all collections beginning with 'tv-'
    try {
        var command = new CreateSecurityPolicyCommand({
            description: 'Encryption policy for TV collections',
            name: 'tv-policy',
            type: 'encryption',
            policy: " \
        { \
            \"Rules\":[ \
                { \
                    \"ResourceType\":\"collection\", \
                    \"Resource\":[ \
                        \"collection\/tv-*\" \
                    ] \
                } \
            ], \
            \"AWSOwnedKey\":true \
        }"
        });
        const response = await client.send(command);
        console.log("Encryption policy created:");
        console.log(response['securityPolicyDetail']);
    } catch (error) {
        if (error.name === 'ConflictException') {
            console.log('[ConflictException] The policy name or rules conflict with an
 existing policy.');
        } else
```

```
            console.error(error);
    };
}

async function createNetworkPolicy(client) {
    // Creates a network policy that matches all collections beginning with 'tv-'
    try {
        var command = new CreateSecurityPolicyCommand({
            description: 'Network policy for TV collections',
            name: 'tv-policy',
            type: 'network',
            policy: " \
            [{ \
                \"Description\":\"Public access for television collection\", \
                \"Rules\":[ \
                    { \
                        \"ResourceType\":\"dashboard\", \
                        \"Resource\":[\"collection\/tv-*\"] \
                    }, \
                    { \
                        \"ResourceType\":\"collection\", \
                        \"Resource\":[\"collection\/tv-*\"] \
                    } \
                ], \
                \"AllowFromPublic\":true \
            }]"
        });
        const response = await client.send(command);
        console.log("Network policy created:");
        console.log(response['securityPolicyDetail']);
    } catch (error) {
        if (error.name === 'ConflictException') {
            console.log('[ConflictException] A network policy with that name already
 exists.');
        } else
            console.error(error);
    };
}

async function createAccessPolicy(client) {
    // Creates a data access policy that matches all collections beginning with 'tv-'
    try {
        var command = new CreateAccessPolicyCommand({
            description: 'Data access policy for TV collections',
```

```
            name: 'tv-policy',
            type: 'data',
            policy: " \
            [{ \
                \"Rules\":[ \
                    { \
                        \"Resource\":[ \
                            \"index\/tv-*\/*\" \
                        ], \
                        \"Permission\":[ \
                            \"aoss:CreateIndex\", \
                            \"aoss:DeleteIndex\", \
                            \"aoss:UpdateIndex\", \
                            \"aoss:DescribeIndex\", \
                            \"aoss:ReadDocument\", \
                            \"aoss:WriteDocument\" \
                        ], \
                        \"ResourceType\": \"index\" \
                    }, \
                    { \
                        \"Resource\":[ \
                            \"collection\/tv-*\" \
                        ], \
                        \"Permission\":[ \
                            \"aoss:CreateCollectionItems\" \
                        ], \
                        \"ResourceType\": \"collection\" \
                    } \
                ], \
                \"Principal\":[ \
                    \"arn:aws:iam::123456789012:role\/Admin\" \
                ] \
            }]"
        });
        const response = await client.send(command);
        console.log("Access policy created:");
        console.log(response['accessPolicyDetail']);
    } catch (error) {
        if (error.name === 'ConflictException') {
            console.log('[ConflictException] An access policy with that name already
exists.');
        } else
            console.error(error);
    };
```

```
}

async function createCollection(client) {
    // Creates a collection to hold TV sitcoms indexes
    try {
        var command = new CreateCollectionCommand({
            name: 'tv-sitcoms',
            type: 'SEARCH'
        });
        const response = await client.send(command);
        return (response)
    } catch (error) {
        if (error.name === 'ConflictException') {
            console.log('[ConflictException] A collection with this name already
 exists. Try another name.');
        } else
            console.error(error);
    };
}

async function waitForCollectionCreation(client) {
    // Waits for the collection to become active
    try {
        var command = new BatchGetCollectionCommand({
            names: ['tv-sitcoms']
        });
        var response = await client.send(command);
        while (response.collectionDetails[0]['status'] == 'CREATING') {
            console.log('Creating collection...')
            await sleep(30000) // Wait for 30 seconds, then check the status again
            function sleep(ms) {
                return new Promise((resolve) => {
                    setTimeout(resolve, ms);
                });
            }
            var response = await client.send(command);
        }
        console.log('Collection successfully created:');
        console.log(response['collectionDetails']);
        // Extract the collection endpoint from the response
        var host = (response.collectionDetails[0]['collectionEndpoint'])
        // Pass collection endpoint to index document request
        indexDocument(host)
    } catch (error) {
```

```
        console.error(error);
    };
}

async function indexDocument(host) {

    var client = new Client({
        node: host,
        Connection: class extends Connection {
            buildRequestObject(params) {
                var request = super.buildRequestObject(params)
                request.service = 'aoss';
                request.region = 'us-east-1'; // e.g. us-east-1
                var body = request.body;
                request.body = undefined;
                delete request.headers['content-length'];
                request.headers['x-amz-content-sha256'] = 'UNSIGNED-PAYLOAD';
                request = aws4.sign(request, AWS.config.credentials);
                request.body = body;

                return request
            }
        }
    });

    // Create an index
    try {
        var index_name = "sitcoms-eighties";

        var response = await client.indices.create({
            index: index_name
        });

        console.log("Creating index:");
        console.log(response.body);

        // Add a document to the index
        var document = "{ \"title\": \"Seinfeld\", \"creator\": \"Larry David\", \"year
\": \"1989\" }\n";

        var response = await client.index({
            index: index_name,
            body: document
        });
```

```
        console.log("Adding document:");
        console.log(response.body);
    } catch (error) {
        console.error(error);
    };
}

execute()
```

使用建AWS CloudFormation立亞馬遜OpenSearch無伺服器集合

您可以用AWS CloudFormation來建立 Amazon OpenSearch 無伺服器資源，例如集合、安全政策和 VPC 端點。如需完整的OpenSearch無伺服器CloudFormation參考資料，請參閱AWS CloudFormation 使用者指南中的 Amazon OpenSearch 無伺服器。

下列範例CloudFormation範本會建立簡單的資料存取原則、網路原則和安全性原則，以及相符的集合。這是使用 Amazon OpenSearch 無伺服器快速啟動和執行，以及佈建必要元素以建立和使用集合的好方法。

> **Important**
>
> 此範例使用公有網路存取，不建議用於生產工作負載。我們建議您使用 VPC 存取權來保護您的集合。如需詳細資訊，請參閱 AWS::OpenSearchServerless::VpcEndpoint 和 the section called “VPC 端點”。

```
AWSTemplateFormatVersion: 2010-09-09
Description: 'Amazon OpenSearch Serverless template to create an IAM user, encryption
 policy, data access policy and collection'
Resources:
  IAMUSer:
    Type: 'AWS::IAM::User'
    Properties:
      UserName:  aossadmin
  DataAccessPolicy:
    Type: 'AWS::OpenSearchServerless::AccessPolicy'
    Properties:
      Name: quickstart-access-policy
      Type: data
      Description: Access policy for quickstart collection
```

```
      Policy: !Sub >-
        [{"Description":"Access for cfn user","Rules":
[{"ResourceType":"index","Resource":["index/*/*"],"Permission":["aoss:*"]},
        {"ResourceType":"collection","Resource":["collection/quickstart"],"Permission":
["aoss:*"]}],
        "Principal":["arn:aws:iam::${AWS::AccountId}:user/aossadmin"]}]
  NetworkPolicy:
    Type: 'AWS::OpenSearchServerless::SecurityPolicy'
    Properties:
      Name: quickstart-network-policy
      Type: network
      Description: Network policy for quickstart collection
      Policy: >-
        [{"Rules":[{"ResourceType":"collection","Resource":["collection/
quickstart"]}, {"ResourceType":"dashboard","Resource":["collection/
quickstart"]}],"AllowFromPublic":true}]
  EncryptionPolicy:
    Type: 'AWS::OpenSearchServerless::SecurityPolicy'
    Properties:
      Name: quickstart-security-policy
      Type: encryption
      Description: Encryption policy for quickstart collection
      Policy: >-
        {"Rules":[{"ResourceType":"collection","Resource":["collection/
quickstart"]}],"AWSOwnedKey":true}
  Collection:
    Type: 'AWS::OpenSearchServerless::Collection'
    Properties:
      Name: quickstart
      Type: TIMESERIES
      Description: Collection to holds timeseries data
    DependsOn: EncryptionPolicy
Outputs:
  IAMUser:
    Value: !Ref IAMUSer
  DashboardURL:
    Value: !GetAtt Collection.DashboardEndpoint
  CollectionARN:
    Value: !GetAtt Collection.Arn
```

管理 Amazon OpenSearch 無伺服器的容量限制

使用 Amazon OpenSearch 無伺服器，您不必自行管理容量。 OpenSearch 無伺服器會根據目前的工作負載，為您的帳戶自動調整運算容量。無伺服器運算容量是以OpenSearch 運算單位 (OCUs) 來衡量。每個都OCU是 6 GiB 記憶體和對應虛擬 CPU (vCPU) 的組合，以及將資料傳輸到 Amazon S3 的組合。如需有關 OpenSearch 無伺服器中解耦架構的詳細資訊，請參閱。the section called “運作方式”

當您建立第一個集合時， OpenSearch 無伺服器會實體化四個 OCUs (兩個用於索引，兩個用於搜尋)。這些OCUs永遠存在，即使沒有索引或搜尋活動也是如此。所有後續集合都可以共享這些 OCUs（除了具有唯一 AWS KMS 鍵的集合，它們實例化了自己的四個集合OCUs）。如有需要，OpenSearch 無伺服器會隨著索引和搜尋使用量的增加OCUs而自動擴充，並新增額外資訊。當收集端點上的流量減少時，容量會縮減至資料大小OCUs所需的最小數量。最多，它將縮小到 1 OCU [0.5 OCU x 2] 進行索引，1 OCU [0.5 OCU x 2] 進行搜索。

對於搜索和向量搜索集合，所有數據都存儲在熱索引上，以確保快速查詢響應時間。時間序列集合使用熱儲存和暖儲存的組合，將最新的資料保留在熱儲存中，以最佳化更頻繁存取資料的查詢回應時間。如需詳細資訊，請參閱the section called “選擇集合類型”。

> **Note**
>
> 向量搜尋集合無法OCUs與搜尋和時間序列集合共用，即使向量搜尋集合使用與搜尋或時間序列集合相同的索KMS引鍵。OCUs將為您的第一個向量集合創建一組新的。向OCUs量集合在相同的KMS索引鍵集合之間共用。

若要管理集合的容量並控制成本，您可以指定目前帳戶和區域的整體最大索引和搜尋容量，而且 OpenSearch Serverless 會根據這些規格自動擴充您的收集資源。

索引編製和搜尋容量會分別調整，因此您可以針對每個容量指定帳戶層級限制：

- 最大索引容量 — OpenSearch 無伺服器可將索引容量增加到這個數OCUs目。
- 最大搜尋容量 — OpenSearch 無伺服器可將搜尋容量增加到這個數OCUs目。

> **Note**
>
> 目前，容量設定僅適用於帳戶層級。您無法設定每個集合的容量限制。

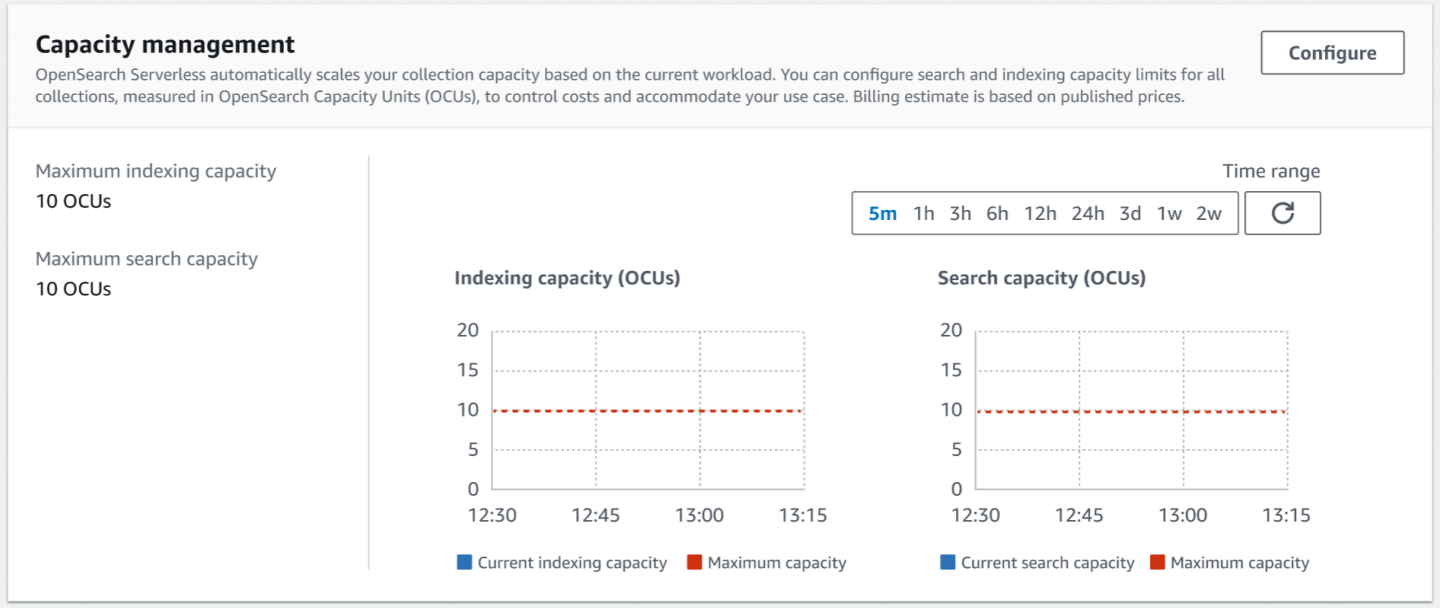
您的目標應該是確保容量上限足以處理尖峰工作負載。根據您的設定， OpenSearch Serverless 會自動擴充集OCUs合的數量，以處理索引和搜尋工作負載。

主題

- 進行容量設定
- 容量限制上限
- 監控容量用量

進行容量設定

若要在 OpenSearch 無伺服器主控台中設定容量設定，請展開左側導覽窗格中的無伺服器，然後選取 [儀表板]。在 Capacity management (容量管理) 下指定索引編製和搜尋容量上限：



若要使用設定容量 AWS CLI，請傳送UpdateAccountSettings要求：

```
aws opensearchserverless update-account-settings \
    --capacity-limits '{ "maxIndexingCapacityInOCU": 8,"maxSearchCapacityInOCU": 9 }'
```

容量限制上限

對於所有三種類型的集合，索引的預設最大容量OCUs為 10，搜尋的預設容量上限OCUs為 10。帳戶的最小允許容量為 1 OCU [0.5 OCU x 2] 進行索引，搜索為 1 OCU [0.5 OCU x 2]。對於所有集合，允許的最大容量是 500 OCUs 索引和 500 OCUs 用於搜索。您可以將OCU計數設定為從 1 到允許容量上限的任何數字，以 2 的倍數為單位。

每個都OCU包含足夠的熱暫時儲存，可容納 120 GiB 的索引資料。 OpenSearch 無伺服器在搜尋和向量搜尋集合中，每個索引最多支援 1 TiB 的資料，在時間序列集合中，每個索引最多支援 10 TiB 的熱資料。對於時間序列集合，您仍然可以內嵌更多資料，這些資料可以作為暖資料存放在 S3 中。

如需所有配額的清單，請參閱OpenSearch 無伺服器配額。

監控容量用量

您可以監控`SearchOCU`和`IndexingOCU`帳戶級 CloudWatch 指標，以了解商品系列的擴展方式。建議您設定警示，以在帳戶接近與容量相關的指標閾值時通知您，如此您就可相應調整容量設定。

您也可使用這些指標，判斷容量上限設定是否合適，或者是否需要進行調整。分析這些指標，以將精力集中於集合效率的優化。如需 OpenSearch 無伺服器傳送指標的詳細資訊 CloudWatch，請參閱the section called “監控 OpenSearch 無伺服器”。

將資料導入 Amazon OpenSearch 無伺服器集合

這些章節提供有關支援的擷取管道以將資料擷取至 Amazon OpenSearch 無伺服器集合的詳細資訊。它們還涵蓋了一些您可以用來與 OpenSearch API操作進行交互的客戶端。您的用戶端應與 OpenSearch 2.x 相容，才能與 OpenSearch 無伺服器整合。

主題

- 所需的最低許可
- OpenSearch 攝入
- Fluent Bit
- Amazon 數據 Firehose
- Go
- Java
- JavaScript
- Logstash
- Python
- Ruby
- 與其他用戶端簽署HTTP要求

所需的最低許可

若要將資料內嵌至 OpenSearch 無伺服器集合，寫入資料的主體必須具有在資料存取原則中指派下列最低權限：

```
[
   {
      "Rules":[
         {
            "ResourceType":"index",
            "Resource":[
               "index/target-collection/logs"
            ],
            "Permission":[
               "aoss:CreateIndex",
               "aoss:WriteDocument",
               "aoss:UpdateIndex"
            ]
         }
      ],
      "Principal":[
         "arn:aws:iam::123456789012:user/my-user"
      ]
   }
]
```

如果您計劃寫入到其他索引，許可的範圍可能會更廣泛。例如，您可以允許所有索引（index/）的權限，而不是指定單個目標索引*target-collection*/*），或索引的子集（索引/*target-collection*/*logs**).

如需所有可用 OpenSearch API作業及其相關權限的參考，請參閱the section called “支援的操作和外掛程式”。

OpenSearch 攝入

您可以使用 Amazon OpenSearch 擷取，而不是使用第三方用戶端將資料直接傳送到 OpenSearch 無伺服器集合。您可以將資料生產者設定為將資料傳送至 OpenSearch 擷取，它會自動將資料傳送至您指定的集合。您也可以將 OpenSearch 擷取設定為在傳送資料之前轉換資料。如需詳細資訊，請參閱Amazon OpenSearch 攝入。

OpenSearch 擷取管線需要權限，才能寫入設定為其接收器的 OpenSearch 無伺服器集合。這些權限包括描述集合並向其傳送HTTP要求的功能。如需使用 OpenSearch 擷取將資料新增至集合的指示，請參閱the section called “授予管道對集合的存取權”。

若要開始使用 OpenSearch 擷取，請參閱the section called “教學課程：將資料擷取至集合”。

Fluent Bit

您可以使用 AWS 用於 Fluent Bit 圖像和OpenSearch 輸出插件，以將數據導入 OpenSearch 無服務器集合。

> **Note**
> 您必須擁有版本 2.30.0 或更新的版本 AWS 用於流利位元影像，以便與 OpenSearch 無伺服器整合。

範例組態：

組態檔的這個範例輸出區段顯示如何使用 OpenSearch 無伺服器集合作為目的地。重要的補充是 `AWS_Service_Name` 參數，也就是 `aoss`。`Host` 是集合端點。

```
[OUTPUT]
    Name  opensearch
    Match *
    Host  collection-endpoint.us-west-2.aoss.amazonaws.com
    Port  443
    Index  my_index
    Trace_Error On
    Trace_Output On
    AWS_Auth On
    AWS_Region <region>
    AWS_Service_Name aoss
    tls     On
    Suppress_Type_Name On
```

Amazon 數據 Firehose

Firehose 支援 OpenSearch 無伺服器作為傳送目的地。如需將資料傳送至 OpenSearch 無伺服器的指示，請參閱 Amazon Data Firehose 開發人員指南中的建立 Kinesis Data Firehose 交付串流和為您的目的地選擇 OpenSearch 無伺服器。

您提供給 Firehose 要傳送的IAM角色必須在具有目標集合的`aoss:WriteDocument`最低權限的資料存取原則中指定，而且您必須擁有可將資料傳送至其中的已存在索引。如需詳細資訊，請參閱the section called “所需的最低許可”。

在將資料傳送至 OpenSearch 無伺服器之前，您可能需要對資料執行轉換。如需進一步了解如何使用 Lambda 函數來執行此任務，請參閱相同指南中的 Amazon Kinesis Data Firehose 資料轉換。

Go

下列範例程式碼會使用 Go 的 opensearch-go 用戶端，建立與指定的 OpenSearch 無伺服器集合的安全連線，並建立單一索引。您必須提供 `region` 和 `host` 的值。

```
package main

import (
  "context"
  "log"
  "strings"
  "github.com/aws/aws-sdk-go-v2/aws"
  "github.com/aws/aws-sdk-go-v2/config"
  opensearch "github.com/opensearch-project/opensearch-go/v2"
  opensearchapi "github.com/opensearch-project/opensearch-go/v2/opensearchapi"
  requestsigner "github.com/opensearch-project/opensearch-go/v2/signer/awsv2"
)

const endpoint = "" // serverless collection endpoint

func main() {
 ctx := context.Background()

 awsCfg, err := config.LoadDefaultConfig(ctx,
  config.WithRegion("<AWS_REGION>"),
  config.WithCredentialsProvider(
   getCredentialProvider("<AWS_ACCESS_KEY>", "<AWS_SECRET_ACCESS_KEY>",
 "<AWS_SESSION_TOKEN>"),
  ),
 )
 if err != nil {
  log.Fatal(err) // don't log.fatal in a production-ready app
 }

 // create an AWS request Signer and load AWS configuration using default config folder
 or env vars.
```

```
signer, err := requestsigner.NewSignerWithService(awsCfg, "aoss") // "aoss" for Amazon
OpenSearch Serverless
if err != nil {
 log.Fatal(err) // don't log.fatal in a production-ready app
}

// create an opensearch client and use the request-signer
client, err := opensearch.NewClient(opensearch.Config{
 Addresses: []string{endpoint},
 Signer:    signer,
})
if err != nil {
 log.Fatal("client creation err", err)
}

indexName := "go-test-index"

 // define index mapping
mapping := strings.NewReader(`{
 "settings": {
   "index": {
        "number_of_shards": 4
        }
      }
 }`)

// create an index
createIndex := opensearchapi.IndicesCreateRequest{
 Index: indexName,
   Body: mapping,
}
createIndexResponse, err := createIndex.Do(context.Background(), client)
if err != nil {
 log.Println("Error ", err.Error())
 log.Println("failed to create index ", err)
 log.Fatal("create response body read err", err)
}
log.Println(createIndexResponse)

// delete the index
deleteIndex := opensearchapi.IndicesDeleteRequest{
 Index: []string{indexName},
}
```

```
 deleteIndexResponse, err := deleteIndex.Do(context.Background(), client)
 if err != nil {
  log.Println("failed to delete index ", err)
  log.Fatal("delete index response body read err", err)
 }
 log.Println("deleting index", deleteIndexResponse)
}

func getCredentialProvider(accessKey, secretAccessKey, token string)
 aws.CredentialsProviderFunc {
 return func(ctx context.Context) (aws.Credentials, error) {
  c := &aws.Credentials{
   AccessKeyID:     accessKey,
   SecretAccessKey: secretAccessKey,
   SessionToken:    token,
  }
  return *c, nil
 }
}
```

Java

下列範例程式碼會使用 Java 的 opensearch-java 用戶端，建立與指定的 OpenSearch 無伺服器集合的安全連線，並建立單一索引。您必須提供 `region` 和 `host` 的值。

與 OpenSearch 服務域相比，重要的區別在於服務名稱（`aoss`而不是`es`）。

```
// import OpenSearchClient to establish connection to OpenSearch Serverless collection
import org.opensearch.client.opensearch.OpenSearchClient;

SdkHttpClient httpClient = ApacheHttpClient.builder().build();
// create an opensearch client and use the request-signer
OpenSearchClient client = new OpenSearchClient(
    new AwsSdk2Transport(
        httpClient,
        "...us-west-2.aoss.amazonaws.com", // serverless collection endpoint
        "aoss" // signing service name
        Region.US_WEST_2, // signing service region
        AwsSdk2TransportOptions.builder().build()
    )
);

String index = "sample-index";
```

```
// create an index
CreateIndexRequest createIndexRequest = new
 CreateIndexRequest.Builder().index(index).build();
CreateIndexResponse createIndexResponse = client.indices().create(createIndexRequest);
System.out.println("Create index reponse: " + createIndexResponse);

// delete the index
DeleteIndexRequest deleteIndexRequest = new
 DeleteIndexRequest.Builder().index(index).build();
DeleteIndexResponse deleteIndexResponse = client.indices().delete(deleteIndexRequest);
System.out.println("Delete index reponse: " + deleteIndexResponse);

httpClient.close();
```

下列範例程式碼會再次建立安全連線，然後搜尋索引。

```
import org.opensearch.client.opensearch.OpenSearchClient;
>>>>>>> aoss-slr-update

SdkHttpClient httpClient = ApacheHttpClient.builder().build();

OpenSearchClient client = new OpenSearchClient(
    new AwsSdk2Transport(
        httpClient,
        "...us-west-2.aoss.amazonaws.com", // serverless collection endpoint
        "aoss" // signing service name
        Region.US_WEST_2, // signing service region
        AwsSdk2TransportOptions.builder().build()
    )
);

Response response = client.generic()
    .execute(
        Requests.builder()
            .endpoint("/" + "users" + "/_search?typed_keys=true")
            .method("GET")
            .json("{"
                + "    \"query\": {"
                + "        \"match_all\": {}"
                + "    }"
                + "}")
            .build());
```

```
httpClient.close();
```

JavaScript

下列範例程式碼會使用 opensearch-js 用戶端 JavaScript 來建立與指定的 OpenSearch 無伺服器集合的安全連線、建立單一索引、新增文件，以及刪除索引。您必須提供 `node` 和 `region` 的值。

與 OpenSearch 服務域相比，重要的區別在於服務名稱（`aoss`而不是`es`）。

Version 3

這個範例 JavaScript 在 Node.js 中使用的版本 3。SDK

```
const { defaultProvider } = require('@aws-sdk/credential-provider-node');
const { Client } = require('@opensearch-project/opensearch');
const { AwsSigv4Signer } = require('@opensearch-project/opensearch/aws');

async function main() {
    // create an opensearch client and use the request-signer
    const client = new Client({
        ...AwsSigv4Signer({
            region: 'us-west-2',
            service: 'aoss',
            getCredentials: () => {
                const credentialsProvider = defaultProvider();
                return credentialsProvider();
            },
        }),
        node: '' # // serverless collection endpoint
    });

    const index = 'movies';

    // create index if it doesn't already exist
    if (!(await client.indices.exists({ index })).body) {
        console.log((await client.indices.create({ index })).body);
    }

    // add a document to the index
    const document = { foo: 'bar' };
    const response = await client.index({
        id: '1',
```

```
        index: index,
        body: document,
    });
    console.log(response.body);

    // delete the index
    console.log((await client.indices.delete({ index })).body);
}

main();
```

Version 2

這個範例 JavaScript 在 Node.js 中使用的版本 2。SDK

```
const AWS = require('aws-sdk');
const { Client } = require('@opensearch-project/opensearch');
const { AwsSigv4Signer } = require('@opensearch-project/opensearch/aws');

async function main() {
    // create an opensearch client and use the request-signer
    const client = new Client({
        ...AwsSigv4Signer({
            region: 'us-west-2',
            service: 'aoss',
            getCredentials: () =>
                new Promise((resolve, reject) => {
                    AWS.config.getCredentials((err, credentials) => {
                        if (err) {
                            reject(err);
                        } else {
                            resolve(credentials);
                        }
                    });
                }),
        }),
        node: '' # // serverless collection endpoint
    });

    const index = 'movies';

    // create index if it doesn't already exist
    if (!(await client.indices.exists({ index })).body) {
        console.log((await client.indices.create({
```

```
            index
        })).body);
    }

    // add a document to the index
    const document = {
        foo: 'bar'
    };
    const response = await client.index({
        id: '1',
        index: index,
        body: document,
    });
    console.log(response.body);

    // delete the index
    console.log((await client.indices.delete({ index })).body);
}

main();
```

Logstash

您可以使用 Logstash OpenSearch 外掛程式將記錄發佈至 OpenSearch 無伺服器集合。

若要使用 Logstash 將資料傳送至無伺服器 OpenSearch

1. 使用泊塢視窗或 Linux 安裝logstash-output-opensearch外掛程式 2.0.0 版或更新版本。

   Docker

   碼頭窗承載預先安裝輸出插件的 Logstash OSS 軟件：開放搜索項目/- OpenSearch 輸出插件。logstash-oss-with-opensearch您可以像任何其他映像一樣提取映像：

   ```
   docker pull opensearchproject/logstash-oss-with-opensearch-output-plugin:latest
   ```

   Linux

   首先，如果您尚未安裝最新版本的 Logstash，請先安裝。然後，安裝輸出外掛程式的 2.0.0 版本：

```
cd logstash-8.5.0/
bin/logstash-plugin install --version 2.0.0 logstash-output-opensearch
```

如果外掛程式已安裝，請將其更新至最新版本：

```
bin/logstash-plugin update logstash-output-opensearch
```

從外掛程式的 2.0.0 版開始， AWS SDK使用版本 3。如果您使用的是 8.4.0 之前的 Logstash 版本，則必須移除任何預先安裝的版本 AWS 插件和安裝`logstash-integration-aws`插件：

```
/usr/share/logstash/bin/logstash-plugin remove logstash-input-s3
/usr/share/logstash/bin/logstash-plugin remove logstash-input-sqs
/usr/share/logstash/bin/logstash-plugin remove logstash-output-s3
/usr/share/logstash/bin/logstash-plugin remove logstash-output-sns
/usr/share/logstash/bin/logstash-plugin remove logstash-output-sqs
/usr/share/logstash/bin/logstash-plugin remove logstash-output-cloudwatch

/usr/share/logstash/bin/logstash-plugin install --version 0.1.0.pre logstash-
integration-aws
```

2. 若要讓 OpenSearch 輸出外掛程式與 OpenSearch 無伺服器搭配使用，您必須對 logstash.conf 的`opensearch`輸出區段進行下列修改：

   - 將 `aoss` 指定為 `auth_type` 下的 `service_name`。
   - 針對 `hosts` 指定您的集合端點。
   - 新增參數 `default_server_major_version` 和 `legacy_template`。外掛程式需要這些參數才能與 OpenSearch 無伺服器搭配使用。

```
output {
  opensearch {
    hosts => "collection-endpoint:443"
    auth_type => {
      ...
      service_name => 'aoss'
    }
    default_server_major_version => 2
    legacy_template => false
```

```
  }
}
```

此範例組態檔案會從 S3 儲存貯體中的檔案取得輸入，並將其傳送至 OpenSearch 無伺服器集合：

```
input {
  s3  {
    bucket => "my-s3-bucket"
    region => "us-east-1"
  }
}

output {
  opensearch {
    ecs_compatibility => disabled
    hosts => "https://my-collection-endpoint.us-east-1.aoss.amazonaws.com:443"
    index => my-index
    auth_type => {
      type => 'aws_iam'
      aws_access_key_id => 'your-access-key'
      aws_secret_access_key => 'your-secret-key'
      region => 'us-east-1'
      service_name => 'aoss'
    }
    default_server_major_version => 2
    legacy_template => false
  }
}
```

3. 然後，使用新的組態執行 Logstash 來測試外掛程式：

```
bin/logstash -f config/test-plugin.conf
```

Python

下列範例程式碼會使用 Python 的 opensearch-py 用戶端，建立與指定的 OpenSearch 無伺服器集合的安全連線、建立單一索引，然後搜尋該索引。您必須提供 `region` 和 `host` 的值。

與 OpenSearch 服務域相比，重要的區別在於服務名稱（`aoss`而不是`es`）。

```
from opensearchpy import OpenSearch, RequestsHttpConnection, AWSV4SignerAuth
```

```
import boto3

host = ''  # serverless collection endpoint, without https://
region = ''  # e.g. us-east-1

service = 'aoss'
credentials = boto3.Session().get_credentials()
auth = AWSV4SignerAuth(credentials, region, service)

# create an opensearch client and use the request-signer
client = OpenSearch(
    hosts=[{'host': host, 'port': 443}],
    http_auth=auth,
    use_ssl=True,
    verify_certs=True,
    connection_class=RequestsHttpConnection,
    pool_maxsize=20,
)

# create an index
index_name = 'books-index'
create_response = client.indices.create(
    index_name
)

print('\nCreating index:')
print(create_response)

# index a document
document = {
  'title': 'The Green Mile',
  'director': 'Stephen King',
  'year': '1996'
}

response = client.index(
    index = 'books-index',
    body = document,
    id = '1'
)


# delete the index
delete_response = client.indices.delete(
```

```
    index_name
)

print('\nDeleting index:')
print(delete_response)
```

Ruby

`opensearch-aws-sigv4`gem 提供對 OpenSearch 無伺服器的存取，以及開箱即用的 OpenSearch 服務。它具有 opensearch-ruby 客戶端的所有功能，因為這是此 Gem 套件的相依項目。

執行個體化 Sigv4 簽署者時，請指定 `aoss` 為服務名稱：

```
require 'opensearch-aws-sigv4'
require 'aws-sigv4'

signer = Aws::Sigv4::Signer.new(service: 'aoss',
                                region: 'us-west-2',
                                access_key_id: 'key_id',
                                secret_access_key: 'secret')

# create an opensearch client and use the request-signer
client = OpenSearch::Aws::Sigv4Client.new(
  { host: 'https://your.amz-opensearch-serverless.endpoint',
    log: true },
  signer)

# create an index
index = 'prime'
client.indices.create(index: index)

# insert data
client.index(index: index, id: '1', body: { name: 'Amazon Echo',
                                            msrp: '5999',
                                            year: 2011 })

# query the index
client.search(body: { query: { match: { name: 'Echo' } } })

# delete index entry
client.delete(index: index, id: '1')

# delete the index
```

```
client.indices.delete(index: index)
```

與其他用戶端簽署HTTP要求

當您向其他用戶端建構要求時，將要求簽署至 OpenSearch 無伺服器集合時，適用下列要HTTP求。

- 您必須將服務名稱指定為 `aoss`。
- `x-amz-content-sha256`頭是必需的所有 AWS 簽名版本 4 請求。其提供請求承載的雜湊。如果有請求有效負載，請將該值設置為其安全哈希算法（SHA）加密哈希（SHA256）。如果沒有請求承載，請將值設定為 `e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855`，這是一個空字串的雜湊。

主題

- 用 c 索引 URL
- 與郵遞員索引

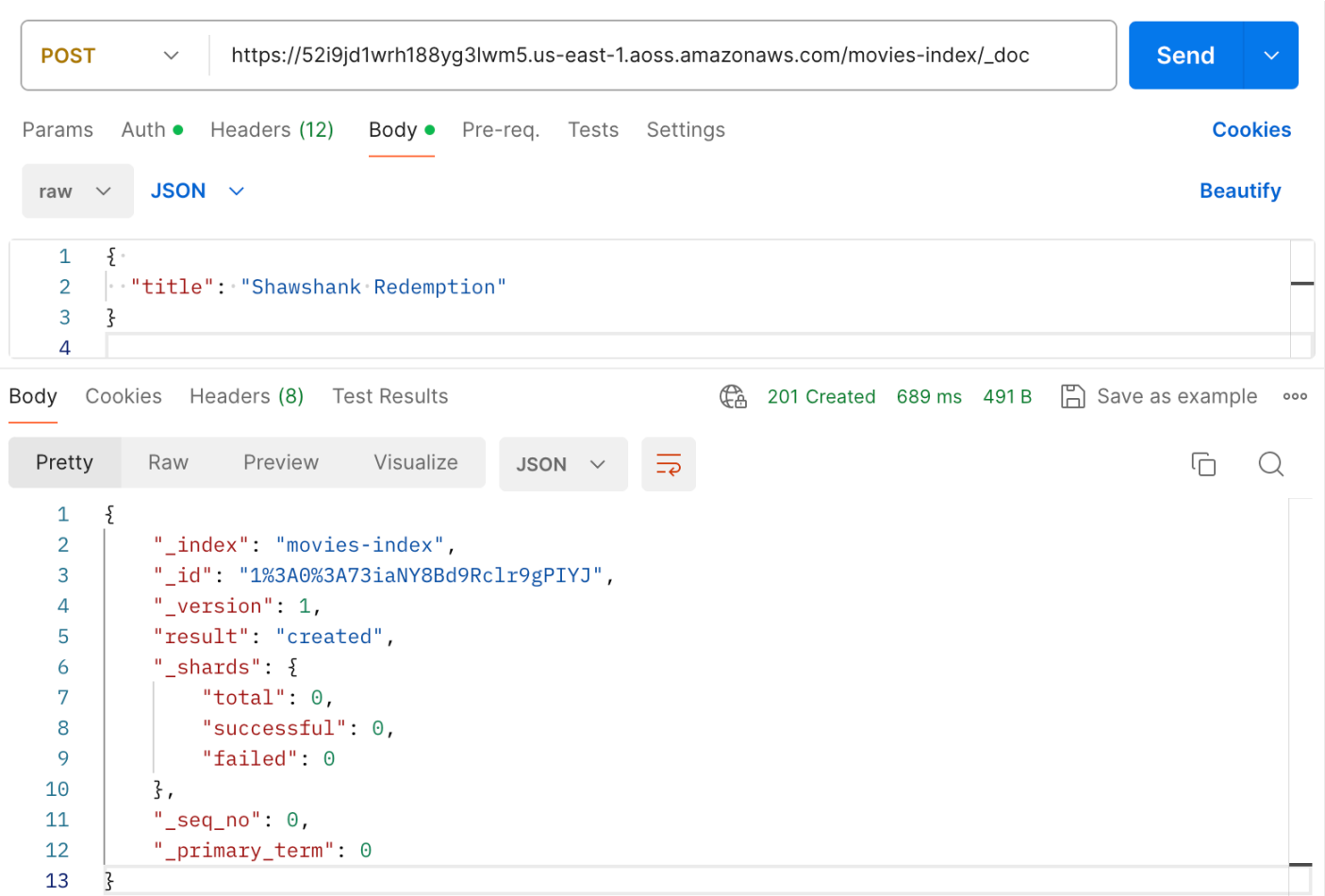
用 c 索引 URL

下列範例要求會使用用戶端URL要求程式庫 (cURL)，將單一文件傳送至集合`movies-index`中指定的索引：

```
curl -XPOST \
    --user "$AWS_ACCESS_KEY_ID":"$AWS_SECRET_ACCESS_KEY" \
    --aws-sigv4 "aws:amz:us-east-1:aoss" \
    --header "x-amz-content-sha256: $REQUEST_PAYLOAD_SHA_HASH" \
    --header "x-amz-security-token: $AWS_SESSION_TOKEN" \
    "https://my-collection-endpoint.us-east-1.aoss.amazonaws.com/movies-index/_doc" \
    -H "Content-Type: application/json" -d '{"title": "Shawshank Redemption"}'
```

與郵遞員索引

下圖顯示了如何使用郵遞員將請求發送到集合。有關進行身份驗證的說明，請參閱驗證 AWS 郵差中的簽名驗證工作流程。

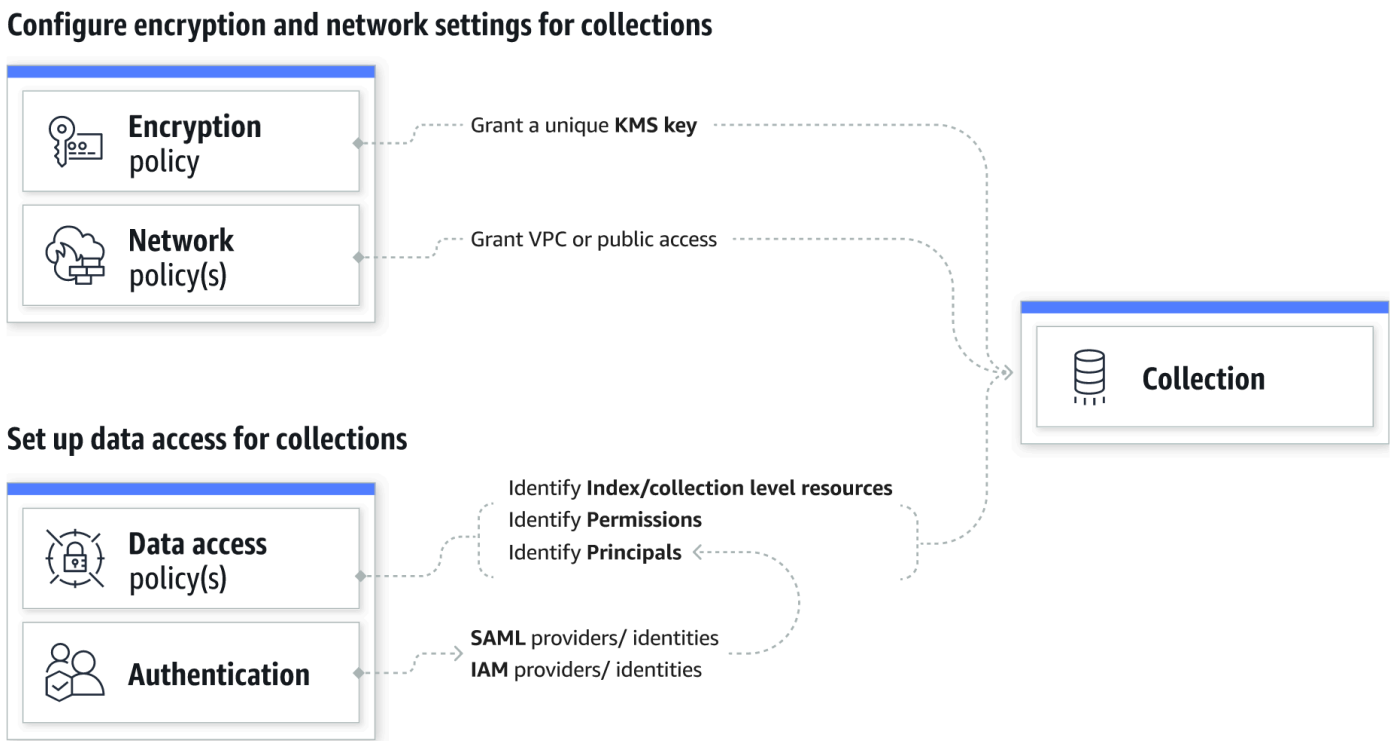


Amazon OpenSearch 無伺服器中的安全性概觀

Amazon OpenSearch 無伺服器中的安全性與 Amazon OpenSearch 服務中的安全性基本上有以下差異：

功能	OpenSearch 服務	OpenSearch 無伺服器
資料存取控制	資料存取由 IAM 政策和精細存取控制決定。	資料存取由資料存取政策決定。
靜態加密	網域的靜態加密是選擇性。	集合需要靜態加密。
安全設定和管理	您必須個別設定每個網域的網路、加密和資料存取。	您可以使用安全政策大規模管理多個集合的安全設定。

下圖說明構成功能集合的安全元件。集合必須具有指派的加密金鑰、網路存取設定和相符的資料存取政策，以授予其資源許可。



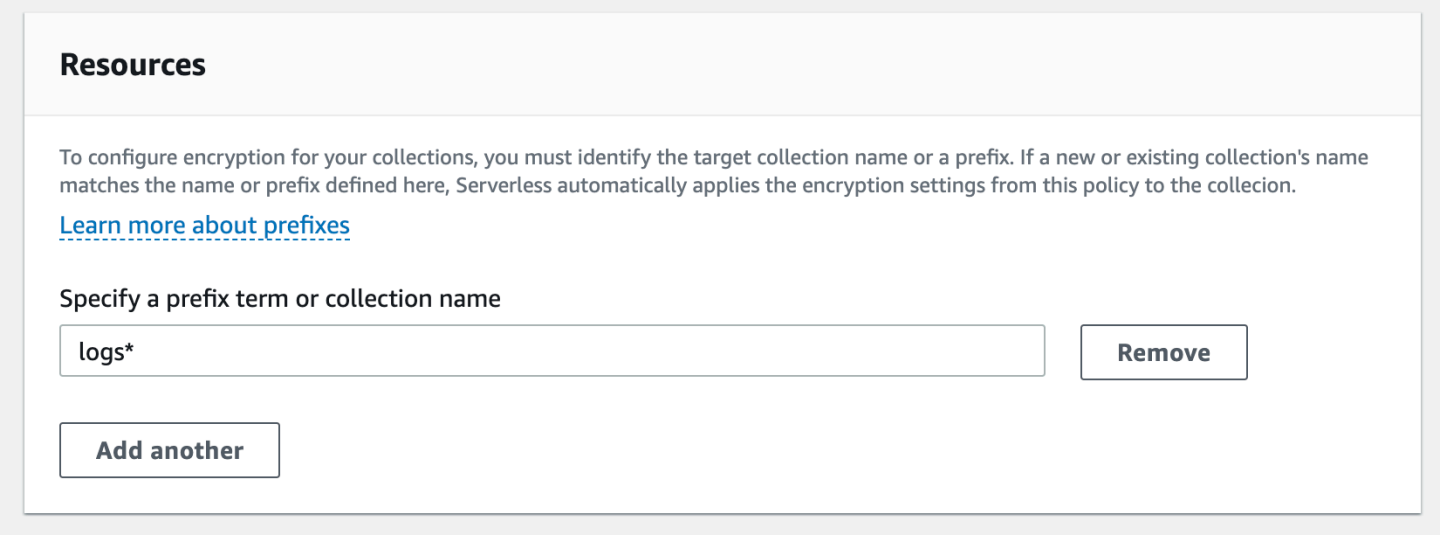
主題

- 加密政策
- 網路政策
- 資料存取政策
- IAM 和 SAML 身分驗證
- 基礎架構安全
- 開始使用 Amazon OpenSearch 無伺服器中的安全性
- 適用於 Amazon OpenSearch 無伺服器的 Identity and Access Management
- Amazon OpenSearch 無伺服器中的加密
- Amazon OpenSearch 無伺服器的網路存取
- 適用於 Amazon OpenSearch 無伺服器的資料存取控制
- 使用界面端點存取 Amazon OpenSearch 無伺服器 ()AWS PrivateLink
- SAML適用於 Amazon OpenSearch 無伺服器的身分
- 適用於 Amazon OpenSearch 無伺服器的合規驗證

加密政策

加密原則會定義您的集合是使用 AWS 擁有的金鑰 或客戶管理的金鑰加密。加密政策由兩個元件組成：資源模式和加密金鑰。資源模式定義政策適用於哪個或哪些集合。加密金鑰決定如何保護相關聯的集合。

若要將政策套用至多個集合，請在政策規則中包含萬用字元 (*)。例如，下列政策適用於名稱以「logs」開頭的所有集合。

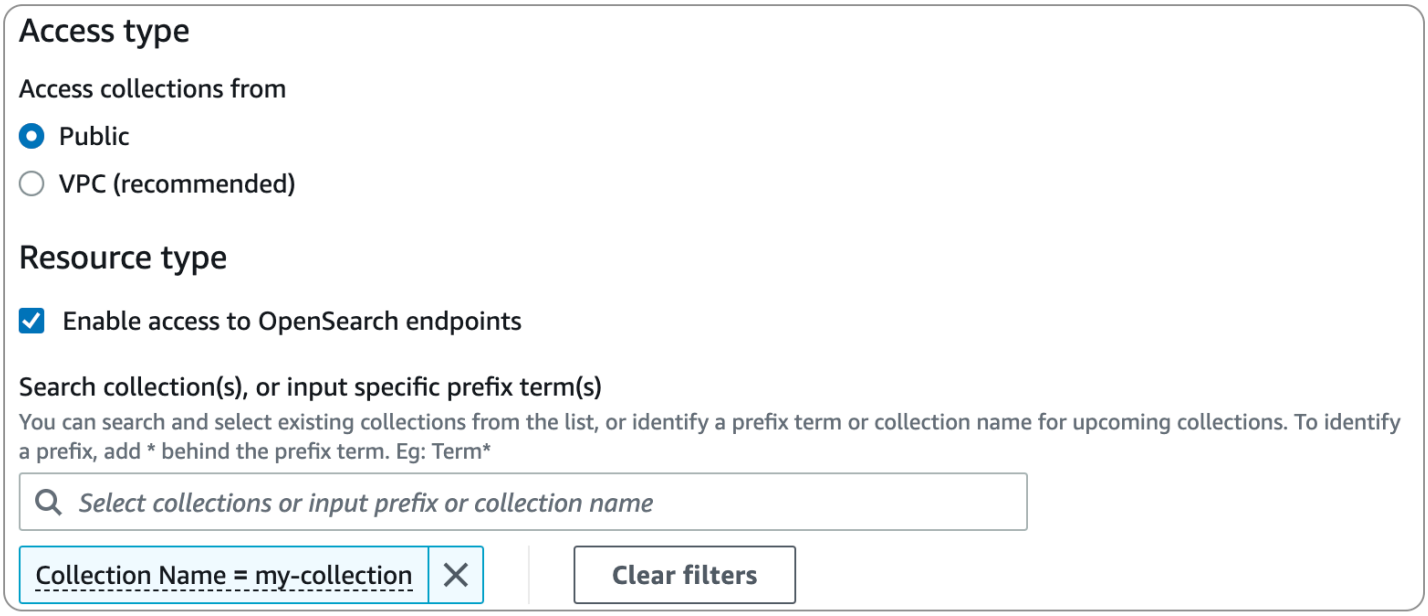


加密政策可簡化建立和管理集合的程序，尤其是以程式設計方式這樣做時。您只需指定名稱即可建立集合，系統會在建立時自動為其指派加密金鑰。

網路政策

網路原則會定義您的集合可以私人存取，還是可透過網際網路從公用網路存取。私有集合可透過 OpenSearch 無伺服器受管 VPC 端點存取，或使用私有存取權由 Amazon 基岩 AWS 服務 等特定存取存取。AWS 服務 正如加密政策，網路政策可套用至多個集合，以便您大規模管理許多集合的網路存取。

網路政策由兩個元件組成：存取類型和資源類型。存取類型可以是公用或私有。資源類型決定您選擇的存取權是套用至集合端點、 OpenSearch 儀表板端點，還是兩者都套用。



如果您計劃在網路原則內設定 VPC 存取，則必須先建立一或多個OpenSearch 無伺服器管理的 VPC 端點。這些端點可讓您像在 VPC 中一樣存取 OpenSearch 無伺服器，而無需使用網際網路閘道、NAT 裝置、VPN 連線或 AWS Direct Connect 連線。

的私人存取權只 AWS 服務 能套用至集合的 OpenSearch 端點，而不能套用至 OpenSearch 儀表板端點。 AWS 服務 無法授與 OpenSearch 儀表板的存取權。

資料存取政策

資料存取政策定義您的使用者如何存取集合內的資料。資料存取政策會自動將存取許可指派給符合特定模式的集合和索引，以協助您大規模管理集合。可將多個政策套用至單一資源。

資料存取政策由一組規則組成，每個規則都有三個元件：資源類型、授予的資源和一組許可。資源類型可以是集合或索引。授予的資源可以是集合/索引名稱或具有萬用字元 (*) 的模式。權限清單會指定原則授與存取權的 OpenSearch API 作業。此外，政策包含主體清單，其中指定要授予存取權的 IAM 角色、使用者和 SAML 身分。

Selected principals

Principals

arn:aws:iam::478253424788:user/Administrator

saml/478253424788/myprovider/user/Annie

Granted resources and permissions (2)

Granted resources	Resource type	Permissions
collection/autopartsinventory	collection	aoss:CreateCollectionItems aoss:UpdateCollectionItems
index/test-collection/*	index	aoss:ReadDocument aoss:DescribeIndex

如需有關資料存取政策格式的詳細資訊，請參閱政策語法。

建立資料存取政策之前，您必須擁有一個或多個 IAM 角色或使用者或 SAML 身分，才能在政策中提供存取權。如需詳細資訊，請參閱下節。

IAM 和 SAML 身分驗證

IAM 主體和 SAML 身分是資料存取政策的其中一個建構區塊。在存取政策的 `principal` 陳述式中，您可以包含 IAM 角色、使用者和 SAML 身分。接著會將您在相關聯政策規則中指定的許可授予這些主體。

```
[
   {
      "Rules":[
         {
            "ResourceType":"index",
            "Resource":[
               "index/marketing/orders*"
            ],
            "Permission":[
               "aoss:*"
            ]
         }
      ],
      "Principal":[
         "arn:aws:iam::123456789012:user/Dale",
         "arn:aws:iam::123456789012:role/RegulatoryCompliance",
         "saml/123456789012/myprovider/user/Annie"
      ]
   }
]
```

您可以直接在 OpenSearch 無伺服器中設定 SAML 驗證。如需詳細資訊，請參閱 the section called “SAML認證”。

基礎架構安全

Amazon OpenSearch 無伺服器受到 AWS 全球網路安全的保護。有關 AWS 安全服務以及如何 AWS 保護基礎結構的詳細資訊，請參閱AWS 雲端安全 若要使用基礎架構安全性的最佳做法來設計您的 AWS 環境，請參閱安全性支柱架構良 AWS 好的架構中的基礎結構保護。

您可以使用 AWS 已發佈的 API 呼叫透過網路存取 Amazon OpenSearch 無伺服器。用戶端必須支援 Transport Layer Security (TLS)。我們需要 TLS 1.2 並建議使用 TLS 1.3。如需 TLS 1.3 支援的加密清單，請參閱 Elastic Load Balancing 文件中的 TLS 通訊協定和密碼。

此外，您必須使用存取金鑰 ID 和與 IAM 主體相關聯的秘密存取金鑰來簽署請求。或者，您可以使用 AWS Security Token Service (AWS STS) 以產生暫時安全憑證以簽署請求。

開始使用 Amazon OpenSearch 無伺服器中的安全性

下列教學課程可協助您開始使用 Amazon OpenSearch 無伺服器。兩個教學課程完成的基本步驟相同，但其中一個使用主控台，另一個則使用 AWS CLI。

請注意，這些教學課程中的使用案例皆已簡化。網路和安全政策都相當公開。在生產工作負載中，建議您設定更強大的安全功能，例如 SAML 身分驗證、VPC 存取權和限制性資料存取政策。

主題

- 教學課程：Amazon OpenSearch 無伺服器 (主控台) 中的安全性入門
- 教學課程：Amazon OpenSearch 無伺服器 (CLI) 中的安全性入門

教學課程：Amazon OpenSearch 無伺服器 (主控台) 中的安全性入門

本教學將引導您完成使用 Amazon OpenSearch 無伺服器主控台建立和管理安全政策的基本步驟。

在本教學課程中，您將完成下列步驟：

1. 設定許可
2. 建立加密政策
3. 建立網路政策

4. 設定資料存取政策
5. 建立集合
6. 上傳並搜尋資料

本教學課程會帶您逐步了解如何使用 AWS Management Console 來設定集合。如需使用 AWS CLI 的相同步驟，請參閱 the section called “教學課程：開始使用安全功能 (CLI)”。

步驟 1：設定許可

> **Note**
>
> 如果您已經使用更廣泛的身分型政策，例如 `Action":"aoss:*"` 或 `Action":"*"`，則可以略過此步驟。不過，在生產環境中，我們建議您遵循最低權限原則，並且僅指派任務完成所需的最低許可。

為完成本教學課程，您必須具備正確的 IAM 許可。使用者或角色必須連接身分型政策，該政策包含以下最低許可：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "aoss:ListCollections",
        "aoss:BatchGetCollection",
        "aoss:CreateCollection",
        "aoss:CreateSecurityPolicy",
        "aoss:GetSecurityPolicy",
        "aoss:ListSecurityPolicies",
        "aoss:CreateAccessPolicy",
        "aoss:GetAccessPolicy",
        "aoss:ListAccessPolicies"
      ],
      "Effect": "Allow",
      "Resource": "*"
    }
  ]
}
```

如需 OpenSearch 無伺服器權限的完整清單，請參閱the section called “身分和存取權管理”。

步驟 2：建立加密政策

加密原則會指定 OpenSearch 無伺服器將用來加密集合的AWS KMS金鑰。您可以使用 AWS 受管金鑰或不同的金鑰來加密集合。為確保本教學課程簡單易懂，我們將使用 AWS 受管金鑰 加密集合。

建立加密政策

1. 在以下位置打開 Amazon OpenSearch 服務控制台 https://console.aws.amazon.com/aos/home。
2. 在左側導覽窗格中，展開 Serverless (無伺服器)，然後選擇 Encryption policies (加密政策)。
3. 選擇 Create encryption policy (建立加密政策)。
4. 將政策命名為 books-policy。如需相關描述，請輸入 Encryption policy for books collection (書籍集合的加密政策)。
5. 在 Resources (資源) 下，輸入 books (書籍)，這就是您將為集合命名的名稱。如果您想要更廣泛的名稱，可以包含星號 (`books*`)，以便將政策套用至以「書籍」一詞開頭的所有集合。
6. 對於加密，請保持選取使用AWS擁有的金鑰。
7. 選擇建立。

步驟 3：建立網路原則

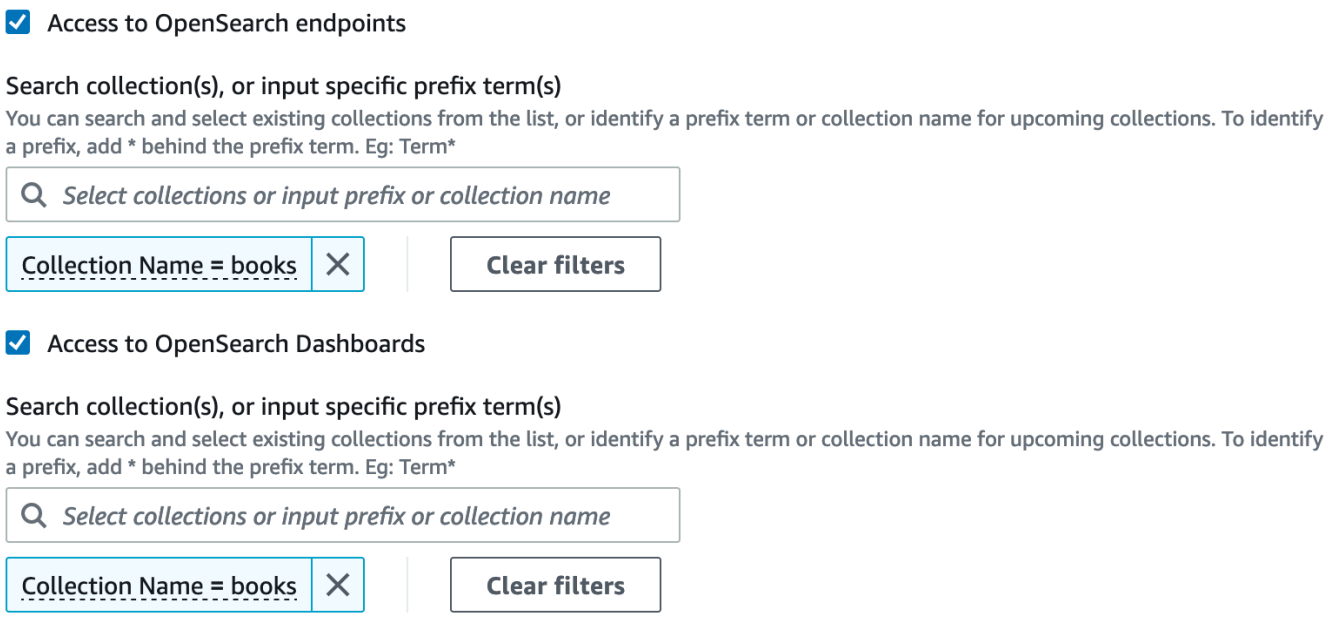
網路原則會決定您的集合是否可透過網際網路從公用網路存取，或是否必須透過 OpenSearch 無伺服器管理的 VPC 端點存取該集合。在本教學課程中，我們將設定公用存取權。

建立網路政策

1. 在左側導覽窗格中，選擇 Network policies (網路政策)，然後選擇 Create network policy (建立網路政策)。
2. 將政策命名為 books-policy。如需相關描述，請輸入 Network policy for books collection (書籍集合的網路政策)。
3. 在 Rule 1 (規則 1) 下，將規則命名為 Public access for books collection (書籍集合的公用存取權)。
4. 為確保本教學課程簡單易懂，我們將為書籍集合設定公用存取權。對於存取類型，選取 Public (公用)。
5. 我們要從 OpenSearch 儀表板存取集合。為此，您需要為儀表板和 OpenSearch 端點設定網路存取權，否則儀表板將無法運作。

對於資源類型，同時啟用 OpenSearch端點存取和 OpenSearch控制面板存取。

6. 在兩個輸入方塊中，輸入 Collection Name = books (集合名稱 = 書籍)。此設定會縮減政策的範圍，使該政策僅套用至單一集合 (books)。您的規則應如下所示：



7. 選擇建立。

步驟 4：建立資料存取原則

在您設定資料存取之前，將無法存取集合資料。資料存取政策與您在步驟 1 中設定的 IAM 身分型政策不同。資料存取政策允許使用者存取集合中的實際資料。

在本教學課程中，我們將為單一使用者提供將資料索引編製為書籍集合所需的許可。

建立資料存取政策

1. 在左側導覽窗格中，選擇 Data access policies (資料存取政策)，然後選擇 Create access policy (建立存取政策)。
2. 將政策命名為 books-policy。如需相關描述，請輸入 Data access policy for books collection (書籍集合的資料存取政策)。
3. 選取 JSON 作為政策定義方法，並將下列政策貼到 JSON 編輯器中。

   將主體 ARN 取代為您將用來登入 OpenSearch 儀表板和索引資料的帳戶的 ARN。

```
[
```

```
    {
       "Rules":[
          {
             "ResourceType":"index",
             "Resource":[
                "index/books/*"
             ],
             "Permission":[
                "aoss:CreateIndex",
                "aoss:DescribeIndex",
                "aoss:ReadDocument",
                "aoss:WriteDocument",
                "aoss:UpdateIndex",
                "aoss:DeleteIndex"
             ]
          }
       ],
       "Principal":[
          "arn:aws:iam::123456789012:user/my-user"
       ]
    }
]
```

此政策為單一使用者提供在書籍集合中建立索引、為某些資料編製索引以及進行搜尋所需的最低許可。

4. 選擇建立。

步驟 5：建立商品系列

現在您已設定加密和網路政策，您可以建立相符的集合，而且安全設定會自動套用至該集合。

建立 OpenSearch 無伺服器集合

1. 在左側導覽窗格中選擇 Collections (集合)，然後選擇 Create collection (建立集合)。
2. 將該集合命名為 books (書籍)。
3. 對於集合類型，選擇 Search (搜尋)。
4. 在「加密」下，「 OpenSearch 無伺服器」會通知您集合名稱符合`books-policy`加密原則。
5. 在 [網路存取設定] 底下， OpenSearch 無伺服器會通知您集合名稱符合`books-policy`網路原則。
6. 選擇下一步。

7. 在 [資料存取原則選項] 底下， OpenSearch 無伺服器會通知您收集名稱符合`books-policy`資料存取原則。
8. 選擇下一步。
9. 檢閱集合組態，然後選擇 Submit (提交)。集合初始化所需的時間通常不到一分鐘。

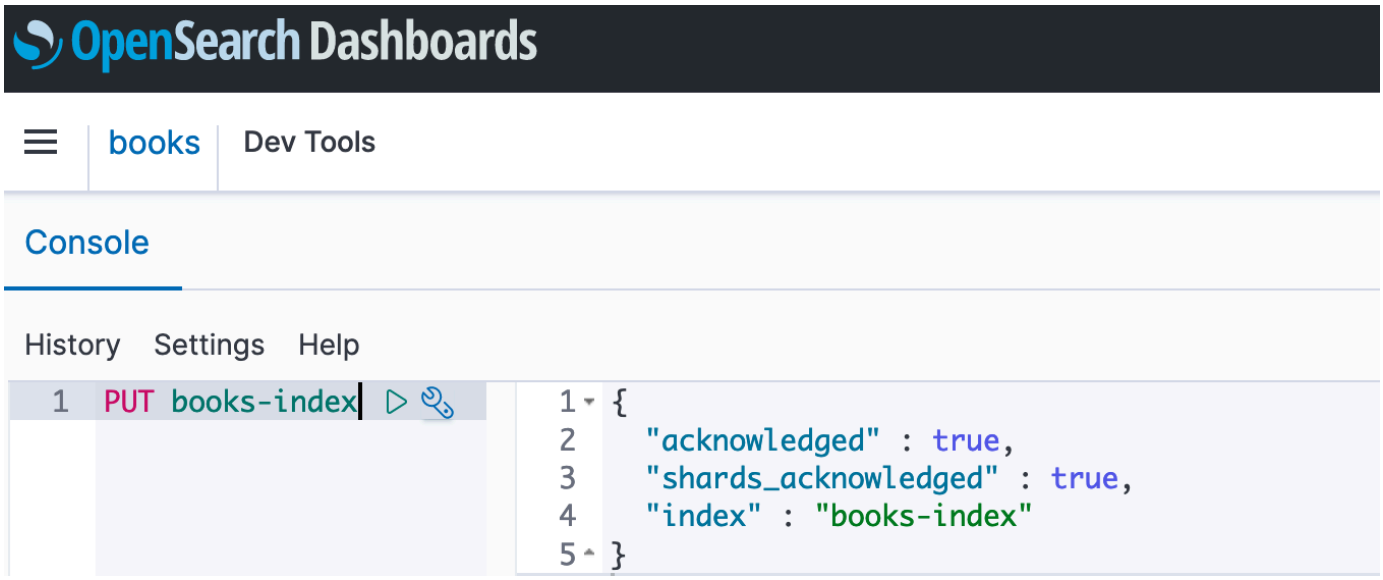
步驟 6：上傳並搜尋資料

您可以使用郵遞員或 curl 將資料上傳至 OpenSearch 無伺服器集合。為了簡潔起見，這些示例使用 OpenSearch 儀表板控制台中的開發工具。

在集合中為資料編製索引和進行搜尋

1. 在左側導覽窗格中選擇 Collections (集合)，然後選擇 books (書籍) 集合以開啟其詳細資訊頁面。
2. 選擇集合的 OpenSearch 儀表板 URL。URL 採用的格式為 `https://collection-id.us-east-1.aoss.amazonaws.com/_dashboards`。
3. 使用您在資料AWS存取原則中指定之主體的存取金鑰和秘密金鑰登入 OpenSearch 儀表板。
4. 在 OpenSearch 儀表板中，開啟左側導覽功能表，然後選擇 [開發工具]。
5. 若要建立名為 books-index 的單一索引，請執行下列命令：

```
PUT books-index
```



6. 若要將單一文件的索引編製為 books-index，請執行下列命令：

```
PUT books-index/_doc/1
```

```
{
  "title": "The Shining",
  "author": "Stephen King",
  "year": 1977
}
```

7. 要搜索 OpenSearch 儀表板中的數據，您需要配置至少一個索引模式。 OpenSearch 使用這些模式來識別您要分析的索引。開啟 Dashboards 主選單，選擇 Stack Management (堆疊管理)，選擇 Index Patterns (索引模式)，然後選擇 Create index pattern (建立索引模式)。在本教學課程中，輸入 books-index。
8. 選擇 Next step (下一步)，然後選擇 Create index pattern (建立索引模式)。建立模式之後，您可以檢視各種文件欄位，例如 `author` 和 `title`。
9. 若要開始搜尋資料，請再次開啟主選單，然後選擇 Discover (探索)，或使用搜尋 API。

教學課程：Amazon OpenSearch 無伺服器 (CLI) 中的安全性入門

本教學課程將逐步引導您完成主控台安全性入門教學課程中所述的步驟，但使用AWS CLI而非 OpenSearch Service 主控台。

在本教學課程中，您會完成下列步驟：

1. 建立 IAM 許可政策
2. 將 IAM 政策附加到 IAM 角色
3. 建立加密政策
4. 建立網路政策
5. 建立集合
6. 設定資料存取政策
7. 擷取收集端點
8. 將數據上傳到您的連接
9. 搜尋集合中的資料

本教學課程的目標是使用相當簡單的加密、網路和資料存取設定來設定單一 OpenSearch 無伺服器集合。例如，我們將設定公用網路存取、用於加密的 AWS 受管金鑰，以及將最低許可授予單一使用者的簡化資料存取政策。

在生產案例中，請考慮實作更強大的組態，包括 SAML 身分驗證、自訂加密金鑰和 VPC 存取權。

開始使用 OpenSearch 無伺服器中的安全性原則

1.

> **Note**
>
> 如果您已經使用更廣泛的身分型政策，例如 `Action":"aoss:*"` 或 `Action":"*"`，則可以略過此步驟。不過，在生產環境中，我們建議您遵循最低權限原則，並且僅指派任務完成所需的最低許可。

若要開始，請使用執行本教學課程中步驟所需的最低許可建立 AWS Identity and Access Management 政策。我們會將該政策命名為 `TutorialPolicy`：

```
aws iam create-policy \
  --policy-name TutorialPolicy \
  --policy-document "{\"Version\": \"2012-10-17\",\"Statement\":
 [{\"Action\": [\"aoss:ListCollections\",\"aoss:BatchGetCollection\",
\"aoss:CreateCollection\",\"aoss:CreateSecurityPolicy\",\"aoss:GetSecurityPolicy\",
\"aoss:ListSecurityPolicies\",\"aoss:CreateAccessPolicy\",\"aoss:GetAccessPolicy\",
\"aoss:ListAccessPolicies\"],\"Effect\": \"Allow\",\"Resource\": \"*\"}]}"
```

回應範例

```
{
    "Policy": {
        "PolicyName": "TutorialPolicy",
        "PolicyId": "ANPAW6WRAECKG6QJWUV7U",
        "Arn": "arn:aws:iam::123456789012:policy/TutorialPolicy",
        "Path": "/",
        "DefaultVersionId": "v1",
        "AttachmentCount": 0,
        "PermissionsBoundaryUsageCount": 0,
        "IsAttachable": true,
        "CreateDate": "2022-10-16T20:57:18+00:00",
        "UpdateDate": "2022-10-16T20:57:18+00:00"
    }
}
```

2. 將 `TutorialPolicy` 連接至 IAM 角色，該角色將在集合中為資料編制索引和進行搜尋。我們會將該使用者命名為 `TutorialRole`：

```
aws iam attach-role-policy \
```

```
  --role-name TutorialRole \
  --policy-arn arn:aws:iam::123456789012:policy/TutorialPolicy
```

3. 建立集合之前，您需要建立加密政策，以將 AWS 擁有的金鑰 指派給您在稍後步驟中建立的書籍集合。

   傳送下列請求，以建立書籍集合的加密政策：

```
aws opensearchserverless create-security-policy \
  --name books-policy \
  --type encryption --policy "{\"Rules\":[{\"ResourceType\":\"collection\",
\"Resource\":[\"collection\/books\"]}],\"AWSOwnedKey\":true}"
```

   回應範例

```
{
    "securityPolicyDetail": {
        "type": "encryption",
        "name": "books-policy",
        "policyVersion": "MTY2OTI0MDAwNTk5MF8x",
        "policy": {
            "Rules": [
                {
                    "Resource": [
                        "collection/books"
                    ],
                    "ResourceType": "collection"
                }
            ],
            "AWSOwnedKey": true
        },
        "createdDate": 1669240005990,
        "lastModifiedDate": 1669240005990
    }
}
```

4. 建立網路政策，該政策會提供書籍集合的公用存取權：

```
aws opensearchserverless create-security-policy --name books-policy --type network
 \
  --policy "[{\"Description\":\"Public access for books collection\",\"Rules
\":[{\"ResourceType\":\"dashboard\",\"Resource\":[\"collection\/books\"]},
```

```
{\"ResourceType\":\"collection\",\"Resource\":[\"collection\/books\"]}],
\"AllowFromPublic\":true}]"
```

回應範例

```
{
    "securityPolicyDetail": {
        "type": "network",
        "name": "books-policy",
        "policyVersion": "MTY2OTI0MDI1Njk1NV8x",
        "policy": [
            {
                "Rules": [
                    {
                        "Resource": [
                            "collection/books"
                        ],
                        "ResourceType": "dashboard"
                    },
                    {
                        "Resource": [
                            "collection/books"
                        ],
                        "ResourceType": "collection"
                    }
                ],
                "AllowFromPublic": true,
                "Description": "Public access for books collection"
            }
        ],
        "createdDate": 1669240256955,
        "lastModifiedDate": 1669240256955
    }
}
```

5. 建立書籍集合：

```
aws opensearchserverless create-collection --name books --type SEARCH
```

回應範例

```
{
```

```
    "createCollectionDetail": {
        "id": "8kw362bpwg4gx9b2f6e0",
        "name": "books",
        "status": "CREATING",
        "type": "SEARCH",
        "arn": "arn:aws:aoss:us-
east-1:123456789012:collection/8kw362bpwg4gx9b2f6e0",
        "kmsKeyArn": "auto",
        "createdDate": 1669240325037,
        "lastModifiedDate": 1669240325037
    }
}
```

6. 建立資料存取政策，該政策會提供在書籍集合中為資料編製索引和進行搜尋的最低許可。將主體 ARN 取代為步驟 1 中的 `TutorialRole` ARN：

```
aws opensearchserverless create-access-policy \
  --name books-policy \
  --type data \
  --policy "[{\"Rules\":[{\"ResourceType\":\"index\",\"Resource\":
[\"index\/books\/books-index\"],\"Permission\":[\"aoss:CreateIndex
\",\"aoss:DescribeIndex\",\"aoss:ReadDocument\",\"aoss:WriteDocument
\",\"aoss:UpdateIndex\",\"aoss:DeleteIndex\"]}],\"Principal\":
[\"arn:aws:iam::123456789012:role\/TutorialRole\"]}]"
```

回應範例

```
{
    "accessPolicyDetail": {
        "type": "data",
        "name": "books-policy",
        "policyVersion": "MTY2OTI0MDM5NDY1M18x",
        "policy": [
            {
                "Rules": [
                    {
                        "Resource": [
                            "index/books/books-index"
                        ],
                        "Permission": [
                            "aoss:CreateIndex",
                            "aoss:DescribeIndex",
                            "aoss:ReadDocument",
```

```
                            "aoss:WriteDocument",
                            "aoss:UpdateDocument",
                            "aoss:DeleteDocument"
                        ],
                        "ResourceType": "index"
                    }
                ],
                "Principal": [
                    "arn:aws:iam::123456789012:role/TutorialRole"
                ]
            }
        ],
        "createdDate": 1669240394653,
        "lastModifiedDate": 1669240394653
    }
}
```

`TutorialRole` 現在應該能夠在書籍集合中為文件編製索引和進行搜尋。

7. 若要呼叫 OpenSearch API，您需要集合端點。傳送下列請求以擷取 `collectionEndpoint` 參數：

```
aws opensearchserverless batch-get-collection --names books
```

回應範例

```
{
    "collectionDetails": [
        {
            "id": "8kw362bpwg4gx9b2f6e0",
            "name": "books",
            "status": "ACTIVE",
            "type": "SEARCH",
            "description": "",
            "arn": "arn:aws:aoss:us-
east-1:123456789012:collection/8kw362bpwg4gx9b2f6e0",
            "createdDate": 1665765327107,
            "collectionEndpoint": "https://8kw362bpwg4gx9b2f6e0.us-
east-1.aoss.amazonaws.com",
            "dashboardEndpoint": "https://8kw362bpwg4gx9b2f6e0.us-
east-1.aoss.amazonaws.com/_dashboards"
        }
    ],
```

```
    "collectionErrorDetails": []
}
```

> **Note**
>
> 在集合狀態變更為 ACTIVE 之前，您都無法看到集合端點。在集合成功建立前，您可能必須進行多次呼叫才能檢查狀態。

8. 使用 Postman 或 curl 等 HTTP 工具，將資料索引編製為書籍集合。我們將建立名為 books-index 的索引，並新增單一文件。

   使用 TutorialRole 的憑證，將下列請求傳送至您在上一步擷取的集合端點。

```
PUT https://8kw362bpwg4gx9b2f6e0.us-east-1.aoss.amazonaws.com/books-index/_doc/1
{
  "title": "The Shining",
  "author": "Stephen King",
  "year": 1977
}
```

   回應範例

```
{
  "_index" : "books-index",
  "_id" : "1",
  "_version" : 1,
  "result" : "created",
  "_shards" : {
    "total" : 0,
    "successful" : 0,
    "failed" : 0
  },
  "_seq_no" : 0,
  "_primary_term" : 0
}
```

9. 若要開始在集合中搜尋資料，請使用搜尋 API。下列查詢會執行基本搜尋：

```
GET https://8kw362bpwg4gx9b2f6e0.us-east-1.aoss.amazonaws.com/books-index/_search
```

   回應範例

```
{
    "took": 405,
    "timed_out": false,
    "_shards": {
        "total": 6,
        "successful": 6,
        "skipped": 0,
        "failed": 0
    },
    "hits": {
        "total": {
            "value": 2,
            "relation": "eq"
        },
        "max_score": 1.0,
        "hits": [
            {
                "_index": "books-index:0::3xJq14MBUaOS0wL26UU9:0",
                "_id": "F_bt4oMBLle5pYmm5q4T",
                "_score": 1.0,
                "_source": {
                    "title": "The Shining",
                    "author": "Stephen King",
                    "year": 1977
                }
            }
        ]
    }
}
```

適用於 Amazon OpenSearch 無伺服器的 Identity and Access Management

AWS Identity and Access Management (IAM) 可協助系統管理員安全地控制 AWS 資源存取權。 AWS 服務 IAM系統管理員控制誰可以驗證 (登入) 和授權 (具有權限) 使用 OpenSearch 無伺服器資源。IAM 是一種您 AWS 服務 可以使用，無需額外費用。

主題

- 無伺服器的身分識別原則 OpenSearch
- OpenSearch 無伺服器的原則動作

- OpenSearch 無伺服器的原則資源
- 適用於 Amazon OpenSearch 無伺服器的政策條件金鑰
- ABAC使用 OpenSearch 無伺服器
- 搭配 OpenSearch 無伺服器使用臨時身分證
- 無伺服器 OpenSearch 的服務連結角色
- 無伺服器的身分識別原則範例 OpenSearch

無伺服器的身分識別原則 OpenSearch

支援身分型政策：是

以身分識別為基礎的原則是您可以附加至身分識別 (例如使用者、使用IAM者群組或角色) 的JSON權限原則文件。這些政策可控制身分在何種條件下能對哪些資源執行哪些動作。若要瞭解如何建立以身分識別為基礎的策略，請參閱《IAM使用指南》中的〈建立IAM策略〉。

使用以IAM身分識別為基礎的策略，您可以指定允許或拒絕的動作和資源，以及允許或拒絕動作的條件。您無法在身分型政策中指定主體，因為這會套用至連接的使用者或角色。若要瞭解可在JSON策略中使用的所有元素，請參閱《使用IAM者指南》中的IAMJSON策略元素參考資料。

無伺服器的身分識別原則範例 OpenSearch

若要檢視 OpenSearch 無伺服器身分識別型原則的範例，請參閱。the section called “身分型政策範例”

OpenSearch 無伺服器的原則動作

支援政策動作：是

JSON策略`Action`元素描述了您可以用來允許或拒絕策略中存取的動作。策略動作通常與關聯的 AWS API操作具有相同的名稱。有一些例外情況，例如沒有匹配API操作的僅限權限的操作。也有一些作業需要政策中的多個動作。這些額外的動作稱為相依動作。

政策會使用動作來授予執行相關聯動作的許可。

OpenSearch 無伺服器中的原則動作會在動作之前使用下列前置詞：

```
aoss
```

若要在單一陳述式中指定多個動作，請用逗號分隔。

```
"Action": [
      "aoss:action1",
      "aoss:action2"
         ]
```

您可以使用萬用字元 (*) 來指定多個動作。例如，若要指定開頭是 Describe 文字的所有動作，請包含以下動作：

```
"Action": "aoss:List*"
```

若要檢視 OpenSearch 無伺服器身分識別型原則的範例，請參閱。 無伺服器的身分識別原則範例 OpenSearch

OpenSearch 無伺服器的原則資源

支援政策資源：是

管理員可以使用 AWS JSON策略來指定誰可以存取什麼內容。也就是說，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

ResourceJSON原則元素會指定要套用動作的一個或多個物件。陳述式必須包含 Resource 或 NotResource 元素。最佳做法是使用其 Amazon 資源名稱 (ARN) 指定資源。您可以針對支援特定資源類型的動作 (稱為資源層級許可) 來這麼做。

對於不支援資源層級許可的動作 (例如列出操作)，請使用萬用字元 (*) 來表示陳述式適用於所有資源。

```
"Resource": "*"
```

適用於 Amazon OpenSearch 無伺服器的政策條件金鑰

支援服務特定政策條件金鑰：是

管理員可以使用 AWS JSON策略來指定誰可以存取什麼內容。也就是說，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

Condition 元素 (或 Condition 區塊) 可讓您指定使陳述式生效的條件。Condition 元素是選用項目。您可以建立使用條件運算子的條件運算式 (例如等於或小於)，來比對政策中的條件和請求中的值。

若您在陳述式中指定多個 Condition 元素，或是在單一 Condition 元素中指定多個索引鍵， AWS 會使用邏輯 AND 操作評估他們。如果您為單一條件索引鍵指定多個值，請使用邏輯OR運算來 AWS 評估條件。必須符合所有條件，才會授與陳述式的許可。

您也可以在指定條件時使用預留位置變數。例如，只有在IAM使用者名稱標記資源時，您才可以授與IAM使用者存取資源的權限。如需詳細資訊，請參閱《IAM使用指南》中的IAM政策元素：變數和標籤。

AWS 支援全域條件金鑰和服務特定條件金鑰。若要查看所有 AWS 全域條件索引鍵，請參閱《使用指南》中的AWS 全域條件內IAM容索引鍵。

除了以屬性為基礎的存取控制 (ABAC) 之外， OpenSearch 無伺服器還支援下列條件金鑰：

- `aoss:collection`
- `aoss:CollectionId`
- `aoss:index`

即使提供存取政策和安全政策的許可，您仍然可以使用這些條件索引鍵。例如：

```
[
   {
      "Effect":"Allow",
      "Action":[
         "aoss:CreateAccessPolicy",
         "aoss:CreateSecurityPolicy"
      ],
      "Resource":"*",
      "Condition":{
         "StringLike":{
            "aoss:collection":"log"
         }
      }
   }
]
```

在此範例中，此條件適用於包含規則的政策，這些規則與集合名稱或模式相符。這些條件具有以下行為：

- `StringEquals`：適用的政策具有包含確切資源字串 "log" (亦即 `collection/log`) 的規則。
- `StringLike`：適用的政策所具備規則包含的資源字串包含字串 "log" (亦即 `collection/log`，但也是 `collection/logs-application` 或 `collection/applogs123`)。

> **Note**
> 集合條件索引鍵不適用於索引層級。例如，在上述政策中，該條件不會套用至包含資源字串 `index/logs-application/*` 的存取或安全政策。

若要查看 OpenSearch 無伺服器條件金鑰清單，請參閱服務授權參考中的 Amazon OpenSearch 無伺服器條件金鑰。若要了解可以使用條件金鑰的動作和資源，請參閱 Amazon OpenSearch 無伺服器定義的動作。

ABAC使用 OpenSearch 無伺服器

支援 ABAC (策略中的標籤): 是

以屬性為基礎的存取控制 (ABAC) 是一種授權策略，可根據屬性定義權限。在中 AWS，這些屬性稱為標籤。您可以將標籤附加至IAM實體 (使用者或角色) 和許多 AWS 資源。標記實體和資源是的第一步ABAC。然後，您可以設計ABAC策略，以便在主參與者的標籤與他們嘗試存取的資源上的標籤相符時允許作業。

ABAC在快速成長的環境中很有幫助，並且有助於原則管理變得繁瑣的情況。

如需根據標籤控制存取，請使用 `aws:ResourceTag/key-name`、`aws:RequestTag/key-name` 或 `aws:TagKeys` 條件索引鍵，在政策的條件元素中，提供標籤資訊。

如果服務支援每個資源類型的全部三個條件金鑰，則對該服務而言，值為 Yes。如果服務僅支援某些資源類型的全部三個條件金鑰，則值為 Partial。

如需有關的詳細資訊ABAC，請參閱什麼是ABAC？ 在《IAM使用者指南》中。若要檢視包含設定步驟的自學課程ABAC，請參閱《使用指南》中的〈使用以屬性為基礎的存取控制 (ABAC) IAM 〉。

如需標記 OpenSearch 無伺服器資源的詳細資訊，請參閱the section called “標記集合”。

搭配 OpenSearch 無伺服器使用臨時身分證

支援臨時憑證：是

當您使用臨時憑據登錄時，某些 AWS 服務 不起作用。如需其他資訊，包括哪些 AWS 服務 與臨時登入資料搭配使用 AWS 服務 ，請參閱《IAM使用指南》IAM中的使用方式。

如果您使用除了使用者名稱和密碼以外的任何方法登入，則您正在 AWS Management Console 使用臨時認證。例如，當您 AWS 使用公司的單一登入 (SSO) 連結存取時，該程序會自動建立臨時認證。當

您以使用者身分登入主控台，然後切換角色時，也會自動建立臨時憑證。如需有關切換角色的詳細資訊，請參閱《IAM使用者指南》中的〈切換到角色 (主控台)〉。

您可以使用 AWS CLI 或手動建立臨時認證 AWS API。然後，您可以使用這些臨時登入資料來存取 AWS。 AWS 建議您動態產生臨時登入資料，而不是使用長期存取金鑰。如需詳細資訊，請參閱IAM。

無伺服器 OpenSearch 的服務連結角色

支援服務連結角色：是

服務連結角色是一種連結至. AWS 服務服務可以擔任代表您執行動作的角色。服務連結角色會顯示在您的中， AWS 帳戶 且屬於服務所有。IAM管理員可以檢視 (但無法編輯服務連結角色) 的權限。

如需有關建立和管理 OpenSearch 無伺服器服務連結角色的詳細資訊，請參閱。the section called “集合建立角色”

無伺服器的身分識別原則範例 OpenSearch

依預設，使用者和角色沒有建立或修改 OpenSearch 無伺服器資源的權限。他們也無法使用 AWS Management Console、 AWS Command Line Interface (AWS CLI) 或執行工作 AWS API。若要授與使用者對所需資源執行動作的權限，IAM管理員可以建立IAM策略。然後，系統管理員可以將IAM原則新增至角色，使用者可以擔任這些角色。

若要瞭解如何使用這些範例原則文件來建立以IAM身分識別為基礎的JSON策略，請參閱使用指南中的IAM建立IAM策略。

如需 Amazon OpenSearch Serverless 定義的動作和資源類型的詳細資訊，包括每種資源類型ARNs的格式，請參閱服務授權參考中適用於 Amazon OpenSearch 無伺服器的動作、資源和條件金鑰。

主題

- 政策最佳實務
- 在主控台中使用 OpenSearch 無伺服器
- 管理 OpenSearch 無伺服器集合
- 檢視 OpenSearch 無伺服器集合
- 使用 OpenSearchAPI操作

政策最佳實務

身分型政策相當強大。他們會決定某人是否可以建立、存取或刪除您帳戶中的 OpenSearch 無伺服器資源。這些動作可能會讓您的 AWS 帳戶產生費用。當您建立或編輯身分型政策時，請遵循下列準則及建議事項：

以身分識別為基礎的原則會決定某人是否可以建立、存取或刪除您帳戶中的 OpenSearch 無伺服器資源。這些動作可能會讓您的 AWS 帳戶產生費用。當您建立或編輯身分型政策時，請遵循下列準則及建議事項：

- 開始使用 AWS 受管原則並邁向最低權限權限 — 若要開始授與使用者和工作負載的權限，請使用可授與許多常見使用案例權限的AWS 受管理原則。它們可用在您的 AWS 帳戶. 建議您透過定義特定於您使用案例的 AWS 客戶管理政策，進一步降低使用權限。如需詳細資訊，請參閱AWS 《IAM使用指南》中針對工作職能的AWS 受管理策略或受管理的策略。
- 套用最低權限權限 — 當您使用原則設定權限時，IAM只授與執行工作所需的權限。為實現此目的，您可以定義在特定條件下可以對特定資源採取的動作，這也稱為最低權限許可。如需有關使用套用權限IAM的詳細資訊，請參閱《使用指南》IAM中的IAM《策略與權限》。
- 使用IAM策略中的條件進一步限制存取 — 您可以在策略中新增條件，以限制對動作和資源的存取。例如，您可以撰寫政策條件，以指定必須使用傳送所有要求SSL。您也可以使用條件來授與對服務動作的存取權 (如透過特定) 使用這些動作 AWS 服務，例如 AWS CloudFormation。如需詳細資訊，請參閱《IAM使用指南》中的IAMJSON策略元素：條件。
- 使用 IAM Access Analyzer 驗證您的原IAM則，以確保安全和功能性的權限 — IAM Access Analyzer 會驗證新的和現有的原則，以便原則遵循IAM原則語言 (JSON) 和IAM最佳做法。IAMAccess Analyzer 提供超過 100 項原則檢查和可行的建議，協助您撰寫安全且功能正常的原則。如需詳細資訊，請參閱IAM使IAM用指南中的存取分析器原則驗證。
- 需要多因素驗證 (MFA) — 如果您的案例需要使IAM用者或 root 使用者 AWS 帳戶，請開啟以取得額外MFA的安全性。若要在呼叫API作業MFA時需要，請將MFA條件新增至您的原則。如需詳細資訊，請參閱《IAM使用指南》中的 < 設定MFA受保護的API存取 >。

如需中最佳作法的詳細資訊IAM，請參閱《IAM使用指南》IAM中的「安全性最佳作法」。

在主控台中使用 OpenSearch 無伺服器

若要在 OpenSearch 服務主控台中存取 OpenSearch 無伺服器，您必須擁有最低限度的權限集。這些權限必須允許您列出並檢視 AWS 帳戶中 OpenSearch 無伺服器資源的詳細資料。如果您建立的以身分識別為基礎的原則，而該原則的限制性比最低所需權限更嚴格，則主控台將無法如預期用於具有該原則的實體 (例如IAM角色) 運作。

您不需要為只對 AWS CLI 或撥打電話的使用者允許最低主控台權限 AWS API。相反地，只允許存取與您嘗試執行之API作業相符的動作。

下列原則可讓使用者在 OpenSearch 服務主控台中存取 OpenSearch 無伺服器：

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Resource": "*",
            "Effect": "Allow",
            "Action": [
                "aoss:ListCollections",
                "aoss:BatchGetCollection",
                "aoss:ListAccessPolicies",
                "aoss:ListSecurityConfigs",
                "aoss:ListSecurityPolicies",
                "aoss:ListTagsForResource",
                "aoss:ListVpcEndpoints",
                "aoss:GetAccessPolicy",
                "aoss:GetAccountSettings",
                "aoss:GetSecurityConfig",
                "aoss:GetSecurityPolicy"
            ]
        }
    ]
}
```

管理 OpenSearch 無伺服器集合

此政策是允許使用者管理和管理 Amazon OpenSearch 無伺服器集合的「集合管理員」政策範例。使用者可以建立、檢視和刪除集合。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Resource": "arn:aws:aoss:region:123456789012:collection/*",
            "Action": [
                "aoss:CreateCollection",
                "aoss:DeleteCollection",
                "aoss:UpdateCollection"
            ],
```

```
            "Effect": "Allow"
        },
        {
            "Resource": "*",
            "Action": [
                "aoss:BatchGetCollection",
                "aoss:ListCollections",
                "aoss:CreateAccessPolicy",
                "aoss:CreateSecurityPolicy"
            ],
            "Effect": "Allow"
        }
    ]
}
```

檢視 OpenSearch 無伺服器集合

此範例政策可讓使用者檢視其帳戶中所有 Amazon OpenSearch 無伺服器系列的詳細資料。使用者無法修改集合或任何關聯的安全政策。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Resource": "*",
            "Action": [
                "aoss:ListAccessPolicies",
                "aoss:ListCollections",
                "aoss:ListSecurityPolicies",
                "aoss:ListTagsForResource",
                "aoss:BatchGetCollection"
            ],
            "Effect": "Allow"
        }
    ]
}
```

使用 OpenSearchAPI操作

資料平面API作業包含您在 OpenSearch 無伺服器中使用的函數，以便從服務衍生即時值。控制平面API操作由您用於設置環境的功能組成。

若要從瀏覽器存取 Amazon OpenSearch 無伺服器資料平面APIs和 OpenSearch 儀表板，您需要為收集資源新增兩個IAM許可。這些權限是`aoss:APIAccessAll`和`aoss:DashboardsAccessAll`。

> **Note**
>
> 從 2023 年 5 月 10 日起， OpenSearch 無伺服器需要這兩個新的收集資源IAM權限。`aoss:APIAccessAll`權限允許資料平面存取，而且`aoss:DashboardsAccessAll`權限允許來自瀏覽器的 OpenSearch 儀表板。未能添加兩個新IAM權限會導致 403 錯誤。

此範例原則可讓使用者存取其帳戶中指定集合的資料平面APIs，以及存取其帳戶中所有集合的 OpenSearch 儀表板。

```
{
    "Version": "2012-10-17",
    "Statement": [
         {
            "Effect": "Allow",
            "Action": "aoss:APIAccessAll",
            "Resource": "arn:aws:aoss:region:account-id:collection/collection-id"
        },
        {
            "Effect": "Allow",
            "Action": "aoss:DashboardsAccessAll",
            "Resource": "arn:aws:aoss:region:account-id:dashboards/default"
        }
    ]
}
```

`aoss:APIAccessAll`並且授`aoss:DashboardsAccessAll`予集合資源的完整IAM權限，而「儀表板」權限也提供 OpenSearch 儀表板存取權。每個權限都可以獨立運作，因此明確拒絕`aoss:APIAccessAll`不會阻止對資源的`aoss:DashboardsAccessAll`訪問，包括開發工具。拒絕的情況也是如此`aoss:DashboardsAccessAll`。

OpenSearch 無伺服器僅在主體的資料平面呼叫IAM原則中的條件設定中支援來源 IP 位址：

```
"Condition": {
    "IpAddress": {
         "aws:SourceIp": "52.95.4.14"
    }
```

```
}
```

Amazon OpenSearch 無伺服器中的加密

靜態加密

您建立的每個 Amazon OpenSearch 無伺服器集合都會受到靜態資料加密的保護，這項安全功能可協助防止未經授權存取您的資料。靜態加密使用 AWS Key Management Service (AWS KMS) 來儲存和管理您的加密金鑰。其會使用 256 位元金鑰的進階加密標準演算法 (AES-256) 來執行加密。

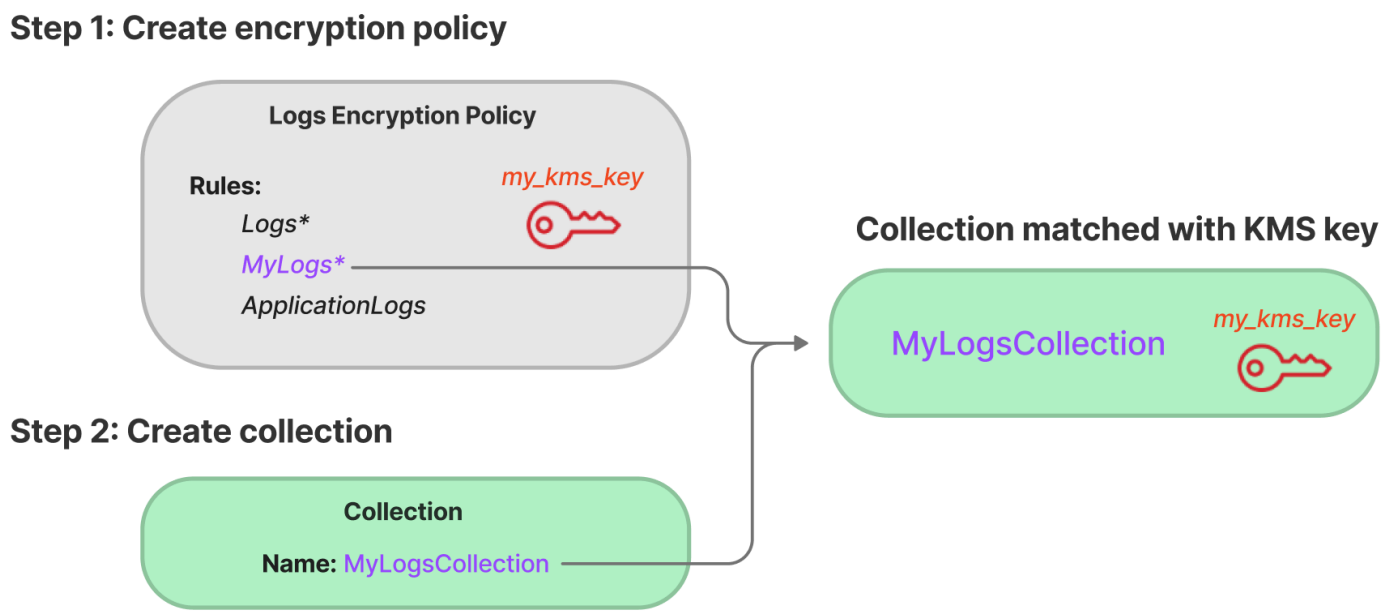
主題

- 加密政策
- 考量事項
- 必要許可
- 客戶受管金鑰的金鑰政策
- OpenSearch 無伺服器如何使用授權 AWS KMS
- 建立加密政策 (主控台)
- 建立加密政策 (AWS CLI)
- 檢視加密政策
- 更新加密政策
- 刪除加密政策

加密政策

您可以使用加密政策，透過自動將加密金鑰指派給符合特定名稱或模式的新建集合，大規模管理許多集合。

建立加密政策時，您可以指定字首，這是以萬用字元為基礎的比對規則 (例如 `MyCollection*`)，或輸入單一集合名稱。然後，當您建立符合該名稱或字首模式的集合時，系統會將該政策和對應的 KMS 金鑰自動指派給該集合。



加密政策包含下列元素：

- `Rules`：一個或多個集合比對規則，每個規則都包含下列子元素：
  - `ResourceType`：目前唯一的選項是「集合」。加密政策僅套用至集合資源。
  - `Resource`：政策套用至的一個或多個集合名稱或模式 (格式為 `collection/<collection name|pattern>`)。
- `AWSOwnedKey`：是否要使用 AWS 擁有的金鑰。
- `KmsARN`：如果您將 `AWSOwnedKey` 設定為 false，請指定用於加密關聯集合之 KMS 金鑰的 Amazon Resource Name (ARN)。如果包括此參數， OpenSearch 無伺服器會忽略該`AWSOwnedKey`參數。

下列範例政策會將客戶受管金鑰指派給任何名為 `autopartsinventory` 的未來集合，以及以「銷售」一詞開頭的集合：

```
{
   "Rules":[
      {
         "ResourceType":"collection",
         "Resource":[
            "collection/autopartsinventory",
            "collection/sales*"
         ]
      }
   ],
```

```
    "AWSOwnedKey":false,
    "KmsARN":"arn:aws:encryption:us-east-1:123456789012:key/93fd6da4-a317-4c17-
bfe9-382b5d988b36"
}
```

即使政策符合集合名稱，如果資源模式包含萬用字元 (*)，您也可以選擇在集合建立期間覆寫此自動指派。如果您選擇覆寫自動金鑰指派， OpenSearch Serverless 會為您建立名為 auto < #### > ##### #########合。該政策最初只適用於單一集合，但您可以加以修改以包含其他集合。

如果您將政策規則修改為不再符合某個集合，則系統不會將關聯的 KMS 金鑰從該集合取消指派。集合一律會使用其初始加密金鑰保持加密的狀態。如果您想要變更集合的加密金鑰，您必須重新建立集合。

如果來自多個政策的規則符合集合，則會使用更明確的規則。例如，如果某個政策包含的規則適用於 `collection/log*`，而另一個適用於 `collection/logSpecial`，則會使用第二個政策的加密金鑰，因為該金鑰更加明確。

如果策略中已有名稱或前置詞存在於另一個策略中，則無法在策略中使用該名稱或前綴。 OpenSearch 如果您嘗試在不同的加密策略中設定相同的資源模式，無伺服器會顯示錯誤。

考量事項

設定集合的加密時應考慮以下事項：

- 所有無伺服器集合都需要靜態加密。
- 您可以選擇使用客戶受管金鑰或 AWS 擁有的金鑰。如果您選擇客戶受管金鑰，建議您啟用自動金鑰輪換。
- 建立集合之後，便無法變更集合的加密金鑰。在您第一次設定商品系列時，請仔細選擇 AWS KMS 要使用的項目。
- 集合只能符合單一加密政策。
- 具有唯一 KMS 金鑰的集合無法與其他集合共用 OpenSearch 運算單位 (OCU)。每個具有唯一金鑰的集合都需要專屬的 4 個 OCU。
- 如果您更新加密政策中的 KMS 金鑰，則變更不會影響已指派 KMS 金鑰的現有相符集合。
- OpenSearch 無伺服器不會明確檢查客戶受管金鑰的使用者權限。如果使用者有權透過資料存取政策存取集合，他們就能夠擷取和查詢透過關聯金鑰加密的資料。

必要許可

OpenSearch 無伺服器的靜態加密使用下列 AWS Identity and Access Management (IAM) 許可。您可以指定 IAM 條件，將使用者限制在特定集合內。

- `aoss:CreateSecurityPolicy`：建立加密政策。
- `aoss:ListSecurityPolicies`：列出連接的所有加密政策和集合。
- `aoss:GetSecurityPolicy`：查看特定加密政策的詳細資訊。
- `aoss:UpdateSecurityPolicy`：修改加密政策。
- `aoss:DeleteSecurityPolicy`：刪除加密政策。

下列身分型存取政策範例提供使用者透過資源模式 `collection/application-logs` 管理加密政策所需的最低許可。

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action":[
            "aoss:CreateSecurityPolicy",
            "aoss:UpdateSecurityPolicy",
            "aoss:DeleteSecurityPolicy",
            "aoss:GetSecurityPolicy"
         ],
         "Resource":"*",
         "Condition":{
            "StringEquals":{
               "aoss:collection":"application-logs"
            }
         }
      },
      {
         "Effect":"Allow",
         "Action":[
            "aoss:ListSecurityPolicies"
         ],
         "Resource":"*"
      }
   ]
}
```

客戶受管金鑰的金鑰政策

如果您選取客戶管理的金鑰來保護集合，則 OpenSearch 無伺服器會取得代表進行選取的主體使用 KMS 金鑰的權限。該主體 (使用者或角色) 必須具有 OpenSearch 無伺服器所需之 KMS 金鑰的權限。您可以在金鑰政策或 IAM 政策中提供這些許可。

OpenSearch 無伺服器至少需要客戶管理金鑰的下列權限：

- 公里：DescribeKey
- 公里：CreateGrant

例如：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "kms:DescribeKey",
        "kms:CreateGrant"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "kms:ViaService": "aoss.us-east-1.amazonaws.com"
        },
        "Bool": {
          "kms:GrantIsForAWSResource": "true"
        }
      }
    }
  ]
}
```

OpenSearch 無伺服器建立具有「公里:」和「KMS: GenerateDataKey 解密」權限的授權。

如需詳細資訊，請參閱 AWS Key Management Service 開發人員指南中的 在 AWS KMS中使用金鑰政策。

OpenSearch 無伺服器如何使用授權 AWS KMS

OpenSearch 無伺服器需要授權才能使用客戶管理的金鑰。

當您使用新金鑰在帳戶中建立加密原則時， OpenSearch Serverless 會將CreateGrant要求傳送至 AWS KMS，以代表您建立授權。中的授權 AWS KMS 用於授予客戶帳戶中 KMS 金鑰的 OpenSearch 無伺服器存取權。

OpenSearch 無伺服器需要授權，才能在下列內部作業中使用您的客戶管理金鑰：

- 傳送DescribeKey AWS KMS 要求以驗證所提供的對稱客戶管理金鑰 ID 是否有效。
- 傳送GenerateDataKey要求至 KMS 金鑰，以建立用來加密物件的資料金鑰。
- 發送解密請求 AWS KMS 以解密加密的數據密鑰，以便將其用於加密您的數據。

您可以隨時撤銷授予的存取權，或移除服務對客戶受管金鑰的存取權。如果您這樣做， OpenSearch Serverless 將無法存取客戶管理金鑰加密的任何資料，這會影響依賴該資料的所有作業，進而導致非同步工作流程中的`AccessDeniedException`錯誤和失敗。

OpenSearch 當指定的客戶受管金鑰未與任何安全性原則或集合相關聯時，無伺服器會在非同步工作流程中淘汰授權。

建立加密政策 (主控台)

在加密政策中，您可以指定政策套用至的 KMS 金鑰和一系列集合模式。當您建立集合時，系統會將對應的 KMS 金鑰指派給符合政策中定義模式之一的任何新集合。建議您先建立加密政策，然後再開始建立集合。

建立 OpenSearch 無伺服器加密原則

1. 打開 Amazon OpenSearch 服務控制台 https://console.aws.amazon.com/aos/home.
2. 在左側導覽面板中，展開 Serverless (無伺服器)，然後選擇 Encryption policies (加密政策)。
3. 選擇 Create encryption policy (建立加密政策)。
4. 提供政策的名稱和描述。
5. 在 Resources (資源) 下，輸入此加密政策的一個或多個資源模式。目前 AWS 帳戶 和區域中符合其中一種模式的任何新建集合都會自動指派給此政策。例如，如果您輸入 `ApplicationLogs` (不含萬用字元)，然後再使用該名稱建立集合，則會將該政策和對應的 KMS 金鑰指派給該集合。

   您也可以提供字首，例如 `Logs*`，此字首會將政策指派給名稱以 `Logs` 開頭的任何新集合。透過使用萬用字元，您可以大規模管理多個集合的加密設定。

6. 在 Encryption (加密) 下，選擇要使用的 KMS 金鑰。
7. 選擇建立。

下一步：建立集合

設定一個或多個加密政策後，您就可以開始建立與這些政策中定義之規則相符的集合。如需說明，請參閱the section called “建立集合”。

在集合建立的「加密」步驟中， OpenSearch Serverless 會通知您您輸入的名稱與加密原則中定義的模式相符，並自動將對應的 KMS 金鑰指派給集合。如果資源模式包含萬用字元 (*)，您可以選擇覆寫相符項目並選取自己的金鑰。

建立加密政策 (AWS CLI)

若要使用 OpenSearch 無伺服器 API 作業建立加密原則，您可以指定資源模式和 JSON 格式的加密金鑰。要CreateSecurityPolicy求接受內嵌政策和 .json 檔案。

加密政策採用下列格式。此範例 `my-policy.json` 檔案符合任何名為 `autopartsinventory` 的未來集合，以及名稱以 `sales` 開頭的任何集合。

```
{
   "Rules":[
      {
         "ResourceType":"collection",
         "Resource":[
            "collection/autopartsinventory",
            "collection/sales*"
         ]
      }
   ],
   "AWSOwnedKey":false,
   "KmsARN":"arn:aws:encryption:us-east-1:123456789012:key/93fd6da4-a317-4c17-
bfe9-382b5d988b36"
}
```

若要使用服務擁有的金鑰，請將 `AWSOwnedKey` 設定為 `true`：

```
{
   "Rules":[
      {
```

```
         "ResourceType":"collection",
         "Resource":[
            "collection/autopartsinventory",
            "collection/sales*"
         ]
      }
   ],
   "AWSOwnedKey":true
}
```

下列請求會建立加密政策：

```
aws opensearchserverless create-security-policy \
    --name sales-inventory \
    --type encryption \
    --policy file://my-policy.json
```

然後，使用 CreateCollectionAPI 作業建立一或多個符合其中一個資源模式的集合。

檢視加密政策

在建立集合之前，您可能想要預覽帳戶中現有的加密政策，以查看哪個政策的資源模式與集合名稱相符。下列ListSecurityPolicies要求會列出您帳戶中的所有加密政策：

```
aws opensearchserverless list-security-policies --type encryption
```

該請求會傳回所有已設定加密政策的相關資訊。使用 `policy` 元素的內容以檢視政策中定義的模式規則：

```
{
   "securityPolicyDetails": [
      {
         "createdDate": 1663693217826,
         "description": "Sample encryption policy",
         "lastModifiedDate": 1663693217826,
         "name": "my-policy",
         "policy": "{\"Rules\":[{\"ResourceType\":\"collection\",\"Resource\":
[\"collection/autopartsinventory\",\"collection/sales*\"]}],\"AWSOwnedKey\":true}",
         "policyVersion": "MTY2MzY5MzIxNzgyNl8x",
         "type": "encryption"
      }
```

```
    ]
}
```

若要檢視有關特定原則 (包括 KMS 金鑰) 的詳細資訊，請使用GetSecurityPolicy命令。

更新加密政策

如果您更新加密政策中的 KMS 金鑰，則變更只會套用至與設定的名稱或模式相符的新建集合。這不會影響已指派 KMS 金鑰的現有集合。

這也適用於政策比對規則。如果您新增、修改或刪除規則，則變更僅適用於新建集合。如果您修改政策的規則，使其不再符合集合的名稱，則現有集合不會遺失其指派的 KMS 金鑰。

如果要更新 OpenSearch 無伺服器主控台中的加密原則，請選擇「加密原則」，選取要修改的原則，然後選擇「編輯」。進行變更，然後選擇 Save (儲存)。

若要使用 OpenSearch 無伺服器 API 更新加密原則，請使用此UpdateSecurityPolicy作業。下列請求會使用新的政策 JSON 文件更新加密政策：

```
aws opensearchserverless update-security-policy \
    --name sales-inventory \
    --type encryption \
    --policy-version 2 \
    --policy file://my-new-policy.json
```

刪除加密政策

當您刪除加密政策時，目前使用政策中定義之 KMS 金鑰的任何集合都不會受到影響。若要刪除 OpenSearch 無伺服器主控台中的原則，請選取該原則，然後選擇刪除。

您也可以使用以下DeleteSecurityPolicy操作：

```
aws opensearchserverless delete-security-policy --name my-policy --type encryption
```

傳輸中加密

在 OpenSearch 無伺服器中，集合中的所有路徑都會使用具有業界標準 AES-256 加密的傳輸層安全性 1.2 (TLS) 進行加密。您也可以透過 TLS 1.2 存取開放搜尋的所有 API 和儀表板。TLS 是一組業界標準的加密通訊協定，用於加密透過網路交換的資訊。

Amazon OpenSearch 無伺服器的網路存取

Amazon OpenSearch 無伺服器集合的網路設定可決定集合是否可透過網際網路從公用網路存取，或者是否必須以私密方式存取集合。

私人存取權可套用至下列其中一項或兩項：

- OpenSearch 無伺服器管理的 VPC 端點
- 支持， AWS 服務 如 Amazon 基岩

您可以針對集合的OpenSearch端點及其對應的OpenSearch 儀表板端點個別設定網路存取。

網路存取是允許從不同來源網路存取的隔離機制。例如，如果集合的 OpenSearch 儀表板端點可公開存取，但 OpenSearch API 端點不是，則從公用網路連線時，使用者只能透過儀表板存取集合資料。如果他們嘗試直接從公用網路呼叫 OpenSearch API，就會封鎖它們。網路設定可用於來源到資源類型的這類排列。Amazon OpenSearch 無伺服器同時支援 IPv4 和 IPv6 連線。

主題

- 網路政策
- 考量事項
- 設定網路原則所需的權限
- 政策優先順序
- 建立網路政策 (主控台)
- 建立網路政策 (AWS CLI)
- 檢視網路政策
- 更新網路政策
- 刪除網路政策

網路政策

網路政策讓您可以自動將網路存取設定指派給符合政策中定義之規則的集合，以便大規模管理許多集合。

在網路政策中，您可以指定一系列規則。這些規則會定義收集端點和 OpenSearch 儀表板端點的存取權限。每個規則都包含一個存取類型 (公用或私人) 和資源類型 (集合和/或 OpenSearch 儀表板端點)。對於每個資源類型 (`collection` 和 `dashboard`)，您可以指定一系列規則來定義政策套用至的集合。

在此範例原則中，第一個規則會指定 VPC 端點存取權限，同時存取所有集合的集合端點和儀表板端點 (從該術語`marketing*`開始)。它還指定了 Amazon 基岩訪問。

> **Note**
>
> 如 Amazon 基岩之 AWS 服務 類的私人存取權限僅適用於集合的 OpenSearch 端點，而不適用於 OpenSearch 儀表板端點。即使`ResourceType`是`dashboard`，也 AWS 服務 無法授與 OpenSearch 儀表板的存取權。

第二個規則會指定對 `finance` 集合的公用存取權，但僅限於集合端點 (無 Dashboards 存取權)。

```
[
   {
      "Description":"Marketing access",
      "Rules":[
         {
            "ResourceType":"collection",
            "Resource":[
               "collection/marketing*"
            ]
         },
         {
            "ResourceType":"dashboard",
            "Resource":[
               "collection/marketing*"
            ]
         }
      ],
      "AllowFromPublic":false,
      "SourceVPCEs":[
         "vpce-050f79086ee71ac05"
      ],
      "SourceServices":[
         "bedrock.amazonaws.com"
      ],
   },
   {
      "Description":"Sales access",
      "Rules":[
         {
            "ResourceType":"collection",
```

```
            "Resource":[
               "collection/finance"
            ]
         }
      ],
      "AllowFromPublic":true
   }
]
```

此原則僅針對以「財務」開頭的集合提供 OpenSearch 儀表板的公開存取權。任何直接訪問 OpenSearch API 的嘗試都將失敗。

```
[
  {
    "Description": "Dashboards access",
    "Rules": [
      {
        "ResourceType": "dashboard",
        "Resource": [
          "collection/finance*"
        ]
      }
    ],
    "AllowFromPublic": true
  }
]
```

網路政策可套用至現有集合以及未來的集合。例如，您可以建立集合，然後使用符合集合名稱的規則建立網路政策。您不需要建立網路政策，就能建立集合。

考量事項

為集合設定網路存取時，請考慮以下項目：

- 如果您計劃設定集合的 VPC 端點存取，則必須先建立至少一個OpenSearch 無伺服器管理的 VPC 端點。
- 私人存取權 AWS 服務 限僅適用於集合的 OpenSearch端點，而不適用於 OpenSearch 儀表板端點。即使`ResourceType`是`dashboard`，也 AWS 服務 無法授與 OpenSearch 儀表板的存取權。
- 如果集合可從公用網路存取，也可以從所有 OpenSearch 無伺服器管理的 VPC 端點和所有端點存取該集合。 AWS 服務

- 多個網路政策可套用至單一集合。如需詳細資訊，請參閱 the section called “政策優先順序”。

設定網路原則所需的權限

OpenSearch 無伺服器的網路存取使用下列 AWS Identity and Access Management (IAM) 許可。您可以指定 IAM 條件，將使用者限制在與特定集合關聯的網路政策內。

- `aoss:CreateSecurityPolicy`：建立網路存取政策。
- `aoss:ListSecurityPolicies`：列出目前帳戶中的所有網路政策。
- `aoss:GetSecurityPolicy`：檢視網路存取政策規格。
- `aoss:UpdateSecurityPolicy`：修改指定的網路存取政策，並變更 VPC ID 或公用存取名稱。
- `aoss:DeleteSecurityPolicy`：刪除網路存取政策 (在將該政策從所有集合中分離之後)。

下列身分型存取政策讓使用者可以檢視所有網路政策，以及更新包含資源模式 `collection/application-logs` 的政策：

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "aoss:UpdateSecurityPolicy"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aoss:collection": "application-logs"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "aoss:ListSecurityPolicies",
                "aoss:GetSecurityPolicy"
            ],
            "Resource": "*"
        }
    ]
```

```
}
```

> **Note**
>
> 此外， OpenSearch 無伺服器需要集合資源的`aoss:APIAccessAll`和`aoss:DashboardsAccessAll`權限。如需詳細資訊，請參閱 the section called “使用 OpenSearchAPI操作”。

政策優先順序

在某些情況下，網路政策規則的重疊情形可能會在政策內部或跨政策發生。發生這種情況時，指定公用存取權的規則會覆寫為兩個規則通用的任何集合指定私有存取權的規則。

例如，在下列政策中，這兩個規則都會將網路存取指派給 `finance` 集合，但其中一個規則指定的是 VPC 存取權，而另一個規則指定的是公用存取權。在此情況下，公用存取權僅會覆寫財務集合的 VPC 存取權 (因為其同時存在於兩個規則中)，因此您可從公用網路存取該財務集合。銷售集合將具有來自指定端點的 VPC 存取權。

```
[
   {
      "Description":"Rule 1",
      "Rules":[
         {
            "ResourceType":"collection",
            "Resource":[
               "collection/sales",
               "collection/finance"
            ]
         }
      ],
      "AllowFromPublic":false,
      "SourceVPCEs":[
         "vpce-050f79086ee71ac05"
      ]
   },
   {
      "Description":"Rule 2",
      "Rules":[
         {
            "ResourceType":"collection",
```

```
            "Resource":[
               "collection/finance"
            ]
         }
      ],
      "AllowFromPublic":true
   }
]
```

如果來自不同規則的多個 VPC 端點套用至某個集合，則這些為附加規則，且可從所有指定端點存取該集合。如果您設定`AllowFromPublic`為`true`但同時提供一或多個`SourceVPCEs`或`SourceServices`，則 OpenSearch Serverless 會忽略 VPC 端點和服務識別碼，而相關聯的集合將具有公開存取權。

建立網路政策 (主控台)

網路政策可套用至現有政策以及未來政策。建議您先建立網路政策，然後再開始建立集合。

建立 OpenSearch 無伺服器網路原則

1. 在以下位置打開 Amazon OpenSearch 服務控制台 https://console.aws.amazon.com/aos/home。
2. 在左側導覽面板中，展開 Serverless (無伺服器)，然後選擇 Network policies (網路政策)。
3. 選擇 Create network policy (建立網路政策)。
4. 提供政策的名稱和描述。
5. 提供一個或多個規則。這些規則會定義 OpenSearch 無伺服器集合及其 OpenSearch 儀表板端點的存取權限。

   每項規則都包含下列要素：

Element	描述
規則名稱	描述規則內容的名稱。例如，「行銷團隊的 VPC 存取權」。
存取類型	選擇公開或私人存取。然後，選取下列其中一項或兩項：

Element	描述
	• 要存取的 VPC 端點 — 指定一或多個OpenSearch 無伺服器管理的 VPC 端點 — 受管 VPC 人雲端端點。 • AWS 服務 私人存取 — 選取一個或多個支援的項目 AWS 服務。
Resource Type (資源類型)	選取是否提供 OpenSearch 端點 (允許呼叫 OpenSearch API)、 OpenSearch 儀表板 (允許存取視覺效果和 OpenSearch 外掛程式使用者介面) 的存取權限，還是提供兩者的存取權。 **Note** AWS 服務 私人存取僅適用於集合的 OpenSearch 端點，而不適用於 OpenSearch 儀表板端點。即使您選取 [OpenSearch 儀表板]，也只 AWS 服務 能授與端點存取權。

對於您選取的每個資源類型，您可以選擇要將政策設定套用至其中的現有集合，和/或建立一個或多個資源模式。資源模式包含字首和萬用字元 (*)，並定義政策設定將套用至的集合。

例如，如果您包含名為 `Marketing*` 的模式，則名稱以「行銷」開頭的任何新的或現有集合都會將此政策中的網路設定自動套用至其中。單一萬用字元 (*) 會將政策套用至所有目前和未來的集合。

此外，您可以指定 future 集合的名稱，而不使用萬用字元，例如`Finance`。 OpenSearch 無伺服器會將原則設定套用至任何具有相同名稱的新建立集合。

6. 如果您對政策組態感到滿意，請選擇 Create (建立)。

建立網路政策 (AWS CLI)

若要使用 OpenSearch 無伺服器 API 作業建立網路原則，請以 JSON 格式指定規則。要CreateSecurityPolicy求接受內嵌政策和 .json 檔案。所有集合和模式採用的格式必須為 `collection/<collection name|pattern>`。

> **Note**
>
> 資源類型`dashboards`僅允許 OpenSearch 控制面板的權限，但為了使 OpenSearch 儀表板功能正常運作，您還必須允許來自相同來源的集合存取。如需範例，請參閱以下第二個政策。

若要指定私人存取權，請包含下列其中一個或兩個元素：

- `SourceVPCEs`— 指定一或多個 OpenSearch 無伺服器管理的 VPC 端點。
- `SourceServices`— 指定一個或多個受支援的識別碼 AWS 服務。目前支援下列服務識別碼：
  - `bedrock.amazonaws.com`— Amazon 基岩

以下範例網路政策提供 VPC 端點和 Amazon 基岩的私有存取權，以便僅針對以前綴開頭的集合收集端點收集端點。`log*`已驗證的使用者無法登入 OpenSearch 儀表板；他們只能以程式設計方式存取集合端點。

```
[
   {
      "Description":"Private access for log collections",
      "Rules":[
         {
            "ResourceType":"collection",
            "Resource":[
               "collection/log*"
            ]
         }
      ],
      "AllowFromPublic":false,
      "SourceVPCEs":[
         "vpce-050f79086ee71ac05"
      ],
      "SourceServices":[
         "bedrock.amazonaws.com"
      ],
```

```
   }
]
```

下列原則會針對名為的單一集合提供 OpenSearch 端點和 OpenSearch 儀表板的公用存取權`finance`。如果該集合不存在，建立集合時，會將網路設定套用至該集合。

```
[
   {
      "Description":"Public access for finance collection",
      "Rules":[
         {
            "ResourceType":"dashboard",
            "Resource":[
               "collection/finance"
            ]
         },
         {
            "ResourceType":"collection",
            "Resource":[
               "collection/finance"
            ]
         }
      ],
      "AllowFromPublic":true
   }
]
```

下列請求會建立上述網路政策：

```
aws opensearchserverless create-security-policy \
    --name sales-inventory \
    --type network \
    --policy "[{\"Description\":\"Public access for finance collection\",\"Rules
\":[{\"ResourceType\":\"dashboard\",\"Resource\":[\"collection\/finance\"]},
{\"ResourceType\":\"collection\",\"Resource\":[\"collection\/finance\"]}],
\"AllowFromPublic\":true}]"
```

若要在 JSON 檔案中提供政策，請使用 `--policy file://my-policy.json` 格式

檢視網路政策

在建立集合之前，您可能想要預覽帳戶中的現有網路政策，以查看哪個政策的資源模式與集合名稱相符。下列ListSecurityPolicies要求會列出您帳戶中的所有網路原則：

```
aws opensearchserverless list-security-policies --type network
```

此請求會傳回所有已設定網路政策的相關資訊。若要檢視在一個特定策略中定義的特徵碼規則，請在回應中的`securityPolicySummaries`元素內容中尋找原則資訊。請注意此原則`type`的`name`和，並在GetSecurityPolicy要求中使用這些屬性，以接收含下列原則詳細資訊的回應：

```
{
    "securityPolicyDetail": [
        {
            "type": "network",
            "name": "my-policy",
            "policyVersion": "MTY2MzY5MTY1MDA3Ml8x",
            "policy": "[{\"Description\":\"My network policy rule\",\"Rules\":
[{\"ResourceType\":\"dashboard\",\"Resource\":[\"collection/*\"]}],\"AllowFromPublic
\":true}]",
            "createdDate": 1663691650072,
            "lastModifiedDate": 1663691650072
        }
    ]
}
```

若要檢視有關特定原則的詳細資訊，請使用GetSecurityPolicy命令。

更新網路政策

當您修改網路的 VPC 端點或公用存取名稱時，所有關聯的集合都會受到影響。若要更新 OpenSearch 無伺服器主控台中的網路原則，請展開 [網路原則]，選取要修改的原則，然後選擇 [編輯]。進行變更，然後選擇 Save (儲存)。

若要使用 OpenSearch 無伺服器 API 更新網路原則，請使用指UpdateSecurityPolicy令。您必須在請求中包含政策版本。您可以使用 `ListSecurityPolicies` 或 `GetSecurityPolicy` 命令擷取政策版本。將最新的政策版本納入其中，可確保您不會意外覆寫其他人所做的變更。

下列請求會使用新的政策 JSON 文件更新網路政策：

```
aws opensearchserverless update-security-policy \
```

```
    --name sales-inventory \
    --type network \
    --policy-version MTY2MzY5MTY1MDA3Ml8x \
    --policy file://my-new-policy.json
```

刪除網路政策

您必須將網路政策從所有集合分離，才能將其刪除。若要刪除 OpenSearch 無伺服器主控台中的原則，請選取該原則，然後選擇刪除。

您也可以使用以下DeleteSecurityPolicy命令：

```
aws opensearchserverless delete-security-policy --name my-policy --type network
```

適用於 Amazon OpenSearch 無伺服器的資料存取控制

透過 Amazon OpenSearch Serverless 中的資料存取控制，無論使用者的存取機制或網路來源為何，都可以讓使用者存取集合和索引。您可以提供 IAM 角色和 SAML 身分的存取權。

您可以透過資料存取政策管理許可，這些政策套用至集合和索引資源。資料存取政策會自動將存取許可指派給符合特定模式的集合和索引，以協助您大規模管理集合。可將多個資料存取政策套用至單一資源。請注意，您必須具有集合的資料存取政策，才能存取 OpenSearch 儀表板 URL。

主題

- 資料存取政策與 IAM 政策比較
- 設定資料存取政策所需的 IAM 許可
- 政策語法
- 支援的政策許可
- OpenSearch 儀表板的範例資料集
- 建立資料存取政策 (主控台)
- 建立資料存取政策 (AWS CLI)
- 檢視資料存取政策
- 更新資料存取政策
- 刪除資料存取政策
- 跨帳戶資料存取

資料存取政策與 IAM 政策比較

資料存取政策在邏輯上與 AWS Identity and Access Management (IAM) 政策分開。IAM 許可會控制對無伺服器 API 操作 (例如 `CreateCollection` 和 `ListAccessPolicies`) 的存取。資料存取原則可控制 OpenSearch 無伺服器支援之OpenSearch 作業的存取，例如`PUT <index>`或`GET _cat/indices`。

控制資料存取政策 API 操作 (例如 `aoss:CreateAccessPolicy` 和 `aoss:GetAccessPolicy`，請參閱下一節所述) 存取的 IAM 許可不會影響資料存取政策中指定的許可。

例如，假設 IAM 政策拒絕使用者為 `collection-a` 建立資料存取政策，但允許其為所有集合 (`*`) 建立資料存取政策：

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [
                "aoss:CreateAccessPolicy"
            ],
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "aoss:collection": "collection-a"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "aoss:CreateAccessPolicy"
            ],
            "Resource": "*"
        }
    ]
}
```

如果使用者建立的資料存取政策允許所有集合 (`collection/*` 或 `index/*/*`) 的特定許可，則該政策將套用至所有集合，包括集合 A。

> **Important**
>
> 在資料存取原則中被授與權限不足以存取您的 OpenSearch 無伺服器集合中的資料。相關聯的主體也必須獲得 IAM 許可`aoss:APIAccessAll`和的存取權`aoss:DashboardsAccessAll`。這兩個權限都會授與對集合資源的完整存取權，而「儀表板」權限也可讓您存取 OpenSearch 儀表板。如果主體沒有這兩個 IAM 許可，則在嘗試將請求傳送至集合時，他們會收到 403 錯誤。如需詳細資訊，請參閱 the section called “使用 OpenSearchAPI操作”。

設定資料存取政策所需的 IAM 許可

OpenSearch 無伺服器的資料存取控制使用下列 IAM 許可。您可以指定 IAM 條件，將使用者限制為特定存取政策名稱。

- `aoss:CreateAccessPolicy`：建立存取政策。
- `aoss:ListAccessPolicies`：列出所有存取政策。
- `aoss:GetAccessPolicy`：請參閱有關特定存取政策的詳細資訊。
- `aoss:UpdateAccessPolicy`：修改存取政策。
- `aoss:DeleteAccessPolicy`：刪除存取政策。

下列身分型存取政策讓使用者可以檢視所有存取政策，以及更新包含資源模式 `collection/logs` 的政策。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "aoss:ListAccessPolicies",
                "aoss:GetAccessPolicy"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": [
                "aoss:UpdateAccessPolicy"
            ],
```

```
            "Effect": "Allow",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aoss:collection": [
                        "logs"
                    ]
                }
            }
        }
    ]
}
```

> **Note**
>
> 此外， OpenSearch 無伺服器需要集合資源的`aoss:APIAccessAll`和`aoss:DashboardsAccessAll`權限。如需詳細資訊，請參閱 the section called “使用 OpenSearchAPI操作”。

政策語法

資料存取政策包含一組規則，每個規則均包含下列元素：

Element	描述
`ResourceType`	許可套用的資源類型 (集合或索引)。別名和範本許可位於集合層級，而建立、修改和搜尋資料的許可則位於索引層級。如需詳細資訊，請參閱 Supported policy permissions (支援的政策許可)。
`Resource`	資源名稱和/或模式的清單。模式是字首後接萬用字元 (*)，允許關聯的許可套用至多個資源。 • 集合採用格式 `collection/` *`<name|pattern>`* 。 • 索引採用格式 `index/`*`<collection-name|pattern>`* `/`*`<index-name|pattern/>`* 。
`Permission`	為指定資源授予的許可清單。(如需許可與其允許之 API 操作的完整清單，請參閱 the section called “支援的 OpenSearch API 作業和權限”)。

Element	描述
`Principal`	要授予存取權的一個或多個主體清單。主體可以是 IAM 角色 ARN，也可以是 SAML 身分。這些主體必須在目前的 AWS 帳戶內。資料存取原則不直接支援跨帳戶存取，但您可以在原則中包含角色，而來自不同的使用者 AWS 帳戶可以在集合擁有的帳戶中承擔這個角色。如需詳細資訊，請參閱 the section called “跨帳戶資料存取”。

下列範例政策會將別名和範本許可授予名為 `autopartsinventory` 的集合以及任何以字首 `sales*` 開頭的集合。同時也會將讀取和寫入許可授予 `autopartsinventory` 集合中的所有索引，以及以字首 `orders*` 開頭的 `salesorders` 集合中的任何索引。

```
[
   {
      "Description": "Rule 1",
      "Rules":[
         {
            "ResourceType":"collection",
            "Resource":[
               "collection/autopartsinventory",
               "collection/sales*"
            ],
            "Permission":[
               "aoss:CreateCollectionItems",
               "aoss:UpdateCollectionItems",
               "aoss:DescribeCollectionItems"
            ]
         },
         {
            "ResourceType":"index",
            "Resource":[
               "index/autopartsinventory/*",
               "index/salesorders/orders*"
            ],
            "Permission":[
               "aoss:*"
            ]
         }
      ],
      "Principal":[
         "arn:aws:iam::123456789012:user/Dale",
```

```
            "arn:aws:iam::123456789012:role/RegulatoryCompliance",
            "saml/123456789012/myprovider/user/Annie",
            "saml/123456789012/anotherprovider/group/Accounting"
        ]
    }
]
```

您無法在政策中明確拒絕存取。因此，所有政策許可均可附加。例如，若一個政策授予使用者 `aoss:ReadDocument`，而另一個政策授予 `aoss:WriteDocument`，則使用者將同時擁有兩個許可。如果第三個政策授予相同的使用者 `aoss:*`，則使用者可以對關聯的索引執行所有動作；限制較多的許可不會覆寫限制較少的許可。

支援的政策許可

資料存取政策支援下列許可。有關每個權限允許的 OpenSearch API 操作，請參閱the section called “支援的 OpenSearch API 作業和權限”。

集合許可

- `aoss:CreateCollectionItems`
- `aoss:DeleteCollectionItems`
- `aoss:UpdateCollectionItems`
- `aoss:DescribeCollectionItems`
- `aoss:*`

索引許可

- `aoss:ReadDocument`
- `aoss:WriteDocument`
- `aoss:CreateIndex`
- `aoss:DeleteIndex`
- `aoss:UpdateIndex`
- `aoss:DescribeIndex`
- `aoss:*`

OpenSearch 儀表板的範例資料集

OpenSearch 儀表板提供隨附視覺效果、儀表板和其他工具的範例資料集，可協助您在新增自己的資料之前探索儀表板。若要從此範例資料建立索引，您需要資料存取原則，以提供您要使用之資料集的權限。下列原則使用萬用字元 (*) 來提供所有三個範例資料集的權限。

```
[
  {
    "Rules": [
      {
        "Resource": [
          "index/<collection-name>/opensearch_dashboards_sample_data_*"
        ],
        "Permission": [
          "aoss:CreateIndex",
          "aoss:DescribeIndex",
          "aoss:ReadDocument"
        ],
        "ResourceType": "index"
      }
    ],
    "Principal": [
      "arn:aws:iam::<account-id>:user/<user>"
    ]
  }
]
```

建立資料存取政策 (主控台)

您可以使用視覺化編輯器，或以 JSON 格式建立資料存取政策。當您建立集合時，系統會將對應的許可指派給符合政策中定義模式之一的任何新集合。

建立 OpenSearch 無伺服器資料存取原則

1. 在以下位置打開 Amazon OpenSearch 服務控制台 https://console.aws.amazon.com/aos/home。
2. 展開左側導覽窗格中的 Serverless (無伺服器)，然後選擇 Data access control (資料存取控制)。
3. 選擇 Create access policy (建立存取政策)。
4. 提供政策的名稱和描述。
5. 為政策中的第一個規則提供名稱。例如，"Logs collection access" (日誌集合存取)。

6. 選擇 Add principals (新增主體)，然後選取要向其提供資料存取權的一個或多個 IAM 角色或 SAML 使用者和群組。

> **Note**
>
> 若要從下拉式選單中選取主體，您必須具有 `iam:ListUsers` 和 `iam:ListRoles` 許可 (對於 IAM 主體) 和 `aoss:ListSecurityConfigs` 許可 (對於 SAML 身分)。

7. 選擇 Grant (授予)，然後選取別名、範本和索引許可，以授予關聯的主體。如需完整的許可及其允許之存取的完整清單，請參閱 the section called “支援的 OpenSearch API 作業和權限”。
8. (選用) 設定政策的其他規則。
9. 選擇建立。在您建立政策與強制執行許可之間，可能會有大約一分鐘的延遲時間。如果延遲超過 5 分鐘，請聯絡 AWS Support。

> **Important**
>
> 如果您的政策僅包含索引許可 (而且沒有集合許可)，您可能仍會看到相符集合的訊息，表示 `Collection cannot be accessed yet. Configure data access policies so that users can access the data within this collection`。您可以忽略此警告。允許的主體仍然可以對集合執行其指派的索引相關操作。

建立資料存取政策 (AWS CLI)

若要使用 OpenSearch 無伺服器 API 建立資料存取原則，請使用指`CreateAccessPolicy`令。該命令接受內嵌政策和 .json 檔案。內嵌政策必須編碼為 JSON 逸出字串。

下列請求會建立資料存取政策：

```
aws opensearchserverless create-access-policy \
    --name marketing \
    --type data \
    --policy "[{\"Rules\":[{\"ResourceType\":\"collection\",\"Resource\":
[\"collection/autopartsinventory\",\"collection/sales*\"],\"Permission\":
[\"aoss:UpdateCollectionItems\"]},{\"ResourceType\":\"index\",\"Resource\":
[\"index/autopartsinventory/*\",\"index/salesorders/orders*\"],\"Permission
\":[\"aoss:ReadDocument\",\"aoss:DescribeIndex\"]}],\"Principal\":
[\"arn:aws:iam::123456789012:user/Shaheen\"]}]"
```

若要在 .json 檔案中提供政策，請使用格式 `--policy file://my-policy.json`。

原則中包含的主參與者現在可以使用被授與其存取權的OpenSearch 作業。

檢視資料存取政策

在建立集合之前，您可能想要預覽帳戶中的現有資料存取政策，以查看哪個政策的資源模式與集合名稱相符。下列ListAccessPolicies要求會列出您帳戶中的所有資料存取政策：

```
aws opensearchserverless list-access-policies --type data
```

該請求會傳回所有已設定資料存取政策的相關資訊。若要檢視在一個特定策略中定義的特徵碼規則，請在回應中的`accessPolicySummaries`元素內容中尋找原則資訊。請注意此原則`type`的`name`和，並在GetAccessPolicy要求中使用這些屬性，以接收含下列原則詳細資訊的回應：

```
{
    "accessPolicyDetails": [
        {
            "type": "data",
            "name": "my-policy",
            "policyVersion": "MTY2NDA1NDE4MDg1OF8x",
            "description": "My policy",
            "policy": "[{\"Rules\":[{\"ResourceType\":\"collection\",
\"Resource\":[\"collection/autopartsinventory\",\"collection/sales*\"],
\"Permission\":[\"aoss:UpdateCollectionItems\"]},{\"ResourceType\":\"index\",
\"Resource\":[\"index/autopartsinventory/*\",\"index/salesorders/orders*\"],
\"Permission\":[\"aoss:ReadDocument\",\"aoss:DescribeIndex\"]}],\"Principal\":
[\"arn:aws:iam::123456789012:user/Shaheen\"]}]",
            "createdDate": 1664054180858,
            "lastModifiedDate": 1664054180858
        }
    ]
}
```

您可以包含資源篩選條件，將結果限制為包含特定集合或索引的政策：

```
aws opensearchserverless list-access-policies --type data --resource
 "index/autopartsinventory/*"
```

若要檢視有關特定策略的詳細資料，請使用GetAccessPolicy命令。

更新資料存取政策

當您更新資料存取政策時，所有關聯的集合均會受到影響。若要更新 OpenSearch 無伺服器主控台中的資料存取原則，請選擇 [資料存取控制]，選取要修改的原則，然後選擇 [編輯]。進行變更，然後選擇 Save (儲存)。

若要使用 OpenSearch 無伺服器 API 更新資料存取原則，請傳送要`UpdateAccessPolicy`求。您必須包含政策版本，您可以使用 `ListAccessPolicies` 或 `GetAccessPolicy` 命令擷取該版本。將最新的政策版本納入其中，可確保您不會意外覆寫其他人所做的變更。

下列UpdateAccessPolicy要求會使用新的原則 JSON 文件更新資料存取原則：

```
aws opensearchserverless update-access-policy \
    --name sales-inventory \
    --type data \
    --policy-version MTY2NDA1NDE4MDg10F8x \
    --policy file://my-new-policy.json
```

在您更新政策與強制執行新許可之間，可能會有幾分鐘的延遲時間。

刪除資料存取政策

當您刪除資料存取政策時，所有關聯的集合均會失去政策中定義的存取權。在刪除政策之前，請確保您的 IAM 和 SAML 使用者具有集合的適當存取權。若要刪除 OpenSearch 無伺服器主控台中的原則，請選取該原則，然後選擇刪除。

您也可以使用以下DeleteAccessPolicy命令：

```
aws opensearchserverless delete-access-policy --name my-policy --type data
```

跨帳戶資料存取

雖然您無法建立具有跨帳戶身分識別或跨帳戶集合的資料存取政策，但您仍然可以使用假設角色選項來設定跨帳戶存取權。例如，如果*account-a*擁有*account-b*需要存取權的集合，則來自的使用者*account-b*可以在中扮演角色*account-a*。角色必須具有 IAM 許可`aoss:DashboardsAccessAll`，`aoss:APIAccessAll`並且包含在的資料存取政策中*account-a*。

使用界面端點存取 Amazon OpenSearch 無伺服器 ()AWS PrivateLink

您可以使 AWS PrivateLink 用在 VPC 和 Amazon OpenSearch 無伺服器之間建立私人連線。您可以像在 VPC 中一樣存取 OpenSearch 無伺服器，而無需使用網際網路閘道、NAT 裝置、VPN 連線或 AWS Direct Connect 連線。VPC 中的執行個體不需要公用 IP 位址即可存取無 OpenSearch 伺服器。

您可以建立由 AWS PrivateLink提供支援的介面端點來建立此私有連線。我們會在您為介面端點指定的每個子網路中建立端點網路介面。這些是由請求者管理的網路介面，可做為無伺服器流量的進入點。OpenSearch

如需詳細資訊，請參閱《AWS PrivateLink 指南》中的透過 AWS PrivateLink存取 AWS 服務。

主題

- 收集端點的 DNS 解析
- VPC 和網路存取原則
- VPC 和端點原則
- 考量事項
- 必要許可
- 建立 OpenSearch 無伺服器的介面端點
- 下一步：授予端點存取權給集合

收集端點的 DNS 解析

建立 VPC 端點時，服務會建立新的 Amazon Route 53 私有託管區域並將其附加至 VPC。此私有託管區域由一筆記錄組成，可將 OpenSearch 無伺服器集合 (`*.aoss.us-east-1.amazonaws.com`) 的萬用字元 DNS 記錄解析為用於端點的介面位址。您只需要 VPC 中的一個 OpenSearch 無伺服器 VPC 端點即可存取每個端點中的任何和所有集合和儀表板。 AWS 區域每個具有 OpenSearch 無伺服器端點的 VPC 都附加了自己的私有託管區域。

OpenSearch 無伺服器也會為區域中的所有系列建立公用 Route 53 萬用字元 DNS 記錄。DNS 名稱會解析為 OpenSearch 無伺服器公用 IP 位址。VPC 中沒有 OpenSearch 無伺服器 VPC 端點或公用網路中的用戶端的用戶端可以使用公用 Route 53 解析器，並使用這些 IP 位址存取集合和儀表板。VPC 端點的 IP 位址類型 (IPv4、IPv6 或 Dualstack) 是根據您為無伺服器建立介面端點時提供的子網路來決定。 OpenSearch

> **Note**
>
> 您可以使用中update-vpc-endpoint的命令，將現有的 IPv4 VPC 端點更新為雙堆疊。 AWS CLI

指定虛擬私人雲端的 DNS 解析器位址是 VPC 人雲端 CIDR 的 VPC 二個 IP 位址。VPC 中的任何用戶端都需要使用該解析器來取得任何集合的 VPC 端點位址。解析器使用由 OpenSearch 無服務器創建的私有託管區域。對任何帳戶中的所有集合使用該解析器就足夠了。您也可以將 VPC 解析器用於某些收集端點，並為其他端點使用公開解析程式，但通常不需要這樣做。

VPC 和網路存取原則

若要為集合授與 OpenSearch API 和儀表板的網路權限，您可以使用 OpenSearch 無伺服器網路存取原則。您可以從 VPC 端點或公用網際網路控制此網路存取。由於您的網路原則僅控制流量權限，因此您還必須設定資料存取原則，以指定對集合中的資料及其索引進行操作的權限。將 OpenSearch 無伺服器 VPC 端點視為服務的存取點，將網路存取原則視為集合和儀表板的網路層級存取點，而資料存取原則則則則是針對集合中資料的任何作業進行精細存取控制的存取點。

由於您可以在網路原則中指定多個 VPC 端點 ID，因此建議您為每個需要存取集合的 VPC 建立 VPC 端點。這些 VPC 可以屬於擁有 OpenSearch 無伺服器集合和網路原則的帳戶不同 AWS 的帳戶。我們不建議您在兩個帳戶之間建立虛擬私人雲端對等或其他 Proxy 解決方案，以便一個帳戶的 VPC 可以使用另一個帳戶的 VPC 端點。與擁有自己端點的每個 VPC 相比，這樣的安全性和成本效益較低。其他 VPC 的管理員無法輕易看到第一個 VPC，他們已在網路政策中設定對該 VPC 端點的存取權。

VPC 和端點原則

Amazon OpenSearch 無伺服器支援虛擬私人雲端的端點政策。端點政策是一種基於 IAM 資源的政策，您可以將其連接到 VPC 端點，以控制哪些 AWS 主體可以使用端點存取您的服務。 AWS 如需詳細資訊，請參閱使用端點策略控制對 VPC 端點的存取。

若要使用端點策略，您必須先建立介面端點。您可以使用無伺服器主控台或 OpenSearch 無伺服器 API 建立介面端點。 OpenSearch 建立介面端點之後，您需要將端點原則新增至端點。如需詳細資訊，請參閱使用界面端點存取 Amazon OpenSearch 無伺服器 (AWS PrivateLink)。

> **Note**
>
> 您無法直接在 OpenSearch 服務主控台中定義端點策略。

端點策略不會覆寫或取代您可能已設定的其他身分型政策、以資源為基礎的策略、網路策略或資料存取策略。如需更新端點策略的詳細資訊，請參閱使用端點策略控制對 VPC 端點的存取。

依預設，端點原則會授與 VPC 端點的完整存取權。

```
{
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": "*",
            "Action": "*",
            "Resource": "*"
        }
    ]
}
```

雖然預設 VPC 端點原則授與完整端點存取權，但您可以設定 VPC 端點原則以允許存取特定角色和使用者。若要這麼做，請參閱下列範例：

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": [
                    "123456789012",
                    "987654321098"
                ]
            },
            "Action": "*",
            "Resource": "*"
        }
    ]
}
```

您可以指定要包含在 VPC 端點策略中作為條件元素的 OpenSearch 無伺服器集合。若要這麼做，請參閱下列範例：

```
{
    "Version": "2012-10-17",
    "Statement": [
```

```
        {
            "Effect": "Allow",
            "Principal": "*",
            "Action": "*",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:CollectionName": [
                        "coll-abc"
                    ]
                }
            }
        }
    ]
}
```

您可以在 VPC 端點原則中使用 SAML 身分識別來判斷 VPC 端點存取。您必須在 VPC 端點策略(*)的主體區段中使用萬用字元。若要這麼做，請參閱下列範例：

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": "*",
            "Action": "*",
            "Resource": "*",
            "Condition": {
                "ForAnyValue:StringEquals": {
                    "aws:SamlGroups": [
                        "saml/123456789012/idp123/group/football",
                        "saml/123456789012/idp123/group/soccer",
                        "saml/123456789012/idp123/group/cricket"
                    ]
                }
            }
        }
    ]
}
```

此外，您可以設定端點原則以包含特定的 SAML 主體原則。若要這麼做，請參閱下列內容：

```
{
```

```
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": "*",
            "Action": "*",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:SamlPrincipal": [
                        "saml/123456789012/idp123/user/user1234"]
                    }
                }
            }
        ]
    }
```

如需將 SAML 身份驗證與 Amazon 無伺服器搭配使用的詳細資訊，請參閱適用於 Amazon OpenSearch 無伺服器的 SAML 身份驗證。 OpenSearch

您也可以在相同的 VPC 端點政策中包含 IAM 和 SAML 使用者。若要這麼做，請參閱下列範例：

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": "*",
            "Action": "*",
            "Resource": "*",
            "Condition": {
                "ForAnyValue:StringEquals": {
                    "aws:SamlGroups": [
                        "saml/123456789012/idp123/group/football",
                        "saml/123456789012/idp123/group/soccer",
                        "saml/123456789012/idp123/group/cricket"
                    ]
                }
            }
        },
        {
            "Effect": "Allow",
            "Principal": {
```

```
                "AWS": [
                    "123456789012"
                ]
            },
            "Action": "*",
            "Resource": "*"
        }
    ]
}
```

考量事項

在為 OpenSearch 無伺服器設定介面端點之前，請考慮下列事項：

- OpenSearch 無伺服器支援透過介面端點呼叫所有支援OpenSearch 的 API 作業 (非組態 API 作業)。
- 建立 OpenSearch 無伺服器的介面端點之後，您仍需要將其包含在網路存取原則中，才能存取無伺服器集合。
- 依預設，允許透過介面端點完整存取 OpenSearch 無伺服器。您可以將安全群組與端點網路介面建立關聯，以透過介面端點控制傳送至 OpenSearch 無伺服器的流量。
- 每個端點最多 AWS 帳戶 可以有 50 個 OpenSearch 無伺服器 VPC 端點。
- 如果您在網路原則中啟用公用網際網路存取集合的 API 或儀表板，則任何 VPC 和公用網際網路都可以存取您的集合。
- 如果您位於內部部署和 VPC 以外，則無法直接將 DNS 解析器用於 OpenSearch 無伺服器 VPC 端點解析。如果您需要 VPN 存取，則 VPC 需要 DNS 代理解析程式供外部用戶端使用。Route 53 提供輸入端點選項，可用於從內部部署網路或其他 VPC 解析對 VPC 的 DNS 查詢。
- OpenSearch 無伺服器建立並附加至 VPC 的私有託管區域由服務管理，但會顯示在您的 Amazon Route 53 資源中，並從您的帳戶中收取費用。
- 如需其他考量，請參閱《AWS PrivateLink 指南》中的考量事項。

必要許可

OpenSearch 無伺服器的 VPC 存取使用下列 AWS Identity and Access Management (IAM) 許可。您可以指定 IAM 條件，將使用者限制在特定集合內。

- `aoss:CreateVpcEndpoint`：建立 VPC 端點。
- `aoss:ListVpcEndpoints`：列出所有 VPC 端點。

- `aoss:BatchGetVpcEndpoint`：查看有關 VPC 端點子集的詳細資訊。
- `aoss:UpdateVpcEndpoint`：修改 VPC 端點。
- `aoss:DeleteVpcEndpoint`：刪除 VPC 端點。

此外，您需要下列 Amazon EC2 和 Route 53 許可，才能建立 VPC 端點。

- `ec2:CreateTags`
- `ec2:CreateVpcEndpoint`
- `ec2:DeleteVpcEndPoints`
- `ec2:DescribeSecurityGroups`
- `ec2:DescribeSubnets`
- `ec2:DescribeVpcEndpoints`
- `ec2:DescribeVpcs`
- `ec2:ModifyVpcEndPoint`
- `route53:AssociateVPCWithHostedZone`
- `route53:ChangeResourceRecordSets`
- `route53:CreateHostedZone`
- `route53:DeleteHostedZone`
- `route53:GetChange`
- `route53:GetHostedZone`
- `route53:ListHostedZonesByName`
- `route53:ListHostedZonesByVPC`
- `route53:ListResourceRecordSets`

建立 OpenSearch 無伺服器的介面端點

您可以使用主控台或 OpenSearch 無伺服器 API 為無伺服 OpenSearch 器建立介面端點。

建立 OpenSearch 無伺服器集合的介面端點

1. 打開 Amazon OpenSearch 服務控制台 https://console.aws.amazon.com/aos/home.
2. 在左側導覽窗格中，展開 Serverless (無伺服器)，然後選擇 VPC endpoints (VPC 端點)。
3. 選擇 Create VPC endpoint (建立 VPC 端點)。

4. 提供端點的名稱。
5. 對於 VPC，請選取您要從中存取 OpenSearch 無伺服器的 VPC。
6. 對於子網路，請選取一個您要從中存取 OpenSearch 無伺服器的子網路。
   - 端點的 IP 位址和 DNS 類型取決於子網路類型
     - 雙堆疊：如果所有子網路同時具有 IPv4 和 IPv6 位址範圍
     - IPv6：如果所有子網路都只有 IPv6 子網路
     - IPv4：如果所有子網路都有 IPv4 位址範圍
7. 對於 Security group (安全群組)，選取要與端點網路介面建立關聯的安全群組。這是一個關鍵步驟，其中您需限制正授權進入端點之傳入流量的連接埠、通訊協定和來源。請確定安全群組規則允許將使用 VPC 端點的資源與 OpenSearch 無伺服器通訊，以便與端點網路介面進行通訊。
8. 選擇建立端點。

若要使用 OpenSearch 無伺服器 API 建立 VPC 端點，請使用指`CreateVpcEndpoint`令。

> **Note**
>
> 建立端點後，請記下其 ID (例如 `vpce-050f79086ee71ac05`)。若要提供端點存取權給您的集合，您必須在一個或多個網路存取政策中包含此 ID。

下一步：授予端點存取權給集合

建立介面端點後，您必須透過網路存取政策，為其提供集合的存取權。如需詳細資訊，請參閱 the section called “網路存取”。

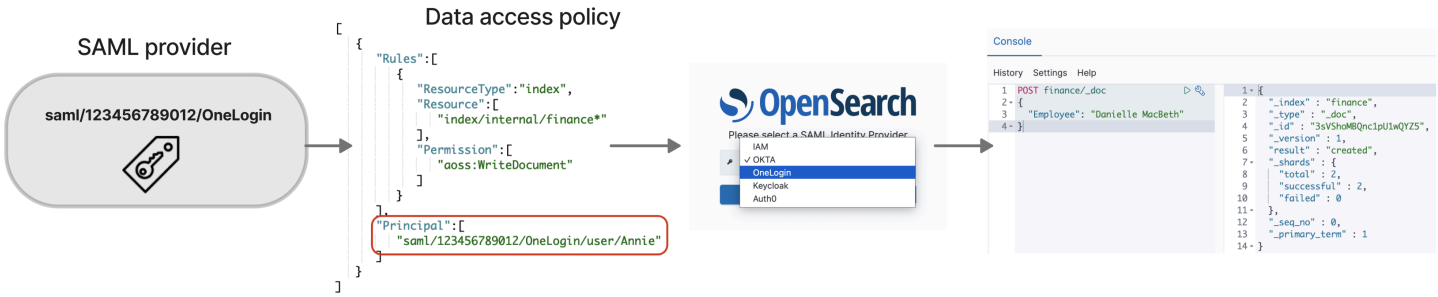
SAML適用於 Amazon OpenSearch 無伺服器的身分

使用適用於 Amazon OpenSearch 無伺服器的身分SAML驗證，您可以使用現有的身分供應商為無伺服器集合的 OpenSearch 儀表板端點提供單一登入 (SSO)。

SAML驗證可讓您使用第三方身分識別提供者登入 OpenSearch 儀表板，以索引和搜尋資料。OpenSearch 無伺服器支援使用 SAML 2.0 標準的提供者，例如IAM身分識別中心、Okta、金鑰遮罩、作用中目錄同盟服務 (AD FS) 和 Auth0。您可以設定IAM身分識別中心， OneLogin以同步處理來自其他身分識別來源 (例如 Okta 和 Microsoft Entra ID) 的使用者和群組。如需 Identity Center 支援的身分識IAM別來源清單及其設定步驟，請參閱IAM身分識別中心使用者指南中的入門教學課程。

> **Note**
>
> SAML驗證僅適用於透過 Web 瀏覽器存取 OpenSearch 儀表板。已驗證的使用者只能透過 OpenSearch 儀表板中的開發工具向 OpenSearch API作業發出要求。您的SAML憑據不允許您直接向 OpenSearch API操作發出HTTP請求。

若要設定SAML驗證，請先設定SAML身分識別提供者 (IdP)。然後，您可以將該 IdP 中的一個或多個使用者納入資料存取政策中。此政策會向它授予集合和/或索引的某些許可。然後，使用者可以登入 OpenSearch 儀表板並執行資料存取原則中允許的動作。



主題

- 考量事項
- 必要許可
- 建立SAML提供者 (主控台)
- 存取 OpenSearch 儀表板
- 授與收集資料的SAML身分存取權
- 建立SAML提供者 (AWS CLI)
- 檢視SAML提供者
- 更新SAML提供者
- 刪除SAML提供者

考量事項

設定SAML驗證時，請考慮下列事項：

- 不支援已簽署和已加密的請求。
- 不支援已加密的聲明。

- 不支援 IdP 啟動的身分驗證和登出。
- 如SAML果是非IAM身分識別 SCP (例如 Amazon OpenSearch 無伺服器SAML和 Amazon 服務的基本內部使用者授權)，則不適用或評估 OpenSearch 服務控制政策 ()。

必要許可

SAML OpenSearch 無伺服器的驗證使用下列項目 AWS Identity and Access Management （IAM）權限：

- `aoss:CreateSecurityConfig`— 建立提SAML供者。
- `aoss:ListSecurityConfig`— 列出當前帳戶中的所有SAML提供商。
- `aoss:GetSecurityConfig`— 查看SAML提供者信息。
- `aoss:UpdateSecurityConfig`— 修改指定的SAML提供者組態，包括中XML繼資料。
- `aoss:DeleteSecurityConfig`— 刪除提SAML供者。

下列身分型存取政策讓使用者可以管理所有 IdP 組態：

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "aoss:CreateSecurityConfig",
                "aoss:DeleteSecurityConfig",
                "aoss:GetSecurityConfig",
                "aoss:UpdateSecurityConfig",
                "aoss:ListSecurityConfigs"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

請注意，`Resource` 元素必須是萬用字元。

建立SAML提供者 (主控台)

這些步驟說明如何建立SAML提供者。這可讓使SAML用服務提供者 (SP) 起始的 OpenSearch 儀表板驗證進行驗證。不支援 IdP 啟動的身分驗證。

啟用 OpenSearch 儀表板的SAML驗證

1. 在https://console.aws.amazon.com/aos/家中登錄 Amazon OpenSearch 服務控制台。
2. 在左側導覽面板上，展開「無伺服器」，然後選擇「SAML驗證」。
3. 選擇新增SAML提供者。
4. 提供提供者的名稱和描述。

> **Note**
> 您指定的名稱可公開存取，當使用者登入 OpenSearch 儀表板時，會出現在下拉式功能表中。確保名稱易於識別，並且不會洩露有關您身分提供者的敏感資訊。

5. 在「設定您的 IdP」下，複製宣告取用者服務 () ACS。URL
6. 使用您剛剛複製的來設定您的身分識別提供者。ACS URL術語和步驟因提供者而異。請咨詢供應商文件。

   例如，在 Okta 中，您建立了「SAML2.0 Web 應用程式」，並指定ACSURL為「單一登入」URL、「收件者 URL」和「目URL的地」。對於 Auth0，您可以在允許的回呼URLs中指定它。
7. 如果 IdP 有此值的欄位，請提供對象限制。受眾限制是SAML斷言中的一個值，用於指定斷言的目的。對於 OpenSearch 無伺服器，請指定`aws:opensearch:<aws account id>`。例如：`aws:opensearch:123456789012`。

   對象限制欄位的名稱因提供者而異。對於奧克塔，它是受眾URI（SP 實體 ID）。IAM身分識別中心是應用程式SAML受眾。
8. 如果您使用的是IAM身分識別中心，您還需要指定下列屬性對應:`Subject=${user:name}`, 格式為`unspecified`.
9. 設定身分提供者之後，它會產生 IdP 中繼資料檔案。此XML檔案包含提供者的相關資訊，例如TLS憑證、單一登入端點和身分識別提供者的實體 ID。

   複製 IdP 中繼資料檔案中的文字，並將其貼到 Provide metadata from your IdP (透過 IdP 提供中繼資料) 欄位下方。或者，選擇「從XML檔案匯入」並上傳檔案。中繼資料檔案如下所示：

```
<?xml version="1.0" encoding="UTF-8"?>
<md:EntityDescriptor entityID="entity-id"
 xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata">
  <md:IDPSSODescriptor WantAuthnRequestsSigned="false"
 protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
    <md:KeyDescriptor use="signing">
      <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:X509Data>
          <ds:X509Certificate>tls-certificate</ds:X509Certificate>
        </ds:X509Data>
      </ds:KeyInfo>s
    </md:KeyDescriptor>
    <md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified</
md:NameIDFormat>
    <md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress</
md:NameIDFormat>
    <md:SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-
POST" Location="idp-sso-url"/>
    <md:SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-
Redirect" Location="idp-sso-url"/>
  </md:IDPSSODescriptor>
</md:EntityDescriptor>
```

10. 將 [自訂使用者 ID] 屬性欄位保持空白，以使用SAML宣告的`NameID`元素作為使用者名稱。如果您的聲明不使用此標準元素，而是將使用者名稱作為自訂屬性，請在此處指定該屬性。屬性區分大小寫。僅支援單一使用者屬性。

    下列範例會顯示SAML宣告`NameID`中的覆寫屬性：

```
<saml2:Attribute Name="UserId" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-
format:basic">
  <saml2:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:type="xs:string">annie</saml2:AttributeValue>
</saml2:Attribute>
```

11. (選用) 在 Group attribute (群組屬性) 欄位中指定自訂屬性，例如 `role` 或 `group`。僅支援單一群組屬性。沒有預設的群組屬性。如果未指定群組屬性，資料存取政策只能包含使用者主體。

    下面的例子顯示了SAML斷言中的 group 屬性：

```
<saml2:Attribute Name="department"
 NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
    <saml2:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xsi:type="xs:string">finance</saml2:AttributeValue>
</saml2:Attribute>
```

12. 依預設， OpenSearch 儀表板會在 24 小時後將使用者登出。您可以透過指定OpenSearch 儀表板逾時，將此值設定為 1 到 12 小時 (15 到 720 分鐘) 之間的任何數字。如果您嘗試將逾時設定為等於或小於 15 分鐘，您的工作階段將重設為一小時。
13. 選擇建立SAML提供者。

存取 OpenSearch 儀表板

設定提供者之後，與該SAML提供者關聯的所有使用者和群組都可以導覽至 OpenSearch 儀表板端點。儀表板URL具有所有集合的格式*collection-endpoint*/_dashboards/。

如果您已SAML啟用，請選取 AWS Management Console 將您導向至 IdP 選擇頁面，您可以在其中使用您的SAML認證登入。首先，使用下拉式清單選取身分提供者：

然後使用 IdP 憑證登入。

如果您尚未SAML啟用，請在 AWS Management Console 指示您以IAM使用者或角色的身分登入，但沒有選項SAML。

授與收集資料的SAML身分存取權

建立SAML提供者之後，您仍然需要授與基礎使用者和群組存取集合中資料的權限。您可以透過資料存取政策授予存取權。在您提供使用者存取權之前，他們將無法讀取、寫入或刪除集合內的任何資料。

要授予訪問權限，請創建數據訪問策略，並在`Principal`聲明IDs中指定您的SAML用戶和/或組：

```
[
   {
      "Rules":[
       ...
```

```
      ],
      "Principal":[
         "saml/987654321098/myprovider/user/Shaheen",
         "saml/987654321098/myprovider/group/finance"
      ]
   }
]
```

您可以授予對集合、索引或兩者的存取權。如果您希望不同的使用者擁有不同的許可，請建立多個規則。如需可用許可的清單，請參閱支援的政策許可。如需有關如何格式化存取政策的資訊，請參閱政策語法。

建立SAML提供者 (AWS CLI)

若要使用 OpenSearch 無伺服器建立SAML提供者API，請傳送要CreateSecurityConfig求：

```
aws opensearchserverless create-security-config \
    --name myprovider \
    --type saml \
    --saml-options file://saml-auth0.json
```

將包括`saml-options`中繼資料XML在內的 .json 檔案中指定為索引鍵值對映。中繼資料XML必須編碼為JSON逸出字串。

```
{
   "sessionTimeout": 70,
   "groupAttribute": "department",
   "userAttribute": "userid",
   "metadata": "<EntityDescriptor xmlns=\"urn:oasis:names:tc:SAML:2.0:metadata
\" ... ... ... IDPSSODescriptor>\r\n<\/EntityDescriptor>"
}
```

檢視SAML提供者

下列ListSecurityConfigs要求會列出您帳戶中的所有SAML供應商：

```
aws opensearchserverless list-security-configs --type saml
```

要求會傳回所有現有提SAML供者的相關資訊，包括身分識別提供者所產生的完整 IdP 中繼資料：

```
{
   "securityConfigDetails": [
      {
         "configVersion": "MTY2NDA1MjY4NDQ5M18x",
         "createdDate": 1664054180858,
         "description": "Example SAML provider",
         "id": "saml/123456789012/myprovider",
         "lastModifiedDate": 1664054180858,
         "samlOptions": {
            "groupAttribute": "department",
            "metadata": "<EntityDescriptor xmlns=\"urn:oasis:names:tc:SAML:2.0:metadata
\" ... ... ... IDPSSODescriptor>\r\n<\/EntityDescriptor>",
            "sessionTimeout": 120,
            "userAttribute": "userid"
         }
      }
   ]
}
```

若要檢視特定提供者的相關詳細資訊 (包括未來更新的 `configVersion`)，請傳送 `GetSecurityConfig` 請求。

更新SAML提供者

若要使用 OpenSearch 無伺服器主控台更新SAML提供者，請選擇SAML驗證，選取您的身分識別提供者，然後選擇編輯。您可以修改所有欄位，包括中繼資料和自訂屬性。

若要透過 OpenSearch 無伺服器更新提供者API，請傳送UpdateSecurityConfig要求並包含要更新之原則的識別碼。您還必須包含組態版本，您可以使用 `ListSecurityConfigs` 或 `GetSecurityConfig` 命令擷取該版本。將最新的版本納入其中，可確保您不會意外覆寫其他人所做的變更。

下列要求會更新提供者的SAML選項：

```
aws opensearchserverless update-security-config \
    --id saml/123456789012/myprovider \
    --type saml \
    --saml-options file://saml-auth0.json \
    --config-version MTY2NDA1MjY4NDQ5M18x
```

將您的SAML組態選項指定為 .json 檔案中的索引鍵值對映。

> **Important**
>
> 對SAML選項的更新不是增量的。如果您在進行更新時未指定 `SAMLOptions` 物件中的參數值，則會以空白值覆寫現有值。例如，如果目前的組態包含 `userAttribute` 的值，然後您進行更新但不包含此值，則系統會將該值從組態中移除。透過呼叫 `GetSecurityConfig` 操作進行更新之前，請確保您知道現有值為何。

刪除SAML提供者

當您刪除SAML提供者時，對資料存取原則中關聯使用者和群組的任何參考將不再起作用。為避免混淆，建議您先移除存取政策中對端點的所有參考，然後再刪除該端點。

若要使用 OpenSearch 無伺服器主控台刪除SAML提供者，請選擇 [驗證]，選取提供者，然後選擇 [刪除]。

若要透過 OpenSearch 無伺服器刪除提供者API，請傳送要DeleteSecurityConfig求：

```
aws opensearchserverless delete-security-config --id saml/123456789012/myprovider
```

適用於 Amazon OpenSearch 無伺服器的合規驗證

第三方稽核員會評估 Amazon OpenSearch 無伺服器的安全性和合規性，作為多個 AWS 合規計劃的一部分。這些程式包括SOCPCI、和HIPAA。

若要瞭解 AWS 服務 是否屬於特定規範遵循方案的範圍內，請參閱AWS 服務 遵循規範計劃方案中的，並選擇您感興趣的合規方案。如需一般資訊，請參閱AWS 規範計劃AWS。

您可以使用下載第三方稽核報告 AWS Artifact。如需詳細資訊，請參閱下載中的報告中的 AWS Artifact。

您在使用時的合規責任取決 AWS 服務 於資料的敏感性、公司的合規目標以及適用的法律和法規。AWS 提供下列資源以協助遵循法規：

- 安全性與合規性快速入門指南 — 這些部署指南討論架構考量，並提供部署以安全性和合規性 AWS 為重點的基準環境的步驟。
- 在 Amazon Web Services 上進行HIPAA安全與合規架構 — 本白皮書說明公司如何使用建立符合資格的應 AWS 用程HIPAA式。

> **Note**
>
> 並非所有 AWS 服務 人都HIPAA符合資格。如需詳細資訊，請參閱合HIPAA格服務參考。

- AWS 合規資源AWS — 此工作簿和指南集合可能適用於您的產業和所在地。
- AWS 客戶合規指南 — 透過合規的角度瞭解共同的責任模式。這份指南總結了在多個架構 (包括美國國家標準 AWS 服務 與技術研究所 (NIST)、支付卡產業安全標準委員會 () 和國際標準化組織 ()PCI) 中保護安全控制指引的最佳做法，並對應至安全控制措施。ISO
- 使用AWS Config 開發人員指南中的規則評估資源 — 此 AWS Config 服務會評估您的資源組態符合內部實務、產業準則和法規的程度。
- AWS Security Hub— 這 AWS 服務 提供了內部安全狀態的全面視圖 AWS。Security Hub 使用安全控制，可評估您的 AWS 資源並檢查您的法規遵循是否符合安全業界標準和最佳實務。如需支援的服務和控制清單，請參閱 Security Hub controls reference。
- Amazon GuardDuty — 透過監控環境中的 AWS 帳戶可疑和惡意活動，藉此 AWS 服務 偵測您的工作負載、容器和資料的潛在威脅。 GuardDuty 可協助您因應各種合規性需求 PCIDSS，例如符合特定合規性架構所要求的入侵偵測需求。
- AWS Audit Manager— 這 AWS 服務 有助於您持續稽核您的 AWS 使用情況，以簡化您管理風險的方式，以及遵守法規和業界標準的方式。

標記 Amazon OpenSearch 無伺服器集合

標籤可讓您將任意資訊指派給 Amazon OpenSearch 無伺服器集合，以便對該資訊進行分類和篩選。標籤是您指派的中繼資料標籤或 AWS 指派給 AWS 資源。

每個標籤皆包含鍵與值。對於您指派的標籤，您可以定義鍵與值。例如，您可以將鍵定義為 `stage`，將資源的值定義為 `test`。

您可以使用標籤執行下列操作：

- 識別和組織您的 AWS 的費用。許多 AWS 服務支援標記，因此您可以將相同標籤指派給來自不同服務的資源，以指出資源是相關的。例如，您可以將相同的標籤指派給指派給 Amazon OpenSearch 服務網域的 OpenSearch 無伺服器集合。

在 OpenSearch 無伺服器中，主要資源是集合。您可以使用 OpenSearch 服務主控台 AWS CLI、OpenSearch 無伺服器API作業，或 AWS SDKs以新增、管理和移除系列中的標籤。

必要許可

OpenSearch 無伺服器使用下列項目 AWS Identity and Access Management Access Analyzer (IAM) 標記集合的權限：

- `aoss:TagResource`
- `aoss:ListTagsForResource`
- `aoss:UntagResource`

處理標籤 (主控台)

主控台是標記集合的最簡單方法。

建立標籤 (主控台)

1. 在https://console.aws.amazon.com/aos/家中登錄 Amazon OpenSearch 服務控制台。
2. 展開左側導覽窗格中的 Serverless (無伺服器)，然後選擇 Collections (集合)。
3. 選取您要新增標籤的集合，然後前往 Tags (標籤) 索引標籤。
4. 選擇 Manage (管理) 和 Add new tag (新增標籤)。
5. 輸入標籤索引鍵和選用的值。
6. 選擇 Save (儲存)。

若要刪除標籤，請按照同樣的步驟進行，然後在 Manage tags (管理標籤) 頁面上選擇 Remove (移除)。

如需有關使用主控台處理標籤的詳細資訊，請參閱 AWS 管理主控台入門指南。

使用標籤 (AWS CLI)

若要使用標記集合 AWS CLI，傳送TagResource請求：

```
aws opensearchserverless tag-resource
  --resource-arn arn:aws:aoss:us-east-1:123456789012:collection/my-collection
  --tags Key=service,Value=aoss Key=source,Value=logs
```

使用以下ListTagsForResource指令檢視集合的現有標籤：

```
aws opensearchserverless list-tags-for-resource
  --resource-arn arn:aws:aoss:us-east-1:123456789012:collection/my-collection
```

使用以下UntagResource命令從集合中刪除標籤：

```
aws opensearchserverless untag-resource
  --resource-arn arn:aws:aoss:us-east-1:123456789012:collection/my-collection
  --tag-keys service
```

Amazon OpenSearch 無伺服器支援的操作和外掛程式

Amazon OpenSearch 無伺服器支援各種 OpenSearch 外掛程式，以及中 OpenSearch提供的索引、搜尋和中繼資料 API 操作的子集。您可以將許可包含在資料存取政策內資料表左欄中，以限制對特定操作的存取。

主題

- 支援的 OpenSearch API 作業和權限
- 支持的 OpenSearch 插件

支援的 OpenSearch API 作業和權限

下表列出 OpenSearch 無伺服器支援的 API 作業，以及其對應的資料存取原則權限：

資料存取政策許可	OpenSearch API 作業	說明和警告
`aoss:CreateIndex`	PUT <index>	建立索引。如需詳細資訊，請參閱 Create index (建立索引)。 **Note** 此權限也適用於使用 OpenSearch 儀表板上的範例資料建立索引。

資料存取政策許可	OpenSearch API 作業	說明和警告
`aoss:DescribeIndex`	• GET <index> • GET <index>/_mapping • GET <index>/_mappings • GET <index>/_setting • GET <index>/_setting/<setting> • GET <index>/_settings • GET <index>/_settings/<setting> • GET _cat/indices • GET _mapping • GET _mappings • GET _resolve/index/<index> • 頭 <index>	描述索引。如需詳細資訊，請參閱下列資源： • 取得索引 • 取得映射 • 取得設定 • 索引已存在 • CAT 索引（響應不包括`health`或`status`字段。）
`aoss:WriteDocument`	• 刪除 <index>/_文件/<id> • POST <index>/_bulk • POST <index>/_create/<id> (僅適用於搜尋集合類型) • POST <index>/_doc • POST <index>/_update/<id> (僅適用於搜尋集合類型) • POST _bulk • PUT <index>/_create/<id> (僅適用於搜尋集合類型) • PUT <index>/_doc/<id> (僅適用於搜尋集合類型)	編寫和更新文件。如需詳細資訊，請參閱下列資源： • 大批 • 為資料編製索引 **Note** 僅允許對類型為 SEARCH 的集合執行某些操作。如需詳細資訊，請參閱 the section called “選擇集合類型”。

資料存取政策許可	OpenSearch API 作業	說明和警告
`aoss:ReadDocument`	• GET <index>/_analyze • GET <index>/_doc/<id> • GET <index>/_explain/<id> • GET <index>/_mget • GET <index>/_source/<id> • GET <index>/_count • GET <index>/_field_caps • GET <index>/_msearch • GET <index>/_rank_eval • GET <index>/_search • GET <index>/_validate/<query> • GET _analyze • GET _field_caps • GET _mget • GET _search • HEAD <index>/_doc/<id> • HEAD <index>/_source/<id> • POST <index>/_analyze • POST <index>/_explain/<id> • POST <index>/_count • POST <index>/_field_caps • POST <index>/_rank_eval • POST <index>/_search • POST _analyze • POST _field_caps • POST _search	閱讀文件。如需詳細資訊，請參閱下列資源： • 執行文字分析 • 取得文件 • Count (計數) • 查詢 DSL • 將評估排名 • 分析 API • 說明

資料存取政策許可	OpenSearch API 作業	說明和警告
`aoss:DeleteIndex`	DELETE <target>	刪除索引。如需詳細資訊，請參閱 Delete index (刪除索引)。
`aoss:UpdateIndex`	• POST _mapping • POST <index>/_mapping/ • POST <index>/_mappings/ • POST <index>/_setting • POST <index>/_settings • POST _setting • POST _settings • PUT _mapping • PUT <index>/_mapping • PUT <index>/_mappings/ • PUT <index>/_setting • PUT <index>/_settings • PUT _setting • PUT _settings	更新索引設定。如需詳細資訊，請參閱下列資源： • 映射 • 更新設定
`aoss:CreateCollectionItems`	POST _aliases	建立索引別名。如需詳細資訊，請參閱 Create aliases (建立別名)。

資料存取政策許可	OpenSearch API 作業	說明和警告
`aoss:DescribeCollectionItems`	• GET <index>/_alias/<alias> • GET _alias • GET _alias/<alias> • GET _cat/aliases • GET _cat/templates • GET _cat/templates/<template_name> • GET _component_template • GET _component_template/<component-template> • GET _index_template • GET _index_template/<index-template> • HEAD _alias/<alias> • HEAD _component_template/<component-template> • HEAD _index_template/<name> • HEAD <index>/_alias/<alias>	描述別名和索引範本。如需詳細資訊，請參閱下列資源： • 管理別名 • 索引範本

資料存取政策許可	OpenSearch API 作業	說明和警告
`aoss:UpdateCollectionItems`	• POST <index>/_alias/<alias> • POST <index>/_aliases/<alias> • POST _component_template/<component-template> • POST _index_template/<index-template> • PUT <index>/_alias/<alias> • PUT <index>/_aliases/<alias> • PUT _component_template/<component-template> • PUT _index_template/<index-template>	更新別名和索引範本。如需詳細資訊，請參閱下列資源： • 索引別名 • 索引範本
`aoss:DeleteCollectionItems`	• DELETE <index>/_alias/<alias> • DELETE _component_template/<component-template> • DELETE _index_template/<index-template> • DELETE <index>/_aliases/<alias>	刪除別名和索引範本。如需詳細資訊，請參閱下列資源： • 刪除別名 • 刪除範本

支持的 OpenSearch 插件

OpenSearch 無伺服器集合已預先封裝社群的下列外掛程式 OpenSearch。Serverless 會為您自動部署和管理外掛程式。

分析外掛程式

- ICU 分析
- 日文 (kuromoji) 分析
- 韓語 (Nori) 分析
- 語音分析
- 智慧型中文分析

- Stempel 波蘭文分析
- 烏克蘭文分析

映射器外掛程式

- 映射器大小
- 映射器 Murmur3
- 映射器註釋文字

指令碼編寫外掛程式

- Painless
- 運算式
- Mustache

此外， OpenSearch 無伺服器包含所有以模組形式出貨的外掛程式。

監控 Amazon OpenSearch 無伺服器

監控是維護 Amazon OpenSearch 無伺服器和其他 AWS 解決方案的可靠性、可用性和效能的重要組成部分。 AWS 提供下列監控工具來監視 OpenSearch 無伺服器、在發生錯誤時回報，並在適當時採取自動處理行動：

- Amazon 會即時 CloudWatch監控您的 AWS 資源和執行 AWS 的應用程式。您可以收集和追蹤指標、建立自訂儀板表，以及設定警示，在特定指標達到您指定的閾值時通知您或採取動作。

  例如，您可以 CloudWatch 追蹤 Amazon EC2 執行個體的 CPU 使用率或其他指標，並在需要時自動啟動新執行個體。如需詳細資訊，請參閱 Amazon CloudWatch 使用者指南。
- AWS CloudTrail 會擷取來自或代表 AWS 帳戶發出的 API 呼叫和相關事件。它會將日誌檔案交付到您指定的 Amazon S3 儲存貯體。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。如需詳細資訊，請參閱《 使用者指南》AWS CloudTrail。
- Amazon EventBridge 提供近乎即時的系統事件串流，描述您 OpenSearch 服務網域中的變更。您可以建立監視某些事件的規則，並在發生這些事件 AWS 服務 時觸發其他事件的自動動作。如需詳細資訊，請參閱 Amazon EventBridge 使用者指南。

使用 Amazon 監控 OpenSearch 無伺服器 CloudWatch

您可以使用 CloudWatch收集原始資料並將其處理為可讀且近乎即時的指標來監控 Amazon OpenSearch 無伺服器。這些統計資料會保留 15 個月，以便您存取歷史資訊，並更清楚 Web 應用程式或服務的執行效能。

您也可以設定留意特定閾值的警示，當滿足這些閾值時傳送通知或採取動作。如需詳細資訊，請參閱 Amazon CloudWatch 使用者指南。

OpenSearch 無伺服器會在AWS/AOSS命名空間中報告下列量度。

指標	描述
ActiveCollection	指出集合是否處於作用中狀態。值 1 表示集合處於 ACTIVE 狀態。系統會在成功建立集合時發出這個值，並在您刪除集合為止保持為 1。指標的值不能為 0。 相關統計資料：上限 維度：ClientId、CollectionId 、CollectionName 頻率：60 秒
DeletedDocuments	已刪除的文件總數。 相關統計資料：平均數、總和 維度：ClientId、CollectionId 、CollectionName 、IndexId、IndexName 頻率：60 秒
IndexingOCU	用來擷取收集資料的 OpenSearch 運算單位 (OCU) 數目。此指標適用於帳戶層級。 相關統計資料：總和 尺寸: ClientId 頻率：60 秒

指標	描述
IngestionDataRate	集合或索引的索引編製速率 (以每秒 GiB 為單位)。此指標僅適用於大量編製索引請求。 相關統計資料：總和 維度：ClientId、CollectionId 、CollectionName 、IndexId、IndexName 頻率：60 秒
IngestionDocumentErrors	擷取集合或索引期間的文件錯誤總數。成功發出大量編製索引請求後，撰寫者會處理該請求，並針對請求內所有失敗的文件發出錯誤。 相關統計資料：總和 維度：ClientId、CollectionId 、CollectionName 、IndexId、IndexName 頻率：60 秒
IngestionDocumentRate	文件擷取至集合或索引的每秒速率。此指標僅適用於大量編製索引請求。 相關統計資料：總和 維度：ClientId、CollectionId 、CollectionName 、IndexId、IndexName 頻率：60 秒

指標	描述
IngestionRequestErrors	要求集合發生錯誤的大量索引總數。 OpenSearch 當大量索引要求因任何原因 (例如驗證或可用性問題) 而失敗時，無伺服器會發出此量度。 相關統計資料：總和 維度：ClientId、CollectionId 、CollectionName 頻率：60 秒
IngestionRequestLatency	大量寫入集合操作的延遲 (以秒為單位)。 相關統計資料：下限、上限、平均數 維度：ClientId、CollectionId 、CollectionName 頻率：60 秒
IngestionRequestRate	集合接收的大量寫入操作總數。 相關統計資料：下限、上限、平均數 維度：ClientId、CollectionId 、CollectionName 頻率：60 秒
IngestionRequestSuccess	成功在集合中執行索引編製操作的總數。 相關統計資料：總和 維度：ClientId、CollectionId 、CollectionName 頻率：60 秒

指標	描述
SearchableDocuments	集合或索引中可搜尋文件的總數。 相關統計資料：總和 維度：ClientId、CollectionId 、CollectionName 、IndexId、IndexName 頻率：60 秒
SearchRequestErrors	集合每分鐘的查詢錯誤總數。 相關統計資料：總和 維度：ClientId、CollectionId 、CollectionName 頻率：60 秒
SearchRequestLatency	針對集合完成搜尋操作所需的平均時間 (以毫秒為單位)。 相關統計資料：下限、上限、平均數 維度：ClientId、CollectionId 、CollectionName 頻率：60 秒
SearchOCU	用於搜尋收集資料的 OpenSearch 運算單位 (OCU) 數目。此指標適用於帳戶層級。 相關統計資料：總和 尺寸: ClientId 頻率：60 秒

指標	描述
SearchRequestRate	集合每分鐘的搜尋請求總數。 相關統計資料：平均數、上限、總和 維度：ClientId、CollectionId 、CollectionName 頻率：60 秒
StorageUsedInS3	使用的 Amazon S3 儲存量 (以位元組為單位)。 OpenSearch 無伺服器會將索引資料存放在 Amazon S3 中。您必須在一分鐘內選取期間，才能取得準確的值。 相關統計資料：總和 維度：ClientId、CollectionId 、CollectionName 、IndexId、IndexName 頻率：60 秒
2xx, 3xx, 4xx, 5xx	產生指定 HTTP 回應碼 (2xx、3xx、4xx、5xx) 的集合請求數。 相關統計資料：總和 維度：ClientId、CollectionId 、CollectionName 頻率：60 秒

使用記錄 OpenSearch 無伺服器 API 呼叫 AWS CloudTrail

Amazon OpenSearch 無伺服器與服務整合 AWS CloudTrail，該服務可提供無伺服器中使用者、角色或 AWS 服務所採取的動作記錄。

CloudTrail 擷取 OpenSearch 無伺服器作為事件的所有 API 呼叫。擷取的呼叫包括來自 Ser OpenSearch vice 主控台「無伺服器」區段的呼叫，以及對 OpenSearch 無伺服器 API 作業的程式碼呼叫。

如果您建立追蹤，您可以啟用持續交付 CloudTrail 事件到 Amazon S3 儲存貯體，包括 OpenSearch 無伺服器事件。如果您未設定追蹤，您仍然可以在 [事件歷程記錄] 中檢視 CloudTrail 主控台中最近的事件。

使用收集的資訊 CloudTrail，您可以判斷向 OpenSearch 無伺服器提出的要求、提出要求的來源 IP 位址、提出要求的人員、提出要求的時間，以及其他詳細資訊。

若要進一步了解 CloudTrail，請參閱使AWS CloudTrail 用者指南。

OpenSearch 無伺服器資訊 CloudTrail

CloudTrail 在您創建帳戶 AWS 帳戶 時啟用。當活動在 OpenSearch 無伺服器中發生時，該活動會與事件歷史記錄中的其他 AWS 服務 CloudTrail 事件一起記錄在事件中。您可以檢視、搜尋和下載您的 AWS 帳戶. 如需詳細資訊，請參閱使用 CloudTrail 事件歷程記錄檢視事件。

如需您 AWS 帳戶的事件 (包括 OpenSearch 無伺服器事件) 的持續記錄，請建立追蹤。追蹤可 CloudTrail 將日誌檔交付到 Amazon S3 儲存貯體。依預設，當您在主控台中建立追蹤時，該追蹤會套用至所有的 AWS 區域。

追蹤記錄來自 AWS 分區中所有區域的事件，並將日誌檔傳送到您指定的 Amazon S3 儲存貯體。此外，您還可以設定其他 AWS 服務，以進一步分析 CloudTrail 記錄中收集的事件資料並採取行動。如需詳細資訊，請參閱下列內容：

- 建立追蹤的概觀
- CloudTrail 支援的服務與整合
- 設定 Amazon SNS 通知 CloudTrail
- 從多個區域接收 CloudTrail 日誌文件並從多個帳戶接收 CloudTrail 日誌文件

所有 OpenSearch 無伺服器動作都會記錄在無伺OpenSearch 服器 API 參考資料中， CloudTrail 並記錄在其中。例如，呼叫`CreateCollection``ListCollections`、和`DeleteCollection`動作會在 CloudTrail 記錄檔中產生項目。

每一筆事件或日誌項目都會包含產生請求者的資訊。身分資訊可協助您判斷：

- 要求是使用根使用者登入資料還是 AWS Identity and Access Management (IAM) 使用者登入資料提出。
- 提出該請求時，是否使用了特定角色或聯合身分使用者的暫時安全憑證。
- 請求是否由其他 AWS 服務提出。

如需詳細資訊，請參閱 CloudTrail userIdentity 元素。

瞭解 OpenSearch 無伺服器記錄檔項目

追蹤是一種組態，可讓事件以日誌檔的形式傳遞到您指定的 Amazon S3 儲存貯體。 CloudTrail 記錄檔包含一或多個記錄項目。

事件代表來自任何來源的單一請求。它包括請求的動作、動作的日期和時間、請求參數等相關資訊。CloudTrail 日誌文件不是公共 API 調用的有序堆棧跟踪，因此它們不會以任何特定順序顯示。

下列範例顯示示範`CreateCollection`動作的 CloudTrail 記錄項目。

```
{
   "eventVersion":"1.08",
   "userIdentity":{
      "type":"AssumedRole",
      "principalId":"AIDACKCEVSQ6C2EXAMPLE",
      "arn":"arn:aws:iam::123456789012:user/test-user",
      "accountId":"123456789012",
      "accessKeyId":"access-key",
      "sessionContext":{
         "sessionIssuer":{
            "type":"Role",
            "principalId":"AIDACKCEVSQ6C2EXAMPLE",
            "arn":"arn:aws:iam::123456789012:role/Admin",
            "accountId":"123456789012",
            "userName":"Admin"
         },
         "webIdFederationData":{

         },
         "attributes":{
            "creationDate":"2022-04-08T14:11:34Z",
            "mfaAuthenticated":"false"
         }
      }
   },
   "eventTime":"2022-04-08T14:11:49Z",
   "eventSource":"aoss.amazonaws.com",
   "eventName":"CreateCollection",
   "awsRegion":"us-east-1",
   "sourceIPAddress":"AWS Internal",
   "userAgent":"aws-cli/2.1.30 Python/3.8.8 Linux/5.4.176-103.347.amzn2int.x86_64 exe/
x86_64.amzn.2 prompt/off command/aoss.create-collection",
```

```
    "errorCode":"HttpFailureException",
    "errorMessage":"An unknown error occurred",
    "requestParameters":{
       "accountId":"123456789012",
       "name":"test-collection",
       "description":"A sample collection",
       "clientToken":"d3a227d2-a2a7-49a6-8fb2-e5c8303c0718"
    },
    "responseElements": null,
    "requestID":"12345678-1234-1234-1234-987654321098",
    "eventID":"12345678-1234-1234-1234-987654321098",
    "readOnly":false,
    "eventType":"AwsApiCall",
    "managementEvent":true,
    "recipientAccountId":"123456789012",
    "eventCategory":"Management",
    "tlsDetails":{
       "clientProvidedHostHeader":"user.aoss-sample.us-east-1.amazonaws.com"
    }
}
```

使用 Amazon 監控 OpenSearch 無伺服器事件 EventBridge

Amazon OpenSearch 服務與 Amazon 集成， EventBridge 以通知您某些事件會影響您的域。來自 AWS 服務的事件會以近乎即時 EventBridge 的方式傳送到。同樣的事件也被發送到 Amazon CloudWatch 活動，Amazon EventBridge 的前身。您可以編寫規則來指出您感興趣的事件，以及當事件符合規則時要採取的自動化動作。您可以自動啟動的動作範例如下：

- 調用函數 AWS Lambda
- 叫用 Amazon EC2 執行命令
- 將事件轉傳至 Amazon Kinesis Data Streams
- 激活 AWS Step Functions 狀態機
- 通知 Amazon SNS 主題或 Amazon SQS 佇列

如需詳細資訊，請參閱 Amazon EventBridge 使用者指南 EventBridge中的開始使用 Amazon。

設定通知

您可以使用「使用AWS 者通知」，在發生 OpenSearch 無伺服器事件時接收通知。事件是 OpenSearch 無伺服器環境變更的指標，例如當您達到 OCU 使用量的上限時。 Amazon EventBridge

接收事件並將通知路由到「通 AWS Management Console 知中心」和您選擇的傳送管道。當事件符合您指定的規則時，便會收到通知。

OpenSearch 運算單位 (OCU) 事件

OpenSearch 無伺服器會在下列其中一個 OCU 相關事件發生 EventBridge 時傳送事件。

OCU 使用量接近最大限制

OpenSearch 當您的搜尋或索引 OCU 使用量達到容量限制的 75% 時，無伺服器會傳送此事件。您的 OCU 使用量是根據您設定的容量限制和目前的 OCU 使用量來計算。

範例

以下是此類型的範例事件 (搜尋 OCU)：

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "OCU Utilization Approaching Max Limit",
  "source": "aws.aoss",
  "account": "123456789012",
  "time": "2016-11-01T13:12:22Z",
  "region": "us-east-1",
  "resources": ["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail": {
    "eventTime" : 1678943345789,
    "description": "Your search OCU usage is at 75% and is approaching the configured
 maximum limit."
  }
}
```

以下是此類型的範例事件 (索引 OCU)：

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "OCU Utilization Approaching Max Limit",
  "source": "aws.aoss",
  "account": "123456789012",
  "time": "2016-11-01T13:12:22Z",
  "region": "us-east-1",
  "resources": ["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
```

```
  "detail": {
    "eventTime" : 1678943345789,
    "description": "Your indexing OCU usage is at 75% and is approaching the configured
 maximum limit."
  }
```

OCU 使用量達到上限

OpenSearch 當您的搜尋或索引 OCU 使用量達到容量限制的 100% 時，無伺服器會傳送此事件。您的 OCU 使用量是根據您設定的容量限制和目前的 OCU 使用量來計算。

範例

以下是此類型的範例事件 (搜尋 OCU)：

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "OCU Utilization Reached Max Limit",
  "source": "aws.aoss",
  "account": "123456789012",
  "time": "2016-11-01T13:12:22Z",
  "region": "us-east-1",
  "resources": ["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail": {
    "eventTime" : 1678943345789,
    "description": "Your search OCU usage has reached the configured maximum limit."
  }
}
```

以下是此類型的範例事件 (索引 OCU)：

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "OCU Utilization Reached Max Limit",
  "source": "aws.aoss",
  "account": "123456789012",
  "time": "2016-11-01T13:12:22Z",
  "region": "us-east-1",
  "resources": ["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail": {
```

```
    "eventTime" : 1678943345789,
    "description": "Your indexing OCU usage has reached the configured maximum limit."
  }
}
```

創建和管理 Amazon OpenSearch 服務域

本章說明如何建立和管理 Amazon OpenSearch 服務網域。網域就是 AWS-佈建等效的開放原始碼 OpenSearch 叢集。建立網域時，您可以指定其設定、執行個體類型、執行個體計數和儲存配置。如需開放原始碼叢集的詳細資訊，請參閱 OpenSearch 說明文件中的建立叢集。

與入門教學課程中的概要說明不同，本章會說明所有選項，並提供相關的參考資訊。您可以使用 OpenSearch 服務主控台的指示來完成每個程序 AWS Command Line Interface (AWS CLI)，或 AWS SDKs.

建立 OpenSearch 服務網域

本節說明如何使用 OpenSearch OpenSearch 服務主控台或使用 AWS CLI 使用`create-domain`命令。

建立 OpenSearch 服務網域 (主控台)

使用下列程序來使用主控台建立 OpenSearch Service 網域。

若要建立 OpenSearch 服務網域 (主控台)

1. 移至https://aws.amazon.com並選擇 [登入主控台]。
2. 在分析下，選擇 Amazon OpenSearch 服務。
3. 選擇 Create domain (建立網域)。
4. 在 Domain name (網域名稱) 中，輸入網域名稱。名稱必須符合下列條件：
   - 唯一的您的帳戶和 AWS 區域
   - 開頭為小寫字母
   - 包含 3 到 28 個之間字元數
   - 只能包含小寫字母 a-z、號碼 0-9 和連字號 (-)
5. 對於網域建立方法，請選擇 [標準建立]。
6. 在「範本」中，請選擇最符合您網域用途的選項：
   - 適用於需要高可用性和效能之工作負載的生產網域。這些網域使用異地同步備份 (有無備用) 和專用主節點，以提高可用性。
   - 用於開發或測試的開發/測試。這些網域可以使用異地同步備份 (有無備用) 或單一可用區域。

> **Important**
>
> 在接下來的頁面中，不同部署類型有不同的選項。這些步驟包括所有選項。

7. 對於部署選項，請選擇備用網域以設定 3-AZ 網域，其中一個區域中的節點會保留為待命。此選項會強制執行一些最佳作法，例如指定的資料節點計數、主節點計數、執行個體類型、複本計數和軟體更新設定。
8. 對於「版本」，請選擇OSS要使用的版本 OpenSearch 或舊版彈性搜尋。我們建議您選擇的最新版本 OpenSearch。如需詳細資訊，請參閱the section called “支援的版本”。

   (選擇性) 如果您選擇網域的 OpenSearch 版本，請選取 [啟用相容性模式]，將其版本 OpenSearch 報告為 7.10，這可讓特定 Elasticsearch 用OSS戶端和外掛程式在連線前檢查版本，以繼續使用服務。
9. 對於 Instance type (執行個體類型)，選擇資料節點的執行個體類型。如需詳細資訊，請參閱the section called “支援的執行個體類型”。

   > **Note**
   >
   > 並非所有可用區域皆支援所有執行個體類型。如果您選擇異地同步備份 (含或不含待命)，建議您選擇目前一代的執行個體類型，例如 R5 或 I3。
10. 請在 Number of nodes (節點類型) 選擇資料節點數目。

    如需最大值，請參閱OpenSearch 服務網域和執行個體配額。單一節點叢集適用於開發和測試，但不應將其用於生產工作負載。如需詳細的指導方針，請參閱 the section called “調整網域大小” 和 the section called “設定多可用區域網域”。
11. 對於存儲類型，選擇 Amazon EBS。此清單中可用的磁碟區類型取決於您選擇的執行個體類型。關於建立特大網域的說明資訊，請參閱 the section called “PB 規模”。
12. 對於EBS儲存區，請設定下列其他設定。根據您選擇的磁碟區類型，部分設定可能不會顯示。

設定	描述
EBS磁碟區類型	選擇一般用途 (SSD)-gp3 和一般用途 (SSD)-gp2，或上一代佈建 IOPS (SSD) 和磁性 (標準)。
EBS每個節點的儲存大小	輸入要附加至每個資料節點的EBS磁碟區大小。

設定	描述
	EBS磁碟區大小是每個節點。您可以計算 OpenSearch Service 網域的叢集總大小，方法是將資料節點數目乘以EBS磁碟區大小。EBS磁碟區的最小和最大大小取決於指定的EBS磁碟區類型和其所連接的執行個體類型。若要深入瞭解，請參閱EBS磁碟區大小限制。
已佈建 IOPS	如果您選取已佈建的IOPSSSD磁碟區類型，請輸入磁碟區可支援的每秒 I/O 作業數目 (IOPS)。

13. (選擇性) 如果您選取gp3磁碟區類型，請展開 [進階設定]，然後指定額外的 IOPS (每個資料節點佈建 3 TiB 磁碟區大小最多 16,000 個) 和輸送量 (每個資料節點佈建的每 3 TiB 磁碟區大小最多可達 1,000 MiB/ 秒)，但需額外付費。如需詳細資訊，請參閱 Amazon OpenSearch 服務定價。
14. (選擇性) 若要啟用UltraWarm 儲存，請選擇啟用 UltraWarm 資料節點。每個執行個體類型都有可處理的儲存量上限。將該數量乘以總計可處理暖儲存的暖資料節點數。
15. (選用) 若要啟用 cold storage (冷儲存)，選擇 Enable cold storage (啟用冷儲存)。您必須啟用 UltraWarm 才能啟用冷庫。
16. 如果您將異地同步備份與待命模式搭配使用，則會啟用三個專用主節點。選擇您想要的主節點類型。如果您選擇不含待命網域的異地同步備份，請選取啟用專用主節點，然後選擇您想要的主節點類型和數目。專用主節點可提高叢集穩定性，也是執行個體計數大於 10 的網域所需要的。我們建議生產網域應具備三個專用主節點。

> **Note**
>
> 您可以為專用主節點及資料節點選擇不同的執行個體類型。例如，您可以針對資料節點選擇一般用途或儲存最佳化執行個體，而不是專用主節點的運算最佳化執行個體。

17. (選擇性) 對於執行中的網域 OpenSearch 或彈性搜尋 5.3 及更新版本，快照組態無關緊要。如需自動拍攝快照的詳細資訊，請參閱the section called “建立索引快照”。
18. 如果您想要使用自訂端點，而不是標準的 `https://search-mydomain-1a2a3a4a5a6a7a8a9a0a9a8a7a.us-east-1.es.amazonaws.com`，請選擇 Enable custom endpoint (啟用自訂端點) 並提供名稱和憑證。如需詳細資訊，請參閱the section called “建立自訂端點”。
19. 在 [網路] 下，選擇 [VPC存取] 或 [公用存取]。如果選擇 Public access (公開存取)，請跳到下一步驟。如果您選擇VPC存取權，請確定您符合先決條件，然後進行下列設定：

設定	描述
VPC	選擇您要使用的虛擬私有雲 (VPC) ID。VPC和網域必須位於相同 AWS 區域，而且您必須選取租VPC用設定為「預設」的租賃。 OpenSearch 服務尚未支援使VPCs用專用租賃服務。
子網	選擇子網路。如果啟用異地同步備份，則必須選擇兩個或三個子網路。OpenSearch 服務會在子網路中放置VPC端點和彈性網路介面。 您必須在子網路中保留足夠數量的 IP 地址給網路界面。如需詳細資訊，請參閱保留VPC子網路中的 IP 位址。
安全群組	選擇一或多個VPC安全性群組，讓您所需的應用程式在網域公開的連接埠 (80 或 443) 和通訊協定 (HTTP或HTTPS) 上存取 OpenSearch Service 網域。如需詳細資訊，請參閱the section called “VPC支持”。
IAM角色	保留預設角色。 OpenSearch 服務使用此預先定義的角色 (也稱為服務連結角色) 來存取您的端點VPC和網路介面，並將VPC端點和網路介面放置在的子網路中VPC。如需詳細資訊，請參閱服務連結角色以進行VPC存取。
IP 位址類型	選擇雙堆疊或IPv4作為您的 IP 位址類型。雙堆疊可讓您跨IPv4IPv6地址類型共用網域資源，並且是建議的選項。如果您將 IP 位址類型設定為雙堆疊，稍後就無法變更位址類型。

20. 啟用或停用精細存取控制：

- 如果您要用IAM於使用者管理，請選擇「設定IAMARN為主要使用者」，然後指ARN定IAM角色的。
- 如果您要使用內部使用者資料庫，請選擇 [建立主要使用者]，然後指定使用者名稱和密碼。

無論您選擇哪個選項，主要使用者都可以存取叢集中的所有索引及所有索引 OpenSearch APIs。如需應選擇哪個選項的指導，請參閱 the section called “重要概念”。

如果您停用精細的存取控制，您仍然可以透過將網域置於VPC、套用限制性存取原則或兩者來控制網域的存取權限。您必須啟用靜 node-to-node 態加密和加密，才能使用精細的存取控制。

> **Note**
>
> 我們強烈建議啟用精細存取控制來保護網域中的資料。精細存取控制可提供叢集、索引、文件和欄位層級安全性。

21. (選擇性) 如果您想要使用 OpenSearch 儀表板的SAML驗證，請選擇啟用SAML驗證並設定網域的SAML選項。如需說明，請參閱 the section called “SAML OpenSearch 儀表板的驗證”。
22. (選擇性) 如果您想要針對 OpenSearch 儀表板使用 Amazon Cognito 身份驗證，請選擇「啟用 Amazon Cognito 身份驗證」。然後選擇您要用於 OpenSearch 儀表板身份驗證的 Amazon Cognito 使用者集區和身分集區。如需建立這些資源的指導方針，請參閱 the section called “用於儀表板的 Amazon Cognito 份 OpenSearch ”。
23. 對於存取原則，請選擇存取原則或設定您自己的原則。如果您選擇建立自訂政策，您可以自行設定，或從另一個網域中匯入。如需詳細資訊，請參閱the section called “身分和存取權管理”。

> **Note**
>
> 如果您已啟用VPC存取權，則無法使用以 IP 為基礎的原則。您反而可以使用安全群組來控制哪些 IP 地址可以存取網域。如需詳細資訊，請參閱the section called “關於網VPC域的存取原則”。

24. (選擇性) 若要求對網域的所有要求都送達HTTPS，請選取所有連至網域的流量都需要HTTPS。若要啟用 node-to-node 加密，請選取 N ode-to-node 加密。如需詳細資訊，請參閱the section called “N ode-to-node 加密技術”。若要啟用靜態資料的加密，請選取啟用靜態資料加密。如果您選擇異地同步備份 (含待命部署) 選項，則會預先選取這些選項。
25. (選擇性) 選取使用 AWS 擁有的密鑰讓 OpenSearch 服務創建一個 AWS KMS 代表您的加密金鑰 (或使用它已建立的金鑰)。否則，請選擇您自己的KMS密鑰。如需詳細資訊，請參閱the section called “靜態加密”。
26. 對於離峰時段，請選取開始時間以排程需要藍/綠部署的服務軟體更新和自動調整最佳化。離峰更新有助於將叢集專用主節點在高流量期間的壓力降至最低。
27. 對於「自動調整」，請選擇是否允許「 OpenSearch 服務」對您的網域建議記憶體相關組態變更，以提高速度和穩定性。如需詳細資訊，請參閱the section called “自動調校”。

    (選擇性) 選取離峰時段以排定週期性時段，在此期間自動微調更新網域。
28. (選擇性) 選取 [自動軟體更新] 以啟用自動軟體更新。

29. (選用) 新增標籤以描述您的網域，以便分類和篩選該資訊。如需詳細資訊，請參閱the section called “標記網域”。
30. (選用) 展開並設定 Advanced cluster settings (進階叢集設定)。如需這些選項的摘要，請參閱the section called “進階叢集設定”。
31. 選擇 Create (建立)。

建立 OpenSearch 服務網域 (AWS CLI)

您可以使用，而不是使用主控台建立 OpenSearch 服務網域 AWS CLI。 有關語法，請參閱中的 Amazon OpenSearch 服務 AWS CLI指令參考 a.

命令範例

第一個範例會示範下列 OpenSearch 服務網域組態：

- 使用 1.2 OpenSearch 版建立名為 mylog 的 OpenSearch 服務網域
- 在網域中填入兩個 `r6g.large.search` 執行個體類型的執行個體
- 為每個資料節點使用 100 GiB 一般用途 (SSD) gp3 EBS 磁碟區進行儲存
- 允許匿名存取，但只從一個 IP 地址：192.0.2.0/32

```
aws opensearch create-domain \
    --domain-name mylogs \
    --engine-version OpenSearch_1.2 \
    --cluster-config  InstanceType=r6g.large.search,InstanceCount=2 \
    --ebs-options
 EBSEnabled=true,VolumeType=gp3,VolumeSize=100,Iops=3500,Throughput=125 \
    --access-policies '{"Version": "2012-10-17", "Statement": [{"Action": "es:*",
 "Principal":"*","Effect": "Allow", "Condition": {"IpAddress":{"aws:SourceIp":
["192.0.2.0/32"]}}}]}'
```

下面的例子演示了以下 OpenSearch 服務域配置：

- 使用彈性搜索 7.10 版創建一個名為 mylog 的 OpenSearch 服務域
- 在網域中填入六個 `r6g.large.search` 執行個體類型的執行個體
- 為每個資料節點使用 100 GiB 一般用途 (SSD) gp2 EBS 磁碟區進行儲存
- 將對服務的訪問限制為單個用戶，由用戶標識 AWS 帳戶 識別碼:5555555555

- 跨三個可用區域分佈執行個體

```
aws opensearch create-domain \
    --domain-name mylogs \
    --engine-version Elasticsearch_7.10 \
    --cluster-config
 InstanceType=r6g.large.search,InstanceCount=6,ZoneAwarenessEnabled=true,ZoneAwarenessConfig={A
 \
    --ebs-options EBSEnabled=true,VolumeType=gp2,VolumeSize=100 \
    --access-policies '{"Version": "2012-10-17", "Statement": [ { "Effect": "Allow",
 "Principal": {"AWS": "arn:aws:iam::555555555555:root" }, "Action":"es:*", "Resource":
 "arn:aws:es:us-east-1:555555555555:domain/mylogs/*" } ] }'
```

下面的例子演示了以下 OpenSearch 服務域配置：

- 使用 1.0 OpenSearch 版建立名為 mylog 的 OpenSearch 服務網域
- 在網域中填入十個 `r6g.xlarge.search` 執行個體類型的執行個體
- 在網域填入三個 `r6g.large.search` 執行個體類型的執行個體，以做為專用主節點
- 使用 100 GiB 佈建的IOPSEBS磁碟區進行儲存，每個資料節點的基準效能設定IOPS為 1000
- 限制對單個用戶和單個子資源的訪問，`_search`API

```
aws opensearch create-domain \
    --domain-name mylogs \
    --engine-version OpenSearch_1.0 \
    --cluster-config
 InstanceType=r6g.xlarge.search,InstanceCount=10,DedicatedMasterEnabled=true,DedicatedMasterTyp
 \
    --ebs-options EBSEnabled=true,VolumeType=io1,VolumeSize=100,Iops=1000 \
    --access-policies '{"Version": "2012-10-17", "Statement": [ { "Effect": "Allow",
 "Principal": { "AWS": "arn:aws:iam::555555555555:root" }, "Action": "es:*",
 "Resource": "arn:aws:es:us-east-1:555555555555:domain/mylogs/_search" } ] }'
```

> **Note**
>
> 如果您嘗試建立 OpenSearch 服務網域，且已存在具有相同名稱的網域，則CLI不會報告錯誤。相反地，它會傳回現有網域的詳細資訊。

建立 OpenSearch 服務網域 (AWS SDKs)

所以此 AWS SDKs（Android 和 iOS 除外SDKs）支持 Amazon OpenSearch 服務API參考中定義的所有操作，包括`CreateDomain`。如需程式碼範例，請參閱 the section called “使用 AWS SDK”。有關安裝和使用的更多信息 AWS SDKs，請參閱 AWS 軟體開發套件。

建立 OpenSearch 服務網域 (AWS CloudFormation)

OpenSearch 服務與 AWS CloudFormation，可協助您建立模型和設定的服務 AWS 這樣您就可以花更少的時間來建立和管理資源和基礎架構。您可以建立描述您要建立的 OpenSearch 網域的範本，並為您 CloudFormation 佈建和設定網域。如需詳細資訊，包括 OpenSearch 網域範例JSON和範YAML本，請參閱中的 Amazon OpenSearch 服務資源類型參考 AWS CloudFormation 使用者指南。

設定存取政策

Amazon OpenSearch 服務提供數種方式來設定對 OpenSearch 服務網域的存取。如需詳細資訊，請參閱 the section called “身分和存取權管理” 和 the section called “精細定義存取控制”。

主控台提供預先設定存取政策，讓您可以為您網域的特定需求自訂。您也可以從其他 OpenSearch 服務網域匯入存取原則。如需有關這些存取原則如何與VPC存取互動的資訊，請參閱the section called “關於網VPC域的存取原則”。

設定存取政策 (主控台)

1. 移至 https://aws.amazon.com，然後選擇 [登入主控台]。
2. 在分析下，選擇 Amazon OpenSearch 服務。
3. 在導覽窗格中，在 My domains (我的網域) 下，選擇您想要更新的網域。
4. 選擇 Actions (動作) 和 Edit security configuration (編輯安全組態)。
5. 編輯存取原則JSON，或匯入預先設定的選項。
6. 選擇 Save changes (儲存變更)。

進階叢集設定

使用進階選項來設定下列項目：

請求主體中的索引

指定是否允許在HTTP要求主體內顯式參照索引。將此屬性設為 `false` 以避免使用者繞開附屬資源的存取控制權。根據預設，此值為 `true`。如需詳細資訊，請參閱the section called “進階選項與API考量”。

欄位資料快取分配

指定分配給欄位資料的 Java 堆積空間的百分比。根據預設，此設定為JVM堆積的 20%。

> **Note**
>
> 許多客戶查詢輪換每日索引。我們建議您針對大多數這些使用案例，開始進行基準測試，並將JVM堆積`indices.fielddata.cache.size`設定為 40%。對於非常大的索引，您可能需要大型的欄位資料快取。

最大子句計數

指定 Lucene 布林查詢中允許的最大子句數量。預設值為 1,024。超過所允許的子句數量的查詢會導致 `TooManyClauses` 錯誤。如需詳細資訊，請參閱 Lucene 文件。

在 Amazon OpenSearch 服務中進行配置更改

Amazon OpenSearch 服務在更新網域時使用藍色/綠色部署程序。藍/綠部署會為複製生產環境的網域更新建立閒置環境，並在這些更新完成後將使用者路由至新環境。在藍/綠部署中，藍色環境是目前的生產環境。綠色環境是閒置的環境。

資料會從藍色環境移轉至綠色環境。當新環境準備就緒時， OpenSearch Service 會在環境中切換，以提升綠色環境成為新的生產環境。切換發生，沒有數據丟失。此作法可將停機時間降至最低，並在部署至新環境失敗的情況下維護原始環境。

主題

- 通常會導致藍/綠部署的變更
- 通常不會導致藍/綠部署的變更
- 判斷變更是否會導致藍/綠部署
- 啟動和追蹤組態變更
- 組態變更的階段

- 藍/綠部署的效能影響
- 組態變更的費用
- 對驗證錯誤進行疑難排解

通常會導致藍/綠部署的變更

以下操作會造成藍/綠部署：

- 變更執行個體類型
- 啟用精細存取控制
- 執行服務軟體更新
- 啟用或停用專用主節點
- 啟用或停用異地同步備份 (無待命
- 變更儲存類型、磁碟區類型或磁碟區大小
- 選擇不同的VPC子網
- 新增或移除VPC安全性群組
- 啟用或停用儀表板的 Amazon Cognito 份驗證 OpenSearch
- 選擇不同的 Amazon Cognito 使用者集區或身分集區
- 修改進階設定
- 升級至新 OpenSearch 版本 (在部分或全部升級期間，OpenSearch 儀表板可能無法使用)
- 啟用靜態或加密資料的 node-to-node 加密
- 啟用或禁用 UltraWarm 或冷存儲
- 停用自動調整並還原其變更
- 將可選插件與域關聯並將可選插件與域分離
- 增加具有兩個專用主節點的異地同步備份網域的專用主節點計數
- 減小EBS磁碟區大小
- 變更EBS磁碟區IOPS大小或輸送量 (如果您上次所做的變更正在進行中或發生時間不到 6 小時)
- 啟用將稽核記錄發佈至 CloudWatch。

對於具備待命網域的異地同步備份，您一次只能提出一個變更請求。如果變更已在進行中，則會拒絕新請求。您可以使用檢查當前「變更」的狀態`DescribeDomainChangeProgressAPI`。

通常不會導致藍/綠部署的變更

在大多數情況下，以下操作不會造成藍/綠部署：

- 修改存取原則
- 修改自訂端點
- 變更傳輸層安全性 (TLS) 原則
- 變更自動快照時間
- 啟用或停用「需要」HTTPS
- 啟用自動調整，或停用且不還原其變更
- 如果您的網域有專用主節點，請變更資料節點或 UltraWarm 節點計數
- 如果您的網域有專用主節點，請變更專用主要執行個體類型或計數 (具有兩個專用主節點的異地同步備份網域除外)
- 啟用或停用發佈錯誤記錄檔或慢速記錄檔 CloudWatch
- 停用將稽核記錄發佈至 CloudWatch
- 將磁碟區大小增加至每個資料節點最多 3 TiB，變更磁碟區類型或輸送量 IOPS
- 新增或移除標籤

> **Note**
>
> 視您的服務軟體版本而定，有一些例外情況。如果您想要確定變更不會造成藍/綠部署，請在更新網域之前執行乾式執行 (如果此選項可用)。某些更改不提供乾運行選項。我們通常建議您在流量尖峰時段之外對叢集進行變更。

判斷變更是否會導致藍/綠部署

您可以測試某些類型的規劃組態變更，以判斷這些變更是否會造成藍/綠部署，而不需要認可這些變更。在啟動組態變更之前，請使用主控台或執行驗證檢查，以確保您的網域符合更新資格。API

Console

若要驗證組態變更

1. 瀏覽至 Amazon OpenSearch 服務主控台，位於https://console.aws.amazon.com/aos/。

2. 在左側導覽窗格中選擇 Domains (網域)。
3. 選取您要進行組態變更的網域。這會開啟網域詳細資訊頁面。選取 Actions (動作) 下拉式功能表，然後選擇 Edit cluster configuration (編輯叢集組態)。
4. 在 Edit cluster configuration (編輯叢集組態) 頁面上，您可以變更執行個體類型、節點數目以及任何其他組態。在摘要面板中確認變更後，請選擇 Run (執行)。
5. 試轉完成後，結果將自動顯示在頁面底部，並附有試轉 ID。這些結果會通知您變更屬於哪個類別：

   - 啟動藍/綠部署
   - 不需要藍/綠部署
   - 包含您需要解決的驗證錯誤，解決後才能儲存變更

   請注意，每次試轉都會覆寫之前的試轉。若要查看稍後每個試轉的詳細資訊，請確保儲存試轉 ID。每個試轉可供使用的天數為 90 天，或直到您進行組態更新為止。
6. 若要繼續進行組態更新，請選擇 Save changes (儲存變更)。否則，請選擇 Cancel (取消)。任一選項都會帶您返回 Cluster configuration (叢集組態) 標籤。在此標籤上，您可以選擇 Dry run details (試轉詳細資訊) 以查看最新試轉的詳細資訊。此頁面還包括乾式運行之前的配置和乾運行配置之間的 side-by-side 比較。

API

您可以通過配置執行乾運行驗證API。若要使用API、設定`DryRun`為和為來`true`測試您的變`DryRunMode`更`Verbose`。詳細資訊模式除了判斷變更是否會啟動藍/綠部署之外，還會執行驗證檢查。例如，此UpdateDomainConfig要求會測試啟用下列項目所產生的部署類型 UltraWarm：

```
POST https://es.us-east-1.amazonaws.com/2021-01-01/opensearch/domain/my-domain/
config
{
   "ClusterConfig": {
    "WarmCount": 3,
    "WarmEnabled": true,
    "WarmType": "ultrawarm1.large.search"
   },
   "DryRun": true,
   "DryRunMode": "Verbose"
}
```

請求會執行驗證檢查並傳回變更將造成之部署類型，但實際上不會執行更新：

```
{
   "ClusterConfig": {
     ...
    },
   "DryRunResults": {
      "DeploymentType": "Blue/Green",
      "Message": "This change will require a blue/green deployment."
    }
}
```

可能的部署類型包括：

- `Blue/Green`：變更將導致藍/綠部署。
- `DynamicUpdate`：變更不會導致藍/綠部署。
- `Undetermined`：網域仍處於處理狀態，因此無法判斷部署類型。
- `None`：無設定變更。

如果驗證失敗，其會傳回驗證失敗的清單。

```
{
   "ClusterConfig":{
      "..."
   },
   "DryRunProgressStatus":{
      "CreationDate":"2023-01-12T01:14:33.847Z",
      "DryRunId":"db00ca39-48b2-4774-bbd3-252cf094d205",
      "DryRunStatus":"failed",
      "UpdateDate":"2023-01-12T01:14:33.847Z",
      "ValidationFailures":[
         {
            "Code":"Cluster.Index.WriteBlock",
            "Message":"Cluster has index write blocks."
         }
      ]
   }
}
```

如果狀態仍然存在pending，您可以在後續DescribeDryRunProgress呼叫的 UpdateDomainConfig 回應中使用乾運行 ID 來檢查驗證狀態。

```
GET https://es.us-east-1.amazonaws.com/2021-01-01/opensearch/domain/my-domain/
dryRun?dryRunId=my-dry-run-id
{
    "DryRunConfig": null,
    "DryRunProgressStatus": {
        "CreationDate": "2023-01-12T01:14:42.998Z",
        "DryRunId": "db00ca39-48b2-4774-bbd3-252cf094d205",
        "DryRunStatus": "succeeded",
        "UpdateDate": "2023-01-12T01:14:49.334Z",
        "ValidationFailures": null
    },
    "DryRunResults": {
        "DeploymentType": "Blue/Green",
        "Message": "This change will require a blue/green deployment."
    }
}
```

若要在不進行驗證檢查的情況下執行乾式分析，請在使用組態Basic時設定DryRunMode為API。

Python

下列 Python 程式碼會使用執UpdateDomainConfigAPI行乾式執行驗證檢查，如果檢查成功，則會在沒有空執行的API情況下呼叫相同的檢查來啟動更新。如果檢查失敗，指令碼會列印錯誤並停止。

```
import time
import boto3

client = boto3.client('opensearch')

response = client.UpdateDomainConfig(
    ClusterConfig={
        'WarmCount': 3,
        'WarmEnabled': True,
        'WarmCount': 123,
    },
    DomainName='test-domain',
    DryRun=True,
    DryRunMode='Verbose'
)
```

```
dry_run_id = response.DryRunProgressStatus.DryRunId

retry_count = 0

while True:

    if retry_count == 5:
        print('An error occured')
        break

    dry_run_progress_response = client.DescribeDryRunProgress('test-domain',
 dry_run_id)
    dry_run_status = dry_run_progress_response.DryRunProgressStatus.DryRunStatus

    if dry_run_status == 'succeeded':
        client.UpdateDomainConfig(
            ClusterConfig={
            'WarmCount': 3,
            'WarmEnabled': True,
            'WarmCount': 123,
        })
        break

    elif dry_run_status == 'failed':
        validation_failures_list =
 dry_run_progress_response.DryRunProgressStatus.ValidationFailures
        for item in validation_failures_list:
            print(f"Code: {item['Code']}, Message: {item['Message']}")
        break

    retry_count += 1
    time.sleep(30)
```

啟動和追蹤組態變更

> **Note**
>
> 您可以一次要求一個組態變更。您也可以在單一要求中分組多個組態變更。請先等待網域狀態變更，`Active`然後再要求任何其他組態變更。

您可以在 Amazon Ser OpenSearch vice 主控台中檢視網域處理狀 Config 和組態變更狀態欄位，以追蹤網域和組態變更。您也可以透過API回應中的和`ConfigChangeStatus`參數追蹤網域`DomainProcessingStatus`和組態變更。如需詳細資訊，請參閱 OpenSearch 服務API參考中的資DomainStatus料類型。

網域處理狀態可見性：您可以查看主控台中的 [網域處理狀態] 欄位，輕鬆判斷網域的組態狀態。同樣地，`DomainProcessingStatus`API參數也可用來識別狀態。下列值為網域的處理狀態：

- `Active`：未進行任何組態變更。您可以提交新的組態變更請求。
- `Creating`：正在建立網域。
- `Modifying`：正在進行組態變更，例如新增資料節點EBS、gp3、IOPS佈建或設定KMS金鑰。

> **Note**
>
> 您可能會看到狀態，就像`Modifying`在域需要分片移動才能完成配置更改的情況下。為了向後兼容，`Processing`參數的行為在API響應中保持不變，並在核心配置更改完成後立即設置為 false，而無需等待碎片移動完成。

- `Upgrading Engine Version`：正在進行引擎版本升級。
- `Updating Service Software`: 正在進行服務軟體更新。
- `Deleting`：正在刪除網域。
- `Isolated`：網域已暫停。

組態狀態可見性：設定變更可由操作員啟動 (例如新增資料節點、執行個體類型變更) 或由服務啟動 (例如，自動調整和離峰時間更新)。您可以在 Amazon Ser OpenSearch vice 主控台的「組態變更狀態」欄位和**`ConfigChangeStatus`**API回應中找到最新組態變更的狀態詳細資訊。下列值表示網域的組態狀態：

- `Pending`：已提交組態變更請求。
- `Initializing`：服務正在初始化組態變更要求。
- `Validating`：服務正在驗證請求的更改和所需的資源。
- `Awaiting user inputs`：當操作員預期某些組態變更 (例如執行個體類型變更) 以繼續進行時套用。您可以編輯組態變更。
- `Applying changes`：服務正在套用要求的組態變更。
- `Cancelled`：已取消組態變更。如果您收到驗證失敗狀態，可以按一下主控台中的「取消」或呼叫`CancelDomainConfigChange`API作業。如果執行此操作，則會復原所有套用的變更。

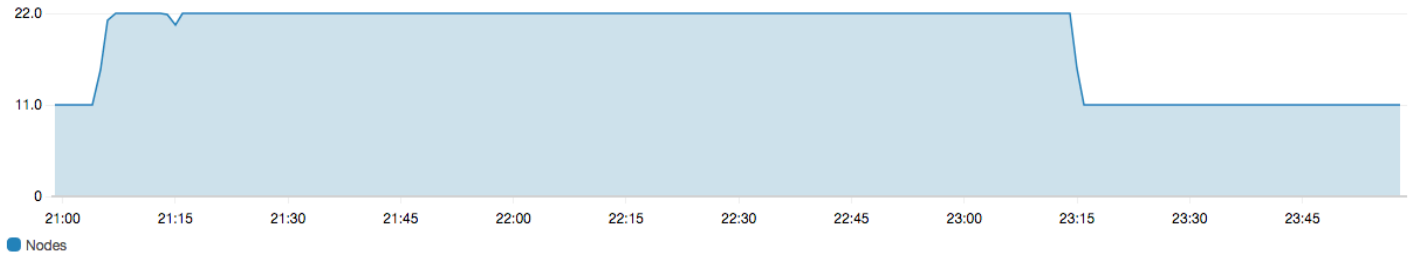
- `Completed`：要求的組態變更已成功完成。
- `Validation Failed`：請求的變更驗證失敗。不會套用任何組態變更。

> **Note**
>
> 驗證失敗可能是因為您的網域中存在紅色索引、選擇的執行個體類型無法使用或磁碟空間不足所造成。如需驗證錯誤的清單，請參閱the section called “對驗證錯誤進行疑難排解”。在驗證失敗事件期間，您可以取消、重試或編輯組態變更。

API摘要：您可以使用`DescribeDomain``DescribeDomainChangeProgress`、與`DescribeDomainConfig`API作業來取得詳細的組態更新狀態。此外，您可以使`CancelDomainConfigChange`用在驗證失敗時取消更新。如需詳細資訊，請參閱OpenSearch 服務API文件

當組態變更完成時，網域狀態會變回`Active`。

您可以檢閱叢集運作狀態和 Amazon CloudWatch 指標，並在網域更新時看到叢集中的節點數目暫時增加 (通常是翻倍)。在下圖中，您可以看到在組態變更期間節點數量從 11 加倍到 22，而在更新完成時恢復回 11。



此暫時增加可能形成叢集專用主節點的負擔，突然可能會有許多節點需要管理。當 OpenSearch Service 將資料從舊叢集複製到新叢集時，也會增加搜尋和索引延遲。在叢集務必維持足夠的容量，以處理與這些藍/綠部署相關的負荷。

> **Important**
>
> 組態變更和服務維護期間，您不需要支付任何額外費用。您也只需要針對您為叢集請求的節點數付費。如需詳細規格，請參閱the section called “組態變更的費用”。

為了防止專用主節點過載，您可以使用 Amazon CloudWatch 指標監控使用情況。如需建議的最大值，請參閱the section called “建議的 CloudWatch 鬧鐘”。

組態變更的階段

啟動組態變更後， OpenSearch 服務會執行一系列步驟來更新您的網域。您可以在主控台的 [組態變更狀態] 下檢視組態變更進度。更新會經歷的確切步驟依您正在執行的變更類型而定。您也可以使用DescribeDomainChangeProgressAPI作業監視組態變更。

以下是更新在組派變更過程中可能會經歷的階段：

階段名稱	描述
驗證	驗證網域是否有資格進行更新，並在必要時顯示驗證問題。
建立新環境	完成必要的先決條件並建立所需資源，以開始進行藍/綠部署。
佈建新節點	在新環境中建立一組新的執行個體。
新節點上的流量路由	將流量重新引導至新建立的資料節點。
舊節點上的流量路由	停用舊資料節點上的流量。
準備要移除的節點	準備移除節點。僅在您縮減網域時 (例

階段名稱	描述
	如，從 8 個節點減少至 6 個節點)，系統才會執行此步驟。
將碎片複製到新節點	將碎片從舊節點移動至新節點。
終止節點	在移除碎片後，終止和刪除舊節點。
刪除舊資源	刪除與舊環境 (例如負載平衡器) 相關聯的資源。
動態更新	已在更新無需藍/綠部署且可動態套用更新時顯示。
套用專屬的主要相關變更	當專用主要執行個體類型或計數變更時顯示。
套用磁碟區相關變更	當磁碟區大小、類型IOPS和輸送量變更時顯示。

藍/綠部署的效能影響

在藍/綠部署期間，您的 Amazon OpenSearch 服務叢集可用於傳入的搜尋和索引請求。不過，您可能會遇到下列效能問題：

- 由於叢集有更多要管理的節點，導線節點的使用量暫時增加。
- 隨著 OpenSearch Service 將資料從舊節點複製到新節點，因此增加了搜尋和索引延遲。
- 隨著叢集負載在藍/綠部署期間增加而增加，對傳入要求的拒絕次數增加。
- 若要避免延遲問題和要求拒絕，您應該在叢集狀態良好且網路流量低時執行藍/綠部署。

組態變更的費用

如果您變更網域的組態， OpenSearch Service 會依照中的說明建立新叢集the section called “組態變更”。在將舊的遷移到新的期間，您需要支付以下費用：

- 如果您變更執行個體類型，會收取兩個叢集第一個小時的費用。在第一個小時後，則只會收取新叢集的費用。EBS磁碟區不會收取兩次費用，因為它們是叢集的一部分，因此它們的計費按照執行個體計費。

  範例：您將組態從三個 `m3.xlarge` 執行個體變更為四個 `m4.large` 執行個體。對於第一個小時，您會被收取兩個叢集 (3 * `m3.xlarge` + 4 * `m4.large`) 的費用。在第一個小時後，則只會收取新叢集 (4 * `m4.large`) 的費用。
- 如果您不變更執行個體類型，您只會被收取最大叢集第一個小時的費用。在第一個小時後，則只會收取新叢集的費用。

  範例：您將組態從六個 `m3.xlarge` 執行個體變更為三個 `m3.xlarge` 執行個體。對於第一個小時，您會被收取最大叢集 (6 * `m3.xlarge`) 的費用。在第一個小時後，則只會收取新叢集 (3 * `m3.xlarge`) 的費用。

對驗證錯誤進行疑難排解

當您啟動組態變更或執行 OpenSearch 或 Elasticsearch 版本升級時， OpenSearch Service 會先執行一系列的驗證檢查，以確保您的網域符合更新資格。如果其中任何一項檢查失敗，您會在主控台中收到通知，其中包含您必須在更新網域之前解決的特定問題。下表列出 OpenSearch Service 可能出現的可能網域問題，以及解決這些問題的步驟。

問題	錯誤代碼	疑難排解步驟
找不到安全群組	SecurityGroupNotFound	與您的 OpenSearch 服務網域相關聯的安全性群組不存在。若要解決此問題，請使用指定的名稱建立安全群組。
找不到子網	SubnetNotFound	與您的 OpenSearch 服務網域相關聯的子網路不存在。若要解決此問題，請在VPC.
未設定服務連結角色	SLRNotConfigured	未設定服務的服 OpenSearch 務連結角色。服務連結角色由 OpenSearch Service 預先定義，並包含服務呼叫其他人所需的所有權限 AWS 代表您提供的服務。如果角色不存在，則可能需要手動建立。
IP 地址不足	InsufficientFreeIPsForSubnets	您的一或多個VPC子網路沒有足夠的 IP 位址來更新您的網域。若要計算您需要多少 IP 地址，請參閱 the section called “在子網路中保留 IP 位VPC址”。
Cognito 使用者集區不存在	CognitoUserPoolNotFound	OpenSearch 服務找不到 Amazon Cognito 使用者集區。確認您已建立一個且具有正確的 ID。要查找 ID，您可以使用 Amazon Cognito 控制台或以下操作 AWS CLI 命令： `aws cognito-idp list-user-pools --max-results 60 --region us-east-1`
Cognito 身分集區不存在	CognitoIdentityPoolNotFound	OpenSearch 服務找不到 Cognito 身分識別集區。確認您已建立一個且具有正確的 ID。要查找 ID，您可以使用 Amazon Cognito 控制台或以下操作 AWS CLI 命令： `aws cognito-identity list-identity-pools --max-results 60 --region us-east-1`
找不到使用者集區的 Cognito 網域	CognitoDomainNotFound	使用者集區沒有網域名稱。您可以使用 Amazon Cognito 主控台或以下方法設定一個主控台 AWS CLI 命令： `aws cognito-idp create-user-pool-domain --domain my-domain --user-pool-id id`

問題	錯誤代碼	疑難排解步驟
未設定 Cognito 角色	`CognitoRoleNotConfigured`	未設定授與 OpenSearch 服務權限以設定 Amazon Cognito 使用者和身分識別集區以及將其用於身分驗證的IAM角色。使用適當的許可集合和信任關係來設定角色。您可以使用主控台來為您建立預設CognitoAccessForAmazonOpenSearch角色，也可以使用 AWS CLI 或 AWS SDK.
無法描述使用者集區	`UserPoolNotDescribable`	指定的 Amazon Cognito 角色沒有許可，無法描述與您的網域相關聯之使用者集區。請確定角色許可政策允許 `cognito-identity:DescribeUserPool` 動作。請參閱 the section called “關於 CognitoAccessForAmazonOpenSearch角色” 了解完整的許可政策。
無法描述身分集區	`IdentityPoolNotDescribable`	指定的 Amazon Cognito 角色沒有許可，無法描述與您的網域相關聯之身分集區。請確定角色許可政策允許 `cognito-identity:DescribeIdentityPool` 動作。請參閱 the section called “關於 CognitoAccessForAmazonOpenSearch角色” 了解完整的許可政策。
無法描述使用者集區和身分集區	`CognitoPoolsNotDescribable`	指定的 Amazon Cognito 角色沒有許可，無法描述與您的網域相關聯之使用者集區和身分集區。請確定角色許可政策允許 `cognito-identity:DescribeIdentityPool` 和 `cognito-identity:DescribeUserPool` 動作。請參閱 the section called “關於 CognitoAccessForAmazonOpenSearch角色” 了解完整的許可政策。
KMS未啟用金鑰	`KMSKeyNotEnabled`	所以此 AWS Key Management Service (AWS KMS) 用來加密您的網域的金鑰已停用。立即重新啟用金鑰。
自訂憑證未ISSUED處於狀態	`InvalidCertificate`	如果您的網域使用自訂端點，您可以在中產生SSL憑證來保護它 AWS Certificate Manager（ACM）或導入您自己的一個。憑證狀態必須為 Issued (已發佈)。如果您收到此錯誤訊息，請在ACM主控台中檢查憑證的狀態。如果狀態為「已到期」、「失敗」、「非作用中」或「擱置中」驗證，請參閱ACM疑難排解文件以解決問題。

問題	錯誤代碼	疑難排解步驟
沒有足夠的容量來啟動選擇的執行個體類型	`InsufficientInstanceCapacity`	請求的執行個體類型容量不可用。例如，您可能已請求五個`i3.16xlarge.search` 節點，但 OpenSearch Service 沒有足夠的可用`i3.16xlarge.search` 主機，因此無法滿足要求。在 OpenSearch Service 中檢查支援的執行個體類型，並選擇不同的執行個體類型。
叢集中的紅色索引	`RedCluster`	叢集中的一個或多個索引具有紅色狀態，這導致整體紅色叢集狀態。若要進行疑難排解並修正此問題，請參閱 the section called “紅色叢集狀態”。
對記憶體斷路器的請求太多	`TooManyRequests`	您的網域有太多搜尋和寫入要求，因此 OpenSearch Service 無法更新其設定。您可以減少請求數量、垂直擴展執行個體至 64 GiBRAM，或透過新增執行個體水平擴展。
新組態無法存放資料 (磁碟空間不足)	`InsufficientStorageCapacity`	設定的儲存空間大小無法存放您網域上的所有資料。若要解決此問題，請選擇更大的磁碟區、刪除未使用的索引或增加叢集中的節點數目，以立即釋放磁碟空間。

固定到特定節點的碎片	`ShardMovementBlocked`	網域中的一個或多個索引會連接至特定節點，且無法重新指派。這很可能是因為您已設定碎片分配篩選，這可讓您指定允許哪些節點託管特定索引的碎片。
		
		若要解決此問題，請從所有受影響的索引中移除碎片分配篩選條件：
		
		`PUT my-index/_settings`
		`{`
		`  "settings": {`
		`  "index.routing.allocation.require._name": null`
		`  }`
		`}`

問題	錯誤代碼	疑難排解步驟
新組態無法存放所有碎片 (碎片計數)	TooManyShards	網域上的碎片計數太高，這會導致 OpenSearch Service 無法將它們移至新的組態。若要解決此問題，請新增與目前叢集節點相同的組態類型的節點，以便水平擴展您的網域。請注意，最大EBS磁碟區大小取決於節點的執行個體類型。 若要避免將來發生此問題，請參閱 the section called “選擇碎片數” 並定義適用於您的使用案例的碎片策略。
與您的網域相關聯的子網路不支援IPv4位址	ResultCodeIPv4BlockNotExists	若要解決此問題，請VPC根據網域的設定 IP 位址類型，建立子網路或更新您中的現有子網路。如果您的網域IPv4只使用位址類型，請使用IPv4唯一的子網路。如果您的網域使用雙堆疊模式，請使用雙堆疊子網路。
與您的網域相關聯的子網路不支援IPv6位址	ResultCodeIPv6BlockNotExists	若要解決此問題，請VPC根據網域的設定 IP 位址類型，建立子網路或更新您中的現有子網路。如果您的網域IPv4只使用位址類型，請使用IPv4唯一的子網路。如果您的網域使用雙堆疊模式，請使用雙堆疊子網路。

Amazon 服務中的服 OpenSearch 務軟件更新

> **Note**
>
> 如需每個主要 (非修補程式) 服務軟體更新所做變更與新增的說明，請參閱版本說明。

Amazon Ser OpenSearch vice 會定期發行服務軟體更新，以新增功能或以其他方式改善您的網域。主控台中的 Notifications (通知) 面板是查看更新是否可用或檢查更新狀態的最簡單方法。每個通知都包含有關服務軟體更新的詳細資訊。所有服務軟體更新都使用藍/綠部署，將停機時間降至最

服務軟體更新與 OpenSearch 版本升級不同。若要取得有關升級到較新版本的資訊 OpenSearch，請參閱the section called “升級網域”。

主題

- 可選更新與必要更新
- 補丁更新

- 考量事項
- 啟動服務軟體更新
- 在離峰時段排程軟體更新
- 監視服務軟體更新
- 網域不符合更新條件時，

可選更新與必要更新

OpenSearch 服務有兩大類服務軟體更新：

可選更新

選用的服務軟體更新通常包括對新功能或功能的增強功能和支援。您的網域不會強制執行選用更新，也沒有嚴格的安裝期限。更新的可用性是透過電子郵件和主控台通知進行通知。您可以選擇立即套用更新，或重新排定更正確的日期和時間。您也可以在網域的離峰時段進行排程。大部分的軟體更新都是選擇性的。

無論您是否排程更新，如果您對導致藍/綠部署的網域進行變更， OpenSearch Service 都會自動為您更新服務軟體。

您可以將網域設定為在離峰時段自動套用選用更新。開啟此選項時，「 OpenSearch 服務」會等待至少 13 天，從選擇性更新可用起，然後將更新排程在 72 小時 (3 天) 之後。您會在排程更新時收到主控台通知，而且您可以選擇將它重新排定為稍後的日期。

若要開啟自動軟體更新，請選取 [建立或更新網域時啟用自動軟體更新]。若要使用配置相同的設定 AWS CLI，`--software-update-options`請在建立或更新網域`true`時設定為。

必要的更新

必要的服務軟體更新通常包括重要的安全性修正或其他強制性更新，以確保您的網域持續完整性和功能。必要更新的範例包括 Log4j 的常見弱點和風險 (CVE)，以及執行個體描述資料服務第 2 版 (IMDSv2) 的強制執行。一年中的強制更新次數通常少於三次。

OpenSearch 服務會自動排程這些更新，並在預約更新前 72 小時 (3 天) 透過電子郵件和主控台通知通知您。您可以選擇立即套用更新，或在允許的時間範圍內重新排定更合適的日期與時間。您也可以在網域的下一個離峰時段進行排程。如果您不對必要的更新採取任何動作，且未進行任何會造成藍/綠部署的網域變更，則 OpenSearch Service 可以在網域的離峰時段內，在指定的截止日期 (通常為 14 天後) 之後的任何時間起始更新。

無論排程何時更新，如果您對導致藍/綠部署的網域進行變更， OpenSearch Service 都會自動為您更新您的網域。

補丁更新

以 "-P" 和數字結尾的服務軟體版本，例如 R20211203-*P4*，是修補程式版本。修補程式可能包括效能改進、小錯誤修復、安全修復或狀態改善。修補程式版本不包含新功能或突破性變更，而且通常不會對使用者產生直接或明顯的影響。服務軟體通知會告訴您修補程式版本是選擇性的還是必要的。

考量事項

在決定是否要更新網域時，請考慮下列各項：

- 手動更新網域可讓您更快速地利用新功能。當您選擇 [更新] 時，[OpenSearch 服務] 會將要求置於佇列中，並在有時間時開始更新。
- 當您啟動服務軟體更新時， OpenSearch Service 會在更新開始和完成時傳送通知。
- 軟體更新使用藍/綠部署盡量減少停機時間。更新可能會暫時損耗叢集的專用主節點，因此請務必維持足夠的容量來處理相關的額外負荷。
- 更新通常在幾分鐘內完成，但如果您的系統負載過重，也可能需要數小時甚至數天的時間。請考慮在設定的離峰期間更新您的網域，以避免較長的更新期間。

啟動服務軟體更新

您可以透過服 OpenSearch 務主控台、或其中一個 SDK 要求服務軟體更新。 AWS CLI

主控台

要求服務軟體更新

1. 在以下位置打開 Amazon OpenSearch 服務控制台 https://console.aws.amazon.com/aos/home。
2. 選取網域名稱以開啟其組態。
3. 選擇「動作」、「更新」，然後選取下列其中一個選項：
    - 立即套用更新-如果有可用容量，請立即排定在目前的小時內執行動作。如果無法使用容量，我們會提供其他可用的時段供您選擇。
    - 在離峰時段中排程 — 只有在網域已啟用離峰時段時才可用。排程在網域設定的離峰時段期間進行更新。不能保證更新會在下一個立即窗口中發生。根據容量，它可能會在隨後的日子發生。如需詳細資訊，請參閱 the section called “離峰窗”。

- 特定日期和時間的排程 — 將更新排程在特定日期和時間進行。如果您指定的時間因為容量原因而無法使用，您可以選取不同的時段。

如果您將更新排程在稍後的日期 (在網域的非尖峰期間內或之外)，您可以隨時重新排程。如需說明，請參閱the section called “重排作業”。

4. 選擇確認。

AWS CLI

傳送要start-service-software-update AWS CLI 求以啟動服務軟體更新。此範例會立即將更新新增至佇列：

```
aws opensearch start-service-software-update \
  --domain-name my-domain \
  --schedule-at "NOW"
```

回應：

```
{
    "ServiceSoftwareOptions": {
        "CurrentVersion": "R20220928-P1",
        "NewVersion": "R20220928-P2",
        "UpdateAvailable": true,
        "Cancellable": true,
        "UpdateStatus": "PENDING_UPDATE",
        "Description": "",
        "AutomatedUpdateDate": "1969-12-31T16:00:00-08:00",
        "OptionalDeployment": true
    }
}
```

> **Tip**
>
> 請求更新之後，您可以在狹窄的時間範圍內取消更新。此`PENDING_UPDATE`狀態的持續時間可能會有很大的差異，並取決於您 AWS 區域 和 OpenSearch 服務正在執行的並行更新數量。若要取消更新，請使用主控台或`cancel-service-software-update` AWS CLI 指令。

如果請求失敗，並顯示為`BaseException`，則表示您指定的時間由於容量原因而無法使用，而且您必須指定不同的時間。 OpenSearch 服務在回應中提供替代可用的插槽建議。

AWS 開發套件

此範例 Python 指令碼使用中的說明網域和起始服務軟體更新方法來檢查網域是否符合服務軟體更新的資格，如果是，則啟動更新。 AWS SDK for Python (Boto3) 您必須提供 `domain_name` 的值。

```
import boto3
from botocore.config import Config
import time

# Build the client using the default credential configuration.
# You can use the CLI and run 'aws configure' to set access key, secret
# key, and default region.

my_config = Config(
    # Optionally lets you specify a Region other than your default.
    region_name='us-east-1'
)

domain_name = ''  # The name of the domain to check and update

client = boto3.client('opensearch', config=my_config)


def getUpdateStatus(client):
    """Determines whether the domain is eligible for an update"""
    response = client.describe_domain(
        DomainName=domain_name
    )
    sso = response['DomainStatus']['ServiceSoftwareOptions']
    if sso['UpdateStatus'] == 'ELIGIBLE':
        print('Domain [' + domain_name + '] is eligible for a service software update
 from version ' +
              sso['CurrentVersion'] + ' to version ' + sso['NewVersion'])
        updateDomain(client)
    else:
        print('Domain is not eligible for an update at this time.')


def updateDomain(client):
    """Starts a service software update for the eligible domain"""
```

```
    response = client.start_service_software_update(
        DomainName=domain_name
    )
    print('Updating domain [' + domain_name + '] to version ' +
          response['ServiceSoftwareOptions']['NewVersion'] + '...')
    waitForUpdate(client)


def waitForUpdate(client):
    """Waits for the domain to finish updating"""
    response = client.describe_domain(
        DomainName=domain_name
    )
    status = response['DomainStatus']['ServiceSoftwareOptions']['UpdateStatus']
    if status == 'PENDING_UPDATE' or status == 'IN_PROGRESS':
        time.sleep(30)
        waitForUpdate(client)
    elif status == 'COMPLETED':
        print('Domain [' + domain_name +
              '] successfully updated to the latest software version')
    else:
        print('Domain is not currently being updated.')

def main():
    getUpdateStatus(client)
```

在離峰時段排程軟體更新

在 2023 年 2 月 16 日之後建立的每個 OpenSearch 服務網域都有一個每日 10 小時的時段，介於當地時間 10:00 到上午 8:00 之間，我們會考慮離峰時段。 OpenSearch 服務會使用此視窗來排定網域的服務軟體更新。離峰更新有助於將叢集專用主節點在高流量期間的壓力降至最低。 OpenSearch 未經您的同意，服務無法在此 10 小時之外啟動更新。

- 對於選擇性更新， OpenSearch 服務會通知您更新的可用性，並提示您在即將到來的離峰期間排程更新。
- 對於必要的更新， OpenSearch 服務會在即將到來的離峰期間自動排程更新，並提前三天通知您。您可以重新排定更新 (在離峰時段內或之外)，但只能在完成更新的所需時間範圍內重新排程。

對於每個網域，您可以選擇以自訂時間覆寫預設的晚上 10:00 開始時間。如需說明，請參閱the section called “設定自訂離峰時段”。

主控台

若要在即將到來的離峰期間排定更新

1. 在以下位置打開 Amazon OpenSearch 服務控制台 https://console.aws.amazon.com/aos/home。
2. 選取網域名稱以開啟其組態。
3. 選擇動作、更新。
4. 選取「在離峰視窗中排程」。
5. 選擇確認。

您可以在「離峰時段」標籤上檢視排定的動作，並隨時重新排程。請參閱 the section called “檢視排程動作”。

CLI

若要使用在即將到來的離峰期間排程更新 AWS CLI，請傳送StartServiceSoftwareUpdate要求並指定`OFF_PEAK_WINDOW``--schedule-at`參數：

```
aws opensearch start-service-software-update \
  --domain-name my-domain \
  --schedule-at "OFF_PEAK_WINDOW"
```

監視服務軟體更新

OpenSearch 服務軟體更新可用、必要、已啟動、已完成或失敗時，Service 會傳送通知。您可以在 OpenSearch 服務主控台的「通知」面板上檢視這些通知。如果更新為可選，則通知嚴重性為`Informational`；如果必須更新，則為 `High`。

OpenSearch 服務也會將服務軟體事件傳送至 Amazon EventBridge。您可以用 EventBridge 來設定在收到事件時傳送電子郵件或執行特定動作的規則。如需範例演練，請參閱 the section called “教學課程：傳送可用更新的 SNS 提醒”。

若要查看傳送至 Amazon 的每個服務軟體事件的格式 EventBridge，請參閱the section called “服務軟體更新事件”。

網域不符合更新條件時，

如果您的網域處於以下任何一種狀態，則不符合服務軟體更新的資格：

州	描述
處理中的網域	組態變更中的網域 請於操作完成後檢查更新資格。
紅色叢集狀態	叢集中一或多個索引是紅色的。如需疑難排解步驟，請參閱the section called “紅色叢集狀態”。
高錯誤率	嘗試處理請求時， OpenSearch 叢集會傳回大量 5 xx 錯誤。此問題通常是因為太多同時讀寫請求造成。請考慮降低叢集流量或擴展網域。
分割大腦	分裂大腦意味著您的 OpenSearch 叢集有多個主節點，並且已分割成兩個叢集，這些叢集永遠不會自行重新加入。您也可以使用建議數量的專用主節點來避免大腦分割。如需從大腦分割中恢復的協助，請聯絡 AWS Support。
Amazon Cognito 整合問題	您的網域使用 OpenSearch 儀表板的身份驗證，而 OpenSearch 服務找不到一或多個 Amazon Cognito 資源。如果缺少 Amazon Cognito 使用者集區，通常就會發生此問題。若要修正此問題，請重新建立遺失的資源，並將 OpenSearch Service 網域設定為使用該資源。
其他 服務問題	OpenSearch 服務本身的問題可能會導致您的網域顯示為不符合更新資格。如果上述情況都不適用於您的網域且問題持續超過一天，請聯絡 AWS Support。

定義 Amazon OpenSearch 服務的離峰窗口

建立 Amazon OpenSearch 服務網域時，您需要定義一個視為離峰時段的每日 10 小時時段。OpenSearch 服務會使用此視窗來排程服務軟體更新和 Auto-Tune 最佳化，這些最佳化需要在相對較低的流量時間 (如果可能) 進行藍/綠部署。藍/綠是指為網域更新建立新環境的程序，並在這些更新完成後將使用者路由至新環境。

雖然藍/綠部署不會中斷，但是為了在藍/綠部署耗用資源時，將任何潛在的效能影響降到最低，我們建議您在網域設定的離峰時段排程這些部署。更新 (例如節點取代) 或需要立即部署至網域的更新，請勿使用離峰期。

您可以修改離峰時段的開始時間，但無法修改視窗的長度。

> **Note**
>
> 離峰時窗於 2023 年 2 月 16 日推出。根據預設，在此日期之前建立的所有網域都會停用離峰時段。您必須手動啟用並設定這些網域的離峰時段。在此日期之後建立的所有網域預設都會啟用離峰時段。啟用網域之後，您就無法停用該網域的離峰時段。

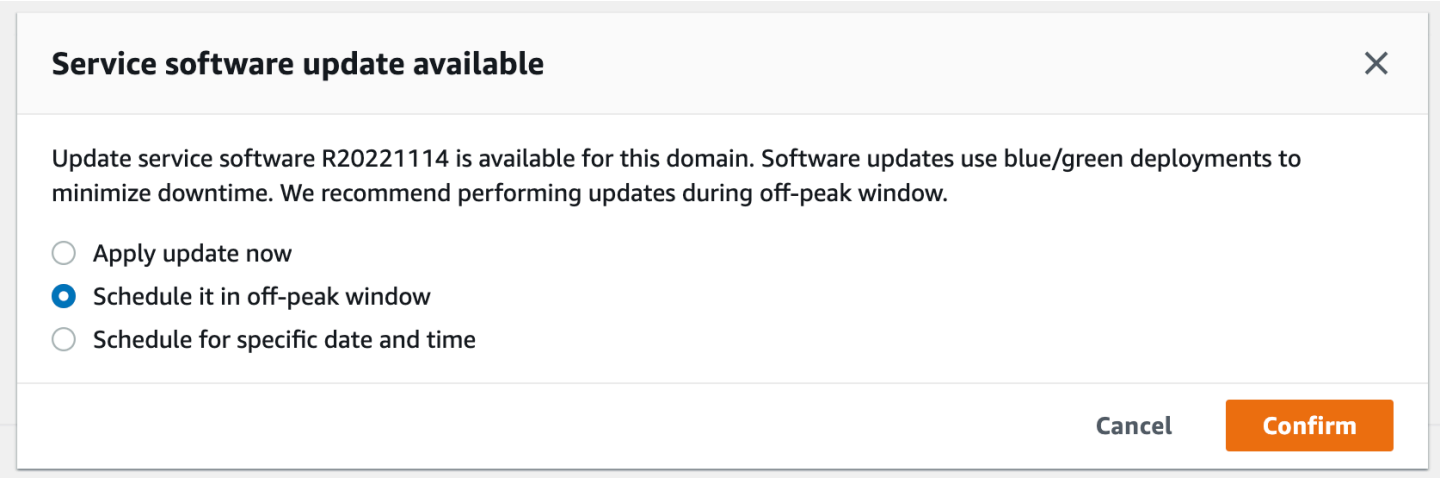
主題

- 離峰服務軟體更新
- 離峰自動調諧最佳化
- 啟用離峰期
- 設定自訂離峰時段
- 檢視排程動作
- 重排作業
- 從自動調整維護時段移轉

離峰服務軟體更新

OpenSearch 服務有兩大類服務軟體更新 — 選用和必要。這兩種類型都需要藍/綠部署。選用更新不會在您的網域上強制執行，而如果您在指定的期限之前未採取任何動作 (通常是在可用性後兩週)，則會自動安裝所需更新。如需詳細資訊，請參閱 the section called “可選更新與必要更新”。

當您啟動選擇性更新時，您可以選擇立即套用更新、為後續的離峰時段排程更新，或是指定要套用更新的自訂日期和時間。



對於必要的更新， OpenSearch 服務會自動排程在離峰時段執行更新的日期和時間。您會在預約更新前三天收到通知，而且您可以選擇在所需的部署期間內將其重新排定為稍後的日期和時間。如需說明，請參閱the section called “重排作業”。

離峰自動調諧最佳化

之前，自動調整使用維護時段來排程需要藍/綠部署的變更。在引入離峰時段之前已啟用自動調整和維護時段的網域，將繼續使用維護時段進行這些更新，除非您將它們移轉為使用離峰時段。

我們建議您移轉網域以使用離峰時段，因為它是用來排程網域上的其他活動，例如服務軟體更新。如需說明，請參閱the section called “從自動調整維護時段移轉”。將網域移轉至離峰時段之後，您無法還原為使用維護時段。

2023 年 2 月 16 日之後建立的所有網域都會使用離峰時段 (而非舊版維護時段) 來排程藍/綠部署。您無法停用網域的離峰時段。如需需要藍/綠部署的自動調整最佳化清單，請參閱。the section called “變更類型”

啟用離峰期

任何在 2023 年 2 月 16 日之前建立的網域 (引入離峰時段時) 預設會停用此功能。您必須針對這些網域手動啟用它。啟用後，您無法停用離峰視窗。

主控台

若要啟用網域的離峰時段

1. 在以下位置打開 Amazon OpenSearch 服務控制台 https://console.aws.amazon.com/aos/home。
2. 選取要開啟其組態的網域名稱。
3. 切換作業選項至離峰時段頁標，然後選擇編輯。
4. 以國際標準時間 (UTC) 指定自訂開始時間。例如，若要在美國西部 (奧勒岡) 區域設定晚上 11:30 的開始時間，請指定 07 :30。
5. 選擇儲存變更。

CLI

若要使用修改離峰時段AWS CLI，請傳送UpdateDomainConfig請求：

```
aws opensearch update-domain-config \
  --domain-name my-domain \
```

```
  --off-peak-window-options 'Enabled=true,
 OffPeakWindow={WindowStartTime={Hours=02,Minutes=00}}'
```

如果您未指定自訂視窗開始時間，則預設值為 00:00 UTC。

設定自訂離峰時段

您可以在國際標準時間 (UTC) 中為您的網域指定自訂離峰時段。例如，如果您希望美國東部 (維吉尼亞北部) 區域中某個網域的離峰時段從晚上 11:00 開始，您必須指定 04:00 UTC。

主控台

若要修改網域的離峰時段

1. 在以下位置打開 Amazon OpenSearch 服務控制台 https://console.aws.amazon.com/aos/home。
2. 選取要開啟其組態的網域名稱。
3. 切換作業選項至「離峰期」 頁標。您可以檢視已設定的離峰時段，以及網域即將進行的排程動作清單。
4. 選擇編輯並以 UTC 指定新的開始時間。例如，若要在美國東部 (維吉尼亞北部) 區域設定 9:00 PM 的開始時間，請指定 02:00 U CT。
5. 選擇儲存變更。

CLI

若要使用設定自訂離峰時段AWS CLI，請傳送UpdateDomainConfig要求，並以 24 小時時間格式指定小時和分鐘。

例如，下列要求會將視窗開始時間變更為 UTC 上午 2:00：

```
aws opensearch update-domain-config \
  --domain-name my-domain \
  --off-peak-window-options 'OffPeakWindow={WindowStartTime={Hours=02,Minutes=00}}'
```

如果您未指定視窗開始時間，則預設為建立網域AWS 區域的當地時間晚上 10:00。

檢視排程動作

您可以檢視每個網域目前已排程、進行中或擱置中的所有動作。動作的嚴重性可能為HIGHMEDIUM、和LOW。

動作可以具有下列狀態：

- `Pending update`— 動作位於待處理的佇列中。
- `In progress`— 動作目前正在進行中。
- `Failed`— 動作無法完成。
- `Completed`— 動作已成功完成。
- `Not eligible`— 僅適用於服務軟件更新。無法繼續更新，因為叢集處於健康狀態不良。
- `Eligible`— 僅適用於服務軟件更新。該網域符合更新資格。

主控台

OpenSearch 服務主控台會顯示網域組態中的所有排程動作，以及每個動作的嚴重性和目前狀態。

若要檢視網域的排程動作

1. 在以下位置打開 Amazon OpenSearch 服務控制台 https://console.aws.amazon.com/aos/home。
2. 選取要開啟其組態的網域名稱。
3. 切換作業選項至「離峰期」 頁標。
4. 在「已排程的動作」下，檢視網域目前已排程、進行中或擱置中的所有動作。

CLI

若要使用檢視排程動作AWS CLI，請傳送ListScheduledActions請求：

```
aws opensearch list-scheduled-actions \
  --domain-name my-domain
```

回應：

```
{
    "ScheduledActions": [
        {
            "Cancellable": true,
            "Description": "The Deployment type is : BLUE_GREEN.",
            "ID": "R20220721-P13",
            "Mandatory": false,
```

```
            "Severity": "HIGH",
            "ScheduledBy": "CUSTOMER",
            "ScheduledTime": 1.673871601E9,
            "Status": "PENDING_UPDATE",
            "Type": "SERVICE_SOFTWARE_UPDATE",
        },
        {
            "Cancellable": true,
            "Description": "Amazon Opensearch will adjust the young generation JVM
 arguments on your domain to improve performance",
            "ID": "Auto-Tune",
            "Mandatory": true,
            "Severity": "MEDIUM",
            "ScheduledBy": "SYSTEM",
            "ScheduledTime": 1.673871601E9,
            "Status": "PENDING_UPDATE",
            "Type": "JVM_HEAP_SIZE_TUNING",
        }
    ]
}
```

重排作業

OpenSearch 服務會通知您排程的服務軟體更新和自動調整最佳化。您可以選擇立即應用「變更」，或重新安排其日期和時間。

> **Note**
>
> OpenSearch 服務可以在您選取的時間後一小時內排程動作。例如，如果您選擇在下午 5 點套用更新，則可以在下午 5 點到下午 6 點之間套用更新。

主控台

若要重新排程動作

1. 在以下位置打開 Amazon OpenSearch 服務控制台 https://console.aws.amazon.com/aos/home。
2. 選取要開啟其組態的網域名稱。
3. 切換作業選項至「離峰期」 頁標。
4. 在「已排程動作」下，選取動作並選擇「重新排程」。

5. 請選擇下列其中一個選項：
   - 立即套用更新-如果有可用容量，請立即排定在目前的小時內執行動作。如果無法使用容量，我們會提供其他可用的時段供您選擇。
   - 在離峰窗口中安排-標記要在即將到來的離峰窗口中拾取的操作。不能保證在下一個窗口中實施更改。根據容量，它可能會在隨後的日子發生。
   - 重新排程此更新-允許您指定應用「變更」的自定義日期和時間。如果您指定的時間因為容量原因而無法使用，您可以選取不同的時段。
   - 取消預約更新-取消更新。此選項僅適用於選用的服務軟體更新。它不適用於自動調整動作或強制軟體更新。
6. 選擇儲存變更。

CLI

若要使用重新排程動作AWS CLI，請傳送UpdateScheduledAction請求。若要擷取動作 ID，請傳送`ListScheduledActions`要求。

下列要求會重新排定特定日期和時間的服務軟體更新：

```
aws opensearch update-scheduled-action \
  --domain-name my-domain \
  --action-id R20220721-P13 \
  --action-type "SERVICE_SOFTWARE_UPDATE" \
  --desired-start-time 1677348395000 \
  --schedule-at TIMESTAMP
```

回應：

```
{
   "ScheduledAction": {
      "Cancellable": true,
      "Description": "Cluster status is updated.",
      "Id": "R20220721-P13",
      "Mandatory": false,
      "ScheduledBy": "CUSTOMER",
      "ScheduledTime": 1677348395000,
      "Severity": "HIGH",
      "Status": "PENDING_UPDATE",
      "Type": "SERVICE_SOFTWARE_UPDATE"
```

```
    }
}
```

如果請求失敗，並顯示為`SlotNotAvailableException`，則表示您指定的時間由於容量原因而無法使用，而且您必須指定不同的時間。 OpenSearch 服務在回應中提供替代可用的插槽建議。

從自動調整維護時段移轉

如果網域是在 2023 年 2 月 16 日之前建立的，它可以使用維護時段來排程需要藍/綠部署的自動調整最佳化。您可以移轉現有的「自動調整」網域，改為使用離峰時段。

> **Note**
>
> 將網域移轉為使用離峰時段後，您無法還原為使用維護時段。

主控台

移轉網域以使用離峰時段

1. 在 Amazon OpenSearch 服務主控台中，選取要開啟其組態的網域名稱。
2. 前往「自動調整」標籤，然後選擇「編輯」。
3. 選取移轉至離峰時段。
4. 對於開始時間 (UTC)，請以世界協調時間 (UTC) 為離峰時段提供每日開始時間。
5. 選擇儲存變更。

CLI

若要使用從「自動調整」維護時段移轉至離峰時段AWS CLI，請傳送請求：UpdateDomainConfig

```
aws opensearch update-domain-config \
  --domain-name my-domain \
  --auto-tune-options
 DesiredState=ENABLED,UseOffPeakWindow=true,MaintenanceSchedules=[]
```

必須開啟離峰時段，才能將網域從「自動調整」維護時段移轉至離峰時段。您可以在個別要求或相同要求中啟用離峰時段。如需說明，請參閱 the section called “啟用離峰期”。

Amazon OpenSearch 服務中的通知

Amazon OpenSearch 服務中的通知包含有關網域效能和運作狀態的重要資訊。 OpenSearch Service 會通知您有關服務軟體更新、自動調整增強功能、叢集健全狀況事件和網域錯誤的資訊。通知適用於所有版本的 OpenSearch 和彈性搜索 OSS。

您可以在 OpenSearch 服務主控台的「通知」面板中檢視通知。有關 OpenSearch 服務的所有通知也在 Amazon EventBridge 中浮出水面。如需通知與範例事件的完整清單，請參閱the section called “監控事件”。

主題

- 開始使用通知
- 通知嚴重性
- 樣品 EventBridge 事件

開始使用通知

當您建立網域時，系統會自動啟用通知。移至 OpenSearch 服務主控台的「通知」面板，以監視和認可通知。每個通知都包含一些資訊，例如發佈時間、其相關網域、嚴重性和狀態等級以及簡短說明。您可以在主控台中檢視最多 90 天的歷史通知。

在存取 Notifications (通知) 面板或確認通知後，您可能會收到錯誤訊息，指出沒有執行 `es:ListNotifications` 或 `es:UpdateNotificationStatus` 的許可。若要解決此問題，請在 IAM 中為您的使用者或角色提供下列許可：

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Action": [
      "es:UpdateNotificationStatus",
      "es:ListNotifications"
    ],
    "Resource": "arn:aws:es:*:123456789012:domain/*"
  }]
}
```

IAM 主控台會擲回可安全忽略的錯誤 (「IAM 無法辨識一或多個動作」)。您也可以將 `es:UpdateNotificationStatus` 動作限定於特定網域。如需進一步了解，請參閱 the section called “政策元素參考”。

通知嚴重性

OpenSearch 服務中的通知可以是資訊性的，它與您已經採取的任何動作或您的網域的作業有關，也可以是可採取動作，而這些通知會要求您採取特定動作，例如套用強制性安全性修補程式。每個通知都有相關聯的嚴重性，可能是 `Informational`、`Low`、`Medium`、`High` 或 `Critical`。下表提供各級嚴重性的摘要：

嚴重性	描述	範例
`Informational`	與您的網域操作相關的資訊。	• 可用的服務軟體更新 • 自動調整已開始
`Low`	建議的動作，但如果未採取任何動作，則不會對網域可用性或效能造成不利影響。	• 自動調整已取消 • 高碎片計數警告
`Medium`	如果沒有採取建議的動作，但所採取的動作需要一段較長的時間，則可能會產生影響。	• 服務軟體更新已失敗 • 已超過碎片數量限制
`High`	必須採取緊急動作，以避免不利影響。	• 需要服務軟體更新 • 無法存取 KMS 金鑰
`Critical`	需要立即採取動作，以避免不利影響或從中恢復。	目前無可用

樣品 EventBridge 事件

下列範例顯示傳送至 Amazon 的 OpenSearch 服務通知事件 EventBridge。通知具有 `Informational` 嚴重性，因為更新是可選的：

```
{
  "version": "0",
```

```
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "Amazon OpenSearch Service Software Update Notification",
  "source": "aws.es",
  "account": "123456789012",
  "time": "2016-11-01T13:12:22Z",
  "region": "us-east-1",
  "resources": ["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail": {
    "event": "Service Software Update",
    "status": "Available",
    "severity": "Informational",
    "description": "Service software update [R20200330-p1] available."
  }
}
```

在 Amazon OpenSearch 服務中配置異地同步備份域

為了防止資料遺失並在服務中斷時將 Amazon Ser OpenSearch vice 叢集停機時間降至最低，您可以將節點分配到同一區域中的兩個或三個可用區域 (稱為異地同步備份的組態)。可用區域是每個區 AWS 域內的隔離位置。

對於執行生產工作負載的網域，我們建議使用異地同步備份搭配待命部署選項，該選項會建立下列組態：

- 跨三個區域部署的網域。
- 專用主節點和資料節點的最新一代執行個體類型。
- 三個專用主節點和三個（或三個中的倍數）資料節點。
- 您網域中的每個索引至少有兩個複本，或三個資料副本 (包括主要節點和複本) 的倍數。

本節的其餘部分提供有關這些配置的說明和上下文。

異地同步備份含待機

具備待命功能的異地同步備份是 Amazon Ser OpenSearch vice 網域的一種部署選項，可提供 99.99% 的可用性、生產工作負載的一致效能，以及簡化的網域組態和管理。當您將異地同步備份與待命模式搭配使用時，網域能夠抵禦基礎架構故障，不會影響效能或可用性。此部署選項透過強制執行許多最佳作法來達成此標準，例如指定的資料節點計數、主節點計數、執行個體類型、複本計數、軟體更新設定和 Auto-Tune 開啟。

當您將異地同步備份與待命搭配使用時， OpenSearch Service 會跨三個可用區域建立一個網域，每個區域都包含完整的資料複本，並且資料平均分佈在每個區域中。您的網域會將其中一個區域中的節點保留為待命狀態，這表示它們不會提供搜尋要求。當 OpenSearch Service 偵測到基礎架構中的故障時，它會在不到一分鐘的時間內自動啟動待命節點。網域會繼續提供索引和搜尋要求，而且任何影響都會限制在執行容錯移轉所需的時間內。不會重新分配資料或資源，這會導致叢集效能不受影響，也不會有可用性降低的風險。異地同步備份提供備用功能，無需額外費用。

您有兩個選項可以建立備用的網域 AWS Management Console。首先，您可以使用 Easy create 建立方法建立網域， OpenSearch Service 會自動使用預先決定的設定，其中包括下列項目：

- 三個可用區域，其中一個作為待命區域
- 三個專用的主節點和數據節點
- 在網域上啟用自動調整
- 用於數據節點的 GP3 存儲

您也可以選擇「標準」建立方法，然後選取「備用網域」作為部署選項。這可讓您自訂網域，同時仍強制執行待命關鍵功能，例如三個區域和三個主節點。建議您選擇三個之倍數的資料節點計數 (可用區域數目)。

建立網域之後，您可以瀏覽至網域詳細資料頁面，然後在叢集組態索引標籤中，確認具有待命功能的 3-AZ 顯示在可用區域下。

如果您在將現有網域移轉至備用狀態的異地同步備份時發生問題，請參閱疑難排解指南中的異地同步備份移轉至異地同步備份

限制

當您設定具備待命狀態的異地同步備份網域時，請考慮下列限制：

- 節點上的碎片總數不能超過 1000，集群上的碎片總數不能超過 75000，並且單個碎片的大小不能超過 65 GB。
- 具備待命功能的異地同步備份僅適用於`m5``c5`、`r5`、`r6g`、`c6gm6g`、`r6gd`和`i3`執行個體類型。如需支援執行個體的詳細資訊，請參閱支援的執行個體類
- 您只能使用佈建的 IOPS SSD、一般用途 SSD (GP3) 或執行個體支援的儲存裝置與待命狀態。
- 如果您UltraWarm在具有待命網域的異地同步備份上啟用，暖節點數目必須是正在使用的可用區域數目的倍數。

異地同步備份 (不含

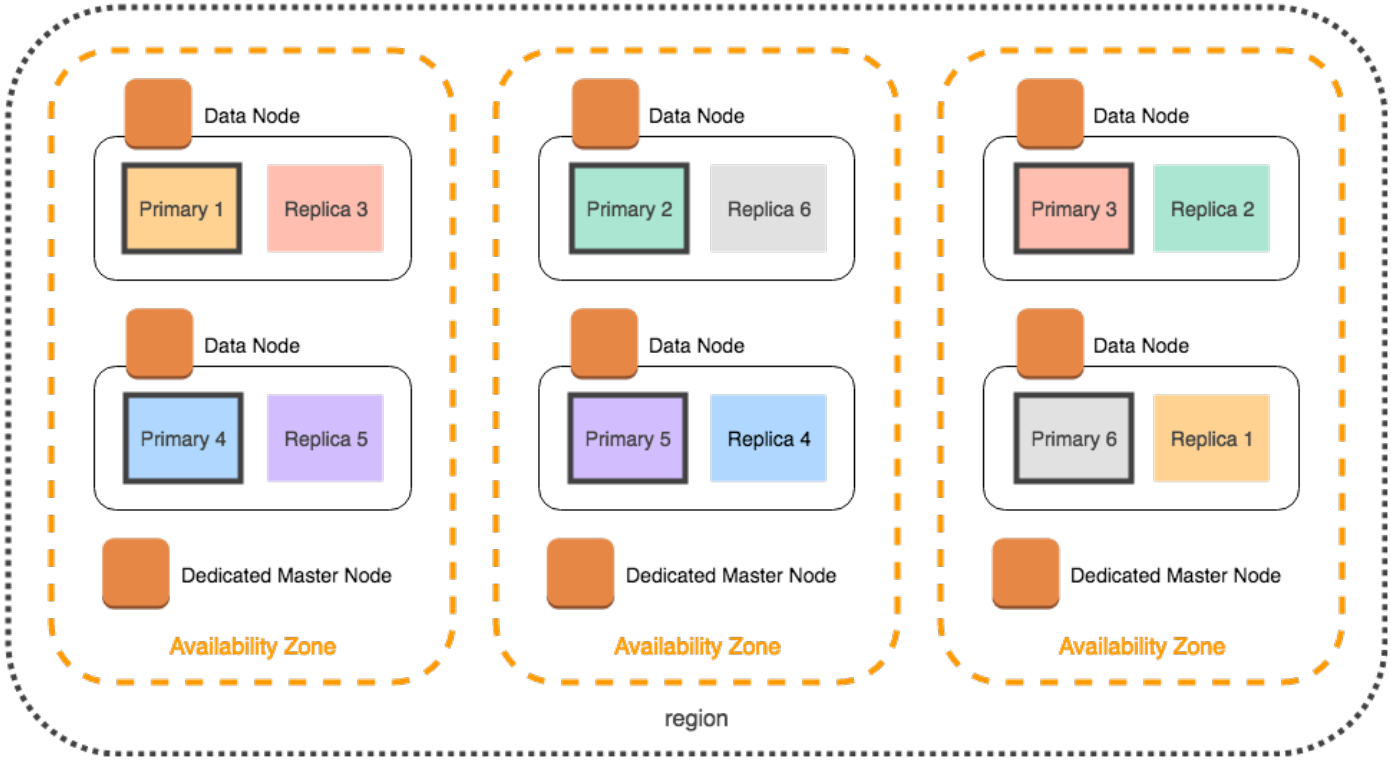
OpenSearch 服務仍支援異地同步備份 (無待命)，提供 99.9% 的可用性。節點分佈在可用區域，可用性取決於可用區域的數量和資料副本。而在待命狀態下，您必須使用最佳做法來設定網域，而無需待命，您可以選擇自己的可用區域、節點和複本數量。除非您現有的工作流程會因為建立待命網域而中斷，否則我們不建議使用此選項。

如果您選擇此選項，我們仍建議您選取三個可用區域，以保持節點、磁碟和單一可用區域故障的彈性。發生故障時，叢集會將資料重新分配至剩餘資源，以維持可用性和備援。此資料移動會增加叢集上的資源使用量，而且可能會影響效能。如果叢集的大小不正確，可能會遇到降級的可用性，這在很大程度上違反異地同步備份的目的。

設定不待命的網域的唯一方法 AWS Management Console 是選擇「標準」建立方法，然後選取「不含待命的網域」作為您的部署選項。

碎片分佈

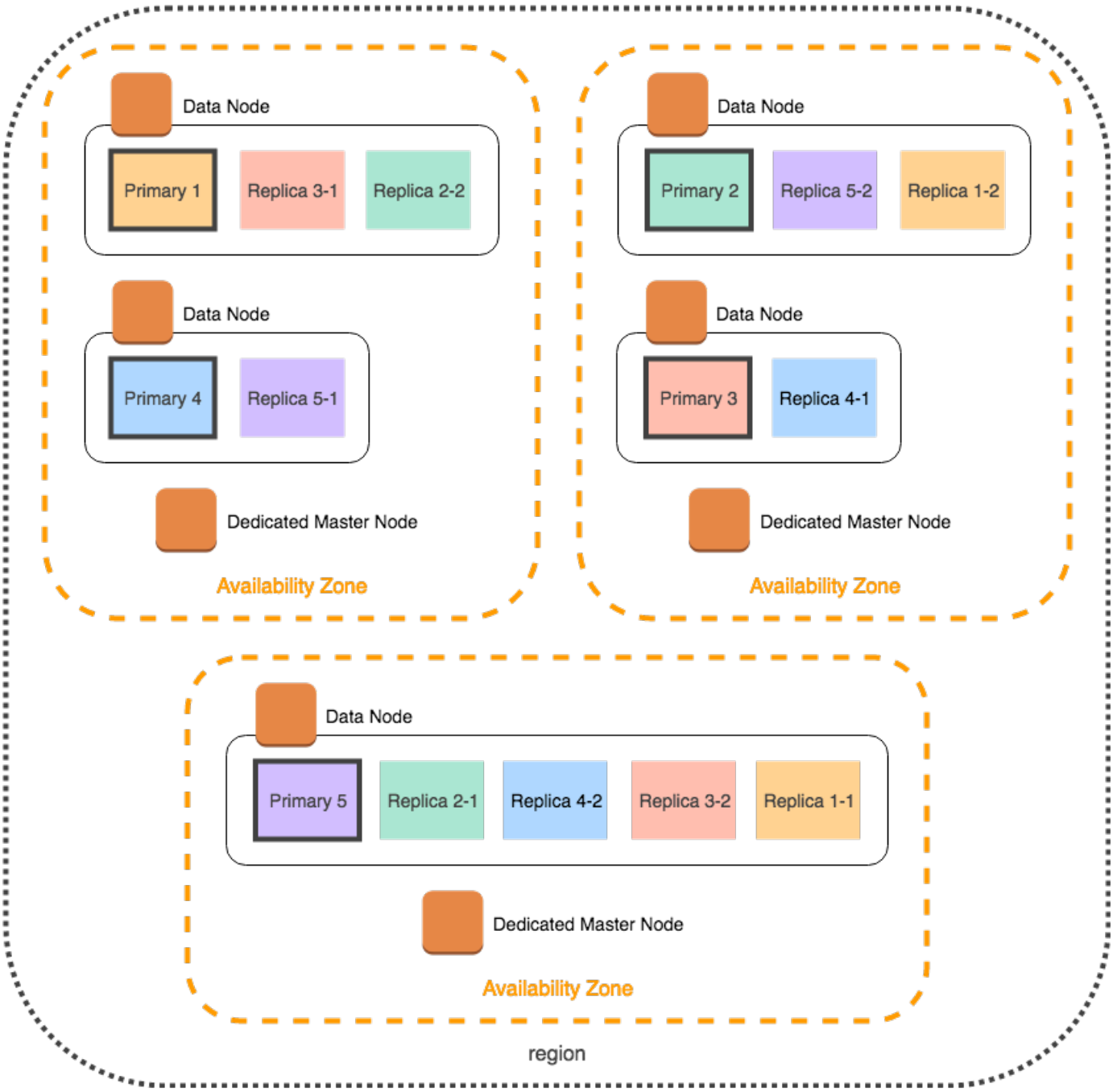
如果啟用異地同步備份 (不含待命)，則應為叢集中的每個索引建立至少一個複本。如果沒有複本，OpenSearch 服務就無法將您的資料副本散發到其他可用區域。還好任何索引的預設組態是複本計數 1。如下圖所示， OpenSearch Service 會盡最大努力將主要碎片及其對應的複本碎片分發到不同的區域。



除了按可用區域分配碎片之外， OpenSearch 服務還會按節點分配它們。然而，特定網域組態會導致不平衡的碎片計數。請考慮以下網域：

- 5 個資料節點
- 5 個主要碎片
- 2 個複本
- 3 個可用區域

在此情況下， OpenSearch Service 必須多載一個節點，才能跨區域散佈主要和複本碎片，如下圖所示。

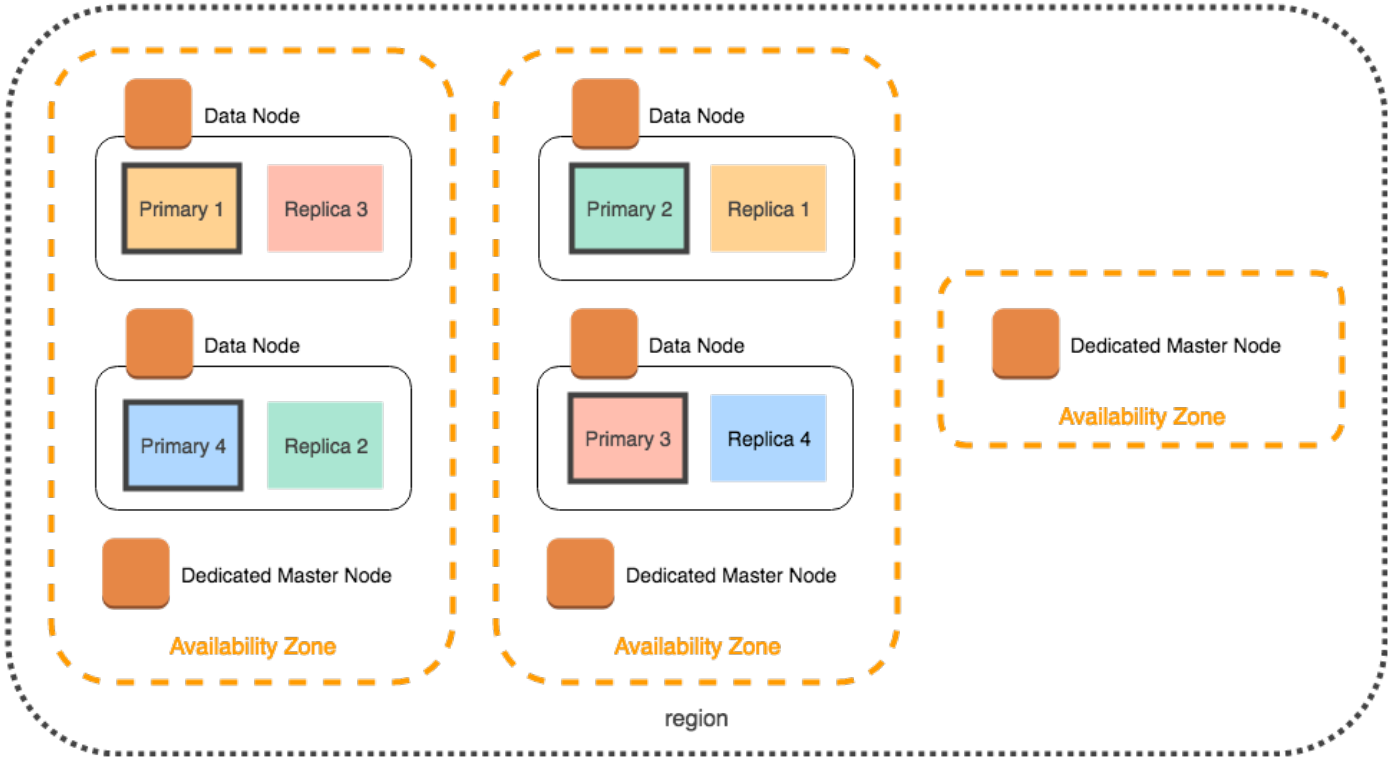


為了避免這些可能會造成個別節點壓力並損害效能的情況，建議您選擇異地同步備份搭配待命模式，或者當您計劃每個索引有兩個或多個複本時，選擇三個倍數的執行個體計數。

專用主節點分佈

即使您在設定網域時選取了兩個可用區域， OpenSearch Service 也會自動將專用主節點分配到三個可用區域。此分發可協助防止區域發生服務中斷時的叢集停機時間。如果建議的三個專用主節點和一個可

用區域在您使用時發生故障，您的叢集仍具有專用主節點的仲裁 (2)，並且可以選擇新的主節點。下圖示範了此組態。



如果您選擇了在三個可用區域中已無法使用的上一代執行個體類型，則適用以下狀況：

- 如果您為網域選擇了三個可用區域， OpenSearch 服務會擲回錯誤。請選擇不同的執行個體類型，然後再試一次。
- 如果您為網域選擇了兩個可用區域， OpenSearch Service 會將專用主節點分散到兩個區域。

可用區域中斷

可用區域中斷雖然極少發生，但仍有可能出現。下表列出不同多個可用區在中段期間的組態和行為。表格中的最後一列適用於具備待命功能的異地同步備份，而所有其他資料列的組態僅適用於異地同步備份 (不含待命)。

區域中的可用區域數量	您選擇的可用區域數量	專用主節點數目	如果一個可用區域中斷時的行為
2 或以上	2	0	停機。您的叢集會失去一半的資料節點，且必須至少替換剩餘可用區域中的其中一個，然後才能選擇主節點。
2	2	3	50/50 的停機機會。 OpenSearch Service 將兩個專用主節點分配到一個可用區域，另一個可用區域： • 如果擁有一個專用主節點的可用區域遭遇中斷，則剩餘可用區域中的兩個專用主節點可以選擇一個主節點。 • 如果擁有兩個專用主節點的可用區域遭遇中斷，則在剩餘可用區域恢復之前，叢集都無法使用。
3 或以上	2	3	沒有停機時間。 OpenSearch Service 會自動將專用主節點分配到三個可用區域，因此剩餘的兩個專用主節點可以選擇一個主節點。
3 或以上	3	0	不會停機。概略而言您資料節點的三分之二仍然可以選擇主節點。
3 或以上	3	3	不會停機。剩餘的兩個專用主節點可以選擇主節點。

在所有組態中，無論原因為何，節點故障都可能導致叢集的剩餘資料節點經歷一段時間的負載增加，而 OpenSearch Service 會自動設定新節點以取代現在遺漏的節點。

例如，如果三個區域組態中的可用區域中斷，則三分之二的資料節點必須處理與叢集一樣多的請求。當處理這些請求時，剩餘的節點也會在上線時複製碎片到新節點，而這可能近一步影響效能。如果可用性與您的工作負載息息相關，請考慮在叢集中新增資源，以便舒緩此問題。

> **Note**
>
> OpenSearch 服務會透明地管理異地同步備份網域，因此您無法手動模擬可用區域中斷情況。

在一個啟動您的 Amazon OpenSearch 服務域 VPC

您可以啟動 AWS 將資源 (例如 Amazon OpenSearch 服務網域) 放入虛擬私有雲端 (VPC)。A VPC 是專用於您的虛擬網路 AWS 帳戶。 它在邏輯上與其他虛擬網絡隔離 AWS 雲端。將 OpenSearch Service 網域置於中，VPC可讓 OpenSearch 服務與其他服務之間的安全通訊，VPC而不需要網際網路閘道、NAT裝置或VPN連線。所有流量都安全地保持在 AWS 雲端。

> **Note**
>
> 如果您將 OpenSearch Service 網域放在一個內VPC，您的電腦必須能夠連線到VPC. 此連線通常採用傳輸閘道VPN、受管理網路或 Proxy 伺服器的形式。您無法從外部直接存取您的網域VPC。

主題

- VPC與公共領域
- 限制
- 架構

VPC與公共領域

以下是網域與公有VPC網域不同的一些方式。稍後會更詳細地說明各項差異。

- 由於其邏輯隔離，與使用公用端點的網域相比，位於內部的網域VPC具有額外的安全層。
- 雖然可以從任何連接互聯網的設備訪問公共域，但VPC域需要某種形式的代理VPN或代理。
- 與公用網域相比，VPC網域在主控台中顯示的資訊較少。特別是，Cluster health (叢集運作狀態) 索引標籤並不包含碎片資訊，並且 Indices (索引) 索引標籤不會出現。
- 網域端點採用不同的形式 (`https://search-domain-name` 與 `https://vpc-domain-name`)。
- 您無法將 IP 型存取原則套用至位於內部的網域，VPC因為安全性群組已強制執行 IP 型存取原則。

限制

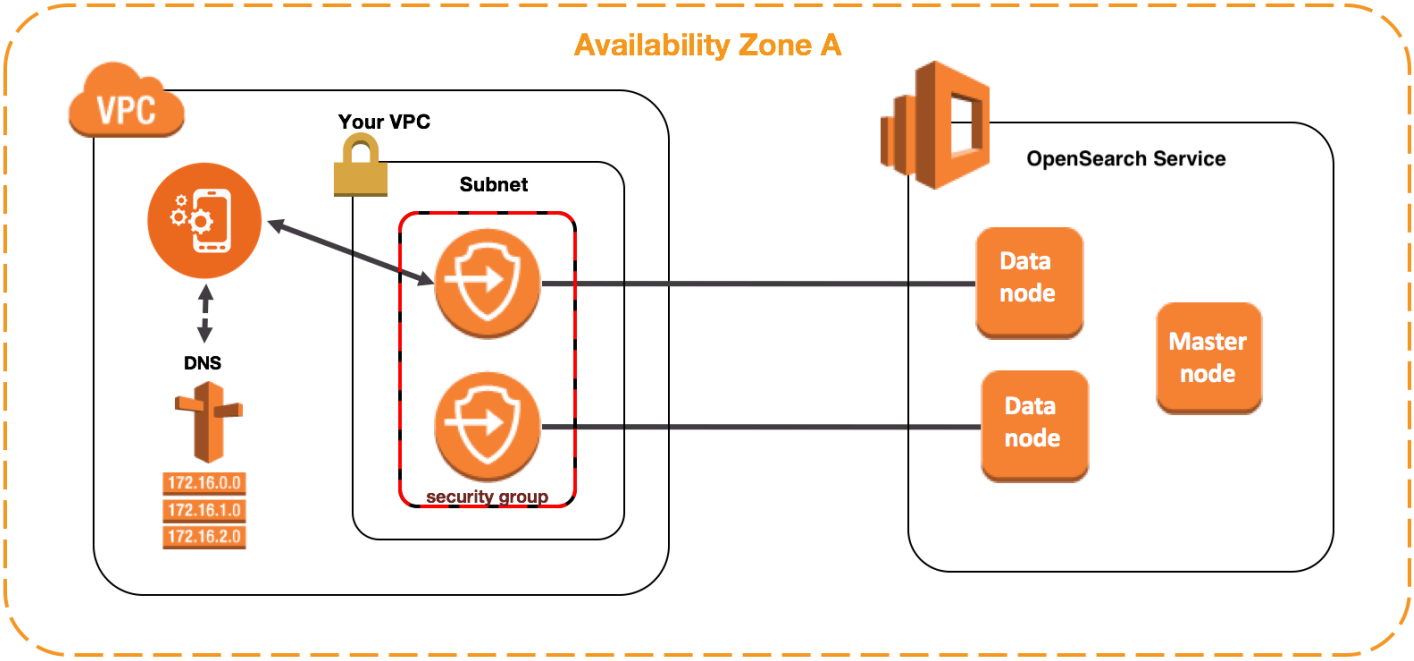
在中操作 OpenSearch 服務域VPC有以下限制：

- 如果您在中啟動新網域VPC，稍後無法將其切換為使用公用端點。相反的情況也是如此：如果您使用公共端點創建域，則以後無法將其放置在VPC. 反之，您必須建立新網域並遷移您的資料。
- 您可以在網域內啟動網域，VPC也可以使用公用端點，但不能同時啟動兩者。您必須在建立網域時選擇其中一個。
- 您無法在使用專用租賃的網域中啟動網域。VPC您必須使用已設定為「預設」VPC 的租用。
- 將網域置於網域之後VPC，您無法將其移至其他網路VPC，但您可以變更子網路和安全性群組設定。
- 若要存取位於某個網域的預設 OpenSearch 儀表板安裝VPC，使用者必須具有的存取權VPC。此程序會因網路組態而異，但可能涉及連線至VPN或受管理的網路，或使用 Proxy 伺服器或傳輸閘道。若要進一步了解the section called “關於網VPC域的存取原則”，請參閱 Amazon VPC 使用者指南和the section called “控制 OpenSearch 儀表板的存取”。

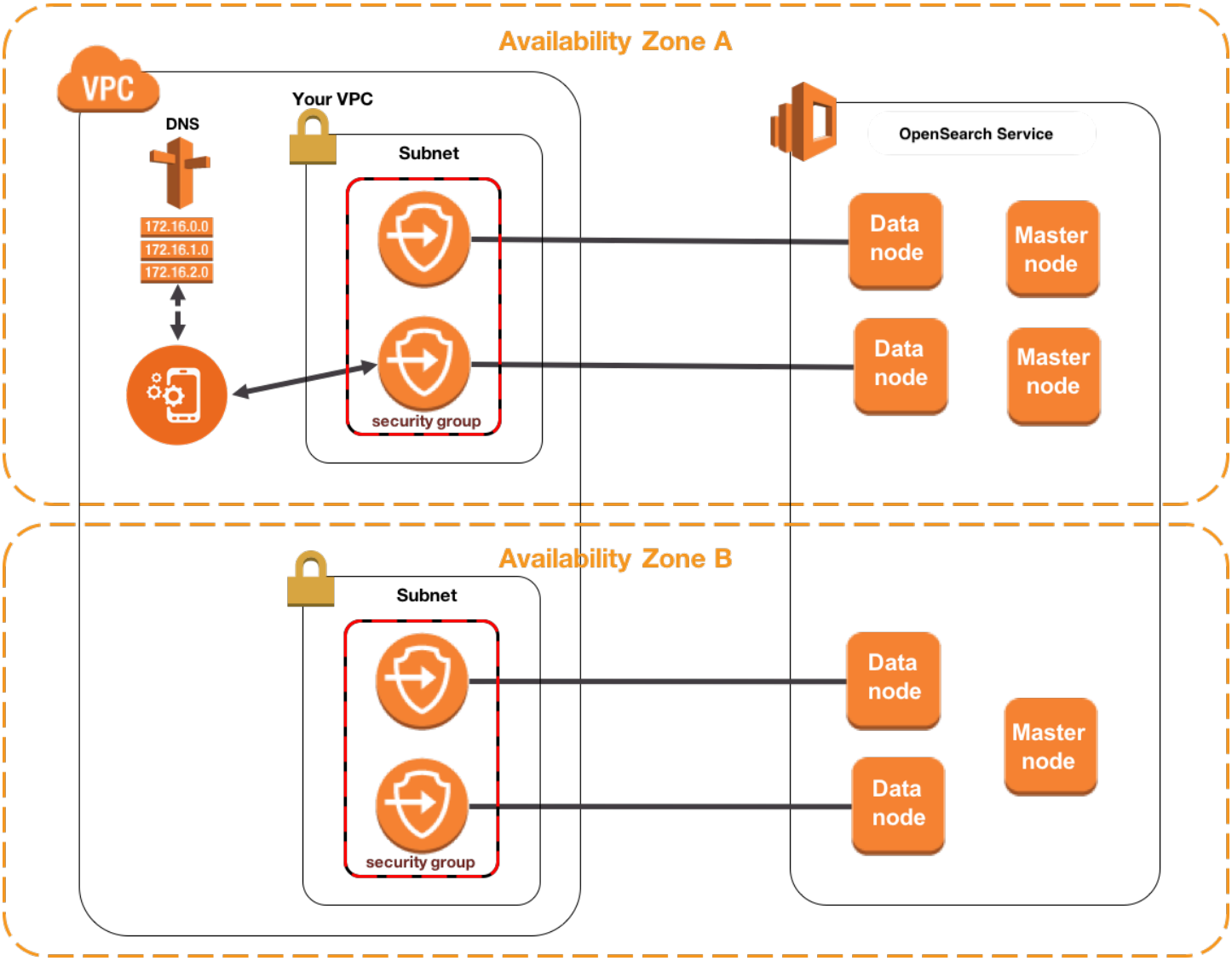
架構

為了支援VPCs， OpenSearch 服務會將端點放入您VPC的. 如果您為網域啟用了多個可用區，每個子網路都必須位於相同區域中的不同可用區域內。如果您只使用一個可用區域，則 OpenSearch 服務只會將端點置於一個子網路中。

下圖顯示一個可用區域的VPC架構：



下圖顯示兩個可用區域的VPC架構：



OpenSearch 服務也會在中為每個資料節點放置VPC一個 elastic network interface (ENI)。OpenSearch 服務會從子網路的位址範圍中，為每個人指派一個私ENI有 IP 位IPv4址。此服務也會指派 IP 位址的公用DNS主機名稱 (也就是網域端點)。您必須使用公用DNS服務將端點（即DNS主機名稱）解析為資料節點適當的 IP 位址：

- 如果您透過將`enableDnsSupport`選項設定為 `true` (預設值) 來VPC使用 Amazon 提供的DNS伺服器，則 OpenSearch 服務端點的解析將會成功。
- 如果您VPC使用私人DNS伺服器，且伺服器可以連線到公用授權DNS伺服器來解析DNS主機名稱，則 OpenSearch Service 端點的解析也會成功。

由於 IP 地址可能變更，您應該定期解析網域端點，以便您可以隨時存取正確的資料節點。建議您將DNS解析度間隔設定為一分鐘。如果您使用的是用戶端，您還應該確保清除用戶端中的DNS快取。

從公共訪問遷移到VPC訪問

建立網域時，您可以指定該網域是否應具有公用端點或位於VPC. 建立之後，您無法從一個切換到另一個。反之，您必須建立新網域並且手動重新建立索引或遷移您的資料。快照提供方便的方法遷移資料。如需有關拍攝和恢復快照的資訊，請參閱the section called “建立索引快照”。

關於網VPC域的存取原則

將您的 OpenSearch Service 網域置於一個可VPC提供固有且強大的安全層。當您建立具有公用存取的網域時，端點的格式如下：

```
https://search-domain-name-identifier.region.es.amazonaws.com
```

如「公有」標籤建議，這個端點可從任何連接網際網路的裝置存取，即使您可以 (且應該) 控制對其的存取。如果您在 Web 瀏覽器中存取端點，您可能會收到 `Not Authorized` 訊息，但請求會到達網域。

當您建立具有VPC存取權的網域時，端點看起來類似於公用端點：

```
https://vpc-domain-name-identifier.region.es.amazonaws.com
```

如果您嘗試在 Web 瀏覽器中存取端點，不過您可能會發現請求逾時。若要執行基本GET要求，您的電腦必須能夠連線到VPC. 此連線通常採用傳輸閘道VPN、受管理網路或 Proxy 伺服器的形式。有關可採用的各種形式的詳細資訊，請參閱 Amazon VPC 使用者指南VPC中的範例。關於以開發為中心的範例，請參閱the section called “測試VPC網域”。

除了此連線需求之外，還可VPCs讓您透過安全性群組管理網域的存取權。對於許多使用案例，這個安全功能的組合已足夠，而您可能感覺可安心將開放的存取政策套用到網域。

使用開放存取原則操作並不意味著網際網路上的任何人都可以存取 OpenSearch 服務網域。相反，這意味著如果請求到達 OpenSearch 服務域，並且相關聯的安全組允許它，則域接受該請求。唯一的例外是，如果您使用精細的存取控制或指定IAM角色的存取原則。在這些情況下，如果網域要接受請求，安全群組必須允許它，並且它必須使用有效的憑證進行簽署。

> **Note**
>
> 由於安全性群組已強制執行 IP 型存取原則，因此您無法將 IP 型存取原則套 OpenSearch 用至位於. VPC 如果您使用公有存取，IP 為基礎的政策仍然可用。

開始之前:VPC存取的先決條件

您必須先執行下列動作，才能啟用VPC與新 OpenSearch 服務網域之間的連線：

- 創建一個 VPC

  要創建您的VPC，您可以使用 Amazon VPC 控制台， AWS CLI，或其中一個 AWS SDKs。如需詳細資訊，請參閱 Amazon VPC 使用者指南VPCs中的使用。如果您已經擁有VPC，則可以跳過此步驟。

- 預留 IP 地址

  OpenSearch Service 會將網路介面放置在的子網路中，藉此啟用網域的連線VPC。VPC每個網路界面都與 IP 地址關聯。您必須在子網路中保留足夠數量的 IP 地址給網路界面。如需詳細資訊，請參閱保留VPC子網路中的 IP 位址。

測試VPC網域

增強的安全性VPC可以使連接到您的域和運行基本測試成為一個挑戰。如果您已經有 OpenSearch Service VPC 網域，而不想建立VPN伺服器，請嘗試下列程序：

1. 對於網域的存取政策，請選擇 Only use fine-grained access control (僅使用精細存取控制)。完成測試後，您隨時可以更新此設定。
2. 在與您的 OpenSearch 服務網域相同VPC、子網路和安全群組中建立 Amazon Linux Amazon EC2 執行個體。

   由於此執行個體是用於進行測試，只需執行極少的工作，因此請選擇較便宜的執行個體類型，如 `t2.micro`。指派公有 IP 地址給執行個體，然後建立新的金鑰對或選擇現有的金鑰對。如果您建立新的金鑰，請將其下載到您的 `~/.ssh` 目錄。

   若要進一步了解如何建立執行個體，請參閱開始使用 Amazon EC2 Linux 執行個體。
3. 將網際網路閘道新增至您的VPC.
4. 在您的路由表中VPC，新增路由。在「目的地」中，指定包含電腦公用 IP 位址的CIDR區塊。對於 Target (目標)，指定您剛建立的網際網路閘道。

   例如，您可以指定 `123.123.123.123/32` 以只用於您的電腦，或指定 `123.123.123.0/24` 以用於一個範圍的電腦。
5. 對於安全群組，指定兩個傳入規則：

Type	通訊協定	連接埠範圍	來源
SSH	TCP(六)	22	*your-cidr-block*
HTTPS	TCP(六)	443	*your-security-group-id*

第一個規則可讓您SSH進入EC2執行個體。第二個允許EC2執行個體透過與 Ser OpenSearch vice 網域通訊HTTPS。

6. 從終端機執行下列命令：

```
ssh -i ~/.ssh/your-key.pem ec2-user@your-ec2-instance-public-ip -N -L
 9200:vpc-domain-name.region.es.amazonaws.com:443
```

此命令會建立通SSH道，透過EC2執行個體將要求轉送至 https://localhost:9200 至您的 OpenSearch 服務網域。在命令中指定連接埠 9200 會模擬本機 OpenSearch 安裝，但使用您想要的任何連接埠。 OpenSearch 服務只接受透過連接埠 80 (HTTP) 或 443 (HTTPS) 的連線。

此命令不會提供任何意見回饋，並且無限期地執行。若要停止命令，請按 `Ctrl + C`。

7. 在您的網絡瀏覽器中導航到 https://localhost:9200/_dashboards/。您可能需要認可安全例外狀況。

或者，您也可以使用 https://localhost:9200curl、Postman 或您愛用的程式設計語言，傳送請求到。

> **Tip**
>
> 如果因為憑證不相符而遇到 Curl 錯誤，請嘗試 `--insecure` 旗標。

在子網路中保留 IP 位VPC址

OpenSearch 服務會將網路介面放置在子網路中 VPC (VPC如果您啟用多個可用區域，則會將網域連線至 VPC 每個網路界面都與 IP 地址關聯。建立 OpenSearch Service 網域之前，每個子網路中必須有足夠數目的可用 IP 位址，以容納網路介面。

以下是基本公式： OpenSearch Service 在每個子網路中保留的 IP 位址數量是資料節點數目的三倍，除以可用區域數目。

範例

- 如果某個網域有 9 個資料節點和 3 個可用區域，則每個子網路的 IP 計數為 9 * 3 / 3 = 9。
- 如果某個網域有 8 個資料節點和 2 個可用區域，則每個子網路的 IP 計數為 8 * 3 / 2 = 12。
- 如果某個網域有 6 個資料節點和 1 個可用區域，則每個子網路的 IP 計數為 6 * 3 / 1 = 18。

當您建立網域時， OpenSearch Service 會保留 IP 位址、針對網域使用部分位址，並保留其餘的 IP 位址供藍色/綠色部署使用。您可以在 Amazon EC2 主控台的「網路界面」區段中查看網路界面及其相關聯的 IP 地址。「描述」欄會顯示與網路介面相關聯的 OpenSearch 服務網域。

> **Tip**
>
> 建議您為 OpenSearch 服務保留的 IP 位址建立專用子網路。透過使用專用的子網路，可避免與其他應用程式和服務重疊，並確保您可以預留額外的 IP 地址供未來若需要擴展叢集時使用。若要深入了解，請參閱在 VPC.

用VPC於存取的服務連結角色

服務連結角色是一種獨特的IAM角色類型，可將權限委派給服務，以便它可以代表您建立和管理資源。OpenSearch 服務需要服務連結角色才能存取您的VPC、建立網域端點，以及將網路介面放置在您VPC的子網路中。

OpenSearch 當您使用服務主控台在中建立網域時， OpenSearch 服務會自動建立角色VPC。若要讓此自動建立成功，您必須有 `iam:CreateServiceLinkedRole` 動作的許可。若要深入了解，請參閱IAM使用者指南中的服務連結角色權限。

OpenSearch Service 建立角色之後，您可以使用IAM主控台檢視它 (`AWSServiceRoleForAmazonOpenSearchService`)。

如需此角色許可以及如何刪除它的完整資訊，請參閱the section called “使用服務連結角色”。

在 Amazon OpenSearch 服務中創建索引快照

Amazon OpenSearch 服務中的快照是叢集索引和狀態的備份。狀態包含叢集設定、節點資訊、索引設定和碎片分配。

OpenSearch 服務快照有下列形式：

- 自動快照僅適用叢集復原。如果發生紅色叢集狀態或資料遺失，您可以使用它們來還原您的網域。如需詳細資訊，請參閱下方的還原快照。 OpenSearch 服務可將自動快照存放在預先設定的 Amazon S3 儲存貯體中，無需額外付費。
- 手動快照適用於叢集復原，或者將資料從一個叢集移至另一個叢集。您必須初始化手動快照。這些快照會存放在您自己的 Simple Storage Service (Amazon S3) 儲存貯體中，而且需支付標準 S3 費用。如果您有來自自我管理 OpenSearch 叢集的快照，則可以使用該快照移轉至 OpenSearch 服務網域。如需詳細資訊，請參閱移轉至 Amazon OpenSearch 服務。

所有 OpenSearch 服務網域都會建立自動快照，但頻率在下列方面有所不同：

- 對於執行中的網域 OpenSearch 或 Elasticsearch 5.3 及更新版本， OpenSearch 服務會每小時擷取每小時自動快照，並保留最多 336 個快照，持續 14 天。由於每小時快照的增量改進性質，所以中斷較少。在發生網域問題時，它們還提供較新的復原點。
- 對於執行 Elasticsearch 5.1 及更早版本的網域， OpenSearch 服務會在您指定的小時內擷取每日自動快照，最多可保留 14 個快照，而且不會保留任何快照資料超過 30 天。

如果您的叢集進入紅色狀態，所有自動快照都會失敗，而叢集狀態會持續存在。如果您未在兩週內修正該問題，則可能會永久遺失叢集中的資料。如需疑難排解步驟，請參閱the section called “紅色叢集狀態”。

主題

- 必要條件
- 註冊手動快照儲存庫
- 手動拍攝快照
- 還原快照
- 刪除手動快照
- 使用快照管理自動化快照
- 使用索引狀態管理自動化快照
- 使用 Curator 進行快照

必要條件

若要手動建立快照，您必須使用 IAM 和 Simple Storage Service (Amazon S3)。嘗試拍攝快照之前，請先確認符合以下先決條件：

先決條件	描述
S3 儲存貯體	建立 S3 儲存貯體以存放 OpenSearch 服務網域的手動快照。如需指示說明，請參閱 Amazon Simple Storage Service 使用者指南中的建立儲存貯體。 請記住儲存貯體的名稱以在下列位置使用它： • 連接至您 IAM 角色的 IAM 政策的 `Resource` 陳述式 • 用於註冊快照儲存庫的 Python 用戶端 (如果您使用此方法) **Important** 請勿將 S3 Glacier 生命週期規則套用至此儲存貯體。手動快照不支援 S3 Glacier 儲存類別。
IAM 角色	建立 IAM 角色以將許可委派給 OpenSearch 服務。如需說明，請參閱 IAM 使用者指南中的建立 IAM 角色 (主控台)。本章其餘各節稱此角色為 `TheSnapshotRole` 。 連接 IAM 政策 將下列政策連接至 `TheSnapshotRole` 以允許存取 S3 儲存貯體：

```
{
  "Version": "2012-10-17",
  "Statement": [{
      "Action": [
        "s3:ListBucket"
      ],
      "Effect": "Allow",
      "Resource": [
        "arn:aws:s3::: s3-bucket-name "
      ]
    },
    {
      "Action": [
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject"
      ],
      "Effect": "Allow",
```

先決條件	描述

	"Resource": [
	"arn:aws:s3::: s3-bucket-name /*"
	]
	}
	]
	}
	
	如需有關將政策連接至角色的說明，請參閱 IAM 使用者指南中的新增 IAM 身分許可。
	
	編輯信任關係
	
	編輯的信任關係，`TheSnapshotRole` 以在`Principal` 陳述式中指定 OpenSearch Service，如下列範例所示：
	
	{
	"Version": "2012-10-17",
	"Statement": [{
	"Sid": "",
	"Effect": "Allow",
	"Principal": {
	"Service": "es.amazonaws.com"
	},
	"Action": "sts:AssumeRole"
	}]
	
	}
	
	如需編輯信任關係的說明，請參閱 IAM 使用者指南中的修改角色信任政策。

先決條件	描述

許可	若要註冊快照儲存庫，您必須能夠傳遞TheSnapshotRole 至 OpenSearch 服務。您也需要存取 es:ESHttpPut 動作。若要授予這兩個許可，請將下列政策連接至其憑證用於簽署請求的 IAM 角色：
	
	{
	"Version": "2012-10-17",
	"Statement": [
	{
	"Effect": "Allow",
	"Action": "iam:PassRole",
	"Resource": "arn:aws:iam:: *123456789012* :role/*TheSnapshotRole* "
	},
	{
	"Effect": "Allow",
	"Action": "es:ESHttpPut",
	"Resource": "arn:aws:es: *region*:*123456789012* :domain/*domain-name* /*"
	}
	]
	}
	
	如果您的使用者或角色沒有通過的iam:PassRole 權限TheSnapshotRole ，則在下一個步驟中嘗試註冊存放庫時，可能會遇到下列常見錯誤：
	
	$ python register-repo.py
	{"Message":"User: arn:aws:iam:: *123456789012* :user/*MyUserAccount* is not authorized to perform: iam:PassRole on resource: arn:aws:iam:: *123456789012* :role/*TheSnapshotRole* "}

註冊手動快照儲存庫

您必須先向 OpenSearch Service 註冊快照儲存庫，才能建立手動索引快照。這項一次性作業會要 AWS 求您使用允許存取的認證來簽署要求TheSnapshotRole，如中所述the section called “必要條件”。

步驟 1：在 OpenSearch 儀表板中對應快照角色 (如果使用精細的存取控制)

精細存取控制會在註冊儲存庫時進行額外的步驟。即使您將 HTTP 基本身分驗證用於所有其他目的，您也需要將 `manage_snapshots` 角色映射至擁有 `iam:PassRole` 許可能夠傳遞 `TheSnapshotRole` 的 IAM 角色。

1. 導覽至 OpenSearch 服務網域的 OpenSearch 儀表板外掛程式。您可以在 OpenSearch 服務主控台上的網域儀表板上找到儀表板端點。
2. 從主選單中選擇 Security (安全性)、Roles (角色)，然後選取 manage_snapshots 角色。
3. 選擇 Mapped users (已映射的使用者)、Manage mapping (管理映射)。
4. 新增擁有許可傳遞 `TheSnapshotRole` 之角色的 ARN。將角色 ARN 放在 Backend roles (後端角色) 下。

   ```
   arn:aws:iam::123456789123:role/role-name
   ```

5. 選擇 Map (映射)，並確認使用者或角色顯示在 Mapped users (已映射的使用者) 中。

步驟 2：註冊儲存庫

下列 [快照] 索引標籤示範如何註冊快照目錄。如需在移轉至新網域後加密手動快照和註冊快照的特定選項，請參閱相關索引標籤。

Snapshots

若要註冊快照存放庫，請將 PUT 要求傳送至 OpenSearch 服務網域端點。您可以使用 curl、Python 用戶端範例、郵遞員或其他方法來傳送已簽署的要求來註冊快照儲存庫。請注意，您無法在 OpenSearch 儀表板主控台中使用 PUT 要求來註冊存放庫。

請求採用下列格式：

```
PUT domain-endpoint/_snapshot/my-snapshot-repo-name
{
  "type": "s3",
  "settings": {
    "bucket": "s3-bucket-name",
    "base_path": "my/snapshot/directory",
    "region": "region",
    "role_arn": "arn:aws:iam::123456789012:role/TheSnapshotRole"
  }
}
```

> **Note**
>
> 儲存庫名稱不能以 "cs-" 開頭。此外，您不應該從多個網域寫入同一個儲存庫。只有一個網域應具有儲存庫的寫入存取權。

如果您的網域存放在 Virtual Private Cloud (VPC) 中，您的電腦必須連接到 VPC，才能讓請求成功註冊快照儲存庫。存取 VPC 因網路組態而異，但可能牽涉到連線 VPN 或公司網路。要檢查您是否可以訪問 OpenSearch 服務域，請`https://your-vpc-domain.region.es.amazonaws.com`在 Web 瀏覽器中導航到並確認您收到默認的 JSON 響應。

當 Amazon S3 儲存貯體位於 OpenSearch網域以 AWS 區域 外的其他儲存貯體時，請將參數新增`"endpoint": "s3.amazonaws.com"`至請求。

Encrypted snapshots

您目前無法使用 AWS Key Management Service (KMS) 金鑰加密手動快照，但可以使用伺服器端加密 (SSE) 來保護它們。

若要針對您用作快照儲存庫的儲存貯體開啟 SSE (含 S3 代管金鑰)，請新增`"server_side_encryption": true`至 PUT 要求的`"settings"`區塊。如需詳細資訊，請參閱 Amazon Simple Storage Service 使用者指南中的使用具有 Simple Storage Service (Amazon S3) 管理的加密金鑰的伺服器端加密保護資料。

或者，您可以在用作快照儲存庫的 S3 儲存貯體上使用 AWS KMS 金鑰進行伺服器端加密。如果您使用此方法，請確保提供對用於加密 S3 儲存貯體的 AWS KMS 金鑰的`TheSnapshotRole`權限。如需詳細資訊，請參閱 AWS KMS中的金鑰政策。

Domain migration

註冊快照儲存庫是一次性操作。但要從一個網域遷移到另一個網域，必須在舊網域和新網域上註冊相同的快照儲存庫。儲存庫名稱是任意的。

遷移至新網域或註冊具有多個網域的相同儲存庫時，請考慮下列準則：

- 在新網域上註冊儲存庫時，請將 `"readonly": true` 新增至 PUT 請求的 `"settings"` 區塊。此設定可防止您意外地從舊網域中覆寫資料。只有一個網域應具有儲存庫的寫入存取權。
- 如果您要將資料遷移到另一個網域 (例如 AWS 區域，從 us-east-2 中的舊網域和值區移轉至 us-west-2 中的新網域)，請在 PUT 陳述式`"endpoint": "s3.amazonaws.com"`中取代`"region": "region"`為，然後重試要求。

使用 Python 用戶端範例

Python 用戶端比簡單的 HTTP 請求更容易自動化，並且具有更好的可重複使用性。如果您選擇使用此方法來註冊快照儲存庫，請將下列範例 Python 程式碼儲存為 Python 檔案，例如 `register-repo.py`。用戶端需要 AWS SDK for Python (Boto3)、請求和 requests-aws4auth 套件。用戶端包含其他快照操作的註解範例。

更新範本程式碼中的下列變數：`host`、`region`、`path` 以及 `payload`。

```
import boto3
import requests
from requests_aws4auth import AWS4Auth

host = '' # domain endpoint
region = '' # e.g. us-west-1
service = 'es'
credentials = boto3.Session().get_credentials()
awsauth = AWS4Auth(credentials.access_key, credentials.secret_key, region, service,
 session_token=credentials.token)

# Register repository

path = '/_snapshot/my-snapshot-repo-name' # the OpenSearch API endpoint
url = host + path

payload = {
  "type": "s3",
  "settings": {
    "bucket": "s3-bucket-name",
    "base_path": "my/snapshot/directory",
    "region": "us-west-1",
    "role_arn": "arn:aws:iam::123456789012:role/snapshot-role"
  }
}

headers = {"Content-Type": "application/json"}

r = requests.put(url, auth=awsauth, json=payload, headers=headers)

print(r.status_code)
print(r.text)

# # Take snapshot
```

```
#
# path = '/_snapshot/my-snapshot-repo-name/my-snapshot'
# url = host + path
#
# r = requests.put(url, auth=awsauth)
#
# print(r.text)
#
# # Delete index
#
# path = 'my-index'
# url = host + path
#
# r = requests.delete(url, auth=awsauth)
#
# print(r.text)
#
# # Restore snapshot (all indexes except Dashboards and fine-grained access control)
#
# path = '/_snapshot/my-snapshot-repo-name/my-snapshot/_restore'
# url = host + path
#
# payload = {
#   "indices": "-.kibana*,-.opendistro_security,-.opendistro-*",
#   "include_global_state": False
# }
#
# headers = {"Content-Type": "application/json"}
#
# r = requests.post(url, auth=awsauth, json=payload, headers=headers)
#
# print(r.text)
#
# # Restore snapshot (one index)
#
# path = '/_snapshot/my-snapshot-repo-name/my-snapshot/_restore'
# url = host + path
#
# payload = {"indices": "my-index"}
#
# headers = {"Content-Type": "application/json"}
#
# r = requests.post(url, auth=awsauth, json=payload, headers=headers)
#
```

```
# print(r.text)
```

手動拍攝快照

快照不是即時的。它們需要時間才能完成，並且不代表叢集的完美 point-in-time 視圖。當快照仍在進行中，您還是可以對文件編製索引並對叢集發出其他請求，但新文件以及對現有文件的更新一般不包括在快照中。快照包含初 OpenSearch 始化快照時存在的主要碎片。視快照執行緒集區的大小而定，快照中可能附有相距些許時間差的不同碎片。如需快照最佳作法，請參閱the section called “改善快照效能”。

快照儲存與效能

OpenSearch 快照是增量的，表示它們只會儲存自上次成功快照以來變更的資料。這種增量性質表示頻率高和頻率低的快照之間的磁碟用量差異通常很小。換言之，每小時拍攝快照長達一週 (總共 168 個快照)，可能不會比在週末拍攝單一快照使用更多的磁碟空間。此外，您拍攝快照的頻率越高，完成快照所需的時間越少。例如，每日快照可能需要 20-30 分鐘才能完成，而每小時快照可能在幾分鐘內即可完成。一些 OpenSearch 用戶每半小時拍攝快照的頻率。

建立快照

建立快照時可以指定以下資訊：

- 快照儲存庫的名稱
- 快照的名稱

為了方便和簡潔，本章中的範例使用 Curl 這個常見的 HTTP 用戶端。要將用戶名和密碼傳遞給您的 curl 請求，請參閱入門教程。

如果您的存取原則指定使用者或角色，則必須簽署快照請求。對於捲曲，您可以使用 7.75.0 或更高版本的`--aws-sigv4`選項。您也可以使用範例 Python 用戶端中已註解的範例，將已簽署的 HTTP 要求傳送至 curl 命令所使用的相同端點。

若要建立手動快照，請執行下列步驟：

1. 如果快照正在進行中，您就無法取得快照。若要檢查，請執行下列命令：

   ```
   curl -XGET 'domain-endpoint/_snapshot/_status'
   ```

2. 執行以下命令來手動拍攝快照：

```
curl -XPUT 'domain-endpoint/_snapshot/repository-name/snapshot-name'
```

若要包含或排除某些索引並指定其他設定，請新增請求主體。有關請求結構，請參閱 OpenSearch 文檔中的拍攝快照。

> **Note**
>
> 建立快照所需的時間會隨著 OpenSearch 服務網域的大小而增加。長時間執行的快照操作有時會發生以下錯誤：`504 GATEWAY_TIMEOUT`。一般而言，您可以忽略這些錯誤，並等待操作成功完成。執行下列命令來驗證您網域的所有快照狀態：
>
> ```
> curl -XGET 'domain-endpoint/_snapshot/repository-name/_all?pretty'
> ```

還原快照

在還原快照之前，請確定目的地網域未使用異地同步備份與待命。啟用待命功能會導致還原作業失敗。

> **Warning**
>
> 如果您使用索引別名，您應該停止寫入別名的要求，或在刪除其索引之前將別名切換至其他索引。停止寫入請求有助於避免以下情況：
>
> 1. 刪除索引也會刪除它的別名。
> 2. 錯誤的寫入請求至現已刪除的別名，會使用和別名相同的名稱建立新索引。
> 3. 因與新索引有命名衝突之故，您不可再使用別名。當您從快照還原，如果您交換別名到另一個索引，此時請指定`"include_aliases": false`。

還原快照

1. 找到您要還原的快照。請確定此索引的所有設定值 (例如自訂分析器套件或配置需求設定) 都與網域相容。若要查看所有快照儲存庫，請執行下列命令：

   ```
   curl -XGET 'domain-endpoint/_snapshot?pretty'
   ```

在識別儲存庫後，請執行下列命令以查看所有快照：

```
curl -XGET 'domain-endpoint/_snapshot/repository-name/_all?pretty'
```

> **Note**
>
> 大多數自動快照存放在 `cs-automated` 儲存庫中。如果您的網域加密靜態資料，會將它們存放在 `cs-automated-enc` 儲存庫中。如果未看到您尋找的手動快照儲存庫，請確定您已將它註冊到網域。

2. (選擇性) 如果叢集上的索引與快照中的索引之間發生命名衝突，請刪除或重新命名 OpenSearch Service 網域中的一或多個索引。您無法將索引的快照還原到已包含具有相同名稱之索引的 OpenSearch 叢集。

   如果您有索引命名衝突，則具有下列選項：

   - 刪除現有 OpenSearch 服務網域上的索引，然後還原快照集。
   - 在您從快照還原索引時將其重新命名，並為其重新編製索引。若要瞭解如何重新命名索引，請參閱 OpenSearch 文件中的此範例要求。
   - 將快照還原到不同的 OpenSearch 服務網域 (僅適用於手動快照)。

   下列命令會刪除網域中的所有現有索引：

   ```
   curl -XDELETE 'domain-endpoint/_all'
   ```

   但是，如果您不打算還原所有索引，則只可以刪除一個索引：

   ```
   curl -XDELETE 'domain-endpoint/index-name'
   ```

3. 若要還原快照，請執行以下命令：

   ```
   curl -XPOST 'domain-endpoint/_snapshot/repository-name/snapshot-name/_restore'
   ```

   由於 OpenSearch 儀表板的特殊權限和精細的存取控制索引，嘗試還原所有索引可能會失敗，尤其是當您嘗試從自動快照還原時。以下範例只從 `my-index` 快照儲存庫中的 `2020-snapshot` 還原一個索引 `cs-automated`：

```
curl -XPOST 'domain-endpoint/_snapshot/cs-automated/2020-snapshot/_restore' \
-d '{"indices": "my-index"}' \
-H 'Content-Type: application/json'
```

或者，您可能想要還原所有索引，Dashboards 和精細存取控制索引除外：

```
curl -XPOST 'domain-endpoint/_snapshot/cs-automated/2020-snapshot/_restore' \
-d '{"indices": "-.kibana*,-.opendistro*"}' \
-H 'Content-Type: application/json'
```

您可以使用`rename_pattern`和`rename_replacement`參數還原快照，而不刪除其資料。如需這些參數的詳細資訊，請參閱 OpenSearch 文件中的還原快照 API 要求欄位和範例要求。

> **Note**
>
> 如果不是所有涉及的索引都有主要碎片，快照可能一個 `state` 的 `PARTIAL`。此值表示至少一個碎片的資料未成功儲存。您仍然可以從部分快照還原，但您可能需要使用舊版的快照來還原任何遺失的索引。

刪除手動快照

若要刪除手動快照，請執行以下命令：

```
DELETE _snapshot/repository-name/snapshot-name
```

使用快照管理自動化快照

您可以在 OpenSearch 儀表板中設定快照管理 (SM) 原則，以自動定期建立和刪除快照。SM 可以快照一組索引，而索引狀態管理只能為每個索引拍攝一個快照。若要在 OpenSearch 服務中使用 SM，您需要註冊自己的 Amazon S3 儲存庫。如需註冊存放庫的指示，請參閱註冊手動快照儲存庫。

在 SM 之前， OpenSearch 服務提供了免費的自動快照功能，依預設為開啟狀態。此功能會將快照傳送至服務維護的`cs-*`儲存庫。要停用該功能，請聯繫 AWS Support。

如需 SM 功能的詳細資訊，請參閱 OpenSearch 文件中的快照管理。

SM 目前不支援在多個索引類型上建立快照集。例如，如果您嘗試在具有多個索引上建立快照，*而某些索引位於暖層，則快照建立將會失敗。如果您需要快照包含多個索引類型，請使用 ISM 快照動作，直到 SM 支援此選項為止。

設定許可

如果您要從先前的 OpenSearch Service 網域版本升級到 2.5，則網域上可能不會定義快照管理安全性權限。非管理員使用者必須對應至此角色，才能使用精細的存取控制在網域上使用快照管理。若要手動建立快照管理角色，請執行下列步驟：

1. 在 OpenSearch 儀表板中，轉到安全性，然後選擇權限。
2. 選擇 Create action group (建立動作群組) 並設定下列群組：

Group name (群組名稱)	許可
`snapshot_management_full_access`	• `cluster:admin/opensearch/snapshot_management/*` • `cluster:admin/opensearch/notifications/feature/publish` • `cluster:admin/repository/*` • `cluster:admin/snapshot/*`
`snapshot_management_read_access`	• `cluster:admin/opensearch/snapshot_management/policy/get` • `cluster:admin/opensearch/snapshot_management/policy/search` • `cluster:admin/opensearch/snapshot_management/policy/explain` • `cluster:admin/repository/get` • `cluster:admin/snapshot/get`

3. 選擇 Roles (角色)，然後選擇 Create role (建立角色)。
4. 命名角色快照管理角色。
5. 對於叢集權限，請選取`snapshot_management_full_access`或`snapshot_management_read_access`。
6. 選擇建立。

7. 建立角色後，請將其對應至任何將管理快照的使用者或後端角色。

考量事項

設定快照管理時，請考慮下列事項：

- 每個儲存庫允許一個策略。
- 一個策略最多允許 400 個快照。
- 如果您的網域狀態為紅色、處於高 JVM 壓力 (85% 或以上)，或快照功能卡住，則此功能將無法執行。當叢集的整體索引和搜尋效能受到影響時，SM 也可能會受到影響。
- 快照作業只會在前一個作業完成後啟動，因此不會由一個原則啟動並行快照作業。
- 具有相同排程的多個策略可能會導致資源尖峰。如果原則的快照索引重疊，則碎片層級快照作業只能依序執行，這可能會造成串聯的效能問題。如果原則共用儲存庫，則該儲存庫的寫入作業將會發生尖峰。
- 除非您有特殊使用案例，否則建議您將快照作業自動化排程為每小時不超過一次。

使用索引狀態管理自動化快照

您可以使用索引狀態管理 (ISM) `snapshot` 操作，根據索引的使用期限、大小或文件數量的變化，自動觸發索引快照。當您需要每個索引一個快照時，ISM 是最佳選擇。如果您需要一組索引的快照，請參閱使用快照管理自動化快照。

若要在 OpenSearch 服務中使用 SM，您需要註冊自己的 Amazon S3 儲存庫。如需使用 `snapshot` 操作的範例 ISM 政策，請參閱範例政策。

使用 Curator 進行快照

如果 ISM 不適用於索引和快照管理，您可以改用 Curator。其提供進階篩選功能，可協助簡化複雜叢集的管理任務。使用 pip 安裝 Curator。

```
pip install elasticsearch-curator
```

您可以使用 Curator 做為命令列界面 (CLI) 或 Python API。如果您使用 Python API，則必須使用版本 7.13.4 或更早版本的舊版 elasticsearch-py 用戶端。不支援 opensearch-py 用戶端。

如果您使用 CLI，在命令列匯出您的登入資料，並且設定 `curator.yml`，如下所示：

```
client:
  hosts: search-my-domain.us-west-1.es.amazonaws.com
  port: 443
  use_ssl: True
  aws_region: us-west-1
  aws_sign_request: True
  ssl_no_validate: False
  timeout: 60

logging:
  loglevel: INFO
```

升級 Amazon OpenSearch 服務域

> **Note**
>
> OpenSearch 和彈性搜尋版本升級與服務軟體更新不同。如需更新 Service 網域之服務軟體的 OpenSearch 資訊，請參閱the section called “服務軟體更新”。

Amazon OpenSearch 服務為執行 OpenSearch 1.0 或更新版本的網域或彈性搜尋 5.1 或更新版本的網域提供就地升級。如果您使用 Amazon Data Firehose 或 Amazon CloudWatch 日誌等服務將資料串流至 OpenSearch 服務，請 OpenSearch 在遷移之前檢查這些服務是否支援較新版本的。

主題

- 支援的升級路徑
- 開始升級 (主控台)
- 開始升級 (CLI)
- 開始升級 (SDK)
- 對驗證失敗進行故障排除
- 升級疑難排解
- 使用快照來遷移資料

支援的升級路徑

目前， OpenSearch 服務支援下列升級路徑：

原始版本	目標版本
OpenSearch 一點三或二. x	OpenSearch 2. x 2.3 版具有以下突破性變更： • 該`type`參數已從 2.0 版中的所有 OpenSearch API 端點中刪除。如需詳細資訊，請參閱 Breaking changes (突破性變更)。 • 如果您的網域包含任何最初在 Elasticsearch 6.8 中建立的索引 (熱索引或冷)，則這些索引與 OpenSearch 2.3 不相容。 UltraWarm 升級至 2.3 版之前，您必須對不相容的索引重新編製索引。對於不相容 UltraWarm 或冷索引，請將它們移轉至熱儲存區，重新建立資料索引，然後將其移轉回暖或冷儲存庫。或者，您也可以在不再需要時刪除索引。 如果您意外將網域升級至 2.3 版，而未先執行這些步驟，則無法從目前的儲存層遷移出不相容的索引。您的唯一選項是刪除它們。
OpenSearch 1. x	OpenSearch 1. x
Elasticsearch 7.x	彈性搜索 7. x 或 OpenSearch 1. x **Important** OpenSearch 1. x 引入了許多突破性變化。如需詳細資訊，請參閱 Amazon OpenSearch Service 重新命名。
Elasticsearch 6.8	彈性搜索 7. x 或 OpenSearch 1. x **Important** 彈性搜索 7.0 和 OpenSearch 1.0 包括許多突破性更改。在啟動就地升級之前，建議您先擷取 6 的手動快照。 x 域，在測試 7 上恢復它。 x 或 OpenSearch 1. x 網域，並使用該測試網域來識別潛在的升級問題。如需中斷 OpenSearch 1.0 中的變更，請參閱Amazon OpenSearch Service 重新命名。

原始版本	目標版本
	如同 Elasticsearch 6.x，索引只能包含一個映射類型，但該類型現在必須名為 `_doc`。因此，特定 API 不再要求在請求內文中有映射類型 (例如 `_bulk` API)。 對於新索引，自託管彈性搜索 7. x 和 OpenSearch 1. x 的預設碎片計數為 1。 OpenSearch 彈性搜索上的服務域 7. x 及更新版本保留先前的預設值 5。
Elasticsearch 6.x	Elasticsearch 6.x
Elasticsearch 5.6	Elasticsearch 6.x **Important** 在 6.x 版建立的索引不再支援多個映射類型。在 5.x 版中建立的索引，在恢復為 6.x 叢集時仍支援多個映射類型。請檢查您的用戶端程式碼是否每個索引只建立單一映射類型。 最大限度地減少從彈性搜索 5.6 升級到 6 期間的停機時間。 x，OpenSearch Service 會將索引重新編製索引`.kibana-6` 、刪除`.kibana`、建立名為的別名`.kibana`，並將新索引對應至新的別名。`.kibana`
Elasticsearch 5.x	Elasticsearch 5.x

升級程序包含三個步驟：

1. 升級前檢查 — OpenSearch 服務會檢查是否有可能阻止升級的問題，除非這些檢查成功，否則不會繼續進行下一個步驟。
2. 快照 — OpenSearch 服務會擷取 OpenSearch 或 Elasticsearch 叢集的快照，除非快照成功，否則不會繼續執行下一個步驟。如果升級失敗， OpenSearch Service 會使用此快照將叢集還原至其原始狀態。如需更多資訊，請參閱 the section called “升級後無法降級”。
3. 升級 — OpenSearch 服務開始升級，可能需要 15 分鐘到數小時才能完成。 OpenSearch 在部分或全部升級期間，儀表板可能無法使用。

開始升級 (主控台)

升級程序無法復原，且無法暫停或取消。升級時，您無法對網域做出組態變更。開始升級前，重複確認您是否要繼續。您可以使用這些相同的步驟，來執行預先升級的檢查，而不用實際開始升級。

如果叢集具有專用的主節點，則 OpenSearch 升級完成而不會停機。否則叢集在選擇主節點時，可能會在升級後數秒沒有回應。

若要將網域升級至較新版本的 OpenSearch 或彈性搜尋

1. 建立您網域的手動快照。此快照可做為備份，如果您想要返回使用舊 OpenSearch 版，您可以在新網域上還原該備份。
2. 前往 https://aws.amazon.com 並選擇 Sign In to the Console (登入主控台)。
3. 在分析下，選擇 Amazon OpenSearch 服務。
4. 在導覽窗格中，於 Domains (網域) 下，選擇您想要升級的網域。
5. 選擇 Actions (動作) 和 Upgrade (升級)。
6. 選取要升級到的版本。如果您要升級至某個 OpenSearch 版本，則會出現「啟用相容模式」選項。如果啟用此設定，請將其版本 OpenSearch 報告為 7.10，以允許 Elasticsearch OSS 用戶端和外掛程式 (例如 Logstash) 繼續使用 Amazon 服務。 OpenSearch 您可以稍後停用此設定
7. 選擇 Upgrade (升級)。
8. 請檢查網域儀表板上的 Status (狀態) 來監控升級狀態。

開始升級 (CLI)

您可以使用下列作業來識別網域的正確版本 OpenSearch 或 Elasticsearch、啟動就地升級、執行升級前檢查，以及檢視進度：

- `get-compatible-versions` (`GetCompatibleVersions`)
- `upgrade-domain` (`UpgradeDomain`)
- `get-upgrade-status` (`GetUpgradeStatus`)
- `get-upgrade-history` (`GetUpgradeHistory`)

如需詳細資訊，請參閱 AWS CLI 命令參考和 Amazon OpenSearch 服務 API 參考。

開始升級 (SDK)

此範例使用中的OpenSearchService低階 Python 用戶端來檢查網域是否符合升級至特定版本的資格、對其進行升級，以及持續檢查升級狀態。 AWS SDK for Python (Boto)

```
import boto3
from botocore.config import Config
import time

# Build the client using the default credential configuration.
# You can use the CLI and run 'aws configure' to set access key, secret
# key, and default Region.

DOMAIN_NAME = ''  # The name of the domain to upgrade
TARGET_VERSION = ''  # The version you want to upgrade the domain to. For example,
 OpenSearch_1.1

my_config = Config(
    # Optionally lets you specify a Region other than your default.
    region_name='us-east-1'
)
client = boto3.client('opensearch', config=my_config)


def check_versions():
    """Determine whether domain is eligible for upgrade"""
    response = client.get_compatible_versions(
        DomainName=DOMAIN_NAME
    )
    compatible_versions = response['CompatibleVersions']
    for i in range(len(compatible_versions)):
        if TARGET_VERSION in compatible_versions[i]["TargetVersions"]:
            print('Domain is eligible for upgrade to ' + TARGET_VERSION)
            upgrade_domain()
            print(response)
        else:
            print('Domain not eligible for upgrade to ' + TARGET_VERSION)


def upgrade_domain():
    """Upgrades the domain"""
    response = client.upgrade_domain(
        DomainName=DOMAIN_NAME,
```

```
        TargetVersion=TARGET_VERSION
    )
    print('Upgrading domain to ' + TARGET_VERSION + '...' + response)
    time.sleep(5)
    wait_for_upgrade()


def wait_for_upgrade():
    """Get the status of the upgrade"""
    response = client.get_upgrade_status(
        DomainName=DOMAIN_NAME
    )
    if (response['UpgradeStep']) == 'UPGRADE' and (response['StepStatus']) ==
 'SUCCEEDED':
        print('Domain successfully upgraded to ' + TARGET_VERSION)
    elif (response['StepStatus']) == 'FAILED':
        print('Upgrade failed. Please try again.')
    elif (response['StepStatus']) == 'SUCCEEDED_WITH_ISSUES':
        print('Upgrade succeeded with issues')
    elif (response['StepStatus']) == 'IN_PROGRESS':
        time.sleep(30)
        wait_for_upgrade()


def main():
    check_versions()


if __name__ == "__main__":
    main()
```

對驗證失敗進行故障排除

當您啟動 OpenSearch 或 Elasticsearch 版本升級時， OpenSearch 服務會先執行一系列驗證檢查，以確保您的網域符合升級資格。如果其中任何一項檢查失敗，您會收到通知，其中包含您必須在更新網域之前解決的特定問題。如需潛在問題的清單以及解決問題的步驟，請參閱 the section called “對驗證錯誤進行疑難排解”。

升級疑難排解

就地 升級需要運作狀態良好的網域。您的網域可能不符合升級的資格，或因各種原因而無法升級。下表顯示最常見的問題。

問題	描述
不支持可選插件	當您使用可選外掛程式升級網域時， OpenSearch Service 也會自動升級外掛程式。因此，您網域的目標版本也必須支援這些選用的外掛程式。如果網域安裝的選用外掛程式不適用於目標版本，則升級要求會失敗。
每個節點有太多碎片	OpenSearch，以及 7. x 個版本的彈性搜索，每個節點的碎片不超過 1,000 個的默認設置。如果目前叢集中的節點超過此設定， OpenSearch Service 將不允許您升級。如需疑難排解選項，請參閱the section called “超出最大碎片限制”。
處理中的網域	組態變更中的網域 在操作完成後檢查升級資格。
紅色叢集狀態	叢集中一或多個索引是紅色的。如需疑難排解步驟，請參閱the section called “紅色叢集狀態”。
高錯誤率	在嘗試處理請求時，叢集傳回大量的 5xx 錯誤。此問題通常是因為太多同時讀寫請求造成。請考慮降低叢集流量或擴展網域。
分割大腦	分割大腦表示叢集有不只一個主節點，且已分為兩個叢集，這兩個叢集將不會自行重新連結。您也可以使用建議數量的專用主節點來避免大腦分割。如需從大腦分割中恢復的協助，請聯絡 AWS Support。
找不到主節點	OpenSearch 服務找不到叢集的主節點。如果您的網域使用的是多個可用區，則可用區域故障可能會導致叢集遺失仲裁，且無法選擇新的主節點。如果問題無法自主解決，請聯絡AWS Support。
待處理任務過多	主節點負載太重且待處理任務過多。請考慮降低叢集流量或擴展網域。
儲存磁碟區受損	一或多個節點的磁碟區無法正常運作。此問題通常與其他問題 (例如高錯誤率或待處理任務過多) 一起發生。如果此問題單獨發生且無法自主解決，請聯絡AWS Support。
KMS 金鑰問題	用於加密網域的 KMS 金鑰無法存取或遺失。如需詳細資訊，請參閱 the section called “監控靜態加密資料的網域”。
快照處理中	網域正在拍攝快照。在快照完成後檢查升級資格。也確認您是否列出手動快照儲存庫、列出這些儲存庫中的快照與手動拍攝快照。如果 OpenSearch 服務無法檢查快照是否正在進行中，升級可能會失敗。

問題	描述
快照逾時或故障	預先升級快照耗時太久，無法完成或失敗。請檢查叢集的運作狀態並再試一次。如果問題仍存在，請聯絡 AWS Support。
索引不相容	一或多個索引與目標版本不相容。如果您從舊版 OpenSearch 或彈性搜尋移轉索引，就可能會發生這個問題。重新編製索引，然後重試。
高磁碟使用量	叢集的磁碟使用量超過 90%。篩除資料或擴展網域，然後重試。
高 JVM 用量	JVM 記憶體壓力超過 75%。 降低叢集的流量或擴展網域，然後重試。
OpenSearch 儀表板別名問題	`.dashboards` 已設定為別名，並對映至不相容的索引，可能是來自舊版 OpenSearch 儀表板的索引。重新建立索引並再試一次。
紅色 Dashboards 狀態	OpenSearch 儀表板狀態為紅色。在升級完成時嘗試使用 Dashboards。如果紅色狀態仍持續，手動解決它，然後重試。
跨叢集相容性	只有在可維持升級後來源和目的地網域之間的跨叢集相容性的情況下，才能進行升級。在升級程序期間，系統會識別任何不相容的連線。若要繼續進行，請升級遠端網域或刪除不相容的連線。請注意，如果複寫在網域上處於啟用狀態，一旦刪除連線，就無法繼續複寫。
其他 OpenSearch 服務服務問題	OpenSearch 服務本身的問題可能會導致您的網域顯示為不符合升級資格。如果上述問題都不適用於您的網域，且問題持續超過一天，請聯絡AWS Support。

使用快照來遷移資料

就地升級是將網域升級至更新版本 OpenSearch 或 Elasticsearch 版本的更簡單、更快速且更可靠的方式。如果您需要從 Elasticsearch 5.1 之前的版本中遷移或想要遷移至全新的叢集，快照會是一個好選擇。

下表顯示如何使用快照將資料移轉至使用其他版本 OpenSearch 或 Elasticsearch 版本的網域。如需有關拍攝和恢復快照的資訊，請參閱the section called “建立索引快照”。

原始版本	目標版本	遷移程序

OpenSearch 一點三或二. x	OpenSearch 2. x	1. 檢閱 OpenSearch 2.3 的重大變更，看看是否需要調整索引或應用程式。
		2. 建立 1.3 或 2 的手動快照。 x 網域名稱。
		3. 創建一個 2. x 域名的版本比原來的 1.3 或 2 更高。 x 網域名稱。
		4. 將快照從原始網域還原到 2。 x 網域名稱。在作業期間，您可能需要以新名稱還原`.opensearch` 索引：
		`POST _snapshot/ <repository-name> /<snapshot-name>/_restore`
		`{`
		`"indices": "*",`
		`"ignore_unavailable": true,`
		`"rename_pattern": ".opensearch",`
		`"rename_replacement": ".backup-opensearch"`
		`}`
		然後，您可以在新網域 `.backup-opensearch` 上重建索引，並將其別名命名為 `.opensearch` 。請注意，`_restore`REST 調用不包括，`include_global_state` 因為默認值`_restore`是假的。因此，測試網域不會包含任何索引範本，也不會有備份的完整狀態。
		5. 如果您不再需要原始網域，請將其刪除。否則，您要繼續負擔網域的費用。

OpenSearch 1. x	OpenSearch 1. x	1. 建立 1 的手動快照。 x 網域名稱。 2. 創建一個 1. x 域名比您原來的版本更高 1。 x 網域名稱。 3. 將快照從原始網域還原到新的 1。 x 網域名稱。在作業期間，您可能需要以新名稱還原`.opensearch` 索引： `POST _snapshot/ <repository-name> /<snapshot-name>/_restore`

原始版本	目標版本	遷移程序

		<pre>{
		  "indices": "*",
		  "ignore_unavailable": true,
		  "rename_pattern": ".opensearch",
		  "rename_replacement": ".backup-opensearch"
		}</pre>
		然後，您可以在新網域 .backup-opensearch 上重建索引，並將其別名命名為 .opensearch 。請注意，_restoreREST 調用不包括，include_global_state 因為默認值_restore是假的。因此，測試網域不會包含任何索引範本，也不會有備份的完整狀態。
		4. 如果您不再需要原始網域，請將其刪除。否則，您要繼續負擔網域的費用。

原始版本	目標版本	遷移程序

Elasticsearch 6.x 或 7.x	OpenSearch 1. x	1. 檢閱 OpenSearch 1.0 的重大變更，看看是否需要調整索引或應用程式。
		2. 建立 Elasticsearch 7.x 或 6.x 網域的手動快照。
		3. 創建一個 OpenSearch 1. x 網域名稱。
		4. 將快照從彈性搜尋網域還原至網域。 OpenSearch 在作業期間，您可能需要以新名稱還原`.elasticsearch` 索引：
		`POST _snapshot/ <repository-name> /<snapshot-name>/_restore`
		`{`
		`  "indices": "*",`
		`  "ignore_unavailable": true,`
		`  "rename_pattern": ".elasticsearch",`
		`  "rename_replacement": ".backup-opensearch"`
		`}`
		然後，您可以在新網域 `.backup-opensearch` 上重建索引，並將其別名命名為 `.elasticsearch` 。請注意，`_restore`REST 調用不包括，`include_global_state` 因為默認值`_restore`是假的。因此，測試網域不會包含任何索引範本，也不會有備份的完整狀態。
		5. 如果您不再需要原始網域，請將其刪除。否則，您要繼續負擔網域的費用。

原始版本	目標版本	遷移程序

Elasticsearch 6.x	Elasticsearch 7.x	1. 檢閱 7.0 的重大變更，以查看是否需要調整您的索引或應用程式。
		2. 建立 6.x 網域的手動快照。
		3. 建立 7.x 網域。
		4. 將快照從原始網域還原到 7.x 網域。在操作期間，您可能需要以新名稱還原 `.opensearch` 索引：
		`POST _snapshot/ <repository-name> /<snapshot-name>/_restore`
		`{`
		`  "indices": "*",`
		`  "ignore_unavailable": true,`
		`  "rename_pattern": ".elasticsearch",`
		`  "rename_replacement": ".backup-elasticsearch"`
		`}`
		然後，您可以在新網域 `.backup-elasticsearch` 上重建索引，並將其別名命名為 `.elasticsearch` 。請注意，`_restore`REST 調用不包括，`include_global_state` 因為默認值`_restore`是假的。因此，測試網域不會包含任何索引範本，也不會有備份的完整狀態。
		5. 如果您不再需要原始網域，請將其刪除。否則，您要繼續負擔網域的費用。

Elasticsearch 6.x	Elasticsearch 6.8	1. 建立 6.x 網域的手動快照。 2. 建立 6.8 網域。 3. 將快照從原始網域還原到 6.8 網域。 4. 如果您不再需要原始網域，請將其刪除。否則，您要繼續負擔網域的費用。

原始版本	目標版本	遷移程序
Elasticsearch 5.x	Elasticsearch 6.x	1. 檢閱 6.0 的重大變更，以得知您是否需要調整您的索引或應用程式。 2. 建立 5.x 網域的手動快照。 3. 建立 6.x 網域。 4. 將快照從原始網域還原到 6.x 網域。 5. 如果您不再需要 5.x 網域，請將其刪除。否則，您要繼續負擔網域的費用。
Elasticsearch 5.x	Elasticsearch 5.6	1. 建立 5.x 網域的手動快照。 2. 建立 5.6 網域。 3. 將快照從原始網域還原到 5.6 網域。 4. 如果您不再需要原始網域，請將其刪除。否則，您要繼續負擔網域的費用。
Elasticsearch 2.3	Elasticsearch 6.x	Elasticsearch 2.3 快照與 6.x 不相容。若要直接將您的資料從 2.3 遷移至 6.x，您必須在新網域手動重新建立索引。 或者，您可以遵照此表中的 2.3 到 5.x 步驟，在全新 5.x 網域中執行 `_reindex` 操作，將您的 2.3 索引轉換為 5.x 索引，接著再遵循 5.x 到 6.x 步驟。
Elasticsearch 2.3	Elasticsearch 5.x	1. 檢閱 5.0 的重大變更，以查看是否需要調整您的索引或應用程式。 2. 建立 2.3 網域的手動快照。 3. 建立 5.x 網域。 4. 將快照從 2.3 網域還原到 5.x 網域。 5. 如果您不再需要 2.3 網域，請將其刪除。否則，您要繼續負擔網域的費用。

原始版本	目標版本	遷移程序
Elasticsearch 1.5	Elasticsearch 5.x	Elasticsearch 1.5 快照與 5.x 不相容。若要將您資料從 1.5 遷移至 5.x，您必須在新網域手動重新建立索引。 **Important** 1.5 快照與 2.3 相容，但 OpenSearch 服務 2.3 網域不支援此*_reindex*作業。因為您無法為其重新編製索引，所以在 1.5 網域中產生的索引仍然無法從 2.3 快照還原到 5.x 網域。
Elasticsearch 1.5	Elasticsearch 2.3	1. 使用遷移外掛程式來確認您是否可以直接升級至 2.3 版。您在遷移前可能需要對資料進行變更。 a. 在 Web 瀏覽器中，開啟 `http://domain-endpoint /_plugin/migration/` 。 b. 選擇 Run checks now (立即執行檢查)。 c. 如有需要，檢閱結果，並依照操作說明來變更您的資料。 2. 建立 1.5 網域的手動快照。 3. 建立 2.3 網域。 4. 將快照從 1.5 網域還原到 2.3 網域。 5. 如果您不再需要 1.5 網域，請將其刪除。否則，您要繼續負擔網域的費用。

為 Amazon OpenSearch 服務創建自定義端點

為您的 Amazon OpenSearch 服務網域建立自訂端點可讓您更輕鬆地參考 OpenSearch 和 OpenSearch 儀表板網址。您可以包含公司的品牌，或者只使用比標準 easier-to-remember 端點更短的端點。

如果您需要切換到新網域，只需更新 DNS 以指向新的 URL 並繼續使用與以前相同的端點。

您可以在 AWS Certificate Manager (ACM) 中產生憑證或匯入自己的憑證，以保護自訂端點的安全。

新網域的自訂端點

您可以使用 OpenSearch 服務主控台或設定 API 為新的 OpenSearch 服務網域啟用自訂端點。 AWS CLI

若要自訂端點 (主控台)

1. 從 OpenSearch 服務主控台，選擇建立網域並提供網域名稱。
2. 在 Custom endpoint (自訂端點) 中，選取 Enable custom endpoint (啟用自訂端點)。
3. 對於 Custom hostname (自訂主機名稱)，輸入您偏好的自訂端點主機名稱。主機名稱應該是完整網域名稱 (FQDN)，例如 www.yourdomain.com 或 example.yourdomain.com。

   > **Note**
   > 如果您沒有萬用字元憑證，則必須為自訂端點的子網域獲取新憑證。

4. 對於 AWS 憑證，選擇您要用於此網域的 SSL 憑證。如果沒有可用的憑證，您可以將憑證匯入 ACM 或使用 ACM 來佈建憑證。如需詳細資訊，請參閱 AWS Certificate Manager 使用者指南中的發行和管理憑證。

   > **Note**
   > 憑證必須具有自訂端點名稱，並且與您的 OpenSearch Service 網域位於相同的帳戶中。憑證狀態應為 ISSUED (已發佈)。

   - 依照其餘步驟建立網域，然後選擇 Create (建立)。
   - 完成處理後，請選取網域以檢視您的自訂端點。

   若要使用 CLI 或組態 API，請使用 `CreateDomain` 和 `UpdateDomainConfig` 操作。如需詳細資訊，請參閱AWS CLI 命令參考和 Amazon OpenSearch 服務 API 參考。

現有網域的自訂端點

若要將自訂端點新增至現有的 OpenSearch 服務網域，請選擇編輯並執行上述步驟 2 至 4。

後續步驟

為 OpenSearch 服務網域啟用自訂端點後，您可以在 Amazon Route 53 (或您偏好的 DNS 服務提供者) 中建立 CNAME 對應。建立 CNAME 對應可讓您將流量路由到自訂端點及其子網域。如果沒有此對應，您將無法將流量路由到自訂端點。如需在 Route 53 中建立此對應的步驟，請參閱設定新網域的 DNS 路由和為子網域建立新的託管區域。如果是其他供應商，請參閱其文件。

建立將自訂端點指向自動產生的網域端點的 CNAME 記錄。如果您的網域是雙堆疊，您可以將 CNAME 記錄指向兩個服務產生的其中一個端點。自訂端點的雙堆疊功能取決於您指向 CNAME 記錄的服務產生端點。自訂端點主機名稱是 CNAME 記錄的名稱，而網域端點主機名稱是 CNAME 記錄的值。

如果您對 OpenSearch儀表板使用 SAML 驗證，則必須使用新的 SSO URL 更新 IdP。

您可以使用 Amazon Route 53 建立別名記錄類型，將網域的自訂端點指向雙堆疊搜尋端點。若要建立別名記錄類型，您必須將網域設定為使用雙堆疊 IP 位址類型。您可以使用路由 53 API 執行此操作。

若要使用 Route 53 API 建立別名記錄類型，請指定網域的別名目標。您可以在 OpenSearch Service 主控台的自訂端點區段的託管區域 (雙堆疊) 欄位中找到網域的別名目標，或使用 `DescribeDomain` API 並複製`DomainEndpointV2HostedZoneId`.

自動調整亞馬遜 OpenSearch 服務

Amazon Ser OpenSearch vice 中的自動調整會使用 OpenSearch 叢集中的效能和使用量指標來建議與記憶體相關的組態變更，包括佇列和快取大小，以及節點上的 Java 虛擬機器 (JVM) 設定。這些選擇性變更可提高叢集速度與穩定性。

某些變更會立即部署，而其他變更則會在網域離峰期間排程。您可以隨時還原為預設的「 OpenSearch 服務」設定。自動調整會收集並分析網域的效能指標時，您可以在「通知」頁面的「 OpenSearch 服務主控台」中檢視其建議。

自動調整功能適用AWS 區域於執行任何 OpenSearch版本的網域，或使用支援執行個體類型的 Elasticsearch 6.7 或更新版本的網域。

主題

- 變更類型
- 啟用或停用自動調整
- 排程自動調整增強功
- 監視自動調整變更

變更類型

自動調整有兩大類變更：

- 叢集執行時套用的不中斷變更。
- 需要藍/綠部署的變更，這些變更會在網域的離峰期間套用。

根據您網域的效能指標，自動調整可建議調整下列設定：

變更類型	類別	描述
JVM 堆積大小	藍/綠	根據預設， OpenSearch 服務會將執行個體的 RAM 用於 JVM 堆積的 50%，最多可達 32 GiB 的堆積大小。 增加此百分比可提供 OpenSearch 更多記憶體，但對作業系統和其他處理程序而言可能會較少。較大的值可以減少廢棄項目收集暫停的數目，但會增加這些暫停的長度。
JVM 新一代設定	藍/綠	JVM「新一代」設定會影響次要廢棄項目收集的頻率。較頻繁的次要收集可減少主要收集和暫停的數目。
佇列大小	不中斷	依預設，搜尋佇列大小為 `1000`，寫入佇列大小為 `10000`。如果有額外的堆積可用來處理請求，自動調整會自動擴展搜尋和寫入佇列。
快取大小	不中斷	欄位快取會監控堆積內的資料結構，因此監控快取的使用非常重要。自動調整可擴展欄位資料快取大小，以避免記憶體不足和斷路器問題。 碎片請求快取在節點級別進行管理，並且默認的大小上限為 1% 的堆積。自動調整可擴展碎片請求快取大小，以接受比設定的叢集可處理的請求更多的搜尋和索引請求。
請求規模	不中斷	根據預設，當執行中要求的彙總大小超過 JVM 總數的 10% (`t2`執行個體類型為 2%，1%`t3.small`) 時，會 OpenSearch 節流所有新`_search`要求和要求，直到現有`_bulk`要求完成為止。 自動調整會依據目前系統占用的 JVM 量自動調整此閾值，通常介於 5-15% 之間。例如，如果 JVM 記憶體壓力很高，則自動調整可能會

變更類型	類別	描述
		將閾值降低至 5%，此時在叢集穩定且閾值增加之前，您可能會看到更多的拒絕數。

啟用或停用自動調整

OpenSearch 服務預設會在新網域上啟用「自動調整」。若要在現有網域上啟用或停用「自動調整」，建議您使用主控台來簡化程序。啟用自動調整不會導致藍/綠部署。

您目前無法使用 AWS CloudFormation 來啟用或停用自動調整。

主控台

在現有網域上啟用自動調整

1. 在以下位置打開亞馬遜 OpenSearch 服務控制台 https://console.aws.amazon.com/aos/home。
2. 在瀏覽窗格的 [網域] 下，選擇要開啟叢集配置的網域名稱。
3. 如果尚未啟用「自動調整」，請選擇「開啟」。
4. 選擇性地選取離峰時段，以排定在網域設定的離峰時段期間需要藍/綠部署的最佳化。如需詳細資訊，請參閱the section called “排程自動調整增強功”。
5. 選擇 Save changes (儲存變更)。

CLI

若要使用啟用「自動調整」AWS CLI，請傳送UpdateDomainConfig請求：

```
aws opensearch update-domain-config \
  --domain-name my-domain \
  --auto-tune-options DesiredState=ENABLED
```

排程自動調整增強功

在 2023 年 2 月 16 日之前，「自動調整」使用維護時段來排程需要藍/綠部署的變更。維護時段現在已被棄用，以支持離峰時段，這是每天 10 小時的時間段，在此期間，您的網域通常會遇到低流量的情況。您可以修改離峰時段的預設開始時間，但無法修改長度。

在 2023 年 2 月 16 日引入離峰時段之前已啟用「自動調整」維護時段的任何網域，都可以繼續使用舊版維護時段而不會中斷。不過，我們建議您移轉現有的網域，改為使用離峰時段進行網域維護。如需相關指示，請參閱the section called “從自動調整維護時段移轉”。

主控台

若要排定離峰時段的自動調整動作

1. 在以下位置打開亞馬遜 OpenSearch 服務控制台 https://console.aws.amazon.com/aos/home。
2. 在瀏覽窗格的 [網域] 下，選擇要開啟叢集配置的網域名稱。
3. 前往「自動調整」標籤，然後選擇「編輯」。
4. 如果尚未啟用「自動調整」，請選擇「開啟」。
5. 在離峰期間排程最佳化下，選取離峰時段。
6. 選擇 Save Changes (儲存變更)。

CLI

若要將您的網域設定為在設定的離峰期間排程自動調整動作，請包含`UseOffPeakWindow`在要求中 UpdateDomainConfig：

```
aws opensearch update-domain-config \
  --domain-name my-domain \
  --auto-tune-options
 DesiredState=ENABLED,UseOffPeakWindow=true,MaintenanceSchedules=null
```

監視自動調整變更

您可以在Amazon CloudWatch中監視自動調整統計資料。如需指標的完整清單，請參閱 the section called “自動調整指標”。

OpenSearch 服務將自動調整事件發送到亞馬遜 EventBridge。您可以用 EventBridge 來設定在收到事件時傳送電子郵件或執行特定動作的規則。若要查看傳送至的每個「自動調整」事件的格式 EventBridge，請參閱the section called “自動調整事件”。

標記 Amazon OpenSearch 服務域

標籤可讓您將任意資訊指派給 Amazon OpenSearch 服務網域，以便對該資訊進行分類和篩選。標籤是您定義並與 OpenSearch 服務網域產生關聯的索引鍵值配對。您可以使用這些標籤來追蹤成本，方

法是將相似標記資源的費用分組。 AWS 不對您的標籤應用任何語義含義。標籤會嚴格解譯為字元字串。所有標籤均包含以下元素：

標籤元素	描述	必要
標籤鍵	標籤金鑰是標籤名稱。金鑰必須是它們所附加的 OpenSearch 服務網域唯一的。如需標籤鍵和標籤值各項基本限制的清單，請參閱使用者定義的標籤限制。	是
標籤值	標籤值即為標籤的字串值。標籤值可以是 `null`，並且在標籤集內不必具有唯一性。例如，在 project/Trinity 及 cost-center/Trinity 標籤集中，均能擁有一個索引鍵/值組。如需標籤鍵和標籤值各項基本限制的清單，請參閱使用者定義的標籤限制。	否

每個 OpenSearch 服務網域都有一個標籤組，其中包含指派給該 OpenSearch 服務網域的所有標籤。AWS 不會自動將任何標籤指派給 OpenSearch 服務網域。標籤集可以包含 0 到 50 個標籤。如果您對網域新增標籤，而該標籤與現有標籤具有相同的鍵，則新值會覆寫舊值。

標記範例

您可以使用鍵來定義類別，其值可為該類別中的某個項目。例如，您可以定義的標籤索引鍵`project`和標籤值`Salix`，表示 OpenSearch 服務網域已指派給 Salix 專案。您也可以使用標籤，透過使用或之類的金鑰，將 OpenSearch Service 網域指定為用於測試`environment=test`或生產環境`environment=production`。嘗試使用一組一致的標籤金鑰，以便更輕鬆地追蹤與 OpenSearch 服務網域相關聯的中繼資料。

您也可以使用標籤來組織帳 AWS 單，以反映您自己的成本結構。為此，請註冊以獲取包含標籤鍵值的 AWS 帳戶 帳單。接著，根據具有相同標籤鍵值的資源來整理您的帳單資訊，以便查看合併資源的成本。例如，您可以使用索引鍵值配對標記多個 OpenSearch Service 網域，然後整理帳單資訊，以查看多個服務中每個網域的總費用。如需詳細資訊，請參閱 https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/cost-alloc-tags.html 帳單與成本管理文件中的AWS 使用成本分配標記。

> **Note**
>
> 標籤是快取用於授權之用。因此， OpenSearch 服務網域上的標籤新增和更新可能需要幾分鐘的時間才能使用。

處理標籤 (主控台)

主控台是標記網域的最簡單方法。

建立標籤 (主控台)

1. 前往 https://aws.amazon.com，然後選擇 Sign In to the Console (登入主控台)。
2. 在分析下，選擇 Amazon OpenSearch 服務。
3. 選取您要新增標籤的目標網域，然後前往 Tags (標籤) 索引標籤。
4. 選擇 Manage (管理) 和 Add new tag (新增標籤)。
5. 輸入標籤索引鍵和選用的值。
6. 選擇 儲存。

若要刪除標籤，請按照同樣的步驟進行，然後在 Manage tags (管理標籤) 頁面上選擇 Remove (移除)。

如需使用主控台處理標籤的詳細資訊，請參閱 《AWS 管理主控台入門指南》中的標籤編輯器。

處理標籤 (AWS CLI)

您可以使用 AWS CLI 與--add-tags指令建立資源標籤。

語法

```
add-tags --arn=<domain_arn> --tag-list Key=<key>,Value=<value>
```

參數	描述
`--arn`	附加標籤之 OpenSearch 服務網域的 Amazon 資源名稱。
`--tag-list`	以空格分隔且格式如下的一系列鍵值組：`Key=<key>,Value=<value>`

範例

以下範例為 logs 網域建立兩個標籤：

```
aws opensearch add-tags --arn arn:aws:es:us-east-1:379931976431:domain/logs --tag-list
 Key=service,Value=OpenSearch Key=instances,Value=m3.2xlarge
```

您可以使用--remove-tags命令從 OpenSearch 服務網域移除標記。

語法

```
remove-tags --arn=<domain_arn> --tag-keys Key=<key>,Value=<value>
```

參數	描述
`--arn`	附加標籤的 OpenSearch 服務網域的 Amazon 資源名稱 (ARN)。
`--tag-keys`	一組要從 OpenSearch 服務域中刪除的空格分隔的鍵-值對。

範例

以下範例會將上述範例所建立的兩個標籤從 logs 網域移除：

```
aws opensearch remove-tags --arn arn:aws:es:us-east-1:379931976431:domain/logs --tag-
keys service instances
```

您可以使用以下--list-tags命令檢視 OpenSearch 服務網域的現有標記：

語法

```
list-tags --arn=<domain_arn>
```

參數	描述
`--arn`	標籤所附加之 OpenSearch 服務網域的 Amazon 資源名稱 (ARN)。

範例

以下範例會列出 logs 網域的所有資源標籤：

```
aws opensearch list-tags --arn arn:aws:es:us-east-1:379931976431:domain/logs
```

使用標籤 (AWS SDK)

開 AWS 發套件 (Android 和 iOS 開發套件除外) 支援 Amazon OpenSearch 服務 API 參考中定義的所有動作，包括`AddTags``ListTags`、和`RemoveTags`操作。如需有關安裝和使用 AWS SDK 的詳細資訊，請參閱AWS 軟體開發套件。

Python

此範例使用適用於 Python (Bodo) 的 AWS 開發套件中的OpenSearchService低階 Python 用戶端，將標籤新增至網域、列出附加至網域的標籤，以及從網域移除標籤。您必須提供 `DOMAIN_ARN`、`TAG_KEY` 和 `TAG_VALUE` 的值。

```
import boto3
from botocore.config import Config  # import configuration

DOMAIN_ARN = ''  # ARN for the domain. i.e "arn:aws:es:us-east-1:123456789012:domain/
my-domain
TAG_KEY = ''  # The name of the tag key. i.e 'Smileyface'
TAG_VALUE = ''  # The value assigned to the tag. i.e 'Practicetag'

# defines the configurations parameters such as region

my_config = Config(region_name='us-east-1')
client = boto3.client('opensearch', config=my_config)


# defines the client variable

def addTags():
    """Adds tags to the domain"""

    response = client.add_tags(ARN=DOMAIN_ARN,
                               TagList=[{'Key': TAG_KEY,
                                         'Value': TAG_VALUE}])

    print(response)


def listTags():
    """List tags that have been added to the domain"""

    response = client.list_tags(ARN=DOMAIN_ARN)
```

```
    print(response)


def removeTags():
    """Remove tags that have been added to the domain"""

    response = client.remove_tags(ARN=DOMAIN_ARN, TagKeys=[TAG_KEY])

    print('Tag removed')
    return response
```

在 Amazon OpenSearch 服務域上執行管理操作

Amazon Ser OpenSearch vice 提供多種管理選項，如果您需要對網域的問題進行疑難排解，可提供精細的控制。這些選項包括在資料節點上重新啟動 OpenSearch 處理序的功能，以及重新啟動資料節點的能力。

OpenSearch Service 會監控節點健全狀況參數，並在發生異常時採取更正措施以保持網域穩定。使用管理選項可在節點上重新啟動 OpenSearch處理序並重新啟動節點本身，您可以控制其中一些緩和動作。

您可以使用 AWS Management Console AWS CLI、或 AWS SDK 來執行這些動作。以下各節說明如何使用主控台執行這些動作。

重新啟動節點上的 OpenSearch 處理序

若要在節點上重新啟動 OpenSearch 處理序

1. 瀏覽至 OpenSearch 服務主控台，位於https://console.aws.amazon.com/aos/。
2. 在左側導覽窗格中選擇 Domains (網域)。選擇您要使用的網域名稱。
3. 網域詳細資料頁面開啟後，瀏覽至 [執行個體健全狀況] 索引標籤
4. 在 [資料] 節點下，選取您要重新啟動處理序的節點旁邊的按鈕。
5. 選擇操作下拉列表，然後選擇重新啟動 OpenSearch/彈性搜索過程。
6. 在強制回應上選擇「確認」。
7. 若要查看您啟動的動作狀態，請選取節點的名稱。節點詳細資料頁面開啟後，選擇節點名稱下的「事件」索引標籤，以查看與該節點相關聯的事件清單。

重新啟動資料節點

若要重新啟動資料節點

1. 瀏覽至 OpenSearch 服務主控台，位於https://console.aws.amazon.com/aos/。
2. 在左側導覽窗格中選擇 Domains (網域)。選擇您要使用的網域名稱。
3. 網域詳細資料頁面開啟後，瀏覽至 [執行個體健全狀況] 索引標籤
4. 在 [資料] 節點下，選取您要重新啟動處理序的節點旁邊的按鈕。
5. 選擇「操作」下拉列表，然後選擇「重新啟
6. 在強制回應上選擇「確認」。
7. 若要查看您啟動的動作狀態，請選取節點的名稱。節點詳細資料頁面開啟後，選擇節點名稱下的「事件」索引標籤，以查看與該節點相關聯的事件清單。

重新啟動節點上的儀表板或 Kibana 處理序

若要在節點上重新啟動儀表板或 Kibana 處理作業

1. 瀏覽至 OpenSearch 服務主控台，位於https://console.aws.amazon.com/aos/。
2. 在左側導覽窗格中選擇 Domains (網域)。選擇您要使用的網域名稱。
3. 網域詳細資料頁面開啟後，瀏覽至 [執行個體健全狀況] 索引標籤
4. 在 [資料] 節點下，選取您要重新啟動處理序的節點旁邊的按鈕。
5. 選擇「操作」下拉列表，然後選擇「重新啟動儀表板/Kibana 過程」。
6. 在強制回應上選擇「確認」。
7. 若要查看您啟動的動作狀態，請選取節點的名稱。節點詳細資料頁面開啟後，選擇節點名稱下的「事件」索引標籤，以查看與該節點相關聯的事件清單。

限制

管理選項有下列限制：

- 彈性搜尋 7.x 版及更新版本支援管理選項。
- 管理選項不支援啟用待命狀態之異地同步備份的網域。
- 具有三個或更多資料節點的網域支援和 Elasticsearch 程序重新啟動和資料節點重新啟動。OpenSearch

- 具有兩個或多個資料節點的網域支援儀表板和 Kibana 程序支援。
- 若要在節點上重新啟動 OpenSearch 程序或將節點重新開機，網域不得處於紅色狀態，且所有索引都必須設定複本。

使用 Amazon OpenSearch 服務直接查詢與 Amazon S3

您可以使用 Amazon OpenSearch 服務直接查詢在 Amazon S3 中查詢數據。Amazon OpenSearch 服務提供與 Amazon S3 的直接查詢整合，作為分析 Amazon S3 中的操作日誌和 Amazon S3 資料湖的一種方式，而無需在服務之間切換。您現在可以分析雲端物件存放區中的 OpenSearch 資料，並同時使用服務的營運分析和視覺化。

透過 Amazon S3 直接查詢，您不再需要建立複雜的ETL管道，也不需要在 OpenSearch 服務和 Amazon S3 儲存中產生複製資料的費用。您也可以安裝包含預先定義儀表板的常用記錄類型範本整合，並設定針對該記錄類型量身打造的資料加速。範本包括VPC流程日AWS CloudTrail誌、日誌和 Amazon S3 日誌。加速度包括跳過索引、具體化視觀表和涵蓋索引。

主題

- 定價
- 限制
- 建議
- 配額
- 支援地區
- 使用 Amazon S3 建立亞馬遜 OpenSearch 服務資料來源整合
- 在 OpenSearch 儀表板中配置資料來源
- 加速查詢
- 查詢 OpenSearch 儀表板中的資料
- 管理資料來源

定價

您需要支付用於建立和處理直接查詢的現有 OpenSearch 服務和 Amazon S3 資源費用。傳送至 Amazon S3 的查詢會使用可計費運算，並顯示為每小時 OpenSearch 運算單位 (OCUs)。

使用 Amazon S3 的直接查詢有兩種類型：互動式和加速度。互動式查詢會對您在 Amazon S3 中的資料執行分析。當您執行新的查詢時， OpenSearch Service 會啟動持續至少三分鐘的新工作階段。OpenSearch 服務會保持工作階段作用中，以確保後續查詢能夠快速執行。加速查詢使用計算來維護 OpenSearch 服務中的索引。這些查詢通常需要更長的時間，因為它們會將不同數量的資料擷取到 OpenSearch Service 中，以便讓互動式查詢執行更快。

如需詳細資訊，請參閱 Amazon OpenSearch 服務定價。

限制

下列限制適用於使用 Amazon S3 進行 OpenSearch 服務直接查詢。

- 您的 OpenSearch 網域必須是 2.13 版或更新版本，才能支援 OpenSearch 服務直接查詢。
- 不適用於 OpenSearch 無伺服器。
- 您的 OpenSearch 網域，且 AWS Glue Data Catalog 必須位於相同的網域 AWS 帳戶。您的 Amazon S3 儲存貯體可以位於不同的帳戶中 (需要將條件新增至您的IAM政策)，但必須與您的網域位於 AWS 區域 同一個帳戶。
- 不支援某些資料類型。支援的資料類型僅限於「實木地板」CSV、和「」JSON。
- OpenSearch 使用 Amazon S3 進行的服務直接查詢僅支援從查詢工作台產生的 Spark 資料表。Spark 串流不支援 AWS Glue Data Catalog 或 Athena 內產生的資料表，這是維持加速度並將索引保持在最新狀態所需的資料表。
- 數據必須在查詢之前展平，或者您必須SQL在 OpenSearch 服務中使用將嵌套列更改為專用列。
- 缺少的列可能需要使用`COALESCE`SQL函數返回結果。
- 如果資料結構發生變更，則 AWS Glue 表格和現有加速度都需要更新。
- OpenSearch 執行個體類型具有網路裝載限制，具體取決於執行個體類型 (10 v. 100)。
- AWS CloudFormation 範本尚不受支援。
- 並非所有PPL指令和功能都受到支援。

建議

我們建議您在使用直接查詢時執行下列動作：

- 使用年、月、日、小時的分區格式將資料內嵌到 Amazon S3，以加快查詢速度。
- 對查詢使用限制，以確保您不會提取太多資料。
- 使用索引狀態管理 (在適用的情況下) 來維護具體化視觀表和涵蓋索引的儲存體。
- 在不再需要的加速工作和索引時刪除。
- 構建跳過索引時，請使用 bloom 過濾器以獲得高基數，對於大範圍使用最小/最大值。建議您使用在高基數欄位上設定的值。
- 使用參考指南將資料匯出到 Amazon S3。您可以使用CloudFront、CloudTrail和 E lastic Load Balancing 等 AWS 記錄檔。

配額

您的帳戶具有下列與 Amazon S3 的 OpenSearch 服務直接查詢相關的配額。每次啟動查詢時，OpenSearch Service 都會開啟工作階段，並使其保持作用狀態至少十分鐘。這會移除後續查詢中的工作階段啟動時間，以減少查詢延遲。

描述	最大值	可以覆寫
每個網域的連線	10	是
每個網域的資料來源	20	是
每個網域的索引	5	是
每個資料來源的並行階段	10	是
OCU每個查詢最大值	60	是
查詢執行時間上限 (分鐘)	30	是
每OCUs個加速度最大	20	是
最大暫時儲存	20	是

支援地區

下列區域適用於 Amazon S3 的直接 OpenSearch 服務查詢：亞太區域 (香港)、亞太區域 (孟買)、亞太區域 (首爾)、亞太區域 (新加坡)、亞太區域 (雪梨)、亞太區域 (東京)、加拿大 (中部)、歐洲 (法蘭克福)、歐洲 (愛爾蘭)、歐洲 (斯德哥爾摩)、美國東部 (維吉尼亞北部)、美國東部 (維吉尼亞北部)、美國東部 (俄亥俄) 和美國西部 (俄亥俄)。

使用 Amazon S3 建立亞馬遜 OpenSearch 服務資料來源整合

您可以透過 AWS Management Console 或為 OpenSearch 服務建立新的 Amazon S3 直接查詢資料來源。API每個新資料來源都會使用 AWS Glue Data Catalog 來管理代表 Amazon S3 儲存貯體的表格。

主題

- 必要條件

- 設定新的直接查詢資料來源
- 對應 AWS Glue Data Catalog 角色 (如果在建立資料來源之後啟用了精細的存取控制)
- 後續步驟

必要條件

您必須先擁有 2.13 版或更新版本的 OpenSearch 網域，才能建立資料來源。如需設定此項目的指示，請參閱the section called “ 建立 OpenSearch 服務網域”。

設定新的直接查詢資料來源

您可以使用 AWS Management Console 或 OpenSearch 服API務在網域上設定直接查詢資料來源。

AWS Management Console

1. 瀏覽至 Amazon OpenSearch 服務主控台，位於https://console.aws.amazon.com/aos/。
2. 在左側導覽窗格中選擇 Domains (網域)。
3. 選取您要為其設定新資料來源的網域。這會開啟網域詳細資訊頁面。選擇一般網域詳細資料下方的「連線」標籤，然後找到「直接查詢」區段。
4. 選擇 Create (建立)。
5. 在資料來源建立頁面上，輸入新資料來源的名稱。在 [資料來源類型] 下，選擇 [Amazon S3]。選擇現有IAM角色，該角色對於可在 AWS Glue Data Catalog 和 Amazon S3 中存取的內容有限制。
6. 選擇 Create (建立)。這會開啟包含 OpenSearch 儀表板的資料來源詳細資訊畫面URL。您可以瀏覽至此項目URL以完成後續步驟。

OpenSearch 服務 API

使用此AddDataSourceAPI作業在您的網域中建立新的資料來源。

```
POST https://es.region.amazonaws.com/2021-01-01/opensearch/domain/domain-name/
dataSource

{
   "DataSourceType": {
        "s3GlueDataCatalog": {
            "RoleArn": "arn:aws:iam::account-id:role/Admin"
        }
    }
```

```
   "Description": "data-source-description",
   "Name": "my-data-source"
}
```

下列範例原則示範建立和管理資料來源所需的最低權限。如果您擁有更廣泛的權限 (例如`s3:*`或`AdminstratorAccess`原則)，這些權限會包含範例原則中最低權限的權限。

整合需要存取寫入 Amazon S3 和 AWS Glue Data Catalog. 對於 Amazon S3，我們需要寫入存取權，以便在建立加速時維護檢查點位置。對於 AWS Glue Data Catalog，我們需要寫入存取權，才能從 OpenSearch 服務中管理整合所需的資料庫、資料表和分割區。

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"HttpActionsForOpenSearchDomain",
         "Effect":"Allow",
         "Action":"es:ESHttp*",
         "Resource":"arn:aws:es:<region>:<account>:domain/<domain_name>/*"
      },
      {
         "Sid":"AmazonOpenSearchS3GlueDirectQueryReadAllS3Buckets",
         "Effect":"Allow",
         "Action":[
            "s3:GetObject",
            "s3:GetObjectVersion",
            "s3:ListBucket"
         ],
         "Condition":{
            "StringEquals":{
               "aws:ResourceAccount":"<account>"
            }
         },
         "Resource":"*"
      },
      {
         "Sid":"AmazonOpenSearchDirectQueryGlueCreateAccess",
         "Effect":"Allow",
         "Action":[
            "glue:CreateDatabase",
            "glue:CreatePartition",
            "glue:CreateTable",
            "glue:BatchCreatePartition"
```

```
            ],
            "Resource":"*"
        },
        {
            "Sid":"AmazonOpenSearchS3GlueDirectQueryModifyAllGlueResources",
            "Effect":"Allow",
            "Action":[
                "glue:DeleteDatabase",
                "glue:DeletePartition",
                "glue:DeleteTable",
                "glue:GetDatabase",
                "glue:GetDatabases",
                "glue:GetPartition",
                "glue:GetPartitions",
                "glue:GetTable",
                "glue:GetTableVersions",
                "glue:GetTables",
                "glue:UpdateDatabase",
                "glue:UpdatePartition",
                "glue:UpdateTable",
                "glue:BatchGetPartition",
                "glue:BatchDeletePartition",
                "glue:BatchDeleteTable"
            ],
            "Resource":[
                "arn:aws:glue:us-east-1:<account>:table/*",
                "arn:aws:glue:us-east-1:<account>:database/*",
                "arn:aws:glue:us-east-1:<account>catalog"
            ],
            "Condition":{
                "StringEquals":{
                    "aws:ResourceAccount":"<account>"
                }
            }
        },
        {
            "Sid":"ReadAndWriteActionsForS3CheckpointBucket",
            "Effect":"Allow",
            "Action":[
                "s3:ListMultipartUploadParts",
                "s3:DeleteObject",
                "s3:GetObject",
                "s3:PutObject",
                "s3:GetBucketLocation",
```

```
            "s3:ListBucket"
         ],
         "Condition":{
            "StringEquals":{
               "aws:ResourceAccount":"<account>"
            }
         },
         "Resource":[
            "arn:aws:s3:::<checkpoint_bucket_name>",
            "arn:aws:s3:::<checkpoint_bucket_name>/*"
         ]
      }
   ]
}
```

若要在不同帳戶中支援 Amazon S3 儲存貯體，您需要在 Amazon S3 政策中加入條件，並新增適當的帳戶。

```
"Condition": {
                "StringEquals": {
                    "aws:ResourceAccount": "{{accountId}}"
                }
```

角色也必須具有下列信任原則，用來指定目標識別碼。

```
{
    "Version":"2012-10-17",
    "Statement":[
       {
          "Effect":"Allow",
          "Principal":{
             "Service": "directquery.opensearchservice.amazonaws.com"
          },
          "Action":"sts:AssumeRole"
       }
     ]
}
```

如需建立角色的指示，請參閱使用自訂信任政策建立角色。

如果您在 OpenSearch Service 中啟用了精細的存取控制，則會自動為您的資料來源建立新的 OpenSearch精細存取控制角色。新的細粒度存取控制角色的名稱將會是AWS `OpenSearchDirectQuery` *`<name of data source>`*。

根據預設，角色只能存取直接查詢資料來源索引。雖然您可以將角色設定為限制或授與資料來源的存取權，但建議您不要調整此角色的存取權。如果刪除資料來源，則會刪除此角色。如果任何其他使用者對應至角色，這將會移除其他使用者的存取權。

對應 AWS Glue Data Catalog 角色 (如果在建立資料來源之後啟用了精細的存取控制)

如果您在建立資料來源後啟用了精細的存取控制，則必須將非管理員使用者對應至具有 AWS Glue Data Catalog 存取權的IAM角色，才能執行直接查詢。若要手動建立可對應至`glue_access`角色的後端IAM角色，請執行下列步驟：

> **Note**
>
> 索引用於對數據源的任何查詢。對指定資料來源的請求索引具有讀取權限的使用者可以讀取該資料來源的所有查詢。具有結果索引讀取權限的使用者可以讀取針對該資料來源的所有查詢的結果。

1. 從 [OpenSearch 儀表板] 的主功能表中，選擇 [安全性]、[角色] 和 [建立角色]。
2. 將角色命名為膠合存取。
3. 對於叢集權限，請選取`indices:data/write/bulk*indices:data/read/scroll`、、`indices:data/read/scroll/clear`。
4. 在 Index 中，輸入下列要授與使用者角色存取權的索引：
   - `.query_execution_request_`*`<name of data source>`*
   - `query_execution_result_`*`<name of data source>`*
   - `flint_*`
5. 對於索引權限，請選取`indices_all`。
6. 選擇 Create (建立)。
7. 選擇 Mapped users (已映射的使用者)、Manage mapping (管理映射)。
8. 在後端角色下，新增需要呼叫網域ARN之權限的角色。 AWS Glue

```
arn:aws:iam::account-id:role/role-name
```

9. 選取 [對應]，並確認角色顯示在 [對應的使用者] 下。

如需對應角色的詳細資訊，請參閱the section called “將角色映射至使用者”。

後續步驟

建立資料來源之後， OpenSearch Service 會為您提供 OpenSearch 儀表板URL。您可以使用此選項來設定存取控制、定義資料表、針對常用的記錄類型設定以記錄類型為基礎的儀表板，以及查詢資料。

在 OpenSearch 儀表板中配置資料來源

現在您已經建立了資料來源，您可以設定安全設定、定義 Amazon S3 表或設定加速資料索引。在查詢資料之前，本節將引導您完成 OpenSearch 儀表板中資料來源的各種使用案例。

若要設定下列各節，您必須先在 OpenSearch 儀表板中巡覽至您的資料來源。在左側導覽列的 [管理] 下方，選擇 [資料來源]。在「管理資料來源」下，選取您在主控台中建立的資料來源名稱。

設定存取控制

在資料來源的詳細資訊頁面上，找到 [存取控制] 區段，然後選擇 [編輯]。如果您已安裝安全性外掛程式，請選擇「受限制」，然後選取您要提供哪些以角色為基礎的群組，以存取新資料來源。如果您只希望管理員能夠存取資料來源，也可以選擇「僅管理員」。

> **Important**
>
> 索引用於對數據源的任何查詢。對指定資料來源的請求索引具有讀取權限的使用者可以讀取該資料來源的所有查詢。具有結果索引讀取權限的使用者可以讀取針對該資料來源的所有查詢的結果。

熱門 AWS 記錄類型的設定整合

OpenSearch 儀表板可讓您使用原始日誌使用 Amazon S3 中存放的常見日誌類型輕鬆快速開始使用，但 Amazon VPC Flow 日誌支援 Parquet 格式的日誌除外。 OpenSearch 儀表板提供整合功能，可安裝資產的存取權，例如資 AWS Glue Data Catalog 料表、儲存的查詢和儀表板。這些資產由

OpenSearch 加速提供支援，並會在您安裝後自動更新。您可以從資料來源詳細資料頁面或左側導覽列設定整合。若要執行此作業：

1. 選取您要安裝的記錄檔類型。請確定您安裝的日誌類型具有 Amazon S3 標籤。
2. 如果尚未選取 Amazon S3 連線，請選取連線類型。
3. 選取要安裝整合的資料來源名稱、資料的 Amazon S3 位置、要用於維持加密索引狀態的檢查點，以及根據您的使用案例選取所需的資產。

> **Note**
>
> 建立IAM角色時，您為具有檢查點位置寫入動作許可的檢查點指定 Amazon S3 資源。您將需要參考具有檢查點位置寫入權限的 Amazon S3 儲存貯體位置。如果不這樣做，整合將安裝的加速度將會失敗。

> **Note**
>
> Amazon VPC 流程日誌整合需要使用 OpenSearch 儀表板安裝修補程式。填入您已安裝的儀表板可能需要幾分鐘的時間。

將資料匯出至 Amazon S3 的參考指南

您可以使用下列參考指南將資料匯出到 Amazon S3：

資料來源：

- 阿帕奇訪問
- CloudFront
- CloudTrail

- Elastic Load Balancing
- Amazon Simple Storage Service (Amazon S3)
- AWS WAF
- Amazon VPC 流
- NGINX

使用查詢工作台創建星火表

從 OpenSearch 服務到 Amazon S3 的直接查詢使用 AWS Glue Data Catalog. 您可以從「查詢工作台」中建立資料表，而不必離開 OpenSearch 儀表板。

若要管理資料來源中的現有資料庫和表格，或建立要使用直接查詢的新表格，請從左側導覽選取「查詢工作台」，然後從資料來源下拉式清單中選取 Amazon S3 資料來源。

若要為以 Parquet 格式存放在 S3 中的VPC流程記錄設定資料表，請執行下列查詢：

```
CREATE TABLE
datasourcename.gluedatabasename.vpclogstable (version INT, account_id STRING,
 interface_id STRING,
srcaddr STRING, dstaddr STRING, srcport INT, dstport INT, protocol INT, packets
 BIGINT,
bytes BIGINT, start BIGINT, end BIGINT, action STRING, log_status STRING,
`aws-account-id` STRING, `aws-service` STRING, `aws-region` STRING, year STRING,
month STRING, day STRING, hour STRING)

USING parquet PARTITIONED BY (aws-account-id, aws-service, aws-region, year, month,
day, hour)

LOCATION "s3://accountnum-vpcflow/AWSLogs"
```

建立資料表之後，請執行下列查詢，以確保其與直接查詢相容：

```
MSCK REPAIR TABLE  datasourcename.databasename.vpclogstable
```

加速查詢

在資料來源的詳細資料頁面上，選擇 [加速效能] 選項。為了確保快速體驗 Amazon S3 中的資料，您可以設定三種不同類型的加速，將資料索引到 OpenSearch 服務中 — 跳過索引、具體化檢視和覆蓋索引。

跳過索引

使用跳過索引，您可以僅索引存放在 Amazon S3 中的資料的中繼資料。當您查詢含有略過索引的資料表時，查詢規劃工具會參考索引並重新寫入查詢以有效率地找到資料，而不是掃描所有分割區和檔案。這允許跳過索引快速縮小存儲數據的特定位置。

在資料來源詳細資訊頁面中，選取加速效能，您可以在其中選取要加速的資料庫和表格來開始使用。交替地，您可以選擇自動生成跳過索引。如果您想要手動新增要加速的欄位，您可以選取 [新增欄位] 按鈕。添加字段時，系統會詢問您要添加哪種類型的跳過索引。您需要從以下選項中選擇一項：

- 分區：使用數據分區詳細信息來查找數據（最適合基於分區的列，例如年，月，日，小時）
- MinMax：使用索引資料行的下限和上限來尋找資料 (最適合數值資料行)
- ValueSet：使用唯一值集來尋找資料 (最適合具有低中等基數且需要精確比對的資料行)
- BloomFilter：使用 bloom 篩選器來尋找資料 (最適合具有高基數且不需要精確比對的欄)

您也可以使用「查詢工作台」在資料表上手動建立略過索引。只要從資料來源下拉式清單中選取 S3 資料來源，然後新增下列查詢即可：

```
CREATE SKIPPING INDEX
ON datasourcename.gluedatabasename.vpclogstable(
 `srcaddr` BLOOM_FILTER,
 `dstaddr` BLOOM_FILTER,
 `day` PARTITION,
 `account_id`BLOOM_FILTER
 ) WITH (
index_settings = '{"number_of_shards":5,"number_of_replicas":1}',
auto_refresh = true,
checkpoint_location = 's3://accountnum-vpcflow/AWSLogs/checkpoint'
)
```

具體化視觀表

透過具體化視觀表，您可以使用複雜的查詢 (例如彙總) 來強化儀表板視覺效果。具體化視觀表會根據查詢，將少量資料擷取至 OpenSearch Service Storage。 OpenSearch 然後，Service 會從可用於視覺效果的擷取資料形成索引。您可以使用管理具體化視觀表索引the section called “索引狀態管理”，就像使用任何其他 OpenSearch 索引一樣。

由於您將指定目標索引，因此系統會要求您命名索引並添加 Watermark Delay，該延遲定義了遲到數據可以進入並仍然處理的方式。

使用下列查詢為您在其中建立的VPC流程日誌表格建立新的具體化視觀表the section called “使用查詢工作台創建星火表”：

```
CREATE MATERIALIZED VIEW {table_name}__week_live_mview AS
  SELECT
```

```
    cloud.account_uid AS `aws.vpc.cloud_account_uid`,
    cloud.region AS `aws.vpc.cloud_region`,
    cloud.zone AS `aws.vpc.cloud_zone`,
    cloud.provider AS `aws.vpc.cloud_provider`,

    CAST(IFNULL(src_endpoint.port, 0) AS LONG) AS `aws.vpc.srcport`,
    CAST(IFNULL(src_endpoint.svc_name, 'Unknown') AS STRING)  AS `aws.vpc.pkt-src-aws-
service`,
    CAST(IFNULL(src_endpoint.ip, '0.0.0.0') AS STRING)  AS `aws.vpc.srcaddr`,
    CAST(IFNULL(src_endpoint.interface_uid, 'Unknown') AS STRING)  AS `aws.vpc.src-
interface_uid`,
    CAST(IFNULL(src_endpoint.vpc_uid, 'Unknown') AS STRING)  AS `aws.vpc.src-vpc_uid`,
    CAST(IFNULL(src_endpoint.instance_uid, 'Unknown') AS STRING)  AS `aws.vpc.src-
instance_uid`,
    CAST(IFNULL(src_endpoint.subnet_uid, 'Unknown') AS STRING)  AS `aws.vpc.src-
subnet_uid`,

    CAST(IFNULL(dst_endpoint.port, 0) AS LONG) AS `aws.vpc.dstport`,
    CAST(IFNULL(dst_endpoint.svc_name, 'Unknown') AS STRING) AS `aws.vpc.pkt-dst-aws-
service`,
    CAST(IFNULL(dst_endpoint.ip, '0.0.0.0') AS STRING)  AS `aws.vpc.dstaddr`,
    CAST(IFNULL(dst_endpoint.interface_uid, 'Unknown') AS STRING)  AS `aws.vpc.dst-
interface_uid`,
    CAST(IFNULL(dst_endpoint.vpc_uid, 'Unknown') AS STRING)  AS `aws.vpc.dst-vpc_uid`,
    CAST(IFNULL(dst_endpoint.instance_uid, 'Unknown') AS STRING)  AS `aws.vpc.dst-
instance_uid`,
    CAST(IFNULL(dst_endpoint.subnet_uid, 'Unknown') AS STRING)  AS `aws.vpc.dst-
subnet_uid`,
    CASE
      WHEN regexp(dst_endpoint.ip, '(10\\..*)|(192\\.168\\..*)|(172\\.1[6-9]\\..*)|
(172\\.2[0-9]\\..*)|(172\\.3[0-1]\\.*)')
        THEN 'ingress'
      ELSE 'egress'
      END AS `aws.vpc.flow-direction`,

    CAST(IFNULL(connection_info['protocol_num'], 0) AS INT) AS
 `aws.vpc.connection.protocol_num`,
    CAST(IFNULL(connection_info['tcp_flags'], '0') AS STRING)  AS
 `aws.vpc.connection.tcp_flags`,
    CAST(IFNULL(connection_info['protocol_ver'], '0') AS STRING)  AS
 `aws.vpc.connection.protocol_ver`,
    CAST(IFNULL(connection_info['boundary'], 'Unknown') AS STRING)  AS
 `aws.vpc.connection.boundary`,
```

```
    CAST(IFNULL(connection_info['direction'], 'Unknown') AS STRING)  AS
 `aws.vpc.connection.direction`,

    CAST(IFNULL(traffic.packets, 0) AS LONG) AS `aws.vpc.packets`,
    CAST(IFNULL(traffic.bytes, 0) AS LONG) AS `aws.vpc.bytes`,

    CAST(FROM_UNIXTIME(time / 1000) AS TIMESTAMP) AS `@timestamp`,
    CAST(FROM_UNIXTIME(start_time / 1000) AS TIMESTAMP) AS `start_time`,
    CAST(FROM_UNIXTIME(start_time / 1000) AS TIMESTAMP) AS `interval_start_time`,
    CAST(FROM_UNIXTIME(end_time / 1000) AS TIMESTAMP) AS `end_time`,
    status_code AS `aws.vpc.status_code`,

    severity AS `aws.vpc.severity`,
    class_name AS `aws.vpc.class_name`,
    category_name AS `aws.vpc.category_name`,
    activity_name AS `aws.vpc.activity_name`,
    disposition AS `aws.vpc.disposition`,
    type_name AS `aws.vpc.type_name`,

    region AS `aws.vpc.region`,
    accountid AS `aws.vpc.account-id`
  FROM
  datasourcename.gluedatabasename.vpclogstable
WITH (
  auto_refresh = true,
  refresh_interval = '15 Minute',
  checkpoint_location = 's3://accountnum-vpcflow/AWSLogs/checkpoint',
  watermark_delay = '1 Minute',
)
```

覆蓋索引

使用涵蓋索引，您可以從表格中的指定欄擷取資料。這是三種索引類型中效能最高的一種。由於 OpenSearch Service 會從您想要的資料行擷取所有資料，因此您可以獲得更好的效能並執行進階分析。

就像具體化視圖一樣， OpenSearch Service 會從覆蓋索引資料建立新的索引。您可以將此新索引用於儀表板視覺效果和其他 OpenSearch 服務功能，例如異常偵測或地理空間功能。您可以使用管理覆蓋視圖索引the section called “索引狀態管理”，就像您可以使用任何其他 OpenSearch 索引一樣。

使用下列查詢為您在中建立的VPC流程記錄資料表建立新的涵蓋索引the section called “使用查詢工作台創建星火表”：

```
CREATE INDEX vpc_covering_index
ON datasourcename.gluedatabasename.vpclogstable (version, account_id, interface_id,
srcaddr, dstaddr, srcport, dstport, protocol, packets,
bytes, start, action, log_status STRING,
`aws-account-id`, `aws-service`, `aws-region`, year,
month, day, hour )
WITH (
  auto_refresh = true,
  refresh_interval = '15 minute',
  checkpoint_location = 's3://accountnum-vpcflow/AWSLogs/checkpoint'
)
```

查詢 OpenSearch 儀表板中的資料

設定資料表並設定所需的選用查詢加速後，您現在就可以開始對資料執行分析。若要查詢資料，請從 [OpenSearch 儀表板] 的 [探索] 頁面或 [可觀測性] 頁面上的下拉式功能表中選取資料來源。

如果您正在使用跳過索引或尚未建立索引，則可以使用SQL或管道處理語言 (PPL) 來查詢資料。如果您已設定具體化視觀表或涵蓋索引，您已經有索引，而且可以在整個儀表板中使用儀表板查詢語言 (DQL)。您也可以使PPL用觀察性插件，並SQL與查詢工作台插件。目前，只有觀察性和查詢工作台外掛程式支援PPL和SQL。如需使用 OpenSearch 服務查詢資料API，請參閱 async API 文件。

> **Note**
>
> 並非所有PPL指令和功能都受到支援。如需支援的命令清單，請參閱支援的命令。

SQL

使用下列查詢針對您在其中建立的VPC流程記錄資料表執行範例SQL查詢the section called “使用查詢工作台創建星火表”：

```
SELECT srcaddr, SUM (CAST(bytes AS LONG)) as total_bytes
 FROM datasourcename.gluedatabasename.vpclogstable GROUP BY srcaddrORDER BY total_bytes
 DESCLIMIT 10;
```

PPL

您可以使用下列查詢，針對您在其中建立的VPC記錄資料表執行範例PPL查詢the section called “使用查詢工作台創建星火表”：

```
source = datasourcename.gluedatabasename.vpclogstable | fields account_id, srcaddr,
 dstaddr, action | head 10
```

建議

在某些情況下，結果無法如預期般傳回。如果您遇到任何問題，我們建議您採取以下措施：

- SELECT* 語句不返回結果-檢查你的表，看看它是否有嵌套 struc 列需要被分解。
- 選取多個資料表時，請使用SQL UNION陳述式來參照多個資料表。
- 加速度設定為使用特定數目的 Worker 來執行查詢。如果查詢傳回緩慢，您可以手動配置更多 Worker 來執行查詢以提高效能。
- 構建跳過索引時，使用 bloom 過濾器進行高基數和大範圍的最小/最大值，以節省域上的空間。如果您需要執行完全相符，建議您在中等基數欄位上設定值。
- 如需常用SQL查詢的詳細資訊，請參閱AWS 服務記錄檔。

管理資料來源

管理資料來源是維持直接查詢資料來源和其他 AWS 解決方案的可靠性、可用性和效能的重要組成部分。 AWS 提供下列工具來監控、在發生錯誤時報告，並在適當時採取自動動作。

主題

- 使用 CloudWatch 指標資料來源監控
- 啟用和停用資料來源
- 使用 AWS 預算監控
- 使用 Amazon S3 刪除亞馬遜 OpenSearch 服務數據源

使用 CloudWatch 指標資料來源監控

您可以使用來監視直接查詢 CloudWatch。 CloudWatch 收集原始數據並將其處理為可讀的近乎實時的指標。這些統計資料會保留 15 個月，以便您存取歷史資訊，並更清楚 Web 應用程式或服務的執行效能。

您也可以設定警示來監控特定閾值，並在達到這些閾值時傳送通知或採取動作。有關更多信息，請參閱什麼是 Amazon CloudWatch。

直接查詢會報告下列量度：

指標	描述
AsyncQueryCreateAPI	API對建立非同步查詢所發出的要求總數。 相關統計數字： 平均值、最大值、總和 尺寸:`ClientId`, `DomainName` 頻率：60 秒
AsyncQueryGetApiRequestCount	API對擷取非同步查詢結果所發出的要求總數。 相關統計數字： 平均值、最大值、總和 尺寸:`ClientId`, `DomainName` 頻率：60 秒
AsyncQueryCancelApiRequestCount	API對取消非同步查詢所做的要求總數。 相關統計數字： 平均值、最大值、總和 尺寸:`ClientId`, `DomainName` 頻率：60 秒
A syncQueryGet ApiFailed RequestCusErrCount	由於客戶相關錯誤 (例如，無效的查詢 ID)，擷取非同步查詢結果時失敗的要求數目。 相關統計數字： 平均值、最大值、總和

指標	描述
	尺寸:`ClientId`, `DomainName` 頻率：60 秒
AsyncQueryCancelApiFailedRequestCusErrCount	由於客戶相關錯誤 (例如，無效的查詢 ID)，擷取非同步查詢結果時失敗的要求數目。 相關統計數字：平均值、最高值、總和 尺寸:`ClientId`, `DomainName` 頻率：60 秒
AsyncQueryCancelApiFailedRequestSysErrCount	因客戶相關錯誤而建立非同步查詢時失敗的要求數目。 相關統計資料：平均數、上限、總和 尺寸:`ClientId`, `DomainName` 頻率：60 秒
A syncQueryGet ApiFailed RequestSysErrCount	擷取非同步查詢結果時因系統相關錯誤而失敗的要求數目。 相關統計資料：平均數、上限、總和 尺寸:`ClientId`, `DomainName` 頻率：60 秒

啟用和停用資料來源

如果您想要停止資料來源的直接查詢使用情況，您可以選擇停用資料來源。停用資料來源將完成執行現有查詢，並停止使用者執行所有新查詢。

一旦停用資料來源，就會將加速設定為提升查詢效能，例如跳過索引、具體化視觀表、涵蓋索引等。停用資料來源後，將資料來源設定為使用中後，使用者查詢將如預期般執行。先前設置並設置為手動的加速度將需要手動配置為再次按計劃運行。

使用 AWS 預算監控

Amazon Ser OpenSearch vice 正在將帳戶層級的OCU用量資料填入帳單和成本管理的 Cost Explorer 中。客戶可以在帳戶層級考慮OCU使用情況，並在超過閾值時設定閾值和警示。

要在 Cost Explorer 中篩選的用法類型格式看起來像 RegionCode-DirectQuery OCU (OCU-hours)。希望在 DirectQuery OCU (OCU-Hours) 使用量達到臨界值時收到通知的客戶，可以建立 AWS 預算帳戶，並根據他們設定的閾值設定警示。或者，客戶可以選擇設定 Amazon SNS 主題，如果符合閾值條件，該主題將關閉資料來源。

> **Note**
>
> AWS 預算中的使用量資料不是即時的，最多可能會延遲 8 小時。

使用 Amazon S3 刪除亞馬遜 OpenSearch 服務數據源

當您刪除資料來源時，Amazon OpenSearch 服務會將其從您的網域中移除。 OpenSearch 服務也會移除與資料來源相關聯的索引。您的交易資料不會從 Amazon S3 刪除，但 Amazon S3 不會將新資料傳送至 OpenSearch 服務。

您可以使用 AWS Management Console 或 OpenSearch 服務刪除資料來源整合API。

AWS Management Console

刪除資料來源

1. 瀏覽至 Amazon OpenSearch 服務主控台，位於https://console.aws.amazon.com/aos/。
2. 在左側導覽窗格中，選擇 [網域]。
3. 選取您要刪除其資料來源的網域。這會開啟網域詳細資訊頁面。選擇一般資訊下方的「連線」標籤，然後找到「直接查詢」區段。
4. 選取要刪除的資料來源，選擇 [刪除]，然後確認刪除。

OpenSearch 服務 API

使用此DeleteDataSourceAPI作業刪除網域中的現有資料來源。

```
POST https://es.region.amazonaws.com/2021-01-01/opensearch/domain/domain-name/
dataSource/data-source-name
```

監控 Amazon Amazon Amazon Ser OpenSearch vice 網域

監控是維護 Amazon Ser OpenSearch vice 及其他AWS解決方案的可靠性、可用性和效能所不可或缺。 AWS提供了以下工具來監控您的 OpenSearch Service 資源，報告問題並適時採取自動作。

Amazon CloudWatch

Amazon Amazon Amazon Amazon Amazon Amazon Amazon Amazon Amazon Amazon Amazon Amazon Amazon Amazon 即時CloudWatch監控您 OpenSearch 您可以收集和追蹤指標、建立自訂儀表板，以及設定警示，在指標達到某個閾值時通知您或採取動作。如需詳細資訊，請參閱 Amazon Amazon CloudWatch 使用者指南。

亞馬遜CloudWatch日誌

您可以使用 Amazon CloudWatch Logs 來監控、存放和存取您的日OpenSearch誌檔案。CloudWatchLogs 可監控日誌檔案中的資訊，並在滿足特定閾值時向您發出通知。如需詳細資訊，請參閱 Amazon CloudWatch Logs 使用者指南。

Amazon EventBridge

Amazon Amazon 即時傳EventBridge遞近乎即時的系統事件串OpenSearch流。您可以建立監看特定事件的規則，並在這些事件發生時在其他 AWS 服務內觸發自動化動作。如需詳細資訊，請參閱 Amazon Amazon EventBridge 使用者指南。

AWS CloudTrail

AWS CloudTrail會擷取 OpenSearch Service 的所有組態 API 呼叫。它可將這些事件傳遞到您指定的 Amazon S3 儲存貯體。使用此資訊，可確認哪些使用者和帳戶提出請求、提出請求的來源 IP 地址以及提出請求的時間。如需詳細資訊，請參閱 AWS CloudTrail使用者指南。

主題

- 使用 Amazon 監控 OpenSearch 叢集指標 CloudWatch
- 使用 Amazon OpenSearch 日誌監控 CloudWatch 日誌
- 監控 Amazon OpenSearch 服務中的審核日誌
- 使用 Amazon 監控 OpenSearch 服務事件 EventBridge
- 使用來監控 Amazon Amazon Ser OpenSearch vice API 呼叫 AWS CloudTrail

使用 Amazon 監控 OpenSearch 叢集指標 CloudWatch

Amazon OpenSearch 服務將數據從您的域發布到 Amazon CloudWatch。 CloudWatch 可讓您擷取有關這些資料點的統計資料，做為一組排序的時間序列資料 (稱為量度)。 OpenSearch 服務會以 60 秒 CloudWatch 的間隔傳送大多數指標。如果您使用一般用途或磁帶磁EBS碟區，磁EBS碟區指標只會每五分鐘更新一次。所有累積指標（例如`ThreadpoolSearchRejected`）都在內存中`ThreadpoolWriteRejected`，並且將失去狀態。指標會在節點卸除、節點退回、節點取代和藍/綠部署期間重設。有關 Amazon 的更多信息 CloudWatch，請參閱 Amazon CloudWatch 用戶指南。

OpenSearch 服務主控台會根據來自的原始資料顯示一系列圖表 CloudWatch。根據您的需求，您可能希望在中檢視叢集資料， CloudWatch 而不是在主控台中檢視圖形。此服務會封存指標兩週，之後才會捨棄它們。這些指標不收取額外費用，但 CloudWatch 仍會收取建立儀表板和警示的費用。如需詳細資訊，請參閱 Amazon CloudWatch 定價。

OpenSearch 服務會將下列指標發佈至 CloudWatch：

- the section called “叢集指標”
- the section called “專用主節點指標”
- the section called “EBS體積指標”
- the section called “執行個體指標”
- the section called “UltraWarm 度量”
- the section called “冷儲存指標”
- the section called “提醒指標”
- the section called “異常偵測指標”
- the section called “非同步搜尋指標”
- the section called “SQL度量”
- the section called “k-NN 指標”
- the section called “跨叢集搜尋指標”
- the section called “跨叢集複寫指標”
- the section called “Learning to Rank 指標”
- the section called “Piped Processing Language 指標”

檢視量度 CloudWatch

CloudWatch 測量結果會先依服務命名空間分組，然後依每個命名空間內的各種維度組合分組。

使用 CloudWatch 主控台檢視指標

1. 在開啟 CloudWatch 主控台https://console.aws.amazon.com/cloudwatch/。
2. 在左側導覽窗格中，尋找 Metrics (指標)，然後選擇 All metrics (所有指標)。選取 ES/OpenSearchService 命名空間。
3. 選擇維度以檢視對應指標。個別節點的指標位於 `ClientId, DomainName, NodeId` 維度中。叢集指標位於 `Per-Domain, Per-Client Metrics` 維度中。某些節點指標會在叢集層級彙總，因此包含在這兩個維度中。碎片指標位於 `ClientId, DomainName, NodeId, ShardRole` 維度中。

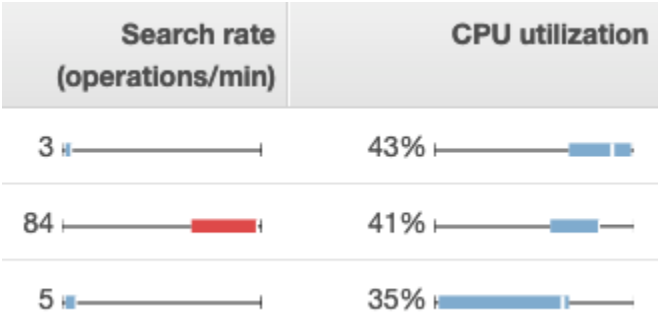
使用檢視測量結果清單 AWS CLI

執行以下命令：

```
aws cloudwatch list-metrics --namespace "AWS/ES"
```

解譯服務中的健康圖表 OpenSearch

若要檢視 OpenSearch Service 中的測量結果，請使用叢集健全狀況和執行個體健全狀況 「執行個體健全狀況」標籤使用方塊圖表來提供每個 OpenSearch節點的健全狀況的 at-a-glance 可見度：



- 每個色彩方塊都能顯示該節點在整段指定時間的值範圍。
- 藍色方塊表示其值與其他節點相符。紅色方塊表示其值出現異常。
- 每個方塊中的白色線條則表示目前節點的值。
- 每個方塊在任何一邊上的「whiskers」則表示所有節點在整段時間的最小值與最大值。

如果您對網域進行組態變更，則 Cluster health (叢集運作狀態) 和 Instance health (執行個體運作狀態) 索引標籤上個別執行個體清單的大小通常會短暫出現加倍的情況，然後才恢復為正確的數字。如需此行為的說明，請參閱the section called “組態變更”。

叢集指標

Amazon OpenSearch 服務為叢集提供以下指標。

指標	描述
`ClusterStatus.green`	1 的值表示將所有索引碎片分配至叢集中的節點。 相關統計資訊：Maximum
`ClusterStatus.yellow`	1 的值表示將所有索引的主要碎片分配給叢集中的節點，但用於至少一個索引的複寫碎片則不分配。如需詳細資訊，請參閱the section called “黃色叢集狀態”。 相關統計資訊：Maximum
`ClusterStatus.red`	1 的值表示至少一個索引的主要碎片和複寫碎片未分配至叢集中的節點。如需詳細資訊，請參閱the section called “紅色叢集狀態”。 相關統計資訊：Maximum
`Shards.active`	作用中主要碎片和複本碎片的總數。 相關統計數字：最大，總和
`Shards.unassigned`	未分配至叢集中節點的碎片數目。 相關統計數字：最大，總和
`Shards.delayedUnassigned`	其節點分配已被逾時設定延遲的碎片數量。 相關統計數字：最大，總和
`Shards.activePrimary`	活動中主要碎片的數量。 相關統計數字：最大，總和
`Shards.initializing`	正在初始化的碎片數量。 相關統計資料：總和
`Shards.relocating`	正在重新放置的碎片數量。

指標	描述
	相關統計資料：總和
Nodes	OpenSearch 服務叢集中的節點數目，包括專用主節點和 UltraWarm 節點。如需詳細資訊，請參閱the section called “組態變更”。 相關統計資訊：Maximum
SearchableDocuments	叢集中跨所有資料節點的可搜尋文件的總數。 相關統計資料：下限、上限、平均數
DeletedDocuments	叢集中跨所有資料節點的標記進行刪除文件的總數。這些文件不再出現在搜尋結果中，而 OpenSearch 只會在區段合併期間從磁碟中移除已刪除的文件。此指標會在刪除請求後增加，在區段合併後降低。 相關統計資料：下限、上限、平均數
CPUUtilization	叢集中資料節點的CPU使用百分比。「最大值」顯示CPU使用率最高的節點。平均值代表叢集中的所有節點。此指標也適用於個別節點。 相關統計資訊：Maximum、Average

指標	描述
`FreeStorageSpace`	叢集中資料節點的可用空間。`Sum` 會顯示叢集的總可用空間，但您必須保留一分鐘的間隔，才能取得正確的值。`Minimum` 和 `Maximum` 分別會顯示具有最少和最多可用空間的節點。此測量結果也可用於個別節點。 OpenSearch `ClusterBlockException` 當此量度達到時，服務會擲回一個`0`。若要復原，您必須刪除索引、新增較大的執行個體，或將EBS基礎儲存新增至現有執行個體。如需進一步了解，請參閱 the section called “缺少可用儲存空間”。 OpenSearch 服務主控台會以 GiB 顯示此值。Amazon 控 CloudWatch 制台將其顯示在 MiB 中。 **Note** `FreeStorageSpace` 將永遠低於 OpenSearch `_cluster/stats` 和`_cat/allocation` APIs提供的值。 OpenSearch Service 會在每個執行個體上保留一定百分比的儲存空間供內部作業使用。如需詳細資訊，請參閱計算儲存需求。 相關統計資訊：Minimum、Maximum、Average、Sum
`ClusterUsedSpace`	已用於叢集的空間總數。您必須保留一分鐘的間隔，才能取得正確的數值。 OpenSearch 服務主控台會以 GiB 顯示此值。Amazon 控 CloudWatch 制台將其顯示在 MiB 中。 相關統計資訊：Minimum、Maximum

指標	描述
`ClusterIndexWrites Blocked`	指示您的叢集是否要接受或封鎖外來的寫入請求。0 值表示叢集接受請求。1 值表示叢集封鎖請求。 常見的因素包括：`FreeStorageSpace` 過低或 `JVMMemory Pressure` 過高。若要減輕此問題，可考慮增加更多的磁碟空間或擴展您的叢集。 相關統計資訊：Maximum
`JVMMemoryPressure`	叢集中所有資料節點所使用之 Java 堆積的最大百分比。OpenSearch 服務RAM對 Java 堆使用一半的實例，最多 32 GiB 的堆積大小。您可以將執行個體垂直縮放至 64 GiBRAM，此時您可以透過新增執行個體來水平縮放。請參閱 the section called “建議的 CloudWatch 鬧鐘”。 相關統計資訊：Maximum **Note** 此指標的邏輯在服務軟體 R20220323 中有所變更。如需詳細資訊，請參閱版本備註。
`OldGenJVMMemoryPre ssure`	用於叢集中所有資料節點的「舊一代」的 Java 堆積的最大百分比。此指標也適用於節點層級。 相關統計資訊：Maximum
`AutomatedSnapshotF ailure`	叢集中失敗的自動快照數量。1 值表示此網域過去 36 小時未執行任何自動快照。 相關統計資訊：Minimum、Maximum
`CPUCreditBalance`	可用於叢集中資料節點的剩餘CPU積分。點CPU數可提供一分鐘的完整CPU核心效能。如需詳細資訊，請參閱 Amazon EC2 開發人員指南中的CPU積分。此指標僅適用於 T2 執行個體類型。 相關統計資訊：Minimum

指標	描述
OpenSearchDashboardsHealthyNodes	OpenSearch 儀表板的健康狀態檢查。如果最小值、最大值和平均值都等於 1，則 Dashboards 的行為正常。如果您有 10 個節點，其中最大為 1，最小為 0，平均為 0.7，這表示 7 個節點 (70%) 狀況良好，3 個節點 (30%) 狀況不良。 相關統計資料：下限、上限、平均數
OpensearchDashboardsReportingFailedRequestSysErrCount	產生因伺服器問題或功能限制而失敗之控制 OpenSearch 面板報告的要求數目。 相關統計資料：總和
OpensearchDashboardsReportingFailedRequestUserErrCount	產生因用戶端問題而失敗的 OpenSearch 控制面板報告的要求數目。 相關統計資料：總和
OpensearchDashboardsReportingRequestCount	產生 OpenSearch 控制面板報表的請求總數。 相關統計資料：總和
OpensearchDashboardsReportingSuccessCount	產生「 OpenSearch 控制面板」報表的成功要求數目。 相關統計資料：總和
KMSKeyError	值 1 表示 AWS KMS 已停用用來加密靜態資料的金鑰。若要使網域恢復正常運作，請重新啟用此金鑰。主控台只會針對加密靜態資料的網域顯示此指標。 相關統計資訊：Minimum、Maximum
KMSKeyInaccessible	值 1 表示 AWS KMS 用於加密靜態數據的密鑰已被刪除或撤銷其授予 OpenSearch 服務。您無法復原此狀態的網域。但是，如果您有手動快照，您可以用它來將網域的資料遷移至新的網域。主控台只會針對加密靜態資料的網域顯示此指標。 相關統計資訊：Minimum、Maximum

指標	描述
`InvalidHostHeaderRequests`	對包含無效 (或遺失) 主機標頭之 OpenSearch 叢集發出的HTTP要求數目。有效要求包含網域主機名稱做為主機標頭值。 OpenSearch 對於沒有限制性存取原則的公用存取網域，服務會拒絕無效要求。我們建議將限制存取政策套用到所有網域。 如果您看到此測量結果的值較大，請確認您的用 OpenSearch 戶端在其要求中包含網域主機名稱 (例如，其 IP 位址)。 相關統計資料：總和
`OpenSearchRequests (previously ElasticsearchRequests)`	對 OpenSearch 叢集發出的要求數目。 相關統計資料：總和
`2xx, 3xx, 4xx, 5xx`	產生指定HTTP回應碼的網域要求數目 (2 xx、3 xx、4 xx、5 xx)。 相關統計資料：總和
`ThroughputThrottle`	指出磁碟是否已節流。當和的合併輸送量高於最大輸送量時`ReadThroughputMicroBursting`，`WriteThroughputMicroBursting` 就會發生節流。`MaxProvisionedThroughput` `MaxProvisionedThroughput` 是執行個體輸送量或佈建磁碟區輸送量的較低值。值 1 表示磁碟已限制。0 值表示正常行為。 有關執行個體輸送量的資訊，請參閱 Amazon EBS 優化執行個體。有關磁碟區輸送量的資訊，請參閱 Amazon EBS 磁碟區類型。 相關統計資訊：Minimum、Maximum

指標	描述
IopsThrottle	指出網域上每秒的輸入/輸出作業數目 (IOPS) 是否已被節流。當IOPS資料節點違反EBS磁碟區或資料節點EC2執行個體的最大允許限制時，就會發生節流。 如需執行個體的相關資訊IOPS，請參閱 Amazon EBS 優化執行個體。如需磁碟區的相關資訊IOPS，請參閱 Amazon EBS 磁碟區類型。 相關統計資訊：Minimum、Maximum
HighSwapUsage	值 1 表示因分頁錯誤而產生的交換可能在特定期間內造成基礎磁碟使用量尖峰。 相關統計資訊：Maximum

專用主節點指標

Amazon OpenSearch 服務為專用主節點提供以下指標。

指標	描述
MasterCPUUtilization	專用主節點使用的CPU資源百分比上限。當這項指標達到 60% 時，建議提高執行個體類型的大小。 相關統計資訊：Maximum
MasterFreeStorageSpace	此指標無關，可忽略。此服務不使用主節點做為資料節點。
MasterJVMMemoryPressure	用於叢集中所有專用主節點的 Java heap 的最大百分比。當這項指標達到 85% 時，建議移至較大的執行個體類型。 相關統計資訊：Maximum

指標	描述
	Note 此指標的邏輯在服務軟體 R20220323 中有所變更。如需詳細資訊，請參閱版本備註。
`MasterOldGenJVMMemoryPressure`	用於每個主節點「舊一代」的 Java 堆積最大百分比。 相關統計資訊：Maximum
`MasterCPUCreditBalance`	可用於叢集中專用主節點的剩餘點CPU數。點CPU數可提供一分鐘的完整CPU核心效能。如需詳細資訊，請參閱 Amazon EC2 開發人員指南中的CPU積分。此指標僅適用於 T2 執行個體類型。 相關統計資訊：Minimum
`MasterReachableFromNode`	`MasterNotDiscovered` 例外狀況的運作狀態檢查。1 值表示正常行為。0 值表示 `/_cluster/health/` 失敗。 失敗表示無法從來源節點存取主節點。它們通常是網絡連接問題或 AWS 依賴性問題。 相關統計資訊：Maximum
`MasterSysMemoryUtilization`	已使用主節點記憶體的百分比。 相關統計資訊：Maximum

EBS體積指標

Amazon OpenSearch 服務為EBS磁碟區提供以下指標。

指標	描述
`ReadLatency`	EBS磁碟區讀取作業的延遲時間 (以秒為單位)。此指標也適用於個別節點。 相關統計資料：下限、上限、平均數

指標	描述
WriteLatency	EBS磁碟區寫入作業的延遲時間 (以秒為單位)。此指標也適用於個別節點。 相關統計資料：下限、上限、平均數
ReadThroughput	EBS磁碟區讀取作業的輸送量 (以每秒位元組為單位)。此指標也適用於個別節點。 相關統計資料：下限、上限、平均數
ReadThroughputMicroBursting	考慮微量爆發時，EBS磁碟區上讀取作業的輸送量 (以每秒位元組為單位)。此指標也適用於個別節點。當EBS磁碟區大量爆發IOPS或輸送量大幅縮短時間 (不到一分鐘) 時，就會發生微突增。 相關統計資料：下限、上限、平均數
WriteThroughput	EBS磁碟區寫入作業的輸送量 (以每秒位元組為單位)。此指標也適用於個別節點。 相關統計資料：下限、上限、平均數
WriteThroughputMicroBursting	考慮微量爆發時，EBS磁碟區上寫入作業的輸送量 (以每秒位元組為單位)。此指標也適用於個別節點。當EBS磁碟區大量爆發IOPS或輸送量大幅縮短時間 (不到一分鐘) 時，就會發生微突增。 相關統計資料：下限、上限、平均數
DiskQueueDepth	磁碟區的擱置輸入和輸出 (I/O) 要求EBS數目。 相關統計資料：下限、上限、平均數
ReadIOPS	EBS磁碟區讀取作業每秒的輸入和輸出 (I/O) 作業數目。此指標也適用於個別節點。 相關統計資料：下限、上限、平均數

指標	描述
`ReadIOPSMicroBursting`	考量微突增時，EBS磁碟區讀取作業每秒的輸入和輸出 (I/O) 作業數目。此指標也適用於個別節點。當EBS磁碟區大量爆發IOPS或輸送量大幅縮短時間 (不到一分鐘) 時，就會發生微突增。 相關統計資料：下限、上限、平均數
`WriteIOPS`	EBS磁碟區上寫入作業每秒的輸入和輸出 (I/O) 作業數目。此指標也適用於個別節點。 相關統計資料：下限、上限、平均數
`WriteIOPSMicroBursting`	考慮微量爆發時，EBS磁碟區上寫入作業每秒的輸入和輸出 (I/O) 作業數目。此指標也適用於個別節點。當EBS磁碟區大量爆發IOPS或輸送量大幅縮短時間 (不到一分鐘) 時，就會發生微突增。 相關統計資料：下限、上限、平均數
`BurstBalance`	EBS磁碟區成組分解儲存貯體中剩餘的輸入和輸出 (I/O) 積分百分比。值 100 表示磁碟區已累積至最大點數。如果此百分比低於 70%，請參閱 the section called “低 EBS 爆量餘額”。對於具有 gp3 磁碟區類型的網域，以及具有磁碟區大小高於 1000 GiB 之 gp2 磁碟區的網域，爆量餘額會保持在 0。 相關統計資料：下限、上限、平均數

執行個體指標

Amazon OpenSearch 服務會為網域中的每個執行個體提供下列指標。 OpenSearch Service 也會彙總這些執行個體指標，以提供整體叢集健康狀況的深入分析 您可以在主控台使用 Sample Count (取樣計數) 統計數字來驗證此行為。請注意，下表中每個指標有節點和叢集的相關統計資料。

> **Important**
>
> 不同版本的 Elasticsearch 會使用不同的執行緒集區來處理對. `_index` API Elasticsearch 1.5 和 2.3 版會使用索引執行緒集區。彈性搜索 5. x、6.0 和 6.2 使用批量執行緒集區。OpenSearch 和彈性搜索 6.3 及更高版本使用寫線程池。目前， OpenSearch 服務主控台不包含批量執行緒集區的圖形。

使用 `GET _cluster/settings?include_defaults=true` 來檢查叢集的執行緒集區和佇列大小。

指標	描述
`ConcurrentSearchRate`	資料節點上所有碎片使用每分鐘並行區段搜尋的搜尋要求總數。單次調用`_search`API可能會返回許多不同碎片的結果。如果上述碎片當中有五個是在同一個節點上，則該節點會回報這個指標為 5，即使該用戶端僅發出一次請求。 相關節點統計資訊：平均數 相關叢集統計資訊：平均數、上限、總和
`ConcurrentSearchLatency`	在分 N 到分鐘 (N-1) 之間的節點中，使用並行區段搜尋所使用的所有搜尋所花費的總時間差異 (以毫秒為單位)。 相關節點統計資訊：平均數 相關叢集統計資訊：平均數、上限
`IndexingLatency`	在分 N 到分鐘 (N-1) 之間的節點中，所有索引作業所採用的總時間差異 (以毫秒為單位)。 相關節點統計資訊：平均數 相關叢集統計資訊：平均數、上限
`IndexingRate`	每分鐘進行的索引操作次數。單一呼叫會新增兩個文件，並將兩個計數更新為四個作業，這些作業可能會散佈在一或多個節點。`_bulk` API如果該索引具有一或多個複本，且位於沒有最佳化執行個體的 OpenSearch網域，叢集中的其他節點也會記錄共四個索引作業。對於具有最佳化執行個體的 OpenSearch 網域，具有複本的其他節點不會記錄任何作業。文件刪除不列入此指標。 相關節點統計資訊：平均數 相關叢集統計資訊：平均數、上限、總和

指標	描述
SearchLatency	在分 N 到分鐘 (N-1) 之間的節點中的所有搜尋所採用的總時間差異 (以毫秒為單位)。 相關節點統計資訊：平均數 相關叢集統計資訊：平均數、上限
SearchRate	資料節點上每分鐘對所有碎片發出搜尋請求的總次數。單次調用_searchAPI可能會返回許多不同碎片的結果。如果上述碎片當中有五個是在同一個節點上，則該節點會回報這個指標為 5，即使該用戶端僅發出一次請求。 相關節點統計資訊：平均數 相關叢集統計資訊：平均數、上限、總和
SegmentCount	資料節點上的區段數。您擁有的區段越多，每次搜尋所需的時間就越長。 OpenSearch 偶爾會將較小的區段合併為較大的區段。 相關節點統計數字：最大，平均 相關叢集統計資訊：總和、上限、平均數
SysMemoryUtilization	已使用執行個體記憶體的百分比。此測量結果的高值是正常的，通常不代表叢集的問題。如需有關潛在效能和穩定性問題的更佳指標，請參閱 JVMMemoryPressure 指標。 相關節點統計資訊：下限、上限、平均數 相關叢集統計資訊：下限、上限、平均數
JVMGCYoungCollectionCount	「新一代」廢棄項目收集的已執行次數。大量、持續擴增的執行次數是叢集操作的正常情況。 相關節點統計資訊：上限 相關叢集統計資訊：總和、上限、平均數

指標	描述
JVMGCYoungCollectionTime	叢集已執行「新一代」廢棄項目收集的時間 (單位為毫秒)。 相關節點統計資訊：上限 相關叢集統計資訊：總和、上限、平均數
JVMGCOldCollectionCount	「舊一代」廢棄項目收集的已執行次數。在資源充足的叢集中，這個數字應該很小，而且不常擴增。 相關節點統計資訊：上限 相關叢集統計資訊：總和、上限、平均數
JVMGCOldCollectionTime	叢集已花在執行「舊一代」廢棄項目收集的時間 (單位為毫秒)。 相關節點統計資訊：上限 相關叢集統計資訊：總和、上限、平均數
OpenSearchDashboardsConcurrentConnections	「 OpenSearch控制面板」的作用中並行連線數目。如果此數值持續增加，請考慮擴展您的叢集。 相關節點統計資訊：上限 相關叢集統計資訊：總和、上限、平均數
OpenSearchDashboardsHealthyNode	個別「 OpenSearch 儀表板」節點的健康狀態檢查。1 值表示正常行為。0 值表示無法存取 Dashboards。 相關節點統計數字：最小 相關叢集統計資訊：下限、上限、平均數
OpenSearchDashboardsHeapTotal	MiB 中配置給 OpenSearch 儀表板的堆積記憶體量。不同的EC2執行個體類型會影響確切的記憶體配置。 相關節點統計資訊：上限 相關叢集統計資訊：總和、上限、平均數

指標	描述
OpenSearchDashboardsHeapUsed	OpenSearch 儀表板在 MiB 中使用的堆積記憶體絕對數量。 相關節點統計資訊：上限 相關叢集統計資訊：總和、上限、平均數
OpenSearchDashboardsHeapUtilization	OpenSearch儀表板使用的可用堆積記憶體百分比上限。如果此值超過 80%，請考慮擴展您的叢集。 相關節點統計資訊：上限 相關叢集統計資訊：下限、上限、平均數
OpenSearchDashboardsOS1MinuteLoad	OpenSearch 儀表板的一分鐘CPU負載平均值。理想情況下，CPU 負載應保持在 1.00 以下。雖然暫時峰值沒問題，但如果此指標一致高於 1.00，建議您增加執行個體類型的大小。 相關節點統計資訊：平均數 相關叢集統計資訊：平均數、上限
OpenSearchDashboardsRequestTotal	向「 OpenSearch 控制面板」發出的HTTP要求總數。如果您的系統速度緩慢或您看到大量 Dashboards 請求，請考慮增加執行個體類型的大小。 相關節點統計數字：總和 相關叢集統計資訊：總和
OpenSearchDashboardsResponseTimesMaxInMillis	OpenSearch 儀表板回應要求所需的時間上限 (以毫秒為單位)。如果請求持續需要很長的時間才能傳回結果，請考慮增加執行個體類型的大小。 相關節點統計資訊：上限 相關叢集統計數字：最大，平均

指標	描述
SearchTaskCancelled	協調節點取消的次數。 相關節點統計數字：總和 相關叢集統計資訊：總和
SearchShardTaskCancelled	資料節點取消的次數。 相關節點統計數字：總和 相關集群統計數字：總和，
ThreadpoolForce_mergeQueue	強制合併執行緒集區中的已排入佇列任務數量。如果佇列大小持續高居不下，請考慮擴展您的叢集。 相關節點統計資訊：上限 相關叢集統計資訊：總和、上限、平均數
ThreadpoolForce_mergeRejected	強制合併執行緒集區中的已拒絕任務數量。如果這個數量持續增加，請考慮擴展您的叢集。 相關節點統計資訊：上限 相關叢集統計資訊：總和
ThreadpoolForce_mergeThreads	強制合併執行緒集區的大小。 相關節點統計資訊：上限 相關叢集統計資訊：平均數、總和
ThreadpoolIndexQueue	索引執行緒集區中的已排入佇列任務數量。如果佇列大小持續高居不下，請考慮擴展您的叢集。索引佇列的大小上限為 200。 相關節點統計資訊：上限 相關叢集統計資訊：總和、上限、平均數

指標	描述
ThreadpoolIndexRejected	索引執行緒集區中的已拒絕任務數量。如果這個數量持續增加，請考慮擴展您的叢集。 相關節點統計資訊：上限 相關叢集統計資訊：總和
ThreadpoolIndexThreads	索引執行緒集區的大小。 相關節點統計資訊：上限 相關叢集統計資訊：平均數、總和
ThreadpoolSearchQueue	搜尋執行緒集區中的已排入佇列任務數量。如果佇列大小持續高居不下，請考慮擴展您的叢集。搜尋佇列的大小上限為 1,000。 相關節點統計資訊：上限 相關叢集統計資訊：總和、上限、平均數
ThreadpoolSearchRejected	搜尋執行緒集區中的已拒絕任務數量。如果這個數量持續增加，請考慮擴展您的叢集。 相關節點統計資訊：上限 相關叢集統計資訊：總和
ThreadpoolSearchThreads	搜尋執行緒集區的大小。 相關節點統計資訊：上限 相關叢集統計資訊：平均數、總和
Threadpoolsql-workerQueue	SQL搜尋繫線集區中排入佇列的工作數目。如果佇列大小持續高居不下，請考慮擴展您的叢集。 相關節點統計資訊：上限 相關叢集統計資訊：總和、上限、平均數

指標	描述
Threadpoolsql-workerRejected	SQL搜尋執行緒集區中拒絕的工作數目。如果這個數量持續增加，請考慮擴展您的叢集。 相關節點統計資訊：上限 相關叢集統計資訊：總和
Threadpoolsql-workerThreads	SQL搜尋繫線集區的大小。 相關節點統計資訊：上限 相關叢集統計資訊：平均數、總和
ThreadpoolBulkQueue	大量執行緒集區中的已排入佇列任務數量。如果佇列大小持續高居不下，請考慮擴展您的叢集。 相關節點統計資訊：上限 相關叢集統計資訊：總和、上限、平均數
ThreadpoolBulkRejected	大量執行緒集區中的已拒絕任務數量。如果這個數量持續增加，請考慮擴展您的叢集。 相關節點統計資訊：上限 相關叢集統計資訊：總和
ThreadpoolBulkThreads	大量執行緒集區的大小。 相關節點統計資訊：上限 相關叢集統計資訊：平均數、總和
ThreadpoolIndexSearcherQueue	索引搜尋器執行緒集區中佇列的工作數目。 相關節點統計資訊：上限 相關叢集統計資訊：總和、上限、平均數

指標	描述
ThreadpoolIndexSearcherRejected	索引搜尋器執行緒集區中拒絕的工作數目。 相關節點統計資訊：上限 相關叢集統計資訊：總和
ThreadpoolIndexSearcherThreads	索引搜尋器執行緒集區的大小。 相關節點統計資訊：上限 相關叢集統計資訊：平均數、總和
ThreadpoolWriteThreads	寫入執行緒集區的大小。 相關節點統計資訊：上限 相關叢集統計資訊：平均數、總和
ThreadpoolWriteQueue	寫入執行緒集區中的已排入佇列任務數量。 相關節點統計資訊：上限 相關叢集統計資訊：平均數、總和
ThreadpoolWriteRejected	寫入執行緒集區中的已拒絕任務數量。 相關節點統計資訊：上限 相關叢集統計資訊：平均數、總和 **Note** 由於 7.1 版中的預設寫入佇列大小從 200 增加到 10000，因此此量度不再是 OpenSearch 服務拒絕的唯一指標。使用 `CoordinatingWriteRejected`、`PrimaryWriteRejected` 和 `ReplicaWriteRejected` 指標來監控 7.1 版及更新版本中的拒絕。

指標	描述
`CoordinatingWriteRejected`	由於上次 OpenSearch 服務程序啟動後的索引壓力，協調節點上發生的拒絕總數。 相關節點統計資訊：上限 相關叢集統計資訊：平均數、總和 在 7.1 版及更高版本中可使用此指標。
`PrimaryWriteRejected`	由於自上次 OpenSearch 服務程序啟動以來的索引壓力，導致主要碎片上發生的拒絕總數。 相關節點統計資訊：上限 相關叢集統計資訊：平均數、總和 在 7.1 版及更高版本中可使用此指標。
`ReplicaWriteRejected`	由於上次 OpenSearch 服務處理序啟動以來的索引壓力，因此複本碎片上發生的拒絕總數。 相關節點統計資訊：上限 相關叢集統計資訊：平均數、總和 在 7.1 版及更高版本中可使用此指標。

UltraWarm 度量

Amazon OpenSearch 服務為UltraWarm節點提供以下指標。

指標	描述
`WarmCPUUtilization`	叢集中 UltraWarm 節點的CPU使用百分比。「最大值」顯示CPU使用率最高的節點。平均值代表叢集中的所有 UltraWarm 節點。此測量結果也可用於個別 UltraWarm 節點。 相關統計資訊：Maximum、Average

指標	描述
WarmFreeStorageSpace	可用暖儲存空間量 (以 MiB 為單位)。因為 UltraWarm使用 Amazon S3 而不是連接的磁碟，所以Sum是唯一相關的統計資料。您必須保留一分鐘的間隔，才能取得正確的數值。 相關統計資料：總和
WarmSearchableDocuments	叢集中跨所有暖索引的可搜尋文件的總數。您必須保留一分鐘的間隔，才能取得正確的數值。 相關統計資料：總和
WarmSearchLatency	在 N 分鐘和分鐘 (N-1) 之間的所有搜尋所採用的總時 UltraWarm 間差異，以毫秒為單位。 相關節點統計資訊：平均數 相關叢集統計資訊：平均數、上限
WarmSearchRate	UltraWarm 節點上所有碎片每分鐘的搜尋要求總數。單次調用_searchAPI可能會返回許多不同碎片的結果。如果上述碎片當中有五個是在同一個節點上，則該節點會回報這個指標為 5，即使該用戶端僅發出一次請求。 相關節點統計資訊：平均數 相關叢集統計資訊：平均數、上限、總和
WarmStorageSpaceUtilization	叢集所使用暖儲存空間的總量 (單位為 MiB)。 相關統計資訊：Maximum
HotStorageSpaceUtilization	叢集所使用熱儲存空間的總量。 相關統計資訊：Maximum
WarmSysMemoryUtilization	已使用溫節點記憶體的百分比。 相關統計資訊：Maximum

指標	描述
HotToWarmMigrationQueueSize	目前等待從熱儲存遷移至暖儲存的索引數目。 相關統計資訊：Maximum
WarmToHotMigrationQueueSize	目前等待從暖儲存遷移至熱儲存的索引數目。 相關統計資訊：Maximum
HotToWarmMigrationFailureCount	從熱儲存遷移至暖儲存的失敗總數。 相關統計資料：總和
HotToWarmMigrationForceMergeLatency	遷移程序的強制合併階段的平均延遲。如果此階段始終需要太長時間，考慮增加 index.ultrawarm.migration.force_merge.max_num_segments 。 相關統計資訊：平均數
HotToWarmMigrationSnapshotLatency	遷移程序的快照階段的平均延遲。如果此階段持續需要太長時間，請確保您的碎片適當調整大小並分佈在整個叢集中。 相關統計資訊：平均數
HotToWarmMigrationProcessingLatency	從熱儲存成功遷移到暖儲存的平均延遲，不包括佇列中花費的時間。此值是完成遷移程序的強制合併、快照和碎片重新放置階段所需的時間總和。 相關統計資訊：平均數
HotToWarmMigrationSuccessCount	從熱儲存遷移至暖儲存的成功總數。 相關統計資料：總和
HotToWarmMigrationSuccessLatency	從熱儲存成功遷移到暖儲存的平均延遲，包括佇列中花費的時間。 相關統計資訊：平均數

指標	描述
`WarmThreadpoolSearchThreads`	UltraWarm 搜尋繫線集區的大小。 相關節點統計資訊：上限 相關叢集統計資訊：平均數、總和
`WarmThreadpoolSearchRejected`	UltraWarm 搜尋執行緒集區中拒絕的工作數目。如果此數字持續增長，請考慮新增更多 UltraWarm節點。 相關節點統計資訊：上限 相關叢集統計資訊：總和
`WarmThreadpoolSearchQueue`	UltraWarm 搜尋繫線集區中排入佇列的工作數目。如果佇列大小一直很高，請考慮新增更多 UltraWarm節點。 相關節點統計資訊：上限 相關叢集統計資訊：總和、上限、平均數
`WarmJVMMemoryPressure`	用於 UltraWarm節點之 Java 堆集的最大百分比。 相關統計資訊：Maximum **Note** 此指標的邏輯在服務軟體 R20220323 中有所變更。如需詳細資訊，請參閱版本備註。
`WarmOldGenJVMMemoryPressure`	用於每個 UltraWarm 節點「舊層代」之 Java 堆積的最大百分比。 相關統計資訊：Maximum

指標	描述
WarmJVMGCYoungCollectionCount	「年輕一代」記憶體回收在 UltraWarm 節點上執行的次數。大量、持續擴增的執行次數是叢集操作的正常情況。 相關節點統計資訊：上限 相關叢集統計資訊：總和、上限、平均數
WarmJVMGCYoungCollectionTime	叢集在 UltraWarm節點上執行「年輕一代」記憶體回收所花費的時間量 (以毫秒為單位)。 相關節點統計資訊：上限 相關叢集統計資訊：總和、上限、平均數
WarmJVMGCOldCollectionCount	在 UltraWarm 節點上執行「舊一代」記憶體回收的次數。在資源充足的叢集中，這個數字應該很小，而且不常擴增。 相關節點統計資訊：上限 相關叢集統計資訊：總和、上限、平均數
WarmConcurrentSearchRate	使用 UltraWarm 節點上所有碎片每分鐘並行區段搜尋的搜尋要求總數。單次調用_searchAPI可能會返回許多不同碎片的結果。如果上述碎片當中有五個是在同一個節點上，則該節點會回報這個指標為 5，即使該用戶端僅發出一次請求。 相關節點統計資訊：平均數 相關叢集統計資訊：總和、上限、平均數
WarmConcurrentSearchLatency	在分 N 到分鐘 (N-1) 之間的 UltraWarm 節點中，使用並行區段搜尋所使用的所有搜尋所花費的總時間差異 (以毫秒為單位)。 相關節點統計資訊：平均數 相關叢集統計數字：最大，平均

指標	描述
WarmThreadpoolIndexSearcherQueue	索 UltraWarm 引搜尋器執行緒集區中佇列的工作數目。 相關節點統計資訊：上限 相關叢集統計資訊：總和、上限、平均數
WarmThreadpoolIndexSearcherRejected	索 UltraWarm 引搜尋器執行緒集區中拒絕的工作數目。 相關節點統計資訊：上限 相關叢集統計資訊：總和
WarmThreadpoolIndexSearcherThreads	索 UltraWarm 引搜尋器執行緒集區的大小。 相關節點統計資訊：上限 相關集群統計：總和，平均

冷儲存指標

Amazon OpenSearch 服務為冷存儲提供以下指標。

指標	描述
ColdStorageSpaceUtilization	叢集所使用冷儲存空間的總量 (單位為 MiB)。 相關統計資料：上限
ColdToWarmMigrationFailureCount	從冷儲存遷移至暖儲存的失敗總數。 相關統計資料：總和
ColdToWarmMigrationLatency	成功完成從冷儲存遷移至暖儲存所需的時間量。 相關統計資訊：平均數
ColdToWarmMigrationQueueSize	目前等待從冷儲存遷移至暖儲存的索引數目。 相關統計資訊：Maximum

指標	描述
ColdToWarmMigrationSuccessCount	從冷儲存遷移至暖儲存的成功總數。 相關統計資料：總和
WarmToColdMigrationFailureCount	從暖儲存遷移至冷儲存的失敗總數。 相關統計資料：總和
WarmToColdMigrationLatency	成功完成從暖儲存遷移至冷儲存所需的時間量。 相關統計資訊：平均數
WarmToColdMigrationQueueSize	目前等待從暖儲存遷移至冷儲存的索引數目。 相關統計資訊：Maximum
WarmToColdMigrationSuccessCount	從暖儲存遷移至冷儲存的成功總數。 相關統計資料：總和

OR1度量

Amazon OpenSearch 服務為OR1執行個體提供以下指標。

指標	描述
RemoteStorageUsedSpace	叢集正在使用的 Amazon S3 空間總量 (以 MiB 為單位)。 相關統計資料：總和
RemoteStorageWriteRejected	由於遠端儲存和複寫壓力，在主要碎片上拒絕的要求總數。這是從上次啟動 OpenSearch 服務程序開始計算的。 相關統計資料：總和
ReplicationLagMaxTime	複本碎片位於主碎片後面的時間量（以毫秒為單位）。 相關統計資訊：Maximum

提醒指標

Amazon OpenSearch 服務提供以下警示指標。

指標	描述
AlertingDegraded	值為 1 表示提醒索引為紅色，或是有一或多個節點不在排程上。0 值表示正常行為。 相關統計資訊：Maximum
AlertingIndexExists	值為 1 表示存在 .opensearch-alerting-config 索引。值為 0 則表示不存在。直到您第一次使用提醒功能為止，這個值都會維持在 0。 相關統計資訊：Maximum
AlertingIndexStatus.green	索引的運作狀態。值為 1 表示綠色。值為 0 表示索引不存在，或是並非綠色。 相關統計資訊：Maximum
AlertingIndexStatus.red	索引的運作狀態。值為 1 表示紅色。值為 0 表示索引不存在，或是並非紅色。 相關統計資訊：Maximum
AlertingIndexStatus.yellow	索引的運作狀態。值為 1 表示黃色。值為 0 表示索引不存在，或是並非黃色。 相關統計資訊：Maximum
AlertingNodesNotOnSchedule	值為 1 表示有些任務並未依照排程執行。值為 0 則表示所有提醒任務都正在依照排程執行 (或是沒有提醒任務)。檢查 OpenSearch 服務主控台或提出_nodes/stats 要求，以查看是否有任何節點顯示高資源使用率。 相關統計資訊：Maximum
AlertingNodesOnSchedule	值為 1 則表示所有提醒任務都正在依照排程執行 (或是沒有提醒任務)。值為 0 表示有些任務並未依照排程執行。 相關統計資訊：Maximum

指標	描述
AlertingScheduledJobEnabled	值為 1 表示 opensearch.scheduled_jobs.enabled 叢集設定為 true。值為 0 表示為 false，且已停用排程任務。 相關統計資訊：Maximum

異常偵測指標

Amazon OpenSearch 服務針對異常偵測提供下列指標。

指標	描述
ADPluginUnhealthy	值 1 表示異常偵測外掛程式無法正常運作，原因是大量失敗或它使用的其中一個索引是紅色。值 0 表示外掛程式如預期般運作。 相關統計資訊：Maximum
ADExecuteRequestCount	偵測異常的請求數。 相關統計資料：總和
ADExecuteFailureCount	偵測異常的失敗請求數。 相關統計資料：總和
ADHCExecuteFailureCount	偵測高基數偵測器異常的失敗請求數。 相關統計資料：總和
ADHCExecuteRequestCount	偵測高基數偵測器異常的請求數。 相關統計資料：總和
ADAnomalyResultsIndexStatusIndexExists	值為 1 表示 .opensearch-anomaly-results 別名指向的索引存在。在您第一次使用異常偵測之前，此值會保持為 0。 相關統計資訊：Maximum

指標	描述
ADAnomalyResultsIndexStatus.red	值為 1 表示 .opensearch-anomaly-results 別名指向的索引是紅色。值為 0 則表示它不是紅色。在您第一次使用異常偵測之前，此值會保持為 0。 相關統計資訊：Maximum
ADAnomalyDetectorsIndexStatusIndexExists	值為 1 表示 .opensearch-anomaly-detectors 索引存在。值為 0 則表示不存在。在您第一次使用異常偵測之前，此值會保持為 0。 相關統計資訊：Maximum
ADAnomalyDetectorsIndexStatus.red	值為 1 表示 .opensearch-anomaly-detectors 索引是紅色。值為 0 則表示它不是紅色。在您第一次使用異常偵測之前，此值會保持為 0。 相關統計資訊：Maximum
ADModelsCheckpointIndexStatusIndexExists	值為 1 表示 .opensearch-anomaly-checkpoints 索引存在。值為 0 則表示不存在。在您第一次使用異常偵測之前，此值會保持為 0。 相關統計資訊：Maximum
ADModelsCheckpointIndexStatus.red	值為 1 表示 .opensearch-anomaly-checkpoints 索引是紅色。值為 0 則表示它不是紅色。在您第一次使用異常偵測之前，此值會保持為 0。 相關統計資訊：Maximum

非同步搜尋指標

Amazon OpenSearch 服務為非同步搜索提供以下指標。

非同步搜尋協調器節點統計數字 (每個協調器節點)

指標	描述
AsynchronousSearchSubmissionRate	過去一分鐘內提交的非同步搜尋數量。
AsynchronousSearchInitializedRate	過去一分鐘內初始化的非同步搜尋數量。
AsynchronousSearchRunningCurrent	目前正在執行的非同步搜尋數量。
AsynchronousSearchCompletionRate	過去一分鐘內成功完成的非同步搜尋數量。
AsynchronousSearchFailureRate	過去一分鐘內完成和失敗的非同步搜尋數量。
AsynchronousSearchPersistRate	過去一分鐘內持續的非同步搜尋數量。
AsynchronousSearchPersistFailedRate	過去一分鐘內無法持續的非同步搜尋數量。
AsynchronousSearchRejected	自節點啟動時間以來拒絕的非同步搜尋總數。

指標	描述
AsynchronousSearchCancelled	自節點啟動時間以來已取消的非同步搜尋總數。
AsynchronousSearchMaxRunningTime	在最後一分鐘的節點上執行非同步搜尋的最長持續時間。

非同步搜尋叢集統計數字

指標	描述
AsynchronousSearchStoreHealth	最後一分鐘持續索引 (RED/non-RED) 中儲存區的健全狀況。
AsynchronousSearchStoreSize	過去一分鐘內所有碎片的系統索引大小。
AsynchronousSearchStoredResponseCount	過去一分鐘內系統索引中存放的回應數量。

自動調整指標

Amazon OpenSearch 服務為自動調整提供以下指標。

指標	描述
AutoTuneChangesHistoryHeapSize	MiB 中堆集大小調整值的變更歷史記錄。

指標	描述
AutoTuneChangesHistoryJVMYoungGenArgs	JVM YongGen 參數的變更歷史記錄。
AutoTuneFailed	布林值，指出自動調整變更是否失敗。
AutoTuneSucceeded	布林值，指出自動調整變更是否成功。
AutoTuneValue	佇列變更歷程記錄 (計數) 和快取調整會變更記錄 (以 MiB 為單位)，以進行不中斷的變更。

異地同步備份含備用量度

Amazon OpenSearch 服務為具備待命功能的異地同步備份提供下列指標。

作用中可用區域中資料節點的節點層級度量

指標	描述
CPUUtilization	叢集中資料節點的CPU使用百分比。「最大值」顯示CPU使用率最高的節點。平均值代表叢集中的所有節點。此指標也適用於個別節點。
FreeStorageSpace	叢集中資料節點的可用空間。Sum 會顯示叢集的總可用空間，但您必須保留一分鐘的間隔，才能取得正確的值。Minimum 和 Maximum 分別會顯示具有最少和最多可用空間的節點。此測量結果也可用於個別節點。OpenSearch ClusterBlockException 當此量度達到時，服務會擲回一個0。若要復原，您必須刪除索引、新增較大的執行個體，或將EBS基礎儲存新增至現有執行個體。如需進一步了解，請參閱 the section called “缺少可用儲存空間”。 OpenSearch 服務主控台會以 GiB 顯示此值。Amazon 控 CloudWatch 制台將其顯示在 MiB 中。

指標	描述
JVMMemory Pressure	叢集中所有資料節點所使用之 Java 堆積的最大百分比。 OpenSearch 服務RAM對 Java 堆使用一半的實例，最多 32 GiB 的堆積大小。您可以將執行個體垂直縮放至 64 GiBRAM，此時您可以透過新增執行個體來水平縮放。請參閱 the section called “建議的 CloudWatch 鬧鐘”。
SysMemory Utilization	已使用執行個體記憶體的百分比。此測量結果的高值是正常的，通常不代表叢集的問題。如需有關潛在效能和穩定性問題的更佳指標，請參閱 JVMMemoryPressure 指標。
IndexingLatency	在分 N 到分鐘 (N-1) 之間的節點中，所有索引作業所採用的總時間差異 (以毫秒為單位)。
IndexingRate	每分鐘進行的索引操作次數。
SearchLatency	在分 N 到分鐘 (N-1) 之間的節點中的所有搜尋所採用的總時間差異 (以毫秒為單位)。
SearchRate	資料節點上每分鐘對所有碎片發出搜尋請求的總次數。
ThreadpoolSearchQueue	搜尋執行緒集區中的已排入佇列任務數量。如果佇列大小持續高居不下，請考慮擴展您的叢集。搜尋佇列的大小上限為 1,000。
ThreadpoolWriteQueue	寫入執行緒集區中的已排入佇列任務數量。
ThreadpoolSearchRejected	搜尋執行緒集區中的已拒絕任務數量。如果這個數量持續增加，請考慮擴展您的叢集。
ThreadpoolWriteRejected	寫入執行緒集區中的已拒絕任務數量。

作用中可用區域中叢集的叢集層級度量

指標	描述
DataNodes	作用中和待命碎片的總數。
DataNodes Shards.active	作用中主要碎片和複本碎片的總數。
DataNodes Shards.un assigned	未分配至叢集中節點的碎片數目。
DataNodes Shards.in itializing	正在初始化的碎片數量。
DataNodes Shards.re locating	正在重新放置的碎片數量。

可用區域輪替量度

如果ActiveReads.*Availability-Zone* = 1，則區域處於作用中狀態。如果ActiveReads.*Availability-Zone* = 0，則區域處於待命狀態。

時間點量度

Amazon OpenSearch 服務針對時間點（PIT）搜索提供以下指標。

PIT協調器節點統計資料 (每個協調節點)

指標	描述
CurrentPo intInTime	節點中使用中PIT搜尋前後關聯的數目。
TotalPoin tInTime	自節點啟動時間以來過期的PIT搜尋前後關聯數目。

指標	描述
AvgPointInTimeAliveTime	自節點啟動時間以來，PIT搜尋前後關聯的平均保持作用狀態。
HasActivePointInTime	值 1 表示自節點啟動時間以來，節點上存在使用中PIT前後關聯。值 0 表示沒有。
HasUsedPointInTime	值 1 表示自節點啟動時間以來，節點上已過期的PIT前後關聯。值 0 表示沒有。

SQL度量

Amazon OpenSearch 服務提供以下SQL支持指標。

指標	描述
SQLFailedRequestCountByCusErr	因為用戶端問題_sqlAPI而失敗的要求數目。例如，請求可能會傳回HTTP狀態碼 400，原因是IndexNotFoundException . 相關統計資料：總和
SQLFailedRequestCountBySysErr	由於伺服器問題或功能限制而失敗的要求數目。_sql API例如，請求可能會傳回HTTP狀態碼 503，原因是VerificationException . 相關統計資料：總和
SQLRequestCount	要求的數目_sqlAPI。 相關統計資料：總和
SQLDefaultCursorRequestCount	類似於SQLRequestCount ，但只計算分頁請求。 相關統計資料：總和
SQLUnhealthy	值 1 表示，為了回應某些要求，SQL外掛程式會傳回 5 xx 回應代碼，或傳遞無效的查詢DSL給 OpenSearch。其他請求應會繼續成功。值為 0 表示最近沒有任何失敗。如果您看到值持續為 1，請針對您用戶端向外掛程式提出的請求進行故障診斷。

指標	描述
	相關統計資訊：Maximum

k-NN 指標

Amazon OpenSearch 服務包括 k 最近鄰居（k-nN）插件的以下指標。

指標	描述
KNNCacheCapacityReached	是否已達到快取容量的每個節點指標。此指標僅與近似的 K-NN 搜尋相關。 相關統計資訊：Maximum
KNNCircuitBreakerTriggered	是否觸發斷路器的每個叢集指標。如果任何節點為 KNNCacheCapacityReached 傳回一個值，此值也將傳回 1。此指標僅與近似的 K-NN 搜尋相關。 相關統計資訊：Maximum
KNNEvictionCount	因記憶體限制或閒置時間而從快取移出的圖形數目的每個節點指標。因索引刪除而發生的明確移出不會計算在內。此指標僅與近似的 K-NN 搜尋相關。 相關統計資料：總和
KNNGraphIndexErrors	將文件的 knn_vector 欄位新增至圖形發生錯誤的請求數的每個節點指標。 相關統計資料：總和
KNNGraphIndexRequests	將文件的 knn_vector 欄位新增至圖形的請求數的每個節點指標。 相關統計資料：總和
KNNGraphMemoryUsage	目前快取大小 (記憶體中所有圖形的總大小) 的每個節點指標 (KB)。此指標僅與近似的 K-NN 搜尋相關。

指標	描述
	相關統計資訊：平均數
KNNGraphQueryErrors	產生錯誤之圖形查詢數目的每個節點指標。 相關統計資料：總和
KNNGraphQueryRequests	圖形查詢數目的每個節點指標。 相關統計資料：總和
KNNHitCount	快取命中次數的每個節點指標。當使用者查詢已載入記憶體的圖形時，就會發生快取命中。此指標僅與近似的 K-NN 搜尋相關。 相關統計資料：總和
KNNLoadExceptionCount	嘗試將圖形載入快取時發生例外狀況的次數的每個節點指標。此指標僅與近似的 K-NN 搜尋相關。 相關統計資料：總和
KNNLoadSuccessCount	外掛程式成功將圖形載入快取的次數的每個節點指標。此指標僅與近似的 K-NN 搜尋相關。 相關統計資料：總和
KNNMissCount	快取遺漏次數的每個節點指標。當使用者查詢尚未載入記憶體的圖形時，就會發生快取遺漏。此指標僅與近似的 K-NN 搜尋相關。 相關統計資料：總和
KNNQueryRequests	K-NN 外掛程式接收之查詢請求數目的每個節點指標。 相關統計資料：總和
KNNScriptCompilationErrors	指令碼編譯期間錯誤數目的每個節點指標。此統計數字僅與 K-NN 分數指令碼搜尋相關。 相關統計資料：總和

指標	描述
KNNScriptCompilations	K-NN 指令碼編譯次數的每個節點指標。此值通常應該為 1 或 0，但是如果包含已編譯指令碼的快取已填滿，K-NN 指令碼可能會被重新編譯。此統計數字僅與 K-NN 分數指令碼搜尋相關。 相關統計資料：總和
KNNScriptQueryErrors	指令碼查詢期間錯誤數目的每個節點指標。此統計數字僅與 K-NN 分數指令碼搜尋相關。 相關統計資料：總和
KNNScriptQueryRequests	指令碼查詢總數的每個節點指標。此統計數字僅與 K-NN 分數指令碼搜尋相關。 相關統計資料：總和
KNNTotalLoadTime	K-NN 將圖形載入到快取所需的時間 (以奈秒為單位)。此指標僅與近似的 K-NN 搜尋相關。 相關統計資料：總和

跨叢集搜尋指標

Amazon OpenSearch 服務提供以下跨叢集搜尋指標。

來源網域指標

指標	維度	描述
CrossClusterOutboundConnections	ConnectionId	連線節點數。如果回應包含一或多個略過的網域，請使用此指標以追蹤任何運作狀態不良的連線。如果這個數字掉到 0，則表示連線運作狀態不良。
CrossClusterOutboundRequests	ConnectionId	傳送至目的地網域的搜尋請求數。用於檢查跨叢集搜尋要求的負載是否壓倒您的網域，並將此指標中的任何尖峰與任何JVM/CPU尖峰產生關聯。

目的地網域指標

指標	維度	描述
CrossClusterInboundRequests	ConnectionId	從來源網域收到的傳入連線請求數。

在您意外失去連接的情況下添加 CloudWatch 警報。如需建立警示的步驟，請參閱根據靜態臨界值建立 CloudWatch警示。

跨叢集複寫指標

Amazon OpenSearch 服務為跨叢集複寫提供以下指標。

指標	描述
ReplicationRate	每秒平均複寫操作速率。此指標類似於 IndexingRate 指標。
LeaderCheckPoint	對於特定連線，為所有複寫索引中領導檢查點值的總和。您可以使用此指標來測量複寫延遲。
FollowerCheckPoint	對於特定連線，為所有複寫索引中追蹤檢查點值的總和。您可以使用此指標來測量複寫延遲。
ReplicationNumSyncingIndices	具有複寫狀態 SYNCING 的索引數目。
ReplicationNumBootstrappingIndices	具有複寫狀態 BOOTSTRAPPING 的索引數目。
ReplicationNumPausedIndices	具有複寫狀態 PAUSED 的索引數目。

指標	描述
ReplicationNumFailedIndices	具有複寫狀態 FAILED 的索引數目。
CrossClusterOutboundReplicationRequests	追隨者網域上的複寫傳輸要求數目。傳輸要求是內部的，每次呼叫複寫API作業時都會發生。當追隨者網域輪詢從領導者網域變更時，也會發生這些問題。
CrossClusterInboundReplicationRequests	領導網域上的複寫傳輸要求數目。傳輸要求是內部的，每次呼叫複寫API作業時都會發生。
AutoFollowNumSuccessStartReplication	針對特定連線，複寫規則成功建立的追蹤索引數目。
AutoFollowNumFailedStartReplication	當有相符模式時，複寫規則無法建立的追蹤索引數目。此問題可能是因為遠端叢集上的網路問題或安全性問題 (也就是說，關聯的角色沒有啟動複寫的許可) 所導致。
AutoFollowLeaderCallFailure	從追蹤索引到領導索引以選取新資料的查詢是否失敗。值 1 意味著在最近一分鐘有 1 個或多個失敗的呼叫。

Learning to Rank 指標

Amazon OpenSearch 服務提供了以下指標來學習排名。

指標	描述
LTRRequestTotalCount	排名請求的總數。
LTRRequestErrorCount	未成功請求的總數。
LTRStatus.red	追蹤需要執行外掛程式的其中一個索引是否為紅色。
LTRMemoryUsage	外掛程式使用的總記憶體。
LTRFeatureMemoryUsageInBytes	Learning to Rank 功能欄位使用的記憶體容量 (以位元組為單位)。
LTRFeatresetMemoryUsageInBytes	所有 Learning to Rank 功能集使用的記憶體容量 (以位元組為單位)。
LTRModelMemoryUsageInBytes	所有 Learning to Rank 模型使用的記憶體容量 (以位元組為單位)。

Piped Processing Language 指標

Amazon OpenSearch 服務為管道處理語言提供以下指標。

指標	描述
PPLFailedRequestCountByCusErr	因為用戶端問題_pplAPI而失敗的要求數目。例如，請求可能會傳回HTTP狀態碼 400，原因是IndexNotFoundException .
PPLFailedRequestCountBySysErr	由於伺服器問題或功能限制而失敗的要求數目。_ppl API例如，請求可能會傳回HTTP狀態碼 503，原因是VerificationException .

指標	描述
PPLRequestCount	要求的數目_pplAPI。

使用 Amazon OpenSearch 日誌監控 CloudWatch 日誌

Amazon OpenSearch 服務通過 Amazon OpenSearch 日誌公開以下 CloudWatch 日誌：

- 錯誤日誌
- 搜索請求慢日誌
- 碎片慢日誌
- 稽核日誌

搜索碎片緩慢日誌，索引分片緩慢日誌和錯誤日誌對於故障排除性能和穩定性問題非常有用。稽核日誌會追蹤使用者活動，以符合規範。所有日誌都預設為停用狀態。如果啟用，則適用標準 CloudWatch 定價。

> **Note**
> 錯誤記錄僅適用於 OpenSearch 和版本 5.1 及更新版本。慢速日誌適用於所有版本 OpenSearch 和彈性搜索版本。

對於它的日誌， OpenSearch 使用 Apache Log4j 2 及其內置的日誌級別（從最小到最嚴重）的 TRACE DEBUGINFO，WARN，ERROR，和FATAL。

如果啟用錯誤記錄檔， OpenSearch Service 會發佈WARNERROR、和的記錄FATAL行 CloudWatch。OpenSearch 服務也會從DEBUG層次發行數個例外狀況，包括下列項目：

- org.opensearch.index.mapper.MapperParsingException
- org.opensearch.index.query.QueryShardException
- org.opensearch.action.search.SearchPhaseExecutionException
- org.opensearch.common.util.concurrent.OpenSearchRejectedExecutionException
- java.lang.IllegalArgumentException

在許多情況下，錯誤日誌可以協助排除故障，包括：

- Painless 指令碼編譯問題
- 無效查詢
- 索引問題
- 快照故障
- 索引狀態管理遷移失敗

> **Note**
>
> OpenSearch 服務不會記錄發生的所有錯誤。

主題

- 啟用日誌發佈 (主控台)
- 啟用日誌發佈 (AWS CLI)
- 啟用記錄發佈 (AWS SDKs)
- 啟用日誌發佈 (CloudFormation)
- 設定搜尋要求慢速記錄閾值
- 設置碎片緩慢日誌閾值
- 測試慢速記錄
- 檢視日誌

啟用日誌發佈 (主控台)

OpenSearch 服務主控台是啟用日誌發佈到的最簡單方法 CloudWatch。

若要啟用記錄發佈至 CloudWatch (主控台)

1. 前往 https://aws.amazon.com，然後選擇 Sign In to the Console (登入主控台)。
2. 在分析下，選擇 Amazon OpenSearch 服務。
3. 選取您要更新的網域。
4. 在 Logs (日誌) 索引標籤上，選取日誌類型，然後選擇 Enable (啟用)。
5. 建立新的 CloudWatch 記錄群組或選擇現有的記錄群組。

> **Note**
>
> 您若打算啟用多個日誌，建議發佈每一個到它自己的日誌群組。這個分隔有助於更輕鬆掃描日誌。

6. 選擇包含適當權限的存取原則，或使用主控台提供的JSON原則建立原則：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "es.amazonaws.com"
      },
      "Action": [
        "logs:PutLogEvents",
        "logs:CreateLogStream"
      ],
      "Resource": "cw_log_group_arn:*"
    }
  ]
}
```

建議您新增 `aws:SourceAccount` 和 `aws:SourceArn` 條件索引鍵至政策，保護自己免受混淆代理人問題的困擾。來源帳戶是網域的擁有者，而來源ARN是網域ARN的擁有者。您的網域必須位於服務軟體 R20211203 或更新版本上，才能新增這些條件索引鍵。

例如，您可以將下列條件區塊新增至政策：

```
"Condition": {
    "StringEquals": {
        "aws:SourceAccount": "account-id"
    },
    "ArnLike": {
        "aws:SourceArn": "arn:aws:es:region:account-id:domain/domain-name"
    }
}
```

> **Important**
>
> CloudWatch 記錄檔支援每個區域 10 個資源策略。如果您打算啟用多個 OpenSearch Service 網域的記錄檔，您應該建立並重複使用包含多個記錄群組的更廣泛原則，以避免達到此限制。如需更新政策的相關步驟，請參閱the section called “啟用日誌發佈 (AWS CLI)”。

7. 選擇 啟用 。

   網域變更的狀態會從 Active (作用中) 變成 Processing (處理)。啟用日誌發佈之前，必須使狀態變回 Active (作用中)。這項變更通常需要 30 分鐘，但可能需要更長的時間，視您的網域組態而定。

如果您啟用了其中一個碎片緩慢日誌，請參閱the section called “設置碎片緩慢日誌閾值”。如果啟用稽核日誌，請參閱the section called “步驟 2：開啟 OpenSearch 儀表板中的稽核記錄”。如果您只啟用了錯誤日誌，則不需要執行任何其他設定步驟。

啟用日誌發佈 (AWS CLI)

啟用記錄檔發佈之前，您需要一個 CloudWatch 記錄群組。如果還沒有日誌群組，您可以使用下列命令建立一個：

```
aws logs create-log-group --log-group-name my-log-group
```

輸入下一個命令以尋找記錄群組 ARN，然後記下它：

```
aws logs describe-log-groups --log-group-name my-log-group
```

現在您可以授與寫入記錄群組的 OpenSearch 服務權限。您必須提供接ARN近命令結尾的記錄群組：

```
aws logs put-resource-policy \
  --policy-name my-policy \
  --policy-document '{ "Version": "2012-10-17", "Statement": [{ "Sid": "",
 "Effect": "Allow", "Principal": { "Service": "es.amazonaws.com"}, "Action":
[ "logs:PutLogEvents","logs:CreateLogStream"],"Resource": "cw_log_group_arn:*"}]}'
```

> **Important**
>
> CloudWatch 記錄檔支援每個區域 10 個資源策略。如果您打算為多個 OpenSearch Service 網域啟用碎片緩慢記錄檔，則應建立並重複使用包含多個記錄群組的更廣泛原則，以避免達到此限制。

如果您稍後需要檢閱此政策，請使用 `aws logs describe-resource-policies` 命令。若要更新此政策，請使用新的政策文件發出相同的 `aws logs put-resource-policy` 命令。

最後，您可以使用 `--log-publishing-options` 選項，以啟用發佈。選項的語法對於 `create-domain` 和 `update-domain-config` 命令都是相同的。

參數	有效值
`--log-publishing-options`	`SEARCH_SLOW_LOGS={CloudWatchLogsLogGroupArn= cw_log_group_arn ,Enabled=true|false}`
	`INDEX_SLOW_LOGS={CloudWatchLogsLogGroupArn= cw_log_group_arn ,Enabled=true|false}`
	`ES_APPLICATION_LOGS={CloudWatchLogsLogGroupArn= cw_log_group_arn ,Enabled=true|false}`
	`AUDIT_LOGS={CloudWatchLogsLogGroupArn= cw_log_group_arn ,Enabled=true|false}`

> **Note**
>
> 您若打算啟用多個日誌，建議發佈每一個到它自己的日誌群組。這個分隔有助於更輕鬆掃描日誌。

範例

下列範例會針對指定的網域啟用搜尋和索引分片緩慢記錄檔的發佈：

```
aws opensearch update-domain-config \
```

```
  --domain-name my-domain \
  --log-publishing-options
 "SEARCH_SLOW_LOGS={CloudWatchLogsLogGroupArn=arn:aws:logs:us-east-1:123456789012:log-
group:my-log-
group,Enabled=true},INDEX_SLOW_LOGS={CloudWatchLogsLogGroupArn=arn:aws:logs:us-
east-1:123456789012:log-group:my-other-log-group,Enabled=true}"
```

若要停用發佈至 CloudWatch，請使用執行相同的命令`Enabled=false`。

如果您啟用了其中一個碎片緩慢日誌，請參閱the section called “設置碎片緩慢日誌閾值”。如果啟用稽核日誌，請參閱the section called “步驟 2：開啟 OpenSearch 儀表板中的稽核記錄”。如果您只啟用了錯誤日誌，則不需要執行任何其他設定步驟。

啟用記錄發佈 (AWS SDKs)

啟用記錄檔發佈之前，您必須先建立 CloudWatch 記錄群組、取得記錄群組ARN，並授與 OpenSearch Service 寫入該群組的權限。相關操作記錄在 Amazon CloudWatch 日誌API參考中：

- `CreateLogGroup`
- `DescribeLogGroup`
- `PutResourcePolicy`

您可以使用存取這些作業AWS SDKs。

AWS SDKs（Android 和 iOS 除外SDKs）支持 Amazon OpenSearch 服務API參考中定義的所有操作，包括`CreateDomain`和的`--log-publishing-options`選項`UpdateDomainConfig`。

如果您啟用了其中一個碎片緩慢日誌，請參閱the section called “設置碎片緩慢日誌閾值”。如果您只啟用了錯誤日誌，則不需要執行任何其他設定步驟。

啟用日誌發佈 (CloudFormation)

在此範例中，我們使用 CloudFormation 建立名為的記錄群組`opensearch-logs`、指派適當的權限，然後建立網域，其中已啟用記錄檔發佈的應用程式記錄檔、搜尋碎片慢速記錄檔，以及編製慢速記錄檔的索引。

您必須先建立記錄群組，才能啟用記 CloudWatch 錄發佈：

```
Resources:
```

```
  OpenSearchLogGroup:
    Type: AWS::Logs::LogGroup
    Properties:
      LogGroupName: opensearch-logs
Outputs:
  Arn:
    Value:
      'Fn::GetAtt':
        - OpenSearchLogGroup
        - Arn
```

範本會輸出ARN記錄群組的。在本案例中，ARN 為 `arn:aws:logs:us-east-1:123456789012:log-group:opensearch-logs`。

使用ARN，建立一個資源策略，該策略授與寫入日誌群組的 OpenSearch Service 權限：

```
Resources:
 OpenSearchLogPolicy:
   Type: AWS::Logs::ResourcePolicy
   Properties:
     PolicyName: my-policy
     PolicyDocument: "{ \"Version\": \"2012-10-17\", \"Statement\": [{ \"Sid\": \"\",
 \"Effect\": \"Allow\", \"Principal\": { \"Service\": \"es.amazonaws.com\"}, \"Action
\":[ \"logs:PutLogEvents\",\"logs:CreateLogStream\"],\"Resource\": \"arn:aws:logs:us-
east-1:123456789012:log-group:opensearch-logs:*\"}]}"
```

最後，創建以下 CloudFormation 堆棧，該堆棧生成帶有日誌發布的 OpenSearch 服務域。存取原則允許使用者 AWS 帳戶 向網域發出所有HTTP要求。

```
Resources:
  OpenSearchServiceDomain:
    Type: "AWS::OpenSearchService::Domain"
    Properties:
      DomainName: my-domain
      EngineVersion: "OpenSearch_1.0"
      ClusterConfig:
        InstanceCount: 2
        InstanceType: "r6g.xlarge.search"
        DedicatedMasterEnabled: true
        DedicatedMasterCount: 3
        DedicatedMasterType: "r6g.xlarge.search"
      EBSOptions:
```

```
        EBSEnabled: true
        VolumeSize: 10
        VolumeType: "gp2"
      AccessPolicies:
        Version: "2012-10-17"
        Statement:
            Effect: "Allow"
            Principal:
                AWS: "arn:aws:iam::123456789012:user/es-user"
            Action: "es:*"
            Resource: "arn:aws:es:us-east-1:123456789012:domain/my-domain/*"
      LogPublishingOptions:
        ES_APPLICATION_LOGS:
          CloudWatchLogsLogGroupArn: "arn:aws:logs:us-east-1:123456789012:log-
group:opensearch-logs"
          Enabled: true
        SEARCH_SLOW_LOGS:
          CloudWatchLogsLogGroupArn: "arn:aws:logs:us-east-1:123456789012:log-
group:opensearch-logs"
          Enabled: true
        INDEX_SLOW_LOGS:
          CloudWatchLogsLogGroupArn: "arn:aws:logs:us-east-1:123456789012:log-
group:opensearch-logs"
          Enabled: true
```

如需詳細的語法資訊，請參閱 AWS CloudFormation 使用者指南中的日誌發佈選項。

設定搜尋要求慢速記錄閾值

搜尋要求緩慢記錄檔可用於在 2.13 版及更新版本上執行的 OpenSearch 服務網域上搜尋。搜尋要求慢速記錄臨界值設定為總要求花費時間。這與碎片請求慢日誌不同，這是為單個碎片配置花費時間。

您可以使用叢集設定來指定搜尋要求慢速記錄。這與碎片緩慢日誌不同，您可以使用索引設置啟用。例如，您可以透過指定下列設定 OpenSearch RESTAPI：

```
PUT domain-endpoint/_cluster/settings
{
  "transient": {
    "cluster.search.request.slowlog.threshold.warn": "5s",
    "cluster.search.request.slowlog.threshold.info": "2s"
  }
}
```

設置碎片緩慢日誌閾值

OpenSearch 默認情況下禁用碎片緩慢日誌。啟用碎片緩慢記錄檔發佈到之後 CloudWatch，您仍然必須為每個 OpenSearch 索引指定記錄閾值。這些閾值精確定義該記錄哪些內容、日誌層級為何等等。

例如，您可以透過以下方式指定這些設定 OpenSearch RESTAPI：

```
PUT domain-endpoint/index/_settings
{
  "index.search.slowlog.threshold.query.warn": "5s",
  "index.search.slowlog.threshold.query.info": "2s"
}
```

測試慢速記錄

若要測試搜尋要求和碎片緩慢記錄檔是否成功發佈，請考慮從非常低的值開始驗證記錄檔是否出現在中 CloudWatch，然後將閾值提高到更有用的層級。

如果日誌未出現，請檢查下列各項：

- CloudWatch 記錄群組是否存在？ 檢查主 CloudWatch 控台。
- OpenSearch 服務是否具有寫入記錄群組的權限？ 檢查服 OpenSearch 務主控台。
- OpenSearch 服務網域是否設定為發佈至記錄群組？ 檢查 OpenSearch 服務主控台、使用 AWS CLI `describe-domain-config`選項，或`DescribeDomainConfig`使用其中一個呼叫SDKs.
- OpenSearch 記錄閾值是否足夠低，以至於您的請求超過它們？

  若要檢閱網域的搜尋要求緩慢記錄閾值，請使用下列命令：

  ```
  GET domain-endpoint/_cluster/settings?flat_settings
  ```

  若要檢閱索引的碎片緩慢記錄閾值，請使用下列命令：

  ```
  GET domain-endpoint/index/_settings?pretty
  ```

如果您想要停用索引的慢速日誌，請傳回變更為其預設值 `-1` 的任何閾值。

停用發佈到 CloudWatch 使用 OpenSearch Service 主控台或 AWS CLI 不會停 OpenSearch 止產生記錄檔；它只會停止發佈這些記錄檔。如果您不再需要碎片緩慢日誌，請務必檢查索引設置；如果您不再需要搜索請求緩慢日誌，請務必檢查您的域設置。

檢視日誌

查看應用程序和緩慢的日誌 CloudWatch 就像查看任何其他日 CloudWatch 誌一樣。如需詳細資訊，請參閱 Amazon CloudWatch 日誌使用者指南中的檢視日誌資料。

以下是檢視日誌的一些考量事項：

- OpenSearch 服務只會將每行的前 255,000 個字元發佈到 CloudWatch。任何剩餘內容會被截斷。對於稽核日誌，每個訊息為 10,000 個字元。
- 在中 CloudWatch，記錄資料流名稱的尾碼為`-index-slow-logs`、、和 `-search-slow-logs`-`application-logs`，`-audit-logs`以協助識別其內容。

監控 Amazon OpenSearch 服務中的審核日誌

如果您的 Amazon OpenSearch 服務網域使用精細的存取控制，您可以為資料啟用稽核日誌。稽核記錄具有高度可自訂性，可讓您追蹤 OpenSearch叢集上的使用者活動，包括驗證成功與失敗、要求 OpenSearch、索引變更以及傳入的搜尋查詢。預設設定會追蹤一組常用的使用者動作，但我們建議您根據您的確切需求量身打造設定。

就像OpenSearch 應用程式記錄檔和慢速記錄檔一樣， OpenSearch Service 會將稽核記錄發佈至 CloudWatch 記錄 如果啟用，則適用標準 CloudWatch 定價。

> **Note**
>
> 若要啟用稽核記錄，您的使用者角`security_manager`色必須對應至可讓您存取 OpenSearch `plugins/_security` REST API 的角色。如需進一步了解，請參閱the section called “修改主要使用者”。

主題

- 限制
- 啟用稽核日誌
- 啟用稽核記錄 AWS CLI
- 使用組態 API 啟用稽核日誌記錄
- 稽核日誌層和類別
- 稽核日誌設定

- 稽核日誌範例
- 使用 REST API 設定稽核日誌

限制

稽核日誌具有下列限制：

- 稽核日誌不包含被目的地網域存取政策拒絕的跨叢集搜尋請求。
- 每個稽核日誌訊息的大小上限為 10,000 個字元。如果稽核日誌訊息超過此限制，就會被截斷。

啟用稽核日誌

啟用稽核日誌分為兩個步驟。首先，您將網域設定為將稽核記錄發佈到 CloudWatch 記錄檔。然後，您可以在 OpenSearch 儀表板中啟用稽核記錄，並對其進行設定以符合您的需求。

> **Important**
>
> 如果您在執行這些步驟時遇到錯誤，請參閱the section called “無法啟用稽核日誌”，瞭解故障診斷資訊。

步驟 1：啟用稽核日誌並設定存取政策

以下步驟說明如何使用主控台啟用稽核日誌。您也可以使用或OpenSearch 服務 API 來啟用它們。AWS CLI

啟用 OpenSearch 服務網域 (主控台) 的稽核記錄

1. 選擇要打開其組態的網域，然後前往 Logs (日誌) 索引標籤。
2. 選取 Audit logs (稽核日誌)，然後選取 Enable (啟用)。
3. 建立 CloudWatch 記錄群組，或選擇現有的記錄群組。
4. 選擇包含適當許可權的存取政策，或使用主控台提供的 JSON 建立政策：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
```

```
      "Principal": {
        "Service": "es.amazonaws.com"
      },
      "Action": [
        "logs:PutLogEvents",
        "logs:CreateLogStream"
      ],
      "Resource": "cw_log_group_arn"
    }
  ]
}
```

建議您新增 `aws:SourceAccount` 和 `aws:SourceArn` 條件索引鍵至政策，保護自己免受混淆代理人問題的困擾。來源帳戶是網域的擁有者，且來源 ARN 是網域 ARN。您的網域必須位於服務軟體 R20211203 或更新版本上，才能新增這些條件索引鍵。

例如，您可以將下列條件區塊新增至政策：

```
"Condition": {
    "StringEquals": {
        "aws:SourceAccount": "account-id"
    },
    "ArnLike": {
        "aws:SourceArn": "arn:aws:es:region:account-id:domain/domain-name"
    }
}
```

5. 選擇 啟用 。

步驟 2：開啟 OpenSearch 儀表板中的稽核記錄

在 OpenSearch Service Console 中啟用稽核記錄之後，您還必須在 OpenSearch 儀表板中啟用它們，並對其進行設定以符合您的需求。

1. 打開 OpenSearch 儀表板，然後從左側菜單中選擇安全性。
2. 選擇 Audit logs (稽核日誌)。
3. 選擇 Enable audit logging (啟用稽核日誌)。

Dashboards UI 在 General settings (一般設定) 和 Compliance settings (合規設定) 下提供稽核日誌設定的完整控制。如需所有組態選項的說明，請參閱稽核日誌設定。

啟用稽核記錄 AWS CLI

下列 AWS CLI 命令會在現有網域上啟用稽核記錄：

```
aws opensearch update-domain-config --domain-name my-domain --log-publishing-options
 "AUDIT_LOGS={CloudWatchLogsLogGroupArn=arn:aws:logs:us-east-1:123456789012:log-
group:my-log-group,Enabled=true}"
```

您也可以在建立網域時啟用稽核日誌。如需詳細資訊，請參閱 AWS CLI 命令參考。

使用組態 API 啟用稽核日誌記錄

下面對組態 API 的請求會啟用現有網域上的稽核日誌：

```
POST https://es.us-east-1.amazonaws.com/2021-01-01/opensearch/domain/my-domain/config
{
  "LogPublishingOptions": {
    "AUDIT_LOGS": {
      "CloudWatchLogsLogGroupArn":"arn:aws:logs:us-east-1:123456789012:log-
group1:sample-domain",
      "Enabled":true
    }
  }
}
```

如需詳細資訊，請參閱 Amazon OpenSearch 服務 API 參考資料。

稽核日誌層和類別

叢集通訊發生在兩個不同的層：REST 層和傳輸層。

- 其餘層涵蓋了與 HTTP 客戶端，如捲曲，日誌信息， OpenSearch 儀表板，Java 高級 REST 客戶端，Python 請求庫，到達集群的所有 HTTP 請求的通信。
- 傳輸層涵蓋節點之間的通訊。例如，搜尋請求到達叢集之後 (透過 REST 層)，服務該請求的協調節點會將查詢傳送至其他節點、接收其回應、收集必要的文件，並將它們整理成最終回應。諸如碎片配置和重新平衡等操作也會發生在傳輸層。

您可以啟用或停用整個層的稽核日誌，以及某層的個別稽核類別。下表包含稽核類別及其可用層的摘要。

類別	描述	適用於 REST	適用於傳輸
FAILED_LOGIN	請求包含無效憑證，且身分驗證失敗。	是	是
MISSING_PRIVILEGES	使用者沒有提出請求的權限。	是	是
GRANTED_PRIVILEGES	使用者擁有提出請求的權限。	是	是
OPENSEARCH_SECURITY_INDEX_ATTEMPT	請求嘗試修改 `.opendistro_security` 索引。	否	是
AUTHENTICATED	請求包含有效憑證，且身分驗證成功。	是	是
INDEX_EVENT	請求對索引執行系統管理操作，例如建立索引、設定別名或執行強制合併。此類別包含的`indices:admin/` 動作完整清單可在OpenSearch 文件中找到。	否	是

除了這些標準類別之外，精細存取控制還提供數個額外的類別，專為符合資料合規要求而設計。

類別	描述
COMPLIANCE_DOC_READ	請求對索引中的文件執行讀取事件。
COMPLIANCE_DOC_WRITE	請求對索引中的文件執行寫入事件。

類別	描述
COMPLIANCE_INTERNAL_CONFIG_READ	請求對 `.opendistro_security` 索引執行讀取事件。
COMPLIANCE_INTERNAL_CONFIG_WRITE	請求對 `.opendistro_security` 索引執行寫入事件。

您可擁有類別和訊息屬性的任意組合。例如，如果您傳送 REST 請求以索引文件，您可能會在稽核日誌中看到下列幾行：

- REST 層上的 AUTHENTICATED (身分驗證)
- 傳輸層上的 GRANTED_PRIVILEGE (授權)
- COMPLIANCE_DOC_WRITE (文件寫入到索引)

稽核日誌設定

稽核日誌有許多組態選項。

一般設定

使用一般設定可啟用或停用個別類別或整個層。我們強烈建議您將 GRANTED_PRIVILEGES 和 AUTHENTICATED 保留為排除類別。否則，會針對每個有效請求將這些類別記錄至叢集。

名稱	後端設定	描述
REST 層	enable_rest	啟用或停用 REST 層上發生的事件。
REST 已停用類別	disabled_rest_categories	指定要在 REST 層上忽略的稽核類別。修改這些類別會大幅增加稽核日誌的大小。
傳輸層	enable_transport	啟用或停用傳輸層上發生的事件。

名稱	後端設定	描述
傳輸已停用類別	disabled_transport_categories	指定必須在傳輸層上忽略的稽核類別。修改這些類別會大幅增加稽核日誌的大小。

使用屬性設定可自訂每個日誌行中的詳細資訊量。

名稱	後端設定	描述
批量請求	resolve_bulk_requests	啟用此設定會為批量請求中的每個文件產生日誌，這會大幅增加稽核日誌的大小。
請求內文	log_request_body	包含請求的要求主體。
解析索引	resolve_indices	將別名解析為索引。

使用忽略設定來排除一組使用者或 API 路徑：

名稱	後端設定	描述
已忽略的使用者	ignore_users	指定想要排除的使用者。
已忽略的請求	ignore_requests	指定想要排除的請求模式。

合規設定

使用合規設定可針對索引、文件或欄位級存取進行調整。

名稱	後端設定	描述
合規日誌	enable_compliance	啟用或停用合規日誌。

您可以針對讀取和寫入事件日誌指定下列設定。

名稱	後端設定	描述
內部組態日誌	internal_config	啟用或停用 `.opendistro_security` 索引上的事件日誌。

您可以針對讀取事件指定下列設定。

名稱	後端設定	描述
讀取中繼資料	read_metadata_only	僅包含讀取事件的中繼資料。不包含任何文件欄位。
已忽略的使用者	read_ignore_users	請勿針對讀取事件包含特定使用者。
監視的欄位	read_watched_fields	指定針對讀取事件而監視的索引和欄位。新增監視的欄位會依據每個文件存取產生一個日誌，這會大幅增加稽核日誌的大小。監視的欄位支援索引模式和欄位模式： `{ "index-name-pattern": [ "field-name-pattern" ], "logs*": [ "message" ], "twitter": [ "id", "user*" ] }`

您可以針對寫入事件指定下列設定。

名稱	後端設定	描述
寫入中繼資料	write_metadata_only	僅包含寫入事件的中繼資料。不包含任何文件欄位。
日誌差異	write_log_diffs	如果 write_metadata_only 為 false，則只包括寫入事件之間的差異。
已忽略的使用者	write_ignore_users	不包括寫入事件的特定使用者。
監視指數	write_watched_indices	指定針對寫入事件而監視的索引或索引模式。新增監視的欄位會依據每個文件存取產生一個日誌，這會大幅增加稽核日誌的大小。

稽核日誌範例

本節包含索引的所有讀取和寫入事件的範例組態、搜尋請求以及產生的稽核日誌。

步驟 1：設定稽核日誌

啟用將稽核記錄發佈至記 CloudWatch 錄群組後，請瀏覽至 [OpenSearch 儀表板稽核記錄] 頁面，然後選擇 [啟用稽核記錄]。

1. 在 General Settings (一般設定) 中，選擇 Configure (設定)，並確保 REST layer (REST 層) 已啟用。
2. 在 Compliance Settings (合規設定) 中，選擇 Configure (設定)。
3. 在 Write (寫入) 下面的 Watched Fields (監視欄位) 中，將所有寫入事件的 `accounts` 新增至此索引。
4. 在 Read (讀取) 下面的 Watched Fields (監視欄位) 中，新增 `accounts` 索引的 `ssn` 和 `id-` 欄位：

```
{
  "accounts-": [
    "ssn",
    "id-"
  ]
```

```
}
```

步驟 2：執行讀取和寫入事件

1. 導覽至 [OpenSearch 儀表板]、選擇 [開發工具]，並索引範例文件：

```
PUT accounts/_doc/0
{
  "ssn": "123",
  "id-": "456"
}
```

2. 若要測試讀取事件，請傳送下列請求：

```
GET accounts/_search
{
  "query": {
    "match_all": {}
  }
}
```

步驟 3：觀察日誌

1. 請在以下位置開啟 CloudWatch 主控台。 https://console.aws.amazon.com/cloudwatch/
2. 在導覽窗格中，選擇 Log groups (日誌群組)。
3. 選擇您在啟用稽核日誌時指定的日誌群組。在記錄群組中， OpenSearch Service 會為網域中的每個節點建立記錄資料流。
4. 在 Log streams (日誌串流) 中，選擇 Search all (搜尋全部)。
5. 如需讀取和寫入事件，請參閱對應的日誌。在日誌出現之前，預計會有 5 秒延遲。

   寫入稽核日誌範例

```
{
  "audit_compliance_operation": "CREATE",
  "audit_cluster_name": "824471164578:audit-test",
  "audit_node_name": "be217225a0b77c2bd76147d3ed3ff83c",
  "audit_category": "COMPLIANCE_DOC_WRITE",
  "audit_request_origin": "REST",
```

```
  "audit_compliance_doc_version": 1,
  "audit_node_id": "3xNJhm4XS_yTzEgDWcGRjA",
  "@timestamp": "2020-08-23T05:28:02.285+00:00",
  "audit_format_version": 4,
  "audit_request_remote_address": "3.236.145.227",
  "audit_trace_doc_id": "lxnJGXQBqZSlDB91r_uZ",
  "audit_request_effective_user": "admin",
  "audit_trace_shard_id": 8,
  "audit_trace_indices": [
    "accounts"
  ],
  "audit_trace_resolved_indices": [
    "accounts"
  ]
}
```

讀取稽核日誌範例

```
{
  "audit_cluster_name": "824471164578:audit-docs",
  "audit_node_name": "806f6050cb45437e2401b07534a1452f",
  "audit_category": "COMPLIANCE_DOC_READ",
  "audit_request_origin": "REST",
  "audit_node_id": "saSevm9ASte0-pjAtYi2UA",
  "@timestamp": "2020-08-31T17:57:05.015+00:00",
  "audit_format_version": 4,
  "audit_request_remote_address": "54.240.197.228",
  "audit_trace_doc_id": "config:7.7.0",
  "audit_request_effective_user": "admin",
  "audit_trace_shard_id": 0,
  "audit_trace_indices": [
    "accounts"
  ],
  "audit_trace_resolved_indices": [
    "accounts"
  ]
}
```

若要包含要求主體，請返回 OpenSearch 儀表板中的符合性設定，並停用寫入中繼資料。若要排除特定使用者的事件，請將使用者新增至 Ignored Users (已忽略的使用者)。

如需每個稽核日誌欄位的說明，請參閱稽核日誌欄位參考。如需搜尋和分析稽核日誌資料的相關資訊，請參閱 Amazon Logs 使用者指南中的利用 CloudWatch 日誌洞察分析 CloudWatch 日誌資料。

使用 REST API 設定稽核日誌

我們建議您使用 OpenSearch 儀表板來設定稽核記錄，但您也可以使用精細的存取控制 REST API。本節包含請求範例。有關 REST API 的完整文檔可在OpenSearch文檔中找到。

```
PUT _opendistro/_security/api/audit/config
{
  "enabled": true,
  "audit": {
    "enable_rest": true,
    "disabled_rest_categories": [
      "GRANTED_PRIVILEGES",
      "AUTHENTICATED"
    ],
    "enable_transport": true,
    "disabled_transport_categories": [
      "GRANTED_PRIVILEGES",
      "AUTHENTICATED"
    ],
    "resolve_bulk_requests": true,
    "log_request_body": true,
    "resolve_indices": true,
    "exclude_sensitive_headers": true,
    "ignore_users": [
      "kibanaserver"
    ],
    "ignore_requests": [
      "SearchRequest",
      "indices:data/read/*",
      "/_cluster/health"
    ]
  },
  "compliance": {
    "enabled": true,
    "internal_config": true,
    "external_config": false,
    "read_metadata_only": true,
    "read_watched_fields": {
      "read-index-1": [
        "field-1",
```

```
        "field-2"
      ],
      "read-index-2": [
        "field-3"
      ]
    },
    "read_ignore_users": [
      "read-ignore-1"
    ],
    "write_metadata_only": true,
    "write_log_diffs": false,
    "write_watched_indices": [
      "write-index-1",
      "write-index-2",
      "log-*",
      "*"
    ],
    "write_ignore_users": [
      "write-ignore-1"
    ]
  }
}
```

使用 Amazon 監控 OpenSearch 服務事件 EventBridge

Amazon OpenSearch 服務與 Amazon 集成， EventBridge 以通知您某些事件會影響您的域。來自 AWS 服務的事件會以近乎即時 EventBridge 的方式傳送到。同樣的事件也被發送到 Amazon CloudWatch 活動，Amazon EventBridge 的前身。您可編寫簡單的規則，來指示您在意的事件，以及當事件符合規則時所要自動執行的動作。可以自動觸發的動作如下：

- 調用一 AWS Lambda 個函數
- 叫用 Amazon EC2 執行命令
- 將事件轉傳至 Amazon Kinesis Data Streams
- 激活 AWS Step Functions 狀態機
- 通知 Amazon SNS 主題或 Amazon SQS 佇列

如需詳細資訊，請參閱 Amazon EventBridge 使用者指南 EventBridge中的開始使用 Amazon。

主題

- 服務軟體更新事件
- 自動調整事件
- 叢集運作狀態事件
- VPC 端點事件
- 節點淘汰事件
- 降級的節點淘汰事件
- 網域錯誤事件
- 教學課程：監聽 Amazon OpenSearch 服務 EventBridge 事件
- 教學課程：可用軟體更新的 Amazon SNS 提醒

服務軟體更新事件

OpenSearch 服務會在發生下列服務軟體更新事件之一 EventBridge 時傳送事件至。

可用的服務軟體更新

OpenSearch 服務會在服務軟體更新可用時傳送此事件。

範例

以下為此類事件的範例：

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "Amazon OpenSearch Service Software Update Notification",
  "source": "aws.es",
  "account": "123456789012",
  "time": "2016-11-01T13:12:22Z",
  "region": "us-east-1",
  "resources": ["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail": {
    "event": "Service Software Update",
    "status": "Available",
    "severity": "Informational",
    "description": "Service software update R20220928 available. Service Software
 Deployment Mechanism:
                    Blue/Green. For more information on deployment configuration,
 please
```

```
                    see: https://docs.aws.amazon.com/opensearch-service/latest/
developerguide/managedomains-configuration-changes.html"
  }
}
```

預約服務軟體更新

OpenSearch 服務會在已排程服務軟體更新時傳送此事件。對於選擇性更新，您會在排程日期收到通知，而且您可以選擇隨時重新排程。針對必要更新，您會在排定日期前三天收到通知，而且您可以選擇在必要時段內重新排程。

範例

以下為此類事件的範例：

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "Amazon OpenSearch Service Software Update Notification",
  "source": "aws.es",
  "account": "123456789012",
  "time": "2016-11-01T13:12:22Z",
  "region": "us-east-1",
  "resources": ["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail": {
    "event": "Service Software Update",
    "status": "Scheduled",
    "severity": "High",
    "description": "A new service software update [R20200330-p1] has been scheduled at
 [21st May 2023 12:40 GMT].
                    Please see documentation for more information on scheduling
 software updates:
                    https://docs.aws.amazon.com/opensearch-service/latest/
developerguide/service-software.html."
  }
}
```

服務軟體更新已重新安排

OpenSearch 服務會在重新排程選用的服務軟體更新時傳送此事件。如需詳細資訊，請參閱 the section called “可選更新與必要更新”。

範例

以下為此類事件的範例：

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "Amazon OpenSearch Service Software Update Notification",
  "source": "aws.es",
  "account": "123456789012",
  "time": "2016-11-01T13:12:22Z",
  "region": "us-east-1",
  "resources": ["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail": {
    "event": "Service Software Update",
    "status": "Rescheduled",
    "severity": "High",
    "description": "The service software update [R20200330-p1], which was originally
 scheduled for
                    [21st May 2023 12:40 GMT], has been rescheduled to [23rd May 2023
 12:40 GMT].
                    Please see documentation for more information on scheduling
 software updates:
                    https://docs.aws.amazon.com/opensearch-service/latest/
developerguide/service-software.html."
  }
}
```

服務軟體更新已開始

OpenSearch 服務會在服務軟體更新已啟動時傳送此事件。

範例

以下為此類事件的範例：

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "Amazon OpenSearch Service Software Update Notification",
  "source": "aws.es",
  "account": "123456789012",
  "time": "2016-11-01T13:12:22Z",
```

```
  "region": "us-east-1",
  "resources": ["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail": {
    "event": "Service Software Update",
    "status": "Started",
    "severity": "Informational",
    "description": "Service software update [R20200330-p1] started.
  }
}
```

服務軟體更新已完成

OpenSearch 服務會在服務軟體更新完成時傳送此事件。

範例

以下為此類事件的範例：

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "Amazon OpenSearch Service Software Update Notification",
  "source": "aws.es",
  "account": "123456789012",
  "time": "2016-11-01T13:12:22Z",
  "region": "us-east-1",
  "resources": ["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail": {
    "event": "Service Software Update",
    "status": "Completed",
    "severity": "Informational",
    "description": "Service software update [R20200330-p1] completed."
  }
}
```

服務軟體更新已取消

OpenSearch 服務會在取消服務軟體更新時傳送此事件。

範例

以下為此類事件的範例：

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "Amazon OpenSearch Service Software Update Notification",
  "source": "aws.es",
  "account": "123456789012",
  "time": "2016-11-01T13:12:22Z",
  "region": "us-east-1",
  "resources": ["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail": {
    "event": "Service Software Update",
    "status": "Cancelled",
    "severity": "Informational",
    "description": "The scheduled service software update [R20200330-p1] has been
 cancelled as a
                    newer update is available. Please schedule the latest update."
  }
}
```

已取消預約服務軟體更新

OpenSearch 服務會在取消先前針對網域排程的服務軟體更新時傳送此事件。

範例

以下為此類事件的範例：

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "Amazon OpenSearch Service Software Update Notification",
  "source": "aws.es",
  "account": "123456789012",
  "time": "2016-11-01T13:12:22Z",
  "region": "us-east-1",
  "resources": ["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail": {
    "event": "Service Software Update",
    "status": "Cancelled",
    "severity": "Informational",
    "description": "The scheduled service software update [R20200330-p1] has been
 cancelled."
  }
```

```
}
```

服務軟體更新未執行

OpenSearch 服務會在無法起始服務軟體更新時傳送此事件。

範例

以下為此類事件的範例：

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "Amazon OpenSearch Service Software Update Notification",
  "source": "aws.es",
  "account": "123456789012",
  "time": "2016-11-01T13:12:22Z",
  "region": "us-east-1",
  "resources": ["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail": {
    "event": "Service Software Update",
    "status": "Unexecuted",
    "severity": "Informational",
    "description": "The scheduled service software update [R20200330-p1] cannot be
 started. Reason: [reason]"
  }
}
```

服務軟體更新已失敗

OpenSearch 服務會在服務軟體更新失敗時傳送此事件。

範例

以下為此類事件的範例：

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "Amazon OpenSearch Service Software Update Notification",
  "source": "aws.es",
  "account": "123456789012",
```

```
  "time": "2016-11-01T13:12:22Z",
  "region": "us-east-1",
  "resources": ["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail": {
    "event": "Service Software Update",
    "status": "Failed",
    "severity": "High",
    "description": "Installation of service software update [R20200330-p1] failed.
 [reason].
  }
}
```

需要服務軟體更新

OpenSearch 服務會在需要服務軟體更新時傳送此事件。如需詳細資訊，請參閱 the section called “可選更新與必要更新”。

範例

以下為此類事件的範例：

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "Amazon OpenSearch Service Software Update Notification",
  "source": "aws.es",
  "account": "123456789012",
  "time": "2016-11-01T13:12:22Z",
  "region": "us-east-1",
  "resources": ["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail": {
    "event": "Service Software Update",
    "status": "Required",
    "severity": "High",
    "description": "Service software update [R20200330-p1] available. Update
                    will be automatically installed after [21st May 2023] if no
                    action is taken. Service Software Deployment Mechanism: Blue/Green.
                    For more information on deployment configuration, please see:
                    https://docs.aws.amazon.com/opensearch-service/latest/
developerguide/managedomains-configuration-changes.html"
  }
}
```

自動調整事件

OpenSearch 當發生下列自動調整事件之一 EventBridge 時，Service 會傳送事件至。

自動調整待定

OpenSearch 「自動調整」已識別改善叢集效能和可用性的調整建議時，Service 會傳送此事件。您只能在已停用「自動調整」的網域中看到此事件。

範例

以下為此類事件的範例：

```
{
  "version": "0",
  "id": "3acb26c8-397c-4c89-a80a-ce672a864c55",
  "detail-type": "Amazon OpenSearch Service Auto-Tune Notification",
  "source": "aws.es",
  "account": "123456789012",
  "time": "2020-10-30T22:06:31Z",
  "region": "us-east-1",
  "resources": ["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail": {
    "event": "Auto-Tune Event",
    "severity": "Informational",
    "status": "Pending",
    "description": "Auto-Tune recommends the following new settings for your
 domain: { JVM Heap size : 60%}. Enable Auto-Tune to improve cluster stability and
 performance.",
    "scheduleTime": "{iso8601-timestamp}"
  }
}
```

自動調整已開始

OpenSearch 服務會在「自動調整」開始將新設定套用至您的網域時傳送此事件。

範例

以下為此類事件的範例：

```
{
```

```
  "version": "0",
  "id": "3acb26c8-397c-4c89-a80a-ce672a864c55",
  "detail-type": "Amazon OpenSearch Service Auto-Tune Notification",
  "source": "aws.es",
  "account": "123456789012",
  "time": "2020-10-30T22:06:31Z",
  "region": "us-east-1",
  "resources": ["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail": {
    "event": "Auto-Tune Event",
    "severity": "Informational",
    "status": "Started",
    "scheduleTime": "{iso8601-timestamp}",
    "startTime": "{iso8601-timestamp}",
    "description" : "Auto-Tune is applying the following settings to your domain: { JVM
 Heap size : 60%}."
  }
}
```

自動調整需要排程的藍/綠部署

OpenSearch 當 Auto-Tune 識別出需要排程藍/綠部署的調整建議時，服務會傳送此事件。

範例

以下為此類事件的範例：

```
{
  "version": "0",
  "id": "3acb26c8-397c-4c89-a80a-ce672a864c55",
  "detail-type": "Amazon OpenSearch Service Auto-Tune Notification",
  "source": "aws.es",
  "account": "123456789012",
  "time": "2020-10-30T22:06:31Z",
  "region": "us-east-1",
  "resources": ["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail": {
    "event": "Auto-Tune Event",
    "severity": "Low",
    "status": "Pending",
    "startTime": "{iso8601-timestamp}",
    "description": "Auto-Tune has identified the following settings for your domain
 that require a blue/green deployment: { JVM Heap size : 60%}.
```

```
                      You can schedule the deployment for your preferred time."
  }
}
```

自動調整已取消

OpenSearch 因為沒有擱置的調整建議而取消「自動調整」排程時，Service 會傳送此事件。

範例

以下為此類事件的範例：

```
{
  "version": "0",
  "id": "3acb26c8-397c-4c89-a80a-ce672a864c55",
  "detail-type": "Amazon OpenSearch Service Auto-Tune Notification",
  "source": "aws.es",
  "account": "123456789012",
  "time": "2020-10-30T22:06:31Z",
  "region": "us-east-1",
  "resources": ["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail": {
    "event": "Auto-Tune Event",
    "severity": "Low",
    "status": "Cancelled",
    "scheduleTime": "{iso8601-timestamp}",
    "description": "Auto-Tune has cancelled the upcoming blue/green deployment."
  }
}
```

自動調整已完成

OpenSearch 「自動調整」已完成藍/綠部署，且叢集正在使用新 JVM 設定的情況下運作時，「服務」會傳送此事件。

範例

以下為此類事件的範例：

```
{
  "version": "0",
```

```
  "id": "3acb26c8-397c-4c89-a80a-ce672a864c55",
  "detail-type": "Amazon OpenSearch Service Auto-Tune Notification",
  "source": "aws.es",
  "account": "123456789012",
  "time": "2020-10-30T22:06:31Z",
  "region": "us-east-1",
  "resources": ["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail": {
    "event": "Auto-Tune Event",
    "severity": "Informational",
    "status": "Completed",
    "completionTime": "{iso8601-timestamp}",
    "description": "Auto-Tune has completed the blue/green deployment and successfully
 applied the following settings: { JVM Heap size : 60%}."
  }
}
```

自動調整已停用且變更已還原

OpenSearch 當「自動調整」已停用且套用的變更已復原時，「服務」會傳送此事件。

範例

以下為此類事件的範例：

```
{
  "version": "0",
  "id": "3acb26c8-397c-4c89-a80a-ce672a864c55",
  "detail-type": "Amazon OpenSearch Service Auto-Tune Notification",
  "source": "aws.es",
  "account": "123456789012",
  "time": "2020-10-30T22:06:31Z",
  "region": "us-east-1",
  "resources": [ "arn:aws:es:us-east-1:123456789012:domain/test-domain" ],
  "detail": {
    "event": "Auto-Tune Event",
    "severity": "Informational",
    "status": "Completed",
    "description": "Auto-Tune is now disabled. All settings have been reverted. Auto-
Tune will continue to evaluate
                     cluster performance and provide recommendations.",
    "completionTime": "{iso8601-timestamp}"
  }
```

```
}
```

自動調整已停用且變更已保留

OpenSearch 當「自動調整」已停用且套用的變更已保留時，「服務」會傳送此事件。

範例

以下為此類事件的範例：

```
{
  "version": "0",
  "id": "3acb26c8-397c-4c89-a80a-ce672a864c55",
  "detail-type": "Amazon OpenSearch Service Auto-Tune Notification",
  "source": "aws.es",
  "account": "123456789012",
  "time": "2020-10-30T22:06:31Z",
  "region": "us-east-1",
  "resources": ["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail": {
    "event": "Auto-Tune Event",
    "severity": "Informational",
    "status": "Completed",
    "description": "Auto-Tune is now disabled. The most-recent settings by Auto-Tune
 have been retained.
                    Auto-Tune will continue to evaluate cluster performance and provide
 recommendations.",
    "completionTime": "{iso8601-timestamp}"
  }
}
```

叢集運作狀態事件

OpenSearch 服務會在叢集的健全狀況受到損害 EventBridge 時傳送特定事件。

紅色叢集恢復已啟動

OpenSearch 服務會在叢集狀態持續變成紅色超過一小時後傳送此事件。其會嘗試自動從快照中恢復一個或多個紅色索引，以修復叢集狀態。

範例

以下為此類事件的範例：

```
{
   "version":"0",
   "id":"01234567-0123-0123-0123-012345678901",
   "detail-type":"Amazon OpenSearch Service Cluster Status Notification",
   "source":"aws.es",
   "account":"123456789012",
   "time":"2016-11-01T13:12:22Z",
   "region":"us-east-1",
   "resources":[
      "arn:aws:es:us-east-1:123456789012:domain/test-domain"
   ],
   "detail":{
      "event":"Automatic Snapshot Restore for Red Indices",
      "status":"Started",
      "severity":"High",
      "description":"Your cluster status is red. We have started automatic snapshot
 restore for the red indices.
                     No action is needed from your side. Red indices [red-index-0, red-
index-1]"
   }
}
```

紅色叢集恢復部分完成

OpenSearch 當服務只能從快照還原紅色索引子集，同時嘗試修復紅色叢集狀態時，才會傳送此事件。

範例

以下為此類事件的範例：

```
{
   "version":"0",
   "id":"01234567-0123-0123-0123-012345678901",
   "detail-type":"Amazon OpenSearch Service Cluster Status Notification",
   "source":"aws.es",
   "account":"123456789012",
   "time":"2016-11-01T13:12:22Z",
   "region":"us-east-1",
   "resources":[
      "arn:aws:es:us-east-1:123456789012:domain/test-domain"
   ],
```

```
   "detail":{
      "event":"Automatic Snapshot Restore for Red Indices",
      "status":"Partially Restored",
      "severity":"High",
      "description":"Your cluster status is red. We were able to restore the following
 Red indices from
                    snapshot: [red-index-0]. Indices not restored: [red-index-1].
 Please refer https://docs.aws.amazon.com/opensearch-service/latest/developerguide/
handling-errors.html#handling-errors-red-cluster-status for troubleshooting steps."
   }
}
```

紅色叢集恢復失敗

OpenSearch 服務會在嘗試修復紅色叢集狀態時，無法還原任何索引時傳送此事件。

範例

以下為此類事件的範例：

```
{
   "version":"0",
   "id":"01234567-0123-0123-0123-012345678901",
   "detail-type":"Amazon OpenSearch Service Cluster Status Notification",
   "source":"aws.es",
   "account":"123456789012",
   "time":"2016-11-01T13:12:22Z",
   "region":"us-east-1",
   "resources":[
      "arn:aws:es:us-east-1:123456789012:domain/test-domain"
   ],
   "detail":{
      "event":"Automatic Snapshot Restore for Red Indices",
      "status":"Failed",
      "severity":"High",
      "description":"Your cluster status is red. We were unable to restore the Red
 indices automatically.
                    Indices not restored: [red-index-0, red-index-1]. Please refer
 https://docs.aws.amazon.com/opensearch-service/latest/developerguide/handling-
errors.html#handling-errors-red-cluster-status for troubleshooting steps."
   }
}
```

待刪除的碎片

OpenSearch 當服務嘗試在紅色叢集狀態持續紅色 14 天之後自動修正紅色叢集狀態時，會傳送此事件，但一或多個索引仍為紅色。再過 7 天 (總共 21 天連續紅色) 之後， OpenSearch 服務會繼續刪除所有紅色索引上未指派的碎片。

範例

以下為此類事件的範例：

```
{
   "version":"0",
   "id":"01234567-0123-0123-0123-012345678901",
   "detail-type":"Amazon OpenSearch Service Cluster Status Notification",
   "source":"aws.es",
   "account":"123456789012",
   "time":"2022-04-09T10:36:48Z",
   "region":"us-east-1",
   "resources":[
      "arn:aws:es:us-east-1:123456789012:domain/test-domain"
   ],
   "detail":{
      "severity":"Medium",
      "description":"Your cluster status is red. Please fix the red indices as soon as
 possible.
                     If not fixed by 2022-04-12 01:51:47+00:00, we will delete all
 unassigned shards,
                     the unit of storage and compute, for these red indices to recover
 your domain and make it green.
                     Please refer to https://docs.aws.amazon.com/opensearch-service/
latest/developerguide/handling-errors.html#handling-errors-red-cluster-status for
 troubleshooting steps.
                     test_data, test_data1",
      "event":"Automatic Snapshot Restore for Red Indices",
      "status":"Shard(s) to be deleted"
   }
}
```

碎片已刪除

OpenSearch 服務會在您的叢集狀態持續變成紅色 21 天後傳送此事件。其會著手刪除所有紅色索引上的未指派碎片（儲存和運算）。如需詳細資訊，請參閱 the section called “紅色叢集的自動修復”。

範例

以下為此類事件的範例：

```
{
   "version":"0",
   "id":"01234567-0123-0123-0123-012345678901",
   "detail-type":"Amazon OpenSearch Service Cluster Status Notification",
   "source":"aws.es",
   "account":"123456789012",
   "time":"2022-04-09T10:54:48Z",
   "region":"us-east-1",
   "resources":[
      "arn:aws:es:us-east-1:123456789012:domain/test-domain"
   ],
   "detail":{
      "severity":"High",
      "description":"We have deleted unassinged shards, the unit of storage and
 compute, in
                     red indices: index-1, index-2 because these indices were red for
 more than
                     21 days and could not be restored with the automated restore
 process.
                     Please refer to https://docs.aws.amazon.com/opensearch-service/
latest/developerguide/handling-errors.html#handling-errors-red-cluster-status for
 troubleshooting steps.",
      "event":"Automatic Snapshot Restore for Red Indices",
      "status":"Shard(s) deleted"
   }
}
```

高碎片計數警告

OpenSearch 當熱資料節點的平均碎片計數已超過建議預設限制 1,000 的 90% 時，服務會傳送此事件。雖然較新版本的 Elasticsearch 並 OpenSearch 支援可設定的每個節點最大碎片計數限制，但我們建議您每個節點的碎片不超過 1,000 個。請參閱選擇碎片數。

範例

以下為此類事件的範例：

```
{
```

```
  "version":"0",
  "id":"01234567-0123-0123-0123-012345678901",
  "detail-type":"Amazon OpenSearch Service Notification",
  "source":"aws.es",
  "account":"123456789012",
  "time":"2016-11-01T13:12:22Z",
  "region":"us-east-1",
  "resources":["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail":{
     "event":"High Shard Count",
     "status":"Warning",
     "severity":"Low",
     "description":"One or more data nodes have close to 1000 shards. To ensure optimum
 performance and stability of your
                    cluster, please refer to the best practice guidelines - https://
docs.aws.amazon.com/opensearch-service/latest/developerguide/sizing-domains.html#bp-
sharding."
  }
}
```

已超過碎片數量限制

OpenSearch 當熱資料節點的平均碎片計數超過建議的預設限制 1,000 時，Service 會傳送此事件。雖然較新版本的 Elasticsearch 並 OpenSearch 支援可設定的每個節點最大碎片計數限制，但我們建議您每個節點的碎片不超過 1,000 個。請參閱選擇碎片數。

範例

以下為此類事件的範例：

```
{
  "version":"0",
  "id":"01234567-0123-0123-0123-012345678901",
  "detail-type":"Amazon OpenSearch Service Notification",
  "source":"aws.es",
  "account":"123456789012",
  "time":"2016-11-01T13:12:22Z",
  "region":"us-east-1",
  "resources":["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail":{
     "event":"High Shard Count",
     "status":"Warning",
     "severity":"Medium",
```

```
     "description":"One or more data nodes have more than 1000 shards. To ensure
 optimum performance and stability of your
                     cluster, please refer to the best practice guidelines - https://
docs.aws.amazon.com/opensearch-service/latest/developerguide/sizing-domains.html#bp-
sharding."
  }
}
```

磁碟空間不足

OpenSearch 當叢集中的一個或多個節點的可用儲存空間少於 25% 或低於 25 GB 時，服務會傳送此事件。

範例

以下為此類事件的範例：

```
{
  "version":"0",
  "id":"01234567-0123-0123-0123-012345678901",
  "detail-type":"Amazon OpenSearch Service Notification",
  "source":"aws.es",
  "account":"123456789012",
  "time":"2017-12-01T13:12:22Z",
  "region":"us-east-1",
  "resources":["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail":{
     "event":"Low Disk Space",
     "status":"Warning",
     "severity":"Medium",
     "description":"One or more data nodes in your cluster has less than 25% of storage
 space or less than 25GB.
                    Your cluster will be blocked for writes at 20% or 20GB. Please refer
 to the documentation for more information - https://docs.aws.amazon.com/opensearch-
service/latest/developerguide/handling-errors.html#troubleshooting-cluster-block"
  }
}
```

低磁碟浮水印違規

OpenSearch 當叢集中的所有節點都少於 10% 的可用儲存空間或小於 10 GB 時，服務會傳送此事件。當所有節點都違反低磁盤水印時，任何新索引都會產生黃色簇，並且當所有節點都低於高磁盤水印時，將導致紅色簇。

範例

以下為此類事件的範例：

```
{
  "version":"0",
  "id":"01234567-0123-0123-0123-012345678901",
  "detail-type":"Amazon OpenSearch Service Notification",
  "source":"aws.es",
  "account":"123456789012",
  "time":"2017-12-01T13:12:22Z",
  "region":"us-east-1",
  "resources":["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail":{
     "event":"Low Disk Watermark Breach",
     "status":"Warning",
     "severity":"Medium",
     "description":"Low Disk Watermark threshold is about to be breached. Once the
 threshold is breached, new index creation will be blocked on all
                    nodes to prevent the cluster status from turning red. Please
 increase disk size to suit your storage needs. For more information,
                    see https://docs.aws.amazon.com/opensearch-service/latest/
developerguide/handling-errors.html#troubleshooting-cluster-block".
  }
}
```

EBS 爆量餘額低於 70%

OpenSearch 當一個或多個資料節點上的 EBS 突發平衡低於 70% 時，服務會傳送此事件。EBS 爆量餘額損耗可能會導致廣泛的叢集無法使用和 I/O 請求限流，進而導致索引和搜尋請求的高延遲和逾時。如需修正此問題的步驟，請參閱 the section called “低 EBS 爆量餘額”。

範例

以下為此類事件的範例：

```
{
  "version":"0",
  "id":"01234567-0123-0123-0123-012345678901",
  "detail-type":"Amazon OpenSearch Service Notification",
  "source":"aws.es",
  "account":"123456789012",
  "time":"2017-12-01T13:12:22Z",
```

```
  "region":"us-east-1",
  "resources":["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail":{
     "event":"EBS Burst Balance",
     "status":"Warning",
     "severity":"Medium",
     "description":"EBS burst balance on one or more data nodes is below 70%.
                    Follow https://docs.aws.amazon.com/opensearch-service/latest/
developerguide/handling-errors.html#handling-errors-low-ebs-burst
                    to fix this issue."
  }
}
```

EBS 爆量餘額低於 20%

OpenSearch 當一個或多個資料節點上的 EBS 突發平衡低於 20% 時，服務會傳送此事件。EBS 爆量餘額損耗可能會導致廣泛的叢集無法使用和 I/O 請求限流，進而導致索引和搜尋請求的高延遲和逾時。如需修正此問題的步驟，請參閱 the section called “低 EBS 爆量餘額”。

範例

以下為此類事件的範例：

```
{
  "version":"0",
  "id":"01234567-0123-0123-0123-012345678901",
  "detail-type":"Amazon OpenSearch Service Notification",
  "source":"aws.es",
  "account":"123456789012",
  "time":"2017-12-01T13:12:22Z",
  "region":"us-east-1",
  "resources":["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail":{
     "event":"EBS Burst Balance",
     "status":"Warning",
     "severity":"High",
     "description":"EBS burst balance on one or more data nodes is below 20%.
                    Follow https://docs.aws.amazon.com/opensearch-service/latest/
developerguide/handling-errors.html#handling-errors-low-ebs-burst
                    to fix this issue.
  }
}
```

磁碟輸送量限流

OpenSearch 由於 EBS 磁碟區或 EC2 執行個體的輸送量限制，當網域的讀取和寫入請求受到限制時，服務會傳送此事件。如果您收到此通知，請考慮按照 AWS 建議的最佳做法擴展磁碟區或執行個體。如果您的磁碟區類型為gp2，請增加磁碟區大小。如果您的磁碟區類型為gp3，請佈建更多輸送量。您也可以檢查執行個體基礎和最大 EBS 輸送量是否大於或等於佈建的磁碟區輸送量，並且可以相應地擴展。

範例

以下為此類事件的範例：

```
{
  "version":"0",
  "id":"01234567-0123-0123-0123-012345678901",
  "detail-type":"Amazon OpenSearch Service Notification",
  "source":"aws.es",
  "account":"123456789012",
  "time":"2017-12-01T13:12:22Z",
  "region":"us-east-1",
  "resources":["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail":{
     "event":"Disk Throughput Throttle",
     "status":"Warning",
     "severity":"Medium",
     "description":"Your domain is experiencing throttling due to instance or volume
 throughput limitations.
                    Please consider scaling your domain to suit your throughput needs.
 In July 2023, we improved
                    the accuracy of throughput throttle calculation by replacing ‘Max
 volume throughput’ with
                    ‘Provisioned volume throughput’. Please refer to the documentation
 for more information."
  }
}
```

大碎片大小

OpenSearch 當叢集中的一個或多個碎片已超過 50GiB 或 65GiB 時，服務會傳送此事件。為了確保最佳的叢集效能和穩定性，請減少碎片大小。

如需詳細資訊，請參閱分片最佳做法。

範例

以下為此類事件的範例：

```
{
  "version":"0",
  "id":"01234567-0123-0123-0123-012345678901",
  "detail-type":"Amazon OpenSearch Service Notification",
  "source":"aws.es",
  "account":"123456789012",
  "time":"2017-12-01T13:12:22Z",
  "region":"us-east-1",
  "resources":["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail":{
     "event":"Large Shard Size",
     "status":"Warning",
     "severity":"Medium",
     "description":"One or more shards are larger than 65GiB. To ensure optimum cluster
 performance and stability, reduce shard sizes.
                    For more information, see https://docs.aws.amazon.com/opensearch-
service/latest/developerguide/monitoring-events.html#monitoring-events-large-shard-
size."
  }
}
```

高 JVM 用量

OpenSearch 當您網域的`JVMMemoryPressure`指標超過 80% 時，服務會傳送此事件。如果在 30 分鐘內超過 92%，則會封鎖叢集的所有寫入作業。為了確保最佳的叢集穩定性，請減少叢集的流量或調整網域，以提供足夠的記憶體來處理工作負載。

範例

以下為此類事件的範例：

```
{
  "version":"0",
  "id":"01234567-0123-0123-0123-012345678901",
  "detail-type":"Amazon OpenSearch Service Notification",
  "source":"aws.es",
  "account":"123456789012",
  "time":"2017-12-01T13:12:22Z",
  "region":"us-east-1",
```

```
  "resources":["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail":{
     "event":"High JVM Usage",
     "status":"Warning",
     "severity":"High",
     "description":"JVM memory pressure has exceeded 80%. If it exceeds 92% for 30
 minutes, all write operations to your cluster
                    will be blocked. To ensure optimum cluster stability, reduce
 traffic to the cluster or use larger instance types.
                    For more information, see https://docs.aws.amazon.com/opensearch-
service/latest/developerguide/monitoring-events.html#monitoring-events-high-jvm."
  }
}
```

GC 不足

OpenSearch 當最大 JVM 超過 70% 且最大值和最小值之間的差異小於 30% 時，服務會發送此事件。這可能表示 JVM 無法在工作負載的記憶體回收週期期間回收足夠的記憶體。這可能會導致回應速度越來越慢，延遲時間越來越高；在某些情況下，甚至節點會因為運作狀態檢查逾時而中斷。為了確保最佳的叢集穩定性，請減少叢集的流量或調整網域，以提供足夠的記憶體來處理工作負載。

範例

以下為此類事件的範例：

```
{
  "version":"0",
  "id":"01234567-0123-0123-0123-012345678901",
  "detail-type":"Amazon OpenSearch Service Notification",
  "source":"aws.es",
  "account":"123456789012",
  "time":"2017-12-01T13:12:22Z",
  "region":"us-east-1",
  "resources":["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail":{
     "event":"Insufficient GC",
     "status":"Warning",
     "severity":"Medium",
     "description":"Maximum JVM is above 70% and JVM range is less than 30%. This may
 indicate insufficient garbage collection for your workload.
                    For more information, see https://docs.aws.amazon.com/opensearch-
service/latest/developerguide/monitoring-events.html#monitoring-events-insufficient-
gc."
```

```
  }
}
```

自訂索引路由警告

OpenSearch 當您的域處於處理狀態並包含具有自定義 index.routing.allocation 設置的索引時，服務發送此事件，這可能會導致藍綠色部署卡住。確認設定已正確套用。

範例

以下為此類事件的範例：

```
{
  "version":"0",
  "id":"01234567-0123-0123-0123-012345678901",
  "detail-type":"Amazon OpenSearch Service Notification",
  "source":"aws.es",
  "account":"123456789012",
  "time":"2017-12-01T13:12:22Z",
  "region":"us-east-1",
  "resources":["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail":{
     "event":"Custom Index Routing Warning",
     "status":"Warning",
     "severity":"Medium",
     "description":"Your domain is in processing state and contains indice(s) with
 custom index.routing.allocation
                    settings which can cause blue-green deployments to get stuck.
 Verify settings are applied properly.
                    For more information, see https://docs.aws.amazon.com/opensearch-
service/latest/developerguide/monitoring-events.html#monitoring-events-index-routing."
  }
}
```

碎片鎖定失敗

OpenSearch 當您的域由於未分配的碎片而不健康時，服務將發送此事件。[ShardLockObtainFailedException]如需詳細資訊，請參閱如何解決 Amazon OpenSearch 服務中的記憶體內碎片鎖定例外狀況？

範例

以下為此類事件的範例：

```
{
  "version":"0",
  "id":"01234567-0123-0123-0123-012345678901",
  "detail-type":"Amazon OpenSearch Service Notification",
  "source":"aws.es",
  "account":"123456789012",
  "time":"2017-12-01T13:12:22Z",
  "region":"us-east-1",
  "resources":["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail":{
     "event":"Failed Shard Lock",
     "status":"Warning",
     "severity":"Medium",
     "description":"Your domain is unhealthy due to unassigned shards with
 [ShardLockObtainFailedException]. For more information,
                    see https://docs.aws.amazon.com/opensearch-service/latest/
developerguide/monitoring-events.html#monitoring-events-failed-shard-lock."
}
```

VPC 端點事件

OpenSearch 服務會將某些事件傳送至 EventBridge 與AWS PrivateLink 介面端點相關。

VPC 端點建立失敗

OpenSearch 服務會在無法建立要求的 VPC 端點時傳送此事件。發生此錯誤的原因可能是您已達到一個區域內允許的 VPC 端點數目上限。如果指定的子網路或安全群組不存在，您也會看到這個錯誤。

範例

以下為此類事件的範例：

```
{
   "version":"0",
   "id":"01234567-0123-0123-0123-012345678901",
   "detail-type":"Amazon OpenSearch Service VPC Endpoint Notification",
   "source":"aws.es",
   "account":"123456789012",
   "time":"2016-11-01T13:12:22Z",
   "region":"us-east-1",
   "resources":[
      "arn:aws:es:us-east-1:123456789012:domain/test-domain"
   ],
```

```
   "detail":{
      "event":"VPC Endpoint Create Validation",
      "status":"Failed",
      "severity":"High",
      "description":"Unable to create VPC endpoint aos-0d4c74c0342343 for domain
                     arn:aws:es:eu-south-1:123456789012:domain/my-domain due to the
 following validation failures: You've reached the limit on the
                     number of VPC endpoints that you can create in the AWS Region."
   }
}
```

VPC 端點更新失敗

OpenSearch 服務會在無法刪除要求的 VPC 端點時傳送此事件。

範例

以下為此類事件的範例：

```
{
   "version":"0",
   "id":"01234567-0123-0123-0123-012345678901",
   "detail-type":"Amazon OpenSearch Service VPC Endpoint Notification",
   "source":"aws.es",
   "account":"123456789012",
   "time":"2016-11-01T13:12:22Z",
   "region":"us-east-1",
   "resources":[
      "arn:aws:es:us-east-1:123456789012:domain/test-domain"
   ],
   "detail":{
      "event":"VPC Endpoint Update Validation",
      "status":"Failed",
      "severity":"High",
      "description":"Unable to update VPC endpoint aos-0d4c74c0342343 for domain
                     arn:aws:es:eu-south-1:123456789012:domain/my-domain due to the
 following validation failures: <failure message>."
   }
}
```

VPC 端點刪除失敗

OpenSearch 服務會在無法刪除要求的 VPC 端點時傳送此事件。

範例

以下為此類事件的範例：

```
{
   "version":"0",
   "id":"01234567-0123-0123-0123-012345678901",
   "detail-type":"Amazon OpenSearch Service VPC Endpoint Notification",
   "source":"aws.es",
   "account":"123456789012",
   "time":"2016-11-01T13:12:22Z",
   "region":"us-east-1",
   "resources":[
      "arn:aws:es:us-east-1:123456789012:domain/test-domain"
   ],
   "detail":{
      "event":"VPC Endpoint Delete Validation",
      "status":"Failed",
      "severity":"High",
      "description":"Unable to delete VPC endpoint aos-0d4c74c0342343 for domain
                     arn:aws:es:eu-south-1:123456789012:domain/my-domain due to the
 following validation failures: Specified subnet doesn't exist."
   }
}
```

節點淘汰事件

OpenSearch 當發生下列節點淘汰事件之一 EventBridge 時，Service 會傳送事件至。

節點處分已排程

OpenSearch 服務會在已排定節點淘汰時傳送此事件。

範例

以下為此類事件的範例：

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "Amazon OpenSearch Service Notification",
  "source": "aws.es",
```

```
  "account": "123456789012",
  "time": "2023-04-07T10:07:33Z",
  "region": "us-east-1",
  "resources": ["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail": {
    "event": "Node Retirement Notification",
    "status": "Scheduled",
    "severity": "Medium",
    "description": "An automated action to retire and replace a node has been scheduled
 on your domain.
                    The node will be replaced in the next off-peak window. For more
 information, see
                    https://docs.aws.amazon.com/opensearch-service/latest/
developerguide/monitoring-events.html."
  }
}
```

節點淘汰已完成

OpenSearch 服務會在節點處分完成時傳送此事件。

範例

以下為此類事件的範例：

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "Amazon OpenSearch Service Notification",
  "source": "aws.es",
  "account": "123456789012",
  "time": "2023-04-07T10:07:33Z",
  "region": "us-east-1",
  "resources": ["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail": {
    "event": "Node Retirement Notification",
    "status": "Completed",
    "severity": "Medium",
    "description": "The node has been retired and replaced with a new node."
  }
}
```

節點淘汰失敗

OpenSearch 服務會在節點淘汰失敗時傳送此事件。

範例

以下為此類事件的範例：

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "Amazon OpenSearch Service Notification",
  "source": "aws.es",
  "account": "123456789012",
  "time": "2023-04-07T10:07:33Z",
  "region": "us-east-1",
  "resources": ["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail": {
    "event": "Node Retirement Notification",
    "status": "Failed",
    "severity": "Medium",
    "description": "Node retirement failed. No actions are required from your end. We
 will automatically
                    retry replacing the node."
  }
}
```

降級的節點淘汰事件

OpenSearch 服務會在因節點上的硬體降級而需要取代節點時傳送這些事件。

降級節點淘汰通知

OpenSearch 當已針對您的網域排定淘汰和取代降級節點的自動動作時，Service 會傳送此事件。

範例

以下為此類事件的範例：

```
{
   "version":"0",
   "id":"db233454-aad1-7676-3b15-10a84b052baa",
```

```
   "detail-type":"Amazon OpenSearch Service Notification",
   "source":"aws.es",
   "account":"123456789012",
   "time":"2024-01-11T08:16:06Z",
   "region":"us-east-1",
   "resources":[
      "arn:aws:es:us-east-1:123456789012:domain/test-node-replacement"
   ],
   "detail":{
      "severity":"Medium",
      "description":"An automated action to retire and replace a node has
 been scheduled on your domain. For more information, please see https://
docs.aws.amazon.com/opensearch-service/latest/developerguide/monitoring-events.html.",
      "event":"Degraded Node Retirement Notification",
      "status":"Scheduled"
   }
}
```

降級節點處分完成

OpenSearch 服務會在降級的節點已淘汰並以新節點取代時傳送此事件。

範例

以下為此類事件的範例：

```
{
   "version":"0",
   "id":"7444215c-90f9-a52d-bcda-e85973a9a762",
   "detail-type":"Amazon OpenSearch Service Notification",
   "source":"aws.es",
   "account":"123456789012",
   "time":"2024-01-11T10:20:30Z",
   "region":"us-east-1",
   "resources":[
      "arn:aws:es:us-east-1:123456789012:domain/test-node-replacement"
   ],
   "detail":{
      "severity":"Medium",
      "description":"The node has been retired and replaced with a new node.",
      "event":"Degraded Node Retirement Notification",
      "status":"Completed"
   }
```

```
}
```

降級的節點淘汰失敗

OpenSearch 如果降級的節點淘汰失敗，服務就會傳送此事件。

範例

以下為此類事件的範例：

```
{
   "version":"0",
   "id":"c328e9bb-93b9-c0b2-b17a-df527fdf96b6",
   "detail-type":"Amazon OpenSearch Service Notification",
   "source":"aws.es",
   "account":"123456789012",
   "time":"2024-01-11T08:31:38Z",
   "region":"us-east-1",
   "resources":[
      "arn:aws:es:us-east-1:123456789012:domain/test-node-replacement"
   ],
   "detail":{
      "severity":"Medium",
      "description":"Node retirement failed. No actions are required from your end. We
 will automatically re-try replacing the node.",
      "event":"Degraded Node Retirement Notification",
      "status":"Failed"
   }
}
```

網域錯誤事件

OpenSearch 發生下列網域錯誤之一 EventBridge 時，服務會傳送事件至。

網域更新驗證失敗

OpenSearch 服務會在嘗試更新或執行網域上的組態變更時，如果遇到一或多個驗證失敗，就會傳送此事件。如需解決這些失敗的步驟，請參閱 the section called “對驗證錯誤進行疑難排解”。

範例

以下為此類事件的範例：

```
{
   "version":"0",
   "id":"01234567-0123-0123-0123-012345678901",
   "detail-type":"Amazon OpenSearch Service Domain Update Notification",
   "source":"aws.es",
   "account":"123456789012",
   "time":"2016-11-01T13:12:22Z",
   "region":"us-east-1",
   "resources":[
      "arn:aws:es:us-east-1:123456789012:domain/test-domain"
   ],
   "detail":{
      "event":"Domain Update Validation",
      "status":"Failed",
      "severity":"High",
      "description":"Unable to perform updates to your domain due to the following
 validation failures: <failures>
                     Please see the documentation for more information https://
docs.aws.amazon.com/opensearch-service/latest/developerguide/managedomains-
configuration-changes.html#validation"
   }
}
```

無法存取 KMS 金鑰

OpenSearch 服務在無法訪問您的 AWS KMS 密鑰時發送此事件。

範例

以下為此類事件的範例：

```
{
  "version":"0",
  "id":"01234567-0123-0123-0123-012345678901",
  "detail-type":"Domain Error Notification",
  "source":"aws.es",
  "account":"123456789012",
  "time":"2016-11-01T13:12:22Z",
  "region":"us-east-1",
  "resources":["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail":{
     "event":"KMS Key Inaccessible",
     "status":"Error",
```

```
     "severity":"High",
     "description":"The KMS key associated with this domain is inaccessible. You are at
 risk of losing access to your domain.
                    For more information, please refer to https://docs.aws.amazon.com/
opensearch-service/latest/developerguide/encryption-at-rest.html#disabled-key."
  }
}
```

網域隔離

OpenSearch 服務會在您的網域變成隔離狀態，而且因為網路無法連線而無法接收、讀取或寫入要求時，就會傳送此事件。

範例

以下為此類事件的範例：

```
{
  "version":"0",
  "id":"01234567-0123-0123-0123-012345678901",
  "detail-type":"Amazon OpenSearch Service Notification",
  "source":"aws.es",
  "account":"123456789012",
  "time":"2023-11-01T13:12:22Z",
  "region":"us-east-1",
  "resources":["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail":{
     "event":"Domain Isolation Notification",
     "status":"Error",
     "severity":"High",
     "description":"Your OpenSearch Service domain has been isolated. An isolated
 domain is unreachable by network and cannot receive, read, or write requests. For more
 information and assistance, please contact AWS Support at https://docs.aws.amazon.com/
opensearch-service/latest/developerguide/encryption-at-rest.html#disabled-key."
  }
}
```

教學課程：監聽 Amazon OpenSearch 服務 EventBridge 事件

在本教學中，您會設定一個簡單的 AWS Lambda 函數，以偵聽 Amazon Ser OpenSearch vice 事件並將其寫入 CloudWatch 日誌記錄串流。

必要條件

本教學課程假設您擁有現有的 OpenSearch 服務網域。若您尚未建立網域，請依照 建立和管理網域 中的步驟建立一個。

步驟 1：建立 Lambda 函數

在此程序中，您可以建立簡單的 Lambda 函數，做為服 OpenSearch 務事件訊息的目標。

若要建立目標 Lambda 函數

1. 請在以下位置開啟 AWS Lambda 主控台。 https://console.aws.amazon.com/lambda/
2. 選擇 Create function (建立函數) 和 Author from scratch (從頭開始撰寫)。
3. 對於 Function name (函數名稱)，輸入 event-handler。
4. 針對執行階段，選擇 Python 3.8。
5. 選擇建立函數。
6. 在 Function code (函數程式碼) 區段中，編輯範本程式碼以符合下列範例：

```
import json

def lambda_handler(event, context):
    if event["source"] != "aws.es":
        raise ValueError("Function only supports input from events with a source
 type of: aws.es")

    print(json.dumps(event))
```

   這是一個簡單的 Python 3.8 函數，打印 OpenSearch 服務發送的事件。如果所有項目都設定正確，則在本教學課程結束時，事件詳細資料會顯示在與此 Lambda 函數相關聯的 CloudWatch 記錄資料流中。
7. 選擇部署。

步驟 2：註冊事件規則

在此步驟中，您會建立擷取 OpenSearch Service 網域中事件的 EventBridge 規則。此規則會擷取定義它的帳戶中的所有事件。事件訊息本身包含事件來源資訊，包括其來源的網域。您可以使用此資訊以程式設計方式篩選和排序事件。

若要建立 EventBridge 規則

1. 請在以下位置開啟 EventBridge 主控台。 https://console.aws.amazon.com/events/
2. 選擇建立規則。
3. 將規則命名為 event-rule。
4. 選擇下一步。
5. 對於事件模式，請選取AWS 服務、Amazon OpenSearch 服務和所有事件。此模式適用於您的所有 OpenSearch 服務域和每個 OpenSearch 服務事件。或者，您可以建立一個更針對性的模式，來篩選掉一些結果。
6. 按下 Next (下一步)。
7. 對於目標，選擇 Lambda function (Lambda 函數)。在函數下拉式選單中，選擇 event-handler。
8. 按下 Next (下一步)。
9. 跳過標籤，然後再按一次 Next (下一步)。
10. 檢閱組態，然後選擇 Create rule (建立規則)。

步驟 3：測試組態

下次您在 OpenSearch 服務主控台的 [通知] 區段收到通知時，如果所有項目設定正確，則會觸發 Lambda 函數，並將事件資料寫入函數的 CloudWatch 記錄檔資料流中。

若要測試組態

1. 請在以下位置開啟 CloudWatch 主控台。 https://console.aws.amazon.com/cloudwatch/
2. 在導覽窗格中，選擇 Logs (日誌)，然後選取 Lambda 函數的日誌群組 (例如，/aws/lambda/event-handler)。
3. 選取日誌串流，以檢視事件資料。

教學課程：可用軟體更新的 Amazon SNS 提醒

在本教學中，您會設定 Amazon EventBridge 事件規則，以擷取 Amazon 服務中可用服務軟體更新的通知，並透過 Amazon Simple Notification Service (Amazon OpenSearch SNS) 向您傳送電子郵件通知。

必要條件

本教學課程假設您擁有現有的 OpenSearch 服務網域。若您尚未建立網域，請依照 建立和管理網域 中的步驟建立一個。

步驟 1：建立並訂閱 Amazon SNS 主題

設定 Amazon SNS 主題以作為新事件規則的事件目標。

若要建立 Amazon SNS 目標

1. 在 https://console.aws.amazon.com/sns/v3/home 開啟 Amazon SNS 主控台。
2. 選擇 Topics (主題) 和 Create topic (建立主題)。
3. 對於任務類型，請選擇 Standard (標準)，並將任務命名為 software-update。
4. 請選擇建立主題。
5. 建立主題之後，選擇 Create subscription (建立訂閱)。
6. 對於通訊協定，選擇電子郵件。對於 Endpoint (端點)，輸入您目前能存取的電子郵件地址，並選擇 Create subscription (建立訂閱)。
7. 檢查您的電子郵件帳戶，並等待接收訂閱確認電子郵件訊息。您收到訊息時，請選擇 Confirm subscription (確認訂閱)。

步驟 2：註冊事件規則

接著，註冊僅擷取服務軟體更新事件的事件規則。

若要建立事件規則

1. 請在以下位置開啟 EventBridge 主控台。 https://console.aws.amazon.com/events/
2. 選擇建立規則。
3. 將規則命名為 softwareupdate-rule。
4. 選擇下一步。
5. 對於事件模式，請選取AWS 服務、Amazon OpenSearch 服務和 Amazon OpenSearch 服務軟體更新通知。此病毒碼會與服務中 OpenSearch 的任何服務軟體更新事件相符。如需有關事件模式的詳細資訊，請參閱 Amazon EventBridge使用者指南中的 Amazon EventBridge 事件模式。
6. 或著，您可以針對特定的嚴重性進行篩選。有關每個事件的嚴重性，請參閱 the section called “服務軟體更新事件”。
7. 選擇下一步。
8. 對於目標，選擇 SNS topic (SNS 主題)，然後選取 software-update。
9. 選擇下一步。
10. 跳過標籤，然後選擇 Next (下一步)。

11. 檢閱規則組態，然後選擇 Create rule (建立規則)。

下次您收到來自 OpenSearch 服務的有關可用服務軟體更新的通知時，如果所有設定正確，Amazon SNS 應該會傳送有關更新的電子郵件警示給您。

使用來監控 Amazon Amazon Ser OpenSearch vice API 呼叫 AWS CloudTrail

Amazon Ser OpenSearch vice 已與整合AWS CloudTrail，這項服務可提供由使用者、角色或AWS服務所採取之動作的記錄。OpenSearchCloudTrail會擷取 OpenSearch Service 的所有組態 API 呼叫。

> **Note**
>
> CloudTrail只會擷取對設定 API 的呼叫，例如`CreateDomain`和`GetUpgradeStatus`。CloudTrail不會擷取對 OpenSearchAPI 的呼叫，例如`_search`和`_bulk`。對於這些呼叫，請參閱the section called “監控稽核日誌”。

擷取的呼叫包括來自 OpenSearch Service 主控台AWS CLI、或AWS開發套件的呼叫。如果您建立追蹤，就可以將CloudTrail事件持續交付到 Amazon S3 儲存貯體，包括OpenSearch服務的事件。如果您不設定追蹤記錄，仍然可以透過 CloudTrail 主控台上的 Event history (事件歷史記錄) 檢視最新的事件。您可以使用CloudTrail收集的資訊來判斷向 OpenSearch Service 發出的請求，以及發出請求的 IP 地址、提出請求的時間，以及其他詳細資訊。

若要進一步了解 CloudTrail，請參閱 AWS CloudTrail 使用者指南。

亞馬遜OpenSearch服務信息 CloudTrail

當您建立帳戶時，系統會在您的 AWS 帳戶 中啟用 CloudTrail。此外，OpenSearchService 中發生活動時，系統便會將該活動記錄至CloudTrail事件，並將其他AWS服務事件記錄到事件歷史記錄中。您可以檢視、搜尋和下載 AWS 帳戶 帳戶的最新事件。如需詳細資訊，請參閱使用 CloudTrail 事件歷程記錄檢視事件。

若要持續記錄AWS 帳戶帳戶中的事件，包括 OpenSearch Service 的事件。線索能CloudTrail將日誌檔案交付至 Amazon S3 儲存貯體。依預設，當您在主控台中建立追蹤時，該追蹤會套用至所有的 AWS 區域。該追蹤會記錄來自 AWS 分割區中所有區域的事件，並將日誌檔案交付到您指定的 Amazon S3 儲存貯體。此外，您可以設定其他 AWS 服務，以進一步分析和處理 CloudTrail 日誌中所收集的事件資料。如需詳細資訊，請參閱下列內容：

- 建立 AWS 帳戶 的追蹤
- AWS與CloudTrail日誌的服務整合
- 設定 CloudTrail 的 Amazon SNS 通知
- 接收多個區域的 CloudTrail 日誌檔案及接收多個帳戶的 CloudTrail 日誌檔案

Amazon Con OpenSearch vice API 動作會記錄在 Amazon Ser OpenSearch vice API 參考中。CloudTrail

每一筆事件或日誌項目都會包含產生請求者的資訊。身分資訊可協助您判斷下列事項：

- 該請求是否使用根或 AWS Identity and Access Management (IAM) 使用者登入資料提出
- 提出該請求時，是否使用了特定角色或聯合身分使用者的暫時安全登入資料
- 該請求是否由另一項 AWS 服務提出

如需詳細資訊，請參閱 CloudTrail 使用者身分元素。

了解 Amazon Amazon Ser OpenSearch vice 日誌檔案項目

追蹤是一種組態，能讓事件以日誌檔案的形式交付到您指定的 Amazon S3 儲存貯體。CloudTrail 日誌檔案包含一個或多個日誌項目。一個事件為任何來源提出的單一請求，並包含請求動作、請求的日期和時間、請求參數等資訊。CloudTrail 日誌檔案並非依公有 API 呼叫追蹤記錄的堆疊排序，因此不會以任何特定順序出現。

以下範例顯示的 CloudTrail 日誌項目會示範 `CreateDomain` 操作：

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "AIDACKCEVSQ6C2EXAMPLE",
    "arn": "arn:aws:iam::123456789012:user/test-user",
    "accountId": "123456789012",
    "accessKeyId": "access-key",
    "userName": "test-user",
    "sessionContext": {
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2018-08-21T21:59:11Z"
      }
```

```
    },
    "invokedBy": "signin.amazonaws.com"
  },
  "eventTime": "2018-08-21T22:00:05Z",
  "eventSource": "es.amazonaws.com",
  "eventName": "CreateDomain",
  "awsRegion": "us-west-1",
  "sourceIPAddress": "123.123.123.123",
  "userAgent": "signin.amazonaws.com",
  "requestParameters": {
    "engineVersion": "OpenSearch_1.0",
    "clusterConfig": {
      "instanceType": "m4.large.search",
      "instanceCount": 1
    },
    "snapshotOptions": {
      "automatedSnapshotStartHour": 0
    },
    "domainName": "test-domain",
    "encryptionAtRestOptions": {},
    "eBSOptions": {
      "eBSEnabled": true,
      "volumeSize": 10,
      "volumeType": "gp2"
    },
    "accessPolicies": "{\"Version\":\"2012-10-17\",\"Statement\":[{\"Effect\":\"Allow
\",\"Principal\":{\"AWS\":[\"123456789012\"]},\"Action\":[\"es:*\"],\"Resource\":
\"arn:aws:es:us-west-1:123456789012:domain/test-domain/*\"}]}",
    "advancedOptions": {
      "rest.action.multi.allow_explicit_index": "true"
    }
  },
  "responseElements": {
    "domainStatus": {
      "created": true,
      "clusterConfig": {
        "zoneAwarenessEnabled": false,
        "instanceType": "m4.large.search",
        "dedicatedMasterEnabled": false,
        "instanceCount": 1
      },
      "cognitoOptions": {
        "enabled": false
      },
```

```
      "encryptionAtRestOptions": {
        "enabled": false
      },
      "advancedOptions": {
        "rest.action.multi.allow_explicit_index": "true"
      },
      "upgradeProcessing": false,
      "snapshotOptions": {
        "automatedSnapshotStartHour": 0
      },
      "eBSOptions": {
        "eBSEnabled": true,
        "volumeSize": 10,
        "volumeType": "gp2"
      },
      "engineVersion": "OpenSearch_1.0",
      "processing": true,
      "aRN": "arn:aws:es:us-west-1:123456789012:domain/test-domain",
      "domainId": "123456789012/test-domain",
      "deleted": false,
      "domainName": "test-domain",
      "accessPolicies": "{\"Version\":\"2012-10-17\",\"Statement\":[{\"Effect\":\"Allow
\",\"Principal\":{\"AWS\":\"arn:aws:iam::123456789012:root\"},\"Action\":\"es:*\",
\"Resource\":\"arn:aws:es:us-west-1:123456789012:domain/test-domain/*\"}]}"
    }
  },
  "requestID": "12345678-1234-1234-1234-987654321098",
  "eventID": "87654321-4321-4321-4321-987654321098",
  "eventType": "AwsApiCall",
  "recipientAccountId": "123456789012"
}
```

Amazon OpenSearch 服務中的安全

雲端安全 AWS 是最高的優先級。作為 AWS 客戶，您可以從資料中心和網路架構中獲益，該架構專為滿足對安全性最敏感的組織的需求而打造。

安全是兩者之間的共同責任 AWS 和你。共同責任模型 將此描述為雲端的安全和雲端內的安全：

- 雲端的安全性 — AWS 負責保護運行的基礎設施 AWS 中的服務 AWS 雲端。 AWS 還為您提供可以安全使用的服務。第三方稽核員會定期測試和驗證我們安全性的有效性，作為 AWS 合規方案。若要了解適用於 Amazon OpenSearch 服務的合規計劃，請參閱 AWS 合規計劃範圍內的服務。
- 雲端中的安全性 — 您的責任取決於 AWS 您使用的服務。您也必須對其他因素負責，包括資料的機密性、您公司的要求和適用法律和法規。

本文檔可幫助您了解如何在使用 OpenSearch 服務時應用共同責任模型。下列主題說明如何設定 OpenSearch Service 以符合您的安全性與合規性目標。您還將學習如何使用其他 AWS 協助您監控和保護 OpenSearch 服務資源的服務。

主題

- Amazon OpenSearch 服務中的數據保護
- Amazon OpenSearch 服務中的 Identity and Access Management
- 預防跨服務混淆代理人
- Amazon OpenSearch 服務中的精細訪問控制
- Amazon OpenSearch 服務的合規驗證
- Amazon CopenSearFront Service 的復原功能
- JWTAmazon OpenSearch 服務的身份驗證和授權
- Amazon OpenSearch 服務基礎設施安全
- SAML OpenSearch 儀表板的驗證
- 為儀表板設定 Amazon Cognito 份驗證 OpenSearch
- 針對 Amazon OpenSearch 服務使用服務連結角色

Amazon OpenSearch 服務中的數據保護

所以此 AWS 共同責任模型適用於 Amazon OpenSearch 服務中的資料保護。如本模型所述， AWS 負責保護運行所有的全球基礎設施 AWS 雲端。 您有責任維持對託管在此基礎結構上的內容的控制權。

您也必須負責 AWS 服務 你使用. 如需有關資料隱私權的詳細資訊，請參閱資料隱私權FAQ。 如需歐洲資料保護的相關資訊，請參閱 AWS 共同責任模型和GDPR博客文章 AWS 安全部落格。

出於數據保護目的，我們建議您進行保護 AWS 帳戶 憑據並設置個別用戶 AWS IAM Identity Center 或 AWS Identity and Access Management (IAM)。如此一來，每個使用者都只會獲得授與完成其任務所必須的許可。我們也建議您採用下列方式保護資料：

- 對每個帳戶使用多重要素驗證 (MFA)。
- 使用SSL/TLS與之溝通 AWS 的費用。我們需要 TLS 1.2 並推薦 TLS 1.3。
- 設定API和使用者活動記錄 AWS CloudTrail。 如需使用 CloudTrail 軌跡進行擷取的相關資訊 AWS 活動，請參閱使用 CloudTrail 系統線 AWS CloudTrail 使用者指南。
- 使用 AWS 加密解決方案，以及其中的所有默認安全控制 AWS 服務.
- 使用進階的受管安全服務 (例如 Amazon Macie)，協助探索和保護儲存在 Amazon S3 的敏感資料。
- 如果您在訪問時需要 FIPS 140-3 驗證的加密模塊 AWS 透過指令行介面或API使用FIPS端點。如需有關可用FIPS端點的詳細資訊，請參閱聯邦資訊處理標準 (FIPS) 140-3。

我們強烈建議您絕對不要將客戶的電子郵件地址等機密或敏感資訊，放在標籤或自由格式的文字欄位中，例如名稱欄位。這包括當您使用 OpenSearch 服務或其他服務時 AWS 服務 使用控制台API，AWS CLI，或 AWS SDKs。您在標籤或自由格式文字欄位中輸入的任何資料都可能用於計費或診斷日誌。如果您提供URL給外部伺服器，我們強烈建議您不要在中包含認證資訊，URL以驗證您對該伺服器的要求。

Amazon OpenSearch 服務的靜態數據加密

OpenSearch 服務網域提供靜態資料的加密功能，這項安全性功能可協助防止未經授權存取您的資料。該功能使用 AWS Key Management Service (AWS KMS) 儲存和管理您的加密金鑰和進階加密標準演算法 (AES256 位元金鑰)，以執行加密。如果啟用，此功能會加密網域的以下層面：

- 所有索引（包括 UltraWarm 存儲中的索引）
- OpenSearch 日誌
- 置換檔案
- 應用程式目錄中的所有其他資料
- 自動快照

當您啟用靜態資料加密時，以下項目不會加密，但您可以採取額外的步驟來保護它們：

- 手動快照：您目前無法使用 AWS KMS 用於加密手動快照的金鑰。不過，您可以使用伺服器端加密搭配 S3 管理的金鑰或金KMS鑰來加密您作為快照儲存庫使用的儲存貯體。如需說明，請參閱 the section called “註冊手動快照儲存庫”。
- 緩慢的日誌和錯誤日誌：如果您發布日誌並想要加密它們，則可以使用相同的方式加密其 CloudWatch 日誌日誌組 AWS KMS 密鑰作為 OpenSearch 服務域。有關詳情，請參閱使用以下方式加密 CloudWatch 記錄檔中的記錄 AWS KMS在 Amazon CloudWatch 日誌用戶指南中。

> **Note**
>
> 如果網域上已啟用 UltraWarm 或已啟用冷儲存，則無法在現有網域上啟用靜態加密。您必須先停用 UltraWarm 或冷儲存、啟用靜態加密，然後重新啟用 UltraWarm 或冷儲存。如果要保留索引 UltraWarm 或冷存儲，則必須在禁用 UltraWarm 或冷存儲之前將其移至熱存儲。

OpenSearch 服務僅支援對稱式加密KMS金鑰，不支援非對稱金鑰。若要瞭解如何建立對稱金鑰，請參閱在 AWS Key Management Service 開發人員指南。

無論是否啟用靜態加密，所有網域都會使用 AES -256 和 OpenSearch 服務管理金鑰自動加密自訂套件。

許可

若要使用 OpenSearch 服務主控台來設定靜態資料的加密，您必須具有讀取權限 AWS KMS，例如下列以身分識別為基礎的原則：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "kms:List*",
        "kms:Describe*"
      ],
      "Resource": "*"
    }
  ]
}
```

如果您想要使用其他金鑰 AWS 擁有的密鑰，您還必須具有為密鑰創建授權的權限。這些許可通常採用以資源為基礎的政策形式，當您建立金鑰時會加以指定。

如果您想要保留 OpenSearch 服務專屬的金鑰，您可以將 kms: ViaService 條件新增至該金鑰原則：

```
"Condition": {
  "StringEquals": {
    "kms:ViaService": "es.us-west-1.amazonaws.com"
  },
  "Bool": {
    "kms:GrantIsForAWSResource": "true"
  }
}
```

如需詳細資訊，請參閱使用金鑰原則 AWS KMS在 AWS Key Management Service 開發人員指南。

啟用靜態資料加密

新網域上的靜態資料加密需要或 Elasticsearch 5.1 OpenSearch 或更新版本。在現有網域上啟用此功能需要 OpenSearch 或彈性搜尋 6.7 或更新版本。

啟用靜態資料加密 (主控台)

1. 在中開啟網域 AWS 控制台，然後選擇「操作」 和 「編輯安全配置」
2. 在 Encryption (加密)，選擇 Enable encryption of data at rest (啟用靜態資料加密)。
3. 選擇一個 AWS KMS 鍵使用，然後選擇保存更改。

您也可以透過設定啟用加密API。下列請求會啟用現有網域上的靜態資料加密：

```
{
   "ClusterConfig":{
      "EncryptionAtRestOptions":{
         "Enabled": true,
         "KmsKeyId":"arn:aws:kms:us-east-1:123456789012:alias/my-key"
      }
   }
}
```

停用或刪除的KMS金鑰

如果您停用或刪除用來加密網域的金鑰，該網域就會變成無法存取。 OpenSearch 服務會傳送通知給您，通知您無法存取KMS金鑰。立即重新啟用金鑰以存取您的網域。

如果您的密鑰被刪除， OpenSearch 服務團隊將無法幫助您恢復數據。 AWS KMS 只會在至少七天的等待期間之後刪除金鑰。如果您的金鑰仍待刪除，請取消刪除或拍攝網域的手動快照，以避免資料損失。

停用靜態資料加密

在您設定網域以加密靜態資料後，您無法停用設定。相反地，您可以拍攝現有網域的手動快照，建立另一個網域，遷移您的資料和刪除舊的網域。

監控靜態加密資料的網域

加密靜態資料的網域有兩個額外的指標：`KMSKeyError` 和 `KMSKeyInaccessible`。如果網域遇到與您加密金鑰相關的問題，這些指標才會顯示。如需這些指標的完整說明，請參閱the section called “叢集指標”。您可以使用 OpenSearch 服務主控台或 Amazon CloudWatch 主控台來檢視它們。

> **Tip**
>
> 每個量度都代表網域的重大問題，因此我們建議您為兩者建立 CloudWatch 警示。如需詳細資訊，請參閱the section called “建議的 CloudWatch 鬧鐘”。

其他考量

- 自動按鍵旋轉保留您的屬性 AWS KMS 按鍵，因此旋轉對您訪問 OpenSearch 數據的能力沒有影響。加密的 OpenSearch 服務網域不支援手動金鑰輪換，這包括建立新金鑰和更新舊金鑰的任何參照。若要深入瞭解，請參閱中的旋轉按鍵 AWS Key Management Service 開發人員指南。
- 有些執行個體類型不支援靜態資料的加密。如需詳細資訊，請參閱 the section called “支援的執行個體類型”。
- 加密靜態資料的網域對於其自動快照使用不同的儲存庫名稱。如需詳細資訊，請參閱the section called “還原快照”。
- 雖然我們強烈建議您啟用靜態加密，但它可能會增加額外的CPU負荷和幾毫秒的延遲。不過，大多數使用案例對這些差異並不敏感，且影響程度取決於叢集、用户端和使用設定檔的組態。

Amazon OpenSearch 服務的 N ode-to-node 加密

N ode-to-node 加密除了 Amazon OpenSearch 服務的預設功能之外，還能提供額外的安全層。

每個 OpenSearch 服務網域 (無論網域是否使用VPC存取) 都位於其專屬的專用網域內。VPC此架構可防止潛在攻擊者攔截 OpenSearch 節點之間的流量，並確保叢集安全。但是，預設情況下，中的流量VPC是未加密的。N ode-to-node 加密啟用 TLS 1.2 加密內的所有通訊VPC。

如果您透過將資料傳送至 OpenSearch ServiceHTTPS， node-to-node 加密有助於確保您的資料保持加密狀態，因為資 OpenSearch 料會在整個叢集中散佈 (和再分配)。如果資料未加密到達HTTP，OpenSearch Service 會在資料到達叢集之後加密該資料。您可以要求HTTPS使用控制台到達域的所有流量， AWS CLI，或組態API。

如果您啟用精細的存取控制，則需要 N ode-to-node 加密。

啟用 node-to-node 加密

在新網域上進行 N ode-to-node 加密需要任何版本的 OpenSearch或彈性搜尋 6.0 或更新版本。在現有網域上啟用 node-to-node 加密需要任何版本的 OpenSearch或 Elasticsearch 6.7 或更新版本。選擇中的現有域 AWS 控制台，操作和編輯安全配置。

或者，您可以使用 AWS CLI 或配置API。如需詳細資訊，請參閱 AWS CLI 命令參考和OpenSearch 服務API參考。

停用 node-to-node 加密

將網域設定為使用 node-to-node 加密之後，就無法停用此設定。相反地，您可以拍攝加密網域的手動快照，建立另一個網域，遷移您的資料和刪除舊的網域。

Amazon OpenSearch 服務中的 Identity and Access Management

Amazon OpenSearch 服務提供了多種方法來控制對您的域的訪問。本主題涵蓋各種政策類型、它們如何彼此互動，以及如何建立自己的自訂政策。

> **Important**
>
> VPC支援為 OpenSearch 服務存取控制提供了一些額外的考量。如需詳細資訊，請參閱the section called “關於網VPC域的存取原則”。

政策的類型

OpenSearch 服務支援三種類型的存取原則：

- the section called “資源型政策”
- the section called “身分型政策”
- the section called “以 IP 為基礎的政策”

資源型政策

建立網域時，您可以新增以資源為基礎的政策 (通常稱為網域存取政策)。這些政策指定主體可以對域的子資源執行哪些操作 (跨叢集搜尋除外)。子資源包括 OpenSearch 索引和APIs. Principal 元素指定允許存取的帳戶、使用者或角色。Resource 元素指定這些委託人可以存取哪些子資源。

例如，以下以資源為基礎的政策向 `test-domain` 上的子資源授予 `test-user` 完整存取權 (`es:*`)：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "arn:aws:iam::123456789012:user/test-user"
        ]
      },
      "Action": [
        "es:*"
      ],
      "Resource": "arn:aws:es:us-west-1:987654321098:domain/test-domain/*"
    }
  ]
}
```

此政策適用兩個重要考量：

- 這些權限只適用於此網域。除非您在其他網域上建立類似的政策，否則 `test-user` 只能存取 `test-domain`。
- `Resource` 元素中的結尾 `/*` 很重要，並指出以資源為基礎的政策僅適用於網域的子資源，不適用於網域本身。在以資源為基礎的政策中，`es:*` 動作相當於 `es:ESHttp*`。

例如，test-user 可以提出索引請求 (GET https://search-test-domain.us-west-1.es.amazonaws.com/test-index)，但不能更新網域的組態 (POST https://es.us-west-1.amazonaws.com/2021-01-01/opensearch/domain/test-domain/config)。請注意兩個端點之間的差異。存取組態API需要以身分識別為基礎的原則。

您可以新增萬用字元來指定部分索引名稱。此範例可識別任何以 commerce 開頭的索引：

```
arn:aws:es:us-west-1:987654321098:domain/test-domain/commerce*
```

在此情況下，該萬用字元代表 test-user 可以向 test-domain 中名稱以 commerce 開頭的索引發出請求。

若要進一步限制 test-user，您可以套用以下政策：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "arn:aws:iam::123456789012:user/test-user"
        ]
      },
      "Action": [
        "es:ESHttpGet"
      ],
      "Resource": "arn:aws:es:us-west-1:987654321098:domain/test-domain/commerce-data/
_search"
    }
  ]
}
```

現在 test-user 可以執行一項操作：根據 commerce-data 搜尋。其他所有網域內的索引均無法存取，而且無使用 es:ESHttpPut 或 es:ESHttpPost 動作的許可，因此 test-user 無法新增或修改文件。

接著，您可能會決定設定進階使用者角色。此原則可讓您power-user-role存取索引URIs中所有項目的HTTPGET和PUT方法：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "arn:aws:iam::123456789012:role/power-user-role"
        ]
      },
      "Action": [
        "es:ESHttpGet",
        "es:ESHttpPut"
      ],
      "Resource": "arn:aws:es:us-west-1:987654321098:domain/test-domain/commerce-data/
*"
    }
  ]
}
```

如果您的網域處於VPC或使用精細的存取控制，您可以使用開放網域存取原則。否則，您的網域存取政策必須包含一些限制 (依委託人或 IP 地址)。

如需有關所有可行動作的詳細資訊，請參閱the section called “政策元素參考”。若要更精細地控制您的資料，請搭配使用開放網域存取政策與精細存取控制。

身分型政策

不同於以資源為基礎的原則 (屬於每個 OpenSearch Service 網域的一部分)，您可以使用 AWS Identity and Access Management () IAM 服務將以身分識別為基礎的原則附加至使用者或角色。就像以資源為基礎的政策一樣，以身分為基礎的政策會指定誰可以存取服務、可以執行哪些動作，以及可以在哪些資源執行那些動作 (如果適用)。

雖然他們不需要這麼做，但以身分為基礎的政策往往更加通用。它們通常只管理使用者可以執行的組態API動作。設定這些原則之後，您可以在 Service 中使用以資源為基礎的原則 (或精細的存取控制)，提 OpenSearch 供使用者存取 OpenSearch 索引和. APIs

> **Note**
>
> 具有 AWS 受管理`AmazonOpenSearchServiceReadOnlyAccess`原則的使用者無法在主控台上看到叢集健全狀況狀態。若要允許使用者查看叢集健康狀態 (和其他 OpenSearch 資料)，請將`es:ESHttpGet`動作新增至存取原則，並將其附加至其帳戶或角色。

由於以識別為基礎的原則會附加至使用者或角色 (主參與者)，因此JSON不會指定主參與者。下列政策授與動作存取權，該動作的開頭是 `Describe` 和 `List`。這組動作提供的唯讀存取權限用於網域組態，而非儲存在網域本身的資料：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "es:Describe*",
        "es:List*"
      ],
      "Effect": "Allow",
      "Resource": "*"
    }
  ]
}
```

管理員可能擁有 OpenSearch Service 的完整存取權，以及儲存在所有網域中的所有資料：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "es:*"
      ],
      "Effect": "Allow",
      "Resource": "*"
    }
  ]
}
```

以身分識別為基礎的原則可讓您使用標籤來控制組態的存取。API例如，如果網域具有 `team:devops` 標籤，下列政策可讓所連接的委託人檢視並更新網域的組態：

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Action": [
      "es:UpdateDomainConfig",
      "es:DescribeDomain",
      "es:DescribeDomainConfig"
    ],
    "Effect": "Allow",
    "Resource": "*",
    "Condition": {
      "ForAnyValue:StringEquals": {
        "aws:ResourceTag/team": [
          "devops"
        ]
      }
    }
  }]
}
```

您也可以使用標籤來控制對 OpenSearch API. 以標籤為基礎的原則 OpenSearch API僅適用於方HTTP法。例 OpenSearch API如，如果網域有`environment:production`標籤，下列原則可讓附加的主參GET與者傳送及PUT要求至：

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Action": [
      "es:ESHttpGet",
      "es:ESHttpPut"
    ],
    "Effect": "Allow",
    "Resource": "*",
    "Condition": {
      "ForAnyValue:StringEquals": {
        "aws:ResourceTag/environment": [
          "production"
        ]
      }
```

```
    }
  }]
}
```

如需更精細的控制 OpenSearch API，請考慮使用精細的存取控制。

> **Note**
>
> 將一或多個新增 OpenSearch APIs至任何以標籤為基礎的原則之後，您必須執行單一標籤作業(例如新增、移除或修改標籤)，變更才能在網域上生效。您必須使用服務軟體 R20211203 或更新版本，才能將 OpenSearch API作業納入標籤式原則中。

OpenSearch 服務支援組態的`RequestTag`和`TagKeys`全域條件索引鍵API，而不是 OpenSearch API. 這些條件僅適用於在要求中包含標籤的API呼叫`CreateDomain`，例如`AddTags`、和`RemoveTags`。下列政策可讓所連接的委託人建立網域，但前提是他們在請求中包含 `team:it` 標籤：

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": [
      "es:CreateDomain",
      "es:AddTags"
    ],
    "Resource": "*",
    "Condition": {
      "StringEquals": {
        "aws:RequestTag/team": [
          "it"
        ]
      }
    }
  }
}
```

有關使用標籤進行存取控制的詳細資訊，以及以資源為基礎和以身分識別為基礎的策略之間的差異，請參閱使用者指IAM南。

以 IP 為基礎的政策

IP 型原則會將網域的存取限制為一或多個 IP 位址或CIDR區塊。從技術層面來看，以 IP 為基礎的政策不是明確的政策類型。反而，其乃以資源為基礎的政策，負責指定匿名委託人並包含特殊的 Condition 元素。

IP 原則的主要吸引力在於它們允許對 OpenSearch Service 網域的未簽署要求，這可讓您使用 curl 和OpenSearch 儀表板等用戶端，或透過 Proxy 伺服器存取網域。如需進一步了解，請參閱 the section called “使用 Proxy 從 OpenSearch 儀表板存取 OpenSearch 服務”。

> **Note**
>
> 如果您已啟用網域的VPC存取權，則無法設定 IP 型原則。您反而可以使用安全群組來控制哪些 IP 地址可以存取網域。如需詳細資訊，請參閱the section called “關於網VPC域的存取原則”。

下列原則會授與源自指定 IP 範圍的所有HTTP要求存取`test-domain`權：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "*"
      },
      "Action": [
        "es:ESHttp*"
      ],
      "Condition": {
        "IpAddress": {
          "aws:SourceIp": [
            "192.0.2.0/24"
          ]
        }
      },
      "Resource": "arn:aws:es:us-west-1:987654321098:domain/test-domain/*"
    }
  ]
}
```

如果您的網域具有公用端點，且未使用精細的存取控制，建議您合併IAM主體和 IP 位址。只有當要求來自指定的 IP 範圍時，此原則才會授與`test-user`HTTP存取權：

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Principal": {
      "AWS": [
        "arn:aws:iam::987654321098:user/test-user"
      ]
    },
    "Action": [
      "es:ESHttp*"
    ],
    "Condition": {
      "IpAddress": {
        "aws:SourceIp": [
          "192.0.2.0/24"
        ]
      }
    },
    "Resource": "arn:aws:es:us-west-1:987654321098:domain/test-domain/*"
  }]
}
```

提出和簽署 OpenSearch 服務請求

即使您設定完全開放的以資源為基礎的存取原則，對 OpenSearch Service 組態的所有要求都API必須簽署。如果您的原則指定IAM角色或使用者，則對 OpenSearch APIs同時的要求必須使用 AWS 簽章版本 4 來簽署。簽署方法的不同之處在於API：

- 若要呼叫 OpenSearch 服務組態API，建議您使用 AWS SDKs. 與建立和簽署您自己的要求相比，可SDKs大幅簡化程序，並且可以節省大量時間。組態API端點使用下列格式：

  ```
  es.region.amazonaws.com/2021-01-01/
  ```

  例如，下列請求提出對 `movies` 網域進行組態變更，但是您必須自行登入 (不建議)：

  ```
  POST https://es.us-east-1.amazonaws.com/2021-01-01/opensearch/domain/movies/config
  {
  ```

```
  "ClusterConfig": {
    "InstanceType": "c5.xlarge.search"
  }
}
```

如果您使用其中一個SDKs，例如 Boto 3，則SDK會自動處理請求簽名：

```
import boto3

client = boto3.client(es)
response = client.update_domain_config(
  DomainName='movies',
  ClusterConfig={
    'InstanceType': 'c5.xlarge.search'
  }
)
```

如需 Java 程式碼範例，請參閱the section called “使用 AWS SDK”。

- 若要撥打電話 OpenSearch APIs，您必須簽署您自己的要求。使 OpenSearch APIs用以下格式：

```
domain-id.region.es.amazonaws.com
```

例如，以下請求將搜尋 thor 的 `movies` 索引：

```
GET https://my-domain.us-east-1.es.amazonaws.com/movies/_search?q=thor
```

> **Note**
>
> 對於使用簽名版本 4 簽署URLs的HTTPPOST請求，服務會忽略傳入的參數。

當政策衝突時

當與政策相違或未明確提及使用者時，事情就變得複雜了。瞭解IAM使用者指南中的IAM運作方式，提供原則評估邏輯的簡要摘要：

- 根據預設，所有的請求一律拒絕。
- 明確允許覆寫這個預設值。

- 明確拒絕覆寫任何允許。

例如，如果以資源為基礎的策略授與您存取網域子資源（OpenSearch 索引或API)，但以身分識別為基礎的策略拒絕您存取，則您將被拒絕存取。如果以身分為基礎的政策授與存取權，但以資源為基礎的政策未指定您是否有存取權，此時您便可以存取。請參閱下表的相交政策，以了解網域子資源的完整結果摘要。

	以資源為基礎的政策允許	以資源為基礎的政策拒絕	以資源為基礎的政策不允許也不拒絕
Allowed in identity-based policy	允許	拒絕	允許
Denied in identity-based policy	拒絕	拒絕	拒絕
Neither allowed nor denied in identity-based policy	允許	拒絕	拒絕

政策元素參考

OpenSearch 服務支援策略元素參考中的大多數IAM政策元素，但不包括`NotPrincipal`. 下表顯示最常見的元素。

JSON策略元素	Summary
`Version`	目前版本的政策語言是 `2012-10-17` 。所有存取政策應該指定這個值。
`Effect`	此元素指定公告內容是否允許或拒絕對指定動作的存取。有效值為 `Allow` 或 `Deny`。
`Principal`	此元素會指定允許 AWS 帳戶 或拒絕存取資源的或IAM角色或使用者，而且可以採用數種形式：

JSON策略元素	Summary
	• AWS 帳戶：`"Principal":{"AWS": ["123456789012"]}` 或 `"Principal":{"AWS": ["arn:aws:iam::123456789012:root"]}` • IAM使用者：`"Principal":{"AWS": ["arn:aws:iam::123456789012:user/test-user"]}` • IAM角色：`"Principal":{"AWS": ["arn:aws:iam::123456789012:role/test-role"]}` **Important** 指定*萬用字元可讓您匿名存取網域，除非您新增 IP 型條件、使用VPC支援或啟用精細的存取控制，否則我們不建議您這麼做。此外，請仔細檢查下列原則，以確認它們未授予廣泛存取權限： • 附加至關聯 AWS 主參與者 (例如，角色) 的識別型原則 IAM • 附加至關聯 AWS 資源的以資源為基礎的政策 (例如， AWS Key Management Service KMS金鑰)

JSON策略元素	Summary

Action	OpenSearch 服務使用 OpenSearch HTTP方法的ESHttp*動作。動作的其餘部分會套用至組態API。
	
	某些特定 es: 動作支援資源層級的許可。例如，您可以許可使用者刪除一個特定網域，而不是許可使用者刪除任何網域。其他動作只適用於服務本身。例如，es:ListDomainNames 在單一網域的內容細節中不具任何意義，因此需要萬用字元。
	
	如需所有可用動作的清單，以及它們是套用至網域子資源 (test-domain/*)、網域組態 (test-domain) 還是僅套用至服務 (*)，請參閱服務授權參考中的 Amazon OpenSearch 服務的動作、資源和條件金鑰
	以資源為基礎的政策不同於資源層級的許可。以資源為基礎的策略是附加到網域的完整JSON策略。資源層級許可則可讓您將動作限制到特定網域或子資源。在實務層面，您可以將資源層級許可當成選用之資源或身分為基礎的政策的一部分。
	
	由於 es:CreateDomain 的資源層級許可不是直覺式的 - 畢竟為何要許可使用者建立一個已經存在的網域？- 使用萬用字元可為您的網域強制執行簡單的命名機制，例如 "Resource": "arn:aws:es:us-west-1:987654321098:domain/my-team-name-*" 。
	
	當然，您有權利納入一些動作來搭配較無限制性的資源元素，如下所示：
	
	{
	"Version": "2012-10-17",
	"Statement": [
	{
	"Effect": "Allow",
	"Action": [
	"es:ESHttpGet",
	"es:DescribeDomain"
	],
	"Resource": "*"
	}
	]
	}

JSON策略元素	Summary
	若要進一步了解有關配對動作和資源的詳細資訊，請參閱此表格中的 `Resource` 元素。
`Condition`	OpenSearch Service 支援IAM使用者指南中AWS 全域條件前後關聯鍵字中所述的大多數條件。值得注意的例外包括`aws:PrincipalTag` 密鑰，該 OpenSearch 服務不支持。 設定 IP 型原則時，您可以將 IP 位址或CIDR封鎖指定為條件，如下所示： `"Condition": { "IpAddress": { "aws:SourceIp": [ "192.0.2.0/32" ] } }` 如中所述 the section called “身分型政策”`aws:ResourceTag` ，`aws:RequestTag` 、和`aws:TagKeys` 條件鍵適用於組態API以及 OpenSearch APIs。

JSON策略元素	Summary

`Resource`	OpenSearch 服務以三種基本方式使用`Resource`元素：
	
	• 對於適用於 OpenSearch 服務本身的操作`es:ListDomainNames`，例如或允許完全訪問權限，請使用以下語法：
	
	`"Resource": "*"`
	
	• 對於涉及網域組態的動作像是 `es:DescribeDomain`，您可以使用以下語法：
	
	`"Resource": "arn:aws:es: region:aws-account-id:domain/domain-name "`
	
	• 對於適用於網域子資源的動作像是 `es:ESHttpGet`，您可以使用以下語法：
	
	`"Resource": "arn:aws:es: region:aws-account-id:domain/domain-name /*"`
	
	您不必使用萬用字元。 OpenSearch 服務可讓您為每個 OpenSearch 索引或定義不同的存取原則API。例如，您可以限制使用者的 `test-index` 索引許可：
	
	`"Resource": "arn:aws:es: region:aws-account-id:domain/domain-name /test-index"`
	
	您可能希望將策略限制為僅搜索`test-index`，而不是完全訪問權限API：
	
	`"Resource": "arn:aws:es: region:aws-account-id:domain/domain-name /test-index/_search"`
	
	您甚至可以控制存取個別文件：
	
	`"Resource": "arn:aws:es: region:aws-account-id:domain/domain-name /test-index/test-type/1"`

JSON策略元素	Summary
	基本上，如果將子資源 OpenSearch 表示為URI，您可以使用存取原則控制對其的存取。如需更進一步控制使用者能夠存取的資源，請參閱 the section called “精細定義存取控制”。 如需有關哪些動作支援資源層級許可的詳細資訊，請參閱此表格中的 `Action` 元素。

進階選項與API考量

OpenSearch 服務有幾個高級選項，其中一個具有訪問控制的含義：`rest.action.multi.allow_explicit_index`。它的預設設定為 true，可讓使用者在特定情況下繞過子資源許可。

例如，請考量以下以資源為基礎的政策：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "arn:aws:iam::123456789012:user/test-user"
        ]
      },
      "Action": [
        "es:ESHttp*"
      ],
      "Resource": [
        "arn:aws:es:us-west-1:987654321098:domain/test-domain/test-index/*",
        "arn:aws:es:us-west-1:987654321098:domain/test-domain/_bulk"
      ]
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "arn:aws:iam::123456789012:user/test-user"
```

```
        ]
      },
      "Action": [
        "es:ESHttpGet"
      ],
      "Resource": "arn:aws:es:us-west-1:987654321098:domain/test-domain/restricted-
index/*"
    }
  ]
}
```

此原則會授`test-user`與 OpenSearch 大量的完整存取權限API。`test-index`它也允許 `GET` 請求 `restricted-index`。

以下索引請求因為許可錯誤而失敗：

```
PUT https://search-test-domain.us-west-1.es.amazonaws.com/restricted-index/movie/1
{
  "title": "Your Name",
  "director": "Makoto Shinkai",
  "year": "2016"
}
```

與索引不同API，批量API允許您在一次調用中創建，更新和刪除許多文檔。不過，您通常會在要求主體中指定這些作業，而不是在要求中URL。由於 OpenSearch Service 用URLs來控制對網域子資源的存取，因此事實上，`test-user`可以使用大量API變更網域子資源。`restricted-index`即使使用者缺少索引的 `POST` 許可，以下請求仍會成功：

```
POST https://search-test-domain.us-west-1.es.amazonaws.com/_bulk
{ "index" : { "_index": "restricted-index", "_type" : "movie", "_id" : "1" } }
{ "title": "Your Name", "director": "Makoto Shinkai", "year": "2016" }
```

在這種情況下，存取政策無法滿足其目的。為了防止使用者繞過這些類型的限制，您可以變更 `rest.action.multi.allow_explicit_index` 為 false。如果此值為 false，則在要求主體中指定索引名稱的大量、mget 和 msearch APIs 的所有呼叫都會停止運作。換言之，呼叫 `_bulk` 不再運作，但呼叫 `test-index/_bulk` 則正常運作。第二個端點包含索引名稱，因此您不需要在請求本文中指定一個。

OpenSearch 儀表板在很大程度上依賴 mget 和 msearch，因此在此更改後不太可能正常工作。對於部分補救，您可以保留`rest.action.multi.allow_explicit_index`為 true，並拒絕某些使用者存取一或多個這些補救措施APIs。

如需變更此設定的詳細資訊，請參閱the section called “進階叢集設定”。

同樣地，以下以資源為基礎的政策包含兩個細微問題：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::123456789012:user/test-user"
      },
      "Action": "es:ESHttp*",
      "Resource": "arn:aws:es:us-west-1:987654321098:domain/test-domain/*"
    },
    {
      "Effect": "Deny",
      "Principal": {
        "AWS": "arn:aws:iam::123456789012:user/test-user"
      },
      "Action": "es:ESHttp*",
      "Resource": "arn:aws:es:us-west-1:987654321098:domain/test-domain/restricted-
index/*"
    }
  ]
}
```

- 儘管明確拒絕，`test-user` 仍然可以呼叫如 `GET https://search-test-domain.us-west-1.es.amazonaws.com/_all/_search` 和 `GET https://search-test-domain.us-west-1.es.amazonaws.com/*/_search` 以存取 `restricted-index` 中的文件。
- 由於 `Resource` 元素參考 `restricted-index/*`，`test-user` 未獲許可來直接存取索引的文件。不過，使用者有權刪除整個索引。為防止存取和刪除，政策必須指定 `restricted-index*`。

不是廣泛允許和專注於拒絕，最安全的方法是遵循最小特權原則，只授與任務所需的許可。如需控制個別索引或 OpenSearch作業存取權的詳細資訊，請參閱the section called “精細定義存取控制”。

> **Important**
>
> 指定 * 萬用字元可讓您以匿名方式存取您的網域。不建議您使用萬用字元。此外，請仔細檢查下列原則，以確認它們未授與廣泛存取權：

- 附加至關聯 AWS 主參與者 (例如，角色) 的識別型原則 IAM
- 附加至關聯 AWS 資源的以資源為基礎的政策 (例如， AWS Key Management Service KMS 金鑰)

設定存取政策

- 如需在 OpenSearch Service 中建立或修改以資源為基礎的原則和 IP 原則的指示，請參閱。the section called “設定存取政策”
- 如需在中建立或修改以身分識別為基礎的策略的指示IAM，請參閱IAM使用指南中的建立IAM策略。

其他範例政策

雖然本章包含許多範例原則，但 AWS 存取控制是一個複雜的主題，最能透過範例瞭解。如需詳細資訊，請參閱《使用指南》中的以IAM身分識別為基礎IAM的範例

Amazon OpenSearch 服務API許可參考

設定存取控制時，您會撰寫可附加至身分識別的權限原則 (以IAM身分識別為基礎的原則)。如需詳細的參考資訊，請參閱《服務授權參考》中的下列主題：

- OpenSearch 服務的動作、資源和條件索引鍵。
- OpenSearch 擷取的動作、資源和條件索引鍵。

此參考資料包含IAM原則中可使用哪些API作業的相關資訊。它還包括您可以授與權限的 AWS 資源，以及可包含用於精細存取控制的條件金鑰。

您可以在政策的 `Action` 欄位中指定動作、在政策的 `Resource` 欄位中指定資源值，以及在政策的 `Condition` 欄位中指定條件。若要指定「 OpenSearch 服務」的動作，請使用`es:`前置詞，後面接著API作業名稱 (例如，`es:CreateDomain`)。若要指定 OpenSearch 擷取的動作，請使用`osis:`前置詞，後面接著API作業 (例如`osis:CreatePipeline`)。

AWS Amazon OpenSearch 服務的受管政策

受 AWS 管理的策略是由建立和管理的獨立策略 AWS。 AWS 受管理的策略旨在為許多常見使用案例提供權限，以便您可以開始將權限指派給使用者、群組和角色。

請記住， AWS 受管理的政策可能不會為您的特定使用案例授與最低權限權限，因為這些權限可供所有 AWS 客戶使用。我們建議您定義使用案例專屬的客戶管理政策，以便進一步減少許可。

您無法變更受 AWS 管理策略中定義的權限。如果 AWS 更新 AWS 受管理原則中定義的權限，則此更新會影響附加原則的所有主體識別 (使用者、群組和角色)。 AWS 當新的啟動或新API作業可供現有服務使 AWS 服務 用時，最有可能更新 AWS 受管理的策略。

如需詳細資訊，請參閱IAM使用指南中的AWS 受管理策略。

AmazonOpenSearchDirectQueryGlueCreateAccess

授予 Amazon OpenSearch 服務直接查詢服務對`CreateDatabase``CreatePartition``CreateTable`、和的存取權`BatchCreatePartition` AWS Glue API。

您可以在IAM控制台中找到AmazonOpenSearchDirectQueryGlueCreateAccess策略。

AmazonOpenSearchServiceFullAccess

授與的 OpenSearch 服務組態API作業和資源的完整存取權 AWS 帳戶。

您可以在IAM控制台中找到AmazonOpenSearchServiceFullAccess策略。

AmazonOpenSearchServiceReadOnlyAccess

授與 AWS 帳戶. OpenSearch

您可以在IAM控制台中找到AmazonOpenSearchServiceReadOnlyAccess策略。

AmazonOpenSearchServiceRolePolicy

您無法附加`AmazonOpenSearchServiceRolePolicy`至您的IAM實體。此原則附加至服務連結角色，可讓 OpenSearch Service 存取帳號資源。如需詳細資訊，請參閱the section called “許可”。

您可以在IAM控制台中找到AmazonOpenSearchServiceRolePolicy策略。

AmazonOpenSearchServiceCognitoAccess

提供啟用 Cognito 身分驗證所必需的最低 Amazon Cognito 許可。

您可以在IAM控制台中找到AmazonOpenSearchServiceCognitoAccess策略。

AmazonOpenSearchIngestionServiceRolePolicy

您無法附加`AmazonOpenSearchIngestionServiceRolePolicy`至您的IAM實體。此原則附加至服務連結角色，可讓 OpenSearch Intection 啟用擷取管道的VPC存取權、建立標記，以及將擷取相 CloudWatch 關指標發佈至您的帳戶。如需詳細資訊，請參閱the section called “使用服務連結角色”。

您可以在IAM控制台中找到AmazonOpenSearchIngestionServiceRolePolicy策略。

OpenSearchIngestionSelfManagedVpcePolicy

您無法附加`OpenSearchIngestionSelfManagedVpcePolicy`至您的IAM實體。此原則附加至服務連結角色，該角色允許 OpenSearch Intection 為擷取管道啟用自我管理VPC存取、建立標記，以及將擷取相關指標發佈到您的帳戶。 CloudWatch 如需詳細資訊，請參閱the section called “使用服務連結角色”。

您可以在IAM控制台中找到OpenSearchIngestionSelfManagedVpcePolicy策略。

AmazonOpenSearchIngestionFullAccess

授與的 OpenSearch 擷取API作業和資源的完整存取權。 AWS 帳戶

您可以在IAM控制台中找到AmazonOpenSearchIngestionFullAccess策略。

AmazonOpenSearchIngestionReadOnlyAccess

授與 OpenSearch . AWS 帳戶

您可以在IAM控制台中找到AmazonOpenSearchIngestionReadOnlyAccess策略。

AmazonOpenSearchServerlessServiceRolePolicy

提供傳送 OpenSearch 無伺服器測量結果資料至所需的最低 Amazon CloudWatch 權限。 CloudWatch

您可以在IAM控制台中找到AmazonOpenSearchServerlessServiceRolePolicy策略。

OpenSearch AWS 受管理策略的服務更新

檢視自此服務開始追蹤變更以來， OpenSearch 服務 AWS 受管理原則的更新詳細資料。

變更	描述	日期
已更新 `AmazonOpenSearchServerlessServiceRolePolicy`	已將 Sid 新增`AllowAOSSCloudwatchMetrics` 至原則`AmazonOpenSearchServerlessServiceRolePolicy` 。Sid 是一個陳述式識別碼，可做為原則陳述式的選擇性識別碼。	2024 年七月十二日
已新增 `OpenSearchIngestionSelfManagedVpcePolicy`	一項新政策，允許 OpenSearch Intection 為擷取管道啟用自我管理VPC存取、建立標記，以及將擷取相關 CloudWatch 指標發佈到您的帳戶。 有關策略JSON，請參閱控IAM制台。	2024 年六月十二日
已新增 `AmazonOpenSearchDirectQueryGlueCreateAccess`	授予 Amazon OpenSearch 服務直接查詢服務對`CreateDatabase` `CreatePartition` `CreateTable` 、和的存取權`BatchCreatePartition` AWS Glue API。	2024 年五月六日
更新 `AmazonOpenSearchServiceRolePolicy` 和 `AmazonElasticsearchServiceRolePolicy`	已新增服務連結角色指派和取IPv6消指派位址所需的權限。 已取代的 Elasticsearch 政策也已更新，以確保向後相容性。	2023 年 10 月 18 日

變更	描述	日期
已新增 `AmazonOpenSearchIngestionServiceRolePolicy`	一項新政策，可讓 OpenSearch 擷VPC取啟用擷取管道的存取權、建立標記，以及將擷取相關 CloudWatch 指標發佈到您的帳戶。 有關策略JSON，請參閱控IAM制台。	2023 年四月二十六日
已新增 `AmazonOpenSearchIngestionFullAccess`	一種新政策， OpenSearch 可API授與. AWS 帳戶 有關策略JSON，請參閱控IAM制台。	2023 年四月二十六日
已新增 `AmazonOpenSearchIngestionReadOnlyAccess`	一種新政策，授與. OpenSearch AWS 帳戶 有關策略JSON，請參閱控IAM制台。	2023 年四月二十六日
已新增 `AmazonOpenSearchServerlessServiceRolePolicy`	提供將 OpenSearch 無伺服器測量結果資料傳送至的最低權限的新原則。 Amazon CloudWatch 有關策略JSON，請參閱控IAM制台。	2022 年 11 月 29 日

變更	描述	日期
更新 `AmazonOpenSearchServiceRolePolicy` 和 `AmazonElasticsearchServiceRolePolicy`	已新增服務連結角色建立服OpenSearch 務管理端VPC點所需的權限。某些動作只能在請求包含標籤 `OpenSearchManaged=true` 時執行。 已取代的 Elasticsearch 政策也已更新，以確保向後相容性。	2022 年 11 月 7 日
更新 `AmazonOpenSearchServiceRolePolicy` 和 `AmazonElasticsearchServiceRolePolicy`	增加了對該`PutMetricData` 操作的支持，這是將 OpenSearch 群集指標發佈到 Amazon 所需的 CloudWatch。 已取代的 Elasticsearch 政策也已更新，以確保向後相容性。 有關策略JSON，請參閱控IAM制台。	2022 年 9 月 12 日
更新 `AmazonOpenSearchServiceRolePolicy` 和 `AmazonElasticsearchServiceRolePolicy`	新增對 `acm` 資源類型的支援。此策略提供服務連結角色所需的最低 AWS Certificate Manager (ACM) 唯讀權限，以驗證和驗證ACM資源，以便建立和更新已啟用自訂端點的網域。 已取代的 Elasticsearch 政策也已更新，以確保向後相容性。	2022 年 7 月 28 日

變更	描述	日期
更新 `AmazonOpenSearchServiceCognitoAccess` 和 `AmazonESCognitoAccess`	已新增對`UpdateUserPoolClient` 動作的支援，這是在從 Elasticsearch 升級至期間設定 Cognito 使用者集區組態所需的動作。OpenSearch 更正 `SetIdentityPoolRoles` 動作的許可，允許對所有資源的存取。 已取代的 Elasticsearch 政策也已更新，以確保向後相容性。	2021 年 12 月 20 日
已更新 `AmazonOpenSearchServiceRolePolicy`	新增對 `security-group` 資源類型的支援。該政策為服務連結角色提供啟用VPC存取所需的最低 Amazon EC2 和 Elastic Load Balancing 許可。	2021 年 9 月 9 日
• 已新增 `AmazonOpenSearchServiceFullAccess` • 已取代 `AmazonESFullAccess`	這項新政策旨在取代舊政策。這兩個原則都提供對 OpenSearch Service 組態的完整存取權，以API及 OpenSearch APIs. HTTP 精細存取控制和以資源為基礎的政策仍然可以限制存取。	2021 年 9 月 7 日

變更	描述	日期
• 已新增 `AmazonOpenSearchServiceReadOnlyAccess` • 已取代 `AmazonESReadOnlyAccess`	這項新政策旨在取代舊政策。這兩個原則都提供 Ser OpenSearch vice 組態 API (`es:Describe* es:List*`、和`es:Get*`) 的唯讀存取權，而且無HTTP法存取 OpenSearch APIs.	2021 年 9 月 7 日
• 已新增 `AmazonOpenSearchServiceCognitoAccess` • 已取代 `AmazonESCognitoAccess`	這項新政策旨在取代舊政策。這兩個政策提供啟用 Cognito 身分驗證所必需的最低 Amazon Cognito 許可。	2021 年 9 月 7 日
• 已新增 AmazonOpenSearchServiceRolePolicy • 已取代 `AmazonElasticsearchServiceRolePolicy`	這項新政策旨在取代舊政策。這兩個政策都提供服務連結角色啟用VPC存取所需的最低 Amazon EC2 和 Elastic Load Balancing 許可。	2021 年 9 月 7 日
開始追蹤變更	Amazon OpenSearch 服務現在會追蹤 AWS受管政策的變更。	2021 年 9 月 7 日

預防跨服務混淆代理人

混淆代理人問題屬於安全性議題，其中沒有執行動作許可的實體可以強制具有更多許可的實體執行該動作。在 AWS 中，跨服務模擬可能會導致混淆代理人問題。在某個服務 (呼叫服務) 呼叫另一個服務 (被呼叫服務) 時，可能會發生跨服務模擬。可以操縱呼叫服務來使用其許可，以其不應有存取許可的方式對其他客戶的資源採取動作。為了預防這種情況，AWS 提供的工具可協助您保護所有服務的資料，而這些服務主體已獲得您帳戶中資源的存取權。

若要限制 Amazon OpenSearch Service 為資源提供另一項服務的許可，我們推薦在資源政策中使用 `aws:SourceArn` 和 `aws:SourceAccount` 全域條件內容索引鍵。如果 `aws:SourceArn` 值不包含

帳戶 ID (例如 Simple Storage Service (Amazon S3) 儲存貯體 ARN)，您必須使用這兩個全域條件內容索引鍵來限制許可。如果同時使用這兩個全域條件內容索引鍵，且 `aws:SourceArn` 值包含帳戶 ID，則在相同政策陳述式中使用 `aws:SourceAccount` 值和 `aws:SourceArn` 值中的帳戶時，必須使用相同的帳戶 ID。如果您想要僅允許一個資源與跨服務存取相關聯，則請使用 `aws:SourceArn`。如果您想要允許該帳戶中的任何資源與跨服務使用相關聯，則請使用 `aws:SourceAccount`。

`aws:SourceArn` 的值必須是 OpenSearch Service 網域的 ARN。

防範混淆代理人問題最有效的方法，是使用 `aws:SourceArn` 全域條件內容金鑰，以及資源的完整 ARN。如果不知道資源的完整 ARN，或者如果您指定了多個資源，請使用 `aws:SourceArn` 全域條件內容金鑰，同時使用萬用字元 (*) 表示 ARN 的未知部分。例如： 。`arn:aws:es:*:123456789012:*`

下列範例示範如何使用 OpenSearch Service 中的 `aws:SourceArn` 和 `aws:SourceAccount` 全域條件內容金鑰，來預防混淆代理人問題。

```
{
   "Version":"2012-10-17",
   "Statement":{
      "Sid":"ConfusedDeputyPreventionExamplePolicy",
      "Effect":"Allow",
      "Principal":{
         "Service":"es.amazonaws.com"
      },
      "Action":"sts:AssumeRole",
      "Condition":{
         "StringEquals":{
            "aws:SourceAccount":"123456789012"
         },
         "ArnLike":{
            "aws:SourceArn":"arn:aws:es:region:123456789012:domain/my-domain"
         }
      }
   }
}
```

Amazon OpenSearch 服務中的精細訪問控制

精細的存取控制提供了控制 Amazon OpenSearch 服務上資料存取的其他方式。例如，根據提出請求的人員，您可能會希望搜尋只傳回一個索引的結果。您可能會希望隱藏文件中的某些欄位，或是排除特定的文件。

精細存取控制具有以下優勢：

- 角色類型存取控制
- 索引、文件和欄位層級的安全
- OpenSearch 多租戶儀表板
- OpenSearch 和 OpenSearch 儀表板的 HTTP 基本驗證

主題

- 更大的局面：精細的訪問控制和 OpenSearch 服務安全
- 重要概念
- 關於主要使用者
- 啟用精細存取控制
- 以主要使用者身分存取 OpenSearch 儀表板
- 管理許可
- 建議的組態
- 限制
- 修改主要使用者
- 其他主要使用者
- 手動快照
- 整合
- REST API 差異
- 教學課程：使用 IAM 主要使用者和 Amazon Cognito 身分驗證設定網域
- 教學課程：使用內部使用者資料庫和 HTTP 基本身分驗證設定網域

更大的局面：精細的訪問控制和 OpenSearch 服務安全

Amazon OpenSearch 服務安全有三個主要層面：

網路

第一個安全層是網路，它決定要求是否到達 OpenSearch Service 網域。如果您在建立網域時選擇 Public access (公有存取)，則來自任何網際網路連線用戶端的請求都能連線到網域端點。如果您選

擇 VPC access (VPC 存取)，用戶端必須連線至 VPC (且相關聯的安全群組也必須允許)，請求才能連線到端點。如需詳細資訊，請參閱 the section called “VPC支持”。

網域存取政策

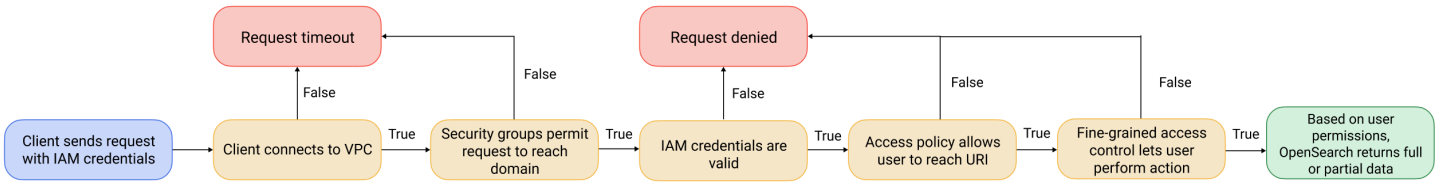
第二個安全層次是網域存取政策。在請求連線到網域端點後，資源類型存取政策會允許或拒絕對指定 URI 的請求存取。存取原則會在網域的「邊緣」處接受或拒絕要求，然後再到達 OpenSearch本身。

精細定義存取控制

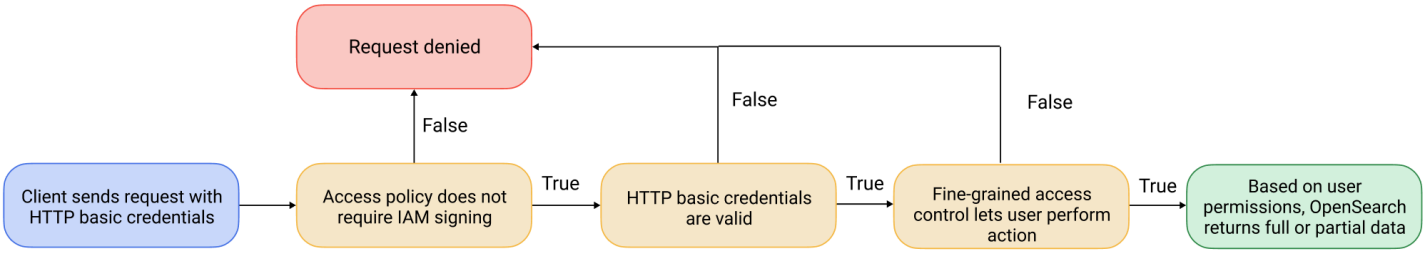
第三個和最後一個安全層次是精細存取控制。在資源類型存取政策允許請求連線到網域端點後，精細存取控制會評估使用者登入資料，並讓使用者通過身分驗證或拒絕請求。如果精細存取控制讓使用者通過身分驗證，則會擷取所有映射到該使用者的角色，並使用完整的許可集合來判斷如何處理請求。

> **Note**
>
> 如果以資源為基礎的存取政策包含 IAM 角色或使用者，用戶端必須使用簽 AWS 名版本 4 傳送已簽署的請求。因此，存取政策可能會和精細存取控制產生衝突，特別是當您使用內部使用者資料庫和 HTTP 基本身分驗證時。您無法使用使用者名稱和密碼以及 IAM 登入資料來簽署請求。一般而言，如果您啟用了精細存取控制，我們建議您使用不需要簽章請求的網域存取政策。

下圖說明了常見的組態：啟用精細存取控制的 VPC 存取網域、IAM 型的存取政策以及 IAM 主要使用者。



下圖說明了另一種常見的組態：啟用精細存取控制的公有存取網域，不使用 IAM 委託人的存取政策，以及內部使用者資料庫中的主要使用者。



範例

假設有一個對 `movies/_search?q=thor` 提出的 GET 請求。使用者具備搜尋 `movies` 索引的許可嗎？ 如果具備的話，使用者是否具備查看其中所有文件的許可？ 回應應該要省略或匿名化任何欄位嗎？ 針對主要使用者，回應看起來可能如下：

```
{
  "hits": {
    "total": 7,
    "max_score": 8.772789,
    "hits": [{
        "_index": "movies",
        "_type": "_doc",
        "_id": "tt0800369",
        "_score": 8.772789,
        "_source": {
          "directors": [
            "Kenneth Branagh",
            "Joss Whedon"
          ],
          "release_date": "2011-04-21T00:00:00Z",
          "genres": [
            "Action",
            "Adventure",
            "Fantasy"
          ],
          "plot": "The powerful but arrogant god Thor is cast out of Asgard to
 live amongst humans in Midgard (Earth), where he soon becomes one of their finest
 defenders.",
          "title": "Thor",
          "actors": [
            "Chris Hemsworth",
            "Anthony Hopkins",
            "Natalie Portman"
          ],
```

```
          "year": 2011
        }
      },
      ...
    ]
  }
}
```

如果具備受限性較高許可的使用者提出了完全相同的請求，則回應看起來可能會如下：

```
{
  "hits": {
    "total": 2,
    "max_score": 8.772789,
    "hits": [{
        "_index": "movies",
        "_type": "_doc",
        "_id": "tt0800369",
        "_score": 8.772789,
        "_source": {
          "year": 2011,
          "release_date":
 "3812a72c6dd23eef3c750c2d99e205cbd260389461e19d610406847397ecb357",
          "plot": "The powerful but arrogant god Thor is cast out of Asgard to
 live amongst humans in Midgard (Earth), where he soon becomes one of their finest
 defenders.",
          "title": "Thor"
        }
      },
      ...
    ]
  }
}
```

回應的命中數會較少，且每個命中的欄位數也會比較少。此外，`release_date` 欄位會進行匿名化。如果沒有具備任何許可的使用者提出相同的請求，則叢集會傳回錯誤：

```
{
  "error": {
    "root_cause": [{
      "type": "security_exception",
      "reason": "no permissions for [indices:data/read/search] and User [name=limited-
user, roles=[], requestedTenant=null]"
```

```
    }],
    "type": "security_exception",
    "reason": "no permissions for [indices:data/read/search] and User [name=limited-
user, roles=[], requestedTenant=null]"
  },
  "status": 403
}
```

如果使用者提供了無效的登入資料，則叢集會傳回 `Unauthorized` 例外狀況。

重要概念

當您開始使用精細的存取控制時，請考慮下列概念：

- 角色 — 使用精細存取控制的核心方式。在這種情況下，角色與 IAM 角色不同。角色包含了任何許可的組合：全叢集、特定索引、文件層級，以及欄位層級。
- 「映射」— 配置角色后，您可以將其映射到一個或多個用戶。例如，您可以將三個角色映射到單一使用者：其中一個角色提供存取給 Dashboards，第二個角色提供唯讀存取給 `index1`，第三個角色則提供寫入存取給 `index2`。或者，您可以在單一角色中包含這些許可。
- 使用者 — 對 OpenSearch 叢集發出要求的人員或應用程式。使用者擁有在提出請求時指定的登入資料 (IAM 存取金鑰或使用者名稱和密碼)。

關於主要使用者

OpenSearch 服務中的主要使用者可以是使用者名稱和密碼組合，或是 IAM 主體，具有基礎 OpenSearch叢集的完整許可。如果使用者具有 OpenSearch 叢集的所有存取權，並且能夠在 OpenSearch 儀表板中建立內部使用者、角色和角色對應，則該使用者將被視為主要使用者。

在 OpenSearch Service 主控台或透過 CLI 建立的主要使用者會自動對應至兩個預先定義的角色：

- `all_access`— 提供對所有叢集範圍作業的完整存取權、寫入所有叢集索引的權限，以及寫入所有租用戶的權限。
- `security_manager`— 提供對安全插件的訪問以及對用戶和權限的管理。

透過這兩個角色，使用者可以存取 OpenSearch 儀表板中的 [安全性] 索引標籤，在此他們可以管理使用者和權限。如果您建立另一個內部使用者，並且僅將其對應至`all_access`角色，則該使用者無法存取 [安全性] 索引標籤。您可以透過將主要使用者明確對應至`all_access`和`security_manager`角色來建立其他主要使用者。如需說明，請參閱the section called “其他主要使用者”。

當您為網域建立主要使用者時，可以指定現有的 IAM 主體，或在內部使用者資料庫中建立主要使用者。決定要使用哪一個時，請考慮下列事項：

- IAM 主體 — 如果您為主要使用者選擇 IAM 主體，則對叢集的所有請求都必須使用 AWS 簽名版本 4 簽署。

  OpenSearch 服務不會考慮任何 IAM 主體的許可。IAM 使用者或角色純粹用於驗證。該使用者或角色的策略與主要使用者的授權無關。授權是透過 OpenSearch 安全性外掛程式中的各種權限來處理。

  例如，您可以為 IAM 主體指派零 IAM 許可，而且只要機器或人員可以向該使用者或角色進行驗證，他們就可以在 OpenSearch 服務中擁有主要使用者的能力。

  如果您想要在多個叢集上使用相同的使用者、想要使用 Amazon Cognito 存取儀表板，或者您的用 OpenSearch 戶端支援簽名版本 4 簽署，我們建議您使用 IAM。
- 內部使用者資料庫 — 如果您在內部使用者資料庫中建立 master (使用者名稱和密碼組合)，則可以使用 HTTP 基本身份驗證 (以及 IAM 登入資料) 向叢集發出請求。大多數客戶端支持基本身份驗證，包括 curl，它還支持帶有 ---aw s-sigv4 選項的 AWS 簽名版本 4。內部使用者資料庫儲存在 OpenSearch 索引中，因此您無法與其他叢集共用。

  如果您不需要跨多個叢集重複使用使用者、希望使用 HTTP 基本身分驗證來存取 Dashboards (而非 Amazon Cognito)，或是您具備只支援基本身分驗證的用戶端，則我們建議您使用內部使用者資料庫。內部使用者資料庫是開始使用 OpenSearch Service 的最簡單方式。

啟用精細存取控制

使用主控台或設定 API 啟用精細的存取控制。 AWS CLI如需這些步驟，請參閱 建立和管理網域。

精細的訪問控制需要 OpenSearch 或彈性搜索 6.7 或更高版本。它還需要 HTTPS 才能進入域的所有流量，靜態數據node-to-node 加密和加密。視您設定精細存取控制進階功能的方式而定，對要求進行額外處理可能需要個別資料節點上的運算和記憶體資源。在您啟用精細存取控制後，您便無法停用此功能。

在現有網域上啟用精細存取控制

您可以對執行中的現有網域 OpenSearch 或 Elasticsearch 6.7 或更新版本啟用精細的存取控制。

在現有網域上啟用精細存取控制 (主控台)

1. 選取網域，並選擇 Actions (動作) 和 Edit security configuration (編輯安全組態)。

2. 選取 Enable fine-grained access control (啟用精細存取控制)。
3. 選擇建立主要使用者的方法：
   - 如果您希望使用 IAM 進行使用者管理，請選擇 Set IAM ARN as master user (將 IAM ARN 設為主要使用者)，並指定 IAM 角色的 ARN。
   - 如果您要使用內部使用者資料庫，請選擇 [建立主要使用者]，然後指定使用者名稱和密碼。
4. (選用) 選取 Enable migration period for open/IP-based access policy (啟用開放/IP 型存取政策的遷移期)。此設定會啟用 30 天的過渡期，在此期間，您目前的使用者可繼續存取網域，不會中斷，且現有的開放和 IP 型存取政策仍可繼續使用您的網域。在此遷移期間，我們建議管理員為網域建立必要角色，並將其映射至使用者。如果您使用以身分為基礎的政策，而非開放或 IP 型存取政策，則您可以停用此設定。

   您也需要更新客戶端，以在遷移期間使用精細存取控制。例如，如果您使用精細的存取控制對應 IAM 角色，則必須更新用戶端以開始使用簽 AWS 名版本 4 簽署請求。如果您使用精細存取控制設定 HTTP 基本身分驗證，則必須更新客戶端，以在請求中提供適當的基本身分驗證憑證。

   在移轉期間，存取網域之 OpenSearch 儀表板端點的使用者將直接登入「探索」頁面，而不是登入頁面。管理員和主要使用者可選擇 Login (登入)，使用管理員憑據登入並設定角色映射。

   > **Important**
   >
   > OpenSearch 服務會在 30 天後自動停用遷移期間。我們建議您在建立必要角色並將其映射至使用者後，立即結束該角色。遷移期結束後，您便無法重新啟用。

5. 選擇儲存變更。

在叢集運作狀態變成紅色期間，變更會觸發藍/綠部署，但所有叢集操作皆不受影響。

在現有網域上啟用精細存取控制 (CLI)

將 `AnonymousAuthEnabled` 設定為 `true`，以使用精細存取控制來啟用遷移期：

```
aws opensearch update-domain-config --domain-name test-domain --region us-east-1 \
      --advanced-security-options '{ "Enabled": true,
 "InternalUserDatabaseEnabled":true, "MasterUserOptions": {"MasterUserName":"master-
username","MasterUserPassword":"master-password"},"AnonymousAuthEnabled": true}'
```

關於 default_role

精細存取控制需要角色映射。如果您的網域使用以身分識別為基礎的存取原則， OpenSearch Service 會自動將您的使用者對應至名為 default_role 的新角色，以協助您正確移轉現有使用者。在您建立自有角色映射之前，此臨時映射可確保您的使用者仍可成功傳送由 IAM 簽署之 GET 和 PUT 請求。

此角色不會在您的 OpenSearch Service 網域中新增任何安全性弱點或瑕疵。我們建議您在設定自有角色後並相應映射它們後，立即刪除預設角色。

遷移案例

下表說明在現有網域上啟用精細存取控制前後的各身分驗證方法的行為，以及若管理員要將其使用者正確映射至角色，必須採取的步驟：

身分驗證方法	在啟用精細存取控制前	在啟用精細存取控制後	管理員任務
以身分為基礎的政策	滿足 IAM 政策的所有使用者都可以存取該網域。	您無需啟用遷移期。 OpenSearch 服務會自動將符合 IAM 政策的所有使用者對應到 default_role，以便他們可以繼續存取網域。	1. 在網域上建立自訂角色映射。 2. 刪除 default_role。
以 IP 為基礎的政策	來自受允許 IP 地址或 CIDR 區塊的所有使用者皆可存取網域。	在 30 天遷移期內，所有來自受允許 IP 地址或 CIDR 區塊的使用者都可繼續存取網域。	1. 在網域上建立自訂角色映射。 2. 依據您的角色映射組態，更新您的客戶端以提供基本身分驗證憑證或 IAM 憑證。 3. 停用遷移期。若來自受允許的 IP 地址或 CIDR 區塊的使用者，在沒有基本身分驗證或 IAM 憑證的情況下傳送請求，將失去網域的存取權限。
開放存取政策	網際網路上的所有使用者皆可存取網域。	在 30 天的遷移期內，網際網路上的所有使用者皆可繼續存取網域。	1. 在網域上建立角色映射。 2. 依據您的角色映射組態，更新您的客戶端以提供基本身分驗證憑證或 IAM 憑證。

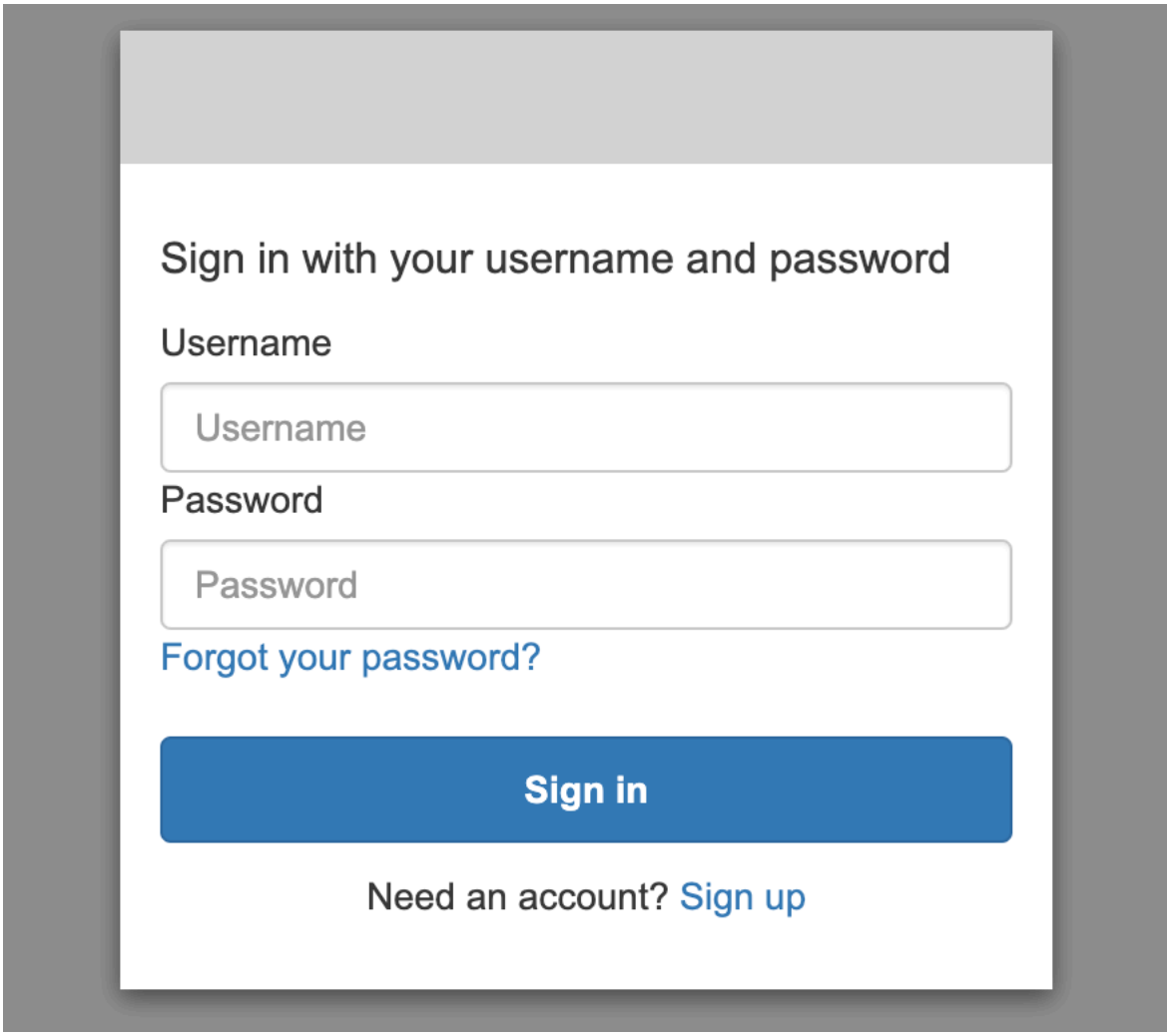
身分驗證方法	在啟用精細存取控制前	在啟用精細存取控制後	管理員任務
			3. 停用遷移期。使用者在沒有基本身分驗證或 IAM 憑證的情況下傳送請求，將失去網域的存取權限。

以主要使用者身分存取 OpenSearch 儀表板

精細的存取控制具有可簡化管理工作的 OpenSearch 儀表板外掛程式。您可以使用 Dashboards 來管理使用者、角色、映射、動作群組和租用戶。但是， OpenSearch 儀表板登入頁面和基礎驗證方法會有所不同，視您管理使用者和設定網域的方式而定。

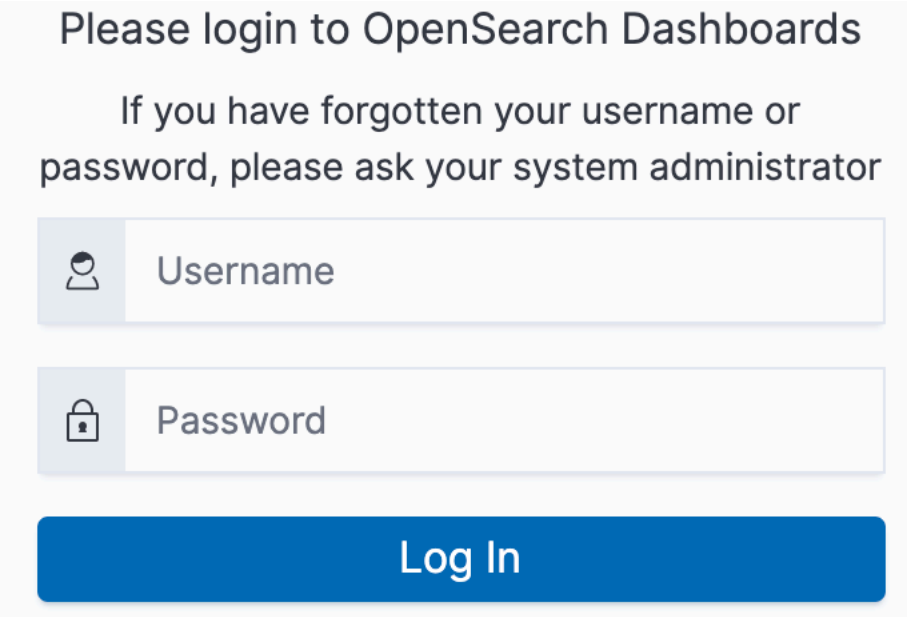
- 如果您想使用 IAM 進行使用者管理，請使用 the section called “用於儀表板的 Amazon Cognito 份 OpenSearch ” 來存取 Dashboards。否則，Dashboards 會顯示沒有任何功能的登入頁面。請參閱the section called “限制”。

  透過 Amazon Cognito 身分驗證，擔任的身分集區中的其中一個角色必須與您為主要使用者指定的 IAM 角色相符。如需此組態的詳細資訊，請參閱 the section called “(選用) 設定精細分級的存取” 和 the section called “教學課程：使用 Cognito 身分驗證進行精細存取控制”。



- 如果您選擇使用內部使用者資料庫，您可以使用主要使用者名稱和密碼登入儀表板。您必須透過 HTTPS 存取 Dashboards。適用於 Dashboards 的 Amazon Cognito 和 SAML 身分驗證都會取代此登入畫面。

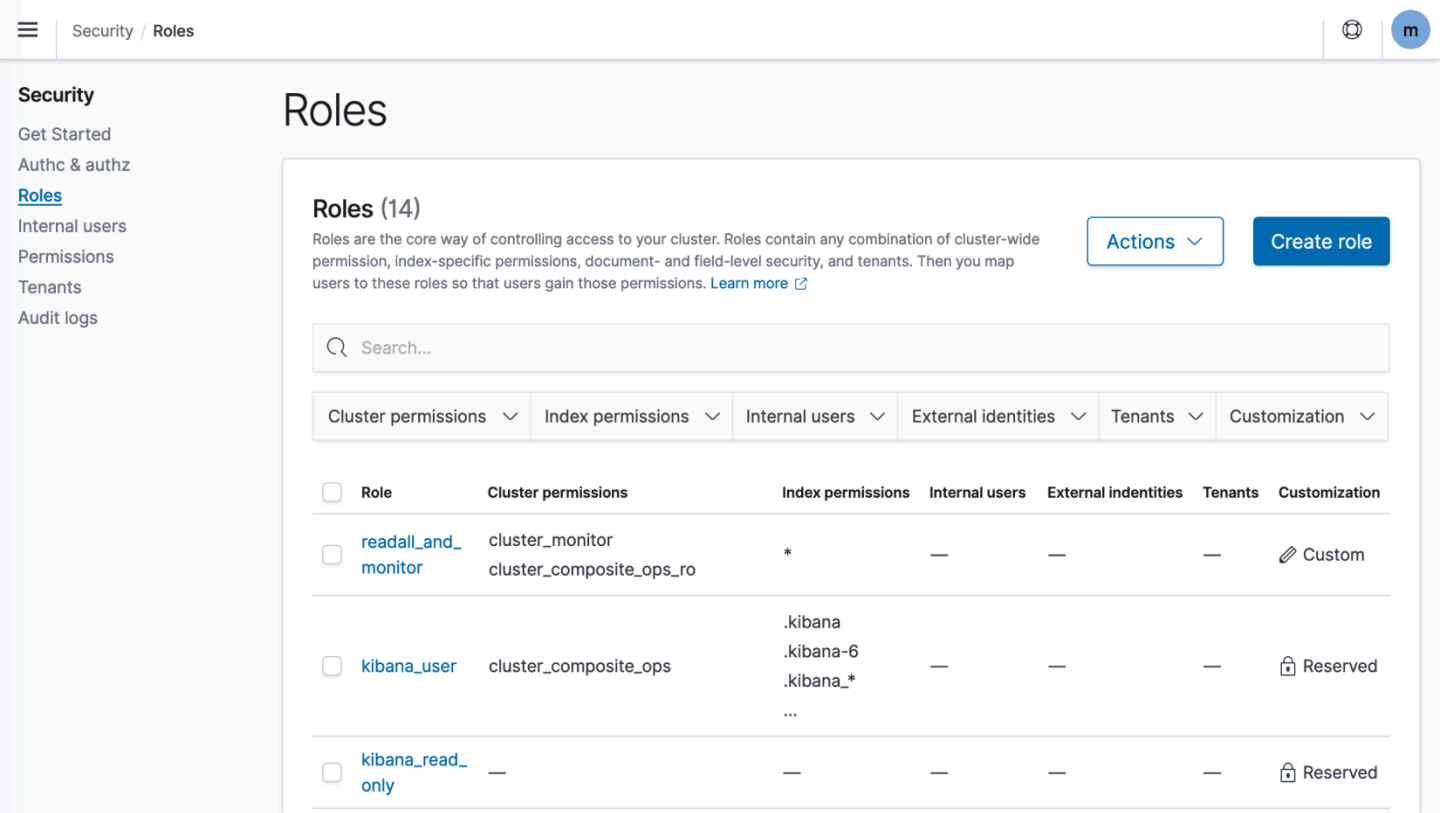
  如需此組態的詳細資訊，請參閱「the section called “教學課程：內部使用者資料庫和基本身分驗證”」。



- 如果您選擇使用 SAML 身分驗證，您可以使用外部身分提供者的憑證登入。如需詳細資訊，請參閱 the section called “SAML OpenSearch 儀表板的驗證”。

管理許可

如 the section called “重要概念” 中所述，您可以使用角色、使用者和映射來管理精細存取控制許可。本節說明如何建立和套用這些資源。我們建議您以主要使用者身分登入 Dashboards，以執行這些操作。



> **Note**
>
> 您選擇授予使用者的許可，根據使用案例有很大差異。我們無法在本文中涵蓋所有案例。當您決定要授與使用者的權限時，請務必參考下列各節中提到的 OpenSearch 叢集和索引權限，並始終遵循最低權限原則。

建立角色

您可以使用 OpenSearch 儀表板或 REST API 中的`_plugins/_security`操作來建立新角色，以進行精細的存取控制。如需詳細資訊，請參閱建立角色。

精細存取控制也包含了許多預先定義角色。 OpenSearch 儀表板和 Logstash 等用戶端會向各種各樣的要求發出 OpenSearch，這可能會讓您難以手動建立具有最低權限集的角色。例如，`opensearch_dashboards_user` 角色包含了使用者使用索引模式、視覺化及儀表板和租用戶所需要的許可。我們建議將其映射至存取 Dashboards 的任何使用者或後端角色，以及允許存取其他索引的其他角色。

Amazon OpenSearch 服務不提供以下 OpenSearch 角色：

- observability_full_access
- observability_read_access
- reports_read_access
- reports_full_access

Amazon OpenSearch 服務提供了幾個角色，這些角色不適用於 OpenSearch：

- ultrawarm_manager
- ml_full_access
- cold_manager
- notifications_full_access
- notifications_read_access

叢集層級安全

叢集層級許可包括能夠發出廣泛請求 (例如 _mget、_msearch 以及 _bulk)、監控運作狀態、擷取快照等。請在建立角色時使用 Cluster Permissions (叢集許可) 部分來管理這些許可。如需完整的叢集層級許可清單，請參閱叢集許可。

您通常可以使用預設動作群組組合，而不是個別許可，達到所需的安全狀態。如需叢集層級動作群組的清單，請參閱叢集層級。

索引層級安全

索引層級許可包含建立新索引、搜尋索引、讀取和寫入文件、刪除文件、管理別名等能力。請在建立角色時使用 Index Permissions (索引許可) 部分來管理這些許可。如需完整的索引層級許可清單，請參閱索引許可。

您通常可以使用預設動作群組組合，而不是個別許可，達到所需的安全狀態。如需索引層級動作群組的清單，請參閱索引層級。

文件層級安全

文件層級安全可讓您限制使用者在索引中可看見的文件。建立角色時，請指定索引模式和 OpenSearch 查詢。任何您映射到該角色的使用者都只能看見與查詢相符的文件。文件層級安全會影響您在搜尋時的命中數。

如需詳細資訊，請參閱文件層級安全。

欄位層級安全

欄位層級安全可讓您控制使用者能看見的文件欄位。建立角色時，請新增欄位清單來加入或排除。如果您加入欄位，則您映射到該角色的任何使用者都只能看到那些欄位。如果您排除欄位，則「除了」遭排除的欄位外，使用者可以看見所有欄位。欄位層級安全會影響您在搜尋時包含在命中中的欄位數。

如需詳細資訊，請參閱欄位層級安全。

欄位遮罩

欄位遮罩是欄位層級安全的替代項目，可讓您匿名化欄位中的資料，而非完全移除。請在建立角色時，新增要進行遮罩的欄位清單。欄位遮罩會影響您在搜尋時是否可以看見欄位的內容。

> **Tip**
> 如果您將標準遮罩套用至欄位， OpenSearch Service 會使用安全的隨機雜湊，這可能會造成不正確的彙總結果。若要在遮罩欄位上執行彙總，請改用以模式為基礎的遮罩。

建立 使用者

如果您啟用了內部使用者資料庫，則可以使用 OpenSearch儀表板或 REST API 中的`_plugins/_security`作業來建立使用者。如需詳細資訊，請參閱建立使用者。

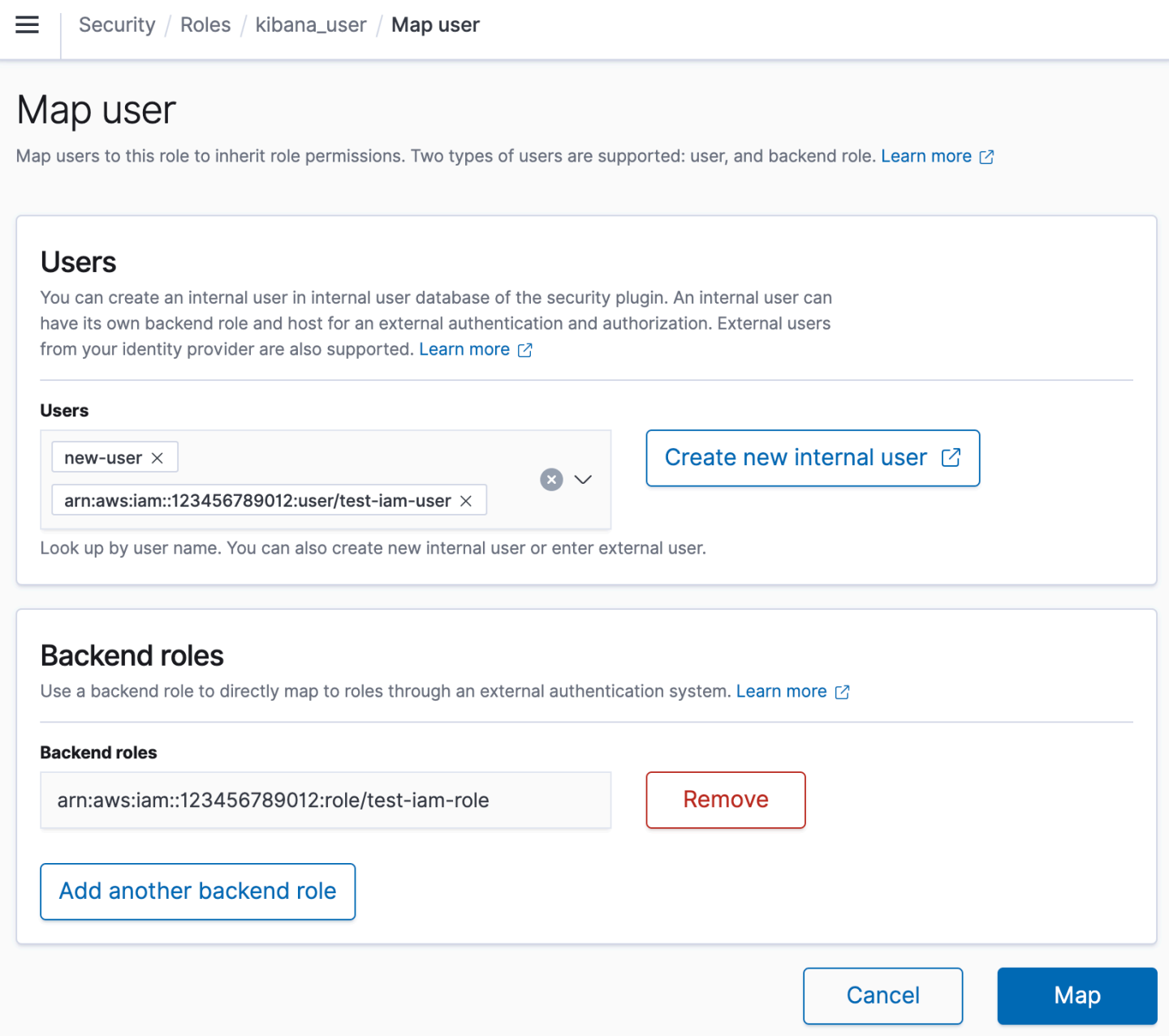
如果您為主要使用者選擇了 IAM，請忽略 Dashboards 的這個部分。請改為建立 IAM 角色。如需詳細資訊，請參閱《IAM 使用者指南》https://docs.aws.amazon.com/IAM/latest/UserGuide/。

將角色映射至使用者

角色映射是精細存取控制中最重要的層面。精細存取控制包含了一些預先定義角色，可協助您開始使用，但除非您將這些角色映射到使用者，否則每個向叢集提出的請求都會導致許可錯誤。

後端角色有助於簡化角色對應程序。您可以將角色對應至所有 100 位使用者共用的單一後端角色，而不是將相同角色對應至 100 位個別使用者。後端角色可以是 IAM 角色或任意字串。

- 在 Users (使用者) 區段中指定使用者、使用者 ARN 和 Amazon Cognito 使用者字串。Cognito 使用者字串的形式為 `Cognito/`*`user-pool-id`*`/`*`username`*。
- 請在 Backend roles (後端角色) 區段中指定後端角色和 IAM 角色 ARN。



您可以使用 OpenSearch 儀表板或 REST API 中的`_plugins/_security`作業將角色對應至使用者。如需詳細資訊，請參閱將使用者映射至角色。

建立動作群組

動作群組是一組許可，可讓您跨不同資源重複使用。您可以使用 OpenSearch 儀表板或 REST API 中的`_plugins/_security`操作來建立新的動作群組，但預設動作群組已足以滿足大多數使用案例的需求。如需預設動作群組的詳細資訊，請參閱預設動作群組。

OpenSearch 多租戶儀表板

租用戶是儲存索引模式、視覺化、儀表板和其他 Dashboards 物件的空間。多租戶儀表板可讓您與其他儀表板使用者安全地共用您的工作 (或將其保持私密)，並動態設定租用戶。您可以控制哪些角色可以存取租用戶，以及這些角色是否具備讀取或寫入存取權限。全域租用戶為預設值。若要深入了解，請參閱多租戶OpenSearch 儀表板。

檢視您目前的租用戶或變更租用戶

1. 導覽至「 OpenSearch 儀表板」並登入。
2. 選取右上角的使用者圖示，然後選擇 Switch tenants (轉換租用戶)。
3. 在建立視覺效果或儀表板之前驗證您的租用戶。如果您希望與其他所有的 Dashboards 使用者共享您的作品，請選擇 Global (全域)。若要與一部分 Dashboards 使用者共享您的作品，請選擇不同的共享租用戶。否則，請選擇 Private (私有)。

> **Note**
>
> OpenSearch 儀表板會為每個承租人維護個別的索引，並建立名為的索引範本`tenant_template`。請勿刪除或修改`tenant_template`索引，因為如果租用戶索引對應設定錯誤，可能會導致 OpenSearch 儀表板發生錯誤。

建議的組態

由於精細存取控制與其他安全功能的互動方式，我們建議使用數種精細存取控制組態。這些組態適合大多數的使用案例。

描述	主要使用者	網域存取政策
使用 IAM 登入資料呼叫 OpenSearch API，並使用 SAML 身份驗證來存取儀表板。使用 Dashboards 或 REST API 管理精細存取控制角色。	IAM 角色或使用者	`{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Principal": { "AWS": "*" }, ...`

描述	主要使用者	網域存取政策

		`"Action": "es:ESHttp*",`
		`"Resource": " domain-arn /*"`
		`}`
		`]`
		`}`

使用 IAM 登入資料或基本身份驗證來呼叫 OpenSearch API。使用 Dashboards 或 REST API 管理精細存取控制角色。
 	
此配置提供了很多靈活性，特別是如果您的 OpenSearch客戶端只支持基本身份驗證。
 	
如果您擁有現有的身分提供者，請使用 SAML 身分驗證來存取 Dashboards。否則，請管理內部使用者資料庫中的 Dashboards 使用者。
	用戶名和密碼	`{`
		`"Version": "2012-10-17",`
		`"Statement": [`
		`{`
		`"Effect": "Allow",`
		`"Principal": {`
		`"AWS": "*"`
		`},`
		`"Action": "es:ESHttp*",`
		`"Resource": " domain-arn /*"`
		`}`
		`]`
		`}`

描述	主要使用者	網域存取政策
使用 IAM 登入資料來呼叫 OpenSearch API，並使用 Amazon Cognito 存取儀表板。使用 Dashboards 或 REST API 管理精細存取控制角色。	IAM 角色或使用者	`{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Principal": { "AWS": "*" }, "Action": "es:ESHttp*", "Resource": " domain-arn /*" } ] }`
使用 IAM 登入資料呼叫 OpenSearch API，並封鎖對儀表板的大多數存取權。使用 REST API 管理精細存取控制角色。	IAM 角色或使用者	`{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Principal": { "AWS": "*" }, "Action": "es:ESHttp*", "Resource": " domain-arn /*" }, { "Effect": "Deny", "Principal": { "AWS": "*" }, "Action": "es:ESHttp*", "Resource": " domain-arn /_dashboards*" } ] }`

限制

精細存取控制有幾個重要的限制：

- 如果網域是位於 VPC 中，則將角色映射到主機名稱或 IP 地址的角色映射 `hosts` 層面會無法正常運作。您仍然可以將角色映射到使用者和後端角色。
- 如果您為主要使用者選擇了 IAM 但並未啟用 Amazon Cognito 或 SAML 身分驗證，則 Dashboards 會顯示沒有任何功能的登入頁面。
- 如果您為主要使用者選擇了 IAM，您仍然可以在內部使用者資料庫中建立使用者。但是，由於沒有在這個組態下啟用 HTTP 基本身分驗證，因此任何使用這些使用者登入資料簽署的請求都會遭到拒絕。
- 如果您使用 SQL 來查詢您無法存取的索引，便會收到「沒有許可」錯誤。如果索引不存在，則您會收到「找不到索引」錯誤。這項錯誤訊息中的差異表示如果您猜測其名稱，您便可以確認該索引是否存在。

  為了將問題降至最低，請不要在索引名稱中包含敏感資訊。如要拒絕所有對 SQL 的存取，請將以下元素新增到您的網域存取政策：

  ```
  {
    "Effect": "Deny",
    "Principal": {
      "AWS": [
        "*"
      ]
    },
    "Action": [
      "es:*"
    ],
    "Resource": "arn:aws:es:us-east-1:123456789012:domain/my-domain/_plugins/_sql"
  }
  ```

- 如果您的網域版本為 2.3 或更高版本，且啟用了精細的存取控制，則設定`max_clause_count`為 1 會導致網域發生問題。我們建議您將此帳戶設定為較高的數字。
- 如果您要在未設定精細存取控制的網域中啟用精細的存取控制，則針對為直接查詢建立的資料來源，您必須自行設定精細的存取控制角色。如需如何設定精細存取角色的詳細資訊，請參閱建立 Amazon OpenSearch 服務資料來源與 Amazon S3 整合。

修改主要使用者

如果您忘記了主要使用者的詳細資訊，您可以使用主控台、 AWS CLI或組態 API 來重新設定。

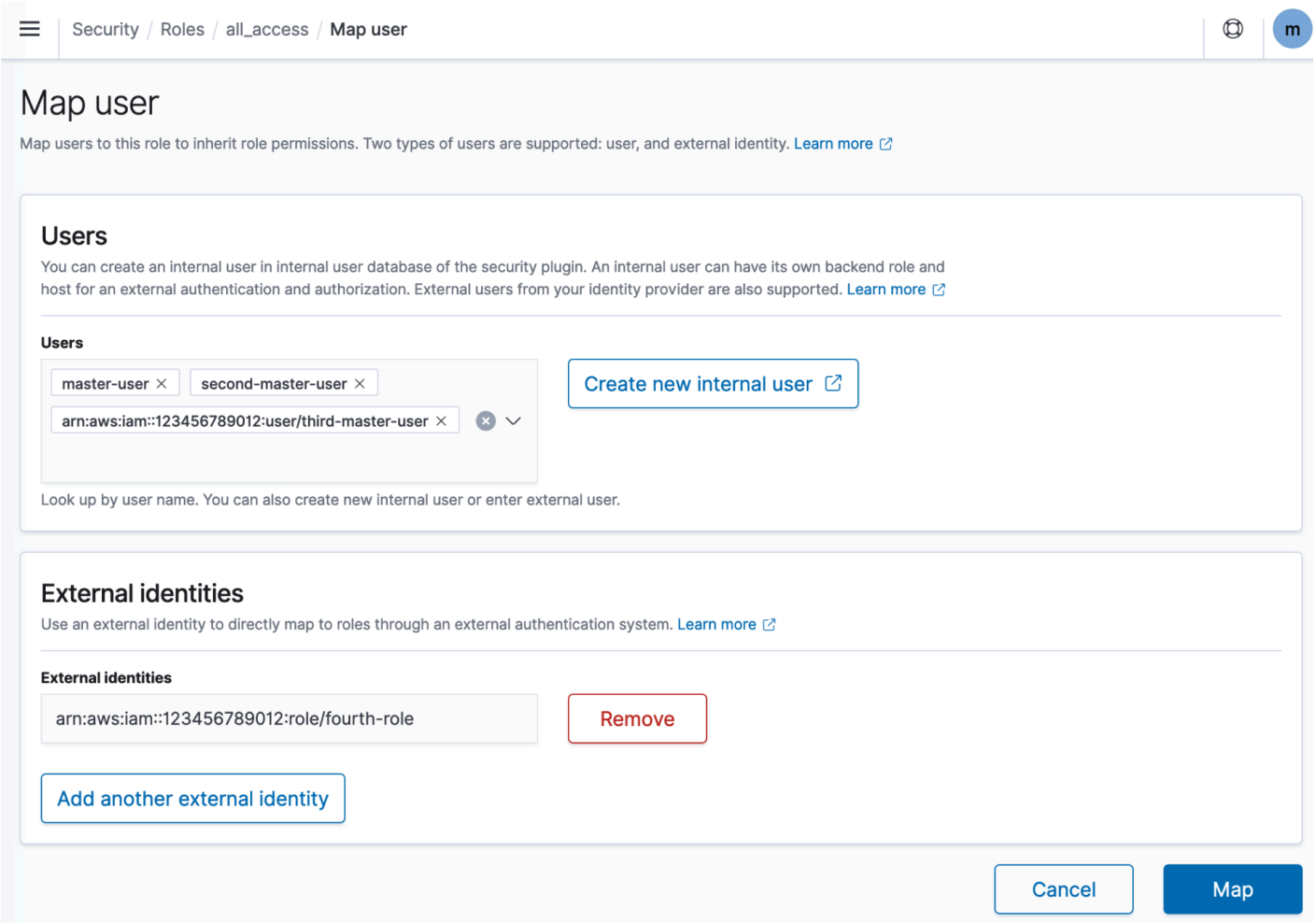
修改主要使用者 (主控台)

1. 導航到 Amazon OpenSearch 服務控制台 https://console.aws.amazon.com/aos/home/.
2. 選取網域，並選擇 Actions (動作)、Edit security configuration (編輯安全組態)。
3. 選擇 Set IAM ARN as master user (將 IAM ARN 設為主要使用者) 或 Create master user (建立主要使用者)。
   - 如果您先前使用了 IAM 主要使用者，精細存取控制會將 `all_access` 角色重新映射到您指定的新 IAM ARN。
   - 如果您先前使用了內部使用者資料庫，則精細存取控制會建立新的主要使用者。您可以使用新的主要使用者來刪除舊的主要使用者。
   - 從內部使用者資料庫切換至 IAM 主要使用者不會刪除內部使用者資料庫中的任何使用者。相反，它只是停用 HTTP 基本身分驗證。從內部使用者資料庫手動刪除使用者，或者保留它們，以防您需要重新啟用 HTTP 基本身分驗證。
4. 選擇儲存變更。

其他主要使用者

您可以在建立網域時指定主要使用者，但是如果您希望的話，您可以使用這個主要使用者來建立其他主要使用者。您有兩個選項： OpenSearch 儀表板或其餘 API。

- 在 Dashboards 中，選擇 Security (安全性)、Role (角色)，然後將新的主要使用者映射到 `all_access` 和 `security_manager` 角色。



- 如要使用 REST API，請傳送下列請求：

```
PUT _plugins/_security/api/rolesmapping/all_access
{
  "backend_roles": [
    "arn:aws:iam::123456789012:role/fourth-master-user"
  ],
  "hosts": [],
  "users": [
    "master-user",
    "second-master-user",
    "arn:aws:iam::123456789012:user/third-master-user"
  ]
}
```

```
PUT _plugins/_security/api/rolesmapping/security_manager
{
```

```
  "backend_roles": [
    "arn:aws:iam::123456789012:role/fourth-master-user"
  ],
  "hosts": [],
  "users": [
    "master-user",
    "second-master-user",
    "arn:aws:iam::123456789012:user/third-master-user"
  ]
}
```

這些請求會「取代」目前的角色映射，因此請先執行 GET 請求，讓您可以在 PUT 請求中包含所有目前的角色。在您無法存取 Dashboards 而又希望將 Amazon Cognito 的 IAM 角色映射到 `all_access` 角色時，REST API 特別有用。

手動快照

精細存取控制在擷取手動快照時複雜度較高。若要註冊快照儲存庫 (即使將 HTTP 基本身分驗證用於所有其他用途)，您必須將 `manage_snapshots` 角色映射至具備 `iam:PassRole` 許可能夠擔任 `TheSnapshotRole` 的 IAM 角色，如 the section called “必要條件” 中所定義。

然後使用該 IAM 角色將簽章的請求傳送到網域，如 the section called “註冊手動快照儲存庫” 中所述。

整合

如果您將其他服 AWS 務與 OpenSearch 服務搭配使用，則必須以適當的許可為這些服務提供 IAM 角色。例如，Firehose 交付串流通常使用稱為`firehose_delivery_role`的 IAM 角色。在 Dashboards 中，建立精細存取控制的角色，然後將 IAM 角色映射到該角色。在此案例中，新的角色需要下列許可：

```
{
  "cluster_permissions": [
    "cluster_composite_ops",
    "cluster_monitor"
  ],
  "index_permissions": [{
    "index_patterns": [
      "firehose-index*"
    ],
    "allowed_actions": [
      "create_index",
```

```
      "manage",
      "crud"
    ]
  }]
}
```

許可會因每個服務執行的動作而不同。索引資料的 AWS IoT 規則或 AWS Lambda 函數可能需要與 Firehose 類似的權限，而只執行搜尋的 Lambda 函數則可以使用更有限的集合。

REST API 差異

細粒度的訪問控制 REST API 略有不同，具體取決於您的 OpenSearch/彈性搜索版本。在提出 PUT 請求前，請先提出 GET 請求以驗證預期的請求主體。例如，向 `_plugins/_security/api/user` 提出的 GET 請求會傳回所有使用者，讓您可以接著進行修改並用來提出有效的 PUT 請求。

在 Elasticsearch 6.x 上，建立使用者的請求如下所示：

```
PUT _opendistro/_security/api/user/new-user
{
  "password": "some-password",
  "roles": ["new-backend-role"]
}
```

在 OpenSearch 或彈性搜索 7.x 上，請求看起來像這樣（`_opendistro`如果使用彈性搜索，則更改`_plugins`為）：

```
PUT _plugins/_security/api/user/new-user
{
  "password": "some-password",
  "backend_roles": ["new-backend-role"]
}
```

此外，租用戶在 Elasticsearch 6.x 中是角色的屬性。

```
GET _opendistro/_security/api/roles/all_access

{
  "all_access": {
    "cluster": ["UNLIMITED"],
    "tenants": {
```

```
      "admin_tenant": "RW"
    },
    "indices": {
      "*": {
        "*": ["UNLIMITED"]
      }
    },
    "readonly": "true"
  }
}
```

在 OpenSearch 和彈性搜索 7.x 中，它們是具有自己的 URI 的對象（`_opendistro`如果使用彈性搜索，則更改`_plugins`為）：

```
GET _plugins/_security/api/tenants

{
  "global_tenant": {
    "reserved": true,
    "hidden": false,
    "description": "Global tenant",
    "static": false
  }
}
```

如需 OpenSearch REST API 的相關文件，請參閱安全性外掛程式 API 參考資料。

> **Tip**
>
> 如果您使用內部用戶資料庫，則可以使用 curl 發出請求並測試您的網域。嘗試以下範例命令：
>
> ```
> curl -XGET -u 'master-user:master-user-password' 'domain-endpoint/_search'
> curl -XGET -u 'master-user:master-user-password' 'domain-endpoint/_plugins/
> _security/api/user'
> ```

教學課程：使用 IAM 主要使用者和 Amazon Cognito 身分驗證設定網域

本教學涵蓋了一個熱門的 Amazon OpenSearch 服務使用案例，用於精確的存取控制：具有適用於儀表板的 Amazon Cognito 身份驗證的 IAM 主使用 OpenSearch 者。

在本教學課程中，我們將設定主要 IAM 角色和有限的 IAM 角色，然後我們將它們與 Amazon Cognito 中的使用者建立關聯。然後，主要使用者可以登入 OpenSearch 儀表板、將受限使用者對應至角色，並使用精細的存取控制來限制使用者的權限。

雖然這些步驟會使用 Amazon Cognito 使用者集區進行身分驗證，但相同的基本程序也適用於任何可讓您將不同 IAM 角色指派給不同使用者的 Cognito 身分驗證提供者。

在本教學課程中，您會完成下列步驟：

1. 建立主要和有限的 IAM 角色
2. 使用 Cognito 身分驗證建立網域
3. 設定 Cognito 使用者集區和身分識別集區
4. 在 OpenSearch 儀表板中對應角色
5. 測試許可

步驟 1：建立主要和有限的 IAM 角色

導覽至 AWS Identity and Access Management (IAM) 主控台並建立兩個獨立的角色：

- `MasterUserRole`：具備叢集完整許可並管理角色與角色映射的主要使用者。
- `LimitedUserRole`：更受限制的角色，您將向其授予作為主要使用者的有限存取權。

如需建立角色的說明，請參閱使用自訂信任政策建立角色。

兩個角色都必須具有下列信任政策，以允許您的 Cognito 身分集區擔任相關角色：

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
```

```
    "Principal": {
      "Federated": "cognito-identity.amazonaws.com"
    },
    "Action": "sts:AssumeRoleWithWebIdentity",
    "Condition": {
      "StringEquals": {
        "cognito-identity.amazonaws.com:aud": "{identity-pool-id}"
      },
      "ForAnyValue:StringLike": {
        "cognito-identity.amazonaws.com:amr": "authenticated"
      }
    }
  }]
}
```

> **Note**
>
> 使用 Amazon Cognito 身分集區的唯一識別符取代 `identity-pool-id`。例如 `us-east-1:0c6cdba7-3c3c-443b-a958-fb9feb207aa6`。

步驟 2：使用 Cognito 身分驗證建立網域

在 https://console.aws.amazon.com/aos/home/ 瀏覽至 Amazon OpenSearch 服務主控台，並使用以下設定建立網域：

- OpenSearch 1.0 或更新版本，或彈性搜尋 7.8 或更新版本
- 公用存取
- 以 `MasterUserRole` 作為主要使用者啟用的精細存取控制 (在上一個步驟中建立)
- 為 OpenSearch 儀表板啟用 Amazon Cognito 份驗證。如需啟用 Cognito 身分驗證，以及選取使用者和身分集區的說明，請參閱the section called “設定網域以使用 Amazon Cognito 身分驗證”。
- 以下網域存取政策：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::{account-id}:root"
```

```
      },
      "Action": [
        "es:ESHttp*"
      ],
      "Resource": "arn:aws:es:{region}:{account-id}:domain/{domain-name}/*"
    }
  ]
}
```

- 要求所有前往網域的流量皆使用 HTTPS
- N ode-to-node 加密技術
- 靜態資料加密

步驟 3：設定 Cognito 使用者

建立您的網域時，請按照 Amazon Cognito 開發人員指南中的建立使用者集區，在 Amazon Cognito 中設定主要使用者和受限使用者。最後，按照在 Amazon Cognito 中建立身分集區中的步驟設定您的身分集區。使用者集區和身分集區必須在相同的 AWS 區域。

步驟 4：在 OpenSearch 儀表板中對應角色

現在已設定使用者，您可以以主要使用者身分登入 OpenSearch 儀表板，並將使用者對應至角色。

1. 返回 OpenSearch 服務主控台並導覽至您建立之網域的 OpenSearch 儀表板 URL。URL 遵循此格式：`domain-endpoint/_dashboards/`。
2. 使用 `master-user` 憑證登入。
3. 選擇 Add sample data (新增範例資料)，並新增範例航班資料。
4. 在左側導覽窗格中，選擇 Security (安全)、Roles (角色)、Create role (建立角色)。
5. 將角色命名為 `new-role`。
6. 對於 Index (索引)，指定 `opensearch_dashboards_sample_data_fli*` (Elasticsearch 網域上的 `kibana_sample_data_fli*`)。
7. 對於 Index permissions (索引許可)，請選擇 read (讀取)。
8. 對於 Document level security (文件層級安全)，指定以下查詢：

```
{
  "match": {
    "FlightDelay": true
  }
```

```
}
```

9. 如需欄位層級的安全性，請選擇 Exclude (排除)，然後指定 `FlightNum`。
10. 對於 Anonymization (匿名化)，請指定 `Dest`。
11. 選擇建立。
12. 選擇 Mapped users (已映射的使用者)、Manage mapping (管理映射)。新增 `LimitedUserRole` 的 Amazon Resource Name (ARN) 作為外部身分，然後選擇 Map (映射)。
13. 傳回角色清單，然後選擇 opensearch_dashboards_user。選擇 Mapped users (已映射的使用者)、Manage mapping (管理映射)。新增 `LimitedUserRole` 的 ARN 作為後端角色，並選擇 Map (映射)。

步驟 5：測試許可

正確對應角色後，您可以以受限使用者身分登入並測試權限。

1. 在新的私人瀏覽器視窗中，導覽至網域的 OpenSearch 儀表板 URL，使用`limited-user`認證登入，然後選擇 [自行探索]。
2. 移至 Dev Tools (開發工具) 並執行預設搜尋：

```
GET _search
{
  "query": {
    "match_all": {}
  }
}
```

   請注意許可錯誤。`limited-user` 沒有執行全叢集搜尋的許可。

3. 執行另一項搜尋：

```
GET opensearch_dashboards_sample_data_flights/_search
{
  "query": {
    "match_all": {}
  }
}
```

   請注意，所有相符文件的都有值為 `true` 的 `FlightDelay` 欄位、匿名化的 `Dest` 欄位，並不包含 `FlightNum` 欄位。

4. 在原始瀏覽器視窗中，以 `master-user` 的身分登入、選擇 Dev Tools (開發工具)，然後執行相同的搜尋。注意許可、命中數、相符文件以及所包含欄位中的差異。

教學課程：使用內部使用者資料庫和 HTTP 基本身分驗證設定網域

本教學課程涵蓋另一個熱門的精細存取控制使用案例：內部使用者資料庫中的主要使用者和 OpenSearch 儀表板的 HTTP 基本驗證。然後，主要使用者可以登入 OpenSearch 儀表板、建立內部使用者、將使用者對應至角色，以及使用精細的存取控制來限制使用者的權限。

在本教學課程中，您會完成下列步驟：

1. 使用主要使用者建立網域
2. 在 OpenSearch 儀表板中設定內部使用者
3. 在 OpenSearch 儀表板中對應角色
4. 測試許可

步驟 1：建立網域

在 https://console.aws.amazon.com/aos/home/ 瀏覽至 Amazon OpenSearch 服務主控台，並使用以下設定建立網域：

- OpenSearch 1.0 或更新版本，或彈性搜尋 7.9 或更新版本
- 公用存取
- 使用內部使用者資料庫 (本教學中的其餘部分稱為 `TheMasterUser`) 中的主要使用者進行精細存取控制。
- Dashboards 的 Amazon Cognito 身分驗證已停用
- 以下存取政策：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::{account-id}:root"
      },
      "Action": [
```

```
        "es:ESHttp*"
      ],
      "Resource": "arn:aws:es:{region}:{account-id}:domain/{domain-name}/*"
    }
  ]
}
```

- 要求所有前往網域的流量皆使用 HTTPS
- N ode-to-node 加密技術
- 靜態資料加密

步驟 2：在 OpenSearch 儀表板中建立內部使用者

現在您已經擁有網域，您可以登入 OpenSearch 儀表板並建立內部使用者。

1. 返回 OpenSearch 服務主控台並導覽至您建立之網域的 OpenSearch 儀表板 URL。URL 遵循此格式：*domain-endpoint*/_dashboards/。
2. 使用TheMasterUser.
3. 選擇 Add sample data (新增範例資料)，並新增範例航班資料。
4. 在左側導覽窗格中，選擇 [安全性]、[內部使用者]、[建立內部使用者
5. 命名使用者 new-user，然後指定密碼。然後選擇 Create (建立)。

步驟 3：對應 OpenSearch 儀表板中的角色

現在您的使用者已設定完成，您可以將使用者對應至角色。

1. 停留在 OpenSearch 儀表板的安全部分，然後選擇角色，創建角色。
2. 將角色命名為 new-role。
3. 在索引中，指定 opensearch_dashboards_sample_data_fli* (kibana_sample_data_fli*在 Elasticsearch 網域上) 做為索引模式。
4. 對於動作群組，請選擇 read (讀取)。
5. 對於 Document level security (文件層級安全)，指定以下查詢：

```
{
  "match": {
    "FlightDelay": true
  }
```

```
}
```

6. 如需欄位層級的安全性，請選擇 Exclude (排除)，然後指定 `FlightNum`。
7. 對於 Anonymization (匿名化)，請指定 `Dest`。
8. 選擇建立。
9. 選擇 Mapped users (已映射的使用者)、Manage mapping (管理映射)。然後將 `new-user` 新增至 Users (使用者)，然後選擇 Map (映射)。
10. 傳回角色清單，然後選擇 opensearch_dashboards_user。選擇 Mapped users (已映射的使用者)、Manage mapping (管理映射)。然後將 `new-user` 新增至 Users (使用者)，然後選擇 Map (映射)。

步驟 4：測試權限

正確對應角色後，您可以以受限使用者身分登入並測試權限。

1. 在新的私人瀏覽器視窗中，導覽至網域的 OpenSearch 儀表板 URL，使用`new-user`認證登入，然後選擇 [自行探索]。
2. 移至 Dev Tools (開發工具) 並執行預設搜尋：

```
GET _search
{
  "query": {
    "match_all": {}
  }
}
```

   請注意許可錯誤。`new-user` 沒有執行全叢集搜尋的許可。

3. 執行另一項搜尋：

```
GET dashboards_sample_data_flights/_search
{
  "query": {
    "match_all": {}
  }
}
```

   請注意，所有相符文件的都有值為 `true` 的 `FlightDelay` 欄位、匿名化的 `Dest` 欄位，並不包含 `FlightNum` 欄位。

4. 在原始瀏覽器視窗中，以 `TheMasterUser` 的身分登入、選擇 Dev Tools (開發工具) 並執行相同的搜尋。注意許可、命中數、相符文件以及所包含欄位中的差異。

Amazon OpenSearch 服務的合規驗證

第三方稽核員會評估 Amazon OpenSearch 服務的安全性和合規性，作為多個核數人的一部 AWS 合規方案。這些程式包括SOCPCI、和HIPAA。

如果您有合規性需求，請考慮使用任何版本的 OpenSearch 或彈性搜尋 6.0 或更新版本。舊版 Elasticsearch 不提供靜態資料加密和node-to-node 加密的組合，因此不太可能符合您的需求。如果精細的存取控制對您的使用案例很重要，您也可以考慮使用任何版本的 OpenSearch 或 Elasticsearch 6.7 或更新版本。無論如何，在創建域時選擇特定 OpenSearch 或 Elasticsearch 版本並不能保證合規性。

要了解是否 AWS 服務 在特定法規遵循計劃的範圍內，請參閱 AWS 服務 在合規計劃的範圍 然後選擇您感興趣的合規計劃。如需一般資訊，請參閱 AWS 合規計劃 。

您可以使用下載第三方稽核報告 AWS Artifact。 如需詳細資訊，請參閱下載報告 AWS Artifact.

您在使用時的合規責任 AWS 服務 取決於您資料的敏感度、貴公司的合規目標，以及適用的法律和法規。 AWS 提供下列資源以協助遵循法規：

- 安全性與合規性快速入門指南 — 這些部署指南討論架構考量，並提供部署基準環境的步驟 AWS 重點是安全性和合規性。
- 在 Amazon Web Services 上進行HIPAA安全與合規架構 — 本白皮書說明公司如何使用 AWS 以建立HIPAA符合資格的應用程式。

> **Note**
>
> 不是全部 AWS 服務 HIPAA符合資格。如需詳細資訊，請參閱合HIPAA格服務參考。

- AWS 合規資源 — 此工作簿和指南集合可能適用於您的產業和所在地。
- AWS 客戶合規指南 — 透過合規的角度瞭解共同的責任模式。這些指南總結了安全性的最佳做法 AWS 服務 並在多個架構 (包括美國國家標準與技術研究所 (NIST)、支付卡產業安全標準委員會 (PCI) 和國際標準化組織 ()) 中對應安全控制指引。ISO
- 使用中的規則評估資源 AWS Config 開發人員指南 — AWS Config 服務評估您的資源配置是否符合內部實踐，行業準則和法規。

- AWS Security Hub— 這個 AWS 服務 提供您安全性狀態的全面檢視 AWS。 Security Hub 使用安全控制來評估您的 AWS 資源，並檢查您的合規性是否符合安全性產業標準和最佳實務。如需支援的服務和控制清單，請參閱 Security Hub controls reference。
- Amazon GuardDuty-這 AWS 服務 檢測潛在的威脅 AWS 帳戶監控環境中的可疑和惡意活動，藉此監控工作負載、容器和資料。 GuardDuty 可協助您因應各種合規性需求 PCIDSS，例如符合特定合規性架構所要求的入侵偵測需求。
- AWS Audit Manager— 這個 AWS 服務 協助您持續稽核 AWS 使用方式可簡化您管理風險以及遵守法規和業界標準的方式。

Amazon CopenSearFront Service 的復原功能

AWS 全球基礎架構是以 AWS 區域 與可用區域為中心建置的。AWS 區域 提供多個分開且隔離的實際可用區域，並以具備低延遲、高輸送量和高度備援特性的聯網相互連結。透過可用區域，您所設計與操作的應用程式和資料庫，就能夠在可用區域之間自動容錯移轉，而不會發生中斷。可用區域的可用性、容錯能力和擴充能力，均較單一或多個資料中心的傳統基礎設施還高。

如需 AWS 區域 與可用區域的詳細資訊，請參閱AWS全球基礎架構。

除了 AWS 全球基礎設施外，OpenSearch Service 還提供數種支援資料復原和備份需求的功能：

- 異地同步備份網域和複本碎片
- 自動和手動快照

JWTAmazon OpenSearch 服務的身份驗證和授權

Amazon OpenSearch 服務現在允許您使用 JSON Web 令牌（JWTs）進行身份驗證和授權。JWTs是用JSON於授予單一登入 (SSO) 存取權的基礎存取權杖。您可以JWTs在 OpenSearch 服務中使用來建立單一登入權杖，以驗證對 OpenSearch Service 網域的要求。若要使用JWTs，您必須啟用精細的存取控制，並且必須提供有效RSA或ECDSAPEM格式化的公開金鑰。如需有關精細存取控制的詳細資訊，請參閱 Amazon OpenSearch 服務中的精細存取控制。

您可以JSON使用 OpenSearch 服務主控台、 AWS Command Line Interface (AWS CLI) 或 AWS SDKs.

考量事項

在JWTs與 Amazon OpenSearch 服務一起使用之前，您必須考慮以下事項：

- 由於PEM格式化的RSA公鑰大小，我們建議使用 AWS 控制台來配置JWT身份驗證和授權。
- 為您指定主旨和角色欄位時，您必須提供有效的使用者和角色JWTs，否則會拒絕要求。
- OpenSearch 2.11 是可用於JWT驗證的最早相容版本。

修改網域存取政策

您必須先更新網域存取原則以允許使用者存取網域，才能將網域設定為使JWT用JWT驗證和授權。否則，所有傳入的JWT授權要求都會遭到拒絕。提供子資源 (/*) 完整存取權的建議網域存取原則為：

```
{
  "Version": "2012-10-17",
  "Statement": [
      {
      "Effect": "Allow",
      "Principal": {
        "AWS": "*"
      },
      "Action": "es:ESHttp*",
      "Resource": "domain-arn/*"
    }
  ]
}
```

設定JWT驗證和授權

您可以在網域建立程序期間或更新現有網域來啟用JWT驗證和授權。根據您選擇的選項，設定步驟略有不同。

下列步驟說明如何在 OpenSearch Service 主控台中設定JWT驗證和授權的現有網域：

1. 在 [網域設定] 下，瀏覽至 [JWT驗證和授權] OpenSearch，選取 [啟用JWT驗證和授權]。
2. 設定要用於網域的公開金鑰。若要這麼做，您可以上傳包含公開金鑰的PEM檔案，也可以手動輸入。

   > **Note**
   >
   > 如果上傳或輸入的金鑰無效，則會在指定問題的文字方塊上方顯示警告。

3. (選擇性) 在其他設定下，您可以設定下列選擇性欄位

- 主旨金鑰 — 您可以將此欄位保留空白，以使用您的預設sub金鑰JWTs。
- 角色鍵 — 您可以將此欄位保留空白，以使用您的預設roles金鑰JWTs。

完成變更後，請儲存您的網域。

使用 a JWT 發送測試請求

JWT使用指定的主題和角色對創建新的後，您可以發送測試請求。若要這麼做，請使用私密金鑰，透過建立JWT. OpenSearch 服務能夠通過驗證此簽名來驗證傳入的請求。

> **Note**
> 如果您為您指定了自訂主旨金鑰或角色金鑰JWT，則必須為您的JWT.

以下是如何透過網域搜尋端點使用JWT權杖存取 OpenSearch 服務的範例：

```
curl -XGET "$search_endpoint" -H "Authorization: Bearer <JWT>"
```

設定JWT驗證和授權 (AWS CLI)

如果網域存在，下列 AWS CLI 命令會啟 OpenSearch 用JWT驗證和授權：

```
aws opensearch update-domain-config --domain-name <your_domain_name> --advanced-
security-options '{"JWTOptions":{"Enabled":true, "PublicKey": "<your_public_key>",
 "SubjectKey": "<your_subject_key>", "RolesKey": "<your_roles_key>"}}'
```

配置JWT身份驗證和授權（通過配置API）

下列對組態的要求會API啟用現有網域 OpenSearch 的JWT驗證和授權：

```
POST https://es.us-east-1.amazonaws.com/2021-01-01/opensearch/domain/my-domain/config
{
  "AdvancedSecurityOptions": {
    "JWTOptions": {
      "Enabled": true,
      "PublicKey": "public-key",
      "RolesKey": "optional-roles-key",
```

```
      "SubjectKey": "optional-subject-key"
    }
  }
}
```

產生 key pair

若要設定您JWTs的 OpenSearch 網域，您必須提供隱私權增強型郵件 () PEM 格式的公開金鑰。Amazon OpenSearch 服務目前在使用時支援兩種對近加密演算法JWTs：RSA和ECDSA。

若要使用通用 openssl 程式庫建立 RSA key pair，請依照下列步驟執行：

1. `openssl genrsa -out privatekey.pem 2048`
2. `openssl rsa -in privatekey.pem -pubout -out publickey.pem`

在此範例中，`publickey.pem`檔案包含可與 Amazon OpenSearch 服務搭配使用的公開金鑰，同時`privatekey.pem`包含用於簽署JWTs傳送至服務的私有金鑰。此外，如果您需要將私鑰轉換為常用`pkcs8`格式來生成JWTs.

如果您使用上傳按鈕將PEM檔案直接新增至主控台，檔案必須具有`.pem`副檔名、其他副檔名`.crt.cert`，例如、或`.key`目前不支援。

Amazon OpenSearch 服務基礎設施安全

作為一項受管服務，Amazon OpenSearch 服務受到 AWS 全球網路安全的保護。有關 AWS 安全服務以及如何 AWS 保護基礎架構的詳細資訊，請參閱AWS 雲端安全 若要使用基礎架構安全性的最佳做法來設計您的 AWS 環境，請參閱安全性支柱架構良 AWS 好的架構中的基礎結構保護。

您可以使用 AWS 已發佈的API呼叫透過網路存取 OpenSearch 服務。使用者端必須支援下列專案：

- 傳輸層安全性 (TLS)。我們需要 TLS 1.2 並推薦 TLS 1.3。
- 具有完美前向保密（ ）的密碼套件，例如（短暫的迪菲-赫爾曼PFS）或DHE（橢圓曲線短暫迪菲-赫爾曼）。ECDHE現代系統(如 Java 7 和更新版本)大多會支援這些模式。

此外，請求必須使用存取金鑰 ID 和與IAM主體相關聯的秘密存取金鑰來簽署。或者，您可以透過 AWS Security Token Service (AWS STS) 來產生暫時安全憑證來簽署請求。

您可以使用 AWS 已發佈的API呼叫API透過網路存取 OpenSearch 服務組態。若要設定要接受的最低需求TLS版本，請在網域端點選項中指定`TLSSecurityPolicy`值：

```
aws opensearch update-domain-config --domain-name my-domain --domain-endpoint-options
 '{"TLSSecurityPolicy": "Policy-Min-TLS-1-2-2019-07"}'
```

如需詳細資訊，請參閱AWS CLI 命令參考。

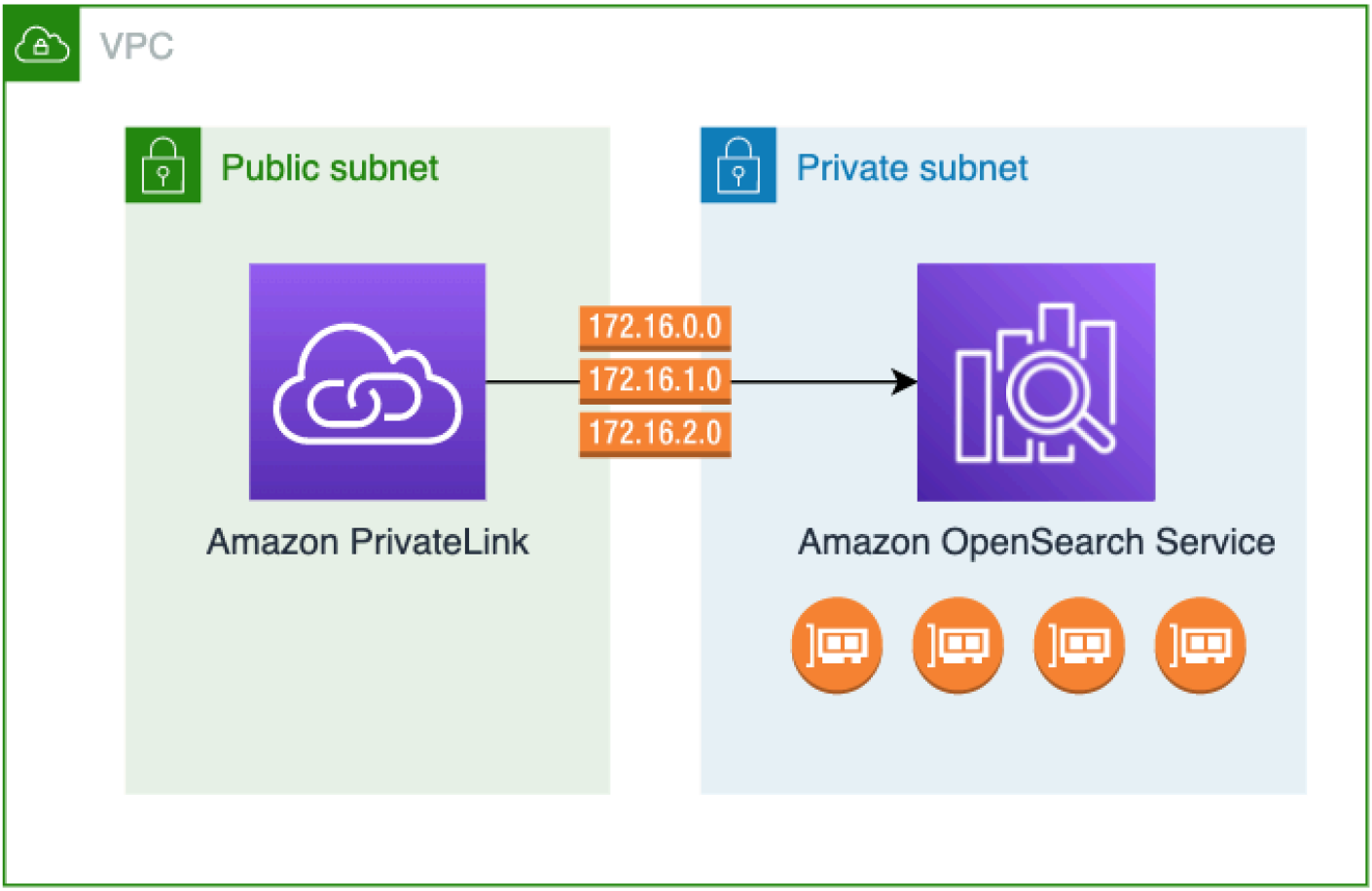
視您的網域組態而定，您可能還需要將要求簽署至 OpenSearch APIs. 如需詳細資訊，請參閱the section called “提出和簽署 OpenSearch 服務請求”。

OpenSearch 服務支持公共訪問域，它可以從任何互聯網連接的設備接收請求，以及VPC訪問域，這是從公共互聯網隔離。

使用 OpenSearch 服務 OpenSearch 受管VPC端點存取 Amazon 服務 ()AWS PrivateLink

您可以透過設定 OpenSearch 服務 OpenSearch 管理的VPC端點 (提供支援 AWS PrivateLink) 來存取 Amazon 服務網域。這些端點會在您VPC和 Amazon OpenSearch 服務之間建立私有連線。您可以像存取您的 OpenSearch 服務網VPC域一樣存取服務網域VPC，而無需使用網際網路閘道、NAT 裝置、VPN連線或 AWS Direct Connect 連線。您中的執行個體VPC不需要公用 IP 位址即可存取 OpenSearch 服務。

您可以設定 OpenSearch Service 網域VPC，以公開在相同、不VPC同或不同的公用或私有子網路上執行的其他端點。 AWS 帳戶這讓您可以新增額外的安全性層，以存取您的網域 (無論網域在何處執行)，而無需管理基礎架構。下圖說明相同VPC內容的 OpenSearch 服務管理VPC端點：



您可以透過建立由服 OpenSearch 務管理的介面VPC端點來建立此私人連線。 AWS PrivateLink我們會在您為介面端點啟用的每個子網路中建立VPC端點網路介面。這些是服務管理的網路介面，可做為「服務」流量的進入點。 OpenSearch 標準AWS PrivateLink 介面端點定價適用於以下 AWS PrivateLink計費的 OpenSearch 服務管理VPC端點。

您可以為執行所有版本 OpenSearch 和舊版 Elasticsearch 的網域建立VPC端點。如需詳細資訊，請參閱《AWS PrivateLink 指南》中的透過 AWS PrivateLink存取 AWS 服務。

OpenSearch 服務的考量和限制

在為 OpenSearch 服務設定介面VPC端點之前，請先檢閱AWS PrivateLink 指南中的考量事項。

使用 OpenSearch 服務管理的VPC端點時，請考慮下列事項：

- 您只能使用介面VPC端點連線至VPC網域。不支援公有網域。
- VPC端點只能連線到相同的網域 AWS 區域。
- HTTPS是VPC端點唯一支援的通訊協定。HTTP是不允許的。

- OpenSearch Service 支援透過介面VPC端點撥打所有支援的 OpenSearch API作業。
- 每個帳戶最多可設定 50 個端點，每個網域最多可設定 10 個端點。單一網域最多可有 10 個授權的主體。
- 您目前無法用 AWS CloudFormation 來建立介面VPC端點。
- 您只能透過 OpenSearch 服務主控台或使用服務建立介面VPC端點API。OpenSearch 您無法使用 Amazon VPC 主控台為 OpenSearch 服務建立介面VPC端點。
- OpenSearch 服務管理的VPC端點無法從網際網路存取。VPC在路由表和安全群組允許的情況下，OpenSearch 服務管理VPC的端點只能在佈建端點的位VPC置或與佈建端點的任何VPCs對等端點內進行存取。
- VPC OpenSearch 服務不支援端點策略。您可以將安全群組與端點網路介面相關聯，以控制透過介面VPC端點連至 OpenSearch 服務的流量。
- 您的服務連結角色必須位於您用來建立VPC端點的同一 AWS 帳戶中。
- 若要建立、更新和刪除 OpenSearch 服務VPC端點，除了 Amazon 服 OpenSearch 務EC2許可外，您還必須擁有以下 Amazon 許可：
  - `ec2:CreateVpcEndpoint`
  - `ec2:DescribeVpcEndpoints`
  - `ec2:ModifyVpcEndpoint`
  - `ec2:DeleteVpcEndpoints`
  - `ec2:CreateTags`
  - `ec2:DescribeTags`
  - `ec2:DescribeSubnets`
  - `ec2:DescribeSecurityGroups`
  - `ec2:DescribeVpcs`

> **Note**
>
> 目前，您無法將VPC端點建立限制為「 OpenSearch 服務」。我們正在努力在 future 的更新中實現這一目標。

提供對網域的存取

如果您想要存取您的網域位於另一個網域中 AWS 帳戶，您必須先從擁有者的帳戶授權，才能建立介面VPC端點。VPC

允許其他網VPC域存 AWS 帳戶 取您的網域

1. 在https://console.aws.amazon.com/aos/家裡打開 Amazon OpenSearch 服務控制台/。
2. 在導覽窗格中選擇 Domains (網域)，然後開啟您要提供存取權的網域。
3. 轉到VPC端點標籤，其中顯示可以訪問您的域VPCs的帳戶和對應的帳戶。
4. 選擇 Authorize principal (授權主體)。
5. 輸入將存取您網域的帳戶 AWS 帳戶 ID。此步驟會授權指定帳號針對網域建立VPC端點。
6. 選擇 Authorize (授權)。

建立VPC網域的介面VPC端點

您可以使用 OpenSearch 服務主控台或 AWS Command Line Interface (AWS CLI) 建立 OpenSearch 服務的介面VPC端點。

若要建立 OpenSearch 服務網域的介面VPC端點

1. 在https://console.aws.amazon.com/aos/家裡打開 Amazon OpenSearch 服務控制台/。
2. 在左側導覽窗格中，選擇「VPC端點」。
3. 選擇建立端點。
4. 選取要連接目前網域 AWS 帳戶 或其他網域中的網域 AWS 帳戶。
5. 選取您與此端點連線的網域。如果網域位於目前網域中 AWS 帳戶，請使用下拉式清單選擇網域。如果網域位於不同的帳戶中，請輸入要連接的網域的 Amazon 資源名稱 (ARN)。若要選擇不同帳戶中的網域，擁有者需為您提供對網域的存取權。
6. 對於 VPC，選VPC取您要存取 OpenSearch 服務的來源。
7. 對於子網路，請選取一或多個您要從中存 OpenSearch 取服務的子網路。
8. 對於 Security group (安全群組)，選取要與端點網路介面建立關聯的安全群組。這是一個關鍵步驟，其中您需限制正授權進入端點之傳入流量的連接埠、通訊協定和來源。安全性群組規則必須允許將使用VPC端點與 OpenSearch Service 通訊的資源，以便與端點網路介面進行通訊。
9. 選擇建立端點。端點應會在 2-5 分鐘內進入作用中狀態。

使用組態使用 OpenSearch 服務管理的VPC端點 API

使用下列API作業建立和管理 OpenSearch 服務管理VPC端點。

- CreateVpcEndpoint
- ListVpcEndpoints
- UpdateVpcEndpoint
- DeleteVpcEndpoint

請使用下列API操作來管理端點對VPC網域的存取：

- AuthorizeVpcEndpointAccess
- ListVpcEndpointAccess
- ListVpcEndpointsForDomain
- RevokeVpcEndpointAccess

SAML OpenSearch 儀表板的驗證

SAML OpenSearch 儀表板的身份驗證可讓您使用現有的身分提供者為執行 OpenSearch 或 Elasticsearch 6.7 或更新版本的 Amazon OpenSearch 服務網域上的儀表板提供單一登入 (SSO)。若要使用SAML驗證，您必須啟用精細的存取控制。

OpenSearch 儀表板身份驗證不是透過 Amazon Cognito 或內部使用者資料庫進行驗SAML證，可讓您使用第三方身分識別提供者登入儀表板、管理精細的存取控制、搜尋資料以及建立視覺效果。OpenSearch 服務支援使用 SAML 2.0 標準的提供者，例如 Okta、鍵盤遮罩、使用中目錄聯合服務 (ADFS)、Auth0 和 AWS IAM Identity Center.

SAML儀表板的驗證僅適用於透過 Web 瀏覽器存取 OpenSearch 儀表板。您的SAML認證不允許您直接向 OpenSearch 或儀表板發出HTTP請求APIs。

SAML組態概觀

本文件假設您擁有現有的身分提供者並且熟悉它。我們無法針對您的 OpenSearch 服務網域，提供您確切的提供者的詳細設定步驟。

OpenSearch 儀表板登入流程可採用以下兩種形式之一：

- 服務供應商 (SP) 已啟動：您瀏覽至 Dashboards (例如 `https://my-domain.us-east-1.es.amazonaws.com/_dashboards`)，它會將您重新引導到登入畫面。登入後，身分提供者會將您重新引導至 Dashboards。
- 已啟動身分識別提供者 (IdP)：您導覽至身分識別提供者、登入，然後從應用程式目錄中選擇 OpenSearch 儀表板。

OpenSearch 服務提供兩種單一登入URLs，即 SP 啟動和 IDP 啟動，但您只需要符合所 OpenSearch 需儀表板登入流程的一種。

無論您使用哪種身份驗證類型，目標都是通過您的身份提供者登錄並接收包含您的用戶名（必需）和任何後端角色（可選，但建議）的SAML斷言。此資訊允許更精細的存取控制，將權限指派給SAML使用者。在外部身分提供者中，後端角色通常稱為「角色」或「群組」。

考量事項

設定SAML驗證時，請考量下列事項：

- 由於 IdP 中繼資料檔案的大小，我們強烈建議您使用 AWS 控制台來配置SAML身份驗證。
- 網域一次只支援一個 Dashboards 身分驗證方法。如果您已啟用 OpenSearch 儀表板的 Amazon Cognito 身份驗證，則必須先將其停用，然後才能啟用身SAML份驗證。
- 如果搭配使用網路負載平衡器SAML，則必須先建立自訂端點。如需詳細資訊，請參閱???。
- 如SAML果是非IAM身分識別 SCP (例如 Amazon OpenSearch 無伺服器SAML和 Amazon 服務的基本內部使用者授權)，則不適用或評估 OpenSearch 服務控制政策 ()。

SAMLVPC網域驗證

SAML您的身份提供商和服務提供商之間不需要直接溝通。因此，即使SAML您的 OpenSearch 網域是在私人網域中託管VPC，只要您的瀏覽器可以與 OpenSearch 叢集和身分識別提供者通訊，您仍然可以使用。您的瀏覽器本質上充當身分提供者和服務供應商之間的媒介。如需說明SAML驗證流程的實用圖表，請參閱 Okta 文件。

修改網域存取政策

在設定SAML驗證之前，您必須更新網域存取原則，以允許SAML使用者存取網域。否則，您將看到存取遭拒錯誤。

我們建議您採用下列網域存取政策，該政策提供對網域上子資源 (/*) 的完整存取權：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "*"
      },
      "Action": "es:ESHttp*",
      "Resource": "domain-arn/*"
    }
  ]
}
```

若要使原則更具限制性，您可以將 IP 位址條件新增至原則。此條件會限制只能存取指定的 IP 位址範圍或子網路。例如，下列原則只允許從 192.0.2.0/24 子網路存取：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "*"
      },
      "Action": [
        "es:ESHttp*"
      ],
      "Condition": {
        "IpAddress": {
          "aws:SourceIp": [
            "192.0.2.0/24"
          ]
        }
      },
      "Resource": "domain-arn/*"
    }
  ]
}
```

> **Note**
>
> 開放網域存取原則需要在您的網域上啟用精細的存取控制，否則您會看到下列錯誤：
> `To protect domains with public access, a restrictive policy or fine-grained access control is required.`
> 如果您的主要使用者或內部使用者設定了可靠的密碼，則從安全性角度來看，在使用精細存取控制的同時，保持原則的開啟狀態可能是可以接受的。如需詳細資訊，請參閱???。

設定 SP 或 IdP 啟動的身分驗證

這些步驟說明如何針對儀表板啟用 SP 起始或 IDP 起始SAML驗證的驗證。 OpenSearch 如需了解啟用兩者所需的額外步驟，請參閱同時啟用 SP 和 IdP 啟動的身分驗證。

步驟 1：啟用SAML驗證

您可以在網域建立期間啟用SAML驗證，或選擇動作、編輯現有網域上的安全性組態來啟用驗證。根據您選擇的動作，以下步驟略有不同。

在網域組態中的 OpenSearch 儀表板 /Kibana SAML 驗證下，選取 [啟用驗證]。SAML

步驟 2：設定身分提供者

根據您設定SAML驗證的時間，執行下列步驟。

如果您正在建立新網域

如果您正在建立新網域， OpenSearch 服務尚無法產生服務提供者實體 ID 或 SSOURLs. 您的身分識別提供者需要這些值才能正確啟用SAML驗證，但只有在建立網域之後才能產生這些值。若要在網域建立期間處理此相互依存性，您可以在 IdP 組態中提供臨時值，以產生必要的中繼資料，然後在網域處於作用中狀態時加以更新。

如果您使用的是自定義端點，則可以推斷出URLs將是什麼。例如，如果您的自訂端點是`www.custom-endpoint.com`，服務提供者實體 ID 將是`www.custom-endpoint.com`、IDP 起始的SSOURL將會是`www.custom-endpoint.com/_dashboards/_opendistro/_security/saml/acs/idpinitiated`，而 SP SSO URL 啟動的將是。`www.custom-endpoint.com/_dashboards/_opendistro/_security/saml/acs`在建立網域之前，您可以使用這些值來設定身分提供者。如需範例，請參閱下一區段。

> **Note**
>
> 您無法使用雙堆疊端點登入，因為HTTP要求FQDN的項目與SAML要求FQDN的不同。如果您想要使用雙堆疊端點登入， OpenSearch系統管理員將需要設定自訂端點並將該CNAME值設定為雙堆疊端點。

如果您未使用自訂端點，可以在 IdP 中輸入臨時值以產生所需的中繼資料，然後在網域處於作用中後加以更新。

例如，在 Okta 中，您可以輸入「單一登**`https://temp-endpoint.amazonaws.com`**入」URL 和「對象 URI (SP 實體 ID)」欄位，這些欄位可讓您產生中繼資料。然後，在網域處於作用中狀態之後，您可以從 OpenSearch Service 擷取正確的值，並在 Okta 中更新它們。如需說明，請參閱 the section called “步驟 6：更新您的 IdP URLs”。

如果您正在編輯現有網域

如果您要在現有網域上啟用SAML驗證，請複製服務提供者實體 ID 及其中一個 SSOURLs. 如需URL要使用的指引，請參閱the section called “SAML組態概觀”。

Service provider entity ID

https://search-my-saml-domain-ob5t7vqdask2pav3r5pjjtvrxy.us-east-1.es.amazonaws.com

IdP-initiated SSO URL

https://search-my-saml-domain-ob5t7vqdask2pav3r5pjjtvrxy.us-east-1.es.amazonaws.com/_dashboards/_opendistro/_security/saml/acs/idpinitiated

SP-initiated SSO URL

https://search-my-saml-domain-ob5t7vqdask2pav3r5pjjtvrxy.us-east-1.es.amazonaws.com/_dashboards/_opendistro/_security/saml/acs

使用這些值來設定身分提供者。這是程序中最複雜的部分，不幸的是，術語和步驟因供應商而千差萬別。請咨詢供應商文件。

例如，在 Okta 中，您可以建立一個 SAML 2.0 網路應用程式。對於「單次登入」URL，請指定 SSOURL。針對對象 URI (SP 實體識別碼)，指定 SP 實體識別碼。

Okta 擁有使用者和群組，而不是使用者和後端角色。對於 Group Attribute Statements (群組屬性陳述式)，我們建議將 `role` 新增至 Name (名稱) 欄位，將常規表達式 `.+` 新增至 Filter (篩選條件) 欄位。此陳述式告訴 Okta 身分提供者在使用者驗證之後，將SAML宣告`role`欄位下的所有使用者群組納入。

在IAM身分識別中心中，您可以將 SP 實體 ID 指定為應用程式SAML對象。您還需要指定下列屬性對應：`Subject=${user:subject}:format=unspecified`和`Role=${user:groups}:format=uri`。

在 Auth0 中，您可以建立一般 Web 應用程式並啟用 SAML 2.0 附加元件。在 KeyCloak 中，您可以建立用戶端。

步驟 3：匯入 IdP 中繼資料

設定身分提供者之後，它會產生 IdP 中繼資料檔案。此XML檔案包含提供者的相關資訊，例如TLS憑證、單一登入端點和身分識別提供者的實體 ID。

複製 IdP 中繼資料檔案的內容，並將其貼到 OpenSearch 服務主控台的「來自 IdP 的中繼資料」欄位中。或者，選擇「從XML檔案匯入」並上傳檔案。中繼資料檔案如下所示：

```
<?xml version="1.0" encoding="UTF-8"?>
<md:EntityDescriptor entityID="entity-id"
 xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata">
  <md:IDPSSODescriptor WantAuthnRequestsSigned="false"
 protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
    <md:KeyDescriptor use="signing">
      <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:X509Data>
          <ds:X509Certificate>tls-certificate</ds:X509Certificate>
        </ds:X509Data>
      </ds:KeyInfo>
    </md:KeyDescriptor>
    <md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified</
md:NameIDFormat>
    <md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress</
md:NameIDFormat>
    <md:SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
 Location="idp-sso-url"/>
    <md:SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-
Redirect" Location="idp-sso-url"/>
  </md:IDPSSODescriptor>
</md:EntityDescriptor>
```

步驟 4：設定SAML欄位

輸入 IdP 中繼資料之後，請在 OpenSearch 服務主控台中設定下列其他欄位：

- IdP entity ID (IdP 實體 ID) – 從中繼資料檔案中複製 `entityID` 屬性的值，然後貼至此欄位。許多身分提供者也會將此值顯示為組態後摘要的一部分。有些供應商稱之為「發行者」。
- SAMLmaster 使用者名稱和SAML主要後端角色 — 您指定的使用者和/或後端角色會接收叢集的完整權限，相當於新的主要使用者，但只能在 OpenSearch 儀表板中使用這些權限。

  例如，在 Okta 中，您可能擁有屬於群組 `admins` 的使用者 `jdoe`。如果您新增`jdoe`至SAML主要使用者名稱欄位，則只有該使用者會收到完整權限。如果您新增`admins`至SAML主要後端角色欄位，屬於該`admins`群組的任何使用者都會收到完整權限。

> **Note**
>
> SAML宣告的內容必須完全符合您用於主要使用者名稱和SAMLSAML主要角色的字串。有些身分識別提供者會在其使用者名稱前加上首碼，這可能會造成 hard-to-diagnose 不相符。在身分識別提供者使用者介面中，您可能會看到`jdoe`，但SAML宣告可能包含`auth0|jdoe`。始終使用SAML斷言中的字符串。

許多身份提供者允許您在配置過程中查看示例斷言，而像 SAML-tracer 這樣的工具可以幫助您檢查和疑難排解實際斷言的內容。聲明看起來像這樣：

```
<?xml version="1.0" encoding="UTF-8"?>
<saml2:Assertion ID="id67229299299259351343340162"
 IssueInstant="2020-09-22T22:03:08.633Z" Version="2.0"
  xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">
  <saml2:Issuer Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity">idp-issuer</
saml2:Issuer>
  <saml2:Subject>
    <saml2:NameID Format="urn:oasis:names:tc:SAML:1.1:nameid-
format:unspecified">username</saml2:NameID>
    <saml2:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
      <saml2:SubjectConfirmationData NotOnOrAfter="2020-09-22T22:08:08.816Z"
 Recipient="domain-endpoint/_dashboards/_opendistro/_security/saml/acs"/>
    </saml2:SubjectConfirmation>
  </saml2:Subject>
  <saml2:Conditions NotBefore="2020-09-22T21:58:08.816Z"
 NotOnOrAfter="2020-09-22T22:08:08.816Z">
```

```
    <saml2:AudienceRestriction>
      <saml2:Audience>domain-endpoint</saml2:Audience>
    </saml2:AudienceRestriction>
  </saml2:Conditions>
  <saml2:AuthnStatement AuthnInstant="2020-09-22T19:54:37.274Z">
    <saml2:AuthnContext>

 <saml2:AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport<
saml2:AuthnContextClassRef>
    </saml2:AuthnContext>
  </saml2:AuthnStatement>
  <saml2:AttributeStatement>
    <saml2:Attribute Name="role" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-
format:unspecified">
      <saml2:AttributeValue
        xmlns:xs="http://www.w3.org/2001/XMLSchema"
        xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
 xsi:type="xs:string">GroupName Match Matches regex ".+" (case-sensitive)
      </saml2:AttributeValue>
    </saml2:Attribute>
  </saml2:AttributeStatement>
</saml2:Assertion>
```

步驟 5：(選用) 設定其他設定

在 Additional settings (其他設定) 下，設定下列選用欄位：

- 主旨金鑰 — 您可以將此欄位保留空白，以使用SAML宣告的`NameID`元素作為使用者名稱。如果您的聲明不使用此標準元素，而是將使用者名稱作為自訂屬性，請在此處指定該屬性。
- Roles key (角色金鑰)– 如果您想要使用後端角色 (建議使用)，請在此欄位中從聲明中指定屬性，例如 `role` 或 `group`。這是像 SAML-tracer 這樣的工具可以提供幫助的另一種情況。
- 工作階段存留時間 — 依預設， OpenSearch 儀表板會在 24 小時後將使用者登出。您可以透過指定新值，將此值設定為 60 至 1,440 分鐘 (24 小時) 之間的任何數字。

如果您對於組態感到滿意，請儲存網域。

步驟 6：更新您的 IdP URLs

如果您在建立網域時啟用SAML驗證，則必須在 IdP 中指定暫時性URLs，才能產生中XML繼資料檔案。網域狀態變更為後`Active`，您可以取得正確的資訊URLs並修改 IdP。

若要擷取，請選取網域URLs，然後選擇 [動作] > [編輯安全性組態]。在 OpenSearch 儀表板 /Kibana 的SAML驗證下，您可以找到正確的服務提供者實體 ID 和。SSO URLs複製URLs這些值並使用它們來設定您的身分識別提供者，取代您在步驟 2 中提供的暫時值。

步驟 7：將SAML使用者對應至角色

一旦您的網域狀態為作用中且 IdP 設定正確，請瀏覽至 [OpenSearch 儀表板]。

- 如果您選擇 SP 啟動URL，請瀏覽至。*domain-endpoint*/_dashboards若要直接登入特定承租人，您可以附加?security_tenant=*tenant-name*至URL.
- 如果您選擇 IDP 起始URL，請導覽至身分識別提供者的應用程式目錄。

在這兩種情況下，請以SAML主要使用者或屬於SAML主要後端角色的使用者身分登入。若要繼續步驟 7 的範例，請以 jdoe 或 admins 群組成員身分登入。

載入 OpenSearch 儀表板後，選擇安全性，角色。然後，對應角色以允許其他使用者存取 OpenSearch 儀表板。

例如，您可將信任的同事 jroe 映射到 all_access 和 security_manager 角色。您也可以將後端角色 analysts 映射到 readall 和 opensearch_dashboards_user 角色。

如果您偏好使用 OpenSearch 儀表板API而不是儀表板，請參閱下列範例請求：

```
PATCH _plugins/_security/api/rolesmapping
[
  {
    "op": "add", "path": "/security_manager", "value": { "users": ["master-user",
 "jdoe", "jroe"], "backend_roles": ["admins"] }
  },
  {
    "op": "add", "path": "/all_access", "value": { "users": ["master-user", "jdoe",
 "jroe"], "backend_roles": ["admins"] }
  },
  {
    "op": "add", "path": "/readall", "value": { "backend_roles": ["analysts"] }
  },
  {
    "op": "add", "path": "/opensearch_dashboards_user", "value": { "backend_roles":
 ["analysts"] }
  }
]
```

同時設定 SP 和 IdP 啟動的身分驗證

如果您要設定 SP 和 IdP 啟動的身分驗證，則必須透過身分提供者進行設定。例如，在 Okta 中，您可以執行下列步驟：

1. 在您的SAML應用程序中，轉到常規，SAML設置。
2. 對於「單一登入」URL，請提供您的 IdP 啟動SSOURL。例如：`https://search-domain-hash/_dashboards/_opendistro/_security/saml/acs/idpinitiated`。
3. 啟用允許此應用程序請求其他SSOURLs。
4. 在 [可要求] 下 SSOURLs，新增一或多個 SP 啟動SSOURLs。例如：`https://search-domain-hash/_dashboards/_opendistro/_security/saml/acs`。

設定SAML驗證 (AWS CLI)

如下所示 AWS CLI 指令會針對現有網域上的 OpenSearch 儀表板啟用SAML驗證：

```
aws opensearch update-domain-config \
  --domain-name my-domain \
  --advanced-security-options '{"SAMLOptions":{"Enabled":true,"MasterUserName":"my-idp-user","MasterBackendRole":"my-idp-group-or-role","Idp":{"EntityId":"entity-id","MetadataContent":"metadata-content-with-quotes-escaped"},"RolesKey":"optional-roles-key","SessionTimeoutMinutes":180,"SubjectKey":"optional-subject-key"}}'
```

您必須逸出中繼資料中的所有引號和換行字元XML。例如，使用 `<KeyDescriptor use=\"signing\">\n`，而不是 `<KeyDescriptor use="signing">` 和換行符。如需使用的詳細資訊 AWS CLI，請參閱 AWS CLI 指令參考。

配置SAML身份驗證（配置API）

下列對組態的要求會API啟用現有網域上 OpenSearch 儀表板的SAML驗證：

```
POST https://es.us-east-1.amazonaws.com/2021-01-01/opensearch/domain/my-domain/config
{
  "AdvancedSecurityOptions": {
    "SAMLOptions": {
      "Enabled": true,
      "MasterUserName": "my-idp-user",
      "MasterBackendRole": "my-idp-group-or-role",
      "Idp": {
```

```
        "EntityId": "entity-id",
        "MetadataContent": "metadata-content-with-quotes-escaped"
      },
      "RolesKey": "optional-roles-key",
      "SessionTimeoutMinutes": 180,
      "SubjectKey": "optional-subject-key"
    }
  }
}
```

您必須逸出中繼資料中的所有引號和換行字元XML。例如，使用 `<KeyDescriptor use=\"signing\">\n`，而不是 `<KeyDescriptor use="signing">` 和換行符。如需有關使用組態的詳細資訊API，請參閱OpenSearch 服務API參考。

SAML疑難排

錯誤	詳細資訊
您的要求：'*/some/path* '是不允許的。	確認您已提供正確的 SSOURL(步驟 3) 給您的身分識別提供者。
請提供要啟用的有效身分提供者中繼資料文件SAML。	您的 IdP 中繼資料檔案不符合 SAML 2.0 標準。使用驗證工具檢查錯誤。
SAML控制台中看不到配置選項。	更新至最新服務軟體。
SAML配置錯誤：檢索SAML配置時出現錯誤，請檢查您的設置。	此一般性錯誤的發生原因很多。 • 檢查您是否向您的身份提供者提供了正確的 SP 實體 ID 和 SSOURL. • 重新產生 IdP 中繼資料檔案，並驗證 IdP 實體 ID。新增任何更新的中繼資料 AWS 控制台。 • 確認您的網域存取原則允許存取 OpenSearch 儀表板和`_plugins/_security/*` .一般而言，對於使用精細存取控制的網域，我們建議使用開放式存取政策。 • 如需設定的步驟，請參閱身分識別提供者的文件SAML。

錯誤	詳細資訊
缺少角色：此使用者沒有可用的角色，請聯絡您的系統管理員。	您已成功驗證，但SAML宣告中的使用者名稱和任何後端角色未對應至任何角色，因此沒有權限。這些映射區分大小寫。 您的系統管理員可以使用 SAML-tracer 等工具來驗證SAML判斷提示的內容，然後使用下列要求檢查您的角色對應： `GET _plugins/_security/api/rolesmapping`
嘗試存取 OpenSearch 儀表板時，您的瀏覽器會持續重新導向或收到 HTTP 500 個錯誤。	如果您的SAML宣告包含大量的角色總計約 1,500 個字元，就會發生這些錯誤。例如，如果您傳遞 80 個角色，平均長度為 20 個字元，您可能會超過 web 瀏覽器中 Cookie 的大小限制。從 2.7 OpenSearch 版開始，SAML斷言支持最多 5000 個字符的角色。
您無法登出ADFS。	ADFS需要簽署所有登出要求，哪些 OpenSearch 服務不支援。`<SingleLogoutService />` 從 IdP 中繼資料檔案中移除，以強制 OpenSearch 服務使用其自己的內部登出機制。
`Could not find entity descriptor for __PATH__.`	OpenSearch 服務的中繼資料XML中提供的 IdP 實體 ID 與SAML回應中的實體 ID 不同。要解決此問題，請確保它們匹配。在您的網域上啟用 CW 應用程式錯誤記錄檔，以尋找錯誤訊息以偵錯SAML整合問題。
`Signature validation failed. SAML response rejected.`	OpenSearch 服務無法使用中繼資料XML中提供的 IdP 憑證來驗證SAML回應中的簽章。這可能是手動錯誤，或者您的 IdP 已輪換其證書。透過XML提供給 OpenSearch 服務的中繼資料中，從您的 IdP 更新最新的憑證 AWS Management Console.

錯誤	詳細資訊
`__PATH__ is not a valid audience for this response.`	SAML回應中的對象欄位與網域端點不相符。若要修正此錯誤，請更新 SP 對象欄位以符合您的網域端點。如果您已啟用自訂端點，則對象欄位應與您的自訂端點相符。在您的網域上啟用 CW 應用程式錯誤記錄檔，以尋找錯誤訊息以偵錯SAML整合問題。
您的瀏覽器在響應`Invalid Request Id`中收到 HTTP 400 錯誤。	如果您已URL使用格式設定 IDP 起始，通常會發生此錯誤。`<DashboardsURL> /_opendistro/_security/saml/acs` 相反，請使用格URL式進行配置`<DashboardsURL> /_opendistro/_security/saml/acs/idpinitiated` 。
收到的回應是在，`__PATH__`而不是`__PATH__`。	SAML回應中的目的地欄位不符合下列其中一URL種格式： • `<DashboardsURL> /_opendistro/_security/saml/acs` • `<DashboardsURL> /_opendistro/_security/saml/acs/idpinitiated` . 根據您使用的登入流程 (SP 起始或 IDP 起始)，輸入符合其中一個的目的地欄位。 OpenSearch URLs
響應有一個`InResponseTo` 屬性，而沒`InResponseTo` 有預期。	您正在使用 IDP 起始的 SP 啟動URL的登入流程。請改用 SP 啟動URL。

停用SAML驗證

若要停用 OpenSearch 儀表板 (主控台) 的SAML驗證

1. 選擇網域、Actions (動作) 和 Edit security configuration (編輯安全組態)。
2. 取消勾選啟用SAML驗證。
3. 選擇 Save changes (儲存變更)。
4. 網域完成處理之後，請使用下列請求確認精細存取控制角色映射：

```
GET _plugins/_security/api/rolesmapping
```

停用儀表板的SAML驗證並不會移除主要使用者名稱和/或SAML主要後端角色的對應。SAML如果您要移除這些對映，請使用內部使用者資料庫 (如果啟用) 登入儀表板，或使用API將其移除：

```
PUT _plugins/_security/api/rolesmapping/all_access
{
  "users": [
    "master-user"
  ]
}
```

為儀表板設定 Amazon Cognito 份驗證 OpenSearch

您可以使用 Amazon Cognito 驗證和保護您的亞馬遜 OpenSearch 服務預設 OpenSearch儀表板安裝。Amazon Cognito 身份驗證是選用的，且僅適用於使用 OpenSearch 或彈性搜尋 5.1 或更新版本的網域。如果您不設定 Amazon Cognito 身分驗證，您仍然可以使用以 IP 為基礎的存取政策和代理伺服器、HTTP 基本身分驗證或 SAML 來保護 Dashboards。

大部分身份驗證程序都發生在 Amazon Cognito 中，但本節提供了將 Amazon Cognito 資源設定為與 OpenSearch 服務網域搭配使用的指導方針和要求。標準定價適用於所有 Amazon Cognito 資源。

> **Tip**
>
> 第一次設定網域以使用 OpenSearch 儀表板的 Amazon Cognito 身份驗證時，建議您使用主控台。Amazon Cognito 資源完全可自訂，而主控台可協助您識別和了解重要的功能。

主題

- 先決條件
- 設定網域以使用 Amazon Cognito 身分驗證
- 允許已經過身分驗證的角色
- 設定身分提供者
- (選用) 設定精細分級的存取
- (選用) 自訂登入頁面

- (選用) 設定進階安全性
- 測試
- 配額
- 常見的設定問題
- 停用儀表板的 Amazon Cognito 份驗證 OpenSearch
- 刪除針對儀表板使用 Amazon Cognito 身份驗證的 OpenSearch 網域

先決條件

您必須滿足數個先決條件，才能為 OpenSearch 儀表板設定 Amazon Cognito 身份驗證。 OpenSearch 服務主控台有助於簡化這些資源的建立，但瞭解每個資源的用途有助於設定和疑難排解。針對 Dashboards 的 Amazon Cognito 身分驗證需要下列資源：

- Amazon Cognito 使用者集區
- Amazon Cognito 身分集區
- 連接 `AmazonOpenSearchServiceCognitoAccess` 政策的 IAM 角色 (`CognitoAccessForAmazonOpenSearch`)

> **Note**
>
> 使用者集區和身分集區必須在相同的 AWS 區域。您可以使用相同的使用者集區、身分集區和 IAM 角色，將儀表板的 Amazon Cognito 身份驗證新增到多個 OpenSearch 服務網域。如需進一步了解，請參閱 the section called “配額”。

關於使用者集區

使用者集區有兩個主要功能：建立和管理使用者目錄，並讓使用者註冊和登入。如需建立使用者集區的說明，請參閱 Amazon Cognito 開發人員指南中的建立使用者集區。

當您建立要搭配 OpenSearch Service 使用的使用者集區時，請考量下列事項：

- 您的 Amazon Cognito 使用者集區必須擁有網域名稱。 OpenSearch 服務使用此網域名稱將使用者重新導向至登入頁面以存取儀表板。除了網域名稱，使用者集區不需要任何非預設組態。
- 您必須指定集區所需的標準屬性 - 例如名稱、出生日期、電子郵件地址和電話號碼等屬性。在您建立使用者集區之後您無法變更這些屬性，因此請選擇目前對您重要的屬性。

- 建立您的使用者集區時，選擇使用者是否可以建立自己的帳戶、帳戶的最低密碼強度，以及是否啟用多重要素驗證。如果您計劃使用外部身分提供者，這些設定是無關緊要的。通常，您可以讓使用者集區做為身分提供者並且啟用外部身分提供者，但大多數使用者偏好非此即彼。

使用者集區 ID 採用 *region*_*ID* 格式。如果您打算使用 AWS CLI 或 AWS SDK 來設定 OpenSearch 服務，請記下 ID。

關於身分集區

身分集區可讓您在使用者登入後將臨時受限的許可角色指派給使用者。如需有關建立身分集區的說明，請參閱 Amazon Cognito 開發人員指南中的身分集區。當您建立要搭配 OpenSearch Service 使用的身分識別集區時，請考量下列事項：

- 如果您使用 Amazon Cognito 主控台，您必須選擇 Enable access to unauthenticated identities (允許存取未經驗證的身分) 核取方塊，以建立身分集區。建立身分集區並設定 OpenSearch 服務網域後，Amazon Cognito 會停用此設定。
- 您不需要新增外部身分提供者到身分集區。當您將 OpenSearch 服務設定為使用 Amazon Cognito 身份驗證時，它會將身分集區設定為使用您剛建立的使用者集區。
- 建立身分集區之後，您必須選擇未經授權和經過授權的 IAM 角色。這些角色指定使用者登入前後的存取政策。如果您使用 Amazon Cognito 主控台，它可為您建立這些角色。在您建立經過授權的角色後，請記下採用 `arn:aws:iam::`*`123456789012`*`:role/Cognito_`*`identitypoolname`*`Auth_Role` 格式的 ARN。

身分集區 ID 採用 *region*:*ID*-*ID*-*ID*-*ID*-*ID* 格式。如果您打算使用 AWS CLI 或 AWS SDK 來設定 OpenSearch 服務，請記下 ID。

關於 CognitoAccessForAmazonOpenSearch角色

OpenSearch 服務需要許可才能設定 Amazon Cognito 使用者和身分集區，並將其用於身分驗證。您可以為此目的使用`AmazonOpenSearchServiceCognitoAccess`，這是一個AWS受管理的策略。 `AmazonESCognitoAccess`是服務重新命名為 Amazon OpenSearch 服務`AmazonOpenSearchServiceCognitoAccess`時所取代的舊版政策。這兩個政策提供啟用Cognito 身分驗證所必需的最低 Amazon Cognito 許可。如需了解政策 JSON，請參閱 IAM 主控台。

如果您使用主控台建立或設定 OpenSearch 服務網域，它會為您建立 IAM 角色，並將`AmazonOpenSearchServiceCognitoAccess`政策 (如果是 Elasticsearch 網域的`AmazonESCognitoAccess`政策) 附加至該角色。此角色的預設名稱為`CognitoAccessForAmazonOpenSearch`。

角色權限原則AmazonOpenSearchServiceCognitoAccess和AmazonESCognitoAccess兩者都允許 OpenSearch Service 在所有身分識別和使用者集區上完成下列動作：

- 動作：cognito-idp:DescribeUserPool
- 動作：cognito-idp:CreateUserPoolClient
- 動作：cognito-idp:DeleteUserPoolClient
- 動作：cognito-idp:UpdateUserPoolClient
- 動作：cognito-idp:DescribeUserPoolClient
- 動作：cognito-idp:AdminInitiateAuth
- 動作：cognito-idp:AdminUserGlobalSignOut
- 動作：cognito-idp:ListUserPoolClients
- 動作：cognito-identity:DescribeIdentityPool
- 動作：cognito-identity:SetIdentityPoolRoles
- 動作：cognito-identity:GetIdentityPoolRoles

如果您使用AWS CLI或其中一個 AWS SDK，則必須在設定 OpenSearch Service 網域時建立自己的角色、附加原則，並指定此角色的 ARN。角色必須具有下列信任關係：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "opensearchservice.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

如需說明，請參閱 IAM 使用者指南中的建立角色以委派許可給 AWS 服務和連接及分開 IAM 政策。

設定網域以使用 Amazon Cognito 身分驗證

完成先決條件後，您可以將 OpenSearch 服務網域設定為使用適用於儀表板的 Amazon Cognito。

> **Note**
>
> 並非所有 AWS 區域 皆可使用 Amazon Cognito。如需支援區域的清單，請參閱 AWS 區域 和節點。您不需要為用於 OpenSearch 服務的 Amazon Cognito 使用相同的區域。

設定 Amazon Cognito 身分驗證 (主控台)

由於主控台會為您建立CognitoAccessForAmazonOpenSearch角色，因此可提供最簡單的設定體驗。除了標準 OpenSearch 服務許可之外，您還需要以下一組許可，才能使用主控台建立使用 Amazon Cognito 身份驗證 OpenSearch 儀表板的網域。

```
{
  "Version": "2012-10-17",
  "Statement": [{
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeVpcs",
        "cognito-identity:ListIdentityPools",
        "cognito-idp:ListUserPools",
        "iam:CreateRole",
        "iam:AttachRolePolicy"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "iam:GetRole",
        "iam:PassRole"
      ],
      "Resource": "arn:aws:iam::123456789012:role/service-
role/CognitoAccessForAmazonOpenSearch"
    }
  ]
}
```

如需有關將許可新增至身分 (使用者、使用者群組或角色) 的說明，請參閱新增 IAM 身分許可 (主控台)。

如果 `CognitoAccessForAmazonOpenSearch` 已存在，您需要的許可更少：

```
{
  "Version": "2012-10-17",
  "Statement": [{
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeVpcs",
        "cognito-identity:ListIdentityPools",
        "cognito-idp:ListUserPools"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "iam:GetRole",
        "iam:PassRole"
      ],
      "Resource": "arn:aws:iam::123456789012:role/service-
role/CognitoAccessForAmazonOpenSearch"
    }
  ]
}
```

若要設定 Dashboards 的 Amazon Cognito 身分驗證 (主控台)

1. 在以下位置打開亞馬遜 OpenSearch 服務控制台 https://console.aws.amazon.com/aos/home/。
2. 在 Domains (網域) 下，選取您要設定的網域。
3. 選擇 Actions (動作)、Edit security configuration (編輯安全組態)。
4. 選擇 Enable Amazon Cognito authentication (啟用 Amazon Cognito 身分驗證)。
5. 對於 Region (區域)，選擇包含您的 Amazon Cognito 使用者集區與身分集區的 AWS 區域。
6. 對於 Cognito user pool (Cognito 使用者集區)，選擇使用者集區或建立集區。如需準則，請參閱the section called “關於使用者集區”。
7. 對於 Cognito identity pool (Cognito 身分集區)，選擇身分集區或建立集區。如需準則，請參閱the section called “關於身分集區”。

> **Note**
>
> Create user pool (建立使用者集區) 和 Create identity pool (建立身分集區) 連結會將您導向到 Amazon Cognito 主控台，並要求您手動建立這些資源。此程序不是自動的。如需進一步了解，請參閱 the section called “先決條件”。

8. 對於 IAM role name (IAM 角色名稱)，使用 `CognitoAccessForAmazonOpenSearch` 的預設值 (建議) 或輸入新名稱。若要進一步了解此角色的目的，請參閱the section called “關於CognitoAccessForAmazonOpenSearch角色”。
9. 選擇 Save Changes (儲存變更)。

在您的網域完成處理之後，請參閱the section called “允許已經過身分驗證的角色”和the section called “設定身分提供者”以取得其他設定步驟。

設定 Amazon Cognito 身分驗證 (AWS CLI)

使用`--cognito-options`參數來設定您的 OpenSearch 服務網域。由 `create-domain` 和 `update-domain-config` 命令使用以下語法：

```
--cognito-options Enabled=true,UserPoolId="user-pool-id",IdentityPoolId="identity-pool-id",RoleArn="arn:aws:iam::123456789012:role/CognitoAccessForAmazonOpenSearch"
```

範例

以下範例在 `us-east-1` 區域建立網域，該區域使用 `CognitoAccessForAmazonOpenSearch` 角色來啟用 Dashboards 的 Amazon Cognito 身分驗證，並提供對 `Cognito_Auth_Role` 的網域存取：

```
aws opensearch create-domain --domain-name my-domain --region us-east-1 --access-policies '{ "Version":"2012-10-17", "Statement":[{"Effect":"Allow","Principal":{"AWS": ["arn:aws:iam::123456789012:role/Cognito_Auth_Role"]},"Action":"es:ESHttp*","Resource":"arn:aws:es:us-east-1:123456789012:domain/*" }]}' --engine-version "OpenSearch_1.0" --cluster-config InstanceType=m4.xlarge.search,InstanceCount=1 --ebs-options EBSEnabled=true,VolumeSize=10 --cognito-options Enabled=true,UserPoolId="us-east-1_123456789",IdentityPoolId="us-east-1:12345678-1234-1234-1234-123456789012",RoleArn="arn:aws:iam::123456789012:role/CognitoAccessForAmazonOpenSearch"
```

在您的網域完成處理之後，請參閱the section called “允許已經過身分驗證的角色”和the section called “設定身分提供者”以取得其他設定步驟。

設定 Amazon Cognito 身分驗證 (AWS 開發套件)

開AWS發套件 (Android 和 iOS 開發套件除外) 支援亞馬遜 OpenSearch 服務 API 參考中定義的所有操作，包括`CreateDomain`和`UpdateDomainConfig`操作的`CognitoOptions`參數。如需安裝與使用 AWS 開發套件的詳細資訊，請參閱 AWS 軟體開發套件。

在您的網域完成處理之後，請參閱the section called “允許已經過身分驗證的角色”和the section called “設定身分提供者”以取得其他設定步驟。

允許已經過身分驗證的角色

依預設，您依照中的準則設定的已驗證 IAM 角色the section called “關於身分集區”沒有存取 OpenSearch 儀表板的必要權限。您必須提供該角色額外的許可。

> **Note**
>
> 如果您設定了精細的存取控制，並使用開放式或 IP 型存取原則，則可以略過此步驟。

您可以在以身分識別為基礎的原則中包含這些權限，但除非您希望經過驗證的使用者能夠存取所有 OpenSearch Service 網域，否則附加至單一網域的資源型原則是較好的方法。

針對 `Principal`，指定您使用 the section called “關於身分集區” 中的準則設定之 Cognito 經身分驗證角色的 ARN。

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Principal":{
            "AWS":[
               "arn:aws:iam::123456789012:role/Cognito_identitypoolnameAuth_Role"
            ]
         },
         "Action":[
            "es:ESHttp*"
         ],
         "Resource":"arn:aws:es:region:123456789012:domain/domain-name/*"
```

```
        }
    ]
}
```

如需將以資源為基礎的原則新增至 OpenSearch 服務網域的指示，請參閱the section called “設定存取政策”。

設定身分提供者

當您將網域設定為針對儀表板使用 Amazon Cognito 身份驗證時，Ser OpenSearch vice 會將應用程式用戶端新增到使用者集區，並將使用者集區作為身分驗證提供者新增至身分集區。

> **Warning**
>
> 不重新命名或刪除應用程式用戶端。

根據您設定使用者集區的方式而定，您可能需要手動建立使用者帳戶，或者使用者可以建立自己的帳戶。如果這些設定是可接受的，您便無需做進一步的動作。不過，許多人偏好使用外部身分提供者。

若要啟用 SAML 2.0 身分提供者，您必須提供 SAML 中繼資料文件。若要啟用社交身分提供者，例如，Login with Amazon、Facebook 和 Google，您必須擁有這些供應商提供的應用程式 ID 和應用程式密碼。您可以啟用任意組合的身分提供者。

設定使用者集區的最簡單方式就是使用 Amazon Cognito 主控台。如需說明，請參閱 Amazon Cognito 開發人員指南中的使用來自使用者集區的聯合和為您的使用者集區應用程式指定身分提供者設定。

(選用) 設定精細分級的存取

您可能已經注意到預設的身分集區設定指派每位登入的使用者相同的 IAM 角色 (`Cognito_identitypoolAuth_Role`)，這表示每位使用者可以存取相同的 AWS 資源。如果您想要搭配使用精細存取控制與 Amazon Cognito (例如，如果希望您組織的分析師擁有多個索引的唯讀存取權，而開發人員擁有所有索引的寫入存取權)，您有兩個選擇：

- 建立使用者群組並設定您的身分提供者，以根據使用者的身分驗證字符選擇 IAM 角色 (建議)。
- 設定您的身分提供者，以根據一個或多個規則選擇 IAM 角色。

如需包含精細存取控制的演練，請參閱 the section called “教學課程：使用 Cognito 身分驗證進行精細存取控制”。

> **Important**
>
> 與預設角色相似，Amazon Cognito 必須是每個額外角色信任關係的一部分。如需詳細資訊，請參閱 Amazon Cognito 開發人員指南中的建立角色以進行角色映射。

使用者群組和字符

當您建立使用者群組時，您為群組成員選擇 IAM 角色。如需有關建立群組的資訊，請參閱 Amazon Cognito 開發人員指南中的使用者群組。

在您建立一或多個使用者群組後，您可以設定您的驗證供應商，以指派使用者其群組的角色，而不是身分集區的預設角色。選取 Choose role from token (從字符中選擇角色)，然後選擇 Use default Authenticated role (使用預設已經過身分驗證的角色) 或 DENY (拒絕)，以指定身分集區應該如何處理不屬於群組的使用者。

規則

規則本質上是 Amazon Cognito 依序評估的一系列 `if` 陳述式。例如，如果使用者的電子郵件地址包含 `@corporate`，Amazon Cognito 會為該使用者指派 `Role_A`。如果使用者的電子郵件地址包含 `@subsidiary`，它會指派該使用者 `Role_B`。否則，它會指派使用者預設驗證角色。

若要進一步了解，請參閱 Amazon Cognito 開發人員指南中的使用以規則為基礎的映射來指派角色給使用者。

(選用) 自訂登入頁面

您可以使用 Amazon Cognito 主控台上傳自訂標誌，並對登入頁面進行 CSS 變更。如需 CSS 屬性的說明和完整清單，請參閱 Amazon Cognito 開發人員指南中的為您的使用者集區指定應用程式 UI 自訂設定。

(選用) 設定進階安全性

Amazon Cognito 使用者集區支援進階安全功能，例如多重驗證、遭盜用認證檢查和調整式驗證。如需進一步了解，請參閱 Amazon Cognito 開發人員指南中的管理安全性。

測試

在您滿意您的設定之後，請驗證使用者體驗是否符合您的期望。

存取 OpenSearch 儀表板

1. 在 Web 瀏覽器中導覽至 `https://opensearch-domain/_dashboards`。若要直接登入特定租用戶，請將 `?security_tenant=tenant-name` 附加至 URL。
2. 使用您慣用的登入資料登入。
3. 載入 OpenSearch 儀表板之後，請至少設定一個索引模式。Dashboards 使用這些模式來識別您要分析的索引。輸入 `*`，選擇 Next step (下一步)，然後選擇 Create index pattern (建立索引模式)。
4. 若要搜尋或探索您的資料，請選擇 Discover (探索)。

如果此程序中的任何步驟失敗，請參閱the section called “常見的設定問題”以取得故障診斷資訊。

配額

Amazon Cognito 對於許多資源有軟性限制。如果您想要為大量 OpenSearch 服務網域啟用儀表板身份驗證，請檢閱 Amazon Cognito 中的配額，並視需要增加請求限制。

每個 OpenSearch 服務網域都會將應用程式用戶端新增至使用者集區，以便將驗證提供者新增至身分識別集區。如果您為 10 個以上的網域啟用 OpenSearch 儀表板身份驗證，則可能會遇到「每個身分集區的 Amazon Cognito 使用者集區提供者上限」限制。如果您超過限制，您嘗試設定為使用儀表板的 Amazon Cognito 身份驗證的任何 OpenSearch 服務網域都可能會卡在「處理」的組態狀態。

常見的設定問題

下表列出常見的設定問題和解決方案。

配置 OpenSearch 服務

問題	解決方案
`OpenSearch Service can't create the role` (主控台)	您沒有正確的 IAM 許可。新增 the section called “設定 Amazon Cognito 身分驗證 (主控台)” 中指定的許可。

`User is not authorized to perform: iam:PassRole on resource CognitoAccessForAmazonOpenSearch` (主控台)	您沒有該CognitoAccessForAmazonOpenSearch角色的`iam:PassRole` 權限。將下列政策連接至您的帳戶：
	`{`
	`"Version": "2012-10-17",`
	`"Statement": [`
	`{`

問題	解決方案
	`"Effect": "Allow", "Action": [ "iam:PassRole" ], "Resource": "arn:aws:iam:: 123456789012:role/service-role/CognitoAccessForAmazonOpenSearch " } ] }` 或者，您可以連接 `IAMFullAccess` 政策。
`User is not authorized to perform: cognito-identity:ListIdentityPools on resource`	您沒有 Amazon Cognito 的讀取許可。將 `AmazonCognitoReadOnly` 政策連接至您的帳戶。
`An error occurred (ValidationException) when calling the CreateDomain operation: OpenSearch Service must be allowed to use the passed role`	OpenSearch 未在`CognitoAccessForAmazonOpenSearch` 角色的信任關係中指定服務。確認您的角色使用 the section called “關於 CognitoAccessForAmazonOpenSearch角色” 中指定的信任關係。或者，使用主控台來設定 Amazon Cognito 身分驗證。主控台會為您建立一個角色。
`An error occurred (ValidationException) when calling the CreateDomain operation: User is not authorized to perform: cognito-idp: action on resource: user pool`	在 `--cognito-options` 中指定的角色沒有存取 Amazon Cognito 的許可。確認角色已與 AWS 受管 `AmazonOpenSearchServiceCognitoAccess` 政策連接。或者，使用主控台來設定 Amazon Cognito 身分驗證。主控台會為您建立一個角色。

問題	解決方案
`An error occurred (ValidationException) when calling the CreateDomain operation : User pool does not exist`	OpenSearch 服務找不到使用者集區。確認您已建立一個且具有正確的 ID。若要尋找 ID，您可以使用 Amazon Cognito 主控台或以下 AWS CLI 命令： `aws cognito-idp list-user-pools --max-results 60 --region region`
`An error occurred (ValidationException) when calling the CreateDomain operation : IdentityPool not found`	OpenSearch 服務找不到身分集區。確認您已建立一個且具有正確的 ID。若要尋找 ID，您可以使用 Amazon Cognito 主控台或以下 AWS CLI 命令： `aws cognito-identity list-identity-pools --max-results 60 --region region`
`An error occurred (ValidationException) when calling the CreateDomain operation : Domain needs to be specified for user pool`	使用者集區沒有網域名稱。您可以使用 Amazon Cognito 主控台或以下 AWS CLI 命令來設定一個： `aws cognito-idp create-user-pool-domain --domain name --user-pool-id id`

存取 OpenSearch 儀表板

問題	解決方案
登入頁面不會顯示我慣用的身分提供者。	檢查您是否已依照中的指定啟用 OpenSearch 服務應用程式用戶端的身分識別提供者the section called “設定身分提供者”。
登入頁面看起來不似與我的組織關聯。	請參閱 the section called “(選用) 自訂登入頁面”。
我的登入資料無法運作。	確認您已如 the section called “設定身分提供者” 中所指定，來設定身分提供者。

問題	解決方案
	如果您使用使用者集區做為身分提供者，請檢查該帳戶是否存在於 Amazon Cognito 主控台上。
OpenSearch 儀表板根本不加載或無法正常工作。	Amazon Cognito 經過身分驗證的角色需要網域 (/*) 的 `es:ESHttp*` 許可來存取和使用 Dashboards。如 the section called “允許已經過身分驗證的角色” 中所指定，檢查您新增的存取政策。
當我從一個索引標籤登出 OpenSearch 儀表板時，剩餘的索引標籤會顯示一則訊息，指出重新整理權杖已被撤銷。	當您在使用 Amazon Cognito 身份驗證時登出 OpenSearch 儀表板工作階段時， OpenSearch 服務會執行一項AdminUserGlobalSignOut作業，將您登出所有使用中的 OpenSearch 儀表板工作階段。
`Invalid identity pool configuration. Check assigned IAM roles for this pool.`	Amazon Cognito 無權代表已經過身分驗證的使用者擔任 IAM 角色。修改角色的信任關係，使其包含：

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Principal": {
      "Federated": "cognito-identity.
amazonaws.com"
    },
    "Action": "sts:AssumeRoleWithWebIdent
ity",
    "Condition": {
      "StringEquals": {
        "cognito-identity.amazonaws.com:aud"
: " identity-pool-id "
      },
      "ForAnyValue:StringLike": {
        "cognito-identity.amazonaws.com:amr"
: "authenticated"
      }
    }
  }]
}
```

問題	解決方案
`Token is not from a supported provider of this identity pool.`	當您從使用者集區移除應用程式用戶端時，可能發生此少見的錯誤。嘗試在新的瀏覽器工作階段中開啟 Dashboards。

停用儀表板的 Amazon Cognito 份驗證 OpenSearch

使用下列步驟來停用 Dashboards 的 Amazon Cognito 身分驗證。

若要停用 Dashboards 的 Amazon Cognito 身分驗證 (主控台)

1. 在以下位置打開亞馬遜 OpenSearch 服務控制台 https://console.aws.amazon.com/aos/home/。
2. 在 Domains (網域) 下，選擇您要設定的網域。
3. 選擇 Actions (動作)、Edit security configuration (編輯安全組態)。
4. 取消選擇 Enable Amazon Cognito authentication (啟用 Amazon Cognito 身分驗證)。
5. 選擇 Save Changes (儲存變更)。

> **Important**
> 如果您不再需要 Amazon Cognito 使用者集區和身分集區，請刪除它們。否則，您需繼續負擔費用。

刪除針對儀表板使用 Amazon Cognito 身份驗證的 OpenSearch 網域

若要防止使用適用於儀表板的 Amazon Cognito 身份驗證的網域卡在處理的組態狀態中，請先刪除 OpenSearch 服務網域，然後再刪除其相關聯的 Amazon Cognito 使用者和身分集區。

針對 Amazon OpenSearch 服務使用服務連結角色

Amazon OpenSearch 服務使用 AWS Identity and Access Management (IAM) 服務連結角色。服務連結角色是直接連結至 OpenSearch 服務的唯一 IAM 角色類型。服務連結角色由 OpenSearch Service 預先定義，並包含服務代表您呼叫其他服 AWS 務所需的所有權限。

服務連結角色可讓您更輕鬆地設定 OpenSearch 服務，因為您不需要手動新增必要的權限。OpenSearch 服務會定義其服務連結角色的權限，除非另有定義，否則只有 OpenSearch Service 可以擔任其角色。定義的許可包括信任政策和許可政策，且該許可政策無法附加至其他 IAM 實體。如需服務連結角色和許可政策的更新，請參閱 Amazon OpenSearch 服務的文件歷史記錄。

如需關於支援服務連結角色的其他服務資訊，請參閱《可搭配 IAM 運作的AWS 服務》，尋找服務連結角色欄中顯示為是的服務。選擇具有連結的是，以檢視該服務的服務連結角色文件。

主題

- 使用服務連結角色建立 VPC 網域
- 使用服務連結角色建立 OpenSearch 無伺服器集合
- 使用服務連結角色建立 OpenSearch 擷取管道

使用服務連結角色建立 VPC 網域

Amazon OpenSearch 服務使用 AWS Identity and Access Management (IAM) 服務連結角色。服務連結角色是直接連結至 OpenSearch 服務的唯一 IAM 角色類型。服務連結角色由 OpenSearch Service 預先定義，並包含服務代表您呼叫其他服 AWS 務所需的所有權限。

OpenSearch 服務使用名為的服務連結角色 AWSServiceRoleForAmazonOpenSearchService，提供角色所需的最低 Amazon EC2 和 Elastic Load Balancing 許可，以啟用網域的 VPC 存取。

舊版 Elasticsearch 角色

Amazon OpenSearch 服務使用稱為`AWSServiceRoleForAmazonOpenSearchService`的服務鏈接角色。您的帳戶可能也會包含名為 `AWSServiceRoleForAmazonElasticsearchService` 的舊版服務連結角色，其使用已被淘汰的 Elasticsearch API 端點運作。

如果舊版 Elasticsearch 角色不存在於您的帳戶中， OpenSearch 服務會在您第一次建立網域時自動建立新的 OpenSearch 服務連結角色。 OpenSearch 否則，您的帳戶將繼續使用 Elasticsearch 角色。若要讓此自動建立作業順利完成，您必須具有 `iam:CreateServiceLinkedRole` 動作的許可。

許可

`AWSServiceRoleForAmazonOpenSearchService` 服務連結角色信任下列服務以擔任角色：

- `opensearchservice.amazonaws.com`

名為的角色權限原則AmazonOpenSearchServiceRolePolicy允許 OpenSearch Service 對指定的資源完成下列動作：

- 動作：* 上的 acm:DescribeCertificate
- 動作：* 上的 cloudwatch:PutMetricData
- 動作：* 上的 ec2:CreateNetworkInterface
- 動作：* 上的 ec2:DeleteNetworkInterface
- 動作：* 上的 ec2:DescribeNetworkInterfaces
- 動作：* 上的 ec2:ModifyNetworkInterfaceAttribute
- 動作：* 上的 ec2:DescribeSecurityGroups
- 動作：* 上的 ec2:DescribeSubnets
- 動作：* 上的 ec2:DescribeVpcs
- 動作：在所有網路介面和 VPC 端點進行 ec2:CreateTags
- 動作：* 上的 ec2:DescribeTags
- 動作：當請求包含標籤 OpenSearchManaged=true 時，在所有 VPC、安全群組、子網路和路由表，以及所有 VPC 端點上進行 ec2:CreateVpcEndpoint
- 動作：當請求包含標籤 OpenSearchManaged=true 時，在所有 VPC、安全群組、子網路和路由表，以及所有 VPC 端點上進行 ec2:ModifyVpcEndpoint
- 動作：當請求包含標籤 OpenSearchManaged=true 時，在所有端點上進行 ec2:DeleteVpcEndpoints
- 動作：* 上的 ec2:AssignIpv6Addresses
- 動作：* 上的 ec2:UnAssignIpv6Addresses
- 動作：* 上的 elasticloadbalancing:AddListenerCertificates
- 動作：* 上的 elasticloadbalancing:RemoveListenerCertificates

您必須設定許可，IAM 實體 (如使用者、群組或角色) 才可建立、編輯或刪除服務連結角色。如需詳細資訊，請參閱 IAM 使用者指南中的服務連結角色許可。

建立 服務連結角色

您不需要手動建立一個服務連結角色。當您使用建立已啟用 VPC 的網域時 AWS Management Console， OpenSearch 服務會為您建立服務連結角色。若要讓此自動建立作業順利完成，您必須具有 iam:CreateServiceLinkedRole 動作的許可。

您也可以使用 IAM 主控台、IAM CLI 或 IAM API 來手動建立服務連結角色。如需詳細資訊，請參閱 IAM 使用者指南中的建立服務連結角色。

編輯服務連結角色

OpenSearch 服務不允許您編輯服`AWSServiceRoleForAmazonOpenSearchService`務連結角色。因為可能有各種實體會參考服務連結角色，所以您無法在建立角色之後變更其名稱。然而，您可使用 IAM 來編輯角色描述。如需詳細資訊，請參閱 IAM 使用者指南中的編輯服務連結角色。

刪除 服務連結角色

若您不再使用需要服務連結角色的功能或服務，我們建議您刪除該角色。如此一來，您就沒有未主動監控或維護的未使用實體。然而，務必清除您的服務連結角色，之後才能以手動方式將其刪除。

清除 服務連結角色

您必須先確認服務連結角色沒有作用中的工作階段，並移除該角色使用的資源，之後才能使用 IAM 將其刪除。

檢查服務連結角色是否於 IAM 主控台有作用中的工作階段

1. 登入 AWS Management Console 並開啟 IAM 主控台，網址為 https://console.aws.amazon.com/iam/。
2. 在 IAM 主控台的導覽窗格中，選擇角色。然後選擇 `AWSServiceRoleForAmazonOpenSearchService` 角色的名稱 (而非核取方塊)。
3. 在所選角色的 Summary (摘要) 頁面中，選擇 Access Advisor (存取 Advisor) 分頁。
4. 在 Access Advisor (存取 Advisor) 分頁中，檢閱服務連結角色的近期活動。

> **Note**
>
> 如果您不確定 OpenSearch 服務是否使用該`AWSServiceRoleForAmazonOpenSearchService`角色，可以嘗試刪除角色。如果服務正在使用該角色，則刪除會失敗，而您可以檢視正在使用該角色的資源。如果角色正在使用中，則您必須先等到工作階段結束，才能刪除該角色，及/或刪除正在使用該角色的資源。您無法撤銷服務連結角色的工作階段。

手動刪除服務連結角色

從 IAM 主控台、API 或 AWS CLI 刪除服務連結角色。如需相關說明，請參閱 IAM 使用者指南中的刪除服務連結角色。

使用服務連結角色建立 OpenSearch 無伺服器集合

OpenSearch 無伺服器使用 AWS Identity and Access Management (IAM) 服務連結角色。服務連結角色是直接連結至 OpenSearch 服務的唯一 IAM 角色類型。服務連結角色由 OpenSearch Service 預先定義，並包含服務代表您呼叫其他服 AWS 務所需的所有權限。

OpenSearch 無伺服器會使用名為的服務連結角色 AWSServiceRoleForAmazonOpenSearchServerless，為角色提供將無伺服器相關 CloudWatch指標發佈到您的帳戶所需的權限。與相關聯的角色權限原 AWSServiceRoleForAmazonOpenSearchServerless 則命名為`AmazonOpenSearchServerlessServiceRolePolicy`。如需有關策略的詳細資訊，請參閱《AWS 受管理策略參考指南》AmazonOpenSearchServerlessServiceRolePolicy中的。

無伺服器 OpenSearch 的服務連結角色權限

OpenSearch 無伺服器使用名為的服務連結角色 AWSServiceRoleForAmazonOpenSearchServerless，可讓 OpenSearch 無伺服器代表您呼叫 AWS 服務。

服 AWSServiceRoleForAmazonOpenSearchServerless 務連結角色會信任下列服務擔任該角色：

- `observability.aoss.amazonaws.com`

名為的角色權限原則`AmazonOpenSearchServerlessServiceRolePolicy`允許 OpenSearch 無伺服器對指定的資源完成下列動作：

- 動作：`cloudwatch:PutMetricData`在所有 AWS 資源上

> **Note**
>
> 此原則包含條件索引鍵`{"StringEquals": {"cloudwatch:namespace": "AWS/AOSS"}}`，這表示服務連結角色只能將指標資料傳送至`AWS/AOSS` CloudWatch命名空間。

您必須設定許可，IAM 實體 (如使用者、群組或角色) 才可建立、編輯或刪除服務連結角色。如需詳細資訊，請參閱 IAM 使用者指南中的服務連結角色許可。

建立無伺服器的服務連結角色 OpenSearch

您不需要手動建立一個服務連結角色。當您在 AWS Management Console、或 AWS API 中建立 OpenSearch 無伺服器集合時 AWS CLI， OpenSearch 無伺服器會為您建立服務連結角色。

> **Note**
>
> 第一次建立集合時，必須在以身分為基礎的政策中指派 `iam:CreateServiceLinkedRole` 給您。

若您刪除此服務連結角色，之後需要再次建立，您可以在帳戶中使用相同程序重新建立角色。當您建立 OpenSearch 無伺服器集合時， OpenSearch 無伺服器會再次為您建立服務連結角色。

您也可以使用 IAM 主控台建立具有 Amazon OpenSearch 無伺服器使用案例的服務連結角色。在 AWS CLI 或 AWS API 中，使用`observability.aoss.amazonaws.com`服務名稱建立服務連結角色：

```
aws iam create-service-linked-role --aws-service-name
 "observability.aoss.amazonaws.com"
```

如需詳細資訊，請參閱《IAM 使用者指南》中的「建立服務連結角色」。如果您刪除此服務連結角色，您可以使用此相同的程序以再次建立該角色。

編輯無伺服器的服務連結角色 OpenSearch

OpenSearch 無伺服器不允許您編輯 AWSServiceRoleForAmazonOpenSearchServerless 服務連結角色。因為可能有各種實體會參考服務連結角色，所以您無法在建立角色之後變更其名稱。然而，您可使用 IAM 來編輯角色描述。如需詳細資訊，請參閱 IAM 使用者指南中的編輯服務連結角色。

刪除無伺服器的服務連結角色 OpenSearch

若您不再使用需要服務連結角色的功能或服務，我們建議您刪除該角色。這會防止您擁有未主動監控或維護的未使用實體。然而，在手動刪除服務連結角色之前，您必須先清除資源。

若要刪除 AWSServiceRoleForAmazonOpenSearchServerless，您必須 OpenSearch 先刪除. AWS 帳戶

> **Note**
>
> 如果 OpenSearch 無伺服器在您嘗試刪除資源時使用此角色，則刪除作業可能會失敗。若此情況發生，請等待數分鐘後並再次嘗試操作。

使用 IAM 手動刪除服務連結角色

使用 IAM 主控台或 AWS API 刪除 AWSServiceRoleForAmazonOpenSearchServerless服務連結角色。 AWS CLI如需詳細資訊，請參閱《IAM 使用者指南》中的刪除服務連結角色。

OpenSearch 無伺服器服務連結角色的支援區域

OpenSearch 無伺服器支援在每個提供無伺 AWSServiceRoleForAmazonOpenSearchServerless 服器服務的區域中使用服務連結角色。 OpenSearch 如需支援區域的清單，請參閱. OpenSearch AWS 一般參考

使用服務連結角色建立 OpenSearch 擷取管道

Amazon OpenSearch 擷取使用 AWS Identity and Access Management (IAM) 服務連結角色。服務連結角色是直接連結至 OpenSearch 擷取的唯一 IAM 角色類型。服務連結角色是由 OpenSearch Intetion 預先定義的，並包含服務代表您呼叫其他 AWS 服務所需的所有權限。

OpenSearch 擷取會使用名為的服務連結角色 AWSServiceRoleForAmazonOpenSearchIngestionService，除非您使用自我管理的 VPC，在此情況下，它會使用名為的服務連結角色。AWSServiceRoleForOpensearchIngestionSelfManagedVpce連結的原則會提供角色在帳戶與 OpenSearch 擷取之間建立虛擬私有雲端 (VPC) 所需的權限，以及將 CloudWatch指標發佈到您的帳戶。

許可

`AWSServiceRoleForAmazonOpenSearchIngestionService` 服務連結角色信任下列服務以擔任角色：

- `osis.amazon.com`

名為的角色權限原則`AmazonOpenSearchIngestionServiceRolePolicy`允許 OpenSearch 擷取對指定的資源完成下列動作：

- 動作：`*` 上的 `ec2:DescribeSubnets`

- 動作：* 上的 ec2:DescribeSecurityGroups
- 動作：* 上的 ec2:DeleteVpcEndpoints
- 動作：* 上的 ec2:CreateVpcEndpoint
- 動作：* 上的 ec2:DescribeVpcEndpoints
- 動作：arn:aws:ec2:*:*:network-interface/* 上的 ec2:CreateTags
- 動作：cloudwatch:namespace": "AWS/OSIS" 上的 cloudwatch:PutMetricData

AWSServiceRoleForOpensearchIngestionSelfManagedVpce 服務連結角色信任下列服務以擔任角色：

- self-managed-vpce.osis.amazon.com

名為的角色權限原則OpenSearchIngestionSelfManagedVpcePolicy允許 OpenSearch 擷取對指定的資源完成下列動作：

- 動作：* 上的 ec2:DescribeSubnets
- 動作：* 上的 ec2:DescribeSecurityGroups
- 動作：* 上的 ec2:DescribeVpcEndpoints
- 動作：cloudwatch:namespace": "AWS/OSIS" 上的 cloudwatch:PutMetricData

您必須設定許可，IAM 實體 (如使用者、群組或角色) 才可建立、編輯或刪除服務連結角色。如需詳細資訊，請參閱 IAM 使用者指南中的服務連結角色許可。

建立用 OpenSearch 於擷取的服務連結角色

您不需要手動建立一個服務連結角色。當您在 AWS Management Console、或 AWS API 中建立 OpenSearch 擷取管線時 AWS CLI， OpenSearch 擷取會為您建立服務連結角色。

若您刪除此服務連結角色，之後需要再次建立，您可以在帳戶中使用相同程序重新建立角色。建立 OpenSearch 擷取管線時， OpenSearch 擷取會再次為您建立服務連結角色。

編輯擷取的服務連結角色 OpenSearch

OpenSearch 擷取不允許您編輯AWSServiceRoleForAmazonOpenSearchIngestionService服務連結角色。因為有各種實體可能會參考服務連結角色，所以您無法在建立角色之後變更角色名稱。然而，您可使用 IAM 來編輯角色描述。如需詳細資訊，請參閱 IAM 使用者指南中的編輯服務連結角色。

刪除擷取的服務連結角色 OpenSearch

若您不再使用需要服務連結角色的功能或服務，我們建議您刪除該角色。如此一來，您就沒有未主動監控或維護的未使用實體。然而，在手動刪除服務連結角色之前，您必須先清除資源。

清除服務連結角色

在您使用 IAM 刪除服務連結角色之前，您必須先刪除該角色所使用的任何資源。

> **Note**
>
> 如果您嘗試刪除資源時 OpenSearch 擷取正在使用此角色，則刪除可能會失敗。若此情況發生，請等待數分鐘後並再次嘗試操作。

刪除**AWSServiceRoleForAmazonOpenSearchIngestionService**或**AWSServiceRoleForOpensearchI**色使用的 OpenSearch 擷取資源

1. 導覽至 Amazon OpenSearch 服務主控台，然後選擇擷取。
2. 刪除所有配管。如需說明，請參閱the section called “刪除配管”。

刪除擷取的服務連結角色 OpenSearch

您可以使用 OpenSearch 擷取主控台刪除服務連結角色。

刪除服務連結角色 (主控台)

1. 導覽至 IAM 主控台。
2. 選擇「角色」，然後搜尋AWSServiceRoleForAmazonOpenSearchIngestionService或AWSServiceRoleForOpensearchIngestio色。
3. 選取角色，然後選擇刪除。

亞馬遜示例代碼OpenSearch服務

本章包含與亞馬遜工作的常見示例代碼OpenSearch服務：使用各種編程語言進行 HTTP 請求簽名，壓縮 HTTP 請求主體，並使用AWS用來建立網域的 SDK。

主題

- Elasticsearch 用戶端相容性
- 在 Amazon OpenSearch 服務中壓縮 HTTP 請求
- 使用AWS與亞馬遜互動的 SDKOpenSearch服務

Elasticsearch 用戶端相容性

Elasticsearch 用戶端的最新版本可能包含會人為破壞相容性的授權或版本檢查。下表包含建議使用哪些用戶端版本以獲得最佳相容性OpenSearch服務。

> **Important**
> 這些用戶端版本已過時，且不會使用最新相依性 (包括 Log4j) 進行更新。我們強烈建議您使用OpenSearch在可能的情況下，用戶端的版本。

用戶端	建議的版本
Java 低階 REST 用戶端	7.13.4
Java 高階 REST 用戶端	7.13.4
Python Elasticsearch 用戶端	7.13.4
Ruby Elasticsearch 用戶端	7.13.3
Node.js Elasticsearch 用戶端	7.13.0

在 Amazon OpenSearch 服務中壓縮 HTTP 請求

您可以使用 gzip 壓縮來壓縮 Amazon OpenSearch 服務網域中的 HTTP 請求和回應。Gzip 壓縮可以幫助您減少文件的大小，降低頻寬使用率和延遲，進而提高傳輸速度。

所有運行 OpenSearch 或彈性搜索 6.0 或更高版本的域都支持 Gzip 壓縮。有些用 OpenSearch 戶端內建 gzip 壓縮支援，而且許多程式設計語言都有簡化程序的程式庫。

啟用 gzip 壓縮

不要與類似的 OpenSearch 設置混淆，特定`http_compression.enabled`於 OpenSearch 服務，並啟用或禁用域上的 gzip 壓縮。域運行 OpenSearch 或彈性搜索 7. x 默認情況下啟用了 gzip 壓縮，而運行彈性搜索 6 的域。 x 默認情況下禁用它。

若要啟用 gzip 壓縮，請傳送以下請求：

```
PUT _cluster/settings
{
  "persistent" : {
    "http_compression.enabled": true
  }
}
```

對 `_cluster/settings` 的請求必須解壓縮，因此您可能需要使用單獨的用戶端或標準 HTTP 請求來更新叢集設定。

若要確認您已成功啟用 gzip 壓縮，請傳送下列要求：

```
GET _cluster/settings?include_defaults=true
```

確保您在響應中看到以下設置：

```
...
"http_compression": {
  "enabled": "true"
}
...
```

必要標頭

當包含 gzip 壓縮的要求主體時，請保留標準 `Content-Type: application/json` 標頭，並新增 `Content-Encoding: gzip` 標頭。若要接受 gzip 壓縮的回應，請也新增 `Accept-Encoding: gzip` 標頭。如果用 OpenSearch 戶端支援 gzip 壓縮，則可能會自動包含這些標頭。

範本程式碼 (Python 3)

下列範例使用 opensearch-py 來執行壓縮並傳送請求。此程式碼使用您的 IAM 憑證來簽署請求。

```
from opensearchpy import OpenSearch, RequestsHttpConnection
from requests_aws4auth import AWS4Auth
import boto3

host = '' # e.g. my-test-domain.us-east-1.es.amazonaws.com
region = '' # e.g. us-west-1
service = 'es'
credentials = boto3.Session().get_credentials()
awsauth = AWS4Auth(credentials.access_key, credentials.secret_key, region, service,
 session_token=credentials.token)

# Create the client.
search = OpenSearch(
    hosts = [{'host': host, 'port': 443}],
    http_auth = awsauth,
    use_ssl = True,
    verify_certs = True,
    http_compress = True, # enables gzip compression for request bodies
    connection_class = RequestsHttpConnection
)

document = {
  "title": "Moneyball",
  "director": "Bennett Miller",
  "year": "2011"
}

# Send the request.
print(search.index(index='movies', id='1', body=document, refresh=True))

# print(search.index(index='movies', doc_type='_doc', id='1', body=document,
 refresh=True))
```

或者，您可以指定適當的標頭，自己壓縮要求主體，並使用標準的 HTTP 程式庫，例如請求。此程式碼使用 HTTP 基本憑證來簽署請求，如果您使用精細存取控制，則您的網域可能會支援。

```
import requests
import gzip
import json

base_url = '' # The domain with https:// and a trailing slash. For example, https://my-test-domain.us-east-1.es.amazonaws.com/
auth = ('master-user', 'master-user-password') # For testing only. Don't store
 credentials in code.

headers = {'Accept-Encoding': 'gzip', 'Content-Type': 'application/json',
           'Content-Encoding': 'gzip'}

document = {
  "title": "Moneyball",
  "director": "Bennett Miller",
  "year": "2011"
}

# Compress the document.
compressed_document = gzip.compress(json.dumps(document).encode())

# Send the request.
path = 'movies/_doc?refresh=true'
url = base_url + path
response = requests.post(url, auth=auth, headers=headers, data=compressed_document)
print(response.status_code)
print(response.text)
```

使用AWS與亞馬遜互動的 SDKOpenSearch服務

本節包括如何使用AWS與亞馬遜互動的 SDKOpenSearch服務設定 API。這些程式碼範例示範如何建立、更新和刪除OpenSearch服務網域。

Java

本節包含 AWS SDK for Java 版本 1 和 2 的範例。

Version 2

此範例使用OpenSearchClientBuilder來自版本 2 的構造函數AWS SDK for Java以建立OpenSearch網域，更新其組態，然後將其刪除。取消對 `waitForDomainProcessing` 呼叫的註解 (並對 `deleteDomain` 呼叫加上註解)，以允許網域上線並變得可用。

```
package com.example.samples;

import java.util.concurrent.TimeUnit;
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.opensearch.OpenSearchClient;
import software.amazon.awssdk.services.opensearch.model.ClusterConfig;
import software.amazon.awssdk.services.opensearch.model.EBSOptions;
import software.amazon.awssdk.services.opensearch.model.CognitoOptions;
import software.amazon.awssdk.services.opensearch.model.NodeToNodeEncryptionOptions;
import software.amazon.awssdk.services.opensearch.model.CreateDomainRequest;
import software.amazon.awssdk.services.opensearch.model.CreateDomainResponse;
import software.amazon.awssdk.services.opensearch.model.DescribeDomainRequest;
import software.amazon.awssdk.services.opensearch.model.UpdateDomainConfigRequest;
import software.amazon.awssdk.services.opensearch.model.UpdateDomainConfigResponse;
import software.amazon.awssdk.services.opensearch.model.DescribeDomainResponse;
import software.amazon.awssdk.services.opensearch.model.DeleteDomainRequest;
import software.amazon.awssdk.services.opensearch.model.DeleteDomainResponse;
import software.amazon.awssdk.services.opensearch.model.OpenSearchException;
import software.amazon.awssdk.auth.credentials.DefaultCredentialsProvider;

/**
 * Sample class demonstrating how to use the Amazon Web Services SDK for Java to
 create, update,
 * and delete Amazon OpenSearch Service domains.
 */

public class OpenSearchSample {

    public static void main(String[] args) {

     String domainName = "my-test-domain";

     // Build the client using the default credentials chain.
        // You can use the CLI and run `aws configure` to set access key, secret
        // key, and default region.

        OpenSearchClient client = OpenSearchClient.builder()
```

```
          // Unnecessary, but lets you use a region different than your default.
          .region(Region.US_EAST_1)
          // Unnecessary, but if desired, you can use a different provider chain.
          .credentialsProvider(DefaultCredentialsProvider.create())
                    .build();

        // Create a new domain, update its configuration, and delete it.
        createDomain(client, domainName);
        //waitForDomainProcessing(client, domainName);
        updateDomain(client, domainName);
        //waitForDomainProcessing(client, domainName);
        deleteDomain(client, domainName);
    }

    /**
     * Creates an Amazon OpenSearch Service domain with the specified options.
     * Some options require other Amazon Web Services resources, such as an Amazon
Cognito user pool
     * and identity pool, whereas others require just an instance type or instance
     * count.
     *
     * @param client
     *            The client to use for the requests to Amazon OpenSearch Service
     * @param domainName
     *            The name of the domain you want to create
     */

    public static void createDomain(OpenSearchClient client, String domainName) {

     // Create the request and set the desired configuration options

        try {

            ClusterConfig clusterConfig = ClusterConfig.builder()
                    .dedicatedMasterEnabled(true)
                    .dedicatedMasterCount(3)
                    // Small, inexpensive instance types for testing. Not
recommended for production.
                    .dedicatedMasterType("t2.small.search")
                    .instanceType("t2.small.search")
                    .instanceCount(5)
                    .build();

            // Many instance types require EBS storage.
```

```
            EBSOptions ebsOptions = EBSOptions.builder()
                    .ebsEnabled(true)
                    .volumeSize(10)
                    .volumeType("gp2")
                    .build();

            NodeToNodeEncryptionOptions encryptionOptions =
 NodeToNodeEncryptionOptions.builder()
                    .enabled(true)
                    .build();

            CreateDomainRequest createRequest = CreateDomainRequest.builder()
                    .domainName(domainName)
                    .engineVersion("OpenSearch_1.0")
                    .clusterConfig(clusterConfig)
                    .ebsOptions(ebsOptions)
                    .nodeToNodeEncryptionOptions(encryptionOptions)
                    // You can uncomment this line and add your account ID, a
 username, and the
                    // domain name to add an access policy.
                    // .accessPolicies("{\"Version\":\"2012-10-17\",
\"Statement\":[{\"Effect\":\"Allow\",\"Principal\":{\"AWS\":
[\"arn:aws:iam::123456789012:user/user-name\"]},\"Action\":[\"es:*\"],\"Resource\":
\"arn:aws:es:region:123456789012:domain/domain-name/*\"}]}")
                    .build();

            // Make the request.
            System.out.println("Sending domain creation request...");
            CreateDomainResponse createResponse =
 client.createDomain(createRequest);
            System.out.println("Domain status:
 "+createResponse.domainStatus().toString());
            System.out.println("Domain ID:
 "+createResponse.domainStatus().domainId());


        } catch (OpenSearchException e) {
            System.err.println(e.awsErrorDetails().errorMessage());
            System.exit(1);
        }
    }

    /**
     * Updates the configuration of an Amazon OpenSearch Service domain with the
```

```
    * specified options. Some options require other Amazon Web Services resources,
such as an
    * Amazon Cognito user pool and identity pool, whereas others require just an
    * instance type or instance count.
    *
    * @param client
    *            The client to use for the requests to Amazon OpenSearch Service
    * @param domainName
    *            The name of the domain to update
    */

   public static void updateDomain(OpenSearchClient client, String domainName) {

    // Updates the domain to use three data instances instead of five.
       // You can uncomment the Cognito line and fill in the strings to enable
Cognito
       // authentication for OpenSearch Dashboards.

       try {

           ClusterConfig clusterConfig = ClusterConfig.builder()
                   .instanceCount(5)
                   .build();

           CognitoOptions cognitoOptions = CognitoOptions.builder()
                   .enabled(true)
                   .userPoolId("user-pool-id")
                   .identityPoolId("identity-pool-id")
                   .roleArn("role-arn")
                   .build();

           UpdateDomainConfigRequest updateRequest =
UpdateDomainConfigRequest.builder()
                   .domainName(domainName)
                   .clusterConfig(clusterConfig)
                   //.cognitoOptions(cognitoOptions)
                   .build();

           System.out.println("Sending domain update request...");
           UpdateDomainConfigResponse updateResponse =
client.updateDomainConfig(updateRequest);
           System.out.println("Domain config:
"+updateResponse.domainConfig().toString());
```

```
        } catch (OpenSearchException e) {
            System.err.println(e.awsErrorDetails().errorMessage());
            System.exit(1);
        }
    }

    /**
     * Deletes an Amazon OpenSearch Service domain. Deleting a domain can take
     * several minutes.
     *
     * @param client
     *            The client to use for the requests to Amazon OpenSearch Service
     * @param domainName
     *            The name of the domain that you want to delete
     */

    public static void deleteDomain(OpenSearchClient client, String domainName) {

        try {

            DeleteDomainRequest deleteRequest = DeleteDomainRequest.builder()
                    .domainName(domainName)
                    .build();

            System.out.println("Sending domain deletion request...");
            DeleteDomainResponse deleteResponse =
client.deleteDomain(deleteRequest);
            System.out.println("Domain status: "+deleteResponse.toString());


        } catch (OpenSearchException e) {
            System.err.println(e.awsErrorDetails().errorMessage());
            System.exit(1);
        }
    }

    /**
     * Waits for the domain to finish processing changes. New domains typically take
15-30 minutes
     * to initialize, but can take longer depending on the configuration. Most
updates to existing domains
     * take a similar amount of time. This method checks every 15 seconds and
finishes only when
```

```
     * the domain's processing status changes to false.
     *
     * @param client
     *            The client to use for the requests to Amazon OpenSearch Service
     * @param domainName
     *            The name of the domain that you want to check
     */

    public static void waitForDomainProcessing(OpenSearchClient client, String
 domainName) {
        // Create a new request to check the domain status.
        DescribeDomainRequest describeRequest = DescribeDomainRequest.builder()
                .domainName(domainName)
                .build();

        // Every 15 seconds, check whether the domain is processing.
        DescribeDomainResponse describeResponse =
 client.describeDomain(describeRequest);
        while (describeResponse.domainStatus().processing()) {
            try {
                System.out.println("Domain still processing...");
                TimeUnit.SECONDS.sleep(15);
                describeResponse = client.describeDomain(describeRequest);
            } catch (InterruptedException e) {
                e.printStackTrace();
            }
        }

        // Once we exit that loop, the domain is available
        System.out.println("Amazon OpenSearch Service has finished processing
 changes for your domain.");
        System.out.println("Domain description: "+describeResponse.toString());
    }
}
```

Version 1

此範例使用AWSElasticsearchClientBuilder來自版本 1 的構造函數AWS SDK for Java若要建立舊版的 Elasticsearch 網域、更新其設定，然後將其刪除。取消對 `waitForDomainProcessing` 呼叫的註解 (並對 `deleteDomain` 呼叫加上註解)，以允許網域上線並變得可用。

```
package com.amazonaws.samples;
```

```
import java.util.concurrent.TimeUnit;
import com.amazonaws.auth.DefaultAWSCredentialsProviderChain;
import com.amazonaws.regions.Regions;
import com.amazonaws.services.elasticsearch.AWSElasticsearch;
import com.amazonaws.services.elasticsearch.AWSElasticsearchClientBuilder;
import com.amazonaws.services.elasticsearch.model.CreateElasticsearchDomainRequest;
import com.amazonaws.services.elasticsearch.model.CreateElasticsearchDomainResult;
import com.amazonaws.services.elasticsearch.model.DeleteElasticsearchDomainRequest;
import com.amazonaws.services.elasticsearch.model.DeleteElasticsearchDomainResult;
import
 com.amazonaws.services.elasticsearch.model.DescribeElasticsearchDomainRequest;
import com.amazonaws.services.elasticsearch.model.DescribeElasticsearchDomainResult;
import com.amazonaws.services.elasticsearch.model.EBSOptions;
import com.amazonaws.services.elasticsearch.model.ElasticsearchClusterConfig;
import com.amazonaws.services.elasticsearch.model.ResourceNotFoundException;
import
 com.amazonaws.services.elasticsearch.model.UpdateElasticsearchDomainConfigRequest;
import
 com.amazonaws.services.elasticsearch.model.UpdateElasticsearchDomainConfigResult;
import com.amazonaws.services.elasticsearch.model.VolumeType;

/**
 * Sample class demonstrating how to use the Amazon Web Services SDK for Java to
 create, update,
 * and delete Amazon OpenSearch Service domains.
 */

public class OpenSearchSample {

    public static void main(String[] args) {

        final String domainName = "my-test-domain";

        // Build the client using the default credentials chain.
        // You can use the CLI and run `aws configure` to set access key, secret
        // key, and default region.
        final AWSElasticsearch client = AWSElasticsearchClientBuilder
                .standard()
                // Unnecessary, but lets you use a region different than your
 default.
                .withRegion(Regions.US_WEST_2)
                // Unnecessary, but if desired, you can use a different provider
 chain.
                .withCredentials(new DefaultAWSCredentialsProviderChain())
```

```
                .build();

        // Create a new domain, update its configuration, and delete it.
        createDomain(client, domainName);
        // waitForDomainProcessing(client, domainName);
        updateDomain(client, domainName);
        // waitForDomainProcessing(client, domainName);
        deleteDomain(client, domainName);
    }

    /**
     * Creates an Amazon OpenSearch Service domain with the specified options.
     * Some options require other Amazon Web Services resources, such as an Amazon
Cognito user pool
     * and identity pool, whereas others require just an instance type or instance
     * count.
     *
     * @param client
     *            The client to use for the requests to Amazon OpenSearch Service
     * @param domainName
     *            The name of the domain you want to create
     */
    private static void createDomain(final AWSElasticsearch client, final String
domainName) {

        // Create the request and set the desired configuration options
        CreateElasticsearchDomainRequest createRequest = new
CreateElasticsearchDomainRequest()
                .withDomainName(domainName)
                .withElasticsearchVersion("7.10")
                .withElasticsearchClusterConfig(new ElasticsearchClusterConfig()
                        .withDedicatedMasterEnabled(true)
                        .withDedicatedMasterCount(3)
                        // Small, inexpensive instance types for testing. Not
recommended for production
                        // domains.
                        .withDedicatedMasterType("t2.small.elasticsearch")
                        .withInstanceType("t2.small.elasticsearch")
                        .withInstanceCount(5))
                // Many instance types require EBS storage.
                .withEBSOptions(new EBSOptions()
                        .withEBSEnabled(true)
                        .withVolumeSize(10)
                        .withVolumeType(VolumeType.Gp2));
```

```
                // You can uncomment this line and add your account ID, a username,
 and the
                // domain name to add an access policy.
                // .withAccessPolicies("{\"Version\":\"2012-10-17\",
\"Statement\":[{\"Effect\":\"Allow\",\"Principal\":{\"AWS\":
[\"arn:aws:iam::123456789012:user/user-name\"]},\"Action\":[\"es:*\"],\"Resource\":
\"arn:aws:es:region:123456789012:domain/domain-name/*\"}]}")


        // Make the request.
        System.out.println("Sending domain creation request...");
        CreateElasticsearchDomainResult createResponse =
 client.createElasticsearchDomain(createRequest);
        System.out.println("Domain creation response from Amazon OpenSearch
 Service:");
        System.out.println(createResponse.getDomainStatus().toString());
    }

    /**
     * Updates the configuration of an Amazon OpenSearch Service domain with the
     * specified options. Some options require other Amazon Web Services resources,
 such as an
     * Amazon Cognito user pool and identity pool, whereas others require just an
     * instance type or instance count.
     *
     * @param client
     *            The client to use for the requests to Amazon OpenSearch Service
     * @param domainName
     *            The name of the domain to update
     */
    private static void updateDomain(final AWSElasticsearch client, final String
 domainName) {
        try {
            // Updates the domain to use three data instances instead of five.
            // You can uncomment the Cognito lines and fill in the strings to enable
 Cognito
            // authentication for OpenSearch Dashboards.
            final UpdateElasticsearchDomainConfigRequest updateRequest = new
 UpdateElasticsearchDomainConfigRequest()
                    .withDomainName(domainName)
                    // .withCognitoOptions(new CognitoOptions()
                            // .withEnabled(true)
                            // .withUserPoolId("user-pool-id")
                            // .withIdentityPoolId("identity-pool-id")
```

```
                            // .withRoleArn("role-arn")
                    .withElasticsearchClusterConfig(new ElasticsearchClusterConfig()
                            .withInstanceCount(3));

            System.out.println("Sending domain update request...");
            final UpdateElasticsearchDomainConfigResult updateResponse = client
                    .updateElasticsearchDomainConfig(updateRequest);
            System.out.println("Domain update response from Amazon OpenSearch
Service:");
            System.out.println(updateResponse.toString());
        } catch (ResourceNotFoundException e) {
            System.out.println("Domain not found. Please check the domain name.");
        }
    }

    /**
     * Deletes an Amazon OpenSearch Service domain. Deleting a domain can take
     * several minutes.
     *
     * @param client
     *            The client to use for the requests to Amazon OpenSearch Service
     * @param domainName
     *            The name of the domain that you want to delete
     */
    private static void deleteDomain(final AWSElasticsearch client, final String
domainName) {
        try {
            final DeleteElasticsearchDomainRequest deleteRequest = new
DeleteElasticsearchDomainRequest()
                    .withDomainName(domainName);

            System.out.println("Sending domain deletion request...");
            final DeleteElasticsearchDomainResult deleteResponse =
client.deleteElasticsearchDomain(deleteRequest);
            System.out.println("Domain deletion response from Amazon OpenSearch
Service:");
            System.out.println(deleteResponse.toString());
        } catch (ResourceNotFoundException e) {
            System.out.println("Domain not found. Please check the domain name.");
        }
    }

    /**
```

```
     * Waits for the domain to finish processing changes. New domains typically take
 15-30 minutes
     * to initialize, but can take longer depending on the configuration. Most
 updates to existing domains
     * take a similar amount of time. This method checks every 15 seconds and
 finishes only when
     * the domain's processing status changes to false.
     *
     * @param client
     *            The client to use for the requests to Amazon OpenSearch Service
     * @param domainName
     *            The name of the domain that you want to check
     */
    private static void waitForDomainProcessing(final AWSElasticsearch client, final
 String domainName) {
        // Create a new request to check the domain status.
        final DescribeElasticsearchDomainRequest describeRequest = new
 DescribeElasticsearchDomainRequest()
                .withDomainName(domainName);

        // Every 15 seconds, check whether the domain is processing.
        DescribeElasticsearchDomainResult describeResponse =
 client.describeElasticsearchDomain(describeRequest);
        while (describeResponse.getDomainStatus().isProcessing()) {
            try {
                System.out.println("Domain still processing...");
                TimeUnit.SECONDS.sleep(15);
                describeResponse =
 client.describeElasticsearchDomain(describeRequest);
            } catch (InterruptedException e) {
                e.printStackTrace();
            }
        }

        // Once we exit that loop, the domain is available
        System.out.println("Amazon OpenSearch Service has finished processing
 changes for your domain.");
        System.out.println("Domain description response from Amazon OpenSearch
 Service:");
        System.out.println(describeResponse.toString());
    }
}
```

Python

此範例使用OpenSearchService從低級 Python 客戶端AWS SDK for Python (Boto)以建立網域、更新其組態並將其刪除。

```
import boto3
import botocore
from botocore.config import Config
import time

# Build the client using the default credential configuration.
# You can use the CLI and run 'aws configure' to set access key, secret
# key, and default region.

my_config = Config(
    # Optionally lets you specify a region other than your default.
    region_name='us-west-2'
)

client = boto3.client('opensearch', config=my_config)

domainName = 'my-test-domain'  # The name of the domain


def createDomain(client, domainName):
    """Creates an Amazon OpenSearch Service domain with the specified options."""
    response = client.create_domain(
        DomainName=domainName,
        EngineVersion='OpenSearch_1.0',
        ClusterConfig={
            'InstanceType': 't2.small.search',
            'InstanceCount': 5,
            'DedicatedMasterEnabled': True,
            'DedicatedMasterType': 't2.small.search',
            'DedicatedMasterCount': 3
        },
        # Many instance types require EBS storage.
        EBSOptions={
            'EBSEnabled': True,
            'VolumeType': 'gp2',
            'VolumeSize': 10
        },
```

```
        AccessPolicies="{\"Version\":\"2012-10-17\",\"Statement\":[{\"Effect\":\"Allow
\",\"Principal\":{\"AWS\":[\"arn:aws:iam::123456789012:user/user-name\"]},\"Action\":
[\"es:*\"],\"Resource\":\"arn:aws:es:us-west-2:123456789012:domain/my-test-domain/*
\"}]}",
        NodeToNodeEncryptionOptions={
            'Enabled': True
        }
    )
    print("Creating domain...")
    print(response)


def updateDomain(client, domainName):
    """Updates the domain to use three data nodes instead of five."""
    try:
        response = client.update_domain_config(
            DomainName=domainName,
            ClusterConfig={
                'InstanceCount': 3
            }
        )
        print('Sending domain update request...')
        print(response)

    except botocore.exceptions.ClientError as error:
        if error.response['Error']['Code'] == 'ResourceNotFoundException':
            print('Domain not found. Please check the domain name.')
        else:
            raise error


def deleteDomain(client, domainName):
    """Deletes an OpenSearch Service domain. Deleting a domain can take several
 minutes."""
    try:
        response = client.delete_domain(
            DomainName=domainName
        )
        print('Sending domain deletion request...')
        print(response)

    except botocore.exceptions.ClientError as error:
        if error.response['Error']['Code'] == 'ResourceNotFoundException':
            print('Domain not found. Please check the domain name.')
```

```
        else:
            raise error


def waitForDomainProcessing(client, domainName):
    """Waits for the domain to finish processing changes."""
    try:
        response = client.describe_domain(
            DomainName=domainName
        )
        # Every 15 seconds, check whether the domain is processing.
        while response["DomainStatus"]["Processing"] == True:
            print('Domain still processing...')
            time.sleep(15)
            response = client.describe_domain(
                DomainName=domainName)

        # Once we exit the loop, the domain is available.
        print('Amazon OpenSearch Service has finished processing changes for your
 domain.')
        print('Domain description:')
        print(response)

    except botocore.exceptions.ClientError as error:
        if error.response['Error']['Code'] == 'ResourceNotFoundException':
            print('Domain not found. Please check the domain name.')
        else:
            raise error


def main():
    """Create a new domain, update its configuration, and delete it."""
    createDomain(client, domainName)
    waitForDomainProcessing(client, domainName)
    updateDomain(client, domainName)
    waitForDomainProcessing(client, domainName)
    deleteDomain(client, domainName)
```

節點

此範例使用 SDK 的第 3 版JavaScript在 Node.js 中OpenSearch客戶以建立網域、更新其組態並將其刪除。

```
var {
    OpenSearchClient,
    CreateDomainCommand,
    DescribeDomainCommand,
    UpdateDomainConfigCommand,
    DeleteDomainCommand
} = require("@aws-sdk/client-opensearch");
var sleep = require('sleep');

var client = new OpenSearchClient();

var domainName = 'my-test-domain'

// Create a new domain, update its configuration, and delete it.
createDomain(client, domainName)
waitForDomainProcessing(client, domainName)
updateDomain(client, domainName)
waitForDomainProcessing(client, domainName)
deleteDomain(client, domainName)

async function createDomain(client, domainName) {
    // Creates an Amazon OpenSearch Service domain with the specified options.
    var command = new CreateDomainCommand({
        DomainName: domainName,
        EngineVersion: 'OpenSearch_1.0',
        ClusterConfig: {
        'InstanceType': 't2.small.search',
        'InstanceCount': 5,
        'DedicatedMasterEnabled': 'True',
        'DedicatedMasterType': 't2.small.search',
        'DedicatedMasterCount': 3
        },
        EBSOptions:{
            'EBSEnabled': 'True',
            'VolumeType': 'gp2',
            'VolumeSize': 10
        },
        AccessPolicies: "{\"Version\":\"2012-10-17\",\"Statement\":[{\"Effect\":\"Allow
\",\"Principal\":{\"AWS\":[\"arn:aws:iam::123456789012:user/user-name\"]},\"Action\":
[\"es:*\"],\"Resource\":\"arn:aws:es:us-east-1:123456789012:domain/my-test-domain/*
\"}]}",
         NodeToNodeEncryptionOptions:{
            'Enabled': 'True'
```

```
        }
    });
    const response = await client.send(command);
    console.log("Creating domain...");
    console.log(response);
}

async function updateDomain(client, domainName) {
    // Updates the domain to use three data nodes instead of five.
    var command = new UpdateDomainConfigCommand({
        DomainName: domainName,
        ClusterConfig: {
        'InstanceCount': 3
        }
    });
    const response = await client.send(command);
    console.log('Sending domain update request...');
    console.log(response);
}

async function deleteDomain(client, domainName) {
    // Deletes an OpenSearch Service domain. Deleting a domain can take several
 minutes.
    var command = new DeleteDomainCommand({
        DomainName: domainName
    });
    const response = await client.send(command);
    console.log('Sending domain deletion request...');
    console.log(response);
}

async function waitForDomainProcessing(client, domainName) {
    // Waits for the domain to finish processing changes.
    try {
        var command = new DescribeDomainCommand({
            DomainName: domainName
        });
        var response = await client.send(command);

        while (response.DomainStatus.Processing == true) {
            console.log('Domain still processing...')
            await sleep(15000) // Wait for 15 seconds, then check the status again
            function sleep(ms) {
                return new Promise((resolve) => {
```

```
                    setTimeout(resolve, ms);
                });
            }
            var response = await client.send(command);
        }
        // Once we exit the loop, the domain is available.
        console.log('Amazon OpenSearch Service has finished processing changes for your
 domain.');
        console.log('Domain description:');
        console.log(response);

    } catch (error) {
        if (error.name === 'ResourceNotFoundException') {
            console.log('Domain not found. Please check the domain name.');
            }
    };
}
```

在 Amazon OpenSearch 服務中索引數據

由於 Amazon OpenSearch 服務使用 REST API，因此存在許多方法來索引文檔。您可以使用標準用戶端，例如 Curl 或任何可以傳送 HTTP 請求的程式設計語言。為了進一步簡化與它交互的過程，OpenSearch Service 有許多編程語言的客戶端。進階使用者可以直接跳到the section called “將串流資料載入 OpenSearch 服務”。

我們強烈建議您使用 Amazon OpenSearch 擷取資料，這是在服務內 OpenSearch 建的全受管資料收集器。如需詳細資訊，請參閱 Amazon OpenSearch 擷取。

如需索引的簡介，請參閱OpenSearch文件。

索引的命名限制

OpenSearch 服務索引具有下列命名限制：

- 所有字母必須小寫。
- 索引名稱的最開頭不可以是 _ 或 -。
- 索引名稱不可以包含空格、逗號、:、"、*、+、/、\、|、?、#、> 或 <。

請勿在索引、類型或文件 ID 名稱中包含敏感資訊。 OpenSearch 服務會在其統一資源識別碼 (URI) 中使用這些名稱。伺服器和應用程式通常會記錄 HTTP 請求，如果 URI 包含敏感資訊，這會導致不必要的資料暴露：

```
2018-10-03T23:39:43 198.51.100.14 200 "GET https://opensearch-domain/dr-jane-doe/flu-patients-2018/202-555-0100/ HTTP/1.1"
```

即使您沒有檢視相關 JSON 文件的許可，您可以從此仿造日誌列推斷出 Doe 醫生的其中一名病人 (其電話號碼為 202-555-0100) 在 2018 年患有流感。

如果 OpenSearch 服務在索引名稱中偵測到真實或適當的 IP 位址 (例如，`my-index-12.34.56.78.91`)，它會遮罩 IP 位址。呼叫 `_cat/indices` 產生下列回應：

```
green open my-index-x.x.x.x.91    soY19tBERoKo71WcEScidw 5 1 0 0   2kb  1kb
```

為防止不必要的混淆，請避免在索引名稱中包含 IP 地址。

縮減回應大小

由 _index 和 _bulk API 而來的回應包含相當多的資訊。這類資訊或許有助於對請求進行故障診斷或實作重試邏輯，但難免會耗用大量頻寬。在此範例中，對 32 個位元組的文件編製索引將產生 339 個位元組的回應 (包括標頭)：

```
PUT opensearch-domain/more-movies/_doc/1
{"title": "Back to the Future"}
```

回應

```
{
  "_index": "more-movies",
  "_type": "_doc",
  "_id": "1",
  "_version": 4,
  "result": "updated",
  "_shards": {
    "total": 2,
    "successful": 2,
    "failed": 0
  },
  "_seq_no": 3,
  "_primary_term": 1
}
```

此回應大小可能看起來很小，但是如果您每天索引 1,000,000 份文件 (大約每秒 11.5 份文件)，則每個回應 339 位元組的運作量達到每月 10.17 GB 的下載流量。

如果需要考慮資料傳輸成本，請使用`filter_path`參數來減少 OpenSearch Service 回應的大小，但請小心不要篩選出識別或重試失敗要求所需的欄位。這類欄位因用戶端而異。該`filter_path`參數適用於所有 OpenSearch 服務 REST API，但對於經常調用的 API（例如`_index`和 _bulk API）尤其有用：

```
PUT opensearch-domain/more-movies/_doc/1?filter_path=result,_shards.total
{"title": "Back to the Future"}
```

回應

```
{
```

```
  "result": "updated",
  "_shards": {
    "total": 2
  }
}
```

除了納入欄位，您還可以使用 - 字首排除欄位。filter_path 也支援萬用字元：

```
POST opensearch-domain/_bulk?filter_path=-took,-items.index._*
{ "index": { "_index": "more-movies", "_id": "1" } }
{"title": "Back to the Future"}
{ "index": { "_index": "more-movies", "_id": "2" } }
{"title": "Spirited Away"}
```

回應

```
{
  "errors": false,
  "items": [
    {
      "index": {
        "result": "updated",
        "status": 200
      }
    },
    {
      "index": {
        "result": "updated",
        "status": 200
      }
    }
  ]
}
```

索引轉碼器

索引轉碼器決定索引上儲存的欄位如何壓縮並儲存在磁碟上。索引轉碼器由靜態設定控制，靜態index.codec設定會指定壓縮演算法。此設定會影響索引碎片大小和作業效能。

如需支援的轉碼器清單及其效能特性，請參閱 OpenSearch 文件中的支援轉碼器。

當您選擇索引轉碼器時，請考慮下列事項：

- 若要避免變更現有索引之轉碼器設定的挑戰，請在使用新的轉碼器設定之前，在非生產環境中測試代表性的工作負載。如需詳細資訊，請參閱變更索引轉碼器。
- 您無法將 Zstandard 壓縮轉碼器 (`"index.codec": "zstd"`或`"index.codec": "zstd_no_dict"`) 用於 k-NN 或安全性分析索引。

將串流資料載入 Amazon OpenSearch 服務

您可以使用 OpenSearch 擷取將串流資料直接載入 Amazon Ser OpenSearch vice 網域，而無需使用第三方解決方案。若要將資料傳送至 OpenSearch 擷取，您必須設定資料生產者，服務會自動將資料傳送至您指定的網域或集合。若要開始使用 OpenSearch 擷取，請參閱the section called “教學課程：將資料擷取至集合”。

您仍然可以使用其他來源載入串流資料，例如 Amazon 資料 Firehose 和 Amazon CloudWatch 日誌，這些資料具有內建的 OpenSearch 服務支援。諸如 Amazon S3、Amazon Kinesis Data Streams 和 Amazon DynamoDB 等其他來源使用 AWS Lambda 函數作為事件處理程序。Lambda 函數透過處理新資料並將其串流到您的網域來對其進行回應。

> **Note**
>
> Lambda 支援數種熱門的程式設計語言，並且可用於大部分 AWS 區域。如需詳細資訊，請參閱開AWS Lambda 發人員指南中的 Lambda 入門和AWSAWS 一般參考.

主題

- 從 OpenSearch 擷取載入串流資料
- 從 Amazon S3 載入串流資料
- 從 Amazon Kinesis Data Streams 中載入串流資料
- 從 Amazon DynamoDB 中載入串流資料
- 從 Amazon 數據防 Firehose 件加載流數據
- 從 Amazon 加載流數據 CloudWatch
- 從 AWS IoT中載入串流資料

從 OpenSearch 擷取載入串流資料

您可以使用 Amazon OpenSearch 擷取將資料載入 OpenSearch 服務網域。您可以將資料生產者設定為將資料傳送至 OpenSearch 擷取，它會自動將資料傳送至您指定的集合。您也可以將 OpenSearch 擷取設定為在傳送資料之前轉換資料。如需詳細資訊，請參閱 Amazon OpenSearch 攝入。

從 Amazon S3 載入串流資料

您可以使用 Lambda 將資料從 Amazon S3 傳送到您的 OpenSearch 服務網域。送達 S3 儲存貯體的新資料會觸發 Lambda 的事件通知，然後執行您的自訂程式碼以執行索引。

這個串流資料方法非常靈活。您可以 索引物件中繼資料 ，若是純文字的話，便可剖析和索引一些物件本體元素。本節包含一些簡單的 Python 範本程式碼，其使用規則表達式來剖析日誌檔案和索引比對。

必要條件

繼續之前，您必須準備好以下資源。

先決條件	描述
Amazon S3 儲存貯體	如需詳細資訊，請參閱 Amazon Simple Storage Service 使用者指南中的建立您的第一個 S3 儲存貯體。值區必須與您的 OpenSearch 服務網域位於相同的區域。
OpenSearch 服務網域	您的 Lambda 函數處理資料後的資料目的地。如需詳細資訊，請參閱 the section called “ 建立 OpenSearch 服務網域”。

建立 Lambda 部署套件

部署套件是指包含您的程式碼及其相依存項目的 ZIP 或 JAR 檔案。本節包括 Python 範本程式碼。如需其他程式設計語言，請參閱 AWS Lambda 開發人員指南中的 Lambda 部署套件。

1. 建立目錄。在此範例中，我們使用 `s3-to-opensearch` 這個名稱。
2. 在目錄中建立名為 `sample.py` 的檔案：

```
import boto3
import re
import requests
from requests_aws4auth import AWS4Auth
```

```
region = '' # e.g. us-west-1
service = 'es'
credentials = boto3.Session().get_credentials()
awsauth = AWS4Auth(credentials.access_key, credentials.secret_key, region, service,
 session_token=credentials.token)

host = '' # the OpenSearch Service domain, e.g. https://search-mydomain.us-
west-1.es.amazonaws.com
index = 'lambda-s3-index'
datatype = '_doc'
url = host + '/' + index + '/' + datatype

headers = { "Content-Type": "application/json" }

s3 = boto3.client('s3')

# Regular expressions used to parse some simple log lines
ip_pattern = re.compile('(\d+\.\d+\.\d+\.\d+)')
time_pattern = re.compile('\[(\d+\/\w\w\w\/\d\d\d\d:\d\d:\d\d:\d\d\s-\d\d\d\d)\]')
message_pattern = re.compile('\"(.+)\"')

# Lambda execution starts here
def handler(event, context):
    for record in event['Records']:

        # Get the bucket name and key for the new file
        bucket = record['s3']['bucket']['name']
        key = record['s3']['object']['key']

        # Get, read, and split the file into lines
        obj = s3.get_object(Bucket=bucket, Key=key)
        body = obj['Body'].read()
        lines = body.splitlines()

        # Match the regular expressions to each line and index the JSON
        for line in lines:
            line = line.decode("utf-8")
            ip = ip_pattern.search(line).group(1)
            timestamp = time_pattern.search(line).group(1)
            message = message_pattern.search(line).group(1)

            document = { "ip": ip, "timestamp": timestamp, "message": message }
```

```
            r = requests.post(url, auth=awsauth, json=document, headers=headers)
```

編輯 `region` 和 `host` 的變數。

3. 安裝 pip (如果您尚未安裝的話)，然後將相依項目安裝到新的 `package` 目錄：

```
cd s3-to-opensearch

pip install --target ./package requests
pip install --target ./package requests_aws4auth
```

所有 Lambda 執行環境均已安裝 Boto3，因此您不需要將其包含在您的部署套件中。

4. 封裝應用程式的程式碼和相依性：

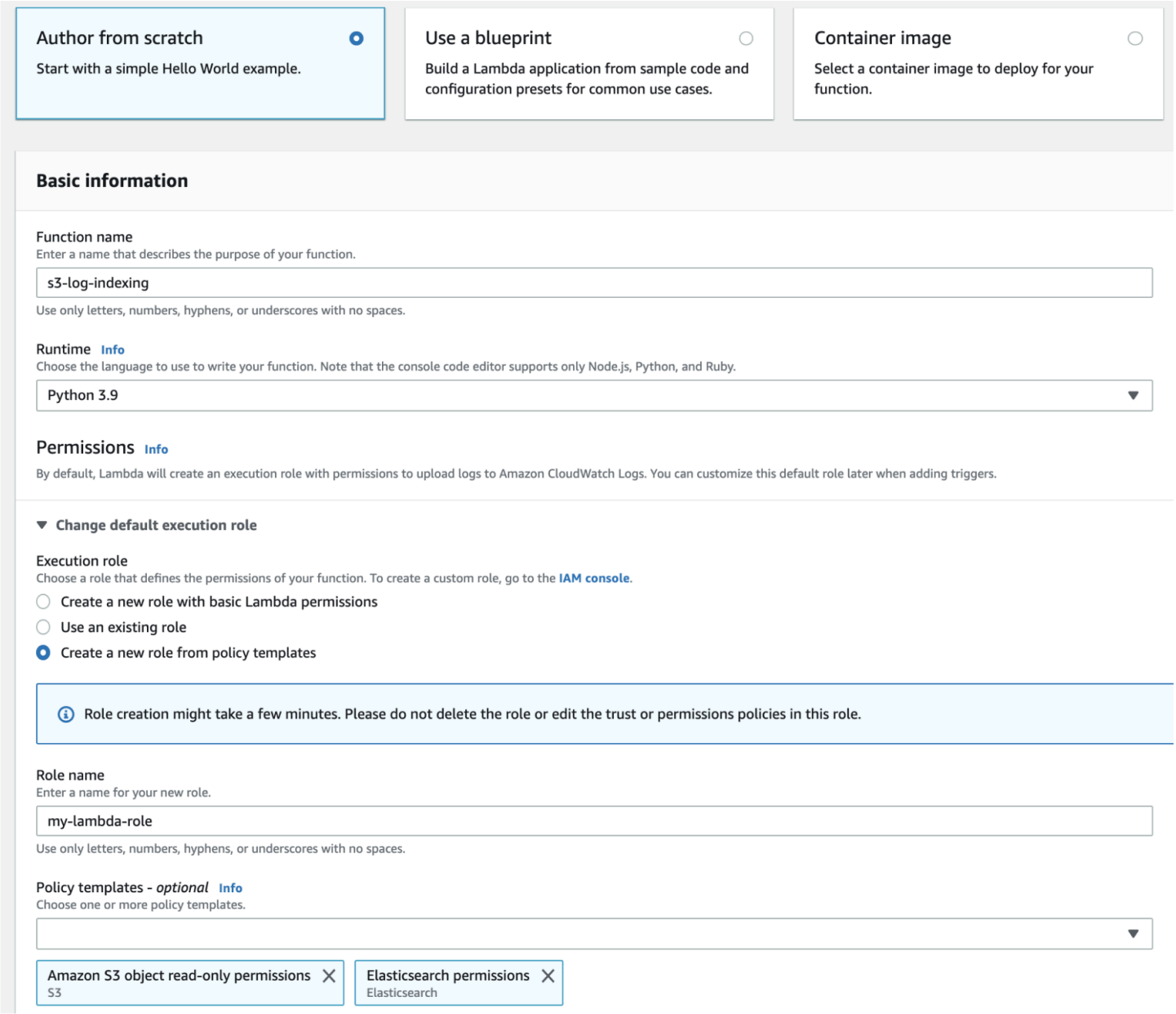
```
cd package
zip -r ../lambda.zip .

cd ..
zip -g lambda.zip sample.py
```

建立 Lambda 函數

建立部署套件後，可建立 Lambda 函數。當您建立函數時，請選擇名稱、執行時間 (例如，Python 3.8) 和 IAM 角色。IAM 角色定義函數的許可。如需詳細說明，請參閱 AWS Lambda 開發人員指南中的使用主控台建立 Lambda 函數。

此範例假設您正在使用主控台。選擇 Python 3.9 以及具有 S3 讀取權限和 OpenSearch 服務寫入權限的角色，如下列螢幕擷取畫面所示：



在建立函數，您必須新增觸發。在此範例中，我們希望只要日誌檔案送達 S3 儲存貯體，便執行程式碼：

1. 選擇 Add trigger (新增觸發條件)，然後選取 S3。
2. 選擇您的儲存貯體。
3. 針對 Event type (事件類型) 選擇 PUT。
4. 針對 Prefix (字首) 輸入 `logs/`。
5. 對於 Suffix (尾碼)，輸入 `.log`。
6. 確認遞迴叫用警告，然後選擇 Add (新增)。

最後，您可以上傳部署套件：

1. 選擇 Upload from (上傳自) 和 .zip file (.zip 檔案)，然後依照提示上傳您的部署套件。
2. 上傳完成後，編輯 Runtime settings (執行時間設定)，然後將 Handler (處理常式) 變更為 `sample.handler`。此設定通知 Lambda 應該在觸發後執行的檔案 (`sample.py`) 和方法 (`handler`)。

此時，您將擁有一組完整的資源：用於記錄檔的值區、每當記錄檔新增至值區時都會執行的函數、執行剖析和索引的程式碼，以及用於搜尋和視覺化的 OpenSearch Service 網域。

測試 Lambda 函數

在建立函數之後，您可以進行測試，做法是上傳檔案到 Amazon S3 儲存貯體。使用下列範例日誌行，建立名為 `sample.log` 的檔案：

```
12.345.678.90 - [10/Oct/2000:13:55:36 -0700] "PUT /some-file.jpg"
12.345.678.91 - [10/Oct/2000:14:56:14 -0700] "GET /some-file.jpg"
```

上傳檔案到您的 S3 儲存貯體的 `logs` 資料夾。如需指示說明，請參閱 Amazon Simple Storage Service 使用者指南中的將物件上傳至您的儲存貯體。

然後使用 OpenSearch 服務主控台或 OpenSearch 儀表板來驗證`lambda-s3-index`索引是否包含兩個文件。您也可以提出標準搜尋請求：

```
GET https://domain-name/lambda-s3-index/_search?pretty
{
  "hits" : {
    "total" : 2,
    "max_score" : 1.0,
    "hits" : [
      {
        "_index" : "lambda-s3-index",
        "_type" : "_doc",
        "_id" : "vTYXaWIBJWV_TTkEuSDg",
        "_score" : 1.0,
        "_source" : {
          "ip" : "12.345.678.91",
          "message" : "GET /some-file.jpg",
          "timestamp" : "10/Oct/2000:14:56:14 -0700"
        }
      },
```

```
      {
        "_index" : "lambda-s3-index",
        "_type" : "_doc",
        "_id" : "vjYmaWIBJWV_TTkEuCAB",
        "_score" : 1.0,
        "_source" : {
          "ip" : "12.345.678.90",
          "message" : "PUT /some-file.jpg",
          "timestamp" : "10/Oct/2000:13:55:36 -0700"
        }
      }
    ]
  }
}
```

從 Amazon Kinesis Data Streams 中載入串流資料

您可以將串流資料從 Kinesis Data Streams 載入 OpenSearch 服務。送達資料串流的新資料會觸發 Lambda 的事件通知，然後執行您的自訂程式碼以執行索引。本節包括一些簡單的 Python 範本程式碼。

必要條件

繼續之前，您必須準備好以下資源。

先決條件	描述
Amazon Kinesis Data Stream	Lambda 函數的事件來源。如需進一步了解，請參閱 Kinesis Data Streams。
OpenSearch 服務網域	您的 Lambda 函數處理資料後的資料目的地。如需詳細資訊，請參閱 the section called “ 建立 OpenSearch 服務網域”。
IAM 角色	此角色必須具有基本的 OpenSearch 服務、Kinesis 和 Lambda 權限，如下所示： `{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow",`

先決條件	描述
	`"Action": [ "es:ESHttpPost", "es:ESHttpPut", "logs:CreateLogGroup", "logs:CreateLogStream", "logs:PutLogEvents", "kinesis:GetShardIterator", "kinesis:GetRecords", "kinesis:DescribeStream", "kinesis:ListStreams" ], "Resource": "*" } ] }` 角色必須具有下列信任關係：`{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Principal": { "Service": "lambda.amazonaws.com" }, "Action": "sts:AssumeRole" } ] }` 如需進一步了解，請參閱 IAM 使用者指南中的建立 IAM 角色。

建立 Lambda 函數

遵循the section called “建立 Lambda 部署套件”中的指示，但要建立名為 `kinesis-to-opensearch` 的目錄，並使用以下適用於 `sample.py` 的程式碼：

```
import base64
```

```
import boto3
import json
import requests
from requests_aws4auth import AWS4Auth

region = '' # e.g. us-west-1
service = 'es'
credentials = boto3.Session().get_credentials()
awsauth = AWS4Auth(credentials.access_key, credentials.secret_key, region, service,
 session_token=credentials.token)

host = '' # the OpenSearch Service domain, e.g. https://search-mydomain.us-
west-1.es.amazonaws.com
index = 'lambda-kine-index'
datatype = '_doc'
url = host + '/' + index + '/' + datatype + '/'

headers = { "Content-Type": "application/json" }

def handler(event, context):
    count = 0
    for record in event['Records']:
        id = record['eventID']
        timestamp = record['kinesis']['approximateArrivalTimestamp']

        # Kinesis data is base64-encoded, so decode here
        message = base64.b64decode(record['kinesis']['data'])

        # Create the JSON document
        document = { "id": id, "timestamp": timestamp, "message": message }
        # Index the document
        r = requests.put(url + id, auth=awsauth, json=document, headers=headers)
        count += 1
    return 'Processed ' + str(count) + ' items.'
```

編輯 `region` 和 `host` 的變數。

安裝 pip (如果您尚未安裝的話)，然後使用下列命令安裝相依項目：

```
cd kinesis-to-opensearch

pip install --target ./package requests
pip install --target ./package requests_aws4auth
```

然後，遵循the section called “建立 Lambda 函數”中的指示，但要從the section called “必要條件”指定 IAM 角色和下列用於觸發的設定：

- Kinesis 串流：您的 Kinesis 串流
- 批次大小：100
- 開始位置：水平修剪

如需進一步了解，請參閱 Amazon Kinesis Data Streams 開發人員指南 中的什麼是 Amazon Kinesis Data Streams？。

此時，您擁有一組完整的資源：Kinesis 資料串流、在串流接收到新資料並為該資料建立索引之後執行的函數，以及用於搜尋和視覺化的 OpenSearch Service 網域。

測試 Lambda 函數

在建立函數後，您可以做測試，方法是將新記錄加入到使用 AWS CLI的資料串流：

```
aws kinesis put-record --stream-name test --data "My test data." --partition-key
 partitionKey1 --region us-west-1
```

然後使用 OpenSearch 服務主控台或 OpenSearch 儀表板來確認`lambda-kine-index`包含文件。您也可以使用以下請求：

```
GET https://domain-name/lambda-kine-index/_search
{
  "hits" : [
    {
      "_index": "lambda-kine-index",
      "_type": "_doc",
      "_id":
 "shardId-000000000000:49583511615762699495012960821421456686529436680496087042",
      "_score": 1,
      "_source": {
        "timestamp": 1523648740.051,
        "message": "My test data.",
        "id":
 "shardId-000000000000:49583511615762699495012960821421456686529436680496087042"
      }
    }
  ]
```

```
}
```

從 Amazon DynamoDB 中載入串流資料

您可以使用 AWS Lambda 將資料從 Amazon DynamoDB 傳送到您的 OpenSearch 服務網域。送達資料庫資料表的新資料會觸發 Lambda 的事件通知，然後執行您的自訂程式碼以執行索引。

必要條件

繼續之前，您必須準備好以下資源。

先決條件	描述
DynamoDB 表	表格中包含您的來源資料。如需詳細資訊，請參閱 Amazon DynamoDB 開發人員指南中的 DynamoDB 資料表上的基本操作。 資料表必須與您的 OpenSearch 服務網域位於相同的區域，並將串流設定為 [新增映像]。如需進一步了解，請參閱啟用串流。
OpenSearch 服務網域	您的 Lambda 函數處理資料後的資料目的地。如需詳細資訊，請參閱 the section called “ 建立 OpenSearch 服務網域”。
IAM 角色	此角色必須具有基本的 OpenSearch 服務、DynamoDB 和 Lambda 執行權限，例如：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "es:ESHttpPost",
        "es:ESHttpPut",
        "dynamodb:DescribeStream",
        "dynamodb:GetRecords",
        "dynamodb:GetShardIterator",
        "dynamodb:ListStreams",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
```

先決條件	描述

	`"Resource": "*"`
	`}`
	`]`
	`}`
	角色必須具有下列信任關係：
	`{`
	`"Version": "2012-10-17",`
	`"Statement": [`
	`{`
	`"Effect": "Allow",`
	`"Principal": {`
	`"Service": "lambda.amazonaws.com"`
	`},`
	`"Action": "sts:AssumeRole"`
	`}`
	`]`
	`}`
	如需進一步了解，請參閱 IAM 使用者指南中的建立 IAM 角色。

建立 Lambda 函數

遵循the section called “建立 Lambda 部署套件”中的指示，但要建立名為 `ddb-to-opensearch` 的目錄，並使用以下適用於 `sample.py` 的程式碼：

```
import boto3
import requests
from requests_aws4auth import AWS4Auth

region = '' # e.g. us-east-1
service = 'es'
credentials = boto3.Session().get_credentials()
awsauth = AWS4Auth(credentials.access_key, credentials.secret_key, region, service,
 session_token=credentials.token)

host = '' # the OpenSearch Service domain, e.g. https://search-mydomain.us-
west-1.es.amazonaws.com
```

```
index = 'lambda-index'
datatype = '_doc'
url = host + '/' + index + '/' + datatype + '/'

headers = { "Content-Type": "application/json" }

def handler(event, context):
    count = 0
    for record in event['Records']:
        # Get the primary key for use as the OpenSearch ID
        id = record['dynamodb']['Keys']['id']['S']

        if record['eventName'] == 'REMOVE':
            r = requests.delete(url + id, auth=awsauth)
        else:
            document = record['dynamodb']['NewImage']
            r = requests.put(url + id, auth=awsauth, json=document, headers=headers)
        count += 1
    return str(count) + ' records processed.'
```

編輯 `region` 和 `host` 的變數。

安裝 pip (如果您尚未安裝的話)，然後使用下列命令安裝相依項目：

```
cd ddb-to-opensearch

pip install --target ./package requests
pip install --target ./package requests_aws4auth
```

然後，遵循the section called “建立 Lambda 函數”中的指示，但要從the section called “必要條件”指定 IAM 角色和下列用於觸發的設定：

- 資料表：您的 DynamoDB 資料表
- 批次大小：100
- 開始位置：水平修剪

如需進一步了解，請參閱 Amazon DynamoDB 開發人員指南中的使用 DynamoDB Streams 和 Lambda 來處理新項目。

此時，您擁有一組完整的資源：來源資料的 DynamoDB 表、表格的 DynamoDB 變更串流、在來源資料變更後執行的函數，並為這些變更建立索引，以及用於搜尋和視覺化的 OpenSearch 服務網域。

測試 Lambda 函數

在建立函數後，您可以進行測試，方法是將新項目新增至使用 AWS CLI的 DynamoDB 資料表：

```
aws dynamodb put-item --table-name test --item '{"director": {"S": "Kevin
 Costner"},"id": {"S": "00001"},"title": {"S": "The Postman"}}' --region us-west-1
```

然後使用 OpenSearch 服務主控台或 OpenSearch 儀表板來確認`lambda-index`包含文件。您也可以使用以下請求：

```
GET https://domain-name/lambda-index/_doc/00001
{
    "_index": "lambda-index",
    "_type": "_doc",
    "_id": "00001",
    "_version": 1,
    "found": true,
    "_source": {
        "director": {
            "S": "Kevin Costner"
        },
        "id": {
            "S": "00001"
        },
        "title": {
            "S": "The Postman"
        }
    }
}
```

從 Amazon 數據防 Firehose 件加載流數據

Firehose 支持 OpenSearch 服務作為送貨目的地。如需有關如何將串流資料載入 OpenSearch 服務的指示，請參閱 Amazon 資料 Firehose 開發人員指南中的建立 Kinesis 資料 Firehose 交付串流和為您的目的地選擇 OpenSearch 服務。

在將資料載入 OpenSearch Service 之前，您可能需要對資料執行轉換。如需進一步了解如何使用 Lambda 函數來執行此任務，請參閱相同指南中的 Amazon Kinesis Data Firehose 資料轉換。

在您設定交付串流時，Firehose 具有「一鍵式」IAM 角色，可讓其具備將資料傳送至 OpenSearch 服務、備份 Amazon S3 上的資料，以及使用 Lambda 轉換資料所需的資源存取權。由於手動建立角色涉及複雜度，我們建議您使用所提供角色。

從 Amazon 加載流數據 CloudWatch

您可以使用 CloudWatch 記錄訂閱將串流資料從 CloudWatch 記錄載入 OpenSearch 服務網域。如需 Amazon CloudWatch 訂閱的相關資訊，請參閱使用訂閱即時處理日誌資料。如需組態資訊，請參閱 Amazon CloudWatch開發人員指南中的將 CloudWatch 日誌資料串流至 Amazon OpenSearch 服務。

從 AWS IoT中載入串流資料

您可以 AWS IoT 使用規則發送數據。若要深入了解，請參閱開AWS IoT 發人員指南中的OpenSearch動作。

使用 Logstash 將資料載入至 Amazon Ser OpenSearch vice

Logstash 的開放原始碼版本 (Logstash OSS) 提供便利的方法來使用大量 API 將資料上傳到您的 Amazon Ser OpenSearch vice 網域。此服務支援所有標準 Logstash 輸入外掛程式，包括 Amazon S3 輸入外掛程式。 OpenSearch Service 可支援基本身分驗證和 IAM 憑證。logstash-output-opensearch該外掛程式可與 Logstash OSS 的 8.1 版及較低版本搭配使用。

組態

Logstash 組態會依據網域使用的身分驗證類型而有所不同。

無論您使用哪種身分驗證方法，都必須在組態檔案的輸出部分中將 `ecs_compatibility` 設定為 `disabled`。Logstash 8.0 引入了一個突破性的變更，其中所有外掛程式都以預設 ECS 相容模式執行。您必須覆寫預設值才能保持舊式行為。

精細存取控制組態

如果您的 OpenSearch Service 網域搭配使用精細存取控制與 HTTP 基本身分驗證，則組態類似於任何其他 OpenSearch 叢集。此組態檔案範例會從 Filebeat 的開源版本 (Filebeat OSS) 取得輸入：

```
input {
  beats  {
    port => 5044
  }
}

output {
  opensearch {
```

```
    hosts       => "https://domain-endpoint:443"
    user        => "my-username"
    password    => "my-password"
    index       => "logstash-logs-%{+YYYY.MM.dd}"
    ecs_compatibility => disabled
    ssl_certificate_verification => false
  }
}
```

組態因 Beats 應用程式和使用案例而異，但您的 Filebeat OSS 組態可能如下所示：

```
filebeat.inputs:
- type: log
  enabled: true
  paths:
    - /path/to/logs/dir/*.log
filebeat.config.modules:
  path: ${path.config}/modules.d/*.yml
  reload.enabled: false
setup.ilm.enabled: false
setup.ilm.check_exists: false
setup.template.settings:
  index.number_of_shards: 1
output.logstash:
  hosts: ["logstash-host:5044"]
```

IAM 組態

如果您的網域使用以 IAM 為基礎的網域存取政策或精細存取控制搭配主要使用者，您必須使用 IAM 憑證簽署所有針對 OpenSearch Service 的請求。以下身分型政策會授予對您網域的子資源的 HTTP 請求。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "es:ESHttp*"
      ],
      "Resource": "arn:aws:es:region:aws-account-id:domain/domain-name/*"
    }
```

```
  ]
}
```

若要設定 Logstash 組態，請變更您的組態檔案以將外掛程式用於其輸出。此組態檔案範例會從 S3 儲存貯體中的檔案取得輸入：

```
input {
  s3 {
    bucket => "my-s3-bucket"
    region => "us-east-1"
  }
}

output {
  opensearch {
    hosts => ["domain-endpoint:443"]
    auth_type => {
      type => 'aws_iam'
      aws_access_key_id => 'your-access-key'
      aws_secret_access_key => 'your-secret-key'
      region => 'us-east-1'
      }
      index  => "logstash-logs-%{+YYYY.MM.dd}"
      ecs_compatibility => disabled
  }
}
```

如果您不想在組態檔案中提供 IAM 憑證，則您可以將其匯出 (或執行 `aws configure`)：

```
export AWS_ACCESS_KEY_ID="your-access-key"
export AWS_SECRET_ACCESS_KEY="your-secret-key"
export AWS_SESSION_TOKEN="your-session-token"
```

如果您的 OpenSearch Service 網域位於 VPC 中，則 Logstash OSS 機器必須能夠連線到 VPC 並可透過 VPC 安全群組存取該網域。如需詳細資訊，請參閱 the section called “關於網VPC域的存取原則”。

在 Amazon OpenSearch 服務中搜索數據

在 Amazon Ser OpenSearch vice 中搜尋文件有幾種常用方法，包括URI搜尋和要求本文搜尋。OpenSearch Service 提供額外的功能，可改善搜尋體驗，例如自訂套件、SQL支援和非同步搜尋。如需完整的 OpenSearch 搜尋API參考資料，請參閱OpenSearch 文件。

> **Note**
>
> 下列範例請求適用於 OpenSearch APIs。部分請求可能無法與較舊的 Elasticsearch 版本搭配使用。

主題

- URI搜尋
- 要求主體搜尋
- 對搜尋結果進行分頁
- 儀表板查詢語言
- Amazon OpenSearch 服務的定制包
- 使用 SQL 查詢您的 Amazon OpenSearch 服務數據
- K-最近的鄰居 (k-NN) 搜索 Amazon 服務 OpenSearch
- Amazon OpenSearch 服務中的跨群集搜索
- 學習排名 Amazon OpenSearch 服務
- Amazon OpenSearch 服務中的異步搜索
- 在 Amazon OpenSearch 服務中的時間點搜索
- 在 Amazon OpenSearch 服務語義搜索
- Amazon OpenSearch 服務中的並發細分搜索
- 自然語言查詢產生 OpenSearch

URI搜尋

通用資源識別碼 (URI) 搜尋是最簡單的搜尋形式。在URI搜尋中，您可以將查詢指定為HTTP要求參數：

```
GET https://search-my-domain.us-west-1.es.amazonaws.com/_search?q=house
```

範例回應看起來類似如下：


```
{
  "took": 25,
  "timed_out": false,
  "_shards": {
    "total": 10,
    "successful": 10,
    "skipped": 0,
    "failed": 0
  },
  "hits": {
    "total": {
      "value": 85,
      "relation": "eq",
    },
    "max_score": 6.6137657,
    "hits": [
      {
        "_index": "movies",
        "_type": "movie",
        "_id": "tt0077975",
        "_score": 6.6137657,
        "_source": {
          "directors": [
            "John Landis"
          ],
          "release_date": "1978-07-27T00:00:00Z",
          "rating": 7.5,
          "genres": [
            "Comedy",
            "Romance"
          ],
          "image_url": "http://ia.media-imdb.com/images/M/
MV5BMTY2OTQxNTc1OF5BMl5BanBnXkFtZTYwNjA3NjI5._V1_SX400_.jpg",
          "plot": "At a 1962 College, Dean Vernon Wormer is determined to expel the
 entire Delta Tau Chi Fraternity, but those troublemakers have other plans for him.",
          "title": "Animal House",
          "rank": 527,
          "running_time_secs": 6540,
          "actors": [
```

```
            "John Belushi",
            "Karen Allen",
            "Tom Hulce"
          ],
          "year": 1978,
          "id": "tt0077975"
        }
      },
      ...
    ]
  }
}
```

根據預設，此查詢在所有索引中的所有欄位裡搜尋含有 house 的詞語。 若要縮小搜尋範圍，請在下列項目中指定索引 (`moviestitle`) 和文件欄位 ()URI：

```
GET https://search-my-domain.us-west-1.es.amazonaws.com/movies/_search?q=title:house
```

您可以在請求中包含其他參數，但支援的參數僅提供一小部分的 OpenSearch 搜尋選項。下列請求傳回 20 個結果 (而非預設的 10 個)，並根據年份排序 (而非依據 `_score`)：

```
GET https://search-my-domain.us-west-1.es.amazonaws.com/movies/_search?
q=title:house&size=20&sort=year:desc
```

要求主體搜尋

若要執行更複雜的搜尋，請使用HTTP要求主體和 OpenSearch網域特定語言 (DSL) 來進行查詢。此查詢DSL可讓您指定 OpenSearch 搜尋選項的完整範圍。

> **Note**
>
> 您不能在文字欄位值中包含 Unicode 特殊字元，否則會將值剖析為由特殊字元分隔的多個值。這種不正確的剖析可能會導致意外對文件進行篩選，並可能影響對其存取權的控制。如需詳細資訊，請參閱文 OpenSearch件中文字欄位中 Unicode 特殊字元的附註。

下列`match`查詢類似於最終URI搜尋範例：

```
POST https://search-my-domain.us-west-1.es.amazonaws.com/movies/_search
{
```

```
  "size": 20,
  "sort": {
    "year": {
      "order": "desc"
    }
  },
  "query": {
    "query_string": {
      "default_field": "title",
      "query": "house"
    }
  }
}
```

> **Note**
>
> _searchAPI接受HTTPGET和POST用於請求主體搜索，但並非所有HTTP客戶端都支持將請求主體添加到GET請求中。 POST是比較普遍的選擇。

在許多情況下，您可能想要搜尋多個欄位，但並非所有欄位。使用 `multi_match` 查詢：

```
POST https://search-my-domain.us-west-1.es.amazonaws.com/movies/_search
{
  "size": 20,
  "query": {
    "multi_match": {
      "query": "house",
      "fields": ["title", "plot", "actors", "directors"]
    }
  }
}
```

增加欄位

您可以透過「增加」特定欄位來提升搜尋相關性。增加功能為運用倍數在一個欄位中加重配對數，使之較其他欄位中的配對數更高。在下面的例子中，匹配 `title` 欄位中的 John 對`_score` 的影響是在 `plot` 欄位中匹配的兩倍，以及在 `actors` 或 `directors` 欄位中匹配的四倍。結果就是 John Wick 和 John Carter 之類的影片會在搜尋結果的頂部，且 John Travolta 主演的影片會出現在底部。

```
POST https://search-my-domain.us-west-1.es.amazonaws.com/movies/_search
```

```
{
  "size": 20,
  "query": {
    "multi_match": {
      "query": "john",
      "fields": ["title^4", "plot^2", "actors", "directors"]
    }
  }
}
```

搜尋結果反白呈現

如果查詢匹配一個或多個字段，該highlight選項告訴 OpenSearch 返回hits數組內的附加對象：

```
POST https://search-my-domain.us-west-1.es.amazonaws.com/movies/_search
{
  "size": 20,
  "query": {
    "multi_match": {
      "query": "house",
      "fields": ["title^4", "plot^2", "actors", "directors"]
    }
  },
  "highlight": {
    "fields": {
      "plot": {}
    }
  }
}
```

如果查詢符合 plot 欄位的內容，則命中看起來會如下：

```
{
  "_index": "movies",
  "_type": "movie",
  "_id": "tt0091541",
  "_score": 11.276199,
  "_source": {
    "directors": [
      "Richard Benjamin"
    ],
    "release_date": "1986-03-26T00:00:00Z",
```

```
    "rating": 6,
    "genres": [
      "Comedy",
      "Music"
    ],
    "image_url": "http://ia.media-imdb.com/images/M/
MV5BMTIzODEzODE2OF5BMl5BanBnXkFtZTcwNjQ3ODcyMQ@@._V1_SX400_.jpg",
    "plot": "A young couple struggles to repair a hopelessly dilapidated house.",
    "title": "The Money Pit",
    "rank": 4095,
    "running_time_secs": 5460,
    "actors": [
      "Tom Hanks",
      "Shelley Long",
      "Alexander Godunov"
    ],
    "year": 1986,
    "id": "tt0091541"
  },
  "highlight": {
    "plot": [
      "A young couple struggles to repair a hopelessly dilapidated <em>house</em>."
    ]
  }
}
```

根據預設，會將相符字串 OpenSearch 包裝在標籤中，在相符項目周圍提供最多 100 個字元的環境，並透過識別標點符號、空格、定位鍵和換行符號，將內容分成句子。所有設定皆可自訂：

```
POST https://search-my-domain.us-west-1.es.amazonaws.com/movies/_search
{
  "size": 20,
  "query": {
    "multi_match": {
      "query": "house",
      "fields": ["title^4", "plot^2", "actors", "directors"]
    }
  },
  "highlight": {
    "fields": {
      "plot": {}
    },
    "pre_tags": "<strong>",
```

```
    "post_tags": "</strong>",
    "fragment_size": 200,
    "boundary_chars": ".,!? "
  }
}
```

伯爵 API

如果您對文件的內容不感興趣，只想知道相符項目的數目，可以使用_countAPI代替 _searchAPI. 下列請求使用 query_string 查詢來識別浪漫喜劇：

```
POST https://search-my-domain.us-west-1.es.amazonaws.com/movies/_count
{
  "query": {
    "query_string": {
      "default_field": "genres",
      "query": "romance AND comedy"
    }
  }
}
```

範例回應看起來類似如下：

```
{
  "count": 564,
  "_shards": {
    "total": 5,
    "successful": 5,
    "skipped": 0,
    "failed": 0
  }
}
```

對搜尋結果進行分頁

如果您需要顯示大量的搜索結果，您可以使用幾種不同的方法來實現分頁。

時間點

時間點 (PIT) 功能是一種搜尋類型，可讓您針對固定時間的資料集執行不同的查詢。這是中首選的分頁方法 OpenSearch，特別是對於深分頁。您可以搭PIT配 OpenSearch 服務 2.5 版及更新版本使用。如需有關 PIT 的詳細資訊，請參閱 ???。

`from`和`size`參數

最簡單的分頁方式是使用`from`和`size`參數。以下請求傳回結果 20-39 項以零為索引的搜尋結果清單：

```
POST https://search-my-domain.us-west-1.es.amazonaws.com/movies/_search
{
  "from": 20,
  "size": 20,
  "query": {
    "multi_match": {
      "query": "house",
      "fields": ["title^4", "plot^2", "actors", "directors"]
    }
  }
}
```

如需搜尋分頁的詳細資訊，請參閱 OpenSearch 文件中的分頁結果。

儀表板查詢語言

您可以使用儀表板查詢語言 (DQL) 來搜尋儀 OpenSearch 表板中的資料和視覺效果。DQL使用四種主要查詢類型：字詞、布林值、日期和範圍，以及巢狀欄位。

術語查詢

術語查詢要求您指定要搜尋的術語。

若要執行術語查詢，請輸入下列內容：

```
host:www.example.com
```

布林值查詢

您可以使用布林運算子 `AND`、`or` 以及 `not` 以合併多個查詢。

要執行布林值查詢，請貼上以下內容：

```
host.keyword:www.example.com and response.keyword:200
```

日期和範圍查詢

您可以使用日期和範圍查詢來尋找查詢之前或之後的日期。

- > 表示搜尋指定日期之後的日期。
- < 表示搜尋指定日期之前的日期。

```
@timestamp > "2020-12-14T09:35:33"
```

巢狀欄位查詢

如果您擁有一個帶巢狀欄位的文件，則必須指定要擷取文件的哪些部分。以下是包含巢狀欄位的範例文件：

```
{"NBA players":[
    {"player-name": "Lebron James",
      "player-position": "Power forward",
      "points-per-game": "30.3"
    },
    {"player-name": "Kevin Durant",
      "player-position": "Power forward",
      "points-per-game": "27.1"
    },
    {"player-name": "Anthony Davis",
      "player-position": "Power forward",
      "points-per-game": "23.2"
    },
    {"player-name": "Giannis Antetokounmpo",
      "player-position": "Power forward",
      "points-per-game":"29.9"
    }
  ]
}
```

若要使用擷取特定欄位DQL，請貼上下列內容：

```
NBA players: {player-name: Lebron James}
```

若要從巢狀文件中擷取多個物件，請貼入下列內容：

```
NBA players: {player-name: Lebron James} and NBA players: {player-name: Giannis
 Antetokounmpo}
```

若要在某個範圍內搜尋，請貼上以下內容：

```
NBA players: {player-name: Lebron James} and NBA players: {player-name: Giannis
 Antetokounmpo and < 30}
```

如果您的文件在另一個物件中有巢狀物件，您仍然可以透過指定所有層級來擷取資料。如要執行此操作，請貼上以下內容：

```
Top-Power-forwards.NBA players: {player-name:Lebron James}
```

Amazon OpenSearch 服務的定制包

Amazon Ser OpenSearch vice 可讓您上傳自訂字典檔案 (例如停用字和同義字)，並提供數個預先封裝的選用外掛程式，讓您與網域建立關聯。這兩種類型的文件的通用術語是包。

字典文件通過告訴忽略某些高頻單詞或 OpenSearch 將諸如「冰淇淋」，「意式冰淇淋」和「冰淇淋」等詞語對待，從而改善您的搜索結果。它們還可以提高字根還原的能力，例如在 Japanese (kuromoji) Analysis 分析外掛程式。

可選插件可以為您的域提供附加功能。例如，您可以使用 Amazon Personalize 外掛程式為您提供個人化的搜尋結果。可選插件使用`ZIP-PLUGIN`包類型。如需選用外掛程式的詳細資訊，請參閱the section called “依引擎版本分類的外掛程式”。

主題

- 套件許可要求
- 將套件上傳至 Amazon S3
- 匯入和關聯套件
- 使用套件搭配 OpenSearch
- 更新套件
- 字典的手動索引更新

- 解除關聯並移除套件

套件許可要求

沒有管理員存取權的使用者需要特定 AWS Identity and Access Management (IAM) 動作才能管理套件：

- `es:CreatePackage`-在 OpenSearch 服務區域中建立套件
- `es:DeletePackage`-從 OpenSearch 服務區域刪除套件
- `es:AssociatePackage` - 將套件關聯到網域
- `es:DissociatePackage` - 取消套件與網域的關聯

您也需要自訂套件所在的 Amazon S3 儲存貯體路徑或物件的許可。

授予 IAM 內的所有許可，而不是在網域存取政策中。如需詳細資訊，請參閱 the section called “身分和存取權管理”。

將套件上傳至 Amazon S3

本節介紹了如何上傳自定義字典包，因為可選插件包已經預先安裝。您必須先將自訂字典上傳到 Amazon S3 儲存貯體，才能將自訂字典與網域建立關聯。如需指示說明，請參閱 Amazon Simple Storage Service 使用者指南中的上傳物件。支持的插件不需要上傳。

如果您的字典包含敏感資訊，請在上傳時使用 S3 管理的金鑰指定伺服器端加密。 OpenSearch 服務無法存取您使用 AWS KMS 金鑰保護的 S3 上的檔案。

上傳檔案後，請記下其 S3 路徑。路徑格式為 `s3://bucket-name/file-path/file-name`。

您可以使用下列同義字檔案進行測試。另存為 `synonyms.txt`。

```
danish, croissant, pastry
ice cream, gelato, frozen custard
sneaker, tennis shoe, running shoe
basketball shoe, hightop
```

某些字典 (例如 Hunspell 字典) 會使用多個檔案並要求在檔案系統上使用自己的字典。目前，OpenSearch 服務僅支援單一檔案字典。

匯入和關聯套件

控制台是將自定義字典導入 OpenSearch 服務的最簡單方法。當您從 Amazon S3 匯入字典時，OpenSearch 服務會存放自己的套件副本，並使用 AES-256 與 OpenSearch 服務受管金鑰自動加密該副本。

可選插件已經預先安裝在 OpenSearch 服務中，因此您不需要自己上傳它們，但您確實需要將插件與域關聯。可用的外掛程式會列在主控台的「套件」畫面上。

匯入封裝並將其與網域建立關聯 AWS Management Console

1. 在 Amazon OpenSearch 服務主控台中，選擇套件。
2. 選擇 Import package (匯入套件)。
3. 為自訂字典指定描述性名稱。
4. 提供檔案的 S3 路徑，然後選擇 Submit (提交)。
5. 返回 Packages (套件) 畫面。
6. 當封裝狀態為 Available (可用) 時，請加以選取。可選插件將自動可用。
7. 選擇「關聯至網域」。
8. 選取網域，然後選擇 Associate (關聯)。
9. 在導覽窗格中，選擇您的網域，然後移至 Packages (套件) 索引標籤。
10. 如果封裝是自訂字典，請在套件變成「可用」時記下 ID。用`analyzers/`*`id`*作要求中的檔案路徑 OpenSearch。

或者，使用 AWS CLI、SDK 或設定 API 匯入和關聯套件。如需詳細資訊，請參閱AWS CLI 命令參考和 Amazon OpenSearch 服務 API 參考。

使用套件搭配 OpenSearch

本節介紹如何使用這兩種類型的軟件包：自定義字典和可選插件。

使用自訂字典

將檔案與網域建立關聯後，您可以在建立分詞器和字符篩選條件時在 `synonyms_path`、`stopwords_path` 和 `user_dictionary` 等參數中使用該檔案。確切的參數因物件而異。多個物件可支援 `synonyms_path` 和 `stopwords_path`，但 `user_dictionary` 專屬於 kuromoji 外掛程式。

對於 IK (中文) 分析外掛程式，您可以將自訂字典檔案做為自定套件上傳，並將其與一個網域相關聯，且外掛程式會自動將其掛載，不需要 `user_dictionary` 參數。如果您的檔案是同義詞檔案，請使用 `synonyms_path` 參數。

以下範例會將同義字檔案新增至新索引：

```
PUT my-index
{
  "settings": {
    "index": {
      "analysis": {
        "analyzer": {
          "my_analyzer": {
            "type": "custom",
            "tokenizer": "standard",
            "filter": ["my_filter"]
          }
        },
        "filter": {
          "my_filter": {
            "type": "synonym",
            "synonyms_path": "analyzers/F111111111",
            "updateable": true
          }
        }
      }
    }
  },
  "mappings": {
    "properties": {
      "description": {
        "type": "text",
        "analyzer": "standard",
        "search_analyzer": "my_analyzer"
      }
    }
  }
}
```

此請求建立使用標準分詞器和同義詞字符篩選條件索引的自訂分析器。

- 分詞器會根據一組規則將字符分解為字符 (通常是字詞)。最簡單的例子是空格分詞器，每次遇到一個空白字符時，便會將前面的字元分解為字符。一個更複雜的例子是標準分詞器，它會使用一組基於語法的規則跨多種語言作業。
- 字符篩選條件會新增、修改或刪除字符。例如，同義字字符篩選條件會在同義字清單中找到單字時加入字符。停止字符篩選條件會在停止字詞清單中找到字詞時移除標記。

此請求還將一個文本字段（`description`）添加到映射，並告訴使 OpenSearch 用新的分析器作為其搜索分析器。您可以看到它仍然使用標準分析器作為其索引分析器。

最後，請注意字符篩選器中的 `"updateable": true` 行。此欄位僅適用於搜尋分析器，不適用於索引分析器，如果您稍後想要自動更新搜尋分析器，此欄位就非常重要。

為了測試，我們加入了一些文件索引：

```
POST _bulk
{ "index": { "_index": "my-index", "_id": "1" } }
{ "description": "ice cream" }
{ "index": { "_index": "my-index", "_id": "2" } }
{ "description": "croissant" }
{ "index": { "_index": "my-index", "_id": "3" } }
{ "description": "tennis shoe" }
{ "index": { "_index": "my-index", "_id": "4" } }
{ "description": "hightop" }
```

然後使用同義詞來搜尋它們：

```
GET my-index/_search
{
  "query": {
    "match": {
      "description": "gelato"
    }
  }
}
```

在此情況下，會 OpenSearch 傳回下列回應：

```
{
  "hits": {
    "total": {
```

```
      "value": 1,
      "relation": "eq"
    },
    "max_score": 0.99463606,
    "hits": [{
      "_index": "my-index",
      "_type": "_doc",
      "_id": "1",
      "_score": 0.99463606,
      "_source": {
        "description": "ice cream"
      }
    }]
  }
}
```

> **Tip**
>
> 字典檔案使用與其大小呈正比的 Java 堆積空間。例如，2 GiB 的字典檔案可能會在節點上使用 2 GiB 的堆積空間。如果您使用大型檔案，請確保節點有足夠的堆積空間可容納這些檔案。監控 `JVMMemoryPressure` 指標，並視需要擴展您的叢集。

使用可選插件

OpenSearch 服務可讓您將預先安裝的選用 OpenSearch 外掛程式與網域建立關聯。選用的外掛程式套件與特定 OpenSearch 版本相容，而且只能與該版本的網域相關聯。您網域的可用套件清單包括所有支援與您的網域版本相容的外掛程式。將外掛程式與網域建立關聯後，網域上的安裝程序便會開始。然後，您可以在向 OpenSearch 服務發出請求時引用並使用該插件。

關聯和解除外掛程式需要藍/綠部署。如需詳細資訊，請參閱 the section called “通常會導致藍/綠部署的變更”。

可選插件包括語言分析儀和自定義搜索結果。例如，Amazon Personalize 搜尋排名外掛程式使用機器學習來為您的客戶個人化搜尋結果。如需有關此外掛程式的詳細資訊，請參閱個人化搜尋結果。OpenSearch如需所有支援外掛程式的清單，請參閱the section called “依引擎版本分類的外掛程式”。

酢橘插件

對於 Sudachi 插件，當您重新關聯字典文件時，它不會立即反映在域上。當下一個藍/綠部署在網域上執行時，做為組態變更或其他更新的一部分時，字典會重新整理。或者，您也可以使用更新的資料建立

新套件、使用這個新套件建立新索引、將現有索引重新建立索引至新索引，然後刪除舊索引。如果您偏好使用重新建立索引的方法，請使用索引別名，這樣就不會中斷流量。

此外，Sudachi 插件僅支持二進制 Sudachi 字典，您可以通過 CreatePackageAPI 操作上傳該字典。有關預構建的系統字典和用於編譯用戶字典的過程的信息，請參閱 Sudachi 文檔。

下面的示例演示瞭如何將系統和用戶字典與 Sudachi 標記生成器一起使用。您必須將這些字典上傳為具有類型的自訂套件，`TXT-DICTIONARY`並在其他設定中提供其套件 ID。

```
PUT sudachi_sample
{
  "settings": {
    "index": {
      "analysis": {
        "tokenizer": {
          "sudachi_tokenizer": {
            "type": "sudachi_tokenizer",
            "additional_settings": "{\"systemDict\": \"<system-dictionary-package-
id>\",\"userDict\": [\"<user-dictionary-package-id>\"]}"
        }
        },
        "analyzer": {
          "sudachi_analyzer": {
            "filter": ["my_searchfilter"],
            "tokenizer": "sudachi_tokenizer",
            "type": "custom"
          }
        },
        "filter":{
          "my_searchfilter": {
            "type": "sudachi_split",
            "mode": "search"
          }
        }
      }
    }
  }
}
```

更新套件

本節僅介紹如何更新自訂字典套件，因為選用的外掛程式套件已經為您更新。將新版本的字典上傳到 Amazon S3 並不會自動更新 Amazon OpenSearch 服務上的套件。 OpenSearch 服務會儲存自己的檔案副本，因此如果您將新版本上傳到 S3，則必須手動更新它。

每個關聯網域也都會儲存其自己的檔案副本。為了保持搜尋行為可預測，網域會繼續使用其目前的套件版本，直到您明確更新它們為止。若要更新自訂套件，請修改中的檔案 Amazon S3 Control、更新 OpenSearch Service 中的套件，然後套用更新。

使用更新套件 AWS Management Console

1. 在 [OpenSearch 服務] 主控台中，選擇 [套件]。
2. 選擇套件和 Update (更新)。
3. 提供檔案的 S3 路徑，然後選擇 Update package (更新套件)。
4. 返回 Packages (套件) 畫面。
5. 當套件狀態變為 Available (可用) 時，請加以選取。然後選擇一個或多個關聯網域，選擇 Apply update (套用更新) 並確認。等待關聯狀態變為 Active (作用中)。
6. 接下來的步驟會有所不同，這取決於您如何設定索引：
   - 如果您的網域正在執行 OpenSearch 或 Elasticsearch 7.8 或更新版本，且僅使用可更新欄位設定為 true 的搜尋分析器，則不需要採取任何進一步的動作。 OpenSearch 服務會使用外掛程式/搜尋分析器 API 自動更新您的索引。
   - 如果您的網域執行 Elasticsearch 7.7 或更早版本，請使用索引分析器，或未使用`updateable`欄位，請參閱。the section called “字典的手動索引更新”

雖然主控台是最簡單的方法，但您也可以使用 AWS CLI、SDK 或設定 API 來更新 OpenSearch 服務套件。如需詳細資訊，請參閱AWS CLI 命令參考和 Amazon OpenSearch 服務 API 參考。

使用 AWS SDK 更新套件

您可以使用開發套件來自動化更新程序，而不是在主控台中手動更新套件。下列範例 Python 指令碼會將新套件檔案上傳至 Amazon S3、更新 OpenSearch 服務中的套件，並將新套件套用至指定的網域。確認更新成功後，它會進行範例呼叫，以 OpenSearch展示已套用新的同義字。

您必須提供
`host`、`region`、`file_name`、`bucket_name`、`s3_key`、`package_id`、`domain_name` 和 `query` 的值。

```
from requests_aws4auth import AWS4Auth
import boto3
import requests
import time
import json
import sys

host = ''  # The OpenSearch domain endpoint with https:// and a trailing slash. For
 example, https://my-test-domain.us-east-1.es.amazonaws.com/
region = ''  # For example, us-east-1
file_name = ''  # The path to the file to upload
bucket_name = ''  # The name of the S3 bucket to upload to
s3_key = ''  # The name of the S3 key (file name) to upload to
package_id = ''  # The unique identifier of the OpenSearch package to update
domain_name = ''  # The domain to associate the package with
query = ''  # A test query to confirm the package has been successfully updated

service = 'es'
credentials = boto3.Session().get_credentials()
client = boto3.client('opensearch')
awsauth = AWS4Auth(credentials.access_key, credentials.secret_key,
                   region, service, session_token=credentials.token)


def upload_to_s3(file_name, bucket_name, s3_key):
    """Uploads file to S3"""
    s3 = boto3.client('s3')
    try:
        s3.upload_file(file_name, bucket_name, s3_key)
        print('Upload successful')
        return True
    except FileNotFoundError:
        sys.exit('File not found. Make sure you specified the correct file path.')


def update_package(package_id, bucket_name, s3_key):
    """Updates the package in OpenSearch Service"""
    print(package_id, bucket_name, s3_key)
    response = client.update_package(
        PackageID=package_id,
        PackageSource={
            'S3BucketName': bucket_name,
            'S3Key': s3_key
```

```
        }
    )
    print(response)


def associate_package(package_id, domain_name):
    """Associates the package to the domain"""
    response = client.associate_package(
        PackageID=package_id, DomainName=domain_name)
    print(response)
    print('Associating...')


def wait_for_update(domain_name, package_id):
    """Waits for the package to be updated"""
    response = client.list_packages_for_domain(DomainName=domain_name)
    package_details = response['DomainPackageDetailsList']
    for package in package_details:
        if package['PackageID'] == package_id:
            status = package['DomainPackageStatus']
            if status == 'ACTIVE':
                print('Association successful.')
                return
            elif status == 'ASSOCIATION_FAILED':
                sys.exit('Association failed. Please try again.')
            else:
                time.sleep(10)  # Wait 10 seconds before rechecking the status
                wait_for_update(domain_name, package_id)


def sample_search(query):
    """Makes a sample search call to OpenSearch"""
    path = '_search'
    params = {'q': query}
    url = host + path
    response = requests.get(url, params=params, auth=awsauth)
    print('Searching for ' + '"' + query + '"')
    print(response.text)
```

> **Note**
>
> 如果您在使用執行指令碼時收到「找不到套件」錯誤 AWS CLI，可能表示 Boto3 正在使用 ~/.aws/config 中指定的任何區域，而不是 S3 儲存貯體所在的區域。執行 `aws configure` 並指定正確的區域，或者明確地將區域新增至用戶端：
>
> ```
> client = boto3.client('opensearch', region_name='us-east-1')
> ```

字典的手動索引更新

手動索引更新僅適用於自訂字典，不適用於選用的外掛程式。若要使用更新的字典，必須在符合下列任一條件時手動更新索引：

- 您的網域執行 Elasticsearch 7.7 或更早版本。
- 您使用自訂套件作為索引分析器。
- 您使用自訂套件作為搜索分析器，但不包含 updateable (可更新) 欄位。

若要使用新套件檔案更新分析器，您有兩個選項：

- 關閉並開啟您要更新的任何索引：

  ```
  POST my-index/_close
  POST my-index/_open
  ```

- 對索引進行重新索引。首先，建立使用更新的同義字檔案 (或全新檔案) 的索引。請注意，僅支援 UTF-8。

  ```
  PUT my-new-index
  {
    "settings": {
      "index": {
        "analysis": {
          "analyzer": {
            "synonym_analyzer": {
              "type": "custom",
              "tokenizer": "standard",
              "filter": ["synonym_filter"]
            }
  ```

```
        },
        "filter": {
          "synonym_filter": {
            "type": "synonym",
            "synonyms_path": "analyzers/F222222222"
          }
        }
      }
    }
  },
  "mappings": {
    "properties": {
      "description": {
        "type": "text",
        "analyzer": "synonym_analyzer"
      }
    }
  }
}
```

然後將舊索引重新索引到該新索引：

```
POST _reindex
{
  "source": {
    "index": "my-index"
  },
  "dest": {
    "index": "my-new-index"
  }
}
```

如果您經常更新索引分析器，請使用索引別名來維持最新索引的一致路徑：

```
POST _aliases
{
  "actions": [
    {
      "remove": {
        "index": "my-index",
        "alias": "latest-index"
      }
```

```
    },
    {
      "add": {
        "index": "my-new-index",
        "alias": "latest-index"
      }
    }
  ]
}
```

如果您不需要舊索引，請將其刪除：

```
DELETE my-index
```

解除關聯並移除套件

將套件 (無論是自訂字典或選用外掛程式) 與網域分離，表示您在建立新索引時無法再使用該套件。解除關聯套件之後，使用該套件的現有索引就無法再使用它。您必須先從任何索引中移除套件，才能將其解除關聯，否則分離會失敗。

主控台是將套件與網域分離並從服務中移除的最簡單方法。 OpenSearch 從 OpenSearch 服務移除套件並不會將其從 Amazon S3 上的原始位置移除。

將套件與網域分離 AWS Management Console

1. 前往 https://aws.amazon.com，然後選擇 Sign In to the Console (登入主控台)。
2. 在分析下，選擇 Amazon OpenSearch 服務。
3. 在導覽窗格中，選擇您的網域，然後選擇 Packages (套件) 標籤。
4. 選擇套件，Actions (動作)，然後選擇 Dissociate (解除關聯)。確認您的選擇。
5. 等待套件從清單中消失。您可能需要重新整理瀏覽器。
6. 如果您想要將套件與其他網域搭配使用，請在這裡停止。若要繼續移除套件（如果它是自訂字典），請在導覽窗格中選擇「封裝」。
7. 選取套件並選擇 Delete (刪除)。

或者，使用 AWS CLI、SDK 或設定 API 來分離和移除套件。如需詳細資訊，請參閱AWS CLI 命令參考和 Amazon OpenSearch 服務 API 參考。

使用 SQL 查詢您的 Amazon OpenSearch 服務數據

您可以使用 SQL 查詢您的 Amazon OpenSearch 服務，而不是使用基於 JSON 的OpenSearch 查詢 DSL。如果您已熟悉 SQL，或想要透過使用它的應用程式來整合您的網域，則使用 SQL 進行查詢非常實用。SQL 支援適用於執行彈性搜尋 6.5 OpenSearch 或更高版本的網域。

> **Note**
>
> 本文件說明 OpenSearch 服務與各種版本的 SQL 外掛程式，以及 JDBC 和 ODBC 驅動程式之間的版本相容性。如需有關基本和複雜查詢、函數、中繼資料查詢和彙總函式語法的資訊，請參閱開放原始碼OpenSearch文件。

使用下表查找每個版本 OpenSearch 和彈性搜索版本支持的 SQL 插件的版本。

OpenSearch

OpenSearch 版本	SQL 外掛程式版本	值得注意的功能
2.13.0	2.13.0.0	
2.11.0	2.11.0.0	添加對 PPL 語言和查詢的支持
2.9.0	2.9.0.0	添加星火連接器，並支持表和 PromQL 功能
2.7.0	2.7.0.0	新增 `datasource` API
2.5.0	2.5.0.0	
2.3.0	2.3.0.0	新增 `maketime` 和 `makedate` 日期時間函數
1.3.0	1.3.0.0	支援預設查詢限制大小和 IN 子句，以便從值清單中進行選擇
1.2.0	1.2.0.0	新增用於視覺化效果回應格式的新協議
1.1.0	1.1.0.0	支援比對功能，作為 SQL 和 PPL 中的篩選條件
1.0.0	1.0.0.0	支援查詢資料串流

Open Distro for Elasticsearch

Elasticsearch 版本	SQL 外掛程式版本	值得注意的功能
7.10	1.13.0	視窗函數的 NULL FIRST 和 LAST，CAST() 函數，SHOW 和 DESCRIBE 命令
7.9	1.11.0	新增其他日期/時間函數，ORDER BY 關鍵字
7.8	1.9.0	
7.7	1.8.0	
7.3	1.3.0	多個字串和數字運算子
7.1	1.1.0	

範例呼叫

若要使用 SQL 查詢資料，請使用以下格式傳送 HTTP 請求到 `_sql`：

```
POST domain-endpoint/_plugins/_sql
{
  "query": "SELECT * FROM my-index LIMIT 50"
}
```

> **Note**
>
> 如果您的網域正在執行彈性搜尋 OpenSearch，而非執行格式。`_opendistro/_sql`

備註和差異

對 `_plugins/_sql` 的呼叫會在請求內文中包含索引名稱，因此有相同的大量、mget、和 msearch 操作的存取政策考量。一如以往，授權許可到 API 操作時請遵循最低權限的原則。

如需了解搭配使用 SQL 與精細存取控制的相關安全考量，請參閱 the section called “精細定義存取控制”。

OpenSearch SQL 外掛程式包含許多可調整的設定。在 OpenSearch 服務中，使用`_cluster/settings`路徑，而不是外掛程式設定 path (`_plugins/_query/settings`)：

```
PUT _cluster/settings
{
  "transient" : {
    "plugins.sql.enabled" : true
  }
}
```

對於舊版 Elasticsearch 網域，請將 `plugins` 取代為 `opendistro`：

```
PUT _cluster/settings
{
  "transient" : {
    "opendistro.sql.enabled" : true
  }
}
```

SQL Workbench

SQL 工作台是 OpenSearch 儀表板使用者介面，可讓您執行隨選 SQL 查詢、將 SQL 翻譯成其他等效項目，以及檢視和儲存結果為文字、JSON、JDBC 或 CSV。如需詳細資訊，請參閱 Query Workbench。

SQL CLI

SQL CLI 是可透過 `opensearchsql` 命令啟動的獨立 Python 應用程式。如需安裝、設定和使用的步驟，請參閱 SQL CLI。

JDBC 驅動程式

Java 資料庫連線 (JDBC) 驅動程式可讓您整合 OpenSearch 服務網域與您最愛的商業智慧 (BI) 應用程式。若要下載驅動程式，請按一下這裡。如需詳細資訊，請參閱存GitHub放庫。

以下表格摘要驅動程式版本的相容性。

OpenSearch

OpenSearch 版本	JDBC 驅動程式版本
2.13	1.1.0.1
2.11	1.1.0.1
2.9	1.1.0.1
2.7	1.1.0.1
2.5	1.1.0.1
2.3	1.1.0.1
1.3	1.1.0.1
1.2	1.1.0.1
1.1	1.1.0.1
1.0	1.1.0.1

Open Distro for Elasticsearch

Elasticsearch 版本	JDBC 驅動程式版本
7.10	1.13.0
7.9	1.11.0
7.8	1.9.0
7.7	1.8.0
7.4	1.4.0
7.1	1.0.0
6.8	0.9.0

Elasticsearch 版本	JDBC 驅動程式版本
6.7	0.9.0
6.5	0.9.0

ODBC 驅動程式

開放式資料庫連線 (ODBC) 驅動程式是 Windows 和 macOS 的唯讀 ODBC 驅動程式，可讓您將商業智慧和資料視覺化應用程式 (如 Microsoft Excel) 連接到 SQL 外掛程式。

您可以在 OpenSearch 成品頁面上下載工作驅動程式範例檔案。如需有關安裝驅動程式的詳細資訊，請參閱上的 SQL 儲存庫 GitHub。

K-最近的鄰居 (k-NN) 搜索 Amazon 服務 OpenSearch

Amazon OpenSearch 服務的 k-nN 是其關聯的 k 最近鄰算法的縮寫，可讓您搜索向量空間中的點，並通過歐幾里得距離或餘弦相似性找到這些點的「最近鄰」。使用案例包括建議 (例如，音樂應用程式中「其他您可能喜歡的歌曲」功能)、影像辨識和詐騙偵測。

> **Note**
>
> 本文件說明 OpenSearch 服務與各種 K-NN 外掛程式版本之間的相容性，以及搭配託管 OpenSearch 服務使用外掛程式時的限制。如需 K-NN 外掛程式的完整文件，包括簡單而複雜的範例、參數參考，以及外掛程式的完整 API 參考資料，請參閱開放原始碼OpenSearch 文件。開放原始碼文件也涵蓋效能調整和 K-NN 專屬叢集設定。

使用下表找出在您的 Amazon OpenSearch 服務網域上執行的 k-NN 外掛程式版本。每個 K-NN 外掛程式版本對應於OpenSearch或彈性搜尋版本。

OpenSearch

OpenSearch 版本	k-NN 外掛程式版本	值得注意的功能
2.13	2.13.0.0	

OpenSearch 版本	k-NN 外掛程式版本	值得注意的功能
2.11	2.11.0.0	增加了對 k-NN 查`ignore_unmapped` 詢的支持
2.9	2.9.0.0	使用 Faiss 引擎實作 K-nN 位元組向量和高效篩選
2.7	2.7.0.0	
2.5	2.5.0.0	擴展 SystemIndexPlugin K-NN 模型系統索引，添加了 Lucene 特定的文件擴展名到核心 HybridFS
2.3	2.3.0.0	
1.3	1.3.0.0	
1.2	1.2.0.0	新增對 Faiss 函式庫的支援
1.1	1.1.0.0	
1.0	1.0.0.0	重新命名 REST API，同時支援向後相容性，將命名空間從 `opendistro` 重新命名為 `opensearch`

Elasticsearch

Elasticsearch 版本	k-NN 外掛程式版本	值得注意的功能
7.1	1.3.0.0	歐幾里德距離
7.4	1.4.0.0	
7.7	1.8.0.0	餘弦相似度
7.8	1.9.0.0	
7.9	1.11.0.0	Warmup API，自訂評分
7.10	1.13.0.0	漢明距離、L1 Norm 距離和 Painless 指令碼

k-NN 入門

若要使用 k-NN，您必須使用 `index.knn` 設定建立索引，並新增資料類型為 `knn_vector` 的一個或多個欄位。

```
PUT my-index
{
  "settings": {
    "index.knn": true
  },
  "mappings": {
    "properties": {
      "my_vector1": {
        "type": "knn_vector",
        "dimension": 2
      },
      "my_vector2": {
        "type": "knn_vector",
        "dimension": 4
      }
    }
  }
}
```

`knn_vector` 資料類型支援最多 10,000 個浮點數的單一清單，其中包含由所需 `dimension` 參數定義的浮點數目。建立索引之後，將一些資料新增至其中。

```
POST _bulk
{ "index": { "_index": "my-index", "_id": "1" } }
{ "my_vector1": [1.5, 2.5], "price": 12.2 }
{ "index": { "_index": "my-index", "_id": "2" } }
{ "my_vector1": [2.5, 3.5], "price": 7.1 }
{ "index": { "_index": "my-index", "_id": "3" } }
{ "my_vector1": [3.5, 4.5], "price": 12.9 }
{ "index": { "_index": "my-index", "_id": "4" } }
{ "my_vector1": [5.5, 6.5], "price": 1.2 }
{ "index": { "_index": "my-index", "_id": "5" } }
{ "my_vector1": [4.5, 5.5], "price": 3.7 }
{ "index": { "_index": "my-index", "_id": "6" } }
{ "my_vector2": [1.5, 5.5, 4.5, 6.4], "price": 10.3 }
{ "index": { "_index": "my-index", "_id": "7" } }
{ "my_vector2": [2.5, 3.5, 5.6, 6.7], "price": 5.5 }
```

```
{ "index": { "_index": "my-index", "_id": "8" } }
{ "my_vector2": [4.5, 5.5, 6.7, 3.7], "price": 4.4 }
{ "index": { "_index": "my-index", "_id": "9" } }
{ "my_vector2": [1.5, 5.5, 4.5, 6.4], "price": 8.9 }
```

然後，您可以使用 knn 查詢類型搜尋資料。

```
GET my-index/_search
{
  "size": 2,
  "query": {
    "knn": {
      "my_vector2": {
        "vector": [2, 3, 5, 6],
        "k": 2
      }
    }
  }
}
```

在此情況下，k 是您想要查詢傳回的近鄰數目，但您亦須包含 `size` 選項。否則，您會獲得每個碎片 (和每個區段) 的 k 結果，而不是整個查詢的 k 結果。KNN 支援的最大 k 值為 10,000。

如果您將 knn 查詢與其他子句混合使用，則可能會收到少於 k 個的結果。在此範例中，`post_filter` 子句會將結果的數目從 2 減少為 1。

```
GET my-index/_search
{
  "size": 2,
  "query": {
    "knn": {
      "my_vector2": {
        "vector": [2, 3, 5, 6],
        "k": 2
      }
    }
  },
  "post_filter": {
    "range": {
      "price": {
        "gte": 6,
        "lte": 10
```

```
        }
      }
    }
  }
```

如果您需要處理大量查詢，同時維持最佳效能，您可以使用 `_msearch`API 建構 JSON 大量搜尋，並傳送單一要求以執行多個搜尋：

```
GET _msearch
{ "index": "my-index"}
{ "query": { "knn": {"my_vector2":{"vector": [2, 3, 5, 6],"k":2 }} } }
{ "index": "my-index", "search_type": "dfs_query_then_fetch"}
{ "query": { "knn": {"my_vector1":{"vector": [2, 3],"k":2 }} } }
```

下列影片示範如何針對 K-NN 查詢設定大量向量搜尋。

k-NN 差異、調校和限制

OpenSearch 可讓您使用 API 修改所有 k-NN 設定`_cluster/settings`。在 OpenSearch 服務上，您可以變更除`knn.memory.circuit_breaker.enabled`和以外的所有設定`knn.circuit_breaker.triggered`。k-nN 統計資料包含在 Amazon CloudWatch 指標中。

特別是，請根據執行處理類型的`knn.memory.circuit_breaker.limit`統計資料和可用 RAM，檢查每個資料節點上的`KNNGraphMemoryUsage`測量結果。 OpenSearch 服務使用 Java 堆積執行個體的一半 RAM (最多 32 GiB 的堆積大小)。根據預設，k-NN 最高會使用剩下一半的 50%，這樣具有 32 GiB 的 RAM 的執行個體類型就能容納 8 GiB 的圖形 (32 * 0.5 * 0.5)。如果圖形記憶體用量超過此值，效能可能會受到影響。

如果索引使用近似的 k-nN ()，則無法將 k-n N 索引遷移到UltraWarm或冷存儲。`"index.knn": true`如果已將 `index.knn` 設為 `false` (準確 k-NN)，則您仍可將索引移動至其他儲存層。

Amazon OpenSearch 服務中的跨群集搜索

Amazon OpenSearch 服務中的跨叢集搜尋可讓您跨多個連線網域執行查詢和彙總。通常使用多個較小的網域 (而不是單一大型網域) 會比較有意義，尤其是在執行不同類型工作負載的情況下。

透過工作負載特定網域可執行以下任務：

- 選擇特定工作負載的執行個體類型以優化每個網域。

- 建立多個工作負載間的故障隔離界限。也就是說，如果其中一個工作負載失敗，此故障會包含在該特定網域內，而且不會影響其他工作負載。
- 更輕鬆地跨網域進行擴展。

跨叢集搜尋支援 OpenSearch 儀表板，因此您可以跨所有網域建立視覺效果和儀表板。您需要支付在網域之間AWS 傳輸的搜尋結果的標準資料傳輸費用。

> **Note**
>
> 開放原始碼 OpenSearch 也有跨叢集搜尋的文件。與受管 Amazon OpenSearch 服務網域相比，開放原始碼叢集的設定差異很大。最值得注意的是，在 OpenSearch 服務中，您可以使用 AWS Management Console 而不是透過 cURL 來設定跨叢集連線。此外，受管服務除了精細的存取控制之外，還使用 AWS Identity and Access Management (IAM) 進行跨叢集身份驗證。因此，我們建議您使用此文件而非開放原始碼 OpenSearch 文件來設定網域的跨叢集搜尋。

主題

- 限制
- 跨叢集搜尋先決條件
- 跨叢集搜尋定價
- 設定連線
- 移除連線
- 設定安全性和範例演練
- OpenSearch 儀表板

限制

跨叢集搜尋有多項重要限制：

- 您無法將彈性搜索域連接到域。 OpenSearch
- 您無法連線至自我管理 OpenSearch/彈性搜尋叢集。
- 若要跨區域連線網域，兩個網域都必須位於彈性搜尋 7.10 或更新版本上。 OpenSearch
- 一個網域最多可以有 20 個外寄連線。同樣地，一個網域最多可以有 20 個傳入連線。換句話說，一個網域最多可連線到 20 個其他網域。

- 來源網域的版本必須與目的網域相同或更高。如果您在兩個網域之間設定了雙向連線，並且想要升級其中一個或兩個網域，則必須先刪除其中一個連線。
- 您無法將自訂字典或 SQL 使用跨叢集搜尋搭配使用。
- 您無法用 AWS CloudFormation 來連線網域。
- 您無法在 M3 或高載 (T2 和 T3) 執行個體上使用跨叢集搜尋。

跨叢集搜尋先決條件

設定跨叢集搜尋前，請確認網域符合下列需求：

- 兩個 OpenSearch 網域，或 6.7 版或更新版本的彈性搜尋網域
- 已啟用精細存取控制
- N ode-to-node 加密已啟用

跨叢集搜尋定價

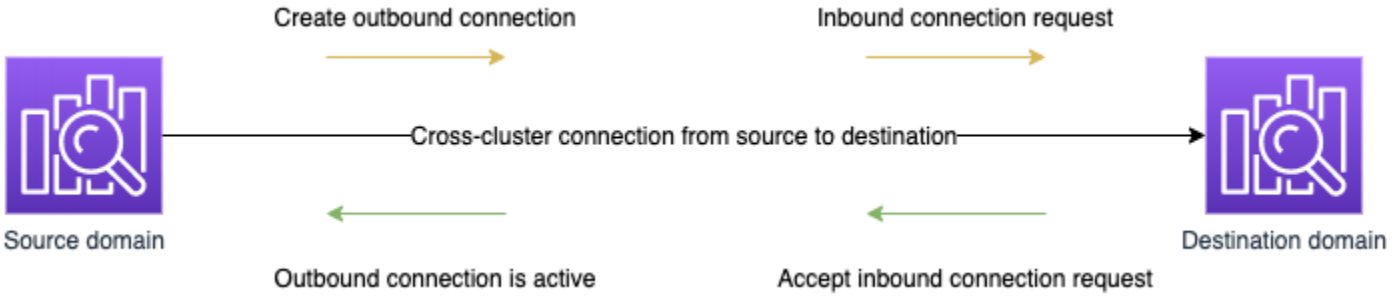
跨網域搜尋無須額外付費。

設定連線

「來源」網域是指跨叢集搜尋請求的來源位置。換句話說，來源網域是您傳送初始搜尋請求的目標位置。

「目的地」網域是來源網域查詢的網域。

跨叢集連線為單向 (從來源到目的地網域)。也就是說，目的地網域無法查詢來源網域。不過，您可以設定相反方向的其他連線。



來源網域會建立「傳出」至目的地網域的連線。目的地網域會接收來自來源網域的「傳入」連線請求。

如何設定連線

1. 在網域儀表板上，選擇網域並移至 Connections (連線) 索引標籤。
2. 在 Outbound connections (傳出連線) 區段中，選擇 Request (請求)。
3. 對於 Connection alias (連線別名)，輸入連線的名稱。
4. 選擇連線至您 AWS 帳戶 和區域或其他帳戶或區域中的網域。
   - 若要連線到您 AWS 帳戶 和區域中的叢集，請從下拉式功能表中選取網域，然後選擇 [請求]。
   - 若要連線至另一個叢集 AWS 帳戶 或區域中的叢集，請選取遠端網域的 ARN，然後選擇 [要求]。若要跨區域連線網域，兩個網域都必須執行彈性搜尋 7.10 版或更新版本。 OpenSearch
5. 若要略過叢集查詢無法使用的叢集，請選取略過無法使用 此設定可確保在一或多個遠端叢集上發生故障時，跨叢集查詢仍會傳回部分結果。
6. 跨叢集搜尋會先驗證連線請求，確認是否符合先決條件。如果發現網域不相容，連線請求則會進入 `Validation failed` 狀態。
7. 連線請求驗證成功後，則會傳送至目的地網域，需要在這裡進行核准。在此核准發生前，連線會保持在 `Pending acceptance` 狀態。在目的地網域接受連線請求後，狀態會變更為 `Active`，而目的地網域會變為可供查詢。
   - 網域頁面會顯示目的地網域的整體網域運作狀態和執行個體運作狀態詳細資訊。只有網域擁有者才能靈活建立、檢視、移除和監控與其網域的連線。

建立連線後，在已連線網域節點之間流動的任何流量都會經過加密。如果您將 VPC 網域連接至非 VPC 網域，且該非 VPC 網域是可從網際網路接收流量的公有端點，網域之間的跨叢集流量仍為加密且安全的狀態。

移除連線

移除連線會停止其索引上的任何跨叢集作業。

1. 在網域儀表板上，前往 Connections (連線) 索引標籤。
2. 選取您要移除的網域連線並選擇 Delete (刪除)，然後確認刪除。

您可以在來源或目的地網域上執行這些步驟，以移除連線。移除連線後，在 15 天內仍可見，狀態為 `Deleted`。

您無法刪除具有作用中跨叢集連線的網域。若要刪除網域，請先從該網域中移除所有傳入和傳出連線。這可確保您在刪除網域前，將跨叢集網域使用者納入考量。

設定安全性和範例演練

1. 您會將跨叢集搜尋請求傳送至來源網域。
2. 來源網域會根據其網域存取政策評估請求。由於跨叢集搜尋需要精細存取控制，建議您在來源網域上使用開放式存取政策。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "*"
        ]
      },
      "Action": [
        "es:ESHttp*"
      ],
      "Resource": "arn:aws:es:region:account:domain/src-domain/*"
    }
  ]
}
```

> **Note**
>
> 如果您在路徑中包含遠端索引，則必須對網域 ARN 中的 URI 進行 URL 編碼。例如，使用 `arn:aws:es:us-east-1:123456789012:domain/my-domain/local_index,dst%3Aremote_index` 而非 `arn:aws:es:us-east-1:123456789012:domain/my-domain/local_index,dst:remote_index`。

除了精細存取控制以外，如果您還選擇使用限制性存取政策，政策則必須至少允許對 `es:ESHttpGet` 的存取權。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
```

```
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "arn:aws:iam::123456789012:user/test-user"
        ]
      },
      "Action": "es:ESHttpGet",
      "Resource": "arn:aws:es:region:account:domain/src-domain/*"
    }
  ]
}
```

3. 來源網域上的精細存取控制會評估請求：

   - 請求是否以有效的 IAM 或 HTTP 基本登入資料簽署？
   - 如果是這樣，使用者是否具備執行搜尋和存取資料的許可？

   如果請求只搜尋目的地網域上的資料 (例如 `dest-alias:dest-index/_search`)，您只需要目的地網域上的許可。

   如果請求同時搜尋兩個網域上的資料 (例如 `source-index,dest-alias:dest-index/_search`)，您需要兩個網域上的許可。

   在細微的存取控制中，除了相關索引的`indices:admin/shards/search_shards`標準`read`或`search`權限之外，使用者還必須擁有權限。

4. 來源網域會將請求傳遞至目的地網域。目的地網域會根據其網域存取政策評估此請求。您必須在目的地網域上包含 `es:ESCrossClusterGet` 許可：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "*"
      },
      "Action": "es:ESCrossClusterGet",
      "Resource": "arn:aws:es:region:account:domain/dst-domain"
    }
  ]
}
```

確認已針對 `/dst-domain` (而不是 `/dst-domain/*`) 套用 `es:ESCrossClusterGet` 許可。

不過，此最低政策只允許跨叢集搜尋。若執行其他操作 (例如為文件編製索引和執行標準搜尋)，則需要額外的許可。建議在目的地網域上使用下列政策：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "*"
        ]
      },
      "Action": [
        "es:ESHttp*"
      ],
      "Resource": "arn:aws:es:region:account:domain/dst-domain/*"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "*"
      },
      "Action": "es:ESCrossClusterGet",
      "Resource": "arn:aws:es:region:account:domain/dst-domain"
    }
  ]
}
```

> **Note**
>
> 依預設，網域之間的所有跨叢集搜尋要求都會在傳輸中加密，做為 node-to-node 加密的一部分。

5. 目的地網域會執行搜尋並將結果傳回至來源網域。
6. 來源網域會將其自身結果 (如果有的話) 與來自目的地網域的結果加以結合，然後將其傳回給您。
7. 建議針對測試請求使用 Postman：

- 在目的地網域上，為文件編製索引：

```
POST https://dst-domain.us-east-1.es.amazonaws.com/books/_doc/1

{
  "Dracula": "Bram Stoker"
}
```

- 若要從來源網域查詢此索引，請在查詢內包含目的地網域的連線別名。

```
GET https://src-domain.us-east-1.es.amazonaws.com/<connection_alias>:books/
_search

{
    ...
  "hits": [
    {
      "_index": "source-destination:books",
      "_type": "_doc",
      "_id": "1",
      "_score": 1,
      "_source": {
        "Dracula": "Bram Stoker"
      }
    }
  ]
}
```

您可以在網域儀表板的 Connections (連線) 索引標籤上找到連線別名。

- 如果在具有連線別名 `cluster_b` 的 `domain-a -> domain-b` 與具有連線別名 `cluster_c` 的 `domain-a -> domain-c` 之間設定連線，請搜尋 `domain-a`、`domain-b` 和 `domain-c`，如下所示：

```
GET https://src-domain.us-east-1.es.amazonaws.com/
local_index,cluster_b:b_index,cluster_c:c_index/_search
{
  "query": {
    "match": {
      "user": "domino"
    }
  }
```

```
}
```

回應

```
{
  "took": 150,
  "timed_out": false,
  "_shards": {
    "total": 3,
    "successful": 3,
    "failed": 0,
    "skipped": 0
  },
  "_clusters": {
    "total": 3,
    "successful": 3,
    "skipped": 0
  },
  "hits": {
    "total": 3,
    "max_score": 1,
    "hits": [
      {
        "_index": "local_index",
        "_type": "_doc",
        "_id": "0",
        "_score": 1,
        "_source": {
          "user": "domino",
          "message": "Lets unite the new mutants",
          "likes": 0
        }
      },
      {
        "_index": "cluster_b:b_index",
        "_type": "_doc",
        "_id": "0",
        "_score": 2,
        "_source": {
          "user": "domino",
          "message": "I'm different",
          "likes": 0
        }
```

```
      },
      {
        "_index": "cluster_c:c_index",
        "_type": "_doc",
        "_id": "0",
        "_score": 3,
        "_source": {
          "user": "domino",
          "message": "So am I",
          "likes": 0
        }
      }
    ]
  }
}
```

如果您未選擇略過連線設定中無法使用的叢集，您搜尋的所有目的地叢集都必須可供搜尋要求使用，才能順利執行。否則，整個請求會失敗，即使其中一個網域無法使用，也不會傳回任何搜尋結果。

OpenSearch 儀表板

您可以透過與從單一網域相同的方式，從多個連線網域視覺化資料，但您必須使用 `connection-alias:index` 存取遠端索引時除外。因此，索引模式必須符合 `connection-alias:index`。

學習排名 Amazon OpenSearch 服務

OpenSearch 使用稱為 BM-25 的概率排名框架來計算相關性分數。如果特殊關鍵字更頻繁地出現在文件中，BM-25 會為該文件指派較高的相關性分數。然而，此架構並不考慮像點選資料這樣的使用者行為，這樣可以進一步改善相關性。

Learning to Rank 是一個開放原始碼外掛程式，可讓您使用機器學習和行為資料來調整文件的相關性。其會使用 XGBoost 和 Ranklib 程式庫中的模型來重新評分搜尋結果。Elasticsearch LTR 插件最初是由OpenSource 連接開發的，由維基媒體基金會，斯納加工程，盆景和 Yelp 工程有重大貢獻。該插件的 OpenSearch 版本來自 Elasticsearch LTR 插件。

學習排名需要 OpenSearch 或彈性搜索 7.7 或更高版本。若要使用 Learning to Rank 外掛程式，您必須擁有完整的管理員許可。如需進一步了解，請參閱the section called “修改主要使用者”。

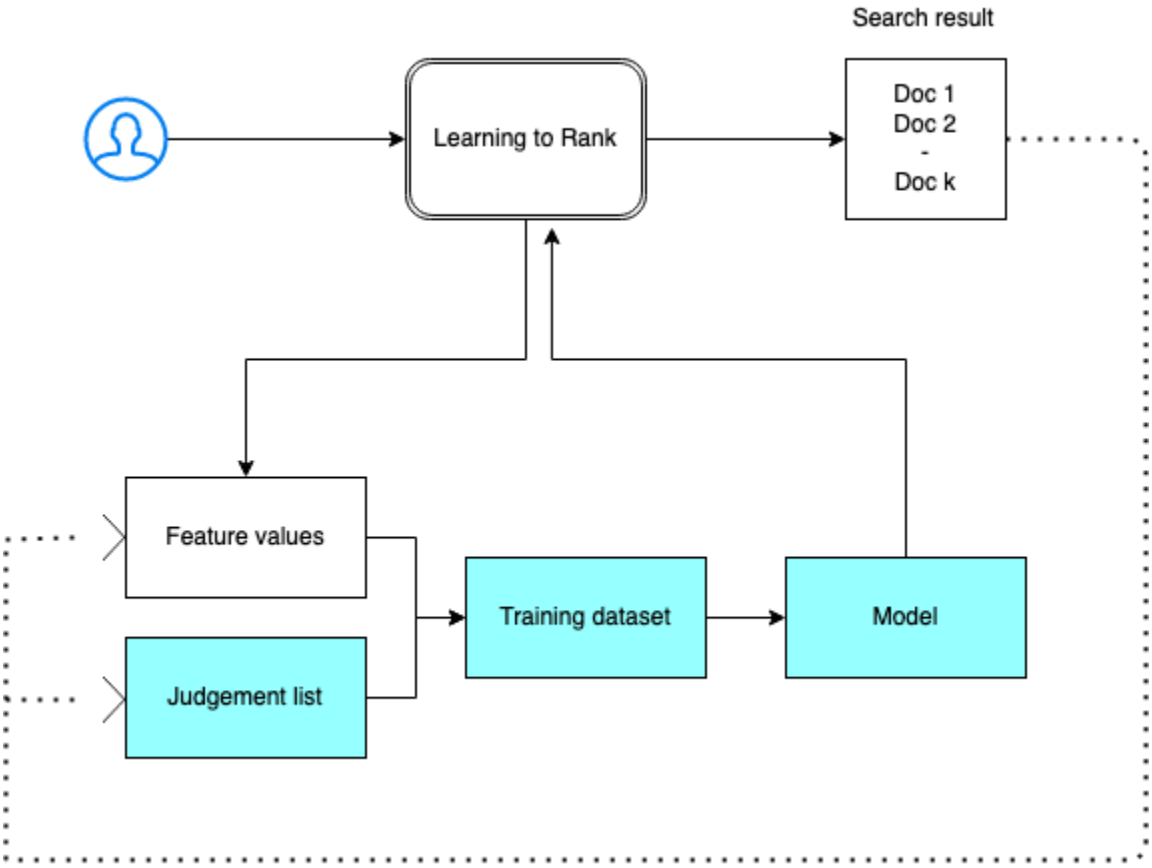
> **Note**
>
> 本文件提供學習排名外掛程式的一般概觀，並協助您開始使用它。如需完整文件，包括詳細步驟和 API 說明，請參閱 Learning to Rank 文件。

主題

- Learning to Rank 入門
- Learning to Rank API

Learning to Rank 入門

您需要提供判斷清單、準備訓練資料集，以及在 Amazon Ser OpenSearch vice 之外訓練模型。以藍色顯示的零件出現在 OpenSearch 服務範圍外：



步驟 1：初始化外掛程式

若要初始化學習排名外掛程式，請將下列要求傳送至您的 OpenSearch 服務網域：

```
PUT _ltr
```

```
{
  "acknowledged" : true,
  "shards_acknowledged" : true,
  "index" : ".ltrstore"
}
```

此命令會建立一個隱藏的 `.ltrstore` 索引，它會存放中繼資料資訊，例如功能集和模型。

步驟 2：建立判斷清單

> **Note**
>
> 您必須在「 OpenSearch 服務」之外執行此步驟。

判斷清單是機器學習模型從中學習的範例集合。您的判斷清單應包含對您很重要的關鍵字，以及每個關鍵字的一組分級文件。

在此例中，我們有一個影片資料集的判斷清單。等級 4 表示完美匹配。等級 0 表示最差匹配。

等級	關鍵字	文件 ID	影片名稱
4	rambo	7555	Rambo
3	rambo	1370	Rambo III
3	rambo	1369	Rambo: First Blood Part II
3	rambo	1368	First Blood

請按下列格式準備判斷清單：

```
4 qid:1 # 7555 Rambo
3 qid:1 # 1370 Rambo III
3 qid:1 # 1369 Rambo: First Blood Part II
```

```
3 qid:1 # 1368 First Blood

where qid:1 represents "rambo"
```

如需判斷清單的更完整範例，請參閱影片判斷。

您可以在人類註釋器的幫助下手動建立此判斷清單，或者從分析資料中以程式設計方式推斷它。

步驟 3：建置功能集

功能是對應於文件相關性的欄位，例如 `title`、`overview`、`popularity score` (視圖數) 等等。

使用每個功能的 Mustache 範本建置一個功能集。如需有關功能的詳細資訊，請參閱使用功能。

在此範例中，我們使用 `title` 和 `overview` 欄位來建置 `movie_features` 功能集：

```
POST _ltr/_featureset/movie_features
{
  "featureset" : {
      "name" : "movie_features",
      "features" : [
        {
          "name" : "1",
          "params" : [
            "keywords"
          ],
          "template_language" : "mustache",
          "template" : {
            "match" : {
              "title" : "{{keywords}}"
            }
          }
        },
        {
          "name" : "2",
          "params" : [
            "keywords"
          ],
          "template_language" : "mustache",
          "template" : {
            "match" : {
              "overview" : "{{keywords}}"
            }
```

```
          }
        }
      ]
    }
}
```

如果您查詢原始 `.ltrstore` 索引，可以返回您的功能集：

```
GET _ltr/_featureset
```

步驟 4：記錄功能值

功能值是 BM-25 針對每個功能計算的相關性分數。

結合功能集和判斷清單來記錄功能值。如需有關記錄功能的詳細資訊，請參閱記錄功能分數。

在此範例中，`bool` 查詢會使用篩選器來擷取已分級的文件，然後使用 `sltr` 查詢選取功能集。`ltr_log` 查詢結合文件和功能來記錄相應的功能值：

```
POST tmdb/_search
{
  "_source": {
    "includes": [
      "title",
      "overview"
    ]
  },
  "query": {
    "bool": {
      "filter": [
        {
          "terms": {
            "_id": [
              "7555",
              "1370",
              "1369",
              "1368"
            ]
          }
        },
        {
          "sltr": {
```

```
            "_name": "logged_featureset",
            "featureset": "movie_features",
            "params": {
              "keywords": "rambo"
            }
          }
        }
      ]
    }
  },
  "ext": {
    "ltr_log": {
      "log_specs": {
        "name": "log_entry1",
        "named_query": "logged_featureset"
      }
    }
  }
}
```

範例回應看起來類似如下：

```
{
  "took" : 7,
  "timed_out" : false,
  "_shards" : {
    "total" : 1,
    "successful" : 1,
    "skipped" : 0,
    "failed" : 0
  },
  "hits" : {
    "total" : {
      "value" : 4,
      "relation" : "eq"
    },
    "max_score" : 0.0,
    "hits" : [
      {
        "_index" : "tmdb",
        "_type" : "movie",
        "_id" : "1368",
        "_score" : 0.0,
```

```
        "_source" : {
          "overview" : "When former Green Beret John Rambo is harassed by local law
enforcement and arrested for vagrancy, the Vietnam vet snaps, runs for the hills and
rat-a-tat-tats his way into the action-movie hall of fame. Hounded by a relentless
sheriff, Rambo employs heavy-handed guerilla tactics to shake the cops off his tail.",
          "title" : "First Blood"
        },
        "fields" : {
          "_ltrlog" : [
            {
              "log_entry1" : [
                {
                  "name" : "1"
                },
                {
                  "name" : "2",
                  "value" : 10.558305
                }
              ]
            }
          ]
        },
        "matched_queries" : [
          "logged_featureset"
        ]
      },
      {
        "_index" : "tmdb",
        "_type" : "movie",
        "_id" : "7555",
        "_score" : 0.0,
        "_source" : {
          "overview" : "When governments fail to act on behalf of captive missionaries,
ex-Green Beret John James Rambo sets aside his peaceful existence along the Salween
River in a war-torn region of Thailand to take action.  Although he's still haunted
by violent memories of his time as a U.S. soldier during the Vietnam War, Rambo can
hardly turn his back on the aid workers who so desperately need his help.",
          "title" : "Rambo"
        },
        "fields" : {
          "_ltrlog" : [
            {
              "log_entry1" : [
                {
```

```
                "name" : "1",
                "value" : 11.2569065
              },
              {
                "name" : "2",
                "value" : 9.936821
              }
            ]
          }
        ]
      },
      "matched_queries" : [
        "logged_featureset"
      ]
    },
    {
      "_index" : "tmdb",
      "_type" : "movie",
      "_id" : "1369",
      "_score" : 0.0,
      "_source" : {
        "overview" : "Col. Troutman recruits ex-Green Beret John Rambo for a highly
secret and dangerous mission. Teamed with Co Bao, Rambo goes deep into Vietnam to
rescue POWs. Deserted by his own team, he's left in a hostile jungle to fight for his
life, avenge the death of a woman and bring corrupt officials to justice.",
        "title" : "Rambo: First Blood Part II"
      },
      "fields" : {
        "_ltrlog" : [
          {
            "log_entry1" : [
              {
                "name" : "1",
                "value" : 6.334839
              },
              {
                "name" : "2",
                "value" : 10.558305
              }
            ]
          }
        ]
      },
      "matched_queries" : [
```

```
          "logged_featureset"
        ]
      },
      {
        "_index" : "tmdb",
        "_type" : "movie",
        "_id" : "1370",
        "_score" : 0.0,
        "_source" : {
          "overview" : "Combat has taken its toll on Rambo, but he's finally begun to
 find inner peace in a monastery. When Rambo's friend and mentor Col. Trautman asks for
 his help on a top secret mission to Afghanistan, Rambo declines but must reconsider
 when Trautman is captured.",
          "title" : "Rambo III"
        },
        "fields" : {
          "_ltrlog" : [
            {
              "log_entry1" : [
                {
                  "name" : "1",
                  "value" : 9.425955
                },
                {
                  "name" : "2",
                  "value" : 11.262714
                }
              ]
            }
          ]
        },
        "matched_queries" : [
          "logged_featureset"
        ]
      }
    ]
  }
}
```

在上一個範例中，第一個功能沒有功能值，因為關鍵字「rambo」不會出現在 ID 等於 1368 的文件的標題欄位中。這是訓練資料中缺少的功能值。

步驟 5：建立訓練資料集

> **Note**
> 您必須在「 OpenSearch 服務」之外執行此步驟。

下一步是結合判斷清單和功能值來建立訓練資料集。如果您的原始判斷清單如下所示：

```
4 qid:1 # 7555 Rambo
3 qid:1 # 1370 Rambo III
3 qid:1 # 1369 Rambo: First Blood Part II
3 qid:1 # 1368 First Blood
```

將它轉換為最終訓練資料集，如下所示：

```
4 qid:1 1:12.318474 2:10.573917 # 7555 rambo
3 qid:1 1:10.357875 2:11.950391 # 1370 rambo
3 qid:1 1:7.010513 2:11.220095 # 1369 rambo
3 qid:1 1:0.0 2:11.220095 # 1368 rambo
```

您可以手動執行此步驟或編寫程式來自動執行此步驟。

第 6 步：選擇一個演算法並建置模型

> **Note**
> 您必須在「 OpenSearch 服務」之外執行此步驟。

訓練資料集到位之後，下一步是使用 XGBoost 或 Ranklib 程式庫來建置一個模型。使用 XGBoost 和 Ranklib 程式庫可建置熱門模型，例如 LambdaMART、Random Forests 等。

有關使用 XGBoost 和蘭克利卜來構建模型的步驟，請分別參閱 XG Boost 和文檔。RankLib若要使用 Amazon 建立 XGBoost 模型，請參閱 X GBoost 演 SageMaker 算法。

步驟 7：部署模型

建置模型之後，請將其部署到 Learning to Rank 外掛程式中。如需有關部署模型的詳細資訊，請參閱上傳訓練模型。

在此範例中，我們使用 Ranklib 程式庫建置 `my_ranklib_model` 模型：

```
POST _ltr/_featureset/movie_features/_createmodel?pretty
{
  "model": {
    "name": "my_ranklib_model",
    "model": {
      "type": "model/ranklib",
      "definition": """## LambdaMART
## No. of trees = 10
## No. of leaves = 10
## No. of threshold candidates = 256
## Learning rate = 0.1
## Stop early = 100

<ensemble>
   <tree id="1" weight="0.1">
      <split>
         <feature>1</feature>
         <threshold>10.357875</threshold>
         <split pos="left">
            <feature>1</feature>
            <threshold>0.0</threshold>
            <split pos="left">
               <output>-2.0</output>
            </split>
            <split pos="right">
               <feature>1</feature>
               <threshold>7.010513</threshold>
               <split pos="left">
                  <output>-2.0</output>
               </split>
               <split pos="right">
                  <output>-2.0</output>
               </split>
            </split>
         </split>
         <split pos="right">
            <output>2.0</output>
         </split>
      </split>
   </tree>
   <tree id="2" weight="0.1">
      <split>
```

```
         <feature>1</feature>
         <threshold>10.357875</threshold>
         <split pos="left">
            <feature>1</feature>
            <threshold>0.0</threshold>
            <split pos="left">
               <output>-1.67031991481781</output>
            </split>
            <split pos="right">
               <feature>1</feature>
               <threshold>7.010513</threshold>
               <split pos="left">
                  <output>-1.67031991481781</output>
               </split>
               <split pos="right">
                  <output>-1.6703200340270996</output>
               </split>
            </split>
         </split>
         <split pos="right">
            <output>1.6703201532363892</output>
         </split>
      </split>
   </tree>
   <tree id="3" weight="0.1">
      <split>
         <feature>2</feature>
         <threshold>10.573917</threshold>
         <split pos="left">
            <output>1.479954481124878</output>
         </split>
         <split pos="right">
            <feature>1</feature>
            <threshold>7.010513</threshold>
            <split pos="left">
               <feature>1</feature>
               <threshold>0.0</threshold>
               <split pos="left">
                  <output>-1.4799546003341675</output>
               </split>
               <split pos="right">
                  <output>-1.479954481124878</output>
               </split>
            </split>
```

```
            <split pos="right">
               <output>-1.479954481124878</output>
            </split>
         </split>
      </split>
   </tree>
   <tree id="4" weight="0.1">
      <split>
         <feature>1</feature>
         <threshold>10.357875</threshold>
         <split pos="left">
            <feature>1</feature>
            <threshold>0.0</threshold>
            <split pos="left">
               <output>-1.3569872379302979</output>
            </split>
            <split pos="right">
               <feature>1</feature>
               <threshold>7.010513</threshold>
               <split pos="left">
                  <output>-1.3569872379302979</output>
               </split>
               <split pos="right">
                  <output>-1.3569872379302979</output>
               </split>
            </split>
         </split>
         <split pos="right">
            <output>1.3569873571395874</output>
         </split>
      </split>
   </tree>
   <tree id="5" weight="0.1">
      <split>
         <feature>1</feature>
         <threshold>10.357875</threshold>
         <split pos="left">
            <feature>1</feature>
            <threshold>0.0</threshold>
            <split pos="left">
               <output>-1.2721362113952637</output>
            </split>
            <split pos="right">
               <feature>1</feature>
```

```
                <threshold>7.010513</threshold>
                <split pos="left">
                   <output>-1.2721363306045532</output>
                </split>
                <split pos="right">
                   <output>-1.2721363306045532</output>
                </split>
             </split>
          </split>
          <split pos="right">
             <output>1.2721362113952637</output>
          </split>
       </split>
    </tree>
    <tree id="6" weight="0.1">
       <split>
          <feature>1</feature>
          <threshold>10.357875</threshold>
          <split pos="left">
             <feature>1</feature>
             <threshold>7.010513</threshold>
             <split pos="left">
                <feature>1</feature>
                <threshold>0.0</threshold>
                <split pos="left">
                   <output>-1.2110036611557007</output>
                </split>
                <split pos="right">
                   <output>-1.2110036611557007</output>
                </split>
             </split>
             <split pos="right">
                <output>-1.2110037803649902</output>
             </split>
          </split>
          <split pos="right">
             <output>1.2110037803649902</output>
          </split>
       </split>
    </tree>
    <tree id="7" weight="0.1">
       <split>
          <feature>1</feature>
          <threshold>10.357875</threshold>
```

```
         <split pos="left">
            <feature>1</feature>
            <threshold>7.010513</threshold>
            <split pos="left">
               <feature>1</feature>
               <threshold>0.0</threshold>
               <split pos="left">
                  <output>-1.165616512298584</output>
               </split>
               <split pos="right">
                  <output>-1.165616512298584</output>
               </split>
            </split>
            <split pos="right">
               <output>-1.165616512298584</output>
            </split>
         </split>
         <split pos="right">
            <output>1.165616512298584</output>
         </split>
      </split>
   </tree>
   <tree id="8" weight="0.1">
      <split>
         <feature>1</feature>
         <threshold>10.357875</threshold>
         <split pos="left">
            <feature>1</feature>
            <threshold>7.010513</threshold>
            <split pos="left">
               <feature>1</feature>
               <threshold>0.0</threshold>
               <split pos="left">
                  <output>-1.131177544593811</output>
               </split>
               <split pos="right">
                  <output>-1.131177544593811</output>
               </split>
            </split>
            <split pos="right">
               <output>-1.131177544593811</output>
            </split>
         </split>
         <split pos="right">
```

```
            <output>1.131177544593811</output>
         </split>
      </split>
   </tree>
   <tree id="9" weight="0.1">
      <split>
         <feature>2</feature>
         <threshold>10.573917</threshold>
         <split pos="left">
            <output>1.1046180725097656</output>
         </split>
         <split pos="right">
            <feature>1</feature>
            <threshold>7.010513</threshold>
            <split pos="left">
               <feature>1</feature>
               <threshold>0.0</threshold>
               <split pos="left">
                  <output>-1.1046180725097656</output>
               </split>
               <split pos="right">
                  <output>-1.1046180725097656</output>
               </split>
            </split>
            <split pos="right">
               <output>-1.1046180725097656</output>
            </split>
         </split>
      </split>
   </tree>
   <tree id="10" weight="0.1">
      <split>
         <feature>1</feature>
         <threshold>10.357875</threshold>
         <split pos="left">
            <feature>1</feature>
            <threshold>7.010513</threshold>
            <split pos="left">
               <feature>1</feature>
               <threshold>0.0</threshold>
               <split pos="left">
                  <output>-1.0838804244995117</output>
               </split>
               <split pos="right">
```

```
                  <output>-1.0838804244995117</output>
               </split>
            </split>
            <split pos="right">
               <output>-1.0838804244995117</output>
            </split>
         </split>
         <split pos="right">
            <output>1.0838804244995117</output>
         </split>
      </split>
   </tree>
</ensemble>
"""
    }
  }
}
```

若要查看模型，請傳送下列請求：

```
GET _ltr/_model/my_ranklib_model
```

步驟 8：使用 Learning to Rank 進行搜尋

部署模型之後，您準備好進行搜尋。

透過您正在使用的功能和您想要執行的模型名稱來執行 `sltr` 查詢：

```
POST tmdb/_search
{
  "_source": {
    "includes": ["title", "overview"]
  },
  "query": {
    "multi_match": {
      "query": "rambo",
      "fields": ["title", "overview"]
    }
  },
  "rescore": {
    "query": {
      "rescore_query": {
        "sltr": {
```

```
          "params": {
            "keywords": "rambo"
          },
          "model": "my_ranklib_model"
        }
      }
    }
  }
}
```

透過 Learning to Rank，您會看到「Rambo」作為第一個結果，因為我們已將其分配在判斷清單中的最高等級：

```
{
  "took" : 12,
  "timed_out" : false,
  "_shards" : {
    "total" : 1,
    "successful" : 1,
    "skipped" : 0,
    "failed" : 0
  },
  "hits" : {
    "total" : {
      "value" : 7,
      "relation" : "eq"
    },
    "max_score" : 13.096414,
    "hits" : [
      {
        "_index" : "tmdb",
        "_type" : "movie",
        "_id" : "7555",
        "_score" : 13.096414,
        "_source" : {
          "overview" : "When governments fail to act on behalf of captive missionaries,
 ex-Green Beret John James Rambo sets aside his peaceful existence along the Salween
 River in a war-torn region of Thailand to take action.  Although he's still haunted
 by violent memories of his time as a U.S. soldier during the Vietnam War, Rambo can
 hardly turn his back on the aid workers who so desperately need his help.",
          "title" : "Rambo"
        }
      },
```

```
      {
        "_index" : "tmdb",
        "_type" : "movie",
        "_id" : "1370",
        "_score" : 11.17245,
        "_source" : {
          "overview" : "Combat has taken its toll on Rambo, but he's finally begun to
find inner peace in a monastery. When Rambo's friend and mentor Col. Trautman asks for
his help on a top secret mission to Afghanistan, Rambo declines but must reconsider
when Trautman is captured.",
          "title" : "Rambo III"
        }
      },
      {
        "_index" : "tmdb",
        "_type" : "movie",
        "_id" : "1368",
        "_score" : 10.442155,
        "_source" : {
          "overview" : "When former Green Beret John Rambo is harassed by local law
enforcement and arrested for vagrancy, the Vietnam vet snaps, runs for the hills and
rat-a-tat-tats his way into the action-movie hall of fame. Hounded by a relentless
sheriff, Rambo employs heavy-handed guerilla tactics to shake the cops off his tail.",
          "title" : "First Blood"
        }
      },
      {
        "_index" : "tmdb",
        "_type" : "movie",
        "_id" : "1369",
        "_score" : 10.442155,
        "_source" : {
          "overview" : "Col. Troutman recruits ex-Green Beret John Rambo for a highly
secret and dangerous mission. Teamed with Co Bao, Rambo goes deep into Vietnam to
rescue POWs. Deserted by his own team, he's left in a hostile jungle to fight for his
life, avenge the death of a woman and bring corrupt officials to justice.",
          "title" : "Rambo: First Blood Part II"
        }
      },
      {
        "_index" : "tmdb",
        "_type" : "movie",
        "_id" : "31362",
        "_score" : 7.424202,
```

```
        "_source" : {
          "overview" : "It is 1985, and a small, tranquil Florida town is being rocked
by a wave of vicious serial murders and bank robberies. Particularly sickening to the
authorities is the gratuitous use of violence by two “Rambo” like killers who dress
themselves in military garb. Based on actual events taken from FBI files, the movie
depicts the Bureau’s efforts to track down these renegades.",
          "title" : "In the Line of Duty: The F.B.I. Murders"
        }
      },
      {
        "_index" : "tmdb",
        "_type" : "movie",
        "_id" : "13258",
        "_score" : 6.43182,
        "_source" : {
          "overview" : """Will Proudfoot (Bill Milner) is looking for an escape from
his family's stifling home life when he encounters Lee Carter (Will Poulter), the
school bully. Armed with a video camera and a copy of "Rambo: First Blood", Lee plans
to make cinematic history by filming his own action-packed video epic. Together, these
two newfound friends-turned-budding-filmmakers quickly discover that their imaginative
— and sometimes mishap-filled — cinematic adventure has begun to take on a life of its
own!""",
          "title" : "Son of Rambow"
        }
      },
      {
        "_index" : "tmdb",
        "_type" : "movie",
        "_id" : "61410",
        "_score" : 3.9719706,
        "_source" : {
          "overview" : "It's South Africa 1990. Two major events are about to happen:
The release of Nelson Mandela and, more importantly, it's Spud Milton's first year
at an elite boys only private boarding school. John Milton is a boy from an ordinary
background who wins a scholarship to a private school in Kwazulu-Natal, South Africa.
Surrounded by boys with nicknames like Gecko, Rambo, Rain Man and Mad Dog, Spud has
his hands full trying to adapt to his new home. Along the way Spud takes his first
tentative steps along the path to manhood. (The path it seems could be a rather long
road). Spud is an only child. He is cursed with parents from well beyond the lunatic
fringe and a senile granny. His dad is a fervent anti-communist who is paranoid that
the family domestic worker is running a shebeen from her room at the back of the
family home. His mom is a free spirit and a teenager's worst nightmare, whether it's
shopping for Spud's underwear in the local supermarket",
          "title" : "Spud"
```

```
        }
      }
    ]
  }
}
```

如果您不使用「學習排名」外掛程式進行搜尋，則會 OpenSearch 傳回不同的結果：

```
POST tmdb/_search
{
  "_source": {
    "includes": ["title", "overview"]
  },
  "query": {
    "multi_match": {
      "query": "Rambo",
      "fields": ["title", "overview"]
    }
  }
}
```

```
{
  "took" : 5,
  "timed_out" : false,
  "_shards" : {
    "total" : 1,
    "successful" : 1,
    "skipped" : 0,
    "failed" : 0
  },
  "hits" : {
    "total" : {
      "value" : 5,
      "relation" : "eq"
    },
    "max_score" : 11.262714,
    "hits" : [
      {
        "_index" : "tmdb",
        "_type" : "movie",
        "_id" : "1370",
        "_score" : 11.262714,
        "_source" : {
```

```
        "overview" : "Combat has taken its toll on Rambo, but he's finally begun to
find inner peace in a monastery. When Rambo's friend and mentor Col. Trautman asks for
his help on a top secret mission to Afghanistan, Rambo declines but must reconsider
when Trautman is captured.",
        "title" : "Rambo III"
      }
    },
    {
      "_index" : "tmdb",
      "_type" : "movie",
      "_id" : "7555",
      "_score" : 11.2569065,
      "_source" : {
        "overview" : "When governments fail to act on behalf of captive missionaries,
ex-Green Beret John James Rambo sets aside his peaceful existence along the Salween
River in a war-torn region of Thailand to take action.  Although he's still haunted
by violent memories of his time as a U.S. soldier during the Vietnam War, Rambo can
hardly turn his back on the aid workers who so desperately need his help.",
        "title" : "Rambo"
      }
    },
    {
      "_index" : "tmdb",
      "_type" : "movie",
      "_id" : "1368",
      "_score" : 10.558305,
      "_source" : {
        "overview" : "When former Green Beret John Rambo is harassed by local law
enforcement and arrested for vagrancy, the Vietnam vet snaps, runs for the hills and
rat-a-tat-tats his way into the action-movie hall of fame. Hounded by a relentless
sheriff, Rambo employs heavy-handed guerilla tactics to shake the cops off his tail.",
        "title" : "First Blood"
      }
    },
    {
      "_index" : "tmdb",
      "_type" : "movie",
      "_id" : "1369",
      "_score" : 10.558305,
      "_source" : {
        "overview" : "Col. Troutman recruits ex-Green Beret John Rambo for a highly
secret and dangerous mission. Teamed with Co Bao, Rambo goes deep into Vietnam to
rescue POWs. Deserted by his own team, he's left in a hostile jungle to fight for his
life, avenge the death of a woman and bring corrupt officials to justice.",
```

```
          "title" : "Rambo: First Blood Part II"
        }
      },
      {
        "_index" : "tmdb",
        "_type" : "movie",
        "_id" : "13258",
        "_score" : 6.4600153,
        "_source" : {
          "overview" : """Will Proudfoot (Bill Milner) is looking for an escape from
 his family's stifling home life when he encounters Lee Carter (Will Poulter), the
 school bully. Armed with a video camera and a copy of "Rambo: First Blood", Lee plans
 to make cinematic history by filming his own action-packed video epic. Together, these
 two newfound friends-turned-budding-filmmakers quickly discover that their imaginative
 – and sometimes mishap-filled – cinematic adventure has begun to take on a life of its
 own!""",
          "title" : "Son of Rambow"
        }
      }
    ]
  }
}
```

根據您認為的模型執行情況，調整判斷清單和功能。然後，重複步驟 2 - 8，以隨著時間改善排名結果。

Learning to Rank API

使用 Learning to Rank 操作，以程式設計方式處理功能集和模型。

建立商店

建立一個隱藏的 `.ltrstore` 索引，它會存放中繼資料資訊，例如功能集和模型。

```
PUT _ltr
```

刪除商店

刪除隱藏的 `.ltrstore` 索引並重置外掛程式。

```
DELETE _ltr
```

建立功能集

建立功能集。

```
POST _ltr/_featureset/<name_of_features>
```

刪除功能集

刪除功能集。

```
DELETE _ltr/_featureset/<name_of_feature_set>
```

取得功能集

擷取功能集。

```
GET _ltr/_featureset/<name_of_feature_set>
```

建立模型

建立模型。

```
POST _ltr/_featureset/<name_of_feature_set>/_createmodel
```

刪除模型

刪除模型。

```
DELETE _ltr/_model/<name_of_model>
```

取得模型

擷取模型。

```
GET _ltr/_model/<name_of_model>
```

取得統計資料

提供外掛程式如何運作的相關資訊。

```
GET _ltr/_stats
```

您還可以使用過濾器來檢索單個統計信息：

```
GET _ltr/_stats/<stat>
```

此外，您可以將資訊限制在叢集中的單一節點：

```
GET _ltr/_stats/<stat>/nodes/<nodeId>

{
  "_nodes" : {
    "total" : 1,
    "successful" : 1,
    "failed" : 0
  },
  "cluster_name" : "873043598401:ltr-77",
  "stores" : {
    ".ltrstore" : {
      "model_count" : 1,
      "featureset_count" : 1,
      "feature_count" : 2,
      "status" : "green"
    }
  },
  "status" : "green",
  "nodes" : {
    "DjelK-_ZSfyzstO5dhGGQA" : {
      "cache" : {
        "feature" : {
          "eviction_count" : 0,
          "miss_count" : 0,
          "entry_count" : 0,
          "memory_usage_in_bytes" : 0,
          "hit_count" : 0
        },
        "featureset" : {
          "eviction_count" : 2,
          "miss_count" : 2,
          "entry_count" : 0,
          "memory_usage_in_bytes" : 0,
          "hit_count" : 0
```

```
        },
        "model" : {
          "eviction_count" : 2,
          "miss_count" : 3,
          "entry_count" : 1,
          "memory_usage_in_bytes" : 3204,
          "hit_count" : 1
        }
      },
      "request_total_count" : 6,
      "request_error_count" : 0
    }
  }
}
```

在兩個層級 (節點和叢集) 提供統計資料，如下表所指定：

節點級統計資料

欄位名稱	描述
request_total_count	排名請求的總數。
request_error_count	未成功請求的總數。
快取	所有快取 (功能、功能集、模型) 的統計資料。當使用者查詢外掛程式且模型已載入記憶體時，就會發生快取命中。
cache.eviction_count	快取移出次數。
cache.hit_count	快取命中次數。
cache.miss_count	快取遺漏次數。當使用者查詢外掛程式並且模型尚未載入到記憶體時，會發生快取遺漏。
cache.entry_count	快取中的項目數。
cache.memory_usage_in_bytes	使用的總記憶體 (以位元組為單位)。
cache.cache_capacity_reached	指示是否已達到快取限制。

叢集層級統計資料

欄位名稱	描述
存放	指出存放功能集和模型中繼資料的位置。(預設值是「.ltrstore」。否則，它的字首為「.ltrstore_」，後面為使用者提供的名稱)。
stores.status	索引狀態。
stores.feature_sets	功能集的數目。
stores.features_count	功能數目。
stores.model_count	模型數目。
status	以特徵存放區索引 (紅色、黃色或綠色) 和斷路器狀態 (開啟或關閉) 為基礎的外掛程式狀態。
cache.cache_capacity_reached	指示是否已達到快取限制。

取得快取統計資料

傳回快取和記憶體用量的相關統計資料。

```
GET _ltr/_cachestats

{
    "_nodes": {
        "total": 2,
        "successful": 2,
        "failed": 0
    },
    "cluster_name": "opensearch-cluster",
    "all": {
        "total": {
            "ram": 612,
            "count": 1
        },
        "features": {
            "ram": 0,
            "count": 0
```

```
        },
        "featuresets": {
            "ram": 612,
            "count": 1
        },
        "models": {
            "ram": 0,
            "count": 0
        }
    },
    "stores": {
        ".ltrstore": {
            "total": {
                "ram": 612,
                "count": 1
            },
            "features": {
                "ram": 0,
                "count": 0
            },
            "featuresets": {
                "ram": 612,
                "count": 1
            },
            "models": {
                "ram": 0,
                "count": 0
            }
        }
    },
    "nodes": {
        "ejF6uutERF20wOFNOXB61A": {
            "name": "opensearch1",
            "hostname": "172.18.0.4",
            "stats": {
                "total": {
                    "ram": 612,
                    "count": 1
                },
                "features": {
                    "ram": 0,
                    "count": 0
                },
                "featuresets": {
```

```
                    "ram": 612,
                    "count": 1
                },
                "models": {
                    "ram": 0,
                    "count": 0
                }
            }
        },
        "Z2RZNWRLSveVcz2c6lHf5A": {
            "name": "opensearch2",
            "hostname": "172.18.0.2",
            "stats": {
                ...
            }
        }
    }
}
```

清除快取

清除外掛程式快取。使用它來重新整理模型。

```
POST _ltr/_clearcache
```

Amazon OpenSearch 服務中的異步搜索

透過 Amazon Ser OpenSearch vice 的非同步搜尋，您可以提交在背景執行的搜尋查詢、監控請求的進度，以及在稍後階段擷取結果。在搜尋完成之前，您可以在部分結果變為可用時進行擷取。搜尋完成之後，儲存結果以供日後擷取和分析。

非同步搜尋需要 OpenSearch 1.0 或更新版本，或彈性搜尋 7.10 或更新版本。

本文件提供非同步搜尋的簡要概觀。同時也討論使用非同步搜尋搭配受管 Amazon Ser OpenSearch vice 網域而非開放原始碼 OpenSearch 叢集的限制。如需非同步搜尋的完整文件，包括可用的設定、權限和完整的 API 參考資料，請參閱 OpenSearch 文件中的非同步搜尋。

搜尋呼叫範例

若要執行非同步搜尋，請使用下列格式將 HTTP 請求傳送至 `_plugins/_asynchronous_search`：

```
POST opensearch-domain/_plugins/_asynchronous_search
```

> **Note**
>
> 如果您使用的是 Elasticsearch 7.10 而不是 OpenSearch 版本，請`_opendistro`在所有非同步搜尋要求中取代`_plugins`為。

您可以指定下列非同步搜尋選項：

選項	描述	預設值	必要
`wait_for_completion_timeout`	指定您計劃等待結果的時間量。您可以看到在這個時間內得到的任何結果與一般搜尋一樣。您可以根據 ID 來輪詢剩餘結果。最高值為 300 秒。	1 秒	否
`keep_on_completion`	指定搜尋完成後是否要將結果儲存在叢集中。您可以在稍後時間檢查儲存的結果。	`false`	否
`keep_alive`	指定在叢集中儲存結果的時間長度。例如：`2d` 表示結果在叢集中儲存 48 小時。儲存的搜尋結果會在此時段之後或取消搜尋時刪除。請注意，這包括查詢執行時間。如果此次查詢超限，處理程序會自動取消此查詢。	12 小時	否

請求範例

```
POST _plugins/_asynchronous_search/?
pretty&size=10&wait_for_completion_timeout=1ms&keep_on_completion=true&request_cache=false
{
  "aggs": {
    "city": {
      "terms": {
        "field": "city",
        "size": 10
      }
```

```
    }
  }
}
```

> **Note**
>
> 支援適用於標準 `_search` 查詢的所有請求參數。如果您使用的是彈性搜索 7.10 而不是 OpenSearch 版本，請替換為. `_plugins _opendistro`

非同步搜尋許可

非同步搜尋支援精細存取控制。如需混合和匹配許可以符合您的使用案例的詳細資訊，請參閱非同步搜尋安全性。

對於已啟用精細存取控制的網域，您需要角色的下列最低許可：

```
# Allows users to use all asynchronous search functionality
asynchronous_search_full_access:
  reserved: true
  cluster_permissions:
    - 'cluster:admin/opensearch/asynchronous-search/*'
  index_permissions:
    - index_patterns:
        - '*'
      allowed_actions:
        - 'indices:data/read/search*'

# Allows users to read stored asynchronous search results
asynchronous_search_read_access:
  reserved: true
  cluster_permissions:
    - 'cluster:admin/opensearch/asynchronous-search/get'
```

對於已停用精細存取控制的網域，請使用您的 IAM 存取權和秘密金鑰來簽署所有請求。您可以使用非同步搜尋 ID 來存取結果。

非同步搜尋設定

OpenSearch 可讓您使用 `_cluster/settings` API 變更所有可用的非同步搜尋設定。在 [OpenSearch 服務] 中，您只能變更下列設定：

- plugins.asynchronous_search.node_concurrent_running_searches
- plugins.asynchronous_search.persist_search_failures

跨叢集搜尋

您可以在具有下列次要限制的叢集間執行非同步搜尋：

- 您只能在來源網域上執行非同步搜尋。
- 您無法將網路往返次數降到最低，作為跨叢集搜尋查詢的一部分。

如果在具有連線別名 cluster_b 的 domain-a -> domain-b 與具有連線別名 cluster_c 的 domain-a -> domain-c 之間設定連線，請非同步搜尋 domain-a、domain-b 和 domain-c，如下所示：

```
POST https://src-domain.us-east-1.es.amazonaws.com/
local_index,cluster_b:b_index,cluster_c:c_index/_plugins/_asynchronous_search/?
pretty&size=10&wait_for_completion_timeout=500ms&keep_on_completion=true&request_cache=false
{
  "size": 0,
  "_source": {
    "excludes": []
  },
  "aggs": {
    "2": {
      "terms": {
        "field": "clientip",
        "size": 50,
        "order": {
          "_count": "desc"
        }
      }
    }
  },
  "stored_fields": [
    "*"
  ],
  "script_fields": {},
  "docvalue_fields": [
    "@timestamp"
  ],
```

```
  "query": {
    "bool": {
      "must": [
        {
          "query_string": {
            "query": "status:404",
            "analyze_wildcard": true,
            "default_field": "*"
          }
        },
        {
          "range": {
            "@timestamp": {
              "gte": 1483747200000,
              "lte": 1488326400000,
              "format": "epoch_millis"
            }
          }
        }
      ],
      "filter": [],
      "should": [],
      "must_not": []
    }
  }
}
```

回應

```
{
  "id" :
 "Fm9pYzJyVG91U19xb0hIQUJnMHJfRFEAAAAAAAknghQ1OWVBczNZQjVEa2dMYTBXaTdEagAAAAAAAAAB",
  "state" : "RUNNING",
  "start_time_in_millis" : 1609329314796,
  "expiration_time_in_millis" : 1609761314796
}
```

如需詳細資訊，請參閱 the section called “跨叢集搜尋”。

UltraWarm

含 UltraWarm 索引的非同步搜尋仍會繼續運作。如需詳細資訊，請參閱 the section called “UltraWarm 儲存”。

> **Note**
>
> 您可以在中監視非同步搜尋統計資料 CloudWatch。如需指標的完整清單，請參閱 the section called “非同步搜尋指標”。

在 Amazon OpenSearch 服務中的時間點搜索

時間點 (PIT) 是一種搜尋類型，可讓您針對固定時間的資料集執行不同的查詢。一般而言，當您在不同時間點對相同索引執行相同的查詢時，您會收到不同的結果，因為文件會持續編製索引、更新和刪除。使用 PIT，您可以根據資料集的固定狀態進行查詢。

PIT 搜索的主要用途是將其與`search_after`功能相結合。這是中的首選分頁方法 OpenSearch，特別是對於深度分頁，因為它在時間凍結的數據集上運行，它不綁定到查詢，並且它支持一致的分頁向前和向後。您可以將 PIT 與運行 OpenSearch 版本 2.5 的域一起使用。

> **Note**
>
> 本主題提供 PIT 的概觀，以及在受管 Amazon Ser OpenSearch vice 網域而非自我管理 OpenSearch 叢集上使用時需要考量的一些事項。有關 PIT 的完整文檔，包括全面的 API 參考，請參閱開源 OpenSearch 文檔中的時間點。

考量事項

設定 PIT 搜尋時，請考慮下列事項：

- 如果您要從執行 2.3 OpenSearch 版的網域進行升級，並且需要對 PIT 動作進行精細的存取控制，則需要手動新增這些動作和角色。
- 沒有 PIT 的復原能力。節點重新啟動、節點終止、藍/綠部署和 OpenSearch 處理序重新啟動會導致所有 PIT 資料遺失。
- 如果碎片在藍/綠部署期間重新定位，則只有即時資料區段會傳輸到新節點。PIT 持有的碎片段（獨家和與實時數據共享的碎片）保留在舊節點上。
- PIT 搜尋目前不適用於非同步搜尋。

創建一個坑

若要執行 PIT 查詢，請_search/point_in_time使用下列格式將 HTTP 要求傳送至：

```
POST opensearch-domain/my-index/_search/point_in_time?keep_alive=time
```

您可以指定下列 PIT 選項：

選項	描述	預設值	必要
keep_alive	的時間，以保持 PIT 量。每次使用搜尋要求存取 PIT 時，PIT 生命週期都會延長等於keep_alive 參數的時間量。當您建立 PIT 時，此查詢參數是必要的，但在搜尋要求中是選用的。		是
preference	字串；指定用來執行搜尋的節點或碎片。	隨機	否
routing	字串；指定將搜尋要求路由至特定碎片。	該文件的 _id	否
expand_wildcards	字串；指定可與萬用字元模式相符的索引類型。支援逗號分隔值。有效值如下： • all：匹配任何索引或數據流，包括隱藏的索引或數據流。 • open：匹配開放的，非隱藏的索引或非隱藏的數據流。 • closed：匹配封閉的，非隱藏的索引或非隱藏的數據流。 • hidden：匹配隱藏的索引或數據流。必須與開放式、封閉式或同時開啟和關閉合併使用。 • none：不接受萬用字元模式。	open	否
allow_partial_pit_creation	布林值；指定是否建立具有部分失敗之 PIT。	true	否

回應範例

```
{
    "pit_id":
 "o463QQEPbXktaW5kZXgtMDAwMDAxFnNOWU43ckt3U3IyaFVpbGE1UWEtMncAFjFyeXBsRGJmVFM2RTB6eVg1aVVqQncAA
    "_shards": {
        "total": 1,
        "successful": 1,
        "skipped": 0,
        "failed": 0
    },
    "creation_time": 1658146050064
}
```

當您建立 PIT 時，您會在回應中收到 PIT ID。這是您用來執行 PIT 搜尋的 ID。

時間點權限

PIT 支援精細的存取控制。如果您要升級到 2.5 OpenSearch 版網域，且需要精細的存取控制，則需要手動建立具有下列權限的角色：

```
# Allows users to use all point in time search search functionality
point_in_time_full_access:
  reserved: true
  index_permissions:
    - index_patterns:
        - '*'
      allowed_actions:
        - "indices:data/read/point_in_time/create"
        - "indices:data/read/point_in_time/delete"
        - "indices:data/read/point_in_time/readall"
        - "indices:data/read/search"
        - "indices:monitor/point_in_time/segments"


# Allows users to use point in time search search functionality for specific index
# All type operations like list all PITs, delete all PITs are not supported in this
 case

point_in_time_index_access:
  reserved: true
  index_permissions:
    - index_patterns:
```

```
        - 'my-index-1'
      allowed_actions:
        - "indices:data/read/point_in_time/create"
        - "indices:data/read/point_in_time/delete"
        - "indices:data/read/search"
        - "indices:monitor/point_in_time/segments"
```

對於 OpenSearch 版本 2.5 及更高版本的網域，您可以使用內建`point_in_time_full_access`角色。如需詳細資訊，請參閱 OpenSearch 文件中的安全性模型。

進地坑設置

OpenSearch 可讓您使用 `_cluster/settings` API 變更所有可用的 PIT 設定。在 [OpenSearch 服務] 中，您目前無法修改設定。

跨叢集搜尋

您可以建立 PIT、使用 PIT ID 進行搜尋、列出 PIT，以及刪除叢集間的 PIT，但有下列次要限制：

- 您只能列出來源網域上的所有 PIT 並刪除所有 PIT。
- 您無法將網路往返次數降到最低，作為跨叢集搜尋查詢的一部分。

如需詳細資訊，請參閱 the section called “跨叢集搜尋”。

UltraWarm

使用 UltraWarm 索引進行 PIT 搜尋繼續運作。如需詳細資訊，請參閱 the section called “UltraWarm 儲存”。

> **Note**
>
> 您可以在中監視 PIT 搜尋統計資料 CloudWatch。如需指標的完整清單，請參閱 the section called “時間點量度”。

在 Amazon OpenSearch 服務語義搜索

從 2.9 OpenSearch 版開始，您可以使用語義搜索來幫助您了解搜索查詢並提高搜索相關性。您可以通過兩種方式之一使用語義搜索-神經搜索和 K 最近的鄰居（K-NN）搜索。

透過 OpenSearch 服務，您可以為 AWS 服務外部服務設定 AI 連接器。使用主控台，您也可以使用 AWS CloudFormation 範本建立 ML 模型。如需詳細資訊，請參閱 the section called “CloudFormation 模板集成”。

有關語義搜索的完整文檔，包括使用語義搜索的 step-by-step 指南，請參閱開源 OpenSearch 文檔中的語義搜索。

Amazon OpenSearch 服務中的並發細分搜索

從 OpenSearch 版本 2.13 開始，您可以使用並行節段搜尋，協助您在查詢階段期間 parallel 搜尋節段。如需並行區段搜尋的完整說明文件，請參閱開放原始碼 OpenSearch 文件中的並行區段搜尋。如需有關並行區段搜尋相關之 Amazon CloudWatch 指標的資訊，請參閱執行個體指標和UltraWarm 指標。

當您搭配 Amazon OpenSearch 服務使用目前的區段搜尋時，還有一些其他限制適用：

- 您無法在 OpenSearch Service 中的索引層級啟用並行區段搜尋。
- 根據預設， OpenSearch Service 會使用具有最大磁碟片段計數機制的 2 個磁碟片段計數。

自然語言查詢產生 OpenSearch

Amazon Ser OpenSearch vice 中的自然語言查詢產生功能可讓您透過自然語言查詢操作和安全日誌資料。 OpenSearch 是探索日誌資料的理想選擇，因為它是一個高度可擴展和高效能的日誌分析和搜索引擎，現在您可以使用自然語言來瀏覽這些日誌。此功能可讓您識別問題，而無需依賴 OpenSearch 管道處理語言 (PPL)，也不必在建立查詢時查詢資料定義。您可以在版本 2.13 及更新版本的 OpenSearch Service 網域上使用自然語言查詢產生功能。您必須啟用精細的存取控制。

此功能是使用OpenSearch 助理工具包構建的。如果您想要建立與大型語言模型連線的類似功能，您可以使用此工具組來設定您自己的代理程式和工具。

必要條件

您的網域必須具備下列項目，才能使用自然語言查詢產生功能：

- 版本 2.13 或更高版本。
- 服務軟體 R20240520-P4 或更高版本。
- 啟用了精細的訪問控制。如需詳細資訊，請參閱啟用精細的存取控制。

開始使用

若要開始使用自然語言查詢產生功能，請確定您已在 OpenSearch Service 網域上啟用此功能。根據預設，所有使用 2.13 版及更新版本建立且啟用精細存取控制的網域都會啟用此功能。

如果您在 2024 年 7 月 2 日之前升級至 2.13 OpenSearch 版，則必須先將服務軟體更新為 (R20240520-P4) 或更新版本，才能啟用自然語言查詢產生。執行此操作之後，您可以選取 [人工智慧 (AI) 和 Machine Learning (ML)] 區段下的 [啟用自然語言產生查詢產生] 核取方塊來啟用此功能。

設定網域之後，瀏覽至 OpenSearch 儀表板中的 [記錄檔總管] 頁面。選擇 [事件總管]，並向查詢助理提出問題。

設定許可

如果您在預先存在的 OpenSearch 服務網域上啟用自然語言查詢產生，則可能不會在網域上定義 query_assistant_access 角色。非系統管理員使用者必須映射至此角色，以便在使用精細存取控制的網域上管理暖索引。若要手動建立查詢助手 _ 存取角色，請執行下列步驟：

1. 在 OpenSearch 儀表板中，移至安全性，然後選擇角色。
2. 選擇 [建立角色] 並設定下列叢集權限：
   - `cluster:admin/opensearch/ml/config/get`
   - `cluster:admin/opensearch/ml/execute`
   - `cluster:admin/opensearch/ml/predict`
   - `cluster:admin/opensearch/ml/ppl`
3. 命名角色查詢助理訪問。
4. 選擇建立角色。現在可以使用查詢助手 _ 存取角色。

> **Note**
>
> 對於要使用自然語言問題的`read`索引，您也必須擁有`indices:admin/mappings/get`和索引權限。

組態自動化

Flow Framework 是一種 OpenSearch 外掛程式，可為使用案例 (例如查詢產生和交談式聊天) 自動化 OpenSearch 設定。由於外掛程式會追蹤啟用自然語言查詢產生功能的資源，因此流程架構索引會為每個使用查詢輔助功能的網域儲存範本。

Flow Framework 可讓您從一組預先定義的範本中進行選取，或為機器學習連接器、工具、代理程式和其他做 OpenSearch 為生成模型後端的元件建立自動化作業。

使用 OpenSearch 儀表板與 Amazon OpenSearch 服務

OpenSearch 儀表板是一種開放原始碼視覺化工具，專為使用 OpenSearch而設 Amazon OpenSearch 服務為每個服 OpenSearch 務域提供 OpenSearch 儀表板的安裝。 OpenSearch 儀表板會在網域中的熱資料節點上執行。

您可以在 OpenSearch 服務主控台的網域 OpenSearch 儀表板上找到儀表板的連結。對於執行中的網域 OpenSearch，URL是*domain-endpoint*/_dashboards/. 對於執行舊版彈性搜尋的網域，則 URL為. *domain-endpoint*/_plugin/kibana

使用此預設 OpenSearch 儀表板安裝的查詢會有 300 秒的逾時時間。

> **Note**
>
> 本文件討論 Amazon OpenSearch 服務內容中的 OpenSearch 儀表板，包括連線到它的不同方式。如需完整的文件，包括入門指南、建立儀表板的指示、儀表板管理和儀表板查詢語言 (DQL)，請參閱開放原始碼 OpenSearch 文件中的OpenSearch 儀表板。

以下各節介紹了 OpenSearch 儀表板的一些常見使用案例：

- the section called “控制 OpenSearch 儀表板的存取”
- the section called “設定 OpenSearch 儀表板以使用地WMS圖伺服器”
- the section called “將本機儀表板伺服器連線至 OpenSearch 服務”

控制 OpenSearch 儀表板的存取

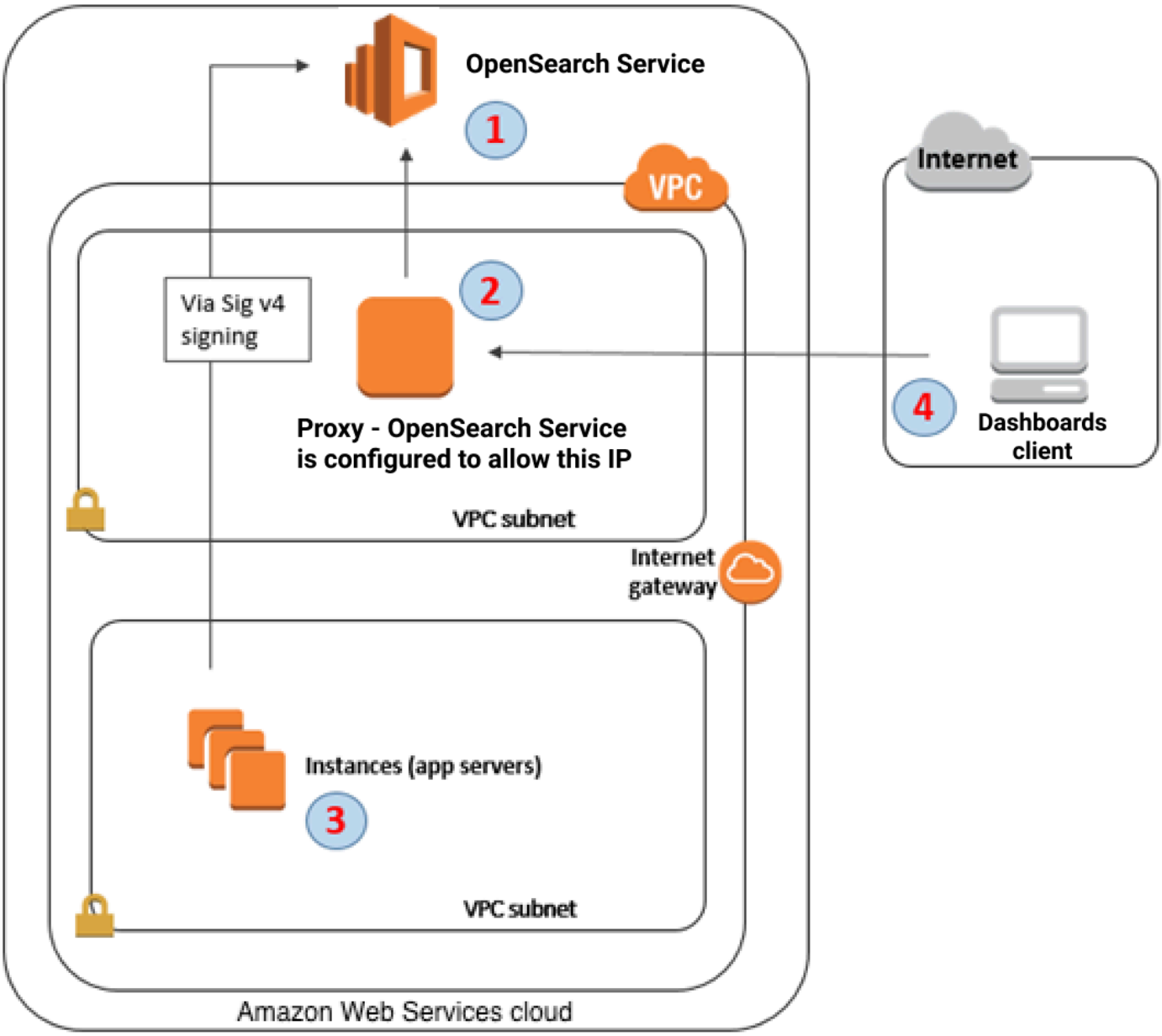
儀表板本身不支援IAM使用者和角色，但 OpenSearch Service 提供數種解決方案來控制儀表板的存取：

- 啟用儀表板的SAML驗證。
- 透過HTTP基本驗證使用精細的存取控制。
- 設定儀表板的 Cognito 身分驗證。
- 對於公有存取網域，設定 IP 型存取政策 (使用或不使用代理伺服器)。
- 對於VPC存取網域，請使用使用或不使用 Proxy 伺服器的開放存取原則，以及安全群組來控制存取。如需進一步了解，請參閱 the section called “關於網VPC域的存取原則”。

使用 Proxy 從 OpenSearch 儀表板存取 OpenSearch 服務

> **Note**
>
> 此程序僅當您的網域使用公有存取而您不想使用 Cognito 身分驗證時才適用。請參閱 the section called “控制 OpenSearch 儀表板的存取”。

由於儀表板是 JavaScript 應用程式，因此請求源自使用者的 IP 位址。以 IP 為基礎的存取控制可能不切實際，因為您為了每個使用者可以存取 Dashboards，而需要允許的 IP 地址相當龐大。一種解決方法是將代理服務器放置在 OpenSearch 儀表板和 OpenSearch 服務之間。然後，您可以新增 IP 為基礎的存取政策，允許僅從一個 IP 地址 (代理的) 發出請求。下圖顯示此組態。



1. 這是您的 OpenSearch 服務網域。IAM提供此網域的授權存取權。額外的 IP 為基礎的存取政策提供代理伺服器的存取。
2. 這是在 Amazon EC2 實例上運行的代理服務器。
3. 其他應用程式可以使用簽章版本 4 簽署程序，將已驗證的要求傳送至 OpenSearch 服務。
4. OpenSearch 儀表板用戶端透過 Proxy 連線到您的 OpenSearch 服務網域。

若要啟用此排序的組態，您需要以資源為基礎的政策，來指定角色和 IP 地址。以下是範例政策：

```
{
```

```
   "Version":"2012-10-17",
   "Statement":[
      {
         "Resource":"arn:aws:es:us-west-2:111111111111:domain/my-domain/*",
         "Principal":{
            "AWS":"arn:aws:iam::111111111111:role/allowedrole1"
         },
         "Action":[
            "es:ESHttpGet"
         ],
         "Effect":"Allow"
      },
      {
         "Effect":"Allow",
         "Principal":{
            "AWS":"*"
         },
         "Action":"es:*",
         "Condition":{
            "IpAddress":{
               "aws:SourceIp":[
                  "203.0.113.0/24",
                  "2001:DB8:1234:5678::/64"
               ]
            }
         },
         "Resource":"arn:aws:es:us-west-2:111111111111:domain/my-domain/*"
      }
   ]
}
```

建議您使用彈性 IP 位址設定EC2執行 Proxy 伺服器的執行個體。如此，您可以在必要時更換執行個體，同時連接相同的公有 IP 地址。若要進一步了解，請參閱 Amazon EC2 使用者指南中的彈性 IP 地址。

如果您使用代理伺服器和 Cognito 身分驗證，您可能需要新增 Dashboards 和 Amazon Cognito 的設定，以避免發生 `redirect_mismatch` 錯誤。請參閱以下 `nginx.conf` 範例：

```
server {
    listen 443;
    server_name $host;
    rewrite ^/$ https://$host/_plugin/_dashboards redirect;
```

```
    ssl_certificate           /etc/nginx/cert.crt;
    ssl_certificate_key       /etc/nginx/cert.key;

    ssl on;
    ssl_session_cache  builtin:1000  shared:SSL:10m;
    ssl_protocols  TLSv1 TLSv1.1 TLSv1.2;
    ssl_ciphers HIGH:!aNULL:!eNULL:!EXPORT:!CAMELLIA:!DES:!MD5:!PSK:!RC4;
    ssl_prefer_server_ciphers on;

    location /_plugin/_dashboards {
        # Forward requests to Dashboards
        proxy_pass https://$dashboards_host/_plugin/_dashboards;

        # Handle redirects to Cognito
        proxy_redirect https://$cognito_host https://$host;

        # Update cookie domain and path
        proxy_cookie_domain $dashboards_host $host;
        proxy_cookie_path / /_plugin/_dashboards/;

        # Response buffer settings
        proxy_buffer_size 128k;
        proxy_buffers 4 256k;
        proxy_busy_buffers_size 256k;
    }

    location ~ \/(log|sign|fav|forgot|change|saml|oauth2) {
        # Forward requests to Cognito
        proxy_pass https://$cognito_host;

        # Handle redirects to Dashboards
        proxy_redirect https://$dashboards_host https://$host;

        # Update cookie domain
        proxy_cookie_domain $cognito_host $host;
    }
}
```

設定 OpenSearch 儀表板以使用地WMS圖伺服器

OpenSearch 服務用 OpenSearch 儀表板的預設安裝包括地圖服務，印度和中國區域中的網域除外。地圖服務最多支援 10 個縮放比例。

無論您的區域為何，您都可以將儀表板設定為使用不同的 Web Map Service (WMS) 伺服器來進行座標地圖視覺效果。區域地圖視覺化僅支援預設地圖服務。

若要將儀表板設定為使用WMS地圖伺服器：

1. 開啟 Dashboards。
2. 選擇 Stack Management (堆疊管理)。
3. 選擇 Advanced Settings (進階設定)。
4. 定位視覺效果tileMap:: WMSdefaults。
5. 變更`enabledurl`為`true`有效WMS地圖伺服器URL的和為：

```
{
  "enabled": true,
  "url": "wms-server-url",
  "options": {
    "format": "image/png",
    "transparent": true
  }
}
```

6. 選擇 Save changes (儲存變更)。

若要將新的預設值套用到視覺化，您可能需要重新載入 Dashboards。如果您已儲存視覺化，請在開啟視覺化後選擇 Options (選項)。確認WMS地圖伺服器已啟用且 WMSurl 包含您偏好的地圖伺服器，然後選擇 [套用變更]。

> **Note**
>
> 地圖服務通常需要授權費或限制。您要對您指定在任何地圖伺服器負責所有這類考量。您可能會發現美國地質調查局的地圖服務適用於測試。

將本機儀表板伺服器連線至 OpenSearch 服務

如果您已經投入了大量時間來設定自己的 OpenSearch 儀表板執行個體，您可以使用它來取代 (或除了) OpenSearch Service 提供的預設儀表板執行個體。下列程序適用於搭配使用精細的存取控制與開放存取政策的網域。

將本機 OpenSearch 儀表板伺服器連線至 OpenSearch 服務

1. 在您的 OpenSearch 服務網域上，建立具有適當權限的使用者：
   a. 在 Dashboards 中，移至 Security (安全性)、Internal users (內部使用者)，然後選擇 Create internal user (建立內部使用者)。
   b. 提供使用者名稱和密碼，然後選擇 Create (建立)。
   c. 移至 Roles (角色)，然後選取角色。
   d. 選取 Mapped users (映射的使用者)，然後選擇 Manage mapping (管理映射)。
   e. 在 Users (使用者) 中，新增您的使用者名稱並選擇 Map (映射)。
2. 在您的自我管理儀表板安裝上下載並安裝適當版本的OSS安 OpenSearch 全性外掛程式。
3. 在您的本機儀表板伺 OpenSearch 服器上，開啟`config/opensearch_dashboards.yml`檔案，並使用您先前建立的使用者名稱和密碼新增服務端點：

```
opensearch.hosts: ['https://domain-endpoint']
opensearch.username: 'username'
opensearch.password: 'password'
```

   您可以使用以下範例 `opensearch_dashboards.yml` 檔案：

```
server.host: '0.0.0.0'

opensearch.hosts: ['https://domain-endpoint']

opensearchDashboards.index: ".username"

opensearch.ssl.verificationMode: none # if not using HTTPS

opensearch_security.auth.type: basicauth
opensearch_security.auth.anonymous_auth_enabled: false
opensearch_security.cookie.secure: false # set to true when using HTTPS
opensearch_security.cookie.ttl: 3600000
opensearch_security.session.ttl: 3600000
opensearch_security.session.keepalive: false
opensearch_security.multitenancy.enabled: false
opensearch_security.readonly_mode.roles: ['opensearch_dashboards_read_only']
opensearch_security.auth.unauthenticated_routes: []
opensearch_security.basicauth.login.title: 'Please log in using your username and
 password'
```

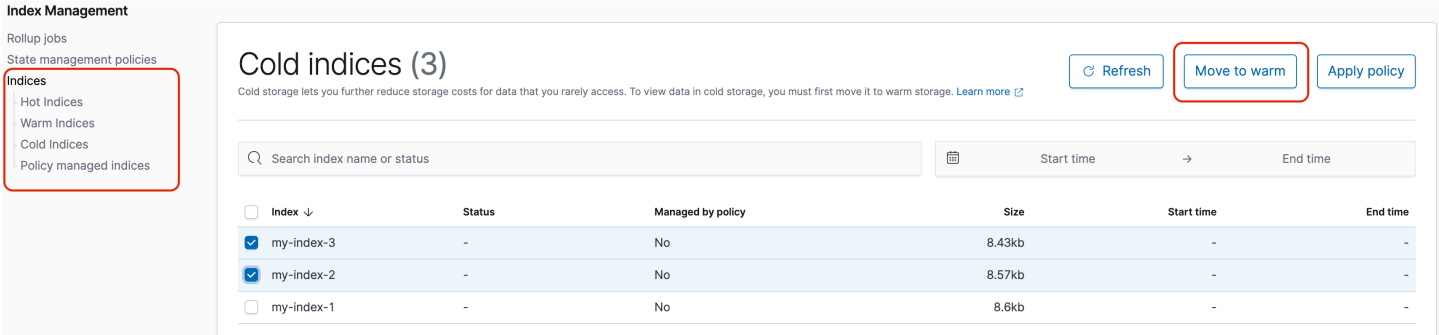
```
opensearch.username: 'username'
opensearch.password: 'password'
opensearch.requestHeadersWhitelist: [authorization, securitytenant,
 security_tenant]
```

要查看您的 OpenSearch 服務索引，請啟動本地儀表板服務器，轉到開發工具並運行以下命令：

```
GET _cat/indices
```

管理 OpenSearch 儀表板中的索引

OpenSearch Service 網域上的 OpenSearch 儀表板安裝提供有用的使用者介面，可用來管理網域上不同儲存層中的索引。從 [儀表板] 主功能表選擇 [索引管理]，以檢視非常用UltraWarm、冷存放區和冷存放區中的所有索引，以及由索引狀態管理 (ISM) 原則管理的索引。使用索引管理在暖儲存和冷儲存之間移動索引，並監控三個層級之間的遷移。



請注意，除非您已啟用和/或冷儲存，否則您將不會看到熱索引、溫索引 UltraWarm 和冷索引選項。

額外功能

每個 OpenSearch Service 網域上的預設 OpenSearch 儀表板安裝都有一些其他功能：

- 各種OpenSearch插件的用戶界面
- 租用戶
- 報告

  使用「CSV報告」功能表，從「探索」頁面以及/或儀表板PDF或視覺效果的PNG報表產生隨選報告。CSV報表有 10,000 個資料列限制。
- 甘特圖

- 筆記本

管理 Amazon OpenSearch 服務中的索引

將資料新增至 Amazon Ser OpenSearch vice 之後，您通常需要重新索引該資料、使用索引別名、將索引移至更具成本效益的儲存體，或將其完全刪除。本章涵蓋 UltraWarm 儲存、冷藏庫和索引狀態管理。如需 OpenSearch 索引 API 的相關資訊，請參閱OpenSearch 文件。

主題

- UltraWarm Amazon 服 OpenSearch 務存儲
- Amazon OpenSearch 服務的冷存儲
- OR1Amazon 服 OpenSearch 務存儲
- Amazon OpenSearch 服務中的索引狀態管理
- 總結 Amazon OpenSearch 服務中的索引與索引匯總
- 轉換 Amazon OpenSearch 服務中的索引
- Amazon OpenSearch 服務的跨叢集複寫
- 使用遠端重新索引遷移 Amazon OpenSearch 服務索引
- 使用資料串流管理 Amazon OpenSearch 服務中的時間序列資料

UltraWarm Amazon 服 OpenSearch 務存儲

UltraWarm 提供符合成本效益的方式，在 Amazon OpenSearch 服務上存放大量唯讀資料。標準資料節點使用「熱」儲存，它採用將執行個體存放區或 Amazon EBS 磁碟區連接到各個節點的形式。熱儲存可盡可能提供最快速的效能，以編製索引和搜尋新資料。

UltraWarm 節點不使用附加儲存，而是使用 Amazon S3 和精密的快取解決方案來提高效能。對於您未主動寫入、查詢頻率較低且不需要相同效能的索引， UltraWarm 可大幅降低每 GiB 資料的成本。因為暖索引是唯讀的，除非您將它們返回到熱存儲，因 UltraWarm 此最適合不可變數據，例如日誌。

在中 OpenSearch，暖索引的行為就像任何其他索引一樣。您可以使用相同的 API 查詢它們，也可以使用它們在 OpenSearch 儀表板中建立視覺效果。

主題

- 必要條件
- UltraWarm 儲存需求和效能考量
- UltraWarm 定價

- 啟用 UltraWarm
- 將索引遷移到 UltraWarm 存儲
- 自動化遷移
- 遷移調整
- 取消遷移
- 列出熱索引和暖索引
- 將暖索引傳回熱儲存區
- 從快照還原暖索引
- 暖索引的手動快照
- 將暖索引遷移到冷儲存
- 禁用 UltraWarm

必要條件

UltraWarm 有一些重要的先決條件：

- UltraWarm 需要 OpenSearch 或彈性搜索 6.8 或更高版本。
- 若要使用暖儲存區，網域必須具有專用的主節點。
- 將異地同步備份與待命網域搭配使用時，暖節點數目必須是正在使用的可用區域數目的倍數。
- 如果您的網域將 T2 或 T3 執行個體類型用於資料節點，您則無法使用暖儲存。
- 如果您的索引使用 近似 k-NN (`"index.knn": true`)，則您無法將其移動至暖儲存。
- 如果網域使用精細的存取控制，則必須將使用者對應至 OpenSearch 儀表板中的`ultrawarm_manager`角色，才能進行 UltraWarm API 呼叫。

> **Note**
>
> `ultrawarm_manager`角色可能未在某些預先存在的 OpenSearch 服務網域上定義。如果在 Dashboards 中沒有看到該角色，您需要手動建立它。

設定許可

如果您在預先存 UltraWarm 在的 OpenSearch 服務網域上啟用，則該`ultrawarm_manager`角色可能不會在網域上定義。非系統管理員使用者必須映射至此角色，以便在使用精細存取控制的網域上管理暖索引。若要手動建立 `ultrawarm_manager` 角色，請執行以下步驟：

1. 在 OpenSearch 儀表板中，轉到安全性，然後選擇權限。
2. 選擇 Create action group (建立動作群組) 並設定下列群組：

Group name (群組名稱)	許可
`ultrawarm_cluster`	• `cluster:admin/ultrawarm/migration/list` • `cluster:monitor/nodes/stats`
`ultrawarm_index_read`	• `indices:admin/ultrawarm/migration/get` • `indices:admin/get`
`ultrawarm_index_write`	• `indices:admin/ultrawarm/migration/warm` • `indices:admin/ultrawarm/migration/hot` • `indices:monitor/stats` • `indices:admin/ultrawarm/migration/cancel`

3. 選擇 Roles (角色)，然後選擇 Create role (建立角色)。
4. 將角色命名為 ultrawarm_manager。
5. 對於 Cluster permissions (叢集許可)，選取 `ultrawarm_cluster` 和 `cluster_monitor`。
6. 對於 Index (索引)，輸入 `*`。
7. 對於 Index permissions (索引許可)，選取 `ultrawarm_index_read`、`ultrawarm_index_write` 以及 `indices_monitor`。
8. 選擇建立。
9. 建立角色之後，請將其對應至任何將管理 UltraWarm 索引的使用者或後端角色。

UltraWarm 儲存需求和效能考量

如中所述the section called “計算儲存需求”，熱存儲中的數據會產生巨大的開銷：複本，Linux 保留空間和 OpenSearch 服務保留空間。例如，含有一個複本碎片的 20 GiB 的主要碎片大約需要 58 GiB 的熱儲存空間。

因為它使用 Amazon S3，所以 UltraWarm 不會產生任何此額外負荷。計算 UltraWarm 儲存需求時，您只會考慮主要碎片的大小。S3 中的資料耐久性不需要複本，且 S3 消除了任何作業系統或服務考量事項。相同的 20 GiB 碎片需要 20 GiB 的暖儲存。如果您佈建了 `ultrawarm1.large.search` 執行個體，您可將其所有 20 TiB 的儲存空間上限用於主要碎片。請參閱the section called “UltraWarm 儲存配額”，了解執行個體類型摘要，以及每個類型可處理的儲存量上限。

使用時 UltraWarm，我們仍建議最大分片大小為 50 GiB。CPU 核心數量和配置給每個 UltraWarm 執行個體類型的 RAM 數量可讓您瞭解它們可以同時搜尋的碎片數量。請注意，雖然只有主要碎片計入 S3 中的 UltraWarm儲存，但 OpenSearch 儀表板`_cat/indices`仍會將 UltraWarm 索引大小報告為所有主要和複本碎片的總數。

例如，每個 `ultrawarm1.medium.search` 執行個體具有兩個 CPU 核心，並且可處理 S3 上最多 1.5 TiB 的儲存。其中兩個執行個體具有 3 TiB 的組合儲存，如果每個碎片為 50 GiB，則可達到大約 62 個碎片。如果對叢集的請求只搜索這些碎片中的四個，則效能可能會很好。如果請求範圍廣泛，並且搜尋所有 62 個碎片，則四個 CPU 核心可能很難執行操作。監控`WarmCPUUtilization`和指`WarmJVMMemoryPressure`UltraWarm 標，瞭解執行個體如何處理您的工作負載。

如果您的搜尋範圍廣泛或頻繁，請考慮將索引留在熱儲存中。就像任何其他 OpenSearch 工作負載一樣，確定是否 UltraWarm 符合您的需求的最重要步驟是使用現實的數據集執行具有代表性的客戶端測試。

UltraWarm 定價

使用熱儲存時，您需要按實際佈建內容付費。有些執行個體需要連接的 Amazon EBS 磁碟區，有些則包含執行個體存放區。無論該儲存空間是空的還是已滿，都是支付相同的價格。

有了 UltraWarm 儲存空間，您就需要支付使用量的費用。一個 `ultrawarm1.large.search` 執行個體可在 S3 上處理高達 20 TiB 的儲存空間，但如果您只儲存 1 TiB 的資料，則只需支付 1 TiB 的資料費用。與所有其他節點類型一樣，您也會為每個 UltraWarm 節點支付小時費率。如需詳細資訊，請參閱the section called “定價”。

啟用 UltraWarm

主控台是建立使用暖儲存之網域最簡單的方法。建立網域時，選擇 [啟用 UltraWarm 資料節點] 和您想要的暖節點數目。同樣的基本程序適用於現有的網域，只要它們符合 先決條件即可。即使網域狀態從 [處理] 變更為 [作用中]，也 UltraWarm 可能在數小時內無法使用。

將異地同步備份與待命網域搭配使用時，暖節點數目必須是正在使用的可用區域數目的倍數。如需詳細資訊，請參閱 the section called “異地同步備份含待機”。

您也可以使用AWS CLI或設定 API 來啟用 UltraWarm，特別是中的`WarmEnabled``WarmCount`、和`WarmType`選項`ClusterConfig`。

> **Note**
>
> 網域支援暖節點數量上限。如需詳細資訊，請參閱 the section called “配額”。

CLI 命令範例

下列 AWS CLI 指令會建立具有三個資料節點、三個專用主節點、六個暖節點，以及啟用精細存取控制的網域：

```
aws opensearch create-domain \
  --domain-name my-domain \
  --engine-version Opensearch_1.0 \
  --cluster-config
 InstanceCount=3,InstanceType=r6g.large.search,DedicatedMasterEnabled=true,DedicatedMasterType=
 \
  --ebs-options EBSEnabled=true,VolumeType=gp2,VolumeSize=11 \
  --node-to-node-encryption-options Enabled=true \
  --encryption-at-rest-options Enabled=true \
  --domain-endpoint-options EnforceHTTPS=true,TLSSecurityPolicy=Policy-Min-
TLS-1-2-2019-07 \
  --advanced-security-options
 Enabled=true,InternalUserDatabaseEnabled=true,MasterUserOptions='{MasterUserName=master-
user,MasterUserPassword=master-password}' \
  --access-policies '{"Version":"2012-10-17","Statement":
[{"Effect":"Allow","Principal":{"AWS":["123456789012"]},"Action":
["es:*"],"Resource":"arn:aws:es:us-west-1:123456789012:domain/my-domain/*"}]}' \
  --region us-east-1
```

如需詳細資訊，請參閱 AWS CLI 命令參考。

組態 API 請求範例

以下對組態 API 的請求會建立一個網域，它具有三個資料節點、三個專用主節點、六個已啟用精細存取控制的暖節點、以及一個限制性存取政策：

```
POST https://es.us-east-2.amazonaws.com/2021-01-01/opensearch/domain
{
  "ClusterConfig": {
    "InstanceCount": 3,
    "InstanceType": "r6g.large.search",
    "DedicatedMasterEnabled": true,
    "DedicatedMasterType": "r6g.large.search",
    "DedicatedMasterCount": 3,
    "ZoneAwarenessEnabled": true,
    "ZoneAwarenessConfig": {
      "AvailabilityZoneCount": 3
    },
    "WarmEnabled": true,
    "WarmCount": 6,
    "WarmType": "ultrawarm1.medium.search"
  },
  "EBSOptions": {
    "EBSEnabled": true,
    "VolumeType": "gp2",
    "VolumeSize": 11
  },
  "EncryptionAtRestOptions": {
    "Enabled": true
  },
  "NodeToNodeEncryptionOptions": {
    "Enabled": true
  },
  "DomainEndpointOptions": {
    "EnforceHTTPS": true,
    "TLSSecurityPolicy": "Policy-Min-TLS-1-2-2019-07"
  },
   "AdvancedSecurityOptions": {
    "Enabled": true,
    "InternalUserDatabaseEnabled": true,
    "MasterUserOptions": {
      "MasterUserName": "master-user",
```

```
      "MasterUserPassword": "master-password"
    }
  },
  "EngineVersion": "Opensearch_1.0",
  "DomainName": "my-domain",
  "AccessPolicies": "{\"Version\":\"2012-10-17\",\"Statement\":[{\"Effect\":\"Allow
\",\"Principal\":{\"AWS\":[\"123456789012\"]},\"Action\":[\"es:*\"],\"Resource\":
\"arn:aws:es:us-east-1:123456789012:domain/my-domain/*\"}]}"
}
```

如需詳細資訊，請參閱 Amazon OpenSearch 服務 API 參考。

將索引遷移到 UltraWarm 存儲

如果您完成索引的寫入，但不再需要最快的搜尋效能，請將其從熱移轉到 UltraWarm：

```
POST _ultrawarm/migration/my-index/_warm
```

接著，檢查遷移狀態：

```
GET _ultrawarm/migration/my-index/_status

{
  "migration_status": {
    "index": "my-index",
    "state": "RUNNING_SHARD_RELOCATION",
    "migration_type": "HOT_TO_WARM",
    "shard_level_status": {
      "running": 0,
      "total": 5,
      "pending": 3,
      "failed": 0,
      "succeeded": 2
    }
  }
}
```

索引運作狀態必須為綠色才能執行遷移。如果您快速地連續遷移多個索引，您可以取得純文字格式的所有遷移摘要，與 `_cat` API 類似：

```
GET _ultrawarm/migration/_status?v
```

```
index     migration_type state
my-index HOT_TO_WARM    RUNNING_SHARD_RELOCATION
```

OpenSearch 服務一次會將一個索引移轉至 UltraWarm。您最多可以在佇列中進行 200 個遷移操作。任何超出限制的請求都會被拒絕。若要檢查佇列中的目前遷移數目，請監控 `HotToWarmMigrationQueueSize` 指標。在整個遷移過程中，索引仍然可用，無需停機。

遷移程序具有下列狀態：

```
PENDING_INCREMENTAL_SNAPSHOT
RUNNING_INCREMENTAL_SNAPSHOT
FAILED_INCREMENTAL_SNAPSHOT
PENDING_FORCE_MERGE
RUNNING_FORCE_MERGE
FAILED_FORCE_MERGE
PENDING_FULL_SNAPSHOT
RUNNING_FULL_SNAPSHOT
FAILED_FULL_SNAPSHOT
PENDING_SHARD_RELOCATION
RUNNING_SHARD_RELOCATION
FINISHED_SHARD_RELOCATION
```

如這些狀態所示，遷移可能在快照、碎片重新配置或強制合併期間失敗。快照或碎片重新配置期間的失敗通常是因為節點故障或 S3 連線問題。磁碟空間不足通常是強制合併失敗的根本原因。

遷移完成後，同一個 `_status` 請求會傳回錯誤。如果您在當下立即檢查索引，您可能會看到暖索引獨有的某些設定：

```
GET my-index/_settings

{
  "my-index": {
    "settings": {
      "index": {
        "refresh_interval": "-1",
        "auto_expand_replicas": "false",
        "provided_name": "my-index",
        "creation_date": "1599241458998",
        "unassigned": {
          "node_left": {
            "delayed_timeout": "5m"
          }
```

```
        },
        "number_of_replicas": "1",
        "uuid": "GswyCdR0RSq0SJYmzsIpiw",
        "version": {
          "created": "7070099"
        },
        "routing": {
          "allocation": {
            "require": {
              "box_type": "warm"
            }
          }
        },
        "number_of_shards": "5",
        "merge": {
          "policy": {
            "max_merge_at_once_explicit": "50"
          }
        }
      }
    }
  }
}
```

- 在此情況下，`number_of_replicas` 則為被動複本的數量，這不會耗用磁碟空間。
- `routing.allocation.require.box_type` 指定索引應使用暖節點，而不是標準資料節點。
- `merge.policy.max_merge_at_once_explicit` 指定遷移期間要同時合併的區段數目。

暖存儲中的索引是只讀的，除非您將它們返回到熱存儲，這使得 UltraWarm 最適合不可變數據，例如日誌。您可以查詢索引並刪除它們，但無法新增、更新或刪除個別文件。如果您嘗試，可能會遇到下列錯誤：

```
{
  "error" : {
    "root_cause" : [
      {
        "type" : "cluster_block_exception",
        "reason" : "index [indexname] blocked by: [TOO_MANY_REQUESTS/12/disk usage
 exceeded flood-stage watermark, index has read-only-allow-delete block];"
      }
    ],
```

```
    "type" : "cluster_block_exception",
    "reason" : "index [indexname] blocked by: [TOO_MANY_REQUESTS/12/disk usage exceeded
 flood-stage watermark, index has read-only-allow-delete block];"
  },
  "status" : 429
}
```

自動化遷移

建議您在索引達到特定存在時間或符合其他條件之後，使用 the section called “索引狀態管理” 自動化移轉程序。請參閱示範此工作流程的範例政策。

遷移調整

將索引移轉至 UltraWarm 儲存區需要強制合併。每個 OpenSearch 索引由一定數量的碎片組成，並且每個分片由一定數量的 Lucene 段組成。強制合併操作會清除標示為刪除的文件，並節省磁碟空間。默認情況下，將索引 UltraWarm 合併為一個段。

您可以使用 `index.ultrawarm.migration.force_merge.max_num_segments` 設定，將此值變更為最多 1,000 個區段。較高的值會加快遷移程序，但會在移轉完成後增加暖索引的查詢延遲。若要變更設定，請提出下列請求：

```
PUT my-index/_settings
{
  "index": {
    "ultrawarm": {
      "migration": {
        "force_merge": {
          "max_num_segments": 1
        }
      }
    }
  }
}
```

若要檢查遷移程序的此階段需要多長時間，請監控 `HotToWarmMigrationForceMergeLatency` 指標。

取消遷移

UltraWarm 按順序處理遷移，在隊列中。如果遷移位於佇列中，但尚未啟動，您可以使用下列請求從佇列中移除它：

```
POST _ultrawarm/migration/_cancel/my-index
```

如果您的網域使用精細存取控制，則您必須擁有 `indices:admin/ultrawarm/migration/cancel` 許可才能提出此請求。

列出熱索引和暖索引

UltraWarm 增加了兩個其他選項，類似於`_all`，以協助管理熱索引和暖索引。如需所有暖索引或熱索引的清單，請提出下列請求：

```
GET _warm
GET _hot
```

您可以在指定索引的其他請求中使用這些選項，例如：

```
_cat/indices/_warm
_cluster/state/_all/_hot
```

將暖索引傳回熱儲存區

如果您需要再次寫入索引，請將其移轉回熱存儲區：

```
POST _ultrawarm/migration/my-index/_hot
```

您一次最多可以有 10 個佇列移轉，從暖色儲存裝置移轉至熱儲存區。 OpenSearch Service 會依照排入佇列的順序，一次處理一個移轉要求。若要檢查目前的數目，請監控 `WarmToHotMigrationQueueSize` 指標。

遷移完成後，請檢查索引設定以確定符合您的需求。索引會使用一個複本傳回熱儲存區。

從快照還原暖索引

除了自動化快照的標準儲存庫之外，還為暖索引 UltraWarm 新增第二個儲存庫`cs-ultrawarm`。此儲存庫中的每個快照只包含一個索引。如果您刪除暖索引，其快照會保留在 `cs-ultrawarm` 儲存庫 14 天，就像任何其他自動快照一樣。

當您從 cs-ultrawarm 還原快照時，快照會還原至暖儲存區，而非熱儲存區。cs-automated 和 cs-automated-enc 儲存庫中的快照會還原為熱儲存。

將 UltraWarm 快照還原到暖儲存

1. 識別包含您要還原之索引的最新快照：

```
GET _snapshot/cs-ultrawarm/_all?verbose=false

{
  "snapshots": [{
    "snapshot": "snapshot-name",
    "version": "1.0",
    "indices": [
      "my-index"
    ]
  }]
}
```

> **Note**
>
> 依預設，GET _snapshot/<repo>作業會顯示儲存庫中每個快照的詳細資料資訊，例如開始時間、結束時間和持續時間。此GET _snapshot/<repo>作業會從儲存庫中包含的每個快照的檔案擷取資訊。如果您不需要開始時間、結束時間和持續時間，而且只需要快照的名稱和索引資訊，建議您在列出快照時使用verbose=false參數，以盡可能減少處理時間並防止逾時。

2. 如果索引已經存在，請將其刪除：

```
DELETE my-index
```

   如果您不想刪除索引，將其還原至熱儲存並重新索引它。

3. 還原快照：

```
POST _snapshot/cs-ultrawarm/snapshot-name/_restore
```

   UltraWarm 會忽略您在此還原要求中指定的任何索引設定，但您可以指定rename_pattern和之類的選項rename_replacement。如需 OpenSearch 快照還原選項的摘要，請參閱OpenSearch 文件。

暖索引的手動快照

您可以拍攝暖索引的手動快照，但我們不建議這樣做。自動化 `cs-ultrawarm` 儲存庫已包含每個暖索引的快照 (在遷移期間取得)，不需額外付費。

根據預設， OpenSearch 服務不會在手動快照中包含暖索引。例如，以下呼叫只包含熱索引：

```
PUT _snapshot/my-repository/my-snapshot
```

如果您選擇拍攝暖索引的手動快照，則需要考慮幾個重要因素。

- 您不能混合熱索引和暖索引。例如，下列請求會失敗：

  ```
  PUT _snapshot/my-repository/my-snapshot
  {
    "indices": "warm-index-1,hot-index-1",
    "include_global_state": false
  }
  ```

  如果它們包含熱索引和暖索引的混合，則萬用字元 (*) 陳述式也會失敗。

- 每個快照只能包含一個暖索引。例如，下列請求會失敗：

  ```
  PUT _snapshot/my-repository/my-snapshot
  {
    "indices": "warm-index-1,warm-index-2,other-warm-indices-*",
    "include_global_state": false
  }
  ```

  此請求成功：

  ```
  PUT _snapshot/my-repository/my-snapshot
  {
    "indices": "warm-index-1",
    "include_global_state": false
  }
  ```

- 手動快照一律還原至熱儲存，即使它們原本包含暖索引。

將暖索引遷移到冷儲存

如果您有不常查詢 UltraWarm 的資料，請考慮將其移轉至冷存放區。冷儲存適合您偶爾才存取的資料，或不再為使用中狀態的資料。您無法讀取或寫入冷索引，但無論何時需要查詢，都可以免費將它們遷移回暖儲存。如需說明，請參閱the section called “將索引遷移至冷儲存”。

禁用 UltraWarm

控制台是最簡單的禁用方法 UltraWarm。選擇網域、Actions (動作) 和 Edit cluster configuration (編輯叢集組態)。取消選取啟用 UltraWarm 資料節點並選擇儲存變更。您也可以使用 AWS CLI 和配置 API 中的 `WarmEnabled` 選項。

停用之前 UltraWarm，您必須刪除所有暖索引，或將它們移轉回常用儲存區。暖儲存空間為空之後，請等待五分鐘，然後再嘗試停用 UltraWarm。

Amazon OpenSearch 服務的冷存儲

冷存儲可讓您在 Amazon Ser OpenSearch vice 網域上存放任何數量的不常存取或歷史資料，並以比其他儲存層更低的成本按需進行分析。如果您需要對舊資料進行定期研究或鑑識分析，則冷儲存適合。適合冷儲存的實際資料範例包括不常存取的日誌、必須保留以滿足合規要求的資料，或是具有歷史價值的日誌。

與UltraWarm儲存類似，冷儲存也由 Amazon S3 提供支援。當您需要查詢冷資料時，可以選擇性地將其貼附至既有 UltraWarm節點。您可以手動或使用索引狀態管理政策來管理冷資料的遷移和生命週期。

主題

- 必要條件
- 冷儲存要求和效能考量
- 冷儲存定價
- 啟用冷儲存
- 管理 OpenSearch 儀表板中的冷索引
- 將索引遷移至冷儲存
- 自動移轉至冷儲存
- 取消遷移至冷儲存

- 列出冷索引
- 將冷索引遷移至暖儲存
- 從快照中還原冷索引
- 取消從冷儲存遷移至暖儲存
- 更新冷索引中繼資料
- 刪除冷索引
- 停用冷儲存

必要條件

冷儲存具有以下先決條件：

- 冷庫需要 OpenSearch 或彈性搜索 7.9 版或更高版本。
- 若要在 OpenSearch 服務網域上啟用冷儲存，您也必須在相同網域 UltraWarm 上啟用。
- 若要使用冷儲存，網域必須具有專用的主節點。
- 如果您的網域將 T2 或 T3 執行個體類型用於資料節點，則無法使用冷儲存。
- 如果您的索引使用 近似 k-NN (`"index.knn": true`)，則您無法將其移動至冷儲存。
- 如果網域使用精細的存取控制，則非管理員使用者必須對應至 OpenSearch 儀表板中的`cold_manager`角色，才能管理冷索引。

> **Note**
>
> `cold_manager`角色可能不存在於某些預先存在的 OpenSearch 服務網域中。如果在 Dashboards 中沒有看到該角色，您需要手動建立它。

設定許可

如果您在預先存在的 OpenSearch 服務網域上啟用冷儲存，則該`cold_manager`角色可能不會在網域上定義。如果網域使用精細的存取控制，則必須將非管理員使用者對應至此角色，才能管理冷索引。若要手動建立 `cold_manager` 角色，請執行以下步驟：

1. 在 OpenSearch 儀表板中，轉到安全性，然後選擇權限。
2. 選擇 Create action group (建立動作群組) 並設定下列群組：

Group name (群組名稱)	許可
`cold_cluster`	• `cluster:monitor/nodes/stats` • `cluster:admin/ultrawarm*` • `cluster:admin/cold/*`
`cold_index`	• `indices:monitor/stats` • `indices:data/read/minmax` • `indices:admin/ultrawarm/migration/get` • `indices:admin/ultrawarm/migration/cancel`

3. 選擇 Roles (角色)，然後選擇 Create role (建立角色)。
4. 將角色命名為 cold_manager。
5. 對於 Cluster permissions (叢集許可)，選擇您建立的 `cold_cluster` 群組。
6. 對於 Index (索引)，輸入 `*`。
7. 對於 Index permissions (索引許可)，選擇您建立的 `cold_index` 群組。
8. 選擇建立。
9. 建立角色之後，請將其對應至管理冷索引的任何使用者或後端角色。

冷儲存要求和效能考量

由於冷儲存使用 Amazon S3，因此不會產生熱儲存的額外負荷，例如複本、Linux 保留空間和 OpenSearch 服務保留空間。冷儲存沒有特定執行個體類型，因為它沒有連接任何運算容量。您可以在冷儲存中儲存任意數量的資料。在 Amazon 中監控`ColdStorageSpaceUtilization`指標，CloudWatch 以查看您正在使用多少冷儲存空間。

冷儲存定價

與 UltraWarm 存儲類似，使用冷存儲，您只需支付數據存儲費用。冷資料沒有運算成本，如果冷儲存中沒有資料，您將無需支付費用。

在冷儲存和暖儲存之間移動資料時，不會產生任何傳輸費用。雖然正在暖儲存和冷儲存之間遷移索引，但您仍然只需支付一份索引副本的費用。遷移完成後，會根據索引遷移到的儲存層計費。如需冷儲存定價的詳細資訊，請參閱 Amazon OpenSearch 服務定價。

啟用冷儲存

主控台是建立使用冷儲存之網域的最簡單方法。建立網域時，選擇 Enable cold storage (啟用冷儲存)。只要滿足先決條件，相同程序也適用於現有網域。即使網域狀態從 Processing (正在處理) 變更為 Active (作用中)，冷儲存可能會長達數小時無法使用。

您也可以使用 AWS CLI 或組態 API 來啟用冷儲存。

CLI 命令範例

下列 AWS CLI 指令會建立具有三個資料節點、三個專用主節點、已啟用冷儲存並啟用精細存取控制的網域：

```
aws opensearch create-domain \
  --domain-name my-domain \
  --engine-version Opensearch_1.0 \
  --cluster-
config ColdStorageOptions={Enabled=true},WarmEnabled=true,WarmCount=4,WarmType=ultrawarm1.mediu
 \
  --ebs-options EBSEnabled=true,VolumeType=gp2,VolumeSize=11 \
  --node-to-node-encryption-options Enabled=true \
  --encryption-at-rest-options Enabled=true \
  --domain-endpoint-options EnforceHTTPS=true,TLSSecurityPolicy=Policy-Min-
TLS-1-2-2019-07 \
  --advanced-security-options
 Enabled=true,InternalUserDatabaseEnabled=true,MasterUserOptions='{MasterUserName=master-
user,MasterUserPassword=master-password}' \
  --region us-east-2
```

如需詳細資訊，請參閱 AWS CLI 命令參考。

組態 API 請求範例

對組態 API 的以下請求會建立一個網域，它具有三個資料節點、三個專用主節點、已啟用冷儲存，以及已啟用精細存取控制：

```
POST https://es.us-east-2.amazonaws.com/2021-01-01/opensearch/domain
{
  "ClusterConfig": {
    "InstanceCount": 3,
    "InstanceType": "r6g.large.search",
```

```
    "DedicatedMasterEnabled": true,
    "DedicatedMasterType": "r6g.large.search",
    "DedicatedMasterCount": 3,
    "ZoneAwarenessEnabled": true,
    "ZoneAwarenessConfig": {
      "AvailabilityZoneCount": 3
     },
    "WarmEnabled": true,
    "WarmCount": 4,
    "WarmType": "ultrawarm1.medium.search",
    "ColdStorageOptions": {
       "Enabled": true
     }
  },
  "EBSOptions": {
    "EBSEnabled": true,
    "VolumeType": "gp2",
    "VolumeSize": 11
  },
  "EncryptionAtRestOptions": {
    "Enabled": true
  },
  "NodeToNodeEncryptionOptions": {
    "Enabled": true
  },
  "DomainEndpointOptions": {
    "EnforceHTTPS": true,
    "TLSSecurityPolicy": "Policy-Min-TLS-1-2-2019-07"
  },
   "AdvancedSecurityOptions": {
    "Enabled": true,
    "InternalUserDatabaseEnabled": true,
    "MasterUserOptions": {
      "MasterUserName": "master-user",
      "MasterUserPassword": "master-password"
    }
  },
  "EngineVersion": "Opensearch_1.0",
  "DomainName": "my-domain"
}
```

如需詳細資訊，請參閱 Amazon OpenSearch 服務 API 參考。

管理 OpenSearch 儀表板中的冷索引

您可以使用 OpenSearch Service 網域中現有的儀表板介面來管理熱索引、溫索引和冷索引。Dashboards 可讓您在暖儲存和冷儲存之間遷移索引並監控索引遷移狀態，而不需要使用 CLI 或組態 API。如需詳細資訊，請參閱管理 OpenSearch 儀表板中的索引。

將索引遷移至冷儲存

當您將索引遷移至冷儲存時，會為資料提供一個時間範圍，以便更輕鬆地探索。您可以根據索引中的資料選取時間戳記欄位，手動提供開始和結束時間戳記，或選擇不指定時間戳記。

參數	支援的值	描述
`timestamp_field`	來自索引映射的日期/時間欄位。	會運算提供的欄位的最小值和最大值並存儲為冷索引的 `start_time` 和 `end_time` 中繼資料。
`start_time` 和 `end_time`	下列其中一個格式： • strict_date_optional_time。例如：`yyyy-MM-dd'T'HH:mm:ss.SSSZ` 或 `yyyy-MM-dd` • Epoch 時間 (以毫秒為單位)	提供的值存儲為冷索引的 `start_time` 和 `end_time` 中繼資料。

如果您不希望指定時間戳記，請將 `?ignore=timestamp` 新增到請求。

下列請求會將暖索引遷移至冷儲存，並提供在該索引中資料的開始和結束時間：

```
POST _ultrawarm/migration/my-index/_cold
  {
    "start_time": "2020-03-09",
    "end_time": "2020-03-09T23:00:00Z"
  }
```

接著，檢查遷移狀態：

```
GET _ultrawarm/migration/my-index/_status
```

```
{
  "migration_status": {
    "index": "my-index",
    "state": "RUNNING_METADATA_RELOCATION",
    "migration_type": "WARM_TO_COLD"
  }
}
```

OpenSearch 服務一次會將一個索引移轉至冷藏庫。您最多可以在佇列中進行 100 個遷移操作。任何超出限制的請求都會被拒絕。若要檢查佇列中的目前遷移數目，請監控 `WarmToColdMigrationQueueSize` 指標。遷移程序具有下列狀態：

```
ACCEPTED_COLD_MIGRATION - Migration request is accepted and queued.
RUNNING_METADATA_MIGRATION - The migration request was selected for execution and
 metadata is migrating to cold storage.
FAILED_METADATA_MIGRATION - The attempt to add index metadata has failed and all
 retries are exhausted.
PENDING_INDEX_DETACH - Index metadata migration to cold storage is completed. Preparing
 to detach the warm index state from the local cluster.
RUNNING_INDEX_DETACH - Local warm index state from the cluster is being removed. Upon
 success, the migration request will be completed.
FAILED_INDEX_DETACH - The index detach process failed and all retries are exhausted.
```

自動移轉至冷儲存

在索引達到特定時間或滿足其他條件時，您可使用索引狀態管理自動化遷移程序。請參閱範例原則，其中示範如何自動將索引從熱儲存移轉 UltraWarm 到冷存放區。

> **Note**
>
> 需要明確定義 `timestamp_field`，才能使用索引狀態管理政策將索引移至冷儲存。

取消遷移至冷儲存

如果遷移至冷儲存已排入佇列或處於失敗狀態，您可以使用下列請求取消遷移：

```
POST _ultrawarm/migration/_cancel/my-index

{
```

```
  "acknowledged" : true
}
```

如果您的網域使用精細存取控制，您需要 `indices:admin/ultrawarm/migration/cancel` 許可來提出此請求。

列出冷索引

在查詢之前，您可以列出冷存儲中的索引，以決定要移轉到哪些索引以 UltraWarm 進一步分析。下列要求會列出所有冷索引，並依索引名稱排序：

```
GET _cold/indices/_search
```

回應範例

```
{
  "pagination_id" : "je7MtGbClwBF/2Zp9Utk/h3yCo8nvbEXAMPLEKEY",
  "total_results" : 3,
  "indices" : [
    {
      "index" : "my-index-1",
      "index_cold_uuid" : "hjEoh26mRRCFxRIMdgvLmg",
      "size" : 10339,
      "creation_date" : "2021-06-28T20:23:31.206Z",
      "start_time" : "2020-03-09T00:00Z",
      "end_time" : "2020-03-09T23:00Z"
    },
    {
      "index" : "my-index-2",
      "index_cold_uuid" : "0vIS2n-oROmOWDFmwFIgdw",
      "size" : 6068,
      "creation_date" : "2021-07-15T19:41:18.046Z",
      "start_time" : "2020-03-09T00:00Z",
      "end_time" : "2020-03-09T23:00Z"
    },
    {
      "index" : "my-index-3",
      "index_cold_uuid" : "EaeXOBodTLiDYcivKsXVLQ",
      "size" : 32403,
      "creation_date" : "2021-07-08T00:12:01.523Z",
      "start_time" : "2020-03-09T00:00Z",
      "end_time" : "2020-03-09T23:00Z"
```

```
    }
  ]
}
```

篩選

您可以根據以字首為基礎的索引模式和時間範圍偏移來篩選冷索引。

以下請求列出了與 `event-*` 的字首模式匹配的索引：

```
GET _cold/indices/_search
 {
   "filters":{
      "index_pattern": "event-*"
   }
 }
```

回應範例

```
{
  "pagination_id" : "je7MtGbClwBF/2Zp9Utk/h3yCo8nvbEXAMPLEKEY",
  "total_results" : 1,
  "indices" : [
    {
      "index" : "events-index",
      "index_cold_uuid" : "4eFiab7rRfSvp3slrIsIKA",
      "size" : 32263273,
      "creation_date" : "2021-08-18T18:25:31.845Z",
      "start_time" : "2020-03-09T00:00Z",
      "end_time" : "2020-03-09T23:00Z"
    }
  ]
}
```

以下請求傳回的索引具有介於 `2019-03-01` 到 `2020-03-01` 之間的 `start_time` 和 `end_time` 中繼資料欄位：

```
GET _cold/indices/_search
{
  "filters": {
    "time_range": {
      "start_time": "2019-03-01",
```

```
      "end_time": "2020-03-01"
    }
  }
}
```

回應範例

```
{
  "pagination_id" : "je7MtGbClwBF/2Zp9Utk/h3yCo8nvbEXAMPLEKEY",
  "total_results" : 1,
  "indices" : [
    {
      "index" : "my-index",
      "index_cold_uuid" : "4eFiab7rRfSvp3slrIsIKA",
      "size" : 32263273,
      "creation_date" : "2021-08-18T18:25:31.845Z",
      "start_time" : "2019-05-09T00:00Z",
      "end_time" : "2019-09-09T23:00Z"
    }
  ]
}
```

排序

您可以按照中繼資料欄位 (例如索引名稱或大小) 來排序冷索引。以下請求列出按照大小排序 (降序) 的所有索引：

```
GET _cold/indices/_search
 {
 "sort_key": "size:desc"
 }
```

回應範例

```
{
  "pagination_id" : "je7MtGbClwBF/2Zp9Utk/h3yCo8nvbEXAMPLEKEY",
  "total_results" : 5,
  "indices" : [
    {
      "index" : "my-index-6",
      "index_cold_uuid" : "4eFiab7rRfSvp3slrIsIKA",
      "size" : 32263273,
```

```
      "creation_date" : "2021-08-18T18:25:31.845Z",
      "start_time" : "2020-03-09T00:00Z",
      "end_time" : "2020-03-09T23:00Z"
    },
    {
      "index" : "my-index-9",
      "index_cold_uuid" : "mbD3ZRVDRI6ONqgEOsJyUA",
      "size" : 57922,
      "creation_date" : "2021-07-07T23:41:35.640Z",
      "start_time" : "2020-03-09T00:00Z",
      "end_time" : "2020-03-09T23:00Z"
    },
    {
      "index" : "my-index-5",
      "index_cold_uuid" : "EaeXOBodTLiDYcivKsXVLQ",
      "size" : 32403,
      "creation_date" : "2021-07-08T00:12:01.523Z",
      "start_time" : "2020-03-09T00:00Z",
      "end_time" : "2020-03-09T23:00Z"
    }
  ]
}
```

其他有效的排序金鑰為 `start_time:asc/desc`、`end_time:asc/desc` 和 `index_name:asc/desc`。

分頁

您可以分頁冷索引清單。使用 `page_size` 參數來設定每頁要傳回的索引數目 (預設值為 10)。針對冷索引的每個 `_search` 請求傳回一個 `pagination_id`，您可以將其用於後續呼叫。

以下請求會對冷索引的 `_search` 請求結果進行分頁，並顯示接下來的 100 個結果：

```
GET _cold/indices/_search?page_size=100
{
"pagination_id": "je7MtGbClwBF/2Zp9Utk/h3yCo8nvbEXAMPLEKEY"
}
```

將冷索引遷移至暖儲存

使用上一節中的篩選準則縮小冷索引清單之後，請將它們移轉回您可以查詢資料的 UltraWarm 位置，並使用它來建立視覺效果。

以下請求會將兩個冷索引遷移回暖儲存：

```
POST _cold/migration/_warm
 {
 "indices": "my-index1,my-index2"
 }


{
  "acknowledged" : true
}
```

若要檢查遷移狀態並擷取遷移 ID，請傳送下列請求：

```
GET _cold/migration/_status
```

回應範例

```
{
  "cold_to_warm_migration_status" : [
    {
      "migration_id" : "tyLjXCA-S76zPQbPVHkOKA",
      "indices" : [
        "my-index1,my-index2"
      ],
      "state" : "RUNNING_INDEX_CREATION"
    }
  ]
}
```

若要取得索引特定的遷移資訊，請包含索引名稱：

```
GET _cold/migration/my-index/_status
```

您可以按照當前遷移狀態列出索引，而不是指定索引。有效值為 `_failed`、`_accepted` 和 `_all`。

以下命令會取得單一遷移請求中所有索引的狀態：

```
GET _cold/migration/_status?migration_id=my-migration-id
```

使用狀態請求擷取遷移 ID。如需詳細的遷移資訊，請新增 `&verbose=true`。

您可以分 10 個或更少批次，將索引從冷儲存遷移到暖儲存，最多可同時遷移 100 個索引。任何超出限制的請求都會被拒絕。若要檢查佇列中的目前遷移數目，請監控 `ColdToWarmMigrationQueueSize` 指標。遷移程序具有下列狀態：

```
ACCEPTED_MIGRATION_REQUEST - Migration request is accepted and queued.
RUNNING_INDEX_CREATION - Migration request is picked up for processing and will create
 warm indexes in the cluster.
PENDING_COLD_METADATA_CLEANUP - Warm index is created and the migration service will
 attempt to clean up cold metadata.
RUNNING_COLD_METADATA_CLEANUP - Cleaning up cold metadata from the indexes migrated to
 warm storage.
FAILED_COLD_METADATA_CLEANUP - Failed to clean up metadata in the cold tier.
FAILED_INDEX_CREATION - Failed to create an index in the warm tier.
```

從快照中還原冷索引

如果您需要還原已刪除的冷索引，可以依照中的指示將其還原回暖層，the section called “從快照還原暖索引”然後再次將索引移轉回冷層。您無法將已刪除的冷索引直接還原回冷層。 OpenSearch 服務會在刪除後保留冷索引 14 天。

取消從冷儲存遷移至暖儲存

如果從冷儲存到暖儲存的索引遷移已排入佇列或處於失敗狀態，您可以使用以下請求取消它：

```
POST _cold/migration/my-index/_cancel

{
  "acknowledged" : true
}
```

若要取消批次索引的遷移 (一次最多 10 個)，請指定遷移 ID：

```
POST _cold/migration/_cancel?migration_id=my-migration-id

{
  "acknowledged" : true
}
```

使用狀態請求擷取遷移 ID。

更新冷索引中繼資料

您可以更新冷索引的 `start_time` 和 `end_time` 欄位：

```
PATCH _cold/my-index
 {
 "start_time": "2020-01-01",
 "end_time": "2020-02-01"
 }
```

您無法更新冷儲存中的索引的 `timestamp_field`。

> **Note**
>
> OpenSearch 儀表板不支援 PATCH 方法。使用 curl、Postman 或其他方法來更新冷中繼資料。

刪除冷索引

如果您未使用 ISM 政策，您可以手動刪除冷索引。以下要求會刪除冷索引：

```
DELETE _cold/my-index

{
  "acknowledged" : true
}
```

停用冷儲存

OpenSearch 服務主控台是停用冷儲存的最簡單方法。選取網域並選擇 Actions (動作)、Edit cluster configuration (編輯叢集組態)，然後取消選取 Enable cold storage (啟用冷儲存)。

若要使用 AWS CLI 或組態 API，請在下`ColdStorageOptions`設定`"Enabled"="false"`。

停用冷儲存之前，您必須刪除所有冷索引，或將它們遷移回暖儲存，否則停用動作會失敗。

OR1Amazon 服 OpenSearch 務存儲

OR1是 Amazon Ser OpenSearch vice 的執行個體系列，可提供一種符合成本效益的方式來存放大量資料。具有OR1執行個體的網域使用 Amazon 彈性區塊存放區 (AmazonEBS) gp3 或io1磁碟區作為主要儲存，並在資料到達時同步複製到 Amazon S3。這種存儲結構提供了更高的索引輸送量和高耐用性。OR1執行個體系列也支援發生故障時的自動資料復原。如需OR1執行個體類型選項的資訊，請參閱the section called “最新一代執行個體類型”。

如果您正在執行大量操作分析工作負載 (例如日誌分析、可觀察性或安全性分析) 的索引，您可以從OR1執行個體的效能和運算效率提升中獲益。此外，OR1執行個體提供的自動資料復原功能可提升網域的整體可靠性。

OpenSearch 服務會將儲存相關OR1指標傳送至 Amazon。 CloudWatch如需可用指標的清單，請參閱???。

OR1執行個體可隨需使用，或以預留執行個體定價提供，Amazon 和 Amazon EBS S3 中佈建的執行個體和儲存按小時費率計算。

主題

- 限制
- 調整以獲得更好的擷取輸送量
- OpenSearch 最佳化執行個體與非 OpenSearch 優化執行個體有何
- 與 UltraWarm儲存空間OR1有何不同
- 使用OR1實例

限制

針對您的網域使用OR1執行個體時，請考慮下列限制。

- 新建立的網域必須執行 2.11 或更新 OpenSearch 版本。
- 現有網域必須執行 2.15 或更高 OpenSearch 版本。
- 您的網域必須啟用靜態加密。如需詳細資訊，請參閱???。
- 如果您的網域使用專用主節點，則必須使用 Graviton 執行個體。如需專用主節點的詳細資訊，請參閱???。
- OR1執行個體上索引的重新整理間隔必須為 10 秒或更高。OR1執行個體的預設重新整理間隔為 10 秒。

調整以獲得更好的擷取輸送量

若要從執行個體取得最佳的索引輸送量，建議您OR1執行下列動作：

- 使用大批量大小來提高緩衝區使用率。建議的大小為 10 MB。
- 使用多個用戶端來改善 parallel 處理效能。
- 設定使用中主要碎片的數量以符合資料節點的數目，以最大化資源使用率。

OpenSearch 最佳化執行個體與非 OpenSearch 優化執行個體有何

OpenSearch 最佳化執行個體與非 OpenSearch 最佳化執行個體的差異如下：

- OpenSearch 針對最佳化的執行個體，只會在主要碎片上執行索引。
- 如果使用複本設定 OpenSearch 最佳化執行個體，則索引速率可能會比實際的低。例如，如果有 1 個主要碎片和 1 個複本碎片，索引速率可能會顯示 1000，但實際索引速率是 2000。
- OpenSearch 最佳化的執行個體會在傳送至遠端來源之前執行緩衝區作業。這會導致更高的攝入延遲。

> **Note**
>
> `IndexingLatency`指標不會受到影響，因為它不包含同步傳輸記錄的時間。)

- 副本碎片可能在主碎片後面幾秒鐘。時間滯後可以從`ReplicationLagMaxTime`指標中看出

與 UltraWarm儲存空間OR1有何不同

OpenSearch Service 提供的 UltraWarm 執行個體是儲存大量唯讀資料的符合成本效益的方式。OR1 和 UltraWarm 執行個體都將資料存放在 Amazon 本機，EBS並在 Amazon S3 遠端存放資料。但是，OR1 UltraWarm 實例在幾個重要方面有所不同：

- OR1執行個體會在您的本機和遠端存放區中保留一份資料副本。在 UltraWarm 實例中，數據主要保存在遠程存儲中以降低存儲成本。根據您的使用模式，資料可以移至本機儲存區。
- OR1執行個體處於作用中狀態，並且可以接受讀取和寫入作業，而 UltraWarm 執行個體上的資料是唯讀的，除非您手動將它移回熱儲存區。

- UltraWarm 依賴索引快照集以確保資料持久性。OR1相較之下，執行個體會在幕後執行複寫和復原。如果出現紅色索引，OR1執行個體將自動從 Amazon S3 中的遠端儲存還原遺失的碎片。恢復時間取決於要恢復的數據量。

如需 UltraWarm 儲存體的詳細資訊，請參閱???。

使用OR1實例

建立新網域時，您可以為資料節點選取OR1執行個體 AWS Management Console，該 AWS Command Line Interface (AWS CLI)，或 AWS SDK。然後，您可以使用現有的工具對資料進行索引和查詢。

主控台

1. 瀏覽至 Amazon OpenSearch 服務主控台，位於https://console.aws.amazon.com/aos/。
2. 在左側導覽窗格中選擇 Domains (網域)。
3. 選擇建立網域。
4. 輸入網域名稱以及其他偏好選項。在「例證族群」下，選擇OR1。選擇 [建立] 以開始網域建立程序。

AWS CLI

1. 導航到您的 AWS CLI 終端。如果您需要安裝 AWS CLI，請參閱安裝或更新最新版本的 AWS CLI.
2. 若要使用OR1儲存體，您必須在建立網域時在`InstanceType`欄位中提供特定OR1執行個體類型大小的值。您還必須啟用靜態加密。

   下列範例會建立具有大小OR1執行個體的網域`2xlarge`。

```
aws opensearch create-domain \
  --domain-name test-domain \
  --engine-version OpenSearch_2.11 \
  --cluster-config
 "InstanceType=or1.2xlarge.search,InstanceCount=3,DedicatedMasterEnabled=true,DedicatedMast
 \
  --ebs-options "EBSEnabled=true,VolumeType=gp3,VolumeSize=200" \
  --encryption-at-rest-options Enabled=true \
  --advanced-security-options
 "Enabled=true,InternalUserDatabaseEnabled=true,MasterUserOptions={MasterUserName=test-
user,MasterUserPassword=test-password}" \
```

```
  --node-to-node-encryption-options Enabled=true \
  --domain-endpoint-options EnforceHTTPS=true \
  --access-policies '{"Version":"2012-10-17","Statement":
[{"Effect":"Allow","Principal":
{"AWS":"*"},"Action":"es:*","Resource":"arn:aws:es:us-east-1:account-
id:domain/test-domain/*"}]}'
```

Amazon OpenSearch 服務中的索引狀態管理

Amazon Ser OpenSearch vice 中的索引狀態管理 (ISM) 可讓您定義自動化例行任務的自訂管理政策，並將其套用至索引和索引模式。您不再需要設定和管理外部程序來執行索引操作。

政策包含預設狀態和狀態清單，供索引進行相互轉換。在每種狀態下，您可以定義要執行的操作清單和觸發這些轉換的條件。典型的使用案例是在一段時間後定期刪除舊的索引。例如，您可以定義一個政策，在 30 天後將索引移至 `read_only` 狀態，然後最終在 90 天後將索引刪除。

在您將政策連接至索引之後，ISM 會建立一個任務，每 5 至 8 分鐘 (或預先 1.3 個叢集為每 30 到 48 分鐘) 執行一次，以執行政策動作、檢查條件，然後將索引轉換為不同的狀態。執行此任務的基準時間是每 5 分鐘一次，再加上隨機的 0-60% 抖動，以確保您不會同時看到來自所有索引的活動突增。如果叢集狀態為紅色，ISM 就不會執行任務。

ISM 需要 OpenSearch 或彈性搜尋 6.8 或更新版本。

> **Note**
>
> 本文件提供 ISM 的簡要概觀以及數個範例政策。它也說明適用於 Amazon OpenSearch 服務網域的 ISM 與自我管理 OpenSearch叢集上的 ISM 有何不同。如需 ISM 的完整文件，包括完整的參數參考、每個設定的說明以及 API 參考，請參閱 OpenSearch 文件中的索引狀態管理。

> **Important**
>
> 您無法再使用索引範本將 ISM 政策套用至新建立的索引。使用 ISM 範本欄位，您可以繼續自動管理新建立的索引。此更新引入了影響使用此設定的現有 CloudFormation 範本的突破性變更。

建立 ISM 政策。

開始使用索引狀態管理

1. 打開 Amazon OpenSearch 服務控制台 https://console.aws.amazon.com/aos/home.
2. 選取您要為其建立 ISM 政策的網域。
3. 從網域的儀表板導覽至 OpenSearch 儀表板 URL，然後使用您的主要使用者名稱和密碼登入。URL 遵循以下格式：

```
domain-endpoint/_dashboards/
```

4. 開啟 OpenSearch 儀表板內的左側導覽面板，然後選擇索引管理，然後選擇建立原則。
5. 使用視覺化編輯器或 JSON 編輯器來建立政策。我們推薦使用視覺化編輯器，因為它提供一種更加結構化的政策定義方式。如需建立政策的協助，請參閱下方的範例政策。
6. 建立政策之後，請將其連接到一或多個索引：

```
POST _plugins/_ism/add/my-index
{
  "policy_id": "my-policy-id"
}
```

> **Note**
>
> 如果您的網域正在執行舊版 Elasticsearch 版本，請使用 `_opendistro` 而非 `_plugins`。

或者，在 OpenSearch 儀表板中選取索引，然後選擇套用原則。

範例政策

下列範例政策示範如何自動化常見的 ISM 使用案例。

熱至暖再至冷儲存

此範例原則會將索引從熱儲存區移至 UltraWarm，最後移至 冷庫。然後，它會刪除索引。

該索引最初位於 hot 狀態。十天之後，ISM 將其移至 warm 狀態。80 天後，索引已經超過 90 天，ISM會將索引移至 cold 狀態。一年之後，服務會將通知傳送到正在刪除索引的 Amazon Chime 空間，然後永久將其刪除。

請注意，冷索引需要 cold_delete 操作，而不是正常的 delete 操作。另請注意，資料中必須有明確的 timestamp_field，以便使用 ISM 管理冷索引。

```
{
  "policy": {
    "description": "Demonstrate a hot-warm-cold-delete workflow.",
    "default_state": "hot",
    "schema_version": 1,
    "states": [{
        "name": "hot",
        "actions": [],
        "transitions": [{
          "state_name": "warm",
          "conditions": {
            "min_index_age": "10d"
          }
        }]
      },
      {
        "name": "warm",
        "actions": [{
          "warm_migration": {},
          "retry": {
            "count": 5,
            "delay": "1h"
          }
        }],
        "transitions": [{
          "state_name": "cold",
          "conditions": {
            "min_index_age": "90d"
          }
        }]
      },
      {
        "name": "cold",
        "actions": [{
            "cold_migration": {
              "timestamp_field": "<your timestamp field>"
```

```
            }
          }
        ],
        "transitions": [{
          "state_name": "delete",
          "conditions": {
             "min_index_age": "365d"
          }
        }]
      },
      {
        "name": "delete",
        "actions": [{
          "notification": {
            "destination": {
              "chime": {
                "url": "<URL>"
              }
            },
            "message_template": {
              "source": "The index {{ctx.index}} is being deleted."
            }
          }
        },
        {
          "cold_delete": {}
        }]
      }
    ]
  }
}
```

減少複本計數

此範例政策會在七天後將複本計數縮減至零以保留磁碟空間，然後在 21 天後刪除索引。此政策會假設索引不重要且不再接收寫入請求；擁有零個複本會伴隨某種程度的資料遺失風險。

```
{
  "policy": {
    "description": "Changes replica count and deletes.",
    "schema_version": 1,
    "default_state": "current",
    "states": [{
```

```
        "name": "current",
        "actions": [],
        "transitions": [{
          "state_name": "old",
          "conditions": {
            "min_index_age": "7d"
          }
        }]
      },
      {
        "name": "old",
        "actions": [{
          "replica_count": {
            "number_of_replicas": 0
          }
        }],
        "transitions": [{
          "state_name": "delete",
          "conditions": {
            "min_index_age": "21d"
          }
        }]
      },
      {
        "name": "delete",
        "actions": [{
          "delete": {}
        }],
        "transitions": []
      }
    ]
  }
}
```

拍攝索引快照

此範例政策會使用 `snapshot` 操作在索引包含至少一個文件時立即拍攝快照。`repository` 是您在 Simple Storage Service (Amazon S3) 中註冊的手動快照儲存庫的名稱。`snapshot` 是快照的名稱。如需快照必要條件和註冊儲存庫的步驟，請參閱the section called “建立索引快照”。

```
{
  "policy": {
    "description": "Takes an index snapshot.",
```

```
    "schema_version": 1,
    "default_state": "empty",
    "states": [{
        "name": "empty",
        "actions": [],
        "transitions": [{
          "state_name": "occupied",
          "conditions": {
            "min_doc_count": 1
          }
        }]
      },
      {
        "name": "occupied",
        "actions": [{
          "snapshot": {
            "repository": "<my-repository>",
            "snapshot": "<my-snapshot>"
            }
          }],
          "transitions": []
      }
    ]
  }
}
```

ISM 範本

您可以在政策中設定 `ism_template` 欄位，以便當您建立符合範本模式的索引時，該政策可自動連接至該索引。在此範例中，您建立的名稱以 "log" 開頭的任何索引都會自動匹配 ISM 政策 `my-policy-id`：

```
PUT _plugins/_ism/policies/my-policy-id
{
  "policy": {
    "description": "Example policy.",
    "default_state": "...",
    "states": [...],
    "ism_template": {
      "index_patterns": ["log*"],
      "priority": 100
    }
  }
```

```
}
```

如需更詳細的範例，請參閱使用 ISM 範本進行自動變換的範例政策。

差異

OpenSearch 與彈性搜索相比，Amazon OpenSearch 服務的 ISM 有幾個區別。

ISM 操作

- OpenSearch 服務支援三種獨特的 ISM 作業`warm_migration``cold_migration`、、和`cold_delete`：
  - 如果您的網域已UltraWarm啟用，`warm_migration`動作會將索引轉換為暖儲存。
  - 如果您的網域啟用了冷儲存，`cold_migration` 動作會將索引轉換為冷儲存，而 `cold_delete` 動作則會從冷存儲中刪除索引。

  即使其中一個動作沒有在設定的逾時期限內完成，仍會繼續遷移至熱索引。針對上述其中一個動作設定一個 error_notification，如果動作未在逾時期限內完成，會通知您該動作失敗，但該通知僅供您自己參考。實際操作沒有固有的逾時，會在最終成功或失敗之前持續執行。
- 如果您的網域執行 OpenSearch 或彈性搜尋 7.4 或更新版本，則 OpenSearch 服務支援 ISM `open` 和`close`作業。
- 如果您的網域執行 OpenSearch 或彈性搜尋 7.7 或更新版本，則 OpenSearch 服務支援 ISM `snapshot` 作業。

冷儲存 ISM 操作

對於冷索引，當您使用下列 ISM API 時，必須指定 `?type=_cold` 參數：

- 新增政策
- 移除政策
- 更新政策
- 重試失敗的索引
- 解釋索引

這些適用於冷索引的 API 具有以下其他不同之處：

- 不支援萬用字元運算子，除非您在結尾處使用。例如，支援 `_plugins/_ism/<add, remove, change_policy, retry, explain>/logstash-*|`，但不支援 `_plugins/_ism/<add, remove, change_policy, retry, explain>/iad-*-prod`。
- 不支援多行索引名稱和模式。例如，支援 `_plugins/_ism/<add, remove, change_policy, retry, explain>/app-logs|`，但不支援 `_plugins/_ism/<add, remove, change_policy, retry, explain>/app-logs,sample-data`。

ISM 設定

OpenSearch 而彈性搜尋可讓您使用 API 變更所有可用的 `_cluster/settings` ISM 設定。在 Amazon OpenSearch 服務上，您只能變更下列 ISM 設定：

- 叢集層級設定：
  - `plugins.index_state_management.enabled`
  - `plugins.index_state_management.history.enabled`
- 索引層級設定：
  - `plugins.index_state_management.rollover_alias`

教學課程：自動化索引狀態管理程序

本教學課程示範如何實作 ISM 政策，該政策可自動化例行索引管理任務並將它們套用至索引和索引模式。

Amazon Ser OpenSearch vice 中的索引狀態管理 (ISM) 可讓您自動執行週期性索引管理活動，因此您可以避免使用其他工具來管理索引生命週期。您可以建立一個政策，根據索引期限、大小和其他條件自動執行這些操作，全部來自 Amazon Ser OpenSearch vice 網域。

OpenSearch 服務支援三個儲存層：用於主動寫入的預設「熱」狀態和低延遲分析、最高三 PB UltraWarm 的唯讀資料，以及冷儲存 (無限制的長期封存)。

本教學課程提供在每日索引中處理時間序列資料的範例使用案例。在本教學課程中，您可設定政策，以在 24 小時後拍攝每個所連接索引的自動快照。然後，它會在兩天後將索引從預設的熱狀態移轉至 UltraWarm 儲存區，30 天後進行冷儲存，最後在 60 天後刪除索引。

必要條件

- 您的 OpenSearch 服務網域必須執行版本 6.8 或更新版本。

- 您的網域必須已啟用UltraWarm並啟用冷儲存。
- 必須為您的網域註冊手動快照儲存庫。
- 您的使用者角色需要足夠的權限才能存取 OpenSearch 服務主控台。如有必要，請驗證並設定網域的存取權。

步驟 1：設定 ISM 政策

首先，在 OpenSearch 儀表板中設定 ISM 原則。

1. 從 OpenSearch 服務主控台中的網域儀表板，導覽至 OpenSearch 儀表板 URL，然後使用您的主要使用者名稱和密碼登入。URL 遵循此格式：*domain-endpoint*/_dashboards/。
2. 在 OpenSearch 儀表板中，選擇 [新增範例資料]，然後將一或多個範例索引新增至您的網域。
3. 開啟左側導覽面板，然後依序選擇 Index Management (索引管理) 和 Create policy (建立政策)。
4. 將政策命名為 `ism-policy-example`。
5. 將預設政策取代為以下政策：

```
{
  "policy": {
    "description": "Move indexes between storage tiers",
    "default_state": "hot",
    "states": [
      {
        "name": "hot",
        "actions": [],
        "transitions": [
          {
            "state_name": "snapshot",
            "conditions": {
              "min_index_age": "24h"
            }
          }
        ]
      },
      {
        "name": "snapshot",
        "actions": [
          {
            "retry": {
              "count": 5,
              "backoff": "exponential",
```

```
              "delay": "30m"
            },
            "snapshot": {
              "repository": "snapshot-repo",
              "snapshot": "ism-snapshot"
            }
          }
        ],
        "transitions": [
          {
            "state_name": "warm",
            "conditions": {
              "min_index_age": "2d"
            }
          }
        ]
      },
      {
        "name": "warm",
        "actions": [
          {
            "retry": {
              "count": 5,
              "backoff": "exponential",
              "delay": "1h"
            },
            "warm_migration": {}
          }
        ],
        "transitions": [
          {
            "state_name": "cold",
            "conditions": {
              "min_index_age": "30d"
            }
          }
        ]
      },
      {
        "name": "cold",
        "actions": [
          {
            "retry": {
              "count": 5,
```

```
              "backoff": "exponential",
              "delay": "1h"
            },
            "cold_migration": {
              "start_time": null,
              "end_time": null,
              "timestamp_field": "@timestamp",
              "ignore": "none"
            }
          }
        ],
        "transitions": [
          {
            "state_name": "delete",
            "conditions": {
              "min_index_age": "60d"
            }
          }
        ]
      },
      {
        "name": "delete",
        "actions": [
          {
            "cold_delete": {}
          }
        ],
        "transitions": []
      }
    ],
    "ism_template": [
      {
        "index_patterns": [
          "index-*"
        ],
        "priority": 100
      }
    ]
  }
}
```

> **Note**
>
> `ism_template` 欄位會自動將政策連接至符合其中一個指定 `index_patterns` 的任何新建立的索引。在此案例中，則為所有以 `index-` 開頭的索引。您可以修改此欄位以符合環境中的索引格式。如需詳細資訊，請參閱 ISM 範本。

6. 在政策的 `snapshot` 區段中,將 *`snapshot-repo`* 取代為您為網域註冊的快照儲存庫的名稱。您也可以選擇取代 *`ism-snapshot`*，這將是建立快照時的名稱。
7. 選擇建立。現在可以在 State management policies (狀態管理政策) 頁面上看到該政策。

步驟 2：將政策連接至一個或多個索引

既然您已建立政策，請將其連接至叢集中的一個或多個索引。

1. 轉至 Hot indicies (熱索引) 標籤並搜尋 `opensearch_dashboards_sample`，這會列出您在步驟 1 中新增的所有範例索引。
2. 選取所有索引並選擇 [套用原則]，然後選擇您剛建立的ism-policy-example原則。
3. 選擇套用。

您可以在 Policy managed indices (政策管理的索引) 頁面上監控索引在各種狀態間的移動。

總結 Amazon OpenSearch 服務中的索引與索引匯總

Amazon Ser OpenSearch vice 中的索引彙總可讓您定期將舊資料彙總成摘要索引，以降低儲存成本。

您可以選擇感興趣的欄位，並使用索引彙總來建立一個新的索引，其中只有這些欄位彙總到更粗糙的時間儲存貯體。您可以很低的成本存放幾個月或幾年的歷史資料，且擁有相同的查詢效能。

索引彙總需要 OpenSearch 或彈性搜索 7.9 或更高版本。

> **Note**
>
> 本文件可協助您開始在 Amazon OpenSearch 服務中建立索引彙總任務。如需完整文件，包括所有可用設定的清單和完整 API 參考資料，請參閱文件中的索引彙總套件 OpenSearch 。

建立索引彙總任務

若要開始使用，請選擇 OpenSearch儀表板中的索引管理。選取 Rollup Jobs (彙總任務)，然後選擇 Create rollup job (建立彙總任務)。

步驟 1：設定索引

設定來源索引和目標索引。來源索引是您想要彙總的索引。目標索引是儲存索引彙總結果的位置。

建立索引彙總任務之後，您無法變更索引選擇。

步驟 2：定義彙總和指標

選取含有您要總計之彙總 (詞彙和直方圖) 和指標 (平均、總和、最大值、最小值和值計數) 的屬性。確保沒有新增很多高精細屬性，因為不會節省太多空間。

步驟 3：指定排程

指定排程，以便在擷取索引時進行彙總。預設啟用索引彙總任務。

步驟 4：檢閱和建立

檢閱您的組態，然後選取 Create (建立)。

步驟 5：搜尋目標索引

您可以使用標準 `_search` API 來搜尋目標索引。您無法存取目標索引中資料的內部結構，因為外掛程式會自動在後台重寫查詢以適應目標索引。這是為了確保您可以對來源索引和目標索引使用相同的查詢。

若要查詢目標索引，請將 `size` 設定為 0：

```
GET target_index/_search
{
  "size": 0,
  "query": {
    "match_all": {}
  },
  "aggs": {
    "avg_cpu": {
      "avg": {
```

```
        "field": "cpu_usage"
      }
    }
  }
}
```

> **Note**
>
> OpenSearch 2.2 版及更高版本支持在一個請求中搜索多個彙總索引。 OpenSearch 2.2 之前的版本和舊版 Elasticsearch OSS 版本僅支援每個搜尋一個彙總索引。

轉換 Amazon OpenSearch 服務中的索引

索引彙總工作可讓您透過將舊資料彙總為精簡索引來減少資料粒度，而轉換工作則可讓您針對以特定欄位為中心的資料建立不同的摘要檢視，以便您以不同的方式視覺化或分析資料。

索引轉換具有 OpenSearch 儀表板使用者介面和 REST API。此功能需要 OpenSearch 1.0 或更新版本。

> **Note**
>
> 本文件提供索引轉換的簡要概觀，以協助您開始在 Amazon OpenSearch 服務網域上使用它。如需完整文件和 REST API 參考資料，請參閱開放原始碼 OpenSearch 文件中的索引轉換。

建立索引轉換任務

如果您的叢集中沒有任何資料，請使用 OpenSearch 儀表板中的範例飛行資料來嘗試轉換工作。新增資料後，啟動 OpenSearch 儀表板。然後依次選擇 Index Management (索引管理)、Transform Jobs (轉換任務) 以及 Create Transform Job (建立轉換任務)。

步驟 1：選擇索引

在 Indices (索引) 區段中，選取來源索引和目標索引。您可以選取現有目標索引，也可以輸入目標索引的名稱來建立新的目標索引。

如果您只想轉換來源索引的子集，請選擇 [新增資料篩選器]，然後使用 OpenSearch 查詢 DSL 來指定來源索引的子集。

步驟 2：選擇欄位

選擇索引之後，請選擇要在轉換工作中使用的欄位，以及是否要使用分組或彙總。

- 您可以使用分組將資料放入轉換索引中的單獨儲存貯體中。例如，如果您想要對範例航班資料中的所有機場目的地進行分組，請將 `DestAirportID` 欄位分組到 `DestAirportID_terms` 欄位的目標欄位中，在轉換任務完成後，您可以在已轉換的索引中找到已分組的機場 ID。
- 另一方面，彙總可讓您執行簡單的計算。例如，您可能會在轉換任務中包含彙總，以定義計算所有機票總和的新欄位 `sum_of_total_ticket_price`。然後，您可以分析已轉換索引中的新資料。

步驟 3：指定排程

轉換任務預設為啟用，並依排程執行。若要轉換執行間隔，請以分鐘、小時或天數來指定間隔。

步驟 4：檢閱和監控

檢閱您的組態，然後選取 Create (建立)。然後監控 Transform job status (轉換任務狀態) 欄。

步驟 5：搜尋目標索引

任務完成後，您可以使用標準 `_search` API 來搜尋目標索引。

例如，在執行根據 `DestAirportID` 欄位轉換航班資料的轉換任務後，您可以執行下列請求以傳回值為 `SFO` 的所有欄位：

```
GET target_index/_search
{
  "query": {
    "match": {
      "DestAirportID_terms" : "SFO"
    }
  }
}
```

Amazon OpenSearch 服務的跨叢集複寫

透過 Amazon Ser OpenSearch vice 中的跨叢集複寫，您可以將使用者索引、對應和中繼資料從一個 OpenSearch 服務網域複寫到另一個服務網域。使用跨叢集複寫有助於確保災難復原是否會中斷，並可讓您跨遠距資料中心複寫資料，以減少延遲。您需要為網域之間傳輸的 AWS 資料支付標準的資料傳輸費用。

跨叢集複寫遵循主動-被動複寫模型，其中本機或從動件索引從遠端或前置索引提取資料。領導者索引是指資料的來源，或您要從中複製資料的索引。追隨者索引是指資料的目標，或您要複製資料的索引。

跨叢集複寫可在執行彈性搜尋 7.10 或 OpenSearch 更新版本的網域上使用。

> **Note**
>
> 本文件說明如何從 Amazon OpenSearch 服務的角度設定跨叢集複寫。這包括使用 AWS Management Console 來設定跨叢集連線，這在自我管理 OpenSearch 叢集上是不可能的。如需完整文件，包括設定參考和完整的 API 參考資料，請參閱 OpenSearch 文件中的跨叢集複寫。

主題

- 限制
- 必要條件
- 許可需求
- 設定跨叢集連線
- 開始複寫
- 確認複寫
- 暫停和繼續複寫
- 停止複寫
- 自動追蹤
- 升級連線的網域

限制

跨叢集複寫有下列限制：

- 您無法在 Amazon OpenSearch 服務網域和自我管理叢集 OpenSearch 或彈性搜尋叢集之間複寫資料。
- 您無法將追隨者網域的索引複製到另一個追隨者網域。如果您想要將索引複製到多個追隨者網域，則只能從單一引線領域複製索引。
- 一個網域可以透過傳入和傳出連線的組合，連線到最多 20 個其他網域。
- 當您初始設定跨叢集連線時，領導網域的版本必須與追隨者網域相同或更高。

- 您無法使用 AWS CloudFormation 來連線網域。
- 您無法在 M3 或高載 (T2 和 T3) 執行個體上使用跨叢集複寫。
- 您無法在索引 UltraWarm 或冷索引之間複製資料。兩個索引都必須位於熱儲存中。
- 當您從領導者網域刪除索引時，不會自動刪除追隨者網域上的對應索引。

必要條件

設定跨叢集複寫前，請確認網域符合下列需求：

- 彈性搜尋 7.10 或 1.1 或 OpenSearch 更新版本
- 已啟用精細存取控制
- N ode-to-node 加密已啟用

許可需求

若要開始複寫，您必須在遠端 (領導) 網域上提供 `es:ESCrossClusterGet` 許可。我們建議您在遠端網域上採用下列 IAM 政策。此原則也可讓您執行其他作業，例如索引文件和執行標準搜尋：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "*"
        ]
      },
      "Action": [
        "es:ESHttp*"
      ],
      "Resource": "arn:aws:es:region:account:domain/leader-domain/*"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "*"
      },
      "Action": "es:ESCrossClusterGet",
```

```
      "Resource": "arn:aws:es:region:account:domain/leader-domain"
    }
  ]
}
```

確認已針對 `/leader-domain` (而不是 `/leader-domain/*`) 套用 `es:ESCrossClusterGet` 許可。

為了讓非管理員使用者執行複寫活動，他們也必須對應至適當的許可。大多數許可均對應特定的 REST API 操作。例如，`indices:admin/plugins/replication/index/_resume` 許可能讓您恢復索引複寫。如需權限的完整清單，請參閱 OpenSearch 文件中的複寫權限。

> **Note**
>
> 開始複寫和建立複寫規則的命令屬於特殊情況。因為它們會在領導者和追隨者網域上叫用背景處理序，因此您必須在要求`follower_cluster_role`中傳遞`leader_cluster_role`和。OpenSearch 服務會在所有後端複寫工作中使用這些角色。如需有關對應和使用這些角色的資訊，請參閱 OpenSearch文件中的對應領導者和追隨者叢集角色。

設定跨叢集連線

若要將索引從一個網域複寫到另一個網域，您需要設定網域之間的跨叢集連線。連線網域最簡單的方法是透過網域儀表板的 Connections (連線) 索引標籤。您也可以使用組態 API 或 AWS CLI。因為跨叢集複寫遵循「提取」模型，您會從追蹤網域啟動連線。

> **Note**
>
> 如果您先前已連線兩個網域以執行跨叢集搜尋，則無法使用相同的連線進行複寫。在主控台中，連線將標記為 `SEARCH_ONLY`。若要在兩個之前連線的網域之間執行複寫，您必須刪除連線，再重新建立連線。完成此操作後，該連線可用於跨叢集搜尋和跨叢集複寫。

如何設定連線

1. 在 Amazon OpenSearch 服務主控台中，選取追蹤者網域，前往「連線」標籤，然後選擇「請求」。
2. 對於 Connection alias (連線別名)，輸入連線的名稱。

3. 選擇連線至您 AWS 帳戶 和區域或其他帳戶或區域中的網域。

   - 若要連線至您 AWS 帳戶 和區域中的網域，請選取網域，然後選擇 [要求]。
   - 若要連線至其他網域 AWS 帳戶 或區域中的網域，請指定遠端網域的 ARN，然後選擇 [要求]。

OpenSearch 服務會驗證連線要求。如果網域不相容，連線會失敗。如果驗證成功，則會將請求傳送至目的地網域進行核准。當目的地網域核准請求時，您就可以開始複寫。

跨叢集複寫支援雙向複寫。這表示您可以建立從網域 A 到網域 B 的輸出連線，並建立另一個從網域 B 到網域 A 的輸出連線。然後您可以設定複寫，讓網域 A 跟隨網域 B 中的索引，而網域 B 會跟隨網域 A 中的索引。

開始複寫

建立跨叢集連線之後，您就可以開始複寫資料。首先，在主導領域上建立要複寫的索引：

```
PUT leader-01
```

若要複寫該索引，請將此命令傳送至追蹤網域：

```
PUT _plugins/_replication/follower-01/_start
{
   "leader_alias": "connection-alias",
   "leader_index": "leader-01",
   "use_roles":{
      "leader_cluster_role": "all_access",
      "follower_cluster_role": "all_access"
   }
}
```

您可以在網域儀表板的 Connections (連線) 索引標籤上找到連線別名。

為了簡單起見，此範例假設管理員發出請求，並針對 `leader_cluster_role` 和 `follower_cluster_role` 使用 `all_access`。不過，在生產環境中，我們建議您同時在領導和追蹤索引上建立複寫使用者，並加以對應。使用者名稱必須相同。如需這些角色以及如何對應這些角色的詳細資訊，請參閱 OpenSearch文件中的對應領導者和追隨者叢集角色。

確認複寫

若要確認正在進行複寫，請取得複寫狀態：

```
GET _plugins/_replication/follower-01/_status

{
  "status" : "SYNCING",
  "reason" : "User initiated",
  "leader_alias" : "connection-alias",
  "leader_index" : "leader-01",
  "follower_index" : "follower-01",
  "syncing_details" : {
    "leader_checkpoint" : -5,
    "follower_checkpoint" : -5,
    "seq_no" : 0
  }
}
```

領導和追蹤檢查點的值以負整數開始，並反映您擁有的碎片數量 (-1 代表一個碎片，-5 代表五個碎片，依此類推)。這些值會隨著您所做的每項變更而遞增為正整數。如果值是相同的，表示索引已完全同步。您可以使用這些檢查點的值來測量跨網域的複寫延遲。

若要進一步驗證複寫，請將文件新增至領導索引：

```
PUT leader-01/_doc/1
{
   "Doctor Sleep":"Stephen King"
}
```

同時確認文件顯示在追蹤索引上：

```
GET follower-01/_search

{
    ...
    "max_score" : 1.0,
    "hits" : [
      {
        "_index" : "follower-01",
        "_type" : "_doc",
        "_id" : "1",
        "_score" : 1.0,
        "_source" : {
          "Doctor Sleep" : "Stephen King"
        }
```

```
      }
    ]
  }
}
```

暫停和繼續複寫

如果您需要修復問題或減少領導網域的負載，可以暫時停止複寫。將此請求傳送至追蹤網域。請務必包含空的請求主體：

```
POST _plugins/_replication/follower-01/_pause
{}
```

隨後獲取狀態，確保複寫已暫停：

```
GET _plugins/_replication/follower-01/_status

{
  "status" : "PAUSED",
  "reason" : "User initiated",
  "leader_alias" : "connection-alias",
  "leader_index" : "leader-01",
  "follower_index" : "follower-01"
}
```

當您完成變更後，請繼續複寫。將此請求傳送至追蹤網域。請務必包含空的請求主體：

```
POST _plugins/_replication/follower-01/_resume
{}
```

您無法在已暫停超過 12 小時後繼續複寫。您必須停止複寫、刪除追蹤者索引，然後重新啟動領導者的複寫。

停止複寫

當您完全停止複寫時，追蹤索引會取消追蹤領導索引，並成為標準索引。停止複寫後，就無法重新開始複寫。

從追蹤網域停止複寫。請務必包含空的請求主體：

```
POST _plugins/_replication/follower-01/_stop
{}
```

自動追蹤

您可以針對單一領導領域定義一組複寫規則，以自動複寫符合指定模式的索引。當領導網域上的索引符合其中一個模式 (例如，books*) 時，會在追隨者網域上建立相符的追隨者索引。 OpenSearch Service 會複寫符合模式的任何現有索引，以及您建立的新索引。不會複寫追隨網域上已經存在的索引。

若要複寫所有索引 (系統建立的索引以及追隨網域上已存在的索引除外)，應使用萬用字元 (*) 模式。

建立複寫規則

在追蹤網域上建立複寫規則，並指定跨叢集連線的名稱：

```
POST _plugins/_replication/_autofollow
{
   "leader_alias" : "connection-alias",
   "name": "rule-name",
   "pattern": "books*",
   "use_roles":{
      "leader_cluster_role": "all_access",
      "follower_cluster_role": "all_access"
   }
}
```

您可以在網域儀表板的 Connections (連線) 索引標籤上找到連線別名。

為了簡單起見，此範例假設管理員發出請求，並使用 `all_access` 作為領導和追蹤網域角色。不過，在生產環境中，我們建議您同時在領導和追蹤索引上建立複寫使用者，並加以對應。使用者名稱必須相同。如需這些角色以及如何對應這些角色的詳細資訊，請參閱 OpenSearch文件中的對應領導者和追隨者叢集角色。

若要擷取網域上現有複寫規則的清單，請使用自動追蹤統計 API 操作。

若要測試規則，請建立與領導網域上模式相符的索引：

```
PUT books-are-fun
```

同時檢查索引副本是否出現在追蹤網域上：

```
GET _cat/indices

health status index          uuid                    pri rep docs.count docs.deleted
 store.size pri.store.size
green  open   books-are-fun  ldfHO78xYYdxRMULuiTvSQ     1   1          0            0
     208b           208b
```

刪除複寫規則

刪除複寫規則時， OpenSearch Service 會停止複寫符合模式的新索引，但會繼續現有的複寫活動，直到您停止複寫這些索引為止。

從追蹤網域刪除複寫規則：

```
DELETE _plugins/_replication/_autofollow
{
   "leader_alias" : "connection-alias",
   "name": "rule-name"
}
```

升級連線的網域

若要升級具有跨叢集連線之兩個網域的引擎版本，請先升級追隨者網域，然後升級領導者網域。請勿刪除它們之間的連線，否則複寫會暫停，您將無法繼續。

使用遠端重新索引遷移 Amazon OpenSearch 服務索引

遠端重新索引可讓您將索引從一個 Amazon OpenSearch 服務網域複製到另一個網域。您可以從任何 OpenSearch 服務網域或自我管理 OpenSearch 和 Elasticsearch 叢集移轉索引。

遠端網域和索引是指資料的來源，或您要從中複製資料的網域和索引。本機網域和索引是指資料的目標，或是您要將資料複製到的網域和索引。

遠端重新建立索引需要 OpenSearch 1.0 或更新版本，或在本機網域上使用彈性搜尋 6.7 或更新版本。遠端網域必須與本機網域較低或相同的主要版本。Elasticsearch 版本被認為低於 OpenSearch 版本，這意味著您可以將數據從 Elasticsearch 域重新索引到域。 OpenSearch 在相同的主要版本中，遠端網域可以是任何次要版本。例如，支持從彈性搜索 7.10.x 到 7.9 的遠程重新索引，但不支持 OpenSearch 1.0 到彈性搜索 7.10.x。

> **Note**
>
> 本文件說明如何在 Amazon OpenSearch 服務網域之間重新索引資料。如需`reindex`作業的完整文件，包括詳細步驟和支援的選項，請參閱文件中的重新建立索引文件。 OpenSearch

主題

- 必要條件
- 重新索引 OpenSearch 服務互聯網域之間的數據
- 當遠端位於 VPC 中時，重新索引 OpenSearch 服務網域之間的資料
- 重新索引非OpenSearch 服務網域之間的資料
- 重新索引大型資料集
- 遠端重新索引設定

必要條件

遠端重新索引有以下要求：

- 遠端網域必須可從本機網域存取。對於位於 VPC 內的遠端網域，本機網域必須具有 VPC 的存取權。此程序會因網路組態而異，但可能涉及連線至 VPN 或受管理網路，或使用原生 VPC 端點連線。如需進一步了解，請參閱the section called “VPC支持”。
- 要求必須由遠端網域授權，就像任何其他 REST 要求一樣。如果遠端網域啟用了精細的存取控制，您必須擁有在遠端網域上執行重新索引並讀取本機網域上索引的權限。如需更多安全性考量，請參閱the section called “精細定義存取控制”。
- 建議您在開始重新建立索引程序之前，在本機網域上建立具有所需設定的索引。
- 如果您的網域為資料節點使用 T2 或 T3 執行個體類型，則無法使用遠端重新索引。

重新索引 OpenSearch 服務互聯網域之間的數據

最基本的案例是，遠端索引與具有可公開存取端點的本機網域相同 AWS 區域 ，而且您已簽署 IAM 登入資料。

在遠端網域中，指定要重新建立索引的來源遠端索引，以及要重新建立索引的本機索引：

```
POST _reindex
{
```

```
  "source": {
    "remote": {
      "host": "https://remote-domain-endpoint:443"
    },
    "index": "remote_index"
  },
  "dest": {
    "index": "local_index"
  }
}
```

您必須在遠端網域端點的結尾新增 443，才能進行驗證檢查。

若要確認索引是否已複製到本機網域，請將此要求傳送至本機網域：

```
GET local_index/_search
```

如果遠端索引位於與本機網域不同的地區，請傳入其區域名稱，例如以下請求範例：

```
POST _reindex
{
  "source": {
    "remote": {
      "host": "https://remote-domain-endpoint:443",
      "region": "eu-west-1"
    },
    "index": "remote_index"
  },
  "dest": {
    "index": "local_index"
  }
}
```

如果是隔離的區域 (例如 AWS GovCloud (US) 中國區域)，端點可能無法存取，因為在這些區域中無法辨識您的 IAM 使用者。

如果遠端網域以基本驗證保護，請指定使用者名稱和密碼：

```
POST _reindex
{
  "source": {
    "remote": {
      "host": "https://remote-domain-endpoint:443",
```

```
      "username": "username",
      "password": "password"
    },
    "index": "remote_index"
  },
  "dest": {
    "index": "local_index"
  }
}
```

當遠端位於 VPC 中時，重新索引 OpenSearch 服務網域之間的資料

每個 OpenSearch 服務網域都是由其自己的內部虛擬私有雲 (VPC) 基礎結構組成。當您在現有的 OpenSearch Service VPC 中建立新網域時，會為 VPC 中的每個資料節點建立 elastic network interface。

由於遠端重新建立索引作業是從遠端 OpenSearch 服務網域執行，因此在其本身的私有 VPC 內執行，因此您需要一種方法來存取本機網域的 VPC。您可以透過使用內建 VPC 端點連線功能建立連線 AWS PrivateLink，或透過設定 Proxy 來執行此操作。

如果您的本機網域使用 1.0 或更新 OpenSearch 版本，您可以使用主控台或建立 AWS PrivateLink 連線。 AWS CLI AWS PrivateLink 連線可讓本機 VPC 中的資源私有連線至遠端 VPC 中的資源。 AWS 區域

使用重新索引資料 AWS Management Console

您可以搭配主控台使用遠端重新索引，在共用 VPC 端點連線的兩個網域之間複製索引。

1. 瀏覽至 Amazon OpenSearch 服務主控台，位於https://console.aws.amazon.com/aos/。
2. 在左側導覽窗格中選擇 Domains (網域)。
3. 選取要將資料複製到的本機網域或網域。這會開啟網域詳細資訊頁面。選擇一般資訊下方的「連線」標籤，然後選擇「要求」。
4. 在 [要求連線] 頁面上，為您的連線模式選取 [VPC 端點連線]，然後輸入其他相關詳細資料。這些詳細資料包括遠端網域，也就是您要從中複製資料的網域。然後，選擇 Request (請求)。
5. 瀏覽至遠端網域的詳細資訊頁面，選擇「連線」標籤，然後找到「輸入連線」表格。選取剛剛從中建立連線的網域名稱 (本機網域) 旁的核取方塊。選擇 Approve (核准)。
6. 瀏覽至本機網域，選擇 Connections (連線) 標籤，然後找到 Outbound connections (傳出連線) 資料表。兩個網域之間的連線處於作用中狀態之後，資料表 Endpoint (端點) 欄中的端點就會變為可用。複製端點。

7. 開啟本機網域的儀表板，然後在左側導覽中選擇 Dev Tools (開發工具)。若要確認遠端網域索引尚未存在於您的本機網域中，請執行下列 GET 要求。替換*remote-domain-index-name*為您自己的索引名稱。

```
GET remote-domain-index-name/_search
{
   "query":{
      "match_all":{}
   }
}
```

在輸出中，您應該會看到一個錯誤，指出未找到索引。

8. 如下所示，在 GET 請求下方，建立 POST 要求並使用端點作為遠端主機。

```
POST _reindex
{
   "source":{
      "remote":{
         "host":"connection-endpoint",
         "username":"username",
         "password":"password"
      },
      "index":"remote-domain-index-name"
   },
   "dest":{
      "index":"local-domain-index-name"
   }
}
```

執行此請求。

9. 再次執行 GET 請求。輸出現在應指出本機索引的存在。您可以查詢此索引，以驗證是否已 OpenSearch複製遠端索引中的所有資料。

使用 OpenSearch 服務 API 作業重新建立資料索引

您可以搭配 API 使用遠端重新索引，在共用 VPC 端點連線的兩個網域之間複製索引。

1. 使用 CreateOutboundConnectionAPI 作業可要求從本機網域到遠端網域的新連線。

```
POST https://es.region.amazonaws.com/2021-01-01/opensearch/cc/outboundConnection
```

```
{
   "ConnectionAlias": "remote-reindex-example",
   "ConnectionMode": "VPC_ENDPOINT",
   "LocalDomainInfo": {
      "AWSDomainInformation": {
         "DomainName": "local-domain-name",
         "OwnerId": "aws-account-id",
         "Region": "region"
      }
   },
   "RemoteDomainInfo": {
      "AWSDomainInformation": {
         "DomainName": "remote-domain-name",
         "OwnerId": "aws-account-id",
         "Region": "region"
      }
   }
}
```

您會在回應`ConnectionId`中收到。儲存此 ID 以在下一個步驟中使用。

2. 使用 AcceptInboundConnectionAPI 作業搭配您的連線 ID 來核准來自本機網域的要求。

```
PUT https://es.region.amazonaws.com/2021-01-01/opensearch/cc/
inboundConnection/ConnectionId/accept
```

3. 使用 DescribeOutboundConnectionsAPI 作業擷取遠端網域的端點。

```
{
    "Connections": [
        {
            "ConnectionAlias": "remote-reindex-example",
            "ConnectionId": "connection-id",
            "ConnectionMode": "VPC_ENDPOINT",
            "ConnectionProperties": {
                "Endpoint": "connection-endpoint"
            },
            ...
        }
    ]
}
```

儲存要在步驟 *5 #######*。

4. 若要確認遠端網域索引尚未存在於您的本機網域中，請執行下列 GET 要求。替換*remote-domain-index-name*為您自己的索引名稱。

```
GET local-domain-endpoint/remote-domain-index-name/_search
{
   "query":{
      "match_all":{}
   }
}
```

在輸出中，您應該會看到一個錯誤，指出未找到索引。

5. 建立 POST 要求並使用您的端點做為遠端主機，如下所示。

```
POST local-domain-endpoint/_reindex
{
   "source":{
      "remote":{
         "host":"connection-endpoint",
         "username":"username",
         "password":"password"
      },
      "index":"remote-domain-index-name"
   },
   "dest":{
      "index":"local-domain-index-name"
   }
}
```

執行此請求。

6. 再次執行 GET 請求。輸出現在應指出本機索引的存在。您可以查詢此索引，以驗證是否已 OpenSearch複製遠端索引中的所有資料。

如果遠端網域託管在 VPC 內，而您不想使用 VPC 端點連線功能，則必須使用可公開存取的端點設定 Proxy。在此情況下， OpenSearch Service 需要公用端點，因為它無法將流量傳送到 VPC。

在 VPC 模式下執行網域時，VPC 中會放置一個或多個端點。但是，這些端點僅適用於進入 VPC 內網域的流量，並且不允許流量進入 VPC 本身。

遠端 reindex 命令是從本機網域執行，因此原始流量無法使用這些端點存取遠端網域。這就是為什麼在這個用例中需要代理。代理網域必須擁有由公有憑證授權單位 (CA) 所簽署的憑證。不支援自我簽署或私有 CA 簽署憑證。

重新索引非OpenSearch 服務網域之間的資料

如果遠端索引託管在 OpenSearch 服務之外，就像在自我管理 EC2 執行個體中一樣，請將`external`參數設定為`true`：

```
POST _reindex
{
  "source": {
    "remote": {
      "host": "https://remote-domain-endpoint:443",
      "username": "username",
      "password": "password",
      "external": true
    },
    "index": "remote_index"
  },
  "dest": {
    "index": "local_index"
  }
}
```

在此情況下，僅支援使用者名稱和密碼的基本驗證。遠端網域必須具有可公開存取的端點 (即使它與本機 OpenSearch 服務網域位於相同的 VPC 中)，以及由公用 CA 簽署的憑證。不支援自我簽署或私有 CA 簽署憑證。

重新索引大型資料集

遠端重新建立索引會使用下列預設值將捲動要求傳送至遠端網域：

- 搜尋 5 分鐘內容
- 通訊端逾時 30 秒
- 批次大小為 1,000

我們建議您調整這些參數以容納您的資料。對於大型文件，請考慮較小的批次大小和/或較長的逾時。如需詳細資訊，請參閱捲動搜尋。

```
POST _reindex?pretty=true&scroll=10h&wait_for_completion=false
{
  "source": {
    "remote": {
      "host": "https://remote-domain-endpoint:443",
      "socket_timeout": "60m"
    },
    "size": 100,
    "index": "remote_index"
  },
  "dest": {
    "index": "local_index"
  }
}
```

我們還建議將以下設置添加到本地索引以獲得更好的性能：

```
PUT local_index
{
  "settings": {
    "refresh_interval": -1,
    "number_of_replicas": 0
  }
}
```

重新索引程序完成後，您可以設定想要的複本數，並移除重新整理間隔設定。

若只要重新索引您透過查詢選取的文件子集，請將此請求傳送至本機網域：

```
POST _reindex
{
  "source": {
    "remote": {
      "host": "https://remote-domain-endpoint:443"
    },
    "index": "remote_index",
    "query": {
      "match": {
        "field_name": "text"
      }
    }
  },
```

```
  "dest": {
    "index": "local_index"
  }
}
```

遠端重新索引不支援分割，因此您無法為同一個請求並行執行多個捲動操作。

遠端重新索引設定

除了標準的重新索引選項之外， OpenSearch Service 還支援下列選項：

選項	有效值	描述	必要
外部	Boolean	如果遠端網域不是 OpenSearch 服務網域，或者您要在兩個 VPC 網域之間重新建立索引，請指定為。`true`	否
region	字串	如果遠端網域位於不同的區域，請指定「地區」名稱。	否

使用資料串流管理 Amazon OpenSearch 服務中的時間序列資料

管理時間序列資料的典型工作流程包含多個步驟，例如建立變換索引別名、定義寫入索引，以及定義備份索引的通用映射和設定。

Amazon OpenSearch 服務中的資料串流有助於簡化此初始設定程序。資料串流可立即用於以時間為基礎的資料，例如通常只附加的應用程式日誌。

資料串流需要 1.0 OpenSearch 版或更新版本。

> **Note**
>
> 本文件提供基本步驟，協助您開始使用 Amazon OpenSearch 服務網域上的資料串流。如需完整文件，請參閱文 OpenSearch 件中的資料串流。

資料串流入門

資料串流內部由多個後備索引組成。搜尋請求會路由至所有後備索引，而索引請求則會路由至最新的寫入索引。

步驟 1：建立索引範本

若要建立資料串流，首先需要建立一個索引範本，設定一組索引作為資料串流。`data_stream` 物件表示它是一個資料串流，而不是一個常規的索引範本。索引模式與資料串流的名稱匹配：

```
PUT _index_template/logs-template
{
  "index_patterns": [
    "my-data-stream",
    "logs-*"
  ],
  "data_stream": {},
  "priority": 100
}
```

在這種情況下，每個擷取的文件都必須有 `@timestamp` 欄位。您也可以將自己的自訂時間戳記欄位定義為 `data_stream` 物件中的一個屬性：

```
PUT _index_template/logs-template
{
  "index_patterns": "my-data-stream",
  "data_stream": {
    "timestamp_field": {
      "name": "request_time"
    }
  }
}
```

步驟 2：建立資料串流

建立索引範本之後，您可以直接開始擷取資料，而不需要建立資料串流。

因為我們有一個匹配的索引模板與`data_stream`對象， OpenSearch 自動創建數據流：

```
POST logs-staging/_doc
{
```

```
  "message": "login attempt failed",
  "@timestamp": "2013-03-01T00:00:00"
}
```

步驟 3：將資料擷取至資料串流

若要將資料擷取至資料串流，您可以使用一般索引 API。確保您索引的每個文件都有一個時間戳記欄位。如果您嘗試擷取沒有時間戳記欄位的文件，會收到錯誤。

```
POST logs-redis/_doc
{
  "message": "login attempt",
  "@timestamp": "2013-03-01T00:00:00"
}
```

步驟 4：搜尋資料串流

您可以像搜尋一般索引或索引別名一樣搜尋資料串流。搜尋操作適用於所有後備索引 (串流中存在的所有資料)。

```
GET logs-redis/_search
{
  "query": {
    "match": {
      "message": "login"
    }
  }
}
```

步驟 5：變換資料串流

您可以設定索引狀態管理 (ISM)政策來自動化資料串流的變換程序。ISM 政策會在建立後備索引時便套用至它們。當您將政策與資料串流產生關聯時，它只會影響該資料串流的未來後備索引。您也不需要提供 `rollover_alias` 設定，因為 ISM 政策會從後備索引中推斷此資訊。

> **Note**
>
> 如果您將後備索引移轉至冷存放區，請從資料串流中移 OpenSearch 除此索引。即使您將索引移回 UltraWarm，索引仍然是獨立的，而不是原始資料串流的一部分。從資料串流中移除索引之後，針對串流進行搜尋將不會從索引傳回任何資料。

> **Warning**
>
> 資料串流的寫入索引無法移轉至冷存放區。如果您想要將資料串流中的資料移轉至冷儲存，則必須在移轉之前翻轉資料串流。

步驟 6：管理 OpenSearch 儀表板中的資料串流

若要從 OpenSearch 儀表板管理資料流，請開啟OpenSearch 儀表板，選擇索引管理，然後選取索引或原則管理索引。

步驟 7：刪除資料串流

刪除操作首先刪除資料串流的後備索引，然後刪除資料串流本身。

若要刪除資料串流及其所有隱藏的後備索引：

```
DELETE _data_stream/name_of_data_stream
```

在 Amazon OpenSearch Service 中監控資料

透過提醒和異常偵測，在 Amazon OpenSearch Service 中主動監控您的資料。設定警示以便在資料超過特定閾值時接收通知。異常偵測會使用機器學習來自動偵測串流資料中的任何極端值。您可以將異常偵測與提醒配對，以確保在偵測到異常時立即通知您。

主題

- 在 Amazon OpenSearch 服務中配置警報
- Amazon OpenSearch 服務中的異常檢測

在 Amazon OpenSearch 服務中配置警報

在 Amazon Ser OpenSearch vice 中設定警示，以便在來自一或多個索引的資料符合特定條件時收到通知。例如，您可能希望在應用程式於 1 個小時內記錄超過 5 個以上的 HTTP 503 錯誤時收到電子郵件，或者在過去 20 分鐘內未有任何新文件編製成索引時通知開發人員。

提醒需要 OpenSearch 或彈性搜索 6.2 或更高版本。

> **Note**
>
> 本文件提供警示的簡短概觀，並重點介紹 Amazon Ser OpenSearch vice 網域上的警示與開放原始碼叢集上的警示有何不同。 OpenSearch 如需完整的警示文件，包括完整的 API 參考資料、複合監視器的可用要求欄位清單，以及可用觸發器和動作變數的說明，請參閱文件中的 OpenSearch Alerting。

主題

- 提醒許可
- 提醒入門
- 通知
- 差異

提醒許可

提醒支援精細存取控制。如需有關混合和比對權限以符合您使用案例的詳細資訊，請參閱 OpenSearch 文件中的警示安全性。

若要存取 [OpenSearch 儀表板] 中的 [警示] 頁面，您必須至少對應至`alerting_read_access`預先定義的角色，或是獲得同等權限。此角色會授與檢視警示、目的地和監視的權限，但不會授與確認警示或修改目的地或監視器的權限。

提醒入門

若要建立警示，請設定監視，監視器是按照定義的排程執行並查詢 OpenSearch 索引的工作。您也可以設定一個或多個觸發條件，這些觸發條件會定義產生事件的條件。最後，您可以設定 action (動作)，這是觸發提醒之後發生的動作。

開始使用提醒

1. 從 OpenSearch 儀表板主功能表中選擇警示，然後選擇建立監視器。
2. 建立每個查詢、每個儲存貯體、每個叢集指標或每個文件監控。如需相關說明，請參閱 Create a monitor (建立監控)。
3. 針對 Trigger (觸發條件)，建立一個或多個觸發條件。如需相關說明，請參閱 Create triggers (建立觸發條件)。
4. 針對 Action (動作)，設定提醒的 notification channel (通知頻道)。在 Slack、Amazon Chime、自訂 Webhook 或 Amazon SNS 之間進行選擇。如您所想，通知需要連線到相關頻道。例如，您的 OpenSearch 服務域必須能夠連接到互聯網才能通知 Slack 頻道或將自定義 webhook 發送到第三方服務器。自定義 webhook 必須具有公共 IP 地址，以便 OpenSearch 服務域向其發送警報。

> **Tip**
>
> 當動作成功傳送簡訊之後，您就必須負責保護該簡訊的存取權 (例如，存取 Slack 頻道)。如果您的網域包含敏感資料，請考慮在沒有動作的情況下使用觸發程序，並定期檢查 Dashboards 是否有提醒。

通知

警報與通知整合，這是一個統一的 OpenSearch通知系統。通知可讓您設定要使用的通訊服務，並查看相關統計資料和疑難排解資訊。如需完整文件，請參閱 OpenSearch 文件中的通知。

您的網域必須執行 2.3 OpenSearch 版或更新版本才能使用通知。

> **Note**
>
> OpenSearch 通知與 OpenSearch 服務通知不同，它提供有關服務軟體更新、自動調整增強功能以及其他重要網域層級資訊的詳細資訊。 OpenSearch 通知是特定於插件的。

從 2.0 OpenSearch 版開始，通知通道取代了警示目的地。目的地已被正式取代，並且所有提醒通知將透過未來的頻道進行管理。

當您將網域升級至 2.3 版或更新版本時 (因為 2.x 的 OpenSearch 服務支援從 2.3 開始)，您現有的目的地會自動移轉至通知管道。如果目的地無法移轉，監控將繼續使用它，直到監控移轉到通知頻道為止。如需詳細資訊，請參閱文件中有關目的地的 OpenSearch 問題。

若要開始使用通知，請登入 OpenSearch 儀表板並選擇 [通知]、[管道] 和 [建立管道]。

Amazon Simple Notification Service (Amazon SNS) 是通知支援的通道類型。為了驗證使用者，您需要為使用者提供對 Amazon SNS 的完整存取權限，或讓他們擔任具有存取 Amazon SNS 許可的 IAM 角色。如需相關指示，請參閱《Amazon SNS 作為頻道類型》。

差異

與的開放原始碼版本相比 OpenSearch，Amazon OpenSearch 服務中的警示有一些明顯的差異。

提醒設定

OpenSearch 「服務」可讓您修改下列警示設定：

- `plugins.scheduled_jobs.enabled`
- `plugins.alerting.alert_history_enabled`
- `plugins.alerting.alert_history_max_age`
- `plugins.alerting.alert_history_max_docs`
- `plugins.alerting.alert_history_retention_period`
- `plugins.alerting.alert_history_rollover_period`
- `plugins.alerting.filter_by_backend_roles`

所有其他設定都會使用您無法變更的預設值。

若要停用提醒，請傳送下列請求：

```
PUT _cluster/settings
{
  "persistent" : {
    "plugins.scheduled_jobs.enabled" : false
  }
}
```

下列要求會設定警示，以便在 7 天後自動刪除歷史記錄索引，而非預設的 30 天：

```
PUT _cluster/settings
{
  "persistent": {
    "plugins.alerting.alert_history_retention_period": "7d"
  }
}
```

如果您先前已建立監視，而且想要停止建立每日警示索引，請刪除所有警示歷史記錄索引：

```
DELETE .plugins-alerting-alert-history-*
```

若要減少歷程索引的碎片計數，請建立索引範本。下列請求將提醒的歷史記錄索引設定為一個碎片和一個複本：

```
PUT _index_template/template-name
{
  "index_patterns": [".opendistro-alerting-alert-history-*"],
  "template": {
    "settings": {
      "number_of_shards": 1,
      "number_of_replicas": 1
    }
  }
}
```

根據您對資料丟失的容忍度，您甚至可以考慮使用零複本。如需有關建立和管理索引範本的詳細資訊，請參閱 OpenSearch 文件中的索引範本。

Amazon OpenSearch 服務中的異常檢測

Amazon Ser OpenSearch vice 中的異常偵測會使用隨機切割林 (RCF) 演算法，以近乎即時的方式自動偵測 OpenSearch 資料中的異常情況。RCF 是一種非監督式的機器學習演算法，它會為傳入資料串流的草圖建立模型。該演算法會為每個傳入資料點計算 `anomaly grade` 和 `confidence score` 值。異常偵測使用這些值來區分資料中的異常與正常變化。

您可以將異常檢測插件與警報插件配對，以便在檢測到異常時立即通知您。

異常偵測適用於執行任何 OpenSearch 版本或彈性搜尋 7.4 或更新版本的網域。除了 `t2.micro` 和 `t2.small` 外，所有執行個體類型都支援異常偵測。

> **Note**
>
> 本文件提供 Amazon OpenSearch 服務範圍內異常偵測的簡要概觀。如需完整的文件，包括詳細步驟、API 參考、所有可用設定的參考，以及建立視覺效果和儀表板的步驟，請參閱開放原始碼 OpenSearch 文件中的異常偵測。

必要條件

異常偵測具有以下先決條件：

- 異常偵測需要 OpenSearch 或彈性搜尋 7.4 或更新版本。
- 異常偵測僅支援 Elasticsearch 7.9 版及更高版本以及所有版本的精細存取控制。 OpenSearch在 Elasticsearch 7.9 之前，只有管理員使用者可以建立、檢視和管理偵測器。
- 如果您的網域使用精細的存取控制，則非管理員使用者必須對應至 OpenSearch 儀表板中的`anomaly_read_access`角色，才能檢視偵測器，或`anomaly_full_access`者建立和管理偵測器。

開始使用異常偵測

若要開始使用，請在 OpenSearch 儀表板中選擇「異常偵測」。

步驟 1：建立偵測器

偵測器是個別的異常偵測任務。您可以建立多個偵測器，且所有偵測器皆可同時執行，而每個偵測器會分析來自不同來源的資料。

步驟 2：將功能新增至偵測器

功能是您檢查異常之索引中的欄位。偵測器可在一或多個功能中探索異常。您必須針對每個功能選擇以下其中一個彙總：`average()`、`sum()`、`count()`、`min()` 或 `max()`。

> **Note**
>
> `count()`彙總方法僅適用於 OpenSearch 和彈性搜尋 7.7 或更新版本。對於 Elasticsearch 7.4，請使用如下所示的自訂表達式：
>
> ```
> {
>  "aggregation_name": {
>  "value_count": {
>  "field": "field_name"
>  }
>  }
> }
> ```

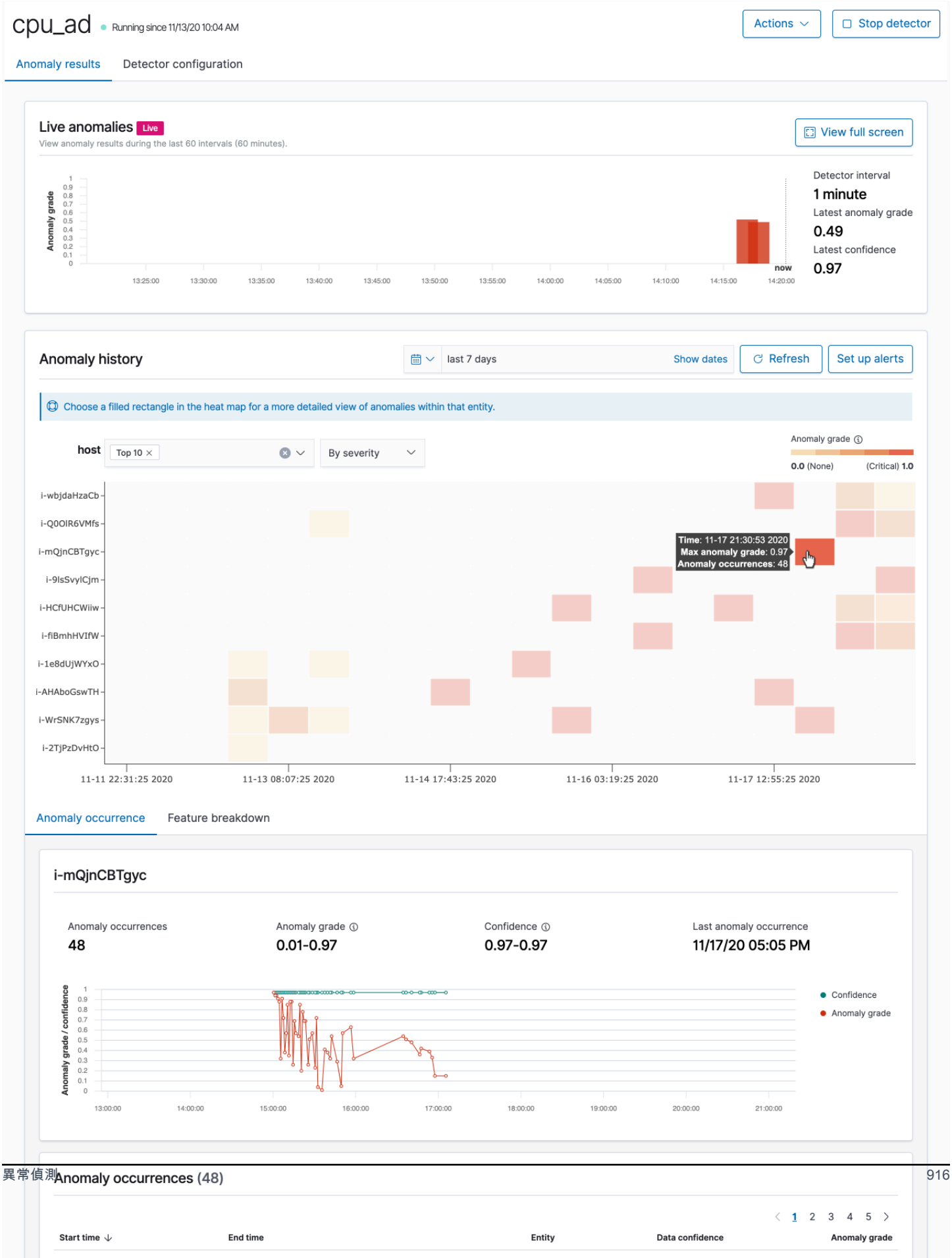
彙總方法會決定構成異常的內容。例如，如果您選擇， `min()`，偵測器會專注於根據功能的最小值來尋找異常。如果您選擇 `average()`，偵測器會根據功能的平均值來尋找異常。每個偵測器最多可以新增五個功能。

您可以配置下列選用設定 (在 Elastisearch 7.7 及更新版本中可用)：

- 類別欄位-使用 IP 地址、產品 ID、國家/地區代碼等維度來分類或分割資料。
- 時段大小-設定要在偵測時段中考量的資料串流彙總間隔數。

設定功能後，請預覽範例異常，並視需要調整功能設定。

步驟 3：觀察結果


cpu_ad
Running since 11/13/20 10:04 AM
Actions
Stop detector
Anomaly results
Detector configuration
Live anomalies
Live
View anomaly results during the last 60 intervals (60 minutes).
View full screen
Anomaly grade
Detector interval
1 minute
Latest anomaly grade
0.49
Latest confidence
0.97
now
Anomaly history
last 7 days
Show dates
Refresh
Set up alerts
Choose a filled rectangle in the heat map for a more detailed view of anomalies within that entity.
host
Top 10
By severity
Anomaly grade
0.0 (None)
(Critical) 1.0
i-wbjdaHzaCb
i-Q0OIR6VMfs
i-mQjnCBTgyc
i-9lsSvylCjm
i-HCfUHCWiiw
i-fiBmhHVIfW
i-1e8dUjWYxO
i-AHAboGswTH
i-WrSNK7zgys
i-2TjPzDvHtO
Time: 11-17 21:30:53 2020
Max anomaly grade: 0.97
Anomaly occurrences: 48
11-11 22:31:25 2020
11-13 08:07:25 2020
11-14 17:43:25 2020
11-16 03:19:25 2020
11-17 12:55:25 2020
Anomaly occurrence
Feature breakdown
i-mQjnCBTgyc
Anomaly occurrences
48
Anomaly grade
0.01-0.97
Confidence
0.97-0.97
Last anomaly occurrence
11/17/20 05:05 PM
Anomaly grade / confidence
Confidence
Anomaly grade
Anomaly occurrences (48)
Start time
End time
Entity
Data confidence
Anomaly grade
11/17/20 5:04 PM
11/17/20 5:05 PM
i-mQjnCBTgyc
0.97
0.15

- Live anomalies (即時異常) - 顯示最後 60 個間隔的即時異常結果。例如，如果間隔設為 10，則會顯示最後 600 分鐘的結果。此圖表每隔 30 秒重新整理一次。
- Anomaly history (異常歷程記錄) - 會使用對應可信度測量來繪製異常分數。
- Feature breakdown (功能明細) - 根據彙總方法來繪製功能。您可以呈現偵測器的日期時間範圍差異。
- Anomaly occurrence (異常出現次數) - 顯示每個偵測到的異常的 `Start time`、`End time`、`Data confidence` 和 `Anomaly grade`。

  如果您設定類別欄位，您會看到額外的熱度圖圖表，它會關聯異常實體的結果。選擇填滿的矩形以查看異常的更詳細檢視。

步驟 4：設定提醒

若要建立監控以在偵測到任何異常時傳送通知，請選擇 Set up alerts (設定提醒)。外掛程式會將您重新導向至 Add monitor (新增監控) 頁面，您可在此設定提醒。

教學課程：使用異常偵測來偵測高 CPU 使用率

本教學課程示範如何在 Amazon OpenSearch 服務中建立異常偵測器，以偵測高 CPU 使用率。您將使用 OpenSearch 儀表板設定偵測器來監控 CPU 使用率，並在 CPU 使用率上升超過指定閾值時產生警示。

> **Note**
>
> 這些步驟適用於最新版本的 OpenSearch ，對於過去的版本可能略有不同。

必要條件

- 您必須擁有執行彈性搜尋 7.4 或更新版本的 OpenSearch 服務網域，或是任何 OpenSearch版本。
- 您必須將應用程式日誌檔案擷取到包含 CPU 使用率資料的叢集中。

步驟 1：建立偵測器

首先，建立偵測器來識別 CPU 使用率資料中的異常情況。

1. 在「 OpenSearch 儀表板」中開啟左側面板選單並選擇「異常偵測」，然後選擇「建立偵測器」。

2. 將偵測器命名為 **high-cpu-usage**。
3. 對於您的資料來源，請選擇包含 CPU 使用率日誌檔案 (您要在其中識別異常情況) 的索引。
4. 從您的資料中選擇 Timestamp field (時間戳記欄位)。您可以選擇性地新增資料篩選條件。此資料篩選條件僅分析資料來源的子集，並減少不相關資料的雜訊。
5. 將 Detector interval (偵測器間隔) 設為 2 分鐘。此間隔定義偵測器收集資料的時間 (按分鐘間隔)。
6. 在 Window delay (時段延遲) 中，新增 1-minute (1 分鐘) 延遲。此延遲會增加額外的處理時間，以確保該時段內的所有資料都存在。
7. 選擇下一步。在異常偵測儀表板的偵測器名稱下，選擇 Configure model (設定模型)。
8. 針對 Feature name (功能名稱)，輸入 **max_cpu_usage**。針對 Feature state (功能狀態)，選取 Enable feature (啟用功能)。
9. 針對 Find anomalies based on (尋找異常的依據)，選擇 Field value (欄位值)。
10. 針對 Aggregation method (彙總方法)，選擇 **max()**。
11. 針對 Field (欄位)，選取資料中的欄位以檢查異常。例如，它可能會稱為 `cpu_usage_percentage`。
12. 將其他所有設定保留為預設值，然後選擇 Next (下一步)。
13. 忽略偵測器任務設定並選擇 Next (下一步)。
14. 在彈出式視窗中，選擇何時啟動偵測器 (自動或手動)，然後選擇 Confirm (確認)。

既然已設定偵測器，在它初始化後，您將能夠在偵測器面板的 Real-time results (即時結果) 區段中看到 CPU 使用率的即時結果。Live anomalies (即時異常) 區段會顯示即時擷取資料時發生的任何異常。

步驟 2：設定警示

既然您已建立偵測器，請建立一個監控器，以在偵測到符合偵測器設定中指定條件的 CPU 使用率時，呼叫警示以便將訊息傳送至 Slack。當來自一個或多個索引的資料符合呼叫警示的條件時，您會收到 Slack 通知。

1. 在 OpenSearch 儀表板中開啟左側面板選單並選擇「警示」，然後選擇「建立監視器」。
2. 提供監控器的名稱。
3. 針對 Monitor type (監控器類型)，選擇 Per-query monitor (每個查詢監控器)。每個查詢監控器會執行指定的查詢並定義觸發條件。
4. 針對 Monitor defining method (監控器定義方法)，選擇 Anomaly detector (異常偵測器)，然後從 Detector (偵測器) 下拉式選單中選取您在上一個區段中建立的偵測器。

5. 針對 Schedule (排程)，選擇監控器收集資料的頻率，以及您接收警示的頻率。為了實現本教學課程的目的，請將排程設定為每 7 分鐘執行一次。
6. 在 Triggers (觸發條件) 區段中，選擇 Add trigger (新增觸發條件)。針對 Trigger name (觸發條件名稱)，輸入 **`High CPU usage`**。在本教學課程中，針對 Severity level (嚴重性等級)，選擇 1 (最高嚴重性等級)。
7. 針對 Anomaly grade threshold (異常等級閾值)，選擇 IS ABOVE (超過)。在其下面的選單中，選擇要套用的等級閾值。針對本教學課程，請將 Anomaly grade (異常等級) 設為 0.7。
8. 針對 Anomaly confidence threshold (異常可信度閾值)，選擇 IS ABOVE (超過)。在其下面的選單中，輸入與異常等級相同的數字。針對本教學課程，請將 Anomaly confidence threshold (異常可信度閾值) 設為 0.7。
9. 在 Actions (動作) 區段中，請選擇 Destination (目的地)。在 Name (名稱) 欄位中，請選擇目的地名稱。在 Type (類型) 選單中，請選擇 Slack。在 Webhook URL 欄位中，請輸入要接收警示的 Webhook URL。如需詳細資訊，請參閱 Sending messages using incoming webhooks (使用傳入的 Webhook 傳送訊息)。
10. 選擇建立。

相關資源

- the section called “提醒”

- the section called “異常偵測”
- 異常偵測 API

Amazon OpenSearch 服務的機器學習

ML 共享資源是一個 OpenSearch 插件，通過傳輸和 REST API 調用提供一組常見的機器學習（ML）算法。這些呼叫會針對每個 ML 要求選擇正確的節點和資源，並監控 ML 工作以確保正常運作時間。這可讓您運用現有的開放原始碼 ML 演算法，減少開發新 ML 功能所需的工作量。如需外掛程式的詳細資訊，請參閱 OpenSearch 文件中的機器學習。本章介紹如何使用插件與 Amazon OpenSearch 服務。

主題

- Amazon OpenSearch 服務 ML 連接器 AWS 服務
- 適用於第三方平台的 Amazon OpenSearch 服務 ML
- 用 AWS CloudFormation 於設定語意搜尋的遠端推論
- 不支援的 ML 共享資源
- OpenSearch 服務流程框架模板

Amazon OpenSearch 服務 ML 連接器 AWS 服務

將 Amazon Ser OpenSearch vice 機器學習 (ML) 連接器與另一個連接器搭配使用時 AWS 服務，您需要設定 IAM 角色，以將 OpenSearch 服務安全地連接到該服務。 AWS 服務 您可以設置一個連接器以包括 Amazon SageMaker 和 Amazon 基岩。在本教程中，我們將介紹如何創建從 OpenSearch 服務到 SageMaker 運行時的連接器。如需連接器的詳細資訊，請參閱支援的連接器。

主題

- 必要條件
- 建立 OpenSearch 服務連接器

必要條件

若要建立連接器，您必須具有授予 OpenSearch 服務存取權的 Amazon SageMaker 網域端點和 IAM 角色。

設置 Amazon SageMaker 域名

請參閱 Amazon SageMaker 開發人員指南中的 SageMaker在 Amazon 部署模型，以部署您的機器學習模型。請記下模型的端點 URL，您需要該 URL 才能建立 AI 連接器。

建立 IAM 角色

設定 IAM 角色以將 SageMaker 執行階段許可委派給 OpenSearch 服務。若要建立新角色，請參閱 IAM 使用者指南中的建立 IAM 角色 (主控台)。或者，您可以使用現有角色，只要該角色具有相同的權限集即可。如果您確實建立新角色而不是使用 AWS 受管理的角色，請將本教學課程`opensearch-sagemaker-role`中的角色名稱取代為您自己的角色名稱。

1. 將以下受管 IAM 政策附加到您的新角色，以允許 OpenSearch Service 存取您的 SageMaker 端點。若要將政策附加至角色，請參閱新增 IAM 身分許可。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "sagemaker:InvokeEndpointAsync",
                "sagemaker:InvokeEndpoint"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

2. 遵循修改角色信任原則中的指示，編輯角色的信任關係。您必須在`Principal`聲明中指定 OpenSearch 服務：

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "sts:AssumeRole"
            ],
            "Effect": "Allow",
            "Principal": {
                "Service": [
                    "opensearchservice.amazonaws.com"
                ]
            }
        }
    ]
```

```
}
```

我們建議您使用`aws:SourceAccount`和`aws:SourceArn`條件金鑰來限制對特定網域的存取。這`SourceAccount`是屬於網域擁有者的 AWS 帳戶 ID，而且`SourceArn`是網域的 ARN。例如，您可以將下列條件區塊新增至信任原則：

```
"Condition": {
    "StringEquals": {
        "aws:SourceAccount": "account-id"
    },
    "ArnLike": {
        "aws:SourceArn": "arn:aws:es:region:account-id:domain/domain-name"
    }
}
```

設定許可

若要建立連接器，您需要將 IAM 角色傳遞給 OpenSearch 服務的權限。您也需要存取 `es:ESHttpPost` 動作。若要授予這兩個許可，請將下列政策連接至其憑證用於簽署請求的 IAM 角色：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "iam:PassRole",
      "Resource": "arn:aws:iam::account-id:role/opensearch-sagemaker-role"
    },
    {
      "Effect": "Allow",
      "Action": "es:ESHttpPost",
      "Resource": "arn:aws:es:region:account-id:domain/domain-name/*"
    }
  ]
}
```

如果您的使用者或角色沒有傳遞角色的`iam:PassRole`權限，則在下一個步驟中嘗試註冊存放庫時可能會遇到授權錯誤。

對應 OpenSearch 儀表板中的 ML 角色 (如果使用精細的存取控制)

精細的存取控制會在設定連接器時引入額外的步驟。即使您將 HTTP 基本身分驗證用於所有其他目的，您也需要將 `ml_full_access` 角色映射至擁有 `iam:PassRole` 許可能夠傳遞 `opensearch-sagemaker-role` 的 IAM 角色。

1. 導覽至 OpenSearch 服務網域的 OpenSearch 儀表板外掛程式。您可以在 OpenSearch 服務主控台上的網域儀表板上找到儀表板端點。
2. 從主功能表中選擇安全性、角色，然後選取 ml_full_ access 角色。
3. 選擇 Mapped users (已映射的使用者)、Manage mapping (管理映射)。
4. 在後端角色下，新增具有通過`opensearch-sagemaker-role`權限之角色的 ARN。

   ```
   arn:aws:iam::account-id:role/role-name
   ```

5. 選擇 Map (映射)，並確認使用者或角色顯示在 Mapped users (已映射的使用者) 中。

建立 OpenSearch 服務連接器

若要建立連接器，請將要`POST`求傳送至 OpenSearch 服務網域端點。您可以使用 curl、Python 用戶端範例、郵遞員或其他方法來傳送已簽署的要求。請注意，您無法在 Kibana 主控台中使用`POST`要求。請求採用下列格式：

```
POST domain-endpoint/_plugins/_ml/connectors/_create
{
   "name": "sagemaker: embedding",
   "description": "Test connector for Sagemaker embedding model",
   "version": 1,
   "protocol": "aws_sigv4",
   "credential": {
      "roleArn": "arn:aws:iam::account-id:role/opensearch-sagemaker-role"
   },
   "parameters": {
      "region": "region",
      "service_name": "sagemaker"
   },
   "actions": [
      {
         "action_type": "predict",
         "method": "POST",
         "headers": {
```

```
            "content-type": "application/json"
         },
         "url": "https://runtime.sagemaker.region.amazonaws.com/endpoints/endpoint-id/
invocations",
         "request_body": "{ \"inputs\": { \"question\": \"${parameters.question}\",
 \"context\": \"${parameters.context}\" } }"
      }
   ]
}
```

如果您的網域位於虛擬私有雲 (VPC) 內，您的電腦必須連線至 VPC，要求才能成功建立 AI 連接器。存取 VPC 會因網路組態而異，但通常涉及連線至 VPN 或公司網路。要檢查您是否可以訪問 OpenSearch 服務域，請`https://your-vpc-domain.region.es.amazonaws.com`在 Web 瀏覽器中導航到並確認您收到默認的 JSON 響應。

示例 Python 客戶端

Python 客戶端比 HTTP 請求更容易自動化，並且具有更好的可重用性。若要使用 Python 用戶端建立 AI 連接器，請將下列範例程式碼儲存至 Python 檔案。用戶端需要AWS SDK for Python (Boto3)`requests`、和`requests-aws4auth`套件。

```
import boto3
import requests
from requests_aws4auth import AWS4Auth

host = 'domain-endpoint/'
region = 'region'
service = 'es'
credentials = boto3.Session().get_credentials()
awsauth = AWS4Auth(credentials.access_key, credentials.secret_key, region, service,
 session_token=credentials.token)

# Register repository
path = '_plugins/_ml/connectors/_create'
url = host + path

payload = {
   "name": "sagemaker: embedding",
   "description": "Test connector for Sagemaker embedding model",
   "version": 1,
   "protocol": "aws_sigv4",
   "credential": {
```

```
      "roleArn": "arn:aws:iam::account-id:role/opensearch-sagemaker-role"
   },
   "parameters": {
      "region": "region",
      "service_name": "sagemaker"
   },
   "actions": [
      {
         "action_type": "predict",
         "method": "POST",
         "headers": {
            "content-type": "application/json"
         },
         "url": "https://runtime.sagemaker.region.amazonaws.com/endpoints/endpoint-id/
invocations",
         "request_body": "{ \"inputs\": { \"question\": \"${parameters.question}\",
 \"context\": \"${parameters.context}\" } }"
      }
   ]
}
headers = {"Content-Type": "application/json"}

r = requests.post(url, auth=awsauth, json=payload, headers=headers)
print(r.status_code)
print(r.text)
```

適用於第三方平台的 Amazon OpenSearch 服務 ML

在本教程中，我們將介紹如何創建從 OpenSearch 服務到 Cohere 的連接器。如需連接器的詳細資訊，請參閱支援的連接器。

當您將 Amazon Ser OpenSearch vice 機器學習 (ML) 連接器與外部遠端模型搭配使用時，您需要將特定的授權登入資料存放在中 AWS Secrets Manager。這可能是 API 密鑰，也可以是用戶名和密碼的組合。這意味著您還需要創建一個 IAM 角色，以允許從 Secrets Manager 讀取 OpenSearch 服務訪問權限。

主題

- 必要條件
- 建立 OpenSearch 服務連接器

必要條件

若要為 Cohere 或任何具有服務的外部提供者建立連接器，您必須具有可授與 OpenSearch 服 OpenSearch 務存取權的 IAM 角色 AWS Secrets Manager，並在其中儲存您的登入資料。您也必須將您的認證儲存在 Secrets Manager 中。

建立 IAM 角色

設定 IAM 角色以將 Secrets Manager 權限委派給 OpenSearch 服務。您也可以使用現有的`SecretManagerReadWrite`角色。若要建立新角色，請參閱 IAM 使用者指南中的建立 IAM 角色(主控台)。如果您確實建立新角色而不是使用 AWS 受管理的角色，請將本教學課程`opensearch-secretmanager-role`中的角色名稱取代為您自己的角色名稱。

1. 將下列受管身分與存取權管理政策附加到您的新角色，以允許 OpenSearch 服務存取您的 Secrets Manager 值。若要將政策附加至角色，請參閱新增 IAM 身分許可。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "secretsmanager:GetSecretValue"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

2. 遵循修改角色信任原則中的指示，編輯角色的信任關係。您必須在`Principal`聲明中指定 OpenSearch 服務：

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "sts:AssumeRole"
            ],
            "Effect": "Allow",
            "Principal": {
                "Service": [
```

```
                    "opensearchservice.amazonaws.com"
                ]
            }
        }
    ]
}
```

我們建議您使用`aws:SourceAccount`和`aws:SourceArn`條件金鑰來限制對特定網域的存取。這`SourceAccount`是屬於網域擁有者的 AWS 帳戶 ID，而且`SourceArn`是網域的 ARN。例如，您可以將下列條件區塊新增至信任原則：

```
"Condition": {
    "StringEquals": {
        "aws:SourceAccount": "account-id"
    },
    "ArnLike": {
        "aws:SourceArn": "arn:aws:es:region:account-id:domain/domain-name"
    }
}
```

設定許可

若要建立連接器，您需要將 IAM 角色傳遞給 OpenSearch 服務的權限。您也需要存取 `es:ESHttpPost` 動作。若要授予這兩個許可，請將下列政策連接至其憑證用於簽署請求的 IAM 角色：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "iam:PassRole",
      "Resource": "arn:aws:iam::account-id:role/opensearch-secretmanager-role"
    },
    {
      "Effect": "Allow",
      "Action": "es:ESHttpPost",
      "Resource": "arn:aws:es:region:account-id:domain/domain-name/*"
    }
  ]
```

```
}
```

如果您的使用者或角色沒有傳遞角色的`iam:PassRole`權限，則在下一個步驟中嘗試註冊存放庫時可能會遇到授權錯誤。

設定 AWS Secrets Manager

若要將您的授權認證儲存在 Secrets Manager 中，請參閱AWS Secrets Manager 使用者指南中的建立密 AWS Secrets Manager 碼。

當 Secrets Manager 接受您的鍵值對作為密碼之後，您會收到一個 ARN，格式為：。`arn:aws:secretsmanager:us-west-2:123456789012:secret:MySecret-a1b2c3`在下一個步驟中建立連接器時，請記錄此 ARN 以及您的金鑰。

在 OpenSearch 儀表板中對應 ML 角色 (如果使用精細的存取控制)

精細的存取控制會在設定連接器時引入額外的步驟。即使您將 HTTP 基本身分驗證用於所有其他目的，您也需要將 `ml_full_access` 角色映射至擁有 `iam:PassRole` 許可能夠傳遞 `opensearch-sagemaker-role` 的 IAM 角色。

1. 導覽至 OpenSearch 服務網域的 OpenSearch 儀表板外掛程式。您可以在 OpenSearch 服務主控台上的網域儀表板上找到儀表板端點。
2. 從主功能表中選擇安全性、角色，然後選取 ml_full_ access 角色。
3. 選擇 Mapped users (已映射的使用者)、Manage mapping (管理映射)。
4. 在後端角色下，新增具有通過`opensearch-sagemaker-role`權限之角色的 ARN。

   ```
   arn:aws:iam::account-id:role/role-name
   ```

5. 選擇 Map (映射)，並確認使用者或角色顯示在 Mapped users (已映射的使用者) 中。

建立 OpenSearch 服務連接器

若要建立連接器，請將要`POST`求傳送至 OpenSearch 服務網域端點。您可以使用 curl、Python 用戶端範例、郵遞員或其他方法來傳送已簽署的要求。請注意，您無法在 Kibana 主控台中使用`POST`要求。請求採用下列格式：

```
POST domain-endpoint/_plugins/_ml/connectors/_create
{
    "name": "Cohere Connector: embedding",
```

```
    "description": "The connector to cohere embedding model",
    "version": 1,
    "protocol": "http",
    "credential": {
        "secretArn": "arn:aws:secretsmanager:region:account-id:secret:cohere-key-id",
        "roleArn": "arn:aws:iam::account-id:role/opensearch-secretmanager-role"
    },
    "actions": [
        {
            "action_type": "predict",
            "method": "POST",
            "url": "https://api.cohere.ai/v1/embed",
            "headers": {
                "Authorization": "Bearer ${credential.secretArn.cohere-key-used-in-
secrets-manager}"
            },
            "request_body": "{ \"texts\": ${parameters.texts}, \"truncate\": \"END\" }"
        }
    ]
}
```

此要求的要求主體與開放原始碼連接器要求的要求主體有兩種不同。在`credential`欄位內，您會傳遞 IAM 角色的 ARN，該角色允許 OpenSearch 服務從 Secrets Manager 讀取，以及 ARN 以取得什麼秘密。在該`headers`字段中，您可以使用秘密密鑰以及其來自 ARN 的事實來參考秘密。

如果您的網域位於虛擬私有雲 (VPC) 內，您的電腦必須連線至 VPC，才能成功建立 AI 連接器的要求。存取 VPC 會因網路組態而異，但通常涉及連線至 VPN 或公司網路。要檢查您是否可以訪問 OpenSearch 服務域，請`https://`*`your-vpc-domain`*`.`*`region`*`.es.amazonaws.com`在 Web 瀏覽器中導航到並確認您收到默認的 JSON 響應。

示例 Python 客戶端

Python 客戶端比 HTTP 請求更容易自動化，並且具有更好的可重用性。若要使用 Python 用戶端建立 AI 連接器，請將下列範例程式碼儲存至 Python 檔案。用戶端需要AWS SDK for Python (Boto3)`requests`、和`requests-aws4auth`套件。

```
import boto3
import requests
from requests_aws4auth import AWS4Auth

host = 'domain-endpoint/'
region = 'region'
```

```
service = 'es'
credentials = boto3.Session().get_credentials()
awsauth = AWS4Auth(credentials.access_key, credentials.secret_key, region, service,
 session_token=credentials.token)

path = '_plugins/_ml/connectors/_create'
url = host + path

payload = {
    "name": "Cohere Connector: embedding",
    "description": "The connector to cohere embedding model",
    "version": 1,
    "protocol": "http",
    "credential": {
        "secretArn": "arn:aws:secretsmanager:region:account-id:secret:cohere-key-id",
        "roleArn": "arn:aws:iam::account-id:role/opensearch-secretmanager-role"
    },
    "actions": [
        {
            "action_type": "predict",
            "method": "POST",
            "url": "https://api.cohere.ai/v1/embed",
            "headers": {
                "Authorization": "Bearer ${credential.secretArn.cohere-key-used-in-
secrets-manager}"
            },
            "request_body": "{ \"texts\": ${parameters.texts}, \"truncate\": \"END\" }"
        }
    ]
}

headers = {"Content-Type": "application/json"}

r = requests.post(url, auth=awsauth, json=payload, headers=headers)
print(r.status_code)
print(r.text)
```

用 AWS CloudFormation 於設定語意搜尋的遠端推論

從 2.9 OpenSearch 版開始，您可以使用具有語意搜尋的遠端推論來託管您自己的機器學習 (ML) 模型。遠端推論使用 ML Commons 外掛程式，讓您可以在 ML 服務 (例如和 Amazon BedRock) 上遠端託管模型推論， Amazon SageMaker 並使用 ML 連接器將它們連接到 Amazon OpenSearch 服務。

為了簡化遠端推論的設定，Amazon OpenSearch 服務會在主控台中提供AWS CloudFormation範本。CloudFormation 是可 AWS 服務 讓您透過將基礎結構視為程式碼來建模、佈建 AWS 和管理協力廠商資源。

OpenSearch CloudFormation 範本會為您自動化模型佈建程序，以便您可以輕鬆地在 OpenSearch Service 網域中建立模型，然後使用模型 ID 擷取資料並執行神經搜尋查詢。

當您使用 OpenSearch 服務版本 2.12 及更新版本的神經稀疏編碼器時，我們建議您使用本機代碼產生器模型，而不是從遠端部署。如需詳細資訊，請參閱 OpenSearch 文件中的稀疏編碼模型。

主題

- 必要條件
- Amazon SageMaker 模板
- Amazon 基岩模板

必要條件

若要將 CloudFormation 範本與 OpenSearch 服務搭配使用，請完成下列先決條件。

設定 OpenSearch 服務網域

在使用 CloudFormation 範本之前，您必須先設定啟用 2.9 版或更新版本且精細存取控制的 Amazon OpenSearch 服務網域。建立 OpenSearch 服務後端角色，以授與 ML Commons 外掛程式為您建立連接器的權限。

CloudFormation 範本會使用預設名稱為您建立 Lambda IAM 角色`LambdaInvokeOpenSearchMLCommonsRole`，如果您想要選擇其他名稱，可以覆寫該角色。範本建立此 IAM 角色後，您需要授與 Lambda 函數呼叫您的 OpenSearch 服務網域的權限。若要這麼做，請使用下列步驟`ml_full_access`將名為的角色對應至您的 OpenSearch Service 後端角色：

1. 導覽至 OpenSearch 服務網域的 OpenSearch 儀表板外掛程式。您可以在 OpenSearch 服務主控台上的網域儀表板上找到儀表板端點。
2. 從主功能表中選擇安全性、角色，然後選取 ml_full_ access 角色。
3. 選擇 Mapped users (已映射的使用者)、Manage mapping (管理映射)。
4. 在後端角色下，新增 Lambda 角色的 ARN，該角色需要權限才能呼叫您的網域。

```
arn:aws:iam::account-id:role/role-name
```

5. 選擇 Map (映射)，並確認使用者或角色顯示在 Mapped users (已映射的使用者) 中。

對應角色後，瀏覽至網域的安全設定，並將 Lambda IAM 角色新增至您的 OpenSearch 服務存取政策。

啟用您的權限 AWS 帳戶

您 AWS 帳戶 必須具有訪問 CloudFormation 和 Lambda 的許可，以 AWS 服務 及您為模板選擇的任何一個- SageMaker 運行時或 Amazon BedRock。

如果您使用的是 Amazon 基岩，則還必須註冊您的模型。請參閱 Amazon 基岩使用者指南中的模型存取以註冊您的模型。

如果您使用自己的 Amazon S3 儲存貯體提供模型成品，則必須將 CloudFormation IAM 角色新增至 S3 存取政策。如需詳細資訊，請參閱《IAM 使用者指南》中的新增和移除 IAM 身分許可。

Amazon SageMaker 模板

Amazon SageMaker CloudFormation 模板定義了多個 AWS 資源，以便為您設置神經插件和語義搜索。

首先，使用透過 Amazon SageMaker 範本與文字嵌入模型整合，在 SageMaker 執行階段中將文字嵌入模型部署為伺服器。如果您未提供模型端點，請 CloudFormation 建立 IAM 角色，以允許 SageMaker 執行階段從 Amazon S3 下載模型成品並將其部署到伺服器。如果您提供端點，請 CloudFormation 建立 IAM 角色，以允許 Lambda 函數存取 OpenSearch 服務網域，或者，如果角色已存在，則會更新並重複使用該角色。端點會使用 ML Commons 外掛程式提供 ML 連接器所使用的遠端模型。

接下來，使用透過 Amazon Sageemaker 範本與稀疏編碼器整合，建立 Lambda 函數，讓您的網域設定遠端推論連接器。在 OpenSearch Service 中建立連接器之後，遠端推論可以在執行 SageMaker 階段中使用遠端模型執行語意搜尋。範本會將網域中的模型 ID 傳回給您，以便您可以開始搜尋。

使用 Amazon SageMaker CloudFormation 模板

1. 在以下位置打開 Amazon OpenSearch 服務控制台 https://console.aws.amazon.com/aos/home。
2. 在左側導覽中，選擇 [整合]。
3. 在每個 Amazon SageMaker 範本下，選擇設定網域，設定公有網域。
4. 依照主 CloudFormation 控台中的提示來佈建堆疊並設定模型。

> **Note**
>
> OpenSearch 服務還提供單獨的範本來設定 VPC 網域。如果您使用此範本，則需要為 Lambda 函數提供 VPC 識別碼。

Amazon 基岩模板

與 Amazon 範本類似，Amazon 基岩 SageMaker CloudFormation 範本佈建在 OpenSearch 服務和 Amazon 基岩 CloudFormation 之間建立連接器所需的 AWS 資源。

首先，範本會建立 IAM 角色，讓 future 的 Lambda 函數存取您的 OpenSearch 服務網域。然後，該模板創建 Lambda 函數，該函數具有域創建使用 ML 共享資源插件的連接器。 OpenSearch 服務建立連接器後，遠端推論設定即完成，您可以使用 Amazon 基岩 API 操作執行語意搜尋。

請注意，由於 Amazon 基岩託管自己的 ML 模型，因此您不需要將模型部署到執行階段。 SageMaker 此範本會改為使用 Amazon 基岩的預先確定端點，並略過端點佈建步驟。

使用 Amazon 基岩範 CloudFormation 本

1. 在以下位置打開 Amazon OpenSearch 服務控制台 https://console.aws.amazon.com/aos/home。
2. 在左側導覽中，選擇 [整合]。
3. 在「透過 Amazon 基礎架構與 Amazon Titan 文字嵌入模型整合」下，選擇「設定網域」，「設定公有網域」。
4. 按照提示設置模型。

> **Note**
>
> OpenSearch 服務還提供單獨的範本來設定 VPC 網域。如果您使用此範本，則需要為 Lambda 函數提供 VPC 識別碼。

此外， OpenSearch 服務還提供下列 Amazon 基岩範本，以連接到 Cohere 模型和 Amazon Titan 多模式嵌入模型：

- `Integration with Cohere Embed through Amazon Bedrock`
- `Integrate with Amazon Bedrock Titan Multi-modal`

不支援的 ML 共享資源

Amazon OpenSearch 服務不支持使用以下 ML 共享資源設置：

- `plugins.ml_commons.allow_registering_model_via_url`
- `plugins.ml_commons.allow_registering_model_via_local_file`

如需 ML 共享資源設定的詳細資訊，請參閱 ML 共享資源叢集設定。

OpenSearch 服務流程框架模板

Amazon Ser OpenSearch vice 流程架構範本可讓您透過為常見使用案例提供範本，將複雜的 OpenSearch 服務設定和預先處理任務自動化。例如，您可以使用流程架構範本自動化機器學習設定工作。Amazon OpenSearch 服務流程架構範本在 JSON 或 YAML 文件中提供設定程序的簡要說明。這些範本說明自動化工作流程組態，適用於對話式聊天或查詢產生、AI 連接器、工具、代理程式，以及準備 OpenSearch Service 以供後端用於生成模型的其他元件。

您可以自訂 Amazon OpenSearch 服務流程架構範本，以滿足您的特定需求。若要查看自訂流程架構範本的範例，請參閱流程架構。如需 OpenSearch 服務提供的範本，請參閱工作流程範本。如需完整的文件，包括詳細步驟、API 參考，以及所有可用設定的參考資料，請參閱開放原始碼 OpenSearch 文件中的自動化設定。

在 OpenSearch 服務中建立 ML 連接器

Amazon OpenSearch 服務流程架構範本可讓您使用 ml-commons 中提供的建立連接器 API 來設定和安裝 ML 連接器。您可以使用 ML 連接器將 OpenSearch 服務連接到其他 AWS 服務或協力廠商平台。如需詳細資訊，請參閱建立協力廠商 ML 平台的連接器。Amazon OpenSearch 服務流程架構 API 可讓您自動化 OpenSearch 服務設定和預先處理任務，並可用於建立機器學習連接器。

您必須先執行下列動作，才能在 OpenSearch 服務中建立連接器：

- 創建一個 Amazon SageMaker 域。
- 建立 IAM 角色。
- 設定傳遞角色權限。
- 在儀表板中映射流程框架和 ml-commons 角色。 OpenSearch

如需如何為 AWS 服務設定 ML 連接器的詳細資訊，請參閱 OpenSearch 服務的 Amazon 服務 ML 連接器。 AWS 若要進一步了解如何在第三方平台上使用 OpenSearch 服務 ML 連接器，請參閱第三方平台的 Amazon Ser OpenSearch vice ML 連接器。

透過流程架構服務建立連接器

若要使用連接器建立流程架構範本，您需要將要POST求傳送至 OpenSearch 服務網域端點。您可以使用 cURL、Python 用戶端範例、郵遞員或其他方法來傳送已簽署的要求。請POST求的格式如下：

```
POST /_plugins/_flow_framework/workflow
{
  "name": "Deploy Claude Model",
  "description": "Deploy a model using a connector to Claude",
  "use_case": "PROVISION",
  "version": {
    "template": "1.0.0",
    "compatibility": [
      "2.12.0",
      "3.0.0"
    ]
  },
  "workflows": {
    "provision": {
      "nodes": [
        {
          "id": "create_claude_connector",
          "type": "create_connector",
          "user_inputs": {
            "name": "Claude Instant Runtime Connector",
            "version": "1",
            "protocol": "aws_sigv4",
            "description": "The connector to BedRock service for Claude model",
            "actions": [
              {
                "headers": {
                  "x-amz-content-sha256": "required",
                  "content-type": "application/json"
                },
                "method": "POST",
                "request_body": "{ \"prompt\":\"${parameters.prompt}\",
 \"max_tokens_to_sample\":${parameters.max_tokens_to_sample},
 \"temperature\":${parameters.temperature},  \"anthropic_version\":
\"${parameters.anthropic_version}\" }",
```

```
                "action_type": "predict",
                "url": "https://bedrock-runtime.us-west-2.amazonaws.com/model/
anthropic.claude-instant-v1/invoke"
              }
            ],
            "credential": {
                "roleArn": "arn:aws:iam::account-id:role/opensearch-secretmanager-
role"
             },
            "parameters": {
              "endpoint": "bedrock-runtime.us-west-2.amazonaws.com",
              "content_type": "application/json",
              "auth": "Sig_V4",
              "max_tokens_to_sample": "8000",
              "service_name": "bedrock",
              "temperature": "0.0001",
              "response_filter": "$.completion",
              "region": "us-west-2",
              "anthropic_version": "bedrock-2023-05-31"
            }
          }
        }
      ]
    }
  }
}
```

如果您的網域位於虛擬私有雲 (Amazon VPC) 內，則必須連線至 Amazon VPC，才能成功建立 AI 連接器的請求。存取 Amazon VPC 會因網路組態而異，但通常涉及連線到 VPN 或公司網路。要檢查您是否可以訪問 OpenSearch 服務域，請`https://your-vpc-domain.region.es.amazonaws.com`在 Web 瀏覽器中導航到並確認您收到默認的 JSON 響應。

示例 Python 客戶端

Python 客戶端比HTTP請求更容易自動化，並且具有更好的可重用性。若要使用 Python 用戶端建立 AI 連接器，請將下列範例程式碼儲存至 Python 檔案。客戶端需要用 AWS SDK for Python (Boto3)，請求：HTTP 為人類，以及請求-aws4Auth 1.2.3 軟件包。

```
import boto3
import requests
from requests_aws4auth import AWS4Auth

host = 'domain-endpoint/'
```

```
region = 'region'
service = 'es'
credentials = boto3.Session().get_credentials()
awsauth = AWS4Auth(credentials.access_key, credentials.secret_key, region, service,
 session_token=credentials.token)

path = '_plugins/_flow_framework/workflow'
url = host + path

payload = {
  "name": "Deploy Claude Model",
  "description": "Deploy a model using a connector to Claude",
  "use_case": "PROVISION",
  "version": {
    "template": "1.0.0",
    "compatibility": [
      "2.12.0",
      "3.0.0"
    ]
  },
  "workflows": {
    "provision": {
      "nodes": [
        {
          "id": "create_claude_connector",
          "type": "create_connector",
          "user_inputs": {
            "name": "Claude Instant Runtime Connector",
            "version": "1",
            "protocol": "aws_sigv4",
            "description": "The connector to BedRock service for Claude model",
            "actions": [
              {
                "headers": {
                  "x-amz-content-sha256": "required",
                  "content-type": "application/json"
                },
                "method": "POST",
                "request_body": "{ \"prompt\":\"${parameters.prompt}\",
 \"max_tokens_to_sample\":${parameters.max_tokens_to_sample},
 \"temperature\":${parameters.temperature},  \"anthropic_version\":
\"${parameters.anthropic_version}\" }",
                "action_type": "predict",
```

```
                "url": "https://bedrock-runtime.us-west-2.amazonaws.com/model/
anthropic.claude-instant-v1/invoke"
              }
            ],
            "credential": {
                "roleArn": "arn:aws:iam::account-id:role/opensearch-secretmanager-
role"
             },
            "parameters": {
              "endpoint": "bedrock-runtime.us-west-2.amazonaws.com",
              "content_type": "application/json",
              "auth": "Sig_V4",
              "max_tokens_to_sample": "8000",
              "service_name": "bedrock",
              "temperature": "0.0001",
              "response_filter": "$.completion",
              "region": "us-west-2",
              "anthropic_version": "bedrock-2023-05-31"
            }
          }
        }
      ]
    }
  }
}

headers = {"Content-Type": "application/json"}

r = requests.post(url, auth=awsauth, json=payload, headers=headers)
print(r.status_code)
print(r.text)
```

預定義工作流程

Amazon OpenSearch 服務針對一些常見的機器學習 (ML) 使用案例提供數個工作流程範本。使用範本可簡化複雜的設定，並為語義或交談式搜尋等使用案例提供許多預設值。您可以在呼叫「建立工作流程 API」時指定工作流程範本。

- 欲使用「 OpenSearch 服務」提供的工作流程範本，請將範本使用案例指定為 `use_case` query 參數。
- 欲使用自訂工作流程範本，請在要求主體中提供完整的範本。如需自訂範本的範例，請參閱範例 JSON 範本或範例 YAML 範本。

範本使用案例

此表格提供可用的不同樣板、樣板說明以及必要參數的簡介。

範本使用案例	描述	必要參數
bedrock_titan_embedding_model_deploy	建立和部署 Amazon 基岩嵌入模型 (依預設 titan-embed-text-v1	create_connector.credential.roleArn
bedrock_titan_embedding_model_deploy	建立和部署 Amazon 基岩多模式嵌入模型 (依預設 titan-embed-text-v1	create_connector.credential.roleArn
cohere_embedding_model_deploy	建立並部署 Cohere 內嵌模型 (預設為 embed-english-v 3.0)。	create_connector.credential.roleArn , create_connector.credential.secretArn
cohere_chat_model_deploy	創建和部署一個 Cohere 聊天模式（默認情況下，Cohere 命令）。	create_connector.credential.roleArn , create_connector.credential.secretArn
open_ai_embedding_model_deploy	建立及部署 OpenAI 內嵌模型 (預設為 text-embedding-ada -002)。	create_connector.credential.roleArn , create_connector.credential.secretArn
openai_chat_model_deploy	創建和部署一個 OpenAI 聊天模型（默認情況下，gpt-3.5 渦輪增壓）。	create_connector.credential.roleArn , create_connector.credential.secretArn
semantic_search_wi	配置語義搜索並部署 Cohere 嵌入模型。您必須提供 Cohere 模型的 API 金鑰。	create_connector.credential.roleArn ,

範本使用案例	描述	必要參數
`th_cohere_embedding`		`create_connector.credential.secretArn`
`semantic_search_with_cohere_embedding_query_enricher`	配置語義搜索並部署 Cohere 嵌入模型。添加一個 query_enrich 搜索處理器，該處理器可設置類神經查詢的默認模型 ID。您必須提供 Cohere 模型的 API 金鑰。	`create_connector.credential.roleArn` ，`create_connector.credential.secretArn`
`multimodal_search_with_bedrock_titan`	部署 Amazon 基岩多模式模型，並使用 text_image_嵌入處理器和k-nN 索引來進行多模態搜尋來設定擷取管道。您必須提供您的 AWS 憑據。	`create_connector.credential.roleArn`

> **Note**
>
> 對於需要秘密 ARN 的所有模板，默認值是在秘 AWS 密管理器中以「密鑰」的密鑰名稱存儲密鑰。

具有預先訓練模型的預設範本

Amazon OpenSearch 服務提供兩個開放 OpenSearch 原始碼服務中無法使用的額外預設工作流程範本。

範本使用案例	描述
`semantic_search_with_local_model`	設定語意搜尋並部署預先訓練的模型 ()。`msmarco-distilbert-base-tas-b`新增`neural_query_enricher` 搜尋處理器，該處理器可設定神經查詢的預設模型 ID，並建立名為 " my-nlp-index 的連結 k-nN 索引。

範本使用案例	描述
hybrid_search_with_local_model	設定混合式搜尋並部署預先訓練的模型 ()。msmarco-distilbert-base-tas-b新增neural_query_enricher 搜尋處理器，該處理器可設定神經查詢的預設模型 ID，並建立名為 " my-nlp-index 的連結 k-nN 索引。

設定許可

如果您使用 2.13 版或更新版本建立新網域，則權限已存在。如果您在 2.11 版或更早版本的既有 OpenSearch 服務網域上啟用流程架構，然後升級至 2.13 版或更新版本，則必須定義角色。flow_framework_manager非系統管理員使用者必須映射至此角色，以便在使用精細存取控制的網域上管理暖索引。若要手動建立 flow_framework_manager 角色，請執行以下步驟：

1. 在 OpenSearch 儀表板中，轉到安全性，然後選擇權限。
2. 選擇 Create action group (建立動作群組) 並設定下列群組：

Group name (群組名稱)	許可
flow_framework_full_access	• cluster:admin/opensearch/flow_framework/* • cluster_monitor
flow_framework_read_accesss	• cluster:admin/opensearch/flow_framework/workflow/get • cluster:admin/opensearch/flow_framework/workflow/search • cluster:admin/opensearch/flow_framework/workflow_state/get • cluster:admin/opensearch/flow_framework/workflow_state/search

3. 選擇 Roles (角色)，然後選擇 Create role (建立角色)。
4. 命名角色流程框架管理器。

5. 對於 Cluster permissions (叢集許可)，選取 `flow_framework_full_access` 和 `flow_framework_read_access`。
6. 對於 Index (索引)，輸入 `*`。
7. 對於 Index permissions (索引許可)，選取 `indices:admin/aliases/get`、`indices:admin/mappings/get` 以及 `indices_monitor`。
8. 選擇建立。
9. 建立角色後，請將其對應至將管理流程架構索引的任何使用者或後端角色。

Amazon OpenSearch 服務的安全分析

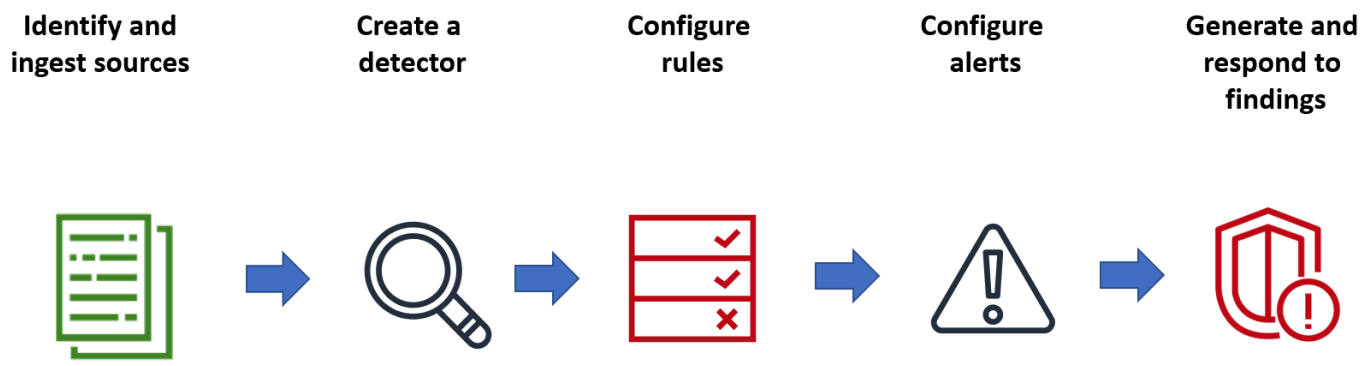
安全性分析是一種 OpenSearch 解決方案，可讓您瞭解組織的基礎架構、監控異常活動、即時偵測潛在安全威脅，以及對預先設定的目的地觸發警示。您可以持續評估安全性規則並檢閱自動產生的安全性發現項目，從安全事件記錄檔監控惡意活動。此外，安全性分析可以產生自動警示，並將其傳送至指定的通知管道，例如 Slack 或電子郵件。

您可以使用 Security Analytics 外掛程式偵測常見威脅， out-of-the-box 並從現有的安全性事件記錄檔 (例如防火牆記錄、Windows 記錄和驗證稽核記錄) 產生重要的安全性洞見。若要使用安全性分析，您的網域必須執行 2.5 OpenSearch 版或更新版本。

> **Note**
>
> 本文件提供適用於 Amazon OpenSearch 服務的安全分析的簡要概觀。它定義了關鍵概念，並提供了配置權限的步驟。如需完整文件，包括設定指南、API 參考，以及所有可用設定的參考資料，請參閱 OpenSearch 文件中的安全性分析。

安全性分析元件和概念

許多工具和功能為安全性分析的運作提供了基礎。構成插件的主要組件包括檢測器，日誌類型，規則，發現和警報。



記錄檔類型

OpenSearch 支援數種類型的記錄，並提供每種類型的 out-of-the-box 對應。您可以在建立偵測器時指定記錄類型並設定時間間隔，然後安全性分析會自動啟動以該間隔執行的一組相關規則。

偵測器

偵測器可識別各種資料索引中某種記錄類型的一系列網路安全威脅。您可以將偵測器設定為使用自訂規則和預先封裝的 Sigma 規則來評估系統中發生的事件。然後，偵測器會從這些事件產生安全發現項目。如需有關偵測器的詳細資訊，請參閱文件中的 OpenSearch 建立偵測器。

規則

威脅偵測規則會定義偵測器套用至擷取記錄檔資料以識別安全事件的條件。安全性分析支援匯入、建立和自訂規則以符合您的需求，並提供預先封裝的開放原始碼 Sigma 規則，以偵測記錄檔中的常見威脅。安全分析將許多規則映射到由 MITRE ATT&CK 組織維護的對手戰術和技術的不斷增長的知識庫。您可以同時使用 OpenSearch 儀表板或 API 來建立和使用規則。如需有關規則的詳細資訊，請參閱使用 OpenSearch 文件中的規則。

問題清單

偵測器將規則與記錄事件相符時，會產生一個發現項目。每個發現項目都包含選取規則、記錄類型和規則嚴重性的唯一組合。發現項目不一定指向系統內即將發生的威脅，但它們總是隔離感興趣的事件。如需有關發現項目的詳細資訊，請參閱 OpenSearch 文件中的使用發現項目。

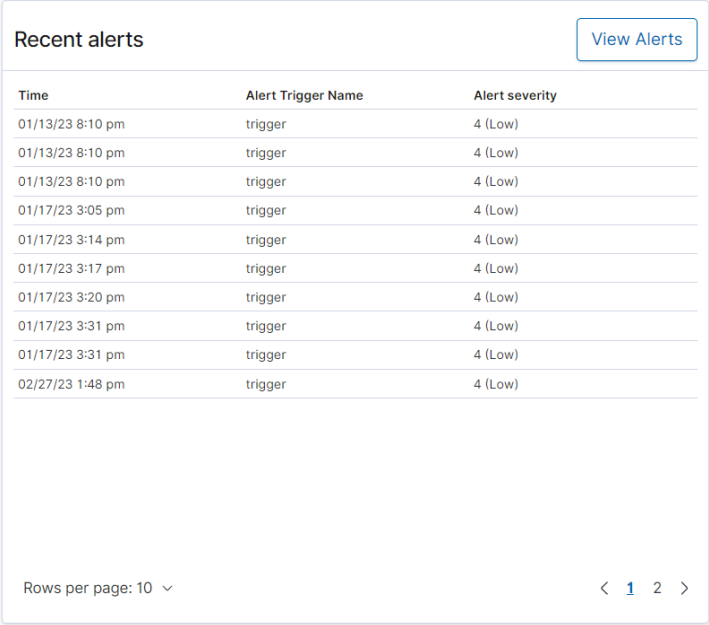
Alerts (提醒)

建立偵測器時，您可以指定一或多個觸發警示的條件。警示是傳送至偏好頻道的通知，例如 Slack 或電子郵件。您可以設定偵測器符合一或多個規則時觸發的警示，並且可以自訂通知訊息。如需警示的詳細資訊，請參閱 OpenSearch 文件中的使用警示。

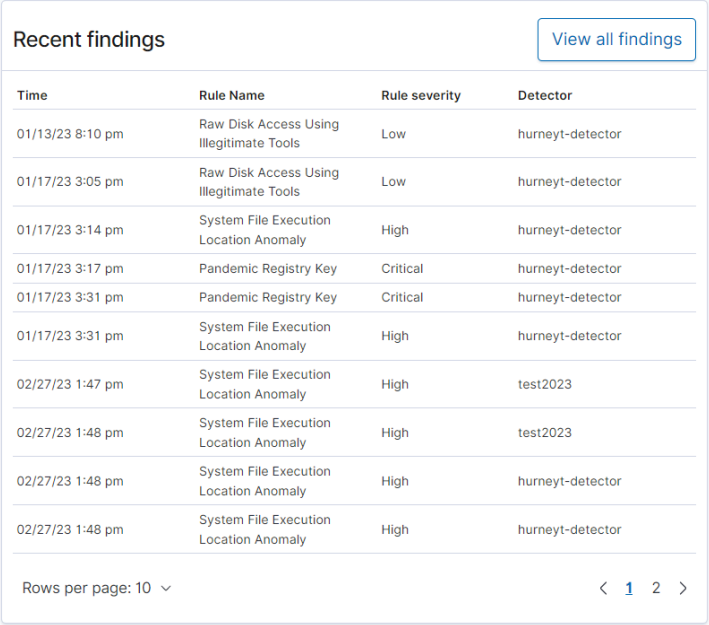
探索安全性分析

您可以使用 OpenSearch 儀表板來視覺化並深入瞭解您的安全性分析外掛程式。「概觀」檢視可提供諸如發現項目和警示計數、最近發現項目和警示、頻繁偵測規則以及偵測器清單等資訊。您可以看到由多個視覺效果組成的摘要檢視。例如，下圖顯示指定期間內各種日誌類型的發現項目和警示趨勢。

在頁面下方，您可以查看最近的發現和警示。



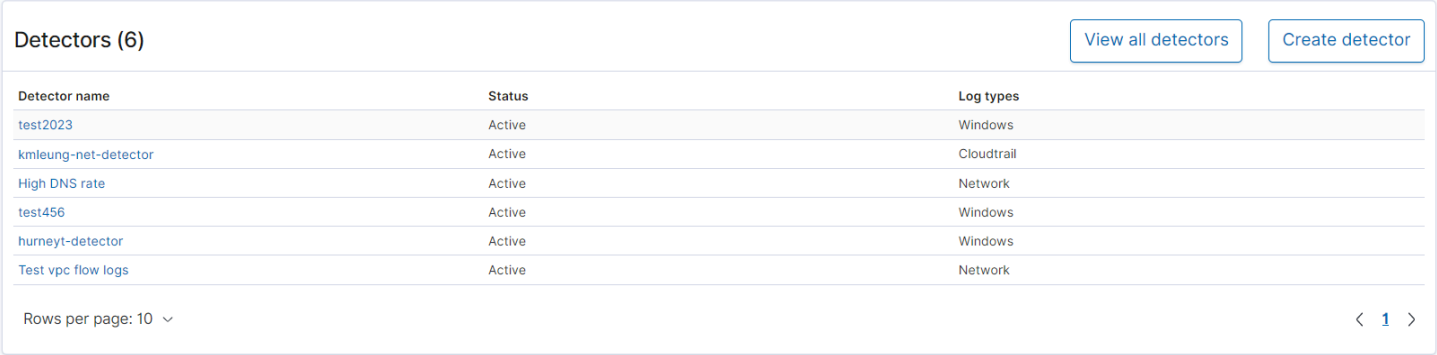
Time	Alert Trigger Name	Alert severity
01/13/23 8:10 pm	trigger	4 (Low)
01/13/23 8:10 pm	trigger	4 (Low)
01/13/23 8:10 pm	trigger	4 (Low)
01/17/23 3:05 pm	trigger	4 (Low)
01/17/23 3:14 pm	trigger	4 (Low)
01/17/23 3:17 pm	trigger	4 (Low)
01/17/23 3:20 pm	trigger	4 (Low)
01/17/23 3:31 pm	trigger	4 (Low)
01/17/23 3:31 pm	trigger	4 (Low)
02/27/23 1:48 pm	trigger	4 (Low)



Time	Rule Name	Rule severity	Detector
01/13/23 8:10 pm	Raw Disk Access Using Illegitimate Tools	Low	hurneyt-detector
01/17/23 3:05 pm	Raw Disk Access Using Illegitimate Tools	Low	hurneyt-detector
01/17/23 3:14 pm	System File Execution Location Anomaly	High	hurneyt-detector
01/17/23 3:17 pm	Pandemic Registry Key	Critical	hurneyt-detector
01/17/23 3:31 pm	Pandemic Registry Key	Critical	hurneyt-detector
01/17/23 3:31 pm	System File Execution Location Anomaly	High	hurneyt-detector
02/27/23 1:47 pm	System File Execution Location Anomaly	High	test2023
02/27/23 1:48 pm	System File Execution Location Anomaly	High	test2023
02/27/23 1:48 pm	System File Execution Location Anomaly	High	hurneyt-detector
02/27/23 1:48 pm	System File Execution Location Anomaly	High	hurneyt-detector

此外，您還可以看到所有作用中偵測器中最常觸發的規則的分佈情況。這可協助您偵測和調查各種記錄類型的不同類型的惡意活動。

最後，您可以檢視已設定偵測器的狀態。從此面板中，您也可以導覽至建立偵測器工作流程。



若要設定安全性分析設定，請使用「規則」頁面建立規則，然後使用這些規則在「偵測器」頁面中撰寫偵測器。若要更集中檢視安全分析結果，您可以使用「發現項目」和「警示」頁面。

設定許可

如果您在預先存在的 OpenSearch 服務網域上啟用安全性分析，則該`security_analytics_manager`角色可能不會在網域上定義。非系統管理員使用者必須映射至此角色，以便在使用精細存取控制的網域上管理暖索引。若要手動建立 `security_analytics_manager` 角色，請執行以下步驟：

1. 在 OpenSearch 儀表板中，轉到安全性，然後選擇權限。
2. 選擇 Create action group (建立動作群組) 並設定下列群組：

Group name (群組名稱)	許可
security_analytics_full_access	• cluster:admin/opensearch/securityanalytics/alerts/* • cluster:admin/opensearch/securityanalytics/detector/* • cluster:admin/opensearch/securityanalytics/findings/* • cluster:admin/opensearch/securityanalytics/mapping/* • cluster:admin/opensearch/securityanalytics/rule/*
security_analytics_read_access	• cluster:admin/opensearch/securityanalytics/alerts/get • cluster:admin/opensearch/securityanalytics/detector/get • cluster:admin/opensearch/securityanalytics/detector/search • cluster:admin/opensearch/securityanalytics/findings/get • cluster:admin/opensearch/securityanalytics/mapping/get • cluster:admin/opensearch/securityanalytics/mapping/view/get • cluster:admin/opensearch/securityanalytics/rule/get • cluster:admin/opensearch/securityanalytics/rule/search

3. 選擇 Roles (角色)，然後選擇 Create role (建立角色)。
4. 將角色命名為安全性管理員。

5. 對於 Cluster permissions (叢集許可)，選取 `security_analytics_full_access` 和 `security_analytics_read_access`。
6. 對於 Index (索引)，輸入 `*`。
7. 對於索引權限，請選取`indices:admin/mapping/put`和`indices:admin/mappings/get`。
8. 選擇建立。
9. 建立角色後，請將其對應至將管理安全性分析索引的任何使用者或後端角色。

故障診斷

沒有這樣的索引錯誤

如果您沒有偵測器，而且開啟「安全分析」儀表板，您可能會在右下角看到通知。`[index_not_found_exception] no such index [.opensearch-sap-detectors-config]`您可以忽略此通知，該通知會在幾秒鐘內消失，並且在創建檢測器後不會再次出現。

Amazon OpenSearch 服務中的可觀察性

Amazon Ser OpenSearch vice 的預設 OpenSearch 儀表板安裝包括可觀察性外掛程式，您可以使用管道處理語言 (PPL) 將資料導向的事件視覺化，以便探索、探索和查詢儲存在中的資料。 OpenSearch該插件需要 OpenSearch 1.2 或更高版本。

可觀測性外掛程式為從常見資料來源收集和監控指標、日誌和跟蹤提供了統一的體驗。在單一位置收集和監控資料，可讓您的整個基礎架構完整堆疊、 end-to-end 可觀察。

> **Note**
>
> 本文件提供 OpenSearch 服務中可觀察性的簡要概觀。如需觀察性外掛程式的完整文件 (包括權限)，請參閱可觀測性。

每個人的資料探索程序都不相同。如果您是探索資料和建立視覺效果的新手，建議您嘗試如下所示的工作流程。

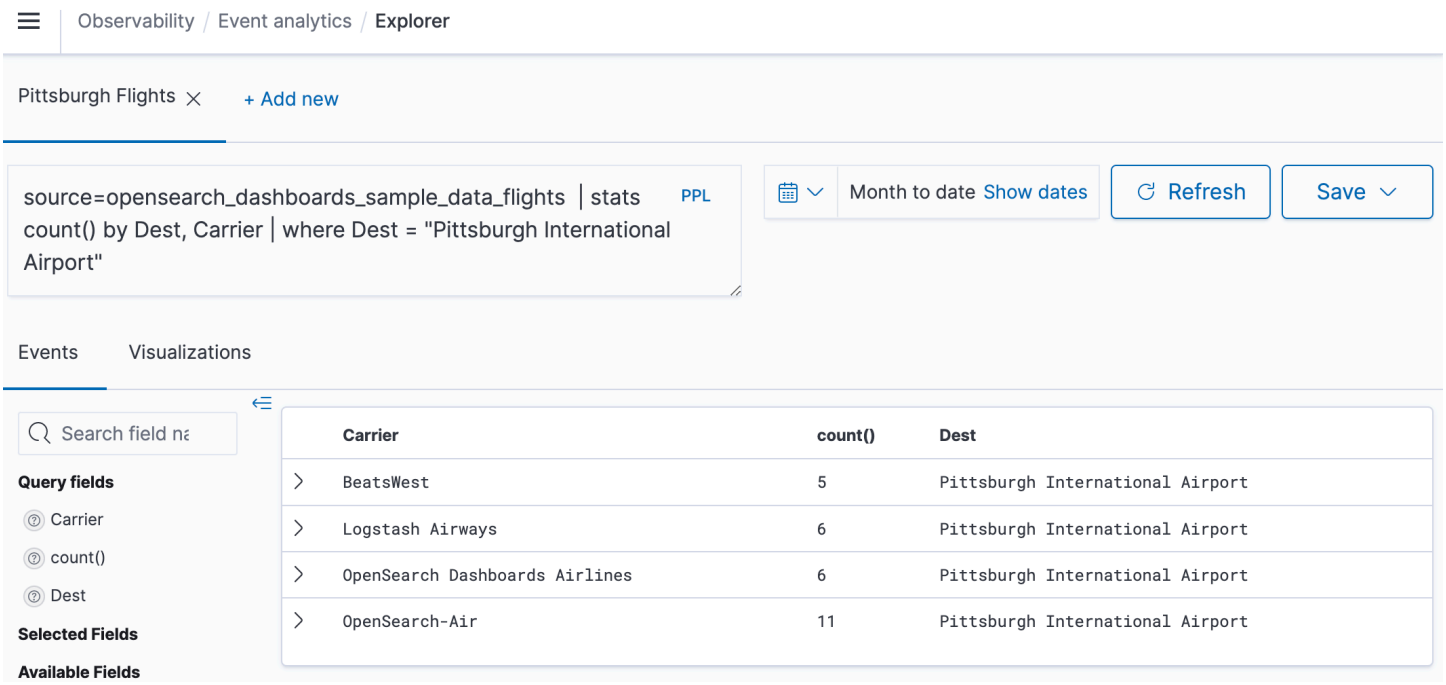
利用事件分析探索您的資料

首先，假設您正在收集 OpenSearch 服務網域中的航班資料，並且想知道上個月抵達匹茲堡國際機場的航班最多的航班是哪家航空公司。您可以編寫以下 PPL 查詢：

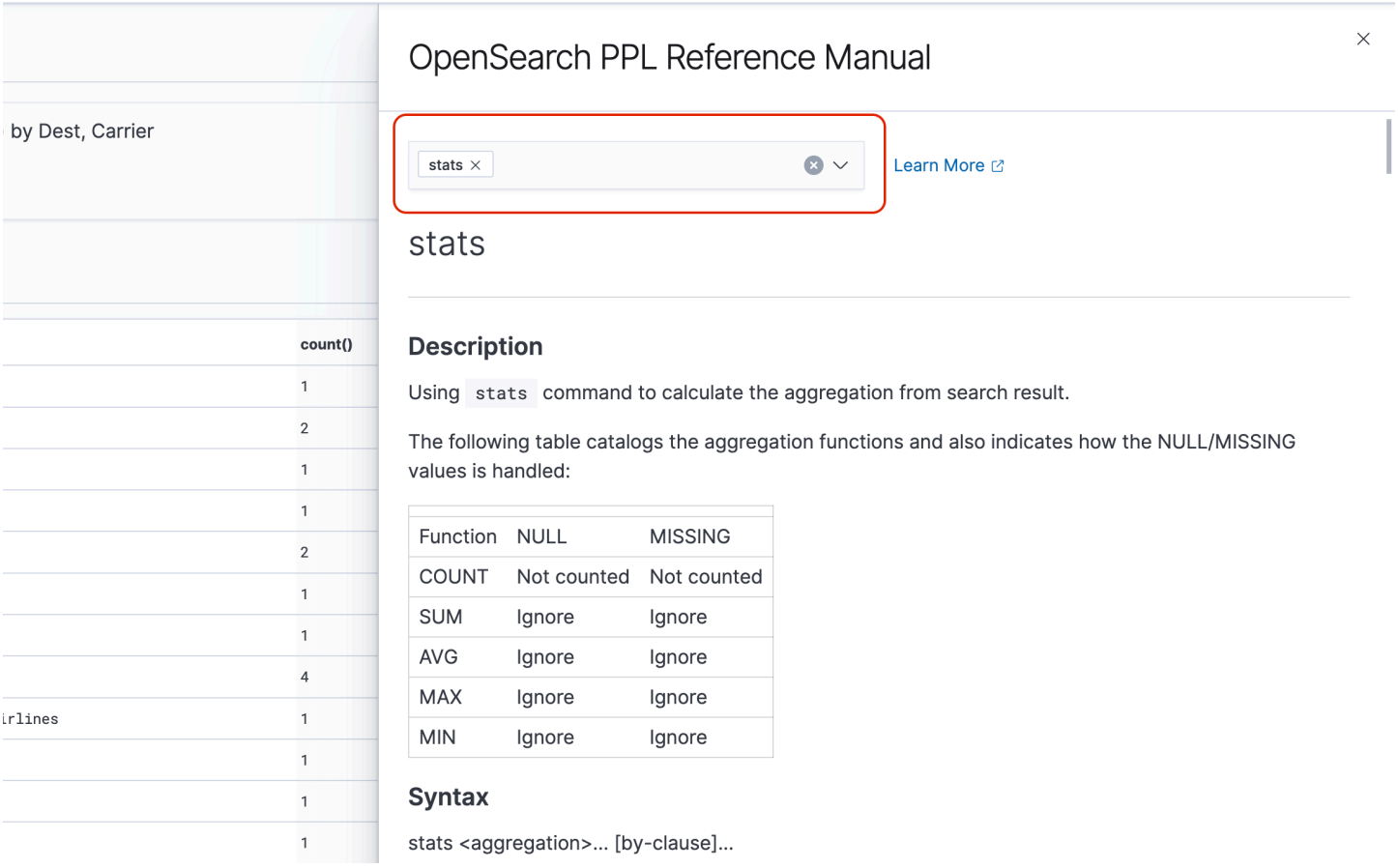
```
source=opensearch_dashboards_sample_data_flights |
    stats count() by Dest, Carrier |
    where Dest = "Pittsburgh International Airport"
```

此查詢從名為 `opensearch_dashboards_sample_data_flights` 的索引中調取資料。然後使用 `stats` 命令取得航班總數，並根據目的地機場和航空公司進行分組。最後，其使用 `where` 子句來篩選結果，找出抵達匹茲堡國際機場的航班。

顯示的上個月資料如下所示：



您可以選擇查詢編輯器中的 PPL 按鈕，取得每個 PPL 命令的使用資訊和示例：



讓我們來看一個更複雜的示例，其查詢與航班誤點有關的資訊：

```
source=opensearch_dashboards_sample_data_flights |
    where FlightDelayMin > 0 |
    stats sum(FlightDelayMin) as minimum_delay, count() as total_delayed by Carrier,
 Dest |
    eval avg_delay=minimum_delay / total_delayed |
    sort - avg_delay
```

查詢中的每個命令都會影響最終輸出：

- `source=opensearch_dashboards_sample_data_flights` – 從與上一個示例相同的索引中調取資料
- `where FlightDelayMin > 0` – 篩選資料，以取得誤點的航班
- `stats sum(FlightDelayMin) as minimum_delay, count() as total_delayed by Carrier` – 針對每家航空公司，取得最短總誤點時間和誤點航班總數
- `eval avg_delay=minimum_delay / total_delayed` – 藉由將最短誤點時間除以誤點航班總數，計算每家航空公司的平均誤點時間
- `sort - avg_delay` – 依平均誤點以降序對結果進行排序

透過此查詢，您可以判斷 OpenSearch 儀表板航空公司的延遲平均較少。

avg_delay	Carrier	minimum_delay	total_delayed
212	Logstash Airways	4470	21
184	OpenSearch-Air	4245	23
155	BeatsWest	2025	13
153	OpenSearch Dashboards Airlines	4305	28

您可以在 Event analytics (事件分析) 頁面的 Queries and Visualizations (查詢和視覺化效果) 之下，找到更多範例 PPL 查詢。

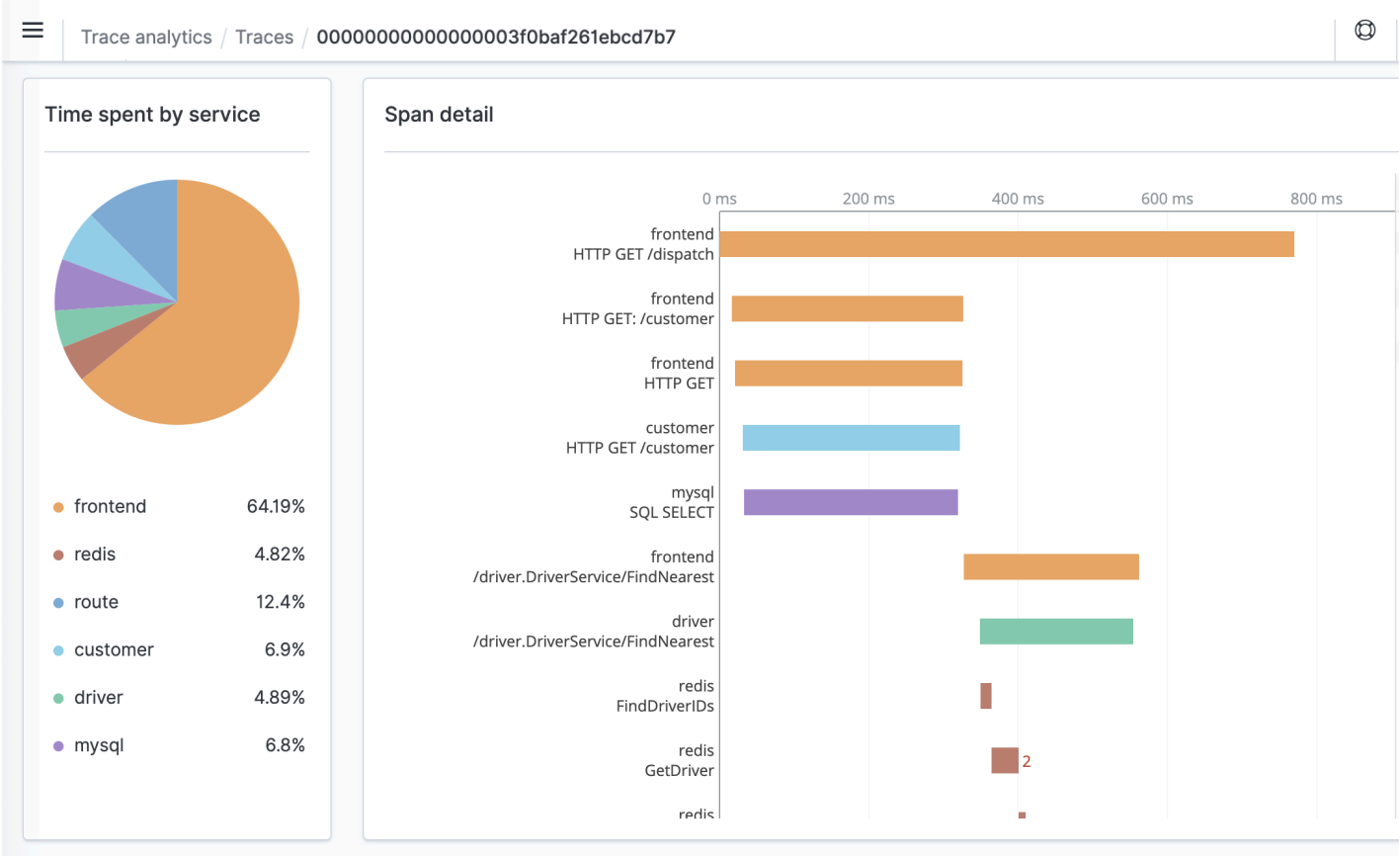
建立視覺化效果

正確查詢到您感興趣的資料後，可將這些查詢另存為視覺化效果：

然後將這些視覺化效果新增到操作面板中，以比較不同的資料片段。利用筆記本來組合可與團隊成員共享的不同視覺化效果和程式碼區塊。

利用 Trace Analytics 進行深入分析

追蹤分析提供一種視覺化 OpenSearch 資料中事件流程的方法，以識別並修正分散式應用程式中的效能問題。



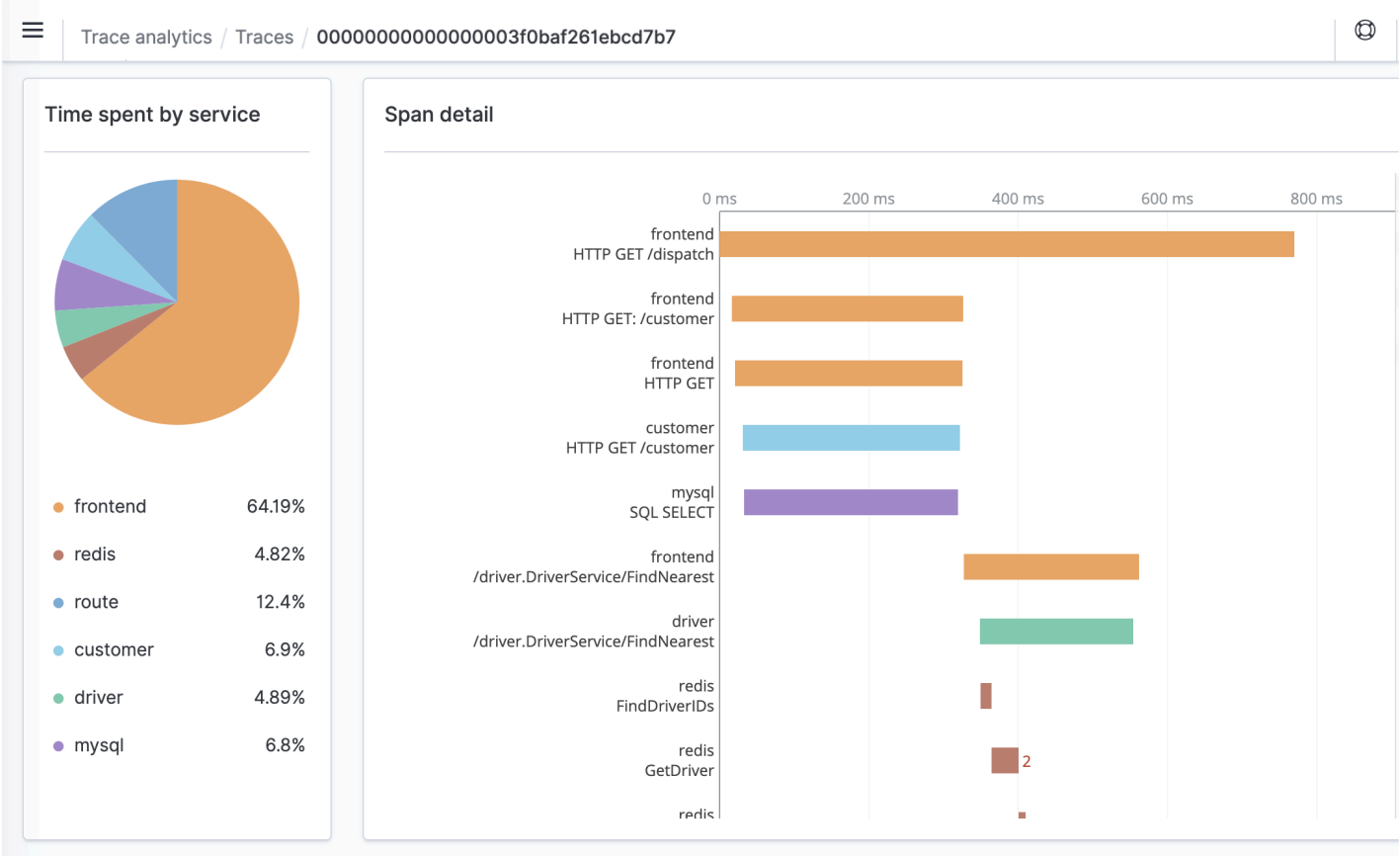
Amazon OpenSearch 服務的跟踪分析

您可以使用追蹤分析 (屬於可 OpenSearch 觀測性外掛程式的一部分) 來分析來自分散式應用程式的追蹤資料。追蹤分析需要 OpenSearch 或彈性搜尋 7.9 或更新版本。

在分散式應用程式中，單一操作 (例如使用者按一下按鈕) 可觸發一系列延伸事件。例如，應用程式前端可能會呼叫後端服務，這會呼叫另一個服務，查詢資料庫，處理查詢並傳回結果。然後，第一個後端服務會將確認傳送到前端，以便更新 UI。

您可以使用 Trace Analytics 來協助您將此事件流程視覺化並發現效能問題。

> **Note**
>
> 本文件提供追蹤分析的簡短概觀。如需完整文件，請參閱開放原始碼 OpenSearch 文件中的追蹤分析。



必要條件

追蹤分析會要求您將儀器新增至應用程式，並使用 OpenTelemetry支援的程式庫 (例如 Jaeger 或 Zipkin) 產生追蹤資料。此步驟完全發生在 OpenSearch 服務之外。用於 OpenTelemetry 文檔的發行AWS 版包含許多編程語言的示例應用程序，可以幫助您開始使用，包括 Java，Python，Go 和 JavaScript.

將檢測新增至應用程式之後，收OpenTelemetry集器會從應用程式接收資料，並將其格式化為 OpenTelemetry 資料。請參閱上的接收機清單GitHub。 AWS 發行版 OpenTelemetry 包括一個接收器 AWS X-Ray.

最後，您可以使用格Amazon OpenSearch 攝入式化該 OpenTelemetry 資料以便搭配使用 OpenSearch。

OpenTelemetry 收集器範例組態

若要搭配使用 OpenTelemetry 收集器Amazon OpenSearch 攝入，請嘗試下列範例組態：

```
extensions:
```

```
  sigv4auth:
    region: "us-east-1"
    service: "osis"

receivers:
  jaeger:
    protocols:
      grpc:

exporters:
  otlphttp:
    traces_endpoint: "https://pipeline-endpoint.us-east-1.osis.amazonaws.com/
opentelemetry.proto.collector.trace.v1.TraceService/Export"
    auth:
      authenticator: sigv4auth
    compression: none

service:
  extensions: [sigv4auth]
  pipelines:
    traces:
      receivers: [jaeger]
      exporters: [otlphttp]
```

OpenSearch 擷取範例組態

若要將追蹤資料傳送至 OpenSearch 服務網域，請嘗試下列 OpenSearch 擷取管線組態範例。如需建立管線的指示，請參閱the section called “建立管道”。

```
version: "2"
otel-trace-pipeline:
  source:
    otel_trace_source:
      "/${pipelineName}/ingest"
  processor:
    - trace_peer_forwarder:
  sink:
    - pipeline:
        name: "trace_pipeline"
    - pipeline:
        name: "service_map_pipeline"
trace-pipeline:
  source:
```

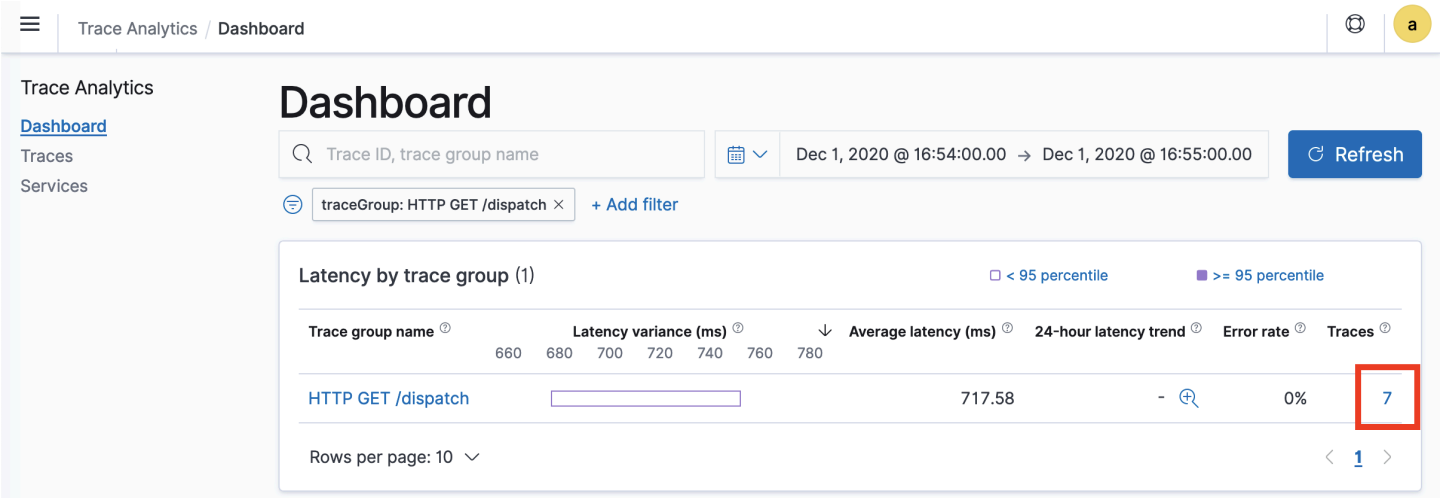
```
    pipeline:
      name: "otel-trace-pipeline"
  processor:
    - otel_traces:
  sink:
    - opensearch:
        hosts: ["https://domain-endpoint"]
        index_type: trace-analytics-raw
        aws:
          # IAM role that OpenSearch Ingestion assumes to access the domain sink
          sts_role_arn: "arn:aws:iam::{account-id}:role/pipeline-role"
          region: "us-east-1"

service-map-pipeline:
  source:
    pipeline:
      name: "otel-trace-pipeline"
  processor:
    - service_map:
  sink:
    - opensearch:
        hosts: ["https://domain-endpoint"]
        index_type: trace-analytics-service-map
        aws:
          # IAM role that the pipeline assumes to access the domain sink
          sts_role_arn: "arn:aws:iam::{account-id}:role/pipeline-role"
          region: "us-east-1"
```

您在`sts_role_arn`選項中指定的管線角色必須具有接收器的寫入權限。如需設定管線角色權限的指示，請參閱the section called “設定角色和使用者”。

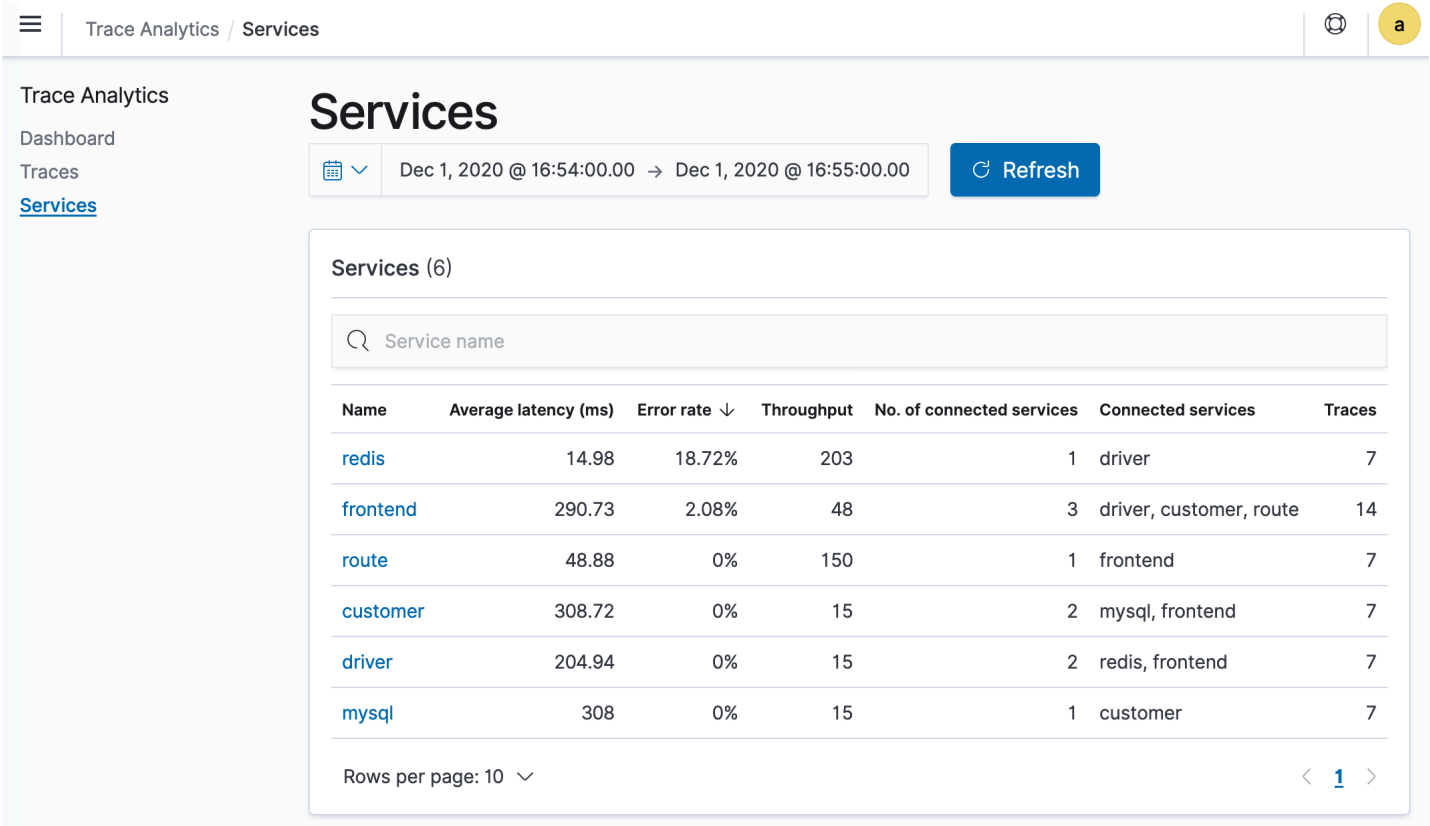
瀏覽追蹤資料

Dashboard (儀表板) 檢視會依 HTTP 方法和路徑將追蹤集中在一起，以便您可以查看與特定操作相關聯的平均延遲、錯誤率和趨勢。如需更詳細的檢視，請嘗試按照追蹤群組名稱進行篩選。



若要深入了解構成追蹤群組的追蹤，請在右欄中選擇追蹤數目。然後選擇個別追蹤以取得詳細摘要。

Services (服務) 檢視會列出應用程式中的所有服務，以及顯示各種服務如何彼此互連的互動式地圖。與儀表板 (可協助依操作發現問題) 相反，服務地圖可協助您透過服務發現問題。嘗試依錯誤率或延遲排序，以了解應用程式的潛在問題區域。



使用管道處理語言查詢 Amazon OpenSearch 服務資料

管道處理語言 (PPL) 是一種查詢語言，可讓您使用管道 (|) 語法查詢儲存在 Amazon OpenSearch 服務中的資料。PPL 需要或彈性搜索 7.9 OpenSearch 或更高版本。

> **Note**
>
> 本文件提供了適用於 Amazon OpenSearch 服務的 PPL 的簡要概述。如需詳細步驟和完整的命令參考資料，請參閱開放原始碼 OpenSearch 文件中的 PPL。

PPL 語法包含以管道字元 (|) 分隔的命令，資料在其中通過每個管道從左流到右。例如，用來尋找具有 HTTP 403 或 503 錯誤的主機數目、依據主機進行彙總並依影響順序對它們排序的 PPL 語法，如下所示：

```
source = dashboards_sample_data_logs | where response='403' or response='503' | stats
 count(request) as request_count by host, response | sort -request_count
```

若要開始使用，請選擇 OpenSearch 儀表板中的查詢工作台，然後選取 PPL。使用 `bulk` 操作來索引一些範例資料：

```
PUT accounts/_bulk?refresh
{"index":{"_id":"1"}}
{"account_number":1,"balance":39225,"firstname":"Amber","lastname":"Duke","age":32,"gender":"M"
 Holmes
 Lane","employer":"Pyrami","email":"amberduke@pyrami.com","city":"Brogan","state":"IL"}
{"index":{"_id":"6"}}
{"account_number":6,"balance":5686,"firstname":"Hattie","lastname":"Bond","age":36,"gender":"M"
 Bristol
 Street","employer":"Netagy","email":"hattiebond@netagy.com","city":"Dante","state":"TN"}
{"index":{"_id":"13"}}
{"account_number":13,"balance":32838,"firstname":"Nanette","lastname":"Bates","age":28,"gender"
 Mady Street","employer":"Quility","city":"Nogal","state":"VA"}
{"index":{"_id":"18"}}
{"account_number":18,"balance":4180,"firstname":"Dale","lastname":"Adams","age":33,"gender":"M"
 Hutchinson Court","email":"daleadams@boink.com","city":"Orick","state":"MD"}
```

下列範例會對 `age` 大於 18 的帳戶索引中的文件傳回 `firstname` 和 `lastname` 欄位：

```
search source=accounts | where age > 18 | fields firstname, lastname
```

回應範例

id	firstname	lastname
0	Amber	Duke
1	Hattie	Bond
2	Nanette	Bates
3	Dale	Adams

您可以使用一組完整的唯讀命令，如 `search`、`where`、`fields`、`rename`、`dedup`、`stats`、`sort`、`eval`、`head`、`top` 以及 `rare`。PPL 外掛程式支援所有 SQL 函數，包括數學、三角函數、日期時間、字串、彙總以及進階運算子和表達式。若要進一步了解，請參閱 OpenSearch PPL 參考手冊。

Amazon OpenSearch 服務的操作最佳實踐

本章提供操作 Amazon OpenSearch 服務網域的最佳實務，並包含適用於許多使用案例的一般準則。每個工作負載都是獨一無二的，具有獨特的特性，因此沒有任何一個通用建議適合每個使用案例。最重要的最佳實務是在連續週期內部署、測試和調整網域，以找出適合您工作負載的最佳組態、穩定性和成本。

主題

- 監控和提醒
- 碎片策略
- 穩定性
- 效能
- 安全
- 成本最佳化
- 調整 Amazon OpenSearch 服務域
- Amazon 服務中的 PB 規模 OpenSearch
- Amazon OpenSearch 服務中的專用主節點
- 推薦的 Amazon 服 OpenSearch 務 CloudWatch 警報

監控和提醒

下列最佳作法適用於監視您的 OpenSearch 服務網域。

設定 CloudWatch 鬧鐘

OpenSearch 服務向 Amazon CloudWatch 發出性能指標。定期檢閱叢集和執行個體指標，並根據工作負載效能設定建議的 CloudWatch 警示。

啟用日誌發佈

OpenSearch 服務會在 Amazon 日誌中公開 OpenSearch 錯誤日誌、搜尋慢速日誌、編製慢速日誌索引以及稽核 CloudWatch 日誌。搜尋慢速日誌、索引慢速日誌和錯誤日誌對於疑難排解效能和穩定性問題非常有用。稽核日誌會追蹤使用者活動，只有在啟用精細存取控制時才能使用。如需詳細資訊，請參閱 OpenSearch 文件中的記錄。

搜尋慢速日誌和索引慢速日誌是了解和疑難排解搜尋和索引操作效能的重要工具。對所有生產網域啟用搜尋和索引慢速日誌傳送。您也必須設定記錄閾值 — 否則， CloudWatch 將不會擷取記錄檔。

碎片策略

碎片會將您的工作負載分配到 OpenSearch 服務網域中的資料節點。正確設定的索引有助於提升整體網域效能。

當您將資料傳送至 OpenSearch 服務時，您會將該資料傳送至索引。索引類似於資料庫的資料表，以文件作為列，欄位作為行。當您建立索引時，您會告訴您要建立多 OpenSearch 少個主要碎片。主碎片是完整數據集的獨立分區。 OpenSearch Service 會自動將您的資料分配到索引中的主要碎片。您也可以設定索引複本。每個複本都包含該索引之主要碎片的完整副本集。

OpenSearch 服務會在叢集中的資料節點之間對應每個索引的碎片。它可確保索引的主要碎片和複本碎片駐留在不同的資料節點上。第一個複本可確保索引中有兩個資料副本。您應該始終使用至少一個複本。額外的複本提供額外的備援和讀取容量。

OpenSearch 將索引請求發送到包含屬於索引的碎片的所有數據節點。它首先將索引請求傳送至包含主要碎片的資料節點，然後傳送至包含複本碎片的資料節點。搜尋請求會由協調器節點路由至屬於索引之所有碎片的主要或複本碎片。

例如，對於具有五個主要碎片和一個複本的索引，每個索引編製請求接觸 10 個碎片。相反，搜尋請求會傳送至 n 個碎片，其中 n 是主要碎片的數量。對於具有五個主要碎片和一個複本的索引，每個搜尋查詢接觸該索引中的五個碎片 (主要碎片或複本碎片)。

確定碎片和資料節點計數

請使用下列最佳實務來確定網域的碎片計數和資料節點計數。

碎片大小 - 磁碟上的資料大小是來源資料大小的直接結果，並且會隨著您編製更多資料的索引而變更。source-to-index 比例可能會有很大的不同，從 1:10 到 10:1 或更大，但通常是 1:1.10 左右。您可以使用該比率來預測磁碟上的索引大小。您也可以為某些資料建立索引，並擷取實際索引大小，以確定工作負載的比率。掌握預測的索引大小後，設定碎片計數，以便每個碎片介於 10–30 GiB 之間 (對於搜尋工作負載)，或介於 30-50 GiB 之間 (對於日誌工作負載)。50 GiB 應該是最大值 – 確保為增長做好計劃。

碎片計數 - 資料節點的碎片分佈對網域的效能有很大影響。當您具有包含多個碎片的索引時，嘗試使碎片計數為資料節點計數的偶數倍。這有助於確保碎片在資料節點之間均勻分佈，並防止熱節點。例如，如果您有 12 個主要碎片，則資料節點計數應為 2、3、4、6 或 12。但是，碎片計數不若碎片大小重要 – 如果您有 5 GiB 的資料，則仍應使用單一碎片。

每個資料節點的碎片 — 節點可以保留的碎片總數與節點的 Java 虛擬機器 (JVM) 堆積記憶體成正比。目標是每 GiB 堆積記憶體有 25 個或更少的碎片。例如，具有 32 GiB 堆積記憶體的節點應保留不超過 800 個碎片。雖然碎片分佈可能會根據您的工作負載模式而有所不同，但每個節點的碎片數限制為 1,000。cat/配置可API快速檢視跨資料節點的碎片數量和碎片儲存總數。

碎片CPU比例 — 當碎片參與索引或搜索請求時，它會使用 v CPU 來處理請求。最佳作法是使用CPU每個碎片 1.5 v 的初始縮放點。如果您的執行個體類型有 8 個vCPUs，請設定資料節點計數，讓每個節點的碎片不超過六個。請注意，這是一個近似值。請務必測試您的工作負載並相應調整叢集的規模。

如需有關儲存磁碟區、碎片大小和執行個體類型的建議，請參閱下列資源：

- the section called “調整網域大小”
- the section called “PB 規模”

避免儲存扭曲

儲存扭曲是指叢集中的一個或多個節點對一個或更多索引的儲存比例高於其他節點。儲存偏差的指示包括不均勻的CPU使用率、間歇性和不均勻的延遲，以及跨資料節點的佇列不均勻。若要判斷是否有扭曲問題，請參閱下列疑難排解部分：

- the section called “節點碎片和儲存扭曲”
- the section called “索引碎片和儲存扭曲”

穩定性

下列最佳作法適用於維護穩定且正常的 OpenSearch 服務網域。

保持最新 OpenSearch

服務軟體更新

OpenSearch Service 會定期發行新增功能或以其他方式改善網域的軟體更新。更新不會更改 OpenSearch 或彈性搜索引擎版本。我們建議您排定執行DescribeDomainAPI作業的週期性時間，並啟動服務軟體更新 (如果`UpdateStatus`是) `ELIGIBLE`。如果您未在特定時間範圍內更新網域 (通常為兩週)， OpenSearch 服務會自動執行更新。

OpenSearch 版本升級

OpenSearch 服務會定期增加對社群維護版本的 OpenSearch支援。請務必在可用時升級至最新 OpenSearch 版本。

OpenSearch 服務同時升級 OpenSearch 和 OpenSearch 儀表板（如果您的域正在運行傳統引擎，則可以同時升級 Elasticsearch 和 Kibana）。如果叢集有專用主節點，無須停機即可完成升級。否則，叢集在選取主節點時，可能會在升級後數秒內沒有回應。 OpenSearch 在部分或全部升級期間，儀表板可能無法使用。

有兩種方式可以升級網域：

- 就地升級 – 此選項更容易，因為您保留相同的叢集。
- 快照/還原升級 - 此選項適用於在新叢集上測試新版本或在叢集之間遷移。

無論您使用哪種升級程序，我們都建議您維護一個僅用於開發和測試的網域，並在升級您的生產網域之前先將其升級到新版本。建立測試網域時，對於部署類型，選擇 Development and testing (開發與測試)。請務必在網域升級後立即將所有用戶端升級至相容版本。

改善快照效能

為了避免快照在處理過程中卡住，專用主節點的執行個體類型應與碎片計數相符。如需詳細資訊，請參閱the section called “選擇專用主節點的執行個體類型”。此外，每個節點的 Java 堆積記憶體不應超過每 GiB 建議的 25 個碎片。如需詳細資訊，請參閱the section called “選擇碎片數”。

啟用專用主節點

專用主節點可改善叢集穩定性。專用主節點會執行叢集管理任務，但不會保留索引資料或回應用戶端請求。此叢集管理任務的卸載可增加網域的穩定性，並可在不停機的情況下進行一些組態變更。

啟用並使用三個專用主節點，以在三個可用區域中獲得最佳的網域穩定性。使用備用異地同步備份部署可為您設定三個專用主節點。如需執行個體類型建議，請參閱 the section called “選擇專用主節點的執行個體類型”。

在多個可用區域中進行部署

若要防止資料遺失，並在服務中斷時將叢集停機時間降到最低，您可以將節點分配到相同的兩個或三個可用區域 AWS 區域。 最佳做法是使用異地同步備份與待命進行部署，該備用區域會設定三個可用區域、兩個作用中的區域、一個作為待命區域，以及每個索引使用兩個複本碎片。此配置可讓 OpenSearch 服務將副本碎片分配到不同AZs於其對應的主碎片。可用區域之間的叢集通訊無需支付跨可用區域資料傳輸費用。

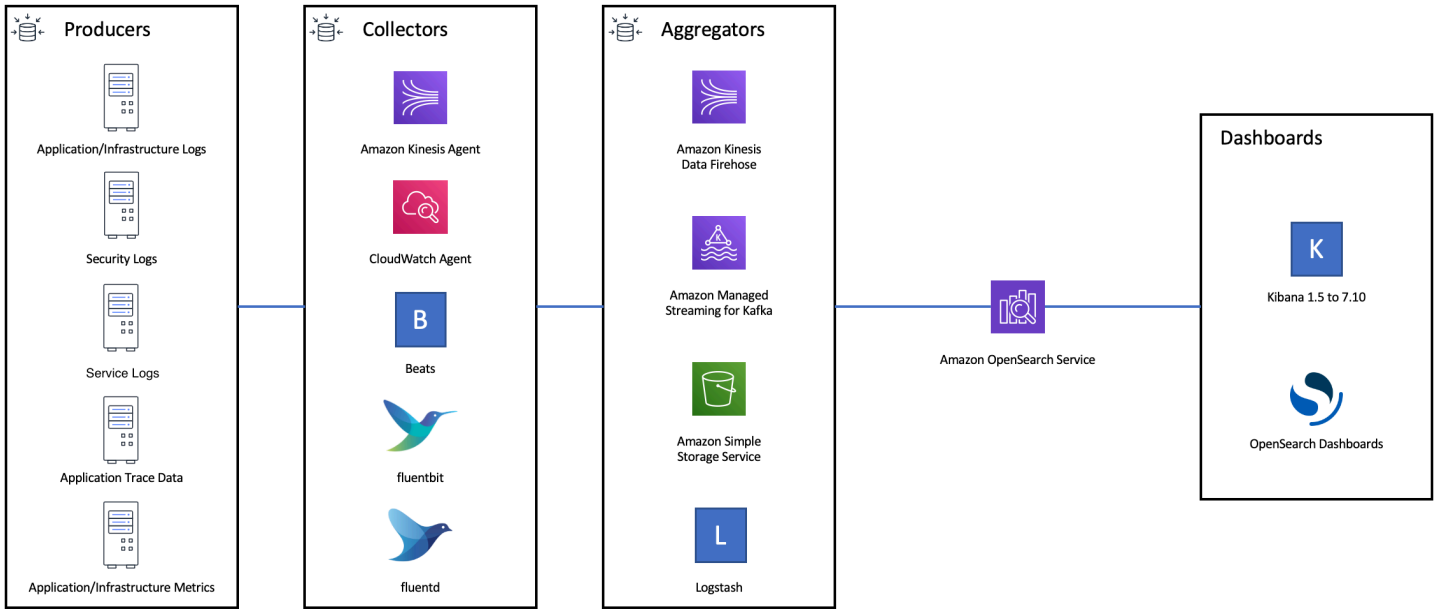
可用區域是每個 區域內的隔離位置。如果使用雙可用區域組態，遺失一個可用區域表示喪失了一半的網域容量。移至三個可用區域可進一步減少遺失單個可用區域的影響。

控制擷取流量和緩衝

建議您使用 _bulk API 作業限制整體要求計數。傳送一個包含 5,000 個文件的 `_bulk` 請求比傳送包含單個文件的 5,000 個請求更有效率。

為了獲得最佳操作穩定性，有時需要限制甚至暫停索引請求的上游流程。限制索引請求的速率是處理請求中意外或偶爾出現的峰值的一種重要機制，否則可能會拖垮叢集。考慮在您的上游架構中建置流量控制機制。

下圖顯示日誌擷取架構的多個元件選項。設定彙整層，以允許有足夠的空間來緩衝傳入資料，從而應對突然的流量峰值和短暫的網域維護。



建立搜尋工作負載的映射

對於搜尋工作負載，請建立對應，以定義文件及其欄位的 OpenSearch 儲存和索引方式。將 `dynamic` 設定為 `strict`，防止意外新增新欄位。

```
PUT my-index
{
  "mappings": {
    "dynamic": "strict",
    "properties": {
      "title": { "type" : "text" },
```

```
      "author": { "type" : "integer" },
      "year": { "type" : "text" }
    }
  }
}
```

使用索引範本

您可以使用索引模板來告訴 OpenSearch 如何在創建索引時配置索引。在建立索引之前先設定索引範本。然後，當您建立索引時，它會繼承範本中的設定和映射。您可以將多個範本套用至單個索引，以便您可以在一個範本中指定設定，並在另一個範本中指定映射。此策略允許多個索引中的一個通用設定版本，以及針對更具體設定和映射的單獨範本。

下列設定對於在範本中進行設定很有用：

- 主要碎片和複本碎片的數量
- 重新整理間隔 (重新整理和對索引進行最新變更以供搜尋的頻率)
- 動態映射控制
- 明確欄位映射

下列範例範本包含每個設定：

```
{
   "index_patterns":[
      "index-*"
   ],
   "order": 0,
   "settings": {
      "index": {
         "number_of_shards": 3,
         "number_of_replicas": 1,
         "refresh_interval": "60s"
      }
   },
   "mappings": {
      "dynamic": false,
      "properties": {
         "field_name1": {
            "type": "keyword"
         }
```

```
        }
    }
}
```

即使它們很少變更，集中 OpenSearch 定義設定和對應也比更新多個上游用戶端更容易管理。

使用索引狀態管理功能來管理索引

如果您要管理記錄檔或時間序列資料，建議您使用索引狀態管理 (ISM)。ISM可讓您自動化定期索引生命週期管理工作。您可以使ISM用建立原則來叫用索引別名變換作業、建立索引快照、在儲存層之間移動索引，以及刪除舊索引。您甚至可以使用ISM變換作業做為替代的資料生命週期管理策略，以避免碎片偏斜。

首先，設定ISM原則。如需範例，請參閱 the section called “範例政策”。接著，將政策連接至一個或多個索引。如果您在原則中包含ISM範本欄位， OpenSearch Service 會自動將原則套用至符合指定模式的任何索引。

移除未使用的索引

定期檢閱叢集中的索引，並識別任何未使用的索引。擷取這些索引的快照，以便它們儲存在 S3 中，然後刪除它們。移除未使用的索引時，您可以減少碎片計數，並可使節點之間的儲存分佈和資源使用率更平衡。即使處於閒置狀態，索引仍會在內部索引維護活動期間耗用部分資源。

您可以使用ISM在一段時間後自動擷取快照並刪除索引，而不是手動刪除未使用的索引。

使用多個網域實現高可用性

要在多個區域實現 99.9% 執行時間以上的高可用性，請考慮使用兩個網域。對於小型或緩慢變更的資料集，您可以設定跨叢集複寫以維護主動-被動模型。在此模型中，只能寫入到領導網域，但是可以從任一網域中讀取。對於較大的資料集和快速變更的資料，請在擷取管道中設定雙重傳遞，以便將所有資料獨立寫入主動-主動模型中的兩個網域。

建構您的上游和下游應用程式，同時考量容錯移轉。請務必測試容錯移轉程序以及其他災難復原程序。

效能

以下最佳實務適用於調整您的網域以獲得最佳效能。

最佳化批量請求大小和壓縮

批量大小取決於您的資料、分析和叢集組態，但是每個批量請求的最佳起點是 3 到 5 MiB。

使用 gzip 壓縮來減少要求和回應的承載大小，從您的 OpenSearch 網域傳送請求和接收回應。您可以將 gzip 壓縮與 OpenSearch Python 用戶端搭配使用，也可以從用戶端包含下列標頭：

- `'Accept-Encoding': 'gzip'`
- `'Content-Encoding': 'gzip'`

若要優化大量請求大小，請先從 3 MiB 的大量請求大小開始。然後，慢慢增加請求大小，直到索引效能停止改善為止。

> **Note**
>
> 若要在執行 Elasticsearch 6.x 版的網域上啟用 gzip 壓縮，您必須在叢集層級設定 `http_compression.enabled`。此設定在彈性搜尋版本 7.x 和所有版本中皆為真。OpenSearch

減少批量請求回應的大小

若要減少 OpenSearch 回應的大小，請使用`filter_path`參數排除不必要的欄位。請確保不要排除用於識別或重試失敗請求所需的任何欄位。如需詳細資訊和範例，請參閱 the section called “縮減回應大小”。

調校重新整理間隔

OpenSearch 索引具有最終讀取一致性。重新整理操作使得索引上執行的所有更新可用於搜尋。預設的重新整理間隔為一秒鐘，這表示在寫入索引時，每秒 OpenSearch 會執行一次重新整理。

重新整理索引的頻率越低 (重新整理間隔越高)，整體索引效能就越好。增加重新整理間隔的折中方案是索引更新與新資料可供搜尋之間有較長的延遲時間。在您能忍受的範圍內，將重新整理間隔設定得盡可能高，以改善整體效能。

我們建議將所有索引的 `refresh_interval` 參數設為 30 秒或更長時間。

啟用自動調整

自動調整會使用 OpenSearch 叢集中的效能和使用狀況指標，針對節點上的佇列大小、快取大小和 Java 虛擬機器 (JVM) 設定建議變更。這些選擇性變更可提高叢集速度與穩定性。您可以隨時還原為預設的「 OpenSearch 服務」設定。在新網域上預設啟用自動調整，除非您明確停用它。

我們建議您在所有網域上啟用自動調整，並設定週期性維護時段或定期檢閱其建議。

安全

以下最佳實務適用於保護您的網域。

啟用精細存取控制

精細的存取控制可讓您控制哪些人可以存取 OpenSearch Service 網域中的特定資料。與一般存取控制相比，精細存取控制可為每個叢集、索引、文件和欄位提供其自己指定的存取政策。存取條件可以基於許多因素，包括請求存取之人員的角色，以及他們打算對資料執行的動作。例如，您可能會授予一位使用者寫入索引的存取權，而授予另一位使用者僅讀取索引上資料的存取權，而不能進行任何變更。

精細存取控制可讓具有不同存取需求的資料存在於相同的儲存空間中，而不會遇到安全性或合規性問題。

我們建議在您的網域中啟用精細存取控制。

部署網域 VPC

將您的 OpenSearch Service 網域置於虛擬私有雲端 (VPC) 中，有助於在 OpenSearch 服務與其他服務之間實現安全通訊，VPC而不需要網際網路閘道、NAT裝置或VPN連線。所有流量都安全地保持在 AWS 雲端。由於其邏輯隔離，與使用公用端點的網域相比，位於內部的網域VPC具有額外的安全層。

我們建議您在 VPC.

套用限制性存取政策

即使您的網域部署在 a 中VPC，最佳做法是分層實作安全性。確保針對您目前的存取政策檢查組態。

將限制性資源型存取原則套用至您的網域，並在授予設定API和作業存取權時遵循最低權限原則 OpenSearch API。一般而言，請避免在存取政策中使用匿名使用者主體 `"Principal": {"AWS": "*" }`。

不過，在某些情況下，您可以接受使用開放存取政策，例如當您啟用精細存取控制時。開放存取政策可讓您在請求簽署困難或不可能的情況下 (例如來自特定用戶端和工具) 存取網域。

啟用靜態加密

OpenSearch 服務網域提供靜態資料的加密功能，以防止未經授權存取您的資料。靜態加密使用 AWS Key Management Service (AWS KMS) 儲存和管理您的加密金鑰，以及使用 256 位元金鑰 (AES-256) 的進階加密標準演算法來執行加密。

如果您的網域存放了敏感資料，請啟用靜態資料加密。

啟用 node-to-node 加密

N ode-to-node 加密在 OpenSearch Service 中的預設安全性功能之上，提供額外的安全性層。它會針對在其中佈建的節點之間的所有通訊實作傳輸層安全性 (TLS) OpenSearch。N ode-to-node 加密：傳送至 OpenSearch Service 網域的任何資料會在節點之間分散和複寫時，在傳輸過程中HTTPS保持加密狀態。

如果您的網域儲存敏感資料，請啟用 node-to-node加密功能。

使用監視器 AWS Security Hub

通過使用監控與安全性最佳實踐相關的 OpenSearch 服務使用情況 AWS Security Hub。 Security Hub 使用安全控制來評估資源配置和安全標準，以幫助您遵守各種合規性架構。如需有關使用 Security Hub 來評估 OpenSearch 服務資源的詳細資訊，請參閱 Amazon OpenSearch Service中的控制項 AWS Security Hub 使用者指南。

成本最佳化

以下最佳做法適用於最佳化和節省您的 OpenSearch 服務成本。

使用最新一代執行個體類型

OpenSearch 服務一直採用新的 Amazon EC2 執行個體類型，以較低的成本提供更好的效能。我們建議始終使用最新一代的執行個體。

對於生產網域，避免使用 T2 或 `t3.small` 執行個體，因為在持續的高負載下，它們可能會變得不穩定。`r6g.large` 執行個體是小型生產工作負載 (資料節點和專用主節點) 的一種選擇。

使用最新的 Amazon EBS gp3 卷

OpenSearch 資料節點需要低延遲和高輸送量儲存，以提供快速的索引和查詢。透過使用 Amazon EBS gp3 磁碟區，您可以比先前提供的 Amazon EBS gp2 磁碟區類型低 9.6%，獲得更高的基準效能 (IOPS和輸送量)。您可以使用 gp3 佈建IOPS與磁碟區大小無關的其他輸送量和輸送量。這些磁碟區也比上一代磁碟區更穩定，因為它們不會使用爆量額度。gp3 磁碟區類型也使 gp2 per-data-node 磁碟區類型的磁碟區大小限制加倍。您可以使用這些更大的磁碟區，透過提高每個資料節點的儲存量來降低被動資料的成本。

使用 UltraWarm 和冷存儲時間序列日誌數據

如果您用 OpenSearch 於日誌分析，請將資料移至 UltraWarm 或冷存儲以降低成本。使用索引狀態管理 (ISM) 在儲存層之間移轉資料並管理資料保留。

UltraWarm提供在 Service 中儲存大量唯讀資料的符合成本效益的方 OpenSearch 式。 UltraWarm 使用 Amazon S3 進行儲存，這表示資料是不可變的，只需要一個副本。您只需支付相當於索引中主要碎片大小的儲存。 UltraWarm 查詢延遲會隨著服務查詢所需的 S3 資料量而增加。在節點上快取資料之後， UltraWarm 索引的查詢會執行類似於 Hot 索引的查詢。

冷儲存也由 S3 支持。當您需要查詢冷資料時，可以選擇性地將其貼附至既有 UltraWarm 節點。冷資料所產生的受管儲存成本與冷存放區相同 UltraWarm，但冷存放區中的物件不會消耗 UltraWarm 節點資源。因此，冷儲存可提供大量的儲存容量，而不會影響 UltraWarm 節點大小或計數。

UltraWarm 如果您有大約 2.5 TiB 的資料要從熱儲存移轉，就會變得符合成本效益。監控您的填寫率，並計劃在達到該資料量 UltraWarm之前將索引移至。

檢閱預留執行個體的建議

在您對效能和運算耗用量有良好的基準之後，請考慮購買預留執行個體 (RIs)。對於無預付款的 1 年預訂，折扣從 30% 左右開始；對於所有預付款的 3 年承諾，折扣可以增加到 50%。

觀察到至少 14 天的穩定操作後，請檢閱 Cost Explorer 中的預留執行個體建議。Amazon OpenSearch 服務標題會顯示特定 RI 購買建議和預計節省成本。

調整 Amazon OpenSearch 服務域

沒有完美的方法來調整 Amazon OpenSearch 服務域的大小。不過，從瞭解您的儲存需求、服務及 OpenSearch 本身開始，您就可以針對硬體需求做出明智的初步估計。此預估可以做為調整網域大小最關鍵環節的實用起點：使用代表性工作負載進行測試和監控其效能。

主題

- 計算儲存需求
- 選擇碎片數
- 選擇執行個體類型並進行測試

計算儲存需求

大多數 OpenSearch 工作負載分為兩大類別之一：

- 長壽命索引：您撰寫的程式碼會將資料處理成一或多個 OpenSearch 索引，然後在來源資料變更時定期更新這些索引。一些常見的範例是網站、文件和電子商務搜尋。
- 動態索引：資料持續流入一組臨時索引，具有建立索引期和保留時段 (例如一組保留兩週的每日索引)。一些常見的範例是日誌分析、時間序列處理和點擊流分析。

對於長效索引的工作負載，您可以在磁碟上檢查來源資料並輕鬆判斷它會消耗多少儲存空間。如果資料來自多個來源，只要一起新增這些來源。

對於動態索引，您可以保留期乘上在代表時段產生的資料量。例如，若您每小時產生 200 MiB 的日誌資料，也就是每天 4.7 GiB，假設您的保留期間為兩週，則在任何指定時間的資料為 66 GiB。

您的來源資料的大小，不過是您的儲存需求的一個面向。您還必須有考量：

- 複本數目每個複本都是主要碎片的完整副本，索引的存放區大小會顯示主要和複本碎片所取用的大小。依預設，每個 OpenSearch 索引都有一個複本。建議您至少有一個以防資料遺失。複本也可提升搜尋效能，因此如果您的讀取工作負載繁重，您也許想要更多複本。使用 `PUT /my-index/_settings` 以更新索引的 `number_of_replicas` 設定。
- OpenSearch 索引開銷：索引的磁盤上大小各不相同。來源資料加上索引的總大小通常是來源的 110%，索引最多可達來源資料的 10%。索引資料之後，您可以使用`_cat/indices?v`API 和`pri.store.size`值來計算確切的額外負荷。 `_cat/allocation?v`還提供了一個有用的摘要。
- 作業系統預留空間：在預設情況下，Linux 會保留 5% 的檔案系統供 `root` 使用者用於關鍵程序、系統復原，以及防止磁碟分段問題。
- OpenSearch 服務額外負荷： OpenSearch 服務會保留每個執行個體 20% 的儲存空間 (最多 20 GiB)，用於區段合併、記錄和其他內部作業。

  由於此 20 GiB 上限，預留空間的總量可能依您網域內的執行個體數目而大不相同。例如，網域可能有三個 `m6g.xlarge.search` 執行個體，各有 500 GiB 的儲存空間，總計 1.46 TiB。在這種情況下，總預留空間僅 60 GiB。另一網域可能有 10 個 `m3.medium.search` 執行個體，各有 100 GiB 的儲存空間，總計 0.98 TiB。在這種情況下，總預留空間是 200 GiB，即使第一個網域大 50%。

  在以下公式中，我們對開銷套用「最壞情況」預估值。此預估值包含額外的可用空間，有助於將節點故障和可用區域中斷的影響降到最低。

總之，如果您在任何指定的時間有 66 GiB 的資料，並且想要一個複本，您的最低儲存需求為接近 66 * 2 * 1.1 / 0.95 / 0.8 = 191 GiB。您可以將此計算一般化，如下所示：

來源資料 * (1 + 複本數目) * (1 + 索引額外負荷)/(1-Linux 保留空間)/(1- OpenSearch 服務額外負荷) = 最低儲存需求

或者，您可以使用此簡化版本：

來源資料 * (1 + 複本的數量) * 1.45 = 最低儲存需求

儲存空間不足是造成叢集不穩定的最常見原因之一。因此，您應在選擇執行個體類型、執行個體計數和儲存磁碟區時反復檢查數字。

也存在其他儲存考量事項：

- 如果您的最低儲存需求超過 1 PB，請參閱 the section called “PB 規模”。
- 如果您有輪流更新的索引，而且想要使用熱暖架構，請參閱the section called “UltraWarm 儲存”。

選擇碎片數

在您了解您的儲存需求之後，您可以調查您的索引策略。根據預設，在 OpenSearch 服務中，每個索引分為五個主要碎片和一個複本（總共 10 個碎片）。這種行為與開源不同 OpenSearch，默認為一個主分片和一個副本分片。由於您無法輕易變更現有索引的主要碎片數，所以您應該在建立第一個文件的索引之前，決定好碎片計數。

選擇一些碎片的整體目標是要將索引平均分佈到叢集中的所有資料節點。不過，這些碎片不應該是太大或太多。一般指導方針是，針對搜尋延遲是關鍵效能目標的工作負載，嘗試將碎片大小保持在 10-30 GiB 之間，對於寫入操作繁重的工作負載 (例如日誌分析)，保持在 30-50 GiB。

較大的碎片可能會使得很難從故障中恢復，但是由於 OpenSearch 每個碎片使用一定數量的CPU和內存，因此具有太多的小碎片可能會導致性能問題和內存不足錯誤。換句話說，碎片應該足夠小，以至於底層的 OpenSearch Service 實例可以處理它們，但不是那麼小，以至於它們對硬件造成不必要的壓力。

例如，假設您有 66 GiB 的資料。您不希望該數量隨著時間增加，並且您想要保持每個碎片大約在 30 GiB 的大小。因此，您的碎片數應該大約為 66 * 1.1 / 30 = 3 個。您可以將此計算一般化，如下所示：

(來源資料 + 成長空間) * (1 + 索引負荷) / 所需碎片大小 = 主要碎片的大約數量

這個方程式有助於補償資料隨時間的成長。如果您預期同樣皆為 66 GiB 的資料到明年成為四倍，大約碎片數則會是 (66 + 198) * 1.1 / 30 = 10 個。不過請記住，您尚未擁有那些額外的 198 GiB 資料。檢查以確保為 future 做好準備不會產生不必要的微小碎片，這些碎片會消耗大量的內存CPU和當前。在這種情況下，66 * 1.1 / 10 個碎片 = 每個碎片 7.26 GiB，這會消耗額外的資源且低於建議的大小範圍。您

可能會考慮六個碎片的更多 middle-of-the-road 方法，這使您今天擁有 12-GiB 碎片，並在 future 使用 48-GiB 碎片。接著，您可能希望再次以三個碎片開始並在碎片超過 50 GiB 時重新建立資料的索引。

有個較不常見的問題包含限制每個節點的碎片數量。如果您適當地調整碎片大小，通常要過很久一段時間才會用完磁碟空間，然後達到此限制。例如，一個 `m6g.large.search` 執行個體具有最大 512 GiB 的磁碟大小。如果您保持在低於 80% 的磁碟用量並將碎片大小調整為 20 GiB，即可容納大約 20 個碎片。彈性搜索 7. x 和更新版本，以及的所有版本 OpenSearch，每個節點都有 1,000 個碎片的限制。若要調整每個節點的最大碎片，請設定 `cluster.max_shards_per_node` 設定。如需範例，請參閱叢集設定。

只要適當地調整碎片大小，幾乎一律可保持低於此限制，但您也可以考慮 Java 堆積的每個 GiB 的碎片數量。在指定的節點上，Java 堆積的每 GiB 擁有不超過 25 個碎片。例如，一個 `m5.large.search` 執行個體具有 4 GiB 堆積，因此每個節點都應擁有不超過 100 個碎片。在該碎片計數，每個碎片的大小約為 5 GiB，這遠低於我們的建議。

選擇執行個體類型並進行測試

在您計算您的儲存需求並選擇所需的碎片數之後，您可以開始做出硬體的決策。硬體需求會依工作負載而大大不同，但是我們仍然可以提供一些基本建議。

一般而言，每個執行個體類型的儲存限制都會對應到輕度工作負載可能需要的大小CPU和記憶體數量。例如，`m6g.large.search`執行個體的EBS磁碟區大小上限為 512 GiB、2 v CPU 核心和 8 GiB 的記憶體。如果您的叢集有許多碎片，執行課稅彙總、頻繁更新文件或處理大量的查詢，這些資源可能不足以滿足您的需求。如果您的叢集屬於這些類別之一，請嘗試從接近 2 v CPU 核心和 8 GiB 記憶體的組態開始，以滿足每 100 GiB 的儲存需求。

> **Tip**
>
> 如需分配給每個執行個體類型的硬體資源摘要，請參閱 Amazon OpenSearch 服務定價。

然而，即使這些資源可能會也不夠。一些 OpenSearch 用戶報告說，他們需要很多次這些資源來滿足他們的要求。若要尋找適用於您的工作負載的合適硬體，您必須有明智的初始預估、測試代表的工作負載、進行調整並再次執行測試。

步驟 1：進行初步預估

首先，我們建議至少使用三個節點來避免潛在的 OpenSearch問題，例如腦部分裂狀態（當通訊失效導致叢集具有兩個主節點時）。如果您有三個專用主節點，我們仍然建議您至少有兩個資料節點用於複寫。

步驟 2：計算每個節點的儲存需求

如果您有 184 GiB 的儲存需求和建議的至少三個節點，請使用方程式 184 / 3 = 61 GiB 算出每個節點所需的儲存量。在此範例中，您可以選取三個`m6g.large.search`執行個體，其中每個執行個體都使用 90-GiB EBS 儲存磁碟區，以便您擁有安全網和一段時間的成長空間。此組態提供 6 v CPU 核心和 24 GiB 記憶體，因此適用於較輕的工作負載。

針對更高額度的範例，則假設是儲存需求為 14 TiB (14,336 GiB) 的繁重工作負載。在這種情況下，您可以選擇以 2 * 144 = 288 v CPU 核心和 8 * 144 = 1152 GiB 的記憶體開始進行測試。這些數字運作大約 18 個 `i3.4xlarge.search` 執行個體。如果您不需要快速的本機儲存空間，也可以測試 18 個執行個`r6g.4xlarge.search`體，每個執行個體都使用 1-TiB EBS 儲存磁碟區。

如果您的叢集包含數百 TB 的資料，請參閱 the section called “PB 規模”。

步驟 3：執行代表性測試

設定叢集之後，您可以使用先前計算的碎片數量來新增索引、使用實際資料集執行一些代表性的用戶端測試，以及監視 CloudWatch 指標以查看叢集如何處理工作負載。

步驟 4：成功或反覆

如果效能滿足您的需求、測試成功，且 CloudWatch 指標正常，則叢集已準備就緒可供使用。請記得設定 CloudWatch 警示以偵測健全狀況不良的資源使用量。

如果無法接受該效能，表示測試失敗或者 `CPUUtilization` 或 `JVMMemoryPressure` 偏高，您可能需要選擇不同的執行個體類型 (或新增執行個體)，並繼續進行測試。當您新增執行個體時，OpenSearch 會自動重新平衡整個叢集中的碎片分佈。

由於這在動力過強的叢集中測量過剩容量比在動力不足的叢集中測量欠缺容量來得容易，我們建議您從比您所需較大的叢集開始。接著，進行測試並縮減到有額外資源可確保在增加活動期間有穩定操作的有效率叢集。

生產叢集或狀態複雜的叢集受益於專用主節點，可提升效能和叢集可靠性。

Amazon 服務中的 PB 規模 OpenSearch

Amazon OpenSearch 服務域提供高達 3 PB 的附加存儲。您可以設定具 200 個 `i3.16xlarge.search` 執行個體類型的網域，每個都有 15 TB 的儲存空間。由於規模上的巨大差異，所以對此大小的網域的建議與我們的一般建議不同。本節討論建立網域、成本、儲存和碎片大小。

雖然此區段經常參考 `i3.16xlarge.search` 執行個體類型，您可以使用多個其他執行個體類型，以達到 1 PB 的總網域儲存。

建立網域

此大小的網域超過每個網域 80 個執行個體的預設限制。若要請求將服務限制提高到每個網域最多 200 個執行個體，請透過 AWS 支援中心立案處理。

定價

建立此大小的網域之前，請先查看 Amazon Ser OpenSearch vice 定價頁面，以確保相關成本符合您的期望。檢查 the section called “UltraWarm 儲存”，確認熱暖架構是否適合您的使用案例。

儲存

此 `i3` 執行個體類型經過設計，可提供快速、本機非揮發性記憶體儲存裝置 (NVMe) 的儲存空間。由於與 Amazon 彈性區塊存放區相比，此本機儲存往往會提供效能優勢，因此當您在 OpenSearch 服務中選取這些執行個體類型時，EBS 磁碟區不是一種選項。如果您偏好使用 EBS 儲存，請使用另一個執行個體類型 (例如 `r6.12xlarge.search`。

碎片大小和計數

常見的 OpenSearch 準則是每個碎片不得超過 50 GB。鑒於大型網域所需的碎片數量，以及可用於 `i3.16xlarge.search` 執行個體的可用資源，我們建議碎片大小為 100 GB。

例如，如果您有 450 TB 的來源資料，並且想要一個複本，您的最低儲空間要求比較接近 450 TB * 2 * 1.1 / 0.95 = 1.04 PB。如需此計算詳細說明，請參閱the section called “計算儲存需求”。雖然有 1.04 PB / 15 TB = 70 個執行個體，但是您可以選擇 90 個或更多的 `i3.16xlarge.search` 執行個體，讓自己擁有儲存安全網並，處理節點故障並將隨時間增加資料量的一些變異納入考量。每個執行個體會新增另一組 20 GiB 到您的最低儲存需求，但對於此大小的磁碟，這組 20 GiB 幾乎可以忽略不計。

控制碎片的數量非常棘手。 OpenSearch 使用者通常每天輪換索引，並保留資料一兩週。在這種情況下，您可能會發現區分「作用中」和「非作用中」的碎片數量很管用。作用中碎片會被主動寫入或讀取。非作用中碎片可能服務一些讀取請求，但大部分都在閒置狀態。一般而言，您應該保留有效碎片數量在數千以下。隨著非作用中碎片數量達到 10,000 個，可觀的效能和穩定性風險也隨之出現。

若要計算主要碎片的數量，請使用下列公式：每個碎片 450,000 GB * 1.1 / 100 GB = 4,950 個碎片。複本數量的兩倍是 9,900 分片，其表示當所有碎片都在作用中時的主要考量。但是，如果您輪換索引，而且只有 1/7 或 1/14 的作用中碎片數量或碎片在任何指定一天 (1,414 或 707 碎片)，叢集

可能有良好的運作狀態。如往常一樣，調整大小和設定您的網域的最重要步驟是使用實際的資料集執行代表性的用戶端測試。

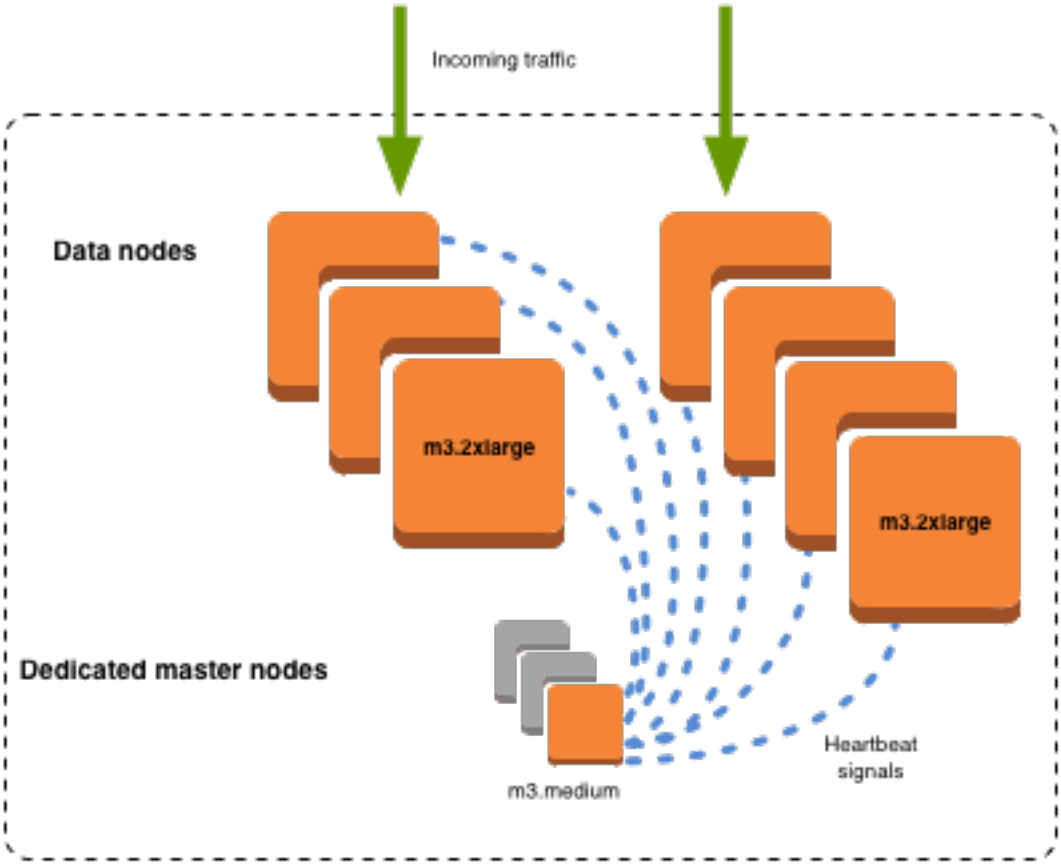
Amazon OpenSearch 服務中的專用主節點

Amazon OpenSearch 服務使用專用的主節點來提高叢集穩定性。專用主節點會執行叢集管理任務，但不會保留資料或回應資料上傳請求。此叢集管理任務的卸載可增加您網域的穩定性。就像所有其他節點類型一樣，您需要按照小時費率為每個專用主節點支付費用。

專用主節點會執行以下叢集管理任務：

- 追蹤叢集中的所有節點。
- 追蹤叢集中的索引數量。
- 追蹤屬於每個索引的碎片數。
- 維持叢集中節點的路由資訊。
- 狀態變更後更新叢集狀態，例如建立索引，以及在叢集中新增或移除節點。
- 跨叢集中的所有節點複製叢集狀態的變更。
- 透過傳送監控叢集中資料節點的可用性的活動訊號、定期信號，來監控所有叢集節點的運作狀態。

下圖顯示具有 10 個執行個體的 OpenSearch 服務網域。其中七個執行個體是資料節點，三個是專用主節點。只有其中一個專用主節點處於作用中狀態。這兩個灰色的專用主節點會等待作為備份，以防作用中的專用主節點發生故障。所有資料上傳請求是由七個資料節點提供服務，而所有叢集管理任務均卸載到作用中的專用主節點。



選擇專用主節點數目

我們建議您將異地同步備份與待命搭配使用，這樣會在每個生產 OpenSearch 服務網域中新增三個專用主節點。如果您使用異地同步備份進行部署，不含待命或單一可用區，我們仍建議使用三個專用主節點 切勿選擇偶數數量的專用主節點。選擇專用主節點的數目時，請考量下列事項：

- OpenSearch Service 明確禁止一個專用主節點，因為您在發生故障時沒有備份。如果您嘗試建立只有一個專用主節點的網域，則會收到驗證例外狀況。
- 如果您具有兩個專用主節點，表示您的叢集沒有節點的必要仲裁，供萬一發生故障時可選擇新的主節點。

  仲裁是專用主節點的數量 / 2 + 1 (四捨五入為最接近的整數)。在此案例中，為 2 / 2 + 1 = 2。因為一個專用主節點已故障且只存在一個備份，所以叢集沒有仲裁並且無法選擇新的主節點。
- 三個專用主節點 (建議的數量) 在萬一主節點故障時提供兩個備份節點，以及必要的仲裁 (2) 以選擇新的主節點。
- 四個專用主節點並不會比三個好，而且如果您使用多個可用區域，則可能導致問題。

- 如果一個主節點發生故障，您有仲裁 (3) 以選擇新的主節點。如果兩個節點故障，您會遺失該仲裁，就如同您使用三個專用主節點。
- 在三個可用區域組態中，兩個具AZs有一個專用主節點，而一個 AZ 則有兩個。如果該 AZ 遇到中斷，剩下的兩個AZs沒有必要的法定人數 (3) 來選擇一個新的主。

- 擁有五個專用主節點的運作與三個的相同，並可讓您在維持仲裁的同時遺失兩個節點。但是因為在任何指定的時間只有一個專用主節點作用中，此組態表示支付四個閒置的節點。許多使用者發現這個層級的容錯移轉保護過於極端。

如果叢集具有偶數個符合主要資格的節點，以 OpenSearch 及彈性搜尋版本 7。 x 和更高版本忽略一個節點，以便投票配置始終是奇數。在這種情況下，四個專用主節點基本上等同於三個專用主節點 (兩個則相當於一個)。

> **Note**
>
> 如果您的叢集不具備必要的仲裁以選擇新的主節點，將請求寫入到叢集「以及」讀取叢集請求則均會失敗。此行為與 OpenSearch 預設不同。

選擇專用主節點的執行個體類型

雖然專用的主節點不會處理搜尋和查詢要求，但它們的大小與執行個體大小以及它們可以管理的執行個體、索引和碎片數量有很高的關聯性。對於生產叢集，我們建議至少針對專用主節點使用下列執行個體類型。

這些建議是根據一般工作負載，並可能依您的需求而異。具有許多碎片或欄位映射的叢集可受益於更大的執行個體類型。監控專用主節點指標，以查看您是否需要使用較大的執行個體類型。

執行個體計數	主節點RAM大小	支援的最大碎片計數	建議的最小專用主要執行個體類型
1–10	8 GiB	10K	`m5.large.search` 或 `m6g.large.search`
11–30	16 GiB	30K	`c5.2xlarge.search`

執行個體計數	主節點RAM大小	支援的最大碎片計數	建議的最小專用主要執行個體類型
			或 `c6g.2xlarge.search`
31–75	32 GiB	40K	`r5.xlarge.search` 或 `r6g.xlarge.search`
76 – 125	64 GiB	75K	`r5.2xlarge.search` 或 `r6g.2xlarge.search`
126 – 200	128 GiB	75K	`r5.4xlarge.search` 或 `r6g.4xlarge.search`

- 如需有關特定的組態變更會如何影響專用主節點的資訊，請參閱the section called “組態變更”。
- 如需執行個體計數限制的說明，請參閱OpenSearch 服務網域和執行個體配額。
- 如需特定執行個體類型 (包括 v CPU、記憶體和定價) 的詳細資訊，請參閱 Amazon OpenSearch 服務價格。

推薦的 Amazon 服 OpenSearch 務 CloudWatch 警報

CloudWatch 當量度在一段時間內超過 CloudWatch 指定值時，警示會執行動作。例如，您可能想要 AWS 如果您的叢集健康狀態超過一分鐘，`red`請傳送電子郵件給您。本節包含 Amazon OpenSearch 服務的一些建議警示，以及如何回應這些警示。

您可以使用自動部署這些警報 AWS CloudFormation。 有關示例堆棧，請參閱相關GitHub存儲庫。

> **Note**
>
> 如果您部署 CloudFormation 堆疊，`KMSKeyError`和`KMSKeyInaccessible`警示會以`Insufficient Data`狀態存在，因為只有在網域遇到加密金鑰問題時，才會顯示這些指標。

如需有關設定警示的詳細資訊，請參閱 Amazon CloudWatch 使用者指南中的建立 Amazon CloudWatch 警示。

警示	問題
`ClusterStatus.red` 上限為 >= 1 達 1 分鐘，連續 1 次	至少一個主要碎片及其複本不會分配到節點。請參閱 the section called “紅色叢集狀態”。
`ClusterStatus.yellow` 上限為 >= 1 持續 1 分鐘，連續 5 次	至少一個複本碎片不會分配到節點。請參閱 the section called “黃色叢集狀態”。
`FreeStorageSpace` 下限為 <= 20480 達 1 分鐘，連續 1 次	您叢集內的節點縮減至 20 GiB 的可用儲存空間。請參閱 the section called “缺少可用儲存空間”。此值的單位為 MiB，所以建議您將其設為每個節點的 25% 儲存空間，而不是 20480。
`ClusterIndexWritesBlocked` 為 >= 1 達 5 分鐘，連續 1 次	您的叢集正在封鎖寫入請求。請參閱 the section called “ClusterBlockException”。
`Nodes`下限為 < x 達 1 天，連續 1 次	x 是您叢集中的節點數。此警示表示您叢集中至少有一個節點已無法連線達 1 天時間。請參閱 the section called “叢集節點失敗”。
`AutomatedSnapshotFailure` 上限為 >= 1 達 1 分鐘，連續 1 次	自動快照失敗。此故障通常是紅色叢集運作狀態的結果。請參閱 the section called “紅色叢集狀態”。 如需所有自動快照的摘要和一些有關故障的資訊，請嘗試以下其中一個請求：

警示	問題
	`GET domain_endpoint /_snapshot/cs-automated/_all` `GET domain_endpoint /_snapshot/cs-automated-enc/_all`
`CPUUtilization` 或 `WarmCPUUtilization` 上限為 >= 80%，15 分鐘，連續 3 次	有時可能會發生 100% 的利用CPU率，但持續的高使用率是有問題的。可考慮使用較大的執行個體類型或新增執行個體。
`JVMMemoryPressure` 上限為 >= 95% 達 1 分鐘，連續 3 次	如果使用量增加，叢集可能遇到記憶體不足錯誤。考慮垂直縮放。OpenSearch 服務RAM對 Java 堆使用一半的實例，最多 32 GiB 的堆積大小。您可以將執行個體垂直縮放至 64 GiBRAM，此時您可以透過新增執行個體來水平縮放。
`OldGenJVMMemoryPressure` 上限為 >= 80% 達 1 分鐘，連續 3 次	
`MasterCPUUtilization` 上限為 >= 50% 達 15 分鐘，連續 3 次	可考慮使用較大的執行個體類型為您的專用主節點。由於它們在叢集穩定性和藍/綠部署中所扮演的角色，因此專用主節點的CPU使用量應該比資料節點低。
`MasterJVMMemoryPressure` 上限為 >= 95% 達 1 分鐘，連續 3 次	
`MasterOldGenJVMMemoryPressure` 上限為 >= 80% 達 1 分鐘，連續 3 次	

警示	問題
`KMSKeyError` 為 >= 1 達 1 分鐘，連續 1 次	所以此 AWS KMS 停用用來加密網域中靜態資料的加密金鑰。重新啟用它來恢復正常操作。如需詳細資訊，請參閱the section called “靜態加密”。
`KMSKeyInaccessible` 為 >= 1 達 1 分鐘，連續 1 次	所以此 AWS KMS 用於加密您網域中靜態資料的加密金鑰已遭刪除或撤銷其授予 OpenSearch 服務。您無法復原此狀態的網域。但是，如果您有手動快照，您可以使用它來遷移至新網域。如需進一步了解，請參閱the section called “靜態加密”。
`shards.active` 為 >= 30000 達 1 分鐘，連續 1 次	作用中主要碎片和複本碎片的總數大於 30,000。您可能太頻繁地輪換索引。考慮在ISM索引達到特定年齡後刪除索引。
5*xx* 警示 >= `OpenSearchRequests` 的 10%	一或多個資料節點可能會過載，或是請求無法在閒置逾時期間內完成。請考慮切換到較大型執行個體類型或在叢集中新增更多節點。確認您遵循碎片和叢集架構的最佳實務。
`MasterReachableFromNode` 最大值小於 1，持續 5 分鐘，連續 1 次	此警示表示主節點已停止或無法存取。這些失敗通常是網路連線問題或 AWS 依賴性問題。
`ThreadpoolWriteQueue` 平均為 >= 100 達 1 分鐘，連續 1 次	叢集正在經歷高索引並行狀況。檢閱和控制索引請求，或增加叢集資源。
`ThreadpoolSearchQueue` 平均為 >= 500 達 1 分鐘，連續 1 次	叢集正在經歷高搜尋並行狀況。考慮擴展您的叢集。您也可以增加搜尋佇列大小，但過度增加可能會導致記憶體不足錯誤。

警示	問題
`ThreadpoolSearchQueue` 上限為 >= 5000 達 1 分鐘，連續 1 次	
連續 1 分鐘的增加為 >=1 {數學運算式 DIFF ()} `ThreadpoolSearchRejected` SUM	這些警示會通知您可能會影響效能和穩定性的網域問題。
連續 1 分鐘的增加為 >=1 {數學運算式 DIFF ()} `ThreadpoolWriteRejected` SUM	

> **Note**
>
> 如果您只是想檢視指標，請參閱 the section called “監控叢集指標”。

您可能會考慮的其他警示

請考慮根據您經常使用的 OpenSearch 服務功能來設定下列警示。

警示	問題
`WarmFreeStorageSpace` 是大於等於 10%	您已達到總免費暖儲存空間的 10%。 `WarmFreeStorageSpace` 測量 MiB 中可用溫度儲存空間的總和。 UltraWarm 使用 Amazon S3 而不是連接的磁盤。
`HotToWarmMigrationQueueSize` 為 >=	大量索引會同時從熱移至 UltraWarm 儲存裝置。考慮擴展您的叢集。

警示	問題
20 達 1 分鐘，連續 3 次	
HotToWarmMigrationSuccessLatency 為 >= 1 天，連續 1 次	設定此警示，以便在您嘗試滾動每日索引，HotToWarmMigrationSuccessCount x 延遲大於 24 小時時收到通知。
WarmJVMMemoryPressure 上限為 >= 95% 達 1 分鐘，連續 3 次	如果使用量增加，叢集可能遇到記憶體不足錯誤。考慮垂直縮放。OpenSearch 服務RAM對 Java 堆使用一半的實例，最多 32 GiB 的堆積大小。您可以將執行個體垂直縮放至 64 GiBRAM，此時您可以透過新增執行個體來水平縮放。
WarmOldGenJVMMemoryPressure 上限為 >= 80% 達 1 分鐘，連續 3 次	
WarmToColdMigrationQueueSize 為 >= 20 達 1 分鐘，連續 3 次	大量索引正在同時從冷庫移動 UltraWarm 到冷庫。考慮擴展您的叢集。
HotToWarmMigrationFailureCount 為 >= 1 達 1 分鐘，連續 1 次	遷移可能在快照、碎片重新配置或強制合併期間失敗。快照或碎片重新配置期間的失敗通常是因為節點故障或 S3 連線問題。磁碟空間不足通常是強制合併失敗的根本原因。
WarmToColdMigrationFailureCount 為 >= 1 達 1 分鐘，連續 1 次	嘗試將索引中繼資料遷移至冷儲存裝置失敗時，遷移通常會失敗。移除熱索引叢集狀態時也可能發生故障。

警示	問題
WarmToColdMigrationLatency 為 >= 1 天，連續 1 次	設定此警示，以便在您嘗試滾動每日索引，WarmToColdMigrationSuccessCount x 延遲大於 24 小時時收到通知。
AlertingDegraded 為 >= 1 達 1 分鐘，連續 1 次	提醒索引為紅色，或是有一或多個節點不在排程上。
ADPluginUnhealthy 為 >= 1 達 1 分鐘，連續 1 次	異常偵測外掛程式無法正常運作，原因是高故障率或使用的其中一個索引是紅色。
AsynchronousSearchFailureRate 為 >= 1 達 1 分鐘，連續 1 次	最後一分鐘內至少有一個非同步搜尋失敗，這可能表示協調器節點失敗。非同步搜尋請求的生命週期僅在協調器節點上受管，因此如果協調器停機，請求即會失敗。
AsynchronousSearchStoreHealth 為 >= 1 達 1 分鐘，連續 1 次	持續性索引中非同步搜尋回應存放區的運作狀態為紅色。您可能正在儲存大型非同步回應，這可能會破壞叢集的穩定性。請嘗試將您的非同步搜尋回應限制在 10 MB 以下。
SQLUnhealthy 為 >= 1 達 1 分鐘，連續 3 次	該SQL插件返回 5 xx 響應代碼或傳遞無效的DSL查詢 OpenSearch。針對用戶端向外掛程式提出的請求進行疑難排解。
LTRStatus.red 為 >= 1 達 1 分鐘，連續 1 次	至少有一個執行 Learning to Rank 外掛程式所需的索引缺少主要碎片，並且無法運作。

Amazon OpenSearch 服務的一般參考

Amazon OpenSearch 服務支援各種執行個體、操作、外掛程式和其他資源。

主題

- Amazon OpenSearch 服務中支持的實例類型
- Amazon OpenSearch 服務中的引擎版本功能
- Amazon OpenSearch 服務中的引擎版本的插件
- Amazon OpenSearch 服務中支持的操作
- Amazon OpenSearch 服務配額
- Amazon OpenSearch Service 中的預留執行個體
- Amazon OpenSearch 服務中的其他支持資源

Amazon OpenSearch 服務中支持的實例類型

Amazon OpenSearch 服務支援下列執行個體類型。並非所有區域皆支援所有執行個體類型。如需可用性詳細資訊，請參閱 Amazon OpenSearch 服務定價。

如需哪些執行個體適合用於您的使用案例之相關資訊，請參閱 the section called “調整網域大小”、the section called “EBS磁碟區大小配額” 與 the section called “網路配額”。

最新一代執行個體類型

為了獲得最佳效能，建議您在建立新的 OpenSearch Service 網域時使用下列執行個體類型。

執行個體類型	執行個體	限制
i4i	i4i.large i4i.xlarge i4i.2xlarge i4i.4xlarge i4i.8xlarge	i4i 執行個體類型需要 Elasticsearch 5.1 或更新版本或任何版本的執行個體 OpenSearch，且不支援磁碟區儲存。EBS

執行個體類型	執行個體	限制
	i4i.12xlarge i4i.16xlarge i4i.24xlarge i4i.32xlarge	
i4g	i4g.large i4g.xlarge i4g.2xlarge i4g.4xlarge i4g.8xlarge i4g.16xlarge	i4g 執行個體類型需要彈性搜尋 7.9 或更新版本或任何版本的執行個體 OpenSearch，且不支援EBS儲存磁碟區。

執行個體類型	執行個體	限制
引力蛋白 3	大 C7 克。大 C7 克。2 倍大 C7 克. 大 C7 克。8 倍大 C. 12 倍大 C7 公克 兆 7 克。大 兆 7 克。大 M7 克。2 倍大 兆 7 克。4 倍大 M7 公克。8 倍大 微米 12 克大 M7 公克 16 克大 R7 克。中 大	重力 3 僅支持。GP3

執行個體類型	執行個體	限制
	大	
	7 克. 大	
	7 克. 大	
	8 克大	
	7 克. 大	
	大号	
	大	
	大	
	L. 2 倍大	
	L. 4 倍大	
	大型 8 公升	
	L. 12 倍大	
	大型	

執行個體類型	執行個體	限制

OR1	`or1.medium.search`
	`or1.large.search`
	`or1.xlarge.search`
	`or1.2xlarge.search`
	`or1.4xlarge.search`
	`or1.8xlarge.search`
	`or1.12xlarge.search`
	`or1.16xlarge.search`
		• OR1執行個體類型需要 OpenSearch 2.11 或更新版本。
		• OR1執行個體僅與其他重力彈執行個體類型主節點 (C6g、M6g、R6g) 相容。

執行個體類型	執行個體	限制

lm4gn	`im4gn.large.search`
	`im4gn.xlarge.search`
	`im4gn.2xlarge.search`
	`im4gn.4xlarge.search`
	`im4gn.8xlarge.search`
	`im4gn.16xlarge.search`
		• IM4GN 執行個體類型需要彈性搜尋 7.9 或更新版本或任何版本的執行個體 OpenSearch，且不支援儲存磁碟區。EBS
		• IM4GN 執行個體僅與其他重力彈執行個體類型 (C6g、M6 公克、R6gD) 相容。您無法在同一個叢集中組合 Graviton 和非 Graviton 執行個體。

執行個體類型	執行個體	限制

C5	`c5.large.search`
	`c5.xlarge.search`
	`c5.2xlarge.search`
	`c5.4xlarge.search`
	`c5.9xlarge.search`
	`c5.18xlarge.search`
		C5 執行個體類型需要彈性搜尋 5.1 或更新版本，或是任何版本的。OpenSearch

執行個體類型	執行個體	限制

C6g	`c6g.large.search`
	`c6g.xlarge.search`
	`c6g.2xlarge.search`
	`c6g.4xlarge.search`
	`c6g.8xlarge.search`
	`c6g.12xlarge.search`
		• C6g 執行個體類型需要彈性搜尋 7.9 或更新版本，或是任何版本的。 OpenSearch
		• C6g 執行個體僅與其他重力彈執行個體類型相容 (IM4GN、M6 公克、R6gD)。您無法在同一個叢集中組合 Graviton 和非 Graviton 執行個體。

執行個體類型	執行個體	限制

I3	`i3.large.search`
	`i3.xlarge.search`
	`i3.2xlarge.search`
	`i3.4xlarge.search`
	`i3.8xlarge.search`
	`i3.16xlarge.search`	

M5	`m5.large.search`
	`m5.xlarge.search`
	`m5.2xlarge.search`
	`m5.4xlarge.search`
	`m5.12xlarge.search`
		M5 執行個體類型需要彈性搜尋 5.1 或更新版本，或是任何版本的。OpenSearch

執行個體類型	執行個體	限制

M6g	`m6g.large.search`
	`m6g.xlarge.search`
	`m6g.2xlarge.search`
	`m6g.4xlarge.search`
	`m6g.8xlarge.search`
	`m6g.12xlarge.search`
		• M6g 執行個體類型需要彈性搜尋 7.9 或更新版本，或是任何版本的。 OpenSearch
		• M6g 執行個體僅與其他重力彈執行個體類型相容 (IM4GN、C6g、R6gD)。您無法在同一個叢集中組合 Graviton 和非 Graviton 執行個體。

執行個體類型	執行個體	限制

R5	`r5.large.search`
	`r5.xlarge.search`
	`r5.2xlarge.search`
	`r5.4xlarge.search`
	`r5.12xlarge.search`
		R5 執行個體類型需要彈性搜尋 5.1 或更新版本，或是任何版本的。OpenSearch

執行個體類型	執行個體	限制

R6g	`r6g.large.search`
	`r6g.xlarge.search`
	`r6g.2xlarge.search`
	`r6g.4xlarge.search`
	`r6g.8xlarge.search`
	`r6g.12xlarge.search`
		• R6g 執行個體類型需要彈性搜尋 7.9 或更新版本或任何版本的。OpenSearch
		• R6g 執行個體僅與其他重力彈執行個體類型相容 (IM4GN、C6 公克、R6gD)。您無法在同一個叢集中組合 Graviton 和非 Graviton 執行個體。

執行個體類型	執行個體	限制

R6gd	`r6gd.large.search`
	`r6gd.xlarge.search`
	`r6gd.2xlarge.search`
	`r6gd.4xlarge.search`
	`r6gd.8xlarge.search`
	`r6gd.12xlarge.search`
	`r6gd.16xlarge.search`
		• R6gD 執行個體類型需要彈性搜尋 7.9 或更新版本或任何版本的 OpenSearch，且不支援儲存磁碟區。EBS
		• R6gD 執行個體僅與其他重力彈執行個體類型相容 (IM4GN、C6g、M6g、R6g)。您無法在同一個叢集中組合 Graviton 和非 Graviton 執行個體。

T3	`t3.small.search` `t3.medium.search`	• T3 執行個體類型需要彈性搜尋 5.6 或更新版本，或是任何版本的。 OpenSearch • 只有在佈建網域時未備用的情況下，您才能使用 T3 執行個體類型。如需詳細資訊，請參閱the section called “異地同步備份 (不含”。 • 只有在網域的執行個體計數為 10 或更少時，您才能使用 T3 執行個體類型。 • T3 執行個體類型不支援 UltraWarm儲存、冷儲存或自動調整。

上一代執行個體類型

OpenSearch Service 為已優化周圍應用程式但尚未升級的使用者提供上一代執行個體類型。建議您使用最新一代的執行個體類型以獲得最佳效能，但我們仍會繼續支援下列上一代執行個體類型。

執行個體類型	執行個體	限制

C4	`c4.large.search`
	`c4.xlarge.search`
	`c4.2xlarge.search`
	`c4.4xlarge.search`
	`c4.8xlarge.search`	

I2	`i2.xlarge.search` `i2.2xlarge.search`	

M3	`m3.medium.search`
	`m3.large.search`
	`m3.xlarge.search`
	`m3.2xlarge.search`
		• M3 執行個體類型不支援靜態資料加密、精細存取控制或跨叢集搜尋。
		• M3 執行個體類型依 OpenSearch 版本而定有其他限制。如需進一步了解，請參閱 the section called “無效的 M3 執行個體類型”。

執行個體類型	執行個體	限制

M4	`m4.large.search`
	`m4.xlarge.search`
	`m4.2xlarge.search`
	`m4.4xlarge.search`
	`m4.10xlarge.search`	

R3	`r3.large.search`
	`r3.xlarge.search`
	`r3.2xlarge.search`
	`r3.4xlarge.search`
	`r3.8xlarge.search`
		R3 執行個體類型不支援靜態資料加密或精細存取控制。

執行個體類型	執行個體	限制

R4	`r4.large.search`
	`r4.xlarge.search`
	`r4.2xlarge.search`
	`r4.4xlarge.search`
	`r4.8xlarge.search`
	`r4.16xlarge.search`	

T2	`t2.micro.search`
	`t2.small.search`
	`t2.medium.search`
		• 如果您網域的執行個體計數為 10 個或更少，您僅可使用 T2 執行個體類型。
		• `t2.micro.search` 執行個體類型只支援 Elasticsearch 1.5 和 2.3。
		• T2 執行個體類型不支援靜態資料加密、精細存取控制、UltraWarm儲存、冷儲存、跨叢集搜尋或自動調整。

> **Tip**
>
> 對於專用主節點及資料節點，我們經常建議使用不同的執行個體類型。

Amazon OpenSearch 服務中的引擎版本功能

許多 OpenSearch 服務功能都有最低 OpenSearch 版本需求或舊版 Elasticsearch OSS 版本需求。如果您符合某項功能的最低版本，但您的網域無法使用該功能，請更新網域的服務軟體。

功能	最低要求 OpenSearch 版本	需要的 Elasticsearch 最低版本
VPC支持	1.0	1.0
需HTTPS要所有流量到網域		
異地同步備份支援		
專用主節點		
自訂套件		
自訂端點		
慢速日誌發佈		
錯誤日誌發佈	1.0	5.1
靜態資料加密		
儀表板的Cognito身份驗證OpenSearch		
就地升級		

功能	最低要求 OpenSearch 版本	需要的 Elasticsearch 最低版本
Curator 支援	不包含	5.1
每小時自動快照	1.0	5.3
N ode-to-node 加密技術	1.0	6.0
Java 高級REST客戶端支持		
HTTP請求和響應壓縮		
提醒	1.0	6.2
SQL	1.0	6.5
跨叢集搜尋	1.0	6.7
精細定義存取控制		
SAML OpenSearch 儀表板的驗證		
自動調校		
遠端重新索引		
UltraWarm	1.0	6.8

功能	最低要求 OpenSearch 版本	需要的 Elasticsearch 最低版本
索引狀態管理		
依歐幾里德距離分類的 k-NN	1.0	7.1
異常偵測	1.0	7.4
依餘弦相似度分類的 k-NN	1.0	7.7
Learning to Rank		
Piped Processing Language	1.0	7.9
OpenSearch 儀表板報告		
OpenSearch 儀表板追蹤分析		
ARM基於重力子例證		
冷儲存		

功能	最低要求 OpenSearch 版本	需要的 Elasticsearch 最低版本
漢明距離、L1 Norm 距離和 K-NN 的 Painless 指令碼	1.0	7.10
非同步搜尋		
索引轉換	1.0	不包含
跨叢集複寫	1.1	7.10
ML Commons	1.3	不包含
通知	2.3	不包含
時間點搜索	2.5	不包含
搜尋管道	2.9	不包含
機器學習連接器	2.9	不包含
多模式语义搜索	2.11	不包含
Amazon S3 的直接查詢資料來源	2.11	不包含

如需啟用這些功能中一部分功能及其他功能的外掛程式資訊，請參閱 the section called “依引擎版本分類的外掛程式”。如需每個版本 OpenSearch API的相關資訊，請參閱the section called “受支援的操作”。

Amazon OpenSearch 服務中的引擎版本的插件

Amazon OpenSearch 服務網域已預先封裝來自 OpenSearch 社群的外掛程式。該服務會自動為您部署和管理插件，但是它會根據您為域選擇的版本 OpenSearch 或舊版 Elasticsearch 版本部署不同的插OSS件。

下表依 OpenSearch 版本列出外掛程式，以及舊版 Elasticsearch OSS 的相容版本。它只包含您可能與之互動的外掛程式，這並不全面。 OpenSearch 服務使用其他外掛程式來啟用核心服務功能，例如快照的 S3 儲存庫外掛程式，以及用於最佳化和監控的OpenSearch效能分析器外掛程式。如需在您的網域上執行的所有外掛程式的完整清單，請進行以下請求：

```
GET _cat/plugins?v
```

外掛程式	最低要求 OpenSearch 版本	需要的 Elasticsearch 最低版本
韓 LP	2.11	不支援
希伯來分析	2.11	不支援
Amazon Personalize 化搜索排	2.9	不支援
神經搜索	2.9	不支援
安全性分析	2.5	不支援
OpenSearch 通知	2.3	不支援
ML Commons	1.3	不支援
酢橘分析（推薦日語）	1.3	不支援
STConvert	1.3	不支援

外掛程式	最低要求 OpenSearch 版本	需要的 Elasticsearch 最低版本
拼音分析	1.3	不支援
紫菜分析	1.3	不支援
OpenSearch 可觀察性	1.2	不支援
OpenSearch 跨叢集複寫	1.1	7.10
OpenSearch 非同步搜尋	1.0	7.10
IK (中文) 分析	1.0	7.7
越南文分析		
泰文分析		
Learning to Rank		
OpenSearch 異常偵測	1.0	7.4
OpenSearch k-NN	1.0	7.1
OpenSearch 索引狀態管理	1.0	6.8
OpenSearch 安全	1.0	6.7

外掛程式	最低要求 OpenSearch 版本	需要的 Elasticsearch 最低版本
OpenSearch SQL	1.0	6.5
OpenSearch 警報	1.0	6.2
烏克蘭文分析	1.0	5.3
映射器大小	1.0	5.3
映射器 Murmur3	1.0	5.1
擷取使用者代理程式處理器	1.0	5.1
擷取附件處理器	1.0	5.1
Stempel 波蘭文分析	1.0	5.1
智慧型中文分析	1.0	5.1
Seunjeon 韓文分析	1.0	5.1
語音分析	1.0	2.3
日文 (kuromoji) 分析	1.0	包含在所有網域中
ICU分析	1.0	包含在所有網域中

可選插件

除了預先安裝的預設外掛程式之外，Amazon Ser OpenSearch vice 還支援多種選用的語言分析器外掛程式。您可以使用 AWS Management Console 以及 AWS CLI 將外掛程式與網域關聯、取消外掛程式與網域的關聯，並列出所有外掛程式。選用的外掛程式套件與特定 OpenSearch 版本相容，而且只能與該版本的網域相關聯。

請注意，對於 Sudachi 插件，當您重新關聯字典文件時，它不會立即反映在域上。當下一個藍/綠部署在網域上執行時，做為組態變更或其他更新的一部分時，字典會重新整理。或者，您也可以使用更新的資料建立新套件、使用這個新套件建立新索引、將現有索引重新建立索引至新索引，然後刪除舊索引。如果您偏好使用重新建立索引的方法，請使用索引別名，這樣就不會中斷流量。

可選插件使用`ZIP-PLUGIN`包類型。如需選用外掛程式的詳細資訊，請參閱the section called “自訂套件”。

Amazon OpenSearch 服務中支持的操作

OpenSearch 服務支持許多版本 OpenSearch 和傳統的彈性搜索OSS。下列各節顯示 OpenSearch Service 針對每個版本所支援的作業。

主題

- 顯著的API差異
- OpenSearch 版本 2.13
- OpenSearch 版本
- OpenSearch 第二版
- OpenSearch 版本 2.7
- OpenSearch 版本 2.5
- OpenSearch 第二版本
- OpenSearch 版本 1.3
- OpenSearch 版本 1.2
- OpenSearch 最新版本
- OpenSearch 1.0 版本
- Elasticsearch 7.10 版
- Elasticsearch 7.9 版

- Elasticsearch 7.8 版
- Elasticsearch 7.7 版
- Elasticsearch 7.4 版
- Elasticsearch 7.1 版
- Elasticsearch 6.8 版
- Elasticsearch 6.7 版
- Elasticsearch 6.5 版
- Elasticsearch 6.4 版
- Elasticsearch 6.3 版
- Elasticsearch 6.2 版
- Elasticsearch 6.0 版
- Elasticsearch 5.6 版
- Elasticsearch 5.5 版
- Elasticsearch 5.3 版
- Elasticsearch 5.1 版
- Elasticsearch 2.3 版
- Elasticsearch 1.5 版

顯著的API差異

設定和統計數字

OpenSearch 服務只接PUT受對使`_cluster/settings`API用「平面」設定表單的要求。並拒絕使用展開設定表單的請求。

```
// Accepted
PUT _cluster/settings
{
  "persistent" : {
    "action.auto_create_index" : false
  }
}

// Rejected
PUT _cluster/settings
```

```
{
  "persistent": {
    "action": {
      "auto_create_index": false
    }
  }
}
```

高級 Java REST 客戶端使用展開的表單，因此如果您需要發送設置請求，那么請使用低級客戶端。

在 Elasticsearch 5.3 之前，`_cluster/settings`API上的 OpenSearch 服務域僅支持該HTTPPUT方法，而不支持該GET方法。 OpenSearch 和更新版本的彈性搜索支持該GET方法，如以下示例所示：

```
GET https://domain-name.region.es.amazonaws.com/_cluster/settings?pretty
```

此為傳回範例：

```
{
  "persistent": {
    "cluster": {
      "routing": {
        "allocation": {
          "cluster_concurrent_rebalance": "2",
          "node_concurrent_recoveries": "2",
          "disk": {
            "watermark": {
              "low": "1.35gb",
              "flood_stage": "0.45gb",
              "high": "0.9gb"
            }
          },
          "node_initial_primarirecoveries": "4"
        }
      }
    },
    "indices": {
      "recovery": {
        "max_bytper_sec": "40mb"
      }
    }
  }
}
```

如果您比較來自開放原始碼 OpenSearch 叢集和 OpenSearch Service 的回應，以取得某些設定和統計資料APIs，您可能會注意到缺少欄位。 OpenSearch Service 會編輯公開服務內部的特定資訊，例如來自的檔案系統資料路徑，`_nodes/stats`或來自的作業系統名稱和版本。`_nodes`

縮小

這`_shrink`API可能會導致升級、組態變更和網域刪除失敗。我們不建議在執行 Elasticsearch 版本 5.3 或 5.1 的網域上使用它。這些版本皆含有可導致已縮小的索引之快照還原失敗。

如果您`_shrink`API在其他 Elasticsearch 或 OpenSearch版本上使用，請在開始壓縮作業之前提出下列要求：

```
PUT https://domain-name.region.es.amazonaws.com/source-index/_settings
{
  "settings": {
    "index.routing.allocation.require._name": "name-of-the-node-to-shrink-to",
    "index.blocks.read_only": true
  }
}
```

然後在完成縮小操作後再提出下列請求：

```
PUT https://domain-name.region.es.amazonaws.com/source-index/_settings
{
  "settings": {
    "index.routing.allocation.require._name": null,
    "index.blocks.read_only": false
  }
}

PUT https://domain-name.region.es.amazonaws.com/shrunken-index/_settings
{
  "settings": {
    "index.routing.allocation.require._name": null,
    "index.blocks.read_only": false
  }
}
```

OpenSearch 版本 2.13

對於 OpenSearch 2.13， OpenSearch 服務支持以下操作。有關大多數操作的信息，請參閱OpenSearchRESTAPI參考或特定插件的API參考。

- 索引路徑中的所有操作 (例如 /*index-name* /_forcemerge 、/*index-name* /update/*id* 以及 /*index-name* /_close)
- /_alias
- /_aliases
- /_all
- /_analyze
- /_bulk
- /_cat (/_cat/nodeattrs 除外)
- /_cluster/allocation/explain
- /_cluster/health
- /_cluster/pending_tasks
- /_cluster/settings 適用於數個屬性[4]：
  - action.auto_create_index
  - action.search.shard_count.limit
  - indices.breaker.fielddata.limit
  - indices.breaker.request.limit
  - indices.breaker.total.limit
  - cluster.max_shards_per_node
  - cluster.search.request.slowlog.level
- /_delete_by_query [1]
- /_explain
- /_field_caps
- /_field_stats
- /_flush
- /_ingest/pipeline
- /_ltr
- /_mapping
- /_mget
- /_msearch
- /_mtermvectors
- /_nodes
- /_plugins/_asynchronous_search
- /_plugins/_alerting
- /_plugins/_anomaly_detection
- /_plugins/_ism
- /_plugins/_ml
- /_plugins/_notifications
- /_plugins/_ppl
- /_plugins/_security
- /_plugins/_security_analytics
- /_plugins/_sm
- /_plugins/_sql
- /_percolate
- /_rank_eval
- /_refresh
- /_reindex [1]
- /_render
- /_resolve/index
- /_rollover
- /_scripts [3]
- /_search[2]
- /_search/pipeline
- /_search/point_in_time
- /_search profile
- /_shard_stores
- /_shrink[5]
- /_snapshot
- /_split
- /_stats
- /_status
- /_tasks
- /_template
- /_update_by_query [1]
- /_validate

• cluster.search.request.slowlog.threshold.warn • cluster.search.request.slowlog.threshold.info • cluster.search.request.slowlog.threshold.debug • cluster.search.request.slowlog.threshold.trace • search.phase_took_enabled • /_cluster/state • /_cluster/stats • /_count • /_dashboards		

1. 叢集組態變更完成之前，這些操作可能中斷。我們建議您隨這些操作一起使用 /_tasks 作業，以確認請求已成功完成。
2. DELETE/_search/scroll使用消息正文的請求必須"Content-Length"在HTTP標題中指定。根據預設，大多數的用戶端新增此標頭。若要避免scroll_id值中的=字元發生問題，請使用要求主體而非查詢字串，將scroll_id值傳遞給 OpenSearch Service。
3. 有關使用指令碼的考量事項，請參閱the section called “其他受支援的資源”。
4. 參考 PUT 方法。如需 GET 方法的詳細資訊，請參閱the section called “顯著的API差異”。此清單僅參照 OpenSearch Service 支援的一般 OpenSearch 作業，不包含針對異常偵測的外掛程式特定支援作業ISM等。
5. 請參閱 the section called “縮小”。

OpenSearch 版本

對於 OpenSearch 2.11， OpenSearch 服務支持以下操作。有關大多數操作的信息，請參閱OpenSearchRESTAPI參考或特定插件的API參考。

- 索引路徑中的所有操作 (例如 /*index-name* /_forcemerge 、/*index-name* /update/*id* 以及 /*index-name* /_close)
- /_alias
- /_aliases
- /_all
- /_analyze
- /_bulk
- /_cat (/_cat/nodeattrs 除外)
- /_cluster/allocation/explain
- /_cluster/health
- /_cluster/pending_tasks
- /_cluster/settings 適用於數個屬性[4]：
  - action.auto_create_index
  - action.search.shard_count.limit
  - indices.breaker.fielddata.limit
  - indices.breaker.request.limit
  - indices.breaker.total.limit
- /_delete_by_query [1]
- /_explain
- /_field_caps
- /_field_stats
- /_flush
- /_ingest/pipeline
- /_ltr
- /_mapping
- /_mget
- /_msearch
- /_mtermvectors
- /_nodes
- /_plugins/_asynchronous_search
- /_plugins/_alerting
- /_plugins/_anomaly_detection
- /_plugins/_ism
- /_plugins/_ml
- /_plugins/_notifications
- /_plugins/_ppl
- /_plugins/_security
- /_plugins/_security_analytics
- /_refresh
- /_reindex [1]
- /_render
- /_resolve/index
- /_rollover
- /_scripts [3]
- /_search[2]
- /_search/pipeline
- /_search/point_in_time
- /_search profile
- /_shard_stores
- /_shrink[5]
- /_snapshot
- /_split
- /_stats
- /_status
- /_tasks
- /_template
- /_update_by_query [1]
- /_validate

• cluster.max_shards_per_node • /_cluster/state • /_cluster/stats • /_count • /_dashboards	• /_plugins/_sm • /_plugins/_sql • /_percolate • /_rank_eval	

1. 叢集組態變更完成之前，這些操作可能中斷。我們建議您隨這些操作一起使用 /_tasks 作業，以確認請求已成功完成。
2. DELETE/_search/scroll使用消息正文的請求必須"Content-Length"在HTTP標題中指定。根據預設，大多數的用戶端新增此標頭。若要避免scroll_id值中的=字元發生問題，請使用要求主體而非查詢字串，將scroll_id值傳遞給 OpenSearch Service。
3. 有關使用指令碼的考量事項，請參閱the section called “其他受支援的資源”。
4. 參考 PUT 方法。如需 GET 方法的詳細資訊，請參閱the section called “顯著的API差異”。此清單僅參照 OpenSearch Service 支援的一般 OpenSearch 作業，不包含針對異常偵測的外掛程式特定支援作業ISM等。
5. 請參閱 the section called “縮小”。

OpenSearch 第二版

對於 OpenSearch 2.9， OpenSearch 服務支持以下操作。有關大多數操作的信息，請參閱OpenSearchRESTAPI參考或特定插件的API參考。

• 索引路徑中的所有操作 (例如 /*index-name* /_forcemerge 、/*index-name* /update/*id* 以及 /*index-name* /_close) • /_alias • /_aliases • /_all • /_analyze	• /_delete_by_query [1] • /_explain • /_field_caps • /_field_stats • /_flush • /_ingest/pipeline • /_ltr • /_mapping • /_mget	• /_refresh • /_reindex [1] • /_render • /_resolve/index • /_rollover • /_scripts [3] • /_search[2] • /_search/pipeline

- /_bulk
- /_cat (/_cat/nodeattrs 除外)
- /_cluster/allocation/explain
- /_cluster/health
- /_cluster/pending_tasks
- /_cluster/settings 適用於數個屬性[4]：
  - action.auto_create_index
  - action.search.shard_count.limit
  - indices.breaker.fielddata.limit
  - indices.breaker.request.limit
  - indices.breaker.total.limit
  - cluster.max_shards_per_node
- /_cluster/state
- /_cluster/stats
- /_count
- /_dashboards
- /_msearch
- /_mtermvectors
- /_nodes
- /_plugins/_asynchronous_search
- /_plugins/_alerting
- /_plugins/_anomaly_detection
- /_plugins/_ism
- /_plugins/_ml
- /_plugins/_notifications
- /_plugins/_ppl
- /_plugins/_security
- /_plugins/_security_analytics
- /_plugins/_sm
- /_plugins/_sql
- /_percolate
- /_rank_eval
- /_search/point_in_time
- /_search profile
- /_shard_stores
- /_shrink[5]
- /_snapshot
- /_split
- /_stats
- /_status
- /_tasks
- /_template
- /_update_by_query [1]
- /_validate

1. 叢集組態變更完成之前，這些操作可能中斷。我們建議您隨這些操作一起使用 /_tasks 作業，以確認請求已成功完成。
2. DELETE/_search/scroll使用消息正文的請求必須"Content-Length"在HTTP標題中指定。根據預設，大多數的用戶端新增此標頭。若要避免scroll_id值中的=字元發生問題，請使用要求主體而非查詢字串，將scroll_id值傳遞給 OpenSearch Service。
3. 有關使用指令碼的考量事項，請參閱the section called “其他受支援的資源”。

4. 參考 PUT 方法。如需 GET 方法的詳細資訊，請參閱the section called “顯著的API差異”。此清單僅參照 OpenSearch Service 支援的一般 OpenSearch 作業，不包含針對異常偵測的外掛程式特定支援作業ISM等。
5. 請參閱 the section called “縮小”。

OpenSearch 版本 2.7

對於 OpenSearch 2.7， OpenSearch 服務支持以下操作。有關大多數操作的信息，請參閱OpenSearchRESTAPI參考或特定插件的API參考。

- 索引路徑中的所有操作 (例如 /*index-name* /_forcemerge 、/*index-name* /update/*id* 以及 /*index-name* /_close)
- /_alias
- /_aliases
- /_all
- /_analyze
- /_bulk
- /_cat (/_cat/nodeattrs 除外)
- /_cluster/allocation/explain
- /_cluster/health
- /_cluster/pending_tasks
- /_cluster/settings 適用於數個屬性[4]：
  - action.auto_create_index
  - action.search.shard_count.limit
- /_delete_by_query [1]
- /_explain
- /_field_caps
- /_field_stats
- /_flush
- /_ingest/pipeline
- /_ltr
- /_mapping
- /_mget
- /_msearch
- /_mtermvectors
- /_nodes
- /_plugins/_asynchronous_search
- /_plugins/_alerting
- /_plugins/_anomaly_detection
- /_plugins/_ism
- /_plugins/_ml
- /_plugins/_notifications
- /_refresh
- /_reindex [1]
- /_render
- /_resolve/index
- /_rollover
- /_scripts [3]
- /_search[2]
- /_search/point_in_time
- /_search profile
- /_shard_stores
- /_shrink[5]
- /_snapshot
- /_split
- /_stats
- /_status
- /_tasks
- /_template
- /_update_by_query [1]
- /_validate

• indices.breaker.fielddata.limit • indices.breaker.request.limit • indices.breaker.total.limit • cluster.max_shards_per_node • /_cluster/state • /_cluster/stats • /_count • /_dashboards	• /_plugins/_ppl • /_plugins/_security • /_plugins/_security_analytics • /_plugins/_sm • /_plugins/_sql • /_percolate • /_rank_eval	

1. 叢集組態變更完成之前，這些操作可能中斷。我們建議您隨這些操作一起使用 /_tasks 作業，以確認請求已成功完成。
2. DELETE/_search/scroll使用消息正文的請求必須"Content-Length"在HTTP標題中指定。根據預設，大多數的用戶端新增此標頭。若要避免scroll_id值中的=字元發生問題，請使用要求主體而非查詢字串，將scroll_id值傳遞給 OpenSearch Service。
3. 有關使用指令碼的考量事項，請參閱the section called “其他受支援的資源”。
4. 參考 PUT 方法。如需 GET 方法的詳細資訊，請參閱the section called “顯著的API差異”。此清單僅參照 OpenSearch Service 支援的一般 OpenSearch 作業，不包含針對異常偵測的外掛程式特定支援作業ISM等。
5. 請參閱 the section called “縮小”。

OpenSearch 版本 2.5

對於 OpenSearch 2.5， OpenSearch 服務支持以下操作。有關大多數操作的信息，請參閱OpenSearchRESTAPI參考或特定插件的API參考。

• 索引路徑中的所有操作 (例如 /*index-name* /_forcemerge 、/*index-name* /	• /_delete_by_query [1] • /_explain • /_field_caps	• /_refresh • /_reindex [1] • /_render

update/*id* 以及 /*index-name* /_close)
- /_alias
- /_aliases
- /_all
- /_analyze
- /_bulk
- /_cat (/_cat/nodeattrs 除外)
- /_cluster/allocation/explain
- /_cluster/health
- /_cluster/pending_tasks
- /_cluster/settings 適用於數個屬性[4]：
  - action.auto_create_index
  - action.search.shard_count.limit
  - indices.breaker.fielddata.limit
  - indices.breaker.request.limit
  - indices.breaker.total.limit
  - cluster.max_shards_per_node
- /_cluster/state
- /_cluster/stats
- /_count
- /_dashboards
- /_field_stats
- /_flush
- /_ingest/pipeline
- /_ltr
- /_mapping
- /_mget
- /_msearch
- /_mtermvectors
- /_nodes
- /_plugins/_asynchronous_search
- /_plugins/_alerting
- /_plugins/_anomaly_detection
- /_plugins/_ism
- /_plugins/_ml
- /_plugins/_notifications
- /_plugins/_ppl
- /_plugins/_security
- /_plugins/_security_analytics
- /_plugins/_sm
- /_plugins/_sql
- /_percolate
- /_rank_eval
- /_resolve/index
- /_rollover
- /_scripts [3]
- /_search[2]
- /_search/point_in_time
- /_search profile
- /_shard_stores
- /_shrink[5]
- /_snapshot
- /_split
- /_stats
- /_status
- /_tasks
- /_template
- /_update_by_query [1]
- /_validate

1. 叢集組態變更完成之前，這些操作可能中斷。我們建議您隨這些操作一起使用 `/_tasks` 作業，以確認請求已成功完成。
2. DELETE`/_search/scroll`使用消息正文的請求必須`"Content-Length"`在HTTP標題中指定。根據預設，大多數的用戶端新增此標頭。若要避免`scroll_id`值中的`=`字元發生問題，請使用要求主體而非查詢字串，將`scroll_id`值傳遞給 OpenSearch Service。
3. 有關使用指令碼的考量事項，請參閱the section called “其他受支援的資源”。
4. 參考 PUT 方法。如需 GET 方法的詳細資訊，請參閱the section called “顯著的API差異”。此清單僅參照 OpenSearch Service 支援的一般 OpenSearch 作業，不包含針對異常偵測的外掛程式特定支援作業ISM等。
5. 請參閱 the section called “縮小”。

OpenSearch 第二版本

對於 OpenSearch 2.3， OpenSearch 服務支持以下操作。有關大多數操作的信息，請參閱OpenSearchRESTAPI參考或特定插件的API參考。

- 索引路徑中的所有操作 (例如 `/index-name /_forcemerge` 、`/index-name /update/id` 以及 `/index-name /_close`)
- `/_alias`
- `/_aliases`
- `/_all`
- `/_analyze`
- `/_bulk`
- `/_cat` (`/_cat/nodeattrs` 除外)
- `/_cluster/allocation/explain`
- `/_cluster/health`
- `/_cluster/pending_tasks`
- `/_delete_by_query` [1]
- `/_explain`
- `/_field_caps`
- `/_field_stats`
- `/_flush`
- `/_ingest/pipeline`
- `/_ltr`
- `/_mapping`
- `/_mget`
- `/_msearch`
- `/_mtermvectors`
- `/_nodes`
- `/_plugins/_asynchronous_search`
- `/_plugins/_alerting`
- `/_refresh`
- `/_reindex` [1]
- `/_render`
- `/_resolve/index`
- `/_rollover`
- `/_scripts` [3]
- `/_search`[2]
- `/_search profile`
- `/_shard_stores`
- `/_shrink`[5]
- `/_snapshot`
- `/_split`
- `/_stats`
- `/_status`
- `/_tasks`
- `/_template`

• /_cluster/settings 適用於數個屬性[4]：
  • action.auto_create_index
  • action.search.shard_count.limit
  • indices.breaker.fielddata.limit
  • indices.breaker.request.limit
  • indices.breaker.total.limit
  • cluster.max_shards_per_node
• /_cluster/state
• /_cluster/stats
• /_count
• /_dashboards
	• /_plugins/_anomaly_detection
	• /_plugins/_ism
	• /_plugins/_ml
	• _plugins/_notifications
	• /_plugins/_ppl
	• /_plugins/_security
	• /_plugins/_sql
	• /_percolate
	• /_rank_eval
		• /_update_by_query [1]
		• /_validate

1. 叢集組態變更完成之前，這些操作可能中斷。我們建議您隨這些操作一起使用 /_tasks 作業，以確認請求已成功完成。
2. DELETE/_search/scroll使用消息正文的請求必須"Content-Length"在HTTP標題中指定。根據預設，大多數的用戶端新增此標頭。若要避免scroll_id值中的=字元發生問題，請使用要求主體而非查詢字串，將scroll_id值傳遞給 OpenSearch Service。
3. 有關使用指令碼的考量事項，請參閱the section called “其他受支援的資源”。
4. 參考 PUT 方法。如需 GET 方法的詳細資訊，請參閱the section called “顯著的API差異”。此清單僅參照 OpenSearch Service 支援的一般 OpenSearch 作業，不包含針對異常偵測的外掛程式特定支援作業ISM等。
5. 請參閱 the section called “縮小”。

OpenSearch 版本 1.3

對於 OpenSearch 1.3，本 OpenSearch 服務支援下列操作。有關大多數操作的信息，請參閱OpenSearchRESTAPI參考或特定插件的API參考。

- 索引路徑中的所有操作 (例如 /*index-name* /_forcemerge 、/*index-name* /update/*id* 以及 /*index-name* /_close)
- /_alias
- /_aliases
- /_all
- /_analyze
- /_bulk
- /_cat (/_cat/nodeattrs 除外)
- /_cluster/allocation/explain
- /_cluster/health
- /_cluster/pending_tasks
- /_cluster/settings 適用於數個屬性[4]：
  - action.auto_create_index
  - action.search.shard_count.limit
  - indices.breaker.fielddata.limit
  - indices.breaker.request.limit
  - indices.breaker.total.limit
- /_delete_by_query [1]
- /_explain
- /_field_caps
- /_field_stats
- /_flush
- /_ingest/pipeline
- /_ltr
- /_mapping
- /_mget
- /_msearch
- /_mtermvectors
- /_nodes
- /_plugins/_asynchronous_search
- /_plugins/_alerting
- /_plugins/_anomaly_detection
- /_plugins/_ism
- /_plugins/_ml
- /_plugins/_ppl
- /_plugins/_security
- /_plugins/_sql
- /_percolate
- /_rank_eval
- /_refresh
- /_reindex [1]
- /_render
- /_resolve/index
- /_rollover
- /_scripts [3]
- /_search[2]
- /_search profile
- /_shard_stores
- /_shrink[5]
- /_snapshot
- /_split
- /_stats
- /_status
- /_tasks
- /_template
- /_update_by_query [1]
- /_validate

• cluster.max_shards_per_node • /_cluster/state • /_cluster/stats • /_count • /_dashboards		

1. 叢集組態變更完成之前，這些操作可能中斷。我們建議您隨這些操作一起使用 /_tasks 作業，以確認請求已成功完成。
2. DELETE/_search/scroll使用消息正文的請求必須"Content-Length"在HTTP標題中指定。根據預設，大多數的用戶端新增此標頭。若要避免scroll_id值中的=字元發生問題，請使用要求主體而非查詢字串，將scroll_id值傳遞給 OpenSearch Service。
3. 有關使用指令碼的考量事項，請參閱the section called “其他受支援的資源”。
4. 參考 PUT 方法。如需 GET 方法的詳細資訊，請參閱the section called “顯著的API差異”。此清單僅參照 OpenSearch Service 支援的一般 OpenSearch 作業，不包含針對異常偵測的外掛程式特定支援作業ISM等。
5. 請參閱 the section called “縮小”。

OpenSearch 版本 1.2

對於 OpenSearch 1.2， OpenSearch 服務支持以下操作。有關大多數操作的信息，請參閱OpenSearchRESTAPI參考或特定插件的API參考。

• 索引路徑中的所有操作 (例如 /*index-name* /_forcemerge 、/*index-name* /update/*id* 以及 /*index-name* /_close) • /_alias • /_aliases • /_all • /_analyze	• /_delete_by_query [1] • /_explain • /_field_caps • /_field_stats • /_flush • /_ingest/pipeline • /_ltr • /_mapping • /_mget	• /_refresh • /_reindex [1] • /_render • /_resolve/index • /_rollover • /_scripts [3] • /_search[2] • /_search profile • /_shard_stores

- /_bulk
- /_cat (/_cat/nodeattrs 除外)
- /_cluster/allocation/explain
- /_cluster/health
- /_cluster/pending_tasks
- /_cluster/settings 適用於數個屬性[4]：
  - action.auto_create_index
  - action.search.shard_count.limit
  - indices.breaker.fielddata.limit
  - indices.breaker.request.limit
  - indices.breaker.total.limit
  - cluster.max_shards_per_node
- /_cluster/state
- /_cluster/stats
- /_count
- /_dashboards
- /_msearch
- /_mtermvectors
- /_nodes
- /_plugins/_asynchronous_search
- /_plugins/_alerting
- /_plugins/_anomaly_detection
- /_plugins/_ism
- /_plugins/_ppl
- /_plugins/_security
- /_plugins/_sql
- /_percolate
- /_rank_eval
- /_shrink[5]
- /_snapshot
- /_split
- /_stats
- /_status
- /_tasks
- /_template
- /_update_by_query [1]
- /_validate

1. 叢集組態變更完成之前，這些操作可能中斷。我們建議您隨這些操作一起使用 /_tasks 作業，以確認請求已成功完成。
2. DELETE/_search/scroll使用消息正文的請求必須"Content-Length"在HTTP標題中指定。根據預設，大多數的用戶端新增此標頭。若要避免scroll_id值中的=字元發生問題，請使用要求主體而非查詢字串，將scroll_id值傳遞給 OpenSearch Service。
3. 有關使用指令碼的考量事項，請參閱the section called “其他受支援的資源”。

4. 參考 PUT 方法。如需 GET 方法的詳細資訊，請參閱the section called “顯著的API差異”。此清單僅參照 OpenSearch Service 支援的一般 OpenSearch 作業，不包含針對異常偵測的外掛程式特定支援作業ISM等。
5. 請參閱 the section called “縮小”。

OpenSearch 最新版本

對於 OpenSearch 1.1， OpenSearch 服務支持以下操作。有關大多數操作的信息，請參閱OpenSearchRESTAPI參考或特定插件的API參考。

- 索引路徑中的所有操作 (例如 /*index-name* /_forcemerge 、/*index-name* /update/*id* 以及 /*index-name* /_close)
- /_alias
- /_aliases
- /_all
- /_analyze
- /_bulk
- /_cat (/_cat/nodeattrs 除外)
- /_cluster/allocation/explain
- /_cluster/health
- /_cluster/pending_tasks
- /_cluster/settings 適用於數個屬性[4]：
  - action.auto_create_index
  - action.search.shard_count.limit
- /_delete_by_query [1]
- /_explain
- /_field_caps
- /_field_stats
- /_flush
- /_ingest/pipeline
- /_ltr
- /_mapping
- /_mget
- /_msearch
- /_mtermvectors
- /_nodes
- /_plugins/_asynchronous_search
- /_plugins/_alerting
- /_plugins/_anomaly_detection
- /_plugins/_ism
- /_plugins/_ppl
- /_plugins/_security
- /_refresh
- /_reindex [1]
- /_render
- /_resolve/index
- /_rollover
- /_scripts [3]
- /_search[2]
- /_search profile
- /_shard_stores
- /_shrink[5]
- /_snapshot
- /_split
- /_stats
- /_status
- /_tasks
- /_template
- /_update_by_query [1]
- /_validate

• indices.breaker.fielddata.limit • indices.breaker.request.limit • indices.breaker.total.limit • cluster.max_shards_per_node • /_cluster/state • /_cluster/stats • /_count • /_dashboards	• /_plugins/_sql • /_plugins/_transforms • /_percolate • /_rank_eval	

1. 叢集組態變更完成之前，這些操作可能中斷。我們建議您隨這些操作一起使用 /_tasks 作業，以確認請求已成功完成。
2. DELETE/_search/scroll使用消息正文的請求必須"Content-Length"在HTTP標題中指定。根據預設，大多數的用戶端新增此標頭。若要避免scroll_id值中的=字元發生問題，請使用要求主體而非查詢字串，將scroll_id值傳遞給 OpenSearch Service。
3. 有關使用指令碼的考量事項，請參閱the section called “其他受支援的資源”。
4. 參考 PUT 方法。如需 GET 方法的詳細資訊，請參閱the section called “顯著的API差異”。此清單僅參照 OpenSearch Service 支援的一般 OpenSearch 作業，不包含針對異常偵測的外掛程式特定支援作業ISM等。
5. 請參閱 the section called “縮小”。

OpenSearch 1.0 版本

對於 OpenSearch 1.0， OpenSearch 服務支持以下操作。有關大多數操作的信息，請參閱OpenSearchRESTAPI參考或特定插件的API參考。

• 索引路徑中的所有操作 (例如 /*index-name* /_forcemerge 、/*index-name* /	• /_delete_by_query [1] • /_explain • /_field_caps	• /_refresh • /_reindex [1] • /_render

update/*id* 以及 /*index-name* /_close)
- /_alias
- /_aliases
- /_all
- /_analyze
- /_bulk
- /_cat (/_cat/nodeattrs 除外)
- /_cluster/allocation/explain
- /_cluster/health
- /_cluster/pending_tasks
- /_cluster/settings 適用於數個屬性[4]：
  - action.auto_create_index
  - action.search.shard_count.limit
  - indices.breaker.fielddata.limit
  - indices.breaker.request.limit
  - indices.breaker.total.limit
  - cluster.max_shards_per_node
- /_cluster/state
- /_cluster/stats
- /_count
- /_dashboards
- /_field_stats
- /_flush
- /_ingest/pipeline
- /_ltr
- /_mapping
- /_mget
- /_msearch
- /_mtermvectors
- /_nodes
- /_plugins/_asynchronous_search
- /_plugins/_alerting
- /_plugins/_anomaly_detection
- /_plugins/_ism
- /_plugins/_ppl
- /_plugins/_security
- /_plugins/_sql
- /_plugins/_transforms
- /_percolate
- /_rank_eval
- /_resolve/index
- /_rollover
- /_scripts [3]
- /_search[2]
- /_search profile
- /_shard_stores
- /_shrink[5]
- /_snapshot
- /_split
- /_stats
- /_status
- /_tasks
- /_template
- /_update_by_query [1]
- /_validate

1. 叢集組態變更完成之前，這些操作可能中斷。我們建議您隨這些操作一起使用 `/_tasks` 作業，以確認請求已成功完成。
2. `DELETE/_search/scroll`使用消息正文的請求必須`"Content-Length"`在HTTP標題中指定。根據預設，大多數的用戶端新增此標頭。若要避免`scroll_id`值中的`=`字元發生問題，請使用要求主體而非查詢字串，將`scroll_id`值傳遞給 OpenSearch Service。
3. 有關使用指令碼的考量事項，請參閱the section called “其他受支援的資源”。
4. 參考 PUT 方法。如需 GET 方法的詳細資訊，請參閱the section called “顯著的API差異”。此清單僅參照 OpenSearch Service 支援的一般 OpenSearch 作業，不包含針對異常偵測的外掛程式特定支援作業ISM等。
5. 請參閱 the section called “縮小”。

Elasticsearch 7.10 版

對於彈性搜索 7.10， OpenSearch 服務支持以下操作。

- 索引路徑中的所有操作 (例如 `/index-name /_forcemerge` 、`/index-name /update/id` 以及 `/index-name /_close`)
- `/_alias`
- `/_aliases`
- `/_all`
- `/_analyze`
- `/_bulk`
- `/_cat` (`/_cat/nodeattrs` 除外)
- `/_cluster/allocation/explain`
- `/_cluster/health`
- `/_cluster/pending_tasks`
- `/_cluster/settings` 適用於數個屬性[4]：
- `/_delete_by_query` [1]
- `/_explain`
- `/_field_caps`
- `/_field_stats`
- `/_flush`
- `/_index_template` [6]
- `/_ingest/pipeline`
- `/_index_template`
- `/_ltr`
- `/_mapping`
- `/_mget`
- `/_msearch`
- `/_mtermvectors`
- `/_nodes`
- `/_opendistro/_alerting`
- `/_refresh`
- `/_reindex` [1]
- `/_render`
- `/_resolve/index`
- `/_rollover`
- `/_scripts` [3]
- `/_search`[2]
- `/_search profile`
- `/_shard_stores`
- `/_shrink`[5]
- `/_snapshot`
- `/_split`
- `/_stats`
- `/_status`
- `/_tasks`
- `/_template` [6]
- `/_update_by_query` [1]

- action.auto_create_index
- action.search.shard_count.limit
- indices.breaker.fielddata.limit
- indices.breaker.request.limit
- indices.breaker.total.limit
- cluster.max_shards_per_node
- /_cluster/state
- /_cluster/stats
- /_count
- /_opendistro/_asynchronous_search
- /_opendistro/_anomaly_detection
- /_opendistro/_ism
- /_opendistro/_ppl
- /_opendistro/_security
- /_opendistro/_sql
- /_percolate
- /_plugin/kibana
- /_plugins/_replication
- /_rank_eval
- /_validate

1. 叢集組態變更完成之前，這些操作可能中斷。我們建議您隨這些操作一起使用 /_tasks 作業，以確認請求已成功完成。
2. DELETE/_search/scroll使用消息正文的請求必須"Content-Length"在HTTP標題中指定。根據預設，大多數的用戶端新增此標頭。若要避免scroll_id值中的=字元發生問題，請使用要求主體而非查詢字串，將scroll_id值傳遞給 OpenSearch Service。
3. 有關使用指令碼的考量事項，請參閱the section called “其他受支援的資源”。
4. 參考 PUT 方法。如需 GET 方法的詳細資訊，請參閱the section called “顯著的API差異”。此清單僅參考 OpenSearch 服務支援的一般 Elasticsearch 作業，不包含針對異常偵測的外掛程式特定支援作業等ISM。
5. 請參閱 the section called “縮小”。
6. 舊版索引範本 (_template) 被可組合的範本 (_index_template) 所取代，從 Elasticsearch 7.8 開始。可組合的範本優先於舊版範本。如果可組合的範本與指定索引不匹配，則舊版範本仍然匹配並套用。該_template操作仍然適用於 Elasticsearch OpenSearch 和更高版本OSS，但GET調用這兩種模板類型會返回不同的結果。

Elasticsearch 7.9 版

對於彈性搜索 7.9， OpenSearch 服務支持以下操作。

- 索引路徑中的所有操作 (例如 /*index-name* /_forcemerge 、/*index-name* /update/*id* 以及 /*index-name* /_close)
- /_alias
- /_aliases
- /_all
- /_analyze
- /_bulk
- /_cat (/_cat/nodeattrs 除外)
- /_cluster/allocation/explain
- /_cluster/health
- /_cluster/pending_tasks
- /_cluster/settings 適用於數個屬性[4]：
  - action.auto_create_index
  - action.search.shard_count.limit
  - indices.breaker.fielddata.limit
  - indices.breaker.request.limit
  - indices.breaker.total.limit
- /_delete_by_query [1]
- /_explain
- /_field_caps
- /_field_stats
- /_flush
- /_index_template [6]
- /_ingest/pipeline
- /_ltr
- /_mapping
- /_mget
- /_msearch
- /_mtermvectors
- /_nodes
- /_opendistro/_alerting
- /_opendistro/_anomaly_detection
- /_opendistro/_ism
- /_opendistro/_ppl
- /_opendistro/_security
- /_opendistro/_sql
- /_percolate
- /_plugin/kibana
- /_rank_eval
- /_refresh
- /_reindex [1]
- /_render
- /_resolve/index
- /_rollover
- /_scripts [3]
- /_search[2]
- /_search profile
- /_shard_stores
- /_shrink[5]
- /_snapshot
- /_split
- /_stats
- /_status
- /_tasks
- /_template [6]
- /_update_by_query [1]
- /_validate

• cluster.max_shards_per_node • /_cluster/state • /_cluster/stats • /_count		

1. 叢集組態變更完成之前，這些操作可能中斷。我們建議您隨這些操作一起使用 /_tasks 作業，以確認請求已成功完成。
2. DELETE/_search/scroll使用消息正文的請求必須"Content-Length"在HTTP標題中指定。根據預設，大多數的用戶端新增此標頭。若要避免scroll_id值中的=字元發生問題，請使用要求主體而非查詢字串，將scroll_id值傳遞給 OpenSearch Service。
3. 有關使用指令碼的考量事項，請參閱the section called “其他受支援的資源”。
4. 參考 PUT 方法。如需 GET 方法的詳細資訊，請參閱the section called “顯著的API差異”。此清單僅參照 OpenSearch Service 支援的一般 OpenSearch 作業，不包含針對異常偵測的外掛程式特定支援作業ISM等。
5. 請參閱 the section called “縮小”。
6. 舊版索引範本 (_template) 被可組合的範本 (_index_template) 所取代，從 Elasticsearch 7.8 開始。可組合的範本優先於舊版範本。如果可組合的範本與指定索引不匹配，則舊版範本仍然匹配並套用。該_template操作仍然適用於 Elasticsearch OpenSearch 和更高版本OSS，但GET調用這兩種模板類型會返回不同的結果。

Elasticsearch 7.8 版

對於彈性搜索 7.8， OpenSearch 服務支持以下操作。

• 索引路徑中的所有操作 (例如 /*index-name* /_forcemerge 、/*index-name* /update/*id* 以及 /*index-name* /_close) • /_alias • /_aliases • /_all	• /_cluster/state • /_cluster/stats • /_count • /_delete_by_query [1] • /_explain • /_field_caps • /_field_stats	• /_refresh • /_reindex [1] • /_render • /_rollover • /_scripts [3] • /_search[2] • /_search profile

- /_analyze
- /_bulk
- /_cat (/_cat/nodeattrs 除外)
- /_cluster/allocation/explain
- /_cluster/health
- /_cluster/pending_tasks
- /_cluster/settings 適用於數個屬性[4]：
  - action.auto_create_index
  - action.search.shard_count.limit
  - indices.breaker.fielddata.limit
  - indices.breaker.request.limit
  - indices.breaker.total.limit
  - cluster.max_shards_per_node
- /_flush
- /_index_template [6]
- /_ingest/pipeline
- /_ltr
- /_mapping
- /_mget
- /_msearch
- /_mtermvectors
- /_nodes
- /_opendistro/_alerting
- /_opendistro/_anomaly_detection
- /_opendistro/_ism
- /_opendistro/_security
- /_opendistro/_sql
- /_percolate
- /_plugin/kibana
- /_rank_eval
- /_shard_stores
- /_shrink[5]
- /_snapshot
- /_split
- /_stats
- /_status
- /_tasks
- /_template [6]
- /_update_by_query [1]
- /_validate

1. 叢集組態變更完成之前，這些操作可能中斷。我們建議您隨這些操作一起使用 /_tasks 作業，以確認請求已成功完成。
2. DELETE/_search/scroll使用消息正文的請求必須"Content-Length"在HTTP標題中指定。根據預設，大多數的用戶端新增此標頭。若要避免scroll_id值中的=字元發生問題，請使用要求主體而非查詢字串，將scroll_id值傳遞給 OpenSearch Service。
3. 有關使用指令碼的考量事項，請參閱the section called “其他受支援的資源”。
4. 參考 PUT 方法。如需 GET 方法的詳細資訊，請參閱the section called “顯著的API差異”。此清單僅參考 OpenSearch 服務支援的一般 Elasticsearch 作業，不包含針對異常偵測的外掛程式特定支援作業等ISM。

5. 請參閱 the section called “縮小”。
6. 舊版索引範本 (`_template`) 被可組合的範本 (`_index_template`) 所取代，從 Elasticsearch 7.8 開始。可組合的範本優先於舊版範本。如果可組合的範本與指定索引不匹配，則舊版範本仍然匹配並套用。該`_template`操作仍然適用於 Elasticsearch OpenSearch 和更高版本OSS，但GET調用這兩種模板類型會返回不同的結果。

Elasticsearch 7.7 版

針對彈性搜尋 7.7， OpenSearch 服務支援下列作業。

- 索引路徑中的所有操作 (例如 `/index-name /_forcemerge` 、`/index-name /update/id` 以及 `/index-name /_close`)
- `/_alias`
- `/_aliases`
- `/_all`
- `/_analyze`
- `/_bulk`
- `/_cat` (`/_cat/nodeattrs` 除外)
- `/_cluster/allocation/explain`
- `/_cluster/health`
- `/_cluster/pending_tasks`
- `/_cluster/settings` 適用於數個屬性[4]：
  - `action.auto_create_index`
  - `action.search.shard_count.limit`
- `/_cluster/state`
- `/_cluster/stats`
- `/_count`
- `/_delete_by_query` [1]
- `/_explain`
- `/_field_caps`
- `/_field_stats`
- `/_flush`
- `/_ingest/pipeline`
- `/_ltr`
- `/_mapping`
- `/_mget`
- `/_msearch`
- `/_mtermvectors`
- `/_nodes`
- `/_opendistro/_alerting`
- `/_opendistro/_anomaly_detection`
- `/_opendistro/_ism`
- `/_opendistro/_security`
- `/_refresh`
- `/_reindex` [1]
- `/_render`
- `/_rollover`
- `/_scripts` [3]
- `/_search`[2]
- `/_search profile`
- `/_shard_stores`
- `/_shrink`[5]
- `/_snapshot`
- `/_split`
- `/_stats`
- `/_status`
- `/_tasks`
- `/_template`
- `/_update_by_query` [1]
- `/_validate`

• indices.breaker.fielddata.limit • indices.breaker.request.limit • indices.breaker.total.limit • cluster.max_shards_per_node	• /_opendistro/_sql • /_percolate • /_plugin/kibana • /_rank_eval	

1. 叢集組態變更完成之前，這些操作可能中斷。我們建議您隨這些操作一起使用 /_tasks 作業，以確認請求已成功完成。
2. DELETE/_search/scroll使用消息正文的請求必須"Content-Length"在HTTP標題中指定。根據預設，大多數的用戶端新增此標頭。若要避免scroll_id值中的=字元發生問題，請使用要求主體而非查詢字串，將scroll_id值傳遞給 OpenSearch Service。
3. 有關使用指令碼的考量事項，請參閱the section called “其他受支援的資源”。
4. 參考 PUT 方法。如需 GET 方法的詳細資訊，請參閱the section called “顯著的API差異”。此清單僅參考 OpenSearch 服務支援的一般 Elasticsearch 作業，不包含針對異常偵測的外掛程式特定支援作業等ISM。
5. 請參閱 the section called “縮小”。

Elasticsearch 7.4 版

對於彈性搜索 7.4， OpenSearch 服務支持以下操作。

• 索引路徑中的所有操作 (例如 /*index-name* /_forcemerge 、/*index-name* /update/*id* 以及 /*index-name* /_close) • /_alias • /_aliases • /_all • /_analyze	• /_cluster/state • /_cluster/stats • /_count • /_delete_by_query [1] • /_explain • /_field_caps • /_field_stats • /_flush	• /_refresh • /_reindex [1] • /_render • /_rollover • /_scripts [3] • /_search[2] • /_search profile • /_shard_stores

- /_bulk
- /_cat (/_cat/nodeattrs 除外)
- /_cluster/allocation/explain
- /_cluster/health
- /_cluster/pending_tasks
- /_cluster/settings 適用於數個屬性[4]：
  - action.auto_create_index
  - action.search.shard_count.limit
  - indices.breaker.fielddata.limit
  - indices.breaker.request.limit
  - indices.breaker.total.limit
  - cluster.max_shards_per_node
- /_ingest/pipeline
- /_mapping
- /_mget
- /_msearch
- /_mtermvectors
- /_nodes
- /_opendistro/_alerting
- /_opendistro/_anomaly_detection
- /_opendistro/_ism
- /_opendistro/_security
- /_opendistro/_sql
- /_percolate
- /_plugin/kibana
- /_rank_eval
- /_shrink[5]
- /_snapshot
- /_split
- /_stats
- /_status
- /_tasks
- /_template
- /_update_by_query [1]
- /_validate

1. 叢集組態變更完成之前，這些操作可能中斷。我們建議您隨這些操作一起使用 /_tasks 作業，以確認請求已成功完成。
2. DELETE/_search/scroll使用消息正文的請求必須"Content-Length"在HTTP標題中指定。根據預設，大多數的用戶端新增此標頭。若要避免scroll_id值中的=字元發生問題，請使用要求主體而非查詢字串，將scroll_id值傳遞給 OpenSearch Service。
3. 有關使用指令碼的考量事項，請參閱the section called “其他受支援的資源”。
4. 參考 PUT 方法。如需 GET 方法的詳細資訊，請參閱the section called “顯著的API差異”。此清單僅參考 OpenSearch 服務支援的一般 Elasticsearch 作業，不包含針對異常偵測的外掛程式特定支援作業等ISM。
5. 請參閱 the section called “縮小”。

Elasticsearch 7.1 版

對於彈性搜索 7.1， OpenSearch 服務支持以下操作。

- 索引路徑中的所有操作 (例如 /*index-name* /_forcemerge 和 /*index-name* /update/*id*)，/*index-name* /_close 除外
- /_alias
- /_aliases
- /_all
- /_analyze
- /_bulk
- /_cat (/_cat/nodeattrs 除外)
- /_cluster/allocation/explain
- /_cluster/health
- /_cluster/pending_tasks
- /_cluster/settings 適用於數個屬性[4]：
  - action.auto_create_index
  - action.search.shard_count.limit
  - indices.breaker.fielddata.limit
  - indices.breaker.request.limit
  - indices.breaker.total.limit
- /_cluster/state
- /_cluster/stats
- /_count
- /_delete_by_query [1]
- /_explain
- /_field_caps
- /_field_stats
- /_flush
- /_ingest/pipeline
- /_mapping
- /_mget
- /_msearch
- /_mtermvectors
- /_nodes
- /_opendistro/_alerting
- /_opendistro/_ism
- /_opendistro/_security
- /_opendistro/_sql
- /_percolate
- /_plugin/kibana
- /_rank_eval
- /_refresh
- /_reindex [1]
- /_render
- /_rollover
- /_scripts [3]
- /_search[2]
- /_search profile
- /_shard_stores
- /_shrink[5]
- /_snapshot
- /_split
- /_stats
- /_status
- /_tasks
- /_template
- /_update_by_query [1]
- /_validate

• cluster.max_shards_per_node		

1. 叢集組態變更完成之前，這些操作可能中斷。我們建議您隨這些操作一起使用 /_tasks 作業，以確認請求已成功完成。
2. DELETE/_search/scroll使用消息正文的請求必須"Content-Length"在HTTP標題中指定。根據預設，大多數的用戶端新增此標頭。若要避免scroll_id值中的=字元發生問題，請使用要求主體而非查詢字串，將scroll_id值傳遞給 OpenSearch Service。
3. 有關使用指令碼的考量事項，請參閱the section called “其他受支援的資源”。
4. 參考 PUT 方法。如需 GET 方法的詳細資訊，請參閱the section called “顯著的API差異”。此清單僅參考 OpenSearch 服務支援的一般 Elasticsearch 作業，不包含針對異常偵測的外掛程式特定支援作業等ISM。
5. 請參閱 the section called “縮小”。

Elasticsearch 6.8 版

對於彈性搜索 6.8， OpenSearch 服務支持以下操作。

• 索引路徑中的所有操作 (例如 /*index-name* /_forcemerge 和 /*index-name* /update/*id*)，/*index-name* /_close 除外 • /_alias • /_aliases • /_all • /_analyze • /_bulk • /_cat (/_cat/nodeattrs 除外) • /_cluster/allocation/explain • /_cluster/health	• /_cluster/state • /_cluster/stats • /_count • /_delete_by_query [1] • /_explain • /_field_caps • /_field_stats • /_flush • /_ingest/pipeline • /_mapping • /_mget • /_msearch • /_mtermvectors	• /_refresh • /_reindex [1] • /_render • /_rollover • /_scripts [3] • /_search[2] • /_search profile • /_shard_stores • /_shrink[5] • /_snapshot • /_split • /_stats • /_status

- /_cluster/pending_tasks
- /_cluster/settings 適用於數個屬性[4]：
  - action.auto_create_index
  - action.search.shard_count.limit
  - indices.breaker.fielddata.limit
  - indices.breaker.request.limit
  - indices.breaker.total.limit
  - cluster.max_shards_per_node
  - cluster.blocks.read_only
- /_nodes
- /_opendistro/_alerting
- /_opendistro/_ism
- /_opendistro/_security
- /_opendistro/_sql
- /_percolate
- /_plugin/kibana
- /_rank_eval
- /_tasks
- /_template
- /_update_by_query [1]
- /_validate

1. 叢集組態變更完成之前，這些操作可能中斷。我們建議您隨這些操作一起使用 /_tasks 作業，以確認請求已成功完成。
2. DELETE/_search/scroll使用消息正文的請求必須"Content-Length"在HTTP標題中指定。根據預設，大多數的用戶端新增此標頭。若要避免scroll_id值中的=字元發生問題，請使用要求主體而非查詢字串，將scroll_id值傳遞給 OpenSearch Service。
3. 有關使用指令碼的考量事項，請參閱the section called “其他受支援的資源”。
4. 參考 PUT 方法。如需 GET 方法的詳細資訊，請參閱the section called “顯著的API差異”。此清單僅參考 OpenSearch 服務支援的一般 Elasticsearch 作業，不包含針對異常偵測的外掛程式特定支援作業等ISM。
5. 請參閱 the section called “縮小”。

Elasticsearch 6.7 版

對於彈性搜索 6.7， OpenSearch 服務支持以下操作。

- 索引路徑中的所有操作 (例如 /*index-name* /_forcemerge 和 /*index-name* /update/*id*) , /*index-name* /_close 除外
- /_alias
- /_aliases
- /_all
- /_analyze
- /_bulk
- /_cat (/_cat/nodeattrs 除外)
- /_cluster/allocation/explain
- /_cluster/health
- /_cluster/pending_tasks
- /_cluster/settings 適用於數個屬性[4]：
  - action.auto_create_index
  - action.search.shard_count.limit
  - indices.breaker.fielddata.limit
  - indices.breaker.request.limit
  - indices.breaker.total.limit
  - cluster.max_shards_per_node
- /_cluster/state
- /_cluster/stats
- /_count
- /_delete_by_query [1]
- /_explain
- /_field_caps
- /_field_stats
- /_flush
- /_ingest/pipeline
- /_mapping
- /_mget
- /_msearch
- /_mtermvectors
- /_nodes
- /_opendistro/_alerting
- /_opendistro/_security
- /_opendistro/_sql
- /_percolate
- /_plugin/kibana
- /_rank_eval
- /_refresh
- /_reindex [1]
- /_render
- /_rollover
- /_scripts [3]
- /_search[2]
- /_search profile
- /_shard_stores
- /_shrink[5]
- /_snapshot
- /_split
- /_stats
- /_status
- /_tasks
- /_template
- /_update_by_query [1]
- /_validate

1. 叢集組態變更完成之前，這些操作可能中斷。我們建議您隨這些操作一起使用 `/_tasks` 作業，以確認請求已成功完成。
2. `DELETE/_search/scroll`使用消息正文的請求必須`"Content-Length"`在HTTP標題中指定。根據預設，大多數的用戶端新增此標頭。若要避免`scroll_id`值中的`=`字元發生問題，請使用要求主體而非查詢字串，將`scroll_id`值傳遞給 OpenSearch Service。
3. 有關使用指令碼的考量事項，請參閱the section called “其他受支援的資源”。
4. 參考 PUT 方法。如需 GET 方法的詳細資訊，請參閱the section called “顯著的API差異”。此清單僅參考 OpenSearch 服務支援的一般 Elasticsearch 作業，不包含針對異常偵測的外掛程式特定支援作業等ISM。
5. 請參閱 the section called “縮小”。

Elasticsearch 6.5 版

對於彈性搜索 6.5， OpenSearch 服務支持以下操作。

• 索引路徑中的所有操作 (例如 `/index-name /_forcemerge` 和 `/index-name /update/id`)，`/index-name /_close` 除外 • `/_alias` • `/_aliases` • `/_all` • `/_analyze` • `/_bulk` • `/_cat` (`/_cat/nodeattrs` 除外) • `/_cluster/allocation/explain` • `/_cluster/health` • `/_cluster/pending_tasks` • `/_cluster/settings` 適用於數個屬性[4]：	• `/_cluster/state` • `/_cluster/stats` • `/_count` • `/_delete_by_query` [1] • `/_explain` • `/_field_caps` • `/_field_stats` • `/_flush` • `/_ingest/pipeline` • `/_mapping` • `/_mget` • `/_msearch` • `/_mtermvectors` • `/_nodes` • `/_opendistro/_alerting` • `/_opendistro/_sql`	• `/_refresh` • `/_reindex` [1] • `/_render` • `/_rollover` • `/_scripts` [3] • `/_search`[2] • `/_search profile` • `/_shard_stores` • `/_shrink`[5] • `/_snapshot` • `/_split` • `/_stats` • `/_status` • `/_tasks` • `/_template` • `/_update_by_query` [1] • `/_validate`

• action.auto_create_index • action.search.shard_count.limit • indices.breaker.fielddata.limit • indices.breaker.request.limit • indices.breaker.total.limit	• /_percolate • /_plugin/kibana • /_rank_eval	

1. 叢集組態變更完成之前，這些操作可能中斷。我們建議您隨這些操作一起使用 /_tasks 作業，以確認請求已成功完成。
2. DELETE/_search/scroll使用消息正文的請求必須"Content-Length"在HTTP標題中指定。根據預設，大多數的用戶端新增此標頭。若要避免scroll_id值中的=字元發生問題，請使用要求主體而非查詢字串，將scroll_id值傳遞給 OpenSearch Service。
3. 有關使用指令碼的考量事項，請參閱the section called “其他受支援的資源”。
4. 參考 PUT 方法。如需 GET 方法的詳細資訊，請參閱the section called “顯著的API差異”。此清單僅參考 OpenSearch 服務支援的一般 Elasticsearch 作業，不包含針對異常偵測的外掛程式特定支援作業等ISM。
5. 請參閱 the section called “縮小”。

Elasticsearch 6.4 版

對於彈性搜索 6.4， OpenSearch 服務支持以下操作。

• 索引路徑中的所有操作 (例如 /*index-name* /_forcemerge 和 /*index-name* /update/*id*)，/*index-name* /_close 除外 • /_alias • /_aliases	• /_cluster/state • /_cluster/stats • /_count • /_delete_by_query [1] • /_explain • /_field_caps	• /_refresh • /_reindex [1] • /_render • /_rollover • /_scripts [3] • /_search[2]

- /_all
- /_analyze
- /_bulk
- /_cat (/_cat/nodeattrs 除外)
- /_cluster/allocation/explain
- /_cluster/health
- /_cluster/pending_tasks
- /_cluster/settings 適用於數個屬性[4]：
  - action.auto_create_index
  - action.search.shard_count.limit
  - indices.breaker.fielddata.limit
  - indices.breaker.request.limit
  - indices.breaker.total.limit
- /_field_stats
- /_flush
- /_ingest/pipeline
- /_mapping
- /_mget
- /_msearch
- /_mtermvectors
- /_nodes
- /_opendistro/_alerting
- /_percolate
- /_plugin/kibana
- /_rank_eval
- /_search profile
- /_shard_stores
- /_shrink[5]
- /_snapshot
- /_split
- /_stats
- /_status
- /_tasks
- /_template
- /_update_by_query [1]
- /_validate

1. 叢集組態變更完成之前，這些操作可能中斷。我們建議您隨這些操作一起使用 /_tasks 作業，以確認請求已成功完成。
2. DELETE/_search/scroll使用消息正文的請求必須"Content-Length"在HTTP標題中指定。根據預設，大多數的用戶端新增此標頭。若要避免scroll_id值中的=字元發生問題，請使用要求主體而非查詢字串，將scroll_id值傳遞給 OpenSearch Service。
3. 有關使用指令碼的考量事項，請參閱the section called “其他受支援的資源”。
4. 參考 PUT 方法。如需 GET 方法的詳細資訊，請參閱the section called “顯著的API差異”。此清單僅參考 OpenSearch 服務支援的一般 Elasticsearch 作業，不包含針對異常偵測的外掛程式特定支援作業等ISM。
5. 請參閱 the section called “縮小”。

Elasticsearch 6.3 版

對於彈性搜索 6.3， OpenSearch 服務支持以下操作。

- 索引路徑中的所有操作 (例如 /*index-name* /_forcemerge 和 /*index-name* /update/*id*)，/*index-name* /_close 除外
- /_alias
- /_aliases
- /_all
- /_analyze
- /_bulk
- /_cat (/_cat/nodeattrs 除外)
- /_cluster/allocation/explain
- /_cluster/health
- /_cluster/pending_tasks
- /_cluster/settings 適用於數個屬性[4]：
  - action.auto_create_index
  - action.search.shard_count.limit
  - indices.breaker.fielddata.limit
  - indices.breaker.request.limit
  - indices.breaker.total.limit
- /_cluster/state
- /_cluster/stats
- /_count
- /_delete_by_query [1]
- /_explain
- /_field_caps
- /_field_stats
- /_flush
- /_ingest/pipeline
- /_mapping
- /_mget
- /_msearch
- /_mtermvectors
- /_nodes
- /_opendistro/_alerting
- /_percolate
- /_plugin/kibana
- /_rank_eval
- /_refresh
- /_reindex [1]
- /_render
- /_rollover
- /_scripts [3]
- /_search[2]
- /_search profile
- /_shard_stores
- /_shrink[5]
- /_snapshot
- /_split
- /_stats
- /_status
- /_tasks
- /_template
- /_update_by_query [1]
- /_validate

1. 叢集組態變更完成之前，這些操作可能中斷。我們建議您隨這些操作一起使用 `/_tasks` 作業，以確認請求已成功完成。
2. `DELETE/_search/scroll`使用消息正文的請求必須`"Content-Length"`在HTTP標題中指定。根據預設，大多數的用戶端新增此標頭。若要避免`scroll_id`值中的`=`字元發生問題，請使用要求主體而非查詢字串，將`scroll_id`值傳遞給 OpenSearch Service。
3. 有關使用指令碼的考量事項，請參閱the section called “其他受支援的資源”。
4. 參考 PUT 方法。如需 GET 方法的詳細資訊，請參閱the section called “顯著的API差異”。此清單僅參考 OpenSearch 服務支援的一般 Elasticsearch 作業，不包含針對異常偵測的外掛程式特定支援作業等ISM。
5. 請參閱 the section called “縮小”。

Elasticsearch 6.2 版

對於彈性搜索 6.2， OpenSearch 服務支持以下操作。

- 索引路徑中的所有操作 (例如 `/index-name /_forcemerge` 和 `/index-name /update/id`)，`/index-name /_close` 除外
- `/_alias`
- `/_aliases`
- `/_all`
- `/_analyze`
- `/_bulk`
- `/_cat` (`/_cat/nodeattrs` 除外)
- `/_cluster/allocation/explain`
- `/_cluster/health`
- `/_cluster/pending_tasks`
- `/_cluster/settings` 適用於數個屬性[4]：
- `/_cluster/state`
- `/_cluster/stats`
- `/_count`
- `/_delete_by_query` [1]
- `/_explain`
- `/_field_caps`
- `/_field_stats`
- `/_flush`
- `/_ingest/pipeline`
- `/_mapping`
- `/_mget`
- `/_msearch`
- `/_mtermvectors`
- `/_nodes`
- `/_opendistro/_alerting`
- `/_percolate`
- `/_refresh`
- `/_reindex` [1]
- `/_render`
- `/_rollover`
- `/_scripts` [3]
- `/_search`[2]
- `/_search profile`
- `/_shard_stores`
- `/_shrink`[5]
- `/_snapshot`
- `/_split`
- `/_stats`
- `/_status`
- `/_tasks`
- `/_template`
- `/_update_by_query` [1]
- `/_validate`

• action.auto_create_index • action.search.shard_count.limit • indices.breaker.fielddata.limit • indices.breaker.request.limit • indices.breaker.total.limit	• /_plugin/kibana • /_rank_eval	

1. 叢集組態變更完成之前，這些操作可能中斷。我們建議您隨這些操作一起使用 /_tasks 作業，以確認請求已成功完成。
2. DELETE/_search/scroll使用消息正文的請求必須"Content-Length"在HTTP標題中指定。根據預設，大多數的用戶端新增此標頭。若要避免scroll_id值中的=字元發生問題，請使用要求主體而非查詢字串，將scroll_id值傳遞給 OpenSearch Service。
3. 有關使用指令碼的考量事項，請參閱the section called “其他受支援的資源”。
4. 參考 PUT 方法。如需 GET 方法的詳細資訊，請參閱the section called “顯著的API差異”。此清單僅參考 OpenSearch 服務支援的一般 Elasticsearch 作業，不包含針對異常偵測的外掛程式特定支援作業等ISM。
5. 請參閱 the section called “縮小”。

Elasticsearch 6.0 版

對於彈性搜索 6.0， OpenSearch 服務支持以下操作。

• 索引路徑中的所有操作 (例如 /*index-name* /_forcemerge 和 /*index-name* /update/*id*)，/*index-name* /_close 除外 • /_alias • /_aliases	• /_cluster/state • /_cluster/stats • /_count • /_delete_by_query [1] • /_explain • /_field_caps	• /_render • /_rollover • /_scripts [3] • /_search[2] • /_search profile • /_shard_stores

- /_all
- /_analyze
- /_bulk
- /_cat (/_cat/nodeattrs 除外)
- /_cluster/allocation/explain
- /_cluster/health
- /_cluster/pending_tasks
- /_cluster/settings 適用於數個屬性[4]：
  - action.auto_create_index
  - action.search.shard_count.limit
  - indices.breaker.fielddata.limit
  - indices.breaker.request.limit
  - indices.breaker.total.limit
- /_field_stats
- /_flush
- /_ingest/pipeline
- /_mapping
- /_mget
- /_msearch
- /_mtermvectors
- /_nodes
- /_percolate
- /_plugin/kibana
- /_refresh
- /_reindex [1]
- /_shrink[5]
- /_snapshot
- /_stats
- /_status
- /_tasks
- /_template
- /_update_by_query [1]
- /_validate

1. 叢集組態變更完成之前，這些操作可能中斷。我們建議您隨這些操作一起使用 /_tasks 作業，以確認請求已成功完成。
2. DELETE/_search/scroll使用消息正文的請求必須"Content-Length"在HTTP標題中指定。根據預設，大多數的用戶端新增此標頭。若要避免scroll_id值中的=字元發生問題，請使用要求主體而非查詢字串，將scroll_id值傳遞給 OpenSearch Service。
3. 有關使用指令碼的考量事項，請參閱the section called “其他受支援的資源”。
4. 參考 PUT 方法。如需 GET 方法的詳細資訊，請參閱the section called “顯著的API差異”。此清單僅參考 OpenSearch 服務支援的一般 Elasticsearch 作業，不包含針對異常偵測的外掛程式特定支援作業等ISM。
5. 請參閱 the section called “縮小”。

Elasticsearch 5.6 版

對於彈性搜索 5.6， OpenSearch 服務支持以下操作。

- 索引路徑中的所有操作 (例如 /*index-name* /_forcemerge 和 /*index-name* /update/*id*)，/*index-name* /_close 除外
- /_alias
- /_aliases
- /_all
- /_analyze
- /_bulk
- /_cat (/_cat/nodeattrs 除外)
- /_cluster/allocation/explain
- /_cluster/health
- /_cluster/pending_tasks
- /_cluster/settings 適用於數個屬性[4]：
  - action.auto_create_index
  - action.search.shard_count.limit
  - indices.breaker.fielddata.limit
  - indices.breaker.request.limit
  - indices.breaker.total.limit
- /_cluster/state
- /_cluster/stats
- /_count
- /_delete_by_query [1]
- /_explain
- /_field_caps
- /_field_stats
- /_flush
- /_ingest/pipeline
- /_mapping
- /_mget
- /_msearch
- /_mtermvectors
- /_nodes
- /_percolate
- /_plugin/kibana
- /_refresh
- /_reindex [1]
- /_render
- /_rollover
- /_scripts [3]
- /_search[2]
- /_search profile
- /_shard_stores
- /_shrink[5]
- /_snapshot
- /_stats
- /_status
- /_tasks
- /_template
- /_update_by_query [1]
- /_validate

1. 叢集組態變更完成之前，這些操作可能中斷。我們建議您隨這些操作一起使用 `/_tasks` 作業，以確認請求已成功完成。
2. `DELETE/_search/scroll`使用消息正文的請求必須`"Content-Length"`在HTTP標題中指定。根據預設，大多數的用戶端新增此標頭。若要避免`scroll_id`值中的`=`字元發生問題，請使用要求主體而非查詢字串，將`scroll_id`值傳遞給 OpenSearch Service。
3. 有關使用指令碼的考量事項，請參閱the section called “其他受支援的資源”。
4. 參考 PUT 方法。如需 GET 方法的詳細資訊，請參閱the section called “顯著的API差異”。此清單僅參考 OpenSearch 服務支援的一般 Elasticsearch 作業，不包含針對異常偵測的外掛程式特定支援作業等ISM。
5. 請參閱 the section called “縮小”。

Elasticsearch 5.5 版

對於彈性搜索 5.5， OpenSearch 服務支持以下操作。

- 索引路徑中的所有操作 (例如 `/index-name /_forcemerge` 和 `/index-name /update/id`)，`/index-name /_close` 除外
- `/_alias`
- `/_aliases`
- `/_all`
- `/_analyze`
- `/_bulk`
- `/_cat` (`/_cat/nodeattrs` 除外)
- `/_cluster/allocation/explain`
- `/_cluster/health`
- `/_cluster/pending_tasks`
- `/_cluster/settings` 適用於數個屬性[4]：
- `/_cluster/state`
- `/_cluster/stats`
- `/_count`
- `/_delete_by_query` [1]
- `/_explain`
- `/_field_caps`
- `/_field_stats`
- `/_flush`
- `/_ingest/pipeline`
- `/_mapping`
- `/_mget`
- `/_msearch`
- `/_mtermvectors`
- `/_nodes`
- `/_percolate`
- `/_plugin/kibana`
- `/_refresh`
- `/_render`
- `/_rollover`
- `/_scripts` [3]
- `/_search`[2]
- `/_search profile`
- `/_shard_stores`
- `/_shrink`[5]
- `/_snapshot`
- `/_stats`
- `/_status`
- `/_tasks`
- `/_template`
- `/_update_by_query` [1]
- `/_validate`

• action.auto_create_index • action.search.shard_count.limit • indices.breaker.fielddata.limit • indices.breaker.request.limit • indices.breaker.total.limit	• /_reindex [1]	

1. 叢集組態變更完成之前，這些操作可能中斷。我們建議您隨這些操作一起使用 /_tasks 作業，以確認請求已成功完成。
2. DELETE/_search/scroll使用消息正文的請求必須"Content-Length"在HTTP標題中指定。根據預設，大多數的用戶端新增此標頭。若要避免scroll_id值中的=字元發生問題，請使用要求主體而非查詢字串，將scroll_id值傳遞給 OpenSearch Service。
3. 有關使用指令碼的考量事項，請參閱the section called “其他受支援的資源”。
4. 參考 PUT 方法。如需 GET 方法的詳細資訊，請參閱the section called “顯著的API差異”。此清單僅參考 OpenSearch 服務支援的一般 Elasticsearch 作業，不包含針對異常偵測的外掛程式特定支援作業等ISM。
5. 請參閱 the section called “縮小”。

Elasticsearch 5.3 版

對於彈性搜索 5.3， OpenSearch 服務支持以下操作。

• 索引路徑中的所有操作 (例如 /*index-name* /_forcemerge 和 /*index-name* /update/*id*)，/*index-name* /_close 除外 • /_alias • /_aliases	• /_cluster/state • /_cluster/stats • /_count • /_delete_by_query [1] • /_explain • /_field_caps	• /_render • /_rollover • /_search[2] • /_search profile • /_shard_stores • /_shrink[4]

- /_all
- /_analyze
- /_bulk
- /_cat (/_cat/nodeattrs 除外)
- /_cluster/allocation/explain
- /_cluster/health
- /_cluster/pending_tasks
- /_cluster/settings 適用於數個屬性[3]：
  - action.auto_create_index
  - action.search.shard_count.limit
  - indices.breaker.fielddata.limit
  - indices.breaker.request.limit
  - indices.breaker.total.limit
- /_field_stats
- /_flush
- /_ingest/pipeline
- /_mapping
- /_mget
- /_msearch
- /_mtermvectors
- /_nodes
- /_percolate
- /_plugin/kibana
- /_refresh
- /_reindex [1]
- /_snapshot
- /_stats
- /_status
- /_tasks
- /_template
- /_update_by_query [1]
- /_validate

1. 叢集組態變更完成之前，這些操作可能中斷。我們建議您隨這些操作一起使用 /_tasks 作業，以確認請求已成功完成。
2. DELETE/_search/scroll使用消息正文的請求必須"Content-Length"在HTTP標題中指定。根據預設，大多數的用戶端新增此標頭。若要避免scroll_id值中的=字元發生問題，請使用要求主體而非查詢字串，將scroll_id值傳遞給 OpenSearch Service。
3. 參考 PUT 方法。如需 GET 方法的詳細資訊，請參閱the section called “顯著的API差異”。此清單僅參考 OpenSearch 服務支援的一般 Elasticsearch 作業，不包含針對異常偵測的外掛程式特定支援作業等ISM。
4. 請參閱 the section called “縮小”。

Elasticsearch 5.1 版

對於彈性搜索 5.1， OpenSearch 服務支持以下操作。

- 索引路徑中的所有操作 (例如 /*index-name* /_forcemerge 和 /*index-name* /update/*id*)，/*index-name* /_close 除外
- /_alias
- /_aliases
- /_all
- /_analyze
- /_bulk
- /_cat (/_cat/nodeattrs 除外)
- /_cluster/allocation/explain
- /_cluster/health
- /_cluster/pending_tasks
- /_cluster/settings 對於幾個屬性（PUT僅）：
  - action.auto_create_index
  - action.search.shard_count.limit
  - indices.breaker.fielddata.limit
  - indices.breaker.request.limit
  - indices.breaker.total.limit
- /_cluster/state
- /_cluster/stats
- /_count
- /_delete_by_query [1]
- /_explain
- /_field_caps
- /_field_stats
- /_flush
- /_ingest/pipeline
- /_mapping
- /_mget
- /_msearch
- /_mtermvectors
- /_nodes
- /_percolate
- /_plugin/kibana
- /_refresh
- /_reindex [1]
- /_render
- /_rollover
- /_search[2]
- /_search profile
- /_shard_stores
- /_shrink[3]
- /_snapshot
- /_stats
- /_status
- /_tasks
- /_template
- /_update_by_query [1]
- /_validate

1. 叢集組態變更完成之前，這些操作可能中斷。我們建議您隨這些操作一起使用 `/_tasks` 作業，以確認請求已成功完成。
2. `DELETE/_search/scroll`使用消息正文的請求必須`"Content-Length"`在HTTP標題中指定。根據預設，大多數的用戶端新增此標頭。若要避免`scroll_id`值中的`=`字元發生問題，請使用要求主體而非查詢字串，將`scroll_id`值傳遞給 OpenSearch Service。
3. 請參閱 the section called “縮小”。

Elasticsearch 2.3 版

對於彈性搜索 2.3， OpenSearch 服務支持以下操作。

- 索引路徑中的所有操作 (例如 `/index-name /_forcemerge` 和 `/index-name /_recovery`)，`/index-name /_close` 除外
- `/_alias`
- `/_aliases`
- `/_all`
- `/_analyze`
- `/_bulk`
- `/_cache/clear` (僅適用於索引)
- `/_cat` (`/_cat/nodeattrs` 除外)
- `/_cluster/health`
- `/_cluster/settings` 對於幾個屬性（PUT僅）：
  - `indices.breaker.fielddata.limit`
  - `indices.breaker.request.limit`
  - `indices.breaker.total.limit`
  - `threadpool.get.queue_size`
  - `threadpool.bulk.queue_size`
  - `threadpool.index.queue_size`
- `/_cluster/stats`
- `/_count`
- `/_flush`
- `/_mapping`
- `/_mget`
- `/_msearch`
- `/_nodes`
- `/_percolate`
- `/_plugin/kibana`
- `/_refresh`
- `/_render`
- `/_search`
- `/_snapshot`
- `/_stats`
- `/_status`
- `/_template`

- threadpool.percolate.queue_size
- threadpool.search.queue_size
- threadpool.suggest.queue_size

Elasticsearch 1.5 版

對於彈性搜索 1.5， OpenSearch 服務支持以下操作。

- 索引路徑中的所有操作 (例如 /*index-name* /_optimize 和 /*index-name* /_warmer)，/*index-name* /_close 除外
- /_alias
- /_aliases
- /_all
- /_analyze
- /_bulk
- /_cat
- /_cluster/health
- /_cluster/settings 對於幾個屬性（PUT僅）：
  - indices.breaker.fielddata.limit
  - indices.breaker.request.limit
  - indices.breaker.total.limit
  - threadpool.get.queue_size
  - threadpool.bulk.queue_size
  - threadpool.index.queue_size
  - threadpool.percolate.queue_size
  - threadpool.search.queue_size
- /_cluster/stats
- /_count
- /_flush
- /_mapping
- /_mget
- /_msearch
- /_nodes
- /_percolate
- /_plugin/kibana
- /_plugin/kibana3
- /_plugin/migration
- /_refresh
- /_search
- /_snapshot
- /_stats
- /_status
- /_template

- `threadpool.suggest.queue_size`

Amazon OpenSearch 服務配額

您的 AWS 每個帳號都有預設配額 (先前稱為限制) AWS 服務。除非另有說明，否則每個配額都是區域特定規定。

若要檢視 OpenSearch 服務網域和執行個體、Amazon OpenSearch 無伺 OpenSearch 服器和 Amazon OpenSearch 擷取的配額，請參閱 AWS 一般參考.

若要檢視中的 OpenSearch 服務配額 AWS Management Console」中，開啟「Service Quotas」主控台。在導覽窗格中，選擇 AWS 服務和選擇 Amazon OpenSearch 服務。若要請求提高配額，請參閱《Service Quotas 使用者指南》中的請求提高配額。

主題

- UltraWarm 儲存配額
- EBS磁碟區大小配額
- 網路配額
- 碎片大小配額
- Java 處理序配額
- 網域政策配額

UltraWarm 儲存配額

下表列出 UltraWarm 執行個體類型和每個類型可以使用的最大儲存容量。如需有關的更多資訊 UltraWarm，請參閱the section called “UltraWarm 儲存”。

執行個體類型	最大儲存空間
`ultrawarm1.medium.search`	1.5 TiB
`ultrawarm1.large.search`	20 TiB

EBS磁碟區大小配額

下表顯示 OpenSearch Service 支援之每個執行個體類型的EBS磁碟區大小下限和上限。有關哪些執行個體類型包括執行個體儲存和其他硬體詳細資訊的資訊，請參閱 Amazon OpenSearch 服務定價

- 如果您在建立網域時，在磁EBS碟區類型下選擇磁性儲存，則除了和以及所有 Graviton 執行個體 (M6g、c6g `t2.medium`、R6g `t2.small` 和 R6gD) 以外的所有執行個體類型的磁碟區大小上限為 100 GiB，這些執行個體不支援磁性儲存。對於下表中列出的最大大小，請選擇其中一個選SSD項。
- 部分舊一代執行個體類型包含執行個體儲存體，但也支援EBS儲存空間。如果您為上述其中一種執行個體類型選擇EBS儲存，則儲存磁碟區不會增加。您可以使用EBS磁碟區或執行個體儲存體，不能同時使用兩者。

執行個體類型	最小EBS尺寸	最大EBS尺寸 (gp2)	最大EBS尺寸 (gp3)
`t2.micro.search`	10 GiB	35 GiB	N/A
`t2.small.search`	10 GiB	35 GiB	N/A
`t2.medium.search`	10 GiB	35 GiB	N/A
`t3.small.search`	10 GiB	100 GiB	100 GiB
`t3.medium.search`	10 GiB	200 GiB	200 GiB
`m3.medium.search`	10 GiB	100 GiB	N/A
`m3.large.search`	10 GiB	512 GiB	N/A
`m3.xlarge.search`	10 GiB	512 GiB	N/A
`m3.2xlarge.search`	10 GiB	512 GiB	N/A
`m4.large.search`	10 GiB	512 GiB	N/A
`m4.xlarge.search`	10 GiB	1 TiB	N/A
`m4.2xlarge.search`	10 GiB	1.5 TiB	N/A

執行個體類型	最小EBS尺寸	最大EBS尺寸 (gp2)	最大EBS尺寸 (gp3)
m4.4xlarge.search	10 GiB	1.5 TiB	N/A
m4.10xlarge.search	10 GiB	1.5 TiB	N/A
m5.large.search	10 GiB	512 GiB	1 TiB
m5.xlarge.search	10 GiB	1 TiB	2 TiB
m5.2xlarge.search	10 GiB	1.5 TiB	3 TiB
m5.4xlarge.search	10 GiB	3 TiB	6 TiB
m5.12xlarge.search	10 GiB	9 TiB	18 TiB
m6g.large.search	10 GiB	512 GiB	1 TiB
m6g.xlarge.search	10 GiB	1 TiB	2 TiB
m6g.2xlarge.search	10 GiB	1.5 TiB	3 TiB
m6g.4xlarge.search	10 GiB	3 TiB	6 TiB
m6g.8xlarge.search	10 GiB	6 TiB	12 TiB
m6g.12xlarge.search	10 GiB	9 TiB	18 TiB
c4.large.search	10 GiB	100 GiB	N/A
c4.xlarge.search	10 GiB	512 GiB	N/A
c4.2xlarge.search	10 GiB	1 TiB	N/A
c4.4xlarge.search	10 GiB	1.5 TiB	N/A
c4.8xlarge.search	10 GiB	1.5 TiB	N/A
c5.large.search	10 GiB	256 GiB	256 GiB
c5.xlarge.search	10 GiB	512 GiB	512 GiB

執行個體類型	最小EBS尺寸	最大EBS尺寸 (gp2)	最大EBS尺寸 (gp3)
`c5.2xlarge.search`	10 GiB	1 TiB	1 TiB
`c5.4xlarge.search`	10 GiB	1.5 TiB	1.5 TiB
`c5.9xlarge.search`	10 GiB	3.5 TiB	3.5 TiB
`c5.18xlarge.search`	10 GiB	7 TiB	7 TiB
`c6g.large.search`	10 GiB	256 GiB	256 GiB
`c6g.xlarge.search`	10 GiB	512 GiB	512 GiB
`c6g.2xlarge.search`	10 GiB	1 TiB	1 TiB
`c6g.4xlarge.search`	10 GiB	1.5 TiB	1.5 TiB
`c6g.8xlarge.search`	10 GiB	3 TiB	3 TiB
`c6g.12xlarge.search`	10 GiB	4.5 TiB	4.5 TiB
`r3.large.search`	10 GiB	512 GiB	N/A
`r3.xlarge.search`	10 GiB	512 GiB	N/A
`r3.2xlarge.search`	10 GiB	512 GiB	N/A
`r3.4xlarge.search`	10 GiB	512 GiB	N/A
`r3.8xlarge.search`	10 GiB	512 GiB	N/A
`r4.large.search`	10 GiB	1 TiB	N/A
`r4.xlarge.search`	10 GiB	1.5 TiB	N/A
`r4.2xlarge.search`	10 GiB	1.5 TiB	N/A
`r4.4xlarge.search`	10 GiB	1.5 TiB	N/A
`r4.8xlarge.search`	10 GiB	1.5 TiB	N/A

執行個體類型	最小EBS尺寸	最大EBS尺寸 (gp2)	最大EBS尺寸 (gp3)
r4.16xlarge.search	10 GiB	1.5 TiB	N/A
r5.large.search	10 GiB	1 TiB	2 TiB
r5.xlarge.search	10 GiB	1.5 TiB	3 TiB
r5.2xlarge.search	10 GiB	3 TiB	6 TiB
r5.4xlarge.search	10 GiB	6 TiB	12 TiB
r5.12xlarge.search	10 GiB	12 TiB	24 TiB
r6g.large.search	10 GiB	1 TiB	2 TiB
r6g.xlarge.search	10 GiB	1.5 TiB	3 TiB
r6g.2xlarge.search	10 GiB	3 TiB	6 TiB
r6g.4xlarge.search	10 GiB	6 TiB	12 TiB
r6g.8xlarge.search	10 GiB	8 TiB	16 TiB
r6g.12xlarge.search	10 GiB	12 TiB	24 TiB
r6gd.large.search	N/A	N/A	N/A
r6gd.xlarge.search	N/A	N/A	N/A
r6gd.2xlarge.search	N/A	N/A	N/A
r6gd.4xlarge.search	N/A	N/A	N/A
r6gd.8xlarge.search	N/A	N/A	N/A
r6gd.12xlarge.search	N/A	N/A	N/A
r6gd.16xlarge.search	N/A	N/A	N/A
i2.xlarge.search	10 GiB	512 GiB	N/A

執行個體類型	最小EBS尺寸	最大EBS尺寸 (gp2)	最大EBS尺寸 (gp3)
i2.2xlarge.search	10 GiB	512 GiB	N/A
i3.large.search	N/A	N/A	N/A
i3.xlarge.search	N/A	N/A	N/A
i3.2xlarge.search	N/A	N/A	N/A
i3.4xlarge.search	N/A	N/A	N/A
i3.8xlarge.search	N/A	N/A	N/A
i3.16xlarge.search	N/A	N/A	N/A
or1.medium.search	20 GiB	N/A	768 GiB
or1.large.search	20 GiB	N/A	1532 GiB
or1.xlarge.search	20 GiB	N/A	3 TiB
or1.2xlarge.search	20 GiB	N/A	6 TiB
or1.4xlarge.search	20 GiB	N/A	12 TiB
or1.8xlarge.search	20 GiB	N/A	16 TiB
or1.12xlarge.search	20 GiB	N/A	24 TiB
or1.16xlarge.search	20 GiB	N/A	36 TiB
im4gn.large.search	N/A	N/A	N/A
im4gn.xlarge.search	N/A	N/A	N/A
im4gn.2xlarge.search	N/A	N/A	N/A
im4gn.4xlarge.search	N/A	N/A	N/A
im4gn.8xlarge.search	N/A	N/A	N/A

執行個體類型	最小EBS尺寸	最大EBS尺寸 (gp2)	最大EBS尺寸 (gp3)
`im4gn.16xlarge.search`	N/A	N/A	N/A
大	10 GiB	N/A	256 GiB
C7 克。大	10 GiB	N/A	512 GiB
C7 克。大	10 GiB	N/A	1 TiB
C7 克. 大	10 GiB	N/A	1.5 TiB
C7 克。8 倍大	10 GiB	N/A	3 TiB
C. 12 倍大	10 GiB	N/A	4.5 TiB
大号	10 GiB	N/A	6 TiB
兆 7 克。大	10 GiB	N/A	768 GiB
兆 8 克。大	10 GiB	N/A	2 TiB
M7 克。2 倍大	10 GiB	N/A	3 TiB
兆 7 克。4 倍大	10 GiB	N/A	6 TiB
M7 公克 8 倍大	10 GiB	N/A	12 TiB
M7 公克。12 倍大	10 GiB	N/A	18 TiB
毫升 .16 克大	10 GiB	N/A	24 TiB
中等	10 GiB	N/A	768 GiB
R7 克。大	10 GiB	N/A	1.5 TiB
大尺寸	10 GiB	N/A	3 TiB
大号	10 GiB	N/A	6 TiB

執行個體類型	最小EBS尺寸	最大EBS尺寸 (gp2)	最大EBS尺寸 (gp3)
7 克. 大	10 GiB	N/A	12 TiB
8 克大	10 GiB	N/A	16 TiB
7 克. 大	10 GiB	N/A	24 TiB
大号	10 GiB	N/A	36 TiB
R7 公升。大	N/A	N/A	N/A
大尺寸	N/A	N/A	N/A
大型 7 公克	N/A	N/A	N/A
L. 4 倍大	N/A	N/A	N/A
大型 8 公升	N/A	N/A	N/A
L. 12 倍大	N/A	N/A	N/A
大型	N/A	N/A	N/A
i4i.large	10 GiB	N/A	N/A
i4i.xlarge	10 GiB	N/A	N/A
i4i.2xlarge	10 GiB	N/A	N/A
i4i.4xlarge	10 GiB	N/A	N/A
i4i.8xlarge	10 GiB	N/A	N/A
i4i.12xlarge	10 GiB	N/A	N/A
i4i.16xlarge	10 GiB	N/A	N/A
i4i.24xlarge	10 GiB	N/A	N/A
i4i.32xlarge	10 GiB	N/A	N/A

執行個體類型	最小EBS尺寸	最大EBS尺寸 (gp2)	最大EBS尺寸 (gp3)
i4g.large	10 GiB	N/A	N/A
i4g.xlarge	10 GiB	N/A	N/A
i4g.2xlarge	10 GiB	N/A	N/A
i4g.4xlarge	10 GiB	N/A	N/A
i4g.8xlarge	10 GiB	N/A	N/A
i4g.16xlarge	10 GiB	N/A	N/A

網路配額

下表顯示HTTP請求有效載荷的最大大小。

執行個體類型	HTTP請求有效載荷的最大大小
`t2.micro.search`	10 MiB
`t2.small.search`	10 MiB
`t2.medium.search`	10 MiB
`t3.small.search`	10 MiB
`t3.medium.search`	10 MiB
`m3.medium.search`	10 MiB
`m3.large.search`	10 MiB
`m3.xlarge.search`	100 MiB
`m3.2xlarge.search`	100 MiB
`m4.large.search`	10 MiB

執行個體類型	HTTP請求有效載荷的最大大小
m4.xlarge.search	100 MiB
m4.2xlarge.search	100 MiB
m4.4xlarge.search	100 MiB
m4.10xlarge.search	100 MiB
m5.large.search	10 MiB
m5.xlarge.search	100 MiB
m5.2xlarge.search	100 MiB
m5.4xlarge.search	100 MiB
m5.12xlarge.search	100 MiB
m6g.large.search	10 MiB
m6g.xlarge.search	100 MiB
m6g.2xlarge.search	100 MiB
m6g.4xlarge.search	100 MiB
m6g.8xlarge.search	100 MiB
m6g.12xlarge.search	100 MiB
c4.large.search	10 MiB
c4.xlarge.search	100 MiB

執行個體類型	HTTP請求有效載荷的最大大小
c4.2xlarge.search	100 MiB
c4.4xlarge.search	100 MiB
c4.8xlarge.search	100 MiB
c5.large.search	10 MiB
c5.xlarge.search	100 MiB
c5.2xlarge.search	100 MiB
c5.4xlarge.search	100 MiB
c5.9xlarge.search	100 MiB
c5.18xlarge.search	100 MiB
c6g.large.search	10 MiB
c6g.xlarge.search	100 MiB
c6g.2xlarge.search	100 MiB
c6g.4xlarge.search	100 MiB
c6g.8xlarge.search	100 MiB
c6g.12xlarge.search	100 MiB
r3.large.search	10 MiB
r3.xlarge.search	100 MiB

執行個體類型	HTTP請求有效載荷的最大大小
r3.2xlarge.search	100 MiB
r3.4xlarge.search	100 MiB
r3.8xlarge.search	100 MiB
r4.large.search	100 MiB
r4.xlarge.search	100 MiB
r4.2xlarge.search	100 MiB
r4.4xlarge.search	100 MiB
r4.8xlarge.search	100 MiB
r4.16xlarge.search	100 MiB
r5.large.search	100 MiB
r5.xlarge.search	100 MiB
r5.2xlarge.search	100 MiB
r5.4xlarge.search	100 MiB
r5.12xlarge.search	100 MiB
r6g.large.search	100 MiB
r6g.xlarge.search	100 MiB
r6g.2xlarge.search	100 MiB
r6g.4xlarge.search	100 MiB

執行個體類型	HTTP請求有效載荷的最大大小
r6g.8xlarge.search	100 MiB
r6g.12xlarge.search	100 MiB
r6gd.large.search	100 MiB
r6gd.xlarge.search	100 MiB
r6gd.2xlarge.search	100 MiB
r6gd.4xlarge.search	100 MiB
r6gd.8xlarge.search	100 MiB
r6gd.12xlarge.search	100 MiB
r6gd.16xlarge.search	100 MiB
i2.xlarge.search	100 MiB
i2.2xlarge.search	100 MiB
i3.large.search	100 MiB
i3.xlarge.search	100 MiB
i3.2xlarge.search	100 MiB
i3.4xlarge.search	100 MiB

執行個體類型	HTTP請求有效載荷的最大大小
i3.8xlarge.search	100 MiB
i3.16xlarge.search	100 MiB
or1.medium.search	10 MiB
or1.large.search	100 MiB
or1.xlarge.search	100 MiB
or1.2xlarge.search	100 MiB
or1.4xlarge.search	100 MiB
or1.8xlarge.search	100 MiB
or1.12xlarge.search	100 MiB
or1.16xlarge.search	100 MiB
im4gn.large.search	100 MiB
im4gn.xlarge.search	100 MiB
im4gn.2xlarge.search	100 MiB
im4gn.4xlarge.search	100 MiB

執行個體類型	HTTP請求有效載荷的最大大小
im4gn.8xlarge.search	100 MiB
im4gn.16xlarge.search	100 MiB
i4i.large	100 MiB
i4i.xlarge	100 MiB
i4i.2xlarge	100 MiB
i4i.4xlarge	100 MiB
i4i.8xlarge	100 MiB
i4i.12xlarge	100 MiB
i4i.16xlarge	100 MiB
i4i.24xlarge	100 MiB
i4i.32xlarge	100 MiB
i4g.large	100 MiB
i4g.xlarge	100 MiB
i4g.2xlarge	100 MiB
i4g.4xlarge	100 MiB
i4g.8xlarge	100 MiB
i4g.16xlarge	100 MiB

碎片大小配額

以下部分列示了各種例證族群的最大碎片大小。

執行個體類型	異地同步備份 (不含	異地同步備份含待機
R5, C5, 平方米	N/A	65 GiB
I3	N/A	65 GiB
R6 克, 六克, M6 克, R6gD	N/A	65 GiB
OR1	100 GiB	65 GiB
Im4gn	N/A	65 GiB

若要申請提高配額，請聯絡 AWS Support 。

Java 處理序配額

OpenSearch 服務將 Java 進程限制為 32 GiB 的堆積大小。進階使用者可以指定用於 field data 之堆積的百分比。如需詳細資訊，請參閱 the section called “進階叢集設定” 和 the section called “JVM OutOfMemoryError”。

網域政策配額

OpenSearch 服務將網域上的存取原則限制為 100 KiB。

Amazon OpenSearch Service 中的預留執行個體

相較於標準隨需執行個體，Amazon OpenSearch Service 中的預留執行個體 (RI) 提供大幅折扣。執行個體本身均相同；RI 是套用到您的帳戶中隨需執行個體的一種計費折扣。對於可預測使用量的長效應用程式，RI 可隨時間的累積產生可觀的節省成果。

OpenSearch Service RI 需要一年或三年期預留執行個體，並且提供三種對折扣費率有相當影響的付款選項：

- 不預付 - 無須任何預付款。在期限內，按折扣後的每小時費率支付每個小時的費用。
- 部分預付 - 您需要預付部分費用，並且在期限內，按折扣後的每小時費率支付每個小時的費用。
- 全部預付 - 您支付整個預付款的費用。您不是按照小時費率支付費用。

一般來說，較大的預付款表示較大的折扣。您無法取消預留執行個體 - 當您預留時，表示您承諾支付整個期限 - 且預付款項不可退還。

RI 並不靈活；它們只適用於您保留的確切執行個體類型。例如，八個 `c5.2xlarge.search` 執行個體保留不適用於十六個 `c5.xlarge.search` 執行個體或四個 `c5.4xlarge.search` 執行個體。如需完整詳細資訊，請參閱 Amazon OpenSearch Service 定價和常見問答集。

主題

- 購買預留執行個體 (主控台)
- 購買預留執行個體 (AWS CLI)
- 購買預留執行個體 (AWS 開發套件)
- 檢查成本

購買預留執行個體 (主控台)

主控台可讓您檢視現有的預留執行個體和購買新的執行個體。

購買預訂

1. 前往 https://aws.amazon.com，然後選擇 Sign In to the Console (登入主控台)。
2. 在 Analytics (分析) 下，選擇 Amazon OpenSearch Service。
3. 在導覽窗格中，選擇 Reserved Instance Leases (預留執行個體租用)。

   在此頁面上，您可以檢視現有的預訂。如果您有許多預訂，您可以篩選以更輕鬆地識別和檢視特定預訂。

   > **Tip**
   > 若您沒有看到 Reserved Instance Leases (預留執行個體租用) 連結，請在 AWS 區域中建立網域。

4. 選擇 Order Reserved Instance (預訂預留執行個體)。
5. 提供唯一且描述性名稱。
6. 選擇執行個體類型和執行個體數量。如需準則，請參閱the section called “調整網域大小”。
7. 選擇期限長度和付款選項。仔細檢閱付款詳細資訊。
8. 選擇 Next (下一步)。

9. 仔細檢閱購買摘要。購買預留執行個體無法退款。
10. 選擇 Order (預訂)。

購買預留執行個體 (AWS CLI)

AWS CLI 具有檢視產品、購買預訂及檢視預訂的命令。以下命令和範例回應顯示某個指定 AWS 區域的產品：

```
aws opensearch describe-reserved-instance-offerings --region us-east-1
{
  "ReservedInstanceOfferings": [
    {
      "FixedPrice": x,
      "ReservedInstanceOfferingId": "1a2a3a4a5-1a2a-3a4a-5a6a-1a2a3a4a5a6a",
      "RecurringCharges": [
        {
          "RecurringChargeAmount": y,
          "RecurringChargeFrequency": "Hourly"
        }
      ],
      "UsagePrice": 0.0,
      "PaymentOption": "PARTIAL_UPFRONT",
      "Duration": 31536000,
      "InstanceType": "m4.2xlarge.search",
      "CurrencyCode": "USD"
    }
  ]
}
```

如需每個傳回值的詳細說明，請參閱下表。

欄位	描述
FixedPrice	預訂的預付費用。
ReservedInstanceOfferingId	方案 ID。如果您想要預訂產品，請備註此值。
RecurringCharges	預訂的小時費率。

欄位	描述
UsagePrice	傳統欄位。對於 OpenSearch Service，此值始終為 0。
PaymentOption	無預付、部分預付或全部預付。
Duration	期限長度，以秒為單位： • 31536000 秒是一年。 • 94608000 秒是三年。
InstanceType	預訂的執行個體類型。如需分配給每個執行個體類型的硬體資源的資訊，請參閱 Amazon OpenSearch Service 定價。
CurrencyCode	用於 FixedPrice 和 RecurringChargeAmount 的貨幣。

這個下一個範例購買預訂：

```
aws opensearch purchase-reserved-instance-offering --reserved-instance-offering-
id 1a2a3a4a5-1a2a-3a4a-5a6a-1a2a3a4a5a6a --reservation-name my-reservation --instance-
count 3 --region us-east-1
{
  "ReservationName": "my-reservation",
  "ReservedInstanceId": "9a8a7a6a-5a4a-3a2a-1a0a-9a8a7a6a5a4a"
}
```

最後，您可以使用下列範例，列出指定區域的預訂：

```
aws opensearch describe-reserved-instances --region us-east-1
{
  "ReservedInstances": [
    {
      "FixedPrice": x,
      "ReservedInstanceOfferingId": "1a2a3a4a5-1a2a-3a4a-5a6a-1a2a3a4a5a6a",
      "ReservationName": "my-reservation",
      "PaymentOption": "PARTIAL_UPFRONT",
      "UsagePrice": 0.0,
```

```
      "ReservedInstanceId": "9a8a7a6a-5a4a-3a2a-1a0a-9a8a7a6a5a4a",
      "RecurringCharges": [
        {
          "RecurringChargeAmount": y,
          "RecurringChargeFrequency": "Hourly"
        }
      ],
      "State": "payment-pending",
      "StartTime": 1522872571.229,
      "InstanceCount": 3,
      "Duration": 31536000,
      "InstanceType": "m4.2xlarge.search",
      "CurrencyCode": "USD"
    }
  ]
}
```

> **Note**
>
> `StartTime` 是 Unix epoch 時間，以秒數計算，從 1970 年 1 月 1 日 UTC 午夜起已經過的秒數。例如，1522872571 epoch 時間是 2018 年 4 月 4 日 20:09:31 UTC。您可以使用線上轉換器。

若要進一步了解前述範例中使用的命令，請參閱 AWS CLI 命令參考。

購買預留執行個體 (AWS 開發套件)

AWS SDK (Android 和 iOS SDK 除外) 支援 Amazon OpenSearch Service API 參考中定義的所有操作，包括下列操作：

- `DescribeReservedInstanceOfferings`
- `PurchaseReservedInstanceOffering`
- `DescribeReservedInstances`

此範例指令碼使用來自 AWS SDK for Python (Boto3) 的 OpenSearchService 低階 Python 用戶端來購買預留執行個體。您必須提供 `instance_type` 的值。

```
import boto3
from botocore.config import Config
```

```
# Build the client using the default credential configuration.
# You can use the CLI and run 'aws configure' to set access key, secret
# key, and default region.

my_config = Config(
    # Optionally lets you specify a region other than your default.
    region_name='us-east-1'
)

client = boto3.client('opensearch', config=my_config)

instance_type = '' # e.g. m4.2xlarge.search


def describe_RI_offerings(client):
    """Gets the Reserved Instance offerings for this account"""

    response = client.describe_reserved_instance_offerings()
    offerings = (response['ReservedInstanceOfferings'])
    return offerings


def check_instance(offering):
    """Returns True if instance type is the one you specified above"""

    if offering['InstanceType'] == instance_type:
        return True

    return False


def get_instance_id():
    """Iterates through the available offerings to find the ID of the one you
 specified"""

    instance_type_iterator = filter(
        check_instance, describe_RI_offerings(client))
    offering = list(instance_type_iterator)
    id = offering[0]['ReservedInstanceOfferingId']
    return id


def purchase_RI_offering(client):
```

```
    """Purchase Reserved Instances"""

    response = client.purchase_reserved_instance_offering(
        ReservedInstanceOfferingId = get_instance_id(),
        ReservationName = 'my-reservation',
        InstanceCount = 1
    )
    print('Purchased reserved instance offering of type ' + instance_type)
    print(response)


def main():
    """Purchase Reserved Instances"""
    purchase_RI_offering(client)
```

如需安裝與使用 AWS 開發套件的詳細資訊，請參閱 AWS 軟體開發套件。

檢查成本

Cost Explorer 是一個免費的工具，可讓您用於檢視過去 13 個月的支出費用資料。分析這項資料可協助您識別趨勢，並了解 RI 是否符合您的使用案例。如果您已經有 RI，可以透過https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/groupdata.html購買選項和顯示分攤成本分類，進而針對隨需執行個體比較該項支出和您的支出。您也可以設定用量預算，確保充分利用您的預留額度。如需詳細資訊，請參閱 AWS Billing 使用者指南中的使用 Cost Explorer 分析您的成本。

Amazon OpenSearch 服務中的其他支持資源

本主題說明 Amazon OpenSearch 服務支援的其他資源。

bootstrap.memory_lock

OpenSearch 服務會`bootstrap.memory_lock`在中啟用`opensearch.yml`，這會鎖定JVM記憶體，並防止作業系統將其交換至磁碟。這適用於所有支援的執行個體類型，但下列項目除外：

- `t2.micro.search`
- `t2.small.search`
- `t2.medium.search`
- `t3.small.search`
- `t3.medium.search`

指令碼模組

OpenSearch 服務支持腳本彈性搜索 5. x 及更新版本的網域。它不支援 1.5 或 2.3 的指令碼。

支援的指令碼選項包括下列項目：

- Painless
- Lucene 表達式
- Mustache

對於 Elasticsearch 5.5 及更新版本的網域，以及所有 OpenSearch 網域， OpenSearch 服務支援使用端點儲存的`_scripts`指令碼。Elasticsearch 5.3 和 5.1 網域僅支援內嵌指令碼。

TLS運輸

OpenSearch 服務支援連接埠 80 和連HTTPS接埠 443 以HTTP上，但不支援TLS傳輸。

Amazon OpenSearch Service 教學課程

本章包含幾個從開始到結束的教學課程，以便使用 Amazon OpenSearch Service，這包括如何遷移到服務、建置簡單的搜尋應用程式以及在 OpenSearch Dashboards 中建立視覺效果。

主題

- 教程：在亞馬遜 OpenSearch 服務中創建和搜索文檔
- 教學課程：遷移到亞馬遜OpenSearch服務
- 教學：使用 Amazon OpenSearch 服務建立搜尋應用程式
- 教學課程：使用 OpenSearch Service 和 OpenSearch Dash，將客戶支援呼叫視覺化

教程：在亞馬遜 OpenSearch 服務中創建和搜索文檔

在本教學中，您將學習如何在 Amazon OpenSearch 服務中建立和搜尋文件。您可以以 JSON 文件的形式將資料新增至索引。 OpenSearch 服務會圍繞您新增的第一個文件建立索引。

本教學課程說明如何發出 HTTP 請求以建立文件、自動產生文件 ID，以及如何對文件執行基本搜尋和進階搜尋。

> **Note**
>
> 本教程課程使用具有開放存取權的網域。為了實現最高等級的安全性，我們建議您將網域放入虛擬私有雲端 (VPC) 內。

先決條件

本教學課程具備下列先決條件：

- 您必須具有 AWS 帳戶。
- 您必須擁有作用中的 OpenSearch 服務網域。

將文件新增至索引

若要將文件新增至索引，您可以使用任何 HTTP 工具，例如郵遞員、cURL 或 OpenSearch 儀表板主控台。這些範例假設您正在使用 OpenSearch 儀表板中的開發人員主控台。如果您使用其他工具，請視需要提供完整的 URL 和憑證進行相應調整。

若要將文件新增至索引

1. 導覽至您網域的 OpenSearch 儀表板 URL。您可以在 OpenSearch 服務主控台的網域儀表板上找到 URL。URL 遵循以下格式：

   ```
   domain-endpoint/_dashboards/
   ```

2. 使用您的主要使用者名稱和密碼登入。
3. 開啟左側導覽面板並選擇 Dev Tools (開發工具)。
4. 用於建立新資源的 HTTP 動詞為 PUT，可使用它來建立新文件和索引。在主控台中，輸入以下命令：

   ```
   PUT fruit/_doc/1
   {
     "name":"strawberry",
     "color":"red"
   }
   ```

   PUT 請求會建立一個名為 fruit 的索引，並將 ID 為 1 的單一文件新增至該索引。它產生如下回應：

   ```
   {
     "_index" : "fruit",
     "_type" : "_doc",
     "_id" : "1",
     "_version" : 1,
     "result" : "created",
     "_shards" : {
       "total" : 2,
       "successful" : 2,
       "failed" : 0
     },
     "_seq_no" : 0,
     "_primary_term" : 1
   }
   ```

建立自動產生的 ID

OpenSearch 服務可以自動為您的文檔生成 ID。產生 ID 的命令使用 POST 請求而非 PUT 請求，並且不需要文件 ID (與之前的請求相比)。

在開發人員主控台中輸入以下請求：

```
POST veggies/_doc
{
  "name":"beet",
  "color":"red",
  "classification":"root"
}
```

此請求會建立一個名為 veggies 的索引並將文件新增至索引。它產生如下回應：

```
{
  "_index" : "veggies",
  "_type" : "_doc",
  "_id" : "3WgyS4IB5DLqbRIvLxtF",
  "_version" : 1,
  "result" : "created",
  "_shards" : {
    "total" : 2,
    "successful" : 2,
    "failed" : 0
  },
  "_seq_no" : 0,
  "_primary_term" : 1
}
```

請注意回應中的額外 `_id` 欄位，它指示已自動建立 ID。

> **Note**
>
> 您在 URL 的 `_doc` 後面沒有提供任何內容，ID 通常會出現在該位置。因為您要使用產生的 ID 建立文件，所以尚未提供 ID。這預留用於更新。

使用 POST 命令更新文件

若要更新文件，請使用帶有 ID 號的 HTTP POST 命令。

首先，建立 ID 為 42 的文件：

```
POST fruits/_doc/42
{
  "name":"banana",
  "color":"yellow"
}
```

然後使用該 ID 更新文件：

```
POST fruits/_doc/42
{
  "name":"banana",
  "color":"yellow",
  "classification":"berries"
}
```

此命令使用新欄位 `classification` 更新文件。它產生如下回應：

```
{
  "_index" : "fruits",
  "_type" : "_doc",
  "_id" : "42",
  "_version" : 2,
  "result" : "updated",
  "_shards" : {
    "total" : 2,
    "successful" : 2,
    "failed" : 0
  },
  "_seq_no" : 1,
  "_primary_term" : 1
}
```

> **Note**
>
> 如果您嘗試更新不存在的文件， OpenSearch Service 會建立文件。

執行大量動作

您可以使用 POST _bulk API 操作對一個請求中的一個或多個索引執行多個動作。大量動作命令採用下列格式：

```
POST /_bulk
<action_meta>\n
<action_data>\n
<action_meta>\n
<action_data>\n
```

每個動作需要兩行 JSON。首先，您要提供動作說明或中繼資料。在下一行中提供該資料。每部分由換行符號 (\n) 分隔。插入的動作描述可能如下所示：

```
{ "create" : { "_index" : "veggies", "_type" : "_doc", "_id" : "7" } }
```

包含資料的下一行可能如下所示：

```
{ "name":"kale", "color":"green", "classification":"leafy-green" }
```

中繼資料和資料結合在一起，表示大量操作中的單一動作。您可以在一個請求中執行許多操作，如下所示：

```
POST /_bulk
{ "create" : { "_index" : "veggies", "_id" : "35" } }
{ "name":"kale", "color":"green", "classification":"leafy-green" }
{ "create" : { "_index" : "veggies", "_id" : "36" } }
{ "name":"spinach", "color":"green", "classification":"leafy-green" }
{ "create" : { "_index" : "veggies", "_id" : "37" } }
{ "name":"arugula", "color":"green", "classification":"leafy-green" }
{ "create" : { "_index" : "veggies", "_id" : "38" } }
{ "name":"endive", "color":"green", "classification":"leafy-green" }
{ "create" : { "_index" : "veggies", "_id" : "39" } }
{ "name":"lettuce", "color":"green", "classification":"leafy-green" }
{ "delete" : { "_index" : "vegetables", "_id" : "1" } }
```

請注意，最後一個動作是 delete。delete 動作之後沒有資料。

搜尋文件

現在您的叢集中存在資料，您可以搜尋它。例如，您可能想要搜尋所有根莖類蔬菜，或取得所有綠葉蔬菜的計數，或者尋找每小時記錄的錯誤數量。

基本搜尋

基本搜尋如下所示：

```
GET veggies/_search?q=name:l*
```

該請求會產生一個包含萵苣文件的 JSON 回應。

進階搜尋

您可以在請求主體中以 JSON 格式提供查詢選項，以執行更進階的搜尋：

```
GET veggies/_search
{
  "query": {
    "term": {
      "name": "lettuce"
    }
  }
}
```

此範例還會產生一個帶有萵苣文件的 JSON 回應。

排序

您可以使用排序功能來執行更多此類查詢。首先，您需要重新建立索引，因為自動欄位映射選擇了預設情況下無法排序的類型。傳送下列請求，以刪除並重新建立索引：

```
DELETE /veggies

PUT /veggies
{
   "mappings":{
      "properties":{
         "name":{
```

```
            "type":"keyword"
         },
         "color":{
            "type":"keyword"
         },
         "classification":{
            "type":"keyword"
         }
      }
   }
}
```

然後用資料重新填入索引：

```
POST /_bulk
{ "create" : { "_index" : "veggies", "_id" : "7"  } }
{ "name":"kale", "color":"green", "classification":"leafy-green" }
{ "create" : { "_index" : "veggies", "_id" : "8" } }
{ "name":"spinach", "color":"green", "classification":"leafy-green" }
{ "create" : { "_index" : "veggies", "_id" : "9" } }
{ "name":"arugula", "color":"green", "classification":"leafy-green" }
{ "create" : { "_index" : "veggies", "_id" : "10" } }
{ "name":"endive", "color":"green", "classification":"leafy-green" }
{ "create" : { "_index" : "veggies", "_id" : "11" } }
{ "name":"lettuce", "color":"green", "classification":"leafy-green" }
```

現在，您可以使用排序進行搜尋。此請求會按照分類新增遞增排序：

```
GET veggies/_search
{
  "query" : {
    "term": { "color": "green" }
  },
  "sort" : [
      "classification"
  ]
}
```

相關資源

如需詳細資訊，請參閱下列資源：

- 開始使用
- 建立資料索引
- 搜尋資料

教學課程：遷移到亞馬遜OpenSearch服務

索引快照是從自我管理移轉的熱門方式OpenSearch或傳統彈性搜索集群到亞馬遜OpenSearch服務。此程序大致包含下列步驟：

1. 建立現有叢集的快照，然後將快照上傳至 Amazon S3 儲存貯體。
2. 創建一個OpenSearch服務網域。
3. 給OpenSearch存取值區的服務權限，並確保您擁有使用快照的權限。
4. 還原上的快照OpenSearch服務網域。

此演練提供更詳細的步驟和替代選項 (如適用)。

建立並上傳快照

雖然您可以使用 repository-s3 外掛程式直接將快照建立在 S3 上，但是您必須在每個節點上安裝外掛程式，如果使用 Elasticsearch 叢集，應調整 `opensearch.yml` (或 `elasticsearch.yml`)，重新啟動每個節點，新增 AWS 憑證，最後才能建立快照。外掛程式是適合持續使用或遷移較大型叢集的絕佳選擇。

若是較小的叢集，可以採用一次性的方法，先建立共用檔案系統快照，然後使用 AWS CLI 將其上傳到 S3。如果您已經有快照，請跳至步驟 4。

若要建立快照並上傳至 Amazon S3

1. 將 `path.repo` 設定新增至所有節點上的 `opensearch.yml` (或 `Elasticsearch.yml`)，然後重新啟動每個節點。

   ```
   path.repo: ["/my/shared/directory/snapshots"]
   ```

2. 註冊快照儲存庫，此為建立快照前所需。儲存庫只是一個儲存位置：共用檔案系統、Amazon S3、Hadoop 分散式檔案系統 (HDFS) 等。在此情況下，我們將使用共用檔案系統 ("fs")：

   ```
   PUT _snapshot/my-snapshot-repo-name
   ```

```
{
  "type": "fs",
  "settings": {
    "location": "/my/shared/directory/snapshots"
  }
}
```

3. 建立快照：

```
PUT _snapshot/my-snapshot-repo-name/my-snapshot-name
{
  "indices": "migration-index1,migration-index2,other-indices-*",
  "include_global_state": false
}
```

4. 安裝 AWS CLI，然後執行 `aws configure` 以新增您的登入資料。
5. 瀏覽至快照目錄。然後執行下列命令以建立新的 S3 儲存貯體，並將快照目錄的內容上傳至該儲存貯體：

```
aws s3 mb s3://bucket-name --region us-west-2
aws s3 sync . s3://bucket-name --sse AES256
```

視快照大小和網際網路連線速度而定，此操作可能需要一段時間。

建立網域

雖然主控台是建立網域最簡單的方法，但在這種情況下，您已經開啟終端機而且已安裝 AWS CLI。修改下列命令即可建立符合您需求的網域：

```
aws opensearch create-domain \
  --domain-name migration-domain \
  --engine-version OpenSearch_1.0 \
  --cluster-config InstanceType=c5.large.search,InstanceCount=2 \
  --ebs-options EBSEnabled=true,VolumeType=gp2,VolumeSize=100 \
  --node-to-node-encryption-options Enabled=true \
  --encryption-at-rest-options Enabled=true \
  --domain-endpoint-options EnforceHTTPS=true,TLSSecurityPolicy=Policy-Min-
TLS-1-2-2019-07 \
  --advanced-security-options
 Enabled=true,InternalUserDatabaseEnabled=true,MasterUserOptions='{MasterUserName=master-
user,MasterUserPassword=master-user-password}' \
```

```
  --access-policies '{"Version":"2012-10-17","Statement":
[{"Effect":"Allow","Principal":{"AWS":["*"]},"Action":
["es:ESHttp*"],"Resource":"arn:aws:es:us-west-2:123456789012:domain/migration-domain/
*"}]}' \
  --region us-west-2
```

若未經修改，此命令會建立具有兩個資料節點的網際網路存取網域，每個節點都有 100 GiB 的儲存空間。它也會啟用具有 HTTP 基本身分驗證和所有加密設定的精細存取控制。使用OpenSearch服務主控台 (如果您需要更進階的安全性設定，例如 VPC)。

發出命令之前，請先變更網域名稱、主要使用者登入資料和帳戶號碼。指定相同AWS 區域您用於 S3 存儲桶和OpenSearch/彈性搜索與您的快照兼容的版本。

> **Important**
>
> 快照只能正向相容，而且只能往前一個主要版本。例如，您無法從OpenSearch1.x彈性搜索 7 上的集群。x叢集，只有一個OpenSearch1.x或 2.x集群。次要版本也很重要。您無法從 5.3.2 上的自我管理 5.3.3 叢集還原快照OpenSearch服務網域。我們建議您選擇最新版本OpenSearch或彈性搜索您的快照支持。如需相容版本的表格，請參閱the section called “使用快照來遷移資料”。

提供許可以存取 S3 儲存貯體。

在 AWS Identity and Access Management (IAM) 主控台中，建立角色，它具有下列許可和信任關係。在建立角色時，選擇 S3 作為 AWS Service。將角色命名為 `OpenSearchSnapshotRole` 以便輕鬆找到。

許可

```
{
  "Version": "2012-10-17",
  "Statement": [{
      "Action": [
        "s3:ListBucket"
      ],
      "Effect": "Allow",
      "Resource": [
        "arn:aws:s3:::bucket-name"
      ]
    },
```

```
    {
      "Action": [
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject"
      ],
      "Effect": "Allow",
      "Resource": [
        "arn:aws:s3:::bucket-name/*"
      ]
    }
  ]
}
```

信任關係

```
{
  "Version": "2012-10-17",
  "Statement": [{
      "Effect": "Allow",
      "Principal": {
        "Service": "es.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

然後授予您的個人 IAM 角色許可，以擔任 `OpenSearchSnapshotRole`。建立下列政策，並將它連接到您的身分：

許可

```
{
  "Version": "2012-10-17",
  "Statement": [{
      "Effect": "Allow",
      "Action": "iam:PassRole",
      "Resource": "arn:aws:iam::123456789012:role/OpenSearchSnapshotRole"
    }
  ]
}
```

對應快照角色OpenSearch儀表板 (如果使用精細的存取控制)

如果您已啟用精細存取控制，即使您將 HTTP 基本身分驗證用於所有其他目的，您也需要將 `manage_snapshots` 角色映射至 IAM 角色，以便您可以使用快照。

若要為您的身分授予許可以便使用快照

1. 使用您在建立OpenSearch服務網域。您可以在OpenSearch服務主控台。其格式為 `https://domain-endpoint/_dashboards/`。
2. 從主選單中選擇 Security (安全性)、Roles (角色)，然後選取 manage_snapshots 角色。
3. 選擇 Mapped users (已映射的使用者)、Manage mapping (管理映射)。
4. 在適當的欄位中新增您的個人 IAM 角色的網域 ARN。ARN 採用下列其中一種格式：

```
arn:aws:iam::123456789123:user/user-name
```

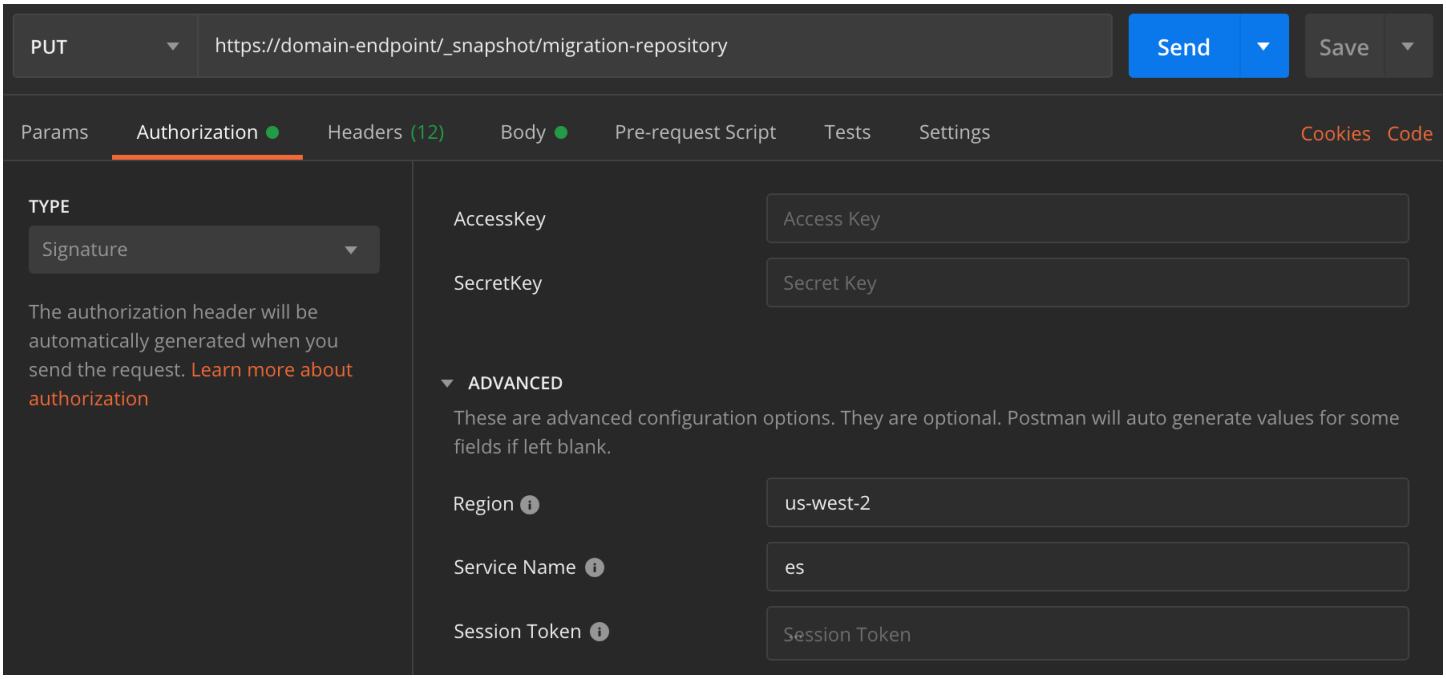
```
arn:aws:iam::123456789123:role/role-name
```

5. 選擇 Map (映射)，並確認角色顯示在 Mapped users (已映射的使用者) 中。

還原快照

此時，您有兩種方法可以訪問OpenSearch服務網域：使用您的主要使用者認證進行 HTTP 基本驗證，或AWS使用 IAM 登入資料進行身份驗證 由於快照使用沒有主要使用者概念的 Amazon S3，因此您必須使用 IAM 登入資料向您的OpenSearch服務網域。

大多數編程語言都有幫助簽名請求的庫，但更簡單的方法是使用類似的工具邮递员並將您的 IAM 登入資料放入授權部分。



還原快照

1. 無論您選擇如何簽署請求，第一步都是註冊儲存庫：

```
PUT _snapshot/my-snapshot-repo-name
{
  "type": "s3",
  "settings": {
    "bucket": "bucket-name",
    "region": "us-west-2",
    "role_arn": "arn:aws:iam::123456789012:role/OpenSearchSnapshotRole"
  }
}
```

2. 然後列出儲存庫中的快照，找到您要還原的快照。此時，您可以繼續使用 Postman，或切換到 curl 等工具。

   速記

```
GET _snapshot/my-snapshot-repo-name/_all
```

   curl

```
curl -XGET -u 'master-user:master-user-password' https://domain-endpoint/
_snapshot/my-snapshot-repo-name/_all
```

3. 還原快照。

   速記

```
POST _snapshot/my-snapshot-repo-name/my-snapshot-name/_restore
{
  "indices": "migration-index1,migration-index2,other-indices-*",
  "include_global_state": false
}
```

   curl

```
curl -XPOST -u 'master-user:master-user-password' https://domain-endpoint/
_snapshot/my-snapshot-repo-name/my-snapshot-name/_restore \
  -H 'Content-Type: application/json' \
  -d '{"indices":"migration-index1,migration-index2,other-indices-
*","include_global_state":false}'
```

4. 最後，確認索引是否已依照預期還原。

   速記

```
GET _cat/indices?v
```

   curl

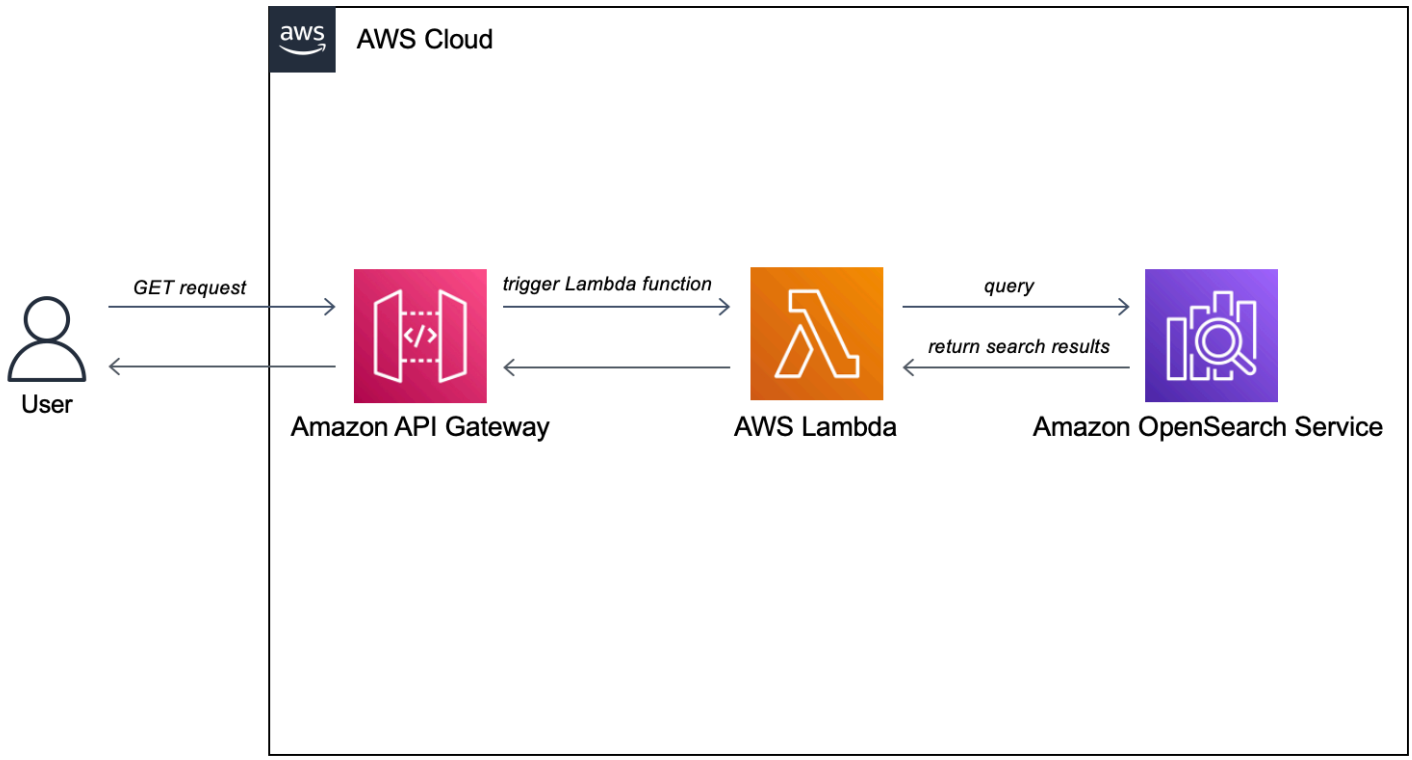
```
curl -XGET -u 'master-user:master-user-password' https://domain-endpoint/_cat/
indices?v
```

此時，遷移即已完成。您可以配置您的客戶端使用新的OpenSearch服務端點調整網域大小以適應您的工作負載，請檢查索引的碎片計數，切換到IAM 主要使用者，或開始建立視覺效果OpenSearch儀表板。

教學：使用 Amazon OpenSearch 服務建立搜尋應用程式

使用 Amazon Ser OpenSearch vice 建立搜尋應用程式的常用方法是使用網頁表單將使用者查詢傳送到伺服器。然後，您可以授權服務器直接調 OpenSearch 用 API，並讓服務器將請求發送到 OpenSearch 服務。但是如果您想要編寫不依賴伺服器的用戶端程式碼，您應彌補安全性和效能風險。不建議允許未簽署的公開存取 OpenSearch API。使用者可能會透過過於廣泛的查詢 (或太多查詢) 存取不安全的端點或影響叢集效能。

本章介紹一個解決方案：使用 Amazon API Gateway 將使用者限制為 OpenSearch API 的子集，並 AWS Lambda簽署從 API Gateway 到 OpenSearch 服務的請求。



> **Note**
>
> 標準 API Gateway 和 Lambda 定價適用，但在此教學課程的限制使用量之內，成本應微乎其微。

必要條件

本教學課程的先決條件是 OpenSearch 服務網域。如果您還沒有服務網域，請依照建立 OpenSearch 服務網域中的步驟建立服務網域。

步驟 1：索引範例資料

下載 sample-movies.zip、進行解壓縮，然後使用 _bulk API 操作來將 5,000 個文件新增到 movies 索引：

```
POST https://search-my-domain.us-west-1.es.amazonaws.com/_bulk
{ "index": { "_index": "movies", "_id": "tt1979320" } }
{"directors":["Ron
 Howard"],"release_date":"2013-09-02T00:00:00Z","rating":8.3,"genres":
["Action","Biography","Drama","Sport"],"image_url":"http://ia.media-imdb.com/images/
M/MV5BMTQyMDE0MTY0OV5BMl5BanBnXkFtZTcwMjI2OTI0OQ@@._V1_SX400_.jpg","plot":"A re-
creation of the merciless 1970s rivalry between Formula One rivals James Hunt and
 Niki Lauda.","title":"Rush","rank":2,"running_time_secs":7380,"actors":["Daniel
 Brühl","Chris Hemsworth","Olivia Wilde"],"year":2013,"id":"tt1979320","type":"add"}
{ "index": { "_index": "movies", "_id": "tt1951264" } }
{"directors":["Francis Lawrence"],"release_date":"2013-11-11T00:00:00Z","genres":
["Action","Adventure","Sci-Fi","Thriller"],"image_url":"http://ia.media-imdb.com/
images/M/
MV5BMTAyMjQ3OTAxMzNeQTJeQWpwZ15BbWU4MDU0NzA1MzAx._V1_SX400_.jpg","plot":"Katniss
 Everdeen and Peeta Mellark become targets of the Capitol after
 their victory in the 74th Hunger Games sparks a rebellion in
 the Districts of Panem.","title":"The Hunger Games: Catching
 Fire","rank":4,"running_time_secs":8760,"actors":["Jennifer Lawrence","Josh
 Hutcherson","Liam Hemsworth"],"year":2013,"id":"tt1951264","type":"add"}
...
```

請注意，上面是一個示例命令，其中包含可用數據的一小部分。要執行該_bulk操作，您需要復制並粘貼sample-movies文件的全部內容。如需進一步的指示，請參閱the section called “選項 2：上傳多個文件”。

您也可以使用以下 curl 命令來實現相同的結果：

```
curl -XPOST -u 'master-user:master-user-password' 'domain-endpoint/_bulk' --data-binary
 @bulk_movies.json -H 'Content-Type: application/json'
```

步驟 2：建立和部署 Lambda 函數

在 API Gateway 中建立 API 之前，請先建立其傳遞要求的 Lambda 函數。

建立 Lambda 函數

在此解決方案中，API Gateway 會將請求傳送至 Lambda 函數，該函數會查詢 OpenSearch 服務並傳回結果。由於此範例函數使用外部程式庫，因此您需要建立部署套件並將其上傳至 Lambda。

建立部署套件

1. 開啟命令提示字元並建立 `my-opensearch-function` 專案目錄。例如，在 macOS 上：

```
mkdir my-opensearch-function
```

2. 導覽至 `my-sourcecode-function` 專案目錄。

```
cd my-opensearch-function
```

3. 複製下列範例 Python 程式碼的內容，並將其儲存在名為的新檔案中`opensearch-lambda.py`。將您的區域和主機端點新增至檔案。

```
import boto3
import json
import requests
from requests_aws4auth import AWS4Auth

region = '' # For example, us-west-1
service = 'es'
credentials = boto3.Session().get_credentials()
awsauth = AWS4Auth(credentials.access_key, credentials.secret_key, region, service,
 session_token=credentials.token)

host = '' # The OpenSearch domain endpoint with https:// and without a trailing
 slash
index = 'movies'
url = host + '/' + index + '/_search'

# Lambda execution starts here
def lambda_handler(event, context):

    # Put the user query into the query DSL for more accurate search results.
```

```
    # Note that certain fields are boosted (^).
    query = {
        "size": 25,
        "query": {
            "multi_match": {
                "query": event['queryStringParameters']['q'],
                "fields": ["title^4", "plot^2", "actors", "directors"]
            }
        }
    }

    # Elasticsearch 6.x requires an explicit Content-Type header
    headers = { "Content-Type": "application/json" }

    # Make the signed HTTP request
    r = requests.get(url, auth=awsauth, headers=headers, data=json.dumps(query))

    # Create the response and add some extra content to support CORS
    response = {
        "statusCode": 200,
        "headers": {
            "Access-Control-Allow-Origin": '*'
        },
        "isBase64Encoded": False
    }

    # Add the search results to the response
    response['body'] = r.text
    return response
```

4. 將外部資源庫安裝到新package目錄。

```
pip3 install --target ./package boto3
pip3 install --target ./package requests
pip3 install --target ./package requests_aws4auth
```

5. 在根目錄中使用已安裝的程式庫建立部署套件。以下命令在您的項目目錄中生成一個my-deployment-package.zip文件。

```
cd package
zip -r ../my-deployment-package.zip .
```

6. 將 opensearch-lambda.py 檔案新增至 zip 檔案的根目錄。

```
cd ..
zip my-deployment-package.zip opensearch-lambda.py
```

如需建立 Lambda 函數和部署套件的詳細資訊，請參閱 AWS Lambda 開發人員指南中的使用 .zip 封存檔部署 Python Lambda 函數以及本指南中的 the section called “建立 Lambda 部署套件”。

若要使用 Lambda 主控台建立函數

1. 瀏覽至 Lambda 主控台，網址為 https://console.aws.amazon.com/lambda/home。在左側導覽窗格中，選擇 [函數]。
2. 選取 Create function (建立函數)。
3. 設定下列欄位：
   - 功能名稱：打開搜索功能
   - 執行階段:Python 3.9
   - 架構：x86_64

   保留所有其他默認選項，然後選擇創建功能。
4. 在函數摘要頁面的 [程式碼原始碼] 區段中，選擇 [上傳自] 下拉式清單，然後選取 .zip 檔案。找到您建立的`my-deployment-package.zip`檔案，然後選擇 [儲存]。
5. 處理常式是函數程式碼中處理事件的方法。在 [執行階段設定] 下，選擇 [編輯]，然後根據 Lambda 函數所在部署套件中的檔案名稱變更處理常式名稱。由於您的檔案已命名`opensearch-lambda.py`，請將處理常式重新命名為*`opensearch-lambda`*`.lambda_handler`。如需詳細資訊，請參閱 Python 中的 Lambda 函數處理常式。

步驟 3：在 API Gateway 中建立 API

使用 API Gateway 可讓您建立更有限的 API，並簡化與 OpenSearch `_search` API 互動的程序。API Gateway 可啟用安全性功能，例如 Amazon Cognito 身分驗證和請求調節。請執行下列步驟，來建立和部署 API：

建立和設定 API

若要使用 API Gateway 主控台建立 API

1. 瀏覽至 API Gateway 主控台，網址為 https://console.aws.amazon.com/apigateway/home。在左側導覽窗格中，選擇 [API]。
2. 找到 REST API (非私有) 並選擇 Build (建置)。
3. 在下一頁上，找到「建立新 API」區段，並確定已選取「新建 API」。
4. 設定下列欄位：
   - API 名稱：opensearch-api
   - 說明：用於搜索 Amazon OpenSearch 服務域的公共 API
   - 端點類型：區域
5. 選擇建立 API。
6. 選擇 Actions (動作) 和 Create Method (建立方法)。
7. 在下拉式選單中選擇 GET，然後按一下核取記號以確認。
8. 進行下列設定，然後選擇 Save (儲存)：

設定	Value
整合類型	Lambda 函數
使用 Lambda 代理整合	是
Lambda 區域	*us-west-1*
Lambda 函數	`opensearch-lambda`
使用預設逾時	是

設定方法請求

選擇 Method Request (方法請求)，然後進行下列設定：

設定	Value
授權	NONE
請求驗證程式	驗證查詢字串參數與標頭

設定	Value
需要 API 金鑰	false

在「URL 查詢字串參數」下，選擇「新增查詢字串」並設定下列參數：

設定	Value
名稱	q
必要	是

部署 API 並設定階段

API Gateway 主控台可讓您透過建立部署並將它與全新或現有階段建立關聯來部署 API。

1. 選擇 Actions (動作) 和 Deploy API (部署 API)。
2. 對於 Deployment stage (部署階段)，選擇 New Stage (新增階段) 並將階段命名為 `opensearch-api-test`。
3. 選擇部署。
4. 在階段編輯器中進行下列設定，然後選擇 Save Changes (儲存變更)：

設定	Value
啟用調節	是
速率	1000
爆量	500

這些設定會設定僅有一個方法的 API：`GET` 對端點根進行要求 (`https://some-id.execute-api.us-west-1.amazonaws.com/search-es-api-test`)。要求需要單一參數 (q)，要搜尋的查詢字串。呼叫時，方法會將請求傳遞至 Lambda，它會執行 `opensearch-lambda` 函數。如需詳細資訊，請參閱在 Amazon API Gateway 中建立 API 和在 Amazon API Gateway 中部署 REST API。

步驟 4：(選用) 修改網域存取政策

您的 OpenSearch 服務網域必須允許 Lambda 函數向`movies`索引發請`GET`求。如果您的網域具有啟用了精細存取控制的開放存取政策，可以保持原樣：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "*"
      },
      "Action": "es:*",
      "Resource": "arn:aws:es:us-west-1:123456789012:domain/domain-name/*"
    }
  ]
}
```

或者，您可以選擇使網域存取政策更精細。例如，下列最低政策提供對 `movies` 索引的 `opensearch-lambda-role` (透過 Lambda 建立) 讀取存取權：若要取得 Lambda 自動建立之角色的確切名稱，請移至 AWS Identity and Access Management (IAM) 主控台，選擇 Roles (角色)，並搜索 "lambda"。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::123456789012:role/service-role/opensearch-lambda-
role-1abcdefg"
      },
      "Action": "es:ESHttpGet",
      "Resource": "arn:aws:es:us-west-1:123456789012:domain/domain-name/movies/_search"
    }
  ]
}
```

> **Important**
>
> 如果您為網域啟用了精細的存取控制，您也需要將角色對應至 OpenSearch 儀表板中的使用者，否則會看到權限錯誤。

如需存取政策的詳細資訊，請參閱the section called “設定存取政策”。

映射 Lambda 角色 (如果使用精細存取控制)

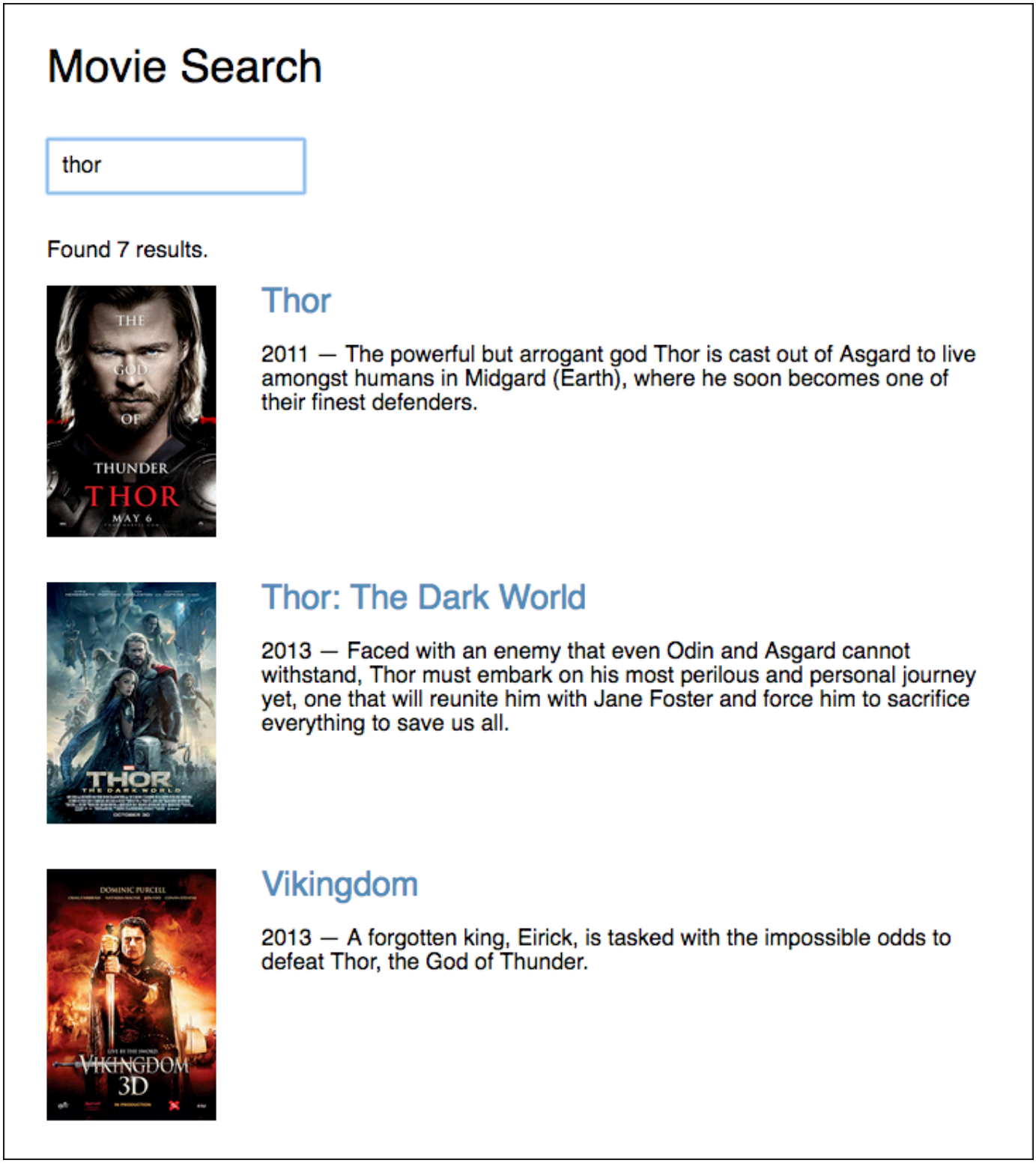
精細存取控制會在您可以測試應用程式之前引進額外的步驟。即使您將 HTTP 基本身分驗證用於所有其他目的，您也需要將 Lambda 角色映射至使用者，否則您會看到許可錯誤。

1. 導覽至網域的 OpenSearch 儀表板 URL。
2. 從主功能表中選擇安全性、角色，然後選取要`all_access`對應 Lambda 角色所需角色的連結。
3. 選擇 Mapped users (已映射的使用者)、Manage mapping (管理映射)。
4. 在 Backend roles (後端角色) 下方，新增 Lambda 角色的 Amazon Resource Name (ARN)。ARN 應採取的`arn:aws:iam::`*`123456789123`*`:role/service-role/`*`opensearch-lambda-role-1abcdefg`*形式.
5. 選擇 Map (映射)，並確認使用者或角色顯示在 Mapped users (已映射的使用者) 中。

步驟 5：測試 Web 應用程式

若要測試 web 應用程式

1. 下載 sample-site.zip，將其解壓縮並使用您最愛的文字編輯器將 `scripts/search.js` 開啟。
2. 更新`apigatewayendpoint`變數以指向您的 API Gateway 端點，並在指定路徑的末尾新增反斜線。您可以透過選擇 Stages (階段)，然後選取 API 的名稱，在 API Gateway 中快速找到端點。`apigatewayendpoint`變數應採用`https://`*`some-id`*`.execute-api.`*`us-west-1`*`.amazonaws.com/opensearch-api-test/`的形式。
3. 開啟 `index.html` 並嘗試對 thor、house 和一些其他術語執行搜尋。



對 CORS 錯誤進行疑難排解

即使 Lambda 函數在回應中包含支援 CORS 的內容，仍可能會看到以下錯誤：

```
Access to XMLHttpRequest at '<api-gateway-endpoint>' from origin 'null' has been
 blocked by CORS policy: No 'Access-Control-Allow-Origin' header is present in the
 requested resource.
```

如果發生此情況，請嘗試下列操作：

1. 在 GET 資源上啟用 CORS。在 Advanced (進階) 下，將 Access-Control-Allow-Credentials 設定為 `'true'`。
2. 在 API Gateway 中重新部署 API (Actions (動作)、Deploy API (部署 API))。
3. 刪除並重新新增您的 Lambda 函數觸發程序。添加重新添加它，選擇添加觸發器並創建調用您的函數的 HTTP 端點。觸發必須具有以下組態：

觸發條件	API	部署階段	安全
API 閘道	opensearch-api	opensearch-api-test	開啟

後續步驟

本章只是展縣概念的起點。您可以考慮以下修改：

- 將您自己的資料新增至 OpenSearch 服務網域。
- 將方法新增至 API
- 在 Lambda 函數中，修改搜尋查詢或提升不同的欄位。
- 樣式結果不同或修改 `search.js` 來向使用者顯示不同的欄位。

教學課程：使用 OpenSearch Service 和 OpenSearch Dash，將客戶支援呼叫視覺化

此章節是一個完整的逐步解說，情況如下：業務收到不少客戶支援呼叫，想要對其進行分析。每個呼叫的主題為何？ 有多少是正面的？ 有多少是負面的？ 主管人員如何搜尋或檢閱這些呼叫的文字記錄？

手動工作流程可能涉及員工聆聽錄音、記下每個呼叫的主題，以及判斷客戶互動是否正面。

這類的程序是非常費工的。假設每個呼叫平均時間為 10 分鐘，那麼每個員工每天只能聆聽 48 個呼叫。排除人的偏見後，所產生的資料使有極高的準確度，而資料量會降到最低：只需呼叫的主題，以及有關客戶是否滿意的布林值。若再加上更多資料如完整的文字記錄，便需要花大量時間。

使用 Amazon S3、Amazon Transcribe、Amazon Comprehend 和 Amazon Ser OpenSearch vice，便能以極少的程式碼自動化類似的程序，所產生的資料量非常多。例如，您可以取得呼叫的完整文字記錄、文字記錄的關鍵字和呼叫的整體「情緒」(正面、負面、中立或混合)。然後，您可以使用 OpenSearch和 OpenSearch Dash boards 來搜尋和視覺化資料。

您可以一字不漏地執行，用意只是為了讓您在 OpenSearch Service 中編製索引之前，激盪出有關如何使 JSON 文件更加豐富的想法。

評估成本

一般而言，執行這個逐步解說中的步驟的成本不到 2 美元。此逐步解說使用下列資源：

- S3 儲存貯體的傳輸和儲存量少於 100 MB

  如需進一步了解，請參閱 Amazon S3 定價。
- OpenSearch具有一個`t2.medium`執行個體和 10 GiB 的 EBS 儲存空間，運作長達數小時的 Service 網域

  如需進一步了解，請參閱 Amazon Ser OpenSearch vice 定價。
- 對 Amazon Transcribe 的數個呼叫

  如需進一步了解，請參閱 Amazon Transcribe 定價。
- 對 Amazon Comprehend 的數個自然語言處理呼叫

  如需進一步了解，請參閱 Amazon Comprehend 定價。

主題

- 步驟 1：設定先決條件
- 步驟 2：複製範本程式碼
- (選用) 步驟 3：索引範例資料
- 步驟 4：分析和視覺化您的資料
- 步驟 5：清除資源和後續步驟

步驟 1：設定先決條件

繼續之前，您必須準備好以下資源。

先決條件	描述
Amazon S3 儲存貯體	如需詳細資訊，請參閱 Amazon Simple Storage Service 主控台使用者指南中的建立儲存貯體。
OpenSearch服務網域	資料的目的地。如需詳細資訊，請參閱建立 OpenSearch Service 網域。

如果尚未擁有這些資源，您可以使用下列 AWS CLI 命令建立資源：

```
aws s3 mb s3://my-transcribe-test --region us-west-2
```

```
aws opensearch create-domain --domain-name my-transcribe-test --engine-version
 OpenSearch_1.0 --cluster-config  InstanceType=t2.medium.search,InstanceCount=1
 --ebs-options EBSEnabled=true,VolumeType=standard,VolumeSize=10 --access-
policies '{"Version":"2012-10-17","Statement":[{"Effect":"Allow","Principal":
{"AWS":"arn:aws:iam::123456789012:root"},"Action":"es:*","Resource":"arn:aws:es:us-
west-2:123456789012:domain/my-transcribe-test/*"}]}' --region us-west-2
```

> **Note**
>
> 這些命令使用 `us-west-2` 區域，但您可以使用 Amazon Comprehend 支援的任何區域。如需進一步了解，請參閱AWS 一般參考。

步驟 2：複製範本程式碼

1. 複製下列 Python 3 範本程式碼，並貼上到名為 `call-center.py` 的新檔案：

```
import boto3
import datetime
import json
import requests
from requests_aws4auth import AWS4Auth
import time
import urllib.request

# Variables to update
audio_file_name = '' # For example, 000001.mp3
bucket_name = '' # For example, my-transcribe-test
```

```
domain = '' # For example, https://search-my-transcribe-test-12345.us-
west-2.es.amazonaws.com
index = 'support-calls'
type = '_doc'
region = 'us-west-2'

# Upload audio file to S3.
s3_client = boto3.client('s3')

audio_file = open(audio_file_name, 'rb')

print('Uploading ' + audio_file_name + '...')
response = s3_client.put_object(
    Body=audio_file,
    Bucket=bucket_name,
    Key=audio_file_name
)

# # Build the URL to the audio file on S3.
# # Only for the us-east-1 region.
# mp3_uri = 'https://' + bucket_name + '.s3.amazonaws.com/' + audio_file_name

# Get the necessary details and build the URL to the audio file on S3.
# For all other regions.
response = s3_client.get_bucket_location(
    Bucket=bucket_name
)
bucket_region = response['LocationConstraint']
mp3_uri = 'https://' + bucket_name + '.s3-' + bucket_region + '.amazonaws.com/' +
 audio_file_name

# Start transcription job.
transcribe_client = boto3.client('transcribe')

print('Starting transcription job...')
response = transcribe_client.start_transcription_job(
    TranscriptionJobName=audio_file_name,
    LanguageCode='en-US',
    MediaFormat='mp3',
    Media={
        'MediaFileUri': mp3_uri
    },
    Settings={
        'ShowSpeakerLabels': True,
```

```
        'MaxSpeakerLabels': 2 # assumes two people on a phone call
    }
)

# Wait for the transcription job to finish.
print('Waiting for job to complete...')
while True:
    response =
 transcribe_client.get_transcription_job(TranscriptionJobName=audio_file_name)
    if response['TranscriptionJob']['TranscriptionJobStatus'] in ['COMPLETED',
 'FAILED']:
        break
    else:
        print('Still waiting...')
    time.sleep(10)

transcript_uri = response['TranscriptionJob']['Transcript']['TranscriptFileUri']

# Open the JSON file, read it, and get the transcript.
response = urllib.request.urlopen(transcript_uri)
raw_json = response.read()
loaded_json = json.loads(raw_json)
transcript = loaded_json['results']['transcripts'][0]['transcript']

# Send transcript to Comprehend for key phrases and sentiment.
comprehend_client = boto3.client('comprehend')

# If necessary, trim the transcript.
# If the transcript is more than 5 KB, the Comprehend calls fail.
if len(transcript) > 5000:
    trimmed_transcript = transcript[:5000]
else:
    trimmed_transcript = transcript

print('Detecting key phrases...')
response = comprehend_client.detect_key_phrases(
    Text=trimmed_transcript,
    LanguageCode='en'
)

keywords = []
for keyword in response['KeyPhrases']:
    keywords.append(keyword['Text'])
```

```
print('Detecting sentiment...')
response = comprehend_client.detect_sentiment(
    Text=trimmed_transcript,
    LanguageCode='en'
)

sentiment = response['Sentiment']

# Build the Amazon OpenSearch Service URL.
id = audio_file_name.strip('.mp3')
url = domain + '/' + index + '/' + type + '/' + id

# Create the JSON document.
json_document = {'transcript': transcript, 'keywords': keywords, 'sentiment':
 sentiment, 'timestamp': datetime.datetime.now().isoformat()}

# Provide all details necessary to sign the indexing request.
credentials = boto3.Session().get_credentials()
awsauth = AWS4Auth(credentials.access_key, credentials.secret_key, region,
 'opensearchservice', session_token=credentials.token)

# Index the document.
print('Indexing document...')
response = requests.put(url, auth=awsauth, json=json_document, headers=headers)

print(response)
print(response.json())
```

2. 更新初始六個變數。
3. 使用以下命令安裝所需套件：

```
pip install boto3
pip install requests
pip install requests_aws4auth
```

4. 將 MP3 放置在和 `call-center.py` 相同的目錄，並執行指令碼。範例輸出如下：

```
$ python call-center.py
Uploading 000001.mp3...
Starting transcription job...
Waiting for job to complete...
Still waiting...
Still waiting...
```

```
Still waiting...
Still waiting...
Still waiting...
Still waiting...
Still waiting...
Detecting key phrases...
Detecting sentiment...
Indexing document...
<Response [201]>
{u'_type': u'call', u'_seq_no': 0, u'_shards': {u'successful': 1, u'failed': 0,
 u'total': 2}, u'_index': u'support-calls4', u'_version': 1, u'_primary_term': 1,
 u'result': u'created', u'_id': u'000001'}
```

`call-center.py` 執行一些操作：

1. 指令碼上傳音訊檔案 (此案例為，MP3，但 Amazon Transcribe 支援數種格式) 到您的 S3 儲存貯體。
2. 它會將音訊檔案的 URL 傳送到 Amazon Transcribe，並等待文字記錄任務完成。

   完成文字記錄工作的時間取決於音訊檔案長度。採用分鐘數，而非秒數。

   > **Tip**
   > 為了改善文字記錄的品質，您可以設定 Amazon Transcribe 適用的自訂詞彙。

3. 文字記錄任務完成後，指令碼會擷取文字，裁剪到 5,000 個字元，然後將其傳送至 Amazon Comprehend 進行關鍵字和情感分析。
4. 最後，指令碼會將完整的文字記錄、關鍵字、情感和目前時間戳記加入到 JSON 文件，並在 OpenSearch Service 中編製索引。

> **Tip**
> LibriVox具有可用於測試的公共領域有聲讀物。

(選用) 步驟 3：索引範例資料

如果您手邊沒有大量呼叫記錄 (誰有呢)？您可以在 sample-calls.zip 中為範例文件編製索引，這與 `call-center.py` 所產生的結果相當。

1. 建立名為 `bulk-helper.py` 的檔案：

```
import boto3
from opensearchpy import OpenSearch, RequestsHttpConnection
import json
from requests_aws4auth import AWS4Auth

host = '' # For example, my-test-domain.us-west-2.es.amazonaws.com
region = '' # For example, us-west-2
service = 'es'

bulk_file = open('sample-calls.bulk', 'r').read()

credentials = boto3.Session().get_credentials()
awsauth = AWS4Auth(credentials.access_key, credentials.secret_key, region, service,
 session_token=credentials.token)

search = OpenSearch(
    hosts = [{'host': host, 'port': 443}],
    http_auth = awsauth,
    use_ssl = True,
    verify_certs = True,
    connection_class = RequestsHttpConnection
)

response = search.bulk(bulk_file)
print(json.dumps(response, indent=2, sort_keys=True))
```

2. 更新 `host` 和 `region` 兩個初始變數。
3. 使用以下命令安裝所需套件：

```
pip install opensearch-py
```

4. 下載並解壓縮 sample-calls.zip。
5. 將 `sample-calls.bulk` 放置在和 `bulk-helper.py` 相同的目錄，並執行協助程式。範例輸出如下：

```
$ python bulk-helper.py
{
  "errors": false,
  "items": [
    {
      "index": {
        "_id": "1",
        "_index": "support-calls",
        "_primary_term": 1,
        "_seq_no": 42,
        "_shards": {
          "failed": 0,
          "successful": 1,
          "total": 2
        },
        "_type": "_doc",
        "_version": 9,
        "result": "updated",
        "status": 200
      }
    },
    ...
  ],
  "took": 27
}
```

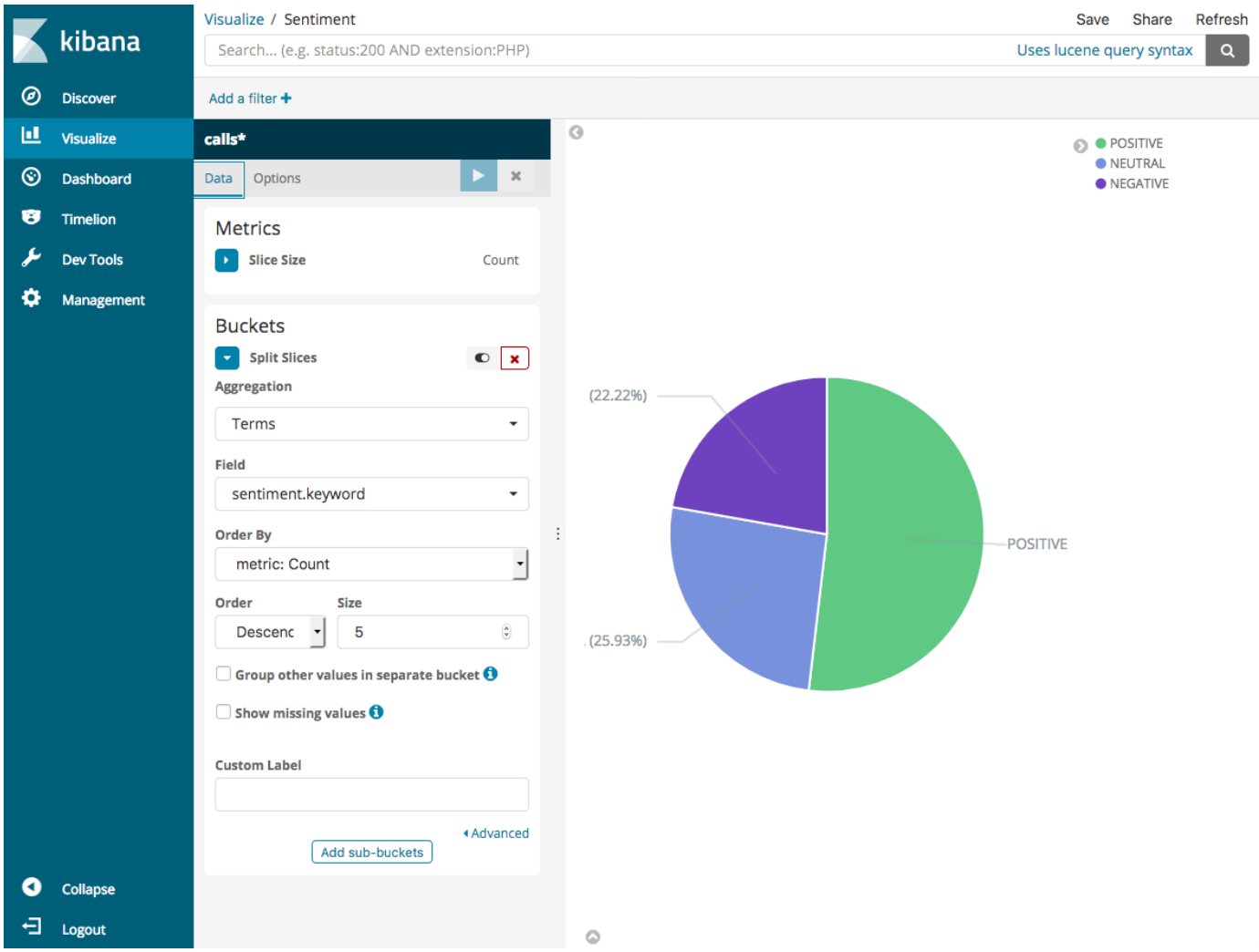
步驟 4：分析和視覺化您的資料

既然您在 OpenSearch Service 中有一些資料，您可以使用 OpenSearch Dash boards 將資料視覺化。

1. 導覽至 `https://search-domain.region.es.amazonaws.com/_dashboards`。
2. 在使用 Dash 之OpenSearch前，您需要索引模式。Dashboards 使用索引模式將分析縮小至一個或多個索引。若要匹配 `call-center.py` 建立的 `support-calls` 索引，請前往 Stack Management (堆疊管理)、Index Patterns (索引模式)，並定義 `support*` 的索引模式，然後選擇 Next step (下一個步驟)。
3. 對於 Time Filter field name (時間篩選條件欄位名稱)，請選擇 timestamp (時間戳記)。
4. 您現在可以開始建立視覺化效果。選擇 Visualize (視覺化)，然後新增視覺化。
5. 選擇圓餅圖和 `support*` 索引模式。

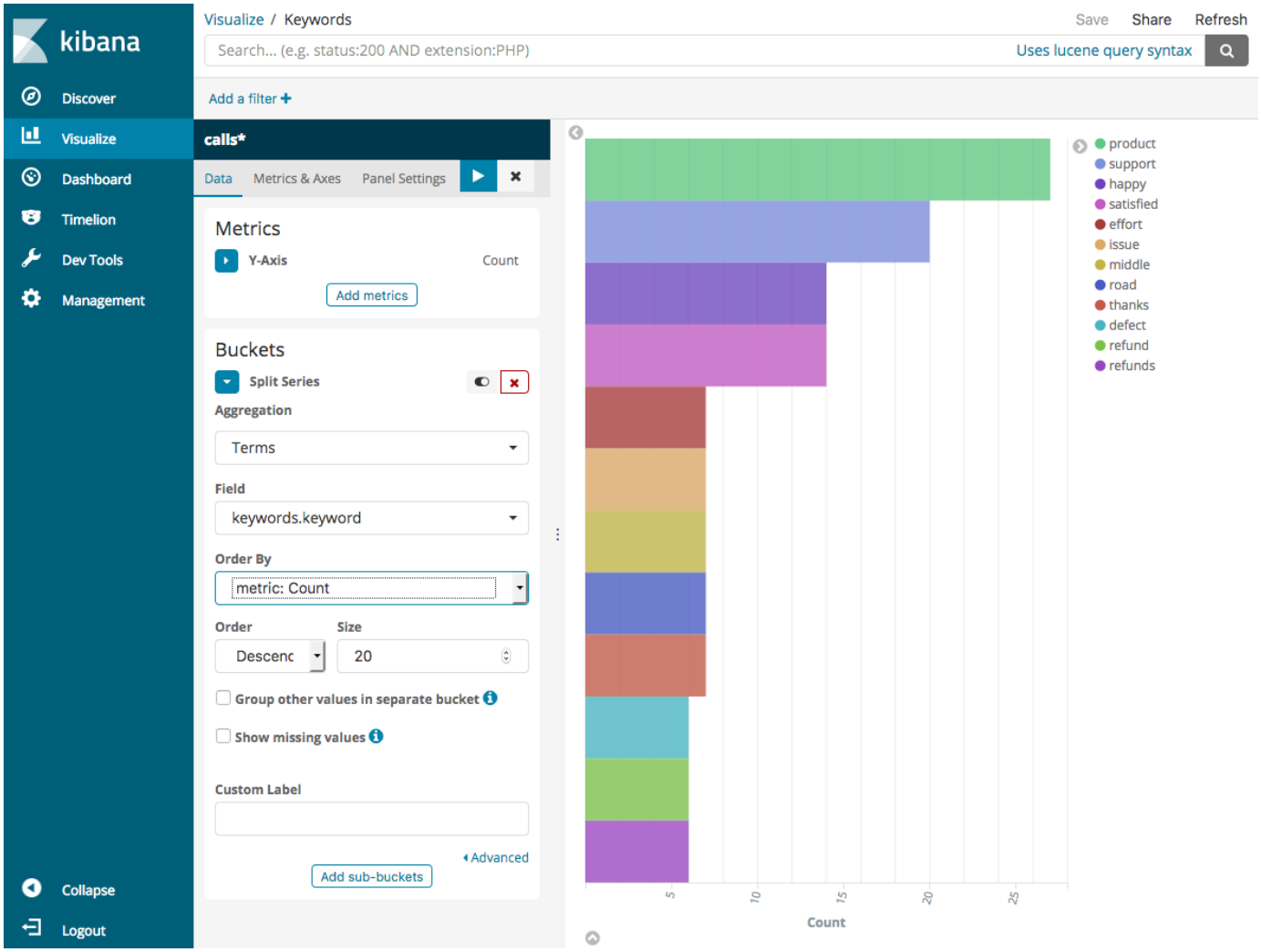
6. 預設視覺化是基本的，因此選擇 Split Slices (分割切片) 來建立更有趣的視覺化效果。

   對於 Aggregation (集合) 選項，請選擇 Terms (條款)。對於 Field (欄位)，選擇 sentiment.keyword。然後選擇 Apply changes (套用變更) 和 Save (儲存)。

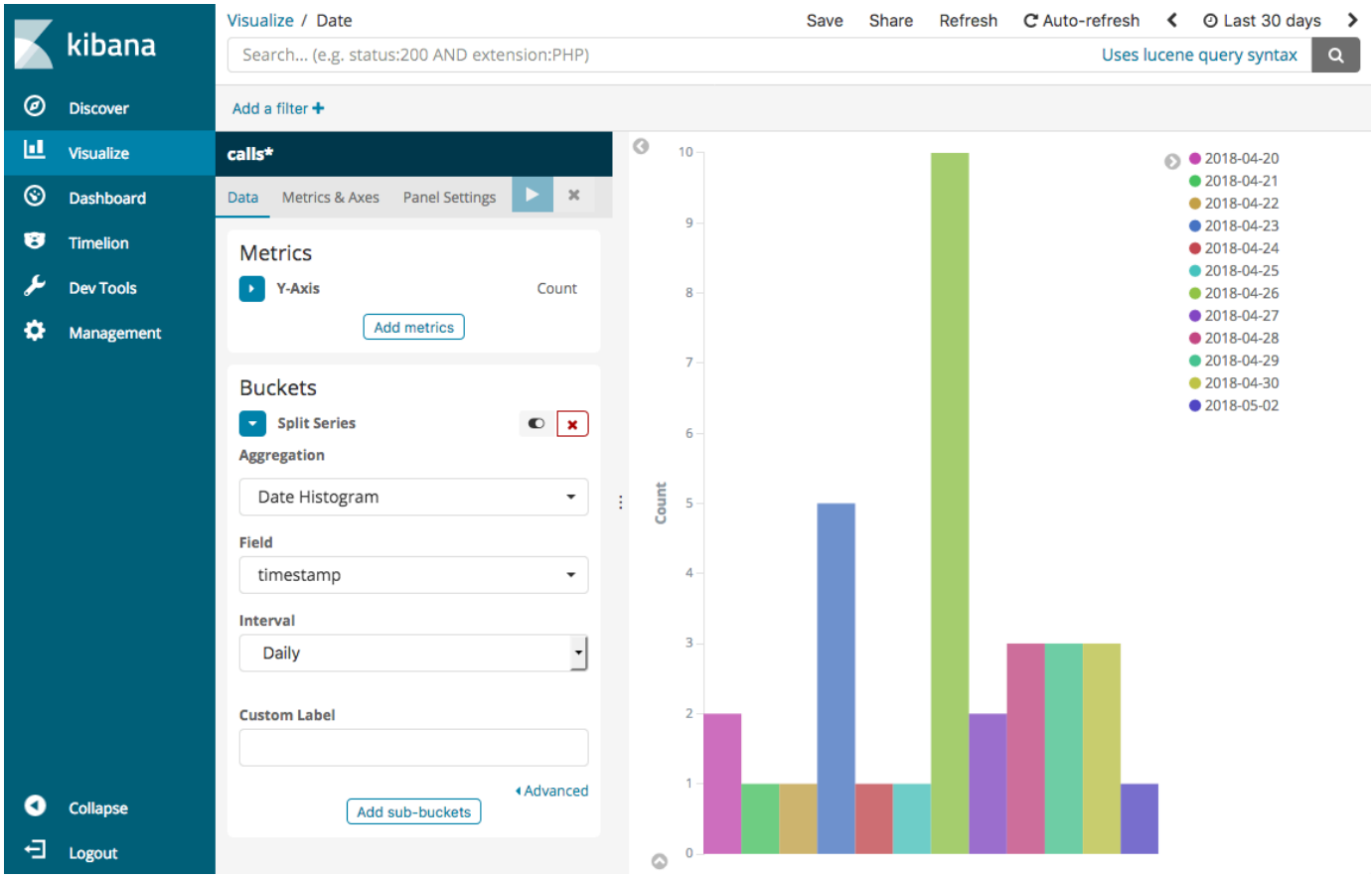


7. 返回 Visualize (視覺化) 頁面，並新增另一個視覺化。這時，選擇水平長條圖。
8. 選擇 Split Series (分割系列)。

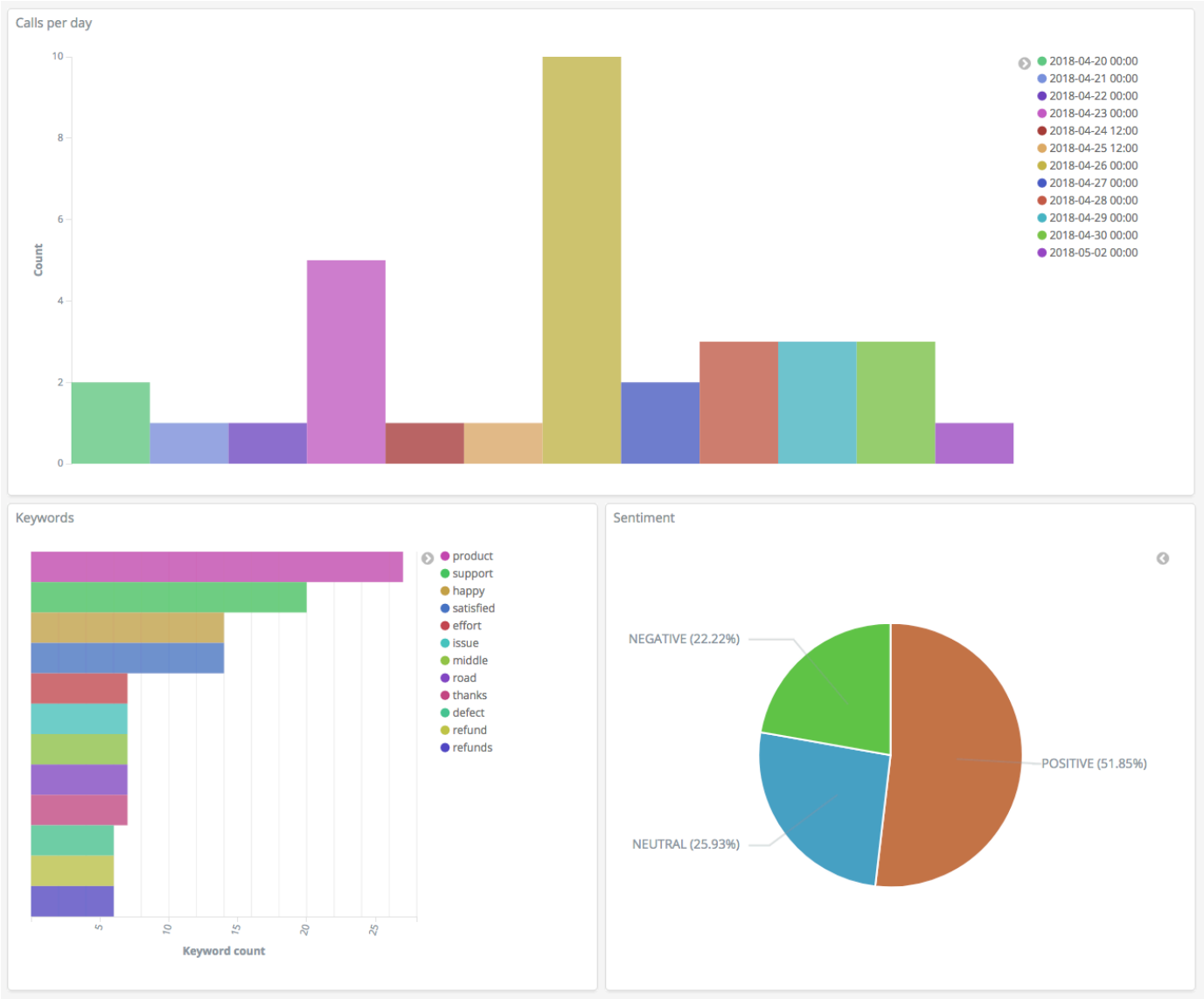
   對於 Aggregation (集合) 選項，請選擇 Terms (條款)。對於 Field (欄位)，選擇 keywords.keyword，並將 Size (大小) 變更為 20。然後選擇 Apply Changes (套用變更) 和 Save (儲存)。



9. 返回 Visualize (視覺化) 頁面，並新增一個最終視覺化垂直長條圖。
10. 選擇 Split Series (分割系列)。對於 Aggregation (彙總)，選擇 Date Histogram (日期分佈圖)。對於 Field (欄位)，選擇 timestamp (時間戳記)，將 Interval (間隔) 變更為 Daily (每日)。
11. 選擇 Metrics & Axes (指標和軸)，並將變更 Mode (模式) 變更為 normal (正常)。
12. 選擇 Apply Changes (套用變更) 和 Save (儲存)。



13. 既然您有三個視覺效果，您可以將它們新增到 Dashboards 視覺效果。選擇 Dashboard (儀表板)、建立儀表板，並新增視覺化效果。



步驟 5：清除資源和後續步驟

為避免不必要的費用，請刪除 S3 儲存貯體和 OpenSearch Service 網域。如需進一步了解，請參閱 Amazon Search Search Service 使用者指南中的刪除儲存貯體和本指南中的刪除 Ser OpenSearch vice 網域。

文字記錄需要比 MP3 檔更少的磁碟空間。您也許可以縮短您的 MP3 保留時段 (例如，從三個月的呼叫記錄到一個月)，保留數年文字記錄，並且仍能節省儲存成本。

您也可以使用 AWS Step Functions 和 Lambda 將文字記錄程序自動化，在編製索引前新增額外的中繼資料，或者打造更複雜的視覺效果以符合您的確切使用案例。

Amazon OpenSearch Service 重新命名：變更摘要

2021 年 9 月 8 日，我們的搜尋和分析套件更名為 Amazon OpenSearch Service。OpenSearch Service 支援 OpenSearch 以及舊版 Elasticsearch OSS。下列各節說明由於重新命名而變更的服務的不同部分，以及您需要採取哪些動作，從而確保您的網域可繼續正常運作。

當您將網域從 Elasticsearch 升級至 OpenSearch 時，一些變更才適用。在其他情況下，例如，在「帳單和成本管理」主控台中，體驗會立即變化。

注意，此清單並不詳盡。雖然產品的其他部分也有所變更，但這些更新是最相關的。

主題

- 新的 API 版本
- 已重新命名的執行個體類型
- 存取政策變更
- 新資源類型
- Kibana 已更名為 OpenSearch Dashboards
- 已重新命名的 CloudWatch 指標
- 「帳單和成本管理」主控台的變更
- 新事件格式
- 什麼保持不變？
- 開始使用：將您的網域升級至 OpenSearch 1.x

新的 API 版本

新版 OpenSearch Service 組態 API (2021-01-01) 可與 OpenSearch 及舊版 Elasticsearch OSS 搭配使用。21 個 API 操作被替換為更簡潔且與引擎無關的名稱 (例如，`CreateElasticsearchDomain` 變更為 `CreateDomain`)，但 OpenSearch Service 會繼續支援這兩個 API 版本。

建議您使用新的 API 操作來建立和管理未來的網域。請注意，當您使用新的 API 操作來建立網域時，您需要指定 `EngineVersion` 參數，格式為 `Elasticsearch_X.Y` 或 `OpenSearch_X.Y`，而不僅僅是版本號。如果您不指定版本，它會預設為 OpenSearch 的最新版本。

將您的 AWS CLI 升級至 1.20.40 版或更新的版本，以使用 `aws opensearch ...` 建立和管理您的網域。如需新的 CLI 格式，請參閱 OpenSearch CLI 參考。

已重新命名的執行個體類型

Amazon OpenSearch Service 中的執行個體類型現在的格式為 `<type>.<size>.search`，例如為 `m6g.large.search` 而非 `m6g.large.elasticsearch`。您無需執行任何動作。現有網域會開始自動參考 API 內以及 Billing and Cost Management 主控台中的新執行個體類型。

如果您有預留執行個體 (RI)，您的合約不會受到變更的影響。舊的組態 API 版本仍然與舊的命名格式相容，但如果您想要使用新的 API 版本，則需要使用新的格式。

存取政策變更

下列各節說明您需要採取哪些動作來更新存取政策。

IAM 政策

我們建議您更新 IAM 政策以使用已重新命名的 API 操作。不過，OpenSearch Service 透過內部複寫舊的 API 許可，繼續遵守現有的政策。例如，如果您目前擁有執行 `CreateElasticsearchDomain` 操作的許可，您現在可以呼叫 `CreateElasticsearchDomain` (舊的 API 操作) 和 `CreateDomain` (新的 API 操作)。這同樣適用於明確拒絕。如需已更新的 API 操作清單，請參閱政策元素參考。

SCP 政策

服務控制政策 (SCP)與標準 IAM 相比，增添另一層複雜性。若要防止您的 SCP 政策中斷，您需要將舊的和新的 API 操作新增至每個 SCP 政策。例如，如果使用者目前擁有 `CreateElasticsearchDomain` 的允許許可，您還需要授予他們 `CreateDomain` 的允許許可，以便他們能夠保留建立網域的能力。這同樣適用於明確拒絕。

例如：

```
"Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "es:CreateElasticsearchDomain",
        "es:CreateDomain"
          ...
      ],
    },
      "Effect": "Deny",
```

```
      "Action:" [
        "es:DeleteElasticsearchDomain",
        "es:DeleteDomain"
         ...
```

新資源類型

OpenSearch Service 引入下列新資源類型：

資源	描述
`AWS::OpenSearchService::Domain`	表示 Amazon OpenSearch Service 網域。此資源存在於服務層級，並非特定於網域上執行的軟體。它適用於諸如 AWS CloudFormation 和 AWS Resource Groups 等服務，您可以在其中建立和管理整個服務的資源。 如需將 CloudFormation 中定義的網域從 Elasticsearch 升級到 OpenSearch 的說明，請參閱《CloudFormation 使用者指南》中的備註。
`AWS::OpenSearch::Domain`	表示在網域上執行的 OpenSearch/Elasticsearch 軟體。此資源適用於 AWS CloudTrail 和 AWS Config 等服務，其參考在網域上執行的軟體而非整個 OpenSearch Service。這些服務現在包含執行 Elasticsearch 的網域 (`AWS::Elasticsearch::Domain`) 與執行 OpenSearch 的網域 (`AWS::OpenSearch::Domain`) 的個別資源類型。

> **Note**
>
> 在 AWS Config 中，在數周內在現有 `AWS::Elasticsearch::Domain` 資源類型下可繼續看到您的資料，即使您將一個或多個網域升級至 OpenSearch。

Kibana 已更名為 OpenSearch Dashboards

OpenSearch Dashboards，Kibana 的 AWS 替代產品，是一種開源視覺化工具，專為與 OpenSearch 一起使用而設計。將網域從 Elasticsearch 升級至 OpenSearch 之後，`/_plugin/kibana` 端點變更為 `/_dashboards`。OpenSearch Service 會將所有請求重新導向至新端點，但如果您在任何 IAM 政策中使用 Kibana 端點，請更新這些政策以包含新的 `/_dashboards` 端點。

如果您使用的是 the section called “SAML OpenSearch 儀表板的驗證”，在將網域升級至 OpenSearch 之前，您必須將身分提供者 (IdP) 中設定的所有 Kibana URL 從 `/_plugin/kibana` 變更為 `/_dashboards`。最常見的 URL 是聲明消費者服務 (ACS) URL 和收件人 URL。

預設的 `kibana_read_only` 角色已重命名為 `opensearch_dashboards_read_only`，`kibana_user` 角色已重新命名為 `opensearch_dashboards_user`。此變更適用於所有新建立的 OpenSearch 1.x 網域，其執行服務軟體 R20211203 或更高版本。如果將現有網域升級為服務軟體 R20211203，角色名稱將保持不變。

已重新命名的 CloudWatch 指標

針對執行 OpenSearch 的網域，數個 CloudWatch 指標會有所變更。當您將網域升級為 OpenSearch 時，指標會自動變更，而您目前的 CloudWatch 警示將中斷。在將叢集從 Elasticsearch 版本升級至 OpenSearch 版本之前，請務必更新您的 CloudWatch 警示以使用新的指標。

下列指標已變更：

原始指標名稱	新名稱
`KibanaHealthyNodes`	`OpenSearchDashboardsHealthyNodes`
`KibanaConcurrentConnections`	`OpenSearchDashboardsConcurrentConnections`
`KibanaHeapTotal`	`OpenSearchDashboardsHeapTotal`
`KibanaHeapUsed`	`OpenSearchDashboardsHeapUsed`
`KibanaHeapUtilization`	`OpenSearchDashboardsHeapUtilization`

原始指標名稱	新名稱
KibanaOS1MinuteLoad	OpenSearchDashboardsOS1MinuteLoad
KibanaRequestTotal	OpenSearchDashboardsRequestTotal
KibanaResponseTimesMaxInMillis	OpenSearchDashboardsResponseTimesMaxInMillis
ESReportingFailedRequestSysErrCount	KibanaReportingFailedRequestSysErrCount
ESReportingRequestCount	KibanaReportingRequestCount
ESReportingFailedRequestUserErrCount	KibanaReportingFailedRequestUserErrCount
ESReportingSuccessCount	KibanaReportingSuccessCount
ElasticsearchRequests	OpenSearchRequests

如需 OpenSearch Service 傳送至 Amazon CloudWatch 的完整指標清單，請參閱the section called “監控叢集指標”。

「帳單和成本管理」主控台的變更

帳單和成本管理主控台及成本與用量報告中的歷史資料將繼續使用舊的服務名稱，因此在搜尋資料時，需要開始針對 Amazon OpenSearch Service 和舊版 Elasticsearch 名稱使用篩選條件。如果您有已儲存的報告，請更新篩選條件，以確定它們也包含 OpenSearch Service。當 Elasticsearch 的使用量減少而 OpenSearch 的使用量增加時，您一開始可能會收到提醒，但它會在幾天內消失。

除了服務名稱以外，對於所有報告、帳單及價格清單 API 操作，下列欄位將變更：

欄位	舊格式	新格式
執行個體類型	m5.large.elasticsearch	m5.large.search

欄位	舊格式	新格式
產品系列	Elasticsearch 執行個體 Elasticsearch 磁碟區	Amazon OpenSearch Service 執行個體 Amazon OpenSearch Service 磁碟區
定價說明	每個 c5.18xlarge.elasticsearch 執行個體小時 (或不足一小時) 5.098 美元 - 歐盟	每個 c5.18xlarge.search 執行個體小時 (或不足一小時) 5.098 美元 - 歐盟
執行個體系列	`ultrawarm.elasticsearch`	`ultrawarm.search`

新事件格式

OpenSearch Service 傳送到 Amazon EventBridge 和 Amazon CloudWatch 的事件格式已變更，尤其是 `detail-type` 欄位。來源欄位 (`aws.es`) 保持不變。如需每個事件類型的完整格式，請參閱the section called “監控事件”。如果您有依賴於舊格式的現有事件規則，請務必更新它們以符合新格式。

什麼保持不變？

下列特性和功能以及未列出項將保持不變：

- 服務委託人 (`es.amazonaws.com`)
- 廠商程式碼
- 網域 ARN
- 網域端點

開始使用：將您的網域升級至 OpenSearch 1.x

OpenSearch 1.x 支援從 Elasticsearch 版本 6.8 升級至 7.x。如需升級網域的指示，請參閱the section called “開始升級 (主控台)”。如果您使用 AWS CLI 或組態 API 來升級您的網域，則必須將 `TargetVersion` 指定為 `OpenSearch_1.x`。

OpenSearch 1.x 引入名為啟用相容性模式的其他網域設定。由於某些 Elasticsearch OSS 用戶端和外掛程式會在連線前檢查叢集版本，因此相容性模式會設定 OpenSearch 以將其版本報告為 7.10，以便這些用戶端可以繼續運作。

在首次建立 OpenSearch 網域時，或是從 Elasticsearch 版本升級至 OpenSearch 時，您可啟用相容性模式。如果沒有設定，當您建立網域時，參數預設為 `false`，而當您升級網域時，預設為 `true`。

若要使用組態 API 啟用相容性模式，將 `override_main_response_version` 設定為 `true`：

```
POST https://es.us-east-1.amazonaws.com/2021-01-01/opensearch/upgradeDomain
{
  "DomainName": "domain-name",
  "TargetVersion": "OpenSearch_1.0",
  "AdvancedOptions": {
    "override_main_response_version": "true"
   }
}
```

若要啟用或停用現有 OpenSearch 網域中的相容性模式，您需要使用 OpenSearch _cluster/settings API 操作：

```
PUT /_cluster/settings
{
  "persistent" : {
    "compatibility.override_main_response_version" : true
  }
}
```

Amazon OpenSearch 服務故障

本主題說明如何識別和解決常見的 Amazon OpenSearch 服務問題。聯絡 AWS 支援之前，先參閱本節資訊。

無法存取 OpenSearch 儀表板

OpenSearch 儀表板端點不支援已簽署的要求。如果網域的存取控制政策只對特定 IAM 角色授予存取權，而且您尚未設定 Amazon Cognito 身分驗證，當您嘗試存取 Dashboards 時可能會收到以下錯誤：

```
"User: anonymous is not authorized to perform: es:ESHttpGet"
```

如果您的 OpenSearch Service 網域使用 VPC 存取，您可能不會收到此錯誤，但要求可能逾時。如要進一步了解有關修正此問題和各種可用組態選項的詳細資訊，請參閱the section called “控制 OpenSearch 儀表板的存取”、the section called “關於網VPC域的存取原則”以及 the section called “身分和存取權管理”。

無法存取 VPC 網域

請參閱 the section called “關於網VPC域的存取原則” 和 the section called “測試VPC網域”。

叢集處於唯讀狀態

與早期的彈性搜索版本 OpenSearch 和彈性搜索 7 相比。 x 使用不同的系統進行叢集協調。在這個新系統中，當叢集遺失仲裁，在您採取動作之前，叢集將無法使用。遺失仲裁有兩種形式：

- 如果您的叢集使用專用主節點，當一半或更多個節點無法使用時，會發生仲裁遺失。
- 如果您的叢集使用專用主節點，當一半或更多個資料節點無法使用時，會發生仲裁遺失。

如果發生仲裁遺失，且叢集有多個節點， OpenSearch Service 會還原仲裁並將叢集置於唯讀狀態。您有兩種選擇：

- 移除唯讀狀態，並依原狀使用叢集。
- 從快照還原叢集或個別索引。

如果您偏好依原樣使用叢集，請使用下列請求來驗證叢集運作狀態為綠色：

```
GET _cat/health?v
```

如果叢集運作狀態為紅色，建議從快照還原叢集。您也可以參閱 the section called “紅色叢集狀態” 以取得疑難排解步驟。如果叢集運作狀態為綠色，請使用下列請求來檢查所有預期索引是否存在：

```
GET _cat/indices?v
```

然後執行一些搜尋來驗證預期的資料存在。如果存在，您可以使用下列請求來移除唯讀狀態：

```
PUT _cluster/settings
{
  "persistent": {
    "cluster.blocks.read_only": false
  }
}
```

如果發生仲裁遺失，而您的叢集只有一個節點， OpenSearch Service 會取代節點，且不會將叢集置於唯讀狀態。否則，您的選項會是相同的：依原樣使用叢集或從快照還原。

在這兩種情況下， OpenSearch Service 都會向您的 AWS Health Dashboard. 第一個會通知您遺失仲裁。第二個發生在 OpenSearch Service 成功還原仲裁之後。若要取得有關使用的更多資訊 AWS Health Dashboard，請參閱《使AWS Health 用指南》。

紅色叢集狀態

紅色叢集狀態表示至少有一個主要碎片及其複本未配置給節點。 OpenSearch 無論其狀態如何，服務都會持續嘗試擷取所有索引的自動快照，但快照集會在紅色叢集狀態持續存在時失敗。

紅色叢集狀態的最常見原因是叢集節點失敗，以及處理 OpenSearch 序因為持續繁重的處理負載而當機。

> **Note**
>
> OpenSearch 無論叢集狀態為何，服務都會儲存自動快照 14 天。因此，如果紅色叢集狀態持續超過兩週，將會刪除最後一個狀況良好的自動快照，而您可能永遠遺失叢集資料。如果您的 OpenSearch 服務網域進入紅色的叢集狀態， AWS Support 可能會與您連絡，詢問您是否要自

行解決問題，或是希望支援團隊協助。您可以設定 CloudWatch 警示，在發生紅色叢集狀態時通知您。

最後，紅色碎片會導致紅色叢集，而紅色索引會造成紅色碎片。若要識別造成紅色叢集狀態的索引，請使用一些 OpenSearch 有用的 API。

- `GET /_cluster/allocation/explain` 選擇第一個發現的未指派碎片，並說明為何無法將它分配到節點：

```
{
    "index": "test4",
    "shard": 0,
    "primary": true,
    "current_state": "unassigned",
    "can_allocate": "no",
    "allocate_explanation": "cannot allocate because allocation is not permitted to
 any of the nodes"
}
```

- `GET /_cat/indices?v` 顯示每個索引的良好運作狀態、文件數量和磁碟使用方式：

```
health status index            uuid                   pri rep docs.count docs.deleted
 store.size pri.store.size
green  open   test1            30h1EiMvS5uAFr2t5CEVoQ   5   0        820            0
       14mb           14mb
green  open   test2            sdIxs_WDT56afFGu5KPbFQ   1   0          0            0
       233b           233b
green  open   test3            GGRZp_TBRZuSaZpAGk2pmw   1   1          2            0
     14.7kb          7.3kb
red    open   test4            BJxfAErbTtu5HBjIXJV_7A   1   0
green  open   test5            _8C6MIXOSxCqVYicH3jsEA   1   0          7            0
     24.3kb         24.3kb
```

刪除紅色索引能以最快速度修正紅色叢集狀態。根據紅色叢集狀態的原因，接著您可能會擴展 OpenSearch Service 網域，以使用較大的執行個體類型、更多執行個體或更多 EBS 型儲存體，並嘗試重新建立有問題的索引。

若無法刪除有問題的索引，您可以還原快照、從索引刪除文件、變更索引設定、減少複本數量，或刪除其他索引以釋出更多可用磁碟空間。重要的步驟是解決紅色的叢集狀態，然後再重新設定 OpenSearch

Service 網域。重新設定具紅色叢集狀態的網域可能使問題複雜化，進而導致網域停滯在 Processing (處理中) 的設定狀態，直到您解決狀態問題為止。

紅色叢集的自動修復

如果叢集的狀態持續為紅色超過一小時， OpenSearch Service 會嘗試透過重新路由傳送未配置的碎片或從過去的快照還原來自動修復叢集。

如果無法修正一或多個紅色索引，且叢集狀態在 14 天內仍保持紅色，則只有在叢集至少符合下列其中一項條件時， OpenSearch Service 才會採取進一步的動作：

- 只有一個可用區域
- 沒有專用主節點
- 包含爆量執行個體類型 (T2 或 T3)

目前，如果您的叢集符合上述條件之一， OpenSearch Service 會在接下來的 7 天內傳送每日通知給您，說明如果您不修正這些索引，則會刪除所有未指派的碎片。如果您的叢集狀態在 21 天後仍為紅色， OpenSearch Service 會刪除所有紅色索引上未指派的碎片 (儲存區和運算)。您會在 OpenSearch Service 主控台的「通知」面板中收到這些事件的通知。如需詳細資訊，請參閱 the section called “叢集運作狀態事件”。

從持續繁重的處理負載中復原

若要判斷紅色叢集狀態是否是資料節點上的持續繁重處理負載所造成，可監控以下叢集指標。

相關指標	描述	復原
JVM MemoryPressure	指定用於叢集中所有資料節點的 Java heap 的百分比。檢視此指標的最大統計資料來獲知這項指標，並且檢視當 Java 垃圾回收器無法回收足夠記憶體，進而造成記憶體越來越小的壓力。此模式可能是因為複雜的查詢或大型資料欄位所造成。 x86 執行個體類型使用 Conconnect Mark Sweep (CMS) 廢棄項目收集器，與應用程式執行緒一起執行，將	設定 JVM 的記憶體斷路器。如需詳細資訊，請參閱 the section called “JVM OutOfMemoryError”。 如果問題仍存在，請刪除不需要的索引、減少對網域的請求數或複雜度、新增執行個體，或使用較大的執行個體類型。

相關指標	描述	復原
	暫停可能情況降到短暫。如果 CMS 在一般收集期間無法回收足夠的記憶體，會觸發完整的廢棄項目收集，導致長時間應用程式暫停和影響叢集穩定性。 ARM 型 Graviton 執行個體類型使用 Garbage-First (G1) 廢棄項目收集器，它類似於 CMS，但使用額外的短暫暫停和堆積磁碟重組，進一步減少對完整廢棄項目收集的需求。 在任何一種情況下，如果記憶體使用量持續超過記憶體回收期間可回收的記憶體回收，則會因記憶體不足錯誤而 OpenSearch 當機。在所有執行個體類型上，最好的經驗法則是將使用量保持低於 80%。 `_nodes/stats/jvm` API 提供有用的 JVM 統計資料摘要、記憶體集區使用量，以及垃圾回收資訊： `GET domain-endpoint /_nodes/stats/jvm?pretty`	
CPUUtilization	指定用於叢集中的資料節點的 CPU 資源百分比。檢視此指標的最大統計資料，尋找持續的高用量模式。	新增資料節點，或增加現有資料節點之執行個體類型的大小。
節點	指定叢集中的節點數。檢視此指標的最小統計資料。當服務為叢集部署新的執行個體時，這個值會有所變動。	新增資料節點。

黃色叢集狀態

黃色叢集狀態表示已將所有索引的主要碎片分配給叢集中的節點，但至少有一個索引的複本碎片未獲分配。單節點叢集一律以黃色叢集狀態初始化，因為沒有其他節點可 OpenSearch 供 Service 指派複本。為了達到綠色叢集狀態，請增加節點數。如需詳細資訊，請參閱 the section called “調整網域大小”。

建立新索引或發送節點故障後，多節點叢集可能會短暫呈現黃色叢集狀態。此狀態會在叢集中 OpenSearch 複寫資料時自行解析。磁碟空間不足也可能導致黃色叢集狀態；如果節點擁有容納它們的磁盤空間，叢集只能分配複本分片。

ClusterBlockException

您可能會接收到 `ClusterBlockException` 錯誤，原因如下。

缺少可用儲存空間

如果叢集中的一或多個節點的儲存空間小於 1) 20% 可用儲存空間的最小值，或 2) 20 GiB 的儲存空間，基本寫入作業 (例如新增文件和建立索引) 可能會開始失敗。 the section called “計算儲存需求”提供 OpenSearch 服務如何使用磁碟空間的摘要。

為避免發生問題，請在 OpenSearch 服務主控台中監視`FreeStorageSpace`指標，並建立 CloudWatch 警示以在`FreeStorageSpace`低於特定臨界值時觸發。 `GET /_cat/allocation?v`還提供碎片分配和磁盤使用情況的有用摘要。若要解決與儲存空間不足相關的問題，請擴展 OpenSearch Service 網域以使用較大的執行個體類型、更多執行個體或更多 EBS 型儲存。

高 JVM 記憶體壓力

當 JVM 指MemoryPressure標在 30 分鐘內超過 92% 時， OpenSearch Service 會觸發保護機制並封鎖所有寫入作業，以防止叢集達到紅色狀態。若保護已啟動，則當寫入操作失敗且出現 `ClusterBlockException` 錯誤時，新的索引將無法建立，並會擲出 `IndexCreateBlockException` 錯誤。

當 JVM MemoryPressure 測量結果返回 88% 或更低五分鐘時，會停用保護，而且會解除封鎖叢集的寫入作業。

高 JVM 記憶體壓力可能是因為叢集的請求數量猛增、節點之間的碎片配置不均衡、叢集中的碎片太多、欄位資料或索引映射激增，或無法處理傳入負載的執行個體類型所致。它也可能是由於在查詢中使用彙總、萬用字元或寬泛的時間範圍造成的。

若要減少叢集的流量並解決高 JVM 記憶體壓力問題，請嘗試執行下列其中一個或多個動作：

- 擴展網域，使每個節點的堆積大小上限為 32 GB。
- 透過刪除舊的或未使用的索引來減少碎片數量。
- 使用 `POST index-name/_cache/clear?fielddata=true` API 操作清除資料快取。請注意，清除快取可能會中斷進行中的查詢。

一般而言，為了避免將來出現高 JVM 記憶體壓力，請遵循下列最佳實務：

- 避免彙總文字欄位，或將您的索引的映射類型變更為 `keyword`。
- 透過選擇正確的碎片數量來優化搜尋和索引請求。
- 設定索引狀態管理 (ISM) 政策以定期移除未使用的索引。

在待命狀態下移轉至異地同步備份

在待命狀態下將現有網域移轉至異地同步備份時，可能會發生下列問題。

在從不待命的網域移轉至待命狀態的網域期間建立索引、索引範本或 ISM 原則

如果您在將異地同步備份網域 (不含待命) 移轉至具備待命狀態的同時建立索引，且索引範本或 ISM 政策未遵循建議的資料複製準則，這可能會造成資料不一致，且移轉可能會失敗。若要避免此情況，請建立具有三個之倍數之資料副本計數 (包括主要節點和複本) 的新索引。您可以使用 API 檢查遷移進度`DescribeDomainChangeProgress`。如果您遇到複本計數錯誤，請修正錯誤，然後聯絡 Sup AWS port 人員以重試移轉。

資料複本數量不正確

如果您的網域中沒有正確數量的資料複本，則透過待命方式移轉至異地同步備份將會失敗。

JVM OutOfMemoryError

JVM `OutOfMemoryError` 通常表示達到以下其中一個 JVM 斷路器。

斷路器	描述	叢集設定屬性
上層中斷器	可用於所有斷路器的 JVM 堆積記憶體總百分比。預設值為 95%。	`indices.breaker.total.limit`
欄位資料中斷器	可讓 JVM 堆積記憶體將單一資料欄位載入到記憶體的百分比。預設值為 40%。如果您上傳具大型欄位的資料，您可能需要提高此限制。	`indices.breaker.fielddata.limit`
請求中斷器	允許資料結構用於回應的服務請求的 JVM 堆積記憶體百分比。預設值為 60%。如果您的服務請求涉及計算彙總，您可能需要提高此限制。	`indices.breaker.request.limit`

叢集節點失敗

Amazon EC2 執行個體可能遇到意外終止和重新啟動。 OpenSearch 服務通常會為您重新啟動節點。不過， OpenSearch叢集中的一或多個節點可能會維持失敗狀態。

若要檢查此狀況，請在 OpenSearch Service 主控台上開啟您的網域儀表板。前往 Cluster health (叢集運作狀態) 標籤，然後找到 Total nodes (總節點) 指標。查看回報節點數是否少於您為叢集設定的數量。如果指標顯示一個或多個節點未運作一天以上，請聯絡 AWS 支援。

您也可以設定 CloudWatch 警示，在發生此問題時通知您。

> **Note**
>
> 叢集組態變更以及服務的例行維護期間，總節點指標不準確。此行為在預期當中。該指標很快就會報告正確的叢集節點數量。如需進一步了解，請參閱the section called “組態變更”。

若要保護叢集免於非預期的節點終止和重新啟動，請為 OpenSearch Service 網域中的每個索引建立至少一個複本。

超出最大碎片限制

OpenSearch 以及 7. x 個版本的彈性搜尋具有每個節點不超過 1,000 個碎片的預設設定。OpenSearch/Elasticsearch 會擲回錯誤，如果要求 (例如建立新索引) 會造成您超過此限制。如果您遇到此錯誤，您有幾個選項：

- 將更多資料節點新增至叢集。
- 增加 `_cluster/settings/cluster.max_shards_per_node` 設定。
- 使用 _shrink API 來減少節點上的碎片數目。

網域卡在處理狀態

當您的 OpenSearch 服務域在配置更改中間時進入「處理中」狀態。當您啟動組態變更時，網域狀態會變更為「處理中」，而 OpenSearch 服務會建立新的環境。在新環境中， OpenSearch Service 會啟動一組新的適用節點 (例如資料、主節點或 UltraWarm)。遷移完成後，舊節點將會終止。

如果發生下列其中一種情況，叢集可能會卡在「處理中」狀態：

- 一組新的資料節點無法啟動。

- 將碎片遷移至新的資料節點集不成功。
- 驗證檢查失敗並顯示錯誤。

如需每種情況的詳細解決步驟，請參閱為什麼我的 Amazon OpenSearch 服務網域卡在「處理中」狀態？ 。

低 EBS 爆量餘額

OpenSearch 當您其中一個一般用途 (SSD) 磁碟區上的 EBS 突發平衡低於 70% 時，服務會傳送主控台通知給您，如果餘額低於 20%，則會向您傳送後續通知。若要解決此問題，您可以縱向擴展叢集，或減少讀取和寫入 IOPS，以便記入爆量餘額。對於具有 gp3 磁碟區類型的網域，以及具有磁碟區大小高於 1000 GiB 之 gp2 磁碟區的網域，爆量餘額會保持在 0。如需詳細資訊，請參閱一般用途 SSD 磁碟區 (gp2)。您可以使用`BurstBalance` CloudWatch 指標監視 EBS 突發平衡。

無法啟用稽核日誌

當您嘗試使用 OpenSearch 服務主控台啟用稽核記錄檔發佈時，可能會遇到下列錯誤：

為 CloudWatch 日誌日誌群組指定的資源存取政策未授予 Amazon Ser OpenSearch vice 建立日誌串流的足夠許可。請檢查資源存取政策。

如果您遇到此錯誤，請確認政策的 `resource` 元素包含正確的日誌群組 ARN。如果有，請遵循以下步驟：

1. 等候幾分鐘。
2. 在 Web 瀏覽器中重新整理該頁面。
3. 選擇 Select existing group (選擇現有群組)。
4. 對於 Existing log group (現有日誌群組)，選擇您在收到錯誤訊息之前建立的日誌群組。
5. 在存取政策區段中，選擇 Select existing policy (選取現有政策)。
6. 對於 Existing policy (現有政策)，選擇您在收到錯誤訊息之前建立的政策。
7. 選擇 啟用 。

如果在重複此程序數次後仍然存在錯誤，請連絡 AWS Support。

無法關閉索引

OpenSearch 服務僅支援彈性搜尋 7.4 OpenSearch 及更新版本的 `_close`API。如果正在使用較舊版本並從快照中恢復索引，您可以刪除現有索引 (在重新編製索引前後)。

用戶端授權檢查

Logstash 和 Beats 的預設發行版包含專有授權檢查，且無法連線至的開放原始碼版本。 OpenSearch 確保您使用這些客戶端的 Apache 2.0（OSS）發行版與服 OpenSearch 務。

請求調節

如果您收到持續的 `403 Request throttled due to too many requests` 或 `429 Too Many Requests` 錯誤，請考慮垂直擴展。如果有效負載會導致記憶體使用量超過 Java 堆積的大小上限，Amazon OpenSearch 服務會節流請求。

無法對節點執行 SSH

您無法使用 SSH 存取 OpenSearch 叢集中的任何節點，也無法直接修改`opensearch.yml`。請改為使用主控 AWS CLI台或 SDK 來設定您的網域。您也可以使用 OpenSearch REST API 指定一些叢集層級設定。若要進一步了解，請參閱 Amazon OpenSearch 服務 API 參考和the section called “受支援的操作”.

如果您需要更深入了解叢集的效能，可以將錯誤記錄和緩慢記錄檔發佈到 CloudWatch.

「無效的物件存放區類別」快照錯誤

OpenSearch 服務快照不支援 S3 Glacier 儲存類別。如果您的 S3 儲存貯體所包含的生命週期規則將物件轉換為 S3 Glacier 儲存類別，當您嘗試列出快照時，您可能遇到此錯誤。

如果您需要從儲存貯體還原快照，請從 S3 Glacier 中還原物件，將物件複製到新的儲存貯體，以及將新的儲存貯體註冊為快照儲存庫。

無效主機標頭

OpenSearch 服務要求用戶端`Host`在要求標頭中指定。有效的 `Host` 值是不含 `https://` 的網域端點，例如：

```
Host: search-my-sample-domain-ih2lhn2ew2scurji.us-west-2.es.amazonaws.com
```

如果您在提出要求時收到`Invalid Host Header`錯誤訊息，請檢查您的用戶端或 Proxy 是否在`Host`標頭中包含 OpenSearch 服務網域端點 (而非其 IP 位址)。

無效的 M3 執行個體類型

OpenSearch 服務不支援將 M3 執行個體新增或修改至執行中的現有網域 OpenSearch 或 Elasticsearch 6.7 及更新版本。您可以繼續搭配 Elasticsearch 6.5 或較舊版本使用 M3 執行個體。

建議您選擇較新的執行個體類型。執行彈性搜尋 6.7 OpenSearch 或更新版本的網域適用下列限制：

- 如果現有網域不使用 M3 執行個體，則無法再變更為它們。
- 如果您將現有網域從 M3 執行個體類型變更為其他執行個體類型，則無法切換回原本的執行個體類型。

啟用後熱查詢停止工作 UltraWarm

當您在網域 UltraWarm 上啟用時，如果設定沒有預先存在的覆寫， OpenSearch Service 會自動將值`search.max_buckets`設定為，以`10000`防止大量記憶體的查詢飽和暖節點。如果您的熱查詢使用的值區超過 10,000 個，則啟用時可能會停止運作 UltraWarm。

由於 Amazon Ser OpenSearch vice 的受管性質，您無法修改此設定，因此您需要開啟支援案例來增加限制。增加限制不需要高級支援訂閱。

升級後無法降級

就地升級是無法復原的作業，但您仍可連絡 AWS 支援；支援人員可協助您在新網域上還原自動、預先升級的快照。例如，如果您將網域從 Elasticsearch 5.6 升級到 6.4 版，Sup AWS port 可協助您在新的彈性搜尋 5.6 網域上還原升級前快照。如果已經製作原有網域的手動快照，則您可以自行執行該步驟。

需要所有 AWS 區域的網域摘要

下列指令碼使用 Amazon EC2 描述區域 AWS CLI 命令來建立可提 OpenSearch 供服務的所有區域清單。然後它list-domain-names要求每個區域：

```
for region in `aws ec2 describe-regions --output text | cut -f4`
do
    echo "\nListing domains in region '$region':"
    aws opensearch list-domain-names --region $region --query 'DomainNames'
done
```

接著，您會收到下列個別區域的輸出：

```
Listing domains in region:'us-west-2'...
[
  {
    "DomainName": "sample-domain"
  }
]
```

OpenSearch 服務無法使用的區域會傳回「無法連線到端點 URL」。

使用 OpenSearch 儀表板時出錯瀏覽器

當您使用儀表板檢視 Service 網域中的資料時，瀏覽器會在 HTTP 回應物件中封裝 OpenSearch 服務錯誤訊息。您可以使用 Web 瀏覽器中的常用開發人員工具，例如 Chrome 中的開發人員模式，來檢視基本服務錯誤和協助您的偵錯工作。

若要檢視 Chrome 中的服務錯誤

1. 從 Chrome 頂部選單列中，選擇 View (檢視)、Developer (開發人員)、Developer Tools (開發人員工具)。
2. 選擇網路標籤。
3. 在 Status (狀態) 欄中，選擇任何狀態為 500 的 HTTP 工作階段。

若要檢視 Firefox 中的服務錯誤

1. 從選單中，選擇 Tools (工具)、Web Developer (Web 開發人員)、Network (網路)。
2. 選擇狀態為 500 的任何 HTTP 工作階段。
3. 選擇 Response (回應) 索引標籤，以檢視服務回應。

節點碎片和儲存扭曲

節點碎片扭曲是指叢集中的一個或多個節點具有比其他節點更多的碎片。節點儲存扭曲是指叢集中的一個或多個節點具有比其他節點更多的儲存空間 (`disk.indices`)。雖然這兩種情況都可能暫時發生，例如當網域已替換節點並仍對其分配碎片，如果它們持續存在，則應進行解決。

若要識別這兩種類型的扭曲，請執行 _cat/allocation API 操作並比較回應中的 `shards` 和 `disk.indices` 條目：

```
shards    | disk.indices  | disk.used  | disk.avail   | disk.total   | disk.percent |
host     | ip       | node
   264    |      465.3mb  |   229.9mb  |      1.4tb   |      1.5tb   |            0 |
 x.x.x.x  | x.x.x.x  | node1
   115    |        7.9mb  |    83.7mb  |     49.1gb   |     49.2gb   |            0 |
x.x.x.x  | x.x.x.x  | node2
   264    |      465.3mb  |   235.3mb  |      1.4tb   |      1.5tb   |            0 |
 x.x.x.x  | x.x.x.x  | node3
   116    |        7.9mb  |    82.8mb  |     49.1gb   |     49.2gb   |            0 |
x.x.x.x  | x.x.x.x  | node4
```

```
    115     |        8.4mb   |      85mb   |     49.1gb    |     49.2gb    |           0 |
 x.x.x.x   | x.x.x.x   | node5
```

雖然一些儲存扭曲是正常的，但超過平均值 10% 需引起注意。當碎片分配扭曲時，CPU、網絡和磁碟頻寬使用率也可能會變得扭曲。由於更多的資料通常意味著更多的索引和搜尋操作，負載最重的節點也往往是資源最緊張的節點，而負載較輕的節點表示未充分利用的容量。

修補：使用數倍於資料節點計數的碎片計數，以確保每個索引均勻分佈在資料節點間。

索引碎片和儲存扭曲

索引碎片扭曲是指一個或多個節點比其他節點持有更多的索引碎片。索引儲存扭曲是指一個或多個節點持有不成比例的大量索引總儲存空間。

索引扭曲比節點扭曲更難識別，因為它需要對 _cat/shards API 輸出結果進行一些處理。如果叢集或節點指標中出現一些扭曲跡象，請調查索引扭曲。以下是索引扭曲的常見跡象：

- 在資料節點的子集上發生 HTTP 429 錯誤
- 跨資料節點的索引或搜尋操作佇列不均勻
- 資料節點間的 JVM 堆積和/或 CPU 利用率不均勻

修補：使用數倍於資料節點計數的碎片計數，以確保每個索引均勻分佈在資料節點間。如果您仍然看到索引儲存或碎片偏斜，則可能需要強制執行碎片重新分配，這會在 Service 網域的每個藍/綠部署時發生。 OpenSearch

在選取 VPC 存取後未經授權的操作

使用 OpenSearch 服務主控台建立新網域時，您可以選取 VPC 或公用存取。如果您選取 VPC 存取，則 OpenSearch 服務會查詢 VPC 資訊，如果您沒有適當的權限，則會失敗：

```
You are not authorized to perform this operation. (Service: AmazonEC2; Status Code:
 403; Error Code: UnauthorizedOperation
```

若要啟用此查詢，您必須有權存取 `ec2:DescribeVpcs`、`ec2:DescribeSubnets` 及 `ec2:DescribeSecurityGroups` 操作。此需求僅適用於主控台。如果您使用 AWS CLI 建立和設定具有 VPC 端點的網域，則不需要存取這些作業。

在建立 VPC 網域後載入停滯

建立使用 VPC 存取的新網域後，網域的 Configuration state (組態狀態) 的進度可能永不會超出 Loading (載入)。如果發生此問題，表示您的地區可能已停用 AWS Security Token Service (AWS STS)。

若要將 VPC 端點新增至您的 VPC， OpenSearch 服務需要擔任該`AWSServiceRoleForAmazonOpenSearchService`角色。因此， AWS STS 必須啟用才能建立在指定區域中使用 VPC 存取權的新網域。若要進一步了解啟用和停用 AWS STS，請參閱 IAM 使用者指南。

拒絕對 OpenSearch API 的要求

隨著 OpenSearch API 引入基於標籤的訪問控制，您可能會開始看到以前沒有訪問被拒絕的錯誤。這可能是因為您的一或多個存取政策包含使用 `ResourceTag` 條件的 `Deny`，且目前遵守這些條件。

例如，以下政策僅用於網域具有標籤 `environment=production` 時，拒絕從組態 API 存取 `CreateDomain` 動作。即使動作清單同時包含 `ESHttpPut`，拒絕陳述式也不會套用於該動作或任何其他 `ESHttp*` 動作。

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Action": [
      "es:CreateDomain",
      "es:ESHttpPut"
    ],
    "Effect": "Deny",
    "Resource": "*",
    "Condition": {
      "ForAnyValue:StringEquals": {
        "aws:ResourceTag/environment": [
          "production"
        ]
      }
    }
  }]
}
```

增加了對 OpenSearch HTTP 方法標籤的支援，如上所述的 IAM 身分型政策將導致附加的使用者遭到拒絕存取動作。`ESHttpPut`之前在沒有標籤驗證的情況下，連接的使用者仍可傳送 PUT 請求。

如果您在將網域更新至服務軟體 R20220323 或更新版本後，開始看到存取遭拒錯誤，請查看身分型存取政策，了解是否是這種情況，並在必要時加以更新以允許存取。

無法從 Alpine Linux 連線

Alpine Linux 會將 DNS 回應大小限制在 512 位元組。如果您嘗試從阿爾派 Linux 3.18.0 或更低版本連線到您的 OpenSearch 服務網域，如果該網域位於 VPC 人雲端中且有超過 20 個節點，則 DNS 解析可能會失敗。如果您使用的是高於 3.18.0 的阿爾派 Linux 版本，您應該能夠解析超過 20 台主機。如需詳細資訊，請參閱阿爾派 Linux 3.18.0 版本說明。

如果您的網域位於 VPC，我們建議使用其他 Linux 發行版本 (如 Debian、Ubuntu、CentOS、Red Hat Enterprise Linux 或 Amazon Linux 2) 來連線到該網域。

搜尋背壓要求太多

以 CPU 為基礎的許可控制是一種閘道機制，可根據節點目前的容量主動限制要求數目，包括隨機增加和流量尖峰。過多的要求會在拒絕時傳回 HTTP 429「要求過多」狀態碼。此錯誤表示叢集資源不足、資源密集型搜尋要求，或工作負載中意外的尖峰。

搜尋背壓提供拒絕的原因，可協助微調耗用大量資源的搜尋要求。對於流量尖峰，我們建議使用指數輪詢和抖動的用戶端重試。

使用開發套件時發生憑證錯誤

由於 AWS SDK 使用電腦上的 CA 憑證，因此當您嘗試使用 SDK 時， AWS 伺服器上的憑證變更可能會導致連線失敗。錯誤訊息會不同，但通常包含以下文字：

```
Failed to query OpenSearch
...
SSL3_GET_SERVER_CERTIFICATE:certificate verify failed
```

您可以保留電腦的 CA 憑證和作業系統，以防止這些失敗 up-to-date。如果您在企業環境中遇到此問題，且並無管理使用專屬的電腦，則您可能需要尋求管理員協助更新程序。

以下清單列出作業系統及 Java 版本的最低版本需求：

- 具備自 2005 年 1 月起之更新的 Microsoft Windows 版本，或更新版本 (其信任清單中需包含至少其中一項所需的 CA)。

- Mac OS X 10.4 搭配適用於 Mac OS X 10.4 發行版本 5 (2007 年 2 月) 的 Java，Mac OS X 10.5 (2007 年 10 月) 和更新版本 (其信任清單中需包含至少其中一項所需的 CA)。
- Red Hat Enterprise Linux 5 (2007 年 3 月)、6 和 7 以及 CentOS 5、6 和 7，全部均需在其預設信任 CA 清單中包含至少其中一項所需的 CA。
- Java 1.4.2_12 (2006 年 5 月)、5 更新版本 2 (2005 年 3 月) 及所有更新版本，包括 Java 6 (2006 年 12 月)、7 和 8 (其預設信任 CA 清單中需包含至少其中一項所需的 CA)。

三個憑證授權機構如下：

- Amazon 根 CA 1
- Starfield Services 根憑證授權機構：G2
- Starfield 類別 2 憑證授權機構

前兩個授權單位的根憑證可從 Amazon 信任服務取得，但保留電腦 up-to-date 是更直接的解決方案。若要進一步了解 ACM 提供的憑證，請參閱 AWS Certificate Manager 常見問答集。

> **Note**
>
> 目前，us-east-1 區域中的 OpenSearch 服務網域使用來自不同授權單位的憑證。我們計劃更新區域，於近期使用這些新的憑證授權機構。

Amazon OpenSearch 服務的文檔歷史

本主題說明 Amazon OpenSearch 服務的重要變更。服務軟體更新會新增對新功能、安全修補程式和其他改進項目的支援。若要使用新功能，您可能需要更新網域上的服務軟體。如需詳細資訊，請參閱the section called “服務軟體更新”。

服務功能會逐步推出至可用服務的 AWS 區域 位置。我們僅針對第一個版本更新此文件。我們不會提供有關區域可用性的資訊，也不會宣布後續區域的推展情況。如需有關服務功能的區域可用性，以及訂閱更新相關通知的資訊，請參閱有什麼新功能 AWS？

此歷史記錄的相關日期：

- 目前的產品版本—2021-01-01
- 最新產品發布 — 2024 年 7 月 12 日
- 。最新的文檔更新。。- 2024 年 7 月 12 日

如需有關更新的通知，您可以訂閱RSS摘要。

> **Note**
>
> 修補程式版本：以 "-P" 和數字結尾的服務軟體版本，例如 R20211203-P4，是修補程式版本。修補程式可能包括效能改進、小錯誤修復、安全修復或狀態改善。由於修補程式不包括新功能或重大變更，因此通常不會對使用者或文件產生直接影響，這就是為什麼在此文件歷史記錄中不包含每個修補程式的詳細資訊。

變更	描述	日期
服務連結角色原則的更新	將 Sid 新增`AllowAOSSCloudwatchMetrics` 至服務連結的角色原則`AmazonOpenSearchServerlessServiceRolePolicy` 。	2024年7月12日
新的服務連結角色	Amazon Ser OpenSearch vice 新增了一個名為的服務連結角色`AWSServiceRoleFor0`	2024年6月12日

	`pensearchIngestion SelfManagedVpce` ，可讓 Amazon OpenSearch 擷取將指標資料傳送至具有自我VPC管理端點 Amazon CloudWatch 的管道。	
Amazon OpenSearch 服務與 Amazon S3 零ETL集成	Amazon OpenSearch 服務現在支持直接查詢以查詢 Amazon S3 中的數據。	2024年5月22 日
OpenSearch 技術支援	Amazon OpenSearch 服務現在支持 OpenSearch 版本 2.13。此版本包括版本 2.12 和 2.13 的所有功能。如需詳細資訊，請參閱 2.12 和 2.13 版本說明。	2024年5月21 日
資料準備器 2.7 版的 Amazon OpenSearch 擷取支援	Amazon OpenSearch 擷取新增對資料準備器 2.7 版的支援。如需詳細資訊，請參閱 2.7 版本說明。	2024年4月4日
AWS 服務 OpenSearch 無伺服器集合的私人存取	您現在可以在網路存取政策中授予特定 AWS 服務的存取權，例如 Amazon Bdrock 存取您的 OpenSearch 無伺服器集合。	2024年3月28日
就地EBS更新	您現在可以對網域進行一些EBS變更，而不需要在 Amazon OpenSearch 服務中進行藍色/綠色部署。	2024年2月14日
組態變更可見性	您現在可以在 Amazon OpenSearch 服務主控台中追蹤網域組態變更，並使用組態 API。	2024年2月6日

向量搜尋集合一般可用性	Amazon OpenSearch 無伺服器向量搜尋集合現已正式推出。在預覽階段進行以下顯著的改進： • 向量搜尋集合現在支援具有數十億個向量的工作負載，每個向量最多可達 128 個維度。 • OpenSearch 儀表板現在支援向量搜尋集合。	2023 年 11 月 29 日
OR1實例	Amazon OpenSearch 服務現在支持OR1實例類型。	2023 年 11 月 29 日
使用 Amazon S3 直接查詢 (預覽)	直接查詢提供全受管解決方案，可在將交易資料寫入 Amazon S3 儲存貯體後的幾秒鐘內即可在 Amazon OpenSearch 服務中使用。	2023 年 11 月 29 日
10 TiB 容量，適用於時間序列集合	Amazon OpenSearch 無伺服器為時間序列集合新增最多 10 TiB 索引資料的支援。此版本也支援所有類型的集合允許 OCUs的最大容量為 200，以及在建立集合時停用待命複本的功能。	2023 年 11 月 29 日
OpenSearch 技術支援	Amazon OpenSearch 服務現在支持 OpenSearch 版本 2.11。此版本包括版本 2.10 和 2.11 的所有功能。如需詳細資訊，請參閱 2.10 和 2.11 版本說明。	2023 年 11 月 17 日

資料準備器 2.6 版的 Amazon OpenSearch 擷取支援	Amazon OpenSearch 擷取新增資料準備器 2.6 版的支援。如需詳細資訊，請參閱 2.6 版本說明。此外，您可以將 Amazon DynamoDB 指定為管道來源。如需詳細資訊，請參閱搭配 Amazon DynamoDB 使用 OpenSearch 擷取管道。	2023 年 11 月 17 日
資料準備器 2.5 版的 Amazon OpenSearch 擷取支援	Amazon OpenSearch 擷取新增資料準備器 2.5 版的支援。如需詳細資訊，請參閱 2.5 版本說明。此外，您現在可以將 Ser OpenSearch vice 網域或 OpenSearch 無伺服器集合指定為管線來源。如需詳細資訊，請參閱「資料預留程式」文件中的OpenSearch 來源外掛程式。	2023 年 11 月 17 日
CloudFormation 遠端推論的範本	為了簡化語義搜尋的遠端推論設定，Amazon Ser OpenSearch vice 在主控台中提供了一個 AWS CloudFormation 範本，為您自動化模型佈建程序。	2023 年 11 月 7 日
服務連結角色原則的更新	新增服務連結角色原則所需的權限，`AmazonOpenSearchServiceRolePolicy` 以指派和取消IPv6指派位址。已取代的 Elasticsearch 政策也`AmazonElasticsearchServiceRolePolicy` 已更新，以確保向後相容性。	2023 年 10 月 26 日

Amazon OpenSearch 無伺服器生命週期政策	Amazon OpenSearch 無伺服器引入索引生命週期政策，以簡化資料保留和刪除的管理。您現在可以在主控台中使用APIs或設定介面來設定時間序列集合的資料保留原則，無需建立每日索引或指令碼來刪除舊資料。	2023 年 10 月 25 日
支援執行個體	Amazon OpenSearch 服務現在支持 IM4GN 實例類型。IM4GN 執行個體已針對管理大型資料集且每 v 需要高儲存密度的工作負載進行最佳化。CPU	2023 年 10 月 20 日
管理選項	Amazon Ser OpenSearch vice 現在提供多個管理選項，如果您需要對網域的問題進行疑難排解，可提供精細的控制。這些選項包括在資料節點上重新啟動 OpenSearch 處理序的功能，以及重新啟動資料節點的能力。	2023 年 10 月 17 日
可選插件	Amazon OpenSearch 服務增加了對四種新語言分析器插件的支持：紫菜（韓語），Sudachi（日語），拼音（中文）和STConvert分析（中文）以及 Amazon Personalize 化搜索排名插件。	2023 年 10 月 16 日

OpenSearch 2.9 支援服務	Amazon OpenSearch 服務現在支持 2.9 OpenSearch 版本。此版本包含屬於 2.8 和 2.9 版本的所有功能。如需詳細資訊，請參閱 2.8 和 2.9 版本說明。	2023 年 10 月 2 日
ML 連接器	Amazon OpenSearch 服務新增了對機器學習 (ML) 連接器的支援。連接器有助於存取其他 AWS 服務或協力廠商機器學習 (ML) 平台上託管的 ML 模型。	2023 年 9 月 6 日
Amazon OpenSearch 擷取新增對資料準備器 2.4 版的支援	Amazon OpenSearch 擷取新增對資料準備器 2.4 版的支援。如需詳細資訊，請參閱 2.4 版本說明。此外，您現在可以將 Amazon Managed Streaming for Apache Kafka (AmazonMSK) 指定為管道來源。	2023 年 8 月 31 日
6 TiB 容量，適用於時間序列集合	Amazon OpenSearch 無伺服器為時間序列集合新增最多 6 TiB 索引資料的支援。此版本也支援搜尋和時間序列集合的允許容量上限OCUs為 100。	2023 年 8 月 15 日
向量搜尋集合	Amazon OpenSearch Serverless 新增建立向量搜尋集合的選項，您可以使用這個選項來儲存向量嵌入，以支援相似性和語意搜尋。	2023 年 7 月 26 日

OpenSearch 2.7 支援服務	Amazon OpenSearch 服務現在支持 2.7 OpenSearch 版本。此版本包含屬於版本 2.6 和 2.7 的所有功能。如需詳細資訊，請參閱 2.6 和 2.7 版本說明。	2023 年 7 月 10 日
資料預留程式 2.3 支援	Amazon OpenSearch 擷取新增支援資料準備器 2.3 版本。如需詳細資訊，請參閱 2.3 版本說明。此外，您現在可以將 Amazon 安全湖指定為管道來源。	2023 年 6 月 26 日
異地同步備份含待機	Amazon Ser OpenSearch vice 新增了跨三個可用區域部署網域的選項 (AZs)，每個可用區域包含完整的資料副本，其中一個節點則AZs充當待命區域。具備待命部署選項的異地同步備份可在基礎架構故障時提供 99.99% 的可用性和一致的效能。	2023 年 5 月 3 日
新的服務連結角色	Amazon OpenSearch 服務新增了一個名為的服務連結角色`AWSServiceRoleForAmazonOpenSearchIngestionService`，可讓 Amazon OpenSearch 擷取將指標資料傳送到。 Amazon CloudWatch	2023年4月26日

Amazon OpenSearch 攝入	Amazon OpenSearch Intetion 是全受管的資料收集器，可將即時日誌和追蹤資料傳遞至 OpenSearch 服務網域和 OpenSearch 無伺服器集合。OpenSearch 擷取讓您無需使用第三方解決方案 (例如 Logstash 或 Jaeger)，將資料導入您的網域和集合。	2023年4月26日
OpenSearch 2.5 支援服務	Amazon OpenSearch 服務現在支持 2.5 OpenSearch 版本。此版本包含屬於 2.4 和 2.5 版本的所有功能。如需詳細資訊，請參閱 2.4 和 2.5 版本說明。	2023 年 3 月 13 日
離峰維護窗	Amazon Ser OpenSearch vice 新增離峰時段，這是每天 10 小時、低流量的時間區塊，在此期間，可以排程需要藍/綠部署的服務軟體更新和自動調整最佳化。離峰更新有助於將叢集專用主節點在高流量期間的壓力降至最低。 對於 2 月 16 日之後建立的新網域，離峰時段會自動設定為當地時間晚上 10:00 到上午 8:00 之間。對於現有網域，您必須明確啟用視窗。	2023 年 2 月 16 日
在網域建立期間設定SAML驗證	Amazon OpenSearch 服務現在支援在網域建立期間設定SAML身份驗證。先前，您必須在建立網域之後設定SAML選項。	2023 年 2 月 1 日

網域的遠端重新索VPC引	Amazon OpenSearch 服務為兩個域之間的VPC端點連接添加了選項。您現在可以使用遠端重新索引將索引從一個VPC網域複製到另一個網域，而不需要反向 Proxy。您的VPC網域必須執行服務軟體R20221114 或更新版本，才能使用此功能。	2023 年 1 月 31 日
Amazon OpenSearch 無伺服器一般可用	Amazon OpenSearch 無伺服器現已正式推出。在預覽階段進行以下顯著的改進： • 當收集端點上的流量減少OCUs時，容量現在可以縮減到設定的最小值。 • 索引和搜OCUs索允許的最大值從 20 增加到 50。每個都OCU包含足夠的熱暫時儲存，可容納 120 GiB 的索引資料。 • 您現在可以在建立集合時設定資料存取設定，而不必在單獨的工作流程中進行設定。	2023 年 1 月 25 日
非同步試轉	Amazon Ser OpenSearch vice 現在支援非同步乾執行，可讓您在變更組態之前執行驗證檢查，並通知您變更是否會導致藍/綠部署。	2023 年 1 月 19 日

新的服務連結角色	Amazon Ser OpenSearch vice 新增了一個名為的服務連結角色`AWSServiceRoleForAmazonOpenSearchServerless` ，可讓 OpenSearch 無伺服器將指標資料傳送至。Amazon CloudWatch	2022 年 11 月 29 日
Amazon OpenSearch 無伺服器預覽	Amazon OpenSearch 無伺服器是適用於 Amazon OpenSearch 服務的隨需、auto 擴展、無伺服器組態。無伺服器可免除佈建、設定和調整叢集的作業複雜性。OpenSearch	2022 年 11 月 29 日
OpenSearch 2.3 技術支援	Amazon OpenSearch 服務現在支持 2.3 OpenSearch 版本。此版本包含屬於 2.0、2.1 和 2.2 版的所有功能。如需詳細資訊，請參閱 2.0、2.1、2.2 和 2.3 版本備註。2.3 版包含突破性變更。如需詳細資訊，請參閱支援的升級路徑。	2022 年 11 月 15 日
支援通知外掛程式	Amazon OpenSearch 服務現在支援通知外掛程式，該 OpenSearch 外掛程式可為您的所有通知提供集中位置。從 2.0 版開始，提醒目的地已棄用，並由通知頻道取代。	2022 年 11 月 15 日

支援 Kibana 7.1.1	執行 Elasticsearch 7.1 的 Amazon OpenSearch 服務網域現在支援 Kibana 7.1.1 的最新修補程式版本，可新增錯誤修正並改善安全性。當您將 7.1 網域更新為服務軟體 R20221114 時， OpenSearch 服務會自動將它們升級至此修補程式版本。	2022 年 11 月 15 日
支援 Kibana 6.8.13	執行 Elasticsearch 6.8 的 Amazon OpenSearch 服務網域現在支援 Kibana 6.8.13 的最新修補程式版本，可新增錯誤修正並改善安全性。當您將 6.8 網域更新為服務軟體 R20221114 時， OpenSearch 服務會自動將其升級至此修補程式版本。	2022 年 11 月 15 日
支援 Kibana 6.3.2	執行 Elasticsearch 6.3 的 Amazon OpenSearch 服務網域現在支援 Kibana 6.3.2 的最新修補程式版本，可新增錯誤修正並提高安全性。當您將 6.3 網域更新為服務軟體 R20221114 時， OpenSearch 服務會自動將它們升級至此修補程式版本。	2022 年 11 月 15 日

AWS PrivateLink	使用 Amazon Service OpenSearch 受管VPC端點，您可以使用界面端VPC點直接連接到 OpenSearch 服務網VPC域，而不是透過網際網路連線。 OpenSearch 服務管理的VPC端點只能在佈建端點的VPC位置內存取，或從佈建端VPCs點位VPC置的任何對等端點存取 (如路由表和安全群組允許)。您的VPC網域必須執行服務軟體 R20220928 或更新版本，才能連線到介面VPC端點。	2022 年 11 月 7 日
錯誤修正與效能改進	服務軟體 R20220928 包含錯誤修正和效能增強功能，包括改良的SAML記錄功能。此更新也會將預設租用戶變更為 `Global` 而非 `Private`。	2022 年 10 月 3 日
改進的API參考	Amazon OpenSearch 服務提供改進的全方位組態參考。API 新的參考資料包含所有可用的動作和資料類型、範例要求和回應語法，以及所有支援語言之對應SDK參考的連結。	2022 年 9 月 13 日
藍/綠驗證	Amazon Ser OpenSearch vice 現在會在藍/綠部署之前執行驗證檢查，如果您的網域不符合更新資格，則會顯示驗證錯誤。	2022 年 8 月 16 日

OpenSearch 1.3 技術支援	Amazon OpenSearch 服務現在支持 1.3 OpenSearch 版本。如需詳細資訊，請參閱 1.3 版本備註。	2022 年 7 月 27 日
支援 ML Commons 外掛程式	Amazon Ser OpenSearch vice 增加了對 ML Commons 外掛程式的支援，該外掛程式可透過傳輸和RESTAPI呼叫提供一組常見的機器學習演算法。您還可以通過PPL命令與 ML 共享資源插件進行交互。	2022 年 7 月 27 日
支援 gp3 磁碟區	Amazon OpenSearch 服務增加了對gp3EBS一般用途SSD磁碟區類型的支援。您可以在建立或修改網域時指定其他佈建IOPS和輸送量。	2022 年 7 月 26 日
增強型最佳實務文件	Amazon OpenSearch 服務文件提供改良的營運最佳實務，以及建立和操作 OpenSearch 服務網域的一般建議。	2022 年 7 月 6 日
與 Service Quotas 整合	您現在可以從 Ser OpenSearc h vice Quotas 主控台檢視 Amazon 服務的配額，並請求增加配額。	2022 年 6 月 29 日
以標籤為基礎的存取控制 OpenSearch API	您現在可以使用標籤來控制對 OpenSearch APIs. 以前，您只能使用標籤來控制對配置的存取API。	2022 年 6 月 16 日

區域間跨叢集搜尋	現在只要兩個網域都執行 Elasticsearch 7.10 版或更新版本，或是任何版本的，就能支援跨叢集搜尋。 AWS 區域 OpenSearch	2022 年 6 月 14 日
支援單一 Kibana 5.6	Amazon OpenSearch 服務增加了對單 Kibana 的支持 5.6.16. 藉助單一 Kibana 5.6.16，您可以將 Kibana 5.6 做為您的前端，同時連接至 Elasticsearch 版本 5.1、5.3、5.5 和 5.6。您必須使用服務軟體 R20220323 或更新版本，才能使用單一 Kibana 5.6。	2022 年 4 月 4 日
R20220323-P1	Amazon OpenSearch 服務最近發布了服務軟件更新 R20220323，但由於出現問題，更新隨後被回滾。我們建議您將網域更新至修補程式版本 R20220323-P1 或更新版本，以解決此問題。	2022 年 4 月 4 日
OpenSearch 1.2 技術支援	Amazon OpenSearch 服務現在支持 1.2 OpenSearch 版本。如需詳細資訊，請參閱 1.2 版本備註。	2022 年 4 月 4 日

可觀測性	Amazon Ser OpenSearch vice 的預設 OpenSearch 儀表板安裝包括可觀察性外掛程式，您可以使用管道處理語言 (PPL) 將資料導向的事件視覺化，以探索和查詢資料。該插件需要 OpenSearch 1.2 或更高版本以及服務軟件 R20220323 或更高版本。	2022 年 4 月 4 日
支援 Kibana 7.7.1	執行 Elasticsearch 7.7 的 Amazon OpenSearch 服務網域現在支援 Kibana 7.7 的最新修補程式版本，可新增錯誤修正並改善安全性。當您將 7.7 網域更新為服務軟體 R20220323 或更新版本時，OpenSearch 服務會自動將它們升級至此修補程式版本。	2022 年 4 月 4 日
JVM記憶體壓力指標變更	Amazon OpenSearch 服務變更了`JVMMemoryPressure` CloudWatch 指標的邏輯，以更準確地反映記憶體使用率。之前，指標只會考慮JVM堆積的舊一代記憶體集區。經由此變更，該指標亦會考慮新世代記憶體集區。將網域更新為服務軟體 R20220323 後，您可能會看到 `JVMMemoryPressure` 、`MasterJVMMemoryPressure` 及/或 `WarmJVMMemoryPressure` 指標有所增加。	2022 年 4 月 4 日

自訂字典搭配 IK (中文) 分析外掛程式	Amazon OpenSearch 服務現在支援搭配 IK (中文) 分析外掛程式使用自訂字典。	2022 年 4 月 4 日
現有網域上的跨叢集複寫	Amazon Ser OpenSearch vice 取消了您只能在 2020 年 6 月 3 日或之後建立的網域上實作跨叢集搜尋和跨叢集複寫的限制。現在，不論網域是在何時建立，您都能在所有網域上啟用這些功能。兩個網域都必須位於服務軟體 R20220323 或更新版本上。	2022 年 4 月 4 日
藍/綠部署可見性	Amazon OpenSearch 服務現在提供更多藍/綠部署進度的可見性。您可以在控制台中或使用配置監視這些詳細信息API。	2022 年 1 月 27 日
現有網域上的精細存取控制	您現可在現有網域上啟用精細存取控制。您可以啟用開放/IP 型存取政策的臨時遷移期，以確保使用者在您建立和映射角色時可以繼續存取您的網域。若要在現有網域上啟用精細存取控制，則需使用服務軟體 R20211203 或更新版本。	2022 年 1 月 6 日

重新命名 OpenSearch 儀表板	使用服務軟體 R20211203，`kibana_user` 角色已重新命名為 `opensearch_dashboards_user`，`kibana_read_only` 已重新命名為 `opensearch_dashboards_read_only`。此變更適用於所有新建立的 OpenSearch 1。x 網域名稱。對於升級為服務軟體 R20211203 的現有 OpenSearch 網域，角色保持不變。	2022 年 1 月 4 日
OpenSearch 1.1 支援服務	Amazon OpenSearch 服務現在支持 1.1 OpenSearch 版本。如需詳細資訊，請參閱 1.1 版本備註。	2022 年 1 月 4 日
ISM可視化編輯	Amazon OpenSearch 服務的預設 OpenSearch 儀表板安裝現在支援ISM政策的視覺化編輯器。此功能需要 OpenSearch 1.1 或更新版本。	2022 年 1 月 4 日
跨服務混淆代理人預防更新	Amazon Ser OpenSearch vice 支援在IAM資源政策中使用`aws:SourceArn` 和`aws:SourceAccount` 全域條件上下文金鑰，以防止混淆的副問題。您必須位於服務軟體 R20211203 或更新版本上，才能使用這些條件索引鍵。	2022 年 1 月 4 日

Log4j 修補程式	服務軟體 R20211203-P2 會根據建議的建議，更新「OpenSearch 服務中使用」中使用的 Log4j 版本CVE。CVE此修補程式適用於執行所有版本 OpenSearch 和彈性搜尋的網域。 OpenSearch 服務將繼續在內部更新各種 Log4j 版本，並且它們不一定被限制為 Log4j 的最新版本。您網域上的 Log4j 版本取決於網域執行的軟體版本。不過，無論 Log4j 版本為何，只要您執行的是 R20211203-P2 或更新版本，您的網域都會包含處理 -2021-44228 和 CVE -2021-45046 所需的 Log4j 更新。CVE	2021 年 12 月 15 日
跨叢集複寫	跨叢集複寫可讓您將索引、對應和中繼資料從一個 OpenSearch 服務網域複寫到另一個服務網域。跨叢集複寫需要執行彈性搜尋 7.10 或 1.1 或 OpenSearch 更新版本的網域。	2021 年 10 月 5 日
新的 AWS受管原則	Amazon OpenSearch 服務的推出包括新的 AWS託管政策和舊政策的棄用。	2021 年 9 月 8 日

支援 Kibana 6.4.3	執行舊版 Elasticsearch 6.4 版的 Amazon OpenSearch 服務網域現在支援 Kibana 6.4 的最新修補程式版本，可新增錯誤修正並提高安全性。OpenSearch 服務會自動將網域升級至此修補程式版本。	2021 年 9 月 8 日
資料串流	Amazon Ser OpenSearch vice 增加了對資料串流的支援，簡化了時間序列資料的管理程序。您的網域必須執行 OpenSearch 1.0 或更新版本才能使用資料串流。	2021 年 9 月 8 日
Amazon OpenSearch 服務	AWS 重命名 Amazon OpenSearch 服務以刪除傳統的「彈性搜索」品牌。Amazon OpenSearch 服務支持 OpenSearch 和傳統的彈性搜索OSS。建立叢集時，您可以選擇要使用的搜尋引擎。OpenSearch 服務提供了與軟件的最終開源版本 Elasticsearch OSS 7.10 廣泛的兼容性。	2021 年 9 月 8 日
冷儲存	冷儲存是用於不常存取的資料或歷史資料的新儲存層。冷索引僅佔用 S3 儲存體，並且沒有連接任何運算。冷存儲需要一個執行 Elasticsearch 7.9 或更新版本的網域以及服務軟體 R20210426 或更新版本。	2021 年 5 月 13 日

ARM以重力彈為基礎的例證	Amazon OpenSearch 服務現在支援ARM以重力彈為基礎的執行個體類型 (M6G、C6G、R6G 和 R6GD)。Graviton 執行個體類型適用於執行 Elasticsearch 7.9 或更新版本的新網域和現有網域，以及服務軟件 R20210331 或更新版本。	2021 年 5 月 4 日
ISM模板	Amazon Ser OpenSearch vice 新增了對ISM範本的支援，如果索引符合ISM政策中定義的模式，可讓您自動將政策附加到索引。ISM範本需要服務軟體 R20210426 或更新版本。此更新也會取代此`policy_id` 設定，表示您無法再使用索引範本將ISM原則套用至新建立的索引。此更新會為使用此設定的現有 CloudFormation 範本引入重大變更。	2021 年 4 月 27 日
支援 Elasticsearch 7.10	Amazon OpenSearch 服務現在支持彈性搜索版本 7.10。如需詳細資訊，請參閱 7.10 版本備註。	2021 年 4 月 21 日
非同步搜尋	Amazon OpenSearch 服務現在支援非同步搜尋，可讓您在背景執行搜尋請求。非同步搜尋需要一個執行 Elasticsearch 7.10 或更新版本的網域以及服務軟體 R20210331 或更新版本。	2021 年 4 月 21 日

組態的以標籤為基礎的存取控制 API	您現在可以使用 AWS 標籤來控制對 Amazon ES 組態的存取API。	2021 年 3 月 2 日
自動調校	Amazon Ser OpenSearch vice 新增了自動調整功能，該功能會使用叢集中的效能和使用量指標來建議節點上的JVM設定變更。自動調整需要一個執行 Elasticsearch 6.7 或更新版本的網域以及服務軟體 R20201117 或更新版本。	2021 年 2 月 24 日
Trace Analytics	Amazon OpenSearch 服務專用 Kibana 的預設安裝現在包含追蹤分析外掛程式，可讓您監控來自分散式應用程式的追蹤資料。外掛程式需要一個執行 Elasticsearch 7.9 或更新版本的網域以及服務軟體 R20210201 或更新版本。	2021 年 2 月 17 日
碎片指標	Amazon OpenSearch 服務新增下列 CloudWatch 指標來追蹤碎片狀態：`Shards.active` 、、`Shards.unassigned` 、`Shards.delayedUnassigned` `Shards.activePrimary` 、`Shards.initializing` 、`Shards.relocating` 。可在執行服務軟體 R20210201 或更新版本的網域上取得這些指標。	2021 年 2 月 17 日

Kibana 報告	Amazon OpenSearch 服務的 Kibana 預設安裝現在支援探索、視覺化和儀表板頁面的隨需報告。此功能需要 Elasticsearch 7.9 或更新版本以及服務軟體 R20210201 或更新版本。	2021 年 2 月 17 日
支援 Kibana 5.6.16	執行 Elasticsearch 5.6 的 Amazon OpenSearch 服務網域現在支援 Kibana 5.6 的最新修補程式版本，可新增錯誤修正並提高安全性。Amazon ES 會自動將網域升級至此修補程式版本。	2021 年 2 月 17 日
現有網域的加密	Amazon OpenSearch 服務現在支援在執行 Elasticsearch 6.7 或更新版本的現有網域上啟用靜態資料 node-to-node加密和加密。啟用這些設定後，您便無法加以停用。	2021 年 1 月 27 日
遠端重新索引	Amazon OpenSearch 服務現在支援遠端重新索引，可讓您從遠端網域遷移索引。此功能需要服務軟體 R20201117 或更新版本。	2020 年 11 月 24 日
Piped Processing Language	Amazon OpenSearch 服務現在支援管道處理語言 (PPL)，這是一種查詢語言，可讓您使用管道 (|) 語法查詢儲存在 Elasticsearch 中的資料。此功能需要服務軟體 R20201117 或更新版本。如需進一步了解，請參閱 。	2020 年 11 月 24 日

Kibana 筆記本	Amazon Ser OpenSearch vice 新增了對 Kibana 筆記本的支援，可讓您在單一介面中結合即時視覺效果和敘述文字。此功能需要服務軟體 R20201117 或更新版本。	2020 年 11 月 24 日
甘特圖	Amazon OpenSearch 服務的 Kibana 預設安裝現在支援新的視覺化類型甘特圖。此功能需要服務軟體 R20201117 或更新版本。	2020 年 11 月 24 日
支援 Elasticsearch 7.9	Amazon OpenSearch 服務現在支持彈性搜索 7.9 版。如需詳細資訊，請參閱 7.9 版本備註。	2020 年 11 月 24 日
異常偵測更新	Amazon Ser OpenSearch vice 的異常偵測增加了對高基數的支援，可讓您使用 IP 位址、產品 ID、國家/地區代碼等維度對異常進行分類。此功能需要服務軟體 R20201117 或更新版本。	2020 年 11 月 24 日
動態字典更新	Amazon Ser OpenSearch vice 現在可讓您更新搜尋分析器，而無需重新建立索引。您可以更新部分或全部網域上的字典檔案，Amazon ES 會隨著時間追蹤套件版本，以便您擁有變更內容和變更時間的歷史記錄。此功能需要服務軟體 R20201019 或更新版本。	2020 年 11 月 17 日

自訂端點	Amazon OpenSearch 服務現在支援自訂端點，讓您為 Amazon ES 網域提供一個新的 URL。如果您曾經交換域，則可以保持相同的域URL。此功能需要服務軟體 R20201019 或更新版本。	2020 年 11 月 5 日
新的語言外掛程式	Amazon OpenSearch 服務現在可透過 R20201019 或更新版本的服務軟體，在執行 Elasticsearch 7.7 或更新版本的網域上支援 IK (中文) 分析、越南文分析和泰文分析外掛程式。	2020 年 10 月 28 日
支援 Elasticsearch 7.8	Amazon OpenSearch 服務現在支持彈性搜索 7.8 版。如需詳細資訊，請參閱 7.8 版本備註。	2020 年 10 月 28 日
SAML木花的認證	Amazon Ser OpenSearch vice 現在支援 Kibana 的身分SAML驗證，可讓您使用第三方身分供應商登入 Kibana、管理精細的存取控制、搜尋資料以及建立視覺效果。此功能需要服務軟體 R20201019 或更新版本。	2020 年 10 月 27 日
T3 執行個體	Amazon OpenSearch 服務現在支持`t3.small`和`t3.medium` 實例類型。	2020 年 9 月 23 日

稽核日誌	Amazon Ser OpenSearch vice 現在支援資料的稽核日誌，可讓您追蹤失敗的登入嘗試、使用者對索引、文件和欄位的存取權限等。此功能需要服務軟體 R20200910 或更新版本。	2020 年 9 月 16 日
UltraWarm 更新	UltraWarm 對於 Amazon Ser OpenSearch vice，則會新增新指標、新設定、更大的移轉佇列和取消API。這些更新需要服務軟體 R20200910 或更新版本。如需詳細資訊，請參閱。	2020 年 9 月 14 日
Learning to Rank	Amazon Ser OpenSearch vice 現在支援開放原始碼學習排名外掛程式，可讓您使用機器學習技術來改善搜尋相關性。此功能需要服務軟體 R20200721 或更新版本。	2020 年 7 月 27 日
k-NN 餘弦相似度	除了歐幾里德距離外，K 近鄰 (k-NN) 現在允許您按照餘弦相似度來搜尋「近鄰」。此功能需要服務軟體 R20200721 或更新版本。	2020 年 7 月 23 日
gzip 壓縮	Amazon OpenSearch 服務現在支援大多數HTTP請求和回應的 gzip 壓縮，這樣可以減少延遲並節省頻寬。此功能需要服務軟體 R20200721 或更新版本。	2020 年 7 月 23 日

支援 Elasticsearch 7.7	Amazon OpenSearch 服務現在支持彈性搜索 7.7 版。如需詳細資訊，請參閱 7.7 版本備註。	2020 年 7 月 23 日
Kibana 地圖服務	Amazon OpenSearch 服務 Kibana 的默認安裝現在包括一個WMS地圖服務器，但印度和中國區域的域名除外。	2020 年 6 月 18 日
SQL改進	SQLAmazon OpenSearch 服務的支援現在支援許多新作業、用於資料探索的專用 Kibana 使用者介面，以及互動式。CLI如需詳細資訊，請參閱。	2020 年 6 月 3 日
跨叢集搜尋	Amazon OpenSearch 服務可讓您跨多個連線網域執行跨叢集查詢和彙總。	2020 年 6 月 3 日
異常偵測	Amazon OpenSearch 服務可讓您近乎即時地自動偵測異常情況。	2020 年 6 月 3 日
UltraWarm	UltraWarm Amazon OpenSearch 服務的儲存空間已保留公開預覽版，現已正式推出。該功能現在支持更廣泛的版本和 AWS 區域. 如需詳細資訊，請參閱。	2020 年 5 月 5 日
自訂字典	Amazon OpenSearch 服務可讓您上傳自訂字典檔案，以便與叢集搭配使用。字典檔案透過讓 Elasticsearch 忽略某些高頻詞或將術語視為相同字詞，來改善您的搜尋結果。	2020 年 4 月 21 日

支援 Elasticsearch 7.4	Amazon OpenSearch 服務現在支持彈性搜索 7.4 版。如需詳細資訊，請參閱支援的版本。	2020 年 3 月 12 日
k-NN	Amazon OpenSearch 服務增加了對 K-最近鄰（k-NN）搜索的支持。k-NN 需要服務軟件 R20200302 或更高版本。	2020 年 3 月 3 日
索引狀態管理	Amazon Ser OpenSearch vice 新增了索引狀態管理 (ISM)，可讓您自動執行例行任務，例如在索引到達特定年齡時刪除索引。此功能需要服務軟體 R20200302 或更新版本。	2020 年 3 月 3 日
支援 Elasticsearch 5.6.16	Amazon OpenSearch 服務現在支援 5.6 版的最新修補程式版本，可新增錯誤修正並提高安全性。Amazon ES 會自動將現有 5.6 網域升級至此版本。請注意，此 Elasticsearch 版本會錯誤地將其版本報告為 5.6.17。	2020 年 3 月 2 日
精細定義存取控制	Amazon Ser OpenSearch vice 現在支援精細的存取控制，可為您的叢集提供索引、文件和欄位層級的安全性、Kibana 多租戶，以及選用的HTTP基本身份驗證。	2020 年 2 月 11 日

UltraWarm 儲存空間 (預覽)	Amazon OpenSearch 服務新增了 UltraWarm使用 Amazon S3 的全新暖儲存層，以及可提升效能的精密快取解決方案。對於您沒有主動寫入和查詢頻率較低的索引， UltraWarm 儲存體可大幅降低每 GiB 的成本。	2019 年 12 月 3 日
適用於中國區域的加密功能	`cn-north-1` 中國（北京）地區和中國（寧夏）地區現已提供靜態數據 node-to-node 加密和`cn-northwest-1` 加密。	2019 年 11 月 20 日
需要 HTTPS	您現在可以要求 Amazon ES 網域的所有流量都要求到達 HTTPS。設定網域時，請勾選「需要 HTTPS」方塊。此功能需要服務軟體 R20190808 或更新版本。	2019 年 10 月 3 日
支援 Elasticsearch 7.1 和 6.8	Amazon OpenSearch 服務現在支持彈性搜索版本 7.1 和 6.8。如需詳細資訊，請參閱支援的版本。	2019 年 8 月 13 日
每小時快照	Amazon OpenSearch 服務現在會針對執行 Elasticsearch 5.3 及更新版本的網域進行每小時快照，而不是每日快照，因此您可以更頻繁地從中還原資料的備份。	2019 年 7 月 8 日
支援 Elasticsearch 6.7	Amazon OpenSearch 服務現在支持彈性搜索 6.7 版。如需詳細資訊，請參閱支援的版本。	2019 年 5 月 29 日

SQL支持	Amazon OpenSearch 服務現在可讓您使用SQL. SQL支援需要 R20190418 或更新版本的服務軟體。	2019 年 5 月 15 日
5 系列執行個體類型	Amazon OpenSearch 服務現在支援 M5、C5 和 R5 執行個體類型。相較於上一代執行個體類型，這些新類型價格較低，效能更優異。如需詳細資訊，請參閱限制。	2019 年 4 月 24 日
支援 Elasticsearch 6.5	Amazon OpenSearch 服務現在支持彈性搜索版本 6.5。	2019 年 4 月 8 日
提醒	當來自一個或多個 Amazon ES 指數的資料符合特定條件時，Amazon OpenSearch 服務的警示會通知您。提醒需要服務軟體 R20190221 或更新版本。	2019 年 3 月 25 日
支援三個可用區域	Amazon OpenSearch 服務現在支援多個區域中的三個可用區域。此版本還包含簡化的主控台體驗。此多可用區域需要服務軟體 R20181023 或更新版本。	2019 年 2 月 7 日
支援 Elasticsearch 6.4	Amazon OpenSearch 服務現在支持彈性搜索版本 6.4。	2019 年 1 月 23 日
200 個節點叢集	Amazon ES 現在可讓您建立擁有高達 200 個資料節點的叢集，總共 3 PB 的儲存空間。	2019 年 1 月 22 日

服務軟體更新	Amazon ES 如今讓您能夠手動更新網域的服務軟體，從而更快地受益於新功能或選擇在低流量的時段進行更新。如需進一步了解，請參閱 。	2018 年 11 月 20 日
新 CloudWatch 量度	在 Amazon ES 主控台中，Amazon ES 現在提供節點層級指標和新的叢集運作狀態和執行個體運作狀態索引標籤。	2018 年 11 月 20 日
支援中國 (北京)	Amazon OpenSearch 服務現在可在 CN 北 -1 區域使用，該區域支援 M4、C4 和 R4 執行個體類型。	2018 年 10 月 17 日
N ode-to-node 加密技術	Amazon OpenSearch 服務現在支援 node-to-node 加密，因為 Amazon ES 會在您的叢集中分發資料時，保持資料的加密狀態。	2018 年 9 月 18 日
就地版本升級	Amazon OpenSearch 服務現在支持就地版本升級。	2018 年 8 月 14 日
支援 Elasticsearch 6.3 和 5.6	Amazon OpenSearch 服務現在支持彈性搜索版本 6.3 和 5.6。	2018 年 8 月 14 日
錯誤日誌	Amazon ES 現在允許您將彈性搜索錯誤日誌發佈到 Amazon。 CloudWatch	2018 年 7 月 31 日
中國 (寧夏) 預留執行個體	Amazon ES 目前在中國 (寧夏) 區域提供預留執行個體。	2018 年 5 月 29 日

預留執行個體	Amazon ES 現在提供對預留執行個體的支援。	2018 年 5 月 7 日

舊版更新

下表說明 2018 年 5 月前 Amazon ES 的重要變更。

變更	描述	日期
Kibana 的 Amazon Cognito 身分驗證	Amazon ES 現在提供 Kibana 的登入頁面保護。如需進一步了解，請參閱 the section called “用於儀表板的 Amazon Cognito 份 OpenSearch ”。	2018 年 4 月 2 日
支援 Elasticsearch 6.2	Amazon OpenSearch 服務現在支持彈性搜索版本 6.2。	2018 年 3 月 14 日
韓文分析外掛程式	Amazon ES 現在支援 Seunjeon 韓文分析外掛程式的記憶體最佳化版本。	2018 年 3 月 13 日
立即存取控制更新	Amazon ES 網域的存取控制政策變更現在會立即生效。	2018 年 3 月 7 日
PB 規模	Amazon ES 現在支援 I3 執行個體類型且網域總儲存量最多為 1.5 PB。如需進一步了解，請參閱 the section called “PB 規模”。	2017 年 12 月 19 日
靜態資料加密	Amazon ES 現在支援靜態資料加密。如需進一步了解，請參閱 the section called “靜態加密”。	2017 年 12 月 7 日
支援 Elasticsearch 6.0	Amazon ES 現在支援 Elasticsearch 6.0 版。如需遷移的考量和說明，請參閱the section called “升級網域”。	2017 年 12 月 6 日
VPCSupport	Amazon ES 現在可讓您在 Amazon Virtual Private Cloud 中啟動網域。VPC支援可提供額外的安全層，並簡化 Amazon ES 與其他服務之間的通訊VPC。如需進一步了解，請參閱 the section called “VPC支持”。	2017 年 10 月 17 日

變更	描述	日期
慢速日誌發佈	Amazon ES 現在支援將慢速日誌發佈到 CloudWatch 日誌。如需進一步了解，請參閱 the section called “監控日誌”。	2017 年 10 月 16 日
支援 Elasticsearch 5.5	Amazon ES 現在支援 Elasticsearch 5.5 版。 您現在可以還原自動快照，而無需使用 `_scriptsAPI`. AWS Support	2017 年 9 月 7 日
支援 Elasticsearch 5.3	Amazon ES 已新增對 Elasticsearch 5.3 版的支援。	2017 年 6 月 1 日
每個叢集更多執行個體和EBS容量	Amazon ES 現在每個叢集最多可支援 100 個節點和 150 TB 的EBS容量。	2017 年 4 月 5 日
加拿大 (中部) 和歐洲 (倫敦) 支援	Amazon ES 已新增對下列區域的支援：加拿大 (中部)、ca-central-1 和歐洲 (倫敦)、eu-west-2。	2017 年 3 月 20 日
更多實例和更大的EBS磁碟區	Amazon ES 增加了對更多實例和更大EBS容量的支持。	2017 年 2 月 21 日
支援 Elasticsearch 5.1	Amazon ES 已新增對 Elasticsearch 5.1 版的支援。	2017 年 1 月 30 日
支援語音分析外掛程式	Amazon ES 現在提供內建的語音分析外掛程式整合，其可讓您對您的資料執行「類似聲音」的查詢。	2016 年 12 月 22 日
美國東部 (俄亥俄) 支援	Amazon ES 已新增支援以下區域：美國東部 (俄亥俄)、us-east-2。	2016 年 10 月 17 日
新的效能指標	Amazon ES 新增效能指標 `ClusterUsedSpace` 。	2016 年 7 月 29 日
支援 Elasticsearch 2.3	Amazon ES 已新增對 Elasticsearch 2.3 版的支援。	2016 年 7 月 27 日
亞太區域 (孟買) 支援	Amazon ES 已新增對以下區域的支援：亞太區域 (孟買)、ap-south-1。	2016 年 6 月 27 日

變更	描述	日期
每個叢集更多執行個體	Amazon ES 已將每個叢集的執行個體數目上限 (執行個體計數) 從 10 提高到 20。	2016 年 5 月 18 日
亞太區域 (首爾) 支援	Amazon ES 已新增支援以下區域：亞太區域 (首爾)、ap-northeast-2。	2016 年 1 月 28 日
Amazon ES	初始版本。	2015 年 10 月 1 日

AWS 詞彙表

如需最新的 AWS 術語，請參閱《AWS 詞彙表 參考》中的 AWS 詞彙表。

本文為英文版的機器翻譯版本，如內容有任何歧義或不一致之處，概以英文版為準。