



開發人員指南

Amazon Kendra



Amazon Kendra: 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

.....	xiii
什麼是 Amazon Kendra ?	1
查詢 Amazon Kendra	1
Amazon Kendra 的優點	2
Amazon Kendra 版本	2
Amazon Kendra 的定價	3
您是第一次使用 Amazon Kendra 的新手嗎？	3
Amazon Kendra 的運作方式	5
索引	5
使用 Amazon Kendra 保留或一般文件欄位	6
搜尋索引	7
Documents	7
文件類型或格式	8
文件屬性或欄位	10
資料來源	12
查詢	13
標籤	14
標記資源	14
標籤限制	15
設置 Amazon Kendra	16
註冊成為 AWS	16
區域與端點	16
正在設定 AWS CLI	17
設定 AWS 軟體開發套件	17
IAM 存取角色 Amazon Kendra	19
IAM 索引的角色	19
IAM 應用 BatchPutDocument 程式介面的角色	22
IAM 資料來源的角色	25
虛擬私有雲 (VPC) IAM 角色	114
IAM 常見問題的角色	116
IAM 查詢建議的角色	117
IAM 使用者與群組之主參與者對應的角色	119
IAM 角色 AWS IAM Identity Center	121
IAM Amazon Kendra 體驗的角色	122

IAM 自訂文件增強功能的角色	125
部署 Amazon Kendra	129
概要	130
先決條件	130
設定範例查詢	130
主搜索頁面	131
搜尋元件	131
結果元件	131
多面元件	132
分頁組件	132
部署不含程式碼的搜尋應用程式	132
搜尋體驗產生器的運作方式	132
設計和調整您的搜尋體驗	133
提供您搜尋頁面的存取	134
設定搜尋體驗	135
調整容量	140
檢視容量	141
新增和移除容量	141
Amazon Kendra 智能排名能力	142
查詢建議容量	142
Amazon Kendra 經驗能力	142
搜尋體驗能力	142
調適性查詢成組分解	142
開始使用	144
必要條件	144
註冊一個 AWS 帳戶	144
建立具有管理權限的使用者	145
Amazon Kendra 資源: AWS CLI, SDK, 控制台	146
開始使用主 Amazon Kendra 控台	152
開始使用 (AWS CLI)	152
開始使用 (開 SDK for Python (Boto3))	154
開始使用 (SDK for Java)	157
開始使用 S3 (主控台)	161
開始使用 MySQL (控制台)	162
開始使用 IAM 身分中心身分識別來源 (主控台)	165
變更您的 IAM 身分中心身分來源	167

建立索引	168
使用批次上傳將文件直接新增至索引	172
使用 BatchPutDocument API 新增文件	173
從 S3 儲存貯體新增文件	175
將常見問題 (FAQ) 添加到索引	178
建立常見問題集檔案的索引欄位	179
基本 CSV 檔案	179
自訂 CSV 檔案	180
JSON 檔案	181
使用常見問題解答檔	183
英語以外的語言常見問題解答文件	185
建立自訂文件欄位	185
更新自訂文件欄位	186
使用權杖控制使用者對文件的存取	189
使用 OpenID	190
使用 JSON 網絡令牌 (JWT) 與共享密鑰	192
使用 JSON 網絡令牌 (JWT) 與公鑰	195
使用 JSON	198
建立資料來源連接器	201
設定更新排程	202
設定語言	202
資料來源連接器	202
資料來源範本架構	204
Adobe Experience Manager	542
Alfresco	550
Aurora (MySQL)	557
Aurora (PostgreSQL)	564
Amazon FSx (視窗)	570
Amazon FSx (NetApp ONTAP)	577
Amazon RDS/Aurora	584
Amazon RDS (Microsoft SQL 服務器)	592
Amazon RDS (MySQL)	599
Amazon RDS (Oracle)	605
Amazon RDS (PostgreSQL)	612
Amazon S3	619
Amazon Kendra 網絡爬蟲	633

Amazon WorkDocs	651
立方體	656
Confluence	662
自訂資料來源連接器	679
Dropbox	687
Drupal	694
GitHub	702
Gmail	711
Google 雲端硬碟	719
IBM DB2	734
Jira	740
Microsoft Exchange	746
Microsoft OneDrive	753
Microsoft SharePoint	766
Microsoft SQL Server	795
Microsoft Teams	802
Microsoft 亞默	811
MySQL	817
Oracle Database	824
PostgreSQL	830
諷刺語	837
Salesforce	842
ServiceNow	857
Slack	873
Zendesk	881
對映資料來源欄位	888
使用 Amazon Kendra 保留或一般文件欄位	6
以英文以外的語言新增文件	893
配置 Amazon Kendra 為使用 Amazon VPC	895
配置 Amazon VPC	896
連接到 Amazon VPC	898
連線至資料庫	899
VPC 連線問題疑難排解	901
刪除索引、資料來源或批次上傳的文件	904
刪除索引	904
刪除資料來源	905

刪除批次上傳的文件	907
擷取期間豐富您的文件	908
自訂文件擴充的運作方式	908
更改元數據的基本操作	909
Lambda 函數：擷取和變更中繼資料或內容	917
Lambda 函數的資料合約	925
結構化文件格式	926
符合資料合約的 Lambda 函數範例	927
搜尋索引	930
查詢索引	930
必要條件	931
搜尋索引 (主控台)	931
搜尋索引 (SDK)	932
搜索索引 (郵遞員)	934
使用進階查詢語法搜尋	935
以語言搜尋	940
擷取段落	943
瀏覽索引	946
特色搜尋結果	949
以表格方式搜尋	952
查詢建議	956
使用查詢歷史查詢建議	957
使用文件欄位查詢建議	962
封鎖建議中的某些查詢或文件欄位內容	966
查詢拼字檢查	971
使用具有預設限制的查詢拼字檢查程式	972
篩選和平面搜尋	972
面向	973
使用文件屬性篩選搜尋結果	977
篩選搜尋結果中每個文件的屬性	978
篩選使用者內容	978
按用戶令牌過濾	979
依使用者 ID 和群組篩選	980
依使用者屬性篩選	981
直接新增至索引的文件的使用者前後關聯篩選	982
常見問題集的使用者內容篩選	982

資料來源的使用者內容篩選	983
查詢回應和回應類型	999
查詢回應	999
回應類型	1003
調整和排序回應	1007
調整回應	1007
排序回應	1008
摺疊/展開查詢結果	1010
摺疊結果	1012
使用排序順序選擇主要文件	1012
缺少文件金鑰策略	1013
擴大結果	1013
與其他 Amazon Kendra 功能的互動	1013
調整搜尋相關性	1014
在索引層級進行相關性調整	1015
在查詢層級進行相關性調整	1016
透過搜尋分析獲得洞察	1017
搜尋量度	1017
點擊率	1018
零點擊率	1018
零搜索結果率	1018
即時答案率	1018
熱門查詢	1019
零點擊的熱門查詢	1019
搜尋結果為零的熱門查詢	1019
點擊頂部的文檔	1020
查詢總數	1020
文件總數	1020
擷取測量結果資料的範例	1020
從指標到可行的洞察	1022
視覺化和報告搜尋分析	1022
查詢總計圖表	1023
點擊率圖	1023
零點擊率圖	1023
零搜尋結果比率圖	1023
即時答案率圖	1023

提交漸進學習的意見反應	1025
使用圖 Amazon Kendra JavaScript 書館提交意見反應	1026
步驟 1：在 Amazon Kendra 搜尋應用程式中插入指令碼標記	1026
步驟 2：將意見反應記號新增至搜尋結果	1029
步驟 3：測試意見反應指令碼	1029
使用 Amazon Kendra API 提交意見反應	1030
將自訂同義字新增至索引	1033
建立同義字辭典檔案	1035
將索引典新增至索引	1037
更新索引典	1041
刪除索引典	1045
搜尋結果中的亮點	1046
教學課程：建置智慧搜尋解決方案	1047
必要條件	1048
步驟 1：新增文件	1049
下載範例資料集	1049
建立 Amazon S3 儲存貯體	1051
在 S3 儲存貯體中建立資料和中繼資料資料夾	1054
上傳輸入數據	1056
步驟 2：偵測圖元	1059
執行 Amazon Comprehend 實體分析任務	1059
步驟 3：格式化中繼資料	1067
下載和提取 Amazon Comprehend 輸出	1068
將輸出上傳到 S3 儲存貯體	1071
將輸出轉換為 Amazon Kendra 元數據格式	1073
清理你的 Amazon S3 存儲桶	1077
步驟 4：建立索引並擷取中繼資料	1079
創建一個 Amazon Kendra 索引	1080
更新 Amazon S3 存取的 IAM 角色	1087
創建 Amazon Kendra 自定義搜索索引字段	1091
將 Amazon S3 儲存貯體新增為索引的資料來源	1096
同步 Amazon Kendra 索引	1100
步驟 5：查詢索引	1102
查詢您的 Amazon Kendra 索引	1103
篩選搜尋結果	1109
步驟 6：清理	1113

清理您的文件	1113
.....	1114
監控和記錄	1115
監視索引	1115
Amazon Kendra 監控與 CloudTrail	1119
Amazon Kendra 的資訊 CloudTrail	1119
Amazon Kendra 的記錄	1120
監控 Amazon Kendra 智慧排名 API 呼叫 CloudTrail	1121
Amazon Kendra 智慧排名資訊 CloudTrail	1121
範例：Amazon Kendra 智慧排名記錄檔項目	1122
Amazon Kendra 監控 CloudWatch	1123
Amazon Kendra 的檢控	1123
建立警示	1124
CloudWatch 索引同步工作的測量結果	1125
Amazon Kendra 的指標	1126
索引文件的量度	1128
Amazon Kendra 監控 CloudWatch 日誌	1129
資料來源日誌串流	1130
記錄	1131
安全	1133
資料保護	1133
靜態加密	1134
傳輸中加密	1134
金鑰管理	1135
VPC 端點 (AWS PrivateLink)	1135
亞馬遜肯德拉和亞馬遜肯德拉智慧排名 VPC 端點的注意事項	1135
為亞馬遜肯德拉和 Amazon Kendra 智能排名創建接口 VPC 端點	1135
為亞馬遜肯德拉和 Amazon Kendra 智慧排名建立 VPC 端點政策	1136
身分與存取管理	1137
物件	1138
使用身分驗證	1138
使用政策管理存取權	1140
亞馬遜肯德拉如何與 IAM 合作	1142
身分型政策範例	1147
AWS 受管政策	1152
故障診斷	1156

安全最佳實務	1158
套用最低權限準則	1158
角色型存取控制 (RBAC) 許可	1158
在 Amazon Kendra 中進行記錄和監控	1159
法規遵循驗證	1159
恢復能力	1160
基礎架構安全	1160
組態與漏洞分析	1161
配額	1162
支援的 區域	1162
配額	1162
索引配額	1162
資料來源連接器配額	1163
常見問題集	1163
索引典配額	1164
Amazon Kendra 體驗配額	1164
查詢和搜尋結果配額	1165
查詢建議配額	1166
文件配額	1167
特色搜尋結果配額	1168
重新核心/重新排名搜尋結果額度	1168
故障診斷	1170
疑難排解資料來	1170
我的文件沒有編製索引	1170
我的同步工作失敗	1170
我的同步工作不完整	1171
我的同步處理工作成功，但沒有編製索引的文件	1171
我在同步資料來源時遇到檔案格式問題	1172
我想要為我的文件產生同步記錄報告	1172
同步資料來源需要多少時間？	1173
同步資料來源的費用為何？	1173
我收到 Amazon EC2 授權錯誤	1173
我無法使用搜索索引鏈接打開我的 Amazon S3 對象	1173
我收到「使用 SSL 憑證檔案AccessDenied 時」錯誤訊息	1174
我在使用 SharePoint 資料來源時收到授權錯誤	1174
我的索引不會從我的匯合資料來源抓取文件	1174

文件搜尋結果的疑難	1174
我的搜尋結果與我的搜尋條件不相關	1174
為什麼我只看到 100 個結果？	1175
為什麼我希望看到的文檔丟失？	1175
為什麼我會看到具有 ACL 政策的文件？	1175
疑難排解一般問題	1175
Amazon Kendra 智慧排名	1177
自我管理的智慧排名 OpenSearch	1177
智能搜索插件的工作原理	1177
設定智慧型搜尋外掛程式	1178
與智慧型搜尋外掛程式互動	1183
比較 OpenSearch 結果與 Amazon Kendra 結果	1189
語義上對搜索服務的結果進行排名	1190
文件歷史紀錄	1199
API 參考	1211
AWS 詞彙表	1212
.....	mccxiii

什麼是 Amazon Kendra ?

Amazon Kendra 是一種智慧型搜尋服務，它使用自然語言處理和進階機器學習演算法，傳回資料中搜尋問題的特定答案。

與傳統的關鍵字搜尋不同，Amazon Kendra 使用其語義和上下文理解功能來決定文件是否與搜尋查詢相關。它返回問題的具體答案，為用戶提供接近與人類專家互動的體驗。

Note

您也可以使用 Amazon Kendra 的語意搜尋功能來重新排名其他搜尋服務的結果。如需詳細資訊，請參閱 [Amazon Kendra 智慧排名](#)。

您可以使用將多個資料儲存庫連接至索引 Amazon Kendra，並擷取和編目文件，以建立統一的搜尋體驗。您可以使用文件中繼資料為使用者建立功能豐富且自訂的搜尋體驗，協助他們有效率地找到查詢的正確答案。

[什麼是 Amazon Kendra ?](#)

查詢 Amazon Kendra

您可以詢問以 Amazon Kendra 下類型的查詢：

Factoid 問題 — 簡單的是誰，什麼，何時或在哪裡問題，例如離西雅圖最近的服務中心在哪裡？

Factoid 問題具有基於事實的答案，可以作為單個單詞或短語返回。答案是從常見問題集或索引文件中擷取的。

描述性問題 — 答案可以是句子、段落或整份文件的問題。例如，如何將我的 Echo Plus 連接到我的網絡？或者，如何為低收入家庭獲得稅收優惠？

關鍵字和自然語言問題 — 包含含義可能不清楚的複雜對話內容的問題。例如，關鍵註記地址。當 Amazon Kendra 遇到像「地址」這樣具有多個上下文意義的單詞時，它會正確推斷搜索查詢背後的含義並返回相關信息。

Amazon Kendra 的優點

Amazon Kendra 具備高度擴充能力、能夠滿足效能需求、與其他 AWS 服務 (例如 [Amazon S3](#) 和) 緊密整合 [Amazon Lex](#)，並提供企業級安全性。使用 Amazon Kendra 的若干優點包括：

簡易性 — Amazon Kendra 提供主控台和 API 來管理您要搜尋的文件。您可以使用簡單的搜尋 API 整合 Amazon Kendra 至用戶端應用程式，例如網站或行動應用程式。

連線能力 — Amazon Kendra 可連線至協力廠商資料儲存庫或資料來源 (例如 Microsoft) SharePoint。您可以使用資料來源輕鬆索引和搜尋文件。

準確性：與使用關鍵字搜尋的傳統搜尋服務不同，會 Amazon Kendra 嘗試瞭解問題的內容，並傳回查詢最相關的文字、片段或文件。Amazon Kendra 使用機器學習來改善一段時間的搜尋結果。

安全性 — Amazon Kendra 提供高度安全的企業搜尋體驗。您的搜尋結果會反映組織的安全性模型，並且可以根據使用者或群組對文件的存取權進行篩選。客戶須負責驗證及授權使用者存取權。

Amazon Kendra 版本

Amazon Kendra 有兩個版本：開發版和企業版。下表概述了它們的特徵以及兩者之間的差異。

Amazon Kendra 開發人員版	Amazon Kendra 企業版
Amazon Kendra 開發人員版以較低的成本提供 Amazon Kendra 的所有功能。	Amazon Kendra 企業版提供的所有功能，Amazon Kendra 並且專為生產環境而設計。
理想的使用案例	理想的使用案例
<ul style="list-style-type: none"> • 探索文件 Amazon Kendra 編製索引的方式 • 嘗試功能 • 開發使用的應用程式 Amazon Kendra 	<ul style="list-style-type: none"> • 為整個企業文件庫建立索引 • 在生產環境中部署應用程式
功能	功能
<ul style="list-style-type: none"> • 包含 750 小時使用的免費方案 • 最多 5 個索引，每個索引最多 5 個資料來源 • 10,000 份文件或 3 GB 擷取的文字 	<ul style="list-style-type: none"> • 最多 5 個索引，每個索引最多 50 個資料來源 • 10 萬份文件或 30 GB 擷取的文字 • 每天約 8,000 個查詢或每秒 0.1 個查詢 • 在 3 個可用區域 (AZ) 中執行 — 請參閱 可用區域 (區域中的資料中AWS心)

Amazon Kendra開發人員版

- 每天大約 4,000 個查詢或每秒 0.05 個查詢
- 在 1 個可用區域 (AZ) 中執行 — 請參閱[可用區域 \(區域\)](#)中的資料中AWS心)

限制

- 不適用於生產應用
- 不保證延遲或可用性

Amazon Kendra企業版

Note

您可以使用[服務配額主控台](#)增加此配額。

限制

- 無

Note

如需支援的區域、端點和服務配額清單Amazon Kendra，請參閱[Amazon Kendra端點和配額](#)。

Amazon Kendra 的定價

您可以使用開發Amazon Kendra人員版免費開始使用，該版本在前 30 天最多可使用 750 小時。

試用期到期後，即使所有佈建的Amazon Kendra索引為空且未執行任何查詢，您仍需支付所有佈建索引的費用。試用期到期後，使用Amazon Kendra資料來源掃描和同步文件需支付額外費用。

如需費用和價格的完整清單，請參閱[Amazon Kendra定價](#)。

您是第一次使用 Amazon Kendra 的新手嗎？

若是第一次使用 Amazon Kendra，建議您依序閱讀以下章節：

1	2	3	4	5	6
Amazon Kendra 的運作方式	開始使用	建立索引	使用批次上傳將文件直接新增至索引	建立資料來源連接器	搜尋索引
介紹Amazon Kendra元件	說明如何設定帳戶及測	說明如Amazon	說明如何將文件直接新	說明如何將文件從資料儲存	說明如何使

1	2	3	4	5	6
Amazon Kendra 的運作方式	開始使用	建立索引	使用批次上傳將文件直接新增至索引	建立資料來源連接器	搜尋索引
並說明如何使用它們來建立搜尋解決方案。	試Amazon Kendra搜尋API。	Kendra何使用建立搜尋索引，以及新增資料來源以同步您的文件。	增至Amazon Kendra索引。	庫新增至Amazon Kendra索引。	Kendra搜尋API來搜尋索引。

Amazon Kendra 的運作方式

Amazon Kendra 為您的應用程式提供搜尋功能。它可以直接或從協力廠商文件儲存庫索引您的文件，並智慧地將相關資訊提供給使用者。您可以使用 Amazon Kendra 來建立各種類型的文件的可更新索引。如需支援的文件類型清單，Amazon Kendra 請參閱[文件類型](#)。

Amazon Kendra 與其他服務整合。例如，您可以通過 Amazon Kendra 搜索功能強化[Amazon Lex 聊天機器人](#)，以便為用戶的問題提供有用的答案。您可以使用[Amazon Simple Storage Service 值區](#)做為資料來源，以連線 Amazon Kendra 至文件並建立索引。您也可以使用設定資源的存取原則或權限[AWS Identity and Access Management](#)。

Amazon Kendra 具有以下組件：

- 一種[索引](#)，用於保存您的文檔並使其可搜索。
- 儲存文件並 Amazon Kendra 連線到的[資料來源](#)。您可以自動將資料來源與 Amazon Kendra 索引同步，以便您的索引隨來源儲存庫保持更新。
- 將[文件直接新增至索引的文件新增 API](#)。

您可以 Amazon Kendra 通過控制台或 API 使用。您可以建立、更新和刪除索引。刪除索引會刪除其所有資料來源連接器，並從中永久刪除所有文件資訊 Amazon Kendra。

主題

- [索引](#)
- [Documents](#)
- [資料來源](#)
- [查詢](#)
- [標籤](#)

索引

索引會保留文件的內容，並以可搜尋文件的方式結構化。將文件新增至索引的方式取決於您儲存文件的方式。

- 如果您將文件儲存在某種存放庫 (例如儲存 Amazon S3 貯體或 Microsoft SharePoint 網站) 中，您可以使用[資料來源連接器](#)從存放庫編製文件的索引。

- 如果您沒有將文件儲存在儲存庫中，您可以使用 [BatchPutDocument](#) API 直接為文件編製索引。
- 對於必須存儲在 Amazon Kendra (Amazon S3) 存儲桶中的常見問題和答案，請從存儲桶上傳它們

您可以使用主 Amazon Kendra 控制台 AWS CLI、或 AWS SDK 建立索引。如需可編製索引之文件類型的相關資訊，請參閱[文件類型](#)。

使用 Amazon Kendra 保留或一般文件欄位

使用 [UpdateIndex API](#)，您可以使用 `DocumentMetadataConfigurationUpdates` 並指定保留索引欄位名稱來建立 Amazon Kendra 保留或通用欄位，以對應至對等的文件屬性/欄位名稱。您也可以建立自訂欄位。如果您使用資料來源連接器，大多數都會包含將資料來源文件欄位對映至 Amazon Kendra 索引欄位的欄位對映。如果您使用主控台，您可以透過選取資料來源、選取編輯動作，然後繼續進行欄位對應區段旁邊以配置資料來源來更新欄位。

您可以設定 Search 物件以將欄位設定為可顯示、可變更、可搜尋和可排序。您可以將 Relevance 物件設定為設定欄位的排名順序、提升持續時間或時段，以套用至提升、新鮮度、重要性值，以及對應至特定欄位值的重要性值。如果您使用控制台，則可以透過選取導覽功能表中的 Facet 選項來設定欄位的搜尋設定。若要設定相關性調整，請在導覽功能表中選取搜尋索引的選項、輸入查詢，然後使用側邊面板選項來調整搜尋相關性。建立欄位後，就無法變更欄位類型。

Amazon Kendra 您可以使用下列保留或一般文件欄位：

- `_authors` 負責文件內容的一或多個作者清單。
- `_category` 將文件放置在特定群組中的類別。
- `_created_at` 以 ISO 8601 格式建立文件的日期和時間。例如，2012-03-25T12:30:10+01:00 是以 ISO 8601 日期時間格式表示的歐洲中部時間 2012 年 3 月 25 日中午 12:30 (加上 10 秒)。
- `_data_source_id` 包含文件之資料來源的識別碼。
- `_document_body` 文件的內容。
- `_document_id` 文件的唯一識別元。
- `_document_title` 文件的標題。
- `_excerpt_page_number` 顯示文件摘錄的 PDF 檔案中的頁碼。如果您的索引是在 2020 年 9 月 8 日之前建立的，您必須重新建立文件索引，才能使用此屬性。
- `_faq_id` 如果這是問答類型文件 (FAQ)，這是常見問題集的唯一識別碼。
- `_file_type` 文件的檔案類型，例如 pdf 或 doc。

- `_last_updated_at`上次更新文件的日期和時間 (使用 ISO 8601 格式)。例如，2012-03-25T12:30:10+01:00 是以 ISO 8601 日期時間格式表示的歐洲中部時間 2012 年 3 月 25 日中午 12:30 (加上 10 秒)。
- `_source_uri`可使用文件的 URI。例如，在公司網站上的文件 URI。
- `_version`文件特定版本的識別元。
- `_view_count`檢視文件的次數。
- `_language_code`(字串)-套用至文件之語言的程式碼。如果您未指定語言，則預設為英文。如需支援語言 (包括其代碼) 的詳細資訊，請參閱以[英文以外的語言新增文件](#)。

對於自訂欄位，您可以使 `DocumentMetadataConfigurationUpdates` 用 `UpdateIndex` API 建立這些欄位，就像建立保留或公用欄位時一樣。您必須為自訂欄位設定適當的資料類型。如果您使用主控台，您可以透過選取資料來源、選取編輯動作，然後繼續進行欄位對應區段旁邊以配置資料來源來更新欄位。某些資料來源不支援新增欄位或自訂欄位。建立欄位後，就無法變更欄位類型。

以下是您可以為自訂欄位設定的類型：

- 日期
- Number
- 字串
- 字串清單

如果您使用 [BatchPutDocument](#) API 將文件新增至索引，會 `Attributes` 列出文件的欄位/屬性，並使用物件建立欄位。 `DocumentAttribute`

對於從 Amazon S3 資料來源編製索引的文件，您可以使用包含欄位資訊的 [JSON 中繼資料檔案](#) 建立欄位。

如果您使用支援的資料庫做為資料來源，您可以使用欄位 [對應選項來設定欄位](#)。

搜尋索引

建立索引之後，您就可以開始搜尋文件。如需詳細資訊，請參閱[搜尋索引](#)。

Documents

本節說明如何 Amazon Kendra 索引它支持的多種文檔格式以及文檔的不同字段/屬性。

主題

- [文件類型或格式](#)
- [文件屬性或欄位](#)

文件類型或格式

Amazon Kendra 支持流行的文檔類型或格式，例如 PDF，HTML PowerPoint，Word 等。索引可以包含多種文件格式。

Amazon Kendra 擷取文件內的內容，以便使文件可搜尋。文檔被解析的方式來優化對提取的文本和文檔中的任何表格內容 (HTML 表格) 的搜索。這表示將文件結構化為用於搜尋的欄位或屬性。文件中繼資料 (例如上次修改日期) 可能是有用的搜尋欄位。

文件可以組織成列和欄。例如，每個文件都是一列，而每個文件欄位/屬性 (例如標題和內文內容) 都是一欄。例如，如果您使用資料庫做為資料來源，則應將資料結構化或組織成列和欄。

您可以透過下列方式將文件新增至索引：

- [BatchPutDocument](#) API
- [資料來源連接器](#)

如果要新增常見問題集檔案，請使用 [CreateFaq](#) API 新增儲存在 Amazon S3 值區中的檔案。您可以選擇基本 CSV 格式、在標題中包含海關欄位/屬性的 CSV 格式，以及包含自訂欄位的 JSON 格式。預設格式為基本 CSV。

以下提供每種支援文件格式的資訊，以及編製文件索引時如何 Amazon Kendra 處理每種格式的資訊。

文件格式	被視為	如何處理文件	原始結構
可攜式文件格式 (PDF)	HTML	轉換為 HTML，然後提取內容。	非结构化
HyperText 标记语言	HTML	HTML 標籤被過濾掉以提取內容。內容必須在主要 HTML 開始和結束標籤之間 (<HTML>content</HTML>)。	半结构化

文件格式	被視為	如何處理文件	原始結構
可擴展標記語言 (XML)	XML	XML 標籤被過濾掉以提取內容。	半结构化
可擴展樣式表語言轉換 (XSLT)	XSLT	標籤被過濾掉以提取內容。	半结构化
Markdown (馬里蘭州)	純文字	內容提取並包含 Markdown 語法。	半结构化
逗號分隔符號值 (CSV)	CSV	從每個儲存格擷取的內容，並將單一檔案視為單一文件結果。	结构化常見問題解答文件，否則半結構
Microsoft Excel (XLS 和 XLSX)	XLS 和 XLSX	從每個儲存格擷取的內容，並將單一檔案視為單一文件結果。	半结构化
JavaScript 对象标记法	純文字	使用 JSON 語法提取內容。	半结构化
RTF 格式 (RTF)	RTF	RTF 語法被過濾掉以提取內容。	半结构化
Microsoft 軟件 PowerPoint (PPT)	PPT	僅從 PowerPoint 幻燈片中提取文本內容進行搜索。不會擷取影像和其他內容。	非结构化
Microsoft 文字	DOCX	僅從 Word 頁面中提取文本內容進行搜索。不會擷取影像和其他內容。	非结构化
純文字 (TXT)	TXT	會擷取文字文件中的所有文字。	非结构化

文件屬性或欄位

文件具有與其相關聯的屬性或欄位。一個文檔的字段是一個文檔或什麼是包含在一個文檔的結構中的屬性。例如，您的每份文件可能包含標題、內文和作者。您還可以為特定文檔添加自定義字段。例如，如果您的索引搜尋稅務文件，您可以指定稅務文件類型的自訂欄位，例如 W-2、1099 等。

您必須先對應至索引欄位，才能在查詢中使用文件欄位。例如，標題欄位可以對應至欄位 `_document_title`。如需詳細資訊，請參閱[對應欄位](#)。若要新增欄位，您必須建立索引欄位來對應欄位。您可以使用主控台或使用 [UpdateIndex](#) API 建立索引欄位。

您可以使用文件欄位來篩選回應，以及製作多面向搜尋結果。例如，您可以篩選回應，使其只傳回特定版本的文件，或者您可以篩選搜尋結果，使其僅傳回符合搜尋字詞的 1099 類型稅務文件。如需詳細資訊，請參閱[篩選和刻面搜尋](#)。

您也可以使用文件欄位來手動調整查詢回應。例如，您可以選擇增加 `title` 欄位的重要性，以便在決定回應中傳回的文件時，增加 Amazon Kendra 指派給欄位的權重。如需詳細資訊，請參閱[調整搜尋相關性](#)。

如果您要直接將文件新增至索引，則可以將 [Document](#) 輸入參數中的欄位指定至 [BatchPutDocument](#) API。您可以在 [DocumentAttribute](#) 物件陣列中指定自訂欄位值。如果您使用的是資料來源，則用來新增文件欄位的方法取決於資料來源。如需詳細資訊，請參閱[映射資料來源欄位](#)。

使用 Amazon Kendra 保留或一般文件欄位

使用 [UpdateIndex API](#)，您可以使用 `DocumentMetadataConfigurationUpdates` 並指定保留索引欄位名稱來建立 Amazon Kendra 保留或通用欄位，以對應至對等的文件屬性/欄位名稱。您也可以建立自訂欄位。如果您使用資料來源連接器，大多數都會包含將資料來源文件欄位對映至 Amazon Kendra 索引欄位的欄位對映。如果您使用主控台，您可以透過選取資料來源、選取編輯動作，然後繼續進行欄位對應區段旁邊以配置資料來源來更新欄位。

您可以設定 `Search` 物件以將欄位設定為可顯示、可變更、可搜尋和可排序。您可以將 `Relevance` 物件設定為設定欄位的排名順序、提升持續時間或時段，以套用至提升、新鮮度、重要性值，以及對應至特定欄位值的重要性值。如果您使用控制台，則可以透過選取導覽功能表中的 `Facet` 選項來設定欄位的搜尋設定。若要設定相關性調整，請在導覽功能表中選取搜尋索引的選項、輸入查詢，然後使用側邊面板選項來調整搜尋相關性。建立欄位後，就無法變更欄位類型。

Amazon Kendra 您可以使用下列保留或一般文件欄位：

- `_authors` 負責文件內容的一或多個作者清單。
- `_category` 將文件放置在特定群組中的類別。

- `_created_at`以 ISO 8601 格式建立文件的日期和時間。例如，2012-03-25T12:30:10+01:00 是以 ISO 8601 日期時間格式表示的歐洲中部時間 2012 年 3 月 25 日中午 12:30 (加上 10 秒)。
- `_data_source_id`包含文件之資料來源的識別碼。
- `_document_body`文件的內容。
- `_document_id`文件的唯一識別元。
- `_document_title`文件的標題。
- `_excerpt_page_number`顯示文件摘錄的 PDF 檔案中的頁碼。如果您的索引是在 2020 年 9 月 8 日之前建立的，您必須重新建立文件索引，才能使用此屬性。
- `_faq_id`如果這是問答類型文件 (FAQ)，這是常見問題集的唯一識別碼。
- `_file_type`文件的檔案類型，例如 pdf 或 doc。
- `_last_updated_at`上次更新文件的日期和時間 (使用 ISO 8601 格式)。例如，2012-03-25T12:30:10+01:00 是以 ISO 8601 日期時間格式表示的歐洲中部時間 2012 年 3 月 25 日中午 12:30 (加上 10 秒)。
- `_source_uri`可使用文件的 URI。例如，在公司網站上的文件 URI。
- `_version`文件特定版本的識別元。
- `_view_count`檢視文件的次數。
- `_language_code`(字串)-套用至文件之語言的程式碼。如果您未指定語言，則預設為英文。如需支援語言 (包括其代碼) 的詳細資訊，請參閱以[英文以外的語言新增文件](#)。

對於自訂欄位，您可以使 `DocumentMetadataConfigurationUpdates` 用 `UpdateIndex` API 建立這些欄位，就像建立保留或公用欄位時一樣。您必須為自訂欄位設定適當的資料類型。如果您使用主控台，您可以透過選取資料來源、選取編輯動作，然後繼續進行欄位對應區段旁邊以配置資料來源來更新欄位。某些資料來源不支援新增欄位或自訂欄位。建立欄位後，就無法變更欄位類型。

以下是您可以為自訂欄位設定的類型：

- 日期
- Number
- 字串
- 字串清單

如果您使用 [BatchPutDocument](#) API 將文件新增至索引，會 `Attributes` 列出文件的欄位/屬性，並使用物件建立欄位。 `DocumentAttribute`

對於從資 Amazon S3 料來源編製索引的文件，您可以使用包含欄位資訊的 [JSON 中繼資料檔案](#) 建立欄位。

如果您使用支援的資料庫做為資料來源，您可以使用欄位 [對應選項來設定欄位](#)。

資料來源

資料來源是 Amazon Kendra 連線至文件或內容並編製索引的資料儲存庫或位置。例如，您可以設定為連線 Amazon Kendra SharePoint 至 Microsoft，以編目和索引儲存在此來源中的文件。您也可以透過提供要檢索的 URL Amazon Kendra 來編製網頁索引。您可以自動將資料來源與 Amazon Kendra 索引同步，以便在索引中新增、更新或刪除資料來源中的文件也會新增、更新或刪除。

支援的資料來源包括：

- [體驗管理器](#)
- [露天](#)
- [Aurora \(MySQL\)](#)
- [Aurora \(PostgreSQL\)](#)
- [Amazon FSx \(視窗\)](#)
- [Amazon FSx \(NetApp ONTAP\)](#)
- [資料庫資料來源](#)
- [Amazon RDS \(Microsoft SQL 服務器 \)](#)
- [Amazon RDS \(MySQL\)](#)
- [Amazon RDS \(甲骨文\)](#)
- [Amazon RDS \(PostgreSQL\)](#)
- [Amazon S3 水桶](#)
- [Amazon Kendra 網絡爬蟲](#)
- [Amazon WorkDocs](#)
- [Box \(立方體\)](#)
- [匯合](#)
- [自訂資料來源](#)
- [Dropbox](#)
- [Drupal](#)
- [GitHub](#)

- [Gmail](#)
- [谷歌工作區硬盤](#)
- [IBM](#)
- [吉拉](#)
- [Microsoft 交易所](#)
- [Microsoft OneDrive](#)
- [Microsoft SharePoint](#)
- [Microsoft Teams](#)
- [Microsoft SQL Server](#)
- [Microsoft 亞默](#)
- [MySQL](#)
- [Oracle 資料庫](#)
- [PostgreSQL](#)
- [混雜的](#)
- [Salesforce](#)
- [ServiceNow](#)
- [Slack](#)
- [Zendesk](#)

如需支援的文件類型或格式清單，Amazon Kendra 請參閱[文件類型](#)。您必須先建立索引，然後再建立資料來源連接器，以便從資料來源編製文件索引。

Note

若要建立文件索引，您不需要使用資料來源。您可以使用批次上傳將文件直接新增至索引。如需詳細資訊，請參閱[將文件直接新增至索引](#)。

如需使用 Amazon Kendra 主控台、AWS CLI 或 SDK 的逐步解說，請參閱[入門](#)。

查詢

為了獲得答案，用戶查詢索引。使用者可以在查詢中使用自然語言。回應包含資訊，例如標題、文字摘錄，以及索引中提供最佳答案的文件位置。

Amazon Kendra 使用您提供的有關文件的所有資訊，而不僅僅是文件的內容，來判斷文件是否與查詢相關。例如，如果您的索引包含上次更新文件時間的相關資訊，您可 Amazon Kendra 以告訴您指定與最近更新的文件更高的相關性。

查詢也可以包含如何篩選回應的條件，以便只 Amazon Kendra 傳回符合篩選條件的文件。例如，如果您創建了一個名為「部門」的索引字段，那麼您可以過濾響應，以便只返回部門字段設置為合法的文件。如需詳細資訊，請參閱[篩選搜尋](#)。

您可以透過調整索引中個別欄位的相關性來影響查詢結果。調整會變更欄位對結果的重要性。例如，如果您使用新類別提高文件的重要性，則具有此類別的文件更有可能包含在回應中。如需詳細資訊，請參閱[調整搜尋相關性](#)。

如需有關使用查詢的詳細資訊，請參閱[搜尋索引](#)。

標籤

透過指派標籤或標記來管理索引、資料來源和常見問題集。您可以使用標籤以各種方式對 Amazon Kendra 源進行分類。例如，按目的、擁有者、應用程式或任何組合。每個標籤皆包含由您定義的索引鍵和值。

標籤可協助您：

- 識別和組織您的 AWS 資源。許多 AWS 服務都支援標記，因此您可以將相同標籤指派給不同服務中的資源，以指出資源是相關的。例如，您可以使用相同的標籤來標記索引和使用索引的 Amazon Lex 機器人。
- 配置成本。您可以在 AWS Billing and Cost Management 管控面板上啟用標籤。AWS 使用標籤來分類您的成本，並提供每月成本分配報告給您。如需詳細資訊，請參閱關於 AWS 帳單與成本管理中的成本分配與[標記](#)。
- 控制對資源的存取。您可以在 AWS Identity and Access Management (IAM) 原則中使用控制 Amazon Kendra 資源存取的標籤。您可以將這些原則附加至 IAM 角色或使用者，以啟動以標籤為基礎的存取控制。如需詳細資訊，請參閱[基於標籤的授權](#)。

您可以使用 AWS Management Console、AWS Command Line Interface (AWS CLI) 或 Amazon Kendra API 建立和管理標籤。

標記資源

如果您使用 Amazon Kendra 主控台，您可以在建立資源時標記資源，或稍後新增資源。您也可以使用主控台更新或移除標籤。

如果您使用的是 AWS Command Line Interface (AWS CLI) 或 Amazon Kendra API，請使用下列操作來管理資源的標籤：

- [CreateDataSource](#) 建立資料來源時套用標籤。
- [CreateFaq](#) 建立常見問題集時套用標籤。
- [CreateIndex](#) 建立索引時套用標籤。
- [ListTagsForResource](#) 檢視與資源相關聯的標籤。
- [TagResource](#) 新增和修改資源的標籤。
- [UntagResource](#) 從資源中移除標籤。

標籤限制

下列限制適用於 Amazon Kendra 資源上的標籤：

- 標籤的最大數量 —50
- 最大金鑰長度 —128 個字元
- 最大值長度 —256 個字元
- 索引鍵和值的有效字元 — a—z、A—Z、空格及下列字元：_./=+-和 @
- 鍵和值會區分大小寫
- 請不要使用 aws：做為鍵的字首；它已保留供 AWS 使用

設置 Amazon Kendra

在使用 Amazon Kendra 之前，您必須擁有一個 Amazon Web Services (AWS) 帳戶。擁有 AWS 帳戶後，您可以透過 Amazon Kendra 主控台、 AWS Command Line Interface (AWS CLI) 或軟體開發套件存取亞馬遜 Kendra。 AWS

本指南包含 Java 和 Python 的 AWS CLI 範例。

主題

- [註冊成為 AWS](#)
- [區域與端點](#)
- [正在設定 AWS CLI](#)
- [設定 AWS 軟體開發套件](#)

註冊成為 AWS

當您註冊 Amazon Web Services (AWS) 時，您的帳戶會自動註冊中的所有服務 AWS，包括 Amazon Kendra。您只需支付實際使用服務的費用。

如果您已經有 AWS 帳號，請跳至下一個工作。若您尚未擁有 AWS 帳戶，請使用下列程序建立帳戶。

若要註冊 AWS

1. 開啟 <https://aws.amazon.com>，然後選擇「建立 AWS 帳戶」。
2. 依照畫面指示完成帳戶建立。請記下您的 12 位數字 AWS 帳戶號碼。部分註冊程序需接收來電，並使用電話鍵盤輸入 PIN 碼。
3. 建立 AWS Identity and Access Management (IAM) 管理員使用者。如需指示，請參閱[使用指南中的建立您的第一個 IAM AWS Identity and Access Management 使用者和群組](#)。

區域與端點

端點是指 web 服務進入點的 URL。每個端點都與特定 AWS 區域相關聯。如果您使用 Amazon Kendra 主控台 AWS CLI、和 Amazon Kendra 開發套件的組合，請注意其預設區域，因為指定行銷活動 (索引、查詢等) 的所有 Amazon Kendra 元件都必須在相同區域建立。如需 Amazon Kendra 支援的區域和端點，請參閱[區域和端點](#)。

正在設定 AWS CLI

命令 AWS 命令行界面 (AWS CLI) 是一種統一的開發人員工具，用於管理 AWS 服務，包括 Amazon Kendra。建議您安裝它。

1. 若要安裝 AWS CLI，請遵循《指[AWS 命令行界面使用者指南](#)》中的〈[安裝指AWS 命令行界面](#)〉中的指示。
2. 若要配置 AWS CLI 並設定要呼叫的設定檔 AWS CLI，請遵循《指AWS 命令行界面使用者指南》[AWS CLI中的〈配置〉](#)中的指示進行操作。
3. 若要確認設定 AWS CLI 檔已正確設定，請執行下列命令：

```
aws configure --profile default
```

如果已正確設定設定檔，則您看到的輸出將如下所示：

```
AWS Access Key ID [*****52FQ]:  
AWS Secret Access Key [*****xgyZ]:  
Default region name [us-west-2]:  
Default output format [json]:
```

4. 若要確認已設定 AWS CLI 為與 Amazon Kendra 搭配使用，請執行下列命令：

```
aws kendra help
```

如果設定 AWS CLI 正確，您會看到 Amazon Kendra、亞馬遜肯德拉執行階段和 Amazon Kendra 事件支援的 AWS CLI 命令清單。

設定 AWS 軟體開發套件

下載並安裝您要使用的 AWS SDK。本指南提供了有關 Python 的示例。如需其他 AWS 開發套件的相關資訊，請參閱 [Amazon Web Services 的工具](#)。

對於 Python SDK 的軟件包被稱為博托 3。

在運行下面的 Python 命令，你必須先下載並安裝 [Python 3.6 或更高版本](#) 為您的操作系統。對 Python 3.5 及更早版本的 Support 已被棄用。如果您的 Python 腳本目錄中沒有包含點子，則可以下載 [get-pip.py](#) 並將其存儲在腳本目錄中。您也可以使用終端程式將 Python 目錄設定為 [路徑或環境變數](#)。

```
# Install the latest Boto3 release via pip
pip install boto3

# You can install a specific version of Boto3 for compatibility reasons
# Install Boto3 version 1.0 specifically
pip install boto3==1.0.0

# Make sure Boto3 is no older than version 1.15.0
pip install boto3>=1.15.0

# Avoid versions of Boto3 newer than version 1.15.3
pip install boto3<=1.15.3
```

若要使用 Boto3，您必須使用 [IAM](#) 主控台為您的 AWS 帳戶設定身份驗證登入資料。

IAM 存取角色 Amazon Kendra

當您建立索引、AWS 資料來源或常見問題集時，Amazon Kendra 需要存取建立資源所需的 Amazon Kendra 資源。您必須先建立 AWS Identity and Access Management (IAM) 策略，然後再建立 Amazon Kendra 源。當您呼叫作業時，您會提供角色的 Amazon 資源名稱 (ARN)，並附加政策。例如，如果您要呼叫 [BatchPutDocument](#) API 以從值區新增文件，您會提供 Amazon Kendra 具有儲存 Amazon S3 貯體存取權限之政策的角色。

您可以在 Amazon Kendra 主控台中建立新 IAM 角色，或選擇要使用的 IAM 現有角色。主控台會顯示角色名稱中具有字串「kendra」或「Kendra」字串的角色。

下列主題提供必要原則的詳細資料。如果您使用 Amazon Kendra 主控台建立 IAM 角色，則會為您建立這些原則。

主題

- [IAM 索引的角色](#)
- [IAM 應用 BatchPutDocument 程式介面的角色](#)
- [IAM 資料來源的角色](#)
- [虛擬私有雲 \(VPC\) IAM 角色](#)
- [IAM 常見問題的角色](#)
- [IAM 查詢建議的角色](#)
- [IAM 使用者與群組之主參與者對應的角色](#)
- [IAM 角色 AWS IAM Identity Center](#)
- [IAM Amazon Kendra 體驗的角色](#)
- [IAM 自訂文件增強功能的角色](#)

IAM 索引的角色

建立索引時，您必須 IAM 提供具有寫入 Amazon CloudWatch。您還必須提供允許 Amazon Kendra 擔任該角色的信任策略。以下是必須提供的策略。

IAM 索引的角色

允許存取 CloudWatch 記錄檔 Amazon Kendra 的角色原則。

```
{
```

```

"Version": "2012-10-17",
"Statement": [
  {
    "Effect": "Allow",
    "Action": "cloudwatch:PutMetricData",
    "Resource": "*",
    "Condition": {
      "StringEquals": {
        "cloudwatch:namespace": "AWS/Kendra"
      }
    }
  },
  {
    "Effect": "Allow",
    "Action": "logs:DescribeLogGroups",
    "Resource": "*"
  },
  {
    "Effect": "Allow",
    "Action": "logs:CreateLogGroup",
    "Resource": "arn:aws:logs:your-region:your-account-id:log-group:/aws/
kendra/*"
  },
  {
    "Effect": "Allow",
    "Action": [
      "logs:DescribeLogStreams",
      "logs:CreateLogStream",
      "logs:PutLogEvents"
    ],
    "Resource": "arn:aws:logs:your-region:your-account-id:log-group:/aws/
kendra/*:log-stream:*"
  }
]
}

```

允許 Amazon Kendra 存取的角色原則 AWS Secrets Manager。如果您使用的使用者前後關聯 Secrets Manager 做為索引鍵位置，您可以使用下列原則。

```

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

```

```

    "Effect": "Allow",
    "Action": "cloudwatch:PutMetricData",
    "Resource": "*",
    "Condition": {
      "StringEquals": {
        "cloudwatch:namespace": "AWS/Kendra"
      }
    }
  },
  {
    "Effect": "Allow",
    "Action": "logs:DescribeLogGroups",
    "Resource": "*"
  },
  {
    "Effect": "Allow",
    "Action": "logs:CreateLogGroup",
    "Resource": "arn:aws:logs:your-region:your-account-id:log-group:/aws/kendra/*"
  },
  {
    "Effect": "Allow",
    "Action": [
      "logs:DescribeLogStreams",
      "logs:CreateLogStream",
      "logs:PutLogEvents"
    ],
    "Resource": "arn:aws:logs:your-region:your-account-id:log-group:/aws/kendra/
*:log-stream:*"
  },
  {
    "Effect": "Allow",
    "Action": [
      "secretsmanager:GetSecretValue"
    ],
    "Resource": [
      "arn:aws:secretsmanager:your-region:your-account-id:secret:secret-id"
    ]
  },
  {
    "Effect": "Allow",
    "Action": [
      "kms:Decrypt"
    ],
    "Resource": [

```

```

        "arn:aws:kms:your-region:your-account-id:key/key-id"
    ],
    "Condition":{
        "StringLike":{
            "kms:ViaService":[
                "secretsmanager.your-region.amazonaws.com"
            ]
        }
    }
}
]
}

```

允許擔任角色 Amazon Kendra 的信任原則。

```

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

```

IAM 應用 BatchPutDocument 程式介面的角色

Warning

Amazon Kendra 不使用將許可授予 Amazon Kendra 主體與 S3 儲存貯體互動的儲存貯體政策。而是使用 IAM 角色。請確定該成員 Amazon Kendra 未包含在儲存貯體政策中，以避免在意外授與任意主體權限時出現任何資料安全性問題。不過，您可以新增值區政策，以便跨不同帳戶使用 Amazon S3 儲存貯體。如需詳細資訊，請參閱 [Amazon S3 跨帳戶使用的策略](#)。如需 S3 資料來源 IAM 角色的相關資訊，請參閱 [IAM 角色](#)。

當您使用 [BatchPutDocument](#) API 為 Amazon S3 值區中的文件編製索引時，您必須 Amazon Kendra 提供可存取值區的 IAM 角色。您還必須提供允許 Amazon Kendra 擔任該角色的信任策略。如果值區中的文件已加密，您必須提供使用 AWS KMS 客戶主金鑰 (CMK) 解密文件的權限。

IAM 應用 BatchPutDocument 程式介面的角色

允許 Amazon Kendra 存取 Amazon S3 值區的必要角色原則。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetObject"
      ],
      "Resource": [
        "arn:aws:s3:::bucket-name/*"
      ]
    }
  ]
}
```

允許擔任角色 Amazon Kendra 的信任原則。

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

建議您將 `aws:sourceAccount` 和包含 `aws:sourceArn` 在信任原則中。這會限制權限，並安全地檢查 `aws:sourceArn` 是否 `aws:sourceAccount` 與 `sts:AssumeRole` 動作的 IAM 角色原則中提供的相

同，以及是否相同。這可防止未經授權的實體存取您的 IAM 角色及其權限。有關更多信息，請參閱有關[困惑的副問題](#)的 AWS Identity and Access Management 指南。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "kendra.amazonaws.com"
        ]
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "your-account-id"
        },
        "StringLike": {
          "aws:SourceArn": "arn:aws:kendra:your-region:your-account-id:index/*"
        }
      }
    }
  ]
}
```

可選角色政策，Amazon Kendra 允許使用 AWS KMS 客戶主金鑰 (CMK) 解密 Amazon S3 值區中的文件。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "kms:Decrypt"
      ],
      "Resource": [
        "arn:aws:kms:your-region:your-account-id:key/key-id"
      ]
    }
  ]
}
```

```
}
```

IAM 資料來源的角色

使用 [CreateDataSource](#) API 時，您必須授予 Amazon Kendra 具有資源存取權限的 IAM 角色。所需的特定權限取決於資料來源。

IAM Adobe 體驗管理員資料來源的角色

當您使用 Adobe 體驗管理員時，您會提供具有下列原則的角色。

- 存取 AWS Secrets Manager 密碼以驗證您的 Adobe 體驗管理員的權限。
- 呼叫 Adobe 體驗管理員連接器所需公用 API 的權限。
- 呼叫 `BatchPutDocument`、`BatchDeleteDocument`、`PutPrincipalMapping`、`DeletePrincipalMapping` 和 `ListGroupsOlderThanOrderingId` API 的權限。

Note

您可以透過將 Adobe 體驗管理員資料來源連線 Amazon Kendra 至 Amazon VPC。如果您使用的是 Amazon VPC，則需要新增 [其他權限](#)。

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

```

    "kms:Decrypt"
  ],
  "Resource": [
    "arn:aws:kms:{{your-region}}:{{your-account-id}}:key/[key-id]"
  ],
  "Condition": {
    "StringLike": {
      "kms:ViaService": [
        "secretsmanager.{{your-region}}.amazonaws.com"
      ]
    }
  }
},
{
  "Effect": "Allow",
  "Action": [
    "kendra:PutPrincipalMapping",
    "kendra>DeletePrincipalMapping",
    "kendra:ListGroupOlderThanOrderingId",
    "kendra:DescribePrincipalMapping"
  ],
  "Resource": ["arn:aws:kendra:{{your-region}}:{{your-account-id}}:index/{{index-id}}", "arn:aws:kendra:{{your-region}}:{{your-account-id}}:index/{{index-id}}/data-source/*"]
},
{
  "Effect": "Allow",
  "Action": [
    "kendra:BatchPutDocument",
    "kendra:BatchDeleteDocument"
  ],
  "Resource": "arn:aws:kendra:{{your-region}}:{{your-account-id}}:index/{{index-id}}"
}]
}

```

允許擔任角色 Amazon Kendra 的信任原則。

```

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

```

```

        "Service": "kendra.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}

```

IAM 戶外資料來源的角色

當您使用 Alfresco 時，您會提供具有下列政策的角色。

- 允許訪問您的 AWS Secrets Manager 密碼以驗證您的露天。
- 呼叫 Alfresco 連接器所需的公用 API 的權限。
- 呼
叫 BatchPutDocument、BatchDeleteDocumentPutPrincipalMappingDeletePrincipalMapping 和 ListGroupsOlderThanOrderingId API 的權限。

Note

您可以通過將露天資料來源連接到 Amazon Kendra。Amazon VPC 如果您使用的是 Amazon VPC，則需要新增 [其他權限](#)。

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "secretsmanager:GetSecretValue"
      ],
      "Resource": [
        "arn:aws:secretsmanager:{{your-region}}:{{your-account-id}}:secret:[secret-id]"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "kms:Decrypt"
      ],

```

```

"Resource": [
  "arn:aws:kms:{{your-region}}:{{your-account-id}}:key/[{{key-id}}]"
],
"Condition": {
  "StringLike": {
    "kms:ViaService": [
      "secretsmanager.{{your-region}}.amazonaws.com"
    ]
  }
}
},
{
  "Effect": "Allow",
  "Action": [
    "kendra:PutPrincipalMapping",
    "kendra>DeletePrincipalMapping",
    "kendra:ListGroupsWithOrderingId",
    "kendra:DescribePrincipalMapping"
  ],
  "Resource": ["arn:aws:kendra:{{your-region}}:{{your-account-id}}:index/{{index-id}}", "arn:aws:kendra:{{your-region}}:{{your-account-id}}:index/{{index-id}}/data-source/*"]
},
{
  "Effect": "Allow",
  "Action": [
    "kendra:BatchPutDocument",
    "kendra:BatchDeleteDocument"
  ],
  "Resource": "arn:aws:kendra:{{your-region}}:{{your-account-id}}:index/{{index-id}}"
}]
}

```

允許擔任角色 Amazon Kendra 的信任原則。

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "kendra.amazonaws.com"
      },

```

```

        "Action": "sts:AssumeRole"
    }
]
}

```

IAMAurora (MySQL) 資料來源的角色

當您使用 Aurora (MySQL) 時，您會提供具有下列原則的角色。

- 訪問您的 AWS Secrets Manager 密碼以驗證您的 Aurora (MySQL) 的權限。
- 呼叫 Aurora (MySQL) 連接器所需公用 API 的權限。
- 呼叫 BatchPutDocument、BatchDeleteDocumentPutPrincipalMappingDeletePrincipalMapping 和 ListGroupsOlderThanOrderingId API 的權限。

Note

您可以透過將 Aurora (MySQL) 資料來源連 Amazon Kendra 接到 Amazon VPC。如果您使用的是 Amazon VPC，則需要新增 [其他權限](#)。

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "secretsmanager:GetSecretValue"
      ],
      "Resource": [
        "arn:aws:secretsmanager:{{region}}:{{account_id}}:secret:[secret_id]"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "kms:Decrypt"
      ],
      "Resource": [
        "arn:aws:kms:{{region}}:{{account_id}}:key/[key_id]"
      ]
    }
  ]
}

```

```

    ],
    "Condition": {
      "StringLike": {
        "kms:ViaService": [
          "secretsmanager.*.amazonaws.com"
        ]
      }
    }
  },
  {
    "Effect": "Allow",
    "Action": [
      "kendra:PutPrincipalMapping",
      "kendra>DeletePrincipalMapping",
      "kendra:ListGroupsWithOrderingId",
      "kendra:DescribePrincipalMapping"
    ],
    "Resource": ["arn:aws:kendra:{{region}}:{{account_id}}:index/{{index_id}}",
"arn:aws:kendra:{{region}}:{{account_id}}:index/{{index_id}}/data-source/*"]
  },
  {
    "Effect": "Allow",
    "Action": [
      "kendra:BatchPutDocument",
      "kendra:BatchDeleteDocument"
    ],
    "Resource": "arn:aws:kendra:{{region}}:{{account_id}}:index/{{index_id}}"
  }
]
}

```

允許擔任角色 Amazon Kendra 的信任原則。

```

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

```

}

IAMAurora (PostgreSQL) 資料來源的角色

當您使用 Aurora (PostgreSQL) 時，您會提供具有下列原則的角色。

- 存取您的 AWS Secrets Manager 密碼以驗證您的 Aurora (PostgreSQL) 的權限。
- 呼叫 Aurora (PostgreSQL) 連接器所需公用 API 的權限。
- 呼叫 BatchPutDocument、BatchDeleteDocumentPutPrincipalMappingDeletePrincipalMapping 和 ListGroupsOlderThanOrderingId API 的權限。

Note

您可以透過以下方式將 Aurora (PostgreSQL) 資料來源連線到 Amazon Kendra . Amazon VPC 如果您使用的是 Amazon VPC，則需要新增[其他權限](#)。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "secretsmanager:GetSecretValue"
      ],
      "Resource": [
        "arn:aws:secretsmanager:{{region}}:{{account_id}}:secret:[secret_id]"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "kms:Decrypt"
      ],
      "Resource": [
        "arn:aws:kms:{{region}}:{{account_id}}:key/[key_id]"
      ],
      "Condition": {
        "StringLike": {
```



```

        "kms:ViaService": [
            "secretsmanager.*.amazonaws.com"
        ]
    }
},
{
    "Effect": "Allow",
    "Action": [
        "kendra:PutPrincipalMapping",
        "kendra:DeletePrincipalMapping",
        "kendra:ListGroupsWithOrderingId",
        "kendra:DescribePrincipalMapping"
    ],
    "Resource": ["arn:aws:kendra:{{region}}:{{account_id}}:index/{{index_id}}",
"arn:aws:kendra:{{region}}:{{account_id}}:index/{{index_id}}/data-source/*"]
},
{
    "Effect": "Allow",
    "Action": [
        "kendra:BatchPutDocument",
        "kendra:BatchDeleteDocument"
    ],
    "Resource": "arn:aws:kendra:{{region}}:{{account_id}}:index/{{index_id}}"
}]
}

```

允許擔任角色 Amazon Kendra 的信任原則。

```

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

```

IAM Amazon FSx 資料來源的角色

使用時 Amazon FSx，您會提供具有下列原則的角色。

- 存取 AWS Secrets Manager 密碼以驗證您的 Amazon FSx 檔案系統的權限。
- 存取 Amazon FSx 檔案系統所在位置 Amazon Virtual Private Cloud (VPC) 的權限。
- 取得 Amazon FSx 檔案系統使用中目錄網域名稱的權限。
- 呼叫 Amazon FSx 連接器所需公用 API 的權限。
- 呼叫 BatchPutDocument 和 BatchDeleteDocument API 以更新索引的權限。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "secretsmanager:GetSecretValue"
      ],
      "Resource": [
        "arn:aws:secretsmanager:{{your-region}}:{{your-account-id}}:secret:
{{secret-id}}"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "kms:Decrypt"
      ],
      "Resource": [
        "arn:aws:kms:{{your-region}}:{{your-account-id}}:key/{{key-id}}"
      ],
      "Condition": {
        "StringLike": {
          "kms:ViaService": [
            "secretsmanager.{{your-region}}.amazonaws.com"
          ]
        }
      }
    }
  ],
  {
    "Effect": "Allow",
```

```

    "Action": [
      "ec2:CreateNetworkInterface",
      "ec2>DeleteNetworkInterface"
    ],
    "Resource": [
      "arn:aws:ec2:{{your-region}}:{{your-account-id}}:network-interface/*",
      "arn:aws:ec2:{{your-region}}:{{your-account-id}}:subnet/[[subnet-ids]]"
    ]
  },
  {
    "Effect": "Allow",
    "Action": [
      "ec2:DescribeSubnets",
      "ec2:DescribeNetworkInterfaces"
    ],
    "Resource": "*"
  },
  {
    "Effect": "Allow",
    "Action": [
      "ec2:CreateNetworkInterfacePermission"
    ],
    "Resource": "arn:aws:ec2:{{your-region}}:{{your-account-id}}:network-
interface/*",
    "Condition": {
      "StringEquals": {
        "ec2:AuthorizedService": "kendra.*.amazonaws.com"
      },
      "ArnEquals": {
        "ec2:Subnet": [
          "arn:aws:ec2:{{your-region}}:{{your-account-id}}:subnet/[[subnet-ids]]"
        ]
      }
    }
  },
  {
    "Sid": "AllowsKendraToGetDomainNameOfActiveDirectory",
    "Effect": "Allow",
    "Action": "ds:DescribeDirectories",
    "Resource": "*"
  },
  {
    "Sid": "AllowsKendraToCallRequiredFsxAPIs",
    "Effect": "Allow",

```

```

    "Action": [
      "fsx:DescribeFileSystems"
    ],
    "Resource": "*"
  },
  {
    "Sid": "iamPassRole",
    "Effect": "Allow",
    "Action": "iam:PassRole",
    "Resource": "*",
    "Condition": {
      "StringEquals": {
        "iam:PassedToService": [
          "kendra.*.amazonaws.com"
        ]
      }
    }
  },
  {
    "Effect": "Allow",
    "Action": [
      "kendra:BatchPutDocument",
      "kendra:BatchDeleteDocument"
    ],
    "Resource": "arn:aws:kendra:{{your-region}}:{{your-account-id}}:index/
    {{index-id}}"
  }
]
}

```

允許擔任角色 Amazon Kendra 的信任原則。

```

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

```

```
}
```

IAM 資料庫資料來源的角色

當您使用資料庫做為資料來源時，您會 Amazon Kendra 提供一個角色，該角色具有連線到。其中包含：

- 存取包含網站使用者名稱和密碼之密碼的權限。AWS Secrets Manager 有關密碼內容的詳細資訊，請參閱[資料來源](#)。
- 使用 AWS KMS 客戶主要金鑰 (CMK) 解密儲存的使用者名稱和密碼密碼的 Secrets Manager 權限。
- 使用 BatchPutDocument 和作 BatchDeleteDocument 業更新索引的權限。
- 存取包含用於與網站通訊之 SSL 憑證的 Amazon S3 值區的權限。

Note

您可以透過將資料庫資料來源連線 Amazon Kendra 到 Amazon VPC。如果您使用的是 Amazon VPC，則需要新增[其他權限](#)。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "secretsmanager:GetSecretValue"
      ],
      "Resource": [
        "arn:aws:secretsmanager:your-region:your-account-id:secret:secret-id"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "kms:Decrypt"
      ],
      "Resource": [
        "arn:aws:kms:your-region:your-account-id:key/key-id"
      ]
    }
  ]
}
```

```

    },
    {
      "Effect": "Allow",
      "Action": [
        "kendra:BatchPutDocument",
        "kendra:BatchDeleteDocument"
      ],
      "Resource": [
        "arn:aws:kendra:your-region:your-account-id:index/index-id"
      ],
      "Condition": {
        "StringLike": {
          "kms:ViaService": [
            "kendra.your-region.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetObject"
      ],
      "Resource": [
        "arn:aws:s3:::bucket-name/*"
      ]
    }
  ]
}

```

您可以搭配資料來源使用兩種選擇性原則。

如果您已加密包含用於與通訊之 SSL 憑證的儲存 Amazon S3 貯體，請提供授予金鑰 Amazon Kendra 存取權的政策。

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "kms:Decrypt"
      ],
      "Resource": [

```

```

        "arn:aws:kms:your-region:your-account-id:key/key-id"
    ]
}
]
}

```

如果您使用的是 VPC，請提供可 Amazon Kendra 存取所需資源的原則。[如需所需原則，請參閱資料來源的IAM 角色、VPC。](#)

允許擔任角色 Amazon Kendra 的信任原則。

```

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

```

IAM 角色 Amazon RDS (Microsoft SQL 伺服器) 資料來源

當您使用 Amazon RDS (Microsoft SQL Server) 資料來源連接器時，您會提供具有下列原則的角色。

- 存取 AWS Secrets Manager 密碼以驗證您 Amazon RDS (Microsoft SQL Server) 資料來源執行個體的權限。
- 呼叫 Amazon RDS (Microsoft SQL Server) 資料來源連接器所需公用 API 的權限。
- 呼叫 BatchPutDocument、BatchDeleteDocumentPutPrincipalMappingDeletePrincipalMapping 和 ListGroupsOlderThanOrderingId API 的權限。

Note

您可以通過將 Amazon RDS (Microsoft SQL 服務器) 數據源連 Amazon Kendra 接到 Amazon VPC。如果您使用的是 Amazon VPC，則需要新增[其他權限](#)。

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "secretsmanager:GetSecretValue"
      ],
      "Resource": [
        "arn:aws:secretsmanager:{{region}}:{{account_id}}:secret:[secret_id]"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "kms:Decrypt"
      ],
      "Resource": [
        "arn:aws:kms:{{region}}:{{account_id}}:key/[key_id]"
      ],
      "Condition": {
        "StringLike": {
          "kms:ViaService": [
            "secretsmanager.*.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": [
        "kendra:PutPrincipalMapping",
        "kendra>DeletePrincipalMapping",
        "kendra:ListGroupsWithOrderingId",
        "kendra:DescribePrincipalMapping"
      ],
      "Resource": ["arn:aws:kendra:{{region}}:{{account_id}}:index/{{index_id}}",
        "arn:aws:kendra:{{region}}:{{account_id}}:index/{{index_id}}/data-source/*"]
    },
    {
      "Effect": "Allow",
      "Action": [
        "kendra:BatchPutDocument",

```



```

    "kendra:BatchDeleteDocument"
  ],
  "Resource": "arn:aws:kendra:{{region}}:{{account_id}}:index/{{index_id}}"
}]
}

```

允許擔任角色 Amazon Kendra 的信任原則。

```

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

```

IAM Amazon RDS (MySQL) 資料來源的角色

當您使用 Amazon RDS (MySQL) 資料來源連接器時，您會提供具有下列原則的角色。

- 存取 AWS Secrets Manager 密碼以驗證您的 Amazon RDS (MySQL) 資料來源執行個體的權限。
- 呼叫 Amazon RDS (MySQL) 資料來源連接器所需公用 API 的權限。
- 呼叫 `BatchPutDocument`、`BatchDeleteDocument`、`PutPrincipalMapping`、`DeletePrincipalMapping` 和 `ListGroupsOlderThanOrderingId` API 的權限。

Note

您可以透過將 Amazon RDS (MySQL) 資料來源連 Amazon Kendra 接到 Amazon VPC。如果您使用的是 Amazon VPC，則需要新增[其他權限](#)。

```

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

```

```

"Statement": [
  {
    "Effect": "Allow",
    "Action": [
      "secretsmanager:GetSecretValue"
    ],
    "Resource": [
      "arn:aws:secretsmanager:{{region}}:{{account_id}}:secret:[secret_id]"
    ]
  },
  {
    "Effect": "Allow",
    "Action": [
      "kms:Decrypt"
    ],
    "Resource": [
      "arn:aws:kms:{{region}}:{{account_id}}:key/[key_id]"
    ],
    "Condition": {
      "StringLike": {
        "kms:ViaService": [
          "secretsmanager.*.amazonaws.com"
        ]
      }
    }
  },
  {
    "Effect": "Allow",
    "Action": [
      "kendra:PutPrincipalMapping",
      "kendra>DeletePrincipalMapping",
      "kendra:ListGroupsWithOrderingId",
      "kendra:DescribePrincipalMapping"
    ],
    "Resource": ["arn:aws:kendra:{{region}}:{{account_id}}:index/{{index_id}}",
      "arn:aws:kendra:{{region}}:{{account_id}}:index/{{index_id}}/data-source/*"]
  },
  {
    "Effect": "Allow",
    "Action": [
      "kendra:BatchPutDocument",
      "kendra:BatchDeleteDocument"
    ],
    "Resource": "arn:aws:kendra:{{region}}:{{account_id}}:index/{{index_id}}"]
  }
]

```

```
  ]]
}
```

允許擔任角色 Amazon Kendra 的信任原則。

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

IAM Amazon RDS (Oracle) 資料來源的角色

當您使用 Amazon RDS Oracle 資料來源連接器時，您會提供具有下列原則的角色。

- 存取 AWS Secrets Manager 密碼以驗證 Amazon RDS (Oracle) 資料來源執行環境的權限。
- 呼叫 Amazon RDS (Oracle) 資料來源連接器所需公用 API 的權限。
- 呼叫 BatchPutDocument、BatchDeleteDocumentPutPrincipalMappingDeletePrincipalMapping 和 ListGroupsOlderThanOrderingId API 的權限。

Note

您可以透過將 Amazon RDS Oracle 資料來源連線 Amazon Kendra 到 Amazon VPC。如果您使用的是 Amazon VPC，則需要新增[其他權限](#)。

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

```

    "Action": [
      "secretsmanager:GetSecretValue"
    ],
    "Resource": [
      "arn:aws:secretsmanager:{{region}}:{{account_id}}:secret:[secret_id]"
    ]
  },
  {
    "Effect": "Allow",
    "Action": [
      "kms:Decrypt"
    ],
    "Resource": [
      "arn:aws:kms:{{region}}:{{account_id}}:key/[key_id]"
    ],
    "Condition": {
      "StringLike": {
        "kms:ViaService": [
          "secretsmanager.*.amazonaws.com"
        ]
      }
    }
  },
  {
    "Effect": "Allow",
    "Action": [
      "kendra:PutPrincipalMapping",
      "kendra>DeletePrincipalMapping",
      "kendra:ListGroupsWithOrderingId",
      "kendra:DescribePrincipalMapping"
    ],
    "Resource": ["arn:aws:kendra:{{region}}:{{account_id}}:index/{{index_id}}",
      "arn:aws:kendra:{{region}}:{{account_id}}:index/{{index_id}}/data-source/*"
    ],
  },
  {
    "Effect": "Allow",
    "Action": [
      "kendra:BatchPutDocument",
      "kendra:BatchDeleteDocument"
    ],
    "Resource": "arn:aws:kendra:{{region}}:{{account_id}}:index/{{index_id}}"
  }
]
}

```

允許擔任角色 Amazon Kendra 的信任原則。

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

IAM Amazon RDS (PostgreSQL) 資料來源的角色

當您使用 Amazon RDS (PostgreSQL) 資料來源連接器時，您會提供具有下列原則的角色。

- 存取 AWS Secrets Manager 密碼以驗證您的 Amazon RDS (PostgreSQL) 資料來源執行個體的權限。
- 呼叫 Amazon RDS (PostgreSQL) 資料來源連接器所需公用 API 的權限。
- 呼叫 BatchPutDocument、BatchDeleteDocumentPutPrincipalMappingDeletePrincipalMapping 和 ListGroupsOlderThanOrderingId API 的權限。

Note

您可以透過以下方式將 Amazon RDS (PostgreSQL) 資料來源連線到 Amazon Kendra . Amazon VPC 如果您使用的是 Amazon VPC，則需要新增[其他權限](#)。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "secretsmanager:GetSecretValue"
      ]
    }
  ]
}
```

```

    ],
    "Resource": [
      "arn:aws:secretsmanager:{{region}}:{{account_id}}:secret:[{{secret_id}}]"
    ]
  },
  {
    "Effect": "Allow",
    "Action": [
      "kms:Decrypt"
    ],
    "Resource": [
      "arn:aws:kms:{{region}}:{{account_id}}:key/[{{key_id}}]"
    ],
    "Condition": {
      "StringLike": {
        "kms:ViaService": [
          "secretsmanager.*.amazonaws.com"
        ]
      }
    }
  },
  {
    "Effect": "Allow",
    "Action": [
      "kendra:PutPrincipalMapping",
      "kendra>DeletePrincipalMapping",
      "kendra:ListGroupsWithOrderingId",
      "kendra:DescribePrincipalMapping"
    ],
    "Resource": ["arn:aws:kendra:{{region}}:{{account_id}}:index/{{index_id}}",
      "arn:aws:kendra:{{region}}:{{account_id}}:index/{{index_id}}/data-source/*"
    ],
  },
  {
    "Effect": "Allow",
    "Action": [
      "kendra:BatchPutDocument",
      "kendra:BatchDeleteDocument"
    ],
    "Resource": "arn:aws:kendra:{{region}}:{{account_id}}:index/{{index_id}}"
  }
]
}

```

允許擔任角色 Amazon Kendra 的信任原則。

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

IAM Amazon S3 資料來源的角色

Warning

Amazon Kendra 不使用將許可授予 Amazon Kendra 主體與 S3 儲存貯體互動的儲存貯體政策。而是使用 IAM 角色。請確定該成員 Amazon Kendra 未包含在儲存貯體政策中，以避免在意外授與任意主體權限時出現任何資料安全性問題。不過，您可以新增值區政策，以便跨不同帳戶使用 Amazon S3 儲存貯體。如需詳細資訊，請參閱 [Amazon S3 跨帳戶使用的策略](#) (向下捲動)。

當您使用 Amazon S3 值區做為資料來源時，您需要提供具有存取值區以及使用 BatchPutDocument 和 BatchDeleteDocument 作業之權限的角色。如果 Amazon S3 值區中的文件已加密，您必須提供使用 AWS KMS 客戶主金鑰 (CMK) 解密文件的權限。

下列角色原則必須 Amazon Kendra 允許擔任角色。進一步向下捲動以檢視要擔任角色的信任原則。

允許 Amazon Kendra 將 Amazon S3 值區用作資料來源的必要角色原則。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "s3:GetObject"
      ],
      "Resource": [
        "arn:aws:s3:::bucket-name/*"
      ]
    }
  ]
}
```

```

    ],
    "Effect": "Allow"
  },
  {
    "Action": [
      "s3:ListBucket"
    ],
    "Resource": [
      "arn:aws:s3:::bucket-name"
    ],
    "Effect": "Allow"
  },
  {
    "Effect": "Allow",
    "Action": [
      "kendra:BatchPutDocument",
      "kendra:BatchDeleteDocument"
    ],
    "Resource": [
      "arn:aws:kendra:your-region:your-account-id:index/index-id"
    ]
  }
]
}

```

可選角色政策，Amazon Kendra 允許使用 AWS KMS 客戶主金鑰 (CMK) 解密 Amazon S3 值區中的文件。

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "kms:Decrypt"
      ],
      "Resource": [
        "arn:aws:kms:your-region:your-account-id:key/key-id"
      ]
    }
  ]
}

```


選用角色原則，可 Amazon Kendra 讓您在使用、且不啟動 AWS KMS 或共用 AWS KMS 權 Amazon VPC 限的情況下存取 Amazon S3 值區。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "s3:GetObject"
      ],
      "Resource": [
        "arn:aws:s3:::{{bucket-name}}/*"
      ],
      "Effect": "Allow"
    },
    {
      "Action": [
        "s3:ListBucket"
      ],
      "Resource": [
        "arn:aws:s3:::{{bucket-name}}"
      ],
      "Effect": "Allow"
    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2:CreateNetworkInterface"
      ],
      "Resource": [
        "arn:aws:ec2:{{your-region}}:{{your-account-id}}:subnet/[[subnet-ids]]",
        "arn:aws:ec2:{{your-region}}:{{your-account-id}}:security-group/[[security-
group]]"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2:CreateNetworkInterface"
      ],
      "Resource": "arn:aws:ec2:{{your-region}}:{{your-account-id}}:network-interface/
**",
      "Condition": {
```

```

        "StringLike": {
            "aws:RequestTag/AWS_KENDRA": "kendra_{{your-account-id}}_{{index-
id}}_{{data-source-id}}_*"
        }
    },
    {
        "Effect": "Allow",
        "Action": [
            "ec2:CreateTags"
        ],
        "Resource": "arn:aws:ec2:{{your-region}}:{{your-account-id}}:network-interface/
*",
        "Condition": {
            "StringEquals": {
                "ec2:CreateAction": "CreateNetworkInterface"
            }
        }
    },
    {
        "Effect": "Allow",
        "Action": [
            "ec2:DescribeSubnets"
        ],
        "Resource": "*"
    },
    {
        "Effect": "Allow",
        "Action": [
            "ec2:DescribeNetworkInterfaces"
        ],
        "Resource": "*"
    },
    {
        "Effect": "Allow",
        "Action": [
            "ec2:CreateNetworkInterfacePermission"
        ],
        "Resource": "arn:aws:ec2:{{your-region}}:{{your-account-id}}:network-interface/
*",
        "Condition": {
            "StringEquals": {
                "ec2:AuthorizedService": "kendra.amazonaws.com"
            }
        },

```

```

    "ArnEquals": {
      "ec2:Subnet": [
        "arn:aws:ec2:{{your-region}}:{{your-account-id}}:subnet/[{{subnet-ids}}]"
      ]
    }
  },
  {
    "Effect": "Allow",
    "Action": [
      "kendra:PutPrincipalMapping",
      "kendra>DeletePrincipalMapping",
      "kendra:ListGroupsWithOrderingId",
      "kendra:DescribePrincipalMapping"
    ],
    "Resource": [
      "arn:aws:kendra:{{your-region}}:{{your-account-id}}:index/{{index-id}}",
      "arn:aws:kendra:{{your-region}}:{{your-account-id}}:index/{{index-id}}/data-
source/*"
    ]
  },
  {
    "Effect": "Allow",
    "Action": [
      "kendra:BatchPutDocument",
      "kendra:BatchDeleteDocument"
    ],
    "Resource": "arn:aws:kendra:{{your-region}}:{{your-account-id}}:index/{{index-
id}}*"
  }
]
}

```

一種可選角色策略，Amazon Kendra 允許在使用時訪問 Amazon S3 值區 Amazon VPC，並激活了 AWS KMS 權限。

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "s3:GetObject"
      ],

```

```

    "Resource": [
      "arn:aws:s3:::{{bucket-name}}/*"
    ],
    "Effect": "Allow"
  },
  {
    "Action": [
      "s3:ListBucket"
    ],
    "Resource": [
      "arn:aws:s3:::{{bucket-name}}"
    ],
    "Effect": "Allow"
  },
  {
    "Effect": "Allow",
    "Action": [
      "kms:Decrypt"
    ],
    "Resource": [
      "arn:aws:kms:{{your-region}}:{{your-account-id}}:key/{{key-id}}"
    ],
    "Condition": {
      "StringLike": {
        "kms:ViaService": [
          "s3.{{your-region}}.amazonaws.com"
        ]
      }
    }
  },
  {
    "Effect": "Allow",
    "Action": [
      "ec2:CreateNetworkInterface"
    ],
    "Resource": [
      "arn:aws:ec2:{{your-region}}:{{your-account-id}}:subnet/[{{subnet-ids}}]",
      "arn:aws:ec2:{{your-region}}:{{your-account-id}}:security-group/[{{security-group}}]"
    ]
  },
  {
    "Effect": "Allow",
    "Action": [

```

```

        "ec2:CreateNetworkInterface"
    ],
    "Resource": "arn:aws:ec2:{{your-region}}:{{your-account-id}}:network-interface/
**",
    "Condition": {
        "StringLike": {
            "aws:RequestTag/AWS_KENDRA": "kendra_{{your-account-id}}_{{index-
id}}_{{data-source-id}}_*"
        }
    }
},
{
    "Effect": "Allow",
    "Action": [
        "ec2:CreateTags"
    ],
    "Resource": "arn:aws:ec2:{{your-region}}:{{your-account-id}}:network-interface/
**",
    "Condition": {
        "StringEquals": {
            "ec2:CreateAction": "CreateNetworkInterface"
        }
    }
},
{
    "Effect": "Allow",
    "Action": [
        "ec2:DescribeSubnets"
    ],
    "Resource": "*"
},
{
    "Effect": "Allow",
    "Action": [
        "ec2:DescribeNetworkInterfaces"
    ],
    "Resource": "*"
},
{
    "Effect": "Allow",
    "Action": [
        "ec2:CreateNetworkInterfacePermission"
    ],

```

```

    "Resource": "arn:aws:ec2:{{your-region}}:{{your-account-id}}:network-interface/
*",
    "Condition": {
      "StringEquals": {
        "ec2:AuthorizedService": "kendra.amazonaws.com"
      },
      "ArnEquals": {
        "ec2:Subnet": [
          "arn:aws:ec2:{{your-region}}:{{your-account-id}}:subnet/[{{subnet-ids}}]"
        ]
      }
    },
  },
  {
    "Effect": "Allow",
    "Action": [
      "kendra:PutPrincipalMapping",
      "kendra>DeletePrincipalMapping",
      "kendra:ListGroupsWithOrderingId",
      "kendra:DescribePrincipalMapping"
    ],
    "Resource": [
      "arn:aws:kendra:{{your-region}}:{{your-account-id}}:index/{{index-id}}",
      "arn:aws:kendra:{{your-region}}:{{your-account-id}}:index/{{index-id}}/data-
source/*"
    ]
  },
  {
    "Effect": "Allow",
    "Action": [
      "kendra:BatchPutDocument",
      "kendra:BatchDeleteDocument"
    ],
    "Resource": "arn:aws:kendra:{{your-region}}:{{your-account-id}}:index/{{index-
id}}*"
  }
]
}

```

允許擔任角色 Amazon Kendra 的信任原則。

```

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

```

```

    "Statement": [
      {
        "Effect": "Allow",
        "Principal": {
          "Service": "kendra.amazonaws.com"
        },
        "Action": "sts:AssumeRole"
      }
    ]
  }

```

Amazon S3 跨帳戶使用的策略

如果您的 Amazon S3 值區與 Amazon Kendra 索引所使用的帳戶位於不同的帳戶中，您可以建立政策以跨帳戶使用。

當 Amazon S3 值區位於 Amazon Kendra 索引的不同帳戶時，使用值區做為資料來源的角色政策。請注意，s3:PutObject和s3:PutObjectAcl是可選的，如果您想要在[存取控制清單中包含組態檔案](#)，請使用此選項。

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "s3:GetObject"
      ],
      "Resource": [
        "arn:aws:s3:::$bucket-in-other-account/*"
      ],
      "Effect": "Allow"
    },
    {
      "Action": [
        "s3:ListBucket"
      ],
      "Resource": [
        "arn:aws:s3:::$bucket-in-other-account/*"
      ],
      "Effect": "Allow"
    },
    {
      "Effect": "Allow",

```

```

    "Action": [
      "kendra:BatchPutDocument",
      "kendra:BatchDeleteDocument"
    ],
    "Resource": [
      "arn:aws:kendra:$your-region:$your-account-id:index/$index-id"
    ]
  },
  {
    "Effect": "Allow",
    "Action": [
      "s3:GetObject",
      "s3:PutObject",
      "s3:PutObjectAcl"
    ],
    "Resource": "arn:aws:s3:::$bucket-in-other-account/*"
  }
]
}

```

儲存貯體政策，允許 Amazon S3 資料來源角色跨帳戶存取 Amazon S3 值區。請注意，s3:PutObject和s3:PutObjectAcl是可選的，如果您想要在[存取控制清單中包含組態檔案](#)，請使用此選項。

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "$kendra-s3-connector-role-arn"
      },
      "Action": [
        "s3:GetObject",
        "s3:PutObject",
        "s3:PutObjectAcl"
      ],
      "Resource": [
        "arn:aws:s3:::$bucket-in-other-account/*"
      ]
    },
    {
      "Effect": "Allow",

```



```

    "Principal": {
      "AWS": "$kendra-s3-connector-role-arn"
    },
    "Action": "s3:ListBucket",
    "Resource": "arn:aws:s3:::$bucket-in-other-account"
  }
]
}

```

允許擔任角色 Amazon Kendra 的信任原則。

```

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

```

IAM Amazon Kendra Web 爬行者程式資料來源的角色

當您使用 Amazon Kendra Web 爬行者程式時，您會提供具有下列原則的角色：

- 存取密碼的權限，該 AWS Secrets Manager 密碼包含憑證以連線到網站或基本驗證支援的 Web Proxy 伺服器。如需有關密碼內容的詳細資訊，請參閱[使用網路爬行者程式資料來源](#)。
- 使用 AWS KMS 客戶主要金鑰 (CMK) 解密儲存的使用者名稱和密碼密碼的 Secrets Manager 權限。
- 使用 BatchPutDocument 和作 BatchDeleteDocument 業更新索引的權限。
- 如果您使用 Amazon S3 值區來儲存種子 URL 或網站地圖清單，請提供存取 Amazon S3 值區的權限。

Note

您可以透過將「Amazon Kendra Web 爬行者程式」資料來源連線 Amazon Kendra 到 Amazon VPC。如果您使用的是 Amazon VPC，則需要新增[其他權限](#)。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "secretsmanager:GetSecretValue"
      ],
      "Resource": [
        "arn:aws:secretsmanager:your-region:your-account-id:secret:secret-id"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "kms:Decrypt"
      ],
      "Resource": [
        "arn:aws:kms:your-region:your-account:key/key-id"
      ],
      "Condition": {
        "StringLike": {
          "kms:ViaService": [
            "secretsmanager.your-region.amazonaws.com"
          ]
        }
      }
    }
  ],
  {
    "Effect": "Allow",
    "Action": [
      "kendra:BatchPutDocument",
      "kendra:BatchDeleteDocument"
    ],
    "Resource": "arn:aws:kendra:your-region:your-account-id:index/index-id"
  }
}]
```

```
}

```

如果您將種子 URL 或網站地圖儲存在 Amazon S3 值區中，則必須將此權限新增至該角色。

```
,
{"Effect": "Allow",
  "Action": [
    "s3:GetObject"
  ],
  "Resource": [
    "arn:aws:s3:::bucket-name/*"
  ]
}

```

允許擔任角色 Amazon Kendra 的信任原則。

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

```

IAM Amazon WorkDocs 資料來源的角色

使用時 Amazon WorkDocs，您會提供具有下列原則的角色

- 驗證與 Amazon WorkDocs 場地存放庫對應的目錄 ID (組織 ID) 的權限。
- 獲取包含 Amazon WorkDocs 站點目錄的活動目錄的域名的權限。
- 呼叫 Amazon WorkDocs 連接器所需公用 API 的權限。
- 呼叫 BatchPutDocument 和 BatchDeleteDocument API 以更新索引的權限。

```
{

```

```
"Version": "2012-10-17",
"Statement": [
  {
    "Sid": "AllowsKendraToGetDomainNameOfActiveDirectory",
    "Effect": "Allow",
    "Action": "ds:DescribeDirectories",
    "Resource": "*"
  },
  {
    "Sid": "AllowsKendraToCallRequiredWorkDocsAPIs",
    "Effect": "Allow",
    "Action": [
      "workdocs:GetDocumentPath",
      "workdocs:GetGroup",
      "workdocs:GetDocument",
      "workdocs:DownloadDocumentVersions",
      "workdocs:DescribeUsers",
      "workdocs:DescribeFolderContents",
      "workdocs:DescribeActivities",
      "workdocs:DescribeComments",
      "workdocs:GetFolder",
      "workdocs:DescribeResourcePermissions",
      "workdocs:GetFolderPath",
      "workdocs:DescribeInstances"
    ],
    "Resource": "*"
  },
  {
    "Sid": "iamPassRole",
    "Effect": "Allow",
    "Action": "iam:PassRole",
    "Resource": "*",
    "Condition": {
      "StringEquals": {
        "iam:PassedToService": [
          "kendra.amazonaws.com"
        ]
      }
    }
  },
  {
    "Sid": "AllowsKendraToCallBatchPutDeleteAPIs",
    "Effect": "Allow",
    "Action": [
```

```

    "kendra:BatchPutDocument",
    "kendra:BatchDeleteDocument"
  ],
  "Resource": [
    "arn:aws:kendra:your-region:account-id:index/$index-id"
  ]
}
]
}

```

允許擔任角色 Amazon Kendra 的信任原則。

```

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

```

IAM Box 資料來源的角色

當您使用 Box 時，您會提供具有下列原則的角色。

- 存取 AWS Secrets Manager 密碼以驗證您的 Slack 的權限。
- 呼叫 Box 連接器所需公用 API 的權限。
- 呼
叫 BatchPutDocument、BatchDeleteDocumentPutPrincipalMappingDeletePrincipalMapping 和 ListGroupsOlderThanOrderingId API 的權限。

Note

您可以透過將 Box 資料來源連 Amazon Kendra 接到 Amazon VPC。如果您使用的是 Amazon VPC，則需要新增 [其他權限](#)。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "secretsmanager:GetSecretValue"
      ],
      "Resource": [
        "arn:aws:secretsmanager:{{your-region}}:{{your-account-id}}:secret:[secret-id]"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "kms:Decrypt"
      ],
      "Resource": [
        "arn:aws:kms:{{your-region}}:{{your-account-id}}:key/[key-id]"
      ],
      "Condition": {
        "StringLike": {
          "kms:ViaService": [
            "secretsmanager.{{your-region}}.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": [
        "kendra:PutPrincipalMapping",
        "kendra>DeletePrincipalMapping",
        "kendra:ListGroupOlderThanOrderingId",
        "kendra:DescribePrincipalMapping"
      ],
      "Resource": ["arn:aws:kendra:{{your-region}}:{{your-account-d}}:index/{{index-id}}", "arn:aws:kendra:{{your-region}}:{{your-account-id}}:index/{{index-id}}/data-source/*"]
    },
    {
      "Effect": "Allow",
      "Action": [
```

```

    "kendra:BatchPutDocument",
    "kendra:BatchDeleteDocument"
  ],
  "Resource": "arn:aws:kendra:{{your-region}}:{{your-account-id}}:index/{{index-id}}"
}]
}

```

允許擔任角色 Amazon Kendra 的信任原則。

```

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

```

IAM 匯流資料來源的角色

IAM 角色匯流連接器 V1.0

當您使用 Confluence 伺服器做為資料來源時，您會提供具有下列原則的角色：

- 訪問包含連接到匯流所需憑據的 AWS Secrets Manager 密鑰的權限。如需有關密碼內容的詳細資訊，請參閱[匯流資料來源](#)。
- 使用 AWS KMS 客戶主要金鑰 (CMK) 解密儲存的使用者名稱和密碼密碼的 Secrets Manager 權限。
- 使用 BatchPutDocument 和作 BatchDeleteDocument 業更新索引的權限。

Note

您可以通過將匯流數據源連接到 Amazon Kendra。Amazon VPC 如果您使用的是 Amazon VPC，則需要新增[其他權限](#)。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "secretsmanager:GetSecretValue"
      ],
      "Resource": [
        "arn:aws:secretsmanager:your-region:your-account-id:secret:secret-id"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "kms:Decrypt"
      ],
      "Resource": [
        "arn:aws:kms:your-region:your-account-id:key/key-id"
      ],
      "Condition": {
        "StringLike": {
          "kms:ViaService": [
            "secretsmanager.your-region.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": [
        "kendra:BatchPutDocument",
        "kendra:BatchDeleteDocument"
      ],
      "Resource": "arn:aws:kendra:your-region:your-account-id:index/index-id"
    }
  ]
}
```

如果您使用的是 VPC，請提供可 Amazon Kendra 存取所需資源的原則。[如需所需原則，請參閱資料來源的IAM 角色、VPC。](#)

允許擔任角色 Amazon Kendra 的信任原則。


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

IAM 角色匯流連接器 V2.0

對於匯流連接器 v2.0 資料來源，您可以提供具有下列原則的角色。

- 存取包含聯合驗證認證之 AWS Secrets Manager 密碼的權限。如需有關密碼內容的詳細資訊，請參閱[匯流資料來源](#)。
- 使用 AWS KMS 客戶主要金鑰 (CMK) 解密儲存的使用者名稱和密碼密碼的 AWS Secrets Manager 權限。
- 使用 BatchPutDocument 和作 BatchDeleteDocument 業更新索引的權限。

您還必須附加允許 Amazon Kendra 擔任該角色的信任策略。

Note

您可以通過將匯流數據源連接到 Amazon Kendra。Amazon VPC 如果您使用的是 Amazon VPC，則需要新增[其他權限](#)。

允許連線 Amazon Kendra 至匯流的角色原則。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "secretsmanager:GetSecretValue"
      ]
    }
  ]
}
```

```

    ],
    "Resource": [
      "arn:aws:secretsmanager:your-region:your-account-id:secret:secret-id"
    ]
  },
  {
    "Effect": "Allow",
    "Action": [
      "kms:Decrypt"
    ],
    "Resource": [
      "arn:aws:kms:your-region:your-account-id:key/key-id"
    ],
    "Condition": {
      "StringLike": {
        "kms:ViaService": [
          "secretsmanager.your-region.amazonaws.com"
        ]
      }
    }
  },
  {
    "Effect": "Allow",
    "Action": [
      "kendra:PutPrincipalMapping",
      "kendra>DeletePrincipalMapping",
      "kendra:ListGroupOlderThanOrderingId",
      "kendra:DescribePrincipalMapping"
    ],
    "Resource": [
      "arn:aws:kendra:your-region:your-account-id:index/index-id",
      "arn:aws:kendra:your-region:your-account-id:index/index-id/data-source/*"
    ]
  },
  {
    "Effect": "Allow",
    "Action": [
      "kendra:BatchPutDocument",
      "kendra:BatchDeleteDocument"
    ],
    "Resource": "arn:aws:kendra:your-region:your-account-id:index/index-id"
  }
]

```

```
}

```

允許擔任角色 Amazon Kendra 的信任原則。

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

IAM 資料來源的角色

使用 Dropbox 時，您會提供具有下列政策的角色。

- 存取 AWS Secrets Manager 密碼以驗證 Dropbox 的權限。
- 允許為 Dropbox 連接器呼叫所需的公開 API。
- 呼
叫 BatchPutDocument、BatchDeleteDocumentPutPrincipalMappingDeletePrincipalMapping 和 ListGroupsOlderThanOrderingId API 的權限。

Note

您可以透過將 Dropbox 資料來源連線 Amazon Kendra 到 Amazon VPC。如果您使用的是 Amazon VPC，則需要新增[其他權限](#)。

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

```

    "secretsmanager:GetSecretValue"
  ],
  "Resource": [
    "arn:aws:secretsmanager:{{your-region}}:{{your-account-id}}:secret:[secret-id]"
  ]
},
{"Effect": "Allow",
 "Action": [
   "kms:Decrypt"
 ],
 "Resource": [
   "arn:aws:kms:{{your-region}}:{{your-account-id}}:key/[key-id]"
 ],
 "Condition": {"StringLike": {"kms:ViaService": [
   "secretsmanager.{{your-region}}.amazonaws.com"
 ]
 }
 }
},
{"Effect": "Allow",
 "Action": [
   "kendra:PutPrincipalMapping",
   "kendra:DeletePrincipalMapping",
   "kendra:ListGroupsOlderThanOrderingId",
   "kendra:DescribePrincipalMapping"
 ],
 "Resource": ["arn:aws:kendra:{{your-region}}:{{your-account-id}}:index/{{index-id}}", "arn:aws:kendra:{{your-region}}:{{your-account-id}}:index/{{index-id}}/data-source/*"]
},
{"Effect": "Allow",
 "Action": [
   "kendra:BatchPutDocument",
   "kendra:BatchDeleteDocument"
 ],
 "Resource": "arn:aws:kendra:{{your-region}}:{{your-account-id}}:index/{{index-id}}"
}]
}

```

允許擔任角色 Amazon Kendra 的信任原則。

```

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

```

```

    "Statement": [
      {
        "Effect": "Allow",
        "Principal": {
          "Service": "kendra.amazonaws.com"
        },
        "Action": "sts:AssumeRole"
      }
    ]
  }
}

```

IAM 對於 Drupal 數據源的角色

當您使用 Drupal 時，您可以使用以下策略提供一個角色。

- 許可訪問您的 AWS Secrets Manager 秘密來驗證您的 Drupal。
- 允許為 Drupal 連接器調用所需的公共 API。
- 呼
叫 BatchPutDocument、BatchDeleteDocumentPutPrincipalMappingDeletePrincipalMapping 和 ListGroupsOlderThanOrderingId API 的權限。

Note

您可以將 Drupal 的數據源連接到 Amazon Kendra 通過 Amazon VPC。如果您使用的是 Amazon VPC，則需要新增[其他權限](#)。

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "secretsmanager:GetSecretValue"
      ],
      "Resource": [
        "arn:aws:secretsmanager:{{region}}:{{account_id}}:secret:[[secret_id]]"
      ]
    },
    {

```

```

    "Effect": "Allow",
    "Action": [
      "kms:Decrypt"
    ],
    "Resource": [
      "arn:aws:kms:{{region}}:{{account_id}}:key/[key_id]"
    ],
    "Condition": {
      "StringLike": {
        "kms:ViaService": [
          "secretsmanager.*.amazonaws.com"
        ]
      }
    }
  },
  {
    "Effect": "Allow",
    "Action": [
      "kendra:PutPrincipalMapping",
      "kendra>DeletePrincipalMapping",
      "kendra:ListGroupOlderThanOrderingId",
      "kendra:DescribePrincipalMapping"
    ],
    "Resource": ["arn:aws:kendra:{{region}}:{{account_id}}:index/{{index_id}}",
      "arn:aws:kendra:{{region}}:{{account_id}}:index/{{index_id}}/data-source/*"
    ],
    {
      "Effect": "Allow",
      "Action": [
        "kendra:BatchPutDocument",
        "kendra:BatchDeleteDocument"
      ],
      "Resource": "arn:aws:kendra:{{region}}:{{account_id}}:index/{{index_id}}"
    }
  ]
}

```

允許擔任角色 Amazon Kendra 的信任原則。

```

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

```

```

    "Principal":{
      "Service":"kendra.amazonaws.com"
    },
    "Action":"sts:AssumeRole"
  }
]
}

```

IAM GitHub 資料來源的角色

使用時 GitHub，您會提供具有下列原則的角色。

- 訪問您的 AWS Secrets Manager 密碼以驗證您的 GitHub.
- 呼叫 GitHub 連接器所需公用 API 的權限。
- 呼
叫 BatchPutDocument、BatchDeleteDocumentPutPrincipalMappingDeletePrincipalMapping 和 ListGroupsOlderThanOrderingId API 的權限。

Note

您可以透過將 GitHub 資料來源連接 Amazon Kendra 至 Amazon VPC。如果您使用的是 Amazon VPC，則需要新增 [其他權限](#)。

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "secretsmanager:GetSecretValue"
      ],
      "Resource": [
        "arn:aws:secretsmanager:{{your-region}}:{{your-account-id}}:secret:[secret-id]"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "kms:Decrypt"
      ]
    }
  ]
}

```

```

    ],
    "Resource": [
      "arn:aws:kms:{{your-region}}:{{your-account-id}}:key/[{{key-id}}]"
    ],
    "Condition": {
      "StringLike": {
        "kms:ViaService": [
          "secretsmanager.{{your-region}}.amazonaws.com"
        ]
      }
    }
  },
  {
    "Effect": "Allow",
    "Action": [
      "kendra:PutPrincipalMapping",
      "kendra>DeletePrincipalMapping",
      "kendra:ListGroupsWithOrderingId",
      "kendra:DescribePrincipalMapping"
    ],
    "Resource": ["arn:aws:kendra:{{your-region}}:{{your-account-id}}:index/{{index-id}}", "arn:aws:kendra:{{your-region}}:{{your-account-id}}:index/{{index-id}}/data-source/*"]
  },
  {
    "Effect": "Allow",
    "Action": [
      "kendra:BatchPutDocument",
      "kendra:BatchDeleteDocument"
    ],
    "Resource": "arn:aws:kendra:{{your-region}}:{{your-account-id}}:index/{{index-id}}"
  }
]
}

```

允許擔任角色 Amazon Kendra 的信任原則。

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "kendra.amazonaws.com"
      }
    }
  ]
}

```



```

    },
    "Action": "sts:AssumeRole"
  }
]
}

```

IAM Gmail 資料來源的角色

使用 Gmail 時，您會提供具有下列政策的角色。

- 有權訪問您的 AWS Secrets Manager 密碼以驗證您的 Gmail。
- 呼叫 Gmail 連接器所需公用 API 的權限。
- 呼叫 BatchPutDocument、BatchDeleteDocumentPutPrincipalMappingDeletePrincipalMapping 和 ListGroupsOlderThanOrderingId API 的權限。

Note

您可以通過將 Gmail 數據源連 Amazon Kendra 接到 Amazon VPC。如果您使用的是 Amazon VPC，則需要新增[其他權限](#)。

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "secretsmanager:GetSecretValue"
      ],
      "Resource": [
        "arn:aws:secretsmanager:{{your-region}}:{{your-account-id}}:secret:[secret-id]"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "kms:Decrypt"
      ],
      "Resource": [
        "arn:aws:kms:{{your-region}}:{{your-account-id}}:key/[key-id]"
      ]
    }
  ]
}

```

```

    "Condition": {"StringLike": {"kms:ViaService": [
      "secretsmanager.{{your-region}}.amazonaws.com"
    ]}
  },
  {"Effect": "Allow",
    "Action": [
      "kendra:PutPrincipalMapping",
      "kendra:DeletePrincipalMapping",
      "kendra:ListGroupOlderThanOrderingId",
      "kendra:DescribePrincipalMapping"
    ],
    "Resource": ["arn:aws:kendra:{{your-region}}:{{your-account-id}}:index/{{index-id}}", "arn:aws:kendra:{{your-region}}:{{your-account-id}}:index/{{index-id}}/data-source/*"]
  },
  {"Effect": "Allow",
    "Action": [
      "kendra:BatchPutDocument",
      "kendra:BatchDeleteDocument"
    ],
    "Resource": "arn:aws:kendra:{{your-region}}:{{your-account-id}}:index/{{index-id}}"
  }
]
}

```

允許擔任角色 Amazon Kendra 的信任原則。

```

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

```

IAM Google 雲端硬碟資料來源的角色

當您使用 Google Workspace 雲端硬碟資料來源時，您所 Amazon Kendra 提供的角色具有連線至網站所需權限的角色。其中包含：

- 獲取和解密包含客戶端帳戶電子郵件，管理員帳戶電子郵件和連接到 Google 雲端硬碟站點所需的私鑰的密鑰的權限。AWS Secrets Manager 如需密碼內容的詳細資訊，請參閱 [Google 雲端硬碟資料來源](#)。
- 使用 [BatchPutDocument](#) 和 [BatchDeleteDocument](#) API 的權限。

Note

您可以通過將 Google 雲端硬碟數據源連 Amazon Kendra 接到 Amazon VPC。如果您使用的是 Amazon VPC，則需要新增 [其他權限](#)。

下列 IAM 原則提供必要的權限：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "secretsmanager:GetSecretValue"
      ],
      "Resource": [
        "arn:aws:secretsmanager:your-region:your-account-id:secret:secret-id"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "kms:Decrypt"
      ],
      "Resource": [
        "arn:aws:kms:your-region:your-account-id:key/key-id"
      ],
      "Condition": {
        "StringLike": {
          "kms:ViaService": [
```

```

        "secretsmanager.your-region.amazonaws.com"
    ]
}
},
{
    "Effect": "Allow",
    "Action": [
        "kendra:BatchPutDocument",
        "kendra:BatchDeleteDocument"
    ],
    "Resource": "arn:aws:kendra:your-region:your-account-id:index/index-id"
}]
}

```

允許擔任角色 Amazon Kendra 的信任原則。

```

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

```

IAM IBM DB2 資料來源的角色

當您使用 IBM DB2 資料來源連接器時，您會提供具有下列原則的角色。

- 存取 AWS Secrets Manager 密碼以驗證 IBM DB2 資料來源執行個體的權限。
- 呼叫 IBM DB2 資料來源連接器所需公用 API 的權限。
- 呼
叫 BatchPutDocument、BatchDeleteDocumentPutPrincipalMappingDeletePrincipalMapping 和 ListGroupsOlderThanOrderingId API 的權限。

Note

您可以透過將 IBM DB2 資料來源連線 Amazon Kendra 到 Amazon VPC。如果您使用的是 Amazon VPC，則需要新增[其他權限](#)。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "secretsmanager:GetSecretValue"
      ],
      "Resource": [
        "arn:aws:secretsmanager:{{region}}:{{account_id}}:secret:[[secret_id]]"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "kms:Decrypt"
      ],
      "Resource": [
        "arn:aws:kms:{{region}}:{{account_id}}:key/[[key_id]]"
      ],
      "Condition": {
        "StringLike": {
          "kms:ViaService": [
            "secretsmanager.*.amazonaws.com"
          ]
        }
      }
    }
  ],
  {
    "Effect": "Allow",
    "Action": [
      "kendra:PutPrincipalMapping",
      "kendra>DeletePrincipalMapping",
      "kendra:ListGroupsWithOrderingId",
      "kendra:DescribePrincipalMapping"
    ],
  ]
}
```

```

    "Resource": ["arn:aws:kendra:{{region}}:{{account_id}}:index/{{index_id}}",
    "arn:aws:kendra:{{region}}:{{account_id}}:index/{{index_id}}/data-source/*"]
  },
  {
    "Effect": "Allow",
    "Action": [
      "kendra:BatchPutDocument",
      "kendra:BatchDeleteDocument"
    ],
    "Resource": "arn:aws:kendra:{{region}}:{{account_id}}:index/{{index_id}}"
  ]
}

```

允許擔任角色 Amazon Kendra 的信任原則。

```

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

```

IAM Jira 資料來源的角色

當您使用 Jira 時，您會提供具有下列原則的角色。

- 訪問您的 AWS Secrets Manager 密碼以驗證您的 Jira 的權限。
- 呼叫 Jira 連接器所需公用 API 的權限。
- 呼
叫 BatchPutDocument、BatchDeleteDocumentPutPrincipalMappingDeletePrincipalMapping 和 ListGroupsOlderThanOrderingId API 的權限。

Note

您可以透過將 Jira 資料來源連接 Amazon Kendra 到 Amazon VPC。如果您使用的是 Amazon VPC，則需要新增[其他權限](#)。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "secretsmanager:GetSecretValue"
      ],
      "Resource": [
        "arn:aws:secretsmanager:{{your-region}}:{{your-account-id}}:secret:[secret-id]"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "kms:Decrypt"
      ],
      "Resource": [
        "arn:aws:kms:{{your-region}}:{{your-account-id}}:key/[key-id]"
      ],
      "Condition": {
        "StringLike": {
          "kms:ViaService": [
            "secretsmanager.{{your-region}}.amazonaws.com"
          ]
        }
      }
    }
  ],
  {
    "Effect": "Allow",
    "Action": [
      "kendra:PutPrincipalMapping",
      "kendra>DeletePrincipalMapping",
      "kendra:ListGroupOlderThanOrderingId",
      "kendra:DescribePrincipalMapping"
    ],
  ]
}
```

```

    "Resource": ["arn:aws:kendra:{{your-region}}:{{your-account-id}}:index/{{index-id}}", "arn:aws:kendra:{{your-region}}:{{your-account-id}}:index/{{index-id}}/data-source/*"],
  },
  {
    "Effect": "Allow",
    "Action": [
      "kendra:BatchPutDocument",
      "kendra:BatchDeleteDocument"
    ],
    "Resource": "arn:aws:kendra:{{your-region}}:{{your-account-id}}:index/{{index-id}}"
  }
]
}

```

允許擔任角色 Amazon Kendra 的信任原則。

```

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

```

IAM Microsoft 交換資料來源的角色

當您使用 Microsoft Exchange 資料來源時，您會提供 Amazon Kendra 具有連線至網站所需權限的角色。其中包含：

- 取得及解密密碼的 AWS Secrets Manager 權限，其中包含連線至 Microsoft Exchange 網站所需之應用程式識別碼和秘密金鑰。如需密碼內容的詳細資訊，請參閱 [Microsoft Exchange 資料來源](#)。
- 使用 [BatchPutDocument](#) 和 [BatchDeleteDocument](#) API 的權限。

Note

您可以通過將 Microsoft 交換數據源連 Amazon Kendra 接到 Amazon VPC。如果您使用的是 Amazon VPC，則需要新增[其他權限](#)。

下列 IAM 原則提供必要的權限：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "secretsmanager:GetSecretValue"
      ],
      "Resource": [
        "arn:aws:secretsmanager:your-region:your-account-id:secret:secret-id"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "kms:Decrypt"
      ],
      "Resource": [
        "arn:aws:kms:your-region:your-account-id:key/key-id"
      ],
      "Condition": {
        "StringLike": {
          "kms:ViaService": [
            "secretsmanager.your-region.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": [
        "kendra:BatchPutDocument",
        "kendra:BatchDeleteDocument"
      ],
      "Resource": "arn:aws:kendra:your-region:your-account-id:index/index-id"
    }
  ]
}
```

```

    ]]
  }
}

```

如果要將索引的使用者清單儲存在儲存 Amazon S3 貯體中，則還必須提供使用 S3 GetObject 作業的權限。下列 IAM 原則提供必要的權限：

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "secretsmanager:GetSecretValue"
      ],
      "Resource": [
        "arn:aws:secretsmanager:your-region:your-account-id:secret:secret-id"
      ]
    },
    {
      "Action": [
        "s3:GetObject"
      ],
      "Resource": [
        "arn:aws:s3:::bucket-name/*"
      ],
      "Effect": "Allow"
    },
    {
      "Effect": "Allow",
      "Action": [
        "kms:Decrypt"
      ],
      "Resource": [
        "arn:aws:kms:your-region:your-account-id:key/[key-ids]"
      ],
      "Condition": {
        "StringLike": {
          "kms:ViaService": [
            "secretsmanager.your-region.amazonaws.com",
            "s3.your-region.amazonaws.com"
          ]
        }
      }
    }
  ]
}

```

```

},
{
  "Effect": "Allow",
  "Action": [
    "kendra:BatchPutDocument",
    "kendra:BatchDeleteDocument"
  ],
  "Resource": "arn:aws:kendra:your-region:your-account-id:index/index-id"
}]
}

```

允許擔任角色 Amazon Kendra 的信任原則。

```

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

```

IAM Microsoft OneDrive 資料來源的角色

當您使用 Microsoft OneDrive 資料來源時，您會提供 Amazon Kendra 具有連線至網站所需權限的角色。其中包含：

- 獲取和解密包含連接到 OneDrive 站點所需的應用程式 ID 和密鑰的密鑰的密鑰的權限。AWS Secrets Manager 如需密碼內容的詳細資訊，請參閱 [Microsoft 資 OneDrive 料來源](#)。
- 使用 [BatchPutDocument](#) 和 [BatchDeleteDocument](#) API 的權限。

Note

您可以透過將 Microsoft OneDrive 資料來源連線 Amazon Kendra 至 Amazon VPC。如果您使用的是 Amazon VPC，則需要新增 [其他權限](#)。

下列 IAM 原則提供必要的權限：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "secretsmanager:GetSecretValue"
      ],
      "Resource": [
        "arn:aws:secretsmanager:your-region:your-account-id:secret:secret-id"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "kms:Decrypt"
      ],
      "Resource": [
        "arn:aws:kms:your-region:your-account-id:key/key-id"
      ],
      "Condition": {
        "StringLike": {
          "kms:ViaService": [
            "secretsmanager.your-region.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": [
        "kendra:BatchPutDocument",
        "kendra:BatchDeleteDocument"
      ],
      "Resource": "arn:aws:kendra:your-region:your-account-id:index/index-id"
    }
  ]
}
```

如果要將索引的使用者清單儲存在儲存 Amazon S3 貯體中，則還必須提供使用 S3 GetObject 作業的權限。下列 IAM 原則提供必要的權限：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "secretsmanager:GetSecretValue"
      ],
      "Resource": [
        "arn:aws:secretsmanager:your-region:your-account-id:secret:secret-id"
      ]
    },
    {
      "Action": [
        "s3:GetObject"
      ],
      "Resource": [
        "arn:aws:s3:::bucket-name/*"
      ],
      "Effect": "Allow"
    },
    {
      "Effect": "Allow",
      "Action": [
        "kms:Decrypt"
      ],
      "Resource": [
        "arn:aws:kms:your-region:your-account-id:key/[key-ids]"
      ],
      "Condition": {
        "StringLike": {
          "kms:ViaService": [
            "secretsmanager.your-region.amazonaws.com",
            "s3.your-region.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": [
        "kendra:BatchPutDocument",
        "kendra:BatchDeleteDocument"
      ]
    }
  ]
}
```

```

    ],
    "Resource": "arn:aws:kendra:your-region:your-account-id:index/index-id"
  ]]
}

```

允許擔任角色 Amazon Kendra 的信任原則。

```

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

```

IAM Microsoft SharePoint 資料來源的角色

IAM SharePoint 連接器 V1.0 的角色

對於 Microsoft SharePoint 連接器 1.0 資料來源，您可以提供具有下列原則的角色。

- 存取包含網站使用者名稱和密碼之密碼的 SharePoint 權限。AWS Secrets Manager 如需密碼內容的詳細資訊，請參閱 [Microsoft 資 SharePoint 料來源](#)。
- 使用 AWS KMS 客戶主要金鑰 (CMK) 解密儲存的使用者名稱和密碼密碼的 AWS Secrets Manager 權限。
- 使用 BatchPutDocument 和作 BatchDeleteDocument 業更新索引的權限。
- 存取包含用於與 SharePoint 網站通訊之 SSL 憑證的 Amazon S3 值區的權限。

您還必須附加允許 Amazon Kendra 擔任該角色的信任策略。

Note

您可以透過將 Microsoft SharePoint 資料來源連線 Amazon Kendra 至 Amazon VPC。如果您使用的是 Amazon VPC，則需要新增 [其他權限](#)。

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "secretsmanager:GetSecretValue"
      ],
      "Resource": [
        "arn:aws:secretsmanager:your-region:your-account-id:secret:secret-id"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "kms:Decrypt"
      ],
      "Resource": [
        "arn:aws:kms:your-region:your-account-id:key/key-id"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "kendra:BatchPutDocument",
        "kendra:BatchDeleteDocument"
      ],
      "Resource": [
        "arn:aws:kendra:your-region:your-account-id:index/index-id"
      ],
      "Condition": {
        "StringLike": {
          "kms:ViaService": [
            "kendra.your-region.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetObject"
      ],

```

```
        "Resource": [
            "arn:aws:s3:::bucket-name/*"
        ]
    }
]
}
```

如果您已加密包含用於與 SharePoint 網站通訊之 SSL 憑證的儲存 Amazon S3 貯體，請提供授予金鑰 Amazon Kendra 存取權的原則。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "kms:Decrypt"
      ],
      "Resource": [
        "arn:aws:kms:your-region:your-account-id:key/key-id"
      ]
    }
  ]
}
```

允許擔任角色 Amazon Kendra 的信任原則。

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


IAM SharePoint 連接器 V2.0 的角色

對於 Microsoft SharePoint 連接器 2.0 資料來源，您可以提供具有下列原則的角色。

- 存取包含網站驗證認證之 AWS Secrets Manager 密碼的 SharePoint 權限。如需密碼內容的詳細資訊，請參閱 [Microsoft 資 SharePoint 料來源](#)。
- 使用 AWS KMS 客戶主要金鑰 (CMK) 解密儲存的使用者名稱和密碼密碼的 AWS Secrets Manager 權限。
- 使用 BatchPutDocument 和作 BatchDeleteDocument 業更新索引的權限。
- 存取包含用於與 SharePoint 網站通訊之 SSL 憑證的 Amazon S3 值區的權限。

您還必須附加允許 Amazon Kendra 擔任該角色的信任策略。

Note

您可以透過將 Microsoft SharePoint 資料來源連線 Amazon Kendra 至 Amazon VPC。如果您使用的是 Amazon VPC，則需要新增 [其他權限](#)。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "secretsmanager:GetSecretValue"
      ],
      "Resource": [
        "arn:aws:secretsmanager:your-region:your-account-id:secret:secret-id"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "kms:Decrypt"
      ],
      "Resource": [
        "arn:aws:kms:your-region:your-account-id:key/key-id"
      ],
      "Condition": {
```

```
    "StringLike": {
      "kms:ViaService": [
        "secretsmanager.your-region.amazonaws.com"
      ]
    }
  },
  {
    "Effect": "Allow",
    "Action": [
      "kendra:PutPrincipalMapping",
      "kendra>DeletePrincipalMapping",
      "kendra:ListGroupsWithOrderingId",
      "kendra:DescribePrincipalMapping"
    ],
    "Resource": [
      "arn:aws:kendra:your-region:your-account-id:index/index-id",
      "arn:aws:kendra:your-region:your-account-id:index/index-id/data-source/*"
    ]
  },
  {
    "Action": [
      "s3:GetObject"
    ],
    "Resource": [
      "arn:aws:s3:::bucket-name/key-name"
    ],
    "Effect": "Allow"
  },
  {
    "Effect": "Allow",
    "Action": [
      "kendra:BatchPutDocument",
      "kendra:BatchDeleteDocument"
    ],
    "Resource": "arn:aws:kendra:your-region:your-account-id:index/index-id"
  },
  {
    "Effect": "Allow",
    "Action": [
      "ec2:CreateNetworkInterface"
    ],
    "Resource": [
      "arn:aws:ec2:your-region:your-account-id:subnet/subnet-ids",

```

```

    "arn:aws:ec2:your-region:your-account-id:security-group/security-group"
  ],
},
{
  "Effect": "Allow",
  "Action": [
    "ec2:CreateNetworkInterface"
  ],
  "Resource": "arn:aws:ec2:region:account_id:network-interface/*",
  "Condition": {
    "StringLike": {
      "aws:RequestTag/AWS_KENDRA": "kendra_your-account-id_index-id_*"
    }
  }
},
{
  "Effect": "Allow",
  "Action": [
    "ec2:CreateTags"
  ],
  "Resource": "arn:aws:ec2:your-region:your-account-id:network-interface/*",
  "Condition": {
    "StringEquals": {
      "ec2:CreateAction": "CreateNetworkInterface"
    }
  }
},
{
  "Effect": "Allow",
  "Action": [
    "ec2:CreateNetworkInterfacePermission"
  ],
  "Resource": "arn:aws:ec2:your-region:your-account-id:network-interface/*",
  "Condition": {
    "StringLike": {
      "aws:ResourceTag/AWS_KENDRA": "kendra_your-account-id_index-id_*"
    }
  }
},
{
  "Effect": "Allow",
  "Action": [
    "ec2:DescribeNetworkInterfaces",

```

```

    "ec2:DescribeAvailabilityZones",
    "ec2:DescribeNetworkInterfaceAttribute",
    "ec2:DescribeVpcs",
    "ec2:DescribeRegions",
    "ec2:DescribeNetworkInterfacePermissions",
    "ec2:DescribeSubnets"
  ],
  "Resource": "*"
}
]
}

```

如果您已加密包含用於與 SharePoint 網站通訊之 SSL 憑證的儲存 Amazon S3 貯體，請提供授予金鑰 Amazon Kendra 存取權的原則。

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "kms:Decrypt"
      ],
      "Resource": [
        "arn:aws:kms:your-region:youraccount-id:key/key-id"
      ]
    }
  ]
}

```

允許擔任角色 Amazon Kendra 的信任原則。

```

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

```

```
]
}
```

IAM Microsoft SQL 伺服器資料來源的角色

當您使用 Microsoft SQL Server 時，您會提供具有下列原則的角色。

- 存取 AWS Secrets Manager 密碼以驗證您的 Microsoft SQL Server 執行個體的權限。
- 呼叫 Microsoft SQL 伺服器連接器所需公用 API 的權限。
- 呼叫 `BatchPutDocument`、`BatchDeleteDocument`、`PutPrincipalMapping`、`DeletePrincipalMapping` 和 `ListGroupsOlderThanOrderingId` API 的權限。

Note

您可以透過將 Microsoft SQL 伺服器資料來源連 Amazon Kendra 接到 Amazon VPC。如果您使用的是 Amazon VPC，則需要新增[其他權限](#)。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "secretsmanager:GetSecretValue"
      ],
      "Resource": [
        "arn:aws:secretsmanager:{{region}}:{{account_id}}:secret:[[secret_id]]"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "kms:Decrypt"
      ],
      "Resource": [
        "arn:aws:kms:{{region}}:{{account_id}}:key/[[key_id]]"
      ],
      "Condition": {
```

```

    "StringLike": {
      "kms:ViaService": [
        "secretsmanager.*.amazonaws.com"
      ]
    }
  },
  {
    "Effect": "Allow",
    "Action": [
      "kendra:PutPrincipalMapping",
      "kendra:DeletePrincipalMapping",
      "kendra:ListGroupsWithOrderingId",
      "kendra:DescribePrincipalMapping"
    ],
    "Resource": ["arn:aws:kendra:{{region}}:{{account_id}}:index/{{index_id}}",
"arn:aws:kendra:{{region}}:{{account_id}}:index/{{index_id}}/data-source/*"]
  },
  {
    "Effect": "Allow",
    "Action": [
      "kendra:BatchPutDocument",
      "kendra:BatchDeleteDocument"
    ],
    "Resource": "arn:aws:kendra:{{region}}:{{account_id}}:index/{{index_id}}"
  ]
}

```

允許擔任角色 Amazon Kendra 的信任原則。

```

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

```

IAM Microsoft 團隊資料來源的角色

當您使用 Microsoft Teams 資料來源時，您會提供 Amazon Kendra 具有連線至網站所需權限的角色。其中包含：

- 取得及解密密碼的權限，其中 AWS Secrets Manager 包含連線至 Microsoft Teams 所需的用戶端識別碼和用戶端密碼。如需密碼內容的詳細資訊，請參閱 [Microsoft 團隊資料來源](#)。

Note

您可以透過將 Microsoft 團隊資料來源連線 Amazon Kendra 到 Amazon VPC。如果您使用的是 Amazon VPC，則需要新增[其他權限](#)。

下列 IAM 原則提供必要的權限：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "secretsmanager:GetSecretValue"
      ],
      "Resource": [
        "arn:aws:secretsmanager:your-region:client-id:secret:secret-id"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "kms:Decrypt"
      ],
      "Resource": [
        "arn:aws:kms:your-region:your-account-id:key/key-id"
      ],
      "Condition": {
        "StringLike": {
          "kms:ViaService": [
            "secretsmanager.your-region.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

```
    }
  }
},
{
  "Effect": "Allow",
  "Action": [
    "kendra:BatchPutDocument",
    "kendra:BatchDeleteDocument"
  ],
  "Resource": "arn:aws:kendra:your-region:your-account-id:index/index-id"
}]
}
```

允許擔任角色 Amazon Kendra 的信任原則。

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

IAM Microsoft Yammer 資料來源的角色

當您使用 Microsoft Yammer 資料來源時，您會提供 Amazon Kendra 具有連線至網站所需權限的角色。其中包含：

- 取得及解密密碼的權限，其中 AWS Secrets Manager 包含連線至 Microsoft Yammer 網站所需的應用程式識別碼和秘密金鑰。如需密碼內容的詳細資訊，請參閱 [Microsoft Yammer 資料來源](#)。
- 使用 [BatchPutDocument](#) 和 [BatchDeleteDocument](#) API 的權限。

Note

您可以透過將 Microsoft Yammer 資料來源連線 Amazon Kendra 到 Amazon VPC。如果您使用的是 Amazon VPC，則需要新增[其他權限](#)。

下列 IAM 原則提供必要的權限：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "secretsmanager:GetSecretValue"
      ],
      "Resource": [
        "arn:aws:secretsmanager:your-region:your-account-id:secret:secret-id"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "kms:Decrypt"
      ],
      "Resource": [
        "arn:aws:kms:your-region:your-account-id:key/key-id"
      ],
      "Condition": {
        "StringLike": {
          "kms:ViaService": [
            "secretsmanager.your-region.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": [
        "kendra:BatchPutDocument",
        "kendra:BatchDeleteDocument"
      ],
      "Resource": "arn:aws:kendra:your-region:your-account-id:index/index-id"
    }
  ]
}
```

```

    ]]
  }
}

```

如果要將索引的使用者清單儲存在儲存 Amazon S3 貯體中，則還必須提供使用 S3 GetObject 作業的權限。下列 IAM 原則提供必要的權限：

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "secretsmanager:GetSecretValue"
      ],
      "Resource": [
        "arn:aws:secretsmanager:your-region:your-account-id:secret:secret-id"
      ]
    },
    {
      "Action": [
        "s3:GetObject"
      ],
      "Resource": [
        "arn:aws:s3:::bucket-name/*"
      ],
      "Effect": "Allow"
    },
    {
      "Effect": "Allow",
      "Action": [
        "kms:Decrypt"
      ],
      "Resource": [
        "arn:aws:kms:your-region:your-account-id:key/[key-ids]"
      ],
      "Condition": {
        "StringLike": {
          "kms:ViaService": [
            "secretsmanager.your-region.amazonaws.com",
            "s3.your-region.amazonaws.com"
          ]
        }
      }
    }
  ]
}

```

```

    },
    {
      "Effect": "Allow",
      "Action": [
        "kendra:BatchPutDocument",
        "kendra:BatchDeleteDocument"
      ],
      "Resource": "arn:aws:kendra:your-region:your-account-id:index/index-id"
    }
  ]
}

```

允許擔任角色 Amazon Kendra 的信任原則。

```

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

```

IAM MySQL 資料來源的角色

當您使用 My SQL 資料來源連接器時，您會提供具有下列原則的角色。

- 存取 AWS Secrets Manager 密碼以驗證 My SQL 資料來源執行個體的權限。
- 呼叫 My SQL 資料來源連接器所需公用 API 的權限。
- 呼
叫 BatchPutDocument、BatchDeleteDocumentPutPrincipalMappingDeletePrincipalMapping 和 ListGroupsOlderThanOrderingId API 的權限。

Note

您可以透過將 MySQL 資料來源連 Amazon Kendra 接到 Amazon VPC。如果您使用的是 Amazon VPC，則需要新增[其他權限](#)。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "secretsmanager:GetSecretValue"
      ],
      "Resource": [
        "arn:aws:secretsmanager:{{region}}:{{account_id}}:secret:[secret_id]"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "kms:Decrypt"
      ],
      "Resource": [
        "arn:aws:kms:{{region}}:{{account_id}}:key/[key_id]"
      ],
      "Condition": {
        "StringLike": {
          "kms:ViaService": [
            "secretsmanager.*.amazonaws.com"
          ]
        }
      }
    }
  ],
  {
    "Effect": "Allow",
    "Action": [
      "kendra:PutPrincipalMapping",
      "kendra>DeletePrincipalMapping",
      "kendra:ListGroupsWithOrderingId",
      "kendra:DescribePrincipalMapping"
    ],
  ]
}
```

```

    "Resource": ["arn:aws:kendra:{{region}}:{{account_id}}:index/{{index_id}}",
"arn:aws:kendra:{{region}}:{{account_id}}:index/{{index_id}}/data-source/*"]
  },
  {
    "Effect": "Allow",
    "Action": [
      "kendra:BatchPutDocument",
      "kendra:BatchDeleteDocument"
    ],
    "Resource": "arn:aws:kendra:{{region}}:{{account_id}}:index/{{index_id}}"
  }
]
}

```

允許擔任角色 Amazon Kendra 的信任原則。

```

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

```

IAM Oracle 資料來源的角色

當您使用 Oracle 資料來源連接器時，您會提供具有下列原則的角色。

- 存取 AWS Secrets Manager 密碼以驗證 Oracle 資料來源執行環境的權限。
- 呼叫 Oracle 資料來源連接器所需公用 API 的權限。
- 呼
叫 BatchPutDocument、BatchDeleteDocumentPutPrincipalMappingDeletePrincipalMapping 和 ListGroupsOlderThanOrderingId API 的權限。

Note

您可以透過將 Oracle 資料來源連線 Amazon Kendra 到 Amazon VPC。如果您使用的是 Amazon VPC，則需要新增[其他權限](#)。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "secretsmanager:GetSecretValue"
      ],
      "Resource": [
        "arn:aws:secretsmanager:{{region}}:{{account_id}}:secret:[secret_id]"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "kms:Decrypt"
      ],
      "Resource": [
        "arn:aws:kms:{{region}}:{{account_id}}:key/[key_id]"
      ],
      "Condition": {
        "StringLike": {
          "kms:ViaService": [
            "secretsmanager.*.amazonaws.com"
          ]
        }
      }
    }
  ],
  {
    "Effect": "Allow",
    "Action": [
      "kendra:PutPrincipalMapping",
      "kendra>DeletePrincipalMapping",
      "kendra:ListGroupsWithOrderingId",
      "kendra:DescribePrincipalMapping"
    ],
  ]
}
```

```

    "Resource": ["arn:aws:kendra:{{region}}:{{account_id}}:index/{{index_id}}",
"arn:aws:kendra:{{region}}:{{account_id}}:index/{{index_id}}/data-source/*"]
  },
  {
    "Effect": "Allow",
    "Action": [
      "kendra:BatchPutDocument",
      "kendra:BatchDeleteDocument"
    ],
    "Resource": "arn:aws:kendra:{{region}}:{{account_id}}:index/{{index_id}}"
  }
]
}

```

允許擔任角色 Amazon Kendra 的信任原則。

```

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

```

IAM PostgreSQL 資料來源的角色

當您使用 PostgreSQL 資料來源連接器時，您會提供具有下列原則的角色。

- 存取 AWS Secrets Manager 密碼以驗證 PostgreSQL 資料來源執行個體的權限。
- 呼叫 PostgreSQL 資料來源連接器所需公用 API 的權限。
- 呼
叫 BatchPutDocument、BatchDeleteDocumentPutPrincipalMappingDeletePrincipalMapping 和 ListGroupsOlderThanOrderingId API 的權限。

Note

您可以透過將 PostgreSQL 資料來源連接到 Amazon Kendra。Amazon VPC 如果您使用的是 Amazon VPC，則需要新增[其他權限](#)。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "secretsmanager:GetSecretValue"
      ],
      "Resource": [
        "arn:aws:secretsmanager:{{region}}:{{account_id}}:secret:[[secret_id]]"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "kms:Decrypt"
      ],
      "Resource": [
        "arn:aws:kms:{{region}}:{{account_id}}:key/[[key_id]]"
      ],
      "Condition": {
        "StringLike": {
          "kms:ViaService": [
            "secretsmanager.*.amazonaws.com"
          ]
        }
      }
    }
  ],
  {
    "Effect": "Allow",
    "Action": [
      "kendra:PutPrincipalMapping",
      "kendra>DeletePrincipalMapping",
      "kendra:ListGroupsWithOrderingId",
      "kendra:DescribePrincipalMapping"
    ],
  ]
}
```



```

    "Resource": ["arn:aws:kendra:{{region}}:{{account_id}}:index/{{index_id}}",
    "arn:aws:kendra:{{region}}:{{account_id}}:index/{{index_id}}/data-source/*"]
  },
  {
    "Effect": "Allow",
    "Action": [
      "kendra:BatchPutDocument",
      "kendra:BatchDeleteDocument"
    ],
    "Resource": "arn:aws:kendra:{{region}}:{{account_id}}:index/{{index_id}}"
  ]
}

```

允許擔任角色 Amazon Kendra 的信任原則。

```

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

```

IAM Quip 資料來源的角色

當您使用 Quip 時，您會提供具有下列原則的角色。

- 訪問您的 AWS Secrets Manager 密碼以驗證您的 Quip 的權限。
- 呼叫 Quip 連接器所需公用 API 的權限。
- 呼
叫 BatchPutDocument、BatchDeleteDocumentPutPrincipalMappingDeletePrincipalMapping 和 ListGroupsOlderThanOrderingId API 的權限。

Note

您可以透過將 Quip 資料來源連線 Amazon Kendra 到 Amazon VPC。如果您使用的是 Amazon VPC，則需要新增[其他權限](#)。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "secretsmanager:GetSecretValue"
      ],
      "Resource": [
        "arn:aws:secretsmanager:{{your-region}}:{{your-account-id}}:secret:[secret-id]"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "kms:Decrypt"
      ],
      "Resource": [
        "arn:aws:kms:{{your-region}}:{{your-account-id}}:key/[key-id]"
      ],
      "Condition": {
        "StringLike": {
          "kms:ViaService": [
            "secretsmanager.{{your-region}}.amazonaws.com"
          ]
        }
      }
    }
  ],
  {
    "Effect": "Allow",
    "Action": [
      "kendra:PutPrincipalMapping",
      "kendra>DeletePrincipalMapping",
      "kendra:ListGroupsWithOrderingId",
      "kendra:DescribePrincipalMapping"
    ]
  }
]
```

```

    "Resource": ["arn:aws:kendra:{{your-region}}:{{your-account-id}}:index/{{your-index-id}}", "arn:aws:kendra:{{your-region}}:{{your-account-id}}:index/{{your-index-id}}/data-source/*"]
  },
  {
    "Effect": "Allow",
    "Action": [
      "kendra:BatchPutDocument",
      "kendra:BatchDeleteDocument"
    ],
    "Resource": "arn:aws:kendra:{{your-region}}:{{your-account-id}}:index/{{index-id}}"
  }
]
}

```

允許擔任角色 Amazon Kendra 的信任原則。

```

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

```

IAM Salesforce 資料來源的角色

當您使用 Salesforce 做為資料來源時，您會提供具有下列原則的角色：

- 存取包含 Salesforce 網站之使用者名稱和密碼之密碼的權限。AWS Secrets Manager 如需密碼內容的詳細資訊，請參閱 [Salesforce 資料來源](#)。
- 使用 AWS KMS 客戶主要金鑰 (CMK) 解密儲存的使用者名稱和密碼密碼的 Secrets Manager 權限。
- 使用 BatchPutDocument 和作 BatchDeleteDocument 業更新索引的權限。

Note

您可以透過將 Salesforce 資料來源連線 Amazon Kendra 到 Amazon VPC。如果您使用的是 Amazon VPC，則需要新增[其他權限](#)。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "secretsmanager:GetSecretValue"
      ],
      "Resource": [
        "arn:aws:secretsmanager:your-region:your-account-id:secret:secret-id"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "kms:Decrypt"
      ],
      "Resource": [
        "arn:aws:kms:your-region:your-account-id:key/key-id"
      ],
      "Condition": {
        "StringLike": {
          "kms:ViaService": [
            "secretsmanager.your-region.amazonaws.com"
          ]
        }
      }
    }
  ],
  {
    "Effect": "Allow",
    "Action": [
      "kendra:BatchPutDocument",
      "kendra:BatchDeleteDocument"
    ],
    "Resource": "arn:aws:kendra:your-region:account-id:index/index-id"
  }
}]
```

```
}
```

允許擔任角色 Amazon Kendra 的信任原則。

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

IAM ServiceNow 資料來源的角色

當您使用 ServiceNow 作為資料來源時，您會提供具有下列原則的角色：

- 存取包含網站使用者名稱和密碼之密碼的 ServiceNow 權限。Secrets Manager 有關密碼內容的詳細資訊，請參閱[ServiceNow 資料來源](#)。
- 使用 AWS KMS 客戶主要金鑰 (CMK) 解密儲存的使用者名稱和密碼密碼的 Secrets Manager 權限。
- 使用 BatchPutDocument 和作 BatchDeleteDocument 業更新索引的權限。

Note

您可以透過將 ServiceNow 資料來源連接 Amazon Kendra 至 Amazon VPC。如果您使用的是 Amazon VPC，則需要新增[其他權限](#)。

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

```

    "secretsmanager:GetSecretValue"
  ],
  "Resource": [
    "arn:aws:secretsmanager:your-region:your-account-id:secret:secret-id"
  ]
},
{
  "Effect": "Allow",
  "Action": [
    "kms:Decrypt"
  ],
  "Resource": [
    "arn:aws:kms:your-region:your-account-id:key/key-id"
  ],
  "Condition": {
    "StringLike": {
      "kms:ViaService": [
        "secretsmanager.your-region.amazonaws.com"
      ]
    }
  }
},
{
  "Effect": "Allow",
  "Action": [
    "kendra:BatchPutDocument",
    "kendra:BatchDeleteDocument"
  ],
  "Resource": "arn:aws:kendra:your-region:your-account-id:index/index-id"
}]
}

```

允許擔任角色 Amazon Kendra 的信任原則。

```

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

```

```

    }
  ]
}

```

IAM Slack 資料來源的角色

當您使用 Slack 時，您會提供具有下列原則的角色。

- 存取 AWS Secrets Manager 密碼以驗證您的 Slack 的權限。
- 呼叫 Slack 連接器所需公用 API 的權限。
- 呼叫 BatchPutDocument、BatchDeleteDocumentPutPrincipalMappingDeletePrincipalMapping 和 ListGroupsOlderThanOrderingId API 的權限。

Note

您可以透過將 Slack 資料來源連線 Amazon Kendra 到 Amazon VPC。如果您使用的是 Amazon VPC，則需要新增[其他權限](#)。

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "secretsmanager:GetSecretValue"
      ],
      "Resource": [
        "arn:aws:secretsmanager:{{your-region}}:{{your-account-id}}:secret:[secret-id]"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "kms:Decrypt"
      ],
      "Resource": [
        "arn:aws:kms:{{your-region}}:{{account-id}}:key/[key-id]"
      ]
    }
  ]
}

```

```

    "Condition": {
      "StringLike": {
        "kms:ViaService": [
          "secretsmanager.{{region}}.amazonaws.com"
        ]
      }
    },
    {
      "Effect": "Allow",
      "Action": [
        "kendra:PutPrincipalMapping",
        "kendra>DeletePrincipalMapping",
        "kendra:ListGroupsWithOrderingId",
        "kendra:DescribePrincipalMapping"
      ],
      "Resource": ["arn:aws:kendra:{{your-region}}:{{your-account-id}}:index/{{index-id}}", "arn:aws:kendra:{{your-region}}:{{your-account-id}}:index/{{index-id}}/data-source/*"]
    },
    {
      "Effect": "Allow",
      "Action": [
        "kendra:BatchPutDocument",
        "kendra:BatchDeleteDocument"
      ],
      "Resource": "arn:aws:kendra:{{your-region}}:{{your-account-id}}:index/{{index-id}}"
    }
  ]
}

```

允許擔任角色 Amazon Kendra 的信任原則。

```

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

```


}

IAM Zendesk 資料來源的角色

當您使用 Zendesk 時，您會提供具有下列原則的角色。

- 存取 AWS Secrets Manager 密碼以驗證您的 Zendesk 套件的權限。
- 呼叫 Zendesk 連接器所需公用 API 的權限。
- 呼叫 BatchPutDocument、BatchDeleteDocumentPutPrincipalMappingDeletePrincipalMapping 和 ListGroupsOlderThanOrderingId API 的權限。

Note

您可以透過將 Zendesk 資料來源連線 Amazon Kendra 到 Amazon VPC。如果您使用的是 Amazon VPC，則需要新增[其他權限](#)。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "secretsmanager:GetSecretValue"
      ],
      "Resource": [
        "arn:aws:secretsmanager:{{your-region}}:{{your-account-id}}:secret:[secret-id]"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "kms:Decrypt"
      ],
      "Resource": [
        "arn:aws:kms:{{your-region}}:{{your-account-id}}:key/[key-id]"
      ],
      "Condition": {
        "StringLike": {
```

```

    "kms:ViaService": [
      "secretsmanager.{{your-region}}.amazonaws.com"
    ]
  }
},
{
  "Effect": "Allow",
  "Action": [
    "kendra:PutPrincipalMapping",
    "kendra>DeletePrincipalMapping",
    "kendra:ListGroupsOlderThanOrderingId",
    "kendra:DescribePrincipalMapping"
  ],
  "Resource": ["arn:aws:kendra:{{your-region}}:{{your-account-id}}:index/{{index-id}}", "arn:aws:kendra:{{your-region}}:{{your-account-id}}:index/{{index-id}}/data-source/*"]
},
{
  "Effect": "Allow",
  "Action": [
    "kendra:BatchPutDocument",
    "kendra:BatchDeleteDocument"
  ],
  "Resource": "arn:aws:kendra:{{your-region}}:{{your-account-id}}:index/{{index-id}}"
}]
}

```

允許擔任角色 Amazon Kendra 的信任原則。

```

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

```

虛擬私有雲 (VPC) IAM 角色

如果您使用虛擬私有雲 (VPC) 連線到資料來源，則必須提供下列其他權限。

VPC 角 IAM 色

```
{
  "Effect": "Allow",
  "Action": [
    "ec2:CreateNetworkInterface"
  ],
  "Resource": [
    "arn:aws:ec2:{{region}}:{{account_id}}:subnet/[[]subnet_ids[]]",
    "arn:aws:ec2:{{region}}:{{account_id}}:security-group/[[]security_group[]]"
  ]
},
{
  "Effect": "Allow",
  "Action": [
    "ec2:CreateNetworkInterface"
  ],
  "Resource": "arn:aws:ec2:{{region}}:{{account_id}}:network-interface/*",
  "Condition": {
    "StringLike": {
      "aws:RequestTag/AWS_KENDRA": "kendra_{{account_id}}_{{index_id}}_*"
    }
  }
},
{
  "Effect": "Allow",
  "Action": [
    "ec2:CreateTags"
  ],
  "Resource": "arn:aws:ec2:{{region}}:{{account_id}}:network-interface/*",
  "Condition": {
    "StringEquals": {
      "ec2:CreateAction": "CreateNetworkInterface"
    }
  }
},
{
  "Effect": "Allow",
```

```

    "Action": [
      "ec2:CreateNetworkInterfacePermission"
    ],
    "Resource": "arn:aws:ec2:{{region}}:{{account_id}}:network-interface/*",
    "Condition": {
      "StringLike": {
        "aws:ResourceTag/AWS_KENDRA": "kendra_{{account_id}}_{{index_id}}_*"
      }
    }
  },
  {
    "Effect": "Allow",
    "Action": [
      "ec2:DescribeNetworkInterfaces",
      "ec2:DescribeAvailabilityZones",
      "ec2:DescribeNetworkInterfaceAttribute",
      "ec2:DescribeVpcs",
      "ec2:DescribeRegions",
      "ec2:DescribeNetworkInterfacePermissions",
      "ec2:DescribeSubnets"
    ],
    "Resource": "*"
  }
}

```

允許擔任角色 Amazon Kendra 的信任原則。

```

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

```

IAM 常見問題的角色

當您使用 [CreateFaq](#) API 將問題和答案載入索引時，您必須提供 Amazon Kendra 供可存取包含來源檔案之 Amazon S3 值區的 IAM 角色。如果來源檔案已加密，您必須提供使用 AWS KMS 客戶主要金鑰 (CMK) 解密檔案的權限。

IAM 常見問題的角色

允許 Amazon Kendra 存取 Amazon S3 值區的必要角色原則。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetObject"
      ],
      "Resource": [
        "arn:aws:s3:::bucket-name/*"
      ]
    }
  ]
}
```

可選角色政策，Amazon Kendra 允許使用 AWS KMS 客戶主金鑰 (CMK) 解密 Amazon S3 值區中的檔案。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "kms:Decrypt"
      ],
      "Resource": [
        "arn:aws:kms:your-region:your-account-id:key/key-id"
      ],
      "Condition": {
        "StringLike": {
```

```

        "kms:ViaService": [
            "kendra.your-region.amazonaws.com"
        ]
    }
}

```

允許擔任角色 Amazon Kendra 的信任原則。

```

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

```

IAM 查詢建議的角色

當您使用 Amazon S3 檔案做為查詢建議封鎖清單時，您會提供具有存取 Amazon S3 檔案和 Amazon S3 值區之權限的角色。如果 Amazon S3 儲存貯體中的封鎖清單文字 Amazon S3 檔案 (檔案) 已加密，您必須提供使用 AWS KMS 客戶主金鑰 (CMK) 解密文件的權限。

IAM 查詢建議的角色

允許 Amazon Kendra 將 Amazon S3 檔案用作查詢建議封鎖清單的必要角色原則。

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetObject"
      ]
    }
  ]
}

```

```
    ],
    "Resource": [
      "arn:aws:s3:::bucket-name/*"
    ]
  }
]
```

可選角色政策，Amazon Kendra 允許使用 AWS KMS 客戶主金鑰 (CMK) 解密 Amazon S3 值區中的文件。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "kms:Decrypt"
      ],
      "Resource": [
        "arn:aws:kms:your-region:your-account-id:key/key-id"
      ]
    }
  ]
}
```

允許擔任角色 Amazon Kendra 的信任原則。

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

IAM 使用者與群組之主參與者對應的角色

當您使用 [PutPrincipalMapping](#) API 將使用者對應至其群組以依使用者內容篩選搜尋結果時，您需要提供屬於群組的使用者或子群組清單。如果您的清單超過 1000 個使用者或群組的子群組，您必須提供具有存取清單和 Amazon S3 值區 Amazon S3 檔案之權限的角色。如果 Amazon S3 存儲桶中列表的文本文件（文件）已加密，則必須提供使用 AWS KMS 客戶主密鑰（CMK）來解密 Amazon S3 檔的權限。

IAM 主參與者對應的角色

允許將 Amazon S3 檔案用作屬 Amazon Kendra 於群組的使用者和子群組清單的必要角色原則。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetObject"
      ],
      "Resource": [
        "arn:aws:s3:::bucket-name/*"
      ]
    }
  ]
}
```

可選角色政策，Amazon Kendra 允許使用 AWS KMS 客戶主金鑰 (CMK) 解密 Amazon S3 值區中的文件。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "kms:Decrypt"
      ],
      "Resource": [
        "arn:aws:kms:your-region:your-account-id:key/key-id"
      ]
    }
  ]
}
```



```
}

```

允許擔任角色 Amazon Kendra 的信任原則。

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

建議您將 `aws:sourceAccount` 和包含 `aws:sourceArn` 在信任原則中。這會限制權限，並安全地檢查 `aws:sourceArn` 是否 `aws:sourceAccount` 與 `sts:AssumeRole` 動作的 IAM 角色原則中提供的相同，以及是否相同。這可防止未經授權的實體存取您的 IAM 角色及其權限。有關更多信息，請參閱有關 [困惑的副問題](#) 的 AWS Identity and Access Management 指南。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "kendra.amazonaws.com"
        ]
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "your-account-id"
        },
        "StringLike": {
          "aws:SourceArn": "arn:aws:kendra:your-region:your-account-id:index-id/*"
        }
      }
    }
  ]
}
```

```
    }  
  ]  
}
```

IAM 角色 AWS IAM Identity Center

當您使用 [UserGroupResolutionConfiguration](#) 物件從 AWS IAM Identity Center 身分識別來源擷取群組和使用者的存取層級時，您需要提供具有存取權限的角色 IAM Identity Center。

IAM 角色 AWS IAM Identity Center

允許 Amazon Kendra 存取的必要角色原則 IAM Identity Center。

```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Effect": "Allow",  
      "Action": [  
        "sso-directory:SearchUsers",  
        "sso-directory:ListGroupsWithUser",  
        "sso-directory:DescribeGroups",  
        "sso:ListDirectoryAssociations"  
      ],  
      "Resource": [  
        "*"   
      ]  
    },  
    {  
      "Sid": "iamPassRole",  
      "Effect": "Allow",  
      "Action": "iam:PassRole",  
      "Resource": "*",  
      "Condition": {  
        "StringEquals": {  
          "iam:PassedToService": [  
            "kendra.amazonaws.com"  
          ]  
        }  
      }  
    }  
  ]  
}
```

```
}
```

允許擔任角色 Amazon Kendra 的信任原則。

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

IAM Amazon Kendra 體驗的角色

使用 [CreateExperience](#) 或 [UpdateExperience](#) API 建立或更新搜尋應用程式時，必須提供具有存取必要操作和 IAM 身分中心權限的角色。

IAM Amazon Kendra 搜尋體驗的角色

允許 Amazon Kendra 存取儲存 Query 使用者和群組資訊的 QuerySuggestions 操作、SubmitFeedback 作業、作業和 IAM 身分中心的必要角色政策。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowsKendraSearchAppToCallKendraApi",
      "Effect": "Allow",
      "Action": [
        "kendra:GetQuerySuggestions",
        "kendra:Query",
        "kendra:DescribeIndex",
        "kendra:ListFaqs",
        "kendra:DescribeDataSource",
        "kendra:ListDataSources",
        "kendra:DescribeFaq",

```

```

    "kendra:SubmitFeedback"
  ],
  "Resource": [
    "arn:aws:kendra:your-region:your-account-id:index/index-id"
  ]
},
{
  "Sid": "AllowKendraSearchAppToDescribeDataSourcesAndFaq",
  "Effect": "Allow",
  "Action": [
    "kendra:DescribeDataSource",
    "kendra:DescribeFaq"
  ],
  "Resource": [
    "arn:aws:kendra:your-region:your-account-id:index/index-id/data-source/data-source-id",
    "arn:aws:kendra:your-region:your-account-id:index/index-id/faq/faq-id"
  ]
},
{
  "Sid": "AllowKendraSearchAppToCallSSODescribeUsersAndGroups",
  "Effect": "Allow",
  "Action": [
    "sso-directory:ListGroupForUser",
    "sso-directory:SearchGroups",
    "sso-directory:SearchUsers",
    "sso-directory:DescribeUser",
    "sso-directory:DescribeGroup",
    "sso-directory:DescribeGroups",
    "sso-directory:DescribeUsers",
    "sso:ListDirectoryAssociations"
  ],
  "Resource": [
    "*"
  ],
  "Condition": {
    "StringLike": {
      "kms:ViaService": [
        "kendra.your-region.amazonaws.com"
      ]
    }
  }
}
]

```

```
}
```

允許擔任角色 Amazon Kendra 的信任原則。

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

建議您將 `aws:sourceAccount` 和包含 `aws:sourceArn` 在信任原則中。這會限制權限，並安全地檢查 `aws:sourceArn` 是否 `aws:sourceAccount` 與 `sts:AssumeRole` 動作的 IAM 角色原則中提供的相同，以及是否相同。這可防止未經授權的實體存取您的 IAM 角色及其權限。有關更多信息，請參閱有關 [困惑的副問題](#) 的 AWS Identity and Access Management 指南。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "kendra.amazonaws.com"
        ]
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "your-account-id"
        },
        "StringLike": {
          "aws:SourceArn": "arn:aws:kendra:your-region:your-account-id:index-id/*"
        }
      }
    }
  ]
}
```

```

    }
  ]
}

```

IAM 自訂文件增強功能的角色

當您使用 [CustomDocumentEnrichmentConfiguration](#) 物件來套用文件中繼資料和內容的進階變更時，您必須提供具有執行 `PreExtractionHookConfiguration` 和/或所需權限的角色。 `PostExtractionHookConfiguration` 您可以設定 Lambda 函數， `PostExtractionHookConfiguration` 以便在擷取程序期間套用文件中繼資料和內容的進階變更。 `PreExtractionHookConfiguration` 如果您選擇啟用儲存 Amazon S3 貯體的伺服器端加密，您必須提供使用 AWS KMS 客戶主金鑰 (CMK) 的權限來加密和解密儲存在 Amazon S3 值區中的物件。

IAM 自訂文件增強功能的角色

允許 Amazon Kendra 執

行 `PreExtractionHookConfiguration` 並 `PostExtractionHookConfiguration` 加密 Amazon S3 儲存貯體的必要角色原則。

```

{
  "Version": "2012-10-17",
  "Statement": [{
    "Action": [
      "s3:GetObject",
      "s3:PutObject"
    ],
    "Resource": [
      "arn:aws:s3:::bucket-name/*"
    ],
    "Effect": "Allow"
  },
  {
    "Action": [
      "s3:ListBucket"
    ],
    "Resource": [
      "arn:aws:s3:::bucket-name"
    ],
    "Effect": "Allow"
  },

```

```
{
  "Effect": "Allow",
  "Action": [
    "kms:Decrypt",
    "kms:GenerateDataKey"
  ],
  "Resource": [
    "arn:aws:kms:your-region:your-account-id:key/key-id"
  ]
},
{
  "Effect": "Allow",
  "Action": [
    "lambda:InvokeFunction"
  ],
  "Resource": "arn:aws:lambda:your-region:your-account-id:function:lambda-function"
}]
}
```

選用的角色原則，Amazon Kendra 允許執行PreExtractionHookConfiguration且PostExtractionHookConfiguration不加密Amazon S3 儲存貯體。

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Action": [
      "s3:GetObject",
      "s3:PutObject"
    ],
    "Resource": [
      "arn:aws:s3:::bucket-name/*"
    ],
    "Effect": "Allow"
  },
  {
    "Action": [
      "s3:ListBucket"
    ],
    "Resource": [
      "arn:aws:s3:::bucket-name"
    ],
    "Effect": "Allow"
  }
]
```

```

},
{
  "Effect": "Allow",
  "Action": [
    "lambda:InvokeFunction"
  ],
  "Resource": "arn:aws:lambda:your-region:your-account-id:function:lambda-function"
}]
}

```

允許擔任角色 Amazon Kendra 的信任原則。

```

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

```

建議您將 `aws:sourceAccount` 和包含 `aws:sourceArn` 在信任原則中。這會限制權限，並安全地檢查 `aws:sourceArn` 是否 `aws:sourceAccount` 與 `sts:AssumeRole` 動作的 IAM 角色原則中提供的相同，以及是否相同。這可防止未經授權的實體存取您的 IAM 角色及其權限。有關更多信息，請參閱有關 [困惑的副問題](#) 的 AWS Identity and Access Management 指南。

```

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

```



```
        "StringEquals": {
            "aws:SourceAccount": "your-account-id"
        },
        "StringLike": {
            "aws:SourceArn": "arn:aws:kendra:your-region:your-account-id:index-  
id/*"
        }
    }
}
```

部署 Amazon Kendra

需要部署的時間Amazon Kendra搜索到您的網站，我們提供源代碼，您可以與 React 一起使用，以便在您的應用程序上獲得良好的開端。源代碼在修改後的 MIT 許可證下免費提供。您可以根據自己的需求調整這兩個範例查詢。提供的 React 應用程序是一個幫助你入門的例子。它不是生產就緒應用程序。

若要部署不含程式碼的搜尋應用程式，並在具有存取控制的搜尋頁面產生端點 URL，請參閱[Amazon Kendra 體驗建置器](#)。

下面的示例代碼添加Amazon Kendra搜索到現有的 React Web 應用程序：

- <https://kendasamples.s3.amazonaws.com/kendasamples-react-app>. 拉鍊開發人員可以用來在現有的 React Web 應用程式中建立功能性搜尋體驗的範例檔案。

這些範例是根據的搜尋頁面建模Amazon Kendra控制台。它們具有搜索和顯示搜索結果相同的功能。您可以使用整個示例，也可以僅選擇其中一個功能供您自己使用。

若要查看搜尋頁面中的三個元件Amazon Kendra控制台中，選擇代碼圖標 (</>) 從右側菜單。將指標懸停在每個部分上，以查看組件的簡短描述並獲取組件的源代碼的 URL。

主題

- [概要](#)
- [先決條件](#)
- [設定範例查詢](#)
- [主搜索頁面](#)
- [搜尋元件](#)
- [結果元件](#)
- [多面元件](#)
- [分頁組件](#)
- [建立不含程式碼的搜尋體驗](#)

概要

您可以將示例代碼添加到現有的 React Web 應用程序中以激活搜索。範例程式碼包含 Readme 檔案，其中包含設定新 React 開發環境的步驟。程式碼範例中的範例資料可用來示範搜尋。範例程式碼中的搜尋檔案和元件結構如下：

- 主要搜尋頁面 (Search.tsx)-這是包含所有元件的主要頁面。這是您將應用程序與Amazon KendraAPI。
- 搜尋列-這是使用者輸入搜尋詞彙並呼叫搜尋功能的元件。
- 結果-這是顯示結果的元件Amazon Kendra。它有三個組成部分：建議的答案，常見問題解答結果和推薦的文檔。
- 多面 (Facet)-這是在搜尋結果中顯示多面的元件，可讓您選擇多面來縮小搜尋範圍。
- 分頁-這是分頁回應來源的元件Amazon Kendra。

先決條件

開始之前，您必須準備好以下事項：

- Node.js 和故宮[已安裝](#)。需要 Node.js 版本 19 (含) 以上版本。
- Python 3 或 Python 2[下載並安裝](#)。
- [SDK for Java](#)或者[AWS SDK for JavaScript](#)以根據自己的需求調整 APIAmazon Kendra。
- 一個現有的反應 Web 應用程序。示例代碼包括一個 Readme 文件，其中包含如何設置新的 React 開發環境的步驟，包括使用所需的框架/庫。您也可以按照中的快速入門指示進行操作[有關創建 React Web 應用程序的反應文檔](#)。
- 在您的開發環境中配置的所需庫和依賴項。範例程式碼包含一個 Readme 檔案，其中列出必要的程式庫和套件相依性。請注意sass是必需的，如node-sass已棄用。如果您之前已安裝node-sass，卸載並安裝sass。

設定範例查詢

一個完整的添加過程Amazon Kendra搜索 React 應用程序位於代碼示例中包含的自述文件中。

開始使用 kendrasamples-react-app. 拉鍊

1. 請確定您已完成[先決條件](#)，包括下載和安裝 Node.js 和故宮。

2. 下載 `kendrasamples-react-app`。拉鍊和解壓縮。
3. 打開您的終端並轉到 `aws-kendra-example-react-app/src/services/`。打開 `local-dev-credentials.json` 並提供您的憑據。請勿將這個檔案加入任何公共存放庫。
4. 前往 `aws-kendra-example-react-app` 並安裝依賴關係 `package.json`。執行 `npm install`。
5. 在本地服務器上啟動應用程序的演示版本。執行 `npm start`。您可以通過在鍵盤上輸入來停止本地服務器 `Cmd/Ctrl + C`。
6. 您可以通過轉到更改端口或主機 (例如 , IP 地址) `package.json` 並更新主機和端口 : `"start": "HOST=[host] PORT=[port] react-scripts start"`。如果您使用視窗 : `"start": "set HOST=[host] && set PORT=[port] && react-scripts start"`。
7. 如果您有註冊的網站域 , 則可以在 `package.json` 您的應用程式名稱之後。例如 : `"homepage": "https://mywebsite.com"`。你必須跑 `npm install` 再次更新新的依賴關係 , 然後運行 `npm start`。
8. 若要建立應用程式 , 請執行 `npm build`。將構建目錄的內容上傳到您的託管服務提供商。

Warning

該應用程序是不生產準備。這是部署應用程序的示例 Amazon Kendra 搜索。

主搜索頁面

主搜索頁面 (`Search.tsx`) 包含所有範例搜尋元件。它包括用於輸出的搜索欄組件 , 結果組件顯示來自 [查詢](#) API 和用於通過響應分頁的分頁組件。

搜尋元件

搜尋元件提供用於輸入查詢文字的文字方塊。該 `onSearch` 函數是一個調用 `main` 函數的鉤子 `Search.tsx` 以使 Amazon Kendra [查詢](#) API 呼叫。

結果元件

結果元件會顯示來自 `Query` API。結果會顯示在三個獨立的區域中。

- 建議的答案 — 這些是QueryAPI。它包含最多三個建議的答案。在響應中，它們具有結果類型ANSWER。
- 常見問題解答 — 這些是回應傳回的常見問題結果。常見問題解答會分別新增至索引。在響應中，他們有類型QUESTION_ANSWER。如需詳細資訊，請參閱[問題和答案](#)。
- 建議文件 — 這些是其他文件Amazon Kendra在回應中傳回。在從回應QueryAPI，他們有類型DOCUMENT。

結果元件會共用一組元件，用於亮顯、標題、連結等功能。共用元件必須存在，結果元件才能運作。

多面元件

多面元件會列出搜尋結果中可用的多面。每個 Facet 會沿著特定維度 (例如作者) 對回應進行分類。您可以從清單中選擇一個，將搜尋精簡為特定 Facet。

選取 Facet 之後，元件會呼叫Query具有屬性篩選器，可將搜尋限制為符合 Facet 的文件。

分頁組件

分頁元件可讓您顯示搜尋結果Query多個頁面中的 API。它調整這個Query使用指令介面PageSize和PageNumber用於獲取特定結果頁面的參數。

建立不含程式碼的搜尋體驗

您可以建置和部署Amazon Kendra搜索應用程序，而無需任何前端代碼。Amazon Kendra體驗建置器只要按幾下滑鼠，就能協助您建置和部署功能齊全的搜尋應用程式，讓您立即開始搜尋。您可以自定義設計搜索頁面並調整搜索，以根據用戶的需求量身定制體驗。Amazon Kendra為您的搜尋頁面產生唯一且完全託管的端點 URL，以開始搜尋您的文件和常見問題集。您可以快速建立搜尋體驗的概念證明，並與其他人分享。

您可以使用建置器中提供的搜尋體驗範本來自訂搜尋。您可以邀請其他人協作建立您的搜尋體驗，或評估搜尋結果以供調整。當您的搜尋體驗準備好讓使用者開始搜尋之後，您只需共用安全端點 URL 即可。

搜尋體驗產生器的運作方式

建立搜尋體驗的整體程序如下：

1. 您可以為搜尋體驗提供名稱、說明並選擇要用於搜尋體驗的資料來源，以建立搜尋體驗。
2. 您可以根據自己的使用者和群組清單AWS IAM Identity Center然後將存取權指派給他們您的搜尋體驗。您將自己納入為體驗的擁有者。如需詳細資訊，請參閱[the section called “提供您搜尋頁面的存取”](#)。
3. 您可以開啟這個Amazon Kendra體驗產生器可設計和調整您的搜尋頁面。您可以將搜尋體驗的端點 URL 分享給您指派自己編輯存取權或檢視搜尋存取權限的其他使用者。

你打電話給[CreateExperience](#)用於建立和設定搜尋體驗的 API。如果您使用控制台，請選擇索引，然後選擇體驗在導覽功能表中設定您的體驗。

設計和調整您的搜尋體驗

建立並設定搜尋體驗後，您可以使用端點 URL 開啟搜尋體驗，開始將您的搜尋自訂為具有編輯者存取權限的擁有者。您可以在搜尋方塊中輸入查詢，然後使用側邊面板上的編輯選項自訂搜尋，以查看它們如何套用至您的頁面。當您準備好發佈時，請選取發佈。您也可以在其間切換至即時檢視，以檢視您的搜尋頁面的最新發佈版本，以及切換到建置模式，以編輯或自訂您的搜尋頁面。

以下是您可以自訂搜尋體驗的方式。

篩選條件

新增多面向搜尋或依文件屬性篩選。這包括自訂屬性。您可以使用自己設定的中繼資料欄位來新增篩選器。例如，要按每個城市類別進行搜索，請使用 `_category` 包含所有城市類別的自定義文檔屬性。

建議答案

將機器學習產生的答案新增至使用者的查詢。例如，「這門課程有多困難？」。Amazon Kendra 可以檢索與課程難度相關的所有文檔中最相關的文本，並提出最相關的答案。

常見問答集

新增常見問題集文件以提供常見問題的答案。例如，「完成這個課程需要多少小時？」。Amazon Kendra 可以使用包含此問題答案的 FAQ 文檔並給出正確答案。

Sort

添加搜索結果的排序，以便您的用戶可以按照相關性，創建時間，上次更新時間和其他排序條件來組織結果。

Documents

設定文件或搜尋結果在搜尋頁面上的顯示方式。您可以設定頁面上顯示的結果數目、包括分頁 (例如頁碼)、啟用使用者回饋按鈕，以及排列文件中繼資料欄位在搜尋結果中的顯示方式。

語言

選取語言以篩選所選語言的搜尋結果或文件。

搜索框

設定搜尋方塊的大小和預留位置文字，以及允許查詢建議。

相關調整

為文件中繼資料欄位新增提升功能，以便在使用者搜尋文件時對這些欄位增加權重。您可以添加一個從 1 開始並逐步增加到 10 的權重。您可以提升文字、日期和數字欄位類型。例如，給 `_last_updated_at` 和 `_created_at` 比其他欄位更重要或重要性，視其重要性而定，將這些欄位的權數指定為 1 到 10。您可以針對每個搜尋應用程式或體驗套用不同的相關性調整設定。

提供您搜尋頁面的存取

透過 IAM 身分中心存取您的搜尋體驗。設定搜尋體驗時，您會授與 Identity Center 目錄中列出的其他人存取您的 Amazon Kendra 搜索頁面。他們會收到一封電子郵件，指示他們使用 IAM 身分中心中的登入資料登入以存取搜尋頁面。您必須在組織層級或帳戶持有人層級設定 IAM 身分中心 AWS Organizations。如需設定 IAM 身分中心的詳細資訊，請參閱 [開始使用 IAM 身分識別中心](#)。

您可以透過搜尋體驗在 IAM 身分中心啟用使用者身分並指派檢視器或者擁有者使用 API 或控制台訪問權限。

- 檢視器: 允許發出查詢，接收與其搜索相關的建議答案，並提供他們的反饋 Amazon Kendra 以便它不斷改善搜索。
- 擁有者: 允許自定義搜索頁面的設計，調整搜索，並將搜索應用程序用作檢視器。目前不支援在主控台中停用檢視器的存取權。

若要指派其他人存取您的搜尋體驗，請先在 IAM 身分中心啟用使用者身分，Amazon Kendra 使用體驗 [ExperienceConfiguration](#) 物件。您可以指定包含使用者識別碼 (例如使用者名稱或電子郵件地址) 的欄位名稱。然後，您可以使用 [AssociateEntitiesToExperience](#) API 並將其權限定義為檢視器或者擁有

者使用 [AssociatePersonasToEntities](#) API。您可以使用 [EntityConfiguration](#) 物件，以及該使用者或群組是否為檢視器或者擁有者使用 [EntityPersonaConfiguraton](#) 物件。

若要指派其他人使用主控台存取您的搜尋體驗，您必須先建立體驗並確認您的身分，並確認您是擁有者。然後，您可以將其他使用者或群組指派為檢視者或擁有者。在主控台中，選取您的索引，然後選取這個索引體驗在導航功能表中。建立體驗之後，您可以從清單中選取您的體驗。前往存取管理，將使用者或群組指派為檢閱者或擁有者。

設定搜尋體驗

下列是設定或建立搜尋體驗的範例。

Console

若要建立 Amazon Kendra 搜索體驗

1. 在左側導覽窗格的索引，選取體驗然後選取創造體驗。
2. 在「」設定體驗頁面上，輸入體驗的名稱和描述，選擇內容來源，然後選擇體驗的名稱和描述。如需 IAM 角色的詳細資訊，請參閱 [適用的 IAM 角色 Amazon Kendra 經驗](#)。
3. 在「」從身分識別中心目錄確認您的身分頁面上，選擇您的用戶 ID，例如您的電子郵件。如果您沒有身分識別中心目錄，只要輸入您的全名和電子郵件即可建立身分識別中心目錄。這包括您身為體驗的使用者，並自動指派擁有者存取權限給您。
4. 在「」檢閱以開啟體驗建置器頁面上，查看您的組態詳細資訊並選取建立體驗並開啟體驗產生器，開始編輯您的搜尋頁面。

CLI

若要建立 Amazon Kendra 經驗

```
aws kendra create-experience \  
  --name experience-name \  
  --description "experience description" \  
  --index-id index-id \  
  --role-arn arn:aws:iam::account-id:role/role-name \  
  --configuration '{"ExperienceConfiguration":[{"ContentSourceConfiguration":  
{"DataSourceIds":["data-source-1","data-source-2"]},  
"UserIdentityConfiguration":"identity attribute name"]}]}'  
  
aws kendra describe-experience \  
  --endpoints experience-endpoint-URL(s)
```


Python

若要建立Amazon Kendra經驗

```
import boto3
from botocore.exceptions import ClientError
import pprint
import time

kendra = boto3.client("kendra")

print("Create an experience.")

# Provide a name for the experience
name = "experience-name"
# Provide an optional description for the experience
description = "experience description"
# Provide the index ID for the experience
index_id = "index-id"
# Provide the IAM role ARN required for Amazon Kendra experiences
role_arn = "arn:aws:iam::${account-id}:role/${role-name}"
# Configure the experience
configuration = {"ExperienceConfiguration":
    [
        {
            "ContentSourceConfiguration": {"DataSourceIds": ["data-source-1", "data-
source-2"]},
            "UserIdentityConfiguration": "identity attribute name"
        }
    ]
}

try:
    experience_response = kendra.create_experience(
        Name = name,
        Description = description,
        IndexId = index_id,
        RoleArn = role_arn,
        Configuration = configuration
    )

    pprint.pprint(experience_response)

    experience_endpoints = experience_response["Endpoints"]

    print("Wait for Amazon Kendra to create the experience.")
```

```
while True:
    # Get the details of the experience, such as the status
    experience_description = kendra.describe_experience(
        Endpoints = experience_endpoints
    )
    status = experience_description["Status"]
    print(" Creating experience. Status: "+status)
    time.sleep(60)
    if status != "CREATING":
        break

except ClientError as e:
    print("%s" % e)

print("Program ends.")
```

Java

建立 Amazon Kendra

```
package com.amazonaws.kendra;

import java.util.concurrent.TimeUnit;
import software.amazon.awssdk.services.kendra.KendraClient;
import software.amazon.awssdk.services.kendra.model.CreateExperienceRequest;
import software.amazon.awssdk.services.kendra.model.CreateExperienceResponse;
import software.amazon.awssdk.services.kendra.model.DescribeExperienceRequest;
import software.amazon.awssdk.services.kendra.model.DescribeExperienceResponse;
import software.amazon.awssdk.services.kendra.model.ExperienceStatus;

public class CreateExperienceExample {

    public static void main(String[] args) throws InterruptedException {
        System.out.println("Create an experience");

        String experienceName = "experience-name";
        String experienceDescription = "experience description";
        String indexId = "index-id";
        String experienceRoleArn = "arn:aws:iam::account-id:role/role-name";

        KendraClient kendra = KendraClient.builder().build();
```

```
CreateExperienceRequest createExperienceRequest = CreateExperienceRequest
    .builder()
    .name(experienceName)
    .description(experienceDescription)
    .roleArn(experienceRoleArn)
    .configuration(
        ExperienceConfiguration
            .builder()
            .contentSourceConfiguration(
                ContentSourceConfiguration(
                    .builder()
                    .dataSourceIds("data-source-1","data-source-2")
                    .build()
                )
            )
            .userIdentityConfiguration(
                UserIdentityConfiguration(
                    .builder()
                    .identityAttributeName("identity-attribute-name")
                    .build()
                )
            ).build()
    ).build();

CreateExperienceResponse createExperienceResponse =
kendra.createExperience(createExperienceRequest);
System.out.println(String.format("Experience response %s",
createExperienceResponse));

String experienceEndpoints = createExperienceResponse.endpoints();

System.out.println(String.format("Wait for Kendra to create the
experience.", experienceEndpoints));
while (true) {
    DescribeExperienceRequest describeExperienceRequest =
DescribeExperienceRequest.builder().endpoints(experienceEndpoints).build();
    DescribeExperienceResponse describeEpxerienceResponse =
kendra.describeExperience(describeExperienceRequest);
    ExperienceStatus status = describeExperienceResponse.status();
    TimeUnit.SECONDS.sleep(60);
    if (status != ExperienceStatus.CREATING) {
        break;
    }
}
```

```
        System.out.println("Experience creation is complete.");  
    }  
}
```

調整容量

Amazon Kendra 以容量單位為索引提供資源。每個容量單位都會為索引提供額外的資源。有單獨的容量單位用於文檔存儲和查詢。您只能將容量單位新增至 Amazon Kendra 企業版索引。您無法將容量新增至開發人員版索引。

文件儲存容量單位為索引提供下列額外儲存空間。

- 10 萬份文件或 30 GB 的儲存空間。

查詢容量單位會針對索引提供下列額外查詢。

- 每秒 0.1 個查詢或每天約 8,000 個查詢。

每個索引的基本容量等於 1 個容量單位 (30 GB 的儲存空間和每秒 0.1 個查詢)。每個額外的容量單位都會產生額外費用。如需詳細資訊，請參閱 [Amazon Kendra 定價](#)。

您最多可以將 100 個額外容量單位新增至儲存空間，並查詢資源以取得索引。如果您需要更多單位，只需[聯絡 Support](#) 部門。

您每天最多可以調整 5 次容量單位，以符合您的使用需求。您無法將文件儲存容量減少到索引中儲存的文件數量以下。例如，如果您要儲存 150,000 份文件，則無法將儲存容量減少到 1 個額外單元以下。

您可以選取索引名稱以開啟索引設定和其他資訊，以檢視索引在主控台中使用的資源，或者您也可以使用 [DescribeIndexAPI](#)。

Amazon Kendra 當您超過索引的容量時，也會傳回例外狀況。ServiceQuotaExceededException 當所有文檔的總提取大小超過索引的限制時，您會得到一個。當文檔數量超過索引的限制時，您會得到每個文檔的 InvalidRequest 個。ThrottlingException 當每秒查詢次數超過限制時，您會得到一個。如需有關限制的詳細資訊，[請參閱 Amazon Kendra](#)。

累計查詢最多可持續 24 小時。

檢視容量

選取索引名稱以存取詳細資料，以檢視索引與 Amazon Kendra 主控台搭配使用的資源。主控台也提供使用情況圖表，讓您可以判斷索引使用多少儲存空間和查詢容量。您可以使用此資訊來協助您規劃何時增加額外容量。

要查看文檔存儲和查詢使用 (控制台)

1. 請登入 AWS Management Console 並開啟 Amazon Kendra 主控台，網址為 <https://console.aws.amazon.com/kendra/home>。
2. 從索引清單中，選擇您要存取的索引。
3. 捲動至 [設定] 區段以檢視目前的總文件儲存空間和查詢容量。

若要使用 Amazon Kendra API 檢視容量，請使用 [DescribeIndex](#) API 中的 CapacityUnits 參數。

新增和移除容量

如果您的索引需要額外的容量，可以使用主控台或 Amazon Kendra API 新增它。

若要新增或移除儲存空間或查詢容量 (主控台)

1. 請登入 AWS Management Console 並開啟 Amazon Kendra 主控台，網址為 <https://console.aws.amazon.com/kendra/home>。
2. 從索引清單中，選擇您要存取的索引。
3. 選取編輯，或從動作下拉式清單中選取編輯。
4. 選取下一步，即可移至啟動設定詳細資訊頁面。
5. 新增或移除文件儲存空間和/或查詢容量單位。
6. 繼續選取 [下一步] 以移至檢閱頁面，然後選取 [更新] 以儲存變更。

更新索引的容量之後，變更可能需要數分鐘才會生效。

若要使用 Amazon Kendra API 新增或移除容量，請使用 [UpdateIndex](#) API 中的 CapacityUnits 參數。

Amazon Kendra 智能排名能力

容量單位會針對重新評分執行計畫，每秒提供下列額外的重新評分要求。重新評分執行計畫是用來佈建 [重新分數 API](#) 的資源。

- 每秒 0.01 個要求。

每個重新評分執行計畫都具有等於 1 個容量單位的基本容量（每秒 0.01 個請求）。每個額外的容量單位都會產生額外費用。如需詳細資訊，請參閱 [Amazon Kendra 定價](#)。

您最多可以為重新評分執行計畫新增 1000 個額外容量單位。如果您需要更多單位，只需 [聯絡 Support](#) 部門。

查詢建議容量

使用 [查詢建議](#) 時，基本查詢容量為每秒 2.5 次 [GetQuerySuggestions](#) 呼

叫。GetQuerySuggestions 容量是索引佈建查詢容量的五倍，或每秒 2.5 次呼叫的基本容量（以較高者為準）。例如，索引的基本容量是每秒 0.1 個查詢，GetQuerySuggestions 容量的基礎為每秒 2.5 個呼叫。如果將每秒另外 0.1 次查詢新增到索引的每秒 0.2 次查詢總數，則 GetQuerySuggestions 容量為每秒 2.5 次呼叫（高於每秒 0.2 次查詢的五倍）。

Amazon Kendra 經驗能力

搜尋體驗能力

Amazon Kendra 開始節流 Query，SubmitFeedback 為了您的 Amazon Kendra 體驗 QuerySuggestions，每秒 15 個請求和每秒 40 個請求以進行查詢大量批量。對於查詢容量單位超過 150 個的索引，這些限制仍然適用。

例如，索引的查詢容量單位為 150，因此您的搜尋體驗應用程式每秒可處理 15 個要求。但是，如果您擴展到 200 個查詢容量單位，則您的搜索體驗應用程式仍然只能處理每秒 15 個請求。如果您將索引限制為 100 個查詢容量單位，則您的搜尋體驗應用程式每秒只能處理 10 個要求。

調適性查詢成組分解

Amazon Kendra 具有 1 個查詢容量單位的佈建基本容量。您每天最多可以使用 8,000 個查詢，最低輸送量為每秒 0.1 個查詢（每個查詢容量單位）。累積的查詢將持續長達 24 小時，並且可以容納突發的流

量。允許的突發量會有所不同，因為它取決於任何給定時間的叢集負載。佈建足夠的查詢容量單位來處理尖峰負載層級。

內建的調適性查詢大量批次處理超出佈建輸送量的非預期流量突增 Amazon Kendra 的調適性方法。調適性查詢成組分解可在的企業版中使用。 Amazon Kendra

調適性查詢大量批次處理是一項內建功能，可讓您套用未使用的查詢容量來處理非預期的流量。

Amazon Kendra 以每秒佈建的查詢速率 (每秒) 累積未使用的查詢，直到您為 Amazon Kendra 索引佈建的最大查詢數目為止。這些累積的查詢會用於超過配置容量的非預期流量。調適性查詢成組分解的最佳效能可能會有所不同，這取決於數個因素，例如總索引大小、查詢複雜度、累積未使用的查詢，以及索引的整體負載。建議您執行自己的負載測試，以準確測量爆發能力。

開始使用

本節說明如何建立資料來源，並將文件新增至 Amazon Kendra 索引。提供了 AWS 主控台、Python 程式使用的指示 AWS SDK for Python (Boto3)，以及 Java 程式使用 AWS SDK for Java. AWS CLI

主題

- [必要條件](#)
- [開始使用主 Amazon Kendra 控制台](#)
- [開始使用 \(AWS CLI\)](#)
- [開始使用 \(AWS SDK for Python \(Boto3\)\)](#)
- [開始使用 \(AWS SDK for Java\)](#)
- [開始使用 Amazon S3 資料來源 \(主控台\)](#)
- [開始使用 MySQL 資料庫資料來源 \(主控台\)](#)
- [開始使用 AWS IAM Identity Center 身分識別來源 \(主控台\)](#)

必要條件

以下步驟是入門練習的準備位置。這些步驟會示範如何設定帳戶、建立可代表您撥打電話之 Amazon Kendra 權限的 IAM 角色，以及為 Amazon S3 值區中的文件建立索引。使用 S3 儲存貯體做為範例，但您可以使用 Amazon Kendra 支援的其他資料來源。請參閱[資料來源](#)。

註冊一個 AWS 帳戶

如果您沒有 AWS 帳戶，請完成以下步驟來建立一個。

若要註冊成為 AWS 帳戶

1. 開啟 <https://portal.aws.amazon.com/billing/signup>。
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。

當您註冊一個時 AWS 帳戶，將創建 AWS 帳戶根使用者一個。根使用者有權存取該帳戶中的所有 AWS 服務 和資源。安全性最佳做法是將管理存取權指派給使用者，並僅使用 [root 使用者來執行需要 root 使用者存取權](#)的工作。

AWS 註冊過程完成後，會向您發送確認電子郵件。您可以隨時登錄 <https://aws.amazon.com/> 並選擇我的帳戶，以檢視您目前的帳戶活動並管理帳戶。

建立具有管理權限的使用者

註冊後，請保護您的 AWS 帳戶 AWS 帳戶根使用者 AWS IAM Identity Center、啟用和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. 選擇 Root 使用者並輸入您的 AWS 帳戶 電子郵件地址，以帳戶擁有者身分登入。[AWS Management Console](#)在下一頁中，輸入您的密碼。

如需使用根使用者登入的說明，請參閱 AWS 登入 使用者指南中的[以根使用者身分登入](#)。

2. 若要在您的根使用者帳戶上啟用多重要素驗證 (MFA)。

如需指示，請參閱《IAM 使用者指南》中的[為 AWS 帳戶 根使用者啟用虛擬 MFA 裝置 \(主控台\)](#)。

建立具有管理權限的使用者

1. 啟用 IAM Identity Center。

如需指示，請參閱 AWS IAM Identity Center 使用者指南中的[啟用 AWS IAM Identity Center](#)。

2. 在 IAM 身分中心中，將管理存取權授予使用者。

[若要取得有關使用 IAM Identity Center 目錄 做為身分識別來源的自學課程，請參閱《使用指南》IAM Identity Center 目錄中的「以預設值設定使用AWS IAM Identity Center 者存取」。](#)

以具有管理權限的使用者身分登入

- 若要使用您的 IAM Identity Center 使用者簽署，請使用建立 IAM Identity Center 使用者時傳送至您電子郵件地址的簽署 URL。

如需使用 IAM 身分中心使用者[登入的說明](#)，請參閱[使用AWS 登入 者指南中的登入 AWS 存取入口網站](#)。

指派存取權給其他使用者

1. 在 IAM 身分中心中，建立遵循套用最低權限許可的最佳做法的權限集。

如需指示，請參閱《AWS IAM Identity Center 使用指南》中的「[建立權限集](#)」。

2. 將使用者指派給群組，然後將單一登入存取權指派給群組。

如需指示，請參閱《AWS IAM Identity Center 使用指南》中的「[新增群組](#)」。

- 如果您使用的 S3 儲存貯體包含要測試的文件 Amazon Kendra，請在您使用的相同區域建立 S3 儲存貯體 Amazon Kendra。如需指示，請參閱 [Amazon 簡單儲存服務使用者指南中的建立和設定 S3 儲存貯體](#)。

將您的文件上傳到 S3 儲存貯體。如需指示，請參閱 Amazon 簡易儲存服務使用者指南中的 [上傳、下載和管理物件](#)。

如果您使用其他資料來源，則必須具有作用中的站台和認證才能連線到資料來源。

如果您要使用主控台開始使用，請從開始 [開始使用主 Amazon Kendra 控制台](#)。

Amazon Kendra 資源: AWS CLI, SDK, 控制台

如果您使用 CLI、SDK 或主控台，則需要特定權限。

若要用 Amazon Kendra 於 CLI、SDK 或主控台，您必須具有允許代表您 Amazon Kendra 建立和管理資源的權限。視您的使用案例而定，如果您想要透過自訂 CMK、Identity Center 目錄加密資料 (AWS KMS keys 如果您想要整合 AWS IAM Identity Center 或 [建立搜尋體驗](#))，則這些權限包括對 [Amazon Kendra API 本身](#) 的存取權。如需不同使用案例的完整權限清單，請參閱 [IAM 角色](#)。

首先，您必須將以下許可附加到 IAM 使用者。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Stmt1644430853544",
      "Action": [
        "kms:CreateGrant",
        "kms:DescribeKey"
      ],
      "Effect": "Allow",
      "Resource": "*"
    }
  ]
}
```

```
"Sid": "Stmt1644430878150",
"Action": "kendra:*",
"Effect": "Allow",
"Resource": "*"
},
{
  "Sid": "Stmt1644430973706",
  "Action": [
    "sso:AssociateProfile",
    "sso:CreateManagedApplicationInstance",
    "sso>DeleteManagedApplicationInstance",
    "sso:DisassociateProfile",
    "sso:GetManagedApplicationInstance",
    "sso:GetProfile",
    "sso:ListDirectoryAssociations",
    "sso:ListProfileAssociations",
    "sso:ListProfiles"
  ],
  "Effect": "Allow",
  "Resource": "*"
},
{
  "Sid": "Stmt1644430999558",
  "Action": [
    "sso-directory:DescribeGroup",
    "sso-directory:DescribeGroups",
    "sso-directory:DescribeUser",
    "sso-directory:DescribeUsers"
  ],
  "Effect": "Allow",
  "Resource": "*"
},
{
  "Sid": "Stmt1644431025960",
  "Action": [
    "identitystore:DescribeGroup",
    "identitystore:DescribeUser",
    "identitystore:ListGroups",
    "identitystore:ListUsers"
  ],
  "Effect": "Allow",
  "Resource": "*"
}
]
```

```
}
```

其次，如果您使用 CLI 或 SDK，您還必須建立 IAM 角色和原則才能存取 Amazon CloudWatch Logs。如果您使用的是主控台，則不需要為此建立 IAM 角色和原則。您可以將其創建為控制台過程的一部分。

為和 SDK 創建一個 IAM 角色 AWS CLI 和策略，Amazon Kendra 以便訪問您的 Amazon CloudWatch Logs。

1. 登入 AWS Management Console 並開啟身分與存取權管理主控台，網址為 <https://console.aws.amazon.com/iam/>。
2. 從左側功能表中選擇 [策略]，然後選擇 [建立策略]。
3. 選擇 [JSON]，然後使用下列項目取代預設原則：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "cloudwatch:PutMetricData"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "cloudwatch:namespace": "AWS/Kendra"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": [
        "logs:DescribeLogGroups"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "logs:CreateLogGroup"
      ],
      "Resource": [
```

```

        "arn:aws:logs:region:account ID:log-group:/aws/kendra/*"
    ]
},
{
    "Effect": "Allow",
    "Action": [
        "logs:DescribeLogStreams",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
    ],
    "Resource": [
        "arn:aws:logs:region:account ID:log-group:/aws/kendra/*:log-
stream:*"
    ]
}
]
}

```

4. 選擇檢閱政策。
5. 為原則命名，"KendraPolicyForGettingStartedIndex"然後選擇 [建立原則]。
6. 從左側功能表中選擇 [角色]，然後選擇 [建立角色]。
7. 選擇 [其他 AWS 帳戶]，然後在 [帳戶 ID] 中輸入您的帳戶 ID。選擇下一步：許可。
8. 選擇您在上面創建的策略，然後選擇下一步：標籤
9. 不要新增任何標籤。選擇下一步：檢閱。
10. 為角色命名，"KendraRoleForGettingStartedIndex"然後選擇 [建立角色]。
11. 尋找您剛建立的角色。選擇要開啟摘要的角色名稱。選擇 [信任關係]，然後選擇 [編輯信任關係]
12. 以下列項目取代現有的信任關係：

```

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

```

13. 選擇更新信任政策。

第三，如果您使 Amazon S3 用存放文件或使用 S3 進行測試 Amazon Kendra，則還必須建立 IAM 角色和政策來存取儲存貯體。如果您正在使用其他資料來源，請參閱[資料來源的IAM 角色](#)。

建立允許 Amazon Kendra 存取 Amazon S3 值區並建立索引的 IAM 角色和政策。

1. 登入 AWS Management Console 並開啟身分與存取權管理主控台，網址為 <https://console.aws.amazon.com/iam/>。
2. 從左側功能表中選擇 [策略]，然後選擇 [建立策略]。
3. 選擇 [JSON]，然後使用下列項目取代預設原則：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "s3:GetObject"
      ],
      "Resource": [
        "arn:aws:s3:::bucket name/*"
      ],
      "Effect": "Allow"
    },
    {
      "Action": [
        "s3:ListBucket"
      ],
      "Resource": [
        "arn:aws:s3:::bucket name"
      ],
      "Effect": "Allow"
    },
    {
      "Effect": "Allow",
      "Action": [
        "kendra:BatchPutDocument",
        "kendra:BatchDeleteDocument"
      ],
      "Resource": "arn:aws:kendra:region:account ID:index/*"
    }
  ]
}
```

```
]
}
```

4. 選擇檢閱政策。
5. 將策略命名為 "KendraPolicyForGettingStartedDataSource"，然後選擇 [建立策略]。
6. 從左側功能表中選擇 [角色]，然後選擇 [建立角色]。
7. 選擇 [其他 AWS 帳戶]，然後在 [帳戶 ID] 中輸入您的帳戶 ID。選擇下一步：許可。
8. 選擇您在上面創建的策略，然後選擇下一步：標籤
9. 不要新增任何標籤。選擇下一步：檢閱。
10. 將角色命名為 "KendraRoleForGettingStartedDataSource"，然後選擇 [建立角色]。
11. 尋找您剛建立的角色。選擇要開啟摘要的角色名稱。選擇 [信任關係]，然後選擇 [編輯信任關係]
12. 以下列項目取代現有的信任關係：

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

13. 選擇更新信任政策。

根據您要使用 Amazon Kendra API 的方式，執行下列其中一個動作。

- [開始使用 \(AWS CLI\)](#)
- [開始使用 \(AWS SDK for Java\)](#)
- [開始使用 \(AWS SDK for Python \(Boto3\)\)](#)

開始使用主 Amazon Kendra 控制台

下列程序顯示如何使用 AWS 主控台建立及測試 Amazon Kendra 索引。在程序中，您可以為索引建立索引和資料來源。最後，您可以透過提出搜尋要求來測試索引。

第 1 步：要創建一個索引 (控制台)

1. 登入 AWS 管理主控台，然後開啟 Amazon Kendra 主控台，網址為 <https://console.aws.amazon.com/kendra/>。
2. 選取 [索引] 區段中的 [建立索引]。
3. 在 [指定索引詳細資訊] 頁面中，為您的索引指定名稱和說明。
4. 在 [IAM 角色] 中，選擇 [建立新角色]，然後為該角色指定名稱。該 IAM 角色的前綴為「AmazonKendra-」。
5. 將所有其他欄位保留為預設值。選擇下一步。
6. 在 [設定使用者存取控制] 頁面中選擇 [下一步]。
7. 在佈建詳細資料頁面中，選擇開發人員版本。
8. 選擇 [建立] 以建立索引。
9. 等待您的索引創建。Amazon Kendra 為您的索引佈建硬體。此操作可能需要一些時間。

步驟 2：若要將資料來源新增至索引 (主控台)

1. 檢視可用的 [資料來源](#)，以連線 Amazon Kendra 到文件並建立索引。
2. 在導覽窗格中，選取 [資料來源]，然後為所選資料來源選取 [新增資料來源]。
3. 請依照下列步驟設定資料來源。

步驟 3：要搜索索引 (控制台)

1. 在功能窗格中，選擇搜尋索引的選項。
2. 輸入適合您索引的搜尋字詞。顯示排名最前的結果和頂端的文件結果。

開始使用 (AWS CLI)

下列程序顯示如何使用建立 Amazon Kendra 索引 AWS CLI。此程序會建立資料來源、索引，並在索引上執行查詢。

若要建立 Amazon Kendra 索引 (CLI)

1. 執行[必要條件](#).
2. 輸入下列命令以建立索引。

```
aws kendra create-index \  
  --name cli-getting-started-index \  
  --description "Index for CLI getting started guide." \  
  --role-arn arn:aws:iam::account id:role/KendraRoleForGettingStartedIndex
```

3. 等待 Amazon Kendra 建立索引。使用以下命令檢查進度。當狀態欄位為時ACTIVE，請繼續執行下一個步驟。

```
aws kendra describe-index \  
  --id index id
```

4. 在命令提示字元中，輸入下列命令以建立資料來源。

```
aws kendra create-data-source \  
  --index-id index id \  
  --name data source name \  
  --role-arn arn:aws:iam::account id:role/KendraRoleForGettingStartedDataSource \  
  --type S3 \  
  --configuration '{"S3Configuration":{"BucketName":"S3 bucket name"}}'
```

如果您使用範本資料架構連接至資料來源，請設定範本資料架構。

```
aws kendra create-data-source \  
  --index-id index id \  
  --name data source name \  
  --role-arn arn:aws:iam::account id:role/KendraRoleForGettingStartedDataSource \  
  --type TEMPLATE \  
  --configuration '{"TemplateConfiguration":{"Template":{"JSON schema}}}'
```

5. 創建數據源需要 Amazon Kendra 一段時間。輸入以下命令以檢查進度。當狀態為時ACTIVE，請繼續進行下一個步驟。

```
aws kendra describe-data-source \  
  --id data source ID \  
  --index-id index ID
```

6. 輸入以下命令以同步化資料來源。

```
aws kendra start-data-source-sync-job \  
  --id data source ID \  
  --index-id index ID
```

7. Amazon Kendra 將為您的資料來源建立索引。所花費的時間取決於文檔的數量。您可以使用以下命令檢查同步工作的狀態。當狀態為時ACTIVE，請繼續進行下一個步驟。

```
aws kendra describe-data-source \  
  --id data source ID \  
  --index-id index ID
```

8. 輸入以下命令以進行查詢。

```
aws kendra query \  
  --index-id index ID \  
  --query-text "search term"
```

搜尋結果會以 JSON 格式顯示。

開始使用 (AWS SDK for Python (Boto3))

下面的程序是在 Python 程序 Amazon Kendra 中使用的一個例子。該程序執行以下操作：

1. 使用[CreateIndex](#)操作創建一個新的索引。
2. 等待索引建立完成。它使用[DescribeIndex](#)操作來監視索引的狀態。
3. 索引處於作用中狀態之後，它會使用[CreateDataSource](#)作業建立資料來源。
4. 等待資料來源建立完成。它使用[DescribeDataSource](#)操作來監視數據源的狀態。
5. 當資料來源處於[StartDataSourceSyncJob](#)作用中狀態時，它會使用作業將索引與資料來源的內容同步化。

```
import boto3  
from botocore.exceptions import ClientError  
import pprint  
import time  
  
kendra = boto3.client("kendra")
```

```
print("Create an index.")

# Provide a name for the index
index_name = "python-getting-started-index"
# Provide an optional decription for the index
description = "Getting started index"
# Provide the IAM role ARN required for indexes
index_role_arn = "arn:aws:iam::${accountId}:role/KendraRoleForGettingStartedIndex"

try:
    index_response = kendra.create_index(
        Description = description,
        Name = index_name,
        RoleArn = index_role_arn
    )

    pprint.pprint(index_response)

    index_id = index_response["Id"]

    print("Wait for Amazon Kendra to create the index.")

    while True:
        # Get the details of the index, such as the status
        index_description = kendra.describe_index(
            Id = index_id
        )
        # When status is not CREATING quit.
        status = index_description["Status"]
        print(" Creating index. Status: "+status)
        time.sleep(60)
        if status != "CREATING":
            break

    print("Create an S3 data source.")

    # Provide a name for the data source
    data_source_name = "python-getting-started-data-source"
    # Provide an optional description for the data source
    data_source_description = "Getting started data source."
    # Provide the IAM role ARN required for data sources
    data_source_role_arn = "arn:aws:iam::${accountId}:role/
KendraRoleForGettingStartedDataSource"
```

```
# Provide the data source connection information
S3_bucket_name = "S3-bucket-name"
data_source_type = "S3"
# Configure the data source
configuration = {"S3Configuration":
    {
        "BucketName": S3_bucket_name
    }
}

"""
If you connect to your data source using a template schema,
configure the template schema
configuration = {"TemplateConfiguration":
    {
        "Template": {JSON schema}
    }
}
"""

data_source_response = kendra.create_data_source(
    Name = data_source_name,
    Description = data_source_name,
    RoleArn = data_source_role_arn,
    Type = data_source_type,
    Configuration = configuration,
    IndexId = index_id
)

pprint.pprint(data_source_response)

data_source_id = data_source_response["Id"]

print("Wait for Amazon Kendra to create the data source.")

while True:
    # Get the details of the data source, such as the status
    data_source_description = kendra.describe_data_source(
        Id = data_source_id,
        IndexId = index_id
    )
    # If status is not CREATING, then quit
    status = data_source_description["Status"]
    print(" Creating data source. Status: "+status)
```

```
        time.sleep(60)
        if status != "CREATING":
            break

    print("Synchronize the data source.")

    sync_response = kendra.start_data_source_sync_job(
        Id = data_source_id,
        IndexId = index_id
    )

    pprint.pprint(sync_response)

    print("Wait for the data source to sync with the index.")

    while True:

        jobs = kendra.list_data_source_sync_jobs(
            Id = data_source_id,
            IndexId = index_id
        )

        # For this example, there should be one job
        status = jobs["History"][0]["Status"]

        print(" Syncing data source. Status: "+status)
        if status != "SYNCING":
            break
        time.sleep(60)

    except ClientError as e:
        print("%s" % e)

    print("Program ends.")
```

開始使用 (AWS SDK for Java)

下面的程序是在 Java 程序 Amazon Kendra 中使用的一個例子。該程序執行以下操作：

1. 使用 [CreateIndex](#) 操作創建一個新的索引。
2. 等待索引建立完成。它使用 [DescribeIndex](#) 操作來監視索引的狀態。
3. 索引處於作用中狀態之後，它會使用 [CreateDataSource](#) 作業建立資料來源。

4. 等待資料來源建立完成。它使用[DescribeDataSource](#)操作來監視數據源的狀態。
5. 當資料來源處於[StartDataSourceSyncJob](#)作用中狀態時，它會使用作業將索引與資料來源的內容同步化。

```
package com.amazonaws.kendra;

import java.util.concurrent.TimeUnit;
import software.amazon.awssdk.services.kendra.KendraClient;
import software.amazon.awssdk.services.kendra.model.CreateDataSourceRequest;
import software.amazon.awssdk.services.kendra.model.CreateDataSourceResponse;
import software.amazon.awssdk.services.kendra.model.CreateIndexRequest;
import software.amazon.awssdk.services.kendra.model.CreateIndexResponse;
import software.amazon.awssdk.services.kendra.model.DataSourceConfiguration;
import software.amazon.awssdk.services.kendra.model.DataSourceStatus;
import software.amazon.awssdk.services.kendra.model.DataSourceSyncJob;
import software.amazon.awssdk.services.kendra.model.DataSourceSyncJobStatus;
import software.amazon.awssdk.services.kendra.model.DataSourceType;
import software.amazon.awssdk.services.kendra.model.DescribeDataSourceRequest;
import software.amazon.awssdk.services.kendra.model.DescribeDataSourceResponse;
import software.amazon.awssdk.services.kendra.model.DescribeIndexRequest;
import software.amazon.awssdk.services.kendra.model.DescribeIndexResponse;
import software.amazon.awssdk.services.kendra.model.IndexStatus;
import software.amazon.awssdk.services.kendra.model.ListDataSourceSyncJobsRequest;
import software.amazon.awssdk.services.kendra.model.ListDataSourceSyncJobsResponse;
import software.amazon.awssdk.services.kendra.model.S3DataSourceConfiguration;
import software.amazon.awssdk.services.kendra.model.StartDataSourceSyncJobRequest;
import software.amazon.awssdk.services.kendra.model.StartDataSourceSyncJobResponse;

public class CreateIndexAndDataSourceExample {

    public static void main(String[] args) throws InterruptedException {
        System.out.println("Create an index");

        String indexDescription = "Getting started index for Kendra";
        String indexName = "java-getting-started-index";
        String indexRoleArn = "arn:aws:iam::<your AWS account ID>:role/<name of an IAM role>";

        System.out.println(String.format("Creating an index named %s", indexName));
        KendraClient kendra = KendraClient.builder().build();
```

```
        CreateIndexRequest createIndexRequest = CreateIndexRequest
            .builder()
            .description(indexDescription)
            .name(indexName)
            .roleArn(indexRoleArn)
            .build();
        CreateIndexResponse createIndexResponse =
kendra.createIndex(createIndexRequest);
        System.out.println(String.format("Index response %s", createIndexResponse));

        String indexId = createIndexResponse.id();

        System.out.println(String.format("Waiting until the index with index ID %s is
created", indexId));
        while (true) {
            DescribeIndexRequest describeIndexRequest =
DescribeIndexRequest.builder().id(indexId).build();
            DescribeIndexResponse describeIndexResponse =
kendra.describeIndex(describeIndexRequest);
            IndexStatus status = describeIndexResponse.status();
            if (status != IndexStatus.CREATING) {
                break;
            }

            TimeUnit.SECONDS.sleep(60);
        }

        System.out.println("Creating an S3 data source");
        String dataSourceName = "java-getting-started-data-source";
        String dataSourceDescription = "Getting started data source";
        String s3BucketName = "an-aws-kendra-test-bucket";
        String dataSourceRoleArn = "arn:aws:iam::<your AWS account ID>:role/<name of an
IAM role>";

        CreateDataSourceRequest createDataSourceRequest = CreateDataSourceRequest
            .builder()
            .indexId(indexId)
            .name(dataSourceName)
            .description(dataSourceDescription)
            .roleArn(dataSourceRoleArn)
            .type(DataSourceType.S3)
            .configuration(
                DataSourceConfiguration
                    .builder()
```



```
        .s3Configuration(
            S3DataSourceConfiguration
                .builder()
                .bucketName(s3BucketName)
                .build()
        ).build()
    ).build();

    CreateDataSourceResponse createDataSourceResponse =
kendra.createDataSource(createDataSourceRequest);
    System.out.println(String.format("Response of creating data source: %s",
createDataSourceResponse));

    String dataSourceId = createDataSourceResponse.id();
    System.out.println(String.format("Waiting for Kendra to create the data source
%s", dataSourceId));
    DescribeDataSourceRequest describeDataSourceRequest = DescribeDataSourceRequest
        .builder()
        .indexId(indexId)
        .id(dataSourceId)
        .build();

    while (true) {
        DescribeDataSourceResponse describeDataSourceResponse =
kendra.describeDataSource(describeDataSourceRequest);

        DataSourceStatus status = describeDataSourceResponse.status();
        System.out.println(String.format("Creating data source. Status: %s",
status));
        if (status != DataSourceStatus.CREATING) {
            break;
        }

        TimeUnit.SECONDS.sleep(60);
    }

    System.out.println(String.format("Synchronize the data source %s",
dataSourceId));
    StartDataSourceSyncJobRequest startDataSourceSyncJobRequest =
StartDataSourceSyncJobRequest
        .builder()
        .indexId(indexId)
        .id(dataSourceId)
        .build();
```

```
        StartDataSourceSyncJobResponse startDataSourceSyncJobResponse =
kendra.startDataSourceSyncJob(startDataSourceSyncJobRequest);
        System.out.println(String.format("Waiting for the data
source to sync with the index %s for execution ID %s", indexId,
startDataSourceSyncJobResponse.executionId()));

        // For this particular list, there should be just one job
        ListDataSourceSyncJobsRequest listDataSourceSyncJobsRequest =
ListDataSourceSyncJobsRequest
            .builder()
            .indexId(indexId)
            .id(dataSourceId)
            .build();

        while (true) {
            ListDataSourceSyncJobsResponse listDataSourceSyncJobsResponse =
kendra.listDataSourceSyncJobs(listDataSourceSyncJobsRequest);
            DataSourceSyncJob job = listDataSourceSyncJobsResponse.history().get(0);
            System.out.println(String.format("Syncing data source. Status: %s",
job.status()));

            if (job.status() != DataSourceSyncJobStatus.SYNCING) {
                break;
            }

            TimeUnit.SECONDS.sleep(60);
        }

        System.out.println("Index setup is complete");
    }
}
```

開始使用 Amazon S3 資料來源 (主控台)

您可以使用 Amazon Kendra 主控台開始使用 Amazon S3 值區做為資料存放區。當您使用主控台時，您需要指定所有連線資訊，以索引值區的內容。如需詳細資訊，請參閱 [Amazon S3](#)。

使用下列程序，使用預設組態建立基本的 S3 儲存貯體資料來源。此程序假設您已按照的步驟 1 中的步驟建立索引 [開始使用主 Amazon Kendra 控制台](#)。

使用Amazon Kendra主控台建立 S3 儲存貯體資料來源

1. 請登入AWS Management Console並開啟Amazon Kendra主控台，網址為 <https://console.aws.amazon.com/kendra/home>。
2. 從索引清單中，選擇要新增資料來源的索引。
3. 選擇 [新增資料來源]。
4. 從資料來源連接器清單中選擇Amazon S3。
5. 在 [定義屬性] 頁面上，為您的資料來源指定名稱並選擇性地提供描述。將「標籤」欄位保留空白。選擇 Next (下一步) 繼續。
6. 在輸入資料來源位置欄位中，輸入包含文件的 S3 儲存貯體的名稱。您可以直接輸入名稱，也可以選擇「瀏覽」來瀏覽名稱。值區必須與索引位於相同的區域。
7. 在IAM角色中選擇創建一個新的角色，然後鍵入一個角色名稱。有關詳情，請參閱[Amazon S3資料來源的IAM角色](#)。
8. 在「設定同步執行排程」區段中，選擇「視需求執行」。
9. 選擇 Next (下一步) 繼續。
10. 在「檢閱和建立」頁面上，檢閱 S3 資料來源的詳細資訊。如果您想進行變更，請選擇要變更的物件旁邊的「編輯」按鈕。如果您滿意您的選擇，請選擇建立以建立 S3 資料來源。

選擇 [建立] 之後，Amazon Kendra開始建立資料來源。建立資料來源可能需要幾分鐘的時間。完成後，資料來源的狀態會從 [建立] 變更為 [作用中]。

建立資料來源之後，您需要將Amazon Kendra索引與資料來源同步。選擇立即同步以開始同步過程。同步處理資料來源可能需要幾分鐘到數小時，具體取決於文件的數量和大小。

開始使用 MySQL 資料庫資料來源 (主控台)

您可以使用Amazon Kendra控制台開始使用 MySQL 數據庫作為數據源。當您使用控制台時，指定您需要索引 MySQL 數據庫的內容的連接信息。如需詳細資訊，請參閱[使用資料庫資料來源](#)。

你首先需要創建一個 MySQL 數據庫，然後你可以為數據庫創建一個數據源。

使用下列程序來建立基本的 MySQL 資料庫。此程序假設您已經在之後的步驟 1 建立索引[開始使用主 Amazon Kendra 控制台](#)。

若要建立 MySQL 資料庫

1. 登入 AWS Management Console，並開啟 Amazon RDS 主控台，網址為 <https://console.aws.amazon.com/rds/>。
2. 在瀏覽窗格中，選擇子網路群組，然後選擇建立資料庫子網路群組。
3. 為群組命名，然後選擇您的虛擬私有雲 (VPC)。如需有關設定 VPC 的詳細資訊，請參閱[設定 Amazon Kendra 為使用 VPC](#)。
4. 新增 VPC 的私有子網路。您的私人子網路是未連線到 NAT 的子網路。選擇 建立。
5. 在瀏覽窗格中，選擇 [資料庫]，然後選擇 [建立資料庫]。
6. 使用下列參數來建立資料庫。將所有其他參數保留為預設值。
 - 引擎選項
 - 範本 — 免費方案
 - 身份證明設定 — 輸入並確認密碼
 - 在 [連線] 下，選擇 [其他連線組態] 做出下列選擇。
 - 子網路群組 — 選擇您在步驟 4 中建立的子網路群組。
 - VPC 安全群組 — 選擇包含您在 VPC 中建立的輸入和輸出規則的群組。例如：**DataSourceSecurityGroup**。如需有關設定 VPC 的詳細資訊，請參閱[設定 Amazon Kendra 為使用 VPC](#)。
 - 在其他組態下，將初始資料庫名稱設定為 **content**。
7. 選擇 Create database (建立資料庫)。
8. 從資料庫清單中，選擇您的新資料庫。記下資料庫端點。
9. 建立資料庫之後，您必須建立一個表格來保存您的文件。建立資料表不在這些指示的範圍之外。建立表格時，請注意下列事項：
 - 資料庫名稱 — **content**
 - 表格名稱 — **documents**
 - 列-**IDTitle**，**Body**，和**LastUpdate**。如果需要，您可以包括其他列。

現在您已經建立了 MySQL 資料庫，您可以為資料庫建立資料來源。

若要建立 MySQL 資料來源

1. 請登入 AWS Management Console 並開啟 Amazon Kendra 主控台，網址為 <https://console.aws.amazon.com/kendra/home>。

2. 在導覽窗格中，選擇 [索引]，然後選擇您的索引。
3. 選擇新增資料來源，然後選擇亞馬遜 RDS。
4. 輸入資料來源的名稱和說明，然後選擇 [下一步]。
5. 選擇 MySQL。
6. 在「連線存取」下，輸入下列資訊：
 - 端點-您先前建立的資料庫的端點。
 - 連接埠-資料庫的連接埠號碼。對於 MySQL，默認值是 3306。
 - 驗證類型 — 選擇 [新增]。
 - 新密碼容器名稱 — 資料庫認證之 Secrets Manager 容器的名稱。
 - 使用者名稱-具有資料庫管理存取權的使用者名稱。
 - 密碼 — 使用者的密碼，然後選擇 [儲存驗證]。
 - 資料庫名稱 — **content**。
 - 表格名稱 — **documents**。
 - IAM 角色 — 選擇 [建立新角色]，然後輸入角色的名稱。
7. 在欄組態中輸入以下內容：
 - 文件 ID 欄名稱 — **ID**
 - 文件標題欄名稱 — **Title**
 - 文件資料欄名稱 — **Body**
8. 在欄變更偵測中輸入下列內容：
 - 更改檢測列-**LastUpdate**
9. 在配置 VPC 和安全組中提供以下內容：
 - 在虛擬私有雲 (VPC) 中，選擇您的 VPC。
 - 在子網路中，選擇您在 VPC 中建立的私人子網路。
 - 在 VPC 安全群組中，選擇包含您在 VPC 適用於 MySQL 資料庫中建立的輸入和輸出規則的安全群組。例如：**DataSourceSecurityGroup**。
10. 在設定同步執行排程中，選擇視需求執行，然後選擇下一步。
11. 在 [資料來源欄位對應] 中，選擇 [下一步]
12. 檢閱資料來源的組態，以確保資料來源正確無誤。如果您滿意所有項目都正確無誤，請選擇 [建立]。

開始使用 AWS IAM Identity Center 身分識別來源 (主控台)

AWS IAM Identity Center 身分識別來源包含有關您的使用者和群組的資訊。這對於設定使用者前後關聯篩選非常有用，其 Amazon Kendra 中會根據使用者或其群組對文件的存取權限來篩選不同使用者的搜尋結果。

若要建立 IAM 身分中心身分識別來源，您必須啟用 IAM 身分中心並在中建立組織 AWS Organizations。當您首次啟用 IAM 身分中心並建立組織時，它會自動預設為身分識別中心目錄做為身分識別來源。您可以變更為使用中目錄 (Amazon 受管或自我管理) 或外部身分識別供應商做為您的身分來源。您必須遵循正確的指引 — 請參閱[變更您的 IAM 身分中心身分來源](#)。每個組織只能有一個身分識別來源。

為了讓您的使用者和群組被指派不同層級的文件存取權限，您需要在將文件內嵌至索引時，將使用者和群組包含在存取控制清單中。這可讓您的使用者和群組根據其存取層級來搜尋文件。Amazon Kendra 當您發出查詢時，使用者 ID 必須與 IAM 身分中心中的使用者名稱完全相符。

您還必須授予所需的許可，才能將 IAM 身分中心與 Amazon Kendra。如需詳細資訊，請參閱[IAM IAM 身分中心](#)的角色。

設定 IAM 身分中心身分識別來源

1. 開啟 [IAM 身分中心主控台](#)。
2. 選擇 [啟用 IAM 身分中心]，然後選擇 [建立 AWS 組織]。

依預設會建立 Identity Center 目錄，並傳送電子郵件給您以驗證與組織相關聯的電子郵件地址。

3. 若要將群組新增至您的 AWS 組織，請在功能窗格中選擇 [群組]。
4. 在「群組」頁面上，選擇「建立群組」，然後在對話方塊中輸入群組名稱和說明。選擇建立。
5. 若要將使用者新增至 [Organizations]，請在導覽窗格中選擇 [使用者]。
6. 在 Users (使用者) 頁面上，選擇 Add user (新增使用者)。在 User details (使用者詳細資訊) 下，指定所有必要欄位。在 Password (密碼) 中，選擇 Send an email to the user (傳送電子郵件給使用者)。選擇下一步。
7. 若要將使用者新增至群組，請選擇群組，然後選取群組。
8. 在 [詳細資料] 頁面的 [群組成員] 下，選擇 [新增使用者]
9. 在 [新增使用者至群組] 頁面上，選取要新增為群組成員的使用者。您可以選取多個使用者以新增至群組。
10. 若要將使用者和群組清單與 IAM 身分中心同步，請將您的身分識別來源變更為 Active Directory 或外部身分識別提供者。

Identity Center 目錄是預設的身分識別來源，如果您沒有由提供者管理自己的清單，則需要使用此來源手動新增使用者和群組。若要變更身分識別來源，您必須遵循正確的指引 — 請參閱[變更 IAM 身分中心身分識別來源](#)。

Note

如果使用 Active Directory 或外部身分識別提供者做為身分識別來源，當您指定跨網域身分識別管理 (SCIM) 通訊協定的系統時，必須將使用者的電子郵件地址對應至 IAM 身分中心使用者名稱。如需詳細資訊，請參閱[SCIM 上啟用 IAM 身分中心的 IAM 身分中心指南](#)。

設定 IAM 身分中心身分識別來源後，您可以在建立或編輯索引時在主控制台啟用此身分識別來源。前往索引設定中的使用者存取控制，然後編輯設定，以允許從 IAM 身分中心擷取使用者群組資訊。

您也可以使用[UserGroupResolutionConfiguration](#)物件啟用 IAM 身分中心。

您可以提供 `UserGroupResolutionMode as AWS_SSO` 並建立授與呼

叫 `sso:ListDirectoryAssociations`、`sso-directory:SearchUsers`、權限的 IAM 角色 `sso-directory:ListGroupsForUser` 和 `sso-directory:DescribeGroups`。

Warning

Amazon Kendra 目前不支援 `UserGroupResolutionConfiguration` 與組 AWS 織成員帳戶搭配 IAM 身分中心身分識別來源使用。您必須在組織的管理帳戶中建立索引才能使用 `UserGroupResolutionConfiguration`。

以下概述如何使用 `UserGroupResolutionConfiguration` 和使用者存取控制來設定資料來源，以篩選使用者前後關聯的搜尋結果。這假設您已經建立索引和索引的 IAM 角色。您可以建立索引，並使用 [CreateIndex](#) API 提供 IAM 角色。

使用 `UserGroupResolutionConfiguration` 和使用者內容篩選設定資料來源

1. 建立可授與存取 IAM 身分中心身分識別來源權限的 [IAM 角色](#)。
2. [UserGroupResolutionConfiguration](#) 透過將模式設定為 `AWS_SSO` 並撥打電話更新索引 `UpdateIndex` 以使用 IAM 身分中心進行設定。
3. 如果您想要使用以權杖為基礎的使用者存取控制來篩選使用者前後關聯的搜尋結果，請在呼叫 `USER_TOKEN` 時設定 [UserContextPolicy](#) 為 `UpdateIndex` 否則，請針對大多數資料來源連接

器 Amazon Kendra 編目每個文件的存取控制清單。您也可以在中提供使用者和群組資訊，根據 [Query](#) API 中的使用者內容篩選搜尋結果 `UserContext`。您也可以使用將使用者對應至其群組，以 [PutPrincipalMapping](#) 便在發出查詢時只需提供使用者 ID。

4. 建立授與存取資料來源權限的 [IAM 角色](#)。
5. [設定](#) 您的資料來源。您必須提供必要的連線資訊才能連線到資料來源。
6. 使用 [CreateDataSource](#) API 建立資料來源。提供 `DataSourceConfiguration` 物件，其中包括 `TemplateConfiguration` 索引的 ID、資料來源的 IAM 角色、資料來源類型，並為資料來源命名。您也可以更新資料來源。

變更您的 IAM 身分中心身分來源

Warning

在 IAM 身分中心設定中變更身分來源可能會影響使用者和群組資訊的保留。若要安全地執行此操作，建議您檢閱 [變更身分識別來源的考量事項](#)。當您變更身分識別來源時，會產生新的身分識別來源 ID。AWS_SSO 在將模式設定為「中」之前，請檢查您是否使用正確的 ID [UserGroupResolutionConfiguration](#)。

變更您的 IAM 身分中心身分來源

1. 開啟 [IAM 身分中心 > 主控台](#)。
2. 選擇設定。
3. 在 [設定] 頁面的 [身分識別來源] 下，選擇 [變更]。
4. 在 [變更身分識別來源] 頁面上，選取偏好的身分識別來源，然後選擇 [下一步]。

建立索引

您可以使用主控台或呼叫 [CreateIndex](#) API 來建立索引。您可以將 AWS Command Line Interface (AWS CLI) 或 SDK 與 API 搭配使用。建立索引之後，您可以直接將文件新增至索引或從資料來源新增文件。

若要建立索引，您必須提供 () 角色的 Amazon 資源名稱 AWS Identity and Access Management (ARNIAM) 才能存取 CloudWatch 索引。如需詳細資訊，請參閱 [索引的IAM 角色](#)。

下列索引標籤提供使用 AWS Management Console、和 Python 和 Java SDK 的程式碼範例來 AWS CLI 建立索引的程序。

Console

若要建立索引

1. 登入 AWS 管理主控台，然後開啟 Amazon Kendra 主控台，網址為 <https://console.aws.amazon.com/kendra/>。
2. 選取 [索引] 區段中的 [建立索引]。
3. 在 [指定索引詳細資料] 中，為您的索引指定名稱和說明。
4. 在 IAM 角色中提供一個 IAM 角色。若要尋找角色，請從帳戶中包含「kendra」一詞的角色中選擇，或輸入其他角色的名稱。如需角色所需權限的詳細資訊，請參閱 [索引的IAM 角色](#)。
5. 選擇下一步。
6. 在 [設定使用者存取控制] 頁面上選擇 [下一步]。建立索引之後，您可以更新索引以使用 Token 進行存取控制。如需詳細資訊，請參閱 [控制文件的存取](#)。
7. 在啟動設定詳細資訊頁面上，選擇建立。
8. 建立索引可能需要一些時間。檢查索引清單以觀察建立索引的進度。當索引的狀態為時 ACTIVE，您的索引就可以使用了。

AWS CLI

若要建立索引

1. 使用下面的命令來創建一個索引。role-arn 必須是可以執行 Amazon Kendra 動作之 IAM 角色的 Amazon 資源名稱 (ARN)。如需詳細資訊，請參閱 [IAM 角色](#)。

此指令已針對 Linux 和 macOS 進行格式化。如果您使用的是 Windows，請使用插入符號 (^) 取代 Unix 行接續字元 (\)。

```
aws kendra create-index \  
  --name index name \  
  --description "index description" \  
  --role-arn arn:aws:iam::account ID:role/role name
```

2. 建立索引可能需要一些時間。若要檢查索引的狀態，請使用下列命令傳回 create-index 的索引 ID。當索引的狀態為時 ACTIVE，您的索引就可以使用了。

```
aws kendra describe-index \  
  --index-id index ID
```

Python

若要建立索引

- 在下列程式碼範例中提供下列變數的值：
 - `description` 您正在建立之索引的說明。這是選用的。
 - `index_name` 您正在建立的索引名稱。
 - `role_arn` 可以執行 Amazon Kendra API 的角色的 Amazon 資源名稱 (ARN)。如需詳細資訊，請參閱 [IAM 角色](#)。

```
import boto3  
from botocore.exceptions import ClientError  
import pprint  
import time  
  
kendra = boto3.client("kendra")  
  
print("Create an index.")  
  
# Provide a name for the index  
index_name = "index-name"  
# Provide an optional description for the index  
description = "index description"
```

```
# Provide the IAM role ARN required for indexes
role_arn = "arn:aws:iam::${account id}:role/${role name}"

try:
    index_response = kendra.create_index(
        Name = index_name,
        Description = description,
        RoleArn = role_arn
    )

    pprint.pprint(index_response)

    index_id = index_response["Id"]

    print("Wait for Amazon Kendra to create the index.")

    while True:
        # Get the details of the index, such as the status
        index_description = kendra.describe_index(
            Id = index_id
        )
        # If status is not CREATING, then quit
        status = index_description["Status"]
        print(" Creating index. Status: "+status)
        if status != "CREATING":
            break
        time.sleep(60)

except ClientError as e:
    print("%s" % e)

print("Program ends.")
```

Java

若要建立索引

- 在下列程式碼範例中提供下列變數的值：
 - `description`您正在建立之索引的說明。這是選用的。
 - `index_name`您正在建立的索引名稱。

- `role_arn` 可以執行 Amazon Kendra API 的角色的 Amazon 資源名稱 (ARN)。如需詳細資訊，請參閱 [IAM 角色](#)。

```
package com.amazonaws.kendra;

import java.util.concurrent.TimeUnit;
import software.amazon.awssdk.services.kendra.KendraClient;
import software.amazon.awssdk.services.kendra.model.CreateIndexRequest;
import software.amazon.awssdk.services.kendra.model.CreateIndexResponse;
import software.amazon.awssdk.services.kendra.model.DescribeIndexRequest;
import software.amazon.awssdk.services.kendra.model.DescribeIndexResponse;
import software.amazon.awssdk.services.kendra.model.IndexStatus;

public class CreateIndexExample {

    public static void main(String[] args) throws InterruptedException {

        String indexDescription = "Getting started index for Kendra";
        String indexName = "java-getting-started-index";
        String indexRoleArn = "arn:aws:iam::<your AWS account ID>:role/KendraRoleForGettingStartedIndex";

        System.out.println(String.format("Creating an index named %s",
indexName));
        CreateIndexRequest createIndexRequest = CreateIndexRequest
            .builder()
            .description(indexDescription)
            .name(indexName)
            .roleArn(indexRoleArn)
            .build();
        KendraClient kendra = KendraClient.builder().build();
        CreateIndexResponse createIndexResponse =
kendra.createIndex(createIndexRequest);
        System.out.println(String.format("Index response %s",
createIndexResponse));

        String indexId = createIndexResponse.id();

        System.out.println(String.format("Waiting until the index with ID %s is
created.", indexId));
        while (true) {
```

```
        DescribeIndexRequest describeIndexRequest =
DescribeIndexRequest.builder().id(indexId).build();
        DescribeIndexResponse describeIndexResponse =
kendra.describeIndex(describeIndexRequest);
        IndexStatus status = describeIndexResponse.status();
        if (status != IndexStatus.CREATING) {
            break;
        }

        TimeUnit.SECONDS.sleep(60);
    }

    System.out.println("Index creation is complete.");
}
}
```

建立索引之後，您可以在索引中加入文件。您可以直接新增它們，也可以建立可定期更新索引的資料來源。

主題

- [使用批次上傳將文件直接新增至索引](#)
- [將常見問題 \(FAQ \) 添加到索引](#)
- [建立自訂文件欄位](#)
- [使用權杖控制使用者對文件的存取](#)

使用批次上傳將文件直接新增至索引

您可以使用 [BatchPutDocument](#) API 將文件直接新增至索引。您無法直接使用主控台新增文件。如果使用控制台，則連接到資料來源以將文件新增至索引。您可以從 S3 儲存貯體新增文件，或以二進位資料形式提供。如需支援的文件類型清單，Amazon Kendra 請參閱[文件類型](#)。

使用將文件新增至索引BatchPutDocument是非同步作業。呼叫 BatchPutDocument API 之後，您可以使用 [BatchGetDocumentStatus](#) API 監視文件索引的進度。當您使用文件 ID 清單呼叫 BatchGetDocumentStatus API 時，它會傳回文件的狀態。當文件的狀態為INDEXED或時FAILED，文件的處理已完成。當狀態為時FAILED，BatchGetDocumentStatusAPI 會傳回文件無法編製索引的原因。

如果您想要在文件擷取程序期間變更內容和文件中繼資料欄位或屬性，請參閱[Amazon Kendra 自訂文件擴充](#)功能。如果您想要使用自訂資料來源，則使用 BatchPutDocument API 提交的每份文件都需要資料來源 ID 和執行 ID 作為屬性或欄位。有關詳情，請參閱[自訂資料來源的必要屬性](#)。

Note

每個文件 ID 必須是每個索引唯一的。您無法建立資料來源以使用其唯一 ID 為文件建立索引，然後使用 BatchPutDocument API 來索引相同的文件，反之亦然。您可以刪除資料來源，然後使用 BatchPutDocument API 索引相同的文件，反之亦然。針對同一組文件使用 BatchPutDocument 和 BatchDeleteDocument API 搭配 Amazon Kendra 資料來源連接器，可能會導致資料不一致。相反地，我們建議使用[Amazon Kendra 自訂資料來源連接器](#)。

下列開發人員指南文件說明如何將文件直接新增至索引。

主題

- [使用 BatchPutDocument API 新增文件](#)
- [從 S3 儲存貯體新增文件](#)

使用 BatchPutDocument API 新增文件

下列範例會透過呼叫，將一組文字加入索引[BatchPutDocument](#)。您可以使用 BatchPutDocument API 將文件直接新增至索引。如需支援的文件類型清單，Amazon Kendra 請參閱[文件類型](#)。

如需使用 AWS CLI 和 SDK 建立索引的範例，請參閱[建立索引](#)。若要設定 CLI 和 SDK，請參閱[設定 Amazon Kendra](#)。

Note

新增至索引的檔案必須位於 UTF-8 編碼位元組串流中。

在下列範例中，UTF-8 編碼的文字會新增至索引。

CLI

在中 AWS Command Line Interface，使用下列命令。此指令已針對 Linux 和 macOS 進行格式化。如果您使用的是 Windows，請使用插入符號 (^) 取代 Unix 行接續字元 (\)。

```
aws kendra batch-put-document \  
  --index-id index-id \  
  --documents '{"Id":"doc-id-1", "Blob":"Amazon.com is an online retailer.",  
  "ContentType":"PLAIN_TEXT", "Title":"Information about Amazon.com"}'
```

Python

```
import boto3  
  
kendra = boto3.client("kendra")  
  
# Provide the index ID  
index_id = "index-id"  
  
# Provide the title and text  
title = "Information about Amazon.com"  
text = "Amazon.com is an online retailer."  
  
document = {  
    "Id": "1",  
    "Blob": text,  
    "ContentType": "PLAIN_TEXT",  
    "Title": title  
}  
  
documents = [  
    document  
]  
  
result = kendra.batch_put_document(  
    IndexId = index_id,  
    Documents = documents  
)  
  
print(result)
```

Java

```
package com.amazonaws.kendra;  
  
import software.amazon.awssdk.core.SdkBytes;  
import software.amazon.awssdk.services.kendra.KendraClient;
```

```
import software.amazon.awssdk.services.kendra.model.BatchPutDocumentRequest;
import software.amazon.awssdk.services.kendra.model.BatchPutDocumentResponse;
import software.amazon.awssdk.services.kendra.model.ContentType;
import software.amazon.awssdk.services.kendra.model.Document;

public class AddDocumentsViaAPIExample {
    public static void main(String[] args) {
        KendraClient kendra = KendraClient.builder().build();

        String indexId = "yourIndexId";

        Document testDoc = Document
            .builder()
            .title("The title of your document")
            .id("a_doc_id")
            .blob(SdkBytes.fromUtf8String("your text content"))
            .contentType(ContentType.PLAIN_TEXT)
            .build();

        BatchPutDocumentRequest batchPutDocumentRequest = BatchPutDocumentRequest
            .builder()
            .indexId(indexId)
            .documents(testDoc)
            .build();

        BatchPutDocumentResponse result =
            kendra.batchPutDocument(batchPutDocumentRequest);

        System.out.println(String.format("BatchPutDocument Result: %s", result));
    }
}
```

從 S3 儲存貯體新增文件

您可以使用 [BatchPutDocument](#) API 將文件直接從 Amazon S3 值區新增至索引。您最多可以在同一通話中添加 10 個文檔。使用 S3 儲存貯體時，必須提供具有存取包含文件儲存貯體之存取權限的 IAM 角色。您可以在 `RoleArn` 參數中指定角色。

使用 [BatchPutDocument](#) API 從 Amazon S3 值區新增文件是一次性作業。若要使索引與值區的內容保持同步，請建立 Amazon S3 資料來源。有關詳情，請參閱 [Amazon S3 資料來源](#)。

如需使用 AWS CLI 和 SDK 建立索引的範例，請參閱[建立索引](#)。若要設定 CLI 和 SDK，請參閱[設定 Amazon Kendra](#)。如需建立 S3 儲存貯體的相關資訊，請參閱[Amazon Simple Storage Service 文件](#)。

在下面的例子中，兩個 Microsoft Word 文檔被添加到使用 BatchPutDocument API 的索引。

Python

```
import boto3

kendra = boto3.client("kendra")

# Provide the index ID
index_id = "index-id"
# Provide the IAM role ARN required to index documents in an S3 bucket
role_arn = "arn:aws:iam::${accountID}:policy/${roleName}"

doc1_s3_file_data = {
    "Bucket": "bucket-name",
    "Key": "document1.docx"
}

doc1_document = {
    "S3Path": doc1_s3_file_data,
    "Title": "Document 1 title",
    "Id": "doc_1"
}

doc2_s3_file_data = {
    "Bucket": "bucket-name",
    "Key": "document2.docx"
}

doc2_document = {
    "S3Path": doc2_s3_file_data,
    "Title": "Document 2 title",
    "Id": "doc_2"
}

documents = [
    doc1_document,
    doc2_document
]

result = kendra.batch_put_document(
```

```
    Documents = documents,  
    IndexId = index_id,  
    RoleArn = role_arn  
)  
  
print(result)
```

Java

```
package com.amazonaws.kendra;  
  
import software.amazon.awssdk.services.kendra.KendraClient;  
import software.amazon.awssdk.services.kendra.model.BatchPutDocumentRequest;  
import software.amazon.awssdk.services.kendra.model.BatchPutDocumentResponse;  
import software.amazon.awssdk.services.kendra.model.Document;  
import software.amazon.awssdk.services.kendra.model.S3Path;  
  
public class AddFilesFromS3Example {  
    public static void main(String[] args) {  
        KendraClient kendra = KendraClient.builder().build();  
  
        String indexId = "yourIndexId";  
        String roleArn = "yourIndexRoleArn";  
  
        Document pollyDoc = Document  
            .builder()  
            .s3Path(  
                S3Path.builder()  
                    .bucket("an-aws-kendra-test-bucket")  
                    .key("What is Amazon Polly.docx")  
                    .build()  
            ).title("What is Amazon Polly")  
            .id("polly_doc_1")  
            .build();  
  
        Document rekognitionDoc = Document  
            .builder()  
            .s3Path(  
                S3Path.builder()  
                    .bucket("an-aws-kendra-test-bucket")  
                    .key("What is Amazon Rekognition.docx")  
                    .build()  
            ).title("What is Amazon rekognition")
```

```
        .id("rekognition_doc_1")
        .build();

    BatchPutDocumentRequest batchPutDocumentRequest = BatchPutDocumentRequest
        .builder()
        .indexId(indexId)
        .roleArn(roleArn)
        .documents(pollyDoc, rekognitionDoc)
        .build();

    BatchPutDocumentResponse result =
    kendra.batchPutDocument(batchPutDocumentRequest);

    System.out.println(String.format("BatchPutDocument result: %s", result));
}
}
```

將常見問題 (FAQ) 添加到索引

您可以使用主控台或 [CreateFaq](#) API 將常見問題 (FAQ) 直接新增至索引。將常見問題集新增至索引是非同步作業。您可以將常見問題集的資料放在儲存 Amazon Simple Storage Service 貯體中的檔案中。您可以使用 CSV 或 JSON 文件作為常見問題解答的輸入：

- 基本 CSV — CSV 檔案，其中每一列包含一個問題、答案和一個選用的來源 URI。
- 自訂 CSV — 包含自訂欄位/屬性的問題、答案和標題的 CSV 檔案，您可以使用此檔案進行複製、顯示或排序常見問題集回覆。您也可以定義存取控制欄位，將常見問題集回應限制給某些使用者和群組，這些使用者和群組可以看到常見問題集回應。
- JSON — 包含問題、答案和自訂欄位/屬性的 JSON 檔案，您可以用來刻面、顯示或排序常見問題集回應。您也可以定義存取控制欄位，將常見問題集回應限制給某些使用者和群組，這些使用者和群組可以看到常見問題集回應。

例如，以下是一個基本的 CSV 文件，該文件提供有關美國華盛頓州斯波坎免費診所和美國密蘇里州山景城的問題的答案。

```
How many free clinics are in Spokane WA?, 13
How many free clinics are there in Mountain View Missouri?, 7
```

Note

常見問題集檔案必須是 UTF-8 編碼的檔案。

主題

- [建立常見問題集檔案的索引欄位](#)
- [基本 CSV 檔案](#)
- [自訂 CSV 檔案](#)
- [JSON 檔案](#)
- [使用常見問題解答檔](#)
- [英語以外的語言常見問題解答文件](#)

建立常見問題集檔案的索引欄位

當您使用 [自訂 CSV](#) 或 [JSON](#) 檔案進行輸入時，您可以為常見問題集問題宣告自訂欄位。例如，您可以建立一個自訂欄位，將每個常見問題集問題指派給業務部門。在回應中傳回常見問題集時，您可以使用部門做為方面，將搜尋範圍縮小為僅限「HR」或「財務」。

自訂欄位必須對應至索引欄位。在主控台中，您可以使用 Facet 定義頁面來建立索引欄位。使用 API 時，您必須先使用 [UpdateIndex](#) API 建立索引欄位。

FAQ 檔案中的欄位/屬性類型必須與關聯索引欄位的類型相符。例如，「部門」字段是一個 `STRING_LIST` 類型字段。因此，您必須在 FAQ 檔案中以字串清單形式提供部門欄位的值。您可以使用主控台內的 Facet 定義頁面或使用 [DescribeIndex](#) API 來檢查索引欄位的類型。

當您建立對應至自訂屬性的索引欄位時，您可以將其標示為可顯示、可列印或排序。您無法將自訂屬性設為可搜尋。

除了自訂屬性之外，您還可以在自訂 CSV 或 JSON 檔案中使用 Amazon Kendra 保留或通用欄位。如需詳細資訊，請參閱 [文件屬性或欄位](#)。

基本 CSV 檔案

當您想為常見問題解答使用簡單的結構時，請使用基本的 CSV 文件。在基本 CSV 檔案中，每一列都有兩個或三個欄位：一個問題、一個答案，以及指向包含更多資訊的文件的選用來源 URI。

[對於逗號分隔值 \(CSV\) 檔案，檔案的內容必須遵循 RFC 4180 一般格式和 MIME 類型。](#)

以下是基本 CSV 格式的常見問題集檔案。

```
How many free clinics are in Spokane WA?, 13, https://s3.region.company.com/bucket-name/directory/faq.csv
How many free clinics are there in Mountain View Missouri?, 7, https://s3.region.company.com/bucket-name/directory/faq.csv
```

自訂 CSV 檔案

當您想要在常見問題集中新增自訂欄位/屬性時，請使用自訂 CSV 檔案。對於自訂 CSV 檔案，您可以在 CSV 檔案中使用標題列來定義其他屬性。

CSV 檔案必須包含下列兩個必要欄位：

- `_question`— 常見問題
- `_answer`— 常見問題的答案

您的檔案可以同時包含 Amazon Kendra 保留欄位和自訂欄位。以下是自訂 CSV 檔案的範例。

```
_question,_answer,_last_updated_at,custom_string
How many free clinics are in Spokane WA?, 13, 2012-03-25T12:30:10+01:00, Note: Some free clinics require you to meet certain criteria in order to use their services
How many free clinics are there in Mountain View Missouri?, 7, 2012-03-25T12:30:10+01:00, Note: Some free clinics require you to meet certain criteria in order to use their services
```

[對於逗號分隔值 \(CSV\) 檔案，自訂檔案的內容必須遵循 RFC 4180 一般格式和 MIME 類型。](#)

以下列出了自定義字段的類型：

- 日期 — 以 ISO 8601 編碼的日期和時間值。

例如，2012-03-25T12:30:10 + 01:00 是二零一二年三月二十五日的 ISO 8601 日期時間格式，在歐洲中部時區的下午 12 時 30 分 (加上 10 秒)。

- 長 — 數字，例如。1234
- 字串 — 字串值。如果您的字串包含逗號，請以雙引號 (「) 括住整個值 (例如，"custom attribute, and more")。
- 字串清單-字串值清單。在以逗號分隔的清單中列出以引號 (「) 括住的值 (例如，"item1, item2, item3")。如果清單只包含單一項目，您可以省略引號 (例如item1)。

自訂 CSV 檔案可以包含使用者存取控制欄位。您可以使用這些欄位來限制特定使用者和群組對常見問題集的存取。若要篩選使用者前後關聯，使用者必須在查詢中提供使用者和群組資訊。否則，將返回所有相關常見問題解答。如需詳細資訊，請參閱[使用者內容篩選](#)。

以下列出了常見問題解答的用戶上下文過濾器：

- `_acl_user_allow` 允許清單中的使用者可以在查詢回應中看到常見問題集。常見問題集不會傳回給其他使用者。
- `_acl_user_deny` 拒絕清單中的使用者無法在查詢回應中看到常見問題集。當常見問題集與查詢相關時，會傳回給所有其他使用者。
- `_acl_group_allow` 屬於允許群組成員的使用者可以在查詢回應中看到常見問題集。常見問題集不會傳回給身為其他群組成員的使用者。
- `_acl_group_deny` 屬於拒絕群組成員的使用者無法在查詢回應中看到常見問題集。常見問題集會在與查詢相關時傳回給其他群組。

在以引號括住的逗號分隔清單中，提供允許和拒絕清單的值 (例如，`"user1,user2,user3"`)。您可以將使用者或群組包含在允許清單或拒絕清單中，但不能同時包含個別允許相同使用者但群組遭拒的地方。如果您在兩者中都包含使用者或群組，就會收到錯誤訊息。

以下是包含使用者內容資訊的自訂 CSV 檔案範例。

```
_question, _answer, _acl_user_allow, _acl_user_deny, _acl_group_allow, _acl_group_deny
How many free clinics are in Spokane WA?, 13, "userID6201,userID7552",
"userID1001,userID2020", groupBasicPlusRate, groupPremiumRate
```

JSON 檔案

您可以使用 JSON 檔案來提供索引的問題、答案和欄位。您可以將任何 Amazon Kendra 保留欄位或自訂欄位新增至常見問題集。

以下是 JSON 檔案的結構定義。

```
{
  "SchemaVersion": 1,
  "FaqDocuments": [
    {
      "Question": string,
      "Answer": string,
      "Attributes": {
```

```

        string: object
        additional attributes
    },
    "AccessControlList": [
        {
            "Name": string,
            "Type": enum( "GROUP" | "USER" ),
            "Access": enum( "ALLOW" | "DENY" )
        },
        additional user context
    ]
},
additional FAQ documents
]
}

```

下面的示例 JSON 文件顯示兩個常見問題解答文檔。其中一個文件只有所需的問題和答案。另一個文件也包括其他欄位和使用者前後關聯或存取控制資訊。

```

{
  "SchemaVersion": 1,
  "FaqDocuments": [
    {
      "Question": "How many free clinics are in Spokane WA?",
      "Answer": "13"
    },
    {
      "Question": "How many free clinics are there in Mountain View Missouri?",
      "Answer": "7",
      "Attributes": {
        "_source_uri": "https://s3.region.company.com/bucket-name/directory/faq.csv",
        "_category": "Charitable Clinics"
      }
    },
    "AccessControlList": [
      {
        "Name": "user@amazon.com",
        "Type": "USER",
        "Access": "ALLOW"
      },
      {
        "Name": "Admin",
        "Type": "GROUP",

```

```

    "Access": "ALLOW"
  }
]
}

```

以下列出了自定義字段的類型：

- 日期 — 具有 ISO 8601 編碼日期和時間值的 JSON 字串值。例如，2012-03-25T12:30:10 + 01:00 是二零一二年三月二十五日的 ISO 8601 日期時間格式，在歐洲中部時區的下午 12 時 30 分（加上 10 秒）。
- 長 — JSON 數字值，例如 1234。
- 字串-JSON 字串值 (例如，"custom attribute")。
- 字串清單-字串值的 JSON 陣列 (例如，["item1,item2,item3"])

JSON 檔案可以包含使用者存取控制欄位。您可以使用這些欄位來限制特定使用者和群組對常見問題集的存取。若要篩選使用者前後關聯，使用者必須在查詢中提供使用者和群組資訊。否則，將返回所有相關常見問題解答。如需詳細資訊，請參閱[使用者內容篩選](#)。

您可以將使用者或群組包含在允許清單或拒絕清單中，但不能同時包含個別允許相同使用者但群組遭拒的地方。如果您在兩者中都包含使用者或群組，就會收到錯誤訊息。

以下是將使用者存取控制納入 JSON 常見問題集的範例。

```

"AccessControlList": [
  {
    "Name": "group or user name",
    "Type": "GROUP | USER",
    "Access": "ALLOW | DENY"
  },
  additional user context
]

```

使用常見問題解答檔

將常見問題集輸入檔案存放在 S3 儲存貯體後，您可以使用主控台或 CreateFaq API 將問題和答案放入索引中。如果您想要更新常見問題集，請刪除常見問題集並重新建立。您可以使用 DeleteFaq API 刪除常見問題集。

您必須提供可存取包含來源檔案之 S3 儲存貯體的 IAM 角色。您可以在主控台或RoleArn參數中指定角色。以下是將常見問題集檔案新增至索引的範例。

Python

```
import boto3

kendra = boto3.client("kendra")

# Provide the index ID
index_id = "index-id"
# Provide the IAM role ARN required to index documents in an S3 bucket
role_arn = "arn:aws:iam::${accountId}:role/${roleName}"

# Provide the S3 bucket path information to the FAQ file
faq_path = {
    "Bucket": "bucket-name",
    "Key": "FreeClinicsUSA.csv"
}

response = kendra.create_faq(
    S3Path = faq_path,
    Name = "FreeClinicsUSA",
    IndexId = index_id,
    RoleArn = role_arn
)

print(response)
```

Java

```
package com.amazonaws.kendra;

import software.amazon.awssdk.services.kendra.KendraClient;
import software.amazon.awssdk.services.kendra.model.CreateFaqRequest;
import software.amazon.awssdk.services.kendra.model.CreateFaqResponse;
import software.amazon.awssdk.services.kendra.model.S3Path;

public class AddFaqExample {
    public static void main(String[] args) {
        KendraClient kendra = KendraClient.builder().build();

        String indexId = "yourIndexId";
```

```
String roleArn = "your role for accessing S3 files";

CreateFaqRequest createFaqRequest = CreateFaqRequest
    .builder()
    .indexId(indexId)
    .name("FreeClinicsUSA")
    .roleArn(roleArn)
    .s3Path(
        S3Path
            .builder()
            .bucket("an-aws-kendra-test-bucket")
            .key("FreeClinicsUSA.csv")
            .build()
    )
    .build();

CreateFaqResponse response = kendra.createFaq(createFaqRequest);

System.out.println(String.format("The result of creating FAQ: %s",
response));

    }
}
```

英語以外的語言常見問題解答文件

您可以使用支援的語言編製常見問題集的索引。Amazon Kendra 索引常見問題解答默認情況下，如果你沒有指定語言。您可以在呼叫 [CreateFaq](#) 作業時指定語言代碼，或在常見問題集中繼資料中包含常見問題集的語言代碼做為欄位。如果常見問題集在中繼資料欄位中指定的中繼資料中沒有語言代碼，常見問題集會使用您呼叫 [CreateFAQ](#) 作業時指定的語言代碼編製索引。若要在主控台中以支援的語言編製常見問題集文件的索引，請前往常見問題集並選取新增常見問題 您可以從下拉菜單中選擇一種語言語言。

建立自訂文件欄位

您可以在 Amazon Kendra 索引中為文件建立自訂屬性或欄位。例如，您可以建立名為「部門」的自訂欄位或屬性，其值為「HR」、「業務」和「製造」。例如，如果將這些自訂欄位或屬性對應至 Amazon Kendra 索引，您可以使用這些欄位來篩選搜尋結果，以便依「HR」部門屬性包含文件。

您必須先在索引中建立欄位，才能使用自訂欄位或屬性。使用主控台編輯資料來源欄位對應，以新增自訂欄位，或使用 [UpdateIndex](#) API 建立索引欄位。建立欄位後，就無法變更欄位資料類型。

對於大多數資料來源，您可以將外部資料來源中的欄位對映至中的對應欄位 Amazon Kendra。如需詳細資訊，請參閱[映射資料來源欄位](#)。對於 S3 資料來源，您可以使用 JSON 中繼資料檔案建立自訂欄位或屬性。

您最多可以建立 500 個自訂欄位或屬性。

您也可以使用 Amazon Kendra 保留欄位或公用欄位。如需詳細資訊，請參閱[文件屬性或欄位](#)。

主題

- [更新自訂文件欄位](#)

更新自訂文件欄位

透過 UpdateIndex API，您可以使用 DocumentMetadataConfigurationUpdates 參數新增自訂欄位或屬性。

下面的 JSON 示例使 DocumentMetadataConfigurationUpdates 用一個名為「部門」的字段添加到索引。

```
"DocumentMetadataConfigurationUpdates": [  
  {  
    "Name": "Department",  
    "Type": "STRING_VALUE"  
  }  
]
```

以下各節包括使用 [BatchPutDocument](#) 和為 Amazon S3 資料來源新增自訂屬性或欄位的範例。

主題

- [使用 BatchPutDocument API 新增自訂屬性或欄位](#)
- [將自訂屬性或欄位新增至 Amazon S3 資料來源](#)

使用 BatchPutDocument API 新增自訂屬性或欄位

當您使用 [BatchPutDocument](#) API 將文件新增至索引時，您可以指定自訂欄位或屬性做為的一部分 Attributes。您可以在呼叫 API 時新增多個欄位或屬性。您最多可以建立 500 個自訂欄位或屬性。下列範例是將「部門」新增至文件的自訂欄位或屬性。

```
"Attributes":
```

```
{
  "Department": "HR",
  "_category": "Vacation policy"
}
```

將自訂屬性或欄位新增至 Amazon S3 資料來源

當您使用 S3 儲存貯體做為索引的資料來源時，您可以使用隨附的中繼資料檔案將中繼資料新增至文件。您可以將中繼資料 JSON 檔案放置在與文件 `parallel` 的目錄結構中。如需詳細資訊，請參閱 [S3 文件中繼資料](#)。

您可以在 Attributes JSON 結構中指定自訂欄位或屬性。您最多可以建立 500 個自訂欄位或屬性。例如，下列範例使用 Attributes 定義三個自訂欄位或屬性以及一個保留欄位。

```
"Attributes": {
  "brand": "Amazon Basics",
  "price": 1595,
  "_category": "sports",
  "subcategories": ["outdoors", "electronics"]
}
```

以下步驟將引導您完成將自訂屬性新增至 Amazon S3 資料來源的步驟。

主題

- [步驟 1：建立 Amazon Kendra 索引](#)
- [第 2 步：更新索引以添加自定義文檔字段](#)
- [步驟 3：建立 Amazon S3 資料來源，並將資料來源欄位對應至自訂屬性](#)

步驟 1：建立 Amazon Kendra 索引

請依照中的步驟[建立索引](#)建立您的 Amazon Kendra 索引。

第 2 步：更新索引以添加自定義文檔字段

建立索引之後，您可以將欄位新增至索引。下列程序顯示如何使用主控台和 CLI 將欄位新增至索引。

Console

若要建立索引欄位

1. 請確定您已[建立索引](#)。

2. 然後，從左側導覽功能表中，從資料管理中選擇 Facet 定義。
3. 在 [索引欄位設定指南] 的 [索引欄位] 中，選擇 [新增欄位] 以新增自訂欄位。
4. 在 [新增索引欄位] 對話方塊中，執行下列動作：
 - 欄位名稱 — 新增欄位名稱。
 - 資料類型 — 選取資料類型，無論是「字串」、「字串清單」還是「日期」。
 - 使用類型 — 選取使用類型，是否可分解、可搜尋、可顯示及可排序。

然後，選取 [新增]。

對您要對映的任何其他欄位重複最後一個步驟。

CLI

```
aws kendra update-index \
--region $region \
--endpoint-url $endpoint \
--application-id $applicationId \
--index-id $indexId \
--document-metadata-configuration-updates \
"[
  {
    "Name": "string",
    "Type": "STRING_VALUE"|"STRING_LIST_VALUE"|"LONG_VALUE"|"DATE_VALUE",
    "Relevance": {
      "Freshness": true|false,
      "Importance": integer,
      "Duration": "string",
      "RankOrder": "ASCENDING"|"DESCENDING",
      "ValueImportanceMap": {"string": integer
      ...}
    },
    "Search": {
      "Facetable": true|false,
      "Searchable": true|false,
      "Displayable": true|false,
      "Sortable": true|false
    }
  }
]
...
```

```
]"
```

步驟 3：建立 Amazon S3 資料來源，並將資料來源欄位對應至自訂屬性

若要建立 Amazon S3 資料來源並將欄位對應至該資料來源，請遵循中的指示[Amazon S3](#)。

如果您使用的是 API，請在使用 [CreateDataSource](#) API configuration 時使用下方的 fieldMappings 屬性。

有關如何對應資料來源欄位的概觀，請參閱[對映資料來源欄位](#)。

使用權杖控制使用者對文件的存取

您可以控制哪些使用者或群組可以存取索引中的特定文件，或在其搜尋結果中查看某些文件。這稱為使用者內容篩選。它是一種個性化搜索，具有控制對文檔的訪問的好處。例如，並非所有在公司入口網站中搜尋資訊的團隊都應該存取絕密的公司文件，這些文件也不適用於所有使用者。只有具備絕密文件存取權的特定使用者或專案團隊群組才能在搜尋結果中看到這些文件。

Amazon Kendra 使用以下令牌類型支持基於令牌的用戶訪問控制：

- 開放識別碼
- 具有共享秘密的 JWT
- 帶有公鑰的 JWT
- JSON

Amazon Kendra 為您的搜尋應用程式提供高度安全的企業搜尋。搜尋結果會反映組織的安全性模型。客戶有責任驗證並授權使用者存取其搜尋應用程式。在搜尋時，Amazon Kendra 服務會根據客戶的搜尋應用程式提供的使用者識別碼，以及文件存取控制清單 (ACL) 來篩選搜尋結果 Amazon Kendra 編目/索引時間期間的連接器。搜尋結果會傳回指向原始文件儲存庫的 URL 以及簡短摘錄。對完整文件的存取仍由原始存放庫強制執行。

主題

- [使用 OpenID](#)
- [使用 JSON 網絡令牌 \(JWT\) 與共享密鑰](#)
- [使用 JSON 網絡令牌 \(JWT\) 與公鑰](#)
- [使用 JSON](#)

使用 OpenID

要配置 Amazon Kendra 索引以使用 OpenID 令牌進行訪問控制，您需要 OpenID 提供程序提供的 JWKS (JSON 網絡密鑰集) URL。在大多數情況下，JWKS 網址採用以下格式 (如果他們正在遵循 OpenID 發現)。https://domain-name/.well_known/jwks.json

下列範例說明如何在建立索引時使用 OpenID 權杖進行使用者存取控制。

Console

1. 選擇 [建立索引] 以開始建立新索引。
2. 在 [指定索引詳細資訊] 頁面上，為索引提供名稱和說明。
3. 對於 IAM 角色，請選取角色或選取建立新角色，然後指定角色名稱以建立新角色。IAM 角色的字首為「AmazonKendra-」。
4. 將所有其他欄位保留為預設值。選擇下一步。
5. 在 [設定使用者存取控制] 頁面的 [存取控制設定] 下，選擇 [是] 以使用權杖進行存取控制。
6. 在令牌配置下，選擇 OpenID 作為令牌類型。
7. 指定簽署金鑰 URL。該網址應指向一組 JSON 網絡密鑰。
8. 進階組態下的選用性：
 - a. 指定 ACL 檢查中要使用的「使用者名稱」。
 - b. 指定一個或多個要在 ACL 檢查中使用的群組。
 - c. 指定將驗證權杖發行者的發行者。
 - d. 指定用戶端識別碼。您必須指定符合 JWT 中對象的規則運算式。
9. 在佈建詳細資料頁面中，選擇開發人員版本。
10. 選擇 [建立] 以建立索引。
11. 等待您的索引創建。Amazon Kendra 為您的索引佈建硬體。此操作可能需要一些時間。

CLI

若要 AWS CLI 使用 JSON 輸入檔案建立索引，請先使用您想要的參數建立 JSON 檔案：

```
{
  "Name": "user-context",
  "Edition": "ENTERPRISE_EDITION",
  "RoleArn": "arn:aws:iam::account-id:role:/my-role",
```

```

    "UserTokenConfigurations": [
      {
        "JwtTokenTypeConfiguration": {
          "KeyLocation": "URL",
          "Issuer": "optional: specify the issuer url",
          "ClaimRegex": "optional: regex to validate claims in the token",
          "UserNameAttributeField": "optional: user",
          "GroupAttributeField": "optional: group",
          "URL": "https://example.com/.well-known/jwks.json"
        }
      }
    ],
    "UserContextPolicy": "USER_TOKEN"
  }

```

您可以覆寫預設的使用者和群組欄位名稱。的預設值UserNameAttributeField為「使用者」。的預設值GroupAttributeField為「群組」。

接下來，create-index使用輸入文件調用。例如，如果JSON檔案的名稱是create-index-openid.json，您可以使用下列命令：

```
aws kendra create-index --cli-input-json file://create-index-openid.json
```

Python

```

response = kendra.create_index(
    Name='user-context',
    Edition='ENTERPRISE_EDITION',
    RoleArn='arn:aws:iam::account-id:role:/my-role',
    UserTokenConfigurations=[
      {
        "JwtTokenTypeConfiguration": {
          "KeyLocation": "URL",
          "Issuer": "optional: specify the issuer url",
          "ClaimRegex": "optional: regex to validate claims in the token",
          "UserNameAttributeField": "optional: user",
          "GroupAttributeField": "optional: group",
          "URL": "https://example.com/.well-known/jwks.json"
        }
      }
    ],
    UserContextPolicy='USER_TOKEN'
)

```


)

使用 JSON 網絡令牌 (JWT) 與共享密鑰

下列範例說明如何在建立索引時使用 JSON Web Token (JWT) 搭配共用密碼權杖，以供使用者存取控制。

Console

1. 選擇 [建立索引] 以開始建立新索引。
2. 在 [指定索引詳細資訊] 頁面上，為索引提供名稱和說明。
3. 對於 IAM 角色，請選取角色或選取 [建立新角色]，然後指定角色名稱以建立新角色。該 IAM 角色的前綴為「AmazonKendra-」。
4. 將所有其他欄位保留為預設值。選擇下一步。
5. 在 [設定使用者存取控制] 頁面的 [存取控制設定] 下，選擇 [是] 以使用權杖進行存取控制。
6. 在令牌配置下，選擇具有共享密鑰的 JWT 作為令牌類型。
7. 在 [簽署共用密碼的參數] 下，選擇 [密碼類型]。您可以使用現有的 AWS Secrets Manager 共用密碼或建立新的共用密碼。

若要建立新的共用密碼，請選擇 [新增]，然後依照下列步驟執行：

- a. 在 [新 AWS Secrets Manager 密碼] 下，指定 [密碼] 名稱。當您儲存公開金鑰時，AmazonKendra-會新增前置字元。
 - b. 指定金鑰識別碼。密鑰 ID 是一個提示，指示哪個密鑰用於保護令牌的 JSON Web 簽名。
 - c. 選擇權杖的簽署演算法。這是用於保護 ID 令牌的加密算法。如需 RSA 的詳細資訊，請參閱 [RSA 加密法](#)。
 - d. 透過輸入 base64 URL 編碼的密碼來指定共用密碼。您也可以選取 [產生密碼]，為您產生密碼。您必須確保密碼是一個 base64 網址編碼的密碼。
 - e. (選擇性) 指定共用密碼的有效時間。您可以指定密碼的有效起始日期和時間、有效截止日期或兩者兼而有之。密碼將在指定的間隔內有效。
 - f. 選取 [儲存密碼] 以儲存新密碼。
8. (選擇性) 在「進階組態」下：
 - a. 指定 ACL 檢查中要使用的「使用者名稱」。
 - b. 指定一個或多個要在 ACL 檢查中使用的群組。

- c. 指定將驗證權杖發行者的發行者。
 - d. 指定宣告識別碼。您必須指定符合 JWT 中對象的規則運算式。
9. 在佈建詳細資料頁面中，選擇開發人員版本。
 10. 選擇 [建立] 以建立索引。
 11. 等待您的索引創建。Amazon Kendra 為您的索引佈建硬體。此操作可能需要一些時間。

CLI

您可以在中使用帶有共享密鑰的 AWS Secrets Manager JWT 令牌。密碼必須是以 base64 網址編碼的密碼。您需要 Secrets Manager ARN，並且您的 Amazon Kendra 角色必須具有 Secrets Manager 資源的 GetSecretValue 存取權。如果您使用加密資 Secrets Manager 源 AWS KMS，則角色也必須具有解密動作的存取權。

若要 AWS CLI 使用 JSON 輸入檔案建立索引，請先使用您想要的參數建立 JSON 檔案：

```
{
  "Name": "user-context",
  "Edition": "ENTERPRISE_EDITION",
  "RoleArn": "arn:aws:iam::account-id:role:/my-role",
  "UserTokenConfigurations": [
    {
      "JwtTokenTypeConfiguration": {
        "KeyLocation": "SECRET_MANAGER",
        "Issuer": "optional: specify the issuer url",
        "ClaimRegex": "optional: regex to validate claims in the token",
        "UserNameAttributeField": "optional: user",
        "GroupAttributeField": "optional: group",
        "SecretManagerArn": "arn:aws:secretsmanager:us-west-2:account
id:secret:/my-user-context-secret"
      }
    }
  ],
  "UserContextPolicy": "USER_TOKEN"
}
```

您可以覆寫預設的使用者和群組欄位名稱。的預設值 UserNameAttributeField 為「使用者」。的預設值 GroupAttributeField 為「群組」。

接下來，create-index 使用輸入文件調用。例如，如果 JSON 文件的名稱是 create-index-openid.json，則可以使用以下命令：

```
aws kendra create-index --cli-input-json file://create-index-openid.json
```

密碼必須具有以下格式 AWS Secrets Manager :

```
{
  "keys": [
    {
      "kid": "key_id",
      "alg": "HS256|HS384|HS512",
      "kty": "OCT",
      "use": "sig", //this value can be sig only for now
      "k": "secret",
      "nbf": "ISO1806 date format"
      "exp": "ISO1806 date format"
    }
  ]
}
```

如需有關 JWT 的詳細資訊，請參閱 jwt.io。

Python

您可以在中使用帶有共享密鑰的 AWS Secrets Manager JWT 令牌。密碼必須是以 base64 網址編碼的密碼。您需要 Secrets Manager ARN，並且您的 Amazon Kendra 角色必須具有 Secrets Manager 資源的 GetSecretValue 存取權。如果您使用加密資 Secrets Manager 源 AWS KMS，則角色也必須具有解密動作的存取權。

```
response = kendra.create_index(
    Name='user-context',
    Edition='ENTERPRISE_EDITION',
    RoleArn='arn:aws:iam::account-id:role:/my-role',
    UserTokenConfigurations=[
        {
            "JwtTokenTypeConfiguration": {
                "KeyLocation": "URL",
                "Issuer": "optional: specify the issuer url",
                "ClaimRegex": "optional: regex to validate claims in the token",
                "UserNameAttributeField": "optional: user",
                "GroupAttributeField": "optional: group",
                "SecretManagerArn": "arn:aws:secretsmanager:us-west-2:account
id:secret:/my-user-context-secret"
            }
        }
    ]
)
```

```
    }  
  ],  
  UserContextPolicy='USER_TOKEN'  
)
```

使用 JSON 網絡令牌 (JWT) 與公鑰

下列範例會示範如何在建立索引時，使用 JSON Web Token (JWT) 搭配公開金鑰來進行使用者存取控制。如需有關 JWT 的詳細資訊，請參閱 jwt.io。

Console

1. 選擇 [建立索引] 以開始建立新索引。
2. 在 [指定索引詳細資訊] 頁面上，為索引提供名稱和說明。
3. 對於 IAM 角色，請選取角色或選取 [建立新角色]，然後指定角色名稱以建立新角色。該 IAM 角色的前綴為「AmazonKendra-」。
4. 將所有其他欄位保留為預設值。選擇下一步。
5. 在 [設定使用者存取控制] 頁面的 [存取控制設定] 下，選擇 [是] 以使用權杖進行存取控制。
6. 在令牌配置下，選擇具有公共密鑰的 JWT 作為令牌類型。
7. 在 [簽署公用金鑰的參數] 下，選擇 [密碼類型]。您可以使用現有 AWS Secrets Manager 密碼或建立新密碼。

若要建立新密碼，請選擇 [新增]，然後依照下列步驟執行：

- a. 在 [新 AWS Secrets Manager 密碼] 下，指定 [密碼] 名稱。當您儲存公開金鑰時，AmazonKendra- 會新增前置字元。
- b. 指定金鑰識別碼。密鑰 ID 是一個提示，指示哪個密鑰用於保護令牌的 JSON Web 簽名。
- c. 選擇權杖的簽署演算法。這是用於保護 ID 令牌的加密算法。如需 RSA 的詳細資訊，請參閱 [RSA 加密法](#)。
- d. 在 [憑證屬性] 下，指定選擇性的憑證鏈結。憑證鏈結是由憑證清單所組成。它以伺服器的憑證開頭，並以根憑證終止。
- e. 選擇性指定指紋或指紋。它應該是一個證書的哈希值，計算在所有證書數據及其簽名上。
- f. 指定「指數」。這是 RSA 公開金鑰的指數值。它以 Base64urlUInt 編碼值表示。
- g. 指定模數。這是 RSA 公開金鑰的指數值。它以 Base64urlUInt 編碼值表示。
- h. 選取 [儲存金鑰] 以儲存新的金鑰。

8. 進階組態下的選用性：
 - a. 指定 ACL 檢查中要使用的「使用者名稱」。
 - b. 指定一個或多個要在 ACL 檢查中使用的群組。
 - c. 指定將驗證權杖發行者的發行者。
 - d. 指定用戶端識別碼。您必須指定符合 JWT 中對象的規則運算式。
9. 在佈建詳細資料頁面中，選擇開發人員版本。
10. 選擇 [建立] 以建立索引。
11. 等待您的索引創建。Amazon Kendra 為您的索引佈建硬體。此操作可能需要一些時間。

CLI

您可以將 JWT 與 AWS Secrets Manager 您需要 Secrets Manager ARN，並且您的 Amazon Kendra 角色必須具有 Secrets Manager 資源的 `GetSecretValue` 存取權。如果您使用加密資 Secrets Manager 源 AWS KMS，則角色也必須具有解密動作的存取權。

若要 AWS CLI 使用 JSON 輸入檔案建立索引，請先使用您想要的參數建立 JSON 檔案：

```
{
  "Name": "user-context",
  "Edition": "ENTERPRISE_EDITION",
  "RoleArn": "arn:aws:iam::account id:role:/my-role",
  "UserTokenConfigurationList": [
    {
      "JwtTokenTypeConfiguration": {
        "KeyLocation": "SECRET_MANAGER",
        "Issuer": "optional: specify the issuer url",
        "ClaimRegex": "optional: regex to validate claims in the token",
        "UserNameAttributeField": "optional: user",
        "GroupAttributeField": "optional: group",
        "SecretManagerArn": "arn:aws:secretsmanager:us-west-2:account
id:secret:/my-user-context-secret"
      }
    }
  ],
  "UserContextPolicy": "USER_TOKEN"
}
```

您可以覆寫預設的使用者和群組欄位名稱。的預設值 `UserNameAttributeField` 為「使用者」。的預設值 `GroupAttributeField` 為「群組」。

接下來，`create-index` 使用輸入文件調用。例如，如果 JSON 文件的名稱是 `create-index-openid.json`，則可以使用以下命令：

```
aws kendra create-index --cli-input-json file://create-index-openid.json
```

密碼必須具有以下格式 Secrets Manager：

```
{
  "keys": [
    {
      "alg": "RS256|RS384|RS512",
      "kty": "RSA", //this can be RSA only for now
      "use": "sig", //this value can be sig only for now
      "n": "modulus of standard pem",
      "e": "exponent of standard pem",
      "kid": "key_id",
      "x5t": "certificate thumbprint for x.509 cert",
      "x5c": [
        "certificate chain"
      ]
    }
  ]
}
```

如需有關 JWT 的詳細資訊，請參閱 jwt.io。

Python

```
response = kendra.create_index(
    Name='user-context',
    Edition='ENTERPRISE_EDITION',
    RoleArn='arn:aws:iam::account id:role:/my-role',
    UserTokenConfigurationList=[
        {
            "JwtTokenTypeConfiguration": {
                "KeyLocation": "URL",
                "Issuer": "optional: specify the issuer url",
                "ClaimRegex": "optional: regex to validate claims in the token",
                "UserNameAttributeField": "optional: user",
                "GroupAttributeField": "optional: group",
                "SecretManagerArn": "arn:aws:secretsmanager:us-west-2:account
id:secret:/my-user-context-secret"
            }
        }
    ]
)
```

```
    }  
  ],  
  UserContextPolicy='USER_TOKEN'  
)
```

使用 JSON

下列範例顯示如何在建立索引時使用 JSON 進行使用者存取控制。

Warning

JSON 令牌是未經驗證的有效負載。只有當請求來自受信任的服務器而不是 Amazon Kendra 來自瀏覽器時，才應使用此功能。

Console

1. 選擇 [建立索引] 以開始建立新索引。
2. 在 [指定索引詳細資訊] 頁面上，為索引提供名稱和說明。
3. 對於 IAM 角色，請選取角色或選取建立新角色，然後指定角色名稱以建立新角色。該 IAM 角色的前綴為「AmazonKendra-」。
4. 將所有其他欄位保留為預設值。選擇下一步。
5. 在 [設定使用者存取控制] 頁面的 [存取控制設定] 下，選擇 [是] 以使用權杖進行存取控制。
6. 在權杖組態下，選取 JSON 作為權杖類型。
7. 指定 ACL 檢查中要使用的使用者名稱。
8. 指定一個或多個要在 ACL 檢查中使用的群組。
9. 選擇下一步。
10. 在佈建詳細資料頁面中，選擇開發人員版本。
11. 選擇 [建立] 以建立索引。
12. 等待您的索引創建。Amazon Kendra 為索引佈建硬體。此操作可能需要一些時間。

CLI

若要 AWS CLI 使用 JSON 輸入檔案建立索引，請先使用您想要的參數建立 JSON 檔案：

```
{
```

```

    "Name": "user-context",
    "Edition": "ENTERPRISE_EDITION",
    "RoleArn": "arn:aws:iam::account-id:role:/my-role",
    "UserTokenConfigurations": [
      {
        "JsonTokenTypeConfiguration": {
          "UserNameAttributeField": "user",
          "GroupAttributeField": "group"
        }
      }
    ],
    "UserContextPolicy": "USER_TOKEN"
  }

```

接下來，`create-index` 使用輸入文件調用。例如，如果 JSON 文件的名稱是 `create-index-openid.json`，則可以使用以下命令：

```
aws kendra create-index --cli-input-json file://create-index-openid.json
```

如果您沒有使用 Open ID AWS IAM Identity Center，您可以以 JSON 格式向我們發送令牌。如果這樣做，您必須指定 JSON Token 中的哪個欄位包含使用者名稱，以及哪個欄位包含群組。群組欄位值必須是 JSON 字串陣列。例如，如果您正在使用 SAML，則您的令牌將類似於以下內容：

```

{
  "username" : "user1",
  "groups": [
    "group1",
    "group2"
  ]
}

```

`TokenConfiguration` 會指定使用者名稱和群組欄位名稱：

```

{
  "UserNameAttributeField": "username",
  "GroupAttributeField": "groups"
}

```

Python

```
response = kendra.create_index(
```



```
Name='user-context',
Edition='ENTERPRISE_EDITION',
RoleArn='arn:aws:iam::account-id:role:/my-role',
UserTokenConfigurations=[
  {
    "JwtTokenTypeConfiguration": {
      "UserNameAttributeField": "user",
      "GroupAttributeField": "group",
    }
  }
],
UserContextPolicy='USER_TOKEN'
)
```

建立資料來源連接器

您可以建立資料來源連接器 Amazon Kendra，以連接至文件並編製索引。Amazon Kendra 可以連接到 Microsoft SharePoint，Google 雲端硬碟和許多其他提供商。當您建立資料來源連接器時，您會提供 Amazon Kendra 連線至來源儲存庫所需的組態資訊。與直接將文件新增至索引不同，您可以定期掃描資料來源以更新索引。

例如，假設您有儲存在 Amazon S3 值區中的稅捐文件儲存庫。會不時變更現有文件，並將新文件新增至存放庫。如果您將存放庫 Amazon Kendra 作為資料來源新增至，則可以透過設定資料來源和索引之間的定期同步來使索引保持最新狀態。

您可以選擇使用主控台或 [StartDataSourceSyncJob](#) API 手動更新索引。否則，您可以設定排程來更新索引，並讓它與您的資料來源同步。

一個索引可以有許多資料來源。每個資料來源都可以有自己的更新排程。例如，您可以每天甚至每小時更新工作文件的索引，同時在封存變更時手動更新已封存文件。

如果您想要在文件擷取程序期間變更文件中繼資料或屬性和內容，請參閱 [Amazon Kendra 自訂文件增強功能](#)。

Note

每個文件 ID 必須是每個索引唯一的。您無法建立資料來源以使用其唯一 ID 為文件建立索引，然後使用 BatchPutDocument API 來索引相同的文件，反之亦然。您可以刪除資料來源，然後使用 BatchPutDocument API 索引相同的文件，反之亦然。針對同一組文件使用 BatchPutDocument 和 BatchDeleteDocument API 搭配 Amazon Kendra 資料來源連接器，可能會導致資料不一致。相反地，我們建議使用 [Amazon Kendra 自訂資料來源連接器](#)。

Note

新增至索引的檔案必須位於 UTF-8 編碼位元組串流中。如需中文文件的詳細資訊 Amazon Kendra，請參閱 [文件](#)。

設定更新排程

將資料來源設定為定期使用主控台進行更新，或在建立或更新資料來源時使用Schedule參數進行更新。參數的內容是一個字串，其中包含 cron-format 排程字串或空字串，表示索引會隨需更新。如需 Cron 運算式的格式，請參閱《Amazon CloudWatch Events 使用指南》中的[規則排程運算式](#)。Amazon Kendra 僅支持 cron 表達式。它不支援速率運算式。

設定語言

您可以使用支援的語言，為資料來源中的所有文件建立索引。您可以在呼叫時為資料來源中的所有文件指定語言代碼 [CreateDataSource](#)。如果文件沒有在中繼資料欄位中指定的語言代碼，則會使用在資料來源層級為所有文件指定的語言代碼為文件編製索引。如果您未指定語言，則依預設會以英文 Amazon Kendra 編製資料來源中的文件索引。如需支援語言 (包括其代碼) 的詳細資訊，請參閱以[英文以外的語言新增文件](#)。

您可以使用主控台以支援的語言編製資料來源中的所有文件索引。轉到數據源並編輯您的數據源或添加數據源 (如果要添加新的數據源)。在 [指定資料來源詳細資料] 頁面上，從下拉式清單中選擇語言 [語言]。您可以選取 [更新] 或繼續輸入組態資訊以連線至資料來源。

資料來源連接器

本節說明如何使 Amazon Kendra 用和 Amazon Kendra API 連線 Amazon Kendra 到支援的資料庫 AWS Management Console 和資料來源儲存庫。

主題

- [資料來源範本架構](#)
- [Adobe Experience Manager](#)
- [Alfresco](#)
- [Aurora \(MySQL\)](#)
- [Aurora \(PostgreSQL\)](#)
- [Amazon FSx \(視窗\)](#)
- [Amazon FSx \(NetApp ONTAP\)](#)
- [Amazon RDS/Aurora](#)
- [Amazon RDS \(Microsoft SQL 服務器\)](#)

- [Amazon RDS \(MySQL\)](#)
- [Amazon RDS \(Oracle\)](#)
- [Amazon RDS \(PostgreSQL\)](#)
- [Amazon S3](#)
- [Amazon Kendra 網絡爬蟲](#)
- [Amazon WorkDocs](#)
- [立方體](#)
- [Confluence](#)
- [自訂資料來源連接器](#)
- [Dropbox](#)
- [Drupal](#)
- [GitHub](#)
- [Gmail](#)
- [Google 雲端硬碟](#)
- [IBM DB2](#)
- [Jira](#)
- [Microsoft Exchange](#)
- [Microsoft OneDrive](#)
- [Microsoft SharePoint](#)
- [Microsoft SQL Server](#)
- [Microsoft Teams](#)
- [Microsoft 亞默](#)
- [MySQL](#)
- [Oracle Database](#)
- [PostgreSQL](#)
- [諷刺語](#)
- [Salesforce](#)
- [ServiceNow](#)
- [Slack](#)
- [Zendesk](#)

資料來源範本架構

以下是支援範本之資料來源的範本結構描述。

主題

- [Adobe Experience Manager 模板架構](#)
- [Amazon FSx \(視窗\) 範本結構](#)
- [Amazon FSx \(NetApp ONTAP\) 範本結構描述](#)
- [Alfresco 模板架構](#)
- [Aurora \(MySQL\) 模板架構](#)
- [Aurora 模板模板架構](#)
- [Amazon RDS \(Microsoft SQL 服務器 \) 模板架構](#)
- [Amazon RDS \(MySQL\) 模板架構](#)
- [Amazon RDS \(甲骨文\) 樣板綱要](#)
- [Amazon RDS 模板模板架構](#)
- [Amazon S3 模板架構](#)
- [Amazon Kendra 網路爬蟲範本結構描述](#)
- [匯流模板架構](#)
- [模板架構](#)
- [Drupal 的模板架構](#)
- [GitHub 模板架構](#)
- [模板架構](#)
- [谷歌驅動器模板架構](#)
- [模板架構](#)
- [Microsoft 交易所模板架構](#)
- [Microsoft OneDrive 模板架構](#)
- [Microsoft SharePoint 模板架構](#)
- [Microsoft SQL 服務器模板架構](#)
- [Microsoft 團隊模板架構](#)
- [Microsoft 模板架構](#)
- [MySQL 板架構](#)

- [Oracle 資料庫範本綱要](#)
- [PostgreSQL 架構](#)
- [銷售力範本結構描述](#)
- [ServiceNow 模板架構](#)
- [鬆弛模板架構](#)
- [ZENDESK 模板架構](#)

Adobe Experience Manager 模板架構

您可以將包含資料來源結構描述的 JSON 納入為 [TemplateConfiguration](#) 物件的一部分。您可以提供 Adobe Experience Manager 主機 URL、驗證類型，以及是否將 Adobe Experience Manager (AEM) 用作雲端服務還是 AEM 內部部署作為連線組態或存放庫端點詳細資料的一部分。此外，請將資料來源類型指定為 AEM、驗證認證的密碼，以及其他必要的組態。然後，您將指定 TEMPLATE 為呼叫 Type 時 [CreateDataSource](#)。

您可以使用本開發人員指南中提供的模板。如需詳細資訊，請參閱 [Adobe Experience Manager 結構定義](#)。

下表說明 AEM JSON 結構描述的參數。

組態	描述
連線組態	資料來源端點的組態資訊。
repositoryEndpointMetadata	資料來源的端點資訊。
AEMURL	Adobe Experience Manager 主持人網址。例如，如果您使用 AEM 內部部署，則會包含主機名稱和連接埠：https://hostname:port 或者，如果您使用 AEM 做為雲端服務，您可以使用作者 URL：https://author-xxxxxx-xxxxxx.adobe.aemcloud.com。
authType	您使用的驗證類型，無論是 Basic 或 OAuth2。
deploymentType	您使用 Adobe Experience Manager 的類型，CLOUD 或 ON_PREMISE。

組態	描述
儲存庫組態 <ul style="list-style-type: none"> • page • 資產 	資料來源內容的組態資訊。例如，配置特定類型的內容和欄位對應。 將Adobe Experience Manager頁面和資產的屬性或欄位名稱對應至 Amazon Kendra 索引欄位名稱的物件清單。如需詳細資訊，請參閱 映射資料來源欄位 。
附加屬性 timeZoneId <ul style="list-style-type: none"> • pageRootPaths • assetRootPaths 	資料來源中內容的其他組態選項。 如果您使用 AEM 內部部署，且伺服器的時區與 AEM 連接器或索引的時區不同，則可以指定要與 Amazon Kendra AEM 連接器或索引對齊的伺服器時區。 AEM 內部部署的預設時區是 Amazon Kendra AEM 連接器或索引的時區。AEM 做為雲端服務的預設時區是格林威治標準時間。
爬行資產	true以編目資產。
抓取頁面 <ul style="list-style-type: none"> • pagePathInclusion模式 • pageNameInclusion模式 • assetPathInclusion模式 • assetTypeInclusion模式 • assetNameInclusion模式 	true抓取頁面。 規則運算式模式清單，可在資Adobe Experience Manager料來源中包含特定頁面和資產。與模式匹配的頁面和資產都包含在索引中。不符合模式的頁面和資產會從索引中排除。如果頁面或資產同時符合包含模式和排除模式，則排除模式優先，而且內容不會包含在索引中。

組態	描述
<ul style="list-style-type: none"> • pagePathExclusion 模式 • pageNameExclusion 模式 • assetPathExclusion 模式 • assetTypeInclusion 模式 • assetNameInclusion 模式 	<p>用於排除資 Adobe Experience Manager 料來源中某些頁面和資產的規則運算式模式清單。符合模式的頁面和資產會從索引中排除。不符合模式的頁面和資產會包含在索引中。如果頁面或資產同時符合包含模式和排除模式，則排除模式優先，而且內容不會包含在索引中。</p>
<p>頁面組件</p>	<p>您要索引之特定頁面元件的名稱清單。</p>
<p>contentFragmentVariations</p>	<p>您要建立索引之 Adobe Experience Manager 內容片段之特定儲存變體的名稱清單。</p>
<p>type</p>	<p>資料來源的類型。指定 AEM 為您的資料來源類型。</p>
<p>enableIdentityCrawler</p>	<p>true，以使用 Amazon Kendra 的身分識別爬行者程式來同步使用者和群組的身分識別/主體資訊，以存取特定文件。如果關閉身分搜索器，則可以公開搜索所有文檔。如果您想要對文件使用存取控制，且身分識別編目程式已關閉，您也可以使用 PutPrincipalMapping API 來上傳使用者和群組存取資訊。</p>

組態	描述
同步模式	<p>指定資料來源內容變更時 Amazon Kendra 應如何更新索引。您可以選擇：</p> <ul style="list-style-type: none"> • FORCED_FULL_CRAWL 新建索引所有內容，並在每次資料來源與索引同步時取代現有內容。 • FULL_CRAWL ，每次您的資料來源與索引同步時，僅對新的、修改和刪除的內容建立索引。Amazon Kendra 可以使用資料來源的機制來追蹤內容變更，並為上次同步後變更的內容建立索引。 • CHANGE_LOG 每次資料來源與索引同步時，僅對新內容和修改的內容建立索引。Amazon Kendra 可以使用資料來源的機制來追蹤內容變更，並為上次同步後變更的內容建立索引。
秘書	<p>AWS Secrets Manager 密碼的 Amazon 資源名稱 (ARN)，其中包含連接到 Adobe 體驗管理器所需的鍵值對。如需這些機碼值配對的詳細資訊，請參閱 Adobe 體驗管理員的連線指示。</p>
version	<p>目前支援的此範本版本。</p>

Adobe Experience Manager 結構定義

```
{
  "$schema": "http://json-schema.org/draft-04/schema#",
  "type": "object",
  "properties": {
    {
      "connectionConfiguration": {
        "type": "object",
        "properties": {
          {
            "repositoryEndpointMetadata":
              {
```

```
"type": "object",
"properties":
{
  "aemUrl":
  {
    "type": "string",
    "pattern": "https:.*"
  },
  "authType": {
    "type": "string",
    "enum": ["Basic", "OAuth2"]
  },
  "deploymentType": {
    "type": "string",
    "enum": ["CLOUD", "ON_PREMISE"]
  }
},
"required":
[
  "aemUrl",
  "authType",
  "deploymentType"
]
},
"required":
[
  "repositoryEndpointMetadata"
]
},
"repositoryConfigurations": {
  "type": "object",
  "properties":
  {
    "page":
    {
      "type": "object",
      "properties":
      {
        "fieldMappings":
        {
          "type": "array",
          "items":
          [
```

```
    {
      "type": "object",
      "properties":
      {
        "indexFieldName":
        {
          "type": "string"
        },
        "indexFieldType":
        {
          "type": "string",
          "enum":
          [
            "STRING",
            "STRING_LIST",
            "DATE",
            "LONG"
          ]
        },
        "dataSourceFieldName":
        {
          "type": "string"
        },
        "dateFieldFormat":
        {
          "type": "string",
          "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
        }
      },
      "required":
      [
        "indexFieldName",
        "indexFieldType",
        "dataSourceFieldName"
      ]
    }
  ],
  "required":
  [
    "fieldMappings"
  ]
},
```

```
"asset":
{
  "type": "object",
  "properties":
  {
    "fieldMappings":
    {
      "type": "array",
      "items":
      [
        {
          "type": "object",
          "properties":
          {
            "indexFieldName":
            {
              "type": "string"
            },
            "indexFieldType":
            {
              "type": "string",
              "enum":
              [
                "STRING",
                "STRING_LIST",
                "DATE",
                "LONG"
              ]
            },
            "dataSourceFieldName":
            {
              "type": "string"
            },
            "dateFieldFormat":
            {
              "type": "string",
              "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
            }
          }
        },
        "required":
        [
          "indexFieldName",
          "indexFieldType",
          "dataSourceFieldName"
        ]
      ]
    }
  }
}
```

```
        ]
      }
    ]
  }
},
"required":
[
  "fieldMappings"
]
}
},
"additionalProperties": {
  "type": "object",
  "properties": {
    {
      "timeZoneId": {
        "type": "string",
        "enum": [
          "Africa/Abidjan",
          "Africa/Accra",
          "Africa/Addis_Ababa",
          "Africa/Algiers",
          "Africa/Asmara",
          "Africa/Asmera",
          "Africa/Bamako",
          "Africa/Bangui",
          "Africa/Banjul",
          "Africa/Bissau",
          "Africa/Blantyre",
          "Africa/Brazzaville",
          "Africa/Bujumbura",
          "Africa/Cairo",
          "Africa/Casablanca",
          "Africa/Ceuta",
          "Africa/Conakry",
          "Africa/Dakar",
          "Africa/Dar_es_Salaam",
          "Africa/Djibouti",
          "Africa/Douala",
          "Africa/El_Aaiun",
          "Africa/Freetown",
          "Africa/Gaborone",
          "Africa/Harare",
```

```
"Africa/Johannesburg",
"Africa/Juba",
"Africa/Kampala",
"Africa/Khartoum",
"Africa/Kigali",
"Africa/Kinshasa",
"Africa/Lagos",
"Africa/Libreville",
"Africa/Lome",
"Africa/Luanda",
"Africa/Lubumbashi",
"Africa/Lusaka",
"Africa/Malabo",
"Africa/Maputo",
"Africa/Maseru",
"Africa/Mbabane",
"Africa/Mogadishu",
"Africa/Monrovia",
"Africa/Nairobi",
"Africa/Ndjamena",
"Africa/Niamey",
"Africa/Nouakchott",
"Africa/Ouagadougou",
"Africa/Porto-Novo",
"Africa/Sao_Tome",
"Africa/Timbuktu",
"Africa/Tripoli",
"Africa/Tunis",
"Africa/Windhoek",
"America/Adak",
"America/Anchorage",
"America/Anguilla",
"America/Antigua",
"America/Araguaina",
"America/Argentina/Buenos_Aires",
"America/Argentina/Catamarca",
"America/Argentina/ComodRivadavia",
"America/Argentina/Cordoba",
"America/Argentina/Jujuy",
"America/Argentina/La_Rioja",
"America/Argentina/Mendoza",
"America/Argentina/Rio_Gallegos",
"America/Argentina/Salta",
"America/Argentina/San_Juan",
```

```
"America/Argentina/San_Luis",  
"America/Argentina/Tucuman",  
"America/Argentina/Ushuaia",  
"America/Aruba",  
"America/Asuncion",  
"America/Atikokan",  
"America/Atka",  
"America/Bahia",  
"America/Bahia_Banderas",  
"America/Barbados",  
"America/Belem",  
"America/Belize",  
"America/Blanc-Sablon",  
"America/Boa_Vista",  
"America/Bogota",  
"America/Boise",  
"America/Buenos_Aires",  
"America/Cambridge_Bay",  
"America/Campo_Grande",  
"America/Cancun",  
"America/Caracas",  
"America/Catamarca",  
"America/Cayenne",  
"America/Cayman",  
"America/Chicago",  
"America/Chihuahua",  
"America/Ciudad_Juarez",  
"America/Coral_Harbour",  
"America/Cordoba",  
"America/Costa_Rica",  
"America/Creston",  
"America/Cuiaba",  
"America/Curacao",  
"America/Danmarkshavn",  
"America/Dawson",  
"America/Dawson_Creek",  
"America/Denver",  
"America/Detroit",  
"America/Dominica",  
"America/Edmonton",  
"America/Eirunepe",  
"America/El_Salvador",  
"America/Ensenada",  
"America/Fort_Nelson",
```

```
"America/Fort_Wayne",
"America/Fortaleza",
"America/Glace_Bay",
"America/Godthab",
"America/Goose_Bay",
"America/Grand_Turk",
"America/Grenada",
"America/Guadeloupe",
"America/Guatemala",
"America/Guayaquil",
"America/Guyana",
"America/Halifax",
"America/Havana",
"America/Hermosillo",
"America/Indiana/Indianapolis",
"America/Indiana/Knox",
"America/Indiana/Marengo",
"America/Indiana/Petersburg",
"America/Indiana/Tell_City",
"America/Indiana/Vevay",
"America/Indiana/Vincennes",
"America/Indiana/Winamac",
"America/Indianapolis",
"America/Inuvik",
"America/Iqaluit",
"America/Jamaica",
"America/Jujuy",
"America/Juneau",
"America/Kentucky/Louisville",
"America/Kentucky/Monticello",
"America/Knox_IN",
"America/Kralendijk",
"America/La_Paz",
"America/Lima",
"America/Los_Angeles",
"America/Louisville",
"America/Lower_Princes",
"America/Maceio",
"America/Managua",
"America/Manaus",
"America/Marigot",
"America/Martinique",
"America/Matamoros",
"America/Mazatlan",
```



```
"America/Mendoza",
"America/Menominee",
"America/Merida",
"America/Metlakatla",
"America/Mexico_City",
"America/Miquelon",
"America/Moncton",
"America/Monterrey",
"America/Montevideo",
"America/Montreal",
"America/Montserrat",
"America/Nassau",
"America/New_York",
"America/Nipigon",
"America/Nome",
"America/Noronha",
"America/North_Dakota/Beulah",
"America/North_Dakota/Center",
"America/North_Dakota/New_Salem",
"America/Nuuk",
"America/Ojinaga",
"America/Panama",
"America/Pangnirtung",
"America/Paramaribo",
"America/Phoenix",
"America/Port-au-Prince",
"America/Port_of_Spain",
"America/Porto_Acre",
"America/Porto_Velho",
"America/Puerto_Rico",
"America/Punta_Arenas",
"America/Rainy_River",
"America/Rankin_Inlet",
"America/Recife",
"America/Regina",
"America/Resolute",
"America/Rio_Branco",
"America/Rosario",
"America/Santa_Isabel",
"America/Santarem",
"America/Santiago",
"America/Santo_Domingo",
"America/Sao_Paulo",
"America/Scoresbysund",
```

```
"America/Shiprock",
"America/Sitka",
"America/St_Barthelemy",
"America/St_Johns",
"America/St_Kitts",
"America/St_Lucia",
"America/St_Thomas",
"America/St_Vincent",
"America/Swift_Current",
"America/Tegucigalpa",
"America/Thule",
"America/Thunder_Bay",
"America/Tijuana",
"America/Toronto",
"America/Tortola",
"America/Vancouver",
"America/Virgin",
"America/Whitehorse",
"America/Winnipeg",
"America/Yakutat",
"America/Yellowknife",
"Antarctica/Casey",
"Antarctica/Davis",
"Antarctica/DumontDUrville",
"Antarctica/Macquarie",
"Antarctica/Mawson",
"Antarctica/McMurdo",
"Antarctica/Palmer",
"Antarctica/Rothera",
"Antarctica/South_Pole",
"Antarctica/Syowa",
"Antarctica/Troll",
"Antarctica/Vostok",
"Arctic/Longyearbyen",
"Asia/Aden",
"Asia/Almaty",
"Asia/Amman",
"Asia/Anadyr",
"Asia/Aqtau",
"Asia/Aqtobe",
"Asia/Ashgabat",
"Asia/Ashkhabad",
"Asia/Atyrau",
"Asia/Baghdad",
```

```
"Asia/Bahrain",
"Asia/Baku",
"Asia/Bangkok",
"Asia/Barnaul",
"Asia/Beirut",
"Asia/Bishkek",
"Asia/Brunei",
"Asia/Calcutta",
"Asia/Chita",
"Asia/Choibalsan",
"Asia/Chongqing",
"Asia/Chungking",
"Asia/Colombo",
"Asia/Dacca",
"Asia/Damascus",
"Asia/Dhaka",
"Asia/Dili",
"Asia/Dubai",
"Asia/Dushanbe",
"Asia/Famagusta",
"Asia/Gaza",
"Asia/Harbin",
"Asia/Hebron",
"Asia/Ho_Chi_Minh",
"Asia/Hong_Kong",
"Asia/Hovd",
"Asia/Irkutsk",
"Asia/Istanbul",
"Asia/Jakarta",
"Asia/Jayapura",
"Asia/Jerusalem",
"Asia/Kabul",
"Asia/Kamchatka",
"Asia/Karachi",
"Asia/Kashgar",
"Asia/Kathmandu",
"Asia/Katmandu",
"Asia/Khandyga",
"Asia/Kolkata",
"Asia/Krasnoyarsk",
"Asia/Kuala_Lumpur",
"Asia/Kuching",
"Asia/Kuwait",
"Asia/Macao",
```

```
"Asia/Macau",  
"Asia/Magadan",  
"Asia/Makassar",  
"Asia/Manila",  
"Asia/Muscat",  
"Asia/Nicosia",  
"Asia/Novokuznetsk",  
"Asia/Novosibirsk",  
"Asia/Omsk",  
"Asia/Oral",  
"Asia/Phnom_Penh",  
"Asia/Pontianak",  
"Asia/Pyongyang",  
"Asia/Qatar",  
"Asia/Qostanay",  
"Asia/Qyzylorda",  
"Asia/Rangoon",  
"Asia/Riyadh",  
"Asia/Saigon",  
"Asia/Sakhalin",  
"Asia/Samarkand",  
"Asia/Seoul",  
"Asia/Shanghai",  
"Asia/Singapore",  
"Asia/Srednekolymsk",  
"Asia/Taipei",  
"Asia/Tashkent",  
"Asia/Tbilisi",  
"Asia/Tehran",  
"Asia/Tel_Aviv",  
"Asia/Thimbu",  
"Asia/Thimphu",  
"Asia/Tokyo",  
"Asia/Tomsk",  
"Asia/Ujung_Pandang",  
"Asia/Ulaanbaatar",  
"Asia/Ulan_Bator",  
"Asia/Urumqi",  
"Asia/Ust-Nera",  
"Asia/Vientiane",  
"Asia/Vladivostok",  
"Asia/Yakutsk",  
"Asia/Yangon",  
"Asia/Yekaterinburg",
```

```
"Asia/Yerevan",
"Atlantic/Azores",
"Atlantic/Bermuda",
"Atlantic/Canary",
"Atlantic/Cape_Verde",
"Atlantic/Faeroe",
"Atlantic/Faroe",
"Atlantic/Jan_Mayen",
"Atlantic/Madeira",
"Atlantic/Reykjavik",
"Atlantic/South_Georgia",
"Atlantic/St_Helena",
"Atlantic/Stanley",
"Australia/ACT",
"Australia/Adelaide",
"Australia/Brisbane",
"Australia/Broken_Hill",
"Australia/Canberra",
"Australia/Currie",
"Australia/Darwin",
"Australia/Eucla",
"Australia/Hobart",
"Australia/LHI",
"Australia/Lindeman",
"Australia/Lord_Howe",
"Australia/Melbourne",
"Australia/NSW",
"Australia/North",
"Australia/Perth",
"Australia/Queensland",
"Australia/South",
"Australia/Sydney",
"Australia/Tasmania",
"Australia/Victoria",
"Australia/West",
"Australia/Yancowinna",
"Brazil/Acre",
"Brazil/DeNoronha",
"Brazil/East",
"Brazil/West",
"CET",
"CST6CDT",
"Canada/Atlantic",
"Canada/Central",
```

```
"Canada/Eastern",  
"Canada/Mountain",  
"Canada/Newfoundland",  
"Canada/Pacific",  
"Canada/Saskatchewan",  
"Canada/Yukon",  
"Chile/Continental",  
"Chile/EasterIsland",  
"Cuba",  
"EET",  
"EST5EDT",  
"Egypt",  
"Eire",  
"Etc/GMT",  
"Etc/GMT+0",  
"Etc/GMT+1",  
"Etc/GMT+10",  
"Etc/GMT+11",  
"Etc/GMT+12",  
"Etc/GMT+2",  
"Etc/GMT+3",  
"Etc/GMT+4",  
"Etc/GMT+5",  
"Etc/GMT+6",  
"Etc/GMT+7",  
"Etc/GMT+8",  
"Etc/GMT+9",  
"Etc/GMT-0",  
"Etc/GMT-1",  
"Etc/GMT-10",  
"Etc/GMT-11",  
"Etc/GMT-12",  
"Etc/GMT-13",  
"Etc/GMT-14",  
"Etc/GMT-2",  
"Etc/GMT-3",  
"Etc/GMT-4",  
"Etc/GMT-5",  
"Etc/GMT-6",  
"Etc/GMT-7",  
"Etc/GMT-8",  
"Etc/GMT-9",  
"Etc/GMT0",  
"Etc/Greenwich",
```

```
"Etc/UCT",  
"Etc/UTC",  
"Etc/Universal",  
"Etc/Zulu",  
"Europe/Amsterdam",  
"Europe/Andorra",  
"Europe/Astrakhan",  
"Europe/Athens",  
"Europe/Belfast",  
"Europe/Belgrade",  
"Europe/Berlin",  
"Europe/Bratislava",  
"Europe/Brussels",  
"Europe/Bucharest",  
"Europe/Budapest",  
"Europe/Busingen",  
"Europe/Chisinau",  
"Europe/Copenhagen",  
"Europe/Dublin",  
"Europe/Gibraltar",  
"Europe/Guernsey",  
"Europe/Helsinki",  
"Europe/Isle_of_Man",  
"Europe/Istanbul",  
"Europe/Jersey",  
"Europe/Kaliningrad",  
"Europe/Kiev",  
"Europe/Kirov",  
"Europe/Kyiv",  
"Europe/Lisbon",  
"Europe/Ljubljana",  
"Europe/London",  
"Europe/Luxembourg",  
"Europe/Madrid",  
"Europe/Malta",  
"Europe/Mariehamn",  
"Europe/Minsk",  
"Europe/Monaco",  
"Europe/Moscow",  
"Europe/Nicosia",  
"Europe/Oslo",  
"Europe/Paris",  
"Europe/Podgorica",  
"Europe/Prague",
```

```
"Europe/Riga",
"Europe/Rome",
"Europe/Samara",
"Europe/San_Marino",
"Europe/Sarajevo",
"Europe/Saratov",
"Europe/Simferopol",
"Europe/Skopje",
"Europe/Sofia",
"Europe/Stockholm",
"Europe/Tallinn",
"Europe/Tirane",
"Europe/Tiraspol",
"Europe/Ulyanovsk",
"Europe/Uzhgorod",
"Europe/Vaduz",
"Europe/Vatican",
"Europe/Vienna",
"Europe/Vilnius",
"Europe/Volgograd",
"Europe/Warsaw",
"Europe/Zagreb",
"Europe/Zaporozhye",
"Europe/Zurich",
"GB",
"GB-Eire",
"GMT",
"GMT0",
"Greenwich",
"Hongkong",
"Iceland",
"Indian/Antananarivo",
"Indian/Chagos",
"Indian/Christmas",
"Indian/Cocos",
"Indian/Comoro",
"Indian/Kerguelen",
"Indian/Mahe",
"Indian/Maldives",
"Indian/Mauritius",
"Indian/Mayotte",
"Indian/Reunion",
"Iran",
"Israel",
```



```
"Jamaica",
"Japan",
"Kwajalein",
"Libya",
"MET",
"MST7MDT",
"Mexico/BajaNorte",
"Mexico/BajaSur",
"Mexico/General",
"NZ",
"NZ-CHAT",
"Navajo",
"PRC",
"PST8PDT",
"Pacific/Apia",
"Pacific/Auckland",
"Pacific/Bougainville",
"Pacific/Chatham",
"Pacific/Chuuk",
"Pacific/Easter",
"Pacific/Efate",
"Pacific/Enderbury",
"Pacific/Fakaofu",
"Pacific/Fiji",
"Pacific/Funafuti",
"Pacific/Galapagos",
"Pacific/Gambier",
"Pacific/Guadalcanal",
"Pacific/Guam",
"Pacific/Honolulu",
"Pacific/Johnston",
"Pacific/Kanton",
"Pacific/Kiritimati",
"Pacific/Kosrae",
"Pacific/Kwajalein",
"Pacific/Majuro",
"Pacific/Marquesas",
"Pacific/Midway",
"Pacific/Nauru",
"Pacific/Niue",
"Pacific/Norfolk",
"Pacific/Noumea",
"Pacific/Pago_Pago",
"Pacific/Palau",
```

```
"Pacific/Pitcairn",
"Pacific/Pohnpei",
"Pacific/Ponape",
"Pacific/Port_Moresby",
"Pacific/Rarotonga",
"Pacific/Saipan",
"Pacific/Samoa",
"Pacific/Tahiti",
"Pacific/Tarawa",
"Pacific/Tongatapu",
"Pacific/Truk",
"Pacific/Wake",
"Pacific/Wallis",
"Pacific/Yap",
"Poland",
"Portugal",
"ROK",
"Singapore",
"SystemV/AST4",
"SystemV/AST4ADT",
"SystemV/CST6",
"SystemV/CST6CDT",
"SystemV/EST5",
"SystemV/EST5EDT",
"SystemV/HST10",
"SystemV/MST7",
"SystemV/MST7MDT",
"SystemV/PST8",
"SystemV/PST8PDT",
"SystemV/YST9",
"SystemV/YST9YDT",
"Turkey",
"UCT",
"US/Alaska",
"US/Aleutian",
"US/Arizona",
"US/Central",
"US/East-Indiana",
"US/Eastern",
"US/Hawaii",
"US/Indiana-Starke",
"US/Michigan",
"US/Mountain",
"US/Pacific",
```

```
    "US/Samoa",
    "UTC",
    "Universal",
    "W-SU",
    "WET",
    "Zulu",
    "EST",
    "HST",
    "MST",
    "ACT",
    "AET",
    "AGT",
    "ART",
    "AST",
    "BET",
    "BST",
    "CAT",
    "CNT",
    "CST",
    "CTT",
    "EAT",
    "ECT",
    "IET",
    "IST",
    "JST",
    "MIT",
    "NET",
    "NST",
    "PLT",
    "PNT",
    "PRT",
    "PST",
    "SST",
    "VST"
  ]
},
"pageRootPaths":
{
  "type": "array",
  "items":
  {
    "type": "string"
  }
},
},
```

```
"assetRootPaths":
{
  "type": "array",
  "items":
  {
    "type": "string"
  }
},
"crawlAssets":
{
  "type": "boolean"
},
"crawlPages":
{
  "type": "boolean"
},
"pagePathInclusionPatterns":
{
  "type": "array",
  "items":
  {
    "type": "string"
  }
},
"pagePathExclusionPatterns":
{
  "type": "array",
  "items":
  {
    "type": "string"
  }
},
"pageNameInclusionPatterns":
{
  "type": "array",
  "items":
  {
    "type": "string"
  }
},
"pageNameExclusionPatterns":
{
  "type": "array",
  "items":
```

```
    {
      "type": "string"
    }
  },
  "assetPathInclusionPatterns":
  {
    "type": "array",
    "items":
    {
      "type": "string"
    }
  },
  "assetPathExclusionPatterns":
  {
    "type": "array",
    "items":
    {
      "type": "string"
    }
  },
  "assetTypeInclusionPatterns":
  {
    "type": "array",
    "items":
    {
      "type": "string"
    }
  },
  "assetTypeExclusionPatterns":
  {
    "type": "array",
    "items":
    {
      "type": "string"
    }
  },
  "assetNameInclusionPatterns":
  {
    "type": "array",
    "items":
    {
      "type": "string"
    }
  },
},
```

```
"assetNameExclusionPatterns":
{
  "type": "array",
  "items":
  {
    "type": "string"
  }
},
"pageComponents": {
  "type": "array",
  "items": {
    "type": "object"
  }
},
"contentFragmentVariations": {
  "type": "array",
  "items": {
    "type": "object"
  }
},
"cugExemptedPrincipals": {
  "type": "array",
  "items": {
    "type": "string"
  }
}
},
"required":
[]
},
"type": {
  "type": "string",
  "pattern": "AEM"
},
"enableIdentityCrawler": {
  "type": "boolean"
},
"syncMode": {
  "type": "string",
  "enum": [
    "FORCED_FULL_CRAWL",
    "FULL_CRAWL",
    "CHANGE_LOG"
  ]
}
```

```

    },
    "secretArn": {
      "type": "string",
      "minLength": 20,
      "maxLength": 2048
    }
  },
  "version": {
    "type": "string",
    "anyOf": [
      {
        "pattern": "1.0.0"
      }
    ]
  },
  "required": [
    "connectionConfiguration",
    "repositoryConfigurations",
    "syncMode",
    "additionalProperties",
    "secretArn",
    "type"
  ]
}

```

Amazon FSx (視窗) 範本結構

您可以將包含資料來源結構描述的 JSON 納入為 [TemplateConfiguration](#) 物件的一部分。您可以提供檔案系統 ID 做為連線組態或存放庫端點詳細資料的一部分。您也必須將資料來源類型指定為 FSX、驗證認證的密碼，以及其他必要的組態。然後，您將指定 TEMPLATE 為呼叫 Type 時 [CreateDataSource](#)。

您可以使用本開發人員指南中提供的模板。請參閱 [Amazon FSx \(視窗\) 結構定義](#)。

下表說明 Amazon FSx (視窗) JSON 結構定義的參數。

組態	描述
連線組態	資料來源端點的組態資訊。
repositoryEndpointMetadata	資料來源的端點資訊。

組態	描述
fileSystemId	Amazon FSx 檔案系統的識別碼。您可以在 Amazon FSx 主控台的 [檔案系統] 儀表板上找到您的檔案系統 ID。
fileSystemType	Amazon FSx 檔案系統類型。若要用 Windows File Server 作您的檔案系統類型，請指定 WINDOWS。
儲存庫組態	資料來源內容的組態資訊。例如，配置特定類型的內容和欄位對應。
全部	將 Amazon FSx 資料來源中檔案的屬性或欄位名稱對映至 Amazon Kendra 索引欄位名稱的物件清單。如需詳細資訊，請參閱 映射資料來源欄位 。
附加屬性	資料來源中內容的其他組態選項。
isCrawlAcl	true 以編目文件的存取控制清單 (ACL) 資訊，如果您有 ACL，並且想要將其用於存取控制。ACL 會指定使用者和群組可存取的文件。ACL 資訊可用來根據使用者或使用者對文件的群組存取權來篩選搜尋結果。如需詳細資訊，請參閱 使用者內容篩選 。
包含模式	在 Amazon FSx 資料來源中包含某些檔案的規則運算式模式清單。符合模式的檔案會包括在索引中。不符合模式的檔案會從索引中排除。如果檔案同時符合包括模式和排除模式，則以排除模式為優先，且該項目不會包括在索引中。
排除模式	用於排除 Amazon FSx 資料來源中某些檔案的規則運算式模式清單。符合模式的檔案會從索引中排除。與模式不匹配的文件包含在索引中。如果檔案同時符合排除和包含模式，則排除模式優先，且檔案不會包含在索引中。

組態	描述
enableIdentityCrawler	true，以使用 Amazon Kendra 的身分識別爬行者程式來同步使用者和群組的身分識別/主體資訊，以存取特定文件。如果關閉身分搜索器，則可以公開搜索所有文檔。如果您想要對文件使用存取控制，且身分識別編目程式已關閉，您也可以使用 PutPrincipalMapping API 來上傳使用者和群組存取資訊。
同步模式	指定資料來源內容變更時 Amazon Kendra 應如何更新索引。您可以選擇： <ul style="list-style-type: none"> FORCED_FULL_CRAWL 新建索引所有內容，並在每次資料來源與索引同步時取代現有內容。 FULL_CRAWL，每次您的資料來源與索引同步時，僅對新的、修改和刪除的內容建立索引。Amazon Kendra 可以使用資料來源的機制來追蹤內容變更，並為上次同步後變更的內容建立索引。
type	資料來源的類型。對於 Windows 檔案系統資料來源，請指定 FSX。

Amazon FSx (視窗) 結構定義

```
{
  "$schema": "http://json-schema.org/draft-04/schema#",
  "type": "object",
  "properties": {
    "connectionConfiguration": {
      "type": "object",
      "properties": {
        "repositoryEndpointMetadata": {
          "type": "object",
          "properties": {
            "filesystemId": {
              "type": "string",
```

```
        "pattern": "fs-.*"
      },
      "fileSystemType": {
        "type": "string",
        "pattern": "WINDOWS"
      }
    },
    "required": ["fileSystemId", "fileSystemType"]
  }
},
"repositoryConfigurations": {
  "type": "object",
  "properties": {
    "All": {
      "type": "object",
      "properties": {
        "fieldMappings": {
          "type": "array",
          "items": [
            {
              "type": "object",
              "properties": {
                "indexFieldName": {
                  "type": "string"
                },
                "indexFieldType": {
                  "type": "string",
                  "enum": ["STRING", "STRING_LIST", "DATE"]
                },
                "dataSourceFieldName": {
                  "type": "string"
                },
                "dateFieldFormat": {
                  "type": "string",
                  "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                }
              }
            }
          ]
        },
        "required": [
          "indexFieldName",
          "indexFieldType",
          "dataSourceFieldName"
        ]
      }
    }
  }
}
```

```
        ]
      }
    },
    "required": ["fieldMappings"]
  }
},
"required": ["All"]
},
"additionalProperties": {
  "type": "object",
  "properties": {
    "isCrawlAcl": {
      "type": "boolean"
    },
    "exclusionPatterns": {
      "type": "array",
      "items": {
        "type": "string"
      }
    },
    "inclusionPatterns": {
      "type": "array",
      "items": {
        "type": "string"
      }
    }
  },
  "required": []
},
"enableIdentityCrawler": {
  "type": "boolean"
},
"syncMode": {
  "type": "string",
  "enum": [
    "FORCED_FULL_CRAWL",
    "FULL_CRAWL"
  ]
},
"type" : {
  "type" : "string",
  "pattern": "FSX"
}
},
```

```

"version": {
  "type": "string",
  "anyOf": [
    {
      "pattern": "1.0.0"
    }
  ]
},
"required": [
  "connectionConfiguration",
  "repositoryConfigurations",
  "syncMode",
  "enableIdentityCrawler",
  "additionalProperties",
  "type"
]
}

```

Amazon FSx (NetApp ONTAP) 範本結構描述

您可以將包含資料來源結構描述的 JSON 納入為 [TemplateConfiguration](#) 物件的一部分。您可以提供檔案系統識別碼和儲存區虛擬機器 (SVM) 做為連線組態或存放庫端點詳細資料的一部分。您也必須將資料來源類型指定為 FSXONTAP、驗證認證的密碼，以及其他必要的組態。然後，您將指定 TEMPLATE 為呼叫 Type 時 [CreateDataSource](#)。

您可以使用本開發人員指南中提供的模板。請參閱 [Amazon FSx JSON 結構定義 NetApp](#)。

下表說明 Amazon FSx (NetApp ONTAP) JSON 結構定義的參數。

組態	描述
連線組態	資料來源端點的組態資訊。
repositoryEndpointMetadata	資料來源的端點資訊。
fileSystemId	Amazon FSx 檔案系統的識別碼。您可以在 Amazon FSx 主控台的 [檔案系統] 儀表板上找到您的檔案系統 ID。如需如何在 Amazon FSx 主控台中為 NetApp ONTAP 建立檔案系統的詳細資訊，請參閱 使 FSx for ONTAP 用者指南中的 NetApp ONTAP 入門指南 。

組態	描述
fileSystemType	Amazon FSx 檔案系統類型。若要用 NetApp ONTAP 作您的檔案系統類型，請指定 ONTAP。
SVMid	與 Amazon FSx 檔案系統搭配使用的儲存區虛擬機器 (SVM) 識別碼。NetApp ONTAP 您可以移至 Amazon FSx 主控台中的 [檔案系統] 儀表板，選取您的檔案系統 ID，然後選取 [儲存區虛擬機器]，以尋找您的 SVM ID。如需如何在的 Amazon FSx 主控台中建立檔案系統的詳細資訊 NetApp ONTAP，請參閱 使用指南中的 NetApp ONTAP 入門FSx for ONTAP 指南。
通訊協定型態	您是否使用 Windows 的通用網際網路檔案系統 (CIFS) 通訊協定，還是使用 Linux 的網路檔案系統 (NFS) 通訊協定。
儲存庫組態	資料來源內容的組態資訊。例如，配置特定類型的內容和欄位對應。
file	將 Amazon FSx 資料來源中檔案的屬性或欄位名稱對映至 Amazon Kendra 索引欄位名稱的物件清單。如需詳細資訊，請參閱 映射資料來源欄位 。資料來源欄位名稱必須存在於檔案自訂中繼資料中。
附加屬性	資料來源中內容的其他組態選項。
克勞拉克	true 以編目文件的存取控制清單 (ACL) 資訊，如果您有 ACL，並且想要將其用於存取控制。ACL 會指定使用者和群組可存取的文件。ACL 資訊可用來根據使用者或使用者對文件的群組存取權來篩選搜尋結果。如需詳細資訊，請參閱 使用者內容篩選 。

組態	描述
包含模式	<p>在 Amazon FSx 資料來源中包含某些檔案的規則運算式模式清單。符合模式的檔案會包括在索引中。不符合模式的檔案會從索引中排除。如果檔案同時符合包括模式和排除模式，則以排除模式為優先，且該項目不會包括在索引中。</p>
排除模式	<p>用於排除 Amazon FSx 資料來源中某些檔案的規則運算式模式清單。符合模式的檔案會從索引中排除。與模式不匹配的文件包含在索引中。如果檔案同時符合排除和包含模式，則排除模式優先，且檔案不會包含在索引中。</p>
type	<p>資料來源的類型。對於 NetApp ONTAP 檔案系統資料來源，請指定 FSXONTAP。</p>
同步模式	<p>指定資料來源內容變更時 Amazon Kendra 應如何更新索引。您可以選擇：</p> <ul style="list-style-type: none"> • <code>FORCED_FULL_CRAWL</code> 新建索引所有內容，並在每次資料來源與索引同步時取代現有內容。 • <code>FULL_CRAWL</code>，每次您的資料來源與索引同步時，僅對新的、修改和刪除的內容建立索引。Amazon Kendra 可以使用資料來源的機制來追蹤內容變更，並為上次同步後變更的內容建立索引。

組態	描述
秘書	<p>AWS Secrets Manager 密碼的 Amazon 資源名稱 (ARN)，其中包含連線到 Amazon FSx 檔案系統所需的金鑰值配對。私密必須包含具有下列索引鍵的 JSON 結構：</p> <pre data-bbox="829 443 1507 680"> { "username": " <i>user@corp.example.com</i> ", "password": " <i>password</i>" } </pre> <p>如果您的 Amazon FSx 檔案系統使用 NFS 通訊協定，密碼會以下列金鑰儲存在 JSON 結構中：</p> <pre data-bbox="829 884 1507 1121"> { "leftId": " <i>left ID</i>", "rightId": " <i>right ID</i>", "preSharedKey": " <i>pre-shared key</i> " } </pre>

Amazon FSx JSON 結構定義 NetApp

```

{
  "$schema": "http://json-schema.org/draft-04/schema#",
  "type": "object",
  "properties": {
    "connectionConfiguration": {
      "type": "object",
      "properties": {
        "repositoryEndpointMetadata": {
          "type": "object",
          "properties": {
            "filesystemId": {
              "type": "string",
              "pattern": "^(fs-[0-9a-f]{8,21})$"
            },
          },
        },
      },
    },
  },
}

```

```

    "fileSystemType": {
      "type": "string",
      "enum": ["ONTAP"]
    },
    "svmId": {
      "type": "string",
      "pattern": "^(svm-[0-9a-f]{17,21})$"
    },
    "protocolType": {
      "type": "string",
      "enum": [
        "CIFS",
        "NFS"
      ]
    }
  },
  "required": [
    "fileSystemId",
    "fileSystemType"
  ]
},
"required": [
  "repositoryEndpointMetadata"
],
"repositoryConfigurations": {
  "type": "object",
  "properties": {
    "file": {
      "type": "object",
      "properties": {
        "fieldMappings": {
          "type": "array",
          "items": [
            {
              "type": "object",
              "properties": {
                "indexFieldName": {
                  "type": "string",
                  "pattern": "^[a-zA-Z_]{1,20}$"
                },
                "indexFieldType": {
                  "type": "string",

```



```
        "enum": [
            "STRING",
            "STRING_LIST",
            "DATE",
            "LONG"
        ]
    },
    "dataSourceFieldName": {
        "type": "string",
        "pattern": "^[a-zA-Z_]{1,20}$"
    },
    "dateFieldFormat": {
        "type": "string",
        "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
    }
},
"required": [
    "indexFieldName",
    "indexFieldType",
    "dataSourceFieldName"
]
}
],
"maxItems": 50
}
},
"required": [
    "fieldMappings"
]
}
},
"required": [
    "file"
]
},
"additionalProperties": {
    "type": "object",
    "properties": {
        "crawlAcl": {
            "type": "boolean"
        },
        "inclusionPatterns": {
            "type": "array",
            "items": {
```

```
        "type": "string",
        "maxLength": 30
    },
    "maxItems": 100
},
"exclusionPatterns": {
    "type": "array",
    "items": {
        "type": "string",
        "maxLength": 30
    },
    "maxItems": 100
}
}
},
"type": {
    "type": "string",
    "pattern": "FSXONTAP"
},
"syncMode": {
    "type": "string",
    "enum": [
        "FORCED_FULL_CRAWL",
        "FULL_CRAWL"
    ]
},
"secretArn": {
    "type": "string",
    "pattern": "arn:aws:secretsmanager:.*"
}
},
"required": [
    "connectionConfiguration",
    "repositoryConfigurations",
    "additionalProperties",
    "secretArn",
    "type"
]
}
```

Alfresco 模板架構

您可以將包含資料來源結構描述的 JSON 納入為 [TemplateConfiguration](#) 物件的一部分。您可以提供 Alfresco 網站 ID、存放庫 URL、使用者介面 URL、驗證類型、無論您使用雲端還是內部部署，以及要編目的內容類型。您可以提供此連線組態或存放庫端點詳細資料的一部分。同時將資料來源類型指定為 ALFRESCO、驗證認證的密碼，以及其他必要的組態。然後，您將指定 TEMPLATE 為呼叫 Type 時 [CreateDataSource](#)。

您可以使用本開發人員指南中提供的模板。請參閱 [Alfresco 結構定義](#)。

下表說明露天 JSON 結構定義的參數。

組態	描述
連線組態	資料來源端點的組態資訊。
repositoryEndpointMetadata	資料來源的端點資訊。
網站 ID	露天網站的標識符。
回味	Alfresco 儲存庫的網址。您可以向 Alfresco 管理員取得存放庫 URL。例如，如果您使用 Alfresco 雲端 (PaaS)，則存放庫 URL 可能是 <code>https://company.alfrescocloud.com</code> 。或者，如果您使用 Alfresco 內部部署，則存放庫 URL 可能是 <code>https://company-alfresco-instance.company-domain.suffix:port</code> 。
webAppUrl	您的 Alfresco 使用者介面的 URL。您可以從 Alfresco 管理員取得 Alfresco 使用者介面 URL。例如，使用者介面網址可以是 <code>https://example.com</code> 。
repositoryAdditionalProperties	與儲存庫/資料來源端點連線的其他內容。
authType	您使用的驗證類型，無論是 OAuth2 或 Basic。
類型 (部署)	您使用 Alfresco 的類型，無論是 PAAS 或 ON-PREM。

組態	描述
爬行型	您要搜索的內容類型，無論是ASPECT（在中標有「面向」的內容Alfresco），SITE_ID（特定Alfresco網站內的內容）還是ALL_SITES（您所有網Alfresco站上的內容）。
儲存庫組態	資料來源內容的組態資訊。例如，配置特定類型的內容和欄位對應。
<ul style="list-style-type: none"> • 文件 • comment 	將 Alfresco 文檔的屬性或字段名稱和注釋映射到 Amazon Kendra 索引字段名稱的對象列表。如需詳細資訊，請參閱 映射資料來源欄位 。
附加屬性	資料來源中內容的其他組態選項。
方面名稱	您要索引的特定「方面」的名稱。
方面屬性	您要索引的特定「縱橫」內容屬性的列表。
enableFineGrained控制	true爬行「方面」。
isCrawlComment	true抓取評論。
<ul style="list-style-type: none"> • inclusionFileName模式 • inclusionFileType模式 • inclusionFilePath模式 	在Alfresco資料來源中包含某些檔案的規則運算式模式清單。符合模式的檔案會包括在索引中。不符合模式的檔案會從索引中排除。如果檔案同時符合包含模式和排除模式，則排除模式優先，且檔案不會包含在索引中。
<ul style="list-style-type: none"> • exclusionFileName模式 • exclusionFileType模式 • exclusionFilePath模式 	用於排除Alfresco資料來源中某些檔案的規則運算式模式清單。符合模式的檔案會從索引中排除。與模式不匹配的文件包含在索引中。如果檔案同時符合包含模式和排除模式，則排除模式優先，且檔案不會包含在索引中。
type	資料來源的類型。指定ALFRESCO為您的資料來源類型。

組態	描述
秘书	<p>Amazon 資源名稱 (ARN) 的 AWS Secrets Manager 秘密，其中包含連接到 Alfresco 私密必須包含具有下列索引鍵的 JSON 結構：</p> <p>如果使用基本驗證：</p> <pre data-bbox="831 472 1507 672"> { "username": " <i>user name</i>", "password": " <i>password</i>" } </pre> <p>如果使用 OAuth 2.0 身份驗證：</p> <pre data-bbox="831 781 1507 1018"> { "clientId": " <i>client ID</i>", "clientSecret": " <i>client secret</i>", "tokenUrl": " <i>token URL</i>" } </pre>
同步模式	<p>指定資料來源內容變更時 Amazon Kendra 應如何更新索引。您可以選擇：</p> <ul data-bbox="831 1186 1507 1564" style="list-style-type: none"> • <code>FORCED_FULL_CRAWL</code> 新建索引所有內容，並在每次資料來源與索引同步時取代現有內容。 • <code>FULL_CRAWL</code> ，每次您的資料來源與索引同步時，僅對新的、修改和刪除的內容建立索引。Amazon Kendra 可以使用資料來源的機制來追蹤內容變更，並為上次同步後變更的內容建立索引。

組態	描述
enableIdentityCrawler	true，以使用 Amazon Kendra 的身分識別爬行者程式來同步使用者和群組的身分識別/主體資訊，以存取特定文件。如果關閉身分搜索器，則可以公開搜索所有文檔。如果您想要對文件使用存取控制，且身分識別編目程式已關閉，您也可以使用 PutPrincipalMapping API 來上傳使用者和群組存取資訊。
version	目前支援的此範本版本。

Alfresco 結構定義

```
{
  "$schema": "http://json-schema.org/draft-04/schema#",
  "type": "object",
  "properties": {
    "connectionConfiguration": {
      "type": "object",
      "properties": {
        "repositoryEndpointMetadata": {
          "type": "object",
          "properties": {
            "siteId": {
              "type": "string"
            },
            "repoUrl": {
              "type": "string"
            },
            "webAppUrl": {
              "type": "string"
            }
          }
        },
        "repositoryAdditionalProperties": {
          "type": "object",
          "properties": {
            "authType": {
              "type": "string",
              "enum": [
                "OAuth2",
                "Basic"
              ]
            }
          }
        }
      }
    }
  }
}
```

```
    ]
  },
  "type": {
    "type": "string",
    "enum": [
      "PAAS",
      "ON_PREM"
    ]
  },
  "crawlType": {
    "type": "string",
    "enum": [
      "ASPECT",
      "SITE_ID",
      "ALL_SITES"
    ]
  }
}
}
}
}
},
"required": [
  "repositoryEndpointMetadata"
]
},
"repositoryConfigurations": {
  "type": "object",
  "properties": {
    "document": {
      "type": "object",
      "properties": {
        "fieldMappings": {
          "type": "array",
          "items": {
            "anyOf": [
              {
                "type": "object",
                "properties": {
                  "indexFieldName": {
                    "type": "string"
                  },
                },
                "indexFieldType": {
                  "type": "string",

```

```
        "enum": [
          "STRING",
          "DATE",
          "STRING_LIST",
          "LONG"
        ],
      },
      "dataSourceFieldName": {
        "type": "string"
      },
      "dateFieldFormat": {
        "type": "string",
        "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
      }
    },
    "required": [
      "indexFieldName",
      "indexFieldType",
      "dataSourceFieldName"
    ]
  }
]
}
},
"required": [
  "fieldMappings"
],
"comment": {
  "type": "object",
  "properties": {
    "fieldMappings": {
      "type": "array",
      "items": {
        "anyOf": [
          {
            "type": "object",
            "properties": {
              "indexFieldName": {
                "type": "string"
              },
            },
            "indexFieldType": {
              "type": "string",
            }
          }
        ]
      }
    }
  }
}
```



```
        "enum": [
            "STRING",
            "DATE",
            "STRING_LIST",
            "LONG"
        ],
    },
    "dataSourceFieldName": {
        "type": "string"
    },
    "dateFieldFormat": {
        "type": "string",
        "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
    }
},
"required": [
    "indexFieldName",
    "indexFieldType",
    "dataSourceFieldName"
]
}
]
}
},
"required": [
    "fieldMappings"
]
}
},
"additionalProperties": {
    "type": "object",
    "properties": {
        "aspectName": {
            "type": "string"
        },
        "aspectProperties": {
            "type": "array"
        },
        "enableFineGrainedControl": {
            "type": "boolean"
        },
        "isCrawlComment": {
```

```
    "type": "boolean"
  },
  "inclusionFileNamePatterns": {
    "type": "array"
  },
  "exclusionFileNamePatterns": {
    "type": "array"
  },
  "inclusionFileTypePatterns": {
    "type": "array"
  },
  "exclusionFileTypePatterns": {
    "type": "array"
  },
  "inclusionFilePathPatterns": {
    "type": "array"
  },
  "exclusionFilePathPatterns": {
    "type": "array"
  }
}
},
"type": {
  "type": "string",
  "pattern": "ALFRESCO"
},
"secretArn": {
  "type": "string",
  "minLength": 20,
  "maxLength": 2048
},
"syncMode": {
  "type": "string",
  "enum": [
    "FORCED_FULL_CRAWL",
    "FULL_CRAWL"
  ]
},
"enableIdentityCrawler": {
  "type": "boolean"
},
"version": {
  "type": "string",
  "anyOf": [
```

```

    {
      "pattern": "1.0.0"
    }
  ]
},
"required": [
  "connectionConfiguration",
  "repositoryConfigurations",
  "additionalProperties",
  "type",
  "secretArn"
]
}

```

Aurora (MySQL) 模板架構

您可以將包含資料來源結構描述的 JSON 納入為 [TemplateConfiguration](#) 物件的一部分。將資料來源的類型指定為 JDBC、資料庫類型為 mysql、驗證認證的密碼，以及其他必要的組態。然後，您將指定 TEMPLATE 為呼叫 Type 時 [CreateDataSource](#)。

您可以使用本開發人員指南中提供的模板。請參閱 [Aurora \(MySQL\) 結構描述](#)。

下表說明 Aurora (MySQL) JSON 結構定義的參數。

組態	描述
連線組態	資料來源端點的組態資訊。
repositoryEndpointMetadata	連線資料來源所需的組態資訊。 <ul style="list-style-type: none"> 資料庫類型-您使用的 Java 資料庫類型 (無論是 mysql、db2、postgresql oracle、或)。sqlserver 資料庫主機 — 資料庫主機名稱。 資料庫埠 — 資料庫連接埠。 資料庫實例 — 資料庫執行處理。

組態	描述
儲存庫組態	資料來源內容的組態資訊。例如，配置特定類型的內容和欄位對應。指定資料來源的類型和秘密 ARN。
文件	將資料庫內容的屬性或欄位名稱對應至 Amazon Kendra 索引欄位名稱的物件清單。如需詳細資訊，請參閱 映射資料來源欄位 。
附加屬性	資料來源中內容的其他組態選項。用於在資料庫資料來源中包含或排除特定內容。
主要金鑰	提供資料庫表格的主索引鍵。這標識數據庫中的一個表。
標題欄	提供資料庫表格中文件標題欄的名稱。
身體專欄	提供資料庫表格中文件標題欄的名稱。
sqlQuery	輸入 SQL 查詢語句，如選擇和連接操作。SQL 查詢必須小於 32 KB。Amazon Kendra 會編目符合您查詢的所有資料庫內容。
時間戳記列	輸入包含時間戳記的列的名稱。Amazon Kendra 使用時間戳記資訊偵測內容中的變更，並僅同步變更的內容。
時間戳記格式	輸入包含時間戳記格式的資料欄名稱，可用來偵測內容變更並重新同步處理內容。
timezone	輸入包含要探索之內容之時區的資料欄名稱。
changeDetectingColumns	輸入 Amazon Kendra 將用來偵測內容變更的欄名稱。Amazon Kendra 當這些列中的任何一個更改時，將重新索引內容
allowedUsersColumns	輸入包含允許存取內容之使用者 ID 的欄名稱。
allowedGroupsColumn	輸入包含允許存取內容之使用者 ID 的欄名稱。

組態	描述
來源尿酸氧胺	輸入包含要編製索引之來源 URL 的資料欄名稱。
isSslEnabled	輸入 SQL 查詢語句，如選擇和連接操作。SQL 查詢必須小於 32 KB。Amazon Kendra 會編目符合您查詢的所有資料庫內容。
type	資料來源的類型。指定JDBC為您的資料來源類型。
同步模式	<p>指定資料來源內容變更時 Amazon Kendra 應如何更新索引。您可以選擇：</p> <ul style="list-style-type: none"> • FORCED_FULL_CRAWL 新建索引所有內容，並在每次資料來源與索引同步時取代現有內容。 • FULL_CRAWL ，每次您的資料來源與索引同步時，僅對新的、修改和刪除的內容建立索引。Amazon Kendra 可以使用資料來源的機制來追蹤內容變更，並為上次同步後變更的內容建立索引。 • CHANGE_LOG 每次資料來源與索引同步時，僅對新內容和修改的內容建立索引。Amazon Kendra 可以使用資料來源的機制來追蹤內容變更，並為上次同步後變更的內容建立索引。
秘密	<p>秘密 Secrets Manager 密碼的 Amazon 資源名稱 (ARN)，其中包含連線到資料庫所需的使用者名稱和密碼。秘密必須包含具有下列索引鍵的 JSON 結構：</p> <pre data-bbox="829 1629 1507 1829"> { "user name": "database user name", "password": " password" } </pre>

組態	描述
version	目前支援的範本版本。

Aurora (MySQL) 結構描述

```
{
  "$schema": "http://json-schema.org/draft-04/schema#",
  "type": "object",
  "properties": {
    "connectionConfiguration": {
      "type": "object",
      "properties": {
        "repositoryEndpointMetadata": {
          "type": "object",
          "properties": {
            "dbType": {
              "type": "string",
              "enum": [
                "mysql",
                "db2",
                "postgresql",
                "oracle",
                "sqlserver"
              ]
            },
            "dbHost": {
              "type": "string"
            },
            "dbPort": {
              "type": "string"
            },
            "dbInstance": {
              "type": "string"
            }
          },
          "required": [
            "dbType",
            "dbHost",
            "dbPort",
            "dbInstance"
          ]
        }
      }
    }
  }
}
```

```
    }
  },
  "required": [
    "repositoryEndpointMetadata"
  ]
},
"repositoryConfigurations": {
  "type": "object",
  "properties": {
    "document": {
      "type": "object",
      "properties": {
        "fieldMappings": {
          "type": "array",
          "items": [
            {
              "type": "object",
              "properties": {
                "indexFieldName": {
                  "type": "string"
                },
                "indexFieldType": {
                  "type": "string"
                },
                "dataSourceFieldName": {
                  "type": "string"
                }
              }
            },
            {
              "type": "object",
              "properties": {
                "indexFieldName": {
                  "type": "string"
                },
                "indexFieldType": {
                  "type": "string"
                },
                "dataSourceFieldName": {
                  "type": "string"
                }
              }
            }
          ]
        }
      }
    }
  },
  "required": [
    "fieldMappings"
  ]
}
},
"required": [
  "fieldMappings"
]
```

```
},
"additionalProperties": {
  "type": "object",
  "properties": {
    "primaryKey": {
      "type": "string"
    },
    "titleColumn": {
      "type": "string"
    },
    "bodyColumn": {
      "type": "string"
    },
    "sqlQuery": {
      "type": "string",
      "not": {
        "pattern": ";+"
      }
    },
    "timestampColumn": {
      "type": "string"
    },
    "timestampFormat": {
      "type": "string"
    },
    "timezone": {
      "type": "string"
    },
    "changeDetectingColumns": {
      "type": "array",
      "items": {
        "type": "string"
      }
    },
    "allowedUsersColumn": {
      "type": "string"
    },
    "allowedGroupsColumn": {
      "type": "string"
    },
    "sourceURIColumn": {
      "type": "string"
    },
    "isSslEnabled": {
```



```
        "type": "boolean"
    }
},
"required": ["primaryKey", "titleColumn", "bodyColumn", "sqlQuery"]
},
"type" : {
    "type" : "string",
    "pattern": "JDBC"
},
"syncMode": {
    "type": "string",
    "enum": [
        "FORCED_FULL_CRAWL",
        "FULL_CRAWL",
        "CHANGE_LOG"
    ]
},
"secretArn": {
    "type": "string"
}
},
"version": {
    "type": "string",
    "anyOf": [
        {
            "pattern": "1.0.0"
        }
    ]
},
"required": [
    "connectionConfiguration",
    "repositoryConfigurations",
    "syncMode",
    "additionalProperties",
    "secretArn",
    "type"
]
}
```

Aurora 模板模板架構

您可以將包含資料來源結構描述的 JSON 納入為 [TemplateConfiguration](#) 物件的一部分。將資料來源的類型指定為 JDBC、資料庫類型為 postgresql、驗證認證的密碼，以及其他必要的組態。然後，您將指定 TEMPLATE 為呼叫 Type 時 [CreateDataSource](#)。

您可以使用本開發人員指南中提供的模板。請參閱 [Aurora JSON 結構描述](#)。

下表說明 Aurora (PostgreSQL) JSON 結構描述的參數。

組態	描述
連線組態	資料來源端點的組態資訊。
repositoryEndpointMetadata	連線資料來源所需的組態資訊。 <ul style="list-style-type: none"> • 資料庫類型-您使用的 Java 資料庫類型 (無論是mysql、db2、postgresql oracle、或)。sqlserver • 資料庫主機 — 資料庫主機名稱。 • 資料庫埠 — 資料庫連接埠。 • 資料庫實例 — 資料庫執行處理。
儲存庫組態	資料來源內容的組態資訊。例如，配置特定類型的內容和欄位對應。指定資料來源的類型和秘密 ARN。
文件	將資料庫內容的屬性或欄位名稱對應至 Amazon Kendra 索引欄位名稱的物件清單。如需詳細資訊，請參閱 映射資料來源欄位 。
附加屬性	資料來源中內容的其他組態選項。用於在資料庫資料來源中包含或排除特定內容。
主要金鑰	提供資料庫表格的主索引鍵。這標識數據庫中的一個表。
標題欄	提供資料庫表格中文件標題欄的名稱。

組態	描述
身體專欄	提供資料庫表格中文件標題欄的名稱。
sqlQuery	輸入 SQL 查詢語句，如選擇和連接操作。SQL 查詢必須小於 32 KB。Amazon Kendra 會編目符合您查詢的所有資料庫內容。
時間戳記列	輸入包含時間戳記的列的名稱。Amazon Kendra 使用時間戳記資訊偵測內容中的變更，並僅同步變更的內容。
時間戳記格式	輸入包含時間戳記格式的資料欄名稱，可用來偵測內容變更並重新同步處理內容。
timezone	輸入包含要探索之內容之時區的資料欄名稱。
changeDetectingColumns	輸入 Amazon Kendra 將用來偵測內容變更的欄名稱。Amazon Kendra 當這些列中的任何一個更改時，將重新索引內容
allowedUsersColumns	輸入包含允許存取內容之使用者 ID 的欄名稱。
allowedGroupsColumn	輸入包含允許存取內容之使用者 ID 的欄名稱。
來源尿酸氧胺	輸入包含要編製索引之來源 URL 的資料欄名稱。
isSslEnabled	輸入 SQL 查詢語句，如選擇和連接操作。SQL 查詢必須小於 32 KB。Amazon Kendra 會編目符合您查詢的所有資料庫內容。
type	資料來源的類型。指定JDBC為您的資料來源類型。

組態	描述
同步模式	<p>指定資料來源內容變更時 Amazon Kendra 應如何更新索引。您可以選擇：</p> <ul style="list-style-type: none"> • FORCED_FULL_CRAWL 新建索引所有內容，並在每次資料來源與索引同步時取代現有內容。 • FULL_CRAWL ，每次您的資料來源與索引同步時，僅對新的、修改和刪除的內容建立索引。Amazon Kendra 可以使用資料來源的機制來追蹤內容變更，並為上次同步後變更的內容建立索引。 • CHANGE_LOG 每次資料來源與索引同步時，僅對新內容和修改的內容建立索引。Amazon Kendra 可以使用資料來源的機制來追蹤內容變更，並為上次同步後變更的內容建立索引。
秘書	<p>秘密 Secrets Manager 密碼的 Amazon 資源名稱 (ARN)，其中包含連線到資料庫所需的使用者名稱和密碼。私密必須包含具有下列索引鍵的 JSON 結構：</p> <pre data-bbox="829 1192 1507 1394"> { "user name": "database user name", "password": "password" } </pre>
version	目前支援的範本版本。

Aurora JSON 結構描述

```

{
  "$schema": "http://json-schema.org/draft-04/schema#",
  "type": "object",
  "properties": {
    "connectionConfiguration": {
      "type": "object",

```

```
"properties": {
  "repositoryEndpointMetadata": {
    "type": "object",
    "properties": {
      "dbType": {
        "type": "string",
        "enum": [
          "mysql",
          "db2",
          "postgresql",
          "oracle",
          "sqlserver"
        ]
      },
      "dbHost": {
        "type": "string"
      },
      "dbPort": {
        "type": "string"
      },
      "dbInstance": {
        "type": "string"
      }
    },
    "required": [
      "dbType",
      "dbHost",
      "dbPort",
      "dbInstance"
    ]
  },
  "required": [
    "repositoryEndpointMetadata"
  ]
},
"repositoryConfigurations": {
  "type": "object",
  "properties": {
    "document": {
      "type": "object",
      "properties": {
        "fieldMappings": {
          "type": "array",
```

```
    "items": [
      {
        "type": "object",
        "properties": {
          "indexFieldName": {
            "type": "string"
          },
          "indexFieldType": {
            "type": "string"
          },
          "dataSourceFieldName": {
            "type": "string"
          }
        },
        "required": [
          "indexFieldName",
          "indexFieldType",
          "dataSourceFieldName"
        ]
      }
    ]
  },
  "required": [
    "fieldMappings"
  ]
},
"required": [
]
},
"additionalProperties": {
  "type": "object",
  "properties": {
    "primaryKey": {
      "type": "string"
    },
    "titleColumn": {
      "type": "string"
    },
    "bodyColumn": {
      "type": "string"
    },
    "sqlQuery": {
```

```
    "type": "string",
    "not": {
      "pattern": ";+"
    }
  },
  "timestampColumn": {
    "type": "string"
  },
  "timestampFormat": {
    "type": "string"
  },
  "timezone": {
    "type": "string"
  },
  "changeDetectingColumns": {
    "type": "array",
    "items": {
      "type": "string"
    }
  },
  "allowedUsersColumn": {
    "type": "string"
  },
  "allowedGroupsColumn": {
    "type": "string"
  },
  "sourceURIColumn": {
    "type": "string"
  },
  "isSslEnabled": {
    "type": "boolean"
  }
},
"required": ["primaryKey", "titleColumn", "bodyColumn", "sqlQuery"]
},
"type" : {
  "type" : "string",
  "pattern": "JDBC"
},
"syncMode": {
  "type": "string",
  "enum": [
    "FORCED_FULL_CRAWL",
    "FULL_CRAWL",
```

```

        "CHANGE_LOG"
      ]
    },
    "secretArn": {
      "type": "string"
    }
  },
  "version": {
    "type": "string",
    "anyOf": [
      {
        "pattern": "1.0.0"
      }
    ]
  },
  "required": [
    "connectionConfiguration",
    "repositoryConfigurations",
    "syncMode",
    "additionalProperties",
    "secretArn",
    "type"
  ]
}

```

Amazon RDS (Microsoft SQL 服務器) 模板架構

您可以將包含資料來源結構描述的 JSON 納入為 [TemplateConfiguration](#) 物件的一部分。將資料來源的類型指定為 JDBC、資料庫類型為 sqlserver、驗證認證的密碼，以及其他必要的組態。然後，您將指定 TEMPLATE 為呼叫 Type 時 [CreateDataSource](#)。

您可以使用本開發人員指南中提供的模板。請參閱 [Amazon RDS \(Microsoft SQL 服務器 \) JSON 模式](#)。

下表說明 Amazon RDS (Microsoft SQL 伺服器) JSON 結構描述的參數。

組態	描述
連線組態	資料來源端點的組態資訊。
repositoryEndpointMetadata	連線資料來源所需的組態資訊。

組態	描述
	<ul style="list-style-type: none"> • 資料庫類型-您使用的 Java 資料庫類型 (無論是mysql、db2、postgresql oracle、或)。sqlserver • 資料庫主機 — 資料庫主機名稱。 • 資料庫埠 — 資料庫連接埠。 • 資料庫實例 — 資料庫執行處理。
儲存庫組態	資料來源內容的組態資訊。例如，配置特定類型的內容和欄位對應。指定資料來源的類型和秘密 ARN。
文件	將資料庫內容的屬性或欄位名稱對應至 Amazon Kendra 索引欄位名稱的物件清單。如需詳細資訊，請參閱 映射資料來源欄位 。
附加屬性	資料來源中內容的其他組態選項。用於在資料庫資料來源中包含或排除特定內容。
主要金鑰	提供資料庫表格的主索引鍵。這標識數據庫中的一個表。
標題欄	提供資料庫表格中文件標題欄的名稱。
身體專欄	提供資料庫表格中文件標題欄的名稱。
sqlQuery	輸入 SQL 查詢語句，如選擇和連接操作。SQL 查詢必須小於 32 KB。Amazon Kendra 會編目符合您查詢的所有資料庫內容。
時間戳記列	輸入包含時間戳記的列的名稱。Amazon Kendra 使用時間戳記資訊偵測內容中的變更，並僅同步變更的內容。
時間戳記格式	輸入包含時間戳記格式的資料欄名稱，可用來偵測內容變更並重新同步處理內容。
timezone	輸入包含要探索之內容之時區的資料欄名稱。

組態	描述
changeDetectingColumns	輸入 Amazon Kendra 將用來偵測內容變更的欄名稱。Amazon Kendra 當這些列中的任何一個更改時，將重新索引內容。
allowedUsersColumns	輸入包含允許存取內容之使用者 ID 的欄名稱。
allowedGroupsColumn	輸入包含允許存取內容之使用者 ID 的欄名稱。
來源尿酸氧胺	輸入包含要編製索引之來源 URL 的資料欄名稱。
isSslEnabled	輸入 SQL 查詢語句，如選擇和連接操作。SQL 查詢必須小於 32 KB。Amazon Kendra 會編目符合您查詢的所有資料庫內容。
type	資料來源的類型。指定 JDBC 為您的資料來源類型。
同步模式	<p>指定資料來源內容變更時 Amazon Kendra 應如何更新索引。您可以選擇：</p> <ul style="list-style-type: none"> • FORCED_FULL_CRAWL 新建索引所有內容，並在每次資料來源與索引同步時取代現有內容。 • FULL_CRAWL，每次您的資料來源與索引同步時，僅對新的、修改和刪除的內容建立索引。Amazon Kendra 可以使用資料來源的機制來追蹤內容變更，並為上次同步後變更的內容建立索引。 • CHANGE_LOG 每次資料來源與索引同步時，僅對新內容和修改的內容建立索引。Amazon Kendra 可以使用資料來源的機制來追蹤內容變更，並為上次同步後變更的內容建立索引。

組態	描述
秘书	<p>秘密 Secrets Manager 密碼的 Amazon 資源名稱 (ARN)，其中包含連線到資料庫所需的使用者名稱和密碼。私密必須包含具有下列索引鍵的 JSON 結構：</p> <pre data-bbox="831 445 1507 638"> { "user name": "<i>database user name</i>", "password": "<i>password</i>" } </pre>
version	目前支援的範本版本。

Amazon RDS (Microsoft SQL 服務器) JSON 模式

```

{
  "$schema": "http://json-schema.org/draft-04/schema#",
  "type": "object",
  "properties": {
    "connectionConfiguration": {
      "type": "object",
      "properties": {
        "repositoryEndpointMetadata": {
          "type": "object",
          "properties": {
            "dbType": {
              "type": "string",
              "enum": [
                "mysql",
                "db2",
                "postgresql",
                "oracle",
                "sqlserver"
              ]
            },
            "dbHost": {
              "type": "string"
            },
            "dbPort": {
              "type": "string"
            }
          }
        }
      }
    }
  }
}

```

```
    },
    "dbInstance": {
      "type": "string"
    }
  },
  "required": [
    "dbType",
    "dbHost",
    "dbPort",
    "dbInstance"
  ]
},
"required": [
  "repositoryEndpointMetadata"
],
"repositoryConfigurations": {
  "type": "object",
  "properties": {
    "document": {
      "type": "object",
      "properties": {
        "fieldMappings": {
          "type": "array",
          "items": [
            {
              "type": "object",
              "properties": {
                "indexFieldName": {
                  "type": "string"
                },
                "indexFieldType": {
                  "type": "string"
                },
                "dataSourceFieldName": {
                  "type": "string"
                }
              }
            }
          ]
        },
        "required": [
          "indexFieldName",
          "indexFieldType",
          "dataSourceFieldName"
        ]
      }
    }
  }
}
```

```
        }
      ]
    }
  },
  "required": [
    "fieldMappings"
  ]
}
},
"required": [
]
},
"additionalProperties": {
  "type": "object",
  "properties": {
    "primaryKey": {
      "type": "string"
    },
    "titleColumn": {
      "type": "string"
    },
    "bodyColumn": {
      "type": "string"
    },
    "sqlQuery": {
      "type": "string",
      "not": {
        "pattern": ";+"
      }
    },
    "timestampColumn": {
      "type": "string"
    },
    "timestampFormat": {
      "type": "string"
    },
    "timezone": {
      "type": "string"
    },
    "changeDetectingColumns": {
      "type": "array",
      "items": {
        "type": "string"
      }
    }
  }
}
```

```
    },
    "allowedUsersColumn": {
      "type": "string"
    },
    "allowedGroupsColumn": {
      "type": "string"
    },
    "sourceURIColumn": {
      "type": "string"
    },
    "isSslEnabled": {
      "type": "boolean"
    }
  },
  "required": ["primaryKey", "titleColumn", "bodyColumn", "sqlQuery"]
},
"type" : {
  "type" : "string",
  "pattern": "JDBC"
},
"syncMode": {
  "type": "string",
  "enum": [
    "FORCED_FULL_CRAWL",
    "FULL_CRAWL",
    "CHANGE_LOG"
  ]
},
"secretArn": {
  "type": "string"
}
},
"version": {
  "type": "string",
  "anyOf": [
    {
      "pattern": "1.0.0"
    }
  ]
}
},
"required": [
  "connectionConfiguration",
  "repositoryConfigurations",
  "syncMode",
```

```

    "additionalProperties",
    "secretArn",
    "type"
  ]
}

```

Amazon RDS (MySQL) 模板架構

您可以將包含資料來源結構描述的 JSON 納入為 [TemplateConfiguration](#) 物件的一部分。將資料來源的類型指定為 JDBC、資料庫類型為 mysql、驗證認證的密碼，以及其他必要的組態。然後，您將指定 TEMPLATE 為呼叫 Type 時 [CreateDataSource](#)。

您可以使用本開發人員指南中提供的模板。請參閱 [Amazon RDS \(MySQL\) 結構描述](#)。

下表說明 Amazon RDS (MySQL) JSON 結構定義的參數。

組態	描述
連線組態	資料來源端點的組態資訊。
repositoryEndpointMetadata	連線資料來源所需的組態資訊。 <ul style="list-style-type: none"> • 資料庫類型-您使用的 Java 資料庫類型 (無論是 mysql、db2、postgresql oracle、或)。sqlserver • 資料庫主機 — 資料庫主機名稱。 • 資料庫埠 — 資料庫連接埠。 • 資料庫實例 — 資料庫執行處理。
儲存庫組態	資料來源內容的組態資訊。例如，配置特定類型的內容和欄位對應。指定資料來源的類型和秘密 ARN。
文件	將資料庫內容的屬性或欄位名稱對應至 Amazon Kendra 索引欄位名稱的物件清單。如需詳細資訊，請參閱 映射資料來源欄位 。
附加屬性	資料來源中內容的其他組態選項。用於在資料庫資料來源中包含或排除特定內容。

組態	描述
主要金鑰	提供資料庫表格的主索引鍵。這標識數據庫中的一個表。
標題欄	提供資料庫表格中文件標題欄的名稱。
身體專欄	提供資料庫表格中文件標題欄的名稱。
sqlQuery	輸入 SQL 查詢語句，如選擇和連接操作。SQL 查詢必須小於 32 KB。Amazon Kendra 會編目符合您查詢的所有資料庫內容。
時間戳記列	輸入包含時間戳記的列的名稱。Amazon Kendra 使用時間戳記資訊偵測內容中的變更，並僅同步變更的內容。
時間戳記格式	輸入包含時間戳記格式的資料欄名稱，可用來偵測內容變更並重新同步處理內容。
timezone	輸入包含要探索之內容之時區的資料欄名稱。
changeDetectingColumns	輸入 Amazon Kendra 將用來偵測內容變更的欄名稱。Amazon Kendra 當這些列中的任何一個更改時，將重新索引內容
allowedUsersColumns	輸入包含允許存取內容之使用者 ID 的欄名稱。
allowedGroupsColumn	輸入包含允許存取內容之使用者 ID 的欄名稱。
來源尿酸氧胺	輸入包含要編製索引之來源 URL 的資料欄名稱。
isSslEnabled	輸入 SQL 查詢語句，如選擇和連接操作。SQL 查詢必須小於 32 KB。Amazon Kendra 會編目符合您查詢的所有資料庫內容。
type	資料來源的類型。指定JDBC為您的資料來源類型。

組態	描述
同步模式	<p>指定資料來源內容變更時 Amazon Kendra 應如何更新索引。您可以選擇：</p> <ul style="list-style-type: none"> • FORCED_FULL_CRAWL 新建索引所有內容，並在每次資料來源與索引同步時取代現有內容。 • FULL_CRAWL ，每次您的資料來源與索引同步時，僅對新的、修改和刪除的內容建立索引。Amazon Kendra 可以使用資料來源的機制來追蹤內容變更，並為上次同步後變更的內容建立索引。 • CHANGE_LOG 每次資料來源與索引同步時，僅對新內容和修改的內容建立索引。Amazon Kendra 可以使用資料來源的機制來追蹤內容變更，並為上次同步後變更的內容建立索引。
秘書	<p>秘密 Secrets Manager 密碼的 Amazon 資源名稱 (ARN)，其中包含連線到資料庫所需的使用者名稱和密碼。私密必須包含具有下列索引鍵的 JSON 結構：</p> <pre data-bbox="829 1192 1507 1394"> { "user name": "database user name", "password": "password" } </pre>
version	目前支援的範本版本。

Amazon RDS (MySQL) 結構描述

```

{
  "$schema": "http://json-schema.org/draft-04/schema#",
  "type": "object",
  "properties": {
    "connectionConfiguration": {
      "type": "object",

```

```
"properties": {
  "repositoryEndpointMetadata": {
    "type": "object",
    "properties": {
      "dbType": {
        "type": "string",
        "enum": [
          "mysql",
          "db2",
          "postgresql",
          "oracle",
          "sqlserver"
        ]
      },
      "dbHost": {
        "type": "string"
      },
      "dbPort": {
        "type": "string"
      },
      "dbInstance": {
        "type": "string"
      }
    },
    "required": [
      "dbType",
      "dbHost",
      "dbPort",
      "dbInstance"
    ]
  },
  "required": [
    "repositoryEndpointMetadata"
  ]
},
"repositoryConfigurations": {
  "type": "object",
  "properties": {
    "document": {
      "type": "object",
      "properties": {
        "fieldMappings": {
          "type": "array",
```

```
    "items": [
      {
        "type": "object",
        "properties": {
          "indexFieldName": {
            "type": "string"
          },
          "indexFieldType": {
            "type": "string"
          },
          "dataSourceFieldName": {
            "type": "string"
          }
        },
        "required": [
          "indexFieldName",
          "indexFieldType",
          "dataSourceFieldName"
        ]
      }
    ]
  },
  "required": [
    "fieldMappings"
  ]
},
"required": [
]
},
"additionalProperties": {
  "type": "object",
  "properties": {
    "primaryKey": {
      "type": "string"
    },
    "titleColumn": {
      "type": "string"
    },
    "bodyColumn": {
      "type": "string"
    },
    "sqlQuery": {
```

```
    "type": "string",
    "not": {
      "pattern": ";+"
    }
  },
  "timestampColumn": {
    "type": "string"
  },
  "timestampFormat": {
    "type": "string"
  },
  "timezone": {
    "type": "string"
  },
  "changeDetectingColumns": {
    "type": "array",
    "items": {
      "type": "string"
    }
  },
  "allowedUsersColumn": {
    "type": "string"
  },
  "allowedGroupsColumn": {
    "type": "string"
  },
  "sourceURIColumn": {
    "type": "string"
  },
  "isSslEnabled": {
    "type": "boolean"
  }
},
"required": ["primaryKey", "titleColumn", "bodyColumn", "sqlQuery"]
},
"type" : {
  "type" : "string",
  "pattern": "JDBC"
},
"syncMode": {
  "type": "string",
  "enum": [
    "FORCED_FULL_CRAWL",
    "FULL_CRAWL",
```

```

    "CHANGE_LOG"
  ]
},
"secretArn": {
  "type": "string"
}
},
"version": {
  "type": "string",
  "anyOf": [
    {
      "pattern": "1.0.0"
    }
  ]
},
"required": [
  "connectionConfiguration",
  "repositoryConfigurations",
  "syncMode",
  "additionalProperties",
  "secretArn",
  "type"
]
}

```

Amazon RDS (甲骨文) 樣板綱要

您可以將包含資料來源結構描述的 JSON 納入為 [TemplateConfiguration](#) 物件的一部分。將資料來源的類型指定為 JDBC、資料庫類型為 oracle、驗證認證的密碼，以及其他必要的組態。然後，您將指定 TEMPLATE 為呼叫 Type 時 [CreateDataSource](#)。

您可以使用本開發人員指南中提供的模板。請參閱 [Amazon RDS \(甲骨文\) JSON 模式](#)。

下表說明 Amazon RDS (Oracle) JSON 結構定義的參數。

組態	描述
連線組態	資料來源端點的組態資訊。
repositoryEndpointMetadata	連線資料來源所需的組態資訊。

組態	描述
	<ul style="list-style-type: none"> • 資料庫類型-您使用的 Java 資料庫類型 (無論是mysql、db2、postgresql oracle、或)。sqlserver • 資料庫主機 — 資料庫主機名稱。 • 資料庫埠 — 資料庫連接埠。 • 資料庫實例 — 資料庫執行處理。
儲存庫組態	資料來源內容的組態資訊。例如，配置特定類型的內容和欄位對應。指定資料來源的類型和秘密 ARN。
文件	將資料庫內容的屬性或欄位名稱對應至 Amazon Kendra 索引欄位名稱的物件清單。如需詳細資訊，請參閱 映射資料來源欄位 。
附加屬性	資料來源中內容的其他組態選項。用於在資料庫資料來源中包含或排除特定內容。
主要金鑰	提供資料庫表格的主索引鍵。這標識數據庫中的一個表。
標題欄	提供資料庫表格中文件標題欄的名稱。
身體專欄	提供資料庫表格中文件標題欄的名稱。
sqlQuery	輸入 SQL 查詢語句，如選擇和連接操作。SQL 查詢必須小於 32 KB。Amazon Kendra 會編目符合您查詢的所有資料庫內容。
時間戳記列	輸入包含時間戳記的列的名稱。Amazon Kendra 使用時間戳記資訊偵測內容中的變更，並僅同步變更的內容。
時間戳記格式	輸入包含時間戳記格式的資料欄名稱，可用來偵測內容變更並重新同步處理內容。
timezone	輸入包含要探索之內容之時區的資料欄名稱。

組態	描述
changeDetectingColumns	輸入 Amazon Kendra 將用來偵測內容變更的欄名稱。Amazon Kendra 當這些列中的任何一個更改時，將重新索引內容
allowedUsersColumns	輸入包含允許存取內容之使用者 ID 的欄名稱。
allowedGroupsColumn	輸入包含允許存取內容之使用者 ID 的欄名稱。
來源尿酸氧胺	輸入包含要編製索引之來源 URL 的資料欄名稱。
isSslEnabled	輸入 SQL 查詢語句，如選擇和連接操作。SQL 查詢必須小於 32 KB。Amazon Kendra 會編目符合您查詢的所有資料庫內容。
type	資料來源的類型。指定 JDBC 為您的資料來源類型。
同步模式	<p>指定資料來源內容變更時 Amazon Kendra 應如何更新索引。您可以選擇：</p> <ul style="list-style-type: none"> • FORCED_FULL_CRAWL 新建索引所有內容，並在每次資料來源與索引同步時取代現有內容。 • FULL_CRAWL，每次您的資料來源與索引同步時，僅對新的、修改和刪除的內容建立索引。Amazon Kendra 可以使用資料來源的機制來追蹤內容變更，並為上次同步後變更的內容建立索引。 • CHANGE_LOG 每次資料來源與索引同步時，僅對新內容和修改的內容建立索引。Amazon Kendra 可以使用資料來源的機制來追蹤內容變更，並為上次同步後變更的內容建立索引。

組態	描述
秘书	<p>秘密 Secrets Manager 密碼的 Amazon 資源名稱 (ARN)，其中包含連線到資料庫所需的使用者名稱和密碼。私密必須包含具有下列索引鍵的 JSON 結構：</p> <pre data-bbox="829 443 1507 642"> { "user name": "<i>database user name</i>", "password": "<i>password</i>" } </pre>
version	目前支援的範本版本。

Amazon RDS (甲骨文) JSON 模式

```

{
  "$schema": "http://json-schema.org/draft-04/schema#",
  "type": "object",
  "properties": {
    "connectionConfiguration": {
      "type": "object",
      "properties": {
        "repositoryEndpointMetadata": {
          "type": "object",
          "properties": {
            "dbType": {
              "type": "string",
              "enum": [
                "mysql",
                "db2",
                "postgresql",
                "oracle",
                "sqlserver"
              ]
            },
            "dbHost": {
              "type": "string"
            },
            "dbPort": {
              "type": "string"
            }
          }
        }
      }
    }
  }
}

```



```
    },
    "dbInstance": {
      "type": "string"
    }
  },
  "required": [
    "dbType",
    "dbHost",
    "dbPort",
    "dbInstance"
  ]
},
"required": [
  "repositoryEndpointMetadata"
],
"repositoryConfigurations": {
  "type": "object",
  "properties": {
    "document": {
      "type": "object",
      "properties": {
        "fieldMappings": {
          "type": "array",
          "items": [
            {
              "type": "object",
              "properties": {
                "indexFieldName": {
                  "type": "string"
                },
                "indexFieldType": {
                  "type": "string"
                },
                "dataSourceFieldName": {
                  "type": "string"
                }
              }
            }
          ]
        },
        "required": [
          "indexFieldName",
          "indexFieldType",
          "dataSourceFieldName"
        ]
      }
    }
  }
}
```

```
        }
      ]
    }
  },
  "required": [
    "fieldMappings"
  ]
}
},
"required": [
]
},
"additionalProperties": {
  "type": "object",
  "properties": {
    "primaryKey": {
      "type": "string"
    },
    "titleColumn": {
      "type": "string"
    },
    "bodyColumn": {
      "type": "string"
    },
    "sqlQuery": {
      "type": "string",
      "not": {
        "pattern": ";+"
      }
    },
    "timestampColumn": {
      "type": "string"
    },
    "timestampFormat": {
      "type": "string"
    },
    "timezone": {
      "type": "string"
    },
    "changeDetectingColumns": {
      "type": "array",
      "items": {
        "type": "string"
      }
    }
  }
}
```

```
    },
    "allowedUsersColumn": {
      "type": "string"
    },
    "allowedGroupsColumn": {
      "type": "string"
    },
    "sourceURIColumn": {
      "type": "string"
    },
    "isSslEnabled": {
      "type": "boolean"
    }
  },
  "required": ["primaryKey", "titleColumn", "bodyColumn", "sqlQuery"]
},
"type" : {
  "type" : "string",
  "pattern": "JDBC"
},
"syncMode": {
  "type": "string",
  "enum": [
    "FORCED_FULL_CRAWL",
    "FULL_CRAWL",
    "CHANGE_LOG"
  ]
},
"secretArn": {
  "type": "string"
}
},
"version": {
  "type": "string",
  "anyOf": [
    {
      "pattern": "1.0.0"
    }
  ]
}
},
"required": [
  "connectionConfiguration",
  "repositoryConfigurations",
  "syncMode",
```

```

    "additionalProperties",
    "secretArn",
    "type"
  ]
}

```

Amazon RDS 模板模板架構

您可以將包含資料來源結構描述的 JSON 納入為 [TemplateConfiguration](#) 物件的一部分。將資料來源的類型指定為 JDBC、資料庫類型為 postgresql、驗證認證的密碼，以及其他必要的組態。然後，您將指定 TEMPLATE 為呼叫 Type 時 [CreateDataSource](#)。

您可以使用本開發人員指南中提供的模板。請參閱 [Amazon RDS JSON 結構描述](#)。

下表說明 Amazon RDS (PostgreSQL) JSON 結構描述的參數。

組態	描述
連線組態	資料來源端點的組態資訊。
repositoryEndpointMetadata	連線資料來源所需的組態資訊。 <ul style="list-style-type: none"> 資料庫類型-您使用的 Java 資料庫類型 (無論是 mysql、db2、postgresql oracle、或)。sqlserver 資料庫主機 — 資料庫主機名稱。 資料庫埠 — 資料庫連接埠。 資料庫實例 — 資料庫執行處理。
儲存庫組態	資料來源內容的組態資訊。例如，配置特定類型的內容和欄位對應。指定資料來源的類型和秘密 ARN。
文件	將資料庫內容的屬性或欄位名稱對應至 Amazon Kendra 索引欄位名稱的物件清單。如需詳細資訊，請參閱 映射資料來源欄位 。
附加屬性	資料來源中內容的其他組態選項。用於在資料庫資料來源中包含或排除特定內容。

組態	描述
主要金鑰	提供資料庫表格的主索引鍵。這標識數據庫中的一個表。
標題欄	提供資料庫表格中文件標題欄的名稱。
身體專欄	提供資料庫表格中文件標題欄的名稱。
sqlQuery	輸入 SQL 查詢語句，如選擇和連接操作。SQL 查詢必須小於 32 KB。Amazon Kendra 會編目符合您查詢的所有資料庫內容。
時間戳記列	輸入包含時間戳記的列的名稱。Amazon Kendra 使用時間戳記資訊偵測內容中的變更，並僅同步變更的內容。
時間戳記格式	輸入包含時間戳記格式的資料欄名稱，可用來偵測內容變更並重新同步處理內容。
timezone	輸入包含要探索之內容之時區的資料欄名稱。
changeDetectingColumns	輸入 Amazon Kendra 將用來偵測內容變更的欄名稱。Amazon Kendra 當這些列中的任何一個更改時，將重新索引內容
allowedUsersColumns	輸入包含允許存取內容之使用者 ID 的欄名稱。
allowedGroupsColumn	輸入包含允許存取內容之使用者 ID 的欄名稱。
來源尿酸氧胺	輸入包含要編製索引之來源 URL 的資料欄名稱。
isSslEnabled	輸入 SQL 查詢語句，如選擇和連接操作。SQL 查詢必須小於 32 KB。Amazon Kendra 會編目符合您查詢的所有資料庫內容。
type	資料來源的類型。指定JDBC為您的資料來源類型。

組態	描述
同步模式	<p>指定資料來源內容變更時 Amazon Kendra 應如何更新索引。您可以選擇：</p> <ul style="list-style-type: none"> • FORCED_FULL_CRAWL 新建索引所有內容，並在每次資料來源與索引同步時取代現有內容。 • FULL_CRAWL ，每次您的資料來源與索引同步時，僅對新的、修改和刪除的內容建立索引。Amazon Kendra 可以使用資料來源的機制來追蹤內容變更，並為上次同步後變更的內容建立索引。 • CHANGE_LOG 每次資料來源與索引同步時，僅對新內容和修改的內容建立索引。Amazon Kendra 可以使用資料來源的機制來追蹤內容變更，並為上次同步後變更的內容建立索引。
秘書	<p>秘密 Secrets Manager 密碼的 Amazon 資源名稱 (ARN)，其中包含連線到資料庫所需的使用者名稱和密碼。私密必須包含具有下列索引鍵的 JSON 結構：</p> <pre data-bbox="829 1192 1507 1394"> { "user name": "database user name", "password": "password" } </pre>
version	目前支援的範本版本。

Amazon RDS JSON 結構描述

```

{
  "$schema": "http://json-schema.org/draft-04/schema#",
  "type": "object",
  "properties": {
    "connectionConfiguration": {
      "type": "object",

```

```
"properties": {
  "repositoryEndpointMetadata": {
    "type": "object",
    "properties": {
      "dbType": {
        "type": "string",
        "enum": [
          "mysql",
          "db2",
          "postgresql",
          "oracle",
          "sqlserver"
        ]
      },
      "dbHost": {
        "type": "string"
      },
      "dbPort": {
        "type": "string"
      },
      "dbInstance": {
        "type": "string"
      }
    },
    "required": [
      "dbType",
      "dbHost",
      "dbPort",
      "dbInstance"
    ]
  },
  "required": [
    "repositoryEndpointMetadata"
  ]
},
"repositoryConfigurations": {
  "type": "object",
  "properties": {
    "document": {
      "type": "object",
      "properties": {
        "fieldMappings": {
          "type": "array",
```

```
    "items": [
      {
        "type": "object",
        "properties": {
          "indexFieldName": {
            "type": "string"
          },
          "indexFieldType": {
            "type": "string"
          },
          "dataSourceFieldName": {
            "type": "string"
          }
        },
        "required": [
          "indexFieldName",
          "indexFieldType",
          "dataSourceFieldName"
        ]
      }
    ]
  },
  "required": [
    "fieldMappings"
  ]
},
"required": [
]
},
"additionalProperties": {
  "type": "object",
  "properties": {
    "primaryKey": {
      "type": "string"
    },
    "titleColumn": {
      "type": "string"
    },
    "bodyColumn": {
      "type": "string"
    },
    "sqlQuery": {
```



```
    "type": "string",
    "not": {
      "pattern": ";+"
    }
  },
  "timestampColumn": {
    "type": "string"
  },
  "timestampFormat": {
    "type": "string"
  },
  "timezone": {
    "type": "string"
  },
  "changeDetectingColumns": {
    "type": "array",
    "items": {
      "type": "string"
    }
  },
  "allowedUsersColumn": {
    "type": "string"
  },
  "allowedGroupsColumn": {
    "type": "string"
  },
  "sourceURIColumn": {
    "type": "string"
  },
  "isSslEnabled": {
    "type": "boolean"
  }
},
"required": ["primaryKey", "titleColumn", "bodyColumn", "sqlQuery"]
},
"type" : {
  "type" : "string",
  "pattern": "JDBC"
},
"syncMode": {
  "type": "string",
  "enum": [
    "FORCED_FULL_CRAWL",
    "FULL_CRAWL",
```

```

    "CHANGE_LOG"
  ]
},
"secretArn": {
  "type": "string"
}
},
"version": {
  "type": "string",
  "anyOf": [
    {
      "pattern": "1.0.0"
    }
  ]
},
"required": [
  "connectionConfiguration",
  "repositoryConfigurations",
  "syncMode",
  "additionalProperties",
  "secretArn",
  "type"
]
}

```

Amazon S3 模板架構

您可以將包含資料來源結構描述的 JSON 納入為範本組態的一部分。您提供 S3 儲存貯體的名稱作為連線組態或存放庫端點詳細資料的一部分。同時將資料來源的類型指定為 S3，以及其他必要的組態。然後，您將指定 TEMPLATE 為呼叫 Type 時 [CreateDataSource](#)。

您可以使用本開發人員指南中提供的模板。請參閱 [JSON 結構描述](#)。

下表說明 Amazon S3 JSON 結構定義的參數。

組態	描述
連線組態	資料來源端點的組態資訊。
repositoryEndpointMetadata	資料來源的端點資訊。
BucketName	Amazon S3 儲存貯體的名稱。

組態	描述
儲存庫組態	資料來源內容的組態資訊。例如，配置特定類型的內容和欄位對應。
附加屬性	資料來源中內容的其他設定選項
<ul style="list-style-type: none"> • 包含模式 • 排除模式 • 包含前綴 • 排除前置詞 	要在 Amazon S3 資料來源中包含或排除特定檔案的規則運算式模式清單。符合模式的檔案會包括在索引中。不符合模式的檔案會從索引中排除。如果檔案同時符合包括模式和排除模式，則以排除模式為優先，且該項目不會包括在索引中。
aclConfigurationFile路徑	控制 Amazon Kendra 索引中文件存取的檔案路徑。
metadataFilesPrefix	值區中繼資料檔案的位置。
同步模式	<p>指定資料來源內容變更時 Amazon Kendra 應如何更新索引。您可以選擇：</p> <ul style="list-style-type: none"> • FORCED_FULL_CRAWL 新建索引所有內容，並在每次資料來源與索引同步時取代現有內容。 • FULL_CRAWL，每次您的資料來源與索引同步時，僅對新的、修改和刪除的內容建立索引。Amazon Kendra 可以使用資料來源的機制來追蹤內容變更，並為上次同步後變更的內容建立索引。
type	資料來源的類型。指定S3為您的資料來源類型。
version	支援的範本版本。

JSON 結構描述

```
{
```

```
"$schema": "http://json-schema.org/draft-04/schema#",
"type": "object",
"properties": {
  "connectionConfiguration": {
    "type": "object",
    "properties": {
      "repositoryEndpointMetadata": {
        "type": "object",
        "properties": {
          "BucketName": {
            "type": "string"
          }
        },
        "required": [
          "BucketName"
        ]
      },
      "required": [
        "repositoryEndpointMetadata"
      ]
    },
    "required": [
      "repositoryEndpointMetadata"
    ]
  },
  "repositoryConfigurations": {
    "type": "object",
    "properties": {
      "document": {
        "type": "object",
        "properties": {
          "fieldMappings": {
            "type": "array",
            "items": [
              {
                "type": "object",
                "properties": {
                  "indexFieldName": {
                    "type": "string"
                  },
                  "indexFieldType": {
                    "type": "string",
                    "enum": [
                      "STRING"
                    ]
                  }
                }
              }
            ]
          },
          "dataSourceFieldName": {
```

```
        "type": "string"
      }
    },
    "required": [
      "indexFieldName",
      "indexFieldType",
      "dataSourceFieldName"
    ]
  }
]
}
},
"required": [
  "fieldMappings"
]
}
},
"required": [
  "document"
]
},
"additionalProperties": {
  "type": "object",
  "properties": {
    "inclusionPatterns": {
      "type": "array"
    },
    "exclusionPatterns": {
      "type": "array"
    },
    "inclusionPrefixes": {
      "type": "array"
    },
    "exclusionPrefixes": {
      "type": "array"
    },
    "aclConfigurationFilePath": {
      "type": "string"
    },
    "metadataFilesPrefix": {
      "type": "string"
    }
  }
}
},
},
```

```
"syncMode": {
  "type": "string",
  "enum": [
    "FULL_CRAWL",
    "FORCED_FULL_CRAWL"
  ]
},
"type": {
  "type": "string",
  "pattern": "S3"
},
"version": {
  "type": "string",
  "anyOf": [
    {
      "pattern": "1.0.0"
    }
  ]
}
},
"required": [
  "connectionConfiguration",
  "type",
  "syncMode",
  "repositoryConfigurations"
]
}
```

Amazon Kendra 網路爬蟲範本結構描述

您可以將包含資料來源結構描述的 JSON 納入為 [TemplateConfiguration](#) 物件的一部分。

您可以提供種子或起點 URL，或者提供 Sitemap URL，做為連線組態或存放庫端點詳細資料的一部分。除了手動列出所有 URL 之外，您還可以提供儲存貯體的路徑，該儲存 Amazon S3 貯體存放種子 URL 清單或 Sitemap XML 檔案清單的文字檔案，您可以將這些檔案集合在 S3 中的 ZIP 檔案中。

您也可以將資料來源的類型指定為 WEBCRAWLERV2、網站驗證憑證和驗證類型 (如果您的網站需要驗證)，以及其他必要的設定。

然後，您將指定 TEMPLATE 為呼叫 Type 時 [CreateDataSource](#)。

⚠ Important

不支援建立 Web 爬行者程式 v2.0 連接器。AWS CloudFormation 如果您需 AWS CloudFormation 要支援，請使用網路爬行者程式 v1.0 連接器。

選取要索引的網站時，您必須遵守 [Amazon 可接受的使用政策](#) 以及 Amazon 所有其他條款。請記住，您只能使用 Amazon Kendra Web 爬蟲來索引您自己的網頁或您有權索引的網頁。若要瞭解如何停止 Amazon Kendra 網頁爬蟲索引您的網站，請參閱 [設定 Amazon Kendra 網頁爬行者程式的 robots.txt 檔案](#)。

您可以使用本開發人員指南中提供的模板。請參閱 [Amazon Kendra 網路爬蟲結構描述](#)。

下表說明 Amazon Kendra 網路爬行者程式 JSON 結構描述的參數。

組態	描述
連線組態	資料來源端點的組態資訊。
repositoryEndpointMetadata	資料來源的端點資訊。
siteMapUrls	您要檢索之網站的網站地圖 URL 清單。您最多可以列出三個網站地圖 URL。
S3 SeedUrl	存放種子或起點 URL 清單的文字檔案的 S3 路徑。例如 s3://bucket-name/directory/。文字檔案中的每個 URL 都必須以個別的行格式化。您最多可以在一個檔案中列出 100 個種子 URL。
S3 SiteMapUrl	網站地圖 XML 檔案的 S3 路徑。例如 s3://bucket-name/directory/。您最多可以列出三個網站地圖 XML 檔案。您可以將多個 Sitemap 檔案合併為一個 ZIP 檔案，並將 ZIP 檔案儲存在 Amazon S3 值區中。
seedUrlConnections	您要檢索之網站的種子或起點 URL 清單。您最多可以列出 100 個種子 URL。
種子網址	種子或起點 URL。

組態	描述
驗證	驗證類型 (如果您的網站需要相同的驗證) ，否則請指定NoAuthentication 。
儲存庫組態	資料來源內容的組態資訊。例如，配置特定類型的內容和欄位對應。
<ul style="list-style-type: none"> • 网页 • attachment 	將網頁和網頁檔案的屬性或欄位名稱對應至 Amazon Kendra 索引欄位名稱的物件清單。例如，HTML 網頁標題標籤可以對應至索_document_title 引欄位。如需詳細資訊，請參閱 映射資料來源欄位 。
同步模式	<p>指定資料來源內容變更時 Amazon Kendra 應如何更新索引。您可以選擇：</p> <ul style="list-style-type: none"> • FORCED_FULL_CRAWL 新建索引所有內容，並在每次資料來源與索引同步時取代現有內容。 • FULL_CRAWL ，每次您的資料來源與索引同步時，僅對新的、修改和刪除的內容建立索引。Amazon Kendra 可以使用資料來源的機制來追蹤內容變更，並為上次同步後變更的內容建立索引。
附加屬性	資料來源中內容的其他組態選項。
速率限制	每分鐘每個網站主機網路爬取的 URL 數目上限。
maxFileSize	要編目的網頁或附件的大小上限 (MB)。
爬行深度	要編目之種子 URL 的層級數目。例如，種子 URL 頁面是深度 1，而此頁面上也經過探索的任何超連結都是深度 2。

組態	描述
maxLinksPer网址	檢索網站時，網頁上要包含的 URL 數目上限。這個數字是每個網頁。當網站的網頁被抓取時，網頁鏈接到的所有 URL 也會被抓取。網頁上的 URL 會依外觀順序進行檢索。
crawlSubDomain	true 抓取具有子域的網站域。例如，如果種子 URL 是 "abc.example.com"，則也會探索 "b.abc.example.com" 和 ""。a.abc.example.com 如果您未設定 crawlSubDomain 或設 crawlAllDomain 定 true，則 Amazon Kendra 只會檢索您要檢索之網站的網域。
crawlAllDomain	true 抓取具有子域和網頁鏈接到的其他域的網站域。如果您未設定 crawlSubDomain 或設 crawlAllDomain 定 true，則 Amazon Kendra 只會檢索您要檢索之網站的網域。
榮譽機器人	true 尊重您要抓取的網站的 robots.txt 指令。這些指令會控制 Amazon Kendra 網頁爬行者程式搜索網站的方式，是否只 Amazon Kendra 能編目特定內容或不編目任何內容。
爬網附件 <ul style="list-style-type: none"> • 包含網址 CrawlPatterns • 包含網址 IndexPatterns 	true 抓取網頁鏈接到的文件。 <p>規則運算式模式清單，其中包括檢索特定 URL，並為這些 URL 網頁上的任何超連結建立索引。符合模式的 URL 會包括在索引中。不符合模式的 URL 會從索引中排除。如果 URL 同時符合包含和排除模式，則排除模式優先，並且 URL /網站的網頁不包含在索引中。</p>

組態	描述
<ul style="list-style-type: none"> • 排除網址 CrawlPatterns • 排除網址 IndexPatterns 	<p>規則運算式模式清單，可排除檢索特定 URL，並為這些 URL 網頁上的任何超連結建立索引。符合模式的 URL 會從索引中排除。不符合模式的 URL 會包括在索引中。如果 URL 同時符合包含和排除模式，則排除模式優先，並且 URL /網站的網頁不包含在索引中。</p>
inclusionFileIndex模式	<p>包含特定網頁檔案的規則運算式模式清單。符合模式的檔案會包括在索引中。不符合模式的檔案會從索引中排除。如果檔案同時符合包含模式和排除模式，則排除模式優先，且檔案不會包含在索引中。</p>
exclusionFileIndex模式	<p>要排除特定網頁檔案的規則運算式模式清單。符合模式的檔案會從索引中排除。與模式不匹配的文件包含在索引中。如果檔案同時符合包含模式和排除模式，則排除模式優先，且檔案不會包含在索引中。</p>
proxy	<p>透過 Web 代理連線到內部網站所需的組態資訊。</p>
託管	<p>您要用來連線至內部網站的 Proxy 伺服器主機名稱。例如，的主機名稱https://a.example.com/page1.html是 "a.example.com"。</p>
port	<p>您要用來連線到內部網站的 Proxy 伺服器連接埠號碼。例如，443 是 HTTPS 的標準連接埠。</p>
秘书 (代理)	<p>如果需要 Web Proxy 憑證才能連線到網站主機，您可以建立儲存認證的 AWS Secrets Manager 密碼。提供 Amazon 資源名稱 (ARN) 的秘密。</p>
type	<p>資料來源的類型。指定WEBCRAWLERV2 為您的資料來源類型。</p>

組態	描述
秘书	<p>如果您的網站需要身份驗證才能訪問網站，則使用該 AWS Secrets Manager 秘密的 Amazon 資源名稱 (ARN)。您可以將網站的驗證認證儲存在包含 JSON 金鑰值配對的密碼中。</p> <p>如果您使用基本或 NTLM/Kerberos，請輸入使用者名稱和密碼。密碼中的 JSON 金鑰必須是 <code>userName</code> 和 <code>password</code>。NTLM 驗證通訊協定包含密碼雜湊，而 Kerberos 驗證通訊協定則包含密碼加密。</p> <p>如果您使用 SAML 或表單驗證，請輸入使用者名稱和密碼、使用者名稱欄位的 XPath (如果使用 SAML，則輸入使用者名稱按鈕)、密碼欄位和按鈕的 XPath，以及登入頁面 URL。密碼中的 JSON 金鑰必須是 <code>userName</code>、<code>password</code>、<code>userNameFieldXPath</code>、<code>userNameButtonXPath</code>、<code>passwordFieldXPath</code>、<code>passwordButtonXPath</code> 和 <code>loginPageUrl</code>。您可以使用 Web 瀏覽器的開發人員工具找到元素的 XPath (XML 路徑語言)。XPath 通常遵循以下格式：<code>//tagname[@Attribute='Value']</code>。</p> <p>Amazon Kendra 還會檢查密碼中包含的端點資訊 (種子 URL) 是否與資料來源端點組態詳細資料中指定的端點資訊相同。</p>
version	目前支援的此範本版本。

Amazon Kendra 網路爬蟲結構描述

```
{
  "$schema": "http://json-schema.org/draft-04/schema#",
  "type": "object",
```

```
"properties": {
  "connectionConfiguration": {
    "type": "object",
    "properties": {
      "repositoryEndpointMetadata": {
        "type": "object",
        "properties": {
          "siteMapUrls": {
            "type": "array",
            "items": {
              "type": "string",
              "pattern": "https://.*"
            }
          },
          "s3SeedUrl": {
            "type": "string",
            "pattern": "s3:.*"
          },
          "s3SiteMapUrl": {
            "type": "string",
            "pattern": "s3:.*"
          },
          "seedUrlConnections": {
            "type": "array",
            "items": [
              {
                "type": "object",
                "properties": {
                  "seedUrl": {
                    "type": "string",
                    "pattern": "https://.*"
                  }
                }
              }
            ],
            "required": [
              "seedUrl"
            ]
          }
        }
      },
      "authentication": {
        "type": "string",
        "enum": [
          "NoAuthentication",
          "BasicAuth",
```

```

        "NTLM_Kerberos",
        "Form",
        "SAML"
    ]
}
}
},
"required": [
    "repositoryEndpointMetadata"
]
},
"repositoryConfigurations": {
    "type": "object",
    "properties": {
        "webPage": {
            "type": "object",
            "properties": {
                "fieldMappings": {
                    "type": "array",
                    "items": [
                        {
                            "type": "object",
                            "properties": {
                                "indexFieldName": {
                                    "type": "string"
                                },
                                "indexFieldType": {
                                    "type": "string",
                                    "enum": [
                                        "STRING",
                                        "DATE",
                                        "LONG"
                                    ]
                                },
                                "dataSourceFieldName": {
                                    "type": "string"
                                },
                                "dateFieldFormat": {
                                    "type": "string",
                                    "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                                }
                            }
                        }
                    ]
                },
                "required": [

```

```
        "indexFieldName",
        "indexFieldType",
        "dataSourceFieldName"
    ]
  }
]
},
"required": [
  "fieldMappings"
],
"attachment": {
  "type": "object",
  "properties": {
    "fieldMappings": {
      "type": "array",
      "items": [
        {
          "type": "object",
          "properties": {
            "indexFieldName": {
              "type": "string"
            },
            "indexFieldType": {
              "type": "string",
              "enum": [
                "STRING",
                "DATE",
                "LONG"
              ]
            },
            "dataSourceFieldName": {
              "type": "string"
            },
            "dateFieldFormat": {
              "type": "string",
              "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
            }
          }
        }
      ]
    },
    "required": [
      "indexFieldName",
      "indexFieldType",
      "dataSourceFieldName"
    ]
  }
}
```

```
        ]
      }
    ]
  },
  "required": [
    "fieldMappings"
  ]
}
},
"syncMode": {
  "type": "string",
  "enum": [
    "FORCED_FULL_CRAWL",
    "FULL_CRAWL"
  ]
},
"additionalProperties": {
  "type": "object",
  "properties": {
    "rateLimit": {
      "type": "string",
      "default": "300"
    },
    "maxFileSize": {
      "type": "string",
      "default": "50"
    },
    "crawlDepth": {
      "type": "string",
      "default": "2"
    },
    "maxLinksPerUrl": {
      "type": "string",
      "default": "100"
    },
    "crawlSubDomain": {
      "type": "boolean",
      "default": false
    },
    "crawlAllDomain": {
      "type": "boolean",
      "default": false
    }
  }
}
```

```
    },
    "honorRobots": {
      "type": "boolean",
      "default": false
    },
    "crawlAttachments": {
      "type": "boolean",
      "default": false
    },
    "inclusionURLCrawlPatterns": {
      "type": "array",
      "items": {
        "type": "string"
      }
    },
    "exclusionURLCrawlPatterns": {
      "type": "array",
      "items": {
        "type": "string"
      }
    },
    "inclusionURLIndexPatterns": {
      "type": "array",
      "items": {
        "type": "string"
      }
    },
    "exclusionURLIndexPatterns": {
      "type": "array",
      "items": {
        "type": "string"
      }
    },
    "inclusionFileIndexPatterns": {
      "type": "array",
      "items": {
        "type": "string"
      }
    },
    "exclusionFileIndexPatterns": {
      "type": "array",
      "items": {
        "type": "string"
      }
    }
  }
```



```
    },
    "proxy": {
      "type": "object",
      "properties": {
        "host": {
          "type": "string"
        },
        "port": {
          "type": "string"
        },
        "secretArn": {
          "type": "string",
          "minLength": 20,
          "maxLength": 2048
        }
      }
    }
  },
  "required": [
    "rateLimit",
    "maxFileSize",
    "crawlDepth",
    "crawlSubDomain",
    "crawlAllDomain",
    "maxLinksPerUrl",
    "honorRobots"
  ],
  "type": {
    "type": "string",
    "pattern": "WEBCRAWLERV2"
  },
  "secretArn": {
    "type": "string",
    "minLength": 20,
    "maxLength": 2048
  }
},
"version": {
  "type": "string",
  "anyOf": [
    {
      "pattern": "1.0.0"
    }
  ]
}
```

```

    ]
  },
  "required": [
    "connectionConfiguration",
    "repositoryConfigurations",
    "syncMode",
    "type",
    "additionalProperties"
  ]
}

```

匯流模板架構

您可以將包含資料來源結構描述的 JSON 納入為 [TemplateConfiguration](#) 物件的一部分。您可以提供 Confluence 主機 URL、主控方法和驗證類型，做為連線組態或存放庫端點詳細資料的一部分。同時將資料來源類型指定為 CONFLUENCEV2、驗證認證的密碼，以及其他必要的組態。然後，您將指定 TEMPLATE 為呼叫 Type 時 [CreateDataSource](#)。

您可以使用本開發人員指南中提供的模板。請參閱 [匯流模式](#)。

下表說明匯合 JSON 結構描述的參數。

組態	描述
連線組態	資料來源端點的組態資訊。
repositoryEndpointMetadata	資料來源的端點資訊。
主机网址	您的匯流執行個體的 URL。例如： https://example.confluence.com 。
type	您的匯流執行個體的託管方法，無論是否 SAAS 為和。ON_PREM
authType	您的匯流執行個體的驗證方法，無論是 Basic0Auth2、或。Personal-token
儲存庫組態	資料來源內容的組態資訊。例如，配置特定類型的內容和欄位對應。

組態	描述
<ul style="list-style-type: none"> • 空格 • page • 博客 • comment • attachment 	<p>將 Confluence 空間、頁面、部落格、註解和附件的屬性或欄位名稱對應至 Amazon Kendra 索引欄位名稱的物件清單。如需詳細資訊，請參閱映射資料來源欄位。Confluence 資料來源欄位名稱必須存在於您的 Confluence 自訂中繼資料中。</p>
附加屬性	資料來源中內容的其他組態選項。
isCrawlAcl	<p>true以編目文件的存取控制清單 (ACL) 資訊，如果您有 ACL，並且想要將其用於存取控制。ACL 會指定使用者和群組可存取的文件。ACL 資訊可用來根據使用者或使用者對文件的群組存取權來篩選搜尋結果。如需詳細資訊，請參閱使用者內容篩選。</p>
fieldForUser識別碼	<p>指定是email否要使用使用者電子郵件作為使用者 ID。email依預設會使用，而且是目前唯一受支援的使用者 ID 類型。</p>
<ul style="list-style-type: none"> • inclusionSpaceKey過濾器 • exclusionSpaceKey過濾器 • pageTitleReg前 • blogTitleReg前 • commentTitleReg前 • attachmentTitleReg前 • inclusionFileType模式 • exclusionFileType模式 • inclusionUrlPatterns • exclusionUrlPatterns 	<p>要包含和/或排除 Confluence 資料來源中某些檔案的規則運算式模式清單。符合模式的檔案會包括在索引中。不符合模式的檔案會從索引中排除。如果檔案同時符合包括模式和排除模式，則以排除模式為優先，且該項目不會包括在索引中。</p>
代理宿主	<p>您使用的 Web Proxy 主機的主機名稱 (不含http://或https://通訊協定)。</p>

組態	描述
代理端口	主機 URL 傳輸通訊協定所使用的連接埠號碼。必須是介於 0 到 65535 之間的數值。
<ul style="list-style-type: none"> • isCrawlPersonal空間 • isCrawlArchived空間 • isCrawlArchived。頁。 • isCrawlPage • isCrawlBlog • isCrawlPage评论 • isCrawlPage附件 • isCrawlBlog评论 • isCrawlBlog附件 	true在您的 Confluence 個人空間，頁面，博客，頁面評論，頁面附件，博客評論和博客附件中抓取文件。
maxFileSizeInMegaBytes	指定 Amazon Kendra 可編目的檔案大小限制 (MB)。Amazon Kendra 只會探索您定義的大小限制內的檔案。預設檔案大小為 50MB。檔案大小上限應該大於 0MB 且小於或等於 50MB。
type	資料來源的類型。指定CONFLUENCEV2 為您的資料來源類型。
enableIdentityCrawler	true，以使用 Amazon Kendra的身分識別爬行者程式來同步使用者和群組的身分識別/主體資訊，以存取特定文件。如果關閉身分搜索器，則可以公開搜索所有文檔。如果您想要對文件使用存取控制，且身分識別編目程式已關閉，您也可以使用 PutPrincipalMapping API 來上傳使用者和群組存取資訊。

組態	描述
同步模式	<p>指定資料來源內容變更時 Amazon Kendra 應如何更新索引。您可以選擇：</p> <ul style="list-style-type: none"> FORCED_FULL_CRAWL 新建索引所有內容，並在每次資料來源與索引同步時取代現有內容。 FULL_CRAWL ，每次您的資料來源與索引同步時，僅對新的、修改和刪除的內容建立索引。Amazon Kendra 可以使用資料來源的機制來追蹤內容變更，並為上次同步後變更的內容建立索引。
秘書	<p>Amazon 資源名稱 (ARN) 的 AWS Secrets Manager 秘密，其中包含連接到您的匯流所需的鍵值對。有關這些鍵值對的信息，請參閱匯合的連接說明。</p>
version	<p>目前支援的此範本版本。</p>

匯流模式

```
{
  "$schema": "http://json-schema.org/draft-04/schema#",
  "type": "object",
  "properties": {
    "connectionConfiguration": {
      "type": "object",
      "properties": {
        "repositoryEndpointMetadata": {
          "type": "object",
          "properties": {
            "hostUrl": {
              "type": "string",
              "pattern": "https:.*"
            },
            "type": {
              "type": "string",

```

```
        "enum": [
            "SAAS",
            "ON_PREM"
        ]
    },
    "authType": {
        "type": "string",
        "enum": [
            "Basic",
            "OAuth2",
            "Personal-token"
        ]
    }
},
"required": [
    "hostUrl",
    "type",
    "authType"
]
}
},
"required": [
    "repositoryEndpointMetadata"
]
},
"repositoryConfigurations": {
    "type": "object",
    "properties": {
        "space": {
            "type": "object",
            "properties": {
                "fieldMappings": {
                    "type": "array",
                    "items": [
                        {
                            "type": "object",
                            "properties": {
                                "indexFieldName": {
                                    "type": "string"
                                },
                                "indexFieldType": {
                                    "type": "string",
                                    "enum": [
                                        "STRING",
```

```
        "STRING_LIST",
        "DATE"
      ]
    },
    "dataSourceFieldName": {
      "type": "string"
    },
    "dateFieldFormat": {
      "type": "string",
      "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
    }
  ],
  "required": [
    "indexFieldName",
    "indexFieldType",
    "dataSourceFieldName"
  ]
}
]
}
},
"required": [
  "fieldMappings"
]
},
"page": {
  "type": "object",
  "properties": {
    "fieldMappings": {
      "type": "array",
      "items": [
        {
          "type": "object",
          "properties": {
            "indexFieldName": {
              "type": "string"
            },
            "indexFieldType": {
              "type": "string",
              "enum": [
                "STRING",
                "STRING_LIST",
                "DATE",
                "LONG"
              ]
            }
          }
        }
      ]
    }
  }
}
```

```

    ]
    },
    "dataSourceFieldName": {
      "type": "string"
    },
    "dateFieldFormat": {
      "type": "string",
      "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
    }
  },
  "required": [
    "indexFieldName",
    "indexFieldType",
    "dataSourceFieldName"
  ]
}
]
}
},
"required": [
  "fieldMappings"
]
},
"blog": {
  "type": "object",
  "properties": {
    "fieldMappings": {
      "type": "array",
      "items": [
        {
          "type": "object",
          "properties": {
            "indexFieldName": {
              "type": "string"
            },
            "indexFieldType": {
              "type": "string",
              "enum": [
                "STRING",
                "STRING_LIST",
                "DATE",
                "LONG"
              ]
            }
          }
        }
      ]
    }
  }
},

```



```
        "dataSourceFieldName": {
          "type": "string"
        },
        "dateFieldFormat": {
          "type": "string",
          "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
        }
      },
      "required": [
        "indexFieldName",
        "indexFieldType",
        "dataSourceFieldName"
      ]
    }
  ]
}
},
"required": [
  "fieldMappings"
]
},
"comment": {
  "type": "object",
  "properties": {
    "fieldMappings": {
      "type": "array",
      "items": [
        {
          "type": "object",
          "properties": {
            "indexFieldName": {
              "type": "string"
            },
            "indexFieldType": {
              "type": "string",
              "enum": [
                "STRING",
                "STRING_LIST",
                "DATE",
                "LONG"
              ]
            }
          }
        }
      ]
    },
    "dataSourceFieldName": {
      "type": "string"
    }
  }
}
```

```
    },
    "dateFieldFormat": {
      "type": "string",
      "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
    }
  },
  "required": [
    "indexFieldName",
    "indexFieldType",
    "dataSourceFieldName"
  ]
}
]
}
},
"required": [
  "fieldMappings"
]
},
"attachment": {
  "type": "object",
  "properties": {
    "fieldMappings": {
      "type": "array",
      "items": [
        {
          "type": "object",
          "properties": {
            "indexFieldName": {
              "type": "string"
            },
            "indexFieldType": {
              "type": "string",
              "enum": [
                "STRING",
                "STRING_LIST",
                "DATE",
                "LONG"
              ]
            },
            "dataSourceFieldName": {
              "type": "string"
            },
            "dateFieldFormat": {
```

```
        "type": "string",
        "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
      }
    },
    "required": [
      "indexFieldName",
      "indexFieldType",
      "dataSourceFieldName"
    ]
  }
]
}
},
"required": [
  "fieldMappings"
]
}
}
},
"additionalProperties": {
  "type": "object",
  "properties": {
    "usersAclS3FilePath": {
      "type": "string"
    },
    "isCrawlAcl": {
      "type": "boolean"
    },
    "fieldForUserId": {
      "type": "string"
    },
    "inclusionSpaceKeyFilter": {
      "type": "array",
      "items": {
        "type": "string"
      }
    },
    "exclusionSpaceKeyFilter": {
      "type": "array",
      "items": {
        "type": "string"
      }
    },
    "pageTitleRegEX": {
```

```
    "type": "array",
    "items": {
      "type": "string"
    }
  },
  "blogTitleRegEX": {
    "type": "array",
    "items": {
      "type": "string"
    }
  },
  "commentTitleRegEX": {
    "type": "array",
    "items": {
      "type": "string"
    }
  },
  "attachmentTitleRegEX": {
    "type": "array",
    "items": {
      "type": "string"
    }
  },
  "isCrawlPersonalSpace": {
    "type": "boolean"
  },
  "isCrawlArchivedSpace": {
    "type": "boolean"
  },
  "isCrawlArchivedPage": {
    "type": "boolean"
  },
  "isCrawlPage": {
    "type": "boolean"
  },
  "isCrawlBlog": {
    "type": "boolean"
  },
  "isCrawlPageComment": {
    "type": "boolean"
  },
  "isCrawlPageAttachment": {
    "type": "boolean"
  },
  },
```

```
"isCrawlBlogComment": {
  "type": "boolean"
},
"isCrawlBlogAttachment": {
  "type": "boolean"
},
"maxFileSizeInMegaBytes": {
  "type": "string"
},
"inclusionFileTypePatterns": {
  "type": "array",
  "items": {
    "type": "string"
  }
},
"exclusionFileTypePatterns": {
  "type": "array",
  "items": {
    "type": "string"
  }
},
"inclusionUrlPatterns": {
  "type": "array",
  "items": {
    "type": "string"
  }
},
"exclusionUrlPatterns": {
  "type": "array",
  "items": {
    "type": "string"
  }
},
"proxyHost": {
  "type": "string"
},
"proxyPort": {
  "type": "string"
}
},
"required": []
},
"type": {
  "type": "string",
```

```
    "pattern": "CONFLUENCEV2"
  },
  "enableIdentityCrawler": {
    "type": "boolean"
  },
  "syncMode": {
    "type": "string",
    "enum": [
      "FULL_CRAWL",
      "FORCED_FULL_CRAWL"
    ]
  },
  "secretArn": {
    "type": "string",
    "minLength": 20,
    "maxLength": 2048
  }
},
"version": {
  "type": "string",
  "anyOf": [
    {
      "pattern": "1.0.0"
    }
  ]
},
"required": [
  "connectionConfiguration",
  "repositoryConfigurations",
  "syncMode",
  "additionalProperties",
  "secretArn",
  "type"
]
}
```

模板架構

您可以將包含資料來源結構描述的 JSON 納入為 [TemplateConfiguration](#) 物件的一部分。您提供 Dropbox 應用程式金鑰、應用程式密鑰和存取權杖，做為儲存驗證憑證的密碼的一部分。還將數據源的類型指定為 DROPBOX，要使用的訪問令牌的類型（臨時或永久）以及其他必要的配置。然後，您將指定 TEMPLATE 為呼叫 Type 時 [CreateDataSource](#)。

您可以使用本開發人員指南中提供的模板。請參閱[結構描述](#)。

下表說明 JSON 結構定義的參數。

組態	描述
連線組態	資料來源端點的組態資訊。
repositoryEndpointMetadata	資料來源的端點資訊。此資料來源未在中指定端點 <code>repositoryEndpointMetadata</code> 。相反地，連線資訊會包含在您提供的 AWS Secrets Manager 密碼中 <code>secretArn</code> 。
儲存庫組態	資料來源內容的組態資訊。例如，配置特定類型的內容和欄位對應。
<ul style="list-style-type: none"> • file • paper • 紙張 • 捷徑 	對應 Dropbox 檔案屬性或欄位名稱的物件清單、Dropbox Paper，以及 Amazon Kendra 索引欄位名稱的捷徑。如需詳細資訊，請參閱 映射資料來源欄位 。
同步模式	<p>指定資料來源內容變更時 Amazon Kendra 應如何更新索引。您可以選擇：</p> <ul style="list-style-type: none"> • <code>FORCED_FULL_CRAWL</code> 新建索引所有內容，並在每次資料來源與索引同步時取代現有內容。 • <code>FULL_CRAWL</code> ，每次您的資料來源與索引同步時，僅對新的、修改和刪除的內容建立索引。Amazon Kendra 可以使用資料來源的機制來追蹤內容變更，並為上次同步後變更的內容建立索引。 • <code>CHANGE_LOG</code> 每次資料來源與索引同步時，僅對新內容和修改的內容建立索引。Amazon Kendra 可以使用資料來源的機制來追蹤內容變更，並為上次同步後變更的內容建立索引。

組態	描述
enableIdentityCrawler	true，以使用 Amazon Kendra 的身分識別爬行者程式來同步使用者和群組的身分識別/主體資訊，以存取特定文件。如果關閉身分搜索器，則可以公開搜索所有文檔。如果您想要對文件使用存取控制，且身分識別編目程式已關閉，您也可以使用 PutPrincipalMapping API 來上傳使用者和群組存取資訊。
秘书	<p>Amazon 資源名稱 (ARN) 的 AWS Secrets Manager 密鑰，其中包含連接到 Dropbox 所需的鍵值對。私密必須包含具有下列索引鍵的 JSON 結構：</p> <pre data-bbox="829 810 1507 1087"> { "appKey": "Dropbox app key", "appSecret": " Dropbox app secret", "accesstoken": " temporary access token or refresh access token" } </pre>
附加屬性	資料來源中內容的其他組態選項。
isCrawlAcl	true 以編目文件的存取控制清單 (ACL) 資訊，如果您有 ACL，並且想要將其用於存取控制。ACL 會指定使用者和群組可存取的文件。ACL 資訊可用來根據使用者或使用者對文件的群組存取權來篩選搜尋結果。如需詳細資訊，請參閱 使用者內容篩選 。
<ul style="list-style-type: none"> • inclusionFileName 模式 • inclusionFileType 模式 	<p>規則運算式模式清單，可在 Dropbox 資料來源中包含特定檔案名稱和類型。符合模式的檔案會包括在索引中。不符合模式的檔案會從索引中排除。如果檔案同時符合包括模式和排除模式，則以排除模式為優先，且該項目不會包括在索引中。</p>

組態	描述
<ul style="list-style-type: none"> exclusionFileName模式 exclusionFileType模式 	排除 Dropbox 資料來源中特定檔案名稱和類型的規則運算式模式清單。符合模式的檔案會從索引中排除。與模式不匹配的文件包含在索引中。如果檔案同時符合排除和包含模式，則排除模式優先，且檔案不會包含在索引中。
<ul style="list-style-type: none"> 爬網文件 爬行紙 爬行紙 爬行捷徑 	true 抓取儲存在 Dropbox 中的檔案、Paper 文件、Dropbox Paper 範本，以及網頁捷徑。
type	資料來源的類型。指定 DROPBOX 為您的資料來源類型。
令牌類型	指定您的訪問令牌類型：永久或臨時訪問令牌。建議您建立一個永遠不會在 Dropbox 中過期的重新整理存取權杖，而不是仰賴在 4 小時後過期的一次性存取權杖。您可以在 Dropbox 開發人員主控台中建立應用程式和重新整理存取權杖，並在密碼中提供存取權杖。
version	目前支援的此範本版本。

結構描述

```
{
  "$schema": "http://json-schema.org/draft-04/schema#",
  "type": "object",
  "properties": {
    "connectionConfiguration": {
      "type": "object",
      "properties": {
        "repositoryEndpointMetadata": {
          "type": "object",
          "properties": {
            }
          }
        }
      }
    }
  }
}
```

```
    }
  },
  "required": [
    "repositoryEndpointMetadata"
  ]
},
"repositoryConfigurations": {
  "type": "object",
  "properties": {
    "file": {
      "type": "object",
      "properties": {
        "fieldMappings": {
          "type": "array",
          "items": {
            "anyOf": [
              {
                "type": "object",
                "properties": {
                  "indexFieldName": {
                    "type": "string"
                  },
                  "indexFieldType": {
                    "type": "string",
                    "enum": [
                      "STRING",
                      "STRING_LIST",
                      "LONG",
                      "DATE"
                    ]
                  },
                  "dataSourceFieldName": {
                    "type": "string"
                  },
                  "dateFieldFormat": {
                    "type": "string",
                    "pattern": "dd-MM-yyyy HH:mm:ss"
                  }
                }
              },
              {
                "type": "object",
                "properties": {
                  "indexFieldName": {
                    "type": "string"
                  },
                  "indexFieldType": {
                    "type": "string",
                    "enum": [
                      "STRING",
                      "STRING_LIST",
                      "LONG",
                      "DATE"
                    ]
                  },
                  "dataSourceFieldName": {
                    "type": "string"
                  }
                }
              }
            ]
          }
        },
        "required": [
          "indexFieldName",
          "indexFieldType",
          "dataSourceFieldName"
        ]
      }
    }
  }
}
```

```
        }
      ]
    }
  },
  "required": [
    "fieldMappings"
  ]
},
"paper": {
  "type": "object",
  "properties": {
    "fieldMappings": {
      "type": "array",
      "items": {
        "anyOf": [
          {
            "type": "object",
            "properties": {
              "indexFieldName": {
                "type": "string"
              },
              "indexFieldType": {
                "type": "string",
                "enum": [
                  "STRING",
                  "STRING_LIST",
                  "LONG",
                  "DATE"
                ]
              },
              "dataSourceFieldName": {
                "type": "string"
              },
              "dateFieldFormat": {
                "type": "string",
                "pattern": "dd-MM-yyyy HH:mm:ss"
              }
            }
          },
          "required": [
            "indexFieldName",
            "indexFieldType",
            "dataSourceFieldName"
          ]
        ]
      }
    }
  }
}
```

```
        }
      ]
    }
  },
  "required": [
    "fieldMappings"
  ],
},
"papert": {
  "type": "object",
  "properties": {
    "fieldMappings": {
      "type": "array",
      "items": {
        "anyOf": [
          {
            "type": "object",
            "properties": {
              "indexFieldName": {
                "type": "string"
              },
            },
            "indexFieldType": {
              "type": "string",
              "enum": [
                "STRING",
                "STRING_LIST",
                "LONG",
                "DATE"
              ]
            },
          },
          {
            "dataSourceFieldName": {
              "type": "string"
            },
            "dateFieldFormat": {
              "type": "string",
              "pattern": "dd-MM-yyyy HH:mm:ss"
            }
          }
        ],
      },
      "required": [
        "indexFieldName",
        "indexFieldType",
        "dataSourceFieldName"
      ]
    }
  ]
}
```

```
        }
      ]
    }
  },
  "required": [
    "fieldMappings"
  ]
},
"shortcut": {
  "type": "object",
  "properties": {
    "fieldMappings": {
      "type": "array",
      "items": {
        "anyOf": [
          {
            "type": "object",
            "properties": {
              "indexFieldName": {
                "type": "string"
              },
            },
            "indexFieldType": {
              "type": "string",
              "enum": [
                "STRING",
                "STRING_LIST",
                "LONG",
                "DATE"
              ]
            },
          },
          {
            "dataSourceFieldName": {
              "type": "string"
            },
            "dateFieldFormat": {
              "type": "string",
              "pattern": "dd-MM-yyyy HH:mm:ss"
            }
          }
        ]
      },
      "required": [
        "indexFieldName",
        "indexFieldType",
        "dataSourceFieldName"
      ]
    }
  ]
}
```

```
        }
      ]
    }
  },
  "required": [
    "fieldMappings"
  ]
}
},
"syncMode": {
  "type": "string",
  "enum": [
    "FULL_CRAWL",
    "FORCED_FULL_CRAWL",
    "CHANGE_LOG"
  ]
},
"enableIdentityCrawler": {
  "type": "boolean"
},
"secretArn": {
  "type": "string"
},
"additionalProperties": {
  "type": "object",
  "properties": {
    "isCrawlAcl": {
      "type": "boolean"
    },
    "inclusionFileNamePatterns": {
      "type": "array"
    },
    "exclusionFileNamePatterns": {
      "type": "array"
    },
    "inclusionFileTypePatterns": {
      "type": "array"
    },
    "exclusionFileTypePatterns": {
      "type": "array"
    },
    "crawlFile": {
```

```
        "type": "boolean"
      },
      "crawlPaper": {
        "type": "boolean"
      },
      "crawlPapert": {
        "type": "boolean"
      },
      "crawlShortcut": {
        "type": "boolean"
      }
    }
  },
  "type": {
    "type": "string",
    "pattern": "DROPBOX"
  },
  "tokenType": {
    "type": "string",
    "enum": [
      "PERMANENT",
      "TEMPORARY"
    ]
  },
  "version": {
    "type": "string",
    "anyOf": [
      {
        "pattern": "1.0.0"
      }
    ]
  }
},
"additionalProperties": false,
"required": [
  "connectionConfiguration",
  "repositoryConfigurations",
  "additionalProperties",
  "syncMode",
  "enableIdentityCrawler",
  "secretArn",
  "type",
  "tokenType"
]
```

}

Drupal 的模板架構

您可以將包含資料來源結構描述的 JSON 納入為 [TemplateConfiguration](#) 物件的一部分。您提供 Drupal 主機 URL 和身份驗證類型作為連接配置或儲存庫端點詳細信息的一部分。還將數據源的類型指定為 DRUPAL，身份驗證憑據的秘密以及其他必要的配置。然後，您將指定 TEMPLATE 為呼叫 Type 時 [CreateDataSource](#)。

您可以使用本開發人員指南中提供的模板。請參閱 [JSON 模式](#)。

下表描述了 Drupal 的 JSON 模式的參數。

組態	描述
連線組態	資料來源端點的組態資訊。
repositoryEndpointMetadata	資料來源的端點資訊。
主机网址	您的 Drupal 網站的主機網址。例如， <code>HTTPS#/// <hostname><drupals itename></code> 。
儲存庫組態	資料來源內容的組態資訊。
<ul style="list-style-type: none"> 內容 comment attachment 	映射 Drupal 文件的屬性或字段名稱的對象列表。如需詳細資訊，請參閱 映射資料來源欄位 。Drupal 數據源字段名稱必須存在於您的 Drupal 自定義元數據中。
附加屬性	資料來源中內容的其他組態選項。
<ul style="list-style-type: none"> inclusionFileName 模式 articleTitleInclusion 模式 pageTitleInclusion 模式 customContentTitleInclusionPatterns basicBlockTitleInclusionPatterns customBlockTitleInclusionPatterns 	正則表達式模式列表，以包含 Drupal 數據源中的某些文件。符合模式的檔案會包括在索引中。不符合模式的檔案會從索引中排除。如果檔案同時符合包括模式和排除模式，則以排除模式為優先，且該項目不會包括在索引中。

組態	描述
<ul style="list-style-type: none"> • exclusionFileName模式 • articleTitleExclusion模式 • pageTitleExclusion模式 • customContentTitleExclusionPatterns • basicBlockTitleExclusionPatterns • customBlockTitleExclusionPatterns 	<p>正則表達式模式列表，以排除 Drupal 數據源中的某些文件。符合模式的檔案會從索引中排除。與模式不匹配的文件包含在索引中。如果檔案同時符合排除和包含模式，則排除模式優先，且檔案不會包含在索引中。</p>
<p>內容定義</p> <ul style="list-style-type: none"> • ContentType • 欄位定義 • isCrawlComments • isCrawlFiles • isCrawlArticle • isCrawlBasic。頁。 • isCrawlBasic阻止 • isCrawlCustomContentTypesList 	<p>指定要編目的內容類型，以及是否要編目所選內容類型的註解和附件。</p>
<p>type</p>	<p>資料來源的類型。指定DRUPAL為您的資料來源類型。</p>
<p>authType</p>	<p>您使用的驗證類型，無論是BASIC-AUTH 或OAUTH2。</p>

組態	描述
<p>同步模式</p>	<p>指定資料來源內容變更時 Amazon Kendra 應如何更新索引。您可以選擇：</p> <ul style="list-style-type: none"> • FORCED_FULL_CRAWL 新建索引所有內容，並在每次資料來源與索引同步時取代現有內容。 • FULL_CRAWL ，每次您的資料來源與索引同步時，僅對新的、修改和刪除的內容建立索引。Amazon Kendra 可以使用資料來源的機制來追蹤內容變更，並為上次同步後變更的內容建立索引。 • CHANGE_LOG 每次資料來源與索引同步時，僅對新內容和修改的內容建立索引。Amazon Kendra 可以使用資料來源的機制來追蹤內容變更，並為上次同步後變更的內容建立索引。
<p><code>enableIdentityCrawler</code></p>	<p><code>true</code>，以使用 Amazon Kendra 的身分識別爬行者程式來同步使用者和群組的身分識別/主體資訊，以存取特定文件。如果關閉身分搜索器，則可以公開搜索所有文檔。如果您想要對文件使用存取控制，且身分識別編目程式已關閉，您也可以使用 PutPrincipalMapping API 來上傳使用者和群組存取資訊。</p>

組態	描述
秘书	<p>Amazon 資源名稱 (ARN) 的 AWS Secrets Manager 秘密，其中包含連接到 Drupal 所需的鍵值對。私密必須包含具有下列索引鍵的 JSON 結構：</p> <p>如果使用基本驗證：</p> <pre data-bbox="829 520 1507 720"> { "username": "user name", "passwords": "password" } </pre> <p>如果使用 OAuth 2.0 身份驗證：</p> <pre data-bbox="829 831 1507 1108"> { "username": "user name", "password": "password", "clientId": "client id", "clientSecret": "client secret" } </pre>
version	目前支援的此範本版本。

JSON 模式

```

{
  "$schema": "http://json-schema.org/draft-04/schema#",
  "type": "object",
  "properties": {
    "connectionConfiguration": {
      "type": "object",
      "properties": {
        "repositoryEndpointMetadata": {
          "type": "object",
          "properties": {
            "hostUrl": {
              "type": "string",
              "pattern": "https:.*"
            }
          }
        }
      }
    }
  }
}

```

```
    }
  },
  "required": [
    "hostUrl"
  ]
},
"required": [
  "repositoryEndpointMetadata"
],
"repositoryConfigurations": {
  "type": "object",
  "properties": {
    "content": {
      "type": "object",
      "properties": {
        "fieldMappings": {
          "type": "array",
          "items": [
            {
              "type": "object",
              "properties": {
                "indexFieldName": {
                  "type": "string"
                },
                "indexFieldType": {
                  "type": "string",
                  "enum": [
                    "STRING",
                    "DATE"
                  ]
                },
                "dataSourceFieldName": {
                  "type": "string"
                },
                "dateFieldFormat": {
                  "type": "string",
                  "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                }
              }
            }
          ]
        },
        "required": [
          "indexFieldName",
          "indexFieldType",
```

```
        "dataSourceFieldName"
      ]
    }
  ]
},
"required": [
  "fieldMappings"
],
"comment": {
  "type": "object",
  "properties": {
    "fieldMappings": {
      "type": "array",
      "items": [
        {
          "type": "object",
          "properties": {
            "indexFieldName": {
              "type": "string"
            },
            "indexFieldType": {
              "type": "string",
              "enum": [
                "STRING",
                "DATE"
              ]
            },
            "dataSourceFieldName": {
              "type": "string"
            },
            "dateFieldFormat": {
              "type": "string",
              "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
            }
          }
        }
      ]
    },
    "required": [
      "indexFieldName",
      "indexFieldType",
      "dataSourceFieldName"
    ]
  }
}
```

```
    }
  },
  "required": [
    "fieldMappings"
  ]
},
"attachment": {
  "type": "object",
  "properties": {
    "fieldMappings": {
      "type": "array",
      "items": [
        {
          "type": "object",
          "properties": {
            "indexFieldName": {
              "type": "string"
            },
            "indexFieldType": {
              "type": "string",
              "enum": [
                "STRING",
                "DATE"
              ]
            },
            "dataSourceFieldName": {
              "type": "string"
            },
            "dateFieldFormat": {
              "type": "string",
              "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
            }
          }
        }
      ]
    },
    "required": [
      "indexFieldName",
      "indexFieldType",
      "dataSourceFieldName"
    ]
  }
}
},
"required": [
  "fieldMappings"
```

```
    ]
  }
}
},
"additionalProperties": {
  "type": "object",
  "properties": {
    "isCrawlArticle": {
      "type": "boolean"
    },
    "isCrawlBasicPage": {
      "type": "boolean"
    },
    "isCrawlBasicBlock": {
      "type": "boolean"
    },
    "crawlCustomContentTypesList": {
      "type": "array",
      "items": {
        "type": "string"
      }
    },
    "crawlCustomBlockTypesList": {
      "type": "array",
      "items": {
        "type": "string"
      }
    },
    "filePath": {
      "anyOf": [
        {
          "type": "string",
          "pattern": "s3:.*"
        },
        {
          "type": "string",
          "pattern": ""
        }
      ]
    },
    "inclusionFileNamePatterns": {
      "type": "array",
      "items": {
        "type": "string"
      }
    }
  }
}
```

```
    }
  },
  "exclusionFileNamePatterns": {
    "type": "array",
    "items": {
      "type": "string"
    }
  },
  "articleTitleInclusionPatterns": {
    "type": "array",
    "items": {
      "type": "string"
    }
  },
  "articleTitleExclusionPatterns": {
    "type": "array",
    "items": {
      "type": "string"
    }
  },
  "pageTitleInclusionPatterns": {
    "type": "array",
    "items": {
      "type": "string"
    }
  },
  "pageTitleExclusionPatterns": {
    "type": "array",
    "items": {
      "type": "string"
    }
  },
  "customContentTitleInclusionPatterns": {
    "type": "array",
    "items": {
      "type": "string"
    }
  },
  "customContentTitleExclusionPatterns": {
    "type": "array",
    "items": {
      "type": "string"
    }
  },
},
```



```
"basicBlockTitleInclusionPatterns": {
  "type": "array",
  "items": {
    "type": "string"
  }
},
"basicBlockTitleExclusionPatterns": {
  "type": "array",
  "items": {
    "type": "string"
  }
},
"customBlockTitleInclusionPatterns": {
  "type": "array",
  "items": {
    "type": "string"
  }
},
"customBlockTitleExclusionPatterns": {
  "type": "array",
  "items": {
    "type": "string"
  }
},
"contentDefinitions": {
  "type": "array",
  "items": {
    "properties": {
      "contentType": {
        "type": "string"
      }
    },
    "fieldDefinition": {
      "type": "array",
      "items": [
        {
          "type": "object",
          "properties": {
            "machineName": {
              "type": "string"
            }
          },
          "type": {
            "type": "string"
          }
        }
      ]
    }
  }
},
```

```
        "required": [
            "machineName",
            "type"
        ]
    },
    ],
    "isCrawlComments": {
        "type": "boolean"
    },
    "isCrawlFiles": {
        "type": "boolean"
    }
},
"required": [
    "contentType",
    "fieldDefinition",
    "isCrawlComments",
    "isCrawlFiles"
]
}
},
"required": []
},
"type": {
    "type": "string",
    "pattern": "DRUPAL"
},
"authType": {
    "type": "string",
    "enum": [
        "BASIC-AUTH",
        "OAUTH2"
    ]
},
"syncMode": {
    "type": "string",
    "enum": [
        "FORCED_FULL_CRAWL",
        "FULL_CRAWL",
        "CHANGE_LOG"
    ]
}
},
```

```

"enableIdentityCrawler": {
  "type": "boolean"
},
"secretArn": {
  "type": "string",
  "minLength": 20,
  "maxLength": 2048
}
},
"version": {
  "type": "string",
  "anyOf": [
    {
      "pattern": "1.0.0"
    }
  ]
},
"required": [
  "connectionConfiguration",
  "repositoryConfigurations",
  "syncMode",
  "additionalProperties",
  "secretArn",
  "type"
]
}

```

GitHub 模板架構

您可以將包含資料來源結構描述的 JSON 納入為 [TemplateConfiguration](#) 物件的一部分。您可以提供 GitHub 主機 URL、組織名稱，以及是否使用 GitHub 雲端或 GitHub 內部部署做為連線組態或存放庫端點詳細資料的一部分。同時將資料來源類型指定為 GITHUB、驗證認證的密碼，以及其他必要的組態。然後，您將指定 TEMPLATE 為呼叫 Type 時 [CreateDataSource](#)。

您可以使用本開發人員指南中提供的模板。請參閱 [GitHub 結構定義](#)。

下表說明 GitHub JSON 結構定義的參數。

組態	描述
連線組態	資料來源端點的組態資訊。

組態	描述
repositoryEndpointMetadata	資料來源的端點資訊。
type	將類型指定為SAAS或ON_PREMISE。
主机網址	主 GitHub 機網址。例如，如果您使用 GitHub SaaS /企業雲端：。https://api.github.com或者，如果您使用 GitHub內部部署/企業伺服器：。https://on-prem-host-url/api/v3/
組織名稱	您可以在登入 GitHub 桌面時找到您的組織名稱，然後前往您的個人資料圖片下拉式清單下的「您的組織」。
儲存庫組態	資料來源內容的組態資訊。例如，配置特定類型的內容和欄位對應。
<ul style="list-style-type: none"> 血液儲存庫 GHCommit ghIssueDocument ghIssueComment ghIssueAttachment 生長激素文件 生長激素評論 生長激素附件 	將 GitHub 內容的屬性或欄位名稱對應至 Amazon Kendra 索引欄位名稱的物件清單。如需詳細資訊，請參閱 映射資料來源欄位 。
附加屬性	資料來源中內容的其他組態選項。
isCrawlAcl	true以編目文件的存取控制清單 (ACL) 資訊，如果您有 ACL，並且想要將其用於存取控制。ACL 指定使用者和群組可以存取和搜尋的文件。ACL 資訊可用來根據使用者或使用者對文件的群組存取權來篩選搜尋結果。如需詳細資訊，請參閱 使用者內容篩選 。

組態	描述
fieldForUser識別碼	指定您要用於 ACL 探索的使用者識別碼類型。指定是email否要使用使用者電子郵件作為使用者 ID，或是username要使用使用者名稱作為使用者 ID。如果您沒有指定選項，則email默認使用。
儲存庫過濾器	您要索引的特定儲存庫和分支名稱的名稱列表。
爬行儲存庫	true抓取儲存庫。
crawlRepositoryDocuments	true編目儲存庫文件。
克勞利蘇	true抓取問題。
crawlIssueComment	true抓取問題評論。
crawlIssueComment附件	true抓取問題評論附件。
crawlPullRequest	true以編目提取請求。
crawlPullRequest评论	true抓取提取請求註釋。
crawlPullRequestCommentAttachment	true抓取提取請求評論附件。
<ul style="list-style-type: none"> inclusionFolderName模式 inclusionFileType模式 inclusionFileName模式 	在 GitHub資料來源中包含特定內容的規則運算式模式清單。符合模式的內容會包含在索引中。與模式不匹配的內容會從索引中排除。如果有任何內容同時符合包含和排除模式，則排除模式優先，且內容不會包含在索引中。
<ul style="list-style-type: none"> exclusionFolderName模式 exclusionFileType模式 exclusionFileName模式 	用於排除 GitHub資料來源中某些內容的規則運算式模式清單。符合模式的內容會從索引中排除。與模式不匹配的內容包含在索引中。如果有任何內容同時符合包含和排除模式，則排除模式優先，且內容不會包含在索引中。
type	資料來源的類型。指定GITHUB為您的資料來源類型。

組態	描述
enableIdentityCrawler	<p>true，以使用 Amazon Kendra 的身分識別爬行者程式來同步使用者和群組的身分識別/主體資訊，以存取特定文件。如果關閉身分搜索器，則可以公開搜索所有文檔。如果您想要對文件使用存取控制，且身分識別編目程式已關閉，您也可以使用 PutPrincipalMapping API 來上傳使用者和群組存取資訊。</p>
同步模式	<p>指定資料來源內容變更時 Amazon Kendra 應如何更新索引。您可以選擇：</p> <ul style="list-style-type: none"> • FORCED_FULL_CRAWL 新建索引所有內容，並在每次資料來源與索引同步時取代現有內容。 • FULL_CRAWL，每次您的資料來源與索引同步時，僅對新的、修改和刪除的內容建立索引。Amazon Kendra 可以使用資料來源的機制來追蹤內容變更，並為上次同步後變更的內容建立索引。 • CHANGE_LOG 每次資料來源與索引同步時，僅對新內容和修改的內容建立索引。Amazon Kendra 可以使用資料來源的機制來追蹤內容變更，並為上次同步後變更的內容建立索引。
秘書	<p>Amazon 資源名稱 (ARN) 的 AWS Secrets Manager 秘密，其中包含連接到 GitHub 私密必須包含具有下列索引鍵的 JSON 結構：</p> <pre data-bbox="829 1514 1507 1675"> { "personalToken": " <i>token</i> " } </pre>
version	此範本目前支援的版本。

GitHub 結構定義

以下是 GitHub JSON 結構定義：

```
{
  "$schema": "http://json-schema.org/draft-04/schema#",
  "type": "object",
  "properties": {
    "connectionConfiguration": {
      "type": "object",
      "properties": {
        "repositoryEndpointMetadata": {
          "type": "object",
          "properties": {
            "type": {
              "type": "string"
            },
            "hostUrl": {
              "type": "string",
              "pattern": "https://.*"
            },
            "organizationName": {
              "type": "string"
            }
          }
        },
        "required": [
          "type",
          "hostUrl",
          "organizationName"
        ]
      }
    },
    "required": [
      "repositoryEndpointMetadata"
    ]
  },
  "repositoryConfigurations": {
    "type": "object",
    "properties": {
      "ghRepository": {
        "type": "object",
        "properties": {
          "fieldMappings": {
            "type": "array",

```

```

        "items": [
            {
                "type": "object",
                "properties": {
                    "indexFieldName": {
                        "type": "string"
                    },
                    "indexFieldType": {
                        "type": "string",
                        "enum": [
                            "STRING",
                            "STRING_LIST",
                            "DATE"
                        ]
                    },
                    "dataSourceFieldName": {
                        "type": "string"
                    },
                    "dateFieldFormat": {
                        "type": "string",
                        "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                    }
                },
                "required": [
                    "indexFieldName",
                    "indexFieldType",
                    "dataSourceFieldName"
                ]
            }
        ]
    },
    "required": [
        "fieldMappings"
    ]
},
"ghCommit": {
    "type": "object",
    "properties": {
        "fieldMappings": {
            "type": "array",
            "items": [
                {
                    "type": "object",

```



```
        "properties": {
            "indexFieldName": {
                "type": "string"
            },
            "indexFieldType": {
                "type": "string",
                "enum": [
                    "STRING",
                    "STRING_LIST",
                    "DATE"
                ]
            },
            "dataSourceFieldName": {
                "type": "string"
            },
            "dateFieldFormat": {
                "type": "string",
                "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
            }
        },
        "required": [
            "indexFieldName",
            "indexFieldType",
            "dataSourceFieldName"
        ]
    }
}
},
"required": [
    "fieldMappings"
],
"ghIssueDocument": {
    "type": "object",
    "properties": {
        "fieldMappings": {
            "type": "array",
            "items": [
                {
                    "type": "object",
                    "properties": {
                        "indexFieldName": {
                            "type": "string"
                        }
                    }
                }
            ]
        }
    }
}
```

```

        },
        "indexFieldType": {
            "type": "string",
            "enum": [
                "STRING",
                "STRING_LIST",
                "DATE"
            ]
        },
        "dataSourceFieldName": {
            "type": "string"
        },
        "dateFieldFormat": {
            "type": "string",
            "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
        }
    },
    "required": [
        "indexFieldName",
        "indexFieldType",
        "dataSourceFieldName"
    ]
}
]
}
},
"required": [
    "fieldMappings"
]
},
"ghIssueComment": {
    "type": "object",
    "properties": {
        "fieldMappings": {
            "type": "array",
            "items": [
                {
                    "type": "object",
                    "properties": {
                        "indexFieldName": {
                            "type": "string"
                        },
                    },
                    "indexFieldType": {
                        "type": "string",

```

```

        "enum": [
            "STRING",
            "STRING_LIST",
            "DATE"
        ]
    },
    "dataSourceFieldName": {
        "type": "string"
    },
    "dateFieldFormat": {
        "type": "string",
        "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
    }
},
"required": [
    "indexFieldName",
    "indexFieldType",
    "dataSourceFieldName"
]
}
]
}
},
"required": [
    "fieldMappings"
]
},
"ghIssueAttachment": {
    "type": "object",
    "properties": {
        "fieldMappings": {
            "type": "array",
            "items": [
                {
                    "type": "object",
                    "properties": {
                        "indexFieldName": {
                            "type": "string"
                        },
                    },
                    "indexFieldType": {
                        "type": "string",
                        "enum": [
                            "STRING",
                            "STRING_LIST",

```

```

        "DATE"
      ]
    },
    "dataSourceFieldName": {
      "type": "string"
    },
    "dateFieldFormat": {
      "type": "string",
      "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
    }
  },
  "required": [
    "indexFieldName",
    "indexFieldType",
    "dataSourceFieldName"
  ]
}
]
}
},
"required": [
  "fieldMappings"
]
},
"ghPRDocument": {
  "type": "object",
  "properties": {
    "fieldMappings": {
      "type": "array",
      "items": [
        {
          "type": "object",
          "properties": {
            "indexFieldName": {
              "type": "string"
            },
            "indexFieldType": {
              "type": "string",
              "enum": [
                "STRING",
                "STRING_LIST",
                "DATE"
              ]
            }
          }
        }
      ]
    }
  }
},

```

```

        "dataSourceFieldName": {
            "type": "string"
        },
        "dateFieldFormat": {
            "type": "string",
            "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
        }
    },
    "required": [
        "indexFieldName",
        "indexFieldType",
        "dataSourceFieldName"
    ]
}
]
}
},
"required": [
    "fieldMappings"
]
},
"ghPRComment": {
    "type": "object",
    "properties": {
        "fieldMappings": {
            "type": "array",
            "items": [
                {
                    "type": "object",
                    "properties": {
                        "indexFieldName": {
                            "type": "string"
                        },
                        "indexFieldType": {
                            "type": "string",
                            "enum": [
                                "STRING",
                                "STRING_LIST",
                                "DATE"
                            ]
                        }
                    },
                    "dataSourceFieldName": {
                        "type": "string"
                    }
                }
            ]
        }
    }
}

```

```

        "dateFieldFormat": {
            "type": "string",
            "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
        }
    },
    "required": [
        "indexFieldName",
        "indexFieldType",
        "dataSourceFieldName"
    ]
}
]
}
},
"required": [
    "fieldMappings"
]
},
"ghPRAttachment": {
    "type": "object",
    "properties": {
        "fieldMappings": {
            "type": "array",
            "items": [
                {
                    "type": "object",
                    "properties": {
                        "indexFieldName": {
                            "type": "string"
                        },
                    },
                    "indexFieldType": {
                        "type": "string",
                        "enum": [
                            "STRING",
                            "STRING_LIST",
                            "DATE"
                        ]
                    },
                }
            ],
        },
        "dataSourceFieldName": {
            "type": "string"
        },
        "dateFieldFormat": {
            "type": "string",
            "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
        }
    }
}

```

```
        }
      },
      "required": [
        "indexFieldName",
        "indexFieldType",
        "dataSourceFieldName"
      ]
    }
  ]
},
"required": [
  "fieldMappings"
]
}
},
"additionalProperties": {
  "type": "object",
  "properties": {
    "isCrawlAcl": {
      "type": "boolean"
    },
    "fieldForUserId": {
      "type": "string"
    },
    "crawlRepository": {
      "type": "boolean"
    },
    "crawlRepositoryDocuments": {
      "type": "boolean"
    },
    "crawlIssue": {
      "type": "boolean"
    },
    "crawlIssueComment": {
      "type": "boolean"
    },
    "crawlIssueCommentAttachment": {
      "type": "boolean"
    },
    "crawlPullRequest": {
      "type": "boolean"
    }
  },
}
```

```
"crawlPullRequestComment": {
  "type": "boolean"
},
"crawlPullRequestCommentAttachment": {
  "type": "boolean"
},
"repositoryFilter": {
  "type": "array",
  "items": [
    {
      "type": "object",
      "properties": {
        "repositoryName": {
          "type": "string"
        },
        "branchNameList": {
          "type": "array",
          "items": {
            "type": "string"
          }
        }
      }
    }
  ]
},
"inclusionFolderNamePatterns": {
  "type": "array",
  "items": {
    "type": "string"
  }
},
"inclusionFileTypePatterns": {
  "type": "array",
  "items": {
    "type": "string"
  }
},
"inclusionFileNamePatterns": {
  "type": "array",
  "items": {
    "type": "string"
  }
},
"exclusionFolderNamePatterns": {
```



```
        "type": "array",
        "items": {
            "type": "string"
        }
    },
    "exclusionFileTypePatterns": {
        "type": "array",
        "items": {
            "type": "string"
        }
    },
    "exclusionFileNamePatterns": {
        "type": "array",
        "items": {
            "type": "string"
        }
    }
},
"required": []
},
"type": {
    "type": "string",
    "pattern": "GITHUB"
},
"syncMode": {
    "type": "string",
    "enum": [
        "FULL_CRAWL",
        "FORCED_FULL_CRAWL",
        "CHANGE_LOG"
    ]
},
"enableIdentityCrawler": {
    "type": "boolean"
},
"secretArn": {
    "type": "string",
    "minLength": 20,
    "maxLength": 2048
}
},
"version": {
    "type": "string",
    "anyOf": [
```

```

        {
            "pattern": "1.0.0"
        }
    ],
    "required": [
        "connectionConfiguration",
        "repositoryConfigurations",
        "syncMode",
        "additionalProperties",
        "enableIdentityCrawler"
    ]
}

```

模板架構


您可以將包含資料來源結構描述的 JSON 納入為 [TemplateConfiguration](#) 物件的一部分。將資料來源類型指定為 GMAIL、驗證認證的密碼，以及其他必要的組態。然後，您將指定 TEMPLATE 為呼叫 Type 時 [CreateDataSource](#)。

您可以使用本開發人員指南中提供的模板。請參閱 [結構描述](#)。

下表說明 Gmail JSON 結構定義的參數。

組態	描述
連線組態	資料來源端點的組態資訊。
repositoryEndpointMetadata	資料來源的端點資訊。此資料來源未在中指定端點 repositoryEndpointMetadata 。相反地，連線資訊會包含在您提供的 AWS Secrets Manager 密碼中 secretArn 。
儲存庫組態	資料來源內容的組態資訊。例如，配置特定類型的內容和欄位對應。指定資料來源的類型和秘密 ARN。
<ul style="list-style-type: none"> message 附件 	將 Gmail 郵件和附件的屬性或欄位名稱對應至 Amazon Kendra 索引欄位名稱的物件清單。如需詳細資訊，請參閱 映射資料來源欄位 。

組態	描述
附加屬性	資料來源中內容的其他組態選項。
<ul style="list-style-type: none"> • inclusionLabelName 模式 • exclusionLabelName 模式 • inclusionAttachmentType 模式 • exclusionAttachmentType 模式 • inclusionAttachmentName 模式 • exclusionAttachmentName 模式 • inclusionSubjectFilter • exclusionSubjectFilter • isSubjectAnd • inclusionFromFilter • exclusionFromFilter • inclusionToFilter • exclusionToFilter • inclusionCcFilter • exclusionCcFilter • inclusionBccFilter • exclusionBccFilter 	規則運算式模式清單，可在 Gmail 資料來源中包含或排除具有特定主旨名稱的郵件。符合模式的檔案會包括在索引中。如果檔案同時符合包含檔案和排除模式，則排除模式優先，且該檔案不會包含在索引中。
beforeDateFilter	指定在特定日期之前要包含的郵件和附件。
afterDateFilter	指定在特定日期之後要包含的郵件和附件。
isCrawlAttachment	Boolean 值，用來選擇是否要編目附件。訊息會自動編目。
type	資料來源的類型。指定GMAIL為您的資料來源類型。
shouldCrawlDraft 訊息	Boolean 值，用來選擇是否要編目草稿郵件。

組態	描述
同步模式	<p>指定資料來源內容變更時 Amazon Kendra 應如何更新索引。您可以選擇：</p> <ul style="list-style-type: none">• <code>FORCED_FULL_CRAWL</code> 新建索引所有內容，並在每次資料來源與索引同步時取代現有內容。• <code>FULL_CRAWL</code>，每次您的資料來源與索引同步時，僅對新的、修改和刪除的內容建立索引。Amazon Kendra 可以使用資料來源的機制來追蹤內容變更，並為上次同步後變更的內容建立索引。 <div data-bbox="829 806 1507 1560" style="border: 1px solid #f08080; border-radius: 10px; padding: 10px;"><p> Important</p><p>由於沒有 API 可以更新永久刪除的 Gmail 郵件，因此任何新的，修改或刪除的內容同步：</p><ul style="list-style-type: none">• 不會從 Amazon Kendra 索引移除 Gmail 中永久刪除的郵件• 不會同步 Gmail 電子郵件標籤中的變更<p>若要將 Gmail 資料來源標籤變更和永久刪除的電子郵件訊息同步至 Amazon Kendra 索引，您必須定期執行完整檢索。</p></div>

組態	描述
秘書	<p>秘 Secrets Manager 秘密的 Amazon 資源名稱 (ARN) ，其中包含連接到 Gmail 所需的鍵值對。私密必須包含具有下列索引鍵的 JSON 結構：</p> <pre data-bbox="829 443 1507 758"> { "adminAccountEmailId": " <i>service account email</i>", "clientEmailId": " <i>user account email</i>", "privateKey": " <i>private key</i>" } </pre>
version	目前支援的範本版本。

結構描述

```

{
  "$schema": "http://json-schema.org/draft-04/schema#",
  "type": "object",
  "properties": {
    "connectionConfiguration": {
      "type": "object",
      "properties": {
      }
    },
    "repositoryConfigurations": {
      "type": "object",
      "properties": {
        "message": {
          "type": "object",
          "properties": {
            "fieldMappings": {
              "type": "array",
              "items": [
                {
                  "type": "object",
                  "properties": {
                    "indexFieldName": {

```

```
        "type": "string"
      },
      "indexFieldType": {
        "type": "string",
        "enum": ["STRING", "STRING_LIST", "DATE"]
      },
      "dataSourceFieldName": {
        "type": "string"
      },
      "dateFieldFormat": {
        "type": "string"
      }
    },
    "required": [
      "indexFieldName",
      "indexFieldType",
      "dataSourceFieldName"
    ]
  }
]
}
},
"attachments": {
  "type": "object",
  "properties": {
    "fieldMappings": {
      "type": "array",
      "items": [
        {
          "type": "object",
          "properties": {
            "indexFieldName": {
              "type": "string"
            },
            "indexFieldType": {
              "type": "string",
              "enum": ["STRING"]
            },
            "dataSourceFieldName": {
              "type": "string"
            }
          }
        }
      ]
    },
    "required": [
```

```
        "indexFieldName",
        "indexFieldType",
        "dataSourceFieldName"
    ]
  }
]
}
}
},
"required": []
},
"additionalProperties": {
  "type": "object",
  "properties": {
    "inclusionLabelNamePatterns": {
      "type": "array",
      "items": {
        "type": "string"
      }
    },
    "exclusionLabelNamePatterns": {
      "type": "array",
      "items": {
        "type": "string"
      }
    },
    "inclusionAttachmentTypePatterns": {
      "type": "array",
      "items": {
        "type": "string"
      }
    },
    "exclusionAttachmentTypePatterns": {
      "type": "array",
      "items": {
        "type": "string"
      }
    },
    "inclusionAttachmentNamePatterns": {
      "type": "array",
      "items": {
        "type": "string"
      }
    }
  }
}
```

```
    },
    "exclusionAttachmentNamePatterns": {
      "type": "array",
      "items": {
        "type": "string"
      }
    },
  },
  "inclusionSubjectFilter": {
    "type": "array",
    "items": {
      "type": "string"
    }
  },
  "exclusionSubjectFilter": {
    "type": "array",
    "items": {
      "type": "string"
    }
  },
  "isSubjectAnd": {
    "type": "boolean"
  },
  "inclusionFromFilter": {
    "type": "array",
    "items": {
      "type": "string"
    }
  },
  "exclusionFromFilter": {
    "type": "array",
    "items": {
      "type": "string"
    }
  },
  "inclusionToFilter": {
    "type": "array",
    "items": {
      "type": "string"
    }
  },
  "exclusionToFilter": {
    "type": "array",
    "items": {
      "type": "string"
    }
  }
}
```



```
    }
  },
  "inclusionCcFilter": {
    "type": "array",
    "items": {
      "type": "string"
    }
  },
  "exclusionCcFilter": {
    "type": "array",
    "items": {
      "type": "string"
    }
  },
  "inclusionBccFilter": {
    "type": "array",
    "items": {
      "type": "string"
    }
  },
  "exclusionBccFilter": {
    "type": "array",
    "items": {
      "type": "string"
    }
  },
  "beforeDateFilter": {
    "anyOf": [
      {
        "type": "string",
        "pattern": "^[0-9]{4}-[0-9]{2}-[0-9]{2}T[0-9]{2}:[0-9]{2}:[0-9]{2}Z$"
      },
      {
        "type": "string",
        "pattern": ""
      }
    ]
  },
  "afterDateFilter": {
    "anyOf": [
      {
        "type": "string",
        "pattern": "^[0-9]{4}-[0-9]{2}-[0-9]{2}T[0-9]{2}:[0-9]{2}:[0-9]{2}Z$"
      },
    ],
  },
```

```
        {
          "type": "string",
          "pattern": ""
        }
      ]
    },
    "isCrawlAttachment": {
      "type": "boolean"
    },
    "shouldCrawlDraftMessages": {
      "type": "boolean"
    }
  },
  "required": [
    "isCrawlAttachment",
    "shouldCrawlDraftMessages"
  ]
},
"type" : {
  "type" : "string",
  "pattern": "GMAIL"
},
"syncMode": {
  "type": "string",
  "enum": [
    "FORCED_FULL_CRAWL",
    "FULL_CRAWL"
  ]
},
"secretArn": {
  "type": "string"
},
"version": {
  "type": "string",
  "anyOf": [
    {
      "pattern": "1.0.0"
    }
  ]
}
},
"required": [
  "connectionConfiguration",
  "repositoryConfigurations",
```

```

    "additionalProperties",
    "syncMode",
    "secretArn",
    "type"
  ]
}
```

谷歌驅動器模板架構

您可以將包含資料來源結構描述的 JSON 納入為 [TemplateConfiguration](#) 物件的一部分。將資料來源類型指定為 `GOOGLEDRIVE2`、驗證認證的密碼，以及其他必要的組態。然後，您將指定 `TEMPLATE` 為呼叫 `Type` 時 [CreateDataSource](#)。

您可以使用本開發人員指南中提供的模板。請參閱 [谷歌雲端硬盤 JSON 模式](#)。

下表描述了谷歌雲端硬盤 JSON 模式的參數。

組態	描述
連線組態	資料來源的組態資訊。
<code>repositoryEndpointMetadata</code>	資料來源的端點資訊。此資料來源未指定端點。您可以選擇驗證類型： <code>serviceAccount</code> 和 <code>OAuth2</code> 。連線資訊會包含在您提供的 AWS Secrets Manager 密碼中 <code>secretArn</code> 。
<code>authType</code>	<code>OAuth2</code> 根據您的使用案例在 <code>serviceAccount</code> 和之間進行選擇。
儲存庫組態	資料來源內容的組態資訊。例如，配置特定類型的內容和欄位對應。
<ul style="list-style-type: none"> <code>file</code> <code>comment</code> 	將 Google 雲端硬盤的屬性或字段名稱映射到 Amazon Kendra 索引字段名稱的對象列表。如需詳細資訊，請參閱 映射資料來源欄位 。
附加屬性	資料來源中內容的其他設定選項
<ul style="list-style-type: none"> <code>maxFileSizeInMegabytes</code> 	指定 Amazon Kendra 應編目的檔案大小限制 (以 MB 為單位)。

組態	描述
<ul style="list-style-type: none"> • 爬行評論 • isCrawlMyDriveAndSharedWithMe 	<p>true在您的 Google 雲端硬碟數據源中抓取評論。</p> <p>true在您的 Google 雲端硬碟數據源中抓取 MyDrive 和共享「與我的驅動器」。</p>
<ul style="list-style-type: none"> • isCrawlShared磁碟機 	<p>true在您的 Google 雲端硬碟數據源中抓取共享雲端硬碟。</p>
isCrawlAcl	<p>true以編目文件的存取控制清單 (ACL) 資訊，如果您有 ACL，並且想要將其用於存取控制。ACL 指定使用者和群組可以存取和搜尋的文件。ACL 資訊可用來根據使用者或使用者對文件的群組存取權來篩選搜尋結果。如需詳細資訊，請參閱使用者內容篩選。</p>
<ul style="list-style-type: none"> • excludeUserAccounts • excludeSharedDrives • excludeMimeTypes • exclusionFileType模式 • exclusionFileName模式 • exclusionFilePath過濾器 	<p>正則表達式模式列表，用於排除 Google 雲端硬碟數據源中的某些文件。符合模式的檔案會從索引中排除。與模式不匹配的文件包含在索引中。如果檔案同時符合排除和包含模式，則排除模式優先，且該檔案不會包含在索引中。</p>
<ul style="list-style-type: none"> • includeUserAccounts • includeSharedDrives • includeMimeTypes • inclusionFileType模式 • inclusionFileName模式 • inclusionFilePath過濾器 	<p>正則表達式模式列表，用於在 Google 雲端硬碟數據源中包含某些文件。符合模式的檔案會包括在索引中。不符合模式的檔案會從索引中排除。如果檔案同時符合包含模式和排除模式，則排除模式優先，且檔案不會包含在索引中。</p>
type	<p>資料來源的類型。指定GOOGLEDRIVEV2 為您的資料來源類型。</p>

組態	描述
enableIdentityCrawler	<p>true，以使用 Amazon Kendra 的身分識別爬行者程式來同步使用者和群組的身分識別/主體資訊，以存取特定文件。如果關閉身分搜索器，則可以公開搜索所有文檔。如果您想要對文件使用存取控制，且身分識別編目程式已關閉，您也可以使用 PutPrincipalMapping API 來上傳使用者和群組存取資訊。</p>
同步模式	<p>指定資料來源內容變更時 Amazon Kendra 應如何更新索引。您可以選擇：</p> <ul style="list-style-type: none">• FORCED_FULL_CRAWL 新建索引所有內容，並在每次資料來源與索引同步時取代現有內容。• FULL_CRAWL，每次您的資料來源與索引同步時，僅對新的、修改和刪除的內容建立索引。Amazon Kendra 可以使用資料來源的機制來追蹤內容變更，並為上次同步後變更的內容建立索引。• CHANGE_LOG 每次資料來源與索引同步時，僅對新內容和修改的內容建立索引。Amazon Kendra 可以使用資料來源的機制來追蹤內容變更，並為上次同步後變更的內容建立索引。

組態	描述
秘書	<p>一個 AWS Secrets Manager 秘密的 Amazon 資源名稱 (ARN) ，其中包含連接到 Google 雲端硬碟所需的鍵值對。私密必須包含具有下列索引鍵的 JSON 結構：</p> <p>如果使用 Google 服務帳戶身份驗證：</p> <pre data-bbox="829 520 1507 842"> { "clientEmail": " <i>user account email</i>", "adminAccountEmail": " <i>service account email</i>", "privateKey": " <i>private key</i>" } </pre> <p>如果使用 OAuth 2.0 身份驗證：</p> <pre data-bbox="829 947 1507 1188"> { "clientID": " <i>OAuth client ID</i>", "clientSecret": " <i>client secret</i>", "refreshToken": " <i>refresh token</i>" } </pre>
version	目前支援的此範本版本。

谷歌雲端硬碟 JSON 模式

```

{
  "$schema": "http://json-schema.org/draft-04/schema#",
  "type": "object",
  "properties": {
    "connectionConfiguration": {
      "type": "object",
      "properties": {
        "repositoryEndpointMetadata": {
          "type": "object",
          "properties": {
            "authType": {

```

```
        "type": "string",
        "enum": [
            "serviceAccount",
            "OAuth2"
        ]
    },
    "required": [
        "authType"
    ]
},
"required": [
    "repositoryEndpointMetadata"
],
"repositoryConfigurations": {
    "type": "object",
    "properties": {
        "file": {
            "type": "object",
            "properties": {
                "fieldMappings": {
                    "type": "array",
                    "items": [
                        {
                            "type": "object",
                            "properties": {
                                "indexFieldName": {
                                    "type": "string"
                                },
                                "indexFieldType": {
                                    "type": "string",
                                    "enum": [
                                        "STRING",
                                        "DATE",
                                        "STRING_LIST",
                                        "LONG"
                                    ]
                                },
                                "dataSourceFieldName": {
                                    "type": "string"
                                },
                                "dateFieldFormat": {
```

```
        "type": "string",
        "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
      }
    },
    "required": [
      "indexFieldName",
      "indexFieldType",
      "dataSourceFieldName"
    ]
  }
]
},
"required": [
  "fieldMappings"
]
},
"comment": {
  "type": "object",
  "properties": {
    "fieldMappings": {
      "type": "array",
      "items": [
        {
          "type": "object",
          "properties": {
            "indexFieldName": {
              "type": "string"
            },
            "indexFieldType": {
              "type": "string",
              "enum": [
                "STRING",
                "DATE",
                "STRING_LIST"
              ]
            },
            "dataSourceFieldName": {
              "type": "string"
            },
            "dateFieldFormat": {
              "type": "string",
              "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
            }
          }
        }
      ]
    }
  }
}
```



```
        },
        "required": [
            "indexFieldName",
            "indexFieldType",
            "dataSourceFieldName"
        ]
    }
]
}
},
"required": [
    "fieldMappings"
]
}
},
"additionalProperties": {
    "type": "object",
    "properties": {
        "maxFileSizeInMegaBytes": {
            "type": "string"
        },
        "isCrawlComment": {
            "type": "boolean"
        },
        "isCrawlMyDriveAndSharedWithMe": {
            "type": "boolean"
        },
        "isCrawlSharedDrives": {
            "type": "boolean"
        },
        "isCrawlAcl": {
            "type": "boolean"
        },
        "excludeUserAccounts": {
            "type": "array",
            "items": {
                "type": "string"
            }
        },
        "excludeSharedDrives": {
            "type": "array",
            "items": {
                "type": "string"
            }
        }
    }
}
```

```
    }
  },
  "excludeMimeTypes": {
    "type": "array",
    "items": {
      "type": "string"
    }
  },
  "includeUserAccounts": {
    "type": "array",
    "items": {
      "type": "string"
    }
  },
  "includeSharedDrives": {
    "type": "array",
    "items": {
      "type": "string"
    }
  },
  "includeMimeTypes": {
    "type": "array",
    "items": {
      "type": "string"
    }
  },
  "includeTargetAudienceGroup": {
    "type": "array",
    "items": {
      "type": "string"
    }
  },
  "inclusionFileTypePatterns": {
    "type": "array",
    "items": {
      "type": "string"
    }
  },
  "inclusionFileNamePatterns": {
    "type": "array",
    "items": {
      "type": "string"
    }
  },
},
```

```
    "exclusionFileTypePatterns": {
      "type": "array",
      "items": {
        "type": "string"
      }
    },
    "exclusionFileNamePatterns": {
      "type": "array",
      "items": {
        "type": "string"
      }
    },
    "inclusionFilePathFilter": {
      "type": "array",
      "items": {
        "type": "string"
      }
    },
    "exclusionFilePathFilter": {
      "type": "array",
      "items": {
        "type": "string"
      }
    }
  },
  "type": {
    "type": "string",
    "pattern": "GOOGLEDRIVEV2"
  },
  "enableIdentityCrawler": {
    "type": "boolean"
  },
  "syncMode": {
    "type": "string",
    "enum": [
      "FORCED_FULL_CRAWL",
      "FULL_CRAWL",
      "CHANGE_LOG"
    ]
  },
  "secretArn": {
    "type": "string",
    "minLength": 20,
```

```

    "maxLength": 2048
  }
},
"version": {
  "type": "string",
  "anyOf": [
    {
      "pattern": "1.0.0"
    }
  ]
},
"required": [
  "connectionConfiguration",
  "repositoryConfigurations",
  "syncMode",
  "additionalProperties",
  "secretArn",
  "type"
]
}

```

模板架構

您可以將包含資料來源結構描述的 JSON 納入為 [TemplateConfiguration](#) 物件的一部分。將資料來源的類型指定為 JDBC、資料庫類型為 db2、驗證認證的密碼，以及其他必要的組態。然後，您將指定 TEMPLATE 為呼叫 Type 時 [CreateDataSource](#)。

您可以使用本開發人員指南中提供的模板。請參閱 [JSON 結構描述](#)。

下表說明 IBM DB2 JSON 結構描述的參數。

組態	描述
連線組態	資料來源端點的組態資訊。
repositoryEndpointMetadata	連線資料來源所需的組態資訊。 <ul style="list-style-type: none"> 資料庫類型-您使用的 Java 資料庫類型 (無論是mysql、db2、postgresql oracle、或)。sqlserver 資料庫主機 — 資料庫主機名稱。

組態	描述
	<ul style="list-style-type: none"> 資料庫埠 — 資料庫連接埠。 資料庫實例 — 資料庫執行處理。
儲存庫組態	資料來源內容的組態資訊。例如，配置特定類型的內容和欄位對應。指定資料來源的類型和秘密 ARN。
文件	將資料庫內容的屬性或欄位名稱對應至 Amazon Kendra 索引欄位名稱的物件清單。如需詳細資訊，請參閱 映射資料來源欄位 。
附加屬性	資料來源中內容的其他組態選項。用於在資料庫資料來源中包含或排除特定內容。
主要金鑰	提供資料庫表格的主索引鍵。這標識數據庫中的一個表。
標題欄	提供資料庫表格中文件標題欄的名稱。
身體專欄	提供資料庫表格中文件標題欄的名稱。
sqlQuery	輸入 SQL 查詢語句，如選擇和連接操作。SQL 查詢必須小於 32 KB。Amazon Kendra 會編目符合您查詢的所有資料庫內容。
時間戳記列	輸入包含時間戳記的列的名稱。Amazon Kendra 使用時間戳記資訊偵測內容中的變更，並僅同步變更的內容。
時間戳記格式	輸入包含時間戳記格式的資料欄名稱，可用來偵測內容變更並重新同步處理內容。
timezone	輸入包含要探索之內容之時區的資料欄名稱。
changeDetectingColumns	輸入 Amazon Kendra 將用來偵測內容變更的欄名稱。Amazon Kendra 當這些列中的任何一個更改時，將重新索引內容

組態	描述
allowedUsersColumns	輸入包含允許存取內容之使用者 ID 的欄名稱。
allowedGroupsColumn	輸入包含允許存取內容之使用者 ID 的欄名稱。
來源尿酸氧胺	輸入包含要編製索引之來源 URL 的資料欄名稱。
isSslEnabled	輸入 SQL 查詢語句，如選擇和連接操作。SQL 查詢必須小於 32 KB。Amazon Kendra 會編目符合您查詢的所有資料庫內容。
type	資料來源的類型。指定 JDBC 為您的資料來源類型。
同步模式	<p>指定資料來源內容變更時 Amazon Kendra 應如何更新索引。您可以選擇：</p> <ul style="list-style-type: none"> • FORCED_FULL_CRAWL 新建索引所有內容，並在每次資料來源與索引同步時取代現有內容。 • FULL_CRAWL，每次您的資料來源與索引同步時，僅對新的、修改和刪除的內容建立索引。Amazon Kendra 可以使用資料來源的機制來追蹤內容變更，並為上次同步後變更的內容建立索引。 • CHANGE_LOG 每次資料來源與索引同步時，僅對新內容和修改的內容建立索引。Amazon Kendra 可以使用資料來源的機制來追蹤內容變更，並為上次同步後變更的內容建立索引。

組態	描述
秘书	<p>秘密 Secrets Manager 密碼的 Amazon 資源名稱 (ARN)，其中包含連線到資料庫所需的使用者名稱和密碼。私密必須包含具有下列索引鍵的 JSON 結構：</p> <pre data-bbox="829 443 1507 642"> { "user name": "<i>database user name</i>", "password": "<i>password</i>" } </pre>
version	目前支援的範本版本。

JSON 結構描述

```

{
  "$schema": "http://json-schema.org/draft-04/schema#",
  "type": "object",
  "properties": {
    "connectionConfiguration": {
      "type": "object",
      "properties": {
        "repositoryEndpointMetadata": {
          "type": "object",
          "properties": {
            "dbType": {
              "type": "string",
              "enum": [
                "mysql",
                "db2",
                "postgresql",
                "oracle",
                "sqlserver"
              ]
            },
            "dbHost": {
              "type": "string"
            },
            "dbPort": {
              "type": "string"
            }
          }
        }
      }
    }
  }
}

```

```
    },
    "dbInstance": {
      "type": "string"
    }
  },
  "required": [
    "dbType",
    "dbHost",
    "dbPort",
    "dbInstance"
  ]
},
"required": [
  "repositoryEndpointMetadata"
],
"repositoryConfigurations": {
  "type": "object",
  "properties": {
    "document": {
      "type": "object",
      "properties": {
        "fieldMappings": {
          "type": "array",
          "items": [
            {
              "type": "object",
              "properties": {
                "indexFieldName": {
                  "type": "string"
                },
                "indexFieldType": {
                  "type": "string"
                },
                "dataSourceFieldName": {
                  "type": "string"
                }
              }
            }
          ]
        },
        "required": [
          "indexFieldName",
          "indexFieldType",
          "dataSourceFieldName"
        ]
      }
    }
  }
}
```



```
        }
      ]
    }
  },
  "required": [
    "fieldMappings"
  ]
}
},
"required": [
]
},
"additionalProperties": {
  "type": "object",
  "properties": {
    "primaryKey": {
      "type": "string"
    },
    "titleColumn": {
      "type": "string"
    },
    "bodyColumn": {
      "type": "string"
    },
    "sqlQuery": {
      "type": "string",
      "not": {
        "pattern": ";+"
      }
    },
    "timestampColumn": {
      "type": "string"
    },
    "timestampFormat": {
      "type": "string"
    },
    "timezone": {
      "type": "string"
    },
    "changeDetectingColumns": {
      "type": "array",
      "items": {
        "type": "string"
      }
    }
  }
}
```

```
    },
    "allowedUsersColumn": {
      "type": "string"
    },
    "allowedGroupsColumn": {
      "type": "string"
    },
    "sourceURIColumn": {
      "type": "string"
    },
    "isSslEnabled": {
      "type": "boolean"
    }
  },
  "required": ["primaryKey", "titleColumn", "bodyColumn", "sqlQuery"]
},
"type" : {
  "type" : "string",
  "pattern": "JDBC"
},
"syncMode": {
  "type": "string",
  "enum": [
    "FORCED_FULL_CRAWL",
    "FULL_CRAWL",
    "CHANGE_LOG"
  ]
},
"secretArn": {
  "type": "string"
}
},
"version": {
  "type": "string",
  "anyOf": [
    {
      "pattern": "1.0.0"
    }
  ]
}
},
"required": [
  "connectionConfiguration",
  "repositoryConfigurations",
  "syncMode",
```

```

    "additionalProperties",
    "secretArn",
    "type"
  ]
}

```

Microsoft 交易所模板架構

您可以將包含資料來源結構描述的 JSON 納入為 [TemplateConfiguration](#) 物件的一部分。您提供承租人識別碼做為連線組態或存放庫端點詳細資料的一部分。同時將資料來源類型指定為 MSEXCHANGE、驗證認證的密碼，以及其他必要的組態。然後，您將指定 TEMPLATE 為呼叫 Type 時 [CreateDataSource](#)。

您可以使用本開發人員指南中提供的模板。請參閱 [Microsoft 交易所 JSON 架構](#)。

下表說明 Microsoft 交換 JSON 結構描述的參數。

組態	描述
連線組態	資料來源端點的組態資訊。
repositoryEndpointMetadata	資料來源的端點資訊。
特南蒂	Microsoft 365 租戶識別碼。您可以在 Azure 作用中目錄入口網站的內容或 OAuth 應用程式中找到您的租用戶識別碼。
儲存庫組態	資料來源內容的組態資訊。例如，配置特定類型的內容和欄位對應。
<ul style="list-style-type: none"> email attachment 行事曆 連絡人 notes 	將 Microsoft Exchange 資料來源的屬性或欄位名稱對應至 Amazon Kendra 索引欄位的物件清單。如需詳細資訊，請參閱 映射資料來源欄位 。
附加屬性	資料來源中內容的其他組態選項
包含模式	規則運算式模式清單，以包含您的 Microsoft Exchange 資料來源中的某些檔案。符合模式的檔案會包括在索引中。不符合模式的檔案會從索

組態	描述
	索引中排除。如果檔案同時符合包括模式和排除模式，則以排除模式為優先，且該項目不會包括在索引中。
排除模式	規則運算式模式清單，可排除您的 Microsoft Exchange 資料來源中的某些檔案。符合模式的檔案會從索引中排除。與模式不匹配的文件包含在索引中。如果檔案同時符合排除和包含模式，則排除模式優先，且檔案不會包含在索引中。
<ul style="list-style-type: none"> • inclusionUsersList • inclusionUsersFile姓名 • inclusionDomainUsers 	規則運算式模式清單，可將特定使用者和使用者檔案包含在您的 Microsoft 交換資料來源中。符合模式的使用者會包含在索引中。不符合模式的使用者會從索引中排除。如果使用者同時符合包含和排除模式，則排除模式優先，且使用者不會包含在索引中。
<ul style="list-style-type: none"> • exclusionUsersList • exclusionUsersFile姓名 • exclusionDomainUsers 	規則運算式模式清單，可排除 Microsoft Exchange 資料來源中的某些使用者和使用者檔案。符合模式的使用者會從索引中排除。不符合模式的使用者會包含在索引中。如果使用者同時符合排除和包含模式，則排除模式優先，且使用者不會包含在索引中。
S3 儲存格名稱	您的 S3 儲存貯體的名稱 (如果您要使用)。
<ul style="list-style-type: none"> • 爬行日曆 • 爬行筆記 • 爬行聯繫 • crawlFolderAcl 	true編目這些類型的內容和存取控制資訊您的 Microsoft Exchange 資料來源。
startCalendarDate時間	您可以為行事曆內容設定特定的開始日期-時間。
endCalendarDate時間	您可以為行事曆內容設定特定的結束日期-時間。

組態	描述
subject	您可以設定郵件內容的特定主旨行。
電子郵件從	您可以為「寄件者」或寄件者郵件內容設定特定的電子郵件。
電子郵件至	您可以為「收件者」或收件者郵件內容設定特定的電子郵件。
同步模式	<p>指定資料來源內容變更時 Amazon Kendra 應如何更新索引。您可以選擇：</p> <ul style="list-style-type: none"> • <code>FORCED_FULL_CRAWL</code> 新建索引所有內容，並在每次資料來源與索引同步時取代現有內容。 • <code>FULL_CRAWL</code> ，每次您的資料來源與索引同步時，僅對新的、修改和刪除的內容建立索引。Amazon Kendra 可以使用資料來源的機制來追蹤內容變更，並為上次同步後變更的內容建立索引。 • <code>CHANGE_LOG</code> 每次資料來源與索引同步時，僅對新內容和修改的內容建立索引。Amazon Kendra 可以使用資料來源的機制來追蹤內容變更，並為上次同步後變更的內容建立索引。
type	資料來源的類型。指定 <code>MSEXCHANGE</code> 為您的資料來源類型。
秘书	AWS Secrets Manager 秘密的 Amazon 資源名稱 (ARN) ，其中包含連接到 Microsoft 交換所需的鍵值對。這包括您的用戶端識別碼，以及您在 Azure 入口網站中建立 OAuth 應用程式時所產生的用戶端密碼。
version	目前支援的此範本版本。

Microsoft 交易所 JSON 架構

```

{
  "$schema": "http://json-schema.org/draft-04/schema#",
  "type": "object",
  "properties": {
    "connectionConfiguration": {
      "type": "object",
      "properties": {
        "repositoryEndpointMetadata": {
          "type": "object",
          "properties": {
            "tenantId": {
              "type": "string",
              "pattern": "^[0-9a-f]{8}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]
{12}$",
              "minLength": 36,
              "maxLength": 36
            }
          },
          "required": ["tenantId"]
        }
      }
    },
    "repositoryConfigurations": {
      "type": "object",
      "properties": {
        "email": {
          "type": "object",
          "properties": {
            "fieldMappings": {
              "type": "array",
              "items": [
                {
                  "type": "object",
                  "properties": {
                    "indexFieldName": {
                      "type": "string"
                    },
                    "indexFieldType": {
                      "type": "string",
                      "enum": ["STRING", "STRING_LIST", "DATE"]
                    },
                    "dataSourceFieldName": {

```

```

        "type": "string"
      },
      "dateFieldFormat": {
        "type": "string",
        "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
      }
    },
    "required": [
      "indexFieldName",
      "indexFieldType",
      "dataSourceFieldName"
    ]
  }
]
}
},
"required": [
  "fieldMappings"
]
},
"attachment": {
  "type": "object",
  "properties": {
    "fieldMappings": {
      "type": "array",
      "items": [
        {
          "type": "object",
          "properties": {
            "indexFieldName": {
              "type": "string"
            },
            "indexFieldType": {
              "type": "string",
              "enum": ["STRING", "DATE", "LONG"]
            },
            "dataSourceFieldName": {
              "type": "string"
            },
            "dateFieldFormat": {
              "type": "string",
              "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
            }
          }
        }
      ]
    }
  }
},

```

```

        "required": [
            "indexFieldName",
            "indexFieldType",
            "dataSourceFieldName"
        ]
    }
]
},
"required": [
    "fieldMappings"
]
},
"calendar": {
    "type": "object",
    "properties": {
        "fieldMappings": {
            "type": "array",
            "items": [
                {
                    "type": "object",
                    "properties": {
                        "indexFieldName": {
                            "type": "string"
                        },
                        "indexFieldType": {
                            "type": "string",
                            "enum": ["STRING", "STRING_LIST", "DATE"]
                        },
                        "dataSourceFieldName": {
                            "type": "string"
                        },
                        "dateFieldFormat": {
                            "type": "string",
                            "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                        }
                    }
                }
            ]
        },
        "required": [
            "indexFieldName",
            "indexFieldType",
            "dataSourceFieldName"
        ]
    }
}
]

```



```
    }
  },
  "required": [
    "fieldMappings"
  ]
},
"contacts": {
  "type": "object",
  "properties": {
    "fieldMappings": {
      "type": "array",
      "items": [
        {
          "type": "object",
          "properties": {
            "indexFieldName": {
              "type": "string"
            },
            "indexFieldType": {
              "type": "string",
              "enum": ["STRING", "STRING_LIST", "DATE"]
            },
            "dataSourceFieldName": {
              "type": "string"
            },
            "dateFieldFormat": {
              "type": "string",
              "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
            }
          }
        },
        "required": [
          "indexFieldName",
          "indexFieldType",
          "dataSourceFieldName"
        ]
      ]
    }
  },
  "required": [
    "fieldMappings"
  ]
},
"notes": {
```

```
"type": "object",
"properties": {
  "fieldMappings": {
    "type": "array",
    "items": [
      {
        "type": "object",
        "properties": {
          "indexFieldName": {
            "type": "string"
          },
          "indexFieldType": {
            "type": "string",
            "enum": ["STRING", "DATE"]
          },
          "dataSourceFieldName": {
            "type": "string"
          },
          "dateFieldFormat": {
            "type": "string",
            "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
          }
        },
        "required": [
          "indexFieldName",
          "indexFieldType",
          "dataSourceFieldName"
        ]
      }
    ]
  },
  "required": [
    "fieldMappings"
  ]
},
"required": ["email"]
},
"additionalProperties": {
  "type": "object",
  "properties": {
    "inclusionPatterns": {
```

```
    "type": "array",
    "items": {
      "type": "string"
    }
  },
  "exclusionPatterns": {
    "type": "array",
    "items": {
      "type": "string"
    }
  },
  "inclusionUsersList": {
    "type": "array",
    "items": {
      "type": "string",
      "format": "email"
    }
  },
  "exclusionUsersList": {
    "type": "array",
    "items": {
      "type": "string",
      "format": "email"
    }
  },
  "s3bucketName": {
    "type": "string"
  },
  "inclusionUsersFileName": {
    "type": "string"
  },
  "exclusionUsersFileName": {
    "type": "string"
  },
  "inclusionDomainUsers": {
    "type": "array",
    "items": {
      "type": "string"
    }
  },
  "exclusionDomainUsers": {
    "type": "array",
    "items": {
      "type": "string"
    }
  }
}
```

```
    }
  },
  "crawlCalendar": {
    "type": "boolean"
  },
  "crawlNotes": {
    "type": "boolean"
  },
  "crawlContacts": {
    "type": "boolean"
  },
  "crawlFolderAcl": {
    "type": "boolean"
  },
  "startCalendarDateTime": {
    "anyOf": [
      {
        "type": "string",
        "pattern": "^[0-9]{4}-[0-9]{2}-[0-9]{2}T[0-9]{2}:[0-9]{2}:[0-9]{2}Z$"
      },
      {
        "type": "string",
        "pattern": ""
      }
    ]
  },
  "endCalendarDateTime": {
    "anyOf": [
      {
        "type": "string",
        "pattern": "^[0-9]{4}-[0-9]{2}-[0-9]{2}T[0-9]{2}:[0-9]{2}:[0-9]{2}Z$"
      },
      {
        "type": "string",
        "pattern": ""
      }
    ]
  },
  "subject": {
    "type": "array",
    "items": {
      "type": "string"
    }
  }
},
```

```
    "emailFrom": {
      "type": "array",
      "items": {
        "type": "string",
        "format": "email"
      }
    },
    "emailTo": {
      "type": "array",
      "items": {
        "type": "string",
        "format": "email"
      }
    }
  },
  "required": [
  ],
},
"syncMode": {
  "type": "string",
  "enum": [
    "FORCED_FULL_CRAWL",
    "FULL_CRAWL",
    "CHANGE_LOG"
  ]
},
"type" : {
  "type" : "string",
  "pattern": "MSEXCHANGE"
},
"secretArn": {
  "type": "string"
}
},
"version": {
  "type": "string",
  "anyOf": [
    {
      "pattern": "1.0.0"
    }
  ]
}
},
"required": [
  "connectionConfiguration",
```

```

    "repositoryConfigurations",
    "syncMode",
    "additionalProperties",
    "secretArn",
    "type"
  ]
}

```

Microsoft OneDrive 模板架構

您可以將包含資料來源結構描述的 JSON 納入為 [TemplateConfiguration](#) 物件的一部分。您可以提供承租人識別碼做為連線組態或存放庫端點詳細資料的一部分。此外，請將資料來源的類型指定為 ONEDRIVEV2，以及驗證認證的密碼，以及其他必要的組態。然後，您將指定 TEMPLATE 為呼叫 Type 時 [CreateDataSource](#)。

您可以使用本開發人員指南中提供的模板。請參閱 [Microsoft OneDrive 模式](#)。

下表說明 Microsoft OneDrive JSON 結構描述的參數。

組態	描述
連線組態	資料來源端點的組態資訊。
repositoryEndpointMetadata	資料來源的端點資訊。
特南蒂	Microsoft 365 租戶識別碼。您可以在 Azure 作用中目錄入口網站的內容或 OAuth 應用程式中找到您的租用戶識別碼。
儲存庫組態	資料來源內容的組態資訊。例如，配置特定類型的內容和欄位對應。
file	將 Microsoft OneDrive 檔案的屬性或欄位名稱對應至 Amazon Kendra 索引欄位名稱的物件清單。如需詳細資訊，請參閱 映射資料來源欄位 。
附加屬性	資料來源中內容的其他設定選項
<ul style="list-style-type: none"> • userNameFilter • userFilterPath 	您可以選擇索引特定檔案、OneNote 區段、OneNote 頁面，並依使用者名稱進行篩選。

組態	描述
<ul style="list-style-type: none"> • inclusionFileType模式 • exclusionFileType模式 • inclusionFileName模式 • exclusionFileName模式 • inclusionFilePath模式 • exclusionFilePath模式 • inclusionOneNoteSectionNamePatterns • exclusionOneNoteSectionNamePatterns • inclusionOneNotePageNamePatterns • exclusionOneNotepageNamePatterns 	
isUserNameOnS3	true提供儲存在的檔案中的使用者名稱清單 Amazon S3。
type	資料來源的類型。指定ONEDRIVEV2 為您的資料來源類型。
enableIdentityCrawler	true，以使用 Amazon Kendra的身分識別爬行者程式來同步使用者和群組的身分識別/主體資訊，以存取特定文件。如果關閉身分搜索器，則可以公開搜索所有文檔。如果您想要對文件使用存取控制，且身分識別編目程式已關閉，您也可以使用 PutPrincipalMapping API 來上傳使用者和群組存取資訊。
type	資料來源的類型。指定ONEDRIVEV2 為您的資料來源類型。

組態	描述
同步模式	<p>指定資料來源內容變更時 Amazon Kendra 應如何更新索引。您可以選擇：</p> <ul style="list-style-type: none"> • FORCED_FULL_CRAWL 新建索引所有內容，並在每次資料來源與索引同步時取代現有內容。 • FULL_CRAWL ，每次您的資料來源與索引同步時，僅對新的、修改和刪除的內容建立索引。Amazon Kendra 可以使用資料來源的機制來追蹤內容變更，並為上次同步後變更的內容建立索引。 • CHANGE_LOG 每次資料來源與索引同步時，僅對新內容和修改的內容建立索引。Amazon Kendra 可以使用資料來源的機制來追蹤內容變更，並為上次同步後變更的內容建立索引。
秘書	<p>Amazon 資源名稱 (ARN) 的 AWS Secrets Manager 秘密，其中包含連接到 Microsoft 所需的鍵值對。OneDrive 私密必須包含具有下列索引鍵的 JSON 結構：</p> <pre data-bbox="829 1192 1507 1394"> { "clientId": " <i>client ID</i>", "clientSecret": " <i>client secret</i>" } </pre>
version	目前支援的此範本版本。

Microsoft OneDrive 模式

```

{
  "$schema": "http://json-schema.org/draft-04/schema#",
  "type": "object",
  "properties": {
    "connectionConfiguration": {
      "type": "object",

```



```
"properties": {
  "repositoryEndpointMetadata": {
    "type": "object",
    "properties": {
      "tenantId": {
        "type": "string",
        "pattern": "^[0-9a-f]{8}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{12}$",
        "minLength": 36,
        "maxLength": 36
      }
    },
    "required": [
      "tenantId"
    ]
  },
  "required": [
    "repositoryEndpointMetadata"
  ]
},
"repositoryConfigurations": {
  "type": "object",
  "properties": {
    "file": {
      "type": "object",
      "properties": {
        "fieldMappings": {
          "type": "array",
          "items": [
            {
              "type": "object",
              "properties": {
                "indexFieldName": {
                  "type": "string"
                },
                "indexFieldType": {
                  "type": "string",
                  "enum": [
                    "STRING",
                    "STRING_LIST",
                    "DATE",
                    "LONG"
                  ]
                }
              }
            }
          ]
        }
      }
    }
  },
  "required": [
    "file"
  ]
}
```

```
    "dataSourceFieldName": {
      "type": "string"
    },
    "dateFieldFormat": {
      "type": "string",
      "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
    }
  ],
  "required": [
    "indexFieldName",
    "indexFieldType",
    "dataSourceFieldName"
  ]
}
]
}
},
"required": [
  "fieldMappings"
]
}
}
},
"additionalProperties": {
  "type": "object",
  "properties": {
    "userNameFilter": {
      "type": "array",
      "items": {
        "type": "string"
      }
    },
    "userFilterPath": {
      "type": "string"
    },
    "isUserNameOnS3": {
      "type": "boolean"
    },
    "inclusionFileTypePatterns": {
      "type": "array",
      "items": {
        "type": "string"
      }
    }
  }
},
```

```
"exclusionFileTypePatterns": {
  "type": "array",
  "items": {
    "type": "string"
  }
},
"inclusionFileNamePatterns": {
  "type": "array",
  "items": {
    "type": "string"
  }
},
"exclusionFileNamePatterns": {
  "type": "array",
  "items": {
    "type": "string"
  }
},
"inclusionFilePathPatterns": {
  "type": "array",
  "items": {
    "type": "string"
  }
},
"exclusionFilePathPatterns": {
  "type": "array",
  "items": {
    "type": "string"
  }
},
"inclusionOneNoteSectionNamePatterns": {
  "type": "array",
  "items": {
    "type": "string"
  }
},
"exclusionOneNoteSectionNamePatterns": {
  "type": "array",
  "items": {
    "type": "string"
  }
},
"inclusionOneNotePageNamePatterns": {
  "type": "array",
```

```
    "items": {
      "type": "string"
    }
  },
  "exclusionOneNotePageNamePatterns": {
    "type": "array",
    "items": {
      "type": "string"
    }
  }
},
"required": []
},

"enableIdentityCrawler": {
  "type": "boolean"
},
"type": {
  "type": "string",
  "pattern": "ONEDRIVEV2"
},
"syncMode": {
  "type": "string",
  "enum": [
    "FULL_CRAWL",
    "FORCED_FULL_CRAWL",
    "CHANGE_LOG"
  ]
},
"secretArn": {
  "type": "string",
  "minLength": 20,
  "maxLength": 2048
}
},
"version": {
  "type": "string",
  "anyOf": [
    {
      "pattern": "1.0.0"
    }
  ]
},
"required": [
```

```

"connectionConfiguration",
"repositoryConfigurations",
"syncMode",
"additionalProperties",
"secretArn",
"type"
]
}

```

Microsoft SharePoint 模板架構

您可以將包含資料來源結構描述的 JSON 納入為 [TemplateConfiguration](#) 物件的一部分。您可以視需要提供 SharePoint 網站 URL/URL、網域以及承租人識別碼，做為連線組態或存放庫端點詳細資料的一部分。同時將資料來源類型指定為 SHAREPOINTV2、驗證認證的密碼，以及其他必要的組態。然後您在呼叫時指定 TEMPLATE 為 Type [CreateDataSource](#)。

您可以使用本開發人員指南中提供的模板。請參閱 [SharePoint 結構定義](#)。

下表說明 Microsoft SharePoint JSON 結構描述的參數。

組態	描述
連線組態	資料來源端點的組態資訊
repositoryEndpointMetadata	資料來源的端點資訊
特南蒂	您帳戶的租用 SharePoint 戶識別碼。
domain	您 SharePoint 帳戶的網域。
网站网址	您 SharePoint 帳戶的主機 URL。
repositoryAdditionalProperties	與儲存庫/資料來源端點連線的其他內容。
S3 儲存格名稱	儲存您 Azure AD 自我簽署 X.509 憑證的 Amazon S3 值區名稱。
S3 認證名稱	儲存在值區中之 Azure AD 自我簽署 X.509 憑證的 Amazon S3 名稱。
authType	您使用的驗證類型 OAuth2，無論 是 OAuth2Certificate OAuth2App

組態	描述
	、Basic、OAuth2_RefreshToken、NTLM、或Kerberos。
version	您使用的 SharePoint 版本 (無論是Server或) Online。
onPremVersion	您使用的 SharePoint 伺服器版本 (無論是201320162019、或) SubscriptionEdition 。
儲存庫組態	資料來源內容的組態資訊。例如，配置特定類型的內容和欄位對應。
<ul style="list-style-type: none"> • 事件 • page • file • 連結 • attachment • comment 	將 SharePoint內容的屬性或欄位名稱對應至 Amazon Kendra 索引欄位名稱的物件清單。如需詳細資訊，請參閱 映射資料來源欄位 。
附加屬性	資料來源中內容的其他組態選項。

組態	描述
<ul style="list-style-type: none"> • eventTitleFilterRegEx • pageTitleFilterRegEx • linkTitleFilterRegEx • inclusionFilePath • exclusionFilePath • inclusionFileType模式 • exclusionFileType模式 • inclusionFileName模式 • exclusionFileName模式 • inclusionOneNoteSectionNamePatterns • exclusionOneNoteSectionNamePatterns • inclusionOneNotePageNamePatterns • exclusionOneNotePageNamePatterns 	<p>要在 SharePoint 資料來源中包含/排除某些內容的規則運算式模式清單。符合包含模式的內容項目會包含在索引中。不符合包含模式的內容項目會從索引中排除。如果檔案同時符合包含模式和排除模式，則排除模式優先，且檔案不會包含在索引中。</p>
<ul style="list-style-type: none"> • 爬網文件 • 抓取頁面 • 技巧 • 爬網評論 • 爬行鏈接 • 爬網附件 	<p>true來編目這些類型的內容。</p>
<p>克勞拉克</p>	<p>true以編目文件的存取控制清單 (ACL) 資訊，如果您有 ACL，並且想要將其用於存取控制。ACL 指定使用者和群組可以存取和搜尋的文件。ACL 資訊可用來根據使用者或使用者對文件的群組存取權來篩選搜尋結果。如需詳細資訊，請參閱使用者內容篩選。</p>
<p>fieldForUser識別碼</p>	<p>指定是email否要使用使用者電子郵件作為使用者 ID，或是userPrincipalName 要使用使用者名稱作為使用者 ID。如果您沒有指定選項，則email默認使用。</p>

組態	描述
ACL 組態	指定ACLWithLDAPEmailFmt ACLWithManualEmailFmt 、或ACLWithUsernameFmtM 。
電子郵件域	電子郵件的網域。例如，"###"。
<ul style="list-style-type: none"> isCrawlLocalGroupMapping isCrawlAdGroupMapping 	true以編目群組對應資訊。
代理宿主	您使用的網頁代理伺服器的主機名稱，而不使用http://或https://通訊協定。
代理端口	主機 URL 傳輸通訊協定所使用的連接埠號碼。必須是介於 0 到 65535 之間的數值。
type	指定SHAREPOINTV2 為您的資料來源類型
enableIdentityCrawler	true，以使用 Amazon Kendra的身分識別爬行者程式來同步使用者和群組的身分識別/主體資訊，以存取特定文件。如果關閉身分搜索器，則可以公開搜索所有文檔。如果您想要對文件使用存取控制，且身分識別編目程式已關閉，您也可以使用 PutPrincipalMapping API 來上傳使用者和群組存取資訊。

組態	描述
同步模式	<p>指定資料來源內容變更時 Amazon Kendra 應如何更新索引。您可以選擇：</p> <ul style="list-style-type: none"> • FORCED_FULL_CRAWL 新建索引所有內容，並在每次資料來源與索引同步時取代現有內容。 • FULL_CRAWL ，每次您的資料來源與索引同步時，僅對新的、修改和刪除的內容建立索引。Amazon Kendra 可以使用資料來源的機制來追蹤內容變更，並為上次同步後變更的內容建立索引。 • CHANGE_LOG 每次資料來源與索引同步時，僅對新內容和修改的內容建立索引。Amazon Kendra 可以使用資料來源的機制來追蹤內容變更，並為上次同步後變更的內容建立索引。
秘書	<p>Amazon 資源名稱 (ARN) 的 AWS Secrets Manager 秘密，其中包含連接到 SharePoint 如需這些機碼值配對的詳細資訊，請參閱線上與 SharePoint 伺服器的連 SharePoint 線指示。</p>
version	目前支援的此範本版本。

SharePoint 結構定義

```
{
  "$schema": "http://json-schema.org/draft-04/schema#",
  "type": "object",
  "properties": {
    "connectionConfiguration": {
      "type": "object",
      "properties": {
        "repositoryEndpointMetadata": {
          "type": "object",
          "properties": {
            "tenantId": {
```

```
"type": "string",
"pattern": "^[0-9a-f]{8}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{12}$",
"minLength": 36,
"maxLength": 36
},
"domain": {
  "type": "string"
},
"siteUrls": {
  "type": "array",
  "items": {
    "type": "string",
    "pattern": "https://.*"
  }
},
"repositoryAdditionalProperties": {
  "type": "object",
  "properties": {
    "s3bucketName": {
      "type": "string"
    },
    "s3certificateName": {
      "type": "string"
    },
    "authType": {
      "type": "string",
      "enum": [
        "OAuth2",
        "OAuth2Certificate",
        "OAuth2App",
        "Basic",
        "OAuth2_RefreshToken",
        "NTLM",
        "Kerberos"
      ]
    },
    "version": {
      "type": "string",
      "enum": [
        "Server",
        "Online"
      ]
    },
    "onPremVersion": {
```

```
    "type": "string",
    "enum": [
      "",
      "2013",
      "2016",
      "2019",
      "SubscriptionEdition"
    ]
  },
  "required": [
    "authType",
    "version"
  ]
},
"required": [
  "siteUrls",
  "domain",
  "repositoryAdditionalProperties"
]
},
"required": [
  "repositoryEndpointMetadata"
]
},
"repositoryConfigurations": {
  "type": "object",
  "properties": {
    "event": {
      "type": "object",
      "properties": {
        "fieldMappings": {
          "type": "array",
          "items": [
            {
              "type": "object",
              "properties": {
                "indexFieldName": {
                  "type": "string"
                },
                "indexFieldType": {
                  "type": "string",
```

```
    "enum": [
      "STRING",
      "STRING_LIST",
      "DATE"
    ]
  },
  "dataSourceFieldName": {
    "type": "string"
  },
  "dateFieldFormat": {
    "type": "string",
    "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
  }
},
"required": [
  "indexFieldName",
  "indexFieldType",
  "dataSourceFieldName"
]
}
]
}
},
"required": [
  "fieldMappings"
]
},
"page": {
  "type": "object",
  "properties": {
    "fieldMappings": {
      "type": "array",
      "items": [
        {
          "type": "object",
          "properties": {
            "indexFieldName": {
              "type": "string"
            },
            "indexFieldType": {
              "type": "string",
              "enum": [
                "STRING",
                "DATE",
```

```
        "LONG"
      ]
    },
    "dataSourceFieldName": {
      "type": "string"
    },
    "dateFieldFormat": {
      "type": "string",
      "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
    }
  },
  "required": [
    "indexFieldName",
    "indexFieldType",
    "dataSourceFieldName"
  ]
}
]
}
},
"required": [
  "fieldMappings"
]
},
"file": {
  "type": "object",
  "properties": {
    "fieldMappings": {
      "type": "array",
      "items": [
        {
          "type": "object",
          "properties": {
            "indexFieldName": {
              "type": "string"
            },
            "indexFieldType": {
              "type": "string",
              "enum": [
                "STRING",
                "DATE",
                "LONG"
              ]
            }
          }
        }
      ]
    }
  }
},
```

```
    "dataSourceFieldName": {
      "type": "string"
    },
    "dateFieldFormat": {
      "type": "string",
      "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
    }
  },
  "required": [
    "indexFieldName",
    "indexFieldType",
    "dataSourceFieldName"
  ]
}
]
}
},
"required": [
  "fieldMappings"
]
},
"link": {
  "type": "object",
  "properties": {
    "fieldMappings": {
      "type": "array",
      "items": [
        {
          "type": "object",
          "properties": {
            "indexFieldName": {
              "type": "string"
            },
            "indexFieldType": {
              "type": "string",
              "enum": [
                "STRING",
                "STRING_LIST",
                "DATE"
              ]
            }
          }
        }
      ]
    },
    "dataSourceFieldName": {
      "type": "string"
    }
  },
```

```
    "dateFieldFormat": {
      "type": "string",
      "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
    }
  },
  "required": [
    "indexFieldName",
    "indexFieldType",
    "dataSourceFieldName"
  ]
}
]
}
},
"required": [
  "fieldMappings"
]
},
"attachment": {
  "type": "object",
  "properties": {
    "fieldMappings": {
      "type": "array",
      "items": [
        {
          "type": "object",
          "properties": {
            "indexFieldName": {
              "type": "string"
            },
            "indexFieldType": {
              "type": "string",
              "enum": [
                "STRING",
                "STRING_LIST",
                "DATE"
              ]
            },
            "dataSourceFieldName": {
              "type": "string"
            },
            "dateFieldFormat": {
              "type": "string",
              "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
            }
          }
        }
      ]
    }
  }
}
```

```
    }
  },
  "required": [
    "indexFieldName",
    "indexFieldType",
    "dataSourceFieldName"
  ]
}
]
}
},
"required": [
  "fieldMappings"
]
},
"comment": {
  "type": "object",
  "properties": {
    "fieldMappings": {
      "type": "array",
      "items": [
        {
          "type": "object",
          "properties": {
            "indexFieldName": {
              "type": "string"
            },
            "indexFieldType": {
              "type": "string",
              "enum": [
                "STRING",
                "STRING_LIST",
                "DATE"
              ]
            },
            "dataSourceFieldName": {
              "type": "string"
            },
            "dateFieldFormat": {
              "type": "string",
              "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
            }
          }
        }
      ]
    }
  },
  "required": [
```



```
        "indexFieldName",
        "indexFieldType",
        "dataSourceFieldName"
    ]
}
]
}
},
"required": [
    "fieldMappings"
]
}
}
},
"additionalProperties": {
    "type": "object",
    "properties": {
        "eventTitleFilterRegEx": {
            "type": "array",
            "items": {
                "type": "string"
            }
        },
        "pageTitleFilterRegEx": {
            "type": "array",
            "items": {
                "type": "string"
            }
        },
        "linkTitleFilterRegEx": {
            "type": "array",
            "items": {
                "type": "string"
            }
        },
        "inclusionFilePath": {
            "type": "array",
            "items": {
                "type": "string"
            }
        },
        "exclusionFilePath": {
            "type": "array",
            "items": {
```

```
    "type": "string"
  }
},
"inclusionFileTypePatterns": {
  "type": "array",
  "items": {
    "type": "string"
  }
},
"exclusionFileTypePatterns": {
  "type": "array",
  "items": {
    "type": "string"
  }
},
"inclusionFileNamePatterns": {
  "type": "array",
  "items": {
    "type": "string"
  }
},
"exclusionFileNamePatterns": {
  "type": "array",
  "items": {
    "type": "string"
  }
},
"inclusionOneNoteSectionNamePatterns": {
  "type": "array",
  "items": {
    "type": "string"
  }
},
"exclusionOneNoteSectionNamePatterns": {
  "type": "array",
  "items": {
    "type": "string"
  }
},
"inclusionOneNotePageNamePatterns": {
  "type": "array",
  "items": {
    "type": "string"
  }
}
```

```
},
"exclusionOneNotePageNamePatterns": {
  "type": "array",
  "items": {
    "type": "string"
  }
},
"crawlFiles": {
  "type": "boolean"
},
"crawlPages": {
  "type": "boolean"
},
"crawlEvents": {
  "type": "boolean"
},
"crawlComments": {
  "type": "boolean"
},
"crawlLinks": {
  "type": "boolean"
},
"crawlAttachments": {
  "type": "boolean"
},
"crawlListData": {
  "type": "boolean"
},
"crawlAcl": {
  "type": "boolean"
},
"fieldForUserId": {
  "type": "string"
},
"aclConfiguration": {
  "type": "string",
  "enum": [
    "ACLWithLDAPEmailFmt",
    "ACLWithManualEmailFmt",
    "ACLWithUsernameFmt"
  ]
},
"emailDomain": {
  "type": "string"
}
```

```
    },
    "isCrawlLocalGroupMapping": {
      "type": "boolean"
    },
    "isCrawlAdGroupMapping": {
      "type": "boolean"
    },
    "proxyHost": {
      "type": "string"
    },
    "proxyPort": {
      "type": "string"
    }
  },
  "required": [
  ],
  "type": {
    "type": "string",
    "pattern": "SHAREPOINTV2"
  },
  "enableIdentityCrawler": {
    "type": "boolean"
  },
  "syncMode": {
    "type": "string",
    "enum": [
      "FULL_CRAWL",
      "FORCED_FULL_CRAWL",
      "CHANGE_LOG"
    ]
  },
  "secretArn": {
    "type": "string",
    "minLength": 20,
    "maxLength": 2048
  }
},
"version": {
  "type": "string",
  "anyOf": [
    {
      "pattern": "1.0.0"
    }
  ]
}
```

```

]
},
"required": [
  "connectionConfiguration",
  "repositoryConfigurations",
  "enableIdentityCrawler",
  "syncMode",
  "additionalProperties",
  "secretArn",
  "type"
]
}

```

Microsoft SQL 服務器模板架構

您可以將包含資料來源結構描述的 JSON 納入為 [TemplateConfiguration](#) 物件的一部分。將資料來源的類型指定為 JDBC、資料庫類型為 sqlserver、驗證認證的密碼，以及其他必要的組態。然後，您將指定 TEMPLATE 為呼叫 Type 時 [CreateDataSource](#)。

您可以使用本開發人員指南中提供的模板。請參閱 [Microsoft SQL 服務器模式](#)。

下表說明微型 SQL 伺服器 JSON 結構描述的參數。

組態	描述
連線組態	資料來源端點的組態資訊。
repositoryEndpointMetadata	連線資料來源所需的組態資訊。 <ul style="list-style-type: none"> • 資料庫類型-您使用的 Java 資料庫類型 (無論是mysql、db2、postgresql oracle、或)。sqlserver • 資料庫主機 — 資料庫主機名稱。 • 資料庫埠 — 資料庫連接埠。 • 資料庫實例 — 資料庫執行處理。
儲存庫組態	資料來源內容的組態資訊。例如，配置特定類型的內容和欄位對應。指定資料來源的類型和秘密 ARN。

組態	描述
文件	將資料庫內容的屬性或欄位名稱對應至 Amazon Kendra 索引欄位名稱的物件清單。如需詳細資訊，請參閱 映射資料來源欄位 。
附加屬性	資料來源中內容的其他組態選項。用於在資料庫資料來源中包含或排除特定內容。
主要金鑰	提供資料庫表格的主索引鍵。這標識數據庫中的一個表。
標題欄	提供資料庫表格中文件標題欄的名稱。
身體專欄	提供資料庫表格中文件標題欄的名稱。
sqlQuery	輸入 SQL 查詢語句，如選擇和連接操作。SQL 查詢必須小於 32 KB。Amazon Kendra 會編目符合您查詢的所有資料庫內容。
時間戳記列	輸入包含時間戳記的列的名稱。Amazon Kendra 使用時間戳記資訊偵測內容中的變更，並僅同步變更的內容。
時間戳記格式	輸入包含時間戳記格式的資料欄名稱，可用來偵測內容變更並重新同步處理內容。
timezone	輸入包含要探索之內容之時區的資料欄名稱。
changeDetectingColumns	輸入 Amazon Kendra 將用來偵測內容變更的欄名稱。Amazon Kendra 當這些列中的任何一個更改時，將重新索引內容
allowedUsersColumns	輸入包含允許存取內容之使用者 ID 的欄名稱。
allowedGroupsColumn	輸入包含允許存取內容之使用者 ID 的欄名稱。
來源尿酸氧胺	輸入包含要編製索引之來源 URL 的資料欄名稱。

組態	描述
isSslEnabled	輸入 SQL 查詢語句，如選擇和連接操作。SQL 查詢必須小於 32 KB。Amazon Kendra 會編目符合您查詢的所有資料庫內容。
type	資料來源的類型。指定JDBC為您的資料來源類型。
同步模式	<p>指定資料來源內容變更時 Amazon Kendra 應如何更新索引。您可以選擇：</p> <ul style="list-style-type: none"> • FORCED_FULL_CRAWL 新建索引所有內容，並在每次資料來源與索引同步時取代現有內容。 • FULL_CRAWL ，每次您的資料來源與索引同步時，僅對新的、修改和刪除的內容建立索引。Amazon Kendra 可以使用資料來源的機制來追蹤內容變更，並為上次同步後變更的內容建立索引。 • CHANGE_LOG 每次資料來源與索引同步時，僅對新內容和修改的內容建立索引。Amazon Kendra 可以使用資料來源的機制來追蹤內容變更，並為上次同步後變更的內容建立索引。
秘密	<p>秘密 Secrets Manager 密碼的 Amazon 資源名稱 (ARN)，其中包含連線到資料庫所需的使用者名稱和密碼。秘密必須包含具有下列索引鍵的 JSON 結構：</p> <pre data-bbox="829 1499 1507 1696"> { "user name": "database user name", "password": " password" } </pre>
version	目前支援的範本版本。

Microsoft SQL 服務器模式

```
{
  "$schema": "http://json-schema.org/draft-04/schema#",
  "type": "object",
  "properties": {
    "connectionConfiguration": {
      "type": "object",
      "properties": {
        "repositoryEndpointMetadata": {
          "type": "object",
          "properties": {
            "dbType": {
              "type": "string",
              "enum": [
                "mysql",
                "db2",
                "postgresql",
                "oracle",
                "sqlserver"
              ]
            },
            "dbHost": {
              "type": "string"
            },
            "dbPort": {
              "type": "string"
            },
            "dbInstance": {
              "type": "string"
            }
          },
          "required": [
            "dbType",
            "dbHost",
            "dbPort",
            "dbInstance"
          ]
        }
      },
      "required": [
        "repositoryEndpointMetadata"
      ]
    },
  },
}
```



```
"repositoryConfigurations": {
  "type": "object",
  "properties": {
    "document": {
      "type": "object",
      "properties": {
        "fieldMappings": {
          "type": "array",
          "items": [
            {
              "type": "object",
              "properties": {
                "indexFieldName": {
                  "type": "string"
                },
                "indexFieldType": {
                  "type": "string"
                },
                "dataSourceFieldName": {
                  "type": "string"
                }
              },
              "required": [
                "indexFieldName",
                "indexFieldType",
                "dataSourceFieldName"
              ]
            }
          ]
        },
        "required": [
          "fieldMappings"
        ]
      }
    },
    "required": [
      "document"
    ]
  },
  "additionalProperties": {
    "type": "object",
    "properties": {
      "primaryKey": {
        "type": "string"
      }
    }
  }
}
```

```
    },
    "titleColumn": {
      "type": "string"
    },
    "bodyColumn": {
      "type": "string"
    },
    "sqlQuery": {
      "type": "string",
      "not": {
        "pattern": ";+"
      }
    },
    "timestampColumn": {
      "type": "string"
    },
    "timestampFormat": {
      "type": "string"
    },
    "timezone": {
      "type": "string"
    },
    "changeDetectingColumns": {
      "type": "array",
      "items": {
        "type": "string"
      }
    },
    "allowedUsersColumn": {
      "type": "string"
    },
    "allowedGroupsColumn": {
      "type": "string"
    },
    "sourceURIColumn": {
      "type": "string"
    },
    "isSslEnabled": {
      "type": "boolean"
    }
  },
  "required": ["primaryKey", "titleColumn", "bodyColumn", "sqlQuery"]
},
"type" : {
```

```

    "type" : "string",
    "pattern": "JDBC"
  },
  "syncMode": {
    "type": "string",
    "enum": [
      "FORCED_FULL_CRAWL",
      "FULL_CRAWL",
      "CHANGE_LOG"
    ]
  },
  "secretArn": {
    "type": "string"
  }
},
"version": {
  "type": "string",
  "anyOf": [
    {
      "pattern": "1.0.0"
    }
  ]
},
"required": [
  "connectionConfiguration",
  "repositoryConfigurations",
  "syncMode",
  "additionalProperties",
  "secretArn",
  "type"
]
}

```

Microsoft 團隊模板架構

您可以將包含資料來源結構描述的 JSON 納入為 [TemplateConfiguration](#) 物件的一部分。您可以提供承租人識別碼做為連線組態或存放庫端點詳細資料的一部分。同時將資料來源類型指定為 MSTEAMS、驗證認證的密碼，以及其他必要的組態。然後，您將指定 TEMPLATE 為呼叫 Type 時 [CreateDataSource](#)。

您可以使用本開發人員指南中提供的模板。請參閱 [Microsoft 團隊結構描述](#)。

下表說明 JSON 結構描述的參數。

組態	描述
連線組態	資料來源端點的組態資訊。
repositoryEndpointMetadata	資料來源的端點資訊。
特南蒂	Microsoft 365 租戶識別碼。您可以在 Azure 作用中目錄入口網站的內容或 OAuth 應用程式中找到您的租用戶識別碼。
儲存庫組態	資料來源內容的組態資訊。例如，配置特定類型的內容和欄位對應。
<ul style="list-style-type: none"> 聊天留言 聊天附件 渠道郵報 渠道維基 通道附件 會議聊天 會議檔案 會議備註 行事曆會議 	將 Microsoft Teams 內容的屬性或欄位名稱對應至 Amazon Kendra 索引欄位名稱的物件清單。如需詳細資訊，請參閱 映射資料來源欄位 。
附加屬性	資料來源中內容的其他組態選項。
付款模式	指定要搭配 Microsoft Teams 資料來源使用的付款模式類型。Model A 付款模式僅限於需要符合安全性規範的授權和付款模式。B 型付款模式適用於不需要安全性合規的授權和付款模式。
<ul style="list-style-type: none"> inclusionTeamName過濾器 inclusionChannelName過濾器 inclusionFileName模式 inclusionFileType模式 inclusionUserEmail過濾器 inclusionOneNoteSectionNamePatterns 	在 Microsoft Teams 資料來源中包含特定內容的規則運算式模式清單。符合模式的內容會包含在索引中。與模式不匹配的內容會從索引中排除。如果內容同時符合包含和排除模式，則排除模式優先，且內容不會包含在索引中。

組態	描述
<ul style="list-style-type: none"> inclusionOneNotePageNamePatterns 	
<ul style="list-style-type: none"> exclusionTeamName過濾器 exclusionChannelName過濾器 exclusionFileName模式 exclusionFileType模式 exclusionUserEmail過濾器 exclusionOneNoteSectionNamePatterns exclusionOneNotePageNamePatterns 	<p>用來排除 Microsoft Teams 資料來源中某些內容的規則運算式模式清單。符合模式的內容會從索引中排除。與模式不匹配的內容包含在索引中。如果內容同時符合包含和排除模式，則排除模式優先，且內容不會包含在索引中。</p>
<ul style="list-style-type: none"> isCrawlChat訊息 isCrawlChat附件 isCrawlChannel郵政 isCrawlChannel附件 isCrawlChannel維基 isCrawlCalendar會議 isCrawlMeeting聊天 isCrawlMeeting檔案 isCrawlMeeting注意 	<p>true以在您的 Microsoft 團隊資料來源中編目這些類型的內容。</p>
startCalendarDate時間	<p>您可以為行事曆內容設定特定的開始日期-時間。</p>
endCalendarDate時間	<p>您可以為行事曆內容設定特定的結束日期-時間。</p>
type	<p>資料來源的類型。指定MSTEAMS為您的資料來源類型。</p>

組態	描述
enableIdentityCrawler	true，以使用 Amazon Kendra 的身分識別爬行者程式來同步使用者和群組的身分識別/主體資訊，以存取特定文件。如果關閉身分搜索器，則可以公開搜索所有文檔。如果您想要對文件使用存取控制，且身分識別編目程式已關閉，您也可以使用 PutPrincipalMapping API 來上傳使用者和群組存取資訊。
同步模式	<p>指定資料來源內容變更時 Amazon Kendra 應如何更新索引。您可以選擇：</p> <ul style="list-style-type: none"> • FORCED_FULL_CRAWL 新建索引所有內容，並在每次資料來源與索引同步時取代現有內容。 • FULL_CRAWL，每次您的資料來源與索引同步時，僅對新的、修改和刪除的內容建立索引。Amazon Kendra 可以使用資料來源的機制來追蹤內容變更，並為上次同步後變更的內容建立索引。 • CHANGE_LOG 每次資料來源與索引同步時，僅對新內容和修改的內容建立索引。Amazon Kendra 可以使用資料來源的機制來追蹤內容變更，並為上次同步後變更的內容建立索引。
秘書	AWS Secrets Manager 秘密的 Amazon 資源名稱 (ARN)，其中包含連接到您的 Microsoft 團隊所需的鍵值對。這包括您在 Azure 入口網站中建立 OAuth 應用程式時所產生的用戶端識別碼和用戶端密碼。
version	目前支援的此範本版本。

Microsoft 團隊結構描述

```
{
```

```

"$schema": "http://json-schema.org/draft-04/schema#",
"type": "object",
"properties": {
  "connectionConfiguration": {
    "type": "object",
    "properties": {
      "repositoryEndpointMetadata": {
        "type": "object",
        "properties": {
          "tenantId": {
            "type": "string",
            "pattern": "^[0-9a-f]{8}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]
{12}$",
            "minLength": 36,
            "maxLength": 36
          }
        },
        "required": [
          "tenantId"
        ]
      }
    },
    "required": [
      "repositoryEndpointMetadata"
    ]
  },
  "repositoryConfigurations": {
    "type": "object",
    "properties": {
      "chatMessage": {
        "type": "object",
        "properties": {
          "fieldMappings": {
            "type": "array",
            "items": [
              {
                "type": "object",
                "properties": {
                  "indexFieldName": {
                    "type": "string"
                  },
                  "indexFieldType": {
                    "type": "string",
                    "enum": [

```

```
        "STRING",
        "STRING_LIST",
        "DATE"
    ]
  },
  "dataSourceFieldName": {
    "type": "string"
  },
  "dateFieldFormat": {
    "type": "string",
    "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
  }
},
"required": [
  "indexFieldName",
  "indexFieldType",
  "dataSourceFieldName"
]
}
]
}
},
"required": [
  "fieldMappings"
]
},
"chatAttachment": {
  "type": "object",
  "properties": {
    "fieldMappings": {
      "type": "array",
      "items": [
        {
          "type": "object",
          "properties": {
            "indexFieldName": {
              "type": "string"
            },
            "indexFieldType": {
              "type": "string",
              "enum": [
                "STRING",
                "DATE",
                "LONG"
              ]
            }
          }
        }
      ]
    }
  }
}
```



```
    ]
    },
    "dataSourceFieldName": {
      "type": "string"
    },
    "dateFieldFormat": {
      "type": "string",
      "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
    }
  },
  "required": [
    "indexFieldName",
    "indexFieldType",
    "dataSourceFieldName"
  ]
}
]
}
},
"required": [
  "fieldMappings"
]
},
"channelPost": {
  "type": "object",
  "properties": {
    "fieldMappings": {
      "type": "array",
      "items": [
        {
          "type": "object",
          "properties": {
            "indexFieldName": {
              "type": "string"
            },
            "indexFieldType": {
              "type": "string",
              "enum": [
                "STRING",
                "STRING_LIST",
                "DATE"
              ]
            }
          }
        }
      ]
    },
    "dataSourceFieldName": {
```

```

        "type": "string"
      },
      "dateFieldFormat": {
        "type": "string",
        "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
      }
    },
    "required": [
      "indexFieldName",
      "indexFieldType",
      "dataSourceFieldName"
    ]
  }
]
}
},
"required": [
  "fieldMappings"
]
},
"channelWiki": {
  "type": "object",
  "properties": {
    "fieldMappings": {
      "type": "array",
      "items": [
        {
          "type": "object",
          "properties": {
            "indexFieldName": {
              "type": "string"
            },
            "indexFieldType": {
              "type": "string",
              "enum": [
                "STRING",
                "DATE",
                "LONG"
              ]
            },
            "dataSourceFieldName": {
              "type": "string"
            }
          },
          "dateFieldFormat": {

```

```
        "type": "string",
        "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
    }
},
"required": [
    "indexFieldName",
    "indexFieldType",
    "dataSourceFieldName"
]
}
]
}
},
"required": [
    "fieldMappings"
]
},
"channelAttachment": {
    "type": "object",
    "properties": {
        "fieldMappings": {
            "type": "array",
            "items": [
                {
                    "type": "object",
                    "properties": {
                        "indexFieldName": {
                            "type": "string"
                        },
                    },
                    "indexFieldType": {
                        "type": "string",
                        "enum": [
                            "STRING",
                            "DATE",
                            "LONG"
                        ]
                    },
                    "dataSourceFieldName": {
                        "type": "string"
                    },
                    "dateFieldFormat": {
                        "type": "string",
                        "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                    }
                }
            ]
        }
    }
}
```

```
    },
    "required": [
      "indexFieldName",
      "indexFieldType",
      "dataSourceFieldName"
    ]
  }
]
},
"required": [
  "fieldMappings"
]
},
"meetingChat": {
  "type": "object",
  "properties": {
    "fieldMappings": {
      "type": "array",
      "items": [
        {
          "type": "object",
          "properties": {
            "indexFieldName": {
              "type": "string"
            },
            "indexFieldType": {
              "type": "string",
              "enum": [
                "STRING",
                "STRING_LIST",
                "DATE"
              ]
            },
            "dataSourceFieldName": {
              "type": "string"
            },
            "dateFieldFormat": {
              "type": "string",
              "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
            }
          }
        }
      ]
    },
    "required": [
      "indexFieldName",
```

```
        "indexFieldType",
        "dataSourceFieldName"
    ]
}
]
}
},
"required": [
    "fieldMappings"
]
},
"meetingFile": {
    "type": "object",
    "properties": {
        "fieldMappings": {
            "type": "array",
            "items": [
                {
                    "type": "object",
                    "properties": {
                        "indexFieldName": {
                            "type": "string"
                        },
                        "indexFieldType": {
                            "type": "string",
                            "enum": [
                                "STRING",
                                "DATE",
                                "LONG"
                            ]
                        },
                        "dataSourceFieldName": {
                            "type": "string"
                        },
                        "dateFieldFormat": {
                            "type": "string",
                            "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                        }
                    },
                    "required": [
                        "indexFieldName",
                        "indexFieldType",
                        "dataSourceFieldName"
                    ]
                }
            ]
        }
    }
}
```

```
    }
  ]
}
},
"required": [
  "fieldMappings"
]
},
"meetingNote": {
  "type": "object",
  "properties": {
    "fieldMappings": {
      "type": "array",
      "items": [
        {
          "type": "object",
          "properties": {
            "indexFieldName": {
              "type": "string"
            },
            "indexFieldType": {
              "type": "string",
              "enum": [
                "STRING",
                "DATE"
              ]
            },
            "dataSourceFieldName": {
              "type": "string"
            },
            "dateFieldFormat": {
              "type": "string",
              "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
            }
          }
        },
        "required": [
          "indexFieldName",
          "indexFieldType",
          "dataSourceFieldName"
        ]
      ]
    }
  }
},
```

```
    "required": [
      "fieldMappings"
    ]
  },
  "calendarMeeting": {
    "type": "object",
    "properties": {
      "fieldMappings": {
        "type": "array",
        "items": [
          {
            "type": "object",
            "properties": {
              "indexFieldName": {
                "type": "string"
              },
              "indexFieldType": {
                "type": "string",
                "enum": [
                  "STRING",
                  "DATE"
                ]
              },
              "dataSourceFieldName": {
                "type": "string"
              },
              "dateFieldFormat": {
                "type": "string",
                "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
              }
            }
          },
          "required": [
            "indexFieldName",
            "indexFieldType",
            "dataSourceFieldName"
          ]
        ]
      }
    ]
  },
  "required": [
    "fieldMappings"
  ]
}
```

```
    }
  },
  "additionalProperties": {
    "type": "object",
    "properties": {
      "paymentModel": {
        "type": "string",
        "enum": [
          "A",
          "B",
          "Evaluation Mode"
        ]
      },
      "inclusionTeamNameFilter": {
        "type": "array",
        "items": {
          "type": "string"
        }
      },
      "exclusionTeamNameFilter": {
        "type": "array",
        "items": {
          "type": "string"
        }
      },
      "inclusionChannelNameFilter": {
        "type": "array",
        "items": {
          "type": "string"
        }
      },
      "exclusionChannelNameFilter": {
        "type": "array",
        "items": {
          "type": "string"
        }
      },
      "inclusionFileNamePatterns": {
        "type": "array",
        "items": {
          "type": "string"
        }
      },
      "exclusionFileNamePatterns": {
```



```
    "type": "array",
    "items": {
      "type": "string"
    }
  },
  "inclusionFileTypePatterns": {
    "type": "array",
    "items": {
      "type": "string"
    }
  },
  "exclusionFileTypePatterns": {
    "type": "array",
    "items": {
      "type": "string"
    }
  },
  "inclusionUserEmailFilter": {
    "type": "array",
    "items": {
      "type": "string"
    }
  },
  "inclusionOneNoteSectionNamePatterns": {
    "type": "array",
    "items": {
      "type": "string"
    }
  },
  "exclusionOneNoteSectionNamePatterns": {
    "type": "array",
    "items": {
      "type": "string"
    }
  },
  "inclusionOneNotePageNamePatterns": {
    "type": "array",
    "items": {
      "type": "string"
    }
  },
  "exclusionOneNotePageNamePatterns": {
    "type": "array",
    "items": {
```

```
    "type": "string"
  }
},
"isCrawlChatMessage": {
  "type": "boolean"
},
"isCrawlChatAttachment": {
  "type": "boolean"
},
"isCrawlChannelPost": {
  "type": "boolean"
},
"isCrawlChannelAttachment": {
  "type": "boolean"
},
"isCrawlChannelWiki": {
  "type": "boolean"
},
"isCrawlCalendarMeeting": {
  "type": "boolean"
},
"isCrawlMeetingChat": {
  "type": "boolean"
},
"isCrawlMeetingFile": {
  "type": "boolean"
},
"isCrawlMeetingNote": {
  "type": "boolean"
},
"startCalendarDateTime": {
  "anyOf": [
    {
      "type": "string",
      "pattern": "^[0-9]{4}-[0-9]{2}-[0-9]{2}T[0-9]{2}:[0-9]{2}:[0-9]{2}Z$"
    },
    {
      "type": "string",
      "pattern": ""
    }
  ]
},
"endCalendarDateTime": {
  "anyOf": [
```

```
        {
          "type": "string",
          "pattern": "^[0-9]{4}-[0-9]{2}-[0-9]{2}T[0-9]{2}:[0-9]{2}:[0-9]{2}Z$"
        },
        {
          "type": "string",
          "pattern": ""
        }
      ]
    },
    "required": [],
  },
  "type": {
    "type": "string",
    "pattern": "MSTEAMS"
  },
  "enableIdentityCrawler": {
    "type": "boolean"
  },
  "syncMode": {
    "type": "string",
    "enum": [
      "FORCED_FULL_CRAWL",
      "FULL_CRAWL",
      "CHANGE_LOG"
    ]
  },
  "secretArn": {
    "type": "string",
    "minLength": 20,
    "maxLength": 2048
  }
},
"version": {
  "type": "string",
  "anyOf": [
    {
      "pattern": "1.0.0"
    }
  ]
},
"required": [
  "connectionConfiguration",
```

```

    "repositoryConfigurations",
    "syncMode",
    "additionalProperties",
    "secretArn",
    "type"
  ]
}

```

Microsoft 模板架構

您可以將包含資料來源結構描述的 JSON 納入為 [TemplateConfiguration](#) 物件的一部分。將資料來源類型指定為 YAMMER、驗證認證的密碼，以及其他必要的組態。然後您在呼叫時指定 TEMPLATE 為 Type [CreateDataSource](#)。

您可以使用本開發人員指南中提供的模板。

下表說明 Microsoft 的 JSON 結構描述的參數。

組態	描述
連線組態	資料來源的組態資訊。
repositoryEndpointMetadata	資料來源的端點資訊。此資料來源未在中指定端點 <code>repositoryEndpointMetadata</code> 。相反地，連線資訊會包含在您提供的 AWS Secrets Manager 密碼中 <code>secretArn</code> 。
儲存庫組態	資料來源內容的組態資訊。例如，配置特定類型的內容和欄位對應。
<ul style="list-style-type: none"> • 社區 • 使用者 • message • attachment 	將 Microsoft Yammer 內容的屬性或欄位名稱對應至 Amazon Kendra 索引欄位名稱的物件清單。如需詳細資訊，請參閱 映射資料來源欄位 。
附加屬性	資料來源中內容的其他設定選項
包含模式	規則運算式模式清單，以包含 Microsoft Yammer 資料來源中的某些檔案。符合模式的檔案會包括在索引中。不符合模式的檔案會從索

組態	描述
	引中排除。如果檔案同時符合包括模式和排除模式，則以排除模式為優先，且該項目不會包括在索引中。
排除模式	規則運算式模式清單，可排除 Microsoft Yammer 資料來源中的某些檔案。符合模式的檔案會從索引中排除。與模式不匹配的文件包含在索引中。如果檔案同時符合排除和包含模式，則排除模式優先，且檔案不會包含在索引中。
自最新	您可以選擇設定 <code>sinceDate</code> 參數，以便 Microsoft Yammer 連接器根據特定內容進行編目。 <code>sinceDate</code>
<code>communityNameFilter</code>	您可以選擇索引特定的社群內容。
<ul style="list-style-type: none"> <code>isCrawlMessage</code> <code>isCrawlAttachment</code> <code>isCrawlPrivate</code> 訊息 	<code>true</code> 抓取郵件、郵件附件和私人訊息。
<code>type</code>	指定 YAMMER 為您的資料來源類型。
秘书	AWS Secrets Manager 秘密的 Amazon 資源名稱 (ARN)，其中包含連接到 Microsoft Yammer 所需的鍵值對。這包括您的 Microsoft Yammer 使用者名稱和密碼，以及當您在 Azure 入口網站中建立 OAuth 應用程式時所產生的用戶端識別碼和用戶端密碼。
<code>useChangeLog</code>	<code>true</code> 使用 Microsoft Yammer 變更記錄檔來判斷哪些文件需要在索引中更新。

組態	描述
同步模式	<p>指定資料來源內容變更時 Amazon Kendra 應如何更新索引。您可以選擇：</p> <ul style="list-style-type: none"> • FORCED_FULL_CRAWL 新建索引所有內容，並在每次資料來源與索引同步時取代現有內容。 • FULL_CRAWL ，每次您的資料來源與索引同步時，僅對新的、修改和刪除的內容建立索引。Amazon Kendra 可以使用資料來源的機制來追蹤內容變更，並為上次同步後變更的內容建立索引。 • CHANGE_LOG 每次資料來源與索引同步時，僅對新內容和修改的內容建立索引。Amazon Kendra 可以使用資料來源的機制來追蹤內容變更，並為上次同步後變更的內容建立索引。
enableIdentityCrawler	<p>true，以使用 Amazon Kendra 的身分識別爬行者程式來同步使用者和群組的身分識別/主體資訊，以存取特定文件。如果關閉身分搜索器，則可以公開搜索所有文檔。如果您想要對文件使用存取控制，且身分識別編目程式已關閉，您也可以使用 PutPrincipalMapping API 來上傳使用者和群組存取資訊。</p>

Microsoft JSON 架構

```
{
  "$schema": "http://json-schema.org/draft-04/schema#",
  "type": "object",
  "properties": {
    "connectionConfiguration": {
      "type": "object",
      "properties": {
        "repositoryEndpointMetadata": {
          "type": "object",
          "properties": {
```

```
    }
  }
},
"required": [
  "repositoryEndpointMetadata"
],
"repositoryConfigurations": {
  "type": "object",
  "properties": {
    "community": {
      "type": "object",
      "properties": {
        "fieldMappings": {
          "type": "array",
          "items": {
            "anyOf": [
              {
                "type": "object",
                "properties": {
                  "indexFieldName": {
                    "type": "string"
                  },
                  "indexFieldType": {
                    "type": "string",
                    "enum": [
                      "STRING",
                      "DATE"
                    ]
                  }
                }
              },
              {
                "dataSourceFieldName": {
                  "type": "string"
                },
                "dateFieldFormat": {
                  "type": "string",
                  "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                }
              }
            ]
          },
          "required": [
            "indexFieldName",
            "indexFieldType",
            "dataSourceFieldName"
          ]
        }
      }
    }
  }
}
```

```
    ]
  }
}
},
"required": [
  "fieldMappings"
]
},
"user": {
  "type": "object",
  "properties": {
    "fieldMappings": {
      "type": "array",
      "items": {
        "anyOf": [
          {
            "type": "object",
            "properties": {
              "indexFieldName": {
                "type": "string"
              },
              "indexFieldType": {
                "type": "string",
                "enum": [
                  "STRING",
                  "DATE"
                ]
              },
              "dataSourceFieldName": {
                "type": "string"
              },
              "dateFieldFormat": {
                "type": "string",
                "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
              }
            },
            "required": [
              "indexFieldName",
              "indexFieldType",
              "dataSourceFieldName"
            ]
          }
        ]
      }
    }
  }
}
```



```
    }
  },
  "required": [
    "fieldMappings"
  ]
},
"message": {
  "type": "object",
  "properties": {
    "fieldMappings": {
      "type": "array",
      "items": {
        "anyOf": [
          {
            "type": "object",
            "properties": {
              "indexFieldName": {
                "type": "string"
              },
              "indexFieldType": {
                "type": "string",
                "enum": [
                  "STRING",
                  "DATE"
                ]
              },
              "dataSourceFieldName": {
                "type": "string"
              },
              "dateFieldFormat": {
                "type": "string",
                "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
              }
            }
          },
          "required": [
            "indexFieldName",
            "indexFieldType",
            "dataSourceFieldName"
          ]
        ]
      }
    }
  }
},
```

```
    "required": [
      "fieldMappings"
    ]
  },
  "attachment": {
    "type": "object",
    "properties": {
      "fieldMappings": {
        "type": "array",
        "items": {
          "anyOf": [
            {
              "type": "object",
              "properties": {
                "indexFieldName": {
                  "type": "string"
                },
                "indexFieldType": {
                  "type": "string",
                  "enum": [
                    "STRING",
                    "DATE"
                  ]
                },
                "dataSourceFieldName": {
                  "type": "string"
                },
                "dateFieldFormat": {
                  "type": "string",
                  "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                }
              }
            },
            "required": [
              "indexFieldName",
              "indexFieldType",
              "dataSourceFieldName"
            ]
          ]
        }
      }
    }
  },
  "required": [
    "fieldMappings"
  ]
}
```

```

    ]
  }
}
},
"additionalProperties": {
  "type": "object",
  "properties": {
    "inclusionPatterns": {
      "type": "array"
    },
    "exclusionPatterns": {
      "type": "array"
    },
    "sinceDate": {
      "type": "string",
      "pattern": "^(19|2[0-9])[0-9]{2}-(0[1-9]|1[012])-(0[1-9]|[12][0-9]|
3[01])T(0[0-9]|1[0-9]|2[0-3]):([0-5][0-9]):([0-5][0-9])(\\+|-)(0[0-9]|1[0-9]|2[0-3]):
([0-5][0-9]))? $"
    },
    "communityNameFilter": {
      "type": "array",
      "items": {
        "type": "string"
      }
    },
    "isCrawlMessage": {
      "type": "boolean"
    },
    "isCrawlAttachment": {
      "type": "boolean"
    },
    "isCrawlPrivateMessage": {
      "type": "boolean"
    }
  },
  "required": [
    "sinceDate"
  ]
},
"type": {
  "type": "string",
  "pattern": "YAMMER"
},
"secretArn": {

```

```
    "type": "string",
    "minLength": 20,
    "maxLength": 2048
  },
  "useChangeLog": {
    "type": "string",
    "enum": [
      "true",
      "false"
    ]
  },
  "syncMode": {
    "type": "string",
    "enum": [
      "FORCED_FULL_CRAWL",
      "FULL_CRAWL",
      "CHANGE_LOG"
    ]
  },
  "enableIdentityCrawler": {
    "type": "boolean"
  },
  "version": {
    "type": "string",
    "anyOf": [
      {
        "pattern": "1.0.0"
      }
    ]
  }
},
"required": [
  "connectionConfiguration",
  "repositoryConfigurations",
  "additionalProperties",
  "type",
  "secretArn",
  "syncMode"
]
}
```

MySQL 板架構

您可以將包含資料來源結構描述的 JSON 納入為 [TemplateConfiguration](#) 物件的一部分。將資料來源的類型指定為 JDBC、資料庫類型為 `mysql`、驗證認證的密碼，以及其他必要的組態。然後，您將指定 `TEMPLATE` 為呼叫 `Type` 時 [CreateDataSource](#)。

您可以使用本開發人員指南中提供的模板。請參閱 [結構定義](#)。

下表說明 MySQL JSON 結構定義的參數。

組態	描述
連線組態	資料來源端點的組態資訊。
<code>repositoryEndpointMetadata</code>	連線資料來源所需的組態資訊。 <ul style="list-style-type: none"> • 資料庫類型-您使用的 Java 資料庫類型 (無論是 <code>mysql</code>、<code>db2</code>、<code>postgresql</code>、<code>oracle</code>、或)。<code>sqlserver</code> • 資料庫主機 — 資料庫主機名稱。 • 資料庫埠 — 資料庫連接埠。 • 資料庫實例 — 資料庫執行處理。
儲存庫組態	資料來源內容的組態資訊。例如，配置特定類型的內容和欄位對應。指定資料來源的類型和秘密 ARN。
文件	將資料庫內容的屬性或欄位名稱對應至 Amazon Kendra 索引欄位名稱的物件清單。如需詳細資訊，請參閱 映射資料來源欄位 。
附加屬性	資料來源中內容的其他組態選項。用於在資料庫資料來源中包含或排除特定內容。
主要金鑰	提供資料庫表格的主索引鍵。這標識數據庫中的一個表。
標題欄	提供資料庫表格中文件標題欄的名稱。

組態	描述
身體專欄	提供資料庫表格中文件標題欄的名稱。
sqlQuery	輸入 SQL 查詢語句，如選擇和連接操作。SQL 查詢必須小於 32 KB。Amazon Kendra 會編目符合您查詢的所有資料庫內容。
時間戳記列	輸入包含時間戳記的列的名稱。Amazon Kendra 使用時間戳記資訊偵測內容中的變更，並僅同步變更的內容。
時間戳記格式	輸入包含時間戳記格式的資料欄名稱，可用來偵測內容變更並重新同步處理內容。
timezone	輸入包含要探索之內容之時區的資料欄名稱。
changeDetectingColumns	輸入 Amazon Kendra 將用來偵測內容變更的欄名稱。Amazon Kendra 當這些列中的任何一個更改時，將重新索引內容
allowedUsersColumns	輸入包含允許存取內容之使用者 ID 的欄名稱。
allowedGroupsColumn	輸入包含允許存取內容之使用者 ID 的欄名稱。
來源尿酸氧胺	輸入包含要編製索引之來源 URL 的資料欄名稱。
isSslEnabled	輸入 SQL 查詢語句，如選擇和連接操作。SQL 查詢必須小於 32 KB。Amazon Kendra 會編目符合您查詢的所有資料庫內容。
type	資料來源的類型。指定JDBC為您的資料來源類型。

組態	描述
同步模式	<p>指定資料來源內容變更時 Amazon Kendra 應如何更新索引。您可以選擇：</p> <ul style="list-style-type: none"> • FORCED_FULL_CRAWL 新建索引所有內容，並在每次資料來源與索引同步時取代現有內容。 • FULL_CRAWL ，每次您的資料來源與索引同步時，僅對新的、修改和刪除的內容建立索引。Amazon Kendra 可以使用資料來源的機制來追蹤內容變更，並為上次同步後變更的內容建立索引。 • CHANGE_LOG 每次資料來源與索引同步時，僅對新內容和修改的內容建立索引。Amazon Kendra 可以使用資料來源的機制來追蹤內容變更，並為上次同步後變更的內容建立索引。
秘書	<p>秘密 Secrets Manager 密碼的 Amazon 資源名稱 (ARN)，其中包含連線到資料庫所需的使用者名稱和密碼。私密必須包含具有下列索引鍵的 JSON 結構：</p> <pre data-bbox="829 1192 1507 1394"> { "user name": "database user name", "password": "password" } </pre>
version	目前支援的範本版本。

結構定義

```

{
  "$schema": "http://json-schema.org/draft-04/schema#",
  "type": "object",
  "properties": {
    "connectionConfiguration": {
      "type": "object",

```

```
"properties": {
  "repositoryEndpointMetadata": {
    "type": "object",
    "properties": {
      "dbType": {
        "type": "string",
        "enum": [
          "mysql",
          "db2",
          "postgresql",
          "oracle",
          "sqlserver"
        ]
      },
      "dbHost": {
        "type": "string"
      },
      "dbPort": {
        "type": "string"
      },
      "dbInstance": {
        "type": "string"
      }
    },
    "required": [
      "dbType",
      "dbHost",
      "dbPort",
      "dbInstance"
    ]
  },
  "required": [
    "repositoryEndpointMetadata"
  ]
},
"repositoryConfigurations": {
  "type": "object",
  "properties": {
    "document": {
      "type": "object",
      "properties": {
        "fieldMappings": {
          "type": "array",
```



```
    "items": [
      {
        "type": "object",
        "properties": {
          "indexFieldName": {
            "type": "string"
          },
          "indexFieldType": {
            "type": "string"
          },
          "dataSourceFieldName": {
            "type": "string"
          }
        },
        "required": [
          "indexFieldName",
          "indexFieldType",
          "dataSourceFieldName"
        ]
      }
    ],
    "required": [
      "fieldMappings"
    ]
  },
  "required": [
  ]
},
"additionalProperties": {
  "type": "object",
  "properties": {
    "primaryKey": {
      "type": "string"
    },
    "titleColumn": {
      "type": "string"
    },
    "bodyColumn": {
      "type": "string"
    },
    "sqlQuery": {
```

```
    "type": "string",
    "not": {
      "pattern": ";+"
    }
  },
  "timestampColumn": {
    "type": "string"
  },
  "timestampFormat": {
    "type": "string"
  },
  "timezone": {
    "type": "string"
  },
  "changeDetectingColumns": {
    "type": "array",
    "items": {
      "type": "string"
    }
  },
  "allowedUsersColumn": {
    "type": "string"
  },
  "allowedGroupsColumn": {
    "type": "string"
  },
  "sourceURIColumn": {
    "type": "string"
  },
  "isSslEnabled": {
    "type": "boolean"
  }
},
"required": ["primaryKey", "titleColumn", "bodyColumn", "sqlQuery"]
},
"type" : {
  "type" : "string",
  "pattern": "JDBC"
},
"syncMode": {
  "type": "string",
  "enum": [
    "FORCED_FULL_CRAWL",
    "FULL_CRAWL",
```

```

    "CHANGE_LOG"
  ]
},
"secretArn": {
  "type": "string"
}
},
"version": {
  "type": "string",
  "anyOf": [
    {
      "pattern": "1.0.0"
    }
  ]
},
"required": [
  "connectionConfiguration",
  "repositoryConfigurations",
  "syncMode",
  "additionalProperties",
  "secretArn",
  "type"
]
}

```

Oracle 資料庫範本綱要

您可以將包含資料來源結構描述的 JSON 納入為 [TemplateConfiguration](#) 物件的一部分。將資料來源的類型指定為 JDBC、資料庫類型為 oracle、驗證認證的密碼，以及其他必要的組態。然後，您將指定 TEMPLATE 為呼叫 Type 時 [CreateDataSource](#)。

您可以使用本開發人員指南中提供的模板。請參閱 [甲骨文数据库模式](#)。

下表說明 Oracle 資料庫 JSON 結構描述的參數。

組態	描述
連線組態	資料來源端點的組態資訊。
repositoryEndpointMetadata	連線資料來源所需的組態資訊。

組態	描述
	<ul style="list-style-type: none"> • 資料庫類型-您使用的 Java 資料庫類型 (無論是mysql、db2、postgresql oracle、或)。sqlserver • 資料庫主機 — 資料庫主機名稱。 • 資料庫埠 — 資料庫連接埠。 • 資料庫實例 — 資料庫執行處理。
儲存庫組態	資料來源內容的組態資訊。例如，配置特定類型的內容和欄位對應。指定資料來源的類型和秘密 ARN。
文件	將資料庫內容的屬性或欄位名稱對應至 Amazon Kendra 索引欄位名稱的物件清單。如需詳細資訊，請參閱 映射資料來源欄位 。
附加屬性	資料來源中內容的其他組態選項。用於在資料庫資料來源中包含或排除特定內容。
主要金鑰	提供資料庫表格的主索引鍵。這標識數據庫中的一個表。
標題欄	提供資料庫表格中文件標題欄的名稱。
身體專欄	提供資料庫表格中文件標題欄的名稱。
sqlQuery	輸入 SQL 查詢語句，如選擇和連接操作。SQL 查詢必須小於 32 KB。Amazon Kendra 會編目符合您查詢的所有資料庫內容。
時間戳記列	輸入包含時間戳記的列的名稱。Amazon Kendra 使用時間戳記資訊偵測內容中的變更，並僅同步變更的內容。
時間戳記格式	輸入包含時間戳記格式的資料欄名稱，可用來偵測內容變更並重新同步處理內容。
timezone	輸入包含要探索之內容之時區的資料欄名稱。

組態	描述
changeDetectingColumns	輸入 Amazon Kendra 將用來偵測內容變更的欄名稱。Amazon Kendra 當這些列中的任何一個更改時，將重新索引內容。
allowedUsersColumns	輸入包含允許存取內容之使用者 ID 的欄名稱。
allowedGroupsColumn	輸入包含允許存取內容之使用者 ID 的欄名稱。
來源尿酸氧胺	輸入包含要編製索引之來源 URL 的資料欄名稱。
isSslEnabled	輸入 SQL 查詢語句，如選擇和連接操作。SQL 查詢必須小於 32 KB。Amazon Kendra 會編目符合您查詢的所有資料庫內容。
type	資料來源的類型。指定 JDBC 為您的資料來源類型。
同步模式	<p>指定資料來源內容變更時 Amazon Kendra 應如何更新索引。您可以選擇：</p> <ul style="list-style-type: none"> • FORCED_FULL_CRAWL 新建索引所有內容，並在每次資料來源與索引同步時取代現有內容。 • FULL_CRAWL，每次您的資料來源與索引同步時，僅對新的、修改和刪除的內容建立索引。Amazon Kendra 可以使用資料來源的機制來追蹤內容變更，並為上次同步後變更的內容建立索引。 • CHANGE_LOG 每次資料來源與索引同步時，僅對新內容和修改的內容建立索引。Amazon Kendra 可以使用資料來源的機制來追蹤內容變更，並為上次同步後變更的內容建立索引。

組態	描述
秘书	<p>秘密 Secrets Manager 密碼的 Amazon 資源名稱 (ARN)，其中包含連線到資料庫所需的使用者名稱和密碼。私密必須包含具有下列索引鍵的 JSON 結構：</p> <pre data-bbox="829 443 1507 642"> { "user name": "<i>database user name</i>", "password": "<i>password</i>" } </pre>
version	目前支援的範本版本。

甲骨文数据库模式

```

{
  "$schema": "http://json-schema.org/draft-04/schema#",
  "type": "object",
  "properties": {
    "connectionConfiguration": {
      "type": "object",
      "properties": {
        "repositoryEndpointMetadata": {
          "type": "object",
          "properties": {
            "dbType": {
              "type": "string",
              "enum": [
                "mysql",
                "db2",
                "postgresql",
                "oracle",
                "sqlserver"
              ]
            },
            "dbHost": {
              "type": "string"
            },
            "dbPort": {
              "type": "string"
            }
          }
        }
      }
    }
  }
}

```

```
    },
    "dbInstance": {
      "type": "string"
    }
  },
  "required": [
    "dbType",
    "dbHost",
    "dbPort",
    "dbInstance"
  ]
},
"required": [
  "repositoryEndpointMetadata"
],
"repositoryConfigurations": {
  "type": "object",
  "properties": {
    "document": {
      "type": "object",
      "properties": {
        "fieldMappings": {
          "type": "array",
          "items": [
            {
              "type": "object",
              "properties": {
                "indexFieldName": {
                  "type": "string"
                },
                "indexFieldType": {
                  "type": "string"
                },
                "dataSourceFieldName": {
                  "type": "string"
                }
              }
            }
          ]
        },
        "required": [
          "indexFieldName",
          "indexFieldType",
          "dataSourceFieldName"
        ]
      }
    }
  }
}
```

```
        }
      ]
    }
  },
  "required": [
    "fieldMappings"
  ]
}
},
"required": [
]
},
"additionalProperties": {
  "type": "object",
  "properties": {
    "primaryKey": {
      "type": "string"
    },
    "titleColumn": {
      "type": "string"
    },
    "bodyColumn": {
      "type": "string"
    },
    "sqlQuery": {
      "type": "string",
      "not": {
        "pattern": ";+"
      }
    },
    "timestampColumn": {
      "type": "string"
    },
    "timestampFormat": {
      "type": "string"
    },
    "timezone": {
      "type": "string"
    },
    "changeDetectingColumns": {
      "type": "array",
      "items": {
        "type": "string"
      }
    }
  }
}
```



```
    },
    "allowedUsersColumn": {
      "type": "string"
    },
    "allowedGroupsColumn": {
      "type": "string"
    },
    "sourceURIColumn": {
      "type": "string"
    },
    "isSslEnabled": {
      "type": "boolean"
    }
  },
  "required": ["primaryKey", "titleColumn", "bodyColumn", "sqlQuery"]
},
"type" : {
  "type" : "string",
  "pattern": "JDBC"
},
"syncMode": {
  "type": "string",
  "enum": [
    "FORCED_FULL_CRAWL",
    "FULL_CRAWL",
    "CHANGE_LOG"
  ]
},
"secretArn": {
  "type": "string"
}
},
"version": {
  "type": "string",
  "anyOf": [
    {
      "pattern": "1.0.0"
    }
  ]
}
},
"required": [
  "connectionConfiguration",
  "repositoryConfigurations",
  "syncMode",
```

```

    "additionalProperties",
    "secretArn",
    "type"
  ]
}
```

PostgreSQL 架構

您可以將包含資料來源結構描述的 JSON 納入為 [TemplateConfiguration](#) 物件的一部分。將資料來源的類型指定為 JDBC、資料庫類型為 postgresql、驗證認證的密碼，以及其他必要的組態。然後，您將指定 TEMPLATE 為呼叫 Type 時 [CreateDataSource](#)。

您可以使用本開發人員指南中提供的模板。請參閱 [PostgreSQL 構](#)。

下表說明 JSON 結構描述的參數。

組態	描述
連線組態	資料來源端點的組態資訊。
repositoryEndpointMetadata	連線資料來源所需的組態資訊。 <ul style="list-style-type: none"> 資料庫類型-您使用的 Java 資料庫類型 (無論是mysql、db2、postgresql oracle、或)。sqlserver 資料庫主機 — 資料庫主機名稱。 資料庫埠 — 資料庫連接埠。 資料庫實例 — 資料庫執行處理。
儲存庫組態	資料來源內容的組態資訊。例如，配置特定類型的內容和欄位對應。指定資料來源的類型和秘密 ARN。
文件	將資料庫內容的屬性或欄位名稱對應至 Amazon Kendra 索引欄位名稱的物件清單。如需詳細資訊，請參閱 映射資料來源欄位 。
附加屬性	資料來源中內容的其他組態選項。用於在資料庫資料來源中包含或排除特定內容。

組態	描述
主要金鑰	提供資料庫表格的主索引鍵。這標識數據庫中的一個表。
標題欄	提供資料庫表格中文件標題欄的名稱。
身體專欄	提供資料庫表格中文件標題欄的名稱。
sqlQuery	輸入 SQL 查詢語句，如選擇和連接操作。SQL 查詢必須小於 32 KB。Amazon Kendra 會編目符合您查詢的所有資料庫內容。
時間戳記列	輸入包含時間戳記的列的名稱。Amazon Kendra 使用時間戳記資訊偵測內容中的變更，並僅同步變更的內容。
時間戳記格式	輸入包含時間戳記格式的資料欄名稱，可用來偵測內容變更並重新同步處理內容。
timezone	輸入包含要探索之內容之時區的資料欄名稱。
changeDetectingColumns	輸入 Amazon Kendra 將用來偵測內容變更的欄名稱。Amazon Kendra 當這些列中的任何一個更改時，將重新索引內容
allowedUsersColumns	輸入包含允許存取內容之使用者 ID 的欄名稱。
allowedGroupsColumn	輸入包含允許存取內容之使用者 ID 的欄名稱。
來源尿酸氧胺	輸入包含要編製索引之來源 URL 的資料欄名稱。
isSslEnabled	輸入 SQL 查詢語句，如選擇和連接操作。SQL 查詢必須小於 32 KB。Amazon Kendra 會編目符合您查詢的所有資料庫內容。
type	資料來源的類型。指定JDBC為您的資料來源類型。

組態	描述
同步模式	<p>指定資料來源內容變更時 Amazon Kendra 應如何更新索引。您可以選擇：</p> <ul style="list-style-type: none"> • FORCED_FULL_CRAWL 新建索引所有內容，並在每次資料來源與索引同步時取代現有內容。 • FULL_CRAWL ，每次您的資料來源與索引同步時，僅對新的、修改和刪除的內容建立索引。Amazon Kendra 可以使用資料來源的機制來追蹤內容變更，並為上次同步後變更的內容建立索引。 • CHANGE_LOG 每次資料來源與索引同步時，僅對新內容和修改的內容建立索引。Amazon Kendra 可以使用資料來源的機制來追蹤內容變更，並為上次同步後變更的內容建立索引。
秘書	<p>秘密 Secrets Manager 密碼的 Amazon 資源名稱 (ARN)，其中包含連線到資料庫所需的使用者名稱和密碼。私密必須包含具有下列索引鍵的 JSON 結構：</p> <pre data-bbox="829 1192 1507 1394"> { "user name": "database user name", "password": "password" } </pre>
version	目前支援的範本版本。

PostgreSQL 構

```

{
  "$schema": "http://json-schema.org/draft-04/schema#",
  "type": "object",
  "properties": {
    "connectionConfiguration": {
      "type": "object",

```

```
"properties": {
  "repositoryEndpointMetadata": {
    "type": "object",
    "properties": {
      "dbType": {
        "type": "string",
        "enum": [
          "mysql",
          "db2",
          "postgresql",
          "oracle",
          "sqlserver"
        ]
      },
      "dbHost": {
        "type": "string"
      },
      "dbPort": {
        "type": "string"
      },
      "dbInstance": {
        "type": "string"
      }
    },
    "required": [
      "dbType",
      "dbHost",
      "dbPort",
      "dbInstance"
    ]
  },
  "required": [
    "repositoryEndpointMetadata"
  ]
},
"repositoryConfigurations": {
  "type": "object",
  "properties": {
    "document": {
      "type": "object",
      "properties": {
        "fieldMappings": {
          "type": "array",
```

```
    "items": [
      {
        "type": "object",
        "properties": {
          "indexFieldName": {
            "type": "string"
          },
          "indexFieldType": {
            "type": "string"
          },
          "dataSourceFieldName": {
            "type": "string"
          }
        },
        "required": [
          "indexFieldName",
          "indexFieldType",
          "dataSourceFieldName"
        ]
      }
    ],
    "required": [
      "fieldMappings"
    ]
  },
  "required": [
  ]
},
"additionalProperties": {
  "type": "object",
  "properties": {
    "primaryKey": {
      "type": "string"
    },
    "titleColumn": {
      "type": "string"
    },
    "bodyColumn": {
      "type": "string"
    },
    "sqlQuery": {
```

```
    "type": "string",
    "not": {
      "pattern": ";+"
    }
  },
  "timestampColumn": {
    "type": "string"
  },
  "timestampFormat": {
    "type": "string"
  },
  "timezone": {
    "type": "string"
  },
  "changeDetectingColumns": {
    "type": "array",
    "items": {
      "type": "string"
    }
  },
  "allowedUsersColumn": {
    "type": "string"
  },
  "allowedGroupsColumn": {
    "type": "string"
  },
  "sourceURIColumn": {
    "type": "string"
  },
  "isSslEnabled": {
    "type": "boolean"
  }
},
"required": ["primaryKey", "titleColumn", "bodyColumn", "sqlQuery"]
},
"type" : {
  "type" : "string",
  "pattern": "JDBC"
},
"syncMode": {
  "type": "string",
  "enum": [
    "FORCED_FULL_CRAWL",
    "FULL_CRAWL",
```

```

    "CHANGE_LOG"
  ]
},
"secretArn": {
  "type": "string"
}
},
"version": {
  "type": "string",
  "anyOf": [
    {
      "pattern": "1.0.0"
    }
  ]
},
"required": [
  "connectionConfiguration",
  "repositoryConfigurations",
  "syncMode",
  "additionalProperties",
  "secretArn",
  "type"
]
}

```

銷售力範本結構描述

您可以將包含資料來源結構描述的 JSON 納入為 [TemplateConfiguration](#) 物件的一部分。您可以在連線組態或存放庫端點詳細資料中提供 Salesforce 主機 URL。同時將資料來源類型指定為 SALESFORCEV2、驗證認證的密碼，以及其他必要的組態。然後，您將指定 TEMPLATE 為呼叫 Type 時 [CreateDataSource](#)。

您可以使用本開發人員指南中提供的模板。請參閱 [銷售部隊 JSON 結構描述](#)。

下表說明 JSON 結構描述的參數。

組態	描述
連線組態	資料來源端點的組態資訊。
repositoryEndpointMetadata	資料來源的端點資訊。

組態	描述
主機網址	要編製索引之 Salesforce 執行個體的 URL。
儲存庫組態 <ul style="list-style-type: none"> • 帳戶 • contact • 行銷活動 • 案例 • 產品 • 鉛 • contract • 合作夥伴 • profile • 想法 • 價格書 • 任務 • 解決方案 • attachment • 使用者 • 文件 • 知識文章 • 群組 • 機會 • 喋喋不休 • 習慣性 	資料來源內容的組態資訊。例如，配置特定類型的內容和欄位對應。 將 Salesforce 實體的屬性或欄位名稱對應至 Amazon Kendra 索引欄位名稱的物件清單。如需詳細資訊，請參閱 映射資料來源欄位 。

組態	描述
秘書	<p>AWS Secrets Manager 密碼的 Amazon 資源名稱 (ARN) , 其中包含連接到 Salesforce 所需的鍵值對。私密必須包含具有下列索引鍵的 JSON 結構 :</p> <pre data-bbox="829 443 1507 1276">{ "authenticationUrl": " <i>OAUTH endpoint that Amazon Kendra connects to get an OAUTH token</i>", "consumerKey": " <i>Application public key generated when you created your Salesforce application</i> ", "consumerSecret": " <i>Application private key generated when you created your Salesforce application</i> ", "password": " <i>Password associated with the user logging in to the Salesforce instance</i> ", "securityToken": " <i>Token associated with the user account logging in to the Salesforce instance</i> ", "username": " <i>User name of the user logging in to the Salesforce instance</i>" }</pre>
附加屬性	資料來源中內容的其他設定選項

組態	描述
<ul style="list-style-type: none">• 帳戶篩選• 聯絡篩選• 案例篩選• 行銷活動篩選• 合同過濾器• 群組篩選• 鉛過濾器• 產品篩選• 機會篩選• 合作夥伴篩• 價格書過濾• 思想過濾器• 設定檔篩選• 工作篩選• 方案過濾器• 使用者篩選• 聊天篩選• 文件篩選• knowledgeArticleFilter• 自定義	字串集合，指定要篩選哪些實體。

組態	描述
<p>包含模式</p> <ul style="list-style-type: none"> • inclusionDocumentFileTypePatterns • inclusionDocumentFileNamePatterns • inclusionAccountFileTypePatterns • inclusionCampaignFileTypePatterns • inclusionDocumentFileNamePatterns • inclusionCampaignFileNamePatterns • inclusionCaseFileTypePatterns • inclusionCaseFileNamePatterns • inclusionContactFileTypePatterns • inclusionContractFileNamePatterns • inclusionLeadFileTypePatterns • inclusionLeadFileNamePatterns • inclusionOpportunityFileTypePatterns • inclusionOpportunityFileNamePatterns • inclusionSolutionFileTypePatterns • inclusionSolutionFileNamePatterns • inclusionTaskFileTypePatterns • inclusionTaskFileNamePatterns • inclusionGroupFileTypePatterns • inclusionGroupFileNamePatterns • inclusionChatterFileTypePatterns • inclusionChatterFileNamePatterns • inclusionCustomEntityFileTypePatterns • inclusionCustomEntityFileNamePatterns 	<p>在 Salesforce 資料來源中包含特定檔案的規則運算式模式清單。符合模式的檔案會包括在索引中。不符合模式的檔案會從索引中排除。如果檔案同時符合包括模式和排除模式，則以排除模式為優先，且該項目不會包括在索引中。</p>

組態	描述
<p>排除模式</p> <ul style="list-style-type: none"> • exclusionDocumentFileTypePatterns • exclusionDocumentFileNamePatterns • exclusionAccountFileTypePatterns • exclusionCampaignFileTypePatterns • exclusionCampaignFileNamePatterns • exclusionCaseFileTypePatterns • exclusionCaseFileNamePatterns • exclusionContactFileTypePatterns • exclusionContractFileNamePatterns • exclusionLeadFileTypePatterns • exclusionLeadFileNamePatterns • exclusionOpportunityFileTypePatterns • exclusionOpportunityFileNamePatterns • exclusionSolutionFileTypePatterns • exclusionSolutionFileNamePatterns • exclusionTaskFileTypePatterns • exclusionTaskFileNamePatterns • exclusionGroupFileTypePatterns • exclusionGroupFileNamePatterns • exclusionChatterFileTypePatterns • exclusionChatterFileNamePatterns • exclusionCustomEntityFileTypePatterns • exclusionCustomEntityFileNamePatterns 	<p>用來排除 Salesforce 資料來源中某些檔案的規則運算式模式清單。符合模式的檔案會從索引中排除。與模式不匹配的文件包含在索引中。如果檔案同時符合排除和包含模式，則排除模式優先，且檔案不會包含在索引中。</p>

組態	描述
<ul style="list-style-type: none"> • isCrawlAccount • isCrawlContact • isCrawlCase • isCrawlCampaign • isCrawlProduct • isCrawlLead • isCrawlContract • isCrawlPartner • isCrawlProfile • isCrawlIdea • isCrawlPricebook • isCrawlDocument • crawlSharedDocument • isCrawlGroup • isCrawlOpportunity • isCrawlChatter • isCrawlUser • isCrawlSolution • isCrawlTask • isCrawlAccount附件 • isCrawlContact附件 • isCrawlCase附件 • isCrawlCampaign附件 • isCrawlLead附件 • isCrawlContract附件 • isCrawlGroup附件 • isCrawlOpportunity附件 • isCrawlChatter附件 • isCrawlSolution附件 	<p>true以在您的 Salesforce 帳戶中檢索這些類型的檔案。</p>

組態	描述
<ul style="list-style-type: none"> • isCrawlTask附件 • isCrawlCustomEntityAttachments • isCrawlKnowledge文章 <ul style="list-style-type: none"> • isCrawlDraft • isCrawlPublish • isCrawlArchived 	
type	資料來源的類型。指定SALESFORCEV2 為您的資料來源類型。
enableIdentityCrawler	true，以使用 Amazon Kendra的身分識別爬行者程式來同步使用者和群組的身分識別/主體資訊，以存取特定文件。如果關閉身分搜索器，則可以公開搜索所有文檔。如果您想要對文件使用存取控制，且身分識別編目程式已關閉，您也可以使用 PutPrincipalMapping API 來上傳使用者和群組存取資訊。
同步模式	<p>指定資料來源內容變更時 Amazon Kendra 應如何更新索引。您可以選擇：</p> <ul style="list-style-type: none"> • FORCED_FULL_CRAWL 新建索引所有內容，並在每次資料來源與索引同步時取代現有內容。 • FULL_CRAWL ，每次您的資料來源與索引同步時，僅對新的、修改和刪除的內容建立索引。Amazon Kendra 可以使用資料來源的機制來追蹤內容變更，並為上次同步後變更的內容建立索引。 • CHANGE_LOG 每次資料來源與索引同步時，僅對新內容和修改的內容建立索引。Amazon Kendra 可以使用資料來源的機制來追蹤內容變更，並為上次同步後變更的內容建立索引。
version	目前支援的此範本版本。

銷售部隊 JSON 結構描述

```
{
  "$schema": "http://json-schema.org/draft-04/schema#",
  "type": "object",
  "properties": {
    {
      "connectionConfiguration": {
        "type": "object",
        "properties": {
          {
            "repositoryEndpointMetadata": {
              {
                "type": "object",
                "properties": {
                  {
                    "hostUrl": {
                      {
                        "type": "string",
                        "pattern": "https:.*"
                      }
                    }
                  },
                  "required": [
                    "hostUrl"
                  ]
                }
              },
              "required": [
                "repositoryEndpointMetadata"
              ]
            },
            "repositoryConfigurations": {
              "type": "object",
              "properties": {
                {
                  "account": {
                    {
                      "type": "object",
                      "properties": {
                        {
                          "fieldMappings": {
                            {
```



```
    "type": "array",
    "items":
    [
      {
        "type": "object",
        "properties":
        {
          "indexFieldName":
          {
            "type": "string"
          },
          "indexFieldType":
          {
            "type": "string",
            "enum":
            [
              "STRING",
              "STRING_LIST",
              "DATE",
              "LONG"
            ]
          },
          "dataSourceFieldName":
          {
            "type": "string"
          },
          "dateFieldFormat":
          {
            "type": "string",
            "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
          }
        },
        "required":
        [
          "indexFieldName",
          "indexFieldType",
          "dataSourceFieldName"
        ]
      }
    ]
  },
  "required":
  [
```

```
    "fieldMappings"
  ]
},
"contact":
{
  "type": "object",
  "properties":
  {
    "fieldMappings":
    {
      "type": "array",
      "items":
      [
        {
          "type": "object",
          "properties":
          {
            "indexFieldName":
            {
              "type": "string"
            },
            "indexFieldType":
            {
              "type": "string",
              "enum":
              [
                "STRING",
                "STRING_LIST",
                "DATE"
              ]
            },
            "dataSourceFieldName":
            {
              "type": "string"
            },
            "dateFieldFormat":
            {
              "type": "string",
              "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
            }
          }
        },
        "required":
        [
          "indexFieldName",
```

```
        "indexFieldType",
        "dataSourceFieldName"
    ]
}
]
},
"required":
[
    "fieldMappings"
]
},
"campaign":
{
    "type": "object",
    "properties":
    {
        "fieldMappings":
        {
            "type": "array",
            "items":
            [
                {
                    "type": "object",
                    "properties":
                    {
                        "indexFieldName":
                        {
                            "type": "string"
                        },
                        "indexFieldType":
                        {
                            "type": "string",
                            "enum":
                            [
                                "STRING",
                                "STRING_LIST",
                                "DATE",
                                "LONG"
                            ]
                        }
                    },
                    "dataSourceFieldName":
                    {
                        "type": "string"
                    }
                }
            ]
        }
    }
}
```

```
    },
    "dateFieldFormat":
    {
      "type": "string",
      "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
    }
  },
  "required":
  [
    "indexFieldName",
    "indexFieldType",
    "dataSourceFieldName"
  ]
}
]
}
},
"required":
[
  "fieldMappings"
]
},
"case":
{
  "type": "object",
  "properties":
  {
    "fieldMappings":
    {
      "type": "array",
      "items":
      [
        {
          "type": "object",
          "properties":
          {
            "indexFieldName":
            {
              "type": "string"
            },
            "indexFieldType":
            {
              "type": "string",
              "enum":
```

```
        [
          "STRING",
          "STRING_LIST",
          "DATE"
        ]
      },
      "dataSourceFieldName":
      {
        "type": "string"
      },
      "dateFieldFormat":
      {
        "type": "string",
        "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
      }
    },
    "required":
    [
      "indexFieldName",
      "indexFieldType",
      "dataSourceFieldName"
    ]
  }
]
},
"required":
[
  "fieldMappings"
]
},
"product":
{
  "type": "object",
  "properties":
  {
    "fieldMappings":
    {
      "type": "array",
      "items":
      [
        {
          "type": "object",
          "properties":
```

```
        {
          "indexFieldName":
            {
              "type": "string"
            },
          "indexFieldType":
            {
              "type": "string",
              "enum":
                [
                  "STRING",
                  "STRING_LIST",
                  "DATE"
                ]
            },
          "dataSourceFieldName":
            {
              "type": "string"
            },
          "dateFieldFormat":
            {
              "type": "string",
              "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
            }
        },
        "required":
        [
          "indexFieldName",
          "indexFieldType",
          "dataSourceFieldName"
        ]
      }
    ]
  },
  "required":
  [
    "fieldMappings"
  ]
},
"lead":
{
  "type": "object",
  "properties":
```

```
{
  "fieldMappings":
  {
    "type": "array",
    "items":
    [
      {
        "type": "object",
        "properties":
        {
          "indexFieldName":
          {
            "type": "string"
          },
          "indexFieldType":
          {
            "type": "string",
            "enum":
            [
              "STRING",
              "STRING_LIST",
              "DATE",
              "LONG"
            ]
          },
          "dataSourceFieldName":
          {
            "type": "string"
          },
          "dateFieldFormat":
          {
            "type": "string",
            "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
          }
        },
        "required":
        [
          "indexFieldName",
          "indexFieldType",
          "dataSourceFieldName"
        ]
      }
    ]
  }
}
```

```
    },
    "required":
    [
      "fieldMappings"
    ]
  },
  "contract":
  {
    "type": "object",
    "properties":
    {
      "fieldMappings":
      {
        "type": "array",
        "items":
        [
          {
            "type": "object",
            "properties":
            {
              "indexFieldName":
              {
                "type": "string"
              },
              "indexFieldType":
              {
                "type": "string",
                "enum":
                [
                  "STRING",
                  "STRING_LIST",
                  "DATE"
                ]
              },
              "dataSourceFieldName":
              {
                "type": "string"
              },
              "dateFieldFormat":
              {
                "type": "string",
                "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
              }
            }
          }
        ]
      }
    }
  },
```



```
        "required":
        [
            "indexFieldName",
            "indexFieldType",
            "dataSourceFieldName"
        ]
    }
]
},
"required":
[
    "fieldMappings"
]
},
"partner":
{
    "type": "object",
    "properties":
    {
        "fieldMappings":
        {
            "type": "array",
            "items":
            [
                {
                    "type": "object",
                    "properties":
                    {
                        "indexFieldName":
                        {
                            "type": "string"
                        },
                        "indexFieldType":
                        {
                            "type": "string",
                            "enum":
                            [
                                "STRING",
                                "STRING_LIST",
                                "DATE"
                            ]
                        },
                    },
                }
            ],
        },
        "dataSourceFieldName":
```

```
        {
          "type": "string"
        },
        "dateFieldFormat":
        {
          "type": "string",
          "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
        }
      },
      "required":
      [
        "indexFieldName",
        "indexFieldType",
        "dataSourceFieldName"
      ]
    ]
  }
},
"required":
[
  "fieldMappings"
]
},
"profile":
{
  "type": "object",
  "properties":
  {
    "fieldMappings":
    {
      "type": "array",
      "items":
      [
        {
          "type": "object",
          "properties":
          {
            "indexFieldName":
            {
              "type": "string"
            },
            "indexFieldType":
            {
```

```
        "type": "string",
        "enum":
        [
            "STRING",
            "STRING_LIST",
            "DATE"
        ]
    },
    "dataSourceFieldName":
    {
        "type": "string"
    },
    "dateFieldFormat":
    {
        "type": "string",
        "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
    }
},
"required":
[
    "indexFieldName",
    "indexFieldType",
    "dataSourceFieldName"
]
}
]
}
},
"required":
[
    "fieldMappings"
]
},
"idea":
{
    "type": "object",
    "properties":
    {
        "fieldMappings":
        {
            "type": "array",
            "items":
            [
                {
```

```
    "type": "object",
    "properties":
    {
      "indexFieldName":
      {
        "type": "string"
      },
      "indexFieldType":
      {
        "type": "string",
        "enum":
        [
          "STRING",
          "STRING_LIST",
          "DATE",
          "LONG"
        ]
      },
      "dataSourceFieldName":
      {
        "type": "string"
      },
      "dateFieldFormat":
      {
        "type": "string",
        "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
      }
    },
    "required":
    [
      "indexFieldName",
      "indexFieldType",
      "dataSourceFieldName"
    ]
  }
]
},
"required":
[
  "fieldMappings"
]
},
"pricebook":
```

```
{
  "type": "object",
  "properties": {
    {
      "fieldMappings": {
        {
          "type": "array",
          "items": [
            {
              "type": "object",
              "properties": {
                {
                  "indexFieldName": {
                    "type": "string"
                  },
                  "indexFieldType": {
                    "type": "string",
                    "enum": [
                      "STRING",
                      "STRING_LIST",
                      "DATE"
                    ]
                  },
                  "dataSourceFieldName": {
                    "type": "string"
                  },
                  "dateFieldFormat": {
                    "type": "string",
                    "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                  }
                },
                "required": [
                  "indexFieldName",
                  "indexFieldType",
                  "dataSourceFieldName"
                ]
              }
            }
          ]
        }
      }
    }
  }
}
```

```
    ]
  }
},
"required":
[
  "fieldMappings"
]
},
"task":
{
  "type": "object",
  "properties":
  {
    "fieldMappings":
    {
      "type": "array",
      "items":
      [
        {
          "type": "object",
          "properties":
          {
            "indexFieldName":
            {
              "type": "string"
            },
            "indexFieldType":
            {
              "type": "string",
              "enum":
              [
                "STRING",
                "STRING_LIST",
                "DATE"
              ]
            },
            "dataSourceFieldName":
            {
              "type": "string"
            },
            "dateFieldFormat":
            {
              "type": "string",
              "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
            }
          }
        }
      ]
    }
  }
}
```

```
        }
      },
      "required":
      [
        "indexFieldName",
        "indexFieldType",
        "dataSourceFieldName"
      ]
    }
  ]
}
},
"required":
[
  "fieldMappings"
],
"solution":
{
  "type": "object",
  "properties":
  {
    "fieldMappings":
    {
      "type": "array",
      "items":
      [
        {
          "type": "object",
          "properties":
          {
            "indexFieldName":
            {
              "type": "string"
            },
            "indexFieldType":
            {
              "type": "string",
              "enum":
              [
                "STRING",
                "STRING_LIST",
                "DATE"
              ]
            }
          }
        }
      ]
    }
  }
}
```

```
    },
    "dataSourceFieldName":
    {
      "type": "string"
    },
    "dateFieldFormat":
    {
      "type": "string",
      "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
    }
  },
  "required":
  [
    "indexFieldName",
    "indexFieldType",
    "dataSourceFieldName"
  ]
}
]
}
},
"required":
[
  "fieldMappings"
]
},
"attachment":
{
  "type": "object",
  "properties":
  {
    "fieldMappings":
    {
      "type": "array",
      "items":
      [
        {
          "type": "object",
          "properties":
          {
            "indexFieldName":
            {
              "type": "string"
            },

```



```
        "indexFieldType":
        {
            "type": "string",
            "enum":
            [
                "STRING",
                "STRING_LIST",
                "DATE",
                "LONG"
            ]
        },
        "dataSourceFieldName":
        {
            "type": "string"
        },
        "dateFieldFormat":
        {
            "type": "string",
            "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
        }
    },
    "required":
    [
        "indexFieldName",
        "indexFieldType",
        "dataSourceFieldName"
    ]
}
]
}
},
"required":
[
    "fieldMappings"
]
},
"user":
{
    "type": "object",
    "properties":
    {
        "fieldMappings":
        {
            "type": "array",
```

```
    "items":
      [
        {
          "type": "object",
          "properties":
            {
              "indexFieldName":
                {
                  "type": "string"
                },
              "indexFieldType":
                {
                  "type": "string",
                  "enum":
                    [
                      "STRING",
                      "STRING_LIST",
                      "DATE"
                    ]
                },
              "dataSourceFieldName":
                {
                  "type": "string"
                },
              "dateFieldFormat":
                {
                  "type": "string",
                  "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                }
            },
          "required":
            [
              "indexFieldName",
              "indexFieldType",
              "dataSourceFieldName"
            ]
        }
      ]
    },
    "required":
      [
        "fieldMappings"
      ]
  ]
```

```
},
"document":
{
  "type": "object",
  "properties":
  {
    "fieldMappings":
    {
      "type": "array",
      "items":
      [
        {
          "type": "object",
          "properties":
          {
            "indexFieldName":
            {
              "type": "string"
            },
            "indexFieldType":
            {
              "type": "string",
              "enum":
              [
                "STRING",
                "STRING_LIST",
                "DATE",
                "LONG"
              ]
            },
            "dataSourceFieldName":
            {
              "type": "string"
            },
            "dateFieldFormat":
            {
              "type": "string",
              "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
            }
          }
        },
        "required":
        [
          "indexFieldName",
          "indexFieldType",
```

```
        "dataSourceFieldName"
      ]
    }
  ]
}
},
"required":
[
  "fieldMappings"
]
},
"knowledgeArticles":
{
  "type": "object",
  "properties":
  {
    "fieldMappings":
    {
      "type": "array",
      "items":
      [
        {
          "type": "object",
          "properties":
          {
            "indexFieldName":
            {
              "type": "string"
            },
            "indexFieldType":
            {
              "type": "string",
              "enum":
              [
                "STRING",
                "STRING_LIST",
                "DATE"
              ]
            },
            "dataSourceFieldName":
            {
              "type": "string"
            },
            "dateFieldFormat":
```

```
        {
          "type": "string",
          "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
        }
      ],
      "required":
      [
        "indexFieldName",
        "indexFieldType",
        "dataSourceFieldName"
      ]
    }
  ],
  },
  "required":
  [
    "fieldMappings"
  ]
},
"group":
{
  "type": "object",
  "properties":
  {
    "fieldMappings":
    {
      "type": "array",
      "items":
      [
        {
          "type": "object",
          "properties":
          {
            "indexFieldName":
            {
              "type": "string"
            },
            "indexFieldType":
            {
              "type": "string",
              "enum":
              [
                "STRING",
```

```
        "STRING_LIST",
        "DATE"
    ]
},
"dataSourceFieldName":
{
    "type": "string"
},
"dateFieldFormat":
{
    "type": "string",
    "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
}
},
"required":
[
    "indexFieldName",
    "indexFieldType",
    "dataSourceFieldName"
]
}
]
}
},
"required":
[
    "fieldMappings"
]
},
"opportunity":
{
    "type": "object",
    "properties":
    {
        "fieldMappings":
        {
            "type": "array",
            "items":
            [
                {
                    "type": "object",
                    "properties":
                    {
                        "indexFieldName":
```

```
        {
          "type": "string"
        },
        "indexFieldType":
        {
          "type": "string",
          "enum":
          [
            "STRING",
            "STRING_LIST",
            "DATE",
            "LONG"
          ]
        },
        "dataSourceFieldName":
        {
          "type": "string"
        },
        "dateFieldFormat":
        {
          "type": "string",
          "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
        }
      },
      "required":
      [
        "indexFieldName",
        "indexFieldType",
        "dataSourceFieldName"
      ]
    }
  ]
},
"required":
[
  "fieldMappings"
]
},
"chatter":
{
  "type": "object",
  "properties":
  {
```

```
"fieldMappings":
{
  "type": "array",
  "items":
  [
    {
      "type": "object",
      "properties":
      {
        "indexFieldName":
        {
          "type": "string"
        },
        "indexFieldType":
        {
          "type": "string",
          "enum":
          [
            "STRING",
            "STRING_LIST",
            "DATE"
          ]
        },
        "dataSourceFieldName":
        {
          "type": "string"
        },
        "dateFieldFormat":
        {
          "type": "string",
          "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
        }
      },
      "required":
      [
        "indexFieldName",
        "indexFieldType",
        "dataSourceFieldName"
      ]
    }
  ]
},
"required":
```



```
[
  "fieldMappings"
],
"customEntity":
{
  "type": "object",
  "properties":
  {
    "fieldMappings":
    {
      "type": "array",
      "items":
      [
        {
          "type": "object",
          "properties":
          {
            "indexFieldName":
            {
              "type": "string"
            },
            "indexFieldType":
            {
              "type": "string",
              "enum":
              [
                "STRING",
                "STRING_LIST",
                "DATE"
              ]
            },
            "dataSourceFieldName":
            {
              "type": "string"
            },
            "dateFieldFormat":
            {
              "type": "string",
              "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
            }
          },
          "required":
          [
```

```
        "indexFieldName",
        "indexFieldType",
        "dataSourceFieldName"
    ]
    }
    ]
}
},
"required":
[
    "fieldMappings"
]
}
},
"additionalProperties": {
    "type": "object",
    "properties":
    {
        "accountFilter":{
            "type": "array",
            "items":
            {
                "type": "string"
            }
        },
        "contactFilter":{
            "type": "array",
            "items":
            {
                "type": "string"
            }
        },
        "caseFilter":{
            "type": "array",
            "items":
            {
                "type": "string"
            }
        },
        "campaignFilter":{
            "type": "array",
            "items":
            {
```

```
    "type": "string"
  }
},
"contractFilter":{
  "type": "array",
  "items":
  {
    "type": "string"
  }
},
"groupFilter":{
  "type": "array",
  "items":
  {
    "type": "string"
  }
},
"leadFilter":{
  "type": "array",
  "items":
  {
    "type": "string"
  }
},
"productFilter":{
  "type": "array",
  "items":
  {
    "type": "string"
  }
},
"opportunityFilter":{
  "type": "array",
  "items":
  {
    "type": "string"
  }
},
"partnerFilter":{
  "type": "array",
  "items":
  {
    "type": "string"
  }
}
```

```
    },
    "pricebookFilter":{
      "type": "array",
      "items":
        {
          "type": "string"
        }
    },
    "ideaFilter":{
      "type": "array",
      "items":
        {
          "type": "string"
        }
    },
    "profileFilter":{
      "type": "array",
      "items":
        {
          "type": "string"
        }
    },
    "taskFilter":{
      "type": "array",
      "items":
        {
          "type": "string"
        }
    },
    "solutionFilter":{
      "type": "array",
      "items":
        {
          "type": "string"
        }
    },
    "userFilter":{
      "type": "array",
      "items":
        {
          "type": "string"
        }
    },
    "chatterFilter":{
```

```
    "type": "array",
    "items":
    {
      "type": "string"
    }
  },
  "documentFilter":{
    "type": "array",
    "items":
    {
      "type": "string"
    }
  },
  "knowledgeArticleFilter":{
    "type": "array",
    "items":
    {
      "type": "string"
    }
  },
  "customEntities":{
    "type": "array",
    "items":
    {
      "type": "string"
    }
  },
  "isCrawlAccount": {
    "type": "boolean"
  },
  "isCrawlContact": {
    "type": "boolean"
  },
  "isCrawlCase": {
    "type": "boolean"
  },
  "isCrawlCampaign": {
    "type": "boolean"
  },
  "isCrawlProduct": {
    "type": "boolean"
  },
  "isCrawlLead": {
    "type": "boolean"
  }
```

```
    },
    "isCrawlContract": {
      "type": "boolean"
    },
    "isCrawlPartner": {
      "type": "boolean"
    },
    "isCrawlProfile": {
      "type": "boolean"
    },
    "isCrawlIdea": {
      "type": "boolean"
    },
    "isCrawlPricebook": {
      "type": "boolean"
    },
    "isCrawlDocument": {
      "type": "boolean"
    },
    "crawlSharedDocument": {
      "type": "boolean"
    },
    "isCrawlGroup": {
      "type": "boolean"
    },
    "isCrawlOpportunity": {
      "type": "boolean"
    },
    "isCrawlChatter": {
      "type": "boolean"
    },
    "isCrawlUser": {
      "type": "boolean"
    },
    "isCrawlSolution": {
      "type": "boolean"
    },
    "isCrawlTask": {
      "type": "boolean"
    },
    "isCrawlAccountAttachments": {
      "type": "boolean"
    },
  },
```

```
"isCrawlContactAttachments": {
  "type": "boolean"
},
"isCrawlCaseAttachments": {
  "type": "boolean"
},
"isCrawlCampaignAttachments": {
  "type": "boolean"
},
"isCrawlLeadAttachments": {
  "type": "boolean"
},
"isCrawlContractAttachments": {
  "type": "boolean"
},
"isCrawlGroupAttachments": {
  "type": "boolean"
},
"isCrawlOpportunityAttachments": {
  "type": "boolean"
},
"isCrawlChatterAttachments": {
  "type": "boolean"
},
"isCrawlSolutionAttachments":{
  "type": "boolean"
},
"isCrawlTaskAttachments":{
  "type": "boolean"
},
"isCrawlCustomEntityAttachments":{
  "type": "boolean"
},
"isCrawlKnowledgeArticles": {
  "type": "object",
  "properties":
  {
    "isCrawlDraft": {
      "type": "boolean"
    },
    "isCrawlPublish": {
      "type": "boolean"
    },
    "isCrawlArchived": {
```

```
        "type": "boolean"
      }
    }
  },
  "inclusionDocumentFileTypePatterns": {
    "type": "array",
    "items": {
      "type": "string"
    }
  },
  "exclusionDocumentFileTypePatterns": {
    "type": "array",
    "items": {
      "type": "string"
    }
  },
  "inclusionDocumentFileNamePatterns": {
    "type": "array",
    "items": {
      "type": "string"
    }
  },
  "exclusionDocumentFileNamePatterns": {
    "type": "array",
    "items": {
      "type": "string"
    }
  },
  "inclusionAccountFileTypePatterns": {
    "type": "array",
    "items": {
      "type": "string"
    }
  },
  "exclusionAccountFileTypePatterns": {
    "type": "array",
    "items": {
      "type": "string"
    }
  }
}
```



```
    }
  },
  "inclusionAccountFileNamePatterns":{
    "type": "array",
    "items":
    {
      "type": "string"
    }
  },
  "exclusionAccountFileNamePatterns":{
    "type": "array",
    "items":
    {
      "type": "string"
    }
  },
  "inclusionCampaignFileTypePatterns": {
    "type": "array",
    "items":
    {
      "type": "string"
    }
  },
  "exclusionCampaignFileTypePatterns": {
    "type": "array",
    "items":
    {
      "type": "string"
    }
  },
  "inclusionCampaignFileNamePatterns":{
    "type": "array",
    "items":
    {
      "type": "string"
    }
  },
  "exclusionCampaignFileNamePatterns":{
    "type": "array",
    "items":
    {
      "type": "string"
    }
  },
},
```

```
"inclusionCaseFileTypePatterns":{
  "type": "array",
  "items":
  {
    "type": "string"
  }
},
"exclusionCaseFileTypePatterns":{
  "type": "array",
  "items":
  {
    "type": "string"
  }
},
"inclusionCaseFileNamePatterns":{
  "type": "array",
  "items":
  {
    "type": "string"
  }
},
"exclusionCaseFileNamePatterns":{
  "type": "array",
  "items":
  {
    "type": "string"
  }
},
"inclusionContactFileTypePatterns":{
  "type": "array",
  "items":
  {
    "type": "string"
  }
},
"exclusionContactFileTypePatterns":{
  "type": "array",
  "items":
  {
    "type": "string"
  }
},
"inclusionContactFileNamePatterns":{
  "type": "array",
```

```
    "items":
      {
        "type": "string"
      }
  },
  "exclusionContactFileNamePatterns":{
    "type": "array",
    "items":
      {
        "type": "string"
      }
  },
  "inclusionContractFileTypePatterns":{
    "type": "array",
    "items":
      {
        "type": "string"
      }
  },
  "exclusionContractFileTypePatterns":{
    "type": "array",
    "items":
      {
        "type": "string"
      }
  },
  "inclusionContractFileNamePatterns":{
    "type": "array",
    "items":
      {
        "type": "string"
      }
  },
  "exclusionContractFileNamePatterns":{
    "type": "array",
    "items":
      {
        "type": "string"
      }
  },
  "inclusionLeadFileTypePatterns":{
    "type": "array",
    "items":
      {
```

```
    "type": "string"
  }
},
"exclusionLeadFileTypePatterns":{
  "type": "array",
  "items":
  {
    "type": "string"
  }
},
"inclusionLeadFileNamePatterns":{
  "type": "array",
  "items":
  {
    "type": "string"
  }
},
"exclusionLeadFileNamePatterns":{
  "type": "array",
  "items":
  {
    "type": "string"
  }
},
"inclusionOpportunityFileTypePatterns":{
  "type": "array",
  "items":
  {
    "type": "string"
  }
},
"exclusionOpportunityFileTypePatterns":{
  "type": "array",
  "items":
  {
    "type": "string"
  }
},
"inclusionOpportunityFileNamePatterns":{
  "type": "array",
  "items":
  {
    "type": "string"
  }
}
```

```
    },
    "exclusionOpportunityFileNamePatterns":{
      "type": "array",
      "items":
      {
        "type": "string"
      }
    },
    "inclusionSolutionFileTypePatterns":{
      "type": "array",
      "items":
      {
        "type": "string"
      }
    },
    "exclusionSolutionFileTypePatterns":{
      "type": "array",
      "items":
      {
        "type": "string"
      }
    },
    "inclusionSolutionFileNamePatterns":{
      "type": "array",
      "items":
      {
        "type": "string"
      }
    },
    "exclusionSolutionFileNamePatterns":{
      "type": "array",
      "items":
      {
        "type": "string"
      }
    },
    "inclusionTaskFileTypePatterns":{
      "type": "array",
      "items":
      {
        "type": "string"
      }
    },
    "exclusionTaskFileTypePatterns":{
```

```
    "type": "array",
    "items":
      {
        "type": "string"
      }
  },
  "inclusionTaskFileNamePatterns":{
    "type": "array",
    "items":
      {
        "type": "string"
      }
  },
  "exclusionTaskFileNamePatterns":{
    "type": "array",
    "items":
      {
        "type": "string"
      }
  },
  "inclusionGroupFileTypePatterns":{
    "type": "array",
    "items":
      {
        "type": "string"
      }
  },
  "exclusionGroupFileTypePatterns":{
    "type": "array",
    "items":
      {
        "type": "string"
      }
  },
  "inclusionGroupFileNamePatterns":{
    "type": "array",
    "items":
      {
        "type": "string"
      }
  },
  "exclusionGroupFileNamePatterns":{
    "type": "array",
    "items":
```

```
    {
      "type": "string"
    }
  },
  "inclusionChatterFileTypePatterns":{
    "type": "array",
    "items":
    {
      "type": "string"
    }
  },
  "exclusionChatterFileTypePatterns":{
    "type": "array",
    "items":
    {
      "type": "string"
    }
  },
  "inclusionChatterFileNamePatterns":{
    "type": "array",
    "items":
    {
      "type": "string"
    }
  },
  "exclusionChatterFileNamePatterns":{
    "type": "array",
    "items":
    {
      "type": "string"
    }
  },
  "inclusionCustomEntityTypePatterns":{
    "type": "array",
    "items":
    {
      "type": "string"
    }
  },
  "exclusionCustomEntityTypePatterns":{
    "type": "array",
    "items":
    {
      "type": "string"
    }
  }
}
```

```
    }
  },
  "inclusionCustomEntityFileNamePatterns":{
    "type": "array",
    "items":
    {
      "type": "string"
    }
  },
  "exclusionCustomEntityFileNamePatterns":{
    "type": "array",
    "items":
    {
      "type": "string"
    }
  }
},
"required":
[]
},
"enableIdentityCrawler": {
  "type": "boolean"
},
"type": {
  "type": "string",
  "pattern": "SALESFORCEV2"
},
"syncMode": {
  "type": "string",
  "enum": [
    "FULL_CRAWL",
    "FORCED_FULL_CRAWL",
    "CHANGE_LOG"
  ]
},
"secretArn": {
  "type": "string",
  "minLength": 20,
  "maxLength": 2048
}
},
"version": {
  "type": "string",
  "anyOf": [
```



```

    {
      "pattern": "1.0.0"
    }
  ],
  "required": [
    "connectionConfiguration",
    "repositoryConfigurations",
    "syncMode",
    "additionalProperties",
    "secretArn",
    "type"
  ]
}

```

ServiceNow 模板架構

您可以將包含資料來源結構描述的 JSON 納入為 [TemplateConfiguration](#) 物件的一部分。您可以提供 ServiceNow 主機 URL、驗證類型和執行個體版本，做為連線組態或存放庫端點詳細資料的一部分。同時將資料來源類型指定為 `SERVICENOWV2`、驗證認證的密碼，以及其他必要的組態。然後，您將指定 `TEMPLATE` 為呼叫 Type 時 [CreateDataSource](#)。

您可以使用本開發人員指南中提供的模板。請參閱 [ServiceNow 結構定義](#)。

下表說明 ServiceNow JSON 結構定義的參數。

組態	描述
連線組態	資料來源端點的組態資訊。
repositoryEndpointMetadata	資料來源的端點資訊。
主机网址	ServiceNow 主持人網址。例如， <code>###.####.com</code> 。
authType	您使用的驗證類型，無論是 <code>basicAuth</code> 或 <code>OAuth2</code> 。
servicenowInstanceVersion	您使用的 ServiceNow 版本。您可以選擇 <code>Tokyo</code> 、 <code>Sandiego</code> 、 <code>Rome</code> 、和 <code>Others</code> 。
儲存庫組態	資料來源內容的組態資訊。例如，配置特定類型的內容和欄位對應。

組態	描述
<ul style="list-style-type: none"> • 知識文章 • attachment • 服務目錄 • 事件 	<p>將 ServiceNow 知識文章、附件、服務目錄和事件的屬性或欄位名稱對應至 Amazon Kendra 索引欄位名稱的物件清單。如需詳細資訊，請參閱映射資料來源欄位。資料來源欄位名稱必須存在於您的 ServiceNow 自訂中繼資料中。</p>
其他屬性	資料來源中內容的其他組態選項。
maxFileSizeInMegaBytes	<p>指定 Amazon Kendra 將抓取的檔案大小限制 (以 MB 為單位)。Amazon Kendra 只會抓取您定義的大小限制內的檔案。預設檔案大小為 50MB。檔案大小上限應該大於 0MB 且小於或等於 50MB。</p>
<ul style="list-style-type: none"> • knowledgeArticleFilter • incidentQueryFilter • serviceCatalogQuery過濾器 • knowledgeArticleTitleRegExp • serviceCatalogTitleRegExp • incidentTitleReg經驗值 • inclusionFileType模式 • exclusionFileType模式 • inclusionFileName模式 • exclusionFileName模式 • incidentStateType 	<p>要包含和/或排除 ServiceNow 資料來源中某些檔案的規則運算式模式清單。符合模式的檔案會包括在索引中。不符合模式的檔案會從索引中排除。如果檔案同時符合包括模式和排除模式，則以排除模式為優先，且該項目不會包括在索引中。</p>

組態	描述
<ul style="list-style-type: none"> • isCrawlKnowledge文章 • isCrawlKnowledgeArticleAttachment • includePublicArticles只有 • isCrawlService目錄 • isCrawlServiceCatalogAttachment • isCrawlActiveServiceCatalog • isCrawlInactiveServiceCatalog • isCrawlIncident • isCrawlIncident附件 • isCrawlActive事件 • isCrawlInactive事件 • 應用氯化鈉 ForKnowledgeArticle • 應用氯化鈉 ForServiceCatalog • 應用氯化鈉 ForIncident 	<p>true編目 ServiceNow 知識文章、服務目錄、事件和附件。</p>
type	<p>資料來源的類型。指定SERVICENOWV2 為您的資料來源類型。</p>
enableIdentityCrawler	<p>true，以使用 Amazon Kendra的身分識別爬行者程式來同步使用者和群組的身分識別/主體資訊，以存取特定文件。如果關閉身分搜索器，則可以公開搜索所有文檔。如果您想要對文件使用存取控制，且身分識別編目程式已關閉，您也可以使用 PutPrincipalMapping API 來上傳使用者和群組存取資訊。</p>

組態	描述
同步模式	<p>指定資料來源內容變更時 Amazon Kendra 應如何更新索引。您可以選擇：</p> <ul style="list-style-type: none"> • <code>FORCED_FULL_CRAWL</code> 新建索引所有內容，並在每次資料來源與索引同步時取代現有內容。 • <code>FULL_CRAWL</code>，每次您的資料來源與索引同步時，僅對新的、修改和刪除的內容建立索引。Amazon Kendra 可以使用資料來源的機制來追蹤內容變更，並為上次同步後變更的內容建立索引。
秘書	<p>Amazon 資源名稱 (ARN) 的 AWS Secrets Manager 秘密，其中包含連接到 ServiceNow 私密必須包含具有下列索引鍵的 JSON 結構：</p> <pre data-bbox="703 850 1507 1050"> { "username": " <i>user name</i>", "password": " <i>password</i>" } </pre> <p>如果您使用 OAuth2 驗證，您的密鑰必須包含具有以下鍵的 JSON 結構：</p> <pre data-bbox="703 1199 1507 1480"> { "username": " <i>user name</i>", "password": " <i>password</i>", "clientId": " <i>client id</i>", "clientSecret": " <i>client secret</i>" } </pre>
version	目前支援的範本版本。

ServiceNow 結構定義

```

{
  "$schema": "http://json-schema.org/draft-04/schema#",
  "type": "object",

```

```
"properties": {
  "connectionConfiguration": {
    "type": "object",
    "properties": {
      "repositoryEndpointMetadata": {
        "type": "object",
        "properties": {
          "hostUrl": {
            "type": "string",
            "pattern": "^(?!^(https?|ftp|file):\\|\\/))([a-z0-9-]+(.service-
now.com|.servicenowservices.com))$",
            "minLength": 1,
            "maxLength": 2048
          },
          "authType": {
            "type": "string",
            "enum": [
              "basicAuth",
              "OAuth2"
            ]
          },
          "servicenowInstanceVersion": {
            "type": "string",
            "enum": [
              "Tokyo",
              "SanDiego",
              "Rome",
              "Others"
            ]
          }
        }
      },
      "required": [
        "hostUrl",
        "authType",
        "servicenowInstanceVersion"
      ]
    }
  },
  "required": [
    "repositoryEndpointMetadata"
  ]
},
"repositoryConfigurations": {
  "type": "object",
```

```
"properties": {
  "knowledgeArticle": {
    "type": "object",
    "properties": {
      "fieldMappings": {
        "type": "array",
        "items": [
          {
            "type": "object",
            "properties": {
              "indexFieldName": {
                "type": "string"
              },
              "indexFieldType": {
                "type": "string",
                "enum": [
                  "STRING",
                  "DATE",
                  "STRING_LIST"
                ]
              },
              "dataSourceFieldName": {
                "type": "string"
              },
              "dateFieldFormat": {
                "type": "string",
                "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
              }
            },
            "required": [
              "indexFieldName",
              "indexFieldType",
              "dataSourceFieldName"
            ]
          }
        ]
      },
      "required": [
        "fieldMappings"
      ]
    },
    "attachment": {
      "type": "object",
```

```
"properties": {
  "fieldMappings": {
    "type": "array",
    "items": [
      {
        "type": "object",
        "properties": {
          "indexFieldName": {
            "type": "string"
          },
          "indexFieldType": {
            "type": "string",
            "enum": [
              "STRING",
              "LONG",
              "DATE",
              "STRING_LIST"
            ]
          },
          "dataSourceFieldName": {
            "type": "string"
          },
          "dateFieldFormat": {
            "type": "string",
            "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
          }
        },
        "required": [
          "indexFieldName",
          "indexFieldType",
          "dataSourceFieldName"
        ]
      }
    ]
  },
  "required": [
    "fieldMappings"
  ]
},
"serviceCatalog": {
  "type": "object",
  "properties": {
    "fieldMappings": {
```

```
    "type": "array",
    "items": [
      {
        "type": "object",
        "properties": {
          "indexFieldName": {
            "type": "string"
          },
          "indexFieldType": {
            "type": "string",
            "enum": [
              "STRING",
              "DATE",
              "STRING_LIST"
            ]
          },
          "dataSourceFieldName": {
            "type": "string"
          },
          "dateFieldFormat": {
            "type": "string",
            "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
          }
        },
        "required": [
          "indexFieldName",
          "indexFieldType",
          "dataSourceFieldName"
        ]
      }
    ]
  },
  "required": [
    "fieldMappings"
  ],
  "incident": {
    "type": "object",
    "properties": {
      "fieldMappings": {
        "type": "array",
        "items": [
          {
```



```
    "type": "object",
    "properties": {
      "indexFieldName": {
        "type": "string"
      },
      "indexFieldType": {
        "type": "string",
        "enum": [
          "STRING",
          "DATE",
          "STRING_LIST"
        ]
      },
      "dataSourceFieldName": {
        "type": "string"
      },
      "dateFieldFormat": {
        "type": "string",
        "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
      }
    },
    "required": [
      "indexFieldName",
      "indexFieldType",
      "dataSourceFieldName"
    ]
  }
],
"required": [
  "fieldMappings"
]
}
},
"additionalProperties": {
  "type": "object",
  "properties": {
    "maxFileSizeInMegaBytes": {
      "type": "string"
    },
    "isCrawlKnowledgeArticle": {
      "type": "boolean"
    }
  }
}
```

```
    },
    "isCrawlKnowledgeArticleAttachment": {
      "type": "boolean"
    },
    "includePublicArticlesOnly": {
      "type": "boolean"
    },
    "knowledgeArticleFilter": {
      "type": "string"
    },
    "incidentQueryFilter": {
      "type": "string"
    },
    "serviceCatalogQueryFilter": {
      "type": "string"
    },
    "isCrawlServiceCatalog": {
      "type": "boolean"
    },
    "isCrawlServiceCatalogAttachment": {
      "type": "boolean"
    },
    "isCrawlActiveServiceCatalog": {
      "type": "boolean"
    },
    "isCrawlInactiveServiceCatalog": {
      "type": "boolean"
    },
    "isCrawlIncident": {
      "type": "boolean"
    },
    "isCrawlIncidentAttachment": {
      "type": "boolean"
    },
    "isCrawlActiveIncident": {
      "type": "boolean"
    },
    "isCrawlInactiveIncident": {
      "type": "boolean"
    },
    "applyACLForKnowledgeArticle": {
      "type": "boolean"
    },
    "applyACLForServiceCatalog": {
```

```
    "type": "boolean"
  },
  "applyACLForIncident": {
    "type": "boolean"
  },
  "incidentStateType": {
    "type": "array",
    "items": {
      "type": "string",
      "enum": [
        "Open",
        "Open - Unassigned",
        "Resolved",
        "All"
      ]
    }
  },
  "knowledgeArticleTitleRegExp": {
    "type": "string"
  },
  "serviceCatalogTitleRegExp": {
    "type": "string"
  },
  "incidentTitleRegExp": {
    "type": "string"
  },
  "inclusionFileTypePatterns": {
    "type": "array",
    "items": {
      "type": "string"
    }
  },
  "exclusionFileTypePatterns": {
    "type": "array",
    "items": {
      "type": "string"
    }
  },
  "inclusionFileNamePatterns": {
    "type": "array",
    "items": {
      "type": "string"
    }
  },
},
```

```
    "exclusionFileNamePatterns": {
      "type": "array",
      "items": {
        "type": "string"
      }
    },
    "required": []
  },
  "type": {
    "type": "string",
    "pattern": "SERVICENOWV2"
  },
  "enableIdentityCrawler": {
    "type": "boolean"
  },
  "syncMode": {
    "type": "string",
    "enum": [
      "FORCED_FULL_CRAWL",
      "FULL_CRAWL"
    ]
  },
  "secretArn": {
    "type": "string",
    "minLength": 20,
    "maxLength": 2048
  }
},
"version": {
  "type": "string",
  "anyOf": [
    {
      "pattern": "1.0.0"
    }
  ]
},
"required": [
  "connectionConfiguration",
  "repositoryConfigurations",
  "syncMode",
  "additionalProperties",
  "secretArn",
  "type"
```

```
]
}
```

鬆弛模板架構

您可以將包含資料來源結構描述的 JSON 納入為 [TemplateConfiguration](#) 物件的一部分。您可以提供主機 URL 做為連線組態或存放庫端點詳細資料的一部分。同時將資料來源類型指定為 SLACK、驗證認證的密碼，以及其他必要的組態。然後，您將指定 TEMPLATE 為呼叫 Type 時 [CreateDataSource](#)。

您可以使用本開發人員指南中提供的模板。請參閱 [鬆弛結構定義](#)。

下表說明 Slack JSON 結構定義的參數。

組態	描述
連線組態	資料來源端點的組態資訊。
repositoryEndpointMetadata	資料來源的端點資訊。
團隊 ID	您從 Slack 主頁網址複製的 Slack 團隊 ID。
儲存庫組態	資料來源內容的組態資訊。例如，配置特定類型的內容和欄位對應。
全部	將 Slack 內容的屬性或欄位名稱對應至 Amazon Kendra 索引欄位名稱的物件清單。
附加屬性	資料來源中內容的其他組態選項。
包含模式	在 Slack 資料來源中包含特定內容的規則運算式模式清單。符合模式的內容會包含在索引中。與模式不匹配的內容會從索引中排除。如果有任何內容同時符合包含和排除模式，則排除模式優先，且內容不會包含在索引中。
排除模式	用於排除 Slack 資料來源中特定內容的規則運算式模式清單。符合模式的內容會從索引中排除。不符合模式的內容會包含在索引中。如果有任何內容同時符合包含和排除模式，則排除模式優先，且內容不會包含在索引中。

組態	描述
<code>crawlBotMessages</code>	<code>true</code> 抓取機器人消息。
排除已存檔	<code>true</code> 以排除已存檔訊息的探索。
對話類型	您要索引的交談類型是否 <code>PUBLIC_CHANNEL</code> 、 <code>PRIVATE_CHANNEL</code> 、 <code>GROUP_MESSAGE</code> 和 <code>DIRECT_MESSAGE</code> 。
頻道篩選	您要索引是否為 <code>private_channel</code> 或的通道類型 <code>public_channel</code> 。
自最新	您可以選擇設定 <code>sinceDate</code> 參數，以便 Slack 連接器根據特定 <code>sinceDate</code> 內容編目。
回顧	您可以選擇設定 <code>lookBack</code> 參數，讓連接器在上次 Slack 連接器同步之前的指定小時內搜索更新或刪除的內容。
同步模式	<p>指定資料來源內容變更時 Amazon Kendra 應如何更新索引。您可以選擇：</p> <ul style="list-style-type: none"> <code>FORCED_FULL_CRAWL</code> 新建索引所有內容，並在每次資料來源與索引同步時取代現有內容。 <code>FULL_CRAWL</code>，每次您的資料來源與索引同步時，僅對新的、修改和刪除的內容建立索引。Amazon Kendra 可以使用資料來源的機制來追蹤內容變更，並為上次同步後變更的內容建立索引。 <code>CHANGE_LOG</code> 每次資料來源與索引同步時，僅對新內容和修改的內容建立索引。Amazon Kendra 可以使用資料來源的機制來追蹤內容變更，並為上次同步後變更的內容建立索引。
<code>type</code>	資料來源的類型。指定 <code>SLACK</code> 為您的資料來源類型。

組態	描述
enableIdentityCrawler	true，以使用 Amazon Kendra 的身分識別爬行者程式來同步使用者和群組的身分識別/主體資訊，以存取特定文件。如果關閉身分搜索器，則可以公開搜索所有文檔。如果您想要對文件使用存取控制，且身分識別編目程式已關閉，您也可以使用 PutPrincipalMapping API 來上傳使用者和群組存取資訊。
秘书	Amazon 資源名稱 (ARN) 的 AWS Secrets Manager 秘密，其中包含連接到 Slack 私密必須包含具有下列索引鍵的 JSON 結構： <div style="border: 1px solid #ccc; border-radius: 10px; padding: 10px; margin: 10px 0;"> <pre>{ "slackToken": " <i>token</i>" }</pre> </div>
version	此範本目前支援的版本。

鬆弛結構定義

```
{
  "$schema": "http://json-schema.org/draft-04/schema#",
  "type": "object",
  "properties": {
    "connectionConfiguration": {
      "type": "object",
      "properties": {
        "repositoryEndpointMetadata": {
          "type": "object",
          "properties": {
            "teamId": {
              "type": "string"
            }
          },
          "required": ["teamId"]
        }
      }
    }
  }
}
```

```

},
"repositoryConfigurations": {
  "type": "object",
  "properties": {
    "All": {
      "type": "object",
      "properties": {
        "fieldMappings": {
          "type": "array",
          "items": [
            {
              "type": "object",
              "properties": {
                "indexFieldName": {
                  "type": "string"
                },
                "indexFieldType": {
                  "type": "string",
                  "enum": ["STRING", "STRING_LIST", "DATE", "LONG"]
                },
                "dataSourceFieldName": {
                  "type": "string"
                },
                "dateFieldFormat": {
                  "type": "string",
                  "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                }
              }
            },
            "required": [
              "indexFieldName",
              "indexFieldType",
              "dataSourceFieldName"
            ]
          ]
        },
        "required": [
          "fieldMappings"
        ]
      }
    },
    "required": [
      "fieldMappings"
    ]
  }
},
"required": [
]

```



```
},
"additionalProperties": {
  "type": "object",
  "properties": {
    "exclusionPatterns": {
      "type": "array",
      "items": {
        "type": "string"
      }
    },
    "inclusionPatterns": {
      "type": "array",
      "items": {
        "type": "string"
      }
    },
    "crawlBotMessages": {
      "type": "boolean"
    },
    "excludeArchived": {
      "type": "boolean"
    },
    "conversationType": {
      "type": "array",
      "items": {
        "type": "string",
        "enum": [
          "PUBLIC_CHANNEL",
          "PRIVATE_CHANNEL",
          "GROUP_MESSAGE",
          "DIRECT_MESSAGE"
        ]
      }
    },
    "channelFilter": {
      "type": "object",
      "properties": {
        "private_channel": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "public_channel": {
```

```
        "type": "array",
        "items": {
            "type": "string"
        }
    }
},
"channelIdFilter": {
    "type": "array",
    "items": {
        "type": "string"
    }
},
"sinceDate": {
    "anyOf": [
        {
            "type": "string",
            "pattern": "^[0-9]{4}-[0-9]{2}-[0-9]{2}T[0-9]{2}:[0-9]{2}:[0-9]{2}Z$"
        },
        {
            "type": "string",
            "pattern": ""
        }
    ]
},
"lookBack": {
    "type": "string",
    "pattern": "^[0-9]*$"
}
},
"required": [
]
},
"syncMode": {
    "type": "string",
    "enum": [
        "FORCED_FULL_CRAWL",
        "FULL_CRAWL",
        "CHANGE_LOG"
    ]
},
"type" : {
    "type" : "string",
    "pattern": "SLACK"
```

```

    },
    "enableIdentityCrawler": {
      "type": "boolean"
    },
    "secretArn": {
      "type": "string"
    }
  },
  "version": {
    "type": "string",
    "anyOf": [
      {
        "pattern": "1.0.0"
      }
    ]
  },
  "required": [
    "connectionConfiguration",
    "repositoryConfigurations",
    "syncMode",
    "additionalProperties",
    "secretArn",
    "type",
    "enableIdentityCrawler"
  ]
}

```

ZENDESK 模板架構

您可以將包含資料來源結構描述的 JSON 納入為 [TemplateConfiguration](#) 物件的一部分。您可以提供主機 URL 做為連線組態或存放庫端點詳細資料的一部分。同時將資料來源類型指定為 ZENDESK、驗證認證的密碼，以及其他必要的組態。然後，您將指定 TEMPLATE 為呼叫 Type 時 [CreateDataSource](#)。

您可以使用本開發人員指南中提供的模板。請參閱 [天台 JSON 架構](#)。

下表說明 Zendesk JSON 結構定義的參數。

組態	描述
連線組態	資料來源端點的組態資訊。
repositoryEndpointMetadata	資料來源的端點資訊。

組態	描述
主机网址	Zendesk 主機網址。例如： https://yoursubdomain.zendesk.com 。
儲存庫組態	資料來源內容的組態資訊。例如，配置特定類型的內容和欄位對應。
<ul style="list-style-type: none"> • ticket • 票務評論 • ticketCommentAttachment • 文章 • 文章評論 • 文章附件 • 社區主題 • communityPostComment 	將 Zendesk 票證的屬性或欄位名稱對應至 Amazon Kendra 索引欄位名稱的物件清單。如需詳細資訊，請參閱 映射資料來源欄位 。
秘书	AWS Secrets Manager 秘密的 Amazon 資源名稱 (ARN)，其中包含連接到 Zendesk 所需的鍵值對。密碼必須包含具有下列金鑰的 JSON 結構：主機 URL、用戶端 ID、用戶端密碼、使用者名稱和密碼。
附加屬性	資料來源中內容的其他設定選項
organizationNameFilter	您可以選擇索引存在於特定組織內的工單。
自最新	您可以選擇配置sinceDate 參數，以便 Zendesk 連接器根據特定內容進行編目。sinceDate
包含模式	在 Zendesk 資料來源中包含某些檔案的規則運算式模式清單。符合模式的檔案會包括在索引中。不符合模式的檔案會從索引中排除。如果檔案同時符合包含模式和排除模式，則排除模式優先，且檔案不會包含在索引中。

組態	描述
排除模式	用於排除 Zendesk 資料來源中某些檔案的規則運算式模式清單。符合模式的檔案會從索引中排除。與模式不匹配的文件包含在索引中。如果檔案同時符合排除和包含模式，則排除模式優先，且該檔案不會包含在索引中。
<ul style="list-style-type: none"> isCrawlTicket isCrawlTicket评论 isCrawlTicketCommentAttachment isCrawlArticle isCrawlArticle评论 isCrawlArticle附件 isCrawlCommunity主题 isCrawlCommunity郵政 isCrawlCommunityPostComment 	輸入 "true" 以編目這些類型的內容。
type	指定ZENDESK為您的資料來源類型。
useChangeLog	輸入 "true" 以使用 Zendesk 變更記錄檔來決定哪些文件需要在索引中更新。根據變更記錄的大小，在 Zendesk 中掃描文件的速度可能會更快。如果您是第一次將 Zendesk 資料來源與索引同步，則會掃描所有文件。

天台 JSON 架構

```
{
  "$schema": "http://json-schema.org/draft-04/schema#",
  "type": "object",
  "properties": {
    "connectionConfiguration": {
      "type": "object",
      "properties": {
        "repositoryEndpointMetadata": {
          "type": "object",
```

```
    "properties": {
      "hostUrl": {
        "type": "string",
        "pattern": "https:.*"
      }
    },
    "required": [
      "hostUrl"
    ]
  },
  "required": [
    "repositoryEndpointMetadata"
  ],
  "repositoryConfigurations": {
    "type": "object",
    "properties": {
      "ticket": {
        "type": "object",
        "properties": {
          "fieldMappings": {
            "type": "array",
            "items": {
              "anyOf": [
                {
                  "type": "object",
                  "properties": {
                    "indexFieldName": {
                      "type": "string"
                    },
                    "indexFieldType": {
                      "type": "string",
                      "enum": ["STRING", "STRING_LIST", "LONG", "DATE"]
                    },
                    "dataSourceFieldName": {
                      "type": "string"
                    },
                    "dateFieldFormat": {
                      "type": "string",
                      "pattern": "dd-MM-yyyy HH:mm:ss"
                    }
                  }
                }
              ]
            }
          },
          "required": [
```

```

        "indexFieldName",
        "indexFieldType",
        "dataSourceFieldName"
    ]
}
]
}
},
"required": [
    "fieldMappings"
]
},
"ticketComment": {
    "type": "object",
    "properties": {
        "fieldMappings": {
            "type": "array",
            "items": {
                "anyOf": [
                    {
                        "type": "object",
                        "properties": {
                            "indexFieldName": {
                                "type": "string"
                            },
                            "indexFieldType": {
                                "type": "string",
                                "enum": ["STRING", "STRING_LIST", "LONG", "DATE"]
                            },
                            "dataSourceFieldName": {
                                "type": "string"
                            },
                            "dateFieldFormat": {
                                "type": "string",
                                "pattern": "dd-MM-yyyy HH:mm:ss"
                            }
                        }
                    },
                    {
                        "type": "object",
                        "properties": {
                            "indexFieldName",
                            "indexFieldType",
                            "dataSourceFieldName"
                        }
                    }
                ]
            }
        }
    }
}

```

```
    ]
  }
]
}
},
"required": [
  "fieldMappings"
]
},
"ticketCommentAttachment": {
  "type": "object",
  "properties": {
    "fieldMappings": {
      "type": "array",
      "items": {
        "anyOf": [
          {
            "type": "object",
            "properties": {
              "indexFieldName": {
                "type": "string"
              },
              "indexFieldType": {
                "type": "string",
                "enum": ["STRING", "STRING_LIST", "LONG", "DATE"]
              },
              "dataSourceFieldName": {
                "type": "string"
              },
              "dateFieldFormat": {
                "type": "string",
                "pattern": "dd-MM-yyyy HH:mm:ss"
              }
            }
          },
          {
            "type": "string"
          }
        ]
      }
    },
    "required": [
      "indexFieldName",
      "indexFieldType",
      "dataSourceFieldName"
    ]
  }
}
}
```



```
    },
    "required": [
      "fieldMappings"
    ]
  },
  "article": {
    "type": "object",
    "properties": {
      "fieldMappings": {
        "type": "array",
        "items": {
          "anyOf": [
            {
              "type": "object",
              "properties": {
                "indexFieldName": {
                  "type": "string"
                },
                "indexFieldType": {
                  "type": "string",
                  "enum": ["STRING", "STRING_LIST", "LONG", "DATE"]
                },
                "dataSourceFieldName": {
                  "type": "string"
                },
                "dateFieldFormat": {
                  "type": "string",
                  "pattern": "dd-MM-yyyy HH:mm:ss"
                }
              }
            },
            "required": [
              "indexFieldName",
              "indexFieldType",
              "dataSourceFieldName"
            ]
          ]
        }
      }
    }
  },
  "required": [
    "fieldMappings"
  ]
},
```

```
"communityPostComment": {
  "type": "object",
  "properties": {
    "fieldMappings": {
      "type": "array",
      "items": {
        "anyOf": [
          {
            "type": "object",
            "properties": {
              "indexFieldName": {
                "type": "string"
              },
              "indexFieldType": {
                "type": "string",
                "enum": ["STRING", "STRING_LIST", "LONG", "DATE"]
              },
              "dataSourceFieldName": {
                "type": "string"
              },
              "dateFieldFormat": {
                "type": "string",
                "pattern": "dd-MM-yyyy HH:mm:ss"
              }
            }
          },
          {
            "type": "string"
          }
        ]
      }
    },
    "required": [
      "indexFieldName",
      "indexFieldType",
      "dataSourceFieldName"
    ]
  }
},
"required": [
  "fieldMappings"
]
},
"articleComment": {
  "type": "object",
  "properties": {
    "fieldMappings": {
      "type": "array",
```

```
    "items": {
      "anyOf": [
        {
          "type": "object",
          "properties": {
            "indexFieldName": {
              "type": "string"
            },
            "indexFieldType": {
              "type": "string",
              "enum": ["STRING", "STRING_LIST", "LONG", "DATE"]
            },
            "dataSourceFieldName": {
              "type": "string"
            },
            "dateFieldFormat": {
              "type": "string",
              "pattern": "dd-MM-yyyy HH:mm:ss"
            }
          },
          "required": [
            "indexFieldName",
            "indexFieldType",
            "dataSourceFieldName"
          ]
        }
      ]
    },
    "required": [
      "fieldMappings"
    ],
    "articleAttachment": {
      "type": "object",
      "properties": {
        "fieldMappings": {
          "type": "array",
          "items": {
            "anyOf": [
              {
                "type": "object",
                "properties": {
```

```
        "indexFieldName": {
          "type": "string"
        },
        "indexFieldType": {
          "type": "string",
          "enum": ["STRING", "STRING_LIST", "LONG", "DATE"]
        },
        "dataSourceFieldName": {
          "type": "string"
        },
        "dateFieldFormat": {
          "type": "string",
          "pattern": "dd-MM-yyyy HH:mm:ss"
        }
      },
      "required": [
        "indexFieldName",
        "indexFieldType",
        "dataSourceFieldName"
      ]
    }
  ]
}
},
"required": [
  "fieldMappings"
],
"communityTopic": {
  "type": "object",
  "properties": {
    "fieldMappings": {
      "type": "array",
      "items": {
        "anyOf": [
          {
            "type": "object",
            "properties": {
              "indexFieldName": {
                "type": "string"
              },
            },
            "indexFieldType": {
              "type": "string",
            }
          }
        ]
      }
    }
  }
}
```

```

        "enum": ["STRING", "STRING_LIST", "LONG", "DATE"]
    },
    "dataSourceFieldName": {
        "type": "string"
    },
    "dateFieldFormat": {
        "type": "string",
        "pattern": "dd-MM-yyyy HH:mm:ss"
    }
},
"required": [
    "indexFieldName",
    "indexFieldType",
    "dataSourceFieldName"
]
}
]
}
},
"required": [
    "fieldMappings"
]
}
},
"secretArn": {
    "type": "string",
    "minLength": 20,
    "maxLength": 2048
},
"additionalProperties": {
    "type": "object",
    "properties": {
        "organizationNameFilter": {
            "type": "array"
        },
        "sinceDate": {
            "type": "string",
            "pattern": "^[0-9]{4}-[0-9]{2}-[0-9]{2} [0-9]{2}:[0-9]{2}:[0-9]{2}$"
        },
        "inclusionPatterns": {
            "type": "array"
        }
    }
},

```

```
    "exclusionPatterns": {
      "type": "array"
    },
    "isCrawlTicket": {
      "type": "string"
    },
    "isCrawlTicketComment": {
      "type": "string"
    },
    "isCrawlTicketCommentAttachment": {
      "type": "string"
    },
    "isCrawlArticle": {
      "type": "string"
    },
    "isCrawlArticleAttachment": {
      "type": "string"
    },
    "isCrawlArticleComment": {
      "type": "string"
    },
    "isCrawlCommunityTopic": {
      "type": "string"
    },
    "isCrawlCommunityPost": {
      "type": "string"
    },
    "isCrawlCommunityPostComment": {
      "type": "string"
    }
  }
},
"type": {
  "type": "string",
  "pattern": "ZENDESK"
},
"useChangeLog": {
  "type": "string",
  "enum": ["true", "false"]
}
},
"version": {
  "type": "string",
  "anyOf": [
```

```
{
  "pattern": "1.0.0"
}
],
"additionalProperties": false,
"required": [
  "connectionConfiguration",
  "repositoryConfigurations",
  "additionalProperties",
  "useChangeLog",
  "secretArn",
  "type"
]
}
```

Adobe Experience Manager

Adobe Experience Manager 是用於創建網站或移動應用程式內容的內容管理系統。您可以用 Amazon Kendra 來連線到頁面 Adobe Experience Manager 和內容資產，並建立索引。

Amazon Kendra 支援 Adobe Experience Manager (AEM) 做為雲端服務作者執行個體以及 Adobe Experience Manager 內部部署作者和發佈執行個體。

您可以使用 [Amazon Kendra 主控台](#) 或 [TemplateConfiguration API](#) 連線 Amazon Kendra 到 Adobe Experience Manager 資料來源。

如需疑難排解 Amazon Kendra Adobe 體驗管理員資料來源連接器，請參閱 [疑難排解資料來](#)。

主題

- [支援的功能](#)
- [必要條件](#)
- [連接說明](#)

支援的功能

Adobe Experience Manager 資料來源連接器支援下列功能：

- 欄位對映
- 使用者存取控制

- 包含/排除過濾器
- 完整和增量內容同步
- OAuth 2.0 和基本身份驗證
- 虛擬私有雲端 (VPC)

必要條件

在您可以用來 Amazon Kendra 為資料來源建立索引之前，請先在 Adobe Experience Manager 和 AWS 帳戶中進行這些變更。

在中 Adobe Experience Manager，請確定您有：

- 存取具有管理權限的帳戶或管理員使用者。
- 已複製您的 Adobe Experience Manager 主機網址。

Note

(預備內部/伺服器) Amazon Kendra 會檢查中包含的端點資訊 AWS Secrets Manager 是否與資料來源組態詳細資料中指定的端點資訊相同。這有助於防止混淆的副問題，這是一個安全性問題，即使用者沒有執行動作的權限，但用 Amazon Kendra 作 Proxy 來存取設定的密碼並執行動作。如果您稍後變更端點資訊，則必須建立新密碼才能同步此資訊。

- 記下您的管理員使用者名稱和密碼的基本驗證憑證。

Note

我們建議您定期重新整理或輪換您的認證和密碼。僅為您自己的安全提供必要的訪問級別。我們不建議您跨資料來源以及連接器 1.0 和 2.0 版 (如果適用) 重複使用認證和密碼。

- 選用性：在 Adobe Experience Manager (AEM) 中將 OAuth 2.0 認證設定為雲端服務或 AEM 內部部署。如果您使用 AEM 內部部署，認證包括用戶端 ID、用戶端密碼和私密金鑰。如果您使用 AEM 做為雲端服務，則認證包括用戶端 ID、用戶端密碼、私密金鑰、組織 ID、技術帳戶 ID 和 Adobe Identity Management System (IMS) 主機。如需如何為 AEM 做為雲端服務產生這些認證的詳細資訊，請參閱 [Adobe Experience Manager 文件](#)。針對 AEM 內部部署，Adobe 花崗岩 OAuth 2.0 伺服器實作 (com.adobe.granite.oauth.server) 可在 AEM 中提供 OAuth 2.0 伺服器功能的支援。

- 已核取每個文件在 Adobe Experience Manager 中，以及您打算用於相同索引的其他資料來源之間是唯一的。您要用於索引的每個資料來源不得包含跨資料來源的相同文件。文件 ID 對索引來說是全域的，而且每個索引必須是唯一的。

在您的中 AWS 帳戶，請確保您有：

- [建立 Amazon Kendra 索引](#)，如果使用 API，則會記下索引識別碼。
- 為您的[資料來源建立 IAM 角色](#)，如果使用 API，則會記錄 IAM 角色的 ARN。

Note

如果您變更驗證類型和認證，則必須更新 IAM 角色才能存取正確的 AWS Secrets Manager 密碼 ID。

- 將您的 Adobe 體驗管理員驗證憑證儲存在 AWS Secrets Manager 密碼中，如果使用 API，則會記下密碼的 ARN。

Note

我們建議您定期重新整理或輪換您的認證和密碼。僅為您自己的安全提供必要的訪問級別。我們不建議您跨資料來源以及連接器 1.0 和 2.0 版 (如果適用) 重複使用認證和密碼。

如果您沒有現有的 IAM 角色或密碼，則可以在將 Adobe Experience Manager 資料來源連線到時，使用主控台建立新 IAM 角色和 Secrets Manager 密碼 Amazon Kendra。如果您使用 API，則必須提供現有 IAM 角色和 Secrets Manager 密碼的 ARN 以及索引 ID。

連接說明

若要連線 Amazon Kendra 到 Adobe Experience Manager 資料來源，您必須提供資料來源的必要詳細 Adobe Experience Manager 資訊，Amazon Kendra 以便能夠存取您的資料。如果您尚未配置 Amazon Kendra，Adobe Experience Manager 請參閱[必要條件](#)。

Console

若要連線 Amazon Kendra 到 Adobe Experience Manager

1. 登入 AWS Management Console 並開啟[Amazon Kendra 主控台](#)。
2. 在左側導覽窗格中，選擇 [索引]，然後從索引清單中選擇要使用的索引。

Note

您可以選擇在索引設置下配置或編輯您的用戶訪問控制設置。

3. 在 [開始使用] 頁面上，選擇 [新增資料來源]。
4. 在 [新增資料來源] 頁面上，選擇 [Adobe 體驗管理員] 連接器，然後選擇 [新增連接器]。如果使用版本 2 (如果適用)，請選擇具有「V2.0」標籤的 Adobe 體驗管理員連接器。
5. 在 [指定資料來源詳細資訊] 頁面上，輸入下列資訊：
 - a. 在名稱和說明中，對於資料來源名稱 — 輸入資料來源的名稱。您可以包含連字號，但不能包含空格。
 - b. (選擇性) 說明 — 輸入資料來源的選用說明。
 - c. 在預設語言中 — 選擇一種語言來篩選索引的文件。除非另有指定，否則語言預設為英文。文件中繼資料中指定的語言會覆寫選取的語言。
 - d. 在「標籤」中，針對「新增標籤」 — 包含可選標籤以搜尋和篩選資源或追蹤 AWS 成本。
 - e. 選擇下一步。
6. 在 [定義存取權和安全性] 頁面上，輸入下列資訊：
 - a. 來源 — 選擇 AEM 內部部署或 AEM 做為雲端服務。

輸入您的 Adobe Experience Manager 主機網址。例如，如果您使用 AEM 內部部署，則會包含主機名稱和連接埠：https://hostname:port 或者，如果您使用 AEM 做為雲端服務，您可以使用作者 URL: https://author-xxxxxx-xxxxxx.adobecloud.com。


- b. SSL 憑證位置 — 輸入儲存在 Amazon S3 值區中之 SSL 憑證的路徑。您可以使用此選項，透過安全的 SSL 連線連線至 AEM 內部部署。
- c. 授權 — 開啟或關閉文件的存取控制清單 (ACL) 資訊 (如果您有 ACL)，且想要將其用於存取控制。ACL 會指定使用者和群組可存取的文件。ACL 資訊可用來根據使用者或使用者對文件的群組存取權來篩選搜尋結果。如需詳細資訊，請參閱 [使用者內容篩選](#)。
- d. 驗證 — 選擇「基本驗證」或「OAuth 2.0 驗證」。然後選擇現有 AWS Secrets Manager 密碼或建立新密碼來儲存您的 Adobe Experience Manager 認證。如果您選擇建立新密碼，則會開啟一個 AWS Secrets Manager 密碼視窗。

如果您選擇基本驗證，請輸入密碼的名稱、Adobe Experience Manager 網站使用者名稱和密碼。使用者必須具有管理員權限或是管理員使用者。

如果您選擇 OAuth 2.0 驗證，並使用 AEM 內部部署，請輸入密碼、用戶端 ID、用戶端密碼和私密金鑰的名稱。如果您使用 AEM 做為雲端服務，請輸入密碼、用戶端 ID、用戶端密碼、私密金鑰、組織 ID、技術帳戶 ID 和 Adobe Identity Management System (IMS) 主機的名稱。

保存添加您的秘密。

- e. V@@@rtual Private Cloud (VPC) (VPC) — 您可以選擇使用 VPC。如果是這樣，您必須新增子網路和 VPC 安全性群組。
- f. 識別爬行者程式 — 指定是否要開啟身分識別爬行者 Amazon Kendra 程式。識別爬行者程式會使用文件的存取控制清單 (ACL) 資訊，根據使用者或使用者對文件的群組存取權來篩選搜尋結果。如果您有文件的 ACL 並選擇使用 ACL，您也可以選擇開啟的身分識別爬行者程式，以設定搜尋結果的使用者環境定義篩選。Amazon Kendra 否則，如果關閉身分搜索器，則可以公開搜索所有文檔。如果您想要對文件使用存取控制，且身分識別編目程式已關閉，您也可以使用 [PutPrincipalMapping](#) API 來上傳使用者和群組存取資訊以進行使用者內容篩選。
- g. IAM role — 選擇現有 IAM 角色或建立新 IAM 角色以存取存放庫認證和索引內容。

 Note

IAM 用於索引的角色不能用於資料來源。如果您不確定索引或常見問題集是否使用現有角色，請選擇 [建立新角色] 以避免發生錯誤。

- h. 選擇下一步。
7. 在 [設定同步設定] 頁面上，輸入下列資訊：
- a. 同步範圍 — 設定檢索特定內容類型、頁面元件和根路徑的限制，並使用正則運算式模式篩選內容。
 - i. 內容類型 — 選擇是否只編目頁面或資產，或兩者。
 - ii. (選擇性) 其他組態 — 設定下列設定：
 - 頁面元件 — 頁面元件的特定名稱。頁面元件是一種可擴充的頁面元件，可與 Adobe Experience Manager 範本編輯器搭配使用，並允許使用範本編輯器組裝頁首/頁尾和結構元件。

- 內容片段變體-內容片段變體的特定名稱。內容片段可讓您在設計、建立、組織和發佈與頁面無關的內容。Adobe Experience Manager 它們允許您準備可以在多個位置/通道上使用的內容。
 - 根路徑-特定內容的根路徑。
 - 正則表達式模式-包含或排除某些頁面和資產的規則運算式模式。
- b. 同步模式 — 選擇資料來源內容變更時要如何更新索引。當您第一次將資料來源同 Amazon Kendra 步處理時，依預設會檢索所有內容並建立索引。如果初始同步失敗，您必須執行資料的完整同步，即使您沒有選擇完整同步作為同步模式選項。
- 完全同步：新鮮索引所有內容，並在每次資料來源與索引同步時取代現有內容。
 - 新增、修改的同步：每次資料來源與索引同步時，僅對新內容和已修改的內容建立索引。Amazon Kendra 可以使用資料來源的機制來追蹤內容變更，並為上次同步後變更的內容建立索引。
 - 新增、修改、刪除的同步：每次資料來源與索引同步時，僅對新內容、已修改和刪除的內容建立索引。Amazon Kendra 可以使用資料來源的機制來追蹤內容變更，並為上次同步後變更的內容建立索引。
- c. 時區 ID — 如果您使用 AEM 內部部署，且伺服器的時區與 Amazon Kendra AEM 連接器或索引的時區不同，則可以指定伺服器時區以與 AEM 連接器或索引對齊。AEM 內部部署的預設時區是 Amazon Kendra AEM 連接器或索引的時區。AEM 做為雲端服務的預設時區是格林威治標準時間。
- d. 同步執行排程 (針對頻率) — 選擇同步資料來源內容和更新索引的頻率。
- e. 選擇下一步。
8. 在 [設定欄位對映] 頁面上，輸入下列資訊：
- a. 從 Amazon Kendra 產生的預設資料來源欄位中選取您要對映至索引的資料來源欄位。若要新增自訂資料來源欄位，請建立要對映的索引欄位名稱和欄位資料類型。
 - b. 選擇下一步。
9. 在 [檢閱並建立] 頁面上，檢查您輸入的資訊是否正確，然後選取 [新增資料來源]。您也可以從此頁面選擇編輯您的資訊。成功新增資料來源後，您的資料來源將顯示在 [資料來源] 頁面上。

API

若要連線 Amazon Kendra 到 Adobe Experience Manager

您必須使用 [TemplateConfiguration](#) API 指定 [資料來源結構描述](#) 的 JSON。您必須提供以下信息：

- 資料來源 — 指定使用 [TemplateConfiguration](#) JSON 結構定義 AEM 時的資料來源類型。同時將資料來源指定為呼叫 [CreateDataSource](#) API TEMPLATE 時的方式。
- AEM 主機 URL — 指定 Adobe Experience Manager 主機 URL。例如，如果您使用 AEM 內部部署，則會包含主機名稱和連接埠：https://hostname:port 或者，如果您使用 AEM 做為雲端服務，您可以使用作者 URL: https://author-xxxxxx-xxxxxx.adobe.com。
- 同步模式 — 指定資料來源內容變更時 Amazon Kendra 應如何更新索引。當您第一次將資料來源同 Amazon Kendra 步處理時，依預設會檢索所有內容並建立索引。如果初始同步失敗，您必須執行資料的完整同步，即使您沒有選擇完整同步作為同步模式選項。您可以選擇：
 - FORCED_FULL_CRAWL 新建索引所有內容，並在每次資料來源與索引同步時取代現有內容。
 - FULL_CRAWL，以在每次資料來源與索引同步時，僅對新的、修改的和刪除的內容建立索引。Amazon Kendra 可以使用資料來源的機制來追蹤內容變更，並為上次同步後變更的內容建立索引。
 - CHANGE_LOG 每次資料來源與索引同步時，僅對新內容和修改的內容建立索引。Amazon Kendra 可以使用資料來源的機制來追蹤內容變更，並為上次同步後變更的內容建立索引。
- 驗證類型 — 指定要使用的驗證類型 (Basic 或 OAuth2)。
- AEM 類型 — 指定 Adobe Experience Manager 您使用的類型 (或 CLOUD)。ON_PREMISE
- 秘密 Amazon 資源名稱 (ARN) — 如果您想要針對 AEM 內部部署或雲端使用基本身份驗證，請提供一個密碼來儲存使用者名稱和密碼的身份驗證登入資料。您提供一個 AWS Secrets Manager 秘密的 Amazon 資源名稱 (ARN)。密碼會以下列金鑰儲存在 JSON 結構中：

```
{
  "aemUrl": "Adobe Experience Manager On-Premise host URL",
  "username": "user name with admin permissions",
  "password": "password with admin permissions"
}
```

如果您想要針對內部部署 AEM 使用 OAuth 2.0 驗證，密碼會以下列金鑰儲存在 JSON 結構中：

```
{
  "aemUrl": "Adobe Experience Manager host URL",
  "clientId": "client ID",
  "clientSecret": "client secret",
  "privateKey": "private key"
}
```

如果您想要將 OAuth 2.0 驗證用於 AEM 做為雲端服務，則密碼會以下列金鑰儲存在 JSON 結構中：

```
{
  "clientId": "client ID",
  "clientSecret": "client secret",
  "privateKey": "private key",
  "orgId": "organization ID",
  "technicalAccountId": "technical account ID",
  "imsHost": "Adobe Identity Management System (IMS) host"
}
```

- IAM 角色 — 指定 RoleArn 當您呼叫 CreateDataSource 以提供具有存取 Secrets Manager 密碼之權限的 IAM 角色，以及呼叫 Adobe Experience Manager 連接器和 Amazon Kendra 所需公用 API 的時間。如需詳細資訊，請參閱 [Adobe 體驗管理員資料來源的 IAM 角色](#)。

您還可以添加以下可選功能：

- VPC 網際網路 Private Cloud (VPC) — 指定您撥打電話的 VpcConfiguration 時間。CreateDataSource 如需詳細資訊，請參閱 [配置 Amazon Kendra 為使用 Amazon VPC](#)。
- 時區 ID — 如果您使用 AEM 內部部署，且伺服器的時區與 Amazon Kendra AEM 連接器或索引的時區不同，則可以指定伺服器時區以與 AEM 連接器或索引對齊。

AEM 內部部署的預設時區是 Amazon Kendra AEM 連接器或索引的時區。AEM 做為雲端服務的預設時區是格林威治標準時間。

如需有關支援時區 ID 的詳細資訊，請參閱 [Adobe Experience Manager JSON 結構定義](#)。

- 包含和排除篩選器：指定要包含還是排除特定頁面和資產。

Note

大多數資料來源使用規則運算式模式，這些模式是稱為篩選器的包含或排除模式。如果您指定包含篩選器，則只會編製與包含項目篩選器相符的內容編製索引。不符合包含篩選器的任何文件都不會建立索引。如果您指定包含和排除篩選器，符合排除篩選器的文件將不會建立索引，即使它們符合包含篩選器也是如此。

- 識別爬行者程式 — 指定是否要開啟身分識別爬行 Amazon Kendra 者程式。識別爬行者程式會使用文件的存取控制清單 (ACL) 資訊，根據使用者或使用者對文件的群組存取權來篩選搜尋結

果。如果您有文件的 ACL 並選擇使用 ACL，您也可以選擇開啟的身分識別爬行者程式，以設定搜尋結果的使用者環境定義篩選。Amazon Kendra 否則，如果關閉身分搜索器，則可以公開搜索所有文檔。如果您想要對文件使用存取控制，且身分識別編目程式已關閉，您也可以使用 [PutPrincipalMapping](#) API 來上傳使用者和群組存取資訊以進行使用者內容篩選。

- 欄位對應 — 選擇將您的 Adobe 體驗管理員資料來源欄位對應至 Amazon Kendra 索引欄位。如需詳細資訊，請參閱 [映射資料來源欄位](#)。

Note

您的文件需要文件內文欄位或文件內文對等項目，才能搜尋您的文件。Amazon Kendra 您必須將資料來源中的文件內文欄位名稱對應至索引欄位名稱 `_document_body`。所有其他欄位是選用的。

如需要設定的其他重要 JSON 金鑰清單，請參閱 [Adobe Experience Manager 範本結構定義](#)。

Alfresco

Alfresco 是一項內容管理服務，可協助客戶儲存和管理其內容。您可以使 Amazon Kendra 用索引您的 Alfresco 文件庫、Wiki 和部落格。

Amazon Kendra 支援 Alfresco 內部部署和 Alfresco 雲端 (平台即服務)。

您可以使用 [Amazon Kendra 主控台](#) 或 [TemplateConfiguration](#) API 連線 Amazon Kendra 到 Alfresco 資料來源。

有關 Amazon Kendra Alfresco 資料來源連接器的疑難排解，請參閱 [疑難排解資料來](#)

主題

- [支援的功能](#)
- [必要條件](#)
- [連接說明](#)
- [進一步了解](#)

支援的功能

Amazon Kendra Alfresco 資料來源連接器支援下列功能：

- 欄位對映
- 使用者存取控制
- 包含/排除過濾器
- 完整和增量內容同步
- OAuth 2.0 和基本身份驗證
- 虛擬私有雲端 (VPC)

必要條件

在您可以使用 Amazon Kendra 來為 Alfresco 資料來源建立索引之前，請先在和中進行這些變更。Alfresco AWS 帳戶

在中Alfresco，請確定您有：

- 複製您的Alfresco儲存庫 URL 和 Web 應用程式 URL。如果您只想為特定Alfresco網站建立索引，請同時複製網站 ID。
- 記下您的Alfresco驗證認證，其中包括至少具有讀取權限的使用者名稱和密碼。如果要使用 OAuth 2.0 身份驗證，則應將用戶添加到Alfresco管理員組中。

Note

我們建議您定期重新整理或輪換您的認證和密碼。僅為您自己的安全提供必要的訪問級別。我們不建議您跨資料來源以及連接器 1.0 和 2.0 版 (如果適用) 重複使用認證和密碼。

- 選用性：在Alfresco中設定 OAuth 2.0 認證。憑據包括客戶端 ID，客戶端密鑰和令牌 URL。如需如何設定Alfresco內部部署用戶端的詳細資訊，請參閱 [Alfresco](#) 文件。如果您使用Alfresco雲 (PaaS)，則必須聯繫[海蘭支持](#)以進行 Alfresco OAuth 2.0 身份驗證。
- 檢查每個文檔在 Alfresco 和您打算用於同一索引的其他數據源中是唯一的。您要用於索引的每個資料來源不得包含跨資料來源的相同文件。文件 ID 對索引來說是全域的，而且每個索引必須是唯一的。

在您的中 AWS 帳戶，請確保您有：

- [建立 Amazon Kendra 索引](#)，如果使用 API，則會記下索引識別碼。
- 為您的[資料來源建立 IAM 角色](#)，如果使用 API，則會記錄 IAM 角色的 ARN。

Note

如果您變更驗證類型和認證，則必須更新 IAM 角色才能存取正確的 AWS Secrets Manager 密碼 ID。

- 將您的 Alfresco 身份驗證憑據存儲在 AWS Secrets Manager 秘密中，並且如果使用 API，則記錄密鑰的 ARN。

Note

我們建議您定期重新整理或輪換您的認證和密碼。僅為您自己的安全提供必要的訪問級別。我們不建議您跨資料來源以及連接器 1.0 和 2.0 版 (如果適用) 重複使用認證和密碼。

如果您沒有現有的 IAM 角色或密碼，則可以在將 Alfresco 資料來源連線至時使用主控台建立新 IAM 角色和 Secrets Manager 密碼。Amazon Kendra 如果您使用 API，則必須提供現有 IAM 角色和 Secrets Manager 密碼的 ARN 以及索引 ID。

連接說明

若要連線 Amazon Kendra 到 Alfresco 資料來源，您必須提供 Alfresco 資料來源的必要詳細資料，Amazon Kendra 以便能夠存取您的資料。如果尚未設定「露天」Amazon Kendra，請參閱 [必要條件](#)

Console

若要連線 Amazon Kendra 到 Alfresco

1. 登入 AWS Management Console 並開啟 [Amazon Kendra 主控台](#)。
2. 在左側導覽窗格中，選擇 [索引]，然後從索引清單中選擇要使用的索引。

Note

您可以選擇在索引設置下配置或編輯您的用戶訪問控制設置。

3. 在 [開始使用] 頁面上，選擇 [新增資料來源]。
4. 在 [新增資料來源] 頁面上，選擇 [Alfresco 連接器]，然後選擇 [新增連接器]。如果使用版本 2 (如果適用)，請選擇帶有「V2.0」標籤的 Alfresco 連接器。
5. 在 [指定資料來源詳細資訊] 頁面上，輸入下列資訊：

- a. 在名稱和說明中，對於資料來源名稱 — 輸入資料來源的名稱。您可以包含連字號，但不能包含空格。
 - b. (選擇性) 說明 — 輸入資料來源的選用說明。
 - c. 在預設語言中 — 選擇一種語言來篩選索引的文件。除非另有指定，否則語言預設為英文。文件中繼資料中指定的語言會覆寫選取的語言。
 - d. 在「標籤」中，針對「新增標籤」 — 包含可選標籤以搜尋和篩選資源或追蹤 AWS 成本。
 - e. 選擇下一步。
6. 在 [定義存取權和安全性] 頁面上，輸入下列資訊：
- a. Alfrescotype — 選擇您使用內部部Alfresco署/伺服器還是Alfresco雲端 (平台即服務)。
 - b. 露天儲存庫 URL — 輸入您的露天儲存庫 URL。例如，如果您使用Alfresco雲端 (PaaS)，則存放庫 URL 可能是https://company.alfrescocloud.com。或者，如果您使用 Alfresco 內部部署，則存放庫 URL 可能是。https://company-alfresco-instance.company-domain.suffix:port
 - c. 露天用戶應用程式。URL — 輸入您的Alfresco使用者介面 URL。您可以向Alfresco管理員取得存放庫 URL。例如，使用者介面網址可以是 https://example.com。
 - d. SSL 憑證位置 — 輸入儲存在 Amazon S3 值區中之 SSL 憑證的路徑。您可以使用此連線到Alfresco內部部署，透過安全的 SSL 連線。
 - e. 授權 — 開啟或關閉文件的存取控制清單 (ACL) 資訊 (如果您有 ACL)，且想要將其用於存取控制。ACL 會指定使用者和群組可存取的文件。ACL 資訊可用來根據使用者或使用者對文件的群組存取權來篩選搜尋結果。如需詳細資訊，請參閱[使用者內容篩選](#)。
 - f. 驗證 — 選擇「基本驗證」或「OAuth 2.0 驗證」。然後選擇現有 Secrets Manager 密碼或建立新密碼來儲存您的Alfresco認證。如果您選擇建立新密碼，則會開啟一個 AWS Secrets Manager 密碼視窗。


如果您選擇基本驗證，請輸入密碼的名稱、使Alfresco用者名稱和密碼。

如果您選擇 OAuth 2.0 驗證，請輸入密碼、用戶端 ID、用戶端密碼和權杖 URL 的名稱。

- g. V@@@ irtual Private Cloud (VPC) (VPC) — 您可以選擇使用 VPC。如果是這樣，您必須新增子網路和 VPC 安全性群組。
- h. 識別爬行者程式 — 指定是否要開啟身分識別爬行 Amazon Kendra者程式。識別爬行者程式會使用文件的存取控制清單 (ACL) 資訊，根據使用者或使用者對文件的群組存取權來篩選搜尋結果。如果您有文件的 ACL 並選擇使用 ACL，您也可以選擇開啟的身分識別爬行者程式，以設定搜尋結果的使用[者環境定義篩選](#)。Amazon Kendra否則，如果關閉身分搜

索器，則可以公開搜索所有文檔。如果您想要對文件使用存取控制，且身分識別編目程式已關閉，您也可以使用 [PutPrincipalMapping](#) API 來上傳使用者和群組存取資訊以進行使用者內容篩選。

- i. IAM role — 選擇現有 IAM 角色或建立新 IAM 角色以存取存放庫認證和索引內容。

 Note

IAM 用於索引的角色不能用於資料來源。如果您不確定索引或常見問題集是否使用現有角色，請選擇 [建立新角色] 以避免發生錯誤。

- j. 選擇下一步。

7. 在 [設定同步設定] 頁面上，輸入下列資訊：

- a. 同步範圍 — 設定編目特定內容的限制，並使用正則運算式運算式模式篩選內容。
- b.
 - i. 內容 — 選擇是要編目中標有「層面」的內容Alfresco、特定Alfresco網站內的內容，還是搜索所有網站上的Alfresco內容。
 - ii. (選擇性) 其他組態 — 設定下列設定：
 - 包含註解 — 選擇在「Alfresco文件庫」和「部落格」中包含註解。
 - 正則表達式模式-包含或排除某些文件的正則表達式模式。
- c. 同步模式 — 選擇資料來源內容變更時要如何更新索引。當您第一次將資料來源同 Amazon Kendra 步處理時，依預設會檢索所有內容並建立索引。如果初始同步失敗，您必須執行資料的完整同步處理，即使您沒有選擇完整同步作為同步模式選項。
 - 完全同步：新鮮索引所有內容，並在每次資料來源與索引同步時取代現有內容。
 - 新增、修改、刪除的同步：每次資料來源與索引同步時，僅對新內容、已修改和刪除的內容建立索引。Amazon Kendra 可以使用資料來源的機制來追蹤內容變更，並為上次同步後變更的內容建立索引。
- d. 在同步執行排程中，對於頻率 — 選擇同步資料來源內容和更新索引的頻率。
- e. 選擇下一步。

8. 在 [設定欄位對映] 頁面上，輸入下列資訊：

- a. 從 Amazon Kendra 產生的預設資料來源欄位中選取您要對映至索引的資料來源欄位。
- b. 若要新增自訂資料來源欄位，請建立要對映的索引欄位名稱和欄位資料類型。
- c. 選擇下一步。

9. 在 [檢閱並建立] 頁面上，檢查您輸入的資訊是否正確，然後選取 [新增資料來源]。您也可以從此頁面選擇編輯您的資訊。成功新增資料來源後，您的資料來源將顯示在 [資料來源] 頁面上。

API

若要連線 Amazon Kendra 到 Alfresco

您必須使用 [TemplateConfiguration](#) API 指定 [資料來源結構描述](#) 的 JSON。您必須提供以下信息：

- 資料來源 — 指定使用 [TemplateConfiguration](#) JSON 結構定義 ALFRESCO 時的資料來源類型。同時指定呼叫 [CreateDataSource](#) API TEMPLATE 時的資料來源。
- Alfresco 網站 ID — 指定露天網站 ID。
- Alfresco 存放庫 URL — 指定 Alfresco 存放庫 URL。您可以向 Alfresco 管理員取得存放庫 URL。例如，如果您使用 Alfresco 雲端 (PaaS)，則存放庫 URL 可能是 `https://company.alfrescocloud.com`。或者，如果您使用 Alfresco 內部部署，則存放庫 URL 可能是 `https://company-alfresco-instance.company-domain.suffix:port`
- AlfrescoWeb 應用程式 URL — 指定 Alfresco 使用者介面 URL。您可以向 Alfresco 管理員取得存放庫 URL。例如，使用者介面網址可以是 `https://example.com`。
- 驗證類型 — 指定您要使用的驗證類型，無論是 OAuth2 或 Basic。
- AlfrescoType — 指定 Alfresco 您使用的類型 PAAS (雲端/平台即服務) 或 ON_PREM (內部部署)。
- 秘密 Amazon 資源名稱 (ARN) — 如果您想要使用基本身份驗證，請提供一個密碼來儲存您的使用者名稱和密碼身份驗證登入資料。您提供一個 AWS Secrets Manager 秘密的 Amazon 資源名稱 (ARN)。密碼會以下列金鑰儲存在 JSON 結構中：

```
{
  "username": "user name",
  "password": "password"
}
```

如果要使用 OAuth 2.0 身份驗證，則密鑰將使用以下密鑰儲存在 JSON 結構中：

```
{
  "clientId": "client ID",
  "clientSecret": "client secret",
  "tokenUrl": "token URL"
}
```

- IAM role — 指定RoleArn何時呼叫CreateDataSource以提供具有存取 Secrets Manager 密碼權限的 IAM 角色，以及呼叫 Alfresco 連接器和所需的公用 API 的時間。Amazon Kendra有關詳情，請參閱 [Alfresco 資料來源的IAM 角色](#)。

您還可以添加以下可選功能：

- Virtual Private Cloud (VPC) — 指定您撥打電話的VpcConfiguration時間。CreateDataSource如需詳細資訊，請參閱 [配置 Amazon Kendra 為使用 Amazon VPC](#)。
- 內容類型 — 您要編目的內容類型，無論是在中標有「面向」的內容Alfresco、特定Alfresco網站內的內容，還是您所有網Alfresco站上的內容。您還可以列出特定的「方面」內容。
- 包含和排除篩選器 — 指定要包含還是排除某些檔案。

Note

大多數資料來源使用規則運算式模式，這些模式是稱為篩選器的包含或排除模式。如果您指定包含篩選器，則只有符合包含項目篩選器的內容會編製索引。不符合包含篩選器的任何文件都不會建立索引。如果您指定包含和排除篩選器，符合排除篩選器的文件將不會建立索引，即使它們符合包含篩選器也是如此。

- 同步模式 — 指定資料來源內容變更時 Amazon Kendra 應如何更新索引。當您第一次將資料來源同 Amazon Kendra 步處理時，依預設會檢索所有內容並建立索引。如果初始同步失敗，您必須執行資料的完整同步處理，即使您沒有選擇完整同步作為同步模式選項。您可以選擇：
 - FORCED_FULL_CRAWL 新建索引所有內容，並在每次資料來源與索引同步時取代現有內容。
 - FULL_CRAWL，以在每次資料來源與索引同步時，僅對新的、修改的和刪除的內容建立索引。Amazon Kendra 可以使用資料來源的機制來追蹤內容變更，並為上次同步後變更的內容建立索引。
- 識別爬行者程式 — 指定是否要開啟身分識別爬行 Amazon Kendra 者程式。識別爬行者程式會使用文件的存取控制清單 (ACL) 資訊，根據使用者或使用者對文件的群組存取權來篩選搜尋結果。如果您有文件的 ACL 並選擇使用 ACL，您也可以選擇開啟的身分識別爬行者程式，以設定搜尋結果的使用者環境定義篩選。Amazon Kendra 否則，如果關閉身分搜索器，則可以公開搜索所有文檔。如果您想要對文件使用存取控制，且身分識別編目程式已關閉，您也可以使用 [PutPrincipalMapping](#) API 來上傳使用者和群組存取資訊以進行使用者內容篩選。
- 欄位對映 — 選擇將 Alfresco 資料來源欄位對映至索引欄位。Amazon Kendra 如需詳細資訊，請參閱 [映射資料來源欄位](#)。

Note

您的文件需要文件內文欄位或文件內文對等項目，才能搜尋您的文件。Amazon Kendra 您必須將資料來源中的文件內文欄位名稱對應至索引欄位名稱_document_body。所有其他欄位是選用的。

如需要設定的其他重要 JSON 金鑰清單，請參閱[Alfresco 範本結構定義](#)。

進一步了解

若要深入瞭解如何 Amazon Kendra 與 Alfresco 資料來源整合，請參閱：

- [使用智慧搜尋 Alfresco 內容 Amazon Kendra](#)

Aurora (MySQL)

Aurora 是專為雲端建置的關聯式資料庫管理系統 (RDBMS)。如果您是使用 Aurora 者，則可以使用 Amazon Kendra 對資 Aurora (MySQL) 料來源建立索引。資 Amazon Kendra Aurora (MySQL) 料來源連接器支援 Aurora MySQL 3 和 Aurora 無伺服器 MySQL 8.0。

您可以使用[Amazon Kendra 主控台](#)和 [TemplateConfiguration API](#) 連線 Amazon Kendra 到 Aurora (MySQL) 資料來源。

如需對資 Amazon Kendra Aurora (MySQL) 料來源連接器進行疑難排解，請參 [疑難排解資料來](#)

主題

- [支援的功能](#)
- [必要條件](#)
- [連接說明](#)
- [備註](#)

支援的功能

- 欄位對映
- 使用者內容篩選

- 包含/排除過濾器
- 完整和增量內容同步
- 虛擬私有雲端 (VPC)

必要條件

在您可以用來 Amazon Kendra 為資料來源建立索引之前，請先在 Aurora (MySQL) 和 AWS 帳戶中進行這些變更。

在中 Aurora (MySQL)，請確定您有：

- 記下您的資料庫使用者名稱和密碼。

Important

最佳作法是提供 Amazon Kendra 唯讀資料庫認證。

- 複製您的資料庫主機 URL、連接埠和執行個體。您可以在 Amazon RDS 控制台上找到此信息。
- 已勾選的每個文件在您打算用於相同索引的其他資料來源中 Aurora (MySQL) 和其他資料來源之間都是唯一的。您要用於索引的每個資料來源不得包含跨資料來源的相同文件。文件 ID 對索引來說是全域的，而且每個索引必須是唯一的。

在您的 AWS 帳戶，請確保您有：

- [建立 Amazon Kendra 索引](#)，如果使用 API，則會記下索引識別碼。
- 為您的 [資料來源建立 IAM 角色](#)，如果使用 API，則會記錄 IAM 角色的 ARN。

Note

如果您變更驗證類型和認證，則必須更新 IAM 角色才能存取正確的 AWS Secrets Manager 密碼 ID。

- 將您的 Aurora (MySQL) 身份驗證憑據存儲在 AWS Secrets Manager 密鑰中，如果使用 API，則記錄密鑰的 ARN。

Note

我們建議您定期重新整理或輪換您的認證和密碼。僅為您自己的安全提供必要的訪問級別。我們不建議您跨資料來源以及連接器 1.0 和 2.0 版 (如果適用) 重複使用認證和密碼。

如果您沒有現有的 IAM 角色或密碼，則可以在將 Aurora (MySQL) 資料來源連線到時使用主控台建立新 IAM 角色和 Secrets Manager 密碼 Amazon Kendra。如果您使用 API，則必須提供現有 IAM 角色和 Secrets Manager 密碼的 ARN 以及索引 ID。

連接說明

若要連線 Amazon Kendra 到 Aurora (MySQL) 資料來源，您必須提供 Aurora (MySQL) 認證的詳細資料，Amazon Kendra 以便能夠存取您的資料。如果您尚未設定「Amazon Kendra 請 Aurora (MySQL) 參閱 [必要條件](#)」。

Console

若要連線 Amazon Kendra 到 Aurora (MySQL)


1. 登入 AWS Management Console 並開啟 [Amazon Kendra 主控台](#)。
2. 在左側導覽窗格中，選擇 [索引]，然後從索引清單中選擇要使用的索引。

Note

您可以選擇在索引設置下配置或編輯您的用戶訪問控制設置。

3. 在 [開始使用] 頁面上，選擇 [新增資料來源]。
4. 在 [新增資料來源] 頁面上，選擇 [Aurora (MySQL) 連接器]，然後選擇 [新增連接器]。如果使用版本 2 (如果適用)，請選擇帶有「V2.0」標籤的 Aurora (MySQL) 連接器。
5. 在 [指定資料來源詳細資訊] 頁面上，輸入下列資訊：
 - a. 在名稱和說明中，對於資料來源名稱 — 輸入資料來源的名稱。您可以包含連字號，但不能包含空格。
 - b. (選擇性) 說明 — 輸入資料來源的選用說明。
 - c. 在預設語言中 — 選擇一種語言來篩選索引的文件。除非另有指定，否則語言預設為英文。文件中繼資料中指定的語言會覆寫選取的語言。

- d. 在「標籤」中，針對「新增標籤」— 包含可選標籤以搜尋和篩選資源或追蹤 AWS 成本。
 - e. 選擇下一步。
6. 在 [定義存取權和安全性] 頁面上，輸入下列資訊：
- a. 在來源中，輸入下列資訊：
 - b. 主機 — 輸入資料庫主機 URL，例如：`http://instance URL.region.rds.amazonaws.com`
 - c. 連接埠 — 輸入資料庫連接埠，例如5432。
 - d. 執行處理 — 輸入資料庫執行處理。
 - e. 在驗證中 — 輸入下列資訊：
 - AWS Secrets Manager 祕密 — 選擇現有密碼或建立新 Secrets Manager 密碼來儲存您的Aurora (MySQL)驗證認證。如果您選擇建立新密碼，則會開啟一個 AWS Secrets Manager 密碼視窗。
 - A. 在「建立 AWS Secrets Manager 密碼視窗」中輸入下列資訊：
 - I. 秘密名稱 — 您秘密的名稱。前綴 'AmazonKendraAurora (MySQL)-' 會自動添加到您的密碼名稱中。
 - II. 對於資料庫使用者名稱和密碼 — 輸入您從資料庫複製的驗證認證值。
 - B. 選擇儲存。
 - f. V@@@rtual Private Cloud (VPC) (VPC) — 您可以選擇使用 VPC。如果是這樣，您必須新增子網路和 VPC 安全性群組。
 - g. IAM role — 選擇現有 IAM 角色或建立新 IAM 角色以存取存放庫認證和索引內容。

 Note

IAM 用於索引的角色不能用於資料來源。如果您不確定索引或常見問題集是否使用現有角色，請選擇 [建立新角色] 以避免發生錯誤。

- h. 選擇下一步。
7. 在 [設定同步設定] 頁面上，輸入下列資訊：
- a. 在同步範圍中，從下列選項中選擇：

- SQL 查詢 — 輸入 SQL 查詢陳述式，例如 SELECT 和 JOIN 作業。SQL 查詢必須小於 32 KB 的 SQL 查詢小於 32 KB，且不得包含任何分號 (;)。Amazon Kendra 會編目符合您查詢的所有資料庫內容。
 - 主索引鍵欄 — 提供資料庫表格的主索引鍵。這標識數據庫中的一個表。
 - 標題欄 — 提供資料庫表格中文件標題欄的名稱。
 - 主體欄 — 提供資料庫表格中文件主體欄的名稱。
- b. 在 [其他設定 — 選用] 中，從下列選項中選擇以同步特定內容，而非同步所有檔案：
- 變更偵測欄 — 輸入 Amazon Kendra 將用來偵測內容變更的欄名稱。Amazon Kendra 當這些資料行中有任何變更時，會重新建立內容的索引。
 - 使用者 ID 欄 — 輸入包含允許存取內容的使用者 ID 的欄名稱。
 - 群組欄 — 輸入包含允許存取內容之群組的欄名稱。
 - 來源 URL 欄 — 輸入包含要編製索引之來源 URL 的資料欄名稱。
 - 時間戳記欄 — 輸入包含時間戳記的欄名稱。Amazon Kendra 使用時間戳記資訊偵測內容中的變更，並僅同步變更的內容。
 - [時區] 欄 — 輸入資料欄的名稱，其中包含要編目之內容的時區。
 - 時間戳記格式 — 輸入包含時間戳記格式的欄名稱，可用來偵測內容變更並重新同步處理內容。
- c. 同步模式 — 選擇資料來源內容變更時要如何更新索引。當您第一次將資料來源同 Amazon Kendra 步處理時，依預設會檢索所有內容並建立索引。如果初始同步失敗，您必須執行資料的完整同步，即使您沒有選擇完整同步作為同步模式選項。
- 完全同步：新鮮索引所有內容，並在每次資料來源與索引同步時取代現有內容。
 - 新增、修改的同步：每次資料來源與索引同步時，僅對新內容和已修改的內容建立索引。Amazon Kendra 可以使用資料來源的機制來追蹤內容變更，並為上次同步後變更的內容建立索引。
 - 新增、修改、刪除的同步：每次資料來源與索引同步時，僅對新內容、已修改和刪除的內容建立索引。Amazon Kendra 可以使用資料來源的機制來追蹤內容變更，並為上次同步後變更的內容建立索引。
- d. 在同步執行排程中，對於頻率 — 與資料來源同步的頻率。Amazon Kendra
- e. 選擇下一步。
8. 在 [設定欄位對映] 頁面上，輸入下列資訊：

- a. 從產生的預設資料來源欄位中選取您要對應至 Amazon Kendra 索引的文件 ID、文件標題和來源 URL。
 - b. 新增欄位 — 新增自訂資料來源欄位，以建立要對映的索引欄位名稱和欄位資料類型。
 - c. 選擇下一步。
9. 在 [檢閱並建立] 頁面上，檢查您輸入的資訊是否正確，然後選取 [新增資料來源]。您也可以從此頁面選擇編輯您的資訊。成功新增資料來源後，您的資料來源將顯示在 [資料來源] 頁面上。

API

若要連線 Amazon Kendra 到 Aurora (MySQL)

您必須使用 [TemplateConfiguration](#) API 指定下列項目：

- 資料來源 — 指定使用 [TemplateConfiguration](#) JSON 結構定義 JDBC 時的資料來源類型。同時將資料來源指定為呼叫 [CreateDataSource](#) API TEMPLATE 時的方式。
- 資料庫類型 — 您必須將資料庫類型指定為 `mySql`。
- SQL 查詢 — 指定 SQL 查詢陳述式，例如 `SELECT` 和 `JOIN` 作業。SQL 查詢必須小於 32 KB。Amazon Kendra 會編目符合您查詢的所有資料庫內容。
- 同步模式 — 指定資料來源內容變更時 Amazon Kendra 應如何更新索引。當您第一次將資料來源同 Amazon Kendra 步處理時，依預設會檢索所有內容並建立索引。如果初始同步失敗，您必須執行資料的完整同步，即使您沒有選擇完整同步作為同步模式選項。您可以選擇：
 - `FORCED_FULL_CRAWL` 新建索引所有內容，並在每次資料來源與索引同步時取代現有內容。
 - `FULL_CRAWL`，以在每次資料來源與索引同步時，僅對新的、修改的和刪除的內容建立索引。Amazon Kendra 可以使用資料來源的機制來追蹤內容變更，並為上次同步後變更的內容建立索引。
 - `CHANGE_LOG` 每次資料來源與索引同步時，僅對新內容和修改的內容建立索引。Amazon Kendra 可以使用資料來源的機制來追蹤內容變更，並為上次同步後變更的內容建立索引。
- 秘密 Amazon 資源名稱 (ARN) — 提供包含您在帳戶中建立的身份驗證登入資料的 Secrets Manager 密碼的 Amazon 資源名稱 (ARN)。Aurora (MySQL) 密碼會以下列金鑰儲存在 JSON 結構中：

```
{
  "user name": "database user name",
  "password": "password"
}
```

Note

我們建議您定期重新整理或輪換您的認證和密碼。僅為您自己的安全提供必要的訪問級別。我們不建議您跨資料來源以及連接器 1.0 和 2.0 版 (如果適用) 重複使用認證和密碼。

- IAM role — 指定RoleArn何時呼叫CreateDataSource以提供具有存取 Secrets Manager 密碼之權限的 IAM 角色，以及呼叫Aurora (MySQL)連接器和 Amazon Kendra所需公用 API 的時間。有關詳情，請參閱[Aurora \(MySQL\)料來源的IAM 角色](#)。

您還可以添加以下可選功能：

- V@@ irtual Private Cloud (VPC) — 指定您撥打電話的VpcConfiguration時間。CreateDataSource如需詳細資訊，請參閱 [配置 Amazon Kendra 為使用 Amazon VPC](#)。
- 包含和排除篩選器 — 您可以指定是否要使用使用者 ID、群組、來源 URL、時間戳記和時區來包含特定內容。
- 使用者前後關聯篩選與存取控制 — Amazon Kendra 探索文件的存取控制清單 (ACL) (如果您有文件的 ACL)。ACL 資訊可用來根據使用者或使用者對文件的群組存取來篩選搜尋結果。如需詳細資訊，請參閱[使用者內容篩選](#)。
- 欄位對映 — 選擇將資Aurora (MySQL)料來源欄位對映至 Amazon Kendra 索引欄位。如需詳細資訊，請參閱[映射資料來源欄位](#)。

Note

您的文件需要文件內文欄位或文件內文對等項目，才能搜尋您的文件。Amazon Kendra 您必須將資料來源中的文件內文欄位名稱對應至索引欄位名稱_document_body。所有其他欄位是選用的。

如需要設定的其他重要 JSON 金鑰清單，請參閱[Aurora \(MySQL\) 模板架構](#)。

備註

- Amazon Kendra 檢查更新的內容時，不會追蹤已刪除的資料庫列。
- 資料庫中一列中欄位名稱和值的大小不得超過 400 KB。

- 如果您的資料庫資料來源中有大量資料，並且不想 Amazon Kendra 在第一次同步之後對所有資料庫內容建立索引，則可以選擇僅同步新文件、修改或刪除的文件。
- 最佳作法是提供 Amazon Kendra 唯讀資料庫認證。
- 最佳做法是避免新增包含敏感資料或個人可識別資訊 (PII) 的表格。

Aurora (PostgreSQL)

Aurora 是專為雲端建置的關聯式資料庫管理系統 (RDBMS)。如果您是使用 Aurora 者，則可以使用 Amazon Kendra 對資 Aurora (PostgreSQL) 料來源建立索引。資 Amazon Kendra Aurora (PostgreSQL) 料來源連接器支援 Aurora 1。

您可以使用 [Amazon Kendra 主控台](#) 和 [TemplateConfiguration](#) API 連線 Amazon Kendra 到 Aurora (PostgreSQL) 資料來源。

如需疑難排解資 Amazon Kendra Aurora (PostgreSQL) 料來源連接器，請參閱 [疑難排解資料來](#)。

主題

- [支援的功能](#)
- [必要條件](#)
- [連接說明](#)
- [備註](#)

支援的功能

- 欄位對映
- 使用者內容篩選
- 包含/排除過濾器
- 完整和增量內容同步
- 虛擬私有雲端 (VPC)

必要條件

在您可以用來 Amazon Kendra 為資 Aurora (PostgreSQL) 料來源建立索引之前，請先在 Aurora (PostgreSQL) 和 AWS 帳戶中進行這些變更。

在中Aurora (PostgreSQL) ，請確定您有：

- 記下您的資料庫使用者名稱和密碼。

⚠ Important

最佳作法是提供 Amazon Kendra 唯讀資料庫認證。

- 複製您的資料庫主機 URL、連接埠和執行個體。
- 已勾選的每個文件在您打算用於相同索引的其他資料來源中Aurora (PostgreSQL)和其他資料來源之間都是唯一的。您要用於索引的每個資料來源不得包含跨資料來源的相同文件。文件 ID 對索引來說是全域的，而且每個索引必須是唯一的。

在您的中 AWS 帳戶，請確保您有：

- [建立 Amazon Kendra 索引](#)，如果使用 API，則會記下索引識別碼。
- 為您的[資料來源建立 IAM 角色](#)，如果使用 API，則會記錄 IAM 角色的 ARN。

i Note

如果您變更驗證類型和認證，則必須更新 IAM 角色才能存取正確的 AWS Secrets Manager 密碼 ID。

- 將您的Aurora (PostgreSQL)身份驗證憑據存儲在 AWS Secrets Manager 密鑰中，如果使用 API，則記錄密鑰的 ARN。

i Note

我們建議您定期重新整理或輪換您的認證和密碼。僅為您自己的安全提供必要的訪問級別。我們不建議您跨資料來源以及連接器 1.0 和 2.0 版 (如果適用) 重複使用認證和密碼。

如果您沒有現有的 IAM 角色或密碼，則可以在將Aurora (PostgreSQL)資料來源連線到時使用主控台建立新 IAM 角色和 Secrets Manager 密碼 Amazon Kendra。如果您使用 API，則必須提供現有 IAM 角色和 Secrets Manager 密碼的 ARN，以及索引 ID。

連接說明

若要連線 Amazon Kendra 到 Aurora (PostgreSQL) 資料來源，您必須提供 Aurora (PostgreSQL) 認證的詳細資料，Amazon Kendra 以便能夠存取您的資料。如果您尚未設定「Amazon Kendra 請 Aurora (PostgreSQL) 參閱 [必要條件](#)」。

Console

若要連線 Amazon Kendra 到 Aurora (PostgreSQL)


1. 登入 AWS Management Console 並開啟 [Amazon Kendra 主控台](#)。
2. 在左側導覽窗格中，選擇 [索引]，然後從索引清單中選擇要使用的索引。

Note

您可以選擇在索引設置下配置或編輯您的用戶訪問控制設置。

3. 在 [開始使用] 頁面上，選擇 [新增資料來源]。
4. 在 [新增資料來源] 頁面上，選擇 [Aurora (PostgreSQL) 連接器]，然後選擇 [新增連接器]。如果使用版本 2 (如果適用)，請選擇帶有「V2.0」標籤的 Aurora (PostgreSQL) 連接器。
5. 在 [指定資料來源詳細資訊] 頁面上，輸入下列資訊：
 - a. 在名稱和說明中，對於資料來源名稱 — 輸入資料來源的名稱。您可以包含連字號，但不能包含空格。
 - b. (選擇性) 說明 — 輸入資料來源的選用說明。
 - c. 在預設語言中 — 選擇一種語言來篩選索引的文件。除非另有指定，否則語言預設為英文。文件中繼資料中指定的語言會覆寫選取的語言。
 - d. 在「標籤」中，針對「新增標籤」 — 包含可選標籤以搜尋和篩選資源或追蹤 AWS 成本。
 - e. 選擇下一步。
6. 在 [定義存取權和安全性] 頁面上，輸入下列資訊：
 - a. 在來源中，輸入下列資訊：
 - b. 主機 — 輸入資料庫主機 URL，例如：`http://instance URL.region.rds.amazonaws.com`。
 - c. 連接埠 — 輸入資料庫連接埠，例如 5432。
 - d. 執行處理 — 例如，輸入資料庫執行處理 `postgres`。
 - e. 啟用 SSL 憑證位置 — 選擇此選項可輸入 SSL 憑證檔案的 Amazon S3 路徑。

- f. 在驗證中 — 輸入下列資訊：
 - AWS Secrets Manager 祕密 — 選擇現有密碼或建立新 Secrets Manager 密碼來儲存您的 Aurora (PostgreSQL) 驗證認證。如果您選擇建立新密碼，則會開啟一個 AWS Secrets Manager 密碼視窗。
 - A. 在「建立 AWS Secrets Manager 密碼視窗」中輸入下列資訊：
 - I. 秘密名稱 — 您秘密的名稱。前綴 'AmazonKendraAurora (PostgreSQL)-' 會自動添加到您的密碼名稱中。
 - II. 對於資料庫使用者名稱和密碼 — 輸入您從資料庫複製的驗證認證值。
 - B. 選擇儲存。
- g. V@@@ irtual Private Cloud (VPC) (VPC) — 您可以選擇使用 VPC。如果是這樣，您必須新增子網路和 VPC 安全性群組。
- h. IAM role — 選擇現有 IAM 角色或建立新 IAM 角色以存取存放庫認證和索引內容。

 Note

IAM 用於索引的角色不能用於資料來源。如果您不確定索引或常見問題集是否使用現有角色，請選擇 [建立新角色] 以避免發生錯誤。

- i. 選擇下一步。
7. 在 [設定同步設定] 頁面上，輸入下列資訊：
 - a. 在同步範圍中，從下列選項中選擇：
 - SQL 查詢 — 輸入 SQL 查詢陳述式，例如選取和聯結作業。SQL 查詢必須小於 32 KB 的 SQL 查詢小於 32 KB，且不得包含任何分號 (;)。Amazon Kendra 會編目符合您查詢的所有資料庫內容。
 - 主索引鍵欄 — 提供資料庫表格的主索引鍵。這標識數據庫中的一個表。
 - 標題欄 — 提供資料庫表格中文件標題欄的名稱。
 - 主體欄 — 提供資料庫表格中文件主體欄的名稱。
 - b. 在 [其他設定 — 選用] 中，從下列選項中選擇以同步特定內容，而非同步所有檔案：
 - 變更偵測欄 — 輸入 Amazon Kendra 將用來偵測內容變更的欄名稱。Amazon Kendra 當這些資料行中有任何變更時，會重新建立內容的索引。
 - 使用者 ID 欄 — 輸入包含允許存取內容的使用者 ID 的欄名稱。

- 群組欄 — 輸入包含允許存取內容之群組的欄名稱。
 - 來源 URL 欄 — 輸入包含要編製索引之來源 URL 的資料欄名稱。
 - 時間戳記欄 — 輸入包含時間戳記的欄名稱。Amazon Kendra 使用時間戳記資訊偵測內容中的變更，並僅同步變更的內容。
 - [時區] 欄 — 輸入資料欄的名稱，其中包含要編目之內容的時區。
 - 時間戳記格式 — 輸入包含時間戳記格式的欄名稱，可用來偵測內容變更並重新同步處理內容。
- c. 同步模式 — 選擇資料來源內容變更時要如何更新索引。當您第一次將資料來源同 Amazon Kendra 步處理時，依預設會檢索所有內容並建立索引。如果初始同步失敗，您必須執行資料的完整同步處理，即使您沒有選擇完整同步作為同步模式選項。
- 完全同步：新鮮索引所有內容，並在每次資料來源與索引同步時取代現有內容。
 - 新增、修改的同步：每次資料來源與索引同步時，僅對新內容和已修改的內容建立索引。Amazon Kendra 可以使用資料來源的機制來追蹤內容變更，並為上次同步後變更的內容建立索引。
 - 新增、修改、刪除的同步：每次資料來源與索引同步時，僅對新內容、已修改和刪除的內容建立索引。Amazon Kendra 可以使用資料來源的機制來追蹤內容變更，並為上次同步後變更的內容建立索引。
- d. 在同步執行排程中，對於頻率 — 與資料來源同步的頻率。Amazon Kendra
- e. 選擇下一步。
8. 在 [設定欄位對映] 頁面上，輸入下列資訊：
- a. 從產生的預設資料來源欄位中選取您要對應至 Amazon Kendra 索引的文件 ID、文件標題和來源 URL。
 - b. 新增欄位 — 新增自訂資料來源欄位，以建立要對映的索引欄位名稱和欄位資料類型。
 - c. 選擇下一步。
9. 在 [檢閱並建立] 頁面上，檢查您輸入的資訊是否正確，然後選取 [新增資料來源]。您也可以從此頁面選擇編輯您的資訊。成功新增資料來源後，您的資料來源將顯示在 [資料來源] 頁面上。

API

若要連線 Amazon Kendra 到 Aurora (PostgreSQL)

您必須使用 [TemplateConfiguration](#) API 指定下列項目：

- 資料來源 — 指定使用 [TemplateConfiguration](#) JSON 結構定義 JDBC 時的資料來源類型。同時將資料來源指定為呼叫 [CreateDataSource](#) API TEMPLATE 時的方式。
- 資料庫類型 — 您必須將資料庫類型指定為 postgresql。
- SQL 查詢 — 指定 SQL 查詢陳述式，例如 SELECT 和 JOIN 作業。SQL 查詢必須小於 32 KB。Amazon Kendra 會編目符合您查詢的所有資料庫內容。
- 同步模式 — 指定資料來源內容變更時 Amazon Kendra 應如何更新索引。當您第一次將資料來源同 Amazon Kendra 步處理時，依預設會檢索所有內容並建立索引。如果初始同步失敗，您必須執行資料的完整同步處理，即使您沒有選擇完整同步作為同步模式選項。您可以選擇：
 - FORCED_FULL_CRAWL 新建索引所有內容，並在每次資料來源與索引同步時取代現有內容。
 - FULL_CRAWL，以在每次資料來源與索引同步時，僅對新的、修改的和刪除的內容建立索引。Amazon Kendra 可以使用資料來源的機制來追蹤內容變更，並為上次同步後變更的內容建立索引。
 - CHANGE_LOG 每次資料來源與索引同步時，僅對新內容和修改的內容建立索引。Amazon Kendra 可以使用資料來源的機制來追蹤內容變更，並為上次同步後變更的內容建立索引。
- 秘密 Amazon 資源名稱 (ARN) — 提供包含您在帳戶中建立的身份驗證登入資料的 Secrets Manager 密碼的 Amazon 資源名稱 (ARN)。Aurora (PostgreSQL) 密碼會以下列金鑰儲存在 JSON 結構中：

```
{
  "user name": "database user name",
  "password": "password"
}
```


Note

我們建議您定期重新整理或輪換您的認證和密碼。僅為您自己的安全提供必要的訪問級別。我們不建議您跨資料來源以及連接器 1.0 和 2.0 版 (如果適用) 重複使用認證和密碼。

- IAM role — 指定 RoleArn 何時呼叫 CreateDataSource 以提供具有存取 Secrets Manager 密碼之權限的 IAM 角色，以及呼叫 Aurora (PostgreSQL) 連接器和 Amazon Kendra 所需公用 API 的時間。有關詳情，請參閱 [Aurora \(PostgreSQL\) 料來源的 IAM 角色](#)。

您還可以添加以下可選功能：

- V@@ irtual Private Cloud (VPC) — 指定您撥打電話的VpcConfiguration時間。CreateDataSource如需詳細資訊，請參閱 [配置 Amazon Kendra 為使用 Amazon VPC](#)。
- 包含和排除篩選器 — 您可以指定是否要使用使用者 ID、群組、來源 URL、時間戳記和時區來包含特定內容。
- 使用者前後關聯篩選與存取控制 — Amazon Kendra 探索文件的存取控制清單 (ACL) (如果您有文件的 ACL)。ACL 資訊可用來根據使用者或使用者對文件的群組存取權來篩選搜尋結果。如需詳細資訊，請參閱[使用者內容篩選](#)。
- 欄位對映 — 選擇將資料來源 (PostgreSQL) 欄位對映至 Amazon Kendra 索引欄位。如需詳細資訊，請參閱[映射資料來源欄位](#)。

 Note

您的文件需要文件內文欄位或文件內文對等項目，才能搜尋您的文件。Amazon Kendra 您必須將資料來源中的文件內文欄位名稱對應至索引欄位名稱_document_body。所有其他欄位是選用的。

如需要設定的其他重要 JSON 金鑰清單，請參閱[Aurora 模板模板架構](#)。

備註

- Amazon Kendra 檢查更新的內容時，不會追蹤已刪除的資料庫列。
- 資料庫中一列中欄位名稱和值的大小不得超過 400 KB。
- 如果您的資料庫資料來源中有大量資料，並且不想 Amazon Kendra 在第一次同步之後對所有資料庫內容建立索引，則可以選擇僅同步新文件、修改或刪除的文件。
- 最佳作法是提供 Amazon Kendra 唯讀資料庫認證。
- 最佳做法是避免新增包含敏感資料或個人可識別資訊 (PII) 的表格。

Amazon FSx (視窗)

Amazon FSx (Windows) 是全受管理的雲端檔案伺服器系統，提供共用儲存功能。如果您是 Amazon FSx (Windows) 使用者，您可以使用 Amazon Kendra 來為您的 Amazon FSx (Windows) 資料來源建立索引。

Note

Amazon Kendra 現在支援升級的 Amazon FSx (視窗) 連接器。

主機已自動為您升級。您在主控台上建立的任何新連接器都會使用升級的架構。如果您使用 API，您現在必須使用 [TemplateConfiguration](#) 物件而非 FSxConfiguration 物件來設定連接器。

使用舊版主控台和 API 架構設定的連接器將繼續如設定般運作。但是，您將無法編輯或更新它們。如果您要編輯或更新連接器組態，您必須建立新的連接器。

我們建議您將連接器工作流程移轉至升級版本。使用舊架構設定的連接器 Support 排程於 2024 年 6 月結束。

您可以使用 [Amazon Kendra 主控台](#) 或 [TemplateConfiguration API](#) 連線 Amazon Kendra 到您的 Amazon FSx (Windows) 資料來源。

如需對 Amazon Kendra Amazon FSx (Windows) 資料來源連接器進行疑難排解，請參閱 [疑難排解資料](#) 來。

主題

- [支援的功能](#)
- [必要條件](#)
- [連接說明](#)
- [進一步了解](#)

支援的功能

Amazon Kendra Amazon FSx (Windows) 資料來源連接器支援下列功能：

- 欄位對映
- 使用者存取控制
- 使用者身分檢索
- 包含和排除過濾器
- 完整和增量內容同步
- 虛擬私有雲端 (VPC)

必要條件

在您可以使 Amazon Kendra 用您的 Amazon FSx (Windows) 資料來源建立索引之前，請先檢查您的 Amazon FSx (Windows) 和 AWS 帳戶。

對於 Amazon FSx (視窗)，請確保您具有：

- 使用讀取和掛載權限設定 Amazon FSx (Windows)。
- 記下您的檔案系統 ID。您可以在 Amazon FSx (Windows) 主控台的 [檔案系統] 儀表板上找到您的檔案系統識別碼。
- 使用您的 Amazon FSx (Windows) 檔案系統所 Amazon VPC 在位置設定虛擬私有雲。
- 記下您的 Active Directory 使用者帳戶的 Amazon FSx (Windows) 驗證身分證明。這包括您的使用中目錄使用者名稱以及您的 DNS 網域名稱 (例如 user@corp.example.com) 和密碼。

Note

僅使用連接器運作所需的必要認證。請勿使用網域管理員等特權憑證。

Note

我們建議您定期重新整理或輪換您的認證和密碼。僅為您自己的安全提供必要的訪問級別。我們不建議您跨資料來源以及連接器 1.0 和 2.0 版 (如果適用) 重複使用認證和密碼。

- 核取每個文件在 Amazon FSx (Windows) 和您打算用於相同索引的其他資料來源中都是唯一的。您要用於索引的每個資料來源不得包含跨資料來源的相同文件。文件 ID 對索引來說是全域的，而且每個索引必須是唯一的。

在你的 AWS 帳戶，確保你有：

- [建立 Amazon Kendra 索引](#)，如果使用 API，則會記下索引 ID。
- 為您的[資料來源建立 IAM 角色](#)，如果使用 API，則會記錄 IAM 角色的 ARN。

Note

如果您變更驗證類型和認證，則必須更新 IAM 角色才能存取正確的 AWS Secrets Manager 密碼 ID。

- 將您的 Amazon FSx (Windows) 驗證認證儲存在 AWS Secrets Manager 密碼中，如果使用 API，則會記下密碼的 ARN。

Note

我們建議您定期重新整理或輪換您的認證和密碼。僅為您自己的安全提供必要的訪問級別。我們不建議您跨資料來源以及連接器 1.0 和 2.0 版 (如果適用) 重複使用認證和密碼。

如果您沒有現有的 IAM 角色或密碼，則可以在將 Amazon FSx (Windows) 資料來源連線至時使用主控台建立新 IAM 角色和 Secrets Manager 密碼 Amazon Kendra。如果您使用 API，則必須提供現有 IAM 角色和 Secrets Manager 密碼的 ARN，以及索引 ID。

連接說明

若要連線 Amazon Kendra 到您的 Amazon FSx (Windows) 資料來源，您必須提供 Amazon FSx (Windows) 資料來源的必要詳細資料，Amazon Kendra 以便能夠存取您的資料。如果您尚未為 Amazon FSx (Windows) 設定 Amazon Kendra，請參閱[必要條件](#)。

Console

若要連線 Amazon Kendra 到您的 Amazon FSx (視窗) 檔案系統

1. 登入 AWS Management Console 並開啟[Amazon Kendra 主控台](#)。
2. 在左側導覽窗格中，選擇 [索引]，然後從索引清單中選擇要使用的索引。

Note

您可以選擇在索引設置下配置或編輯您的用戶訪問控制設置。


3. 在 [開始使用] 頁面上，選擇 [新增資料來源]。
4. 在 [新增資料來源] 頁面上，選擇 [Amazon FSx (Windows) 連接器]，然後選擇 [新增連接器]。如果使用第 2 版 (如果適用)，請選擇具有「V2.0」標籤的 Amazon FSx (Windows) 連接器。
5. 在 [指定資料來源詳細資訊] 頁面上，輸入下列資訊：
 - a. 在名稱和說明中，對於資料來源名稱 — 輸入資料來源的名稱。您可以包含連字號，但不能包含空格。
 - b. (選擇性) 說明 — 輸入資料來源的選用說明。

- c. 在預設語言中 — 選擇一種語言來篩選索引的文件。除非另有指定，否則語言預設為英文。文件中繼資料中指定的語言會覆寫選取的語言。
 - d. 在「標籤」中，針對「新增標籤」 — 包含可選標籤以搜尋和篩選資源或追蹤 AWS 成本。
 - e. 選擇下一步。
6. 在 [定義存取和安全性] 頁面上，輸入下列資訊：
- a. Amazon FSx (Windows) 檔案系統識別碼 — 從下拉式清單中選取您現有的檔案系統識別碼，並從 Amazon FSx (Windows) 擷取。或者，建立 [Amazon FSx \(視窗\) 檔案系統](#)。您可以在 Amazon FSx (Windows) 主控台的 [檔案系統] 儀表板上找到您的檔案系統識別碼。
 - b. 授權 — 開啟或關閉文件的存取控制清單 (ACL) 資訊 (如果您有 ACL)，且想要將其用於存取控制。ACL 會指定使用者和群組可存取的文件。ACL 資訊可用來根據使用者或使用者對文件的群組存取權來篩選搜尋結果。如需詳細資訊，請參閱[使用者內容篩選](#)。
 - c. 驗證 — 選擇現有 AWS Secrets Manager 密碼，或建立新密碼來儲存您的檔案系統認證。如果您選擇建立新密碼，則會開啟一個 AWS Secrets Manager 密碼視窗。

提供一個密碼，以儲存您的使用者名稱和密碼的驗證憑證。使用者名稱必須包含您的 DNS 網域名稱。例如，user@corp.example.com。

保存並添加您的秘密。

- d. Virtual Private Cloud (VPC) — 您必須選取您的 Amazon FSx (Windows) 所 Amazon VPC 在的位置。您可以包括 VPC 子網路和安全性群組。請參閱[配置 Amazon VPC](#)。
- e. IAM role — 選擇現有 IAM 角色或建立新 IAM 角色以存取存放庫認證和索引內容。

 Note

IAM 用於索引的角色不能用於資料來源。如果您不確定索引或常見問題集是否使用現有角色，請選擇 [建立新角色] 以避免發生錯誤。

- f. 選擇下一步。
7. 在 [設定同步設定] 頁面上，輸入下列資訊：
- a. 同步範圍，正則表達式模式-添加正則表達式模式以包含或排除某些文件。
 - b. 同步模式 — 選擇資料來源內容變更時要如何更新索引。當您第一次將資料來源同 Amazon Kendra 步處理時，依預設會檢索所有內容並建立索引。如果初始同步失敗，您必須執行資料的完整同步處理，即使您沒有選擇完整同步作為同步模式選項。
 - 完全同步：新鮮索引所有內容，並在每次資料來源與索引同步時取代現有內容。

- 新增、修改、刪除的同步：每次資料來源與索引同步時，僅對新內容、已修改和刪除的內容建立索引。Amazon Kendra 可以使用資料來源的機制來追蹤內容變更，並為上次同步後變更的內容建立索引。
 - c. 同步執行排程 — 對於「頻率」，請選擇同步資料來源內容並更新索引的頻率。
 - d. 選擇下一步。
8. 在 [設定欄位對映] 頁面上，輸入下列資訊：
- a. 從檔案 Amazon Kendra 產生的預設欄位中選取您要對應至索引的檔案。若要新增自訂資料來源欄位，請建立要對映的索引欄位名稱和欄位資料類型。
 - b. 選擇下一步。
9. 在 [檢閱並建立] 頁面上，檢查您輸入的資訊是否正確，然後選取 [新增資料來源]。您也可以從此頁面選擇編輯您的資訊。成功新增資料來源後，您的資料來源將顯示在 [資料來源] 頁面上。

API

若要連線 Amazon Kendra 到您的 Amazon FSx (視窗) 檔案系統

您必須使用 [TemplateConfiguration](#) API 指定 [資料來源結構描述](#) 的 JSON。您必須提供以下信息：

- 資料來源 — 指定使用 [TemplateConfiguration](#) JSON 結構定義 FSX 時的資料來源類型。同時將資料來源指定為呼叫 [CreateDataSource](#) API TEMPLATE 時的方式。
- 檔案系統識別碼 - Amazon FSx (Windows) 檔案系統的識別碼。您可以在 Amazon FSx (Windows) 主控台的 [檔案系統] 儀表板上找到您的檔案系統識別碼。
- 檔案系統類型 — 將檔案系統類型指定為 WINDOWS。
- Virtual Private Cloud (VPC) — 指定您撥打電話的 VpcConfiguration 時間。CreateDataSource 如需詳細資訊，請參閱 [配置 Amazon Kendra 為使用 Amazon VPC](#)。

Note

您必須選取您 Amazon VPC 的 Amazon FSx (Windows) 所在的位置。您可以包括 VPC 子網路和安全性群組。

- 同步模式 — 指定資料來源內容變更時 Amazon Kendra 應如何更新索引。當您第一次將資料來源同 Amazon Kendra 步處理時，依預設會檢索所有內容並建立索引。如果初始同步失敗，您必須執行資料的完整同步處理，即使您沒有選擇完整同步作為同步模式選項。您可以選擇：
 - FORCED_FULL_CRAWL 新建索引所有內容，並在每次資料來源與索引同步時取代現有內容。

- **FULL_CRAWL**，以在每次資料來源與索引同步時，僅對新的、修改的和刪除的內容建立索引。Amazon Kendra 可以使用資料來源的機制來追蹤內容變更，並為上次同步後變更的內容建立索引。
- **識別爬行者程式** — 指定是否要開啟身分識別爬行 Amazon Kendra 者程式。識別爬行者程式會使用文件的存取控制清單 (ACL) 資訊，根據使用者或使用者對文件的群組存取權來篩選搜尋結果。如果您有文件的 ACL 並選擇使用 ACL，您也可以選擇開啟的身分識別爬行者程式，以設定搜尋結果的使用者環境定義篩選。Amazon Kendra 否則，如果關閉身分搜索器，則可以公開搜索所有文檔。如果您想要對文件使用存取控制，且身分識別編目程式已關閉，您也可以使用 [PutPrincipalMapping](#) API 來上傳使用者和群組存取資訊以進行使用者內容篩選。
- **秘密 Amazon 資源名稱 (ARN)** — 提供包含您 (Windows) 帳戶身份驗證登入資料的 Secrets Manager 密碼的 Amazon 資源名稱 Amazon FSx (ARN)。密碼會以下列金鑰儲存在 JSON 結構中：

```
{
  "username": "user@corp.example.com",
  "password": "password"
}
```

- **IAM 角色** — 指定 RoleArn 何時呼叫 CreateDataSource 以提供具有存取 Secrets Manager 密碼的權限的 IAM 角色，以及呼叫 Amazon FSx (Windows) 連接器和 Amazon Kendra 所需公用 API 的時間。如需詳細資訊，請參閱 [Amazon FSx \(Windows\) 資料來源的 IAM 角色](#)。

您還可以添加以下可選功能：

- **包含和排除篩選器** — 指定要包含還是排除某些檔案。

Note

大多數資料來源使用規則運算式模式，這些模式是稱為篩選器的包含或排除模式。如果您指定包含篩選器，則只有符合包含項目篩選器的內容會編製索引。不符合包含篩選器的任何文件都不會建立索引。如果您指定包含和排除篩選器，符合排除篩選器的文件將不會建立索引，即使它們符合包含篩選器也是如此。

- **存取控制清單 (ACL)** — 指定是否要編目文件的 ACL 資訊 (如果您有 ACL 並且想要將其用於存取控制)。ACL 會指定使用者和群組可存取的文件。ACL 資訊可用來根據使用者或使用者對文件的群組存取權來篩選搜尋結果。如需詳細資訊，請參閱 [使用者內容篩選](#)。

Note

若要測試使用者的使用者內容篩選，您必須在發出查詢時將 DNS 網域名稱納入使用者名稱中。您必須具有作用中目錄網域的系統管理權限。您也可以針對群組名稱測試使用者內容篩選。

- 欄位對映 — 選擇將您的 Amazon FSx (Windows) 資料來源欄位對映至 Amazon Kendra 索引欄位。如需詳細資訊，請參閱[映射資料來源欄位](#)。

Note

您的文件需要文件內文欄位或文件內文對等項目，才能搜尋您的文件。Amazon Kendra 您必須將資料來源中的文件內文欄位名稱對應至索引欄位名稱_document_body。所有其他欄位是選用的。

如需要設定的其他重要 JSON 金鑰清單，請參閱 [Amazon FSx \(Windows\) 範本結構描述](#)。

進一步了解

若要深入瞭解 Amazon Kendra 與 Amazon FSx (Windows) 資料來源整合的相關資訊，請參閱：

- [使用適用於 Amazon FSx \(Windows\) 的 Amazon Kendra 連接器，在 Windows 檔案系統上安全地搜尋非結構化資料](#)。Windows File Server

Amazon FSx (NetApp ONTAP)

Amazon FSx (NetApp ONTAP) 是全受管的雲端檔案伺服器系統，提供共用儲存功能。如果您是 Amazon FSx (NetApp ONTAP) 使用者，則可以用 Amazon Kendra 來為 Amazon FSx (NetApp ONTAP) 資料來源建立索引。

您可以使用[Amazon Kendra 主控台](#)或 [TemplateConfiguration](#) API 連線 Amazon Kendra 至您的 Amazon FSx (NetApp ONTAP) 資料來源。

如需疑難排解 Amazon Kendra Amazon FSx (NetApp ONTAP) 資料來源連接器，請參閱[疑難排解資料](#)來。

主題

- [支援的功能](#)
- [必要條件](#)
- [連接說明](#)

支援的功能

Amazon Kendra Amazon FSx (NetApp ONTAP) 資料來源連接器支援下列功能：

- 欄位對映
- 使用者存取控制
- 包含和排除過濾器
- 完整和增量內容同步
- 虛擬私有雲端 (VPC)

必要條件

在您可以使 Amazon Kendra 用索引 Amazon FSx (NetApp ONTAP) 資料來源之前，請先檢查您的 Amazon FSx (NetApp ONTAP) 和 AWS 帳戶

對於 Amazon FSx (NetApp ONTAP)，請確定您有：

- 使用讀取和掛載權限設定 Amazon FSx (NetApp ONTAP)。
- 記下您的檔案系統 ID。您可以在 Amazon FSx (NetApp ONTAP) 主控台的 [檔案系統] 儀表板上找到您的檔案系統 ID。
- 記下與檔案系統搭配使用的儲存區虛擬機器 (SVM) 識別碼。您可以移至 Amazon FSx (NetApp ONTAP) 主控台內的 [檔案系統] 儀表板，選取您的檔案系統 ID，然後選取 [儲存區虛擬機器]，以尋找您的 SVM ID。
- 使用您 Amazon FSx (NetApp ONTAP) 檔案系統所 Amazon VPC 在的位置設定虛擬私有雲。
- 記下 Active Directory 使用者帳戶的 Amazon FSx (NetApp ONTAP) 驗證憑證。這包括您的使用中目錄使用者名稱以及您的 DNS 網域名稱 (例如 user@corp.example.com) 和密碼。如果您為 (NetApp ONTAP) 檔案系統使用網路檔案系統 Amazon FSx (NFS) 通訊協定，則驗證認證會包含左側 ID、右側 ID 和預先共用金鑰。

Note

僅使用連接器運作所需的必要認證。請勿使用網域管理員等特權憑證。

Note

我們建議您定期重新整理或輪換您的認證和密碼。僅為您自己的安全提供必要的訪問級別。我們不建議您跨資料來源以及連接器 1.0 和 2.0 版 (如果適用) 重複使用認證和密碼。

- 核取每個文件在 Amazon FSx (NetApp ONTAP) 中，以及您打算用於相同索引的其他資料來源之間是唯一的。您要用於索引的每個資料來源不得包含跨資料來源的相同文件。文件 ID 對索引來說是全域的，而且每個索引必須是唯一的。

在您的中 AWS 帳戶，請確保您有：

- [建立 Amazon Kendra 索引](#)，如果使用 API，則會記下索引識別碼。
- 為您的[資料來源建立 IAM 角色](#)，如果使用 API，則會記錄 IAM 角色的 ARN。

Note

如果您變更驗證類型和認證，則必須更新 IAM 角色才能存取正確的 AWS Secrets Manager 密碼 ID。

- 將您的 Amazon FSx (NetApp ONTAP) 身份驗證憑據存儲在 AWS Secrets Manager 密鑰中，並且如果使用 API，則記錄密鑰的 ARN。

Note

我們建議您定期重新整理或輪換您的認證和密碼。僅為您自己的安全提供必要的訪問級別。我們不建議您跨資料來源以及連接器 1.0 和 2.0 版 (如果適用) 重複使用認證和密碼。

如果您沒有現有的 IAM 角色或密碼，則可以在將 Amazon FSx (NetApp ONTAP) 資料來源連線到時，使用主控台建立新 IAM 角色和 Secrets Manager 密碼。Amazon Kendra 如果您使用 API，則必須提供現有 IAM 角色和 Secrets Manager 密碼的 ARN，以及索引 ID。

連接說明

若要連線 Amazon Kendra 至您的 Amazon FSx (NetApp ONTAP) 資料來源，您必須提供 Amazon FSx (NetApp ONTAP) 資料來源的必要詳細資訊，Amazon Kendra 以便能夠存取您的資料。如果您尚未設定 Amazon FSx (NetApp ONTAP) Amazon Kendra，請參閱[必要條件](#)。

Console

若要連線 Amazon Kendra 至您的 Amazon FSx (NetApp ONTAP) 檔案系統

1. 登入 AWS Management Console 並開啟[Amazon Kendra 主控台](#)。
2. 在左側導覽窗格中，選擇 [索引]，然後從索引清單中選擇要使用的索引。

Note

您可以選擇在索引設置下配置或編輯您的用戶訪問控制設置。

3. 在 [開始使用] 頁面上，選擇 [新增資料來源]。
4. 在 [新增資料來源] 頁面上，選擇 [Amazon FSx (NetApp ONTAP) 連接器]，然後選擇 [新增連接器]。如果使用第 2 版 (如果適用)，請選擇帶有「V2.0」標籤的 Amazon FSx (NetApp ONTAP) 連接器。
5. 在 [指定資料來源詳細資訊] 頁面上，輸入下列資訊：
 - a. 在名稱和說明中，對於資料來源名稱 — 輸入資料來源的名稱。您可以包含連字號，但不能包含空格。
 - b. (選擇性) 說明 — 輸入資料來源的選用說明。
 - c. 在預設語言中 — 選擇一種語言來篩選索引的文件。除非另有指定，否則語言預設為英文。文件中繼資料中指定的語言會覆寫選取的語言。
 - d. 在「標籤」中，針對「新增標籤」— 包含可選標籤以搜尋和篩選資源或追蹤 AWS 成本。
 - e. 選擇下一步。
6. 在 [定義存取權和安全性] 頁面上，輸入下列資訊：
 - a. 來源 — 提供您的檔案系統資訊。
 - 檔案系統通訊協定 — 選擇 Amazon FSx (NetApp ONTAP) 檔案系統的通訊協定。您可以選擇一般網際網路檔案系統 (CIFS) 通訊協定或 Linux 的網路檔案系統 (NFS) 通訊協定。


- Amazon FSx (NetApp ONTAP) 檔案系統 ID — 從下拉式選單中選取您現有的檔案系統 ID，從 Amazon FSx (NetApp ONTAP) 擷取。或者，建立 [Amazon FSx \(NetApp ONTAP\) 檔案系統](#)。您可以在 Amazon FSx (NetApp ONTAP) 主控台的 [檔案系統] 儀表板上找到您的檔案系統 ID。
 - SVM 識別碼 (NetApp ONTAP 僅適用於 Amazon FSx (NetApp ONTAP)) — 提供您 Amazon FSx (ONTAP) 的儲存區虛擬機器 (SVM) 識別碼。NetApp NetApp ONTAP 您可以前往 Amazon FSx (NetApp ONTAP) 主控台內的 [檔案系統] 儀表板，選取您的檔案系統 ID，然後選取 [儲存空間虛擬機器]，以尋找您的 SVM ID。
- b. 授權 — 開啟或關閉文件的存取控制清單 (ACL) 資訊 (如果您有 ACL)，且想要將其用於存取控制。ACL 會指定使用者和群組可存取的文件。ACL 資訊可用來根據使用者或使用者對文件的群組存取權來篩選搜尋結果。如需詳細資訊，請參閱 [使用者內容篩選](#)。
 - c. 驗證 — 選擇現有 AWS Secrets Manager 密碼，或建立新密碼來儲存您的檔案系統認證。如果您選擇建立新密碼，則會開啟一個 AWS Secrets Manager 密碼視窗。

提供一個密碼，以儲存您的使用者名稱和密碼的驗證憑證。使用者名稱必須包含您的 DNS 網域名稱。例如，user@corp.example.com。

如果您的 Amazon FSx (NetApp ONTAP) 檔案系統使用 NFS 通訊協定，請提供一個密碼來儲存您的左 ID、正確 ID 和預先共用金鑰的驗證憑證。

保存並添加您的秘密。

- d. V@@@ irtual Private Cloud (VPC) (VPC) — 您必須選取 Amazon FSx (NetApp ONTAP) 所 Amazon VPC 在的位置。您可以包括 VPC 子網路和安全性群組。請參閱 [配置 Amazon VPC](#)。
- e. IAM role — 選擇現有 IAM 角色或建立新 IAM 角色以存取存放庫認證和索引內容。

 Note

IAM 用於索引的角色不能用於資料來源。如果您不確定索引或常見問題集是否使用現有角色，請選擇 [建立新角色] 以避免發生錯誤。

- f. 選擇下一步。
7. 在 [設定同步設定] 頁面上，輸入下列資訊：
 - a. 同步範圍，正則表達式模式-添加正則表達式模式以包含或排除某些文件。

- b. 同步模式 — 選擇資料來源內容變更時要如何更新索引。當您第一次將資料來源同 Amazon Kendra 步處理時，依預設會檢索所有內容並建立索引。如果初始同步失敗，您必須執行資料的完整同步處理，即使您沒有選擇完整同步作為同步模式選項。
 - 完全同步：新鮮索引所有內容，並在每次資料來源與索引同步時取代現有內容。
 - 新增、修改、刪除的同步：每次資料來源與索引同步時，僅對新內容、已修改和刪除的內容建立索引。Amazon Kendra 可以使用資料來源的機制來追蹤內容變更，並為上次同步後變更的內容建立索引。
 - c. 同步執行排程 — 對於「頻率」，請選擇同步資料來源內容並更新索引的頻率。
 - d. 選擇下一步。
8. 在 [設定欄位對映] 頁面上，輸入下列資訊：
- a. 從檔案 Amazon Kendra 產生的預設欄位中選取您要對應至索引的檔案。若要新增自訂資料來源欄位，請建立要對映的索引欄位名稱和欄位資料類型。
 - b. 選擇下一步。
9. 在 [檢閱並建立] 頁面上，檢查您輸入的資訊是否正確，然後選取 [新增資料來源]。您也可以從此頁面選擇編輯您的資訊。成功新增資料來源後，您的資料來源將顯示在 [資料來源] 頁面上。

API

若要連線 Amazon Kendra 至您的 Amazon FSx (NetApp ONTAP) 檔案系統

您必須使用 [TemplateConfiguration](#) API 指定 [資料來源結構描述](#) 的 JSON。您必須提供以下信息：

- 資料來源 — 指定使用 [TemplateConfiguration](#) JSON 結構定義 FSX ONTAP 時的資料來源類型。同時指定呼叫 [CreateDataSource](#) API TEMPLATE 時的資料來源。
- 檔案系統 ID — Amazon FSx (NetApp ONTAP) 檔案系統的識別元。您可以在 Amazon FSx (NetApp ONTAP) 主控台的 [檔案系統] 儀表板上找到您的檔案系統 ID。
- SVM 識別碼 — 與檔案系統搭配使用的儲存區虛擬機器 (SVM) 識別碼。您可以移至 Amazon FSx (NetApp ONTAP) 主控台內的 [檔案系統] 儀表板，選取您的檔案系統 ID，然後選取 [儲存區虛擬機器]，以尋找您的 SVM ID。
- 通訊協定類型 — 指定您是使用 Linux 的通用網際網路檔案系統 (CIFS) 通訊協定，還是使用網路檔案系統 (NFS) 通訊協定。
- 檔案系統類型 — 將檔案系統類型指定為其 FSX ONTAP 中一種。
- V@@@rtual Private Cloud (VPC) — 指定您撥打電話的 VpcConfiguration 時間。CreateDataSource 如需詳細資訊，請參閱 [配置 Amazon Kendra 為使用 Amazon VPC](#)。

Note

您必須選取您 Amazon VPC 的 Amazon FSx (NetApp ONTAP) 所在的位置。您可以包括 VPC 子網路和安全性群組。

- 秘密 Amazon 資源名稱 (ARN) — 提供包含您 (NetApp ONTAP) 帳戶身份驗證登入資料的 Secrets Manager 密碼的 Amazon 資源名稱 Amazon FSx (ARN)。密碼會以下列金鑰儲存在 JSON 結構中：

```
{
  "username": "user@corp.example.com",
  "password": "password"
}
```

如果您為 Amazon FSx (NetApp ONTAP) 檔案系統使用 NFS 通訊協定，密碼會以下列金鑰儲存在 JSON 結構中：

```
{
  "leftId": "left ID",
  "rightId": "right ID",
  "preSharedKey": "pre-shared key"
}
```

- IAM role — 指定 RoleArn 何時呼叫 CreateDataSource 以提供具有存取 Secrets Manager 密碼之權限的 IAM 角色，以及呼叫 Amazon FSx (NetApp ONTAP) 連接器和所需公用 API 的時間。Amazon Kendra 如需詳細資訊，請參閱 [Amazon FSx \(NetApp ONTAP\) 資料來源的 IAM 角色](#)。

您還可以添加以下可選功能：

- 同步模式 — 指定資料來源內容變更時 Amazon Kendra 應如何更新索引。當您第一次將資料來源同 Amazon Kendra 步處理時，依預設會檢索所有內容並建立索引。如果初始同步失敗，您必須執行資料的完整同步處理，即使您沒有選擇完整同步作為同步模式選項。您可以選擇：
 - FORCED_FULL_CRAWL 新建索引所有內容，並在每次資料來源與索引同步時取代現有內容。
 - FULL_CRAWL，以在每次資料來源與索引同步時，僅對新的、修改的和刪除的內容建立索引。Amazon Kendra 可以使用資料來源的機制來追蹤內容變更，並為上次同步後變更的內容建立索引。
- 包含和排除篩選器 — 指定要包含還是排除某些檔案。

Note

大多數資料來源使用規則運算式模式，這些模式是稱為篩選器的包含或排除模式。如果您指定包含篩選器，則只有符合包含項目篩選器的內容會編製索引。不符合包含篩選器的任何文件都不會建立索引。如果您指定包含和排除篩選器，符合排除篩選器的文件將不會建立索引，即使它們符合包含篩選器也是如此。

- 存取控制清單 (ACL) — 指定是否要編目文件的 ACL 資訊 (如果您有 ACL 並且想要將其用於存取控制)。ACL 會指定使用者和群組可存取的文件。ACL 資訊可用來根據使用者或使用者對文件的群組存取權來篩選搜尋結果。如需詳細資訊，請參閱[使用者內容篩選](#)。

Note

若要測試使用者的使用者內容篩選，當您發出查詢時，您必須將 DNS 網域名稱納入使用者名稱中。您必須具有作用中目錄網域的系統管理權限。您也可以針對群組名稱測試使用者內容篩選。

- 欄位對映 — 選擇將 Amazon FSx (NetApp ONTAP) 資料來源欄位對映至 Amazon Kendra 索引欄位。如需詳細資訊，請參閱[映射資料來源欄位](#)。

Note

您的文件需要文件內文欄位或文件內文對等項目，才能搜尋您的文件。Amazon Kendra 您必須將資料來源中的文件內文欄位名稱對應至索引欄位名稱_document_body。所有其他欄位是選用的。

如需要設定的其他重要 JSON 金鑰清單，請參閱 [Amazon FSx \(NetApp ONTAP\) 範本結構描述](#)。

Amazon RDS/Aurora

您可以使用資料庫資料來源索引儲存在資料庫中的文件。提供資料庫的連線資訊之後，請 Amazon Kendra 連接文件並建立索引。

Amazon Kendra 支援下列資料庫：

- Amazon Aurora MySQL

- Amazon Aurora PostgreSQL
- Amazon RDS 對於 MySQL
- Amazon RDS 對於 PostgreSQL

Note

不支援無伺服器 Aurora 資料庫。

Important

這個 Amazon RDS/Aurora 連接器排定於 2023 年底前淘汰。

Amazon Kendra 現在支援新的資料庫資料來源連接器。為了改善使用體驗，建議您從下列使用案例的新連接器中選擇：

- [Aurora \(MySQL\)](#)
- [Aurora \(PostgreSQL\)](#)
- [Amazon RDS \(MySQL\)](#)
- [Amazon RDS \(Microsoft SQL 服務器\)](#)
- [Amazon RDS \(甲骨文\)](#)
- [Amazon RDS \(PostgreSQL\)](#)
- [IBM](#)
- [Microsoft SQL Server](#)
- [MySQL](#)
- [Oracle 資料庫](#)
- [PostgreSQL](#)

您可以使用 [Amazon Kendra 主控台](#) 和 [DatabaseConfigurationAPI](#) 連線 Amazon Kendra 到資料庫資料來源。

若要疑難排解資料 Amazon Kendra 庫資料來源連接器，請參閱 [疑難排解資料來](#)。

主題

- [支援的功能](#)

- [必要條件](#)
- [連接說明](#)

支援的功能

Amazon Kendra 資料庫資料來源連接器支援下列功能：

- 欄位對映
- 使用者內容篩選
- 虛擬私有雲端 (VPC)

必要條件

在您可以使用 Amazon Kendra 索引資料庫資料來源之前，請先在資料庫和 AWS 帳戶中進行這些變更。

在你的數據庫中，確保你有：

- 記下您資料庫的使用者名稱和密碼的基本驗證憑證。
- 複製主機名稱、連接埠號碼、主機位址、資料庫名稱，以及包含文件資料之資料表的名稱。對於 PostgreSQL，資料表必須是公用資料表或公用結構描述。

Note

主機和端口告訴在 Amazon Kendra 哪裡可以找到互聯網上的數據庫服務器。數據庫名稱和表名稱告訴在 Amazon Kendra 哪裡可以找到數據庫服務器上的文檔數據。

- 複製資料表中包含文件資料的欄名稱。您必須包括文件 ID、文件內文、要偵測文件是否已變更的欄 (例如，上次更新的欄)，以及對應至自訂索引欄位的選擇性資料表欄。您也可以將任何 [Amazon Kendra 保留的欄位名稱](#) 對應至資料表資料行。
- 複製資料庫引擎類型資訊，例如您是否使 Amazon RDS 用 MySQL 或其他類型。
- 核取每個文件在資料庫中，以及您打算用於相同索引的其他資料來源中都是唯一的。您要用於索引的每個資料來源不得包含跨資料來源的相同文件。文件 ID 對索引來說是全域的，而且每個索引必須是唯一的。

在您的 AWS 帳戶，請確保您有：

- [建立 Amazon Kendra 索引](#)，如果使用 API，則會記下索引識別碼。
- 為您的[資料來源建立 IAM 角色](#)，如果使用 API，則會記錄 IAM 角色的 ARN。

Note

如果您變更驗證類型和認證，則必須更新 IAM 角色才能存取正確的 AWS Secrets Manager 密碼 ID。

- 將您的資料庫驗證認證儲存在 AWS Secrets Manager 密碼中，如果使用 API，則會記下密碼的 ARN。

Note

我們建議您定期重新整理或輪換您的認證和密碼。僅為您自己的安全提供必要的訪問級別。我們不建議您跨資料來源以及連接器 1.0 和 2.0 版 (如果適用) 重複使用認證和密碼。

如果您沒有現有的 IAM 角色或密碼，則可以在將資料庫資料來源連線到時，使用主控台建立新 IAM 角色和 Secrets Manager 密碼 Amazon Kendra。如果您使用 API，則必須提供現有 IAM 角色和 Secrets Manager 密碼的 ARN 以及索引 ID。

連接說明

若要連線 Amazon Kendra 到資料庫資料來源，您必須提供資料庫資料來源的必要詳細資訊，Amazon Kendra 以便能夠存取您的資料。如果尚未為其配置資料庫 Amazon Kendra，請參閱[必要條件](#)。

Console

若要連線 Amazon Kendra 至資料庫


1. 登入 AWS Management Console 並開啟[Amazon Kendra 主控台](#)。
2. 在左側導覽窗格中，選擇 [索引]，然後從索引清單中選擇要使用的索引。

Note

您可以選擇在索引設置下配置或編輯您的用戶訪問控制設置。


3. 在 [開始使用] 頁面上，選擇 [新增資料來源]。

4. 在 [新增資料來源] 頁面上，選擇資料庫連接器，然後選擇 [新增連接器]。如果使用版本 2 (如果適用)，請選擇具有「V2.0」標籤的資料庫連接器。
5. 在 [指定資料來源詳細資訊] 頁面上，輸入下列資訊：
 - a. 在名稱和說明中，對於資料來源名稱 — 輸入資料來源的名稱。您可以包含連字號，但不能包含空格。
 - b. (選擇性) 說明 — 輸入資料來源的選用說明。
 - c. 在預設語言中 — 選擇一種語言來篩選索引的文件。除非另有指定，否則語言預設為英文。文件中繼資料中指定的語言會覆寫選取的語言。
 - d. 在「標籤」中，針對「新增標籤」 — 包含可選標籤以搜尋和篩選資源或追蹤 AWS 成本。
 - e. 選擇下一步。
6. 在 [定義存取權和安全性] 頁面上，輸入下列資訊：
 - a. 端點 — DNS 主機名稱、IPv4 位址或 IPv6 位址。
 - b. 連接埠-連接埠號碼。
 - c. 資料庫 — 資料庫名稱。
 - d. 表格名稱 — 表格名稱。
 - e. 在「驗證類型」中選擇「現有」和「新增」，以儲存您的資料庫驗證證明資料。如果您選擇建立新密碼，則會開啟一個 AWS Secrets Manager 密碼視窗。
 - 在「建立 AWS Secrets Manager 密碼視窗」中輸入下列資訊：
 - A. 秘密名稱 — 您秘密的名稱。前綴 'AmazonKendra-data-' 會自動添加到您的密碼名稱中。
 - B. 對於使用者名稱和密碼 — 輸入資料庫帳戶中的驗證認證值。
 - C. 選擇 [儲存驗證]。
 - f. Virtual Private Cloud (VPC) (VPC) — 您可以選擇使用 VPC。如果是這樣，您必須新增子網路和 VPC 安全性群組。

 Note

您必須使用私有子網路。如果 RDS 執行個體位於 VPC 中的公有子網路中，您可以建立私有子網路，該子網路具有對公有子網路中 NAT 閘道的輸出存取權。VPC 組態中提供的子網路必須位於美國西部 (奧勒岡)、美國東部 (維吉尼亞北部)、歐洲 (愛爾蘭)。

- g. IAM role — 選擇現有 IAM 角色或建立新 IAM 角色以存取存放庫認證和索引內容。

 Note

IAM 用於索引的角色不能用於資料來源。如果您不確定索引或常見問題集是否使用現有角色，請選擇 [建立新角色] 以避免發生錯誤。

- h. 選擇下一步。
7. 在 [設定同步設定] 頁面上，輸入下列資訊：
 - a. 根據您的使用案例，在 Aurora MySQL、MySQL、Aurora 和 PostgreSQL 之間進行選擇。
 - b. 以雙引號括住 SQL 識別碼 — 選取此選項可用雙引號括住 SQL 識別碼。例如，「columnName」。
 - c. ACL 欄和變更偵測欄 — 設定 Amazon Kendra 用於變更偵測的欄 (例如，上次更新的資料行) 和存取控制清單。
 - d. 在同步執行排程中，對於頻率 — 選擇與資料來源同步的頻率。Amazon Kendra
 - e. 選擇下一步。
 8. 在 [設定欄位對映] 頁面上，輸入下列資訊：
 - a. Amazon Kendra 預設欄位對映 — 從 Amazon Kendra 產生的預設資料來源欄位中選取您要對映至索引的欄位。您必須新增 document_id 和的 [資料庫] 欄值 document_body
 - b. 自訂欄位對映 — 新增自訂資料來源欄位以建立要對映的索引欄位名稱和欄位資料類型。
 - c. 選擇下一步。
 9. 在 [檢閱並建立] 頁面上，檢查您輸入的資訊是否正確，然後選取 [新增資料來源]。您也可以從此頁面選擇編輯您的資訊。成功新增資料來源後，您的資料來源將顯示在 [資料來源] 頁面上。

API

若要連線 Amazon Kendra 至資料庫

您必須指定下列 [DatabaseConfiguration](#) API：

- ColumnConfiguration 索引應從資料庫取得文件資訊的位置的相關資訊。如需詳細資訊，請參閱 [ColumnConfiguration](#)。您必須指定 DocumentDataColumnName (文件內文或主要文字) 和 DocumentIdColumnName, 和 ChangeDetectingColumn (例如，上次更新的欄) 欄位。對

應至欄 `DocumentIdColumnName` 位的欄必須是整數資料行。下列範例顯示資料庫資料來源的簡易資料行組態：

```
"ColumnConfiguration": {
  "ChangeDetectingColumns": [
    "LastUpdateDate",
    "LastUpdateTime"
  ],
  "DocumentDataColumnName": "TextColumn",
  "DocumentIdColumnName": "IdentifierColumn",
  "DocumentTitleColumnName": "TitleColumn",
  "FieldMappings": [
    {
      "DataSourceFieldName": "AbstractColumn",
      "IndexFieldName": "Abstract"
    }
  ]
}
```

- `ConnectionConfiguration` 連線至資料庫所需的組態資訊。如需詳細資訊，請參閱 [ConnectionConfiguration](#)。
- `DatabaseEngineType` 執行資料庫的資料庫引擎類型。的 `DatabaseHost` 欄位 `ConnectionConfiguration` 必須是資料庫的 Amazon Relational Database Service (Amazon RDS) 執行個體端點。請勿使用叢集端點。
- 秘密 Amazon 資源名稱 (ARN) — 提供包含資料庫帳戶身份驗證登入資料的 Secrets Manager 密碼的 Amazon 資源名稱 (ARN)。密碼會以下列金鑰儲存在 JSON 結構中：

```
{
  "username": "user name",
  "password": "password"
}
```

下列範例顯示資料庫組態，包括秘密 ARN。

```
"DatabaseConfiguration": {
  "ConnectionConfiguration": {
    "DatabaseHost": "host.subdomain.domain.tld",
    "DatabaseName": "DocumentDatabase",
    "DatabasePort": 3306,
    "SecretArn": "arn:aws:secretmanager:region:account ID:secret/secret name",
```

```
    "TableName": "DocumentTable"  
  }  
}
```

Note

我們建議您定期重新整理或輪換您的認證和密碼。僅為您自己的安全提供必要的訪問級別。我們不建議您跨資料來源以及連接器 1.0 和 2.0 版 (如果適用) 重複使用認證和密碼。

- IAM role — 指定RoleArn何時呼叫CreateDataSource以提供具有存取 Secrets Manager 密碼之權限的 IAM 角色，以及呼叫資料庫連接器和 Amazon Kendra所需公用 API 的時間。如需詳細資訊，請參閱[資料庫資料來源的IAM 角色](#)。

您還可以添加以下可選功能：

- Virtual Private Cloud (VPC) — 指定VpcConfiguration為資料來源組態的一部分。請參閱[設定 Amazon Kendra 定以使用 VPC](#)。

Note

您只能使用私有子網路。如果 RDS 執行個體位於 VPC 中的公有子網路中，您可以建立私有子網路，該子網路具有對公有子網路中 NAT 閘道的輸出存取權。VPC 組態中提供的子網路必須位於美國西部 (奧勒岡)、美國東部 (維吉尼亞北部)、歐洲 (愛爾蘭)。

- 欄位對映 — 選擇將資料庫資料來源欄位對映至 Amazon Kendra 索引欄位。如需詳細資訊，請參閱[映射資料來源欄位](#)。

Note

您的文件需要文件內文欄位或文件內文對等項目，才能搜尋您的文件。Amazon Kendra 您必須將資料來源中的文件內文欄位名稱對應至索引欄位名稱_document_body。所有其他欄位是選用的。

- 使用者前後關聯篩選與存取控制 — Amazon Kendra 探索文件的存取控制清單 (ACL) (如果您有文件的 ACL)。ACL 資訊可用來根據使用者或使用者對文件的群組存取權來篩選搜尋結果。如需詳細資訊，請參閱[使用者內容篩選](#)。

Amazon RDS (Microsoft SQL 服務器)

SQL Server 是由 Microsoft 開發的數據庫管理系統。Amazon RDS 適用於 SQL Server 可讓您輕鬆地在雲端中設定、操作和擴展 SQL Server 部署。如果您是 Amazon RDS (Microsoft SQL 服務器) 用戶，則可以使 Amazon Kendra 用索引您 Amazon RDS (Microsoft SQL 服務器) 數據源。Amazon Kendra JDBC 資料來源連接器支援 Microsoft SQL 伺服器 2019。

您可以使用[Amazon Kendra 控制台](#)和 [TemplateConfigurationAPI](#) 連接 Amazon Kendra 到您的 Amazon RDS (Microsoft SQL 服務器) 數據源。

如需對 Amazon Kendra Amazon RDS (Microsoft SQL 伺服器) 資料來源連接器進行疑難排解，請參閱[疑難排解資料來](#)。

主題

- [支援的功能](#)
- [必要條件](#)
- [連接說明](#)
- [備註](#)

支援的功能

- 欄位對映
- 使用者內容篩選
- 包含/排除過濾器
- 完整和增量內容同步
- 虛擬私有雲端 (VPC)

必要條件

在您可 Amazon Kendra 以使用索引 Amazon RDS (Microsoft SQL Server) 資料來源之前，請先在您的 Amazon RDS (Microsoft SQL 伺服器) 和 AWS 帳戶中進行這些變更。

在 Amazon RDS (Microsoft SQL 服務器)，請確保你有：

- 記下您的資料庫使用者名稱和密碼。

⚠ Important

最佳作法是提供 Amazon Kendra 唯讀資料庫認證。

- 複製您的資料庫主機 URL、連接埠和執行個體。
- 核取每個文件在 Amazon RDS (Microsoft SQL Server) 以及您打算用於相同索引的其他資料來源之間是唯一的。您要用於索引的每個資料來源不得包含跨資料來源的相同文件。文件 ID 對索引來說是全域的，而且每個索引必須是唯一的。

在您的中 AWS 帳戶，請確保您有：

- [建立 Amazon Kendra 索引](#)，如果使用 API，則會記下索引識別碼。
- 為您的[資料來源建立 IAM 角色](#)，如果使用 API，則會記錄 IAM 角色的 ARN。

📘 Note

如果您變更驗證類型和認證，則必須更新 IAM 角色以存取正確的 AWS Secrets Manager 密碼 ID。

- 將您的 Amazon RDS (Microsoft SQL Server) 身份驗證憑據存儲在 AWS Secrets Manager 密鑰中，並且如果使用 API，則會記錄密鑰的 ARN。

📘 Note

我們建議您定期重新整理或輪換您的認證和密碼。僅為您自己的安全提供必要的訪問級別。我們不建議您跨資料來源以及連接器 1.0 和 2.0 版 (如果適用) 重複使用認證和密碼。

如果您沒有現有的 IAM 角色或密碼，則可以在將 Amazon RDS (Microsoft SQL Server) 資料來源連線到時，使用主控台建立新 IAM 角色和 Secrets Manager 密碼 Amazon Kendra。如果您使用 API，則必須提供現有 IAM 角色和 Secrets Manager 密碼的 ARN 以及索引 ID。

連接說明

要連接 Amazon Kendra 到您的 Amazon RDS (Microsoft SQL Server) 數據源，您必須提供您的 Amazon RDS (Microsoft SQL Server) 憑據的詳細信息，Amazon Kendra 以便可以訪問您的數據。如果您還沒有配置 Amazon RDS (Microsoft SQL 服務器) 查 Amazon Kendra 看[必要條件](#)。

Console

要連接 Amazon Kendra 到 Amazon RDS (Microsoft SQL 服務器)


1. 登入 AWS Management Console 並開啟 [Amazon Kendra 主控台](#)。
2. 在左側導覽窗格中，選擇 [索引]，然後從索引清單中選擇要使用的索引。

Note

您可以選擇在索引設置下配置或編輯用戶訪問控制設置。


3. 在 [開始使用] 頁面上，選擇 [新增資料來源]。
4. 在 [新增資料來源] 頁面上，選擇 [Amazon RDS (Microsoft SQL Server) 連接器]，然後選擇 [新增連接器]。如果使用版本 2 (如果適用)，請選擇帶有「V2.0」標籤的 Amazon RDS (Microsoft SQL 服務器) 連接器。
5. 在 [指定資料來源詳細資訊] 頁面上，輸入下列資訊：
 - a. 在名稱和說明中，對於資料來源名稱 — 輸入資料來源的名稱。您可以包含連字號，但不能包含空格。
 - b. (選擇性) 說明 — 輸入資料來源的選用說明。
 - c. 在預設語言中 — 選擇一種語言來篩選索引的文件。除非另有指定，否則語言預設為英文。文件中繼資料中指定的語言會覆寫選取的語言。
 - d. 在「標籤」中，針對「新增標籤」— 包含可選標籤以搜尋和篩選資源或追蹤 AWS 成本。
 - e. 選擇下一步。
6. 在 [定義存取權和安全性] 頁面上，輸入下列資訊：
 - a. 在來源中，輸入下列資訊：
 - b. 主機 — 輸入資料庫主機名稱。
 - c. 連接埠 — 輸入資料庫連接埠。
 - d. 執行處理 — 輸入資料庫執行處理。
 - e. 啟用 SSL 憑證位置 — 選擇輸入 SSL 憑證檔案的 Amazon S3 路徑。
 - f. 在驗證中 — 輸入下列資訊：
 - AWS Secrets Manager 密碼 — 選擇現有密碼或建立新 Secrets Manager 密碼來儲存您的 Amazon RDS (Microsoft SQL Server) 驗證認證。如果您選擇建立新密碼，則會開啟一個 AWS Secrets Manager 密碼視窗。

- A. 在「建立 AWS Secrets Manager 密碼視窗」中輸入下列資訊：
 - I. 秘密名稱 — 您秘密的名稱。前綴 'AmazonKendra-Amazon RDS (Microsoft SQL 服務器) -' 會自動添加到您的密碼名稱中。
 - II. 對於資料庫使用者名稱和密碼 — 輸入您從資料庫複製的驗證認證值。
- B. 選擇儲存。
- g. V@@@ irtual Private Cloud (VPC) (VPC) — 您可以選擇使用 VPC。如果是這樣，您必須新增子網路和 VPC 安全性群組。
- h. IAM role — 選擇現有 IAM 角色或建立新 IAM 角色以存取存放庫認證和索引內容。

 Note

IAM 用於索引的角色不能用於資料來源。如果您不確定索引或常見問題集是否使用現有角色，請選擇 [建立新角色] 以避免發生錯誤。

- i. 選擇下一步。
7. 在 [設定同步設定] 頁面上，輸入下列資訊：
- a. 在同步範圍中，從下列選項中選擇：
 - SQL 查詢 — 輸入 SQL 查詢陳述式，例如 SELECT 和 JOIN 作業。SQL 查詢必須小於 32 KB。Amazon Kendra 會編目符合您查詢的所有資料庫內容。

 Note

如果表格名稱在名稱中包含特殊字元 (非字母數字)，則必須在表格名稱周圍使用方括號。例如，# *[my-database-table]* ### *

- 主索引鍵欄 — 提供資料庫表格的主索引鍵。這標識數據庫中的一個表。
 - 標題欄 — 提供資料庫表格中文件標題欄的名稱。
 - 主體欄 — 提供資料庫表格中文件主體欄的名稱。
- b. 在 [其他設定 — 選用] 中，從下列選項中選擇以同步特定內容，而非同步所有檔案：
 - 變更偵測欄 — 輸入 Amazon Kendra 將用來偵測內容變更的欄名稱。Amazon Kendra 當這些資料行中有任何變更時，會重新建立內容的索引。
 - 使用者 ID 欄 — 輸入包含允許存取內容的使用者 ID 的欄名稱。

- 群組欄 — 輸入包含允許存取內容之群組的欄名稱。
 - 來源 URL 欄 — 輸入包含要編製索引之來源 URL 的資料欄名稱。
 - 時間戳記欄 — 輸入包含時間戳記的欄名稱。Amazon Kendra 使用時間戳記資訊偵測內容中的變更，並僅同步變更的內容。
 - [時區] 欄 — 輸入資料欄的名稱，其中包含要編目之內容的時區。
 - 時間戳記格式 — 輸入包含時間戳記格式的欄名稱，可用來偵測內容變更並重新同步處理內容。
- c. 同步模式 — 選擇資料來源內容變更時要如何更新索引。當您第一次將資料來源同 Amazon Kendra 步處理時，依預設會檢索所有內容並建立索引。如果初始同步失敗，您必須執行資料的完整同步，即使您沒有選擇完整同步作為同步模式選項。
- 完全同步：新鮮索引所有內容，並在每次資料來源與索引同步時取代現有內容。
 - 新增、修改的同步：每次資料來源與索引同步時，僅對新內容和已修改的內容建立索引。Amazon Kendra 可以使用資料來源的機制來追蹤內容變更，並為上次同步後變更的內容建立索引。
 - 新增、修改、刪除的同步：每次資料來源與索引同步時，僅對新內容、修改和刪除的內容建立索引。Amazon Kendra 可以使用資料來源的機制來追蹤內容變更，並為上次同步後變更的內容建立索引。
- d. 在同步執行排程中，對於頻率 — 與資料來源同步的頻率。Amazon Kendra
- e. 選擇下一步。
8. 在 [設定欄位對映] 頁面上，輸入下列資訊：
- a. 從產生的預設資料來源欄位中選取您要對應至 Amazon Kendra 索引的文件 ID、文件標題和來源 URL。
 - b. 新增欄位 — 新增自訂資料來源欄位以建立要對映的索引欄位名稱和欄位資料類型。
 - c. 選擇下一步。
9. 在 [檢閱並建立] 頁面上，檢查您輸入的資訊是否正確，然後選取 [新增資料來源]。您也可以從此頁面選擇編輯您的資訊。成功新增資料來源後，您的資料來源將顯示在 [資料來源] 頁面上。

API

要連接 Amazon Kendra 到 Amazon RDS (Microsoft SQL 服務器)

您必須使用 [TemplateConfiguration](#) API 指定下列項目：

- 資料來源 — 指定使用 [TemplateConfiguration](#) JSON 結構定義 JDBC 時的資料來源類型。同時指定呼叫 [CreateDataSource](#) API TEMPLATE 時的資料來源。
- 資料庫類型 — 您必須將資料庫類型指定為 `sqlserver`。
- SQL 查詢 — 指定 SQL 查詢陳述式，例如 SELECT 和 JOIN 作業。SQL 查詢必須小於 32 KB。Amazon Kendra 會編目符合您查詢的所有資料庫內容。

Note

如果表格名稱在名稱中包含特殊字元 (非字母數字)，則必須在表格名稱周圍使用方括號。
例如，`# [my-database-table] ### *`

- 同步模式 — 指定資料來源內容變更時 Amazon Kendra 應如何更新索引。當您第一次將資料來源同 Amazon Kendra 步處理時，依預設會檢索所有內容並建立索引。如果初始同步失敗，您必須執行資料的完整同步，即使您沒有選擇完整同步作為同步模式選項。您可以選擇：
 - `FORCED_FULL_CRAWL` 新建索引所有內容，並在每次資料來源與索引同步時取代現有內容。
 - `FULL_CRAWL`，以在每次資料來源與索引同步時，僅對新的、修改的和刪除的內容建立索引。Amazon Kendra 可以使用資料來源的機制來追蹤內容變更，並為上次同步後變更的內容建立索引。
 - `CHANGE_LOG` 每次資料來源與索引同步時，僅對新內容和修改的內容建立索引。Amazon Kendra 可以使用資料來源的機制來追蹤內容變更，並為上次同步後變更的內容建立索引。
- 秘密 Amazon 資源名稱 (ARN) — 提供 Secrets Manager 秘密的 Amazon 資源名稱 (ARN)，其中包含您在 Amazon RDS (Microsoft SQL Server) 帳戶中建立的身份驗證登入資料。密碼會以下列金鑰儲存在 JSON 結構中：

```
{
  "user name": "database user name",
  "password": "password"
}
```

Note

我們建議您定期重新整理或輪換您的認證和密碼。僅為您自己的安全提供必要的訪問級別。我們不建議您跨資料來源以及連接器 1.0 和 2.0 版 (如果適用) 重複使用認證和密碼。

- IAM 角色 — 指定 RoleArn 何時呼叫 CreateDataSource 以提供具有存取 Secrets Manager 密碼的權限的 IAM 角色，以及呼叫 Amazon RDS (Microsoft SQL Server) 連接器和 Amazon Kendra 所需的公用 API。如需詳細資訊，請參閱 [Amazon RDS \(Microsoft SQL 伺服器\) 資料來源的 IAM 角色](#)。

您還可以添加以下可選功能：

- Virtual Private Cloud (VPC) — 指定您呼叫的 VpcConfiguration 時間。CreateDataSource 如需詳細資訊，請參閱 [配置 Amazon Kendra 為使用 Amazon VPC](#)。
- 包含和排除篩選器 — 您可以指定是否要使用使用者 ID、群組、來源 URL、時間戳記和時區來包含特定內容。
- 使用者前後關聯篩選與存取控制 — Amazon Kendra 探索文件的存取控制清單 (ACL) (如果您有文件的 ACL)。ACL 資訊可用來根據使用者或使用者對文件的群組存取來篩選搜尋結果。如需詳細資訊，請參閱 [使用者內容篩選](#)。
- 欄位對應 — 選擇將您的 Amazon RDS (Microsoft SQL Server) 資料來源欄位對應至 Amazon Kendra 索引欄位。如需詳細資訊，請參閱 [映射資料來源欄位](#)。

Note

您的文件需要文件內文欄位或文件內文對等項目，才能搜尋您的文件。Amazon Kendra 您必須將資料來源中的文件內文欄位名稱對應至索引欄位名稱 `_document_body`。所有其他欄位是選用的。

如需要設定的其他重要 JSON 金鑰清單，請參閱 [Amazon RDS \(Microsoft SQL 伺服器\) 模板架構](#)。

備註

- Amazon Kendra 檢查更新的內容時，不會追蹤已刪除的資料庫列。
- 資料庫中一列中欄位名稱和值的大小不得超過 400 KB。
- 如果您的資料庫資料來源中有大量資料，並且不想 Amazon Kendra 在第一次同步之後對所有資料庫內容建立索引，則可以選擇僅同步新文件、修改或刪除的文件。
- 最佳作法是提供 Amazon Kendra 唯讀資料庫認證。
- 最佳做法是避免新增包含敏感資料或個人可識別資訊 (PII) 的表格。

Amazon RDS (MySQL)

Amazon RDS (Amazon Relational Database Service) 是一種 Web 服務，可讓您更輕鬆地在 AWS 雲端中設定、操作和擴展關聯式資料庫。如果您是使用 Amazon RDS 者，則可以使用 Amazon Kendra 對 Amazon RDS (MySQL) 資料來源建立索引。Amazon Kendra 資料來源連接器支援 Amazon RDS MySQL 5.6、5.7 和 8.0。

您可以使用 [Amazon Kendra 主控台](#) 和 [TemplateConfiguration API](#) 連線 Amazon Kendra 到 Amazon RDS (MySQL) 資料來源。

如需疑難排解 Amazon Kendra Amazon RDS (MySQL) 資料來源連接器，請參閱 [疑難排解資料來](#)。

主題

- [支援的功能](#)
- [必要條件](#)
- [連接說明](#)
- [備註](#)

支援的功能

- 欄位對映
- 使用者內容篩選
- 包含/排除過濾器
- 完整和增量內容同步
- 虛擬私有雲端 (VPC)

必要條件

在您可以用來 Amazon Kendra 為 Amazon RDS (MySQL) 資料來源建立索引之前，請先在 Amazon RDS (MySQL) 和 AWS 帳戶中進行這些變更。

在中 Amazon RDS (MySQL)，請確定您有：

- 記下您的資料庫使用者名稱和密碼。

⚠ Important

最佳作法是提供 Amazon Kendra 唯讀資料庫認證。

- 複製您的資料庫主機 URL、連接埠和執行個體。您可以在 Amazon RDS 控制台上找到此信息。
- 已勾選的每個文件在您打算用於相同索引的其他資料來源中 Amazon RDS (MySQL) 和其他資料來源之間都是唯一的。您要用於索引的每個資料來源不得包含跨資料來源的相同文件。文件 ID 對索引來說是全域的，而且每個索引必須是唯一的。

在你的 AWS 帳戶，確保你有：

- [建立 Amazon Kendra 索引](#)，如果使用 API，則會記下索引 ID。
- 為您的[資料來源建立 IAM 角色](#)，如果使用 API，則會記錄 IAM 角色的 ARN。

ℹ Note

如果您變更驗證類型和認證，則必須更新 IAM 角色才能存取正確的 AWS Secrets Manager 密碼 ID。

- 將您的 Amazon RDS (MySQL) 身份驗證憑據存儲在 AWS Secrets Manager 密鑰中，如果使用 API，則記錄密鑰的 ARN。

ℹ Note

我們建議您定期重新整理或輪換您的認證和密碼。僅為您自己的安全提供必要的訪問級別。我們不建議您跨資料來源以及連接器 1.0 和 2.0 版 (如果適用) 重複使用認證和密碼。

如果您沒有現有的 IAM 角色或密碼，則可以在將 Amazon RDS (MySQL) 資料來源連線到時使用主控台建立新 IAM 角色和 Secrets Manager 密碼 Amazon Kendra。如果您使用 API，則必須提供現有 IAM 角色和 Secrets Manager 密碼的 ARN，以及索引 ID。

連接說明

若要連線 Amazon Kendra 到 Amazon RDS (MySQL) 資料來源，您必須提供 Amazon RDS (MySQL) 認證的詳細資料，Amazon Kendra 以便能夠存取您的資料。如果您尚未設定「Amazon Kendra 請 Amazon RDS (MySQL) 參閱[必要條件](#)」。

Console

若要連線 Amazon Kendra 到 Amazon RDS (MySQL)


1. 登入 AWS Management Console 並開啟 [Amazon Kendra 主控台](#)。
2. 在左側導覽窗格中，選擇 [索引]，然後從索引清單中選擇要使用的索引。

Note

您可以選擇在索引設置下配置或編輯您的用戶訪問控制設置。

3. 在 [開始使用] 頁面上，選擇 [新增資料來源]。
4. 在 [新增資料來源] 頁面上，選擇 [Amazon RDS (MySQL)連接器]，然後選擇 [新增連接器]。如果使用版本 2 (如果適用)，請選擇帶有「V2.0」標籤的 Amazon RDS (MySQL)連接器。
5. 在 [指定資料來源詳細資訊] 頁面上，輸入下列資訊：
 - a. 在名稱和說明中，對於資料來源名稱 — 輸入資料來源的名稱。您可以包含連字號，但不能包含空格。
 - b. (選擇性) 說明 — 輸入資料來源的選用說明。
 - c. 在預設語言中 — 選擇一種語言來篩選索引的文件。除非另有指定，否則語言預設為英文。文件中繼資料中指定的語言會覆寫選取的語言。
 - d. 在「標籤」中，針對「新增標籤」 — 包含可選標籤以搜尋和篩選資源或追蹤 AWS 成本。
 - e. 選擇下一步。
6. 在 [定義存取權和安全性] 頁面上，輸入下列資訊：
 - a. 在來源中，輸入下列資訊：
 - b. 主機 — 輸入資料庫主機 URL，例如：`http://instance URL.region.rds.amazonaws.com`。
 - c. 連接埠 — 輸入資料庫連接埠，例如5432。
 - d. 執行處理 — 例如，輸入資料庫執行處理postgres。
 - e. 啟用 SSL 憑證位置 — 選擇此選項可輸入 SSL 憑證檔案的 Amazon S3 路徑。
 - f. 在驗證中 — 輸入下列資訊：
 - AWS Secrets Manager 祕密 — 選擇現有密碼或建立新 Secrets Manager 密碼來儲存您的 Amazon RDS (MySQL)驗證認證。如果您選擇建立新密碼，則會開啟一個 AWS Secrets Manager 密碼視窗。

- A. 在「建立 AWS Secrets Manager 密碼視窗」中輸入下列資訊：
 - I. 秘密名稱 — 您秘密的名稱。前綴 'AmazonKendraAmazon RDS (MySQL)-' 會自動添加到您的密碼名稱中。
 - II. 對於資料庫使用者名稱和密碼 — 輸入您從資料庫複製的驗證認證值。
- B. 選擇儲存。
- g. V@@@rtual Private Cloud (VPC) (VPC) — 您可以選擇使用 VPC。如果是這樣，您必須新增子網路和 VPC 安全性群組。
- h. IAM role — 選擇現有 IAM 角色或建立新 IAM 角色以存取存放庫認證和索引內容。

 Note

IAM 用於索引的角色不能用於資料來源。如果您不確定索引或常見問題集是否使用現有角色，請選擇 [建立新角色] 以避免發生錯誤。

- i. 選擇下一步。
7. 在 [設定同步設定] 頁面上，輸入下列資訊：
 - a. 在同步範圍中，從下列選項中選擇：
 - SQL 查詢 — 輸入 SQL 查詢陳述式，例如選取和聯結作業。SQL 查詢必須小於 32 KB 的 SQL 查詢小於 32 KB，且不得包含任何分號 (;)。Amazon Kendra 會編目符合您查詢的所有資料庫內容。
 - 主索引鍵欄 — 提供資料庫表格的主索引鍵。這標識數據庫中的一個表。
 - 標題欄 — 提供資料庫表格中文件標題欄的名稱。
 - 主體欄 — 提供資料庫表格中文件主體欄的名稱。
 - b. 在 [其他設定 — 選用] 中，從下列選項中選擇以同步特定內容，而非同步所有檔案：
 - 變更偵測欄 — 輸入 Amazon Kendra 將用來偵測內容變更的欄名稱。Amazon Kendra 當這些資料行中有任何變更時，會重新建立內容的索引。
 - 使用者 ID 欄 — 輸入包含允許存取內容的使用者 ID 的欄名稱。
 - 群組欄 — 輸入包含允許存取內容之群組的欄名稱。
 - 來源 URL 欄 — 輸入包含要編製索引之來源 URL 的資料欄名稱。
 - 時間戳記欄 — 輸入包含時間戳記的欄名稱。Amazon Kendra 使用時間戳記資訊偵測內容中的變更，並僅同步變更的內容。

- [時區] 欄 — 輸入資料欄的名稱，其中包含要編目之內容的時區。
 - 時間戳記格式 — 輸入包含時間戳記格式的欄名稱，可用來偵測內容變更並重新同步處理內容。
- c. 同步模式 — 選擇資料來源內容變更時要如何更新索引。當您第一次將資料來源同 Amazon Kendra 步處理時，依預設會檢索所有內容並建立索引。如果初始同步失敗，您必須執行資料的完整同步處理，即使您沒有選擇完整同步作為同步模式選項。
- 完全同步：新鮮索引所有內容，並在每次資料來源與索引同步時取代現有內容。
 - 新增、修改的同步：每次資料來源與索引同步時，僅對新內容和已修改的內容建立索引。Amazon Kendra 可以使用資料來源的機制來追蹤內容變更，並為上次同步後變更的內容建立索引。
 - 新增、修改、刪除的同步：每次資料來源與索引同步時，僅對新內容、已修改和刪除的內容建立索引。Amazon Kendra 可以使用資料來源的機制來追蹤內容變更，並為上次同步後變更的內容建立索引。
- d. 在同步執行排程中，對於頻率 — 與資料來源同步的頻率。 Amazon Kendra
- e. 選擇下一步。
8. 在 [設定欄位對映] 頁面上，輸入下列資訊：
- a. 從產生的預設資料來源欄位中選取您要對應至 Amazon Kendra 索引的文件 ID、文件標題和來源 URL。
 - b. 新增欄位 — 新增自訂資料來源欄位，以建立要對映的索引欄位名稱和欄位資料類型。
 - c. 選擇下一步。
9. 在 [檢閱並建立] 頁面上，檢查您輸入的資訊是否正確，然後選取 [新增資料來源]。您也可以從此頁面選擇編輯您的資訊。成功新增資料來源後，您的資料來源將顯示在 [資料來源] 頁面上。

API


若要連線 Amazon Kendra 到 Amazon RDS (MySQL)

您必須使用 [TemplateConfiguration](#) API 指定下列項目：

- 資料來源 — 指定使用 [TemplateConfiguration](#) JSON 結構定義 JDBC 時的資料來源類型。同時將資料來源指定為呼叫 [CreateDataSource](#) API TEMPLATE 時的方式。
- 資料庫類型 — 您必須將資料庫類型指定為 mySql。

- SQL 查詢 — 指定 SQL 查詢陳述式，例如 SELECT 和 JOIN 作業。SQL 查詢必須小於 32 KB。Amazon Kendra 會編目符合您查詢的所有資料庫內容。
- 同步模式 — 指定資料來源內容變更時 Amazon Kendra 應如何更新索引。當您第一次將資料來源同 Amazon Kendra 步處理時，依預設會檢索所有內容並建立索引。如果初始同步失敗，您必須執行資料的完整同步處理，即使您沒有選擇完整同步作為同步模式選項。您可以選擇：
 - FORCED_FULL_CRAWL 新建索引所有內容，並在每次資料來源與索引同步時取代現有內容。
 - FULL_CRAWL，以在每次資料來源與索引同步時，僅對新的、修改的和刪除的內容建立索引。Amazon Kendra 可以使用資料來源的機制來追蹤內容變更，並為上次同步後變更的內容建立索引。
 - CHANGE_LOG 每次資料來源與索引同步時，僅對新內容和修改的內容建立索引。Amazon Kendra 可以使用資料來源的機制來追蹤內容變更，並為上次同步後變更的內容建立索引。
- 秘密 Amazon 資源名稱 (ARN) — 提供包含您在帳戶中建立的身份驗證登入資料的 Secrets Manager 密碼的 Amazon 資源名稱 (ARN)。Amazon RDS (MySQL) 密碼會以下列金鑰儲存在 JSON 結構中：

```
{
  "user name": "database user name",
  "password": "password"
}
```

 Note

我們建議您定期重新整理或輪換您的認證和密碼。僅為您自己的安全提供必要的訪問級別。我們不建議您跨資料來源以及連接器 1.0 和 2.0 版 (如果適用) 重複使用認證和密碼。

- IAM role — 指定 RoleArn 何時呼叫 CreateDataSource 以提供具有存取 Secrets Manager 密碼之權限的 IAM 角色，以及呼叫 Amazon RDS (MySQL) 連接器和 Amazon Kendra 所需公用 API 的時間。有關詳情，請參閱 [Amazon RDS \(MySQL\) 料來源的 IAM 角色](#)。

您還可以添加以下可選功能：

- Virtual Private Cloud (VPC) — 指定您撥打電話的 VpcConfiguration 時間。CreateDataSource 如需詳細資訊，請參閱 [配置 Amazon Kendra 為使用 Amazon VPC](#)。
- 包含和排除篩選器 — 您可以指定是否要使用使用者 ID、群組、來源 URL、時間戳記和時區來包含特定內容。

- 欄位對映 — 選擇將資 Amazon RDS (MySQL) 料來源欄位對映至 Amazon Kendra 索引欄位。如需詳細資訊，請參閱[映射資料來源欄位](#)。

Note

您的文件需要文件內文欄位或文件內文對等項目，才能搜尋您的文件。Amazon Kendra 您必須將資料來源中的文件內文欄位名稱對應至索引欄位名稱 `_document_body`。所有其他欄位是選用的。

- 使用者前後關聯篩選與存取控制 — Amazon Kendra 探索文件的存取控制清單 (ACL) (如果您有文件的 ACL)。ACL 資訊可用來根據使用者或使用者對文件的群組存取權來篩選搜尋結果。如需詳細資訊，請參閱[使用者內容篩選](#)。

如需要設定的其他重要 JSON 金鑰清單，請參閱[Amazon RDS \(MySQL\) 模板架構](#)。

備註

- Amazon Kendra 檢查更新的內容時，不會追蹤已刪除的資料庫列。
- 資料庫中一列中欄位名稱和值的大小不得超過 400 KB。
- 如果您的資料庫資料來源中有大量資料，並且不想 Amazon Kendra 在第一次同步之後對所有資料庫內容建立索引，則可以選擇僅同步新文件、修改或刪除的文件。
- 最佳作法是提供 Amazon Kendra 唯讀資料庫認證。
- 最佳做法是避免新增包含敏感資料或個人可識別資訊 (PII) 的表格。

Amazon RDS (Oracle)

Amazon RDS (Amazon Relational Database Service) 是一種 Web 服務，可讓您更輕鬆地在 AWS 雲端中設定、操作和擴展關聯式資料庫。如果您是使用 Amazon RDS (Oracle) 者，則可以使用 Amazon Kendra 對資 Amazon RDS (Oracle) 料來源建立索引。資 Amazon Kendra Amazon RDS (Oracle) 料來源連接器支援 Amazon RDS Oracle 資料庫 21c，Oracle 資料庫 19c，Oracle 資料庫 12c。

您可以使用[Amazon Kendra 主控台](#)和 [TemplateConfiguration](#) API 連線 Amazon Kendra 到 Amazon RDS (Oracle) 資料來源。

如需對資 Amazon Kendra Amazon RDS (Oracle) 料來源連接器進行疑難排解，請參 [疑難排解資料來](#)

主題

- [支援的功能](#)
- [必要條件](#)
- [連接說明](#)
- [備註](#)

支援的功能

- 欄位對映
- 使用者內容篩選
- 包含/排除過濾器
- 完整和增量內容同步
- 虛擬私有雲端 (VPC)

必要條件

在您可以用來 Amazon Kendra 為 Amazon RDS (Oracle) 資料來源建立索引之前，請先在 Amazon RDS (Oracle) 和 AWS 帳戶中進行這些變更。

在 Amazon RDS (Oracle) 中，請確定您有：

- 記下您的資料庫使用者名稱和密碼。

Important

最佳作法是提供 Amazon Kendra 唯讀資料庫認證。

- 複製您的資料庫主機 URL、連接埠和執行個體。
- 已勾選的每個文件在您打算用於相同索引的其他資料來源中 Amazon RDS (Oracle) 和其他資料來源之間都是唯一的。您要用於索引的每個資料來源不得包含跨資料來源的相同文件。文件 ID 對索引來說是全域的，而且每個索引必須是唯一的。

在您的 AWS 帳戶中，請確保您有：

- [建立 Amazon Kendra 索引](#)，如果使用 API，則會記下索引識別碼。
- 為您的 [資料來源建立 IAM 角色](#)，如果使用 API，則會記錄 IAM 角色的 ARN。

Note

如果您變更驗證類型和認證，則必須更新 IAM 角色才能存取正確的 AWS Secrets Manager 密碼 ID。

- 將您的 Amazon RDS (Oracle) 身份驗證憑據存儲在 AWS Secrets Manager 密鑰中，如果使用 API，則記錄密鑰的 ARN。

Note

我們建議您定期重新整理或輪換您的認證和密碼。僅為您自己的安全提供必要的訪問級別。我們不建議您跨資料來源以及連接器 1.0 和 2.0 版 (如果適用) 重複使用認證和密碼。

如果您沒有現有的 IAM 角色或密碼，則可以在將 Amazon RDS (Oracle) 資料來源連線到時使用主控台建立新 IAM 角色和 Secrets Manager 密碼 Amazon Kendra。如果您使用 API，則必須提供現有 IAM 角色和 Secrets Manager 密碼的 ARN，以及索引 ID。

連接說明

若要連線 Amazon Kendra 到 Amazon RDS (Oracle) 資料來源，您必須提供 Amazon RDS (Oracle) 認證的詳細資料，Amazon Kendra 以便能夠存取您的資料。如果您尚未設定「Amazon Kendra 請 Amazon RDS (Oracle) 參閱 [必要條件](#)」。

Console

若要連線 Amazon Kendra 到 Amazon RDS (Oracle)

- 登入 AWS Management Console 並開啟 [Amazon Kendra 主控台](#)。
- 在左側導覽窗格中，選擇 [索引]，然後從索引清單中選擇要使用的索引。

Note

您可以選擇在索引設置下配置或編輯您的用戶訪問控制設置。

- 在 [開始使用] 頁面上，選擇 [新增資料來源]。
- 在 [新增資料來源] 頁面上，選擇 [Amazon RDS (Oracle) 連接器]，然後選擇 [新增連接器]。如果使用版本 2 (如果適用)，請選擇帶有「V2.0」標籤的 Amazon RDS (Oracle) 連接器。

5. 在 [指定資料來源詳細資訊] 頁面上，輸入下列資訊：
 - a. 在名稱和說明中，對於資料來源名稱 — 輸入資料來源的名稱。您可以包含連字號，但不能包含空格。
 - b. (選擇性) 說明 — 輸入資料來源的選用說明。
 - c. 在預設語言中 — 選擇一種語言來篩選索引的文件。除非另有指定，否則語言預設為英文。文件中繼資料中指定的語言會覆寫選取的語言。
 - d. 在「標籤」中，針對「新增標籤」 — 包含可選標籤以搜尋和篩選資源或追蹤 AWS 成本。
 - e. 選擇下一步。
6. 在 [定義存取權和安全性] 頁面上，輸入下列資訊：
 - a. 在來源中，輸入下列資訊：
 - b. 主機 — 輸入資料庫主機名稱。
 - c. 連接埠 — 輸入資料庫連接埠。
 - d. 執行處理 — 輸入資料庫執行處理。
 - e. 啟用 SSL 憑證位置 — 選擇此選項可輸入 SSL 憑證檔案的 Amazon S3 路徑。
 - f. 在驗證中 — 輸入下列資訊：
 - AWS Secrets Manager 祕密 — 選擇現有密碼或建立新 Secrets Manager 密碼來儲存您的 Amazon RDS (Oracle) 驗證認證。如果您選擇建立新密碼，則會開啟一個 AWS Secrets Manager 密碼視窗。
 - A. 在「建立 AWS Secrets Manager 密碼視窗」中輸入下列資訊：
 - I. 祕密名稱 — 您祕密的名稱。前綴 'AmazonKendraAmazon RDS (Oracle)-' 會自動添加到您的密碼名稱中。
 - II. 對於資料庫使用者名稱和密碼 — 輸入您從資料庫複製的驗證認證值。
 - B. 選擇儲存。
 - g. V@@@ irtual Private Cloud (VPC) (VPC) — 您可以選擇使用 VPC。如果是這樣，您必須新增子網路和 VPC 安全性群組。
 - h. IAM role — 選擇現有 IAM 角色或建立新 IAM 角色以存取存放庫認證和索引內容。

Note

IAM 用於索引的角色不能用於資料來源。如果您不確定索引或常見問題集是否使用現有角色，請選擇 [建立新角色] 以避免發生錯誤。

- i. 選擇下一步。
7. 在 [設定同步設定] 頁面上，輸入下列資訊：
 - a. 在同步範圍中，從下列選項中選擇：
 - SQL 查詢 — 輸入 SQL 查詢陳述式，例如 SELECT 和 JOIN 作業。SQL 查詢必須小於 32 KB。Amazon Kendra 會編目符合您查詢的所有資料庫內容。
 - 主索引鍵欄 — 提供資料庫表格的主索引鍵。這標識數據庫中的一個表。
 - 標題欄 — 提供資料庫表格中文件標題欄的名稱。
 - 主體欄 — 提供資料庫表格中文件主體欄的名稱。
 - b. 在 [其他設定 — 選用] 中，從下列選項中選擇以同步特定內容，而非同步所有檔案：
 - 變更偵測欄 — 輸入 Amazon Kendra 將用來偵測內容變更的欄名稱。Amazon Kendra 當這些資料行中有任何變更時，會重新建立內容的索引。
 - 使用者 ID 欄 — 輸入包含允許存取內容的使用者 ID 的欄名稱。
 - 群組欄 — 輸入包含允許存取內容之群組的欄名稱。
 - 來源 URL 欄 — 輸入包含要編製索引之來源 URL 的資料欄名稱。
 - 時間戳記欄 — 輸入包含時間戳記的欄名稱。Amazon Kendra 使用時間戳記資訊偵測內容中的變更，並僅同步變更的內容。
 - [時區] 欄 — 輸入資料欄的名稱，其中包含要編目之內容的時區。
 - 時間戳記格式 — 輸入包含時間戳記格式的欄名稱，可用來偵測內容變更並重新同步處理內容。
 - c. 同步模式 — 選擇資料來源內容變更時要如何更新索引。當您第一次將資料來源同 Amazon Kendra 步處理時，依預設會檢索所有內容並建立索引。如果初始同步失敗，您必須執行資料的完整同步處理，即使您沒有選擇完整同步作為同步模式選項。
 - 完全同步：新鮮索引所有內容，並在每次資料來源與索引同步時取代現有內容。
 - 新增、修改的同步：每次資料來源與索引同步時，僅對新內容和已修改的內容建立索引。Amazon Kendra 可以使用資料來源的機制來追蹤內容變更，並為上次同步後變更的內容建立索引。

- 新增、修改、刪除的同步：每次資料來源與索引同步時，僅對新內容、已修改和刪除的內容建立索引。Amazon Kendra 可以使用資料來源的機制來追蹤內容變更，並為上次同步後變更的內容建立索引。
 - d. 在同步執行排程中，對於頻率 — 與資料來源同步的頻率。Amazon Kendra
 - e. 選擇下一步。
8. 在 [設定欄位對映] 頁面上，輸入下列資訊：
- a. 從產生的預設資料來源欄位中選取您要對應至 Amazon Kendra 索引的文件 ID、文件標題和來源 URL。
 - b. 新增欄位 — 新增自訂資料來源欄位，以建立要對映的索引欄位名稱和欄位資料類型。
 - c. 選擇下一步。
9. 在 [檢閱並建立] 頁面上，檢查您輸入的資訊是否正確，然後選取 [新增資料來源]。您也可以從此頁面選擇編輯您的資訊。成功新增資料來源後，您的資料來源將顯示在 [資料來源] 頁面上。

API

若要連線 Amazon Kendra 到 Amazon RDS (Oracle)

您必須使用 [TemplateConfiguration](#) API 指定下列項目：

- 資料來源 — 指定使用 [TemplateConfiguration](#) JSON 結構定義 JDBC 時的資料來源類型。同時將資料來源指定為呼叫 [CreateDataSource](#) API TEMPLATE 時的方式。
- 資料庫類型 — 您必須將資料庫類型指定為 `oracle`。
- SQL 查詢 — 指定 SQL 查詢陳述式，例如 SELECT 和 JOIN 作業。SQL 查詢必須小於 32 KB。Amazon Kendra 會編目符合您查詢的所有資料庫內容。
- 同步模式 — 指定資料來源內容變更時 Amazon Kendra 應如何更新索引。當您第一次將資料來源同 Amazon Kendra 步處理時，依預設會檢索所有內容並建立索引。如果初始同步失敗，您必須執行資料的完整同步處理，即使您沒有選擇完整同步作為同步模式選項。您可以選擇：
 - FORCED_FULL_CRAWL 新建索引所有內容，並在每次資料來源與索引同步時取代現有內容。
 - FULL_CRAWL，以在每次資料來源與索引同步時，僅對新的、修改的和刪除的內容建立索引。Amazon Kendra 可以使用資料來源的機制來追蹤內容變更，並為上次同步後變更的內容建立索引。
 - CHANGE_LOG 每次資料來源與索引同步時，僅對新內容和修改的內容建立索引。Amazon Kendra 可以使用資料來源的機制來追蹤內容變更，並為上次同步後變更的內容建立索引。

- 秘密 Amazon 資源名稱 (ARN) — 提供包含您在帳戶中建立的身份驗證登入資料的 Secrets Manager 密碼的 Amazon 資源名稱 (ARN)。Amazon RDS (Oracle)密碼會以下列金鑰儲存在 JSON 結構中：

```
{
  "user name": "database user name",
  "password": "password"
}
```

Note

我們建議您定期重新整理或輪換您的認證和密碼。僅為您自己的安全提供必要的訪問級別。我們不建議您跨資料來源以及連接器 1.0 和 2.0 版 (如果適用) 重複使用認證和密碼。

- IAM role — 指定RoleArn何時呼叫CreateDataSource以提供具有存取 Secrets Manager 密碼之權限的 IAM 角色，以及呼叫Amazon RDS (Oracle)連接器和 Amazon Kendra所需公用 API 的時間。有關詳情，請參閱[Amazon RDS \(Oracle\)料來源的IAM 角色](#)。

您還可以添加以下可選功能：

- Virtual Private Cloud (VPC) — 指定您撥打電話的VpcConfiguration時間。CreateDataSource如需詳細資訊，請參閱 [配置 Amazon Kendra 為使用 Amazon VPC](#)。
- 包含和排除篩選器 — 您可以指定是否要使用使用者 ID、群組、來源 URL、時間戳記和時區來包含特定內容。
- 使用者前後關聯篩選與存取控制 — Amazon Kendra 探索文件的存取控制清單 (ACL) (如果您有文件的 ACL)。ACL 資訊可用來根據使用者或使用者對文件的群組存取權來篩選搜尋結果。如需詳細資訊，請參閱[使用者內容篩選](#)。
- 欄位對映 — 選擇將Amazon RDS (Oracle)料來源欄位對映至 Amazon Kendra 索引欄位。如需詳細資訊，請參閱[映射資料來源欄位](#)。

Note

您的文件需要文件內文欄位或文件內文對等項目，才能搜尋您的文件。Amazon Kendra 您必須將資料來源中的文件內文欄位名稱對應至索引欄位名稱_document_body。所有其他欄位是選用的。

如需要設定的其他重要 JSON 金鑰清單，請參閱[Amazon RDS \(甲骨文\) 樣板綱要](#)。

備註

- Amazon Kendra 檢查更新的內容時，不會追蹤已刪除的資料庫列。
- 資料庫中一列中欄位名稱和值的大小不得超過 400 KB。
- 如果您的資料庫資料來源中有大量資料，並且不想 Amazon Kendra 在第一次同步之後對所有資料庫內容建立索引，則可以選擇僅同步新文件、修改或刪除的文件。
- 最佳作法是提供 Amazon Kendra 唯讀資料庫認證。
- 最佳做法是避免新增包含敏感資料或個人可識別資訊 (PII) 的表格。

Amazon RDS (PostgreSQL)

Amazon RDS 是一種 Web 服務，可讓您更輕鬆地在 AWS 雲端中設定、操作和擴展關聯式資料庫。如果您是使用 Amazon RDS 者，則可以使用 Amazon Kendra 對 Amazon RDS (PostgreSQL) 資料來源建立索引。Amazon Kendra Amazon RDS (PostgreSQL) 資料來源連接器支援 PostgreSQL 9.6。

您可以使用[Amazon Kendra 主控台](#)和 [TemplateConfiguration](#) API 連線 Amazon Kendra 到 Amazon RDS (PostgreSQL) 資料來源。

如需疑難排解 Amazon Kendra Amazon RDS (PostgreSQL) 資料來源連接器，請參閱[疑難排解資料](#)。

主題

- [支援的功能](#)
- [必要條件](#)
- [連接說明](#)
- [備註](#)

支援的功能

- 欄位對映
- 使用者內容篩選
- 包含/排除過濾器
- 完整和增量內容同步

- 虛擬私有雲端 (VPC)

必要條件

在您可以用來 Amazon Kendra 為 Amazon RDS (PostgreSQL) 資料來源建立索引之前，請先在 Amazon RDS (PostgreSQL) 和 AWS 帳戶中進行這些變更。

在中 Amazon RDS (PostgreSQL)，請確定您有：

- 記下您的資料庫使用者名稱和密碼。

Important

最佳作法是提供 Amazon Kendra 唯讀資料庫認證。

- 複製您的資料庫主機 URL、連接埠和執行個體。您可以在 Amazon RDS 控制台上找到此信息。
- 已勾選的每個文件在您打算用於相同索引的其他資料來源中 Amazon RDS (PostgreSQL) 和其他資料來源之間都是唯一的。您要用於索引的每個資料來源不得包含跨資料來源的相同文件。文件 ID 對索引來說是全域的，而且每個索引必須是唯一的。

在您的中 AWS 帳戶，請確保您有：

- [建立 Amazon Kendra 索引](#)，如果使用 API，則會記下索引識別碼。
- 為您的 [資料來源建立 IAM 角色](#)，如果使用 API，則會記錄 IAM 角色的 ARN。

Note

如果您變更驗證類型和認證，則必須更新 IAM 角色才能存取正確的 AWS Secrets Manager 密碼 ID。

- 將您的 Amazon RDS (PostgreSQL) 身份驗證憑據存儲在 AWS Secrets Manager 密鑰中，如果使用 API，則記錄密鑰的 ARN。

Note

我們建議您定期重新整理或輪換您的認證和密碼。僅為您自己的安全提供必要的訪問級別。我們不建議您跨資料來源以及連接器 1.0 和 2.0 版 (如果適用) 重複使用認證和密碼。

如果您沒有現有的 IAM 角色或密碼，則可以在將 Amazon RDS (PostgreSQL) 資料來源連線到時使用主控台建立新 IAM 角色和 Secrets Manager 密碼 Amazon Kendra。如果您使用 API，則必須提供現有 IAM 角色和 Secrets Manager 密碼的 ARN 以及索引 ID。

連接說明

若要連線 Amazon Kendra 到 Amazon RDS (PostgreSQL) 資料來源，您必須提供 Amazon RDS (PostgreSQL) 認證的詳細資料，Amazon Kendra 以便能夠存取您的資料。如果您尚未設定「Amazon Kendra 請 Amazon RDS (PostgreSQL) 參閱 [必要條件](#)」。

Console

若要連線 Amazon Kendra 到 Amazon RDS (PostgreSQL)


1. 登入 AWS Management Console 並開啟 [Amazon Kendra 主控台](#)。
2. 在左側導覽窗格中，選擇 [索引]，然後從索引清單中選擇要使用的索引。

Note

您可以選擇在索引設置下配置或編輯您的用戶訪問控制設置。

3. 在 [開始使用] 頁面上，選擇 [新增資料來源]。
4. 在 [新增資料來源] 頁面上，選擇 [Amazon RDS (PostgreSQL) 連接器]，然後選擇 [新增連接器]。如果使用版本 2 (如果適用)，請選擇帶有「V2.0」標籤的 Amazon RDS (PostgreSQL) 連接器。
5. 在 [指定資料來源詳細資訊] 頁面上，輸入下列資訊：
 - a. 在名稱和說明中，對於資料來源名稱 — 輸入資料來源的名稱。您可以包含連字號，但不能包含空格。
 - b. (選擇性) 說明 — 輸入資料來源的選用說明。
 - c. 在預設語言中 — 選擇一種語言來篩選索引的文件。除非另有指定，否則語言預設為英文。文件中繼資料中指定的語言會覆寫選取的語言。
 - d. 在「標籤」中，針對「新增標籤」 — 包含可選標籤以搜尋和篩選資源或追蹤 AWS 成本。
 - e. 選擇下一步。
6. 在 [定義存取權和安全性] 頁面上，輸入下列資訊：
 - a. 在來源中，輸入下列資訊：

- b. 主機 — 輸入資料庫主機 URL，例如：`http://instance URL.region.rds.amazonaws.com`。
- c. 連接埠 — 輸入資料庫連接埠，例如5432。
- d. 執行處理 — 例如，輸入資料庫執行處理postgres。
- e. 啟用 SSL 憑證位置 — 選擇此選項可輸入 SSL 憑證檔案的 Amazon S3 路徑。
- f. 在驗證中 — 輸入下列資訊：
 - AWS Secrets Manager 祕密 — 選擇現有密碼或建立新 Secrets Manager 密碼來儲存您的 Amazon RDS (PostgreSQL) 驗證認證。如果您選擇建立新密碼，則會開啟一個 AWS Secrets Manager 密碼視窗。
 - A. 在「建立 AWS Secrets Manager 密碼視窗」中輸入下列資訊：
 - I. 秘密名稱 — 您秘密的名稱。前綴 'AmazonKendraAmazon RDS (PostgreSQL)-' 會自動添加到您的密碼名稱中。
 - II. 對於資料庫使用者名稱和密碼 — 輸入您從資料庫複製的驗證認證值。
 - B. 選擇儲存。
- g. Virtual Private Cloud (VPC) (VPC) — 您可以選擇使用 VPC。如果是這樣，您必須新增子網路和 VPC 安全性群組。
- h. IAM role — 選擇現有 IAM 角色或建立新 IAM 角色以存取存放庫認證和索引內容。

 Note

IAM 用於索引的角色不能用於資料來源。如果您不確定索引或常見問題集是否使用現有角色，請選擇 [建立新角色] 以避免發生錯誤。

- i. 選擇下一步。
7. 在 [設定同步設定] 頁面上，輸入下列資訊：
 - a. 在同步範圍中，從下列選項中選擇：
 - SQL 查詢 — 輸入 SQL 查詢陳述式，例如選取和聯結作業。SQL 查詢必須小於 32 KB 的 SQL 查詢小於 32 KB，且不得包含任何分號 (;)。Amazon Kendra 會編目符合您查詢的所有資料庫內容。
 - 主索引鍵欄 — 提供資料庫表格的主索引鍵。這標識數據庫中的一個表。
 - 標題欄 — 提供資料庫表格中文件標題欄的名稱。

- 主體欄 — 提供資料庫表格中文件主體欄的名稱。
 - b. 在 [其他設定 — 選用] 中，從下列選項中選擇以同步特定內容，而非同步所有檔案：
 - 變更偵測欄 — 輸入 Amazon Kendra 將用來偵測內容變更的欄名稱。Amazon Kendra 當這些資料行中有任何變更時，會重新建立內容的索引。
 - 使用者 ID 欄 — 輸入包含允許存取內容的使用者 ID 的欄名稱。
 - 群組欄 — 輸入包含允許存取內容之群組的欄名稱。
 - 來源 URL 欄 — 輸入包含要編製索引之來源 URL 的資料欄名稱。
 - 時間戳記欄 — 輸入包含時間戳記的欄名稱。Amazon Kendra 使用時間戳記資訊偵測內容中的變更，並僅同步變更的內容。
 - [時區] 欄 — 輸入資料欄的名稱，其中包含要編目之內容的時區。
 - 時間戳記格式 — 輸入包含時間戳記格式的欄名稱，可用來偵測內容變更並重新同步處理內容。
 - c. 同步模式 — 選擇資料來源內容變更時要如何更新索引。當您第一次將資料來源同 Amazon Kendra 步處理時，依預設會檢索所有內容並建立索引。如果初始同步失敗，您必須執行資料的完整同步，即使您沒有選擇完整同步作為同步模式選項。
 - 完全同步：新鮮索引所有內容，並在每次資料來源與索引同步時取代現有內容。
 - 新增、修改的同步：每次資料來源與索引同步時，僅對新內容和已修改的內容建立索引。Amazon Kendra 可以使用資料來源的機制來追蹤內容變更，並為上次同步後變更的內容建立索引。
 - 新增、修改、刪除的同步：每次資料來源與索引同步時，僅對新內容、已修改和刪除的內容建立索引。Amazon Kendra 可以使用資料來源的機制來追蹤內容變更，並為上次同步後變更的內容建立索引。
 - d. 在同步執行排程中，對於頻率 — 與資料來源同步的頻率。Amazon Kendra
 - e. 選擇下一步。
8. 在 [設定欄位對映] 頁面上，輸入下列資訊：
- a. 從產生的預設資料來源欄位中選取您要對應至 Amazon Kendra 索引的文件 ID、文件標題和來源 URL。
 - b. 新增欄位 — 新增自訂資料來源欄位，以建立要對映的索引欄位名稱和欄位資料類型。
 - c. 選擇下一步。
9. 在 [檢閱並建立] 頁面上，檢查您輸入的資訊是否正確，然後選取 [新增資料來源]。您也可以從此頁面選擇編輯您的資訊。成功新增資料來源後，您的資料來源將顯示在 [資料來源] 頁面上。

API

若要連線 Amazon Kendra 到 Amazon RDS (PostgreSQL)

您必須使用 [TemplateConfiguration](#) API 指定下列項目：

- 資料來源 — 指定使用 [TemplateConfiguration](#) JSON 結構定義 JDBC 時的資料來源類型。同時將資料來源指定為呼叫 [CreateDataSource](#) API TEMPLATE 時的方式。
- 資料庫類型 — 您必須將資料庫類型指定為 postgresql。
- SQL 查詢 — 指定 SQL 查詢陳述式，例如 SELECT 和 JOIN 作業。SQL 查詢必須小於 32 KB。Amazon Kendra 會編目符合您查詢的所有資料庫內容。
- 同步模式 — 指定資料來源內容變更時 Amazon Kendra 應如何更新索引。當您第一次將資料來源同 Amazon Kendra 步處理時，依預設會檢索所有內容並建立索引。如果初始同步失敗，您必須執行資料的完整同步，即使您沒有選擇完整同步作為同步模式選項。您可以選擇：
 - FORCED_FULL_CRAWL 新建索引所有內容，並在每次資料來源與索引同步時取代現有內容。
 - FULL_CRAWL，以在每次資料來源與索引同步時，僅對新的、修改的和刪除的內容建立索引。Amazon Kendra 可以使用資料來源的機制來追蹤內容變更，並為上次同步後變更的內容建立索引。
 - CHANGE_LOG 每次資料來源與索引同步時，僅對新內容和修改的內容建立索引。Amazon Kendra 可以使用資料來源的機制來追蹤內容變更，並為上次同步後變更的內容建立索引。
- 秘密 Amazon 資源名稱 (ARN) — 提供包含您在帳戶中建立的身份驗證登入資料的 Secrets Manager 密碼的 Amazon 資源名稱 (ARN)。Amazon RDS (PostgreSQL) 密碼會以下列金鑰儲存在 JSON 結構中：

```
{
  "user name": "database user name",
  "password": "password"
}
```


Note

我們建議您定期重新整理或輪換您的認證和密碼。僅為您自己的安全提供必要的訪問級別。我們不建議您跨資料來源以及連接器 1.0 和 2.0 版 (如果適用) 重複使用認證和密碼。

- IAM role — 指定RoleArn何時呼叫CreateDataSource以提供具有存取 Secrets Manager 密碼之權限的 IAM 角色，以及呼叫Amazon RDS (PostgreSQL)連接器和 Amazon Kendra所需公用 API 的時間。有關詳情，請參閱[Amazon RDS \(PostgreSQL\)料來源的IAM 角色](#)。

您還可以添加以下可選功能：

- Virtual Private Cloud (VPC) — 指定您撥打電話的VpcConfiguration時間。CreateDataSource如需詳細資訊，請參閱 [配置 Amazon Kendra 為使用 Amazon VPC](#)。
- 包含和排除篩選器 — 您可以指定是否要使用使用者 ID、群組、來源 URL、時間戳記和時區來包含特定內容。
- 使用者前後關聯篩選與存取控制 — Amazon Kendra 探索文件的存取控制清單 (ACL) (如果您有文件的 ACL)。ACL 資訊可用來根據使用者或使用者對文件的群組存取來篩選搜尋結果。如需詳細資訊，請參閱[使用者內容篩選](#)。
- 欄位對映 — 選擇將Amazon RDS (PostgreSQL)料來源欄位對映至 Amazon Kendra 索引欄位。如需詳細資訊，請參閱[映射資料來源欄位](#)。

 Note

您的文件需要文件內文欄位或文件內文對等項目，才能搜尋您的文件。Amazon Kendra 您必須將資料來源中的文件內文欄位名稱對應至索引欄位名稱_document_body。所有其他欄位是選用的。

如需要設定的其他重要 JSON 金鑰清單，請參閱[Amazon RDS 模板模板架構](#)。

備註

- Amazon Kendra 檢查更新的內容時，不會追蹤已刪除的資料庫列。
- 資料庫中一列中欄位名稱和值的大小不得超過 400 KB。
- 如果您的資料庫資料來源中有大量資料，並且不想 Amazon Kendra 在第一次同步之後對所有資料庫內容建立索引，則可以選擇僅同步新文件、修改或刪除的文件。
- 最佳作法是提供 Amazon Kendra 唯讀資料庫認證。
- 最佳做法是避免新增包含敏感資料或個人可識別資訊 (PII) 的表格。

Amazon S3

Amazon S3 是一種物件儲存服務，可將資料儲存為值區中的物件。您可以使 Amazon Kendra 用索引文件的 Amazon S3 值區儲存庫。

Warning

Amazon Kendra 不使用將權限授予 Amazon Kendra 主體與 S3 儲存貯體互動的儲存貯體政策。而是使用 IAM 角色。請確定該成員 Amazon Kendra 未包含在值區政策中，以避免在意外授與任意主體權限時出現任何資料安全性問題。不過，您可以新增值區政策，以便跨不同帳戶使用 Amazon S3 儲存貯體。如需詳細資訊，請參閱[Amazon S3 跨帳戶使用的政策](#) (在 S3 IAM 角色索引標籤的資料來源 IAM 角色下)。如需 S3 資料來源 IAM 角色的相關資訊，請參閱[IAM 角色](#)。

Note

Amazon Kendra 現在支援升級的 Amazon S3 連接器。
主機已自動為您升級。您在主控台中建立的任何新連接器都會使用升級的架構。如果您使用 API，您現在必須使用[TemplateConfiguration](#)物件而非S3DataSourceConfiguration物件來設定連接器。
使用舊版主控台和 API 架構設定的連接器將繼續如設定般運作。但是，您將無法編輯或更新它們。如果您要編輯或更新連接器組態，您必須建立新的連接器。
我們建議您將連接器工作流程移轉至升級版本。使用舊架構設定的連接器 Support 排程於 2024 年 6 月結束。

您可以使用[Amazon Kendra 主控台](#)或 [TemplateConfiguration](#)API 連線到 Amazon S3 資料來源。

Note

若要產生 Amazon S3 資料來源的同步狀態報告，請參閱[疑難排解資料來源](#)。

如需 Amazon Kendra S3 資料來源連接器的疑難排解，請參閱[疑難排解資料來](#)。

主題

- [支援的功能](#)

- [必要條件](#)
- [連接說明](#)
- [建立資 Amazon S3 料來源](#)
- [Amazon S3 文件元資料](#)
- [Amazon S3 資料來源的存取控制](#)
- [Amazon VPC 與資 Amazon S3 料來源搭配使用](#)

支援的功能

- 欄位對映
- 使用者存取控制
- 包含/排除過濾器
- 完整和增量內容同步
- 虛擬私有雲端 (VPC)

必要條件

在您可以使用 Amazon Kendra 來為 S3 資料來源建立索引之前，請先在 S3 和 AWS 帳戶中進行這些變更。

在 S3 中，請確保您具有：

- 複製您的 Amazon S3 存儲桶的名稱。

Note

您的值區必須與 Amazon Kendra 索引位於相同的區域，且索引必須具有存取包含文件之值區的權限。

- 已核取的每個文件在 S3 和您打算用於相同索引的其他資料來源中都是唯一的。您要用於索引的每個資料來源不得包含跨資料來源的相同文件。文件 ID 對索引來說是全域的，而且每個索引必須是唯一的。

在您的 AWS 帳戶中，請確定您有：

- [建立 Amazon Kendra 索引](#)，如果使用 API，則會記下索引識別碼。

- 為您的資料來源建立 IAM 角色，如果使用 API，則會記錄 IAM 角色的 ARN。

如果您沒有現有 IAM 角色，則可以在將 S3 資料來源連接到時使用主控台建立新 IAM 角色 Amazon Kendra。如果您使用 API，則必須提供現有 IAM 角色的 ARN 和索引識別碼。

連接說明

若要連接 Amazon Kendra 到 S3 資料來源，您必須提供 S3 資料來源的必要詳細資訊，Amazon Kendra 以便能夠存取您的資料。如果您尚未為 S3 設定 Amazon Kendra，請參閱[必要條件](#)。

Console

若要連線 Amazon Kendra 到 Amazon S3

1. 登入 AWS Management Console 並開啟[Amazon Kendra 主控台](#)。
2. 在左側導覽窗格中，選擇 [索引]，然後從索引清單中選擇要使用的索引。

Note

您可以選擇在索引設置下配置或編輯用戶訪問控制設置。

3. 在 [開始使用] 頁面上，選擇 [新增資料來源]。
4. 在 [新增資料來源] 頁面上，選擇 [S3 連接器]，然後選擇 [新增連接器]。如果使用版本 2 (如果適用)，請選擇帶有「V2.0」標籤的 S3 連接器。
5. 在 [指定資料來源詳細資訊] 頁面上，輸入下列資訊：
 - a. 在名稱和說明中，對於資料來源名稱 — 輸入資料來源的名稱。您可以包含連字號，但不能包含空格。
 - b. (選擇性) 說明 — 輸入資料來源的選用說明。
 - c. 在預設語言中 — 選擇一種語言來篩選索引的文件。除非另有指定，否則語言預設為英文。文件中繼資料中指定的語言會覆寫選取的語言。
 - d. 在「標籤」中，針對「新增標籤」 — 包含可選標籤以搜尋和篩選資源或追蹤 AWS 成本。
 - e. 選擇下一步。
6. 在「定義存取權與安全性」頁面上，輸入下列選用資訊：
 - a. IAM role — 選擇現有 IAM 角色或建立新 IAM 角色以存取存放庫認證和索引內容。

Note

IAM 用於索引的角色不能用於資料來源。如果您不確定索引或常見問題集是否使用現有角色，請選擇 [建立新角色] 以避免發生錯誤。

- b. Virtual Private Cloud (VPC) (VPC) — 您可以選擇使用 VPC。如果是這樣，您必須新增子網路和 VPC 安全性群組。
 - c. 選擇下一步。
7. 在 [設定同步設定] 頁面上，輸入下列資訊：
- a. 對於資料來源位置 — 指定資料儲存 Amazon S3 區的路徑。選取瀏覽 S3 以選擇您的 S3 儲存貯體。
 - b. 針對檔案大小上限 — 指定以 MB 為單位的限制，以便只編目超過此限制的檔案。允許的最大 Amazon Kendra 檔案大小為 50 MB。
 - c. 對於 (選擇性) 中繼資料檔案首碼資料夾位置 — 指定儲存欄位/屬性和其他文件中繼資料的資料夾路徑。選取瀏覽 S3 以尋找您的中繼資料資料夾。
 - d. 針對 (選用) 存取控制清單組態檔案位置 — 指定包含使用者 JSON 結構及其文件存取權的檔案路徑。選取瀏覽 S3 以尋找您的 ACL 檔案。
 - e. (選擇性) 選取解密金鑰 — 選取以使用解密金鑰。您可以選擇使用現有的 AWS KMS 金鑰。
 - f. 針對 (選用) 其他組態-新增陣列以包含或排除某些檔案。所有路徑均相對於資料來源位置 S3 儲存貯體。
 - g. 同步模式 — 選擇資料來源內容變更時要如何更新索引。當您第一次將資料來源同 Amazon Kendra 步處理時，依預設會檢索所有內容並建立索引。如果初始同步失敗，您必須執行資料的完整同步，即使您沒有選擇完整同步作為同步模式選項。
 - 完全同步：新鮮索引所有內容，並在每次資料來源與索引同步時取代現有內容。
 - 新增、修改、刪除的同步：每次資料來源與索引同步時，僅對新內容、已修改和刪除的內容建立索引。Amazon Kendra 可以使用資料來源的機制來追蹤內容變更，並為上次同步後變更的內容建立索引。
 - h. 在同步執行排程中，對於頻率 — 選擇同步資料來源內容和更新索引的頻率。
 - i. 選擇下一步。
8. 在 [設定欄位對映] 頁面上，輸入下列選用資訊：

- a. 預設欄位對映 — 從 Amazon Kendra 產生的預設資料來源欄位中選取您要對映至索引的欄位。
 - b. 新增欄位 — 選擇新增自訂資料來源欄位，以建立要對映的索引欄位名稱和欄位資料類型。
 - c. 選擇下一步。
9. 在 [檢閱並建立] 頁面上，檢查您輸入的資訊是否正確，然後選取 [新增資料來源]。您也可以從此頁面選擇編輯您的資訊。成功新增資料來源後，您的資料來源將顯示在 [資料來源] 頁面上。

API

若要連線 Amazon Kendra 到 Amazon S3

您必須使用 [TemplateConfiguration](#) API 指定 [資料來源結構描述](#) 的 JSON。您必須提供以下信息：

- 資料來源 — 指定使用 [TemplateConfiguration](#) JSON 結構定義 S3 時的資料來源類型。同時指定呼叫 [CreateDataSource](#) API TEMPLATE 時的資料來源。
- BucketName 包含文件的值區名稱。
- 同步模式 — 指定資料來源內容變更時 Amazon Kendra 應如何更新索引。當您第一次將資料來源同 Amazon Kendra 步處理時，依預設會檢索所有內容並建立索引。如果初始同步失敗，您必須執行資料的完整同步，即使您沒有選擇完整同步作為同步模式選項。您可以選擇：
 - FORCED_FULL_CRAWL 新建索引所有內容，並在每次資料來源與索引同步時取代現有內容。
 - FULL_CRAWL，以在每次資料來源與索引同步時，僅對新的、修改的和刪除的內容建立索引。Amazon Kendra 可以使用資料來源的機制來追蹤內容變更，並為上次同步後變更的內容建立索引。
- IAM role — 指定 RoleArn 何時呼叫 CreateDataSource 以提供具有存取 Secrets Manager 密碼的權限的 IAM 角色，以及呼叫 S3 連接器和 Amazon Kendra 所需的公用 API。如需詳細資訊，請參閱 [S3 資料來源的 IAM 角色](#)。

您還可以添加以下可選功能：

- Virtual Private Cloud (VPC) — 指定您撥打電話的 VpcConfiguration 時間。CreateDataSource 如需詳細資訊，請參閱 [配置 Amazon Kendra 為使用 Amazon VPC](#)。
- 包含和排除篩選器 — 指定要包含還是排除特定檔案名稱、檔案類型和檔案路徑。您可以使用 glob 模式（可以將通配符模式擴展到與給定模式匹配的路徑名稱列表中的模式）。如需範例，請參閱 AWS CLI 命令參考中 [的使用排除和包含篩選器](#)。

- 文件中繼資料和存取控制組態 — 新增文件中繼資料和存取控制檔案，其中包含來源 URI、文件作者或自訂文件屬性/欄位等資訊，以及您的使用者及其可存取的文件。每個中繼資料檔案都包含單一文件的相關中繼資料。
- 欄位對映 — 選擇將 S3 資料來源欄位對應至 Amazon Kendra 索引欄位。如需詳細資訊，請參閱[映射資料來源欄位](#)。

Note

您的文件需要文件內文欄位或文件內文對等項目，才能搜尋您的文件。Amazon Kendra 您必須將資料來源中的文件內文欄位名稱對應至索引欄位名稱_document_body。所有其他欄位是選用的。

如需要設定的其他重要 JSON 金鑰清單，請參閱[S3 範本結構定義](#)。

進一步了解

若要進一步了解 Amazon Kendra 與 S3 資料來源整合的相關資訊，請參閱：

- [使用具有 VPC 支援的 Amazon Kendra S3 連接器準確搜尋答案](#)

建立 Amazon S3 資料來源

下列範例會示範建立 Amazon S3 資料來源。這些範例假設您已經建立索引和具有讀取索引資料之權限的 IAM 角色。如需有關 IAM 角色的詳細資訊，請參閱[IAM 存取角色](#)。如需有關建立索引的詳細資訊，請參閱[建立索引](#)。

CLI

```
aws kendra create-data-source \  
  --index-id index ID \  
  --name example-data-source \  
  --type S3 \  
  --configuration '{"S3Configuration":{"BucketName":"bucket name"}}' \  
  --role-arn 'arn:aws:iam::account id:role:/role name'
```

Python

下面的 Python 代碼片段創建一個 Amazon S3 數據源。如需完整範例，請參閱[開始使用 \(AWS SDK for Python \(Boto3\)\)](#)。

```
print("Create an Amazon S3 data source.")

# Provide a name for the data source
name = "getting-started-data-source"
# Provide an optional description for the data source
description = "Getting started data source."
# Provide the IAM role ARN required for data sources
role_arn = "arn:aws:iam::${accountID}:role/${roleName}"
# Provide the data source connection information
s3_bucket_name = "S3-bucket-name"
type = "S3"
# Configure the data source
configuration = {"S3DataSourceConfiguration":
    {
        "BucketName": s3_bucket_name
    }
}

data_source_response = kendra.create_data_source(
    Configuration = configuration,
    Name = name,
    Description = description,
    RoleArn = role_arn,
    Type = type,
    IndexId = index_id
)
```

建立資料來源可能需要一些時間。您可以使用 [DescribeDataSource](#) API 監控進度。當資料來源狀態為ACTIVE資料來源可供使用時。

下列範例會示範取得資料來源的狀態。

CLI

```
aws kendra describe-data-source \
  --index-id index ID \
  --id data source ID
```

Python

下列 Python 程式碼片段會取得 S3 資料來源的相關資訊。如需完整範例，請參閱[開始使用 \(AWS SDK for Python \(Boto3\)\)](#)。

```
print("Wait for Amazon Kendra to create the data source.")

while True:
    data_source_description = kendra.describe_data_source(
        Id = "data-source-id",
        IndexId = "index-id"
    )
    status = data_source_description["Status"]
    print(" Creating data source. Status: "+status)
    time.sleep(60)
    if status != "CREATING":
        break
```

此資料來源沒有排程，因此不會自動執行。若要為資料來源建立索引，[StartDataSourceSyncJob](#)請呼叫以將索引與資料來源同步化。

下列範例示範同步處理資料來源。

CLI

```
aws kendra start-data-source-sync-job \
  --index-id index ID \
  --id data source ID
```

Python

下面的 Python 代碼片段同步的數 Amazon S3 據源。如需完整範例，請參閱[開始使用 \(AWS SDK for Python \(Boto3\)\)](#)。

```
print("Synchronize the data source.")

sync_response = kendra.start_data_source_sync_job(
    Id = "data-source-id",
    IndexId = "index-id"
)
```

Amazon S3 文件元資料

您可以使用中繼資料檔案，將中繼資料 (文件的其他相關資訊) 新增至 Amazon S3 值區中的文件。每個中繼資料檔案都與索引文件相關聯。

您的中繼資料檔案必須儲存在與索引檔案相同的儲存貯體中。您可以在建立資料來源時，使用主控台或 DocumentsMetadataConfiguration 參數 S3Prefix 欄位為中繼 Amazon S3 資料檔案指定值區中的位置。如果您沒有指定 Amazon S3 字首，您的中繼資料檔案必須儲存在與索引文件相同的位置。

如果您為中繼資料檔案指定 Amazon S3 前置詞，它們會在與索引文件 parallel 的目錄結構中。Amazon Kendra 只會在指定的目錄中尋找您的中繼資料。如果未讀取中繼資料，請檢查目錄位置是否符合中繼資料的位置。

下列範例顯示索引文件位置如何對應至中繼資料檔案位置。請注意，文件的 Amazon S3 索引鍵會附加至中繼資料的 Amazon S3 前置字元，然後加上後綴 .metadata.json 以形成中繼資料檔案的 Amazon S3 路徑。具有中繼資料 Amazon S3 前 .metadata.json 綴和後綴的組合 Amazon S3 鍵不得超過 1024 個字符。建議您將 Amazon S3 金鑰保持在 1000 個字元以下，以便在結合金鑰與前置字元和尾碼時考慮其他字元。

```
Bucket name:
  s3://bucketName
Document path:
  documents
Metadata path:
  none
File mapping
  s3://bucketName/documents/file.txt ->
  s3://bucketName/documents/file.txt.metadata.json
```

```
Bucket name:
  s3://bucketName
Document path:
  documents/legal
Metadata path:
  metadata
File mapping
  s3://bucketName/documents/legal/file.txt ->
  s3://bucketName/metadata/documents/legal/file.txt.metadata.json
```

您的文件中繼資料是在 JSON 檔案中定義的。該文件必須是一個不帶 BOM 標識的 UTF-8 文本文件。JSON 檔案的檔案名稱必須是 <document>.<extension>.metadata.json。在此範例中，

「document」是中繼資料套用的文件名稱，而「副檔名」是文件的副檔名。中的文件 ID 必須是唯一的<document>.<extension>.metadata.json。

JSON 檔案的內容遵循此範本。所有屬性/字段都是可選的，因此不需要包含所有屬性。您必須為要包含的每個屬性提供一個值；該值不能為空。如果未指定_source_uri，則搜尋結果 Amazon Kendra 中傳回的連結會指向包含文件的 Amazon S3 值區。DocumentId會對應至欄位，s3_document_id並且是 S3 中文件的絕對路徑。

```
{
  "DocumentId": "S3 document ID, the S3 path to doc",
  "Attributes": {
    "_category": "document category",
    "_created_at": "ISO 8601 encoded string",
    "_last_updated_at": "ISO 8601 encoded string",
    "_source_uri": "document URI",
    "_version": "file version",
    "_view_count": number of times document has been viewed,
    "custom attribute key": "custom attribute value",
    additional custom attributes
  },
  "AccessControlList": [
    {
      "Name": "user name",
      "Type": "GROUP | USER",
      "Access": "ALLOW | DENY"
    }
  ],
  "Title": "document title",
  "ContentType": "For example HTML | PDF. For supported content types, see Types of documents."
}
```

_created_at和中_last_updated_at繼資料欄位是 ISO 8601 編碼的日期。例如，2012-03-25T12:30:10 + 01:00 是二零一二年三月二十五日的 ISO 8601 日期時間格式，在歐洲中部時區的下午 12 時 30 分（加上 10 秒）。

您可以將其他資訊新增至有關您用來篩選查詢或群組查詢回應之文件的Attributes欄位。如需詳細資訊，請參閱 [建立自訂文件欄位](#)。

您可以使用AccessControlList欄位來篩選查詢的回應。如此一來，只有特定使用者和群組才能存取文件。如需詳細資訊，請參閱 [篩選使用者內容](#)。

Amazon S3 資料來源的存取控制

您可以使用組態檔案控制對 Amazon S3 資料來源中文件的存取。您可以在主控台中指定檔案，或在呼叫 [CreateDataSource](#) 或 [UpdateDataSource](#) API 時指定為 `AccessControlListConfiguration` 參數。

組態檔案包含可識別 S3 前置詞的 JSON 結構，並列出前置詞的存取設定。前綴可以是路徑，也可以是單獨的文件。如果前置詞是路徑，則存取設定會套用至該路徑中的所有檔案。JSON 組態檔中有 S3 前置字元數目上限，預設檔案大小上限。如需更多資訊，請參閱 [配額 Amazon Kendra](#)

您可以在存取設定中指定使用者和群組。當您查詢索引時，您可以指定使用者和群組資訊。如需詳細資訊，請參閱 [依使用者屬性篩選](#)。

組態檔案的 JSON 結構必須採用下列格式：

```
[
  {
    "keyPrefix": "s3://BUCKETNAME/prefix1/",
    "aclEntries": [
      {
        "Name": "user1",
        "Type": "USER",
        "Access": "ALLOW"
      },
      {
        "Name": "group1",
        "Type": "GROUP",
        "Access": "DENY"
      }
    ]
  },
  {
    "keyPrefix": "s3://prefix2",
    "aclEntries": [
      {
        "Name": "user2",
        "Type": "USER",
        "Access": "ALLOW"
      },
      {
        "Name": "user1",
        "Type": "USER",
```

```
        "Access": "DENY"
      },
      {
        "Name": "group1",
        "Type": "GROUP",
        "Access": "DENY"
      }
    ]
  }
]
```

Amazon VPC 與資 Amazon S3 料來源搭配使用

本主題提供一個 step-by-step 範例，說明如何透過 Amazon VPC 使用 Amazon S3 連接器連接到 Amazon S3 儲存貯體。此範例假設您從現有的 S3 儲存貯體開始。我們建議您只將幾份文件上傳到 S3 儲存貯體，以測試範例。

您可以通過連接 Amazon Kendra 到 Amazon S3 儲存桶 Amazon VPC。若要這麼做，您必須在建立 Amazon S3 資料來源連接器時指定 Amazon VPC 子網路和 Amazon VPC 安全群組。

Important

如此一來，Amazon Kendra Amazon S3 連接器才能存取您的儲存 Amazon S3 貯體，請確定您已將 Amazon S3 端點指派給虛擬私有雲 (VPC)。

若 Amazon Kendra 要將文件從 Amazon S3 值區同步到 Amazon VPC，您必須完成以下步驟：

- 設定的 Amazon S3 端點 Amazon VPC。如需有關如何設定 Amazon S3 端點的詳細資訊，請參閱AWS PrivateLink 《指南》 Amazon S3中的 [《開道端點》](#)。
- (選擇性) 檢查 Amazon S3 儲存貯體政策，以確保儲存 Amazon S3 貯體可從您指派給的虛擬私有雲 (VPC) 存取 Amazon Kendra。如需詳細資訊，請參閱 Amazon S3 使用者指南中的 [使用儲存貯體政策控制來自 VPC 端點的存取](#)

步驟

- [步驟 1：配置 Amazon VPC](#)
- (選擇性) [步驟 2：設定 Amazon S3 值區政策](#)
- [步驟 3：建立測試 Amazon S3 資料來源連接器](#)

步驟 1：配置 Amazon VPC

建立虛擬私人雲端網路，包括具有 Amazon S3 閘道端點和安全群組的私有子網路，Amazon Kendra 以供日後使用。

使用私有子網路、S3 端點和安全群組設定 VPC

1. 登入 AWS Management Console 並開啟 Amazon VPC 主控台，位於 <https://console.aws.amazon.com/vpc/>。
2. 建立具有私有子網路和 S3 端點的 VPC Amazon Kendra 以供使用：

從功能窗格中選擇 [您的 VPC]，然後選擇 [建立 VPC]。

- a. 針對 Resources to create (建立資源)，選擇 VPC and more (VPC 等)。
- b. 對於「名稱」標籤，啟用「自動產生」，然後輸入 **kendra-s3-example**。
- c. 對於 IPv4 /IPv6 CIDR 區塊，請保留預設值。
- d. 對於可用區域 (AZ) 的數目，請選擇數字 1。
- e. 選取 [自訂 AZ]，然後從 [第一個可用區域] 清單中選取可用區域。

Amazon Kendra 僅支援一組特定的可用區域。

- f. 針對公用子網路數目，選擇數字 0。
- g. 在私人子網路的數目中，選擇數字 1。
- h. 對於 NAT gateways (NAT 閘道)，選擇 None (無)。
- i. 對於 VPC 端點，請選擇 Amazon S3 閘道。
- j. 將其餘值保留為預設設定。
- k. 選取 Create VPC (建立 VPC)。

等到建立 VPC 工作流程完成。然後，選擇查看 VPC 以檢查剛剛創建的 VPC。

您現在已建立具有私有子網路的 VPC 私人雲端網路，該子網路無法存取公用網際網路。

3. 複製您的 Amazon S3 端點的虛擬私人雲端端點識別碼：
 - a. 從導覽窗格中選擇端點。
 - b. 在「端點」清單中，找到您剛剛與 VPC 擬私人雲端一起建立的 Amazon S3 端點 **kendra-s3-example-vpce-s3**。

您現在已建立 Amazon S3 閘道端點，以透過子網路存取 Amazon S3 儲存貯體。

4. 建立 Amazon Kendra 要使用的安全性群組：
 - a. 從導覽窗格中選擇安全性群組，然後選取建立安全性群組。
 - b. 針對 Security group name (安全群組名稱)，輸入 **s3-data-source-security-group**。
 - c. 從 Amazon VPC 列表中選擇您的 VPC。
 - d. 將輸入規則和輸出規則保留為預設值。
 - e. 選擇建立安全群組。

您現在已建立 VPC 安全性群組。

您可以在連接器組態程序期間，將您建立的子網路和安全群組指派給 Amazon Kendra Amazon S3 資料來源連接器。

(選擇性) 步驟 2：設定 Amazon S3 值區政策

在此可選步驟中，了解如何設定 Amazon S3 儲存貯體政策，以便只能從您指派的 VPC 存取 Amazon S3 儲存貯體。 Amazon Kendra

Amazon Kendra 使用 IAM 角色存取您的 Amazon S3 儲存貯體，而且不需要設定 Amazon S3 儲存貯體政策。不過，如果您想要使用 Amazon S3 儲存貯體設定連接器，且該 Amazon S3 連接器具有限制從公用網際網路存取的現有政策，建立儲存貯體政策可能很有用。

若要設定 Amazon S3 值區政策

1. 在開啟 Amazon S3 主控台<https://console.aws.amazon.com/s3/>。
2. 在導覽窗格中，選擇「值區」。
3. 選擇您要同步處理的 Amazon S3 儲存貯體的名稱 Amazon Kendra。
4. 選擇 [權限] 索引標籤，向下捲動至 [儲存貯體政策]，然後按一下 [編輯]。
5. 新增或修改儲存貯體政策，以僅允許從您建立的 VPC 端點進行存取。

以下為儲存貯體政策的範例。以您先前 *vpce-id* 提到的 Amazon S3 儲存貯體名稱和 Amazon S3 端點識別碼取 *bucket-name* 代和。

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

```
"Statement": [  
  {  
    "Effect": "Deny",  
    "Principal": "*",  
    "Action": "s3:*",  
    "Resource": "arn:aws:s3:::bucket-name/*",  
    "Condition": {  
      "StringNotEquals": {  
        "aws:SourceVpce": "vpce-id"  
      }  
    }  
  }  
]
```

6. 選取儲存變更。

您的 S3 儲存貯體現在只能從您建立的特定 VPC 存取。

步驟 3：建立測試 Amazon S3 資料來源連接器

若要測試您的 Amazon VPC 組態，請建立 Amazon S3 連接器。然後，依照中[Amazon S3](#)所述的步驟，使用您建立的 VPC 進行設定。

對於 Amazon VPC 組態值，請選擇您在此範例中建立的值：

- Amazon VPC(VPC) — kendra-s3-example-vpc
- 子網路 — kendra-s3-example-subnet-private1-[availability zone]
- 安全性群組 — s3-data-source-security-group

等待連接器完成建立。建立 Amazon S3 連接器之後，選擇 [立即同步] 以啟動同步。

完成同步作業可能需要幾分鐘到數小時，視 Amazon S3 值區中的文件數量而定。若要測試範例，我們建議您只將幾份文件上傳到 S3 儲存貯體。如果您的設定正確，您最後應該會看到 [已完成] 的 [同步處理] 狀態。

如果遇到任何錯誤，請參閱[疑難排解 Amazon VPC 連線](#)。

Amazon Kendra 網絡爬蟲

您可以使用 Amazon Kendra Web 爬蟲來檢索和索引網頁。

您只能抓取使用安全通訊協定超文字傳輸通訊協定安全 (HTTPS) 的公開網站或公司內部網站。如果在網路爬取網站時收到錯誤訊息，可能是網站阻止網路爬取。要檢索內部網站，您可以設置 Web 代理。Web 代理必須面對公開。您也可以使用驗證來存取和檢索網站。

選取要索引的網站時，您必須遵守 [Amazon 可接受的使用政策](#) 以及 Amazon 所有其他條款。請記住，您只能使用 Amazon Kendra Web 爬蟲來索引您自己的網頁或您有權索引的網頁。要了解如何阻止 Amazon Kendra Web 爬蟲索引您的網站，請參閱 [設定 Amazon Kendra 網頁爬行者程式的 robots.txt 檔案](#)。

Note

濫用 Amazon Kendra Web 爬蟲積極抓取您不擁有的網站或網頁是不被認為是可接受的使用。

Amazon Kendra 有兩個版本的 web crawler 連接器。每個版本的支援功能包括：

Amazon Kendra 網路爬蟲連接器 1.0 /API [WebCrawlerConfiguration](#)

- 网络代理
- 包含/排除過濾器

Amazon Kendra 網路爬蟲連接器 2.0 版/API [TemplateConfiguration](#)

- 欄位對映
- 包含/排除過濾器
- 完整和增量內容同步
- 网络代理
- 適用於您網站的基本、NTLM /Kerberos、SAML 和表單驗證
- 虛擬私有雲端 (VPC)

Important

不支援建立 Web 爬行者程式 v2.0 連接器。AWS CloudFormation 如果您需 AWS CloudFormation 要支援，請使用 Web 爬行者程式 v1.0 連接器。

如需 Amazon Kendra Web 爬行者程式資料來源連接器的疑難排解，請參閱 [疑難排解資料來](#)。

主題

- [Amazon Kendra 網路爬蟲連接器 v1.0](#)
- [Amazon Kendra 網路爬蟲連接器 v2.0](#)
- [設定 Amazon Kendra 網頁爬行者程式的robots.txt檔案](#)

Amazon Kendra 網路爬蟲連接器 v1.0

您可以使用 Amazon Kendra Web 爬蟲來檢索和索引網頁。

您只能抓取使用安全通訊協定超文字傳輸通訊協定安全 (HTTPS) 的公開網站和網站。如果在網路爬取網站時收到錯誤訊息，可能是網站阻止網路爬取。要檢索內部網站，您可以設置 Web 代理。Web 代理必須面對公開。

選取要索引的網站時，您必須遵守 [Amazon 可接受的使用政策](#) 以及 Amazon 所有其他條款。請記住，您只能使用 Amazon Kendra Web 爬蟲來索引您自己的網頁或您有權索引的網頁。要了解如何阻止 Amazon Kendra Web 爬蟲索引您的網站，請參閱 [設定 Amazon Kendra 網頁爬行者程式的robots.txt檔案](#)。

Note

濫用 Amazon Kendra Web 爬蟲積極抓取您不擁有的網站或網頁是不被認為是可接受的使用。

如需 Amazon Kendra Web 爬行者程式資料來源連接器的疑難排解，請參閱 [疑難排解資料來](#)。

主題

- [支援的功能](#)
- [必要條件](#)
- [連接說明](#)
- [進一步了解](#)

支援的功能

- 网络代理
- 包含/排除過濾器

必要條件

在您可以使用索引您的 Amazon Kendra 的網站之前，請檢查您的網站和 AWS 帳戶的詳細資料。

對於您的網站，請確保您擁有：

- 複製您要索引的網站的種子或站點地圖 URL。
- 對於需要基本驗證的網站：記下使用者名稱和密碼，並複製網站的主機名稱和連接埠號碼。
- 選用性：如果您想要使用 Web Proxy 連線至您要檢索的內部網站，請複製網站的主機名稱和連接埠號碼。Web 代理必須面對公開。Amazon Kendra 支持連接到基本身份驗證支持的 Web 代理服務器，或者您可以在沒有身份驗證的情況下連接。
- 檢查您要索引的每個網頁文檔是唯一的，並且在您計劃用於相同索引的其他數據源中。您要用於索引的每個資料來源不得包含跨資料來源的相同文件。文件 ID 對索引來說是全域的，而且每個索引必須是唯一的。

在您的 AWS 帳戶中，請確定您有：

- [建立 Amazon Kendra 索引](#)，如果使用 API，則會記下索引識別碼。
- 為您的[資料來源建立 IAM 角色](#)，如果使用 API，則會記錄 IAM 角色的 ARN。

Note

如果您變更驗證類型和認證，則必須更新 IAM 角色才能存取正確的 AWS Secrets Manager 密碼 ID。

- 對於需要身份驗證的網站，或者如果使用具有身份驗證的 Web 代理，則將您的身份驗證憑據存儲在 AWS Secrets Manager 密鑰中，並且如果使用 API，則會記錄密鑰的 ARN。

Note

我們建議您定期重新整理或輪換您的認證和密碼。僅為您自己的安全提供必要的訪問級別。我們不建議您跨資料來源以及連接器 1.0 和 2.0 版 (如果適用) 重複使用認證和密碼。

如果您沒有現有的 IAM 角色或密碼，則可以在將 web crawler 資料來源連線到時使用主控台建立新 IAM 角色和 Secrets Manager 密碼 Amazon Kendra。如果您使用 API，則必須提供現有 IAM 角色和 Secrets Manager 密碼的 ARN，以及索引 ID。

連接說明

若要連線 Amazon Kendra 到 web crawler 資料來源，您必須提供資料來源的必要詳細 web crawler 資訊，Amazon Kendra 以便能夠存取您的資料。如果您尚未設定「Amazon Kendra 請 web crawler 參閱 [必要條件](#)」。

Console

若要連線 Amazon Kendra 到 web crawler

1. 登入 AWS Management Console 並開啟 [Amazon Kendra 主控台](#)。
2. 在左側導覽窗格中，選擇 [索引]，然後從索引清單中選擇要使用的索引。

Note

您可以選擇在索引設置下配置或編輯您的用戶訪問控制設置。

3. 在 [開始使用] 頁面上，選擇 [新增資料來源]。
4. 在 [新增資料來源] 頁面上，選擇 Web 爬行者程式連接器，然後選擇 [新增連接器]。如果使用第 2 版（如果適用），請選擇帶有「V2.0」標籤的 Web 爬行者程式連接器。
5. 在 [指定資料來源詳細資訊] 頁面上，輸入下列資訊：
 - a. 在名稱和說明中，對於資料來源名稱 — 輸入資料來源的名稱。您可以包含連字號，但不能包含空格。
 - b. (選擇性) 說明 — 輸入資料來源的選用說明。
 - c. 在預設語言中 — 選擇一種語言來篩選索引的文件。除非另有指定，否則語言預設為英文。文件中繼資料中指定的語言會覆寫選取的語言。
 - d. 在「標籤」中，針對「新增標籤」 — 包含可選標籤以搜尋和篩選資源或追蹤 AWS 成本。
 - e. 選擇下一步。
6. 在 [定義存取權和安全性] 頁面上，輸入下列資訊：
 - a. 對於「來源」，請根據您的使用案例選擇「來源 URL」和「來源網站地圖」，然後輸入每個網站地圖的值。

您最多可以新增 10 個來源 URL 和三個網站地圖。

Note

如果您要檢索 Sitemap，請檢查基礎或根網址是否與 Sitemap 頁面上列出的 URL 相同。例如，如果您的 Sitemap URL 是 `https://example.com/sitemap-page.html`，則此 Sitemap 頁面上列出的網址也應使用基本 URL 「`https://example.com/`」。

- b. (選擇性) 對於 Web 代理伺服器 — 輸入下列資訊：
 - i. 主機名稱 — 需要 Web Proxy 的主機名稱。
 - ii. 連接埠號碼 — 主機 URL 傳輸通訊協定所使用的連接埠。連接埠號碼應該是介於 0 到 65535 之間的數值。
 - iii. 對於 Web Proxy 憑證 — 如果您的 Web Proxy 連線需要驗證，請選擇現有密碼或建立新密碼來儲存您的驗證憑證。如果您選擇建立新密碼，則會開啟一個 AWS Secrets Manager 密碼視窗。
 - iv. 在「建立 AWS Secrets Manager Secrets Manager 密碼視窗」中輸入下列資訊：
 - A. 秘密名稱 — 您秘密的名稱。字首 'AmazonKendra-WebCrawler-' 會自動新增至您的密碼名稱。
 - B. 針對使用者名稱和密碼 — 輸入您網站的這些基本驗證憑證。
 - C. 選擇儲存。
- c. (選擇性) 具有驗證的主機 — 選取此選項可新增具有驗證的其他主機。
- d. IAM role — 選擇現有 IAM 角色或建立新 IAM 角色以存取存放庫認證和索引內容。

Note

IAM 用於索引的角色不能用於資料來源。如果您不確定索引或常見問題集是否使用現有角色，請選擇 [建立新角色] 以避免發生錯誤。

- e. 選擇下一步。
7. 在 [設定同步設定] 頁面上，輸入下列資訊：
 - a. 抓取範圍 — 選擇您要抓取的網頁類型。
 - b. 編目深度 — 從應編目的種子 URL 中選取層級 Amazon Kendra 數目。
 - c. 進階編目設定和其他組態輸入下列資訊：

- i. 檔案大小上限 — 要編目的網頁或附件大小上限。最小 1 MB (1 個字節)。最大值 50 MB
 - ii. 每頁最大連結數 — 每頁編目的連結數目上限。連結會依外觀順序編目。最少 1 個鏈接/頁面。每頁最多 1000 個連結。
 - iii. 節流上限 — 每分鐘每個主機名稱編目的 URL 數目上限。至少 1 個網址/主機名稱/分鐘。最多 300 個網址/主機名稱/分鐘。
 - iv. 正則表達式模式-添加正則表達式模式以包含或排除某些 URL。您最多可以添加 100 個圖案。
- d. 在同步執行排程中，對於頻率 — 選擇與資料來源同步的頻率。 Amazon Kendra
 - e. 選擇下一步。
8. 在 [檢閱並建立] 頁面上，檢查您輸入的資訊是否正確，然後選取 [新增資料來源]。您也可以從此頁面選擇編輯您的資訊。成功新增資料來源後，您的資料來源將顯示在 [資料來源] 頁面上。

API

若要連線 Amazon Kendra 到 web crawler

您必須使用 [WebCrawlerConfiguration](#) API 指定下列項目：

- URL — 指定網站的種子或起點 URL，或是您要使用 [SeedUrlConfiguration](#) 和 [SiteMapsConfiguration](#) 檢索之網站的 Sitemap URL。

Note

如果您要檢索 Sitemap，請檢查基礎或根網址是否與 Sitemap 頁面上列出的 URL 相同。例如，如果您的 Sitemap URL 是 `https://example.com/sitemap-page.html`，則此 Sitemap 頁面上列出的網址也應使用基本 URL 「`https://example.com/`」。

- 秘密 Amazon 資源名稱 (ARN) — 如果網站需要基本身份驗證，您需要提供主機名稱、連接埠號碼和密碼，以儲存使用者名稱和密碼的基本身份驗證登入資料。您可以使用 [AuthenticationConfiguration](#) API 提供秘密 ARN。密碼會以下列金鑰儲存在 JSON 結構中：


```
{
  "username": "user name",
  "password": "password"
}
```


您還可以使用 AWS Secrets Manager 密碼提供 Web 代理憑據。您可以使用 [ProxyConfiguration](#) API 提供網站主機名稱和連接埠號碼，以及選擇性地提供儲存 Web Proxy 憑證的密碼。

- IAM role — 指定 RoleArn 何時呼叫 CreateDataSource 以提供具有存取 Secrets Manager 密碼之權限的 IAM 角色，以及呼叫 Web 爬行者程式連接器和所需公用 API 的時間。Amazon Kendra 如需詳細資訊，請參閱 [Web 爬行者程式資料來源的 IAM 角色](#)。

您還可以添加以下可選功能：

- 編目模式：選擇是僅編目網站主機名稱，還是編目具有子網域的主機名稱，還是檢索網頁連結的其他網域。
- 從種子級別到爬網的「深度」或級別數。例如，種子 URL 頁面是深度 1，而此頁面上也經過探索的任何超連結都是深度 2。
- 單一網頁上要檢索的 URL 數目上限。
- 要抓取的網頁大小上限 (以 MB 為單位)。
- 每分鐘每個網站主機網路爬取的 URL 數目上限。
- 用於連線和爬取內部網站的 Web Proxy 主機和連接埠號碼。例如，的主機名稱 `https://a.example.com/page1.html` 是 "a.example.com"，連接埠號碼是 443，也就是 HTTPS 的標準連接埠。如果需要 Web Proxy 憑證才能連線到網站主機，您可以建立儲存 AWS Secrets Manager 認證的。
- 存取和檢索需要使用者驗證之網站的驗證資訊。
- 您可以使用「自訂文件強化」工具將 HTML 中繼標記擷取為欄位。如需詳細資訊，請參閱 [在擷取過程中自訂文件中繼資料](#)。如需擷取 HTML 中繼標記的範例，請參閱 [CDE 範例](#)。
- 包含和排除篩選器 — 指定要包含還是排除特定 URL。

 Note

大多數資料來源使用規則運算式模式，這些模式是稱為篩選器的包含或排除模式。如果您指定包含篩選器，則只有符合包含項目篩選器的內容會編製索引。不符合包含篩選器的任何文件都不會建立索引。如果您指定包含和排除篩選器，符合排除篩選器的文件將不會建立索引，即使它們符合包含篩選器也是如此。

進一步了解

若要進一步瞭解 Amazon Kendra 與web crawler資料來源整合的相關資訊，請參閱：

- [使用 Amazon Kendra 的 Web 爬蟲重新構想知識發現](#)

Amazon Kendra 網絡爬蟲連接器 v2.0

您可以使用 Amazon Kendra Web 爬蟲來檢索和索引網頁。

您只能抓取使用安全通訊協定超文字傳輸通訊協定安全 (HTTPS) 的公開網站或公司內部網站。如果在網路爬取網站時收到錯誤訊息，可能是網站阻止網路爬取。要檢索內部網站，您可以設置 Web 代理。Web 代理必須面對公開。您也可以使用驗證來存取和檢索網站。

Amazon Kendra 網絡爬蟲 v2.0 使用硒網絡爬蟲包和鉻驅動程序。Amazon Kendra 使用持續集成 (CI) 自動更新硒和鉻驅動程序的版本。

選取要索引的網站時，您必須遵守 [Amazon 可接受的使用政策](#) 以及 Amazon 所有其他條款。請記住，您只能使用 Amazon Kendra Web 爬蟲來索引您自己的網頁或您有權索引的網頁。要了解如何阻止 Amazon Kendra Web 爬蟲索引您的網站，請參閱 [設定 Amazon Kendra 網頁爬行者程式的 robots.txt 檔案](#)。濫用 Amazon Kendra Web 爬蟲積極抓取您不擁有的網站或網頁是不被認為是可接受的使用。

如需 Amazon Kendra Web 爬行者程式資料來源連接器的疑難排解，請參閱 [疑難排解資料來](#)。

Note

Web 爬行者程式連接器 v2.0 不支援從加密儲存貯體檢索網站清單 AWS KMS。Amazon S3 它僅支援使用 Amazon S3 受管理金鑰的伺服器端加密。

Important

不支援建立 Web 爬行者程式 v2.0 連接器。AWS CloudFormation 如果您需 AWS CloudFormation 要支援，請使用 Web 爬行者程式 v1.0 連接器。

主題

- [支援的功能](#)
- [必要條件](#)
- [連接說明](#)

支援的功能

- 欄位對映
- 包含/排除過濾器
- 完整和增量內容同步
- 网络代理
- 適用於您網站的基本、NTLM /Kerberos、SAML 和表單驗證
- 虛擬私有雲端 (VPC)

必要條件

在您可以使用索引您 Amazon Kendra 的網站之前，請檢查您的網站和 AWS 帳戶的詳細資料。

對於您的網站，請確保您擁有：

- 複製您要索引的網站的種子或站點地圖 URL。您可以將 URL 儲存在文字檔案中，然後將其上傳到 Amazon S3 值區。文字檔案中的每個 URL 都必須以個別的行格式化。如果您想要將網站地圖儲存在 Amazon S3 值區中，請確定您已複製 Sitemap XML，並將其儲存在 XML 檔案中。您也可以將多個網站地圖 XML 檔案分割成 ZIP 檔案。

Note

(預備內部/伺服器) Amazon Kendra 會檢查中包含的端點資訊 AWS Secrets Manager 是否與資料來源組態詳細資料中指定的端點資訊相同。這有助於防止[混淆的副問題](#)，這是一個安全性問題，即使用者沒有執行動作的權限，但用 Amazon Kendra 作 Proxy 來存取設定的密碼並執行動作。如果您稍後變更端點資訊，則必須建立新密碼才能同步此資訊。

- 對於需要基本、NTLM 或 Kerberos 驗證的網站：
 - 記下您的網站驗證憑證，其中包括使用者名稱和密碼。

Note

Amazon Kendra 網頁爬行者程式 v2.0 支援 NTLM 驗證通訊協定 (包括密碼雜湊)，以及包含密碼加密的 Kerberos 驗證通訊協定。

- 對於需要 SAML 或登入表單驗證的網站：
 - 記下您的網站驗證憑證，其中包括使用者名稱和密碼。
 - 複製使用者名稱欄位的 XPath (XML 路徑語言) (如果使用 SAML，則為使用者名稱按鈕)、密碼欄位和按鈕，並複製登入頁面 URL。您可以使用 Web 瀏覽器的開發人員工具找到元素的 XPath。XPath 通常遵循以下格式：`//tagname[@Attribute='Value']`。

Note

Amazon Kendra 網絡爬蟲 v2.0 使用無頭 Chrome 瀏覽器和表單中的信息，以使用 OAuth 2.0 受保護的 URL 進行身份驗證和授權訪問。

- 選用性：如果您想要使用 Web Proxy 連線到想要編目的內部網站，請複製 Web Proxy 伺服器的主機名稱和連接埠號碼。Web 代理必須面對公開。Amazon Kendra 支持連接到基本身份驗證支持的 Web 代理服務器，或者您可以在沒有身份驗證的情況下連接。
- 選用性：如果您想要使用 VPC 連線至要編目的內部網站，請複製虛擬私人雲端 (VPC) 子網路 ID。如需詳細資訊，請參閱[配置 Amazon VPC](#)。
- 檢查您要索引的每個網頁文檔是唯一的，並且在您計劃用於相同索引的其他數據源中。您要用於索引的每個資料來源不得包含跨資料來源的相同文件。文件 ID 對索引來說是全域的，而且每個索引必須是唯一的。

在您的 AWS 帳戶中，請確定您有：

- [建立 Amazon Kendra 索引](#)，如果使用 API，則會記下索引識別碼。
- 為您的[資料來源建立 IAM 角色](#)，如果使用 API，請記下該 IAM 角色的 Amazon 資源名稱。

Note

如果您變更驗證類型和認證，則必須更新 IAM 角色才能存取正確的 AWS Secrets Manager 密碼 ID。

- 對於需要身份驗證的網站，或者如果使用具有身份驗證的 Web 代理，則將您的身份驗證憑據存儲在 AWS Secrets Manager 密鑰中，並且如果使用 API，則會記錄密鑰的 ARN。

Note

我們建議您定期重新整理或輪換您的認證和密碼。僅為您自己的安全提供必要的訪問級別。我們不建議您跨資料來源以及連接器 1.0 和 2.0 版 (如果適用) 重複使用認證和密碼。

如果您沒有現有的 IAM 角色或密碼，則可以在將 web crawler 資料來源連線到時使用主控台建立新 IAM 角色和 Secrets Manager 密碼 Amazon Kendra。如果您使用 API，則必須提供現有 IAM 角色和 Secrets Manager 密碼的 ARN，以及索引 ID。

連接說明

若要連線 Amazon Kendra 到 web crawler 資料來源，您必須提供資料來源的必要詳細 web crawler 資訊，Amazon Kendra 以便能夠存取您的資料。如果您尚未設定「Amazon Kendra 請 web crawler 參閱 [必要條件](#)」。

Console

若要連線 Amazon Kendra 到 web crawler


1. 登入 AWS Management Console 並開啟 [Amazon Kendra 主控台](#)。
2. 在左側導覽窗格中，選擇 [索引]，然後從索引清單中選擇要使用的索引。

Note

您可以選擇在索引設置下配置或編輯您的用戶訪問控制設置。


3. 在 [開始使用] 頁面上，選擇 [新增資料來源]。
4. 在 [新增資料來源] 頁面上，選擇 Web 爬行者程式連接器，然後選擇 [新增連接器]。如果使用第 2 版 (如果適用)，請選擇帶有「V2.0」標籤的 Web 爬行者程式連接器。
5. 在 [指定資料來源詳細資訊] 頁面上，輸入下列資訊：
 - a. 在名稱和說明中，對於資料來源名稱 — 輸入資料來源的名稱。您可以包含連字號，但不能包含空格。
 - b. (選擇性) 說明 — 輸入資料來源的選用說明。

- c. 在預設語言中 — 選擇一種語言來篩選索引的文件。除非另有指定，否則語言預設為英文。文件中繼資料中指定的語言會覆寫選取的語言。
 - d. 在「標籤」中，針對「新增標籤」 — 包含可選標籤以搜尋和篩選資源或追蹤 AWS 成本。
 - e. 選擇下一步。
6. 在 [定義存取權和安全性] 頁面上，輸入下列資訊：
- a. 來源 — 選擇「來源 URL」、「來源網站地圖」、「來源 URL 檔案」、「來源網站地圖」檔案。如果您選擇使用包含最多 100 個種子 URL 清單的文字檔案，請指定儲存檔案的 Amazon S3 值區路徑。如果您選擇使用 Sitemap XML 檔案，請指定儲存檔案的 Amazon S3 值區路徑。您也可以將多個網站地圖 XML 檔案分割成 ZIP 檔案。否則，您最多可以手動輸入 10 個種子或起點網址，以及最多三個 Sitemap 網址。

 Note

如果您要檢索 Sitemap，請檢查基礎或根網址是否與 Sitemap 頁面上列出的 URL 相同。例如，如果您的 Sitemap URL 是 `https://example.com/sitemap-page.html`，則此 Sitemap 頁面上列出的網址也應使用基本 URL 「`https://example.com/`」。

如果您的網站需要驗證才能存取網站，您可以選擇以太基本版、NTLM/Kerberos、SAML 或表單驗證。否則，請選擇不驗證的選項。

 Note


如果您想要稍後編輯資料來源，以便透過網站地圖驗證來變更種子 URL，則必須建立新的資料來源。Amazon Kendra 使用 Secrets Manager 密碼中的種子 URL 端點資訊來設定資料來源以進行驗證，因此在變更為網站地圖時，無法重新設定資料來源。

- AWS Secrets Manager 秘密 — 如果您的網站需要相同的身份驗證才能訪問網站，請選擇現有的密碼或創建一個新的 Secrets Manager 密碼來存儲您的網站憑據。如果您選擇建立新密碼，則會開啟一個 AWS Secrets Manager 密碼視窗。

如果您選擇基本或 NTLM/Kerberos 驗證，請輸入密碼的名稱，再加上使用者名稱和密碼。NTLM 驗證通訊協定包含密碼雜湊，而 Kerberos 驗證通訊協定則包含密碼加密。

如果您選擇 SAML 或表單驗證，請輸入密碼的名稱，再加上使用者名稱和密碼。使用 XPath 做為使用者名稱欄位 (如果使用 SAML，請使用 XPath 做為使用者名稱按鈕)。使用 XPath 作為密碼字段和按鈕，以及登錄頁面 URL。您可以使用 Web 瀏覽器的開發人員工具找到元素的 XPath (XML 路徑語言)。XPath 通常遵循以下格式：`//tagname[@Attribute='Value']`。

- b. (選擇性) Web Proxy — 輸入您要用來連線至內部網站之 Proxy 伺服器的主機名稱和連接埠號碼。例如，的主機名稱 `https://a.example.com/page1.html` 是 "a.example.com"，連接埠號碼是 443，也就是 HTTPS 的標準連接埠。如果需要 Web Proxy 憑證才能連線到網站主機，您可以建立儲存 AWS Secrets Manager 認證的。
- c. Virtual Private Cloud (VPC) (VPC) — 您可以選擇使用 VPC。如果是這樣，您必須新增子網路和 VPC 安全性群組。
- d. IAM role — 選擇現有 IAM 角色或建立新 IAM 角色以存取存放庫認證和索引內容。

 Note

IAM 用於索引的角色不能用於資料來源。如果您不確定索引或常見問題集是否使用現有角色，請選擇 [建立新角色] 以避免發生錯誤。

- e. 選擇下一步。
7. 在 [設定同步設定] 頁面上，輸入下列資訊：
- a. 同步範圍 — 設定抓取網頁 (包括網域、檔案大小和連結) 的限制；以及使用正則運算式模式篩選 URL。
 - i. (選擇性) 編目網域範圍 — 選擇是僅編目網站網域、具有子網域的網域，還是要編目網頁連結的其他網域。根據預設，Amazon Kendra 只會檢索您要檢索的網站的網域。
 - ii. (選擇性) 其他組態 — 設定下列設定：
 - 編目深度-從種子層級到爬網的「深度」或層級數。例如，種子 URL 頁面是深度 1，而此頁面上也經過探索的任何超連結都是深度 2。
 - 檔案大小上限 — 要編目的網頁或附件的大小上限 (以 MB 為單位)。
 - 每頁最大連結數 — 單一網頁上要檢索的 URL 數目上限。

- 編目速度的最大限制：每個網站主機每分鐘編目的 URL 數目上限。
 - 檔案 — 選擇搜索網頁連結的檔案。
 - 編目和索引 URL — 新增規則運算式模式以包含或排除檢索特定 URL，以及索引這些 URL 網頁上的任何超連結。
- b. 同步模式 — 選擇資料來源內容變更時要如何更新索引。當您第一次將資料來源同 Amazon Kendra 步處理時，依預設會檢索所有內容並建立索引。如果初始同步失敗，您必須執行資料的完整同步處理，即使您沒有選擇完整同步作為同步模式選項。
- 完全同步：新鮮索引所有內容，並在每次資料來源與索引同步時取代現有內容。
 - 新增、修改、刪除的同步：每次資料來源與索引同步時，僅對新內容、已修改和刪除的內容建立索引。Amazon Kendra 可以使用資料來源的機制來追蹤內容變更，並為上次同步後變更的內容建立索引。
- c. 同步執行排程 — 對於「頻率」，請選擇與資料來源同步的頻率。Amazon Kendra
- d. 選擇下一步。
8. 在 [設定欄位對映] 頁面上，輸入下列資訊：
- a. 從 Amazon Kendra 產生的預設欄位中選取您要對應至索引的網頁和檔案。
 - b. 選擇下一步。
9. 在 [檢閱並建立] 頁面上，檢查您輸入的資訊是否正確，然後選取 [新增資料來源]。您也可以從此頁面選擇編輯您的資訊。成功新增資料來源後，您的資料來源將顯示在 [資料來源] 頁面上。

API

若要連線 Amazon Kendra 到 web crawler

您必須使用 [TemplateConfiguration](#) API 指定 [資料來源結構描述](#) 的 JSON。您必須提供以下信息：

- 資料來源 — 指定使用 [TemplateConfiguration](#) JSON 結構定義 WEBCRAWLERV2 時的資料來源類型。同時將資料來源指定為呼叫 [CreateDataSource](#) API TEMPLATE 時的方式。
- URL — 指定網站的種子或起點 URL，或是您要檢索之網站的 Sitemap URL。您可以指定儲存種子 URL 清單的 Amazon S3 值區路徑。種子 URL 的文字檔案中的每個 URL 都必須以個別的行格式化。您也可以指定儲存 Sitemap XML 檔案的 Amazon S3 值區路徑。您可以將多個 Sitemap 檔案合併為一個 ZIP 檔案，並將 ZIP 檔案儲存在 Amazon S3 值區中。

Note

如果您要檢索 Sitemap，請檢查基礎或根網址是否與 Sitemap 頁面上列出的 URL 相同。例如，如果您的 Sitemap URL 是 `https://example.com/sitemap-page.html`，則此 Sitemap 頁面上列出的網址也應使用基本 URL 「`https://example.com/`」。

- 同步模式 — 指定資料來源內容變更時 Amazon Kendra 應如何更新索引。當您第一次將資料來源同 Amazon Kendra 步處理時，依預設會檢索所有內容並建立索引。如果初始同步失敗，您必須執行資料的完整同步處理，即使您沒有選擇完整同步作為同步模式選項。您可以選擇：
 - `FORCED_FULL_CRAWL` 新建索引所有內容，並在每次資料來源與索引同步時取代現有內容。
 - `FULL_CRAWL`，以在每次資料來源與索引同步時，僅對新的、修改的和刪除的內容建立索引。Amazon Kendra 可以使用資料來源的機制來追蹤內容變更，並為上次同步後變更的內容建立索引。
- 驗證 — 如果您的網站需要相同的驗證，請指定 `BasicAuthNTLM_Kerberos`、`SAML`、或 `Form` 驗證。如果您的網站不需要驗證，請指定 `NoAuthentication`。
- 秘密 Amazon 資源名稱 (ARN) — 如果您的網站需要基本、NTLM 或 Kerberos 身份驗證，您需要提供一個密碼來儲存您的使用者名稱和密碼身份驗證登入資料。您提供一個 AWS Secrets Manager 秘密的 Amazon 資源名稱 (ARN)。密碼會以下列金鑰儲存在 JSON 結構中：

```
{
  "seedUrlsHash": "Hash representation of all seed URLs",
  "userName": "user name",
  "password": "password"
}
```

如果您的網站需要 SAML 驗證，密碼會以下列金鑰儲存在 JSON 結構中：

```
{
  "seedUrlsHash": "Hash representation of all seed URLs",
  "userName": "user name",
  "password": "password",
  "userNameFieldXPath": "XPath for user name field",
  "userNameButtonXPath": "XPath for user name button",
  "passwordFieldXPath": "XPath for password field",
  "passwordButtonXPath": "XPath for password button",
  "loginPageUrl": "Full URL for website login page"
}
```

```
}
```

如果您的網站需要表單驗證，密碼會以下列金鑰儲存在 JSON 結構中：

```
{
  "seedUrlsHash": "Hash representation of all seed URLs",
  "userName": "user name",
  "password": "password",
  "userNameFieldXpath": "XPath for user name field",
  "passwordFieldXpath": "XPath for password field",
  "passwordButtonXpath": "XPath for password button",
  "loginPageUrl": "Full URL for website login page"
}
```

您可以使用 Web 瀏覽器的開發人員工具找到元素的 XPath (XML 路徑語言)。XPath 通常遵循以下格式：`//tagname[@Attribute='Value']`。

您還可以使用和 AWS Secrets Manager 秘密提供 Web 代理憑據。

- IAM role — 指定RoleArn何時呼叫CreateDataSource以提供具有存取 Secrets Manager 密碼之權限的 IAM 角色，以及呼叫 Web 爬行者程式連接器和所需公用 API 的時間。Amazon Kendra如需詳細資訊，請參閱 [Web 爬行者程式資料來源的IAM 角色](#)。

您還可以添加以下可選功能：

- Virtual Private Cloud (VPC) — 指定您撥打電話的VpcConfiguration時間。CreateDataSource如需詳細資訊，請參閱 [配置 Amazon Kendra 為使用 Amazon VPC](#)。
- 網域範圍 — 選擇是否只檢索具有子網域的網站網域，還是檢索網頁連結的其他網域。根據預設，Amazon Kendra 只會檢索您要檢索的網站的網域。
- 從種子級別到爬網的「深度」或級別數。例如，種子 URL 頁面是深度 1，而此頁面上也經過探索的任何超連結都是深度 2。
- 單一網頁上要檢索的 URL 數目上限。
- 要抓取的網頁或附件的最大大小 (以 MB 為單位)。
- 每分鐘每個網站主機網路爬取的 URL 數目上限。
- 用於連線和爬取內部網站的 Web Proxy 主機和連接埠號碼。例如，的主機名稱https://a.example.com/page1.html是 "a.example.com"，連接埠號碼是 443，也就是 HTTPS 的標準連接埠。如果需要 Web Proxy 憑證才能連線到網站主機，您可以建立儲存 AWS Secrets Manager 認證的。

- 包含和排除篩選器 — 指定是否要包含或排除檢索特定 URL，以及為這些 URL 網頁上的任何超連結建立索引。

Note

大多數資料來源使用規則運算式模式，這些模式是稱為篩選器的包含或排除模式。如果您指定包含篩選器，則只有符合包含項目篩選器的內容會編製索引。不符合包含篩選器的任何文件都不會建立索引。如果您指定包含和排除篩選器，符合排除篩選器的文件將不會建立索引，即使它們符合包含篩選器也是如此。

- 欄位對應 — 選擇此選項可將網頁和網頁檔案的欄位對應至 Amazon Kendra 索引欄位。如需詳細資訊，請參閱[映射資料來源欄位](#)。

如需要設定的其他重要 JSON 金鑰清單，請參閱[Amazon Kendra 網路爬行者程式範本結構描述](#)。

設定 Amazon Kendra 網頁爬行者程式的 `robots.txt` 檔案

Amazon Kendra 是一種智慧型搜尋服務，AWS 客戶可用來索引和搜尋自己選擇的文件。為了索引 Web 上的文件，客戶可以使用 Web 爬行者程式 (Amazon Kendra Web Crawler) 來指出應該對哪些 URL 進行索引以及其他操作參數。Amazon Kendra 在索引任何特定網站之前，客戶必須獲得授權。

Amazon Kendra 網路爬蟲尊重標準的 `robots.txt` 指令 `Allow`，如和 `Disallow`。您可以修改網站的 `robots.txt` 檔案，以控制網 Amazon Kendra 路爬蟲如何抓取您的網站。

設定 Amazon Kendra 網路爬蟲存取您網站的方式

您可以控制 Amazon Kendra Web 爬蟲如何使用 `Allow` 和 `Disallow` 指令索引您的網站。您也可以控制哪些網頁要編製索引，以及哪些網頁未被檢索。

若要允許 Amazon Kendra Web 爬蟲檢索所有網頁 (不允許的網頁除外)，請使用下列指令：

```
User-agent: amazon-kendra    # Amazon Kendra Web Crawler
Disallow: /credential-pages/ # disallow access to specific pages
```

若要允許 Amazon Kendra Web 爬蟲只檢索特定網頁，請使用下列指令：

```
User-agent: amazon-kendra    # Amazon Kendra Web Crawler
Allow: /pages/ # allow access to specific pages
```

若要允許 Amazon Kendra Web 爬蟲抓取所有網站內容並禁止其他機器人進行檢索，請使用以下指令：

```
User-agent: amazon-kendra # Amazon Kendra Web Crawler
Allow: / # allow access to all pages
User-agent: * # any (other) robot
Disallow: / # disallow access to any pages
```

停止 Amazon Kendra 網絡爬蟲爬網您的網站

您可以使用該Disallow指令阻止 Amazon Kendra Web 爬蟲索引您的網站。您還可以控制哪些網頁被抓取，哪些網頁不被抓取。

若要停止 Amazon Kendra 網頁爬蟲檢索網站，請使用下列指令：

```
User-agent: amazon-kendra # Amazon Kendra Web Crawler
Disallow: / # disallow access to any pages
```

Amazon Kendra 網絡爬蟲還支持 HTML 頁面中的元標記中的機器人noindex和nofollow指令。這些指令可阻止 Web 爬蟲索引網頁，並停止跟隨網頁上的任何鏈接。您可以將 meta 標籤放在文件的區段中，以指定自動機制規則的規則。

例如，下面的網頁包括指令自動機制noindex和nofollow：

```
<html>
<head>
  <meta name="robots" content="noindex, nofollow"/>
  ...
</head>
<body>...</body>
</html>
```

如果您對 Amazon Kendra 網絡爬蟲有任何疑問或疑慮，可以聯繫[AWS 支持團隊](#)。

Amazon WorkDocs

Amazon WorkDocs 是一種安全的內容協作服務，用於創建，編輯，存儲和共享內容。您可以使 Amazon Kendra 用索引您的 Amazon WorkDocs 資料來源。

您可以使用 [Amazon Kendra 主控台](#) 和 [WorkDocsConfiguration](#) API 連線 Amazon Kendra 到 Amazon WorkDocs 資料來源。

Amazon WorkDocs 可在奧勒岡州、北維吉尼亞州、雪梨、新加坡和愛爾蘭地區使用。

如需對資 Amazon Kendra WorkDocs 料來源連接器進行疑難排解，請參 [疑難排解資料來](#)

主題

- [支援的功能](#)
- [必要條件](#)
- [連接說明](#)
- [進一步了解](#)

支援的功能

Amazon Kendra WorkDocs 資料來源連接器支援下列功能：

- 欄位對映
- 使用者存取控制
- 包含/排除過濾器
- 變更日誌

必要條件

在您可以用來 Amazon Kendra 為資 WorkDocs 料來源建立索引之前，請先在 WorkDocs 和 AWS 帳戶中進行這些變更。

在中 WorkDocs，請確定您有：

- 記下 Amazon WorkDocs 儲存庫的 Amazon WorkDocs 目錄 ID (組織 ID)。
- 已勾選的每個文件在您打算用於相同索引的其他資料來源中 WorkDocs 和其他資料來源之間都是唯一的。您要用於索引的每個資料來源不得包含跨資料來源的相同文件。文件 ID 對索引來說是全域的，而且每個索引必須是唯一的。

在您的 AWS 帳戶中，請確定您有：

- [建立 Amazon Kendra 索引](#)，如果使用 API，則會記下索引識別碼。

- 為您的[資料來源建立 IAM 角色](#)，如果使用 API，則會記錄 IAM 角色的 ARN。

如果您沒有現有 IAM 角色，則可以在將 WorkDocs 資料來源連線到時使用主控台建立新 IAM 角色 Amazon Kendra。如果您使用的是 API，則必須提供現有 IAM 角色的 ARN 和索引識別碼。

連接說明

若要連線 Amazon Kendra 到 WorkDocs 資料來源，您必須提供資料來源的必要詳細 WorkDocs 資訊，Amazon Kendra 以便能夠存取您的資料。如果您尚未配置 Amazon Kendra，WorkDocs 請參閱[必要條件](#)。

Console

若要連線 Amazon Kendra 到 Amazon WorkDocs


1. 登入 AWS Management Console 並開啟[Amazon Kendra 主控台](#)。
2. 在左側導覽窗格中，選擇 [索引]，然後從索引清單中選擇要使用的索引。

Note

您可以選擇在索引設置下配置或編輯您的用戶訪問控制設置。

3. 在 [開始使用] 頁面上，選擇 [新增資料來源]。
4. 在 [新增資料來源] 頁面上，選擇 [WorkDocs 連接器]，然後選擇 [新增連接器]。如果使用版本 2 (如果適用)，請選擇帶有「V2.0」標籤的 WorkDocs 連接器。
5. 在 [指定資料來源詳細資訊] 頁面上，輸入下列資訊：
 - a. 在名稱和說明中，對於資料來源名稱 — 輸入資料來源的名稱。您可以包含連字號，但不能包含空格。
 - b. (選擇性) 說明 — 輸入資料來源的選用說明。
 - c. 在預設語言中 — 選擇一種語言來篩選索引的文件。除非另有指定，否則語言預設為英文。文件中繼資料中指定的語言會覆寫選取的語言。
 - d. 在「標籤」中，針對「新增標籤」— 包含可選標籤以搜尋和篩選資源或追蹤 AWS 成本。
 - e. 選擇下一步。
6. 在 [定義存取權和安全性] 頁面上，輸入下列資訊：
 - a. 您 Amazon WorkDocs 場地專屬的組織 ID — 選取您要建立索引的 Amazon WorkDocs 網站 ID。您必須已建立網站。

- b. IAM role — 選擇現有 IAM 角色或建立新 IAM 角色以存取存放庫認證和索引內容。

 Note

IAM 用於索引的角色不能用於資料來源。如果您不確定索引或常見問題集是否使用現有角色，請選擇 [建立新角色] 以避免發生錯誤。

- c. 選擇下一步。
7. 在 [設定同步設定] 頁面上，輸入下列資訊：
 - a. 編目文件註解-您要編目的 Amazon WorkDocs 實體或內容類型。
 - b. 使用變更記錄 — 選取此選項可僅使用新內容或已修改的內容更新索引，而不是同步所有檔案。
 - c. 正則表達式模式-包含或排除某些文件的正則表達式模式。
 - d. 頻率的同步執行排程 — 選擇同步資料來源內容和更新索引的頻率。
 - e. 選擇下一步。
 8. 在 [設定欄位對映] 頁面上，輸入下列資訊：
 - a. 預設資料來源欄位 — 從 Amazon Kendra 產生的預設資料來源欄位中選取您要對映至索引的資料來源欄位。
 - b. 新增欄位 — 新增自訂資料來源欄位，以建立要對映的索引欄位名稱和欄位資料類型。
 - c. 選擇下一步。
 9. 在 [檢閱並建立] 頁面上，檢查您輸入的資訊是否正確，然後選取 [新增資料來源]。您也可以從此頁面選擇編輯您的資訊。成功新增資料來源後，您的資料來源將顯示在 [資料來源] 頁面上。

API

若要連線 Amazon Kendra 到 Amazon WorkDocs

您必須使用 [WorkDocsConfiguration](#) API 指定下列項目：

- Amazon WorkDocs 目錄 ID — 指定目 Amazon WorkDocs 錄的組織 ID。您可以前往使用中目錄，然後移至目錄，在 AWS Directory Service 中找到組織 ID。
- IAM 角色 — 指定 RoleArn 何時呼叫 CreateDataSource 以提供具有權限的 IAM 角色以存取 WorkDocs 目錄以及呼叫連接器和所需的公用 API。WorkDocs Amazon Kendra 如需詳細資訊，請參閱 [WorkDocs 料來源的 IAM 角色](#)。

您還可以添加以下可選功能：

- **變更記錄** — 是否 Amazon Kendra 應該使用 WorkDocs 資料來源變更記錄機制來判斷是否必須在索引中更新文件。

Note

如果您不想 Amazon Kendra 掃描所有文檔，請使用更改日誌。如果您的變更記錄檔很大，掃描 WorkDocs 資料來源中的文件可能比處理變更記錄所花費的時間更 Amazon Kendra 少。如果您是第一次將 WorkDocs 資料來源與索引同步，則會掃描所有文件。

- **包含和排除篩選器** — 指定要包含還是排除某些文件和文件注釋。每個註解都會編製為單獨的文件編製索引。

Note

大多數資料來源使用規則運算式模式，這些模式是稱為篩選器的包含或排除模式。如果您指定包含篩選器，則只有符合包含項目篩選器的內容會編製索引。不符合包含篩選器的任何文件都不會建立索引。如果您指定包含和排除篩選器，符合排除篩選器的文件將不會建立索引，即使它們符合包含篩選器也是如此。

- **使用者前後關聯篩選與存取控制** — Amazon Kendra 探索文件的存取控制清單 (ACL) (如果您有文件的 ACL)。ACL 資訊可用來根據使用者或使用者對文件的群組存取權來篩選搜尋結果。如需詳細資訊，請參閱[使用者內容篩選](#)。
- **欄位對映** — 選擇將資料來源欄位對映至 Amazon Kendra 索引欄位。如需詳細資訊，請參閱[映射資料來源欄位](#)。

Note

您的文件需要文件內文欄位或文件內文對等項目，才能搜尋您的文件。Amazon Kendra 您必須將資料來源中的文件內文欄位名稱對應至索引欄位名稱 `_document_body`。所有其他欄位是選用的。

進一步了解

若要進一步瞭解 Amazon Kendra 與 WorkDocs 資料來源整合的相關資訊，請參閱：

- [開始使用 Amazon Kendra Amazon WorkDocs 連接器](#)

立方體

Box 是一種雲存儲服務，提供文件託管功能。您可以用 Amazon Kendra 來索引 Box 內容中的內容，包括註解、工作和網頁連結。

您可以使用[Amazon Kendra 主控台](#)和 [BoxConfiguration](#)API 連線 Amazon Kendra 至 Box 資料來源。

有關 Amazon Kendra Box 資料來源連接器的疑難排解，請參閱[疑難排解資料來](#)。

主題

- [支援的功能](#)
- [必要條件](#)
- [連接說明](#)
- [進一步了解](#)

支援的功能

Amazon Kendra Box 資料來源連接器支援下列功能：

- 欄位對映
- 使用者存取控制
- 包含/排除過濾器
- 更改日誌，完整和增量內容同步
- 虛擬私有雲端 (VPC)

必要條件

在您可以使用 Amazon Kendra 對 Box 資料來源建立索引之前，請先在 Box 和 AWS 帳戶中進行這些變更。

在 Box 中，確保您具有：

- 一個盒子企業帳戶或盒子企業 Plus 帳戶。

- 在 Box 開發人員控制台中配置 Box 自定義應用程式，並使用 JSON Web 令牌 (JWT) 進行服務器端身份驗證。有關更多詳細信息，請參閱[有關創建自定義應用程式的 Box 文檔和配置 JWT 身份驗證的 Box 文檔](#)。
- 將您的應用程式訪問級別設置為應用程式 + 企業訪問權限，並允許其使用作為用戶標題進行 API 調用。
- 使用管理員使用者在 Box 應用程式中新增下列應用程式範圍：
 - 寫入存儲在 Box 中的所有文件和文件夾
 - 管理使用者
 - 管理群組
 - 管理企業屬性
- 設定的公開/私密金鑰配key pair，包括用戶端 ID、用戶端密鑰、公開金鑰 ID、私密金鑰 ID、密碼片語以及用作驗證認證的企業 ID。如需詳細資訊，請參閱[公開和私密 key pair](#)。

Note

我們建議您定期重新整理或輪換您的認證和密碼。僅為您自己的安全提供必要的訪問級別。我們不建議您跨資料來源以及連接器 1.0 和 2.0 版 (如果適用) 重複使用認證和密碼。

- 從 Box 開發者主控台設定或 Box 應用程式複製您的 Box 企業 ID。例##
- 核取每個文件在 Box 和您打算用於相同索引的其他資料來源中都是唯一的。您要用於索引的每個資料來源不得包含跨資料來源的相同文件。文件 ID 對索引來說是全域的，而且每個索引必須是唯一的。

在您的中 AWS 帳戶，請確保您有：

- [建立 Amazon Kendra 索引](#)，如果使用 API，則會記下索引識別碼。
- 為您的[資料來源建立 IAM 角色](#)，如果使用 API，則會記錄 IAM 角色的 ARN。

Note

如果您變更驗證類型和認證，則必須更新 IAM 角色才能存取正確的 AWS Secrets Manager 密碼 ID。

- 將您的 Box 身份驗證憑據存儲在 AWS Secrets Manager 密鑰中，如果使用 API，則記錄密鑰的 ARN。

Note

我們建議您定期重新整理或輪換您的認證和密碼。僅為您自己的安全提供必要的訪問級別。我們不建議您跨資料來源以及連接器 1.0 和 2.0 版 (如果適用) 重複使用認證和密碼。

如果您沒有現有的 IAM 角色或密碼，則可以在將 Box 資料來源連線至時使用主控台建立新 IAM 角色和 Secrets Manager 密碼 Amazon Kendra。如果您使用 API，則必須提供現有 IAM 角色和 Secrets Manager 密碼的 ARN 以及索引 ID。

連接說明

若要連線 Amazon Kendra 至 Box 資料來源，您必須提供 Box 資料來源的必要詳細資訊，Amazon Kendra 以便存取您的資料。如果您尚未設定 Box Amazon Kendra，請參閱[必要條件](#)。

Console

若要連接 Amazon Kendra 至 Box


1. 登入 AWS Management Console 並開啟[Amazon Kendra 主控台](#)。
2. 在左側導覽窗格中，選擇 [索引]，然後從索引清單中選擇要使用的索引。

Note

您可以選擇在索引設置下配置或編輯您的用戶訪問控制設置。

3. 在 [開始使用] 頁面上，選擇 [新增資料來源]。
4. 在 [新增資料來源] 頁面上，選擇 [Box 連接器]，然後選擇 [新增連接器]。如果使用第 2 版 (如果適用)，請選擇帶有「V2.0」標籤的 Box 連接器。
5. 在 [指定資料來源詳細資訊] 頁面上，輸入下列資訊：
 - a. 在名稱和說明中，對於資料來源名稱 — 輸入資料來源的名稱。您可以包含連字號，但不能包含空格。
 - b. (選擇性) 說明 — 輸入資料來源的選用說明。
 - c. 在預設語言中 — 選擇一種語言來篩選索引的文件。除非另有指定，否則語言預設為英文。文件中繼資料中指定的語言會覆寫選取的語言。
 - d. 在「標籤」中，針對「新增標籤」 — 包含可選標籤以搜尋和篩選資源或追蹤 AWS 成本。

- e. 選擇下一步。
6. 在 [定義存取權和安全性] 頁面上，輸入下列資訊：
 - a. 方塊企業 ID — 輸入您的企業 ID。例##
 - b. 授權 — 開啟或關閉文件的存取控制清單 (ACL) 資訊 (如果您有 ACL)，且想要將其用於存取控制。ACL 會指定使用者和群組可存取的文件。ACL 資訊可用來根據使用者或使用者對文件的群組存取來篩選搜尋結果。如需詳細資訊，請參閱[使用者內容篩選](#)。
 - c. AWS Secrets Manager 秘密 — 選擇現有密碼或建立新 Secrets Manager 密碼來儲存您的 Box 驗證認證。如果您選擇建立新密碼，則會開啟一個 AWS Secrets Manager 密碼視窗。
 - i. 秘密名稱 — 您秘密的名稱。前綴 'AmazonKendra-Box-' 會自動添加到您的密碼名稱中。
 - ii. 對於用戶端 ID、用戶端密碼、公開金鑰 ID、私密金鑰 ID 和密語 — 輸入您在 Box 中設定的公開/私密金鑰中的值。
 - iii. 添加並保存您的秘密。
 - d. V@@ irtual Private Cloud (VPC) (VPC) — 您可以選擇使用 VPC。如果是這樣，您必須新增子網路和 VPC 安全性群組。
 - e. 識別爬行者程式 — 指定是否要開啟身分識別爬行 Amazon Kendra 者程式。識別爬行者程式會使用文件的存取控制清單 (ACL) 資訊，根據使用者或使用者對文件的群組存取權來篩選搜尋結果。如果您有文件的 ACL 並選擇使用 ACL，您也可以選擇開啟的身分識別爬行者程式，以設定搜尋結果的使用者環境定義篩選。Amazon Kendra 否則，如果關閉身分搜索器，則可以公開搜索所有文檔。如果您想要對文件使用存取控制，且身分識別編目程式已關閉，您也可以使用 [PutPrincipalMapping](#) API 來上傳使用者和群組存取資訊以進行使用者內容篩選。
 - f. IAM role — 選擇現有 IAM 角色或建立新 IAM 角色以存取存放庫認證和索引內容。

 Note

IAM 用於索引的角色不能用於資料來源。如果您不確定索引或常見問題集是否使用現有角色，請選擇 [建立新角色] 以避免發生錯誤。

- g. 選擇下一步。
7. 在 [設定同步設定] 頁面上，輸入下列資訊：
 - a. 方塊資料夾 ID — 輸入您要編目的特定 Box 資料夾 ID，否則會檢索所有資料夾中的內容。

- b. 方塊檔案 — 選擇是否要編目網頁連結、註解和工作。
 - c. 對於其他組態 — 新增規則運算式模式以包含或排除某些內容。
 - d. 同步模式 — 選擇資料來源內容變更時要如何更新索引。當您第一次將資料來源同 Amazon Kendra 步處理時，依預設會檢索所有內容並建立索引。如果初始同步失敗，您必須執行資料的完整同步，即使您沒有選擇完整同步作為同步模式選項。
 - 完全同步：新鮮索引所有內容，並在每次資料來源與索引同步時取代現有內容。
 - 新增、修改的同步：每次資料來源與索引同步時，僅對新內容和已修改的內容建立索引。Amazon Kendra 可以使用資料來源的機制來追蹤內容變更，並為上次同步後變更的內容建立索引。
 - 新增、修改、刪除的同步：每次資料來源與索引同步時，僅對新內容、已修改和刪除的內容建立索引。Amazon Kendra 可以使用資料來源的機制來追蹤內容變更，並為上次同步後變更的內容建立索引。
 - e. 頻率的同步執行排程 — 選擇同步資料來源內容和更新索引的頻率。
 - f. 選擇下一步。
8. 在 [設定欄位對映] 頁面上，輸入下列資訊：
- a. 預設資料來源欄位 — 從 Amazon Kendra 產生的預設資料來源欄位中選取您要對映至索引的資料來源欄位。
 - b. 新增欄位 — 新增自訂資料來源欄位，以建立要對映的索引欄位名稱和欄位資料類型。
 - c. 選擇下一步。
9. 在 [檢閱並建立] 頁面上，檢查您輸入的資訊是否正確，然後選取 [新增資料來源]。您也可以從此頁面選擇編輯您的資訊。成功新增資料來源後，您的資料來源將顯示在 [資料來源] 頁面上。

API

若要連接 Amazon Kendra 至 Box

您必須使用 [BoxConfiguration](#) API 指定下列項目：

盒裝企業 ID — 提供您的企業 ID。您可以在 Box 開發人員控制台設置中或在 Box 中配置應用程式時找到企業 ID。

- 秘密 Amazon 資源名稱 (ARN) — 提供包含 Box 帳戶身份驗證登入資料的 Secrets Manager 密碼的 Amazon 資源名稱 (ARN)。密碼會以下列金鑰儲存在 JSON 結構中：

```
{
  "clientID": "client-id",
  "clientSecret": "client-secret",
  "publicKeyID": "public-key-id",
  "privateKey": "private-key",
  "passphrase": "pass-phrase"
}
```

- IAM role — 指定RoleArn何時呼叫CreateDataSource以提供具有存取 Secrets Manager 密碼的權限的 IAM 角色，以及呼叫 Box 連接器和 Amazon Kendra所需的公用 API 的時間。有關詳情，請參閱 [Box 資料來源的IAM 角色](#)。

您還可以添加以下可選功能：

- Virtual Private Cloud (VPC) — 指定VpcConfiguration為資料來源組態的一部分。請參閱 [設定 Amazon Kendra 定以使用 VPC](#)。
- 變更記錄 — 是否 Amazon Kendra 應該使用 Box 資料來源變更記錄機制來判斷是否必須在索引中更新文件。

Note

如果您不想 Amazon Kendra 掃描所有文檔，請使用更改日誌。如果您的變更記錄很大，掃描 Box 資料來源中的文件可能比處理變更記錄所花費的時間更 Amazon Kendra 少。如果您是第一次將 Box 資料來源與索引同步，則會掃描所有文件。

- 註解、工作、網頁連結 — 指定是否要編目這些類型的內容。

Note

大多數資料來源使用規則運算式模式，這些模式是稱為篩選器的包含或排除模式。如果您指定包含篩選器，則只會編製與包含項目篩選器相符的內容編製索引。不符合包含篩選器的任何文件都不會建立索引。如果您指定包含和排除篩選器，符合排除篩選器的文件將不會建立索引，即使它們符合包含篩選器也是如此。

- 包含和排除篩選器 — 指定要包含還是排除特定 Box 檔案和資料夾。

Note

大多數資料來源使用規則運算式模式，這些模式是稱為篩選器的包含或排除模式。如果您指定包含篩選器，則只會編製與包含項目篩選器相符的內容編製索引。不符合包含篩選器的任何文件都不會建立索引。如果您指定包含和排除篩選器，符合排除篩選器的文件將不會建立索引，即使它們符合包含篩選器也是如此。

- 使用者前後關聯篩選與存取控制 — Amazon Kendra 探索文件的存取控制清單 (ACL) (如果您有文件的 ACL)。ACL 資訊可用來根據使用者或使用者對文件的群組存取來篩選搜尋結果。如需詳細資訊，請參閱[使用者內容篩選](#)。
- 欄位對映 — 選擇將 Box 資料來源欄位對映至 Amazon Kendra 索引欄位。如需詳細資訊，請參閱[映射資料來源欄位](#)。

Note

您的文件需要文件內文欄位或文件內文對等項目，才能搜尋您的文件。Amazon Kendra 您必須將資料來源中的文件內文欄位名稱對應至索引欄位名稱_document_body。所有其他欄位是選用的。

進一步了解

若要深入瞭解如何 Amazon Kendra 與 Box 資料來源整合，請參閱：

- [開始使用 Amazon Kendra Box 連接器](#)

Confluence

Confluence 是一種協作工作管理工具，專為共享，存儲和工作項目規劃，軟件開發和產品管理而設計。您可以用 Amazon Kendra 來索引您的 Confluence 空間、頁面 (包括巢狀頁面)、部落格，以及已編製索引的頁面和部落格的留言和附件。

Amazon Kendra 同時支持匯流服務器/數據中心和匯流雲。

Note

默認情況下，Amazon Kendra 不索引匯流檔案和個人空間。您可以選擇在建立資料來源時對其建立索引。如果您不想索引空間，請在匯合中 Amazon Kendra 將其標記為私有。

您可以使用 [Amazon Kendra 主控台](#)、API 或 [TemplateConfiguration](#) API 連線 Amazon Kendra 到您的匯流資料來源。 [ConfluenceConfiguration](#)

Amazon Kendra 具有兩個版本的匯流連接器。每個版本的支援功能包括：

匯流連接器 [ConfluenceConfiguration](#)

- 欄位對映
- 使用者存取控制
- 包含/排除過濾器
- (僅適用於匯流伺服器) 虛擬私有雲 (VPC)

匯流連接器 V2.0 [TemplateConfiguration](#)

- 欄位對映
- 使用者存取控制
- 包含/排除模式
- 完整和增量內容同步
- 虛擬私有雲端 (VPC)

Note

對匯流連接器 V1.0/ [ConfluenceConfiguration](#) API 的 Support 計劃在 2023 年結束。我們建議遷移到或使用匯流連接器 V2.0 /API。 [TemplateConfiguration](#)

若要疑難排解您的 Amazon Kendra 匯流資料來源連接器，請參閱。 [疑難排解資料來](#)

主題

- [匯流連接器 V1.0](#)

- [匯流連接器 V2.0](#)

匯流連接器 V1.0

Confluence 是一種協作工作管理工具，專為共享，存儲和工作項目規劃，軟件開發和產品管理而設計。您可以用 Amazon Kendra 來索引您的 Confluence 空間、頁面 (包括巢狀頁面)、部落格，以及已編製索引的頁面和部落格的留言和附件。

Note

對匯流連接器 V1.0/ ConfluenceConfiguration API 的 Support 計劃在 2023 年結束。我們建議遷移到或使用匯流連接器 V2.0 /API。 TemplateConfiguration

若要疑難排解您的 Amazon Kendra 匯流資料來源連接器，請參閱。[疑難排解資料來](#)

主題

- [支援的功能](#)
- [必要條件](#)
- [連接說明](#)
- [進一步了解](#)

支援的功能

Amazon Kendra 匯流資料來源連接器支援以下功能：


- 欄位對映
- 使用者存取控制
- 包含/排除過濾器
- (僅適用於匯流伺服器) 虛擬私有雲 (VPC)

必要條件

在您可以用來 Amazon Kendra 為匯流資料來源建立索引之前，請先在您的匯流和帳戶中進行這些變更。AWS

在匯流中，確保您具有：

- 授 Amazon Kendra 予檢視您匯流執行個體中所有內容的權限：
 - 成 Amazon Kendra 為 `confluence-administrators` 群組的成員。
 - 授予所有現有空間、部落格和頁面的網站管理員權限。
- 複製您的匯流實例的 URL。
- 針對 SSO (單一登入) 使用者：在 Confluence 資料中心設定 Confluence 驗證方法時，啟動使用者名稱和密碼的「在登入時顯示」頁面。
- 對於匯流服務器
 - 記下您的基本身份驗證憑據，其中包含您的 Confluence 管理帳戶用戶名和密碼以進行連接。
Amazon Kendra


 Note

我們建議您定期重新整理或輪換您的認證和密碼。僅為您自己的安全提供必要的訪問級別。我們不建議您跨資料來源以及連接器 1.0 和 2.0 版 (如果適用) 重複使用認證和密碼。

- 可選：在您的 Confluence 帳戶中生成要連接的個人訪問令牌。Amazon Kendra 有關更多信息，請參閱有關 [生成個人訪問令牌的匯合文檔](#)。
- 適用於匯流雲
 - 記下您的基本身份驗證憑據，其中包含您的 Confluence 管理帳戶用戶名和密碼以進行連接。
Amazon Kendra
- 核取每個文件在 Confluence 中以及您打算用於相同索引的其他資料來源中都是唯一的。您要用於索引的每個資料來源不得包含跨資料來源的相同文件。文件 ID 對索引來說是全域的，而且每個索引必須是唯一的。

在您的中 AWS 帳戶，請確保您有：

- [建立 Amazon Kendra 索引](#)，如果使用 API，則會記下索引識別碼。
- 為您的 [資料來源建立 IAM 角色](#)，如果使用 API，則會記錄 IAM 角色的 ARN。

 Note

如果您變更驗證類型和認證，則必須更新 IAM 角色才能存取正確的 AWS Secrets Manager 密碼 ID。

- 將您的匯流身份驗證憑據存儲在 AWS Secrets Manager 密鑰中，並且如果使用 API，則註明秘密的 ARN。

Note

我們建議您定期重新整理或輪換您的認證和密碼。僅為您自己的安全提供必要的訪問級別。我們不建議您跨資料來源以及連接器 1.0 和 2.0 版 (如果適用) 重複使用認證和密碼。

如果您沒有現有的 IAM 角色或密碼，則可以在將 Confluence 資料來源連接至時使用主控台建立新 IAM 角色和 Secrets Manager 密碼。Amazon Kendra 如果您使用 API，則必須提供現有 IAM 角色和 Secrets Manager 密碼的 ARN 以及索引 ID。

連接說明

若要連線 Amazon Kendra 到您的 Confluence 資料來源，您必須提供您的匯流認證的詳細資料，以便 Amazon Kendra 可以存取您的資料。如果您尚未配置匯流以查 Amazon Kendra 看。[必要條件](#)

Console

連接至匯流 Amazon Kendra 的步驟

1. 登入 AWS 管理主控台並開啟主 [Amazon Kendra 控制台](#)。
2. 在左側導覽窗格中，選擇 [索引]，然後從索引清單中選擇要使用的索引。

Note

您可以選擇在索引設置下配置或編輯您的用戶訪問控制設置。


3. 在 [開始使用] 頁面上，選擇 [新增資料來源]。
4. 在 [新增資料來源] 頁面上，選擇 [匯流連接器 V1.0]，然後選擇 [新增資料來源]。
5. 在 [指定資料來源詳細資訊] 頁面上，輸入下列資訊：
 - a. 在名稱和說明中，對於資料來源名稱 — 輸入資料來源的名稱。您可以包含連字號，但不能包含空格。
 - b. (選擇性) 說明 — 輸入資料來源的選用說明。
 - c. 在預設語言中 — 選擇一種語言來篩選索引的文件。除非另有指定，否則語言預設為英文。文件中繼資料中指定的語言會覆寫選取的語言。

- d. 在「標籤」中，針對「新增標籤」— 包含可選標籤以搜尋和篩選資源或追蹤 AWS 成本。
 - e. 選擇下一步。
6. 在 [定義存取權和安全性] 頁面上，輸入下列資訊：
- a. 在匯流雲和匯流服務器之間進行選擇。
 - b. 如果您選擇「匯流雲」，請輸入以下資訊：
 - i. 匯流網址 — 您的匯流網址。
 - ii. AWS Secrets Manager 秘密 — 選擇現有密碼或建立新 Secrets Manager 密碼來儲存您的 Confluence 驗證認證。如果您選擇建立新密碼，則會開啟一個 AWS Secrets Manager 密碼視窗。
 - 在「建立 AWS Secrets Manager 密碼視窗」中輸入下列資訊：
 - I. 秘密名稱 — 您秘密的名稱。前綴 'AmazonKendra-匯流-' 會自動添加到您的密碼名稱中。
 - II. 對於使用者名稱和密碼 — 輸入您的 Confluence 使用者名稱和密碼。
 - III. 選擇 [儲存驗證]。
 - c. 如果您選擇「匯流伺服器」，請輸入下列資訊：
 - i. 匯流 URL — 您的匯合使用者名稱和密碼。
 - ii. (選擇性) 若為 Web 代理伺服器，請輸入下列資訊：
 - A. 主機名稱 — 您的匯流帳戶的主機名稱。
 - B. 連接埠號碼 — 主機 URL 傳輸通訊協定使用的連接埠。
 - iii. 對於「驗證」，請選擇「基本驗證」或「(僅限 Confluence 伺服器) 個人存取權杖」。
 - iv. AWS Secrets Manager 秘密 — 選擇現有密碼或建立新 Secrets Manager 密碼來儲存您的 Confluence 驗證認證。如果您選擇建立新密碼，則會開啟一個 AWS Secrets Manager 密碼視窗。
 - 在「建立 AWS Secrets Manager 密碼視窗」中輸入下列資訊：
 - I. 秘密名稱 — 您秘密的名稱。前綴 'AmazonKendra-匯流-' 會自動添加到您的密碼名稱中。
 - II. 對於使用者名稱和密碼 — 輸入您在 Confluence 中設定的驗證認證值。如果使用基本身份驗證，請使用您的匯流用戶名 (電子郵件 ID) 和密碼 (API 令

牌)。如果使用個人訪問令牌，請輸入您在 Confluence 帳戶中配置的個人訪問令牌的詳細信息。

III. 保存並添加您的秘密。

d. IAM role — 選擇現有 IAM 角色或建立新 IAM 角色以存取存放庫認證和索引內容。

 Note

IAM 用於索引的角色不能用於資料來源。如果您不確定索引或常見問題集是否使用現有角色，請選擇 [建立新角色] 以避免發生錯誤。

e. 選擇下一步。

7. 在 [設定同步設定] 頁面上，輸入下列資訊：

- a. 對於「包括個人空間」和「包含封存空間」— 選擇要包含在此資料來源中的選用空間類型。
- b. 對於其他組態 — 指定要包含或排除某些內容的規則運算式模式。您最多可以添加 100 個圖案。
- c. 您也可以選擇在所選空間內搜索附件。
- d. 在同步執行排程中，對於頻率 — 選擇與資料來源同步的頻率。Amazon Kendra
- e. 選擇下一步。

8. 在 [設定欄位對映] 頁面上，輸入下列資訊：

- a. 對於空間、頁面、部落格 — 從 Amazon Kendra 產生的預設資料來源欄位中選取，或選取其他建議欄位對應以新增索引欄位。
- b. 新增欄位 — 新增自訂資料來源欄位，以建立要對映的索引欄位名稱和欄位資料類型。
- c. 選擇下一步。

9. 在 [檢閱並建立] 頁面上，檢查您輸入的資訊是否正確，然後選取 [新增資料來源]。您也可以從此頁面選擇編輯您的資訊。成功新增資料來源後，您的資料來源將顯示在 [資料來源] 頁面上。

API

連接至匯流 Amazon Kendra 的步驟

您必須使用 [ConfluenceConfiguration](#) API 指定下列項目：

- 匯流版本 — 指定要用作的匯流例證版本。CLOUD SERVER

- 秘密 Amazon 資源名稱 (ARN) — 提供包含您的匯流身份驗證登入資料的 Secrets Manager 秘密的 Amazon 資源名稱 (ARN)。

如果您使用 Confluence 服務器，則可以使用您的 Confluence 用戶名和密碼，或者您的個人訪問令牌作為身份驗證憑據。

如果您使用 Confluence 使用者名稱和密碼作為驗證認證，則會將下列認證儲存為 JSON 結構在密 Secrets Manager 碼中：

```
{
  "username": "user name",
  "password": "password"
}
```

如果您使用個人訪問令牌將 Confluence 服務器連接到 Amazon Kendra，則將以下憑據作為 JSON 結構存儲在密 Secrets Manager 鑰中：

```
{
  "patToken": "personal access token"
}
```

如果您使用匯流雲，則使用您的匯流用戶名和 API 令牌，在匯流中配置，作為您的密碼。您可以將下列認證儲存為 Secrets Manager 密碼中的 JSON 結構：

```
{
  "username": "user name",
  "password": "API token"
}
```

- IAM role — 指定RoleArn何時呼叫CreateDataSource以提供具有存取 Secrets Manager 密碼的權限的 IAM 角色，以及呼叫 Confluence 連接器和所需的公用 API 的時間。Amazon Kendra 有關詳情，請參閱[合流資料來源的IAM 角色](#)。

您還可以添加以下可選功能：

- 網頁代理伺服器 — 是否透過網路代理連線到您的匯流 URL 執行個體。您可以將此選項用於匯流伺服器。
- (僅適用於匯流伺服器) Virtual Private Cloud (VPC) — 指定VpcConfiguration為資料來源組態的一部分。請參閱[設定 Amazon Kendra 定以使用 VPC](#)。

- 包含和排除篩選器 — 指定規則運算式模式，以包含或排除特定空格、部落格貼文、頁面、空格和附件。如果您選擇索引附件，則只會編製索引頁面和部落格的附件編製索引。

Note

大多數資料來源使用規則運算式模式，這些模式是稱為篩選器的包含或排除模式。如果您指定包含篩選器，則只有符合包含項目篩選器的內容會編製索引。不符合包含篩選器的任何文件都不會建立索引。如果您指定包含和排除篩選器，符合排除篩選器的文件將不會建立索引，即使它們符合包含篩選器也是如此。

- 欄位對映 — 選擇將您的匯流資料來源欄位對映至索引欄位。Amazon Kendra 如需詳細資訊，請參閱[映射資料來源欄位](#)。

Note

您的文件需要文件內文欄位或文件內文對等項目，才能搜尋您的文件。Amazon Kendra 您必須將資料來源中的文件內文欄位名稱對應至索引欄位名稱_document_body。所有其他欄位是選用的。

- 使用者前後關聯篩選與存取控制 — Amazon Kendra 探索文件的存取控制清單 (ACL) (如果您有文件的 ACL)。ACL 資訊可用來根據使用者或使用者對文件的群組存取權來篩選搜尋結果。如需詳細資訊，請參閱[使用者內容篩選](#)。

進一步了解

若要深入瞭解如何 Amazon Kendra 與您的匯流資料來源整合，請參閱：

- [設定您的 Amazon Kendra 匯流伺服器連接器](#)

匯流連接器 V2.0

Confluence 是一種協作工作管理工具，專為共享，存儲和工作項目規劃，軟件開發和產品管理而設計。您可以用 Amazon Kendra 來索引您的 Confluence 空間、頁面 (包括巢狀頁面)、部落格，以及已編製索引的頁面和部落格的留言和附件。

若要疑難排解您的 Amazon Kendra 匯流資料來源連接器，請參閱。[疑難排解資料來](#)

主題

- [支援的功能](#)
- [必要條件](#)
- [連接說明](#)

支援的功能

Amazon Kendra 匯流資料來源連接器支援以下功能：

- 欄位對映
- 使用者存取控制
- 包含/排除模式
- 完整和增量內容同步
- 虛擬私有雲端 (VPC)

必要條件

在您可以用來 Amazon Kendra 為匯流資料來源建立索引之前，請先在您的匯流和帳戶中進行這些變更。AWS

在匯流中，確保您具有：

- 複製您的匯流實例 URL。例如：<https://example.confluence.com>，或者 <https://www.example.confluence.com/>，或 <https://####網/>。您需要您的匯流實例 URL 才能連接到。Amazon Kendra

[##### atlassian.net/ ###](#)

Note

不支援下列 URL 格式：

- <https://example.confluence.com/xyz>
- <https://www.example.confluence.com//wiki/spacekey/xxx>
- <https://atlassian.net/xyz>

Note

(內部預備/伺服器) Amazon Kendra 會檢查中包含的端點資訊 AWS Secrets Manager 是否與資料來源組態詳細資料中指定的端點資訊相同。這有助於防止[混淆的副問題](#)，這是一個安全性問題，即使用者沒有執行動作的權限，但用 Amazon Kendra 作 Proxy 來存取設定的密碼並執行動作。如果您稍後變更端點資訊，則必須建立新密碼才能同步此資訊。

- 配置了包含用戶名 (用於登錄匯流的電子郵件 ID) 和密碼 (匯流 API 令牌作為密碼) 的基本身份驗證憑據。請參閱[管理您的 Atlassian 帳戶的 API 權杖](#)。

Note

我們建議您定期重新整理或輪換您的認證和密碼。僅為您自己的安全提供必要的訪問級別。我們不建議您跨資料來源以及連接器 1.0 和 2.0 版 (如果適用) 重複使用認證和密碼。

- 可選：配置 OAuth 2.0 憑據包含匯流應用程序密鑰，匯流應用程序秘密，匯流訪問令牌和匯流刷新令牌，以允許連接到您的匯流實例。Amazon Kendra 如果您的訪問令牌過期，則可以使用刷新令牌重新生成訪問令牌並刷新令牌對。或者，您可以重複授權過程。有關訪問令牌的詳細信息，請參閱[管理 OAuth 訪問令牌](#)。
- (僅適用於匯流伺服器/資料中心) 可選：在匯流中設定個人存取權杖 (PAT)。請參閱[使用個人存取權杖](#)。

在您的 AWS 帳戶，請確保您有：

- [建立 Amazon Kendra 索引](#)，如果使用 API，則會記下索引識別碼。
- 為您的[資料來源建立 IAM 角色](#)，如果使用 API，則會記錄 IAM 角色的 ARN。

Note

如果您變更驗證類型和認證，則必須更新 IAM 角色才能存取正確的 AWS Secrets Manager 密碼 ID。

- 將您的匯流身份驗證憑據存儲在 AWS Secrets Manager 密鑰中，並且如果使用 API，則註明秘密的 ARN。

Note

我們建議您定期重新整理或輪換您的認證和密碼。僅為您自己的安全提供必要的訪問級別。我們不建議您跨資料來源以及連接器 1.0 和 2.0 版 (如果適用) 重複使用認證和密碼。

如果您沒有現有的 IAM 角色或密碼，則可以在將 Confluence 資料來源連接至時使用主控台建立新 IAM 角色和 Secrets Manager 密碼。Amazon Kendra 如果您使用 API，則必須提供現有 IAM 角色和 Secrets Manager 密碼的 ARN 以及索引 ID。

連接說明

若要連線 Amazon Kendra 到您的 Confluence 資料來源，您必須提供您的匯流資料來源的必要詳細資訊，Amazon Kendra 以便能夠存取您的資料。如果您尚未配置匯流以查 Amazon Kendra 看。[必要條件](#)

Console

連接至匯流 Amazon Kendra 的步驟

1. 登入 AWS Management Console 並開啟[Amazon Kendra 主控台](#)。
2. 在左側導覽窗格中，選擇 [索引]，然後從索引清單中選擇要使用的索引。

Note

您可以選擇在索引設置下配置或編輯您的用戶訪問控制設置。

3. 在 [開始使用] 頁面上，選擇 [新增資料來源]。
4. 在 [新增資料來源] 頁面上，選擇 [匯流連接器]，然後選擇 [新增連接器]。如果使用版本 2 (如果適用)，請選擇帶有「V2.0」標籤的匯流連接器。
5. 在 [指定資料來源詳細資訊] 頁面上，輸入下列資訊：
 - a. 在名稱和說明中，對於資料來源名稱 — 輸入資料來源的名稱。您可以包含連字號，但不能包含空格。
 - b. (選擇性) 說明 — 輸入資料來源的選用說明。
 - c. 在預設語言中 — 選擇一種語言來篩選索引的文件。除非另有指定，否則語言預設為英文。文件中繼資料中指定的語言會覆寫選取的語言。


- d. 在「標籤」中，針對「新增標籤」— 包含可選標籤以搜尋和篩選資源或追蹤 AWS 成本。
 - e. 選擇下一步。
6. 在 [定義存取權和安全性] 頁面上，輸入下列資訊：
- a. 在「來源」中，選擇「匯流雲」或「匯流伺服器/資料中心」。
 - b. 匯流 URL — 輸入匯合主機 URL。例如：<https://example.confluence.com>。
 - c. (僅適用於匯流伺服器/資料中心) SSL 憑證位置-選擇性 — 輸入 Confluence 伺服器 SSL 憑證檔案的 Amazon S3 路徑。
 - d. (僅適用於匯流伺服器/資料中心) Web Proxy-選用 — 輸入 Web Proxy 主機名稱 (不含http://或https://通訊協定) 和連接埠號碼 (主機 URL 傳輸通訊協定使用的連接埠)。連接埠號碼應該是介於 0 到 65535 之間的數值。
 - e. 授權 — 開啟或關閉文件的存取控制清單 (ACL) 資訊 (如果您有 ACL)，且想要將其用於存取控制。ACL 會指定使用者和群組可存取的文件。ACL 資訊可用來根據使用者或使用者對文件的群組存取權來篩選搜尋結果。如需詳細資訊，請參閱[使用者內容篩選](#)。
 - f. 驗證 — 選擇基本驗證、Oauth 2.0 驗證或 (僅適用於匯流伺服器/資料中心) 個人存取權杖驗證。
 - g. AWS Secrets Manager 秘密 — 選擇現有密碼或建立新 Secrets Manager 密碼來儲存您的 Confluence 驗證認證。如果您選擇建立新密碼，則會開啟一個 AWS Secrets Manager 密碼視窗。在視窗中輸入下列資訊：
 - i. 秘密名稱 — 您秘密的名稱。前綴 'AmazonKendra-匯流-' 會自動添加到您的密碼名稱中。
 - ii. 如果使用基本驗證 — 輸入您在 Confluence 中配置的密碼名稱、使用者名稱和密碼 (匯流 API 權杖作為密碼)。

如果使用 OAuth2.0 身份驗證 — 輸入您在 Confluence 中配置的秘密名稱，應用程式密鑰，應用程式密鑰，訪問令牌和刷新令牌。

(僅限匯流伺服器/數據中心) 如果使用個人訪問令牌身份驗證 — 輸入您在匯流中配置的秘密名稱和匯流令牌。
 - iii. 保存並添加您的秘密。
 - h. Virtual Private Cloud (VPC) (VPC) — 您可以選擇使用 VPC。如果是這樣，您必須新增子網路和 VPC 安全性群組。
 - i. 識別爬行者程式 — 指定是否要開啟身分識別爬行 Amazon Kendra 者程式。識別爬行者程式會使用文件的存取控制清單 (ACL) 資訊，根據使用者或使用者對文件的群組存取權來篩

選擇搜尋結果。如果您有文件的 ACL 並選擇使用 ACL，您也可以選擇開啟的身分識別爬行者程式，以設定搜尋結果的使用者內容篩選。Amazon Kendra 否則，如果關閉身分搜索器，則可以公開搜索所有文檔。如果您想要對文件使用存取控制，且身分識別編目程式已關閉，您也可以使用 [PutPrincipalMapping](#) API 來上傳使用者和群組存取資訊以進行使用者內容篩選。

- j. IAM role — 選擇現有 IAM 角色或建立新 IAM 角色以存取存放庫認證和索引內容。


 Note

IAM 用於索引的角色不能用於資料來源。如果您不確定索引或常見問題集是否使用現有角色，請選擇 [建立新角色] 以避免發生錯誤。


- k. 選擇下一步。

- 7. 在 [設定同步設定] 頁面上，輸入下列資訊：

- a. 在 [同步範圍] 中，針對 [同步內容] — 選擇從下列內容類型同步：頁面、頁面註解、頁面附件、部落格、部落格留言、部落格附件、個人空間和封存空間。

 Note

只有在您選擇同步頁面時，才能選擇頁面注釋和頁面附件。只有在您選擇同步部落格時，才能選取部落格留言和部落格附件。

 Important

如果您沒有在其他配置中指定空格鍵正則表達式模式，默認情況下將檢索所有頁面和博客。

- b. 在其他組態中，對於檔案大小上限 — 指定要編目的檔案大小限制 (以 MB Amazon Kendra 為單位)。Amazon Kendra 只會編目您定義的大小限制內的檔案。預設檔案大小為 50 MB。檔案大小上限應該大於 0 MB 且小於或等於 50 MB。

對於空格正則表達式模式-指定是否使用以下命令在索引中包含或排除特定空格：

- 空格鍵 (例如，#### 123)

Note

如果您沒有指定空格鍵正則表達式模式，默認情況下將檢索所有頁面和博客。

- 網址 (例如，`.*//MySiteMyDocuments/`)
- 檔案類型 (例如 `.*\ .pdf, .*\.txt`)

對於實體標題正則表達式模式-指定規則運算式模式以按標題包含或排除某些部落格、頁面、註解和附件。

Note

如果要包含或排除抓取特定頁面或子頁面，則可以使用頁面標題正則表達式模式。

- 同步模式 — 選擇資料來源內容變更時要如何更新索引。當您第一次將資料來源同 Amazon Kendra 步處理時，依預設會檢索所有內容並建立索引。如果初始同步失敗，您必須執行資料的完整同步，即使您沒有選擇完整同步作為同步模式選項。
 - 完全同步：新鮮索引所有內容，並在每次資料來源與索引同步時取代現有內容。
 - 新增、修改、刪除的同步：每次資料來源與索引同步時，僅對新內容、已修改和刪除的內容建立索引。Amazon Kendra 可以使用資料來源的機制來追蹤內容變更，並為上次同步後變更的內容建立索引。
 - 在同步執行排程中，對於頻率 — 選擇同步資料來源內容和更新索引的頻率。
 - 選擇下一步。
- 在 [設定欄位對映] 頁面上，輸入下列資訊：
 - 從 Amazon Kendra 產生的預設資料來源欄位中選取您要對映至索引的資料來源欄位。若要新增自訂資料來源欄位，請建立要對映的索引欄位名稱和欄位資料類型。
 - 選擇下一步。
 - 在 [檢閱並建立] 頁面上，檢查您輸入的資訊是否正確，然後選取 [新增資料來源]。您也可以從此頁面選擇編輯您的資訊。成功新增資料來源後，您的資料來源將顯示在 [資料來源] 頁面上。

API

連接至匯流 Amazon Kendra 的步驟

您必須使用 [TemplateConfiguration](#) API 指定 [資料來源結構描述](#) 的 JSON。您必須提供以下信息：

- 資料來源 — 指定使用 [TemplateConfiguration](#) JSON 結構定義 CONFLUENCEV2 時的資料來源類型。同時將資料來源指定為呼叫 [CreateDataSource](#) API TEMPLATE 時的方式。
- 主機 URL — 指定合併主機 URL 執行個體。例如：<https://example.confluence.com>。
- 同步模式 — 指定資料來源內容變更時 Amazon Kendra 應如何更新索引。當您第一次將資料來源同 Amazon Kendra 步處理時，依預設會檢索所有內容並建立索引。如果初始同步失敗，您必須執行資料的完整同步，即使您沒有選擇完整同步作為同步模式選項。您可以選擇：
 - FORCED_FULL_CRAWL 新建索引所有內容，並在每次資料來源與索引同步時取代現有內容。
 - FULL_CRAWL，以在每次資料來源與索引同步時，僅對新的、修改的和刪除的內容建立索引。Amazon Kendra 可以使用資料來源的機制來追蹤內容變更，並為上次同步後變更的內容建立索引。
- 驗證類型 — 指定驗證類型，是否為 BasicOAuth2 (僅限「合流伺服器」)。Personal-token
- (選用性 — 僅適用於匯流伺服器) SSL 憑證位置 — 特別是 s3certificateName 您用來儲存 SSL 憑證的 S3bucketName 和。
- 秘密 Amazon 資源名稱 (ARN) — 提供 Secrets Manager 秘密的 Amazon 資源名稱 (ARN)，其中包含您在匯流中設定的身份驗證登入資料。如果您使用基本驗證，密碼會以下列金鑰儲存在 JSON 結構中：

```
{
  "username": "email ID or user name",
  "password": "Confluence API token"
}
```

如果您使用 OAuth 2.0 驗證，則密碼會以下列金鑰儲存在 JSON 結構中：

```
{
  "confluenceAppKey": "app key",
  "confluenceAppSecret": "app secret",
  "confluenceAccessToken": "access token",
  "confluenceRefreshToken": "refresh token"
}
```

(僅適用於匯流服務器) 如果您使用基本身份驗證，密鑰將存儲在帶有以下密鑰的 JSON 結構中：

```
{
```

```

    "hostUrl": "Confluence Server host URL",
    "username": "Confluence Server user name",
    "password": "Confluence Server password"
  }

```

(僅適用於 Confluence 服務器) 如果您使用個人訪問令牌身份驗證，密鑰將存儲在具有以下密鑰的 JSON 結構中：

```

{
  "hostUrl": "Confluence Server host URL",
  "patToken": "personal access token"
}

```

- IAM role — 指定RoleArn何時呼叫CreateDataSource以提供具有存取 Secrets Manager 密碼的權限的 IAM 角色，以及呼叫 Confluence 連接器和所需的公用 API 的時間。Amazon Kendra 有關詳情，請參閱[合流資料來源的IAM 角色](#)。

您還可以添加以下可選功能：

- V@@ irtual Private Cloud (VPC) — 指定您撥打電話的VpcConfiguration時間。CreateDataSource如需詳細資訊，請參閱 [配置 Amazon Kendra 為使用 Amazon VPC](#)。
- 檔案大小 — 指定要編目的最大檔案大小。
- 文件/內容類型 — 指定是否要編目頁面、頁面註解、頁面附件、部落格、部落格註解、部落格附件、空間和封存空間。
- 包含和排除篩選器：指定是否要包含或排除特定空間、頁面、部落格及其註解和附件。

Note

大多數資料來源使用規則運算式模式，這些模式是稱為篩選器的包含或排除模式。如果您指定包含篩選器，則只有符合包含項目篩選器的內容會編製索引。不符合包含篩選器的任何文件都不會建立索引。如果您指定包含和排除篩選器，符合排除篩選器的文件將不會建立索引，即使它們符合包含篩選器也是如此。

- 網頁代理伺服器 — 如果您想要透過網路代理連線到您的匯合 URL 執行個體，請指定您的 Web 代理伺服器資訊。您可以將此選項用於匯流伺服器。
- 存取控制清單 (ACL) — 指定是否要編目文件的 ACL 資訊 (如果您有 ACL 並且想要將其用於存取控制)。ACL 會指定使用者和群組可存取的文件。ACL 資訊可用來根據使用者或使用者對文件的群組存取來篩選搜尋結果。如需詳細資訊，請參閱[使用者內容篩選](#)。

- 識別爬行者程式 — 指定是否要開啟身分識別爬行 Amazon Kendra 爬行者程式。識別爬行者程式會使用文件的存取控制清單 (ACL) 資訊，根據使用者或使用者對文件的群組存取權來篩選搜尋結果。如果您有文件的 ACL 並選擇使用 ACL，您也可以選擇開啟的身分識別爬行者程式，以設定搜尋結果的使用者內容篩選。Amazon Kendra 否則，如果關閉身分搜索器，則可以公開搜索所有文檔。如果您想要對文件使用存取控制，且身分識別編目程式已關閉，您也可以使用 [PutPrincipalMapping](#) API 來上傳使用者和群組存取資訊以進行使用者內容篩選。
- 欄位對映 — 選擇將您的匯流資料來源欄位對映至索引欄位。Amazon Kendra 如需詳細資訊，請參閱 [映射資料來源欄位](#)。

Note

您的文件需要文件內文欄位或文件內文對等項目，才能搜尋您的文件。Amazon Kendra 您必須將資料來源中的文件內文欄位名稱對應至索引欄位名稱 `_document_body`。所有其他欄位是選用的。

如需要設定的其他重要 JSON 金鑰清單，請參閱 [匯流範本](#) 結構描述。

備註

- 個人訪問令牌 (PAT) 不適用於匯流雲。

自訂資料來源連接器

如果存放庫尚 Amazon Kendra 未為其提供資料來源連接器，請使用自訂資料來源。即使您無法使用的 Amazon Kendra 資料來源同步存放庫，您也可以使用它來查看資料來源提供 Amazon Kendra 的相同執行歷程記錄指標。使用此功能可在 Amazon Kendra 資料來源與自訂資料來源之間建立一致的同步監控體驗。具體來說，使用自訂資料來源來查看您使用 [BatchPut文件](#) 和 [BatchDelete文件](#) API 建立之資料來源連接器的同步指標。

如需 Amazon Kendra 自訂資料來源連接器的疑難排解，請參閱 [疑難排解資料來](#)。

建立自訂資料來源時，您可以完全控制如何選取要索引的文件。Amazon Kendra 僅提供可用於監視資料來源同步工作的指標資訊。您必須建立並執行可判斷資料來源索引之文件的爬行者程式。

您必須使用 `Document` 物件指定文件的主要標題，並且才能 `_source_uri` [DocumentAttribute](#) 在 Query 結果的回應中 `DocumentURI` 包含 `DocumentTitle` 並包含在內。

您可以使用控制台或使用 Source API 為自訂資料 [CreateData來源](#) 建立識別碼。若要使用主控台，請為資料來源指定名稱，並選擇性地指定描述和資源標籤。建立資料來源後，會顯示資料來源 ID。複製此 ID，以便在將資料來源與索引同步時使用。

Specify data source details

Name data source

Data source name

Maximum of 1000 alphanumeric characters. Can include hyphens (-), but not spaces.

Description - optional

Tags (0) - optional [Info](#)

A tag is an administrative label that you assign to AWS resources to make it easier to manage them. Each tag consists of a key and an optional value. Use tags to search and filter your resources or track your AWS costs.

This resource has no tags

[Add new tag](#)

You can add up to 50 more tags.

[Cancel](#) [Next](#)

您也可以使用 `CreateDataSource` API 建立自訂資料來源。當您同步資料來源時，API 會傳回要使用的 ID。當您使用 `CreateDataSource` API 建立自訂資料來源時，您無法設定 `Configuration`、`RoleArn` 或 `Schedule` 參數。如果您設定這些參數，Amazon Kendra 會傳回 `ValidationException` 例外狀況。

若要使用自訂資料來源，請建立負責更新 Amazon Kendra 索引的應用程式。應用程式取決於您建立的爬行者程式。爬行者程式會讀取儲存庫中的文件，並決定要傳送到 Amazon Kendra 哪些文件。您的應用程式應該執行下列步驟：

1. 編目您的存放庫，並列出存放庫中新增、更新或刪除的文件。

2. 呼叫 [StartDataSourceSyncJob](#) API，表示同步工作正在開始。您提供資料來源 ID 以識別正在同步的資料來源。Amazon Kendra 會傳回執行 ID，以識別特定的同步工作。
3. 呼叫 [BatchDeleteDocument](#) API 以從索引中移除文件。您可以提供資料來源 ID 和執行 ID，以識別正在同步處理的資料來源以及與此更新相關聯的工作。
4. 呼叫 [StopDataSourceSyncJob](#) API 以表示同步工作結束。呼叫 [StopDataSourceSyncJob](#) API 之後，關聯的執行 ID 將不再有效。
5. 呼叫具有索引和資料來源識別碼的 [ListDataSourceSyncJobs](#) API，以列出資料來源的同步工作，並查看同步工作的指標。

結束同步工作後，您可以開始新的同步工作。在將所有提交的文件新增至索引之前，可能需要一段時間。使用 [ListDataSourceSyncJobs](#) API 查看同步工作的狀態。如果針對同步工作 `Status` 傳回的是 `SYNCING_INDEXING`，則某些文件仍在編製索引。當先前工作的狀態為 `FAILED` 或 `SUCCEEDED` 時，您可以啟動新的同步工作。

呼叫 [StopDataSourceSyncJob](#) API 之後，您無法在呼叫 [BatchPutDocument](#) 或 [BatchDeleteDocument](#) API 時使用同步工作識別碼。如果這樣做，所有提交的文件都會在 API 的回 `FailedDocuments` 應訊息中傳回。

必要屬性

當您 Amazon Kendra 使用 [BatchPutDocument](#) API 提交文件時，每個文件都需要兩個屬性來識別其所屬的資料來源和同步執行。您必須提供下列兩個屬性，才能將自訂資料來源中的文件正確對應至 Amazon Kendra 索引：

- `_data_source_id` 資料來源的識別碼。當您使用主控台或 [CreateDataSource](#) API 建立資料來源時，會傳回此選項。
- `_data_source_sync_job_execution_id` 同步執行的識別碼。當您使用 [StartDataSourceSyncJob](#) API 啟動索引同步處理時，會傳回此選項。

以下是使用自訂資料來源索引文件所需的 JSON。

```
{
  "Documents": [
    {
      "Attributes": [
        {
          "Key": "_data_source_id",
```

```

        "Value": {
            "StringValue": "data source identifier"
        }
    },
    {
        "Key": "_data_source_sync_job_execution_id",
        "Value": {
            "StringValue": "sync job identifier"
        }
    }
],
"Blob": "document content",
"ContentType": "content type",
"Id": "document identifier",
"Title": "document title"
}
],
"IndexId": "index identifier",
"RoleArn": "IAM role ARN"
}

```

當您使用 BatchDeleteDocument API 從索引中移除文件時，您需要
在 DataSourceSyncJobMetricTarget 參數中指定下列兩個欄位：

- DataSourceId 資料來源的識別碼。當您使用主控台或 CreateDataSource API 建立資料來源時，會傳回此選項。
- DataSourceSyncJobId 同步執行的識別碼。當您使用 StartDataSourceSyncJob API 啟動索引同步處理時，會傳回此選項。

以下是使用 BatchDeleteDocument API 從索引中刪除文檔所需的 JSON。

```

{
  "DataSourceSyncJobMetricTarget": {
    "DataSourceId": "data source identifier",
    "DataSourceSyncJobId": "sync job identifier"
  },
  "DocumentIdList": [
    "document identifier"
  ],
  "IndexId": "index identifier"
}

```

檢視 指標

同步工作完成後，您可以使用 [DataSourceSyncJob 指標](#) API 取得與同步工作相關聯的指標。使用此選項可監視您的自訂資料來源同步。

如果您多次提交相同的文件 (作為 BatchPutDocument API、API 的一部分)，或提交文件以進行新增和刪除，則該文件只會在指標中計算一次。BatchDeleteDocument

- DocumentsAdded 使用與此同步工作相關聯的 BatchPutDocument API 提交的文件數目，首次新增至索引。如果在同步中提交文件以供新增多次，則該文件只會在量度中計算一次。
- DocumentsDeleted 使用與此同步工作相關聯的 BatchDeleteDocument API 提交的文件數目，從索引中刪除。如果文件在同步中提交多次要刪除，則該文件只會在量度中計算一次。
- DocumentsFailed 與此同步工作相關聯的文件編製索引失敗的數目。這些是已接受索引 Amazon Kendra，但無法編製索引或刪除的文件。如果文件未被接受 Amazon Kendra，則會在 BatchPutDocument 和 BatchDeleteDocument API 的回 FailedDocuments 應屬性中傳回文件的識別碼。
- DocumentsModified 使用與此同步工作相關聯的 BatchPutDocument API 提交的已修改文件數目 (在 Amazon Kendra 索引中修改過)。

Amazon Kendra 也會在索引文件時發出 Amazon CloudWatch 量度。如需詳細資訊，請參閱 [Amazon Kendra 使用監視 Amazon CloudWatch](#)。

Amazon Kendra 不會傳回自訂資料來源的 DocumentsScanned 指標。它也會 [針對 Amazon Kendra 資料來源發出文件「度量」](#) 中列出的量度。CloudWatch

進一步了解

若要深入瞭解如何 Amazon Kendra 與自訂資料來源整合，請參閱：

- [將自訂資料來源新增至 Amazon Kendra](#)

自訂資料來源

下列程式碼提供使用 Java 之自訂資料來源的範例實作。程式會先建立自訂資料來源，然後將新增的文件與自訂資料來源同步至索引。

下列程式碼會示範建立和使用自訂資料來源。當您在應用程式中使用自訂資料來源時，每次將索引與資料來源同步化時，都不需要建立新的資料來源 (一次性程序)。您可以使用索引 ID 和資料來源 ID 來同步處理資料。

```
package com.amazonaws.kendra;

import java.util.concurrent.TimeUnit;
import software.amazon.awssdk.services.kendra.KendraClient;
import software.amazon.awssdk.services.kendra.model.BatchPutDocumentRequest;
import software.amazon.awssdk.services.kendra.model.BatchPutDocumentResponse;
import software.amazon.awssdk.services.kendra.model.CreateDataSourceRequest;
import software.amazon.awssdk.services.kendra.model.CreateDataSourceResponse;
import software.amazon.awssdk.services.kendra.model.DataSourceType;
import software.amazon.awssdk.services.kendra.model.Document;
import software.amazon.awssdk.services.kendra.model.ListDataSourceSyncJobsRequest;
import software.amazon.awssdk.services.kendra.model.ListDataSourceSyncJobsResponse;
import software.amazon.awssdk.services.kendra.model.StartDataSourceSyncJobRequest;
import software.amazon.awssdk.services.kendra.model.StartDataSourceSyncJobResponse;
import software.amazon.awssdk.services.kendra.model.StopDataSourceSyncJobRequest;
import software.amazon.awssdk.services.kendra.model.StopDataSourceSyncJobResponse;

public class SampleSyncForCustomDataSource {
    public static void main(String[] args) {
        KendraClient kendra = KendraClient.builder().build();

        String myIndexId = "yourIndexId";
        String dataSourceName = "custom data source";
        String dataSourceDescription = "Amazon Kendra custom data source connector"

        // Create custom data source
        CreateDataSourceRequest createDataSourceRequest = CreateDataSourceRequest
            .builder()
            .indexId(myIndexId)
            .name(dataSourceName)
            .description(dataSourceDescription)
            .type(DataSourceType.CUSTOM)
            .build();

        CreateDataSourceResponse createDataSourceResponse =
            kendra.createDataSource(createDataSourceRequest);
        System.out.println(String.format("Response of creating data source: %s",
            createDataSourceResponse));

        // Get the data source ID from createDataSourceResponse
        String dataSourceId = createDataSourceResponse.Id();

        // Wait for the custom data source to become active
```

```
System.out.println(String.format("Waiting for Amazon Kendra to create the data
source %s", dataSourceId));
// You can use the DescribeDataSource API to check the status
DescribeDataSourceRequest describeDataSourceRequest = DescribeDataSourceRequest
    .builder()
    .indexId(myIndexId)
    .id(dataSourceId)
    .build();

while (true) {
    DescribeDataSourceResponse describeDataSourceResponse =
kendra.describeDataSource(describeDataSourceRequest);

    DataSourceStatus status = describeDataSourceResponse.status();
    System.out.println(String.format("Creating data source. Status: %s", status));
    if (status != DataSourceStatus.CREATING) {
        break;
    }

    TimeUnit.SECONDS.sleep(60);
}

// Start syncing your data source by calling StartDataSourceSyncJob and providing
your index ID
// and your custom data source ID
System.out.println(String.format("Synchronize the data source %s", dataSourceId));
StartDataSourceSyncJobRequest startDataSourceSyncJobRequest =
StartDataSourceSyncJobRequest
    .builder()
    .indexId(myIndexId)
    .id(dataSourceId)
    .build();
StartDataSourceSyncJobResponse startDataSourceSyncJobResponse =
kendra.startDataSourceSyncJob(startDataSourceSyncJobRequest);

// Get the sync job execution ID from startDataSourceSyncJobResponse
String executionId = startDataSourceSyncJobResponse.executionId();
System.out.println(String.format("Waiting for the data source to sync with the index
%s for execution ID %s", indexId, startDataSourceSyncJobResponse.executionId()));

// Add 2 documents uploaded to S3 bucket to your index using the BatchPutDocument
API
// The added documents should sync with your custom data source
Document pollyDoc = Document
```

```
.builder()
.s3Path(
    S3Path.builder()
        .bucket("s3-test-bucket")
        .key("what_is_Amazon_Polly.docx")
        .build())
.title("What is Amazon Polly?")
.id("polly_doc_1")
.build();

Document rekognitionDoc = Document
    .builder()
    .s3Path(
        S3Path.builder()
            .bucket("s3-test-bucket")
            .key("what_is_amazon_rekognition.docx")
            .build())
    .title("What is Amazon rekognition?")
    .id("rekognition_doc_1")
    .build();

BatchPutDocumentRequest batchPutDocumentRequest = BatchPutDocumentRequest
    .builder()
    .indexId(myIndexId)
    .documents(pollyDoc, rekognitionDoc)
    .build();

BatchPutDocumentResponse result = kendra.batchPutDocument(batchPutDocumentRequest);
System.out.println(String.format("BatchPutDocument result: %s", result));

// Once custom data source synced, stop the sync job using the
StopDataSourceSyncJob API
StopDataSourceSyncJobResponse stopDataSourceSyncJobResponse =
kendra.stopDataSourceSyncJob(
    StopDataSourceSyncJobRequest()
        .indexId(myIndexId)
        .id(dataSourceId)
    );

// List your sync jobs
ListDataSourceSyncJobsRequest listDataSourceSyncJobsRequest =
ListDataSourceSyncJobsRequest
    .builder()
    .indexId(myIndexId)
```

```
        .id(dataSourceId)
        .build();

    while (true) {
        ListDataSourceSyncJobsResponse listDataSourceSyncJobsResponse =
kendra.listDataSourceSyncJobs(listDataSourceSyncJobsRequest);
        DataSourceSyncJob job = listDataSourceSyncJobsResponse.history().get(0);
        System.out.println(String.format("Status: %s", job.status()));
    }
}
}
```

Dropbox

Dropbox 是一種文件託管服務，提供雲存儲，文檔組織和文檔模板服務。如果您是 Dropbox 使用者，您可以使 Amazon Kendra 用索引您的 Dropbox 檔案、Paper、紙張範本，以及儲存網頁捷徑。您也可以設定 Amazon Kendra 為索引特定的 Dropbox 檔案、Dropbox Paper、Paper 範本，以及儲存的網頁捷徑。

Amazon Kendra Dropbox 企業版同時支援 Dropbox 和進階版。

您可以使用[Amazon Kendra 主控台](#)和 [TemplateConfiguration](#) API 連線 Amazon Kendra 到 Dropbox 資料來源。

如需 Amazon Kendra Dropbox 資料來源連接器的疑難排解，請參閱[疑難排解資料來](#)。

主題

- [支援的功能](#)
- [必要條件](#)
- [連接說明](#)
- [進一步了解](#)

支援的功能

Amazon Kendra Dropbox 資料來源連接器支援下列功能：

- 欄位對映
- 使用者存取控制

- 包含/排除過濾器
- 完整和增量內容同步
- 虛擬私有雲端 (VPC)

必要條件

您可以在 Dropbox 資料來源建立索引之前，請先在 Dropbox 和 AWS 帳戶中進行這些變更。Amazon Kendra

請確認您擁有下列項目：

- 建立 Dropbox 進階帳戶並設定管理員使用者。
- 設定 Dropbox 應用程式使用唯一的應用程式名稱，啟用範圍存取權限。請參閱 [Dropbox 建立應用程式的說明文件](#)。
- 在 Dropbox 主機上啟用 Dropbox 完整權限，並新增下列權限：
 - 文件. 內容.
 - 文件. 元數據. 讀
 - 分享. 閱讀
 - 文件請求. 讀
 - 群組. 閱讀
 - 團隊信息
 - 團隊資料內容
- 記下您的 Dropbox 應用程式金鑰、Dropbox 應用程式密鑰，以及基本驗證憑證的 Dropbox 存取權杖。

Note

我們建議您定期重新整理或輪換您的認證和密碼。僅為您自己的安全提供必要的訪問級別。我們不建議您跨資料來源以及連接器 1.0 和 2.0 版 (如果適用) 重複使用認證和密碼。

- 為您的 Dropbox 應用程式設定並複製了暫時的 OAuth 2.0 存取權杖。此令牌是臨時的，並在 4 小時後過期。請參閱有關 [OAuth 驗證的說明文件](#)。

Note

建議您建立一個永不過期的 Dropbox 重新整理存取權杖，而不是仰賴 4 小時後過期的一次性存取權杖。重新整理存取權杖是永久性的，永不過期，因此您可以在 future 繼續同步資料來源。

- 建議：設定永不過期的 Dropbox 永久重新整理權杖，以便 Amazon Kendra 繼續同步您的資料來源，而不會造成任何干擾。請參閱有[關重新整理權杖的 Dropbox 文件](#)
- 核取每份文件在 Dropbox 和您打算用於相同索引的其他資料來源中都是唯一的。您要用於索引的每個資料來源不得包含跨資料來源的相同文件。文件 ID 對索引來說是全域的，而且每個索引必須是唯一的。

在您的中 AWS 帳戶，請確保您有：

- [建立 Amazon Kendra 索引](#)，如果使用 API，則會記下索引識別碼。
- 為您的[資料來源建立 IAM 角色](#)，如果使用 API，則會記錄 IAM 角色的 ARN。

Note

如果您變更驗證類型和認證，則必須更新 IAM 角色才能存取正確的 AWS Secrets Manager 密碼 ID。

- 將您的 Dropbox 身份驗證憑據存儲在 AWS Secrets Manager 密碼中，如果使用 API，則會記錄密碼的 ARN。

Note

我們建議您定期重新整理或輪換您的認證和密碼。僅為您自己的安全提供必要的訪問級別。我們不建議您跨資料來源以及連接器 1.0 和 2.0 版 (如果適用) 重複使用認證和密碼。

如果您沒有現有的 IAM 角色或密碼，可以在將 Dropbox 資料來源連結至時，使用主控台建立新 IAM 角色和 Secrets Manager 密碼 Amazon Kendra。如果您使用 API，則必須提供現有 IAM 角色和 Secrets Manager 密碼的 ARN 以及索引 ID。

連接說明

若要連線 Amazon Kendra 到 Dropbox 資料來源，您必須提供 Dropbox 資料來源的必要詳細資訊，才 Amazon Kendra 能存取您的資料。如果您尚未為 Dropbox 設定 Amazon Kendra，請參閱[必要條件](#)。

Console

若要連線 Amazon Kendra 到


1. 登入 AWS Management Console 並開啟[Amazon Kendra 主控台](#)。
2. 在左側導覽窗格中，選擇 [索引]，然後從索引清單中選擇要使用的索引。

Note

您可以選擇在索引設置下配置或編輯您的用戶訪問控制設置。

3. 在 [開始使用] 頁面上，選擇 [新增資料來源]。
4. 在 [新增資料來源] 頁面上，選擇 [Dropbox 連接器]，然後選擇 [新增連接器]。如果使用的是第 2 版 (如果適用)，請選擇標記為「V2.0」的 Dropbox 連接器。
5. 在 [指定資料來源詳細資訊] 頁面上，輸入下列資訊：
 - a. 在名稱和說明中，對於資料來源名稱 — 輸入資料來源的名稱。您可以包含連字號，但不能包含空格。
 - b. (選擇性) 說明 — 輸入資料來源的選用說明。
 - c. 在預設語言中 — 選擇一種語言來篩選索引的文件。除非另有指定，否則語言預設為英文。文件中繼資料中指定的語言會覆寫選取的語言。
 - d. 在「標籤」中，針對「新增標籤」 — 包含可選標籤以搜尋和篩選資源或追蹤 AWS 成本。
 - e. 選擇下一步。
6. 在 [定義存取權和安全性] 頁面上，輸入下列資訊：
 - a. 授權 — 開啟或關閉文件的存取控制清單 (ACL) 資訊 (如果您有 ACL)，且想要將其用於存取控制。ACL 會指定使用者和群組可存取的文件。ACL 資訊可用來根據使用者或使用者對文件的群組存取來篩選搜尋結果。如需詳細資訊，請參閱[使用者內容篩選](#)。
 - b. 驗證 Token 的類型 — 選擇永久權杖 (建議使用) 或暫時存取權杖。
 - c. AWS Secrets Manager 密碼：選擇現有密碼或建立新 Secrets Manager 密碼來儲存您的 Dropbox 驗證憑證。如果您選擇建立新密碼，則會開啟一個 AWS Secrets Manager 密碼視窗。

- i. 在「建立 AWS Secrets Manager 密碼視窗」中輸入下列資訊：
 - A. 秘密名稱 — 您秘密的名稱。前綴 'AmazonKendra-Dropbox-' 會自動添加到您的密碼名稱中。
 - B. 針對應用程式金鑰、應用程式密鑰和權杖資訊 (永久或暫時)，請輸入 Dropbox 中設定的驗證憑證值。
- ii. 保存並添加您的秘密。
- d. Virtual Private Cloud (VPC) (VPC) — 您可以選擇使用 VPC。如果是這樣，您必須新增子網路和 VPC 安全性群組。
- e. 識別爬行者程式 — 指定是否要開啟身分識別爬行 Amazon Kendra 爬行者程式。識別爬行者程式會使用文件的存取控制清單 (ACL) 資訊，根據使用者或使用者對文件的群組存取權來篩選搜尋結果。如果您有文件的 ACL 並選擇使用 ACL，您也可以選擇開啟的身分識別爬行者程式，以設定搜尋結果的使用者環境定義篩選。Amazon Kendra 否則，如果關閉身分搜索器，則可以公開搜索所有文檔。如果您想要對文件使用存取控制，且身分識別編目程式已關閉，您也可以使用 [PutPrincipalMapping](#) API 來上傳使用者和群組存取資訊以進行使用者內容篩選。
- f. IAM role — 選擇現有 IAM 角色或建立新 IAM 角色以存取存放庫認證和索引內容。

 Note

IAM 用於索引的角色不能用於資料來源。如果您不確定索引或常見問題集是否使用現有角色，請選擇 [建立新角色] 以避免發生錯誤。

- g. 選擇下一步。
7. 在 [設定同步設定] 頁面上，輸入下列資訊：
 - a. 針對 [選取實體或內容類型]，選擇您要編目的 Dropbox 實體或內容類型。
 - b. 在 Regex 模式的其他配置中-添加正則表達式模式以包含或排除某些文件。
 - c. 同步模式 — 選擇資料來源內容變更時要如何更新索引。當您第一次將資料來源同 Amazon Kendra 步處理時，依預設會檢索所有內容並建立索引。如果初始同步失敗，您必須執行資料的完整同步，即使您沒有選擇完整同步作為同步模式選項。
 - 完全同步：新鮮索引所有內容，並在每次資料來源與索引同步時取代現有內容。

- 新增、修改的同步：每次資料來源與索引同步時，僅對新內容和已修改的內容建立索引。Amazon Kendra 可以使用資料來源的機制來追蹤內容變更，並為上次同步後變更的內容建立索引。
 - 新增、修改、刪除的同步：每次資料來源與索引同步時，僅對新內容、已修改和刪除的內容建立索引。Amazon Kendra 可以使用資料來源的機制來追蹤內容變更，並為上次同步後變更的內容建立索引。
- d. 在同步執行排程中，對於頻率 — 選擇同步資料來源內容和更新索引的頻率。
 - e. 選擇下一步。
8. 在 [設定欄位對映] 頁面上，輸入下列資訊：
 - a. 檔案、Dropbox Paper 和 Dropbox Paper 範本：從 Amazon Kendra 產生的預設資料來源欄位中選取您要對應至索引的預設資料來源欄位。
 - b. 新增欄位 — 新增自訂資料來源欄位，以建立要對映的索引欄位名稱和欄位資料類型。
 - c. 選擇下一步。
 9. 在 [檢閱並建立] 頁面上，檢查您輸入的資訊是否正確，然後選取 [新增資料來源]。您也可以從此頁面選擇編輯您的資訊。成功新增資料來源後，您的資料來源將顯示在 [資料來源] 頁面上。


API

若要連線 Amazon Kendra 到

您必須使用 [TemplateConfiguration](#) API 指定 [資料來源結構描述](#) 的 JSON。您必須提供以下信息：

- 資料來源 — 指定使用 [TemplateConfiguration](#) JSON 結構定義 DROPBOX 時的資料來源類型。同時將資料來源指定為呼叫 [CreateDataSource](#) API TEMPLATE 時的方式。
- 同步模式 — 指定資料來源內容變更時 Amazon Kendra 應如何更新索引。當您第一次將資料來源同 Amazon Kendra 步處理時，依預設會檢索所有內容並建立索引。如果初始同步失敗，您必須執行資料的完整同步，即使您沒有選擇完整同步作為同步模式選項。您可以選擇：
 - FORCED_FULL_CRAWL 新建索引所有內容，並在每次資料來源與索引同步時取代現有內容。
 - FULL_CRAWL，以在每次資料來源與索引同步時，僅對新的、修改的和刪除的內容建立索引。Amazon Kendra 可以使用資料來源的機制來追蹤內容變更，並為上次同步後變更的內容建立索引。
 - CHANGE_LOG 每次資料來源與索引同步時，僅對新內容和修改的內容建立索引。Amazon Kendra 可以使用資料來源的機制來追蹤內容變更，並為上次同步後變更的內容建立索引。

- 存取權杖類型 — 指定您要為儲存驗證信用者的 AWS Secrets Manager 密碼使用永久或暫時存取權杖。

 Note

建議您建立一個永遠不會在 Dropbox 中過期的重新整理存取權杖，而不是仰賴在 4 小時後過期的一次性存取權杖。您可以在 Dropbox 開發人員主控台中建立應用程式和重新整理存取權杖，並在密碼中提供存取權杖。

- 秘密 Amazon 資源名稱 (ARN) — 提供包含 Dropbox 帳戶身份驗證登入資料的 Secrets Manager 密碼的 Amazon 資源名稱 (ARN)。密碼會以下列金鑰儲存在 JSON 結構中：

```
{
  "appKey": "Dropbox app key",
  "appSecret": "Dropbox app secret",
  "accesstoken": "temporary access token or refresh access token"
}
```

- 識別爬行者程式 — 指定是否要開啟身分識別爬行者 Amazon Kendra 程式。識別爬行者程式會使用文件的存取控制清單 (ACL) 資訊，根據使用者或使用者對文件的群組存取權來篩選搜尋結果。如果您有文件的 ACL 並選擇使用 ACL，您也可以選擇開啟的身分識別爬行者程式，以設定搜尋結果的使用者環境定義篩選。Amazon Kendra 否則，如果關閉身分搜索器，則可以公開搜索所有文檔。如果您想要對文件使用存取控制，且身分識別編目程式已關閉，您也可以使用 [PutPrincipalMapping](#) API 來上傳使用者和群組存取資訊以進行使用者內容篩選。
- IAM role — 指定您打電話 CreateDataSource 給 IAM 角色的 RoleArn 時間，以提供具有存取 Secrets Manager 密碼的權限，以及呼叫 Dropbox 連接器和 Amazon Kendra 所需的公開 API 的時間。如需詳細資訊，請參閱 [Dropbox 資料來源的 IAM 角色](#)。

您還可以添加以下可選功能：

- Virtual Private Cloud (VPC) — 指定您撥打電話的 VpcConfiguration 時間。CreateDataSource 如需詳細資訊，請參閱 [配置 Amazon Kendra 為使用 Amazon VPC](#)。
- 文件/內容類型：指定是否要檢索儲存在 Dropbox 中的檔案、Dropbox Paper 文件、Dropbox Paper 範本，以及網頁捷徑。
- 包含和排除篩選器 — 指定要包含還是排除某些檔案。

Note

大多數資料來源使用規則運算式模式，這些模式是稱為篩選器的包含或排除模式。如果您指定包含篩選器，則只會編製與包含項目篩選器相符的內容編製索引。不符合包含篩選器的任何文件都不會建立索引。如果您指定包含和排除篩選器，符合排除篩選器的文件將不會建立索引，即使它們符合包含篩選器也是如此。

- 存取控制清單 (ACL) — 指定是否要編目文件的 ACL 資訊 (如果您有 ACL 並且想要將其用於存取控制)。ACL 會指定使用者和群組可存取的文件。ACL 資訊可用來根據使用者或使用者對文件的群組存取來篩選搜尋結果。如需詳細資訊，請參閱[使用者內容篩選](#)。
- 欄位對應 — 選擇將 Dropbox 資料來源欄位對應至 Amazon Kendra 索引欄位。如需詳細資訊，請參閱[映射資料來源欄位](#)。

Note

您的文件需要文件內文欄位或文件內文對等項目，才能搜尋您的文件。Amazon Kendra 您必須將資料來源中的文件內文欄位名稱對應至索引欄位名稱_document_body。所有其他欄位是選用的。

如需要設定的其他重要 JSON 金鑰清單，請參閱 [Dropbox 範本結構描述](#)。

進一步了解

若要進一步了解如何整合 Amazon Kendra 與您的 Dropbox 資料來源，請參閱：

- [使用下列連接器為您的 Dropbox 內容建立索引 Amazon Kendra](#)

Drupal

Drupal 是一個開源內容管理系統 (CMS)，您可以使用它來創建網站和 Web 應用程序。您可以使 Amazon Kendra 用在 Drupal 中索引以下內容：

- 內容-文章，基本頁面，基本塊，用戶定義的內容類型，用戶定義的塊類型，自定義內容類型，自定義塊類型
- 註解 — 適用於任何內容類型和區塊類型

- 附件 — 適用於任何內容類型和區塊類型

您可以使用[Amazon Kendra 控制台](#)或 [TemplateConfiguration](#)API 連接 Amazon Kendra 到您的 Drupal 數據源。

有關 Amazon Kendra Drupal 數據源連接器的故障排除，請參閱[疑難排解資料](#)。

主題

- [支援的功能](#)
- [必要條件](#)
- [連接說明](#)
- [備註](#)

支援的功能

Amazon Kendra Drupal 的數據源連接器支持以下功能：

- 欄位對映
- 使用者內容篩選
- 包含/排除過濾器
- 完整和增量內容同步
- 虛擬私有雲端 (VPC)


必要條件

在您可以使用 Amazon Kendra 索引您的 Drupal 數據源之前，請在 Drupal 和 AWS 帳戶中進行這些更改。

在 Drupal 中，請確保您有：

- 創建了一個 Drupal (標準) 套件帳戶和一個具有管理員角色的用戶。
- 複製您的 Drupal 站點名稱並配置了主機網址。例如，`HTTPS#///<hostname><drupalsitename>`。
- 包含用戶名 (Drupal 網站登錄用戶名) 和密碼 (Drupal 的網站密碼) 配置基本身份驗證憑據。
- 建議：已設定 OAuth 2.0 憑證權杖。使用此令牌與您的 Drupal 密碼授予，客戶端 ID，客戶機密，用戶名 (Drupal 網站登錄用戶名) 和密碼 (Drupal 的網站密碼) 連接到一起 Amazon Kendra。
- 使用管理員角色在 Drupal 帳戶中添加了以下權限：


- 管理圖塊
- 管理區塊內容顯示
- 管理區塊內容欄位
- 管理區塊內容表單顯示
- 管理檢視
- 檢視使用者電子郵件
- 檢視自己的未發佈內容
- 檢視頁面修訂
- 檢視文章修訂
- 檢視所有修訂
- 檢視管理主題
- 存取內容
- 存取內容概觀
- 存取註解
- 搜尋內容
- 存取檔案概述
- 存取關聯式連結

 Note

如果有用戶定義的內容類型或用戶定義的塊類型，或者將任何視圖和塊添加到 Drupal 網站，則必須為它們提供管理員訪問權限。

在你的 AWS 帳戶，確保你有：

- [建立 Amazon Kendra 索引](#)，如果使用 API，則會記下索引 ID。
- 為您的[資料來源建立 IAM 角色](#)，如果使用 API，則會記錄 IAM 角色的 ARN。

 Note

如果您變更驗證類型和認證，則必須更新 IAM 角色才能存取正確的 AWS Secrets Manager 密碼 ID。

- 將您的 Drupal 身份驗證憑據存儲在一個 AWS Secrets Manager 秘密中，如果使用 API，請注意秘密的 ARN。

Note

我們建議您定期重新整理或輪換您的認證和密碼。僅為您自己的安全提供必要的訪問級別。我們不建議您跨資料來源以及連接器 1.0 和 2.0 版 (如果適用) 重複使用認證和密碼。

如果您沒有現有的 IAM 角色或秘密，則可以在將 Drupal 數據源連接到時使用控制台創建新 IAM 角色和 Secrets Manager 秘密 Amazon Kendra。如果您使用 API，則必須提供現有 IAM 角色和 Secrets Manager 密碼的 ARN 以及索引 ID。

連接說明

要連接 Amazon Kendra 到您的 Drupal 數據源，您必須提供您的 Drupal 憑據的詳細信息，Amazon Kendra 以便可以訪問您的數據。如果您還沒有配置 Drupal 的 Amazon Kendra 查看[必要條件](#)。

Console

要連 Amazon Kendra 接到

1. 登入 AWS Management Console 並開啟[Amazon Kendra 主控台](#)。
2. 在左側導覽窗格中，選擇 [索引]，然後從索引清單中選擇要使用的索引。

Note

您可以選擇在索引設置下配置或編輯用戶訪問控制設置。

3. 在 [開始使用] 頁面上，選擇 [新增資料來源]。
4. 在 [新增資料來源] 頁面上，選擇 [Drupal 連接器]，然後選擇 [新增連接器]。如果使用版本 2 (如果適用)，請選擇帶有「V2.0」標籤的 Drupal 連接器。
5. 在 [指定資料來源詳細資訊] 頁面上，輸入下列資訊：
 - a. 在名稱和說明中，對於資料來源名稱 — 輸入資料來源的名稱。您可以包含連字號，但不能包含空格。
 - b. (選擇性) 說明 — 輸入資料來源的選用說明。
 - c. 在預設語言中 — 選擇一種語言來篩選索引的文件。除非另有指定，否則語言預設為英文。文件中繼資料中指定的語言會覆寫選取的語言。

- d. 在「標籤」中，針對「新增標籤」— 包含可選標籤以搜尋和篩選資源或追蹤 AWS 成本。
 - e. 選擇下一步。
6. 在 [定義存取和安全性] 頁面上，輸入下列資訊：
- a. 在源，對於主機網址-您的 Drupal 網站的主機網址。例如，`HTTPS#<protocol><hostname><drupalsitename>`。
 - b. 對於 SSL 憑證位置，請輸入儲存在 Amazon S3 值區中的 SSL 憑證路徑。
 - c. 授權 — 開啟或關閉文件的存取控制清單 (ACL) 資訊 (如果您有 ACL)，且想要將其用於存取控制。ACL 會指定使用者和群組可存取的文件。ACL 資訊可用來根據使用者或使用者對文件的群組存取來篩選搜尋結果。如需詳細資訊，請參閱[使用者內容篩選](#)。
 - d. 對於驗證 — 根據您的使用案例，在基本驗證和 OAuth 2.0 驗證之間進行選擇。
 - e. AWS Secrets Manager 秘密-選擇現有的秘密或創建一個新的 Secrets Manager 秘密來存儲您的 Drupal 身份驗證憑據。如果您選擇建立新密碼，則會開啟一個 AWS Secrets Manager 密碼視窗。
 - i. 在「建立 AWS Secrets Manager 密碼視窗」中輸入下列資訊：
 - A. 如果您選擇了基本身份驗證，輸入一個秘密名稱，用戶名，(Drupal 的站點用戶名)，和密碼 (Drupal 的站點密碼) 您複製並選擇保存並添加秘密。
 - B. 如果您選擇 OAuth 2.0 身份驗證，輸入一個秘密名稱，用戶名 (Drupal 站點用戶名)，密碼 (Drupal 的站點密碼)，客戶端 ID，並在您的 Drupal 帳戶生成的客戶端密鑰，然後選擇保存並添加秘密。
 - ii. 選擇儲存。
 - f. Virtual Private Cloud (VPC) (VPC) — 您可以選擇使用 VPC。如果是這樣，您必須新增子網路和 VPC 安全性群組。
 - g. 識別爬行者程式 — 指定是否要開啟身分識別爬行者程式。識別爬行者程式會使用文件的存取控制清單 (ACL) 資訊，根據使用者或使用者對文件的群組存取權來篩選搜尋結果。如果您有文件的 ACL 並選擇使用 ACL，您也可以選擇開啟的身分識別爬行者程式，以設定搜尋結果的使用者環境定義篩選。Amazon Kendra 否則，如果關閉身分搜索器，則可以公開搜索所有文檔。如果您想要對文件使用存取控制，且身分識別編目程式已關閉，您也可以使用 [PutPrincipalMapping](#) API 來上傳使用者和群組存取資訊以進行使用者內容篩選。
 - h. IAM role — 選擇現有 IAM 角色或建立新 IAM 角色以存取存放庫認證和索引內容。

Note

IAM 用於索引的角色不能用於資料來源。如果您不確定索引或常見問題集是否使用現有角色，請選擇 [建立新角色] 以避免發生錯誤。

- i. 選擇下一步。
7. 在 [設定同步設定] 頁面上，輸入下列資訊：
 - a. 對於同步範圍，請從下列選項中選擇：

Note

當您選擇檢索「文章」、「基本」頁面和「基本」區塊時，其預設欄位會自動同步。您也可以選擇同步其註解、附件、自訂欄位和其他自訂實體。

- 對於選取圖元：
 - 文章 — 選擇是否要檢索「文章」、其註解「註解」及其附件。
 - 基本頁面 — 選擇是否要編目「基本」頁面、其「註解」及其「附件」。
 - 基本區塊 — 選擇是否要編目基本區塊、其註解及其附件。
 - 您也可以選擇新增「自訂」內容類型和「自訂區塊」。
- b. 對於其他配置-可選：
 - 對於正則表達式模式-添加正則表達式模式以包含或排除特定的實體標題和文件名。您最多可以添加 100 個圖案。
- c. 同步模式 — 選擇資料來源內容變更時要如何更新索引。當您第一次將資料來源同 Amazon Kendra 步處理時，依預設會檢索所有內容並建立索引。如果初始同步失敗，您必須執行資料的完整同步，即使您沒有選擇完整同步作為同步模式選項。
 - 完全同步：新鮮索引所有內容，並在每次資料來源與索引同步時取代現有內容。
 - 新增、修改、刪除的同步：每次資料來源與索引同步時，僅對新內容、已修改和刪除的內容建立索引。Amazon Kendra 可以使用資料來源的機制來追蹤內容變更，並為上次同步後變更的內容建立索引。
- d. 在同步執行排程中，頻率 — 與資料來源同步的頻率。Amazon Kendra
- e. 選擇下一步。

8. 在 [設定欄位對映] 頁面上，輸入下列資訊：
 - a. 對於「內容」、「註解」和「附件」— 從 Amazon Kendra 產生的預設資料來源欄位中選取您要對映至索引的資料來源欄位。
 - b. 新增欄位 — 新增自訂資料來源欄位，以建立要對映的索引欄位名稱和欄位資料類型。
 - c. 選擇下一步。
9. 在 [檢閱並建立] 頁面上，檢查您輸入的資訊是否正確，然後選取 [新增資料來源]。您也可以從此頁面選擇編輯您的資訊。成功新增資料來源後，您的資料來源將顯示在 [資料來源] 頁面上。

API

要連 Amazon Kendra 接到

您必須使用 [TemplateConfiguration](#) API 指定 [資料來源結構描述](#) 的 JSON。您必須提供以下信息：

- 資料來源 — 指定使用 [TemplateConfiguration](#) JSON 結構定義 DRUPAL 時的資料來源類型。同時指定呼叫 [CreateDataSource](#) API TEMPLATE 時的資料來源。
- 同步模式 — 指定資料來源內容變更時 Amazon Kendra 應如何更新索引。當您第一次將資料來源同 Amazon Kendra 步處理時，依預設會檢索所有內容並建立索引。如果初始同步失敗，您必須執行資料的完整同步，即使您沒有選擇完整同步作為同步模式選項。您可以選擇：
 - FORCED_FULL_CRAWL 新建索引所有內容，並在每次資料來源與索引同步時取代現有內容。
 - FULL_CRAWL，以在每次資料來源與索引同步時，僅對新的、修改的和刪除的內容建立索引。Amazon Kendra 可以使用資料來源的機制來追蹤內容變更，並為上次同步後變更的內容建立索引。
 - CHANGE_LOG 每次資料來源與索引同步時，僅對新內容和修改的內容建立索引。Amazon Kendra 可以使用資料來源的機制來追蹤內容變更，並為上次同步後變更的內容建立索引。
- 秘密 Amazon 資源名稱 (ARN) - 提供包含您在 Drupal 帳戶中創建的身份驗證憑據的 Secrets Manager 秘密的 Amazon 資源名稱 (ARN)。

如果您使用基本驗證，密碼會以下列金鑰儲存在 JSON 結構中：

```
{
  "username": "user name",
  "password": "password"
}
```

如果您使用 OAuth 2.0 驗證，則密碼會以下列金鑰儲存在 JSON 結構中：

```
{
  "username": "user name",
  "password": "password",
  "clientId": "client id",
  "clientSecret": "client secret"
}
```

Note

Note

我們建議您定期重新整理或輪換您的認證和密碼。僅為您自己的安全提供必要的訪問級別。我們不建議您跨資料來源以及連接器 1.0 和 2.0 版 (如果適用) 重複使用認證和密碼。

- IAM role — 指定RoleArn何時呼叫CreateDataSource以提供具有存取 Secrets Manager 密碼的權限的 IAM 角色，以及呼叫 Drupal 連接器和 Amazon Kendra所需的公用 API。如需詳細資訊，請參閱 [Drupal 資料來源的IAM 角色](#)。

您還可以添加以下可選功能：

- Virtual Private Cloud (VPC) — 指定您撥打電話的VpcConfiguration時間。CreateDataSource如需詳細資訊，請參閱 [配置 Amazon Kendra 為使用 Amazon VPC](#)。
- 包含和排除篩選器 — 您可以指定是否要包含內容、注釋和附件。您也可以指定規則運算式模式來包含或排除內容、註解和附件。

Note

大多數資料來源使用規則運算式模式，這些模式是稱為篩選器的包含或排除模式。如果您指定包含篩選器，則只會編製與包含項目篩選器相符的內容編製索引。不符合包含篩選器的任何文件都不會建立索引。如果您指定包含和排除篩選器，符合排除篩選器的文件將不會建立索引，即使它們符合包含篩選器也是如此。

- 識別爬行者程式 — 指定是否要開啟身分識別爬行 Amazon Kendra 者程式。識別爬行者程式會使用文件的存取控制清單 (ACL) 資訊，根據使用者或使用者對文件的群組存取權來篩選搜尋結果。如果您有文件的 ACL 並選擇使用 ACL，您也可以選擇開啟的身分識別爬行者程式，以設

定搜尋結果的使用者環境定義篩選。Amazon Kendra 否則，如果關閉身分搜索器，則可以公開搜索所有文檔。如果您想要對文件使用存取控制，且身分識別編目程式已關閉，您也可以使用 [PutPrincipalMapping](#) API 來上傳使用者和群組存取資訊以進行使用者內容篩選。

- 字段映射-選擇您的 Drupal 數據源字段映射到 Amazon Kendra 索引字段。如需詳細資訊，請參閱 [映射資料來源欄位](#)。

Note

您的文件需要文件內文欄位或文件內文對等項目，才能搜尋您的文件。Amazon Kendra 您必須將資料來源中的文件內文欄位名稱對應至索引欄位名稱 `_document_body`。所有其他欄位是選用的。

如需要設定的其他重要 JSON 金鑰清單，請參閱 [Drupal 的模板架構](#)。

備註

- Drupal 的 API 沒有官方的節流限制。
- Java 軟件開發套件不適用於 Drupal。
- Drupal 的數據只能使用本地 JSON API 獲取。
- 不與任何 Drupal 視圖相關聯的內容類型不能被抓取。
- 您需要管理員訪問權限才能從 Drupal 塊抓取數據。
- 沒有可用於使用 HTTP 動詞創建用戶定義的內容類型的 JSON API。
- 「文章」、「基本」頁面、「基本」區塊、使用者定義的內容類型以及使用者定義的區塊類型的文件內文和註解會以 HTML 格式顯示。如果 HTML 內容的格式不正確，則 HTML 相關的標籤將出現在文件內文和註解中，並且會顯示在 Amazon Kendra 搜尋結果中。
- 沒有描述或正文的內容類型和塊類型將不會被攝入 Amazon Kendra。只有這類「內容」或「封鎖」類型的「註解」和「附件」才會擷取到您的 Amazon Kendra 索引中。

GitHub

GitHub 是一種基於 Web 的託管服務，用於軟件開發，提供代碼存儲和管理服務以及版本控制。您可以使用 Amazon Kendra 來為 GitHub 企業雲端 (SaaS) 和 GitHub 企業伺服器 (在 Prem) 儲存庫檔案建立索引、發出和提取要求、發出和提取要求註解，以及發出和提取要求註解附件。您也可以選擇包含或排除特定檔案。

Note

Amazon Kendra 現在支援升級的 GitHub 連接器。

主機已自動為您升級。您在主控台中建立的任何新連接器都會使用升級的架構。如果您使用 API，您現在必須使用 [TemplateConfiguration](#) 物件而非 `GitHubConfiguration` 物件來設定連接器。

使用舊版主控制台和 API 架構設定的連接器將繼續如設定般運作。但是，您將無法編輯或更新它們。如果您要編輯或更新連接器組態，您必須建立新的連接器。

我們建議您將連接器工作流程移轉至升級版本。使用舊架構設定的連接器 Support 排程於 2024 年 6 月結束。

您可以使用 [Amazon Kendra 主控台](#) 和 [TemplateConfiguration](#) API 連線 Amazon Kendra 到 GitHub 資料來源。

如需疑難排解 Amazon Kendra GitHub 資料來源連接器，請參閱 [疑難排解資料來](#)。

主題

- [支援的功能](#)
- [必要條件](#)
- [連接說明](#)
- [進一步了解](#)

支援的功能

Amazon Kendra GitHub 資料來源連接器支援下列功能：

- 欄位對映
- 使用者存取控制
- 包含/排除過濾器
- 完整和增量內容同步
- 虛擬私有雲端 (VPC)

必要條件

在您可以用來 Amazon Kendra 為資 GitHub 料來源建立索引之前，請先在 GitHub 和 AWS 帳戶中進行這些變更。

在中 GitHub，請確定您有：

- 建立具有 GitHub 組 GitHub 織管理權限的使用者。
- 在 Git Hub 中設定個人存取權杖作為您的驗證認證使用。請參[GitHub 閱有關建立個人存取權杖](#)的文件。

Note

我們建議您定期重新整理或輪換您的認證和密碼。僅為您自己的安全提供必要的訪問級別。我們不建議您跨資料來源以及連接器 1.0 和 2.0 版 (如果適用) 重複使用認證和密碼。

- 建議：為驗證憑證設定 OAuth 權杖。使用 OAuth 令牌可獲得更好的 API 節流限制和連接器性能。請參[GitHub 閱有關 OAuth 授權](#)的文件。
- 記下您使用之 GitHub 服務類型的 GitHub 主機 URL。舉例來說，GitHub 雲端的主機網址可以是 <https://api.github.com>，而 GitHub 伺服器的主機網址可以是 <https://api.github.com>，而 GitHub 伺服器的主機網址可以是 <https://api.github.com>。
- 記下您要連線的 GitHub 企業雲端 (SaaS) 帳戶或 GitHub 企業伺服器 (內部部署) 帳戶的組織名稱。GitHub 您可以登入 GitHub 桌面並在您的設定檔圖片下拉式清單中選取您的組織，以找到您的組織名稱。
- 可選 (僅限伺服器)：產生 SSL 憑證，並將路徑複製到儲存在 Amazon S3 值區中的憑證。GitHub 如果您需要安全的 SSL 連線，請使用此連線到。您可以在任何使用 OpenSSL 的電腦上產生自我簽署的 X509 憑證。如需使用 OpenSSL 建立 X509 憑證的範例，請參閱[建立並簽署 X509 憑證](#)。
- 已新增下列權限：

適用於 GitHub 企業雲 (SaaS)

- `repo:status`— 授予讀取/寫入存取權限，以便在公用和私有存放庫中認可 此範圍僅用於授予其他用戶或服務訪問私有存儲庫提交狀態，而不授予對代碼的訪問權限。
- `repo_deployment`— 授予公用和私有存放庫部署狀態的存取權。只有在授與其他使用者或服務存取部署狀態的情況下，才需要此範圍，而不授與程式碼存取權。
- `public_repo`— 限制對公共存儲庫的訪問。這包括對代碼的讀/寫訪問，提交狀態，存儲庫項目，協作者以及公共存儲庫和組織的部署狀態。也需要為公共存儲庫主演。
- `repo:invite`— 授予邀請在存儲庫上協作的接受/拒絕能力。只有在不授與程式碼存取權的情況下授與其他使用者或服務存取邀請時，才需要此範圍。

- `security_events`— 授予：程式碼掃描 API 中安全事件的讀取和寫入存取權。只有在不授與程式碼存取權的情況下授與其他使用者或服務存取安全性事件時，才需要此範圍。
- `read:org`— 組織成員資格、組織專案和小組成員資格的唯讀存取權。
- `user:email`— 授予對使用者電子郵件地址的讀取權限。Amazon Kendra 要求抓取 ACL。
- `user:follow`— 授予關注或取消關注其他用戶的訪問權限。Amazon Kendra 要求抓取 ACL。
- `read:user`— 授予讀取使用者設定檔資料的存取權限。Amazon Kendra 要求抓取 ACL。
- `workflow`— 授予新增和更新 GitHub 動作工作流程檔案的功能。如果相同的檔案 (具有相同的路徑和內容) 存在於相同存放庫中的另一個分支上，則可以在沒有此範圍的情況下提交工作流程檔案。

如需詳細資訊，請參閱GitHub文件中 [OAuth 應用程式的範圍](#)。

適用於 GitHub 企業伺服器 (在內部部署)

- `repo:status`— 授予讀取/寫入存取權限，以便在公用和私有存放庫中認可 此範圍僅用於授予其他用戶或服務訪問私有存儲庫提交狀態，而不授予對代碼的訪問權限。
- `repo_deployment`— 授予公用和私有存放庫部署狀態的存取權。只有在授與其他使用者或服務存取部署狀態的情況下，才需要此範圍，而不授與程式碼存取權。
- `public_repo`— 限制對公共存儲庫的訪問。這包括對代碼的讀/寫訪問權限，提交狀態，存儲庫項目，協作者以及公共存儲庫和組織的部署狀態。也需要為公共存儲庫主演。
- `repo:invite`— 授予邀請在存儲庫上協作的接受/拒絕能力。只有在不授與程式碼存取權的情況下授與其他使用者或服務存取邀請時，才需要此範圍。
- `security_events`— 授予：程式碼掃描 API 中安全事件的讀取和寫入存取權。只有在不授與程式碼存取權的情況下授與其他使用者或服務存取安全性事件時，才需要此範圍。
- `read:user`— 授予讀取使用者設定檔資料的存取權限。Amazon Q 業務需要抓取 ACL。
- `user:email`— 授予對使用者電子郵件地址的讀取權限。Amazon Q 業務需要抓取 ACL。
- `user:follow`— 授予關注或取消關注其他用戶的訪問權限。Amazon Q 業務需要抓取 ACL。
- `site_admin`— 授與網站管理員對 GitHub 企業伺服器管理 API 端點的存取權。
- `workflow`— 授予新增和更新 GitHub 動作工作流程檔案的功能。如果相同的檔案 (具有相同的路徑和內容) 存在於相同存放庫中的另一個分支上，則可以在沒有此範圍的情況下提交工作流程檔案。

如需詳細資訊，請參閱GitHub文件中 [OAuth 應用程式的範圍和了解開發人員中 OAuth 應用程式的GitHub範圍](#)。

- 已勾選的每個文件在您打算用於相同索引的其他資料來源中 GitHub 和其他資料來源之間都是唯一的。您要用於索引的每個資料來源不得包含跨資料來源的相同文件。文件 ID 對索引來說是全域的，而且每個索引必須是唯一的。

在您的 AWS 帳戶中，請確保您有：

- [建立 Amazon Kendra 索引](#)，如果使用 API，則會記下索引 ID。
- 為您的資料來源建立 [IAM 角色](#)，如果使用 API，則會記錄 IAM 角色的 ARN。

Note

如果您變更驗證類型和認證，則必須更新 IAM 角色以存取正確的 AWS Secrets Manager 密碼 ID。

- 將您的 GitHub 身份驗證憑據存儲在 AWS Secrets Manager 密鑰中，如果使用 API，則記錄密鑰的 ARN。

Note

我們建議您定期重新整理或輪換您的認證和密碼。僅為您自己的安全提供必要的訪問級別。我們不建議您跨資料來源以及連接器 1.0 和 2.0 版 (如果適用) 重複使用認證和密碼。

如果您沒有現有的 IAM 角色或密碼，則可以在將 GitHub 資料來源連線到時使用主控台建立新 IAM 角色和 Secrets Manager 密碼 Amazon Kendra。如果您使用 API，則必須提供現有 IAM 角色和 Secrets Manager 密碼的 ARN 以及索引 ID。

連接說明

若要連線 Amazon Kendra 到 GitHub 資料來源，您必須提供資料來源的必要詳細 GitHub 資訊，Amazon Kendra 以便能夠存取您的資料。如果您尚未配置 Amazon Kendra，GitHub 請參閱[必要條件](#)。

Console

若要連線 Amazon Kendra 到 GitHub


1. 登入 AWS Management Console 並開啟[Amazon Kendra 主控台](#)。
2. 在左側導覽窗格中，選擇 [索引]，然後從索引清單中選擇要使用的索引。

Note

您可以選擇在索引設置下配置或編輯用戶訪問控制設置。

3. 在 [開始使用] 頁面上，選擇 [新增資料來源]。
4. 在 [新增資料來源] 頁面上，選擇 [GitHub 連接器]，然後選擇 [新增連接器]。如果使用版本 2 (如果適用)，請選擇帶有「V2.0」標籤的GitHub 連接器。
5. 在 [指定資料來源詳細資訊] 頁面上，輸入下列資訊：
 - a. 在名稱和說明中，對於資料來源名稱 — 輸入資料來源的名稱。您可以包含連字號，但不能包含空格。
 - b. (選擇性) 說明 — 輸入資料來源的選用說明。
 - c. 在預設語言中 — 選擇一種語言來篩選索引的文件。除非另有指定，否則語言預設為英文。文件中繼資料中指定的語言會覆寫選取的語言。
 - d. 在「標籤」中，針對「新增標籤」 — 包含可選標籤以搜尋和篩選資源或追蹤 AWS 成本。
 - e. 選擇下一步。
6. 在 [定義存取權和安全性] 頁面上，輸入下列資訊：
 - a. GitHub來源 — 在GitHub 企業雲和GitHub企業服務器之間進行選擇。
 - b. GitHub 主機網址 — 例如，GitHub 雲端的主機網址可以是 `https://api.github.com`，而 GitHub 伺服器的主機網址可以是 `https://on-prem-host-url/`
 - c. GitHub 組織名稱 — 輸入您的 GitHub組織名稱。您可以在您的 GitHub 帳戶中找到您的組織資訊。
 - d. 授權 — 開啟或關閉文件的存取控制清單 (ACL) 資訊 (如果您有 ACL)，且想要將其用於存取控制。ACL 會指定使用者和群組可存取的文件。ACL 資訊可用來根據使用者或使用者對文件的群組存取來篩選搜尋結果。如需詳細資訊，請參閱[使用者內容篩選](#)。
 - e. AWS Secrets Manager 祕密 — 選擇現有密碼或建立新 Secrets Manager 密碼來儲存您的 GitHub 驗證認證。如果您選擇建立新密碼，則會開啟一個 AWS Secrets Manager 密碼視窗。
 - i. 在「建立 AWS Secrets Manager 密碼視窗」中輸入下列資訊：
 - A. 祕密名稱 — 您祕密的名稱。前綴 'AmazonKendraGitHub-' 會自動添加到您的密碼名稱中。

- B. 對於 GitHubToken — 輸入中 GitHub 配置的驗證認證值。
 - ii. 保存並添加您的秘密。
- f. V@@ irtual Private Cloud (VPC) (VPC) — 您可以選擇使用 VPC。如果是這樣，您必須新增子網路和 VPC 安全性群組。
- g. 識別爬行者程式 — 指定是否要開啟身分識別爬行 Amazon Kendra 者程式。識別爬行者程式會使用文件的存取控制清單 (ACL) 資訊，根據使用者或使用者對文件的群組存取權來篩選搜尋結果。如果您有文件的 ACL 並選擇使用 ACL，您也可以選擇開啟的身分識別爬行者程式，以設定搜尋結果的使用者環境定義篩選。Amazon Kendra 否則，如果關閉身分搜索器，則可以公開搜索所有文檔。如果您想要對文件使用存取控制，且身分識別編目程式已關閉，您也可以使用 [PutPrincipalMapping](#) API 來上傳使用者和群組存取資訊以進行使用者內容篩選。
- h. IAM role — 選擇現有 IAM 角色或建立新 IAM 角色以存取存放庫認證和索引內容。

 Note

IAM 用於索引的角色不能用於資料來源。如果您不確定索引或常見問題集是否使用現有角色，請選擇 [建立新角色] 以避免發生錯誤。

- i. 選擇下一步。
7. 在 [設定同步設定] 頁面上，輸入下列資訊：
- a. 選取存放庫 — 選擇編目所有存放庫或選取。

如果您選擇編目選取的存放庫，請新增存放庫的名稱，並選擇性地新增任何特定分支的名稱。
 - b. 內容類型 — 選擇您要從檔案、問題、提取請求等編目的內容類型。
 - c. 正則表達式模式-添加正則表達式模式以包含或排除某些文件。
 - d. 同步模式 — 選擇資料來源內容變更時要如何更新索引。當您第一次將資料來源同 Amazon Kendra 步處理時，依預設會檢索所有內容並建立索引。如果初始同步失敗，您必須執行資料的完整同步，即使您沒有選擇完整同步作為同步模式選項。
 - 完全同步：新鮮索引所有內容，並在每次資料來源與索引同步時取代現有內容。
 - 新增、修改的同步：每次資料來源與索引同步時，僅對新內容和已修改的內容建立索引。Amazon Kendra 可以使用資料來源的機制來追蹤內容變更，並為上次同步後變更的內容建立索引。

- 新增、修改、刪除的同步：每次資料來源與索引同步時，僅對新內容、已修改和刪除的內容建立索引。Amazon Kendra 可以使用資料來源的機制來追蹤內容變更，並為上次同步後變更的內容建立索引。
 - e. 頻率的同步執行排程 — 選擇同步資料來源內容和更新索引的頻率。
 - f. 選擇下一步。
8. 在 [設定欄位對映] 頁面上，輸入下列資訊：
- a. 預設資料來源欄位 — 從要對映至索引的 Amazon Kendra 產生預設資料來源欄位中選取。
 - b. 新增欄位 — 新增自訂資料來源欄位以建立要對映的索引欄位名稱和欄位資料類型。
 - c. 選擇下一步。
9. 在 [檢閱並建立] 頁面上，檢查您輸入的資訊是否正確，然後選取 [新增資料來源]。您也可以從此頁面選擇編輯您的資訊。成功新增資料來源後，您的資料來源將顯示在 [資料來源] 頁面上。

API

若要連線 Amazon Kendra 到 GitHub

您必須使用 [TemplateConfiguration](#) API 指定 [資料來源結構描述](#) 的 JSON。您必須提供以下信息：

- 資料來源 — 指定使用 [TemplateConfiguration](#) JSON 結構定義 GITHUB 時的資料來源類型。同時指定呼叫 [CreateDataSource](#) API TEMPLATE 時的資料來源。
- GitHub 類型 — 將類型指定為 SAAS 或 ON_PREMISE。
- 主機 URL — 指定 GitHub 主機 URL 或 API 端點網址。例如，如果您使用 GitHub SAAS/ 企業雲，則主機 URL 可能是，對於 GitHub 內部部署/企業服務器 <https://api.github.com>，則主機 URL 可能是。 <https://on-prem-host-url/api/v3/>
- 組織名稱 — 指定 GitHub 帳戶組織的名稱。您可以登入 GitHub 桌面並在您的設定檔圖片下拉式清單中選取您的組織，以找到您的組織名稱。
- 同步模式 — 指定資料來源內容變更時 Amazon Kendra 應如何更新索引。當您第一次將資料來源同 Amazon Kendra 步處理時，依預設會檢索所有內容並建立索引。如果初始同步失敗，您必須執行資料的完整同步，即使您沒有選擇完整同步作為同步模式選項。您可以選擇：
 - FORCED_FULL_CRAWL 新建索引所有內容，並在每次資料來源與索引同步時取代現有內容。
 - FULL_CRAWL，以在每次資料來源與索引同步時，僅對新的、修改的和刪除的內容建立索引。Amazon Kendra 可以使用資料來源的機制來追蹤內容變更，並為上次同步後變更的內容建立索引。

- `CHANGE_LOG`每次資料來源與索引同步時，僅對新內容和修改的內容建立索引。Amazon Kendra 可以使用資料來源的機制來追蹤內容變更，並為上次同步後變更的內容建立索引。
- 識別爬行者程式 — 指定是否要開啟身分識別爬行者 Amazon Kendra 程式。識別爬行者程式會使用文件的存取控制清單 (ACL) 資訊，根據使用者或使用者對文件的群組存取權來篩選搜尋結果。如果您有文件的 ACL 並選擇使用 ACL，您也可以選擇開啟的身分識別爬行者程式，以設定搜尋結果的使用者環境定義篩選。Amazon Kendra 否則，如果關閉身分搜索器，則可以公開搜索所有文檔。如果您想要對文件使用存取控制，且身分識別編目程式已關閉，您也可以使用 [PutPrincipalMapping](#) API 來上傳使用者和群組存取資訊以進行使用者內容篩選。
- 秘密 Amazon 資源名稱 (ARN) — 提供包含您帳戶身份驗證登入資料的 Secrets Manager 密碼的 Amazon 資源名稱 (ARN)。GitHub 密碼會以下列金鑰儲存在 JSON 結構中：

```
{
  "personalToken": "token"
}
```

- IAM role — 指定 `RoleArn` 何時呼叫 `CreateDataSource` 以提供具有存取 Secrets Manager 密碼之權限的 IAM 角色，以及呼叫 GitHub 連接器和 Amazon Kendra 所需公用 API 的時間。有關詳情，請參閱 [GitHub 料來源的 IAM 角色](#)。

您還可以添加以下可選功能：

- Virtual Private Cloud (VPC) — 指定您撥打電話的 `VpcConfiguration` 時間。`CreateDataSource` 如需詳細資訊，請參閱 [配置 Amazon Kendra 為使用 Amazon VPC](#)。

Note

如果您使用 GitHub 伺服器，則必須使用連線 Amazon VPC 到 GitHub 伺服器。

- 存放庫篩選器 — 依名稱和分支名稱篩選儲存庫。
- 文件/內容類型 — 指定是否要編目儲存庫文件、問題、發佈註解、發出註解附件、提取請求、提取請求註解、提取請求註解附件。
- 包含和排除篩選器 — 指定要包含還是排除某些檔案和資料夾。

Note

大多數資料來源使用規則運算式模式，這些模式是稱為篩選器的包含或排除模式。如果您指定包含篩選器，則只有符合包含項目篩選器的內容會編製索引。不符合包含篩選器的任

何文件都不會建立索引。如果您指定包含和排除篩選器，符合排除篩選器的文件將不會建立索引，即使它們符合包含篩選器也是如此。

- 存取控制清單 (ACL) — 指定是否要編目文件的 ACL 資訊 (如果您有 ACL 並且想要將其用於存取控制)。ACL 會指定使用者和群組可存取的文件。ACL 資訊可用來根據使用者或使用者對文件的群組存取來篩選搜尋結果。如需詳細資訊，請參閱[使用者內容篩選](#)。
- 欄位對映 — 選擇將資料來源欄位對映至 Amazon Kendra 索引欄位。您可以包含文件、確認、問題、發放附件、提取請求、提取請求附件、提取請求附件等欄位。如需詳細資訊，請參閱[映射資料來源欄位](#)。

Note

Amazon Kendra 需要文件的文件內文欄位或文件內文對等項目，Amazon Kendra 才能搜尋您的文件。您必須將資料來源中的文件內文欄位名稱對應至索引欄位名稱 `_document_body`。所有其他欄位是選用的。

如需要設定的其他重要 JSON 金鑰清單，請參閱[GitHub 範本結構定義](#)。

進一步了解

若要進一步瞭解 Amazon Kendra 與 GitHub 資料來源整合的相關資訊，請參閱：

- [利用連接器的強大功能，重新想像 GitHub 儲存庫的 Amazon Kendra GitHub 搜尋](#)

Gmail

Gmail 是由 Google 開發的電子郵件客戶端，您可以通過它發送帶有文件附件的電子郵件。Gmail 郵件可以使用文件夾和標籤對您的電子郵件收件箱進行排序和存儲。您可以用 Amazon Kendra 來編製電子郵件訊息和郵件附件的索引。您也可以設定 Amazon Kendra 為包含或排除特定的電子郵件訊息、郵件附件和索引標籤。

您可以使用[Amazon Kendra 主控台](#)和 [TemplateConfiguration](#) API 連線 Amazon Kendra 至 Gmail 資料來源。

如需對 Amazon Kendra Gmail 資料來源連接器的疑難排解，請參閱[疑難排解資料來](#)。

主題

- [支援的功能](#)
- [必要條件](#)
- [連接說明](#)
- [進一步了解](#)
- [備註](#)

支援的功能

- 欄位對映
- 使用者存取控制
- 包含/排除過濾器
- 完整和增量內容同步
- 虛擬私有雲端 (VPC)

必要條件

您可以在 Gmail 資料來源建立索引之前，請先在 Gmail 和 AWS 帳戶中進行這些變更。Amazon Kendra

在 Gmail 中，請確定您擁有以下功能：

- 創建了一個谷歌雲平台管理員帳戶，並創建了一個谷歌雲項目。
- 在您的管理員帳戶中激活了 Gmail API 和管理員 SDK API。
- 創建了一個服務帳戶並為您的 Gmail 下載了一個 JSON 私鑰。如需如何建立和存取私密金鑰的詳細資訊，請參閱 Google Cloud 說明文件，瞭解如何[建立服務帳戶金鑰](#)和[服務帳戶憑證](#)。
- 複製您的管理員帳戶電子郵件，您的服務帳戶電子郵件和私鑰以用作身份驗證憑據。

Note

我們建議您定期重新整理或輪換您的認證和密碼。僅為您自己的安全提供必要的訪問級別。我們不建議您跨資料來源以及連接器 1.0 和 2.0 版 (如果適用) 重複使用認證和密碼。

- 為您的使用者和要建立索引的共用目錄新增下列 OAuth 範圍 (使用管理員角色)：
 - <https://www.googleapis.com/auth/admin.directory.user.readonly>

- <https://www.googleapis.com/auth/gmail.readonly>
- 檢查每個文檔在 Gmail 和您打算用於同一索引的其他數據源中是唯一的。您要用於索引的每個資料來源不得包含跨資料來源的相同文件。文件 ID 對索引來說是全域的，而且每個索引必須是唯一的。

在您的中 AWS 帳戶，請確保您具有：

- [建立 Amazon Kendra 索引](#)，如果使用 API，則會記下索引識別碼。
- 為您的[資料來源建立 IAM 角色](#)，如果使用 API，則會記錄 IAM 角色的 ARN。

Note

如果您變更驗證類型和認證，則必須更新 IAM 角色才能存取正確的 AWS Secrets Manager 密碼 ID。

- 將您的 Gmail 身份驗證憑據存儲在一個 AWS Secrets Manager 秘密中，如果使用 API，則註明秘密的 ARN。

Note

我們建議您定期重新整理或輪換您的認證和密碼。僅為您自己的安全提供必要的訪問級別。我們不建議您跨資料來源以及連接器 1.0 和 2.0 版 (如果適用) 重複使用認證和密碼。

如果您沒有現有的 IAM 角色或密碼，則可以在將 Gmail 資料來源連線至時使用主控台建立新 IAM 角色和 Secrets Manager 密碼 Amazon Kendra。如果您使用 API，則必須提供現有 IAM 角色和 Secrets Manager 密碼的 ARN 以及索引 ID。


連接說明

要連接 Amazon Kendra 到 Gmail 數據源，您必須提供 Gmail 憑據的詳細信息，Amazon Kendra 以便可以訪問您的數據。如果您尚未為 Gmail 設定 Amazon Kendra，請參閱[必要條件](#)。

Console

若要連線 Amazon Kendra 至 Gmail


1. 登入 AWS Management Console 並開啟[Amazon Kendra 主控台](#)。
2. 在左側導覽窗格中，選擇 [索引]，然後從索引清單中選擇要使用的索引。

 Note

您可以選擇在索引設置下配置或編輯您的用戶訪問控制設置。


3. 在 [開始使用] 頁面上，選擇 [新增資料來源]。
4. 在 [新增資料來源] 頁面上，選擇 [Gmail 連接器]，然後選擇 [新增連接器]。如果使用第 2 版（如果適用），請選擇帶有「V2.0」標籤的 Gmail 連接器。
5. 在 [指定資料來源詳細資訊] 頁面上，輸入下列資訊：
 - a. 在名稱和說明中，對於資料來源名稱 — 輸入資料來源的名稱。您可以包含連字號，但不能包含空格。
 - b. (選擇性) 說明 — 輸入資料來源的選用說明。
 - c. 在預設語言中 — 選擇一種語言來篩選索引的文件。除非另有指定，否則語言預設為英文。文件中繼資料中指定的語言會覆寫選取的語言。
 - d. 在「標籤」中，針對「新增標籤」 — 包含可選標籤以搜尋和篩選資源或追蹤 AWS 成本。
 - e. 選擇下一步。
6. 在 [定義存取權和安全性] 頁面上，輸入下列資訊：
 - a. 授權 — 開啟或關閉文件的存取控制清單 (ACL) 資訊 (如果您有 ACL)，且想要將其用於存取控制。ACL 會指定使用者和群組可存取的文件。ACL 資訊可用來根據使用者或使用者對文件的群組存取來篩選搜尋結果。如需詳細資訊，請參閱[使用者內容篩選](#)。
 - b. 在 AWS Secrets Manager 密碼驗證中 — 選擇現有密碼或建立新 Secrets Manager 密碼來儲存您的 Gmail 驗證憑證。如果您選擇建立新密碼，則會開啟一個 AWS Secrets Manager 密碼視窗。
 - 在「建立 AWS Secrets Manager 密碼視窗」中輸入下列資訊：
 - A. 秘密名稱 — 您秘密的名稱。
 - B. 用戶端電子郵件：您從 Google 服務帳戶複製的用戶端電子郵件。
 - C. 管理員帳戶電子郵件 — 您要使用的管理員帳戶電子郵件。
 - D. 私密金鑰 — 您從 Google 服務帳戶複製的私密金鑰。
 - E. 保存並添加您的秘密。
 - c. Virtual Private Cloud (VPC) (VPC) — 您可以選擇使用 VPC。如果是這樣，您必須新增子網路和 VPC 安全性群組。

- d. IAM role — 選擇現有 IAM 角色或建立新 IAM 角色以存取存放庫認證和索引內容。

 Note


IAM 用於索引的角色不能用於資料來源。如果您不確定索引或常見問題集是否使用現有角色，請選擇 [建立新角色] 以避免發生錯誤。

- e. 選擇下一步。
7. 在 [設定同步設定] 頁面上，輸入下列資訊：
 - a. 對於實體類型 — 選擇同步郵件附件。
 - b. (選擇性) 對於其他組態，請輸入下列資訊：
 - i. 日期範圍 — 輸入日期範圍，以指定您要編目的電子郵件的開始和結束日期。
 - ii. 電子郵件網域：包含或排除以「收件者」、「寄件者」、「副本」和「密件副本」電子郵件網域為基礎的某些電子郵件。
 - iii. 主旨中的關鍵字：根據電子郵件主題中的關鍵字加入或排除電子郵件。

 Note

您也可以選擇包含符合您輸入之所有主題關鍵字的任何文件。

- iv. 標籤 — 新增規則運算式模式以包含或排除某些電子郵件標籤。
 - v. 附件 — 新增規則運算式模式以包含或排除特定電子郵件附件。
- c. 同步模式 — 選擇資料來源內容變更時要如何更新索引。當您第一次將資料來源同 Amazon Kendra 步處理時，依預設會檢索所有內容並建立索引。如果初始同步失敗，您必須執行資料的完整同步，即使您沒有選擇完整同步作為同步模式選項。
 - 完全同步：新鮮索引所有內容，並在每次資料來源與索引同步時取代現有內容。
 - 新增、修改、刪除的同步：每次資料來源與索引同步時，僅對新內容、已修改和刪除的內容建立索引。Amazon Kendra 可以使用資料來源的機制來追蹤內容變更，並為上次同步後變更的內容建立索引。


 Important

由於沒有 API 可以更新永久刪除的 Gmail 郵件，因此新的，修改或刪除的內容同步：

- 不會從 Amazon Kendra 索引中移除已從 Gmail 永久刪除的郵件
- 不會同步 Gmail 電子郵件標籤中的變更

若要將 Gmail 資料來源標籤變更和永久刪除的電子郵件訊息同步至 Amazon Kendra 索引，您必須定期執行完整檢索。

- d. 在同步執行排程中，對於頻率 — 選擇同步資料來源內容和更新索引的頻率。
 - e. 選擇下一步。
8. 在 [設定欄位對映] 頁面上，輸入下列資訊：
 - a. 預設資料來源欄位 — 從 Amazon Kendra 產生的預設資料來源欄位中選取您要對映至索引的資料來源欄位。

 Note

Amazon Kendra 由於 API 限制，Gmail 資料來源連接器不支援建立自訂索引欄位。

- b. 選擇下一步。
9. 在 [檢閱並建立] 頁面上，檢查您輸入的資訊是否正確，然後選取 [新增資料來源]。您也可以從此頁面選擇編輯您的資訊。成功新增資料來源後，您的資料來源將顯示在 [資料來源] 頁面上。

API

若要連線 Amazon Kendra 至 Gmail

您必須使用 [TemplateConfiguration](#) API 指定 [資料來源結構描述](#) 的 JSON。您必須提供以下信息：

- 資料來源 — 指定使用 [TemplateConfiguration](#) JSON 結構定義 GMAIL 時的資料來源類型。同時將資料來源指定為呼叫 [CreateDataSource](#) API TEMPLATE 時的方式。
- 同步模式 — 指定資料來源內容變更時 Amazon Kendra 應如何更新索引。當您第一次將資料來源同 Amazon Kendra 步處理時，依預設會檢索所有內容並建立索引。如果初始同步失敗，您必須執行資料的完整同步，即使您沒有選擇完整同步作為同步模式選項。您可以選擇：
 - FORCED_FULL_CRAWL 新建索引所有內容，並在每次資料來源與索引同步時取代現有內容。

- FULL_CRAWL，以在每次資料來源與索引同步時，僅對新的、修改的和刪除的內容建立索引。Amazon Kendra 可以使用資料來源的機制來追蹤內容變更，並為上次同步後變更的內容建立索引。

Important

由於沒有 API 可以更新永久刪除的 Gmail 郵件，因此新的，修改或刪除的內容同步：

- 不會從 Amazon Kendra 索引中移除已從 Gmail 永久刪除的郵件
- 不會同步 Gmail 電子郵件標籤中的變更

若要將 Gmail 資料來源標籤變更和永久刪除的電子郵件訊息同步至 Amazon Kendra 索引，您必須定期執行完整檢索。

- 秘密 Amazon 資源名稱 (ARN) — 提供包含 Gmail 帳戶身份驗證憑據的 Secrets Manager 秘密的 Amazon 資源名稱 (ARN)。密碼會以下列金鑰儲存在 JSON 結構中：

```
{
  "adminAccountEmailId": "service account email",
  "clientEmailId": "user account email",
  "privateKey": "private key"
}
```

- IAM role — 指定您撥打電話的RoleArn時間，CreateDataSource以提供具有存取 Secrets Manager 密碼權限的 IAM 角色，以及呼叫 Gmail 連接器和 Amazon Kendra所需的公用 API 的時間。如需詳細資訊，請參閱 [Gmail 資料來源的IAM 角色](#)。

您還可以添加以下可選功能：

- Virtual Private Cloud (VPC) — 指定您撥打電話的VpcConfiguration時間。CreateDataSource如需詳細資訊，請參閱 [配置 Amazon Kendra 為使用 Amazon VPC](#)。
- 包含和排除篩選器 — 指定是否要包含或排除某些「收件人」、「寄件者」、「副本」、「密件副本」電子郵件。

Note

大多數資料來源使用規則運算式模式，這些模式是稱為篩選器的包含或排除模式。如果您指定包含篩選器，則只有符合包含項目篩選器的內容會編製索引。不符合包含篩選器的任

何文件都不會建立索引。如果您指定包含和排除篩選器，符合排除篩選器的文件將不會建立索引，即使它們符合包含篩選器也是如此。

- 使用者前後關聯篩選與存取控制 — Amazon Kendra 探索文件的存取控制清單 (ACL) (如果您有文件的 ACL)。ACL 資訊可用來根據使用者或使用者對文件的群組存取來篩選搜尋結果。如需詳細資訊，請參閱[使用者內容篩選](#)。
- 欄位對應 — 選擇將 Gmail 資料來源欄位對應至 Amazon Kendra 索引欄位。如需詳細資訊，請參閱[映射資料來源欄位](#)。

Note

您的文件需要文件內文欄位或文件內文對等項目，才能搜尋您的文件。Amazon Kendra 您必須將資料來源中的文件內文欄位名稱對應至索引欄位名稱_document_body。所有其他欄位是選用的。

Note

Amazon Kendra 由於 API 限制，Gmail 資料來源連接器不支援建立自訂索引欄位。

如需要設定的其他重要 JSON 金鑰清單，請參閱[Gmail 範本結構定義](#)。

進一步了解

若要進一步瞭解如何整 Amazon Kendra 合 Gmail 資料來源，請參閱：

- [使用 Gmail 連接器在 Google 工作區中對電子郵件執行智能搜索 Amazon Kendra](#)。

備註

- 由於沒有 API 可以更新永久刪除的 Gmail 郵件，因此可以進行FULL_CRAWL/新增、修改或刪除的內容同步：
 - 不會從 Amazon Kendra 索引中移除已從 Gmail 永久刪除的郵件
 - 不會同步 Gmail 電子郵件標籤中的變更

若要將 Gmail 資料來源標籤變更和永久刪除的電子郵件訊息同步至 Amazon Kendra 索引，您必須定期執行完整檢索。

- Amazon Kendra 由於 API 限制，Gmail 資料來源連接器不支援建立自訂索引欄位。

Google 雲端硬碟

Google 雲端硬碟是一種基於雲的文件存儲服務。您可以使用在 Google 雲端硬碟資料 Amazon Kendra 來源的共用雲端硬碟、「我的雲端硬碟」和「與我共享」資料夾中儲存的文件編製索引。您可以為 Google Workspace 文件和文件[類型中列出的文件](#)編製索引。您也可以使用包含和排除篩選器，依檔案名稱、檔案類型和檔案路徑為內容建立索引。

您可以使用[Amazon Kendra 主控台](#)、API 或 [TemplateConfiguration](#) API 連線 Amazon Kendra 到 Google 雲端硬碟資料來源。[GoogleDriveConfiguration](#)

Amazon Kendra 有兩個版本的谷歌驅動器連接器。每個版本的支援功能包括：

谷歌驅動器連接器 V1.0 /API [GoogleDriveConfiguration](#)

- 欄位對映
- 使用者存取控制
- 包含/排除過濾器

谷歌驅動器連接器 V2.0/[TemplateConfiguration](#) API

- 欄位對映
- 使用者存取控制
- 包含/排除過濾器
- 完整和增量內容同步
- 虛擬私有雲端 (VPC)

Note

Support 谷歌驅動器連接器 V1.0 /谷歌 DriveConfiguration API 計劃在 2023 年結束。我們建議遷移到或使用谷歌驅動器連接器 V2.0/ TemplateConfiguration API。

如需 Amazon Kendra Google 雲端硬碟資料來源連接器的疑難排解，請參閱 [疑難排解資料來](#)

主題

- [谷歌驅動器連接器 V1.0](#)
- [谷歌驅動器連接器 V2.0](#)

谷歌驅動器連接器 V1.0

Google 雲端硬碟是一種基於雲的文件存儲服務。您可以使用在 Google 雲端硬碟資料 Amazon Kendra 來源的共用雲端硬碟、「我的雲端硬碟」和「與我共享」資料夾中儲存的文件和註解建立索引。您可以編製 Google 工作區文件的索引，以及文件[類型中列出的文件](#)。您也可以使用包含和排除篩選器，依檔案名稱、檔案類型和檔案路徑為內容建立索引。

Note

Support 谷歌驅動器連接器 V1.0 /谷歌 DriveConfiguration API 計劃在 2023 年結束。我們建議遷移到或使用谷歌驅動器連接器 V2.0/ TemplateConfiguration API。

如需 Amazon Kendra Google 雲端硬碟資料來源連接器的疑難排解，請參閱 [疑難排解資料來](#)

主題

- [支援的功能](#)
- [必要條件](#)
- [連接說明](#)
- [進一步了解](#)

支援的功能

- 欄位對映
- 使用者存取控制
- 包含/排除過濾器

必要條件

在您可以使用 Amazon Kendra 來為 Google 雲端硬碟資料來源建立索引之前，請先在 Google 雲端硬碟和 AWS 帳戶中進行這些變更。

在 Google 雲端硬碟中，請確保您具有：

- 已被超級管理員角色授與存取權，或者是具有管理權限的使用者。如果您已被超級管理員角色授與存取權，則不需要自己的超級管理員角色。
- 建立服務帳戶時，啟用 G Suite 全網域委派，並使用該帳戶將 JSON 金鑰做為私密金鑰。
- 複製您的使用者帳戶電子郵件和服務帳戶電子郵件。當您連接到您輸入 Amazon Kendra 您的用戶帳戶電子郵件作為管理員帳戶電子郵件和您的服務帳戶電子郵件作為您的 AWS Secrets Manager 秘密客戶電子郵件。

Note

我們建議您定期重新整理或輪換您的認證和密碼。僅為您自己的安全提供必要的訪問級別。我們不建議您跨資料來源以及連接器 1.0 和 2.0 版 (如果適用) 重複使用認證和密碼。

- 在您的帳戶中添加了管理員 SDK API 和谷歌驅動器 API。
- 使用超級管理員角色將下列權限新增至您的服務帳戶 (或要求具有超級管理員角色的使用者新增)：
 - <https://www.googleapis.com/auth/drive.readonly>
 - <https://www.googleapis.com/auth/drive.metadata.readonly>
 - <https://www.googleapis.com/auth/admin.directory.user.readonly>
 - <https://www.googleapis.com/auth/admin.directory.group.readonly>
- 已核取每個文件在 Google 雲端硬碟和您打算用於相同索引的其他資料來源中都是唯一的。您要用於索引的每個資料來源不得包含跨資料來源的相同文件。文件 ID 對索引來說是全域的，而且每個索引必須是唯一的。

在您的 AWS 帳戶中，請確保您有：

- [建立 Amazon Kendra 索引](#)，如果使用 API，則會記下索引識別碼。
- 為您的 [資料來源建立 IAM 角色](#)，如果使用 API，則會記錄 IAM 角色的 ARN。

Note

如果您變更驗證類型和認證，則必須更新 IAM 角色才能存取正確的 AWS Secrets Manager 密碼 ID。

- 將您的 Google 雲端硬碟身份驗證憑據存儲在 AWS Secrets Manager 秘密中，並且如果使用 API，則註明秘密的 ARN。

Note

我們建議您定期重新整理或輪換您的認證和密碼。僅為您自己的安全提供必要的訪問級別。我們不建議您跨資料來源以及連接器 1.0 和 2.0 版 (如果適用) 重複使用認證和密碼。

如果您沒有現有的 IAM 角色或機密，可以在將 Google 雲端硬碟資料來源連線至時，使用主控台建立新 IAM 角色和 Secrets Manager 密碼 Amazon Kendra。如果您使用 API，則必須提供現有 IAM 角色和 Secrets Manager 密碼的 ARN 以及索引 ID。

連接說明

若要連線 Amazon Kendra 至 Google 雲端硬碟資料來源，您必須提供 Google 雲端硬碟資料來源的必要詳細資料，才 Amazon Kendra 能存取您的資料。如果您尚未配置 Google 雲端硬碟以供 Amazon Kendra 查看 [必要條件](#)。

Console


連接 Amazon Kendra 到谷歌雲端硬碟

- 登入 AWS 管理主控台並開啟主 [Amazon Kendra 控制台](#)。
- 在左側導覽窗格中，選擇 [索引]，然後從索引清單中選擇要使用的索引。

Note

您可以選擇在索引設置下配置或編輯您的用戶訪問控制設置。

- 在 [開始使用] 頁面上，選擇 [新增資料來源]。
- 在 [新增資料來源] 頁面上，選擇 [Google 雲端硬碟連接器 V1.0]，然後選擇 [新增連接器]。
- 在 [指定資料來源詳細資訊] 頁面上，輸入下列資訊：

- a. 在名稱和說明中，對於資料來源名稱 — 輸入資料來源的名稱。您可以包含連字號，但不能包含空格。
 - b. (選擇性) 說明 — 輸入資料來源的選用說明。
 - c. 在預設語言中 — 選擇一種語言來篩選索引的文件。除非另有指定，否則語言預設為英文。文件中繼資料中指定的語言會覆寫選取的語言。
 - d. 在「標籤」中，針對「新增標籤」 — 包含可選標籤以搜尋和篩選資源或追蹤 AWS 成本。
 - e. 選擇下一步。
6. 在 [定義存取權和安全性] 頁面上，輸入下列資訊：
- a. 對於驗證類型 — 在現有和新增之間選擇。如果您選擇使用現有的密碼，請使用「選取密碼」來選擇您的密碼。
 - b. 如果您選擇建立新密碼，則會開啟一個 AWS Secrets Manager 密碼選項。
 - 在「建立 AWS Secrets Manager 密碼視窗」中輸入下列資訊：
 - A. 秘密名稱 — 您秘密的名稱。前綴 'AmazonKendra-Google 驅動器' 會自動添加到您的密碼名稱中。
 - B. 如果是管理員帳戶電子郵件、用戶端電子郵件和私密金鑰，請輸入您從 Google 雲端硬碟帳戶產生並下載的驗證憑證值。
 - C. 選擇 [儲存驗證]。
 - c. IAM role — 選擇現有 IAM 角色或建立新 IAM 角色以存取存放庫認證和索引內容。
-  Note

IAM 用於索引的角色不能用於資料來源。如果您不確定索引或常見問題集是否使用現有角色，請選擇 [建立新角色] 以避免發生錯誤。
- d. 選擇下一步。
7. 在 [設定同步設定] 頁面上，輸入下列資訊：
- a. 排除使用者帳戶 — 您要從索引中排除的 Google 雲端硬碟使用者。您最多可以新增 100 個使用者帳戶。
 - b. 排除共用雲端硬碟：您要從索引中排除的 Google 雲端硬碟共用雲端硬碟。您最多可以新增 100 個共用磁碟機。

- c. 排除檔案類型磁碟機 — 您要從索引中排除的 Google 雲端硬碟檔案類型。您也可以選擇編輯 MIME 類型選取項目。
 - d. 其他組態 — 包含或排除某些內容的規則運算式模式。您最多可以添加 100 個圖案。
 - e. 頻率：與資料來源同步的頻率。Amazon Kendra
 - f. 選擇下一步。
8. 在 [設定欄位對映] 頁面上，輸入下列資訊：
- a. 對於GoogleDrive 欄位名稱和其他建議欄位對映 — 從 Amazon Kendra 產生的預設資料來源欄位中選取您要對映至索引的預設資料來源欄位。
 - b. 新增欄位 — 新增自訂資料來源欄位，以建立要對映的索引欄位名稱和欄位資料類型。
 - c. 選擇下一步。
9. 在 [檢閱並建立] 頁面上，檢查您輸入的資訊是否正確，然後選取 [新增資料來源]。您也可以從此頁面選擇編輯您的資訊。成功新增資料來源後，您的資料來源將顯示在 [資料來源] 頁面上。

API

連接 Amazon Kendra 到谷歌雲端硬碟

您必須使用 [GoogleDriveConfiguration](#) API 指定下列項目：

- 秘密 Amazon 資源名稱 (ARN) — 提供包含您 Google 雲端硬碟帳戶身份驗證憑據的 Secrets Manager 秘密的 Amazon 資源名稱 (ARN)。密碼會以下列金鑰儲存在 JSON 結構中：

```
{
  "clientAccount": "service account email",
  "adminAccount": "user account email",
  "privateKey": "private key"
}
```

- IAM role — 指定您撥打電話的RoleArn時間，CreateDataSource以提供具有存取 Secrets Manager 密碼權限的 IAM 角色，以及呼叫 Google 雲端硬碟連接器和 Amazon Kendra所需的公用 API。如需詳細資訊，請參閱 [Google 雲端硬碟資料來源的IAM 角色](#)。

您還可以添加以下可選功能：

- 包含和排除篩選器 — 依預設，為 Google 雲端硬碟中的所有文件 Amazon Kendra 建立索引 您可以指定是否要包含或排除共用雲端硬碟、使用者帳戶、文件 MIME 類型和檔案中的某些內容。如

果您選擇排除使用者帳戶，則帳戶所擁有的「我的雲端硬碟」中的任何檔案都不會建立索引。與使用者共用的檔案會建立索引，除非檔案擁有者也被排除在外。

Note

大多數資料來源使用規則運算式模式，這些模式是稱為篩選器的包含或排除模式。如果您指定包含篩選器，則只有符合包含項目篩選器的內容會編製索引。不符合包含篩選器的任何文件都不會建立索引。如果您指定包含和排除篩選器，符合排除篩選器的文件將不會建立索引，即使它們符合包含篩選器也是如此。

- 欄位對應 — 選擇將 Google 雲端硬碟資料來源欄位對應至 Amazon Kendra 索引欄位。如需詳細資訊，請參閱[映射資料來源欄位](#)。

Note

您的文件需要文件內文欄位或文件內文對等項目，才能搜尋您的文件。Amazon Kendra 您必須將資料來源中的文件內文欄位名稱對應至索引欄位名稱_document_body。所有其他欄位是選用的。

- 使用者前後關聯篩選與存取控制 — Amazon Kendra 探索文件的存取控制清單 (ACL) (如果您有文件的 ACL)。ACL 資訊可用來根據使用者或使用者對文件的群組存取來篩選搜尋結果。如需詳細資訊，請參閱[使用者內容篩選](#)。

進一步了解

若要進一步瞭解如何整 Amazon Kendra 合 Google 雲端硬碟資料來源，請參閱：

- [開始使用 Amazon Kendra Google 雲端硬碟連接器](#)

谷歌驅動器連接器 V2.0

Google 雲端硬碟是一種基於雲的文件存儲服務。您可以使用在 Google 雲端硬碟資料 Amazon Kendra 來源的共用雲端硬碟、「我的雲端硬碟」和「與我共享」資料夾中儲存的文件和註解建立索引。您可以編製 Google 工作區文件的索引，以及文件[類型中列出的文件](#)。您也可以使用包含和排除篩選器，依檔案名稱、檔案類型和檔案路徑為內容建立索引。

Note

Support 谷歌驅動器連接器 V1.0 /谷歌 DriveConfiguration API 計劃在 2023 年結束。我們建議遷移到或使用谷歌驅動器連接器 V2.0/ TemplateConfiguration API。

如需 Amazon Kendra Google 雲端硬碟資料來源連接器的疑難排解，請參閱 [疑難排解資料來](#)

主題

- [支援的功能](#)
- [必要條件](#)
- [連接說明](#)
- [備註](#)

支援的功能

- 欄位對映
- 使用者存取控制
- 包含/排除過濾器
- 完整和增量內容同步
- 虛擬私有雲端 (VPC)

必要條件

在您可以使用 Amazon Kendra 來為 Google 雲端硬碟資料來源建立索引之前，請先在 Google 雲端硬碟和 AWS 帳戶中進行這些變更。

在 Google 雲端硬盤中，請確保您具有：

- 已被超級管理員角色授與存取權，或者是具有管理權限的使用者。如果您已被超級管理員角色授與存取權，則不需要自己的超級管理員角色。
- 已設定的 Google 雲端硬碟服務帳戶連線憑證，其中包含您的管理員帳戶電子郵件、用戶端電子郵件 (服務帳戶電子郵件) 請參閱 [GCP 文件，瞭解如何建立和刪除服務帳戶金鑰](#)。

Note

我們建議您定期重新整理或輪換您的認證和密碼。僅為您自己的安全提供必要的訪問級別。我們不建議您跨資料來源以及連接器 1.0 和 2.0 版 (如果適用) 重複使用認證和密碼。

- 建立 Google Cloud 服務帳戶 (具有委派授權以假設使用者身分的帳戶)，並啟用 G Suite 網域範圍委派以進行 server-to-server 驗證，然後使用該帳戶產生 JSON 私密金鑰。

Note

私密金鑰應在建立服務帳戶之後產生。

- 在您的用戶帳戶中添加了管理員 SDK API 和谷歌驅動器 API。
- 可選：配置 Google 雲端硬碟 OAuth 2.0 連接憑據，其中包含客戶端 ID，客戶端密鑰和刷新令牌作為特定用戶的連接憑據。您需要此功能來檢索個別帳戶資料。請參閱[有關使用 OAuth 2.0 訪問 API 的谷歌文檔](#)。
- 使用超級管理員角色將以下 OAuth 範圍添加 (或要求具有超級管理員角色的用戶添加) 以下 OAuth 範圍。需要這些 API 範圍來編目所有文件，以及 Google 工作區域中所有使用者的存取控制 (ACL) 資訊：
 - <https://www.googleapis.com/auth/drive.readonly>—View 並下載您所有的谷歌雲端硬碟文件
 - <https://www.googleapis.com/auth/drive.metadata.readonly>—View 谷歌雲端硬碟中文件的元數據
 - <https://www.googleapis.com/auth/admin.directory.group.readonly>—Scope 僅用於擷取群組、群組別名和成員資訊。這是 Amazon Kendra 身份爬行者程式所需的。
 - <https://www.googleapis.com/auth/admin.directory.user.readonly>—Scope 僅用於擷取使用者或使用者別名。這是在「Amazon Kendra 識別爬行者程式」中列出使用者以及設定 ACL 時所需要的。
 - <https://www.googleapis.com/auth/cloud-platform>—Scope 用於生成訪問令牌以獲取大型 Google 雲端硬碟文件的內容。
 - <https://www.googleapis.com/auth/forms.body.readonly>—Scope 用於從谷歌表單獲取數據。

若要支援表單 API，請新增下列其他範圍：

- <https://www.googleapis.com/auth/forms.body.readonly>
- 已核取每個文件在 Google 雲端硬碟和您打算用於相同索引的其他資料來源中都是唯一的。您要用於索引的每個資料來源不得包含跨資料來源的相同文件。文件 ID 對索引來說是全域的，而且每個索引必須是唯一的。

在您的中 AWS 帳戶，請確保您有：

- [建立 Amazon Kendra 索引](#)，如果使用 API，則會記下索引識別碼。
- 為您的[資料來源建立 IAM 角色](#)，如果使用 API，則會記錄 IAM 角色的 ARN。

Note

如果您變更驗證類型和認證，則必須更新 IAM 角色才能存取正確的 AWS Secrets Manager 密碼 ID。

- 將您的 Google 雲端硬碟身份驗證憑據存儲在 AWS Secrets Manager 秘密中，並且如果使用 API，則註明秘密的 ARN。

Note

我們建議您定期重新整理或輪換您的認證和密碼。僅為您自己的安全提供必要的訪問級別。我們不建議您跨資料來源以及連接器 1.0 和 2.0 版 (如果適用) 重複使用認證和密碼。

如果您沒有現有的 IAM 角色或機密，可以在將 Google 雲端硬碟資料來源連線至時，使用主控台建立新 IAM 角色和 Secrets Manager 密碼 Amazon Kendra。如果您使用 API，則必須提供現有 IAM 角色和 Secrets Manager 密碼的 ARN 以及索引 ID。

連接說明

若要連線 Amazon Kendra 至 Google 雲端硬碟資料來源，您必須提供 Google 雲端硬碟資料來源的必要詳細資料，才 Amazon Kendra 能存取您的資料。如果您尚未配置 Google 雲端硬碟以供 Amazon Kendra 查看[必要條件](#)。

Console

連接 Amazon Kendra 到谷歌雲端硬碟

1. 登入 AWS Management Console 並開啟[Amazon Kendra 主控台](#)。
2. 在左側導覽窗格中，選擇 [索引]，然後從索引清單中選擇要使用的索引。

Note

您可以選擇在索引設置下配置或編輯您的用戶訪問控制設置。


3. 在 [開始使用] 頁面上，選擇 [新增資料來源]。
4. 在 [新增資料來源] 頁面上選擇 [Google 雲端硬碟連接器]，然後選擇 [新增連接器]。如果使用第 2 版（如果適用），請選擇帶有「V2.0」標籤的 Google 雲端硬碟連接器。
5. 在 [指定資料來源詳細資訊] 頁面上，輸入下列資訊：
 - a. 在名稱和說明中，對於資料來源名稱 — 輸入資料來源的名稱。您可以包含連字號，但不能包含空格。
 - b. (選擇性) 說明 — 輸入資料來源的選用說明。
 - c. 在預設語言中 — 選擇一種語言來篩選索引的文件。除非另有指定，否則語言預設為英文。文件中繼資料中指定的語言會覆寫選取的語言。
 - d. 在「標籤」中，針對「新增標籤」 — 包含可選標籤以搜尋和篩選資源或追蹤 AWS 成本。
 - e. 選擇下一步。
6. 在 [定義存取權和安全性] 頁面上，輸入下列資訊：
 - a. 授權 — 開啟或關閉文件的存取控制清單 (ACL) 資訊 (如果您有 ACL)，且想要將其用於存取控制。ACL 會指定使用者和群組可存取的文件。ACL 資訊可用來根據使用者或使用者對文件的群組存取來篩選搜尋結果。如需詳細資訊，請參閱[使用者內容篩選](#)。
 - b. 對於身份驗證 — 根據您的用例在 Google 服務帳戶和 OAuth 2.0 身份驗證之間進行選擇。
 - c. AWS Secrets Manager 密碼：選擇現有密碼，或建立新 Secrets Manager 密碼來儲存您的 Google 雲端硬碟驗證憑證。如果您選擇建立新密碼，則會開啟一個 AWS Secrets Manager 密碼視窗。
 - i. 如果您選擇 Google 服務帳戶，請在服務帳戶配置（管理員電子郵件）中輸入密鑰的名稱，管理員用戶的電子郵件 ID 或「服務帳戶用戶」，服務帳戶的電子郵件 ID（客戶端電子郵件）以及您在服務帳戶中創建的私鑰。

保存並添加您的密碼
 - ii. 如果您選擇 OAuth 2.0 驗證，請輸入您在 OAuth 帳戶中創建的密碼，客戶端 ID，客戶端密鑰和刷新令牌的名稱。

保存並添加您的秘密。
 - d. V@@@ irtual Private Cloud (VPC) (VPC) — 您可以選擇使用 VPC。如果是這樣，您必須新增子網路和 VPC 安全性群組。
 - e. （僅適用於 Google 服務帳戶身份驗證用戶）

識別爬行者程式 — 指定是否要開啟身分識別爬行 Amazon Kendra 爬行者程式。識別爬行者程式會使用文件的存取控制清單 (ACL) 資訊，根據使用者或使用者對文件的群組存取權來篩選搜尋結果。如果您有文件的 ACL 並選擇使用 ACL，您也可以選擇開啟的身分識別爬行者程式，以設定搜尋結果的使用者環境定義篩選。Amazon Kendra 否則，如果關閉身分搜索器，則可以公開搜索所有文檔。如果您想要對文件使用存取控制，且身分識別編目程式已關閉，您也可以使用 [PutPrincipalMapping](#) API 來上傳使用者和群組存取資訊以進行使用者內容篩選。

- f. IAM role — 選擇現有 IAM 角色或建立新 IAM 角色以存取存放庫認證和索引內容。

 Note

IAM 用於索引的角色不能用於資料來源。如果您不確定索引或常見問題集是否使用現有角色，請選擇 [建立新角色] 以避免發生錯誤。

- g. 選擇下一步。

- 7. 在 [設定同步設定] 頁面上，輸入下列資訊：

- a. 同步內容 — 選取您要編目的選項或內容。您可以選擇檢索「我的雲端硬碟」(個人資料夾)、「共用雲端硬碟」(與您共享的資料夾)，或兩者皆可。您也可以包含檔案註解。

- b. 在其他組態-選用您也可以輸入下列選用資訊：

- i. 目標對象 — 為您要編目的文件新增特定目標對象。
- ii. 最大檔案大小 — 設定要編目的最大檔案大小限制 (以 MB 為單位)。
- iii. 使用者電子郵件 — 新增您要包含或排除的使用者電子郵件。
- iv. 共用雲端硬碟：新增您要包含或排除的共用磁碟機名稱。
- v. MIME 類型 — 新增您要包含或排除的 MIME 類型。
- vi. 實體正則表達式模式 — 添加規則運算式模式以包含或排除所有支援實體的某些附件。您最多可以添加 100 個圖案。

- c. 同步模式 — 選擇資料來源內容變更時要如何更新索引。當您第一次將資料來源同 Amazon Kendra 步處理時，依預設會檢索所有內容並建立索引。如果初始同步失敗，您必須執行資料的完整同步，即使您沒有選擇完整同步作為同步模式選項。


- 完全同步：新鮮索引所有內容，並在每次資料來源與索引同步時取代現有內容。

- 新增、修改的同步：每次資料來源與索引同步時，僅對新內容和已修改的內容建立索引。Amazon Kendra 可以使用資料來源的機制來追蹤內容變更，並為上次同步後變更的內容建立索引。
- 新增、修改、刪除的同步：每次資料來源與索引同步時，僅對新內容、已修改和刪除的內容建立索引。Amazon Kendra 可以使用資料來源的機制來追蹤內容變更，並為上次同步後變更的內容建立索引。

 Important

Google 雲端硬碟 API 不支持從永久刪除的文件中檢索評論。刪除文件中的註釋是可檢索的。刪除檔案時，連接器會刪除 Amazon Kendra 索引中的註解。

- d. 在同步執行排程中，對於頻率 — 選擇同步資料來源內容和更新索引的頻率。
 - e. 在 [同步執行歷程記錄] 中，選擇在同步資料來源 Amazon S3 時將自動產生的報告儲存在中。這對於在系統管理資料來源時追蹤問題非常有用。
 - f. 選擇下一步。
8. 在 [設定欄位對映] 頁面上，輸入下列資訊：
- a. 對於檔案 — 從 Amazon Kendra 產生的預設資料來源欄位中選取您要對映至索引的欄位。

 Note

谷歌雲端硬碟 API 不支持創建自定義字段。Google 雲端硬碟連接器無法使用自訂欄位對應。

- b. 選擇下一步。
9. 在 [檢閱並建立] 頁面上，檢查您輸入的資訊是否正確，然後選取 [新增資料來源]。您也可以從此頁面選擇編輯您的資訊。成功新增資料來源後，您的資料來源將顯示在 [資料來源] 頁面上。

API

連接 Amazon Kendra 到谷歌雲端硬碟

您必須使用 [TemplateConfiguration](#) API 指定 [資料來源結構描述](#) 的 JSON。您必須提供以下信息：

- 資料來源 — 指定使用 [TemplateConfiguration](#) JSON 結構定義 `GOOGLEDRIVEV2` 時的資料來源類型。同時將資料來源指定為呼叫 [CreateDataSource](#) API `TEMPLATE` 時的方式。

- 驗證類型 — 指定要使用服務帳戶驗證還是 OAuth 2.0 驗證。
- 同步模式 — 指定資料來源內容變更時 Amazon Kendra 應如何更新索引。當您第一次將資料來源同 Amazon Kendra 步處理時，依預設會檢索所有內容並建立索引。如果初始同步失敗，您必須執行資料的完整同步，即使您沒有選擇完整同步作為同步模式選項。您可以選擇：
 - FORCED_FULL_CRAWL 新建索引所有內容，並在每次資料來源與索引同步時取代現有內容。
 - FULL_CRAWL，以在每次資料來源與索引同步時，僅對新的、修改的和刪除的內容建立索引。Amazon Kendra 可以使用資料來源的機制來追蹤內容變更，並為上次同步後變更的內容建立索引。
 - CHANGE_LOG 每次資料來源與索引同步時，僅對新內容和修改的內容建立索引。Amazon Kendra 可以使用資料來源的機制來追蹤內容變更，並為上次同步後變更的內容建立索引。

⚠ Important

Google 雲端硬碟 API 不支持從永久刪除的文件中檢索評論。刪除文件中的註釋是可檢索的。刪除檔案時，連接器會刪除 Amazon Kendra 索引中的註解。

- 秘密 Amazon 資源名稱 (ARN) — 提供包含您在 Google 雲端硬碟帳戶中創建的身份驗證憑據的 Secrets Manager 秘密的 Amazon 資源名稱 (ARN)。如果您使用 Google 服務帳戶身份驗證，密鑰將儲存在帶有以下密鑰的 JSON 結構中：

```
{
  "clientEmail": "user account email",
  "adminAccountEmail": "service account email",
  "privateKey": "private key"
}
```

如果您使用 OAuth 2.0 驗證，則密碼會以下列金鑰儲存在 JSON 結構中：

```
{
  "clientId": "OAuth client ID",
  "clientSecret": "client secret",
  "refreshToken": "refresh token"
}
```

- IAM role — 指定您撥打電話的 RoleArn 時間，CreateDataSource 以提供具有存取 Secrets Manager 密碼權限的 IAM 角色，以及呼叫 Google 雲端硬碟連接器和 Amazon Kendra 所需的公用 API。如需詳細資訊，請參閱 [Google 雲端硬碟資料來源的 IAM 角色](#)。

您還可以添加以下可選功能：

- Virtual Private Cloud (VPC) — 指定您撥打電話的VpcConfiguration時間。CreateDataSource如需詳細資訊，請參閱 [配置 Amazon Kendra 為使用 Amazon VPC](#)。
- 我的雲端硬碟、共用雲端硬碟、註解 — 您可以指定是否要編目這些類型的內容。
- 包含和排除篩選器 — 您可以指定是否要包含或排除特定使用者帳戶、共用雲端硬碟和 MIME 類型。

Note

大多數資料來源使用規則運算式模式，這些模式是稱為篩選器的包含或排除模式。如果您指定包含篩選器，則只有符合包含項目篩選器的內容會編製索引。不符合包含篩選器的任何文件都不會建立索引。如果您指定包含和排除篩選器，符合排除篩選器的文件將不會建立索引，即使它們符合包含篩選器也是如此。

- 存取控制清單 (ACL) — 指定是否要編目文件的 ACL 資訊 (如果您有 ACL 並且想要將其用於存取控制)。ACL 會指定使用者和群組可存取的文件。ACL 資訊可用來根據使用者或使用者對文件的群組存取來篩選搜尋結果。如需詳細資訊，請參閱 [使用者內容篩選](#)。
- 識別爬行者程式 — 指定是否要開啟身分識別爬行 Amazon Kendra 爬行者程式。識別爬行者程式會使用文件的存取控制清單 (ACL) 資訊，根據使用者或使用者對文件的群組存取權來篩選搜尋結果。如果您有文件的 ACL 並選擇使用 ACL，您也可以選擇開啟的身分識別爬行者程式，以設定搜尋結果的使用者環境定義篩選。Amazon Kendra 否則，如果關閉身分搜索器，則可以公開搜索所有文檔。如果您想要對文件使用存取控制，且身分識別編目程式已關閉，您也可以使用 [PutPrincipalMapping](#) API 來上傳使用者和群組存取資訊以進行使用者內容篩選。
- 欄位對應 — 選擇將 Google 雲端硬碟資料來源欄位對應至 Amazon Kendra 索引欄位。如需詳細資訊，請參閱 [映射資料來源欄位](#)。

Note

您的文件需要文件內文欄位或文件內文對等項目，才能搜尋您的文件。Amazon Kendra 您必須將資料來源中的文件內文欄位名稱對應至索引欄位名稱_document_body。所有其他欄位是選用的。

如需要設定的其他重要 JSON 金鑰清單，請參閱 [Google 雲端硬碟範本結構描述](#)。

備註

- 自訂欄位對應不適用於 Google 雲端硬碟連接器，因為 Google 雲端硬碟 UI 不支援建立自訂欄位。
- Google 雲端硬碟 API 不支持從永久刪除的文件中檢索評論。但是，對於已刪除的文件，註釋是可以檢索的。刪除檔案時，Amazon Kendra 連接器會刪除 Amazon Kendra 索引中的註解。
- 谷歌雲端硬碟 API 不會返回存在於 .docx 文件中的註釋。

IBM DB2

IBM DB2是一個由IBM. 如果您是使用IBM DB2者，則可以使用 Amazon Kendra 對資IBM DB2料來源建立索引。資 Amazon Kendra IBM DB2料來源連接器支援 DB2 11.5.7。

您可以使用[Amazon Kendra 主控台](#)和 [TemplateConfiguration](#)API 連線 Amazon Kendra 到IBM DB2資料來源。

如需疑難排解資 Amazon Kendra IBM DB2料來源連接器，請參閱[疑難排解資料來](#)。

主題

- [支援的功能](#)
- [必要條件](#)
- [連接說明](#)
- [備註](#)

支援的功能

- 欄位對映
- 使用者內容篩選
- 包含/排除過濾器
- 完整和增量內容同步
- 虛擬私有雲端 (VPC)

必要條件

在您可以用來 Amazon Kendra 為資IBM DB2料來源建立索引之前，請先在IBM DB2和 AWS 帳戶中進行這些變更。

在中IBM DB2，請確定您有：

- 記下您的資料庫使用者名稱和密碼。

⚠ Important

最佳作法是提供 Amazon Kendra 唯讀資料庫認證。

- 複製您的資料庫主機 URL、連接埠和執行個體。
- 已勾選的每個文件在您打算用於相同索引的其他資料來源中IBM DB2和其他資料來源之間都是唯一的。您要用於索引的每個資料來源不得包含跨資料來源的相同文件。文件 ID 對索引來說是全域的，而且每個索引必須是唯一的。

在你的 AWS 帳戶，確保你有：

- [建立 Amazon Kendra 索引](#)，如果使用 API，則會記下索引 ID。
- 為您的[資料來源建立 IAM 角色](#)，如果使用 API，則會記錄 IAM 角色的 ARN。

i Note

如果您變更驗證類型和認證，則必須更新 IAM 角色才能存取正確的 AWS Secrets Manager 密碼 ID。

- 將您的IBM DB2身份驗證憑據存儲在 AWS Secrets Manager 密鑰中，如果使用 API，則記錄密鑰的 ARN。

i Note

我們建議您定期重新整理或輪換您的認證和密碼。僅為您自己的安全提供必要的訪問級別。我們不建議您跨資料來源以及連接器 1.0 和 2.0 版 (如果適用) 重複使用認證和密碼。

如果您沒有現有的 IAM 角色或密碼，則可以在將IBM DB2資料來源連線到時使用主控台建立新 IAM 角色和 Secrets Manager 密碼 Amazon Kendra。如果您使用 API，則必須提供現有 IAM 角色和 Secrets Manager 密碼的 ARN，以及索引 ID。

連接說明

若要連線 Amazon Kendra 到 IBM DB2 資料來源，您必須提供 IBM DB2 認證的詳細資料，Amazon Kendra 以便能夠存取您的資料。如果您尚未設定「Amazon Kendra 請 IBM DB2 參閱 [必要條件](#)」。

Console

若要連線 Amazon Kendra 到 IBM DB2


1. 登入 AWS Management Console 並開啟 [Amazon Kendra 主控台](#)。
2. 在左側導覽窗格中，選擇 [索引]，然後從索引清單中選擇要使用的索引。

Note

您可以選擇在索引設置下配置或編輯您的用戶訪問控制設置。

3. 在 [開始使用] 頁面上，選擇 [新增資料來源]。
4. 在 [新增資料來源] 頁面上，選擇 [IBM DB2 連接器]，然後選擇 [新增連接器]。如果使用版本 2 (如果適用)，請選擇帶有「V2.0」標籤的 IBM DB2 連接器。
5. 在 [指定資料來源詳細資訊] 頁面上，輸入下列資訊：
 - a. 在名稱和說明中，對於資料來源名稱 — 輸入資料來源的名稱。您可以包含連字號，但不能包含空格。
 - b. (選擇性) 說明 — 輸入資料來源的選用說明。
 - c. 在預設語言中 — 選擇一種語言來篩選索引的文件。除非另有指定，否則語言預設為英文。文件中繼資料中指定的語言會覆寫選取的語言。
 - d. 在「標籤」中，針對「新增標籤」— 包含可選標籤以搜尋和篩選資源或追蹤 AWS 成本。
 - e. 選擇下一步。
6. 在 [定義存取和安全性] 頁面上，輸入下列資訊：
 - a. 在來源中，輸入下列資訊：
 - b. 主機 — 輸入資料庫主機名稱。
 - c. 連接埠 — 輸入資料庫連接埠。
 - d. 執行處理 — 輸入資料庫執行處理。
 - e. 啟用 SSL 憑證位置 — 選擇此選項可輸入 SSL 憑證檔案的 Amazon S3 路徑。
 - f. 在驗證中 — 輸入下列資訊：

- AWS Secrets Manager 祕密 — 選擇現有密碼或建立新 Secrets Manager 密碼來儲存您的 IBM DB2 驗證認證。如果您選擇建立新密碼，則會開啟一個 AWS Secrets Manager 密碼視窗。
 - A. 在「建立 AWS Secrets Manager 密碼視窗」中輸入下列資訊：
 - I. 秘密名稱 — 您秘密的名稱。前綴 'AmazonKendraIBM DB2-' 會自動添加到您的密碼名稱中。
 - II. 對於資料庫使用者名稱和密碼 — 輸入您從資料庫複製的驗證認證值。
 - B. 選擇儲存。
- g. Virtual Private Cloud (VPC) (VPC) — 您可以選擇使用 VPC。如果是這樣，您必須新增子網路和 VPC 安全性群組。
- h. IAM role — 選擇現有 IAM 角色或建立新 IAM 角色以存取存放庫認證和索引內容。

 Note

IAM 用於索引的角色不能用於資料來源。如果您不確定索引或常見問題集是否使用現有角色，請選擇 [建立新角色] 以避免發生錯誤。

- i. 選擇下一步。
7. 在 [設定同步設定] 頁面上，輸入下列資訊：
- a. 在同步範圍中，從下列選項中選擇：
 - SQL 查詢 — 輸入 SQL 查詢陳述式，例如選取和聯結作業。SQL 查詢必須小於 32 KB。Amazon Kendra 會編目符合您查詢的所有資料庫內容。
 - 主索引鍵欄 — 提供資料庫表格的主索引鍵。這標識數據庫中的一個表。
 - 標題欄 — 提供資料庫表格中文件標題欄的名稱。
 - 主體欄 — 提供資料庫表格中文件主體欄的名稱。
 - b. 在 [其他設定 — 選用] 中，從下列選項中選擇以同步特定內容，而非同步所有檔案：
 - 變更偵測欄 — 輸入 Amazon Kendra 將用來偵測內容變更的欄名稱。Amazon Kendra 當這些資料行中有任何變更時，會重新建立內容的索引。
 - 使用者 ID 欄 — 輸入包含允許存取內容的使用者 ID 的欄名稱。
 - 群組欄 — 輸入包含允許存取內容之群組的欄名稱。
 - 來源 URL 欄 — 輸入包含要編製索引之來源 URL 的資料欄名稱。

- 時間戳記欄 — 輸入包含時間戳記的欄名稱。Amazon Kendra 使用時間戳記資訊偵測內容中的變更，並僅同步變更的內容。
 - [時區] 欄 — 輸入資料欄的名稱，其中包含要編目之內容的時區。
 - 時間戳記格式 — 輸入包含時間戳記格式的欄名稱，可用來偵測內容變更並重新同步處理內容。
- c. 同步模式 — 選擇資料來源內容變更時要如何更新索引。當您第一次將資料來源同 Amazon Kendra 步處理時，依預設會檢索所有內容並建立索引。如果初始同步失敗，您必須執行資料的完整同步處理，即使您沒有選擇完整同步作為同步模式選項。
- 完全同步：新鮮索引所有內容，並在每次資料來源與索引同步時取代現有內容。
 - 新增、修改的同步：每次資料來源與索引同步時，僅對新內容和已修改的內容建立索引。Amazon Kendra 可以使用資料來源的機制來追蹤內容變更，並為上次同步後變更的內容建立索引。
 - 新增、修改、刪除的同步：每次資料來源與索引同步時，僅對新內容、已修改和刪除的內容建立索引。Amazon Kendra 可以使用資料來源的機制來追蹤內容變更，並為上次同步後變更的內容建立索引。
- d. 在同步執行排程中，對於頻率 — 與資料來源同步的頻率。Amazon Kendra
- e. 選擇下一步。
8. 在 [設定欄位對映] 頁面上，輸入下列資訊：
- a. 從產生的預設資料來源欄位中選取您要對應至 Amazon Kendra 索引的文件 ID、文件標題和來源 URL。
 - b. 新增欄位 — 新增自訂資料來源欄位，以建立要對映的索引欄位名稱和欄位資料類型。
 - c. 選擇下一步。
9. 在 [檢閱並建立] 頁面上，檢查您輸入的資訊是否正確，然後選取 [新增資料來源]。您也可以從此頁面選擇編輯您的資訊。成功新增資料來源後，您的資料來源將顯示在 [資料來源] 頁面上。

API

若要連線 Amazon Kendra 到 IBM DB2

您必須使用 [TemplateConfiguration](#) API 指定下列項目：

- 資料來源 — 指定使用 [TemplateConfiguration](#) JSON 結構定義 JDBC 時的資料來源類型。同時將資料來源指定為呼叫 [CreateDataSource](#) API TEMPLATE 時的方式。

- 資料庫類型 — 您必須將資料庫類型指定為db2。
- SQL 查詢 — 指定 SQL 查詢陳述式，例如 SELECT 和 JOIN 作業。SQL 查詢必須小於 32 KB。Amazon Kendra 會編目符合您查詢的所有資料庫內容。
- 同步模式 — 指定資料來源內容變更時 Amazon Kendra 應如何更新索引。當您第一次將資料來源同 Amazon Kendra 步處理時，依預設會檢索所有內容並建立索引。如果初始同步失敗，您必須執行資料的完整同步處理，即使您沒有選擇完整同步作為同步模式選項。您可以選擇：
 - FORCED_FULL_CRAWL 新建索引所有內容，並在每次資料來源與索引同步時取代現有內容。
 - FULL_CRAWL，以在每次資料來源與索引同步時，僅對新的、修改的和刪除的內容建立索引。Amazon Kendra 可以使用資料來源的機制來追蹤內容變更，並為上次同步後變更的內容建立索引。
 - CHANGE_LOG 每次資料來源與索引同步時，僅對新內容和修改的內容建立索引。Amazon Kendra 可以使用資料來源的機制來追蹤內容變更，並為上次同步後變更的內容建立索引。
- 秘密 Amazon 資源名稱 (ARN) — 提供包含您在帳戶中建立的身份驗證登入資料的 Secrets Manager 密碼的 Amazon 資源名稱 (ARN)。IBM DB2 密碼會以下列金鑰儲存在 JSON 結構中：

```
{
  "user name": "database user name",
  "password": "password"
}
```

Note

我們建議您定期重新整理或輪換您的認證和密碼。僅為您自己的安全提供必要的訪問級別。我們不建議您跨資料來源以及連接器 1.0 和 2.0 版 (如果適用) 重複使用認證和密碼。

- IAM role — 指定 RoleArn 何時呼叫 CreateDataSource 以提供具有存取 Secrets Manager 密碼之權限的 IAM 角色，以及呼叫 IBM DB2 連接器和 Amazon Kendra 所需公用 API 的時間。有關詳情，請參閱 [IBM DB2 資料來源的 IAM 角色](#)。

您還可以添加以下可選功能：

- Virtual Private Cloud (VPC) — 指定您撥打電話的 VpcConfiguration 時間。CreateDataSource 如需詳細資訊，請參閱 [配置 Amazon Kendra 為使用 Amazon VPC](#)。
- 包含和排除篩選器 — 您可以指定是否要使用使用者 ID、群組、來源 URL、時間戳記和時區來包含特定內容。

- 使用者前後關聯篩選與存取控制 — Amazon Kendra 探索文件的存取控制清單 (ACL) (如果您有文件的 ACL)。ACL 資訊可用來根據使用者或使用者對文件的群組存取權來篩選搜尋結果。如需詳細資訊，請參閱[使用者內容篩選](#)。
- 欄位對映 — 選擇將 IBM DB2 資料來源欄位對映至 Amazon Kendra 索引欄位。如需詳細資訊，請參閱[映射資料來源欄位](#)。

Note

您的文件需要文件內文欄位或文件內文對等項目，才能搜尋您的文件。Amazon Kendra 您必須將資料來源中的文件內文欄位名稱對應至索引欄位名稱 `_document_body`。所有其他欄位是選用的。

如需要設定的其他重要 JSON 金鑰清單，請參閱[模板架構](#)。

備註

- Amazon Kendra 檢查更新的內容時，不會追蹤已刪除的資料庫列。
- 資料庫中一列中欄位名稱和值的大小不得超過 400 KB。
- 如果您的資料庫資料來源中有大量資料，並且不想 Amazon Kendra 在第一次同步之後對所有資料庫內容建立索引，則可以選擇僅同步新文件、修改或刪除的文件。
- 最佳作法是提供 Amazon Kendra 唯讀資料庫認證。
- 最佳做法是避免新增包含敏感資料或個人可識別資訊 (PII) 的表格。

Jira

Jira 是用於軟體開發，產品管理和錯誤跟踪的項目管理工具。您可以使 Amazon Kendra 用編制 Jira 專案、問題、注解、附件、工作日誌和狀態的索引。

Amazon Kendra 目前僅支持吉拉雲。

您可以使用[Amazon Kendra 控制台](#)或 [JiraConfiguration](#) API 連接 Amazon Kendra 到 Jira 數據源。如需每個功能所支援的功能清單，請參閱[支援的功能](#)。

如需對 Amazon Kendra Jira 資料來源連接器進行疑難排解，請參閱[疑難排解資料來](#)。

主題

- [支援的功能](#)
- [必要條件](#)
- [連接說明](#)
- [進一步了解](#)

支援的功能

Amazon Kendra Jira 資料來源連接器支援下列功能：

- 欄位對映
- 使用者存取控制
- 包含/排除過濾器
- 完整和增量內容同步
- 虛擬私有雲端 (VPC)

必要條件

在您可以用來 Amazon Kendra 為 Jira 資料來源建立索引之前，請先在 Jira 和 AWS 帳戶中進行這些變更。

在吉拉，確保你有：

- 配置的 API 令牌身份驗證憑據，其中包括 Jira ID (用戶名或電子郵件) 和 Jira 憑據 (Jira API 令牌)。請參閱 [有關管理 API 權杖的使用說明文件](#)。

Note

我們建議您定期重新整理或輪換您的認證和密碼。僅為您自己的安全提供必要的訪問級別。我們不建議您跨資料來源以及連接器 1.0 和 2.0 版 (如果適用) 重複使用認證和密碼。

- 記下您的 Jira 帳戶設定中的 Jira 帳戶網址。例如：<https://company.atlassian.net/>。
- 已核取每個文件在 Jira 以及您打算用於相同索引的其他資料來源中都是唯一的。您要用於索引的每個資料來源不得包含跨資料來源的相同文件。文件 ID 對索引來說是全域的，而且每個索引必須是唯一的。

在您的中 AWS 帳戶，請確保您有：

- [建立 Amazon Kendra 索引](#)，如果使用 API，則會記下索引識別碼。
- 為您的[資料來源建立 IAM 角色](#)，如果使用 API，則會記錄 IAM 角色的 ARN。

Note

如果您變更驗證類型和認證，則必須更新 IAM 角色才能存取正確的 AWS Secrets Manager 密碼 ID。

- 將您的 Jira 身份驗證憑據存儲在 AWS Secrets Manager 密鑰中，如果使用 API，則記錄密鑰的 ARN。

Note

我們建議您定期重新整理或輪換您的認證和密碼。僅為您自己的安全提供必要的訪問級別。我們不建議您跨資料來源以及連接器 1.0 和 2.0 版 (如果適用) 重複使用認證和密碼。

如果您沒有現有的 IAM 角色或密碼，則可以在將 Jira 資料來源連線至時使用主控台建立新 IAM 角色和 Secrets Manager 密碼。Amazon Kendra 如果您使用 API，則必須提供現有 IAM 角色和 Secrets Manager 密碼的 ARN 以及索引 ID。

連接說明

若要連線 Amazon Kendra 到 Jira 資料來源，您必須提供 Jira 資料來源的必要詳細資訊，Amazon Kendra 以便能夠存取您的資料。如果您尚未為其配置 Jira Amazon Kendra，請參閱[必要條件](#)。

Console

若要連接 Amazon Kendra 到吉拉

1. 登入 AWS Management Console 並開啟[Amazon Kendra 主控台](#)。
2. 在左側導覽窗格中，選擇 [索引]，然後從索引清單中選擇要使用的索引。

Note


您可以選擇在索引設置下配置或編輯您的用戶訪問控制設置。

3. 在 [開始使用] 頁面上，選擇 [新增資料來源]。

4. 在 [新增資料來源] 頁面上，選擇 [Jira 連接器]，然後選擇 [新增連接器]。如果使用版本 2 (如果適用)，請選擇帶有「V2.0」標籤的 Jira 連接器。
5. 在 [指定資料來源詳細資訊] 頁面上，輸入下列資訊：
 - a. 在名稱和說明中，對於資料來源名稱 — 輸入資料來源的名稱。您可以包含連字號，但不能包含空格。
 - b. (選擇性) 說明 — 輸入資料來源的選用說明。
 - c. 在預設語言中 — 選擇一種語言來篩選索引的文件。除非另有指定，否則語言預設為英文。文件中繼資料中指定的語言會覆寫選取的語言。
 - d. 在「標籤」中，針對「新增標籤」 — 包含可選標籤以搜尋和篩選資源或追蹤 AWS 成本。
 - e. 選擇下一步。
6. 在 [定義存取權和安全性] 頁面上，輸入下列資訊：
 - a. Jira 帳戶網址 — 輸入您的 Jira 帳戶網址。例如：<https://company.atlassian.net/>。
 - b. 授權 — 開啟或關閉文件的存取控制清單 (ACL) 資訊 (如果您有 ACL)，且想要將其用於存取控制。ACL 會指定使用者和群組可存取的文件。ACL 資訊可用來根據使用者或使用者對文件的群組存取權來篩選搜尋結果。如需詳細資訊，請參閱[使用者內容篩選](#)。
 - c. AWS Secrets Manager 秘密 — 選擇現有密碼或建立新 Secrets Manager 密碼來儲存您的 Jira 驗證認證。如果您選擇建立新密碼，則會開啟一個 AWS Secrets Manager 密碼視窗。
 - i. 在「建立 AWS Secrets Manager 密碼視窗」中輸入下列資訊：
 - A. 秘密名稱 — 您秘密的名稱。前綴 'AmazonKendra-Jira-' 會自動添加到您的密碼名稱中。
 - B. 對於 Jira ID — 輸入 Jira 使用者名稱或電子郵件。
 - C. 對於密碼/權杖 — 輸入在 Jira 中設定的 Jira API 權杖。
 - ii. 保存並添加您的秘密。
 - d. V@@@ irtual Private Cloud (VPC) (VPC) — 您可以選擇使用 VPC。如果是這樣，您必須新增子網路和 VPC 安全性群組。
 - e. 識別爬行者程式 — 指定是否要開啟身分識別爬行 Amazon Kendra 者程式。識別爬行者程式會使用文件的存取控制清單 (ACL) 資訊，根據使用者或使用者對文件的群組存取權來篩選搜尋結果。如果您有文件的 ACL 並選擇使用 ACL，您也可以選擇開啟的身分識別爬行者程式，以設定搜尋結果的使用者[環境定義篩選](#)。Amazon Kendra 否則，如果關閉身分搜

索器，則可以公開搜索所有文檔。如果您想要對文件使用存取控制，且身分識別編目程式已關閉，您也可以使用 [PutPrincipalMapping](#) API 來上傳使用者和群組存取資訊以進行使用者內容篩選。

- f. IAM role — 選擇現有 IAM 角色或建立新 IAM 角色以存取存放庫認證和索引內容。

 Note

IAM 用於索引的角色不能用於資料來源。如果您不確定索引或常見問題集是否使用現有角色，請選擇 [建立新角色] 以避免發生錯誤。

- g. 選擇下一步。

7. 在 [設定同步設定] 頁面上，輸入下列資訊：

- a. 選取要索引的 Jira 專案 — 選擇編目所有專案或特定專案。
- b. 其他配置 — 指定某些狀態和問題類型。選擇編目註解、附件和工作日誌。使用規則運算式模式來包含或排除某些內容。
- c. 同步模式 — 選擇資料來源內容變更時要如何更新索引。當您第一次將資料來源同 Amazon Kendra 步處理時，依預設會檢索所有內容並建立索引。如果初始同步失敗，您必須執行資料的完整同步處理，即使您沒有選擇完整同步作為同步模式選項。
 - 完全同步：新鮮索引所有內容，並在每次資料來源與索引同步時取代現有內容。
 - 新增、修改的同步：每次資料來源與索引同步時，僅對新內容和已修改的內容建立索引。Amazon Kendra 可以使用資料來源的機制來追蹤內容變更，並為上次同步後變更的內容建立索引。
 - 新增、修改、刪除的同步：每次資料來源與索引同步時，僅對新內容、已修改和刪除的內容建立索引。Amazon Kendra 可以使用資料來源的機制來追蹤內容變更，並為上次同步後變更的內容建立索引。
- d. 在同步執行排程中，對於頻率 — 選擇同步資料來源內容和更新索引的頻率。
- e. 選擇下一步。

8. 在 [設定欄位對映] 頁面上，輸入下列資訊：

- a. 預設資料來源欄位 — 從 Amazon Kendra 產生的預設資料來源欄位中選取您要對映至索引的資料來源欄位。
- b. 新增欄位 — 新增自訂資料來源欄位，以建立要對映的索引欄位名稱和欄位資料類型。
- c. 選擇下一步。

9. 在 [檢閱並建立] 頁面上，檢查您輸入的資訊是否正確，然後選取 [新增資料來源]。您也可以從此頁面選擇編輯您的資訊。成功新增資料來源後，您的資料來源將顯示在 [資料來源] 頁面上。

API

若要連接 Amazon Kendra 到吉拉

您必須使用 [JiraConfiguration](#) API 指定下列項目：

- 資料來源網址 — 指定您的 Jira 帳戶 URL。例如，`### .atlassian.net#`
- 秘密 Amazon 資源名稱 (ARN) — 提供包含您 Jira 帳戶身份驗證登入資料的 Secrets Manager 密碼的 Amazon 資源名稱 (ARN)。密碼會以下列金鑰儲存在 JSON 結構中：

```
{
  "jiraId": "Jira user name or email",
  "jiraCredential": "Jira API token"
}
```

- IAM role — 指定 RoleArn 何時呼叫 CreateDataSource 以提供具有存取 Secrets Manager 密碼之權限的 IAM 角色，以及呼叫 Jira 連接器和所需公用 API 的時間。Amazon Kendra 有關詳情，請參閱 [Jira 資料來源的 IAM 角色](#)。

您還可以添加以下可選功能：

- VPC (Virtual Private Cloud) — 指定 VpcConfiguration 為資料來源組態的一部分。請參閱 [設定 Amazon Kendra 定以使用 VPC](#)。
- 變更記錄 — 是否 Amazon Kendra 應該使用 Jira 資料來源變更記錄機制來判斷是否必須在索引中更新文件。

Note

如果您不想 Amazon Kendra 掃描所有文檔，請使用更改日誌。如果您的變更記錄很大，掃描 Jira 資料來源中的文件可能比處理變更記錄所花費的時間更 Amazon Kendra 少。如果您是第一次將 Jira 資料來源與索引同步，則會掃描所有文件。

- 包含和排除篩選器 — 您可以指定要包含還是排除某些檔案。

Note

大多數資料來源使用規則運算式模式，這些模式是稱為篩選器的包含或排除模式。如果您指定包含篩選器，則只有符合包含項目篩選器的內容會編製索引。不符合包含篩選器的任何文件都不會建立索引。如果您指定包含和排除篩選器，符合排除篩選器的文件將不會建立索引，即使它們符合包含篩選器也是如此。

- 註解、附件和工作記錄 — 您可以指定是否編目問題的某些註解、附件和工作記錄。
- 專案、問題、狀態 — 您可以指定是否編目特定專案 ID、問題類型和狀態。
- 使用者前後關聯篩選與存取控制 — Amazon Kendra 探索文件的存取控制清單 (ACL) (如果您有文件的 ACL)。ACL 資訊可用來根據使用者或使用者對文件的群組存取權來篩選搜尋結果。如需詳細資訊，請參閱[使用者內容篩選](#)。
- 欄位對映 — 選擇將您的 Jira 資料來源欄位對映至 Amazon Kendra 索引欄位。如需詳細資訊，請參閱[映射資料來源欄位](#)。

Note

您的文件需要文件內文欄位或文件內文對等項目，才能搜尋您的文件。Amazon Kendra 您必須將資料來源中的文件內文欄位名稱對應至索引欄位名稱_document_body。所有其他欄位是選用的。

進一步了解

若要進一步瞭解 Amazon Kendra 與 Jira 資料來源整合的相關資訊，請參閱：

- [使用 Jira 雲端連接器智慧搜尋您的 Amazon Kendra Jira 專案](#)

Microsoft Exchange

Microsoft Exchange 是用於消息傳遞，會議和文件共享的企業協作工具。如果您是 Microsoft 交換使用者，您可以使用 Amazon Kendra 來索引您的 Microsoft 交換資料來源。

您可以使用[Amazon Kendra 主控台](#)和 [TemplateConfiguration](#)API 連線 Amazon Kendra 到您的 Microsoft Exchange 資料來源。

如需疑難排解 Amazon Kendra Microsoft 的資料來源連接器，請參閱[疑難排解資料來](#)。

支援的功能

- 欄位對映
- 使用者存取控制
- 包含/排除過濾器
- 完整和增量內容同步
- 虛擬私有雲端 (VPC)

必要條件

在您可以使用 Amazon Kendra 來索引您的 Microsoft 交換資料來源之前，請先在您的 Microsoft Exchange 和 AWS 帳戶中進行這些變更。

在 Microsoft 交易所，請確保你有：

- 在辦公室 365 中創建了一個 Microsoft 交換帳戶。
- 注意到您的 Microsoft 365 租戶 ID。您可以在 Azure 作用中目錄入口網站的內容或 OAuth 應用程式中找到您的租用戶識別碼。
- 在 Azure 入口網站中設定 OAuth 應用程式，並記下用戶端識別碼和用戶端密碼或用戶端認證。如需詳細資訊，請參閱 [Microsoft 教學課程](#) 和 [已註冊應用程式](#)

Note

當您在 Azure 入口網站中建立或註冊應用程式時，秘密識別碼代表實際的密碼值。建立密碼和應用程式時，您必須立即記下或儲存實際的密碼值。您可以在 Azure 入口網站中選取應用程式的名稱，然後導覽至憑證和密碼的功能表選項，以存取您的密碼。

您可以在 Azure 入口網站中選取應用程式的名稱，然後導覽至概觀頁面，以存取用戶端識別碼。應用程序 (客戶端) ID 是客戶端 ID。

Note

我們建議您定期重新整理或輪換您的認證和密碼。僅為您自己的安全提供必要的訪問級別。我們不建議您跨資料來源以及連接器 1.0 和 2.0 版 (如果適用) 重複使用認證和密碼。

- 已新增連接器應用程式的下列權限：

Microsoft 圖

辦公室 365 線上交換

- 郵件閱讀 (應用程式)
- 郵件。ReadBasic (應用程式)
- 郵件。ReadBasic. 全部 (應用程式)
- 日曆。閱讀 (應用程式)
- 使用者 .Read. 全部 (應用程式)
- 聯絡閱讀 (應用程式)
- 注意事項閱讀全部 (應用程式)
- 目錄全部 (申請)
- EWS。AccessAsUser. 全部 (已委派)

完整訪問應用程式 (應用程式)

- 核取每個文件在 Microsoft Exchange 和您打算用於相同索引的其他資料來源中都是唯一的。您要用於索引的每個資料來源不得包含跨資料來源的相同文件。文件 ID 對索引來說是全域的，而且每個索引必須是唯一的。

在您的中 AWS 帳戶，請確保您有：

- [建立 Amazon Kendra 索引](#)，如果使用 API，則會記下索引識別碼。
- 為您的[資料來源建立 IAM 角色](#)，如果使用 API，則會記錄 IAM 角色的 ARN。

Note

如果您變更驗證類型和認證，則必須更新 IAM 角色才能存取正確的 AWS Secrets Manager 密碼 ID。

- 將您的 Microsoft Exchange 身份驗證憑據存儲在 AWS Secrets Manager 密鑰中，並且如果使用 API，則會記錄密碼的 ARN。

Note

我們建議您定期重新整理或輪換您的認證和密碼。僅為您自己的安全提供必要的訪問級別。我們不建議您跨資料來源以及連接器 1.0 和 2.0 版 (如果適用) 重複使用認證和密碼。

如果您沒有現有的 IAM 角色或密碼，則可以在將 Microsoft Exchange 資料來源連線到時，使用主控台建立新 IAM 角色和 Secrets Manager 密碼 Amazon Kendra。如果您使用 API，則必須提供現有 IAM 角色和 Secrets Manager 密碼的 ARN，以及索引 ID。

連接說明

若要連線 Amazon Kendra 到您的 Microsoft Exchange 資料來源，您必須提供您的 Microsoft Exchange 資料來源的必要詳細資料，Amazon Kendra 以便能夠存取您的資料。如果您尚未為下列項 Microsoft 設定 Amazon Kendra，請參閱[必要條件](#)。

Console

連接 Amazon Kendra 到 Microsoft 交易所


1. 登入 AWS Management Console 並開啟[Amazon Kendra 主控台](#)。
2. 在左側導覽窗格中，選擇 [索引]，然後從索引清單中選擇要使用的索引。

Note

您可以選擇在索引設置下配置或編輯您的用戶訪問控制設置。

3. 在 [開始使用] 頁面上，選擇 [新增資料來源]。
4. 在 [新增資料來源] 頁面上，選擇 [Microsoft Exchange 連接器]，然後選擇 [新增連接器]。如果使用版本 2 (如果適用)，請選擇帶有「V2.0」標籤的 Microsoft 交換連接器。
5. 在 [指定資料來源詳細資訊] 頁面上，輸入下列資訊：
 - a. 在名稱和說明中，對於資料來源名稱 — 輸入資料來源的名稱。您可以包含連字號，但不能包含空格。
 - b. (選擇性) 說明 — 輸入資料來源的選用說明。
 - c. 在預設語言中 — 選擇一種語言來篩選索引的文件。除非另有指定，否則語言預設為英文。文件中繼資料中指定的語言會覆寫選取的語言。
 - d. 在「標籤」中，針對「新增標籤」 — 包含可選標籤以搜尋和篩選資源或追蹤 AWS 成本。
 - e. 選擇下一步。
6. 在 [定義存取權和安全性] 頁面上，輸入下列資訊：
 - a. 租用戶識別碼 — 輸入您的 Microsoft 365 租用戶識別碼。您可以在 Azure 作用中目錄入口網站的內容或 OAuth 應用程式中找到您的租用戶識別碼。


- b. 授權 — 開啟或關閉文件的存取控制清單 (ACL) 資訊 (如果您有 ACL)，且想要將其用於存取控制。ACL 會指定使用者和群組可存取的文件。ACL 資訊可用來根據使用者或使用者對文件的群組存取權來篩選搜尋結果。如需詳細資訊，請參閱[使用者內容篩選](#)。
- c. AWS Secrets Manager 密碼 — 選擇現有密碼或建立新 Secrets Manager 密碼來儲存您的 Microsoft Exchange 驗證認證。如果您選擇建立新密碼，則會開啟一個 AWS Secrets Manager 密碼視窗。
 - i. 在「建立 AWS Secrets Manager 密碼視窗」中輸入下列資訊：
 - A. 秘密名稱 — 您秘密的名稱。前綴 'AmazonKendra-Microsoft 交易所
 - B. 對於用戶端識別碼，用戶端密碼 — 輸入 Azure 入口網站中在 Microsoft Exchange 中設定的驗證認證。
 - ii. 保存並添加您的秘密。
- d. Virtual Private Cloud (VPC) (VPC) — 您可以選擇使用 VPC。如果是這樣，您必須新增子網路和 VPC 安全性群組。
- e. IAM role — 選擇現有 IAM 角色或建立新 IAM 角色以存取存放庫認證和索引內容。

 Note

IAM 用於索引的角色不能用於資料來源。如果您不確定索引或常見問題集是否使用現有角色，請選擇 [建立新角色] 以避免發生錯誤。

- f. 選擇下一步。
7. 在 [設定同步設定] 頁面上，輸入下列資訊：
- a. 使用者 ID：如果您想要依特定電子郵件篩選內容，請提供使用者電子郵件。
 - b. 其他組態 — 指定您要編目的內容類型。
 - 實體類型 — 您可以選擇編目行事曆或連絡人內容。OneNotes
 - 行事曆搜索 — 輸入在特定日期之間編目內容的開始和結束日期。
 - 包含電子郵件 — 輸入「收件人」、「寄件人」和電子郵件主旨行，以篩選您要檢索的某些電子郵件。
 - 共用資料夾存取權限 — 選擇此選項可啟用存取控制清單的編目，以便控制 Microsoft Exchange 資料來源的存取控制。
 - 網域的 Regex — 新增規則運算式模式以包含或排除特定電子郵件網域。
 - 正則表達式模式 - 添加正則表達式模式以包含或排除某些文件。

- c. 同步模式 — 選擇資料來源內容變更時要如何更新索引。當您第一次將資料來源同 Amazon Kendra 步處理時，依預設會檢索所有內容並建立索引。如果初始同步失敗，您必須執行資料的完整同步處理，即使您沒有選擇完整同步作為同步模式選項。
 - 完全同步：新鮮索引所有內容，並在每次資料來源與索引同步時取代現有內容。
 - 新增、修改的同步：每次資料來源與索引同步時，僅對新內容和已修改的內容建立索引。Amazon Kendra 可以使用資料來源的機制來追蹤內容變更，並為上次同步後變更的內容建立索引。
 - 新增、修改、刪除的同步：每次資料來源與索引同步時，僅對新內容、已修改和刪除的內容建立索引。Amazon Kendra 可以使用資料來源的機制來追蹤內容變更，並為上次同步後變更的內容建立索引。
 - d. 在同步執行排程中，對於頻率 — 選擇同步資料來源內容和更新索引的頻率。
 - e. 選擇下一步。
8. 在 [設定欄位對映] 頁面上，輸入下列資訊：
- a. 預設資料來源欄位 — 從 Amazon Kendra 產生的預設資料來源欄位中選取您要對映至索引的資料來源欄位。

 Note

Amazon Kendra Microsoft Exchange 資料來源連接器不支援自訂欄位對應。

- b. 選擇下一步。
9. 在 [檢閱並建立] 頁面上，檢查您輸入的資訊是否正確，然後選取 [新增資料來源]。您也可以從此頁面選擇編輯您的資訊。成功新增資料來源後，您的資料來源將顯示在 [資料來源] 頁面上。

API

連接 Amazon Kendra 到 Microsoft 交易所

您必須使用 [TemplateConfiguration](#) API 指定 [資料來源結構描述](#) 的 JSON。您必須提供以下信息：

- 資料來源 — 指定使用 [TemplateConfiguration](#) JSON 結構定義 MSEXCHANGE 時的資料來源類型。同時將資料來源指定為呼叫 [CreateDataSource](#) API TEMPLATE 時的方式。
- 租用戶識別碼 — 您可以在 Azure 作用中目錄入口網站的內容或 OAuth 應用程式中找到您的租用戶識別碼。

- 同步模式 — 指定資料來源內容變更時 Amazon Kendra 應如何更新索引。當您第一次將資料來源同 Amazon Kendra 步處理時，依預設會檢索所有內容並建立索引。如果初始同步失敗，您必須執行資料的完整同步處理，即使您沒有選擇完整同步作為同步模式選項。您可以選擇：
 - FORCED_FULL_CRAWL 新建索引所有內容，並在每次資料來源與索引同步時取代現有內容。
 - FULL_CRAWL，以在每次資料來源與索引同步時，僅對新的、修改的和刪除的內容建立索引。Amazon Kendra 可以使用資料來源的機制來追蹤內容變更，並為上次同步後變更的內容建立索引。
 - CHANGE_LOG 每次資料來源與索引同步時，僅對新內容和修改的內容建立索引。Amazon Kendra 可以使用資料來源的機制來追蹤內容變更，並為上次同步後變更的內容建立索引。
- 秘密 Amazon 資源名稱 (ARN) — 提供包含您 Microsoft Exchange 帳戶身份驗證登入資料的 Secrets Manager 秘密的 Amazon 資源名稱 (ARN)。密碼會以下列金鑰儲存在 JSON 結構中：

```
{
  "clientId": "client ID",
  "clientSecret": "client secret"
}
```

- IAM 角色 — 指定 RoleArn 當您呼叫 CreateDataSource 以提供具有存取 Secrets Manager 密碼的權限的 IAM 角色，以及呼叫 Microsoft Exchange 連接器和 Amazon Kendra 所需的公用 API 的時間。如需詳細資訊，請參閱 [Microsoft Exchange 資料來源的 IAM 角色](#)。

您還可以添加以下可選功能：

- V@@ irtual Private Cloud (VPC) — 指定您撥打電話的 VpcConfiguration 時間。CreateDataSource 如需詳細資訊，請參閱 [配置 Amazon Kendra 為使用 Amazon VPC](#)。
- 包含和排除篩選器 — 指定要包含還是排除特定內容。

Note

大多數資料來源使用規則運算式模式，這些模式是稱為篩選器的包含或排除模式。如果您指定包含篩選器，則只會編製與包含項目篩選器相符的內容編製索引。不符合包含篩選器的任何文件都不會建立索引。如果您指定包含和排除篩選器，符合排除篩選器的文件將不會建立索引，即使它們符合包含篩選器也是如此。

- 存取控制清單 (ACL) — 指定是否要編目文件的 ACL 資訊 (如果您有 ACL 並且想要將其用於存取控制)。ACL 會指定使用者和群組可存取的文件。ACL 資訊可用來根據使用者或使用者對文件的群組存取權來篩選搜尋結果。如需詳細資訊，請參閱 [使用者內容篩選](#)。

- 欄位對應 — 選擇此選項可將 Microsoft 的資料來源欄位對應至 Amazon Kendra 索引欄位。如需詳細資訊，請參閱[映射資料來源欄位](#)。

Note

您的文件需要文件內文欄位或文件內文對等項目，才能搜尋您的文件。Amazon Kendra 您必須將資料來源中的文件內文欄位名稱對應至索引欄位名稱_document_body。所有其他欄位是選用的。

如需要設定的其他重要 JSON 金鑰清單，請參閱 [Microsoft Exchange 範本結構描述](#)。

進一步了解

若要深入了解如何 Amazon Kendra 與您的 Exchange Microsoft 料來源整合，請參閱：

- [使用交換連接器為您的 Microsoft 交換內容建立索引 Amazon Kendra](#)

Microsoft OneDrive

Microsoft OneDrive 是雲端式儲存服務，您可以用來儲存、共用和主控您的內容。您可以使 Amazon Kendra 用索引您的 OneDrive 資料來源。

您可以使用[Amazon Kendra 主控台](#)和 [OneDriveConfiguration](#)API 連線 Amazon Kendra 到 OneDrive 資料來源。

Amazon Kendra 有兩個版本的 OneDrive 連接器。每個版本的支援功能包括：

Microsoft OneDrive 連接器 [OneDriveConfiguration](#)

- 欄位對映
- 包含/排除過濾器

Microsoft OneDrive 連接器 [TemplateConfiguration](#)

- 使用者內容篩選
- 使用者身分搜尋器
- 包含/排除過濾器

- 完整和增量內容同步
- 虛擬私有雲端 (VPC)

Note

對 OneDrive 連接器 V1.0/ OneDriveConfiguration API 的 Support 預定於 2023 年 6 月結束。我們建議使用 OneDrive 連接器 V2.0/ TemplateConfigurationAPI。

如需對資 Amazon Kendra OneDrive 料來源連接器進行疑難排解，請參 [疑難排解資料來](#)

主題

- [Microsoft OneDrive 連接器 V1.0](#)
- [Microsoft OneDrive 連接器 V2.0](#)
- [進一步了解](#)

Microsoft OneDrive 連接器 V1.0

Microsoft OneDrive 是雲端儲存服務，您可以用來儲存、共用和主控您的內容。您可以使用 Amazon Kendra 來索引您的 Microsoft OneDrive 資料來源。

Note

對 OneDrive 連接器 V1.0/微軟 OneDrive API 的 Support 預計於 2023 年 6 月結束。我們建議使用 OneDrive 連接器 V2.0/ TemplateConfiguration API。

如需對資 Amazon Kendra OneDrive 料來源連接器進行疑難排解，請參 [疑難排解資料來](#)

主題

- [支援的功能](#)
- [必要條件](#)
- [連接說明](#)

支援的功能

- 欄位對映
- 包含/排除過濾器

必要條件

在您可以用來 Amazon Kendra 為資料來源建立索引之前，請先在 OneDrive 和 AWS 帳戶中進行這些變更。

在您的 Azure 活動目錄 (AD) 中，請確保您具有：

- 創建了一個 Azure 活動目錄 (AD) 的應用程式。
- 使用 AD 應用程式 ID 為 AD 網站上的應用程式註冊秘密金鑰。密鑰必須包含應用程式 ID 和密鑰。
- 複製組織的 AD 網域。
- 將下列應用程式權限新增至您的 AD 應用程式的 Microsoft 圖形選項：
 - 讀取所有網站集中的檔案 (檔案 .Read.All)
 - 閱讀所有用戶的完整個人資料 (用戶 .Read.All)
 - 讀取目錄資料 (目錄讀取全部)
 - 讀取所有群組 (群組閱讀全部)
 - 讀取所有網站集中的項目 (網站 .Read.All)
- 複製其文件必須編製索引的使用者清單。您可以選擇提供使用者名稱清單，也可以在儲存於 Amazon S3。建立資料來源之後，您可以：
 - 修改使用者清單。
 - 從使用者清單變更為儲存在值區中的 Amazon S3 清單。
 - 變更使用者清單的 Amazon S3 值區位置。如果您變更值區位置，也必須更新資料來源的 IAM 角色，以便資料來源具有值區的存取權。

Note

如果您將使用者名稱清單儲存在 Amazon S3 值區中，資料來源的 IAM 政策必須提供儲存貯體的存取權，以及儲存貯體使用加密金鑰的存取權 (如果有的話)。

- 已勾選的每個文件在您打算用於相同索引的其他資料來源中 OneDrive 和其他資料來源之間都是唯一的。您要用於索引的每個資料來源不得包含跨資料來源的相同文件。文件 ID 對索引來說是全域的，而且每個索引必須是唯一的。

在您的中 AWS 帳戶，請確保您有：

- [建立 Amazon Kendra 索引](#)，如果使用 API，則會記下索引識別碼。
- 為您的[資料來源建立 IAM 角色](#)，如果使用 API，則會記錄 IAM 角色的 ARN。

Note

如果您變更驗證類型和認證，則必須更新 IAM 角色以存取正確的 AWS Secrets Manager 密碼 ID。

- 將您的 OneDrive 身份驗證憑據存儲在 AWS Secrets Manager 密鑰中，如果使用 API，則記錄密鑰的 ARN。

Note

我們建議您定期重新整理或輪換您的認證和密碼。僅為您自己的安全提供必要的訪問級別。我們不建議您跨資料來源以及連接器 1.0 和 2.0 版 (如果適用) 重複使用認證和密碼。

如果您沒有現有的 IAM 角色或密碼，則可以在將 OneDrive 資料來源連線到時使用主控台建立新 IAM 角色和 Secrets Manager 密碼 Amazon Kendra。如果您使用 API，則必須提供現有 IAM 角色和 Secrets Manager 密碼的 ARN 以及索引 ID。

連接說明

若要連線 Amazon Kendra 到 OneDrive 資料來源，您必須提供 OneDrive 認證的詳細資料，Amazon Kendra 以便能夠存取您的資料。如果您尚未設定「Amazon Kendra 請 OneDrive 參閱[必要條件](#)」。

Console

若要連線 Amazon Kendra 到 OneDrive


1. 登入 AWS Management Console 並開啟[Amazon Kendra 主控台](#)。
2. 在左側導覽窗格中，選擇 [索引]，然後從索引清單中選擇要使用的索引。

Note

您可以選擇在索引設置下配置或編輯用戶訪問控制設置。

3. 在 [開始使用] 頁面上，選擇 [新增資料來源]。

4. 在 [新增資料來源] 頁面上，選擇 [OneDrive 連接器]，然後選擇 [新增連接器]。如果使用版本 2 (如果適用)，請選擇帶有「V2.0」標籤的 OneDrive 連接器。
5. 在 [指定資料來源詳細資訊] 頁面上，輸入下列資訊：
 - a. 在名稱和說明中，對於資料來源名稱 — 輸入資料來源的名稱。您可以包含連字號，但不能包含空格。
 - b. (選擇性) 說明 — 輸入資料來源的選用說明。
 - c. 在預設語言中 — 選擇一種語言來篩選索引的文件。除非另有指定，否則語言預設為英文。文件中繼資料中指定的語言會覆寫選取的語言。
 - d. 在「標籤」中，針對「新增標籤」 — 包含可選標籤以搜尋和篩選資源或追蹤 AWS 成本。
 - e. 選擇下一步。
6. 在 [定義存取和安全性] 頁面上，輸入下列資訊：
 - a. OneDrive 承租人識別碼 — 輸入不含通訊協定的 OneDrive 承租人識別碼。
 - b. 驗證類型 — 選擇 [新增] 和 [現有]。
 - c.
 - i. 如果您選擇現有密碼，請為選取密碼選取現有的密碼。
 - ii. 如果您選擇 [新增]，請在 [新 AWS Secrets Manager 密碼] 區段中輸入下列資訊：
 - A. 秘密名稱 — 您秘密的名稱。前綴 'AmazonKendraOneDrive-' 會自動添加到您的密碼名稱中。
 - B. 對於應用程式 ID 和應用程式密碼 — 輸入您 OneDrive 帳戶中的驗證認證值，然後選擇 [儲存驗證]。
 - d. IAM role — 選擇現有 IAM 角色或建立新 IAM 角色以存取存放庫認證和索引內容。

 **Note**

IAM 用於索引的角色不能用於資料來源。如果您不確定索引或常見問題集是否使用現有角色，請選擇 [建立新角色] 以避免發生錯誤。
 - e. 選擇下一步。
7. 在 [設定同步設定] 頁面上，輸入下列資訊：
 - a. 根據您的用例在列表文件和名稱列表之間進行選擇。
 - i. 如果您選擇「列出檔案」，請輸入下列資訊：
 - 選取位置 — 輸入 Amazon S3 值區的路徑。

將使用者清單檔案新增至 Amazon S3 — 選取以將使用者清單檔案新增至 Amazon S3 儲存貯體。

使用者本機群組對應 — 選取此選項可使用本機群組對應來篩選您的內容。

ii. 如果您選擇「名稱」清單，請輸入下列資訊：

- 使用者名稱 — 輸入最多 10 個要建立索引的使用者磁碟機。要添加 10 個以上的用戶，請創建一個包含名稱的文件。

新增其他 — 選擇新增更多使用者。

使用者本機群組對應 — 選取此選項可使用本機群組對應來篩選您的內容。

- b. 對於其他組態 — 新增規則運算式模式以包含或排除某些檔案。您最多可以添加 100 個圖案。
- c. 在同步執行排程中，對於頻率 — 選擇與資料來源同步的頻率。Amazon Kendra
- d. 選擇下一步。

8. 在 [設定欄位對映] 頁面上，輸入下列資訊：

- a. 對於「預設資料來源欄位」和「其他建議的欄位對映」 — 從 Amazon Kendra 產生的預設資料來源欄位中選取要對映至索引的資料來源欄位。
- b. 選擇下一步。

9. 在 [檢閱並建立] 頁面上，檢查您輸入的資訊是否正確，然後選取 [新增資料來源]。您也可以從此頁面選擇編輯您的資訊。成功新增資料來源後，您的資料來源將顯示在 [資料來源] 頁面上。

API

若要連線 Amazon Kendra 到 OneDrive

您必須使用 [OneDriveConfiguration](#) API 指定下列項目：

- 租用戶識別碼 — 指定組織的 Azure 作用中目錄網域。
- OneDrive 使用者 — 指定應為其文件編製索引的使用者帳戶清單。
- 秘密 Amazon 資源名稱 (ARN) — 提供包含您帳戶身份驗證登入資料的 Secrets Manager 密碼的 Amazon 資源名稱 (ARN)。OneDrive 密碼會以下列金鑰儲存在 JSON 結構中：

```
{  
  "username": "OAuth client ID",
```



```
"password": "client secret"
}
```

- IAM role — 指定RoleArn何時呼叫CreateDataSource以提供具有存取 Secrets Manager 密碼之權限的 IAM 角色，以及呼叫 OneDrive 連接器和 Amazon Kendra所需公用 API 的時間。有關詳情，請參閱[資 OneDrive 料來源的IAM 角色](#)。

您還可以添加以下可選功能：

- 包含和排除篩選器 — 指定要包含還是排除某些文件。

Note

大多數資料來源使用規則運算式模式，這些模式是稱為篩選器的包含或排除模式。如果您指定包含篩選器，則只有符合包含項目篩選器的內容會編製索引。不符合包含篩選器的任何文件都不會建立索引。如果您指定包含和排除篩選器，符合排除篩選器的文件將不會建立索引，即使它們符合包含篩選器也是如此。

- 欄位對映 — 選擇將資 OneDrive 料來源欄位對映至 Amazon Kendra 索引欄位。如需詳細資訊，請參閱[映射資料來源欄位](#)。

Note

您的文件需要文件內文欄位或文件內文對等項目，才能搜尋您的文件。Amazon Kendra 您必須將資料來源中的文件內文欄位名稱對應至索引欄位名稱_document_body。所有其他欄位是選用的。

- 使用者前後關聯篩選與存取控制 — Amazon Kendra 探索文件的存取控制清單 (ACL) (如果您有文件的 ACL)。ACL 資訊可用來根據使用者或使用者對文件的群組存取來篩選搜尋結果。如需詳細資訊，請參閱[使用者內容篩選](#)。

Microsoft OneDrive 連接器 V2.0

Microsoft OneDrive 是雲端式儲存服務，您可以用來儲存、共用和主控您的內容。您可以使 Amazon Kendra 用索引您的 OneDrive資料來源。

您可以使用[Amazon Kendra 主控台](#)和 [OneDriveConfiguration](#)API 連線 Amazon Kendra 到 OneDrive 資料來源。

Note

對 OneDrive 連接器 1.0/ OneDriveConfiguration API 的 Support 預定於 2023 年 6 月結束。我們建議您使用 OneDrive 連接器 V2.0/ TemplateConfiguration API。2.0 版提供了額外的 ACL 和身份編目器功能。

如需對 Amazon Kendra OneDrive 資料來源連接器進行疑難排解，請參 [疑難排解資料來](#)

主題

- [支援的功能](#)
- [必要條件](#)
- [連接說明](#)

支援的功能

Amazon Kendra OneDrive 資料來源連接器支援下列功能：

- 欄位對映
- 使用者存取控制
- 包含/排除過濾器
- 完整和增量內容同步
- 虛擬私有雲端 (VPC)

必要條件

在您可以用來 Amazon Kendra 為 OneDrive 資料來源建立索引之前，請先在 OneDrive 和 AWS 帳戶中進行這些變更。

在中 OneDrive，請確定您有：

- 在辦公室 365 中創建了一個 OneDrive 帳戶。
- 記下您的 Microsoft 365 租戶識別碼。您可以在 Azure 作用中目錄入口網站的內容或 OAuth 應用程式中找到您的租用戶識別碼。
- 在 Azure 入口網站中建立 OAuth 應用程式，並記下用於驗證密碼的用戶端識別碼和用戶端 AWS Secrets Manager 密碼或用戶端認證。如需詳細資訊，請參閱 [Microsoft 教學課程](#) 和 [已註冊應用程式](#)

Note

當您在 Azure 入口網站中建立或註冊應用程式時，秘密識別碼代表實際的密碼值。建立密碼和應用程式時，您必須立即記下或儲存實際的密碼值。您可以在 Azure 入口網站中選取應用程式的名稱，然後導覽至憑證和密碼上的功能表選項，以存取您的密碼。

您可以在 Azure 入口網站中選取應用程式的名稱，然後導覽至概觀頁面，以存取用戶端識別碼。應用程式 (客戶端) ID 是客戶端 ID。

Note

我們建議您定期重新整理或輪換您的認證和密碼。僅為您自己的安全提供必要的訪問級別。我們不建議您跨資料來源以及連接器 1.0 和 2.0 版 (如果適用) 重複使用認證和密碼。

- 使用 AD 應用程式 ID 為 AD 網站上的應用程式註冊秘密金鑰。密鑰必須包含應用程式 ID 和密鑰。
- 複製組織的 AD 網域。
- 新增下列權限到您的 AD 應用程式上的 Microsoft 圖形選項：
 - 讀取所有網站集合中的檔案 (檔案 .Read.All)
 - 閱讀所有用戶的完整配置文件 (用戶 .Read.All)
 - 讀取所有群組 (群組閱讀全部)
 - 閱讀所有筆記 (注意. 閱讀全部)
- 複製其文件必須編製索引的使用者清單。您可以選擇提供使用者名稱清單，也可以在儲存於 Amazon S3. 建立資料來源之後，您可以：
 - 修改使用者清單。
 - 從使用者清單變更為儲存在值區中的 Amazon S3 清單。
 - 變更使用者清單的 Amazon S3 值區位置。如果您變更值區位置，也必須更新資料來源的 IAM 角色，以便資料來源具有值區的存取權。

Note

如果您將使用者名稱清單儲存在 Amazon S3 值區中，資料來源的 IAM 政策必須提供儲存貯體的存取權，以及儲存貯體使用加密金鑰的存取權 (如果有的話)。

OneDrive 連接器使用 OneDrive 使用者內容中存在的連絡人資訊中的電子郵件。確保您要檢索其數據的用戶在「聯繫信息」頁面中配置了電子郵件字段，因為對於新用戶而言，這可能是空白的。

在您的 AWS 帳戶中，請確定您有：

- 創建了一個 Amazon Kendra 索引，如果使用 API，則註明索引 ID。
- 為您的資料來源建立 IAM 角色，如果使用 API，則會記錄 IAM 角色的 ARN。
- 將您的 OneDrive 身份驗證憑據存儲在 AWS Secrets Manager 密鑰中，如果使用 API，則記錄密鑰的 ARN。

如果您沒有現有的 IAM 角色或密碼，則可以在將 OneDrive 資料來源連線到時使用主控台建立新 IAM 角色和 Secrets Manager 密碼 Amazon Kendra。如果您使用 API，則必須提供現有 IAM 角色和 Secrets Manager 密碼的 ARN 以及索引 ID。

連接說明

若要連線 Amazon Kendra 到 OneDrive 資料來源，您必須提供 OneDrive 認證的詳細資料，Amazon Kendra 以便能夠存取您的資料。如果您尚未配置 Amazon Kendra，OneDrive 請參閱[必要條件](#)。

Console

若要連線 Amazon Kendra 到 OneDrive

1. 登入 AWS Management Console 並開啟[Amazon Kendra 主控台](#)。
2. 在左側導覽窗格中，選擇 [索引]，然後從索引清單中選擇要使用的索引。

Note

您可以選擇在索引設置下配置或編輯用戶訪問控制設置。

3. 在 [開始使用] 頁面上，選擇 [新增資料來源]。
4. 在 [新增資料來源] 頁面上，選擇 [OneDrive 連接器]，然後選擇 [新增連接器]。如果使用版本 2 (如果適用)，請選擇帶有「V2.0」標籤的 OneDrive 連接器。
5. 在 [指定資料來源詳細資訊] 頁面上，輸入下列資訊：

- a. 在名稱和說明中，對於資料來源名稱 — 輸入資料來源的名稱。您可以包含連字號，但不能包含空格。
 - b. (選擇性) 說明 — 輸入資料來源的選用說明。
 - c. 在預設語言中 — 選擇一種語言來篩選索引的文件。除非另有指定，否則語言預設為英文。文件中繼資料中指定的語言會覆寫選取的語言。
 - d. 在「標籤」中，針對「新增標籤」 — 包含可選標籤以搜尋和篩選資源或追蹤 AWS 成本。
 - e. 選擇下一步。
6. 在 [定義存取和安全性] 頁面上，輸入下列資訊：
- a. OneDrive 承租人識別碼 — 輸入不含通訊協定的 OneDrive 承租人識別碼。
 - b. 授權 — 開啟或關閉文件的存取控制清單 (ACL) 資訊 (如果您有 ACL)，且想要將其用於存取控制。ACL 會指定使用者和群組可存取的文件。ACL 資訊可用來根據使用者或使用者對文件的群組存取來篩選搜尋結果。如需詳細資訊，請參閱[使用者內容篩選](#)。
 - c. 在驗證中 — 選擇 [新增] 和 [現有]。
 - d.
 - i. 如果您選擇現有密碼，請為選取密碼選取現有的密碼。
 - ii. 如果您選擇 [新增]，請在 [新 AWS Secrets Manager 密碼] 區段中輸入下列資訊：
 - A. 秘密名稱 — 您秘密的名稱。前綴 'AmazonKendraOneDrive-' 會自動添加到您的密碼名稱中。
 - B. 對於用戶端 ID 和用戶端密碼 — 輸入用戶端 ID 和用戶端密碼。
 - e. V@@@ irtual Private Cloud (VPC) (VPC) — 您可以選擇使用 VPC。如果是這樣，您必須新增子網路和 VPC 安全性群組。
 - f. 識別爬行者程式 — 指定是否要開啟身分爬行 Amazon Kendra 者程式。識別爬行者程式會使用文件的存取控制清單 (ACL) 資訊，根據使用者或使用者對文件的群組存取權來篩選搜尋結果。如果您有文件的 ACL 並選擇使用 ACL，您也可以選擇開啟的身分識別爬行者程式，以設定搜尋結果的使用者[環境定義篩選](#)。Amazon Kendra 否則，如果關閉身分搜索器，則可以公開搜索所有文檔。如果您想要對文件使用存取控制，且身分識別編目程式已關閉，您也可以使用 [PutPrincipalMapping](#) API 來上傳使用者和群組存取資訊以進行使用者內容篩選。
 - g. IAM role — 選擇現有 IAM 角色或建立新 IAM 角色以存取存放庫認證和索引內容。

Note

IAM 用於索引的角色不能用於資料來源。如果您不確定索引或常見問題集是否使用現有角色，請選擇 [建立新角色] 以避免發生錯誤。

- h. 選擇下一步。
7. 在 [設定同步設定] 頁面上，輸入下列資訊：
 8. a. 針對同步範圍 — 選擇要編製索引的使用者 OneDrive 資料。您最多可以手動新增 10 個使用者。
 - b. 對於其他組態 — 新增規則運算式模式以包含或排除某些內容。您最多可以添加 100 個圖案。
 - c. 同步模式 — 選擇資料來源內容變更時要如何更新索引。當您第一次將資料來源同 Amazon Kendra 步處理時，依預設會檢索所有內容並建立索引。如果初始同步失敗，您必須執行資料的完整同步，即使您沒有選擇完整同步作為同步模式選項。
 - 完全同步：新鮮索引所有內容，並在每次資料來源與索引同步時取代現有內容。
 - 新增、修改的同步：每次資料來源與索引同步時，僅對新內容和已修改的內容建立索引。Amazon Kendra 可以使用資料來源的機制來追蹤內容變更，並為上次同步後變更的內容建立索引。
 - 新增、修改、刪除的同步：每次資料來源與索引同步時，僅對新內容、已修改和刪除的內容建立索引。Amazon Kendra 可以使用資料來源的機制來追蹤內容變更，並為上次同步後變更的內容建立索引。
 - d. 在同步執行排程中，對於頻率 — 選擇同步資料來源內容和更新索引的頻率。
 - e. 選擇下一步。
9. 在 [設定欄位對映] 頁面上，輸入下列資訊：
 - a. 預設資料來源欄位 — 從 Amazon Kendra 產生的預設資料來源欄位中選取您要對映至索引的資料來源欄位。
 - b. 選擇下一步。
10. 在 [檢閱並建立] 頁面上，檢查您輸入的資訊是否正確，然後選取 [新增資料來源]。您也可以從此頁面選擇編輯您的資訊。成功新增資料來源後，您的資料來源將顯示在 [資料來源] 頁面上。

API

若要連線 Amazon Kendra 到 OneDrive

您必須使用 [TemplateConfiguration](#) API 指定 [資料來源結構描述](#) 的 JSON。您必須提供以下信息：

- 資料來源 — 指定使用 [TemplateConfiguration](#) JSON 結構定義 ONEDRIVEV2 時的資料來源類型。同時指定呼叫 [CreateDataSource](#) API TEMPLATE 時的資料來源。
- 租用戶識別碼 — 指定 Microsoft 365 租用戶識別碼。您可以在 Azure 作用中目錄入口網站的內容或 OAuth 應用程式中找到您的租用戶識別碼。
- 同步模式 — 指定資料來源內容變更時 Amazon Kendra 應如何更新索引。當您第一次將資料來源同 Amazon Kendra 步處理時，依預設會檢索所有內容並建立索引。如果初始同步失敗，您必須執行資料的完整同步，即使您沒有選擇完整同步作為同步模式選項。您可以選擇：
 - FORCED_FULL_CRAWL 新建索引所有內容，並在每次資料來源與索引同步時取代現有內容。
 - FULL_CRAWL，以在每次資料來源與索引同步時，僅對新的、修改的和刪除的內容建立索引。Amazon Kendra 可以使用資料來源的機制來追蹤內容變更，並為上次同步後變更的內容建立索引。
 - CHANGE_LOG 每次資料來源與索引同步時，僅對新內容和修改的內容建立索引。Amazon Kendra 可以使用資料來源的機制來追蹤內容變更，並為上次同步後變更的內容建立索引。
- 秘密 Amazon 資源名稱 (ARN) — 提供包含您在帳戶中建立的身份驗證登入資料的 Secrets Manager 密碼的 Amazon 資源名稱 (ARN)。OneDrive

如果您使用 OAuth 2.0 驗證，則密碼會以下列金鑰儲存在 JSON 結構中：

```
{
  "clientId": "client ID",
  "clientSecret": "client secret"
}
```

- IAM role — 指定 RoleArn 何時呼叫 CreateDataSource 以提供具有存取 Secrets Manager 密碼之權限的 IAM 角色，以及呼叫 OneDrive 連接器和 Amazon Kendra 所需公用 API 的時間。有關詳情，請參閱 [資料來源的 IAM 角色](#)。

您還可以添加以下可選功能：

- Virtual Private Cloud (VPC) — 指定您呼叫的 VpcConfiguration 時間。CreateDataSource 如需詳細資訊，請參閱 [配置 Amazon Kendra 為使用 Amazon VPC](#)。
- 包含和排除篩選器 — 您可以指定是否要包含或排除特定檔案、OneNote 區段和 OneNote 頁面。

Note

大多數資料來源使用規則運算式模式，這些模式是稱為篩選器的包含或排除模式。如果您指定包含篩選器，則只有符合包含項目篩選器的內容會編製索引。不符合包含篩選器的任何文件都不會建立索引。如果您指定包含和排除篩選器，符合排除篩選器的文件將不會建立索引，即使它們符合包含篩選器也是如此。

- 識別爬行者程式 — 指定是否要開啟身分爬行者 Amazon Kendra 程式。識別爬行者程式會使用文件的存取控制清單 (ACL) 資訊，根據使用者或使用者對文件的群組存取權來篩選搜尋結果。如果您有文件的 ACL 並選擇使用 ACL，您也可以選擇開啟的身分識別爬行者程式，以設定搜尋結果的使用者環境定義篩選。Amazon Kendra 否則，如果關閉身分搜索器，則可以公開搜索所有文檔。如果您想要對文件使用存取控制，且身分識別編目程式已關閉，您也可以使用 [PutPrincipalMapping](#) API 來上傳使用者和群組存取資訊以進行使用者內容篩選。
- 欄位對映 — 您只能對應 Amazon Kendra OneDrive 連接器的內建索引欄位或一般索引欄位。由於 API 限制，OneDrive 連接器無法使用自訂欄位對應。如需詳細資訊，請參閱 [映射資料來源欄位](#)。

如需要設定的其他重要 JSON 金鑰清單，請參閱 [OneDrive 範本結構定義](#)。

進一步了解

若要進一步瞭解 Amazon Kendra 與 OneDrive 資料來源整合的相關資訊，請參閱：

- [宣布更新的 Microsoft OneDrive 連接器 \(V2 \) 的 Amazon Kendra](#).

Microsoft SharePoint

SharePoint 是一種協作式網站建置服務，您可以使用它來自訂網頁內容和建立頁面、網站、文件庫和清單。您可以使 Amazon Kendra 用索引您的 SharePoint 資料來源。

Amazon Kendra 目前支援 SharePoint 線上和 SharePoint 伺服器 (版本 2013、2016 年、2019 年和訂閱版)。

您可以使用 [Amazon Kendra 主控台](#)、API 或 [TemplateConfiguration](#) API 連線 Amazon Kendra 到 SharePoint 資料來源。 [SharePointConfiguration](#)

Amazon Kendra 有兩個版本的 SharePoint 連接器。每個版本的支援功能包括：

SharePoint 連接器 [SharePointConfiguration](#)

- 欄位對映
- 使用者存取控制
- 包含/排除過濾器
- 變更日誌
- 虛擬私有雲端 (VPC)

SharePoint 連接器 2.0 版/[TemplateConfiguration](#)接口

- 欄位對映
- 使用者存取控制
- 包含/排除過濾器
- 完整和增量內容同步
- 虛擬私有雲端 (VPC)

Note

對 SharePoint 連接器 V1.0/ SharePointConfiguration API 的 Support 預定於 2023 年結束。我們建議您移轉至或使用 SharePoint 連接器 V2.0/ TemplateConfiguration API。

如需疑難排解資 Amazon Kendra SharePoint 料來源連接器，請參閱[疑難排解資料來](#)。

主題

- [SharePoint 連接器 1.0 版](#)
- [SharePoint 連接器 2.0 版](#)

SharePoint 連接器 1.0 版

SharePoint 是一種協作式網站建置服務，您可以使用它來自訂網頁內容和建立頁面、網站、文件庫和清單。如果您是使用 SharePoint 者，則可以使用 Amazon Kendra 對資 SharePoint 料來源建立索引。

Note

對 SharePoint 連接器 V1.0/ SharePointConfiguration API 的 Support 預定於 2023 年結束。我們建議您移轉至或使用 SharePoint 連接器 V2.0/ TemplateConfiguration API。

如需疑難排解資 Amazon Kendra SharePoint 料來源連接器，請參閱[疑難排解資料來](#)。

主題

- [支援的功能](#)
- [必要條件](#)
- [連接說明](#)
- [進一步了解](#)

支援的功能

- 欄位對映
- 使用者存取控制
- 包含/排除過濾器
- 變更日誌
- 虛擬私有雲端 (VPC)

必要條件

在您可以用來 Amazon Kendra 為資 SharePoint 料來源建立索引之前，請先在 SharePoint 和 AWS 帳戶中進行這些變更。

您需要提供身份驗證憑據，您可以安全地將其存儲在 AWS Secrets Manager 密碼中。

Note

我們建議您定期重新整理或輪換您的認證和密碼。僅為您自己的安全提供必要的訪問級別。我們不建議您跨資料來源以及連接器 1.0 和 2.0 版 (如果適用) 重複使用認證和密碼。

在中 SharePoint，請確定您有：

- 記下您要索引的 SharePoint 網站的 URL。
- 對於 SharePoint 在線：
 - 記下您的基本驗證憑證，其中包含具有網站管理員權限的使用者名稱和密碼
 - 可選：產生包含使用者名稱、密碼、用戶端 ID 和用戶端密碼的 OAuth 2.0 認證。
 - 使用系統管理使用者停用 Azure 入口網站中的安全性預設值。如需在 Azure 入口網站中管理安全性預設設定的詳細資訊，請參閱 [Microsoft 說明文件](#)，瞭解如何啟用/停用安全性預設
- 對於 SharePoint 伺服器：
 - 記下您的 SharePoint 伺服器網域名稱 (您的作用中目錄中的 NetBIOS 名稱)。您可以使用此連接到 SharePoint 伺服器的 SharePoint 基本驗證使用者名稱和密碼 Amazon Kendra。

Note

如果您使用 SharePoint 伺服器且需要將存取控制清單 (ACL) 轉換為電子郵件格式，以便篩選使用者內容，請提供 LDAP 伺服器 URL 和 LDAP 搜尋庫。或者，您可以使用目錄域覆蓋。LDAP 伺服器網址是完整的網域名稱和連接埠號碼 (例如，`ldap://example.com:389`)。LDAP 搜尋基礎是網域控制站的「範例」和「com」。透過目錄網域覆寫，您可以使用電子郵件網域，而不是使用 LDAP 伺服器 URL 和 LDAP 搜尋庫。舉例來說，`username@example.com` 的電子郵件網域是「例子網站」。如果您不擔心驗證網域，而只是想要使用電子郵件網域，可以使用此覆寫。

- 已新增下列權限至您的 SharePoint 帳戶：

對於 SharePoint 列表

- 開啟項目 — 使用伺服器端檔案處理常式檢視文件來源。
- 檢視應用程式頁面 — 檢視表單、檢視表和應用程式頁面。枚舉列表。
- 檢視項目-檢視清單中的項目，以及文件庫中的文件。
- 檢視版本 — 檢視清單項目或文件的舊版本。


對於 SharePoint 網站

- 瀏覽目錄 — 使用 SharePoint 設計師和 Web DAV 介面列舉網站中的檔案和資料夾。
- 瀏覽使用者資訊 — 檢視有關網站使用者的資訊。
- 列舉權限 — 列舉網站、清單、資料夾、文件或清單項目的權限。
- 開啟 — 開啟網站、清單或資料夾以存取容器內的項目。
- 使用用戶端整合功能 — 使用 SOAP、WebDAV、用戶端物件模型或 SharePoint 設計工具介面來存取網站。

- 使用遠端介面 — 使用啟動用戶端應用程式的功能。
- 檢視頁面 — 檢視網站上的頁面。
- 已勾選的每個文件在您打算用於相同索引的其他資料來源中 SharePoint 和其他資料來源之間都是唯一的。您要用於索引的每個資料來源不得包含跨資料來源的相同文件。文件 ID 對索引來說是全域的，而且每個索引必須是唯一的。


在你的 AWS 帳戶，確保你有：

- [建立 Amazon Kendra 索引](#)，如果使用 API，則會記下索引 ID。
- 為您的[資料來源建立 IAM 角色](#)，如果使用 API，則會記錄 IAM 角色的 ARN。

 Note

如果您變更驗證類型和認證，則必須更新 IAM 角色才能存取正確的 AWS Secrets Manager 密碼 ID。

- 將您的 SharePoint 身份驗證憑據存儲在 AWS Secrets Manager 密鑰中，如果使用 API，則記錄密鑰的 ARN。

 Note

我們建議您定期重新整理或輪換您的認證和密碼。僅為您自己的安全提供必要的訪問級別。我們不建議您跨資料來源以及連接器 1.0 和 2.0 版 (如果適用) 重複使用認證和密碼。

如果您沒有現有的 IAM 角色或密碼，則可以在將 SharePoint 資料來源連線到時使用主控台建立新 IAM 角色和 Secrets Manager 密碼 Amazon Kendra。如果您使用 API，則必須提供現有 IAM 角色和 Secrets Manager 密碼的 ARN 以及索引 ID。


連接說明

若要連線 Amazon Kendra 到 SharePoint 資料來源，您必須提供 SharePoint 認證的詳細資料，Amazon Kendra 以便能夠存取您的資料。如果您尚未設定「Amazon Kendra 請 SharePoint 參閱[必要條件](#)」。

Console

若要連線 Amazon Kendra 到 SharePoint


1. 登入 AWS 管理主控台並開啟主 [Amazon Kendra 控制台](#)。
2. 在左側導覽窗格中，選擇 [索引]，然後從索引清單中選擇要使用的索引。

 Note

您可以選擇在索引設置下配置或編輯您的用戶訪問控制設置。


3. 在 [開始使用] 頁面上，選擇 [新增資料來源]。
4. 在 [新增資料來源] 頁面上，選擇 [SharePoint 連接器 1.0]，然後選擇 [新增資料來源]。
5. 在 [指定資料來源詳細資訊] 頁面上，輸入下列資訊：
 - a. 在名稱和說明中，對於資料來源名稱 — 輸入資料來源的名稱。您可以包含連字號，但不能包含空格。
 - b. (選擇性) 說明 — 輸入資料來源的選用說明。
 - c. 在預設語言中 — 選擇一種語言來篩選索引的文件。除非另有指定，否則語言預設為英文。文件中繼資料中指定的語言會覆寫選取的語言。
 - d. 在「標籤」中，針對「新增標籤」 — 包含可選標籤以搜尋和篩選資源或追蹤 AWS 成本。
 - e. 選擇下一步。
6. 在 [定義存取和安全性] 頁面上，輸入下列資訊：
 - a. 對於託管方法-SharePoint 在線和SharePoint服務器之間進行選擇。
 - i. 對於SharePoint線上 — 輸入 SharePoint存放庫特定的網站 URL。
 - ii. 對於SharePoint伺服器 — 選擇您的SharePoint 版本，輸入 SharePoint 存放庫特定的網站 URL，然後輸入 SSL 憑證位置的 Amazon S3 路徑。
 - b. (僅限SharePoint 伺服器) 針對 Web Proxy — 輸入內部 SharePoint 執行個體的主機名稱和連接埠號碼。連接埠號碼應該是介於 0 到 65535 之間的數值。
 - c. 對於驗證 — 根據您的使用案例在下列選項之間進行選擇：
 - i. 對於 SharePoint 線上 — 在基本驗證和 O Auth 2.0 驗證之間進行選擇。
 - ii. 對於 SharePoint 伺服器 — 選擇「無」、「LDAP」和「手動」。
 - d. 針對AWS Secrets Manager 秘密 — 選擇現有密碼或建立新 Secrets Manager 密碼來儲存您的 SharePoint驗證認證。如果您選擇建立新密碼，則會開啟一個 AWS Secrets Manager 密碼視窗。您必須輸入「機密」名稱。前綴 'AmazonKendraSharePoint-' 會自動添加到您的密碼名稱中。

- e. 在「建立 AWS Secrets Manager 密碼視窗」中輸入下列其他資訊：
 - i. 根據您的使用案例，從下列 SharePoint 雲端驗證選項中選擇：
 - A. 基本驗證 — 輸入您的 SharePoint 帳戶使用者名稱作為使用者名稱和 SharePoint 帳戶密碼作為密碼。
 - B. OAuth 2.0 驗證 — 輸入您的 SharePoint 帳戶使用者名稱作為使用者名稱、SharePoint 帳戶密碼作為密碼、自動生成的唯一 SharePoint ID 作為用戶端 ID，以及與用戶端密碼使用的共用 SharePoint 密碼字串。Amazon Kendra
 - ii. 根據您的使用案例，從下列 SharePoint 伺服器驗證選項中選擇：
 - A. 無 — 輸入您的 SharePoint 帳戶使用者名稱作為使用者名稱、您的 SharePoint 帳戶密碼作為密碼，以及您的伺服器網域名稱。
 - B. LDAP — `#### SharePoint ##### SharePoint###
##LDAP ##### (##### ldap: //example.com:389)###
LDAP ### (###dc= ## dc=com)#`
 - C. 手動 — 輸入您的 SharePoint 帳戶使用者名稱作為使用者名稱、您的 SharePoint 帳戶密碼作為密碼，以及您的電子郵件網域覆寫 (目錄使用者或群組的電子郵件網域)。
 - iii. 選擇儲存。
- f. V@@@ irtual Private Cloud (VPC) — 您還必須新增子網路和 VPC 安全性群組。

 Note

如果您使用 SharePoint 伺服器，則必須使用 VPC。Amazon VPC 對於其他 SharePoint 版本是可選的。

- g. IAM role — 選擇現有 IAM 角色或建立新 IAM 角色以存取存放庫認證和索引內容。

 Note

IAM 用於索引的角色不能用於資料來源。如果您不確定索引或常見問題集是否使用現有角色，請選擇 [建立新角色] 以避免發生錯誤。

- h. 選擇下一步。

7. 在 [設定同步設定] 頁面上，輸入下列資訊：

- a. 使用變更記錄 — 選取此選項可更新索引，而不是同步所有檔案。
 - b. 編目附件 — 選取此選項可編目附件。
 - c. 使用本機群組對映 — 選取此選項可確定已正確篩選文件。
 - d. 其他組態 — 新增規則運算式模式以包含或排除某些檔案。您最多可以添加 100 個圖案。
 - e. 頻率的同步執行排程 — 與資料來源同步的頻 Amazon Kendra 率。
 - f. 選擇下一步。
8. 在 [設定欄位對映] 頁面上，輸入下列資訊：
- a. Amazon Kendra 預設欄位對映 — 從 Amazon Kendra 產生的預設資料來源欄位中選取您要對映至索引的欄位。
 - b. 對於自訂欄位對映 — 新增自訂資料來源欄位以建立要對映的索引欄位名稱和欄位資料類型。
 - c. 選擇下一步。
9. 在 [檢閱並建立] 頁面上，檢查您輸入的資訊是否正確，然後選取 [新增資料來源]。您也可以從此頁面選擇編輯您的資訊。成功新增資料來源後，您的資料來源將顯示在 [資料來源] 頁面上。

API

若要連線 Amazon Kendra 到 SharePoint

您必須使用 [SharePointConfiguration](#) API 指定下列項目：

- SharePoint 版本 — 指定您在配置 SharePoint 時使用的 SharePoint 版本。無論您使用 SharePoint 伺服器 2013、伺服器 2016 年、SharePoint 伺服器 2019 年或 SharePoint 線上，SharePoint 都是這種情況。
- 秘密 Amazon 資源名稱 (ARN) — 提供機密的 Amazon 資源名稱 (ARN)，其中包含您在 SharePoint 帳戶中建立的身份驗證登入資料。密碼儲存在 JSON 結構中。Secrets Manager

對於 SharePoint 線上基本驗證，以下是您密碼中必須包含的最低 JSON 結構：

```
{
  "userName": "user name",
  "password": "password"
}
```

對於在 SharePoint 線 OAuth 2.0 身份驗證，以下是必須在您的密鑰中的最低 JSON 結構：

```
{
  "userName": "SharePoint account user name",
  "password": "SharePoint account password",
  "clientId": "SharePoint auto-generated unique client id",
  "clientSecret": "secret string shared by Amazon Kendra and SharePoint to
  authorize communications"
}
```

對於SharePoint 服務器基本身份驗證，以下是必須在您的密鑰中的最小 JSON 結構：

```
{
  "userName": "user name",
  "password": "password",
  "domain": "server domain name"
}
```

對於SharePoint 伺服器 LDAP 驗證 (如果您需要將存取控制清單 (ACL) 轉換為電子郵件格式以篩選使用者內容，您可以在密碼中包含 LDAP 伺服器 URL 和 LDAP 搜尋庫)，以下是必須在密碼中的最低 JSON 結構：

```
{
  "userName": "user name",
  "password": "password",
  "domain": "server domain name"
  "ldapServerUrl": "ldap://example.com:389",
  "ldapSearchBase": "dc=example,dc=com"
}
```

對於SharePoint 伺服器手動驗證，以下是密碼中必須包含的最低 JSON 結構：


```
{
  "userName": "user name",
  "password": "password",
  "domain": "server domain name",
  "emailDomainOverride": "example.com"
}
```

- IAM role — 指定RoleArn何時呼叫CreateDataSource以提供具有存取 Secrets Manager 密碼之權限的 IAM 角色，以及呼叫 SharePoint 連接器和 Amazon Kendra所需公用 API 的時間。有關詳情，請參閱資 [SharePoint 料來源的IAM 角色](#)。

- Amazon VPC如果您使用「SharePoint 伺服器」，請指定VpcConfiguration為資料來源組態的一部分。請參閱[設 Amazon Kendra 定以使用 VPC](#)。


您還可以添加以下可選功能：

- 網頁代理伺服器 — 是否透過網路代理連線到您的網 SharePoint 站 URL。您只能將此選項用於 SharePoint 伺服器。
- 索引列表 — 是否 Amazon Kendra 應將附件的內容索引到 SharePoint 列表項目中。
- 變更記錄 — 是否 Amazon Kendra 應該使用 SharePoint 資料來源變更記錄機制來判斷是否必須在索引中更新文件。

 Note


如果您不想 Amazon Kendra 掃描所有文檔，請使用更改日誌。如果變更記錄檔很大，掃描 SharePoint 資料來源中的文件所需的時間可能會比處理變更記錄還要 Amazon Kendra 少。如果您是第一次將 SharePoint 資料來源與索引同步，則會掃描所有文件。

- 包含和排除篩選器 — 您可以指定要包含還是排除某些內容。

 Note

大多數資料來源使用規則運算式模式，這些模式是稱為篩選器的包含或排除模式。如果您指定包含篩選器，則只有符合包含項目篩選器的內容會編製索引。不符合包含篩選器的任何文件都不會建立索引。如果您指定包含和排除篩選器，符合排除篩選器的文件將不會建立索引，即使它們符合包含篩選器也是如此。

- 欄位對映 — 選擇將資 SharePoint 料來源欄位對映至 Amazon Kendra 索引欄位。如需詳細資訊，請參閱[映射資料來源欄位](#)。

 Note

您的文件需要文件內文欄位或文件內文對等項目，才能搜尋您的文件。Amazon Kendra 您必須將資料來源中的文件內文欄位名稱對應至索引欄位名稱_document_body。所有其他欄位是選用的。

- 使用者前後關聯篩選與存取控制 —Amazon Kendra 探索文件的存取控制清單 (ACL) (如果您有文件的 ACL)。ACL 資訊可用來根據使用者或使用者對文件的群組存取權來篩選搜尋結果。如需詳細資訊，請參閱[使用者內容篩選](#)。

進一步了解

若要進一步瞭解 Amazon Kendra 與 SharePoint 資料來源整合的相關資訊，請參閱：

- [開始使用 Amazon Kendra SharePoint 線上連接器](#)

SharePoint 連接器 2.0 版

SharePoint 是一種協作式網站建置服務，您可以使用它來自訂網頁內容和建立頁面、網站、文件庫和清單。您可以使 Amazon Kendra 用索引您的 SharePoint 資料來源。

Amazon Kendra 目前支持 SharePoint 在線和 SharePoint 服務器 (2013 年，2016 年，2019 和訂閱版)。

Note

對 SharePoint 連接器 V1.0/ SharePointConfiguration API 的 Support 預定於 2023 年結束。我們建議您移轉至或使用 SharePoint 連接器 V2.0/ TemplateConfiguration API。

如需疑難排解資 Amazon Kendra SharePoint 料來源連接器，請參閱[疑難排解資料來](#)。

主題

- [支援的功能](#)
- [必要條件](#)
- [連接說明](#)
- [備註](#)

支援的功能

Amazon Kendra SharePoint 資料來源連接器支援下列功能：

- 欄位對映
- 使用者存取控制

- 包含/排除過濾器
- 完整和增量內容同步
- 虛擬私有雲端 (VPC)

必要條件

在您可以用來 Amazon Kendra 為資料來源建立索引之前，請先在 SharePoint 和 AWS 帳戶中進行這些變更。

您需要提供身份驗證憑據，您可以安全地將其存儲在 AWS Secrets Manager 密碼中。

Note

我們建議您定期重新整理或輪換您的認證和密碼。僅為您自己的安全提供必要的訪問級別。我們不建議您跨資料來源以及連接器 1.0 和 2.0 版 (如果適用) 重複使用認證和密碼。

在「SharePoint 線上」中，確定您有：

- 已複製您的 SharePoint 執行個體 URL。您輸入的主機網址格式為 `https://yourdomain.sharepoint.com/sites/mysite`。您的網址必須以開頭 https 並包含 sharepoint.com。
- 已複製 SharePoint 執行個體 URL 的網域名稱。
- 記下您的基本驗證認證，其中包含使用者名稱和密碼，並具有網站管理員權限以連 SharePoint 線到線上。
- 使用系統管理使用者停用 Azure 入口網站中的安全性預設值。如需在 Azure 入口網站中管理安全性預設設定的詳細資訊，請參閱 [Microsoft 說明文件](#)，瞭解如何啟用/停用安全性預設。
- 停用您 SharePoint 帳戶中的多重要素驗證 (MFA)，因此不會 Amazon Kendra 封鎖檢索您的內容。
SharePoint
- 如果使用基本驗證以外的驗證類型：已複製 SharePoint 執行個體的租用戶 ID。如需如何尋找您的租用戶識別碼的詳細資訊，請參閱 [尋找您的 Microsoft 365 租用戶識別碼](#)。
- 如果您需要使用 Microsoft Entra 遷移到雲端使用者驗證，請參閱 [雲端驗證的 Microsoft 文件](#)。
- 對於 OAuth 2.0 驗證和 OAuth 2.0 重新整理權杖驗證：記下您的基本驗證認證，其中包含用於連線至 SharePoint 線上的使用者名稱和密碼，以及在 Azure AD 註冊後產生的用戶端識別碼和 SharePoint 用戶端密碼。
 - 如果您未使用 ACL，請新增下列權限：

Microsoft 圖	SharePoint
<ul style="list-style-type: none"> • 備註 .Read. All (應用程式) — 讀取所有筆記本 OneNote • Site.Read.All (應用程式) — 讀取所有網站集合中的項目 	<ul style="list-style-type: none"> • AllSites.Read (委派) — 讀取所有網站集合中的項目

Note

只有當您要編目文件時，才需要「全部」和「全部」。OneNote 如果您想要檢索特定網站，權限可以限制在特定網站，而不是網域中可用的所有網站。您可以設定「網站. 已選取 (應用程式)」權限。有了這個 API 權限，您需要透過 Microsoft Graph API 明確設定每個網站的存取權限。如需詳細資訊，請參閱 [Microsoft 網站上的部落格。選取的權限。](#)

- 如果您使用的是 ACL，請新增下列權限：

Microsoft 圖	SharePoint
<ul style="list-style-type: none"> • 群組成員閱讀全部 (應用程式) — 讀取所有群組成員資格 • 備註 .Read. All (應用程式) — 讀取所有筆記本 OneNote • 網站。FullControl全部 (委派) — 擷取文件的 ACL 所需 • Site.Read.All (應用程式) — 讀取所有網站集合中的項目 • 使用者 .Read.All (應用程式) — 讀取所有使用者的完整設定檔 	<ul style="list-style-type: none"> • AllSites.Read (委派) — 讀取所有網站集合中的項目

Note

GroupMember只有在啟動 [識別爬行者程式] 時，才需要 .Read.All 和 [使用者 .Read.All]。

如果您想要檢索特定網站，權限可以限制在特定網站，而不是網域中可用的所有網站。您可以設定「網站. 已選取 (應用程式)」權限。有了這個 API 權限，您需要透過 Microsoft Graph API 明確設定每個網站的存取權限。如需詳細資訊，請參閱 [Microsoft 網站上的部落格。選取的權限。](#)

- 僅限 Azure AD 應用程式驗證：私密金鑰和您在 Azure AD 註冊 SharePoint 後產生的用戶端識別碼。另請注意 X.509 憑證。
- 如果您未使用 ACL，請新增下列權限：

SharePoint

- Site.Read.All (應用程式) — 存取所有網站集合中的項目和清單所需

Note

如果您想要檢索特定網站，權限可以限制在特定網站，而不是網域中可用的所有網站。您可以設定「網站. 已選取 (應用程式)」權限。有了這個 API 權限，您需要透過 Microsoft Graph API 明確設定每個網站的存取權限。如需詳細資訊，請參閱 [Microsoft 網站上的部落格。選取的權限。](#)

- 如果您使用的是 ACL，請新增下列權限：

SharePoint

- 網站. FullControl. 全部 (應用程式) — 擷取文件的 ACL 所需

Note

如果您想要檢索特定網站，權限可以限制在特定網站，而不是網域中可用的所有網站。您可以設定「網站. 已選取 (應用程式)」權限。有了這個 API 權限，您需要透過 Microsoft Graph API 明確設定每個網站的存取權限。如需詳細資訊，請參閱 [Microsoft 網站上的部落格。選取的權限。](#)

- SharePoint 僅限應用程式驗證：記下您的用 SharePoint 戶端識別碼和用戶端密碼在授予應用程式僅限 SharePoint 應用程式的權限時產生，以及當您向 Azure AD 註冊 SharePoint 應用程式時產生的用戶端識別碼和用戶端密碼。

Note

SharePoint SharePoint 2013 版本不支援僅限應用程式驗證。

- (選擇性) 如果您要探索 OneNote 文件並使用 Identity 爬行者程式，請新增下列權限：

Microsoft 圖

- GroupMember.Read.All (應用程式) — 讀取所有群組成員資格
- 備註 .Read. All (應用程式) — 讀取所有筆記本 OneNote
- Site.Read.All (應用程式) — 讀取所有網站集合中的項目
- 使用者 .Read.All (應用程式) — 讀取所有使用者的完整設定檔

Note

使用基本驗證和僅限應用 SharePoint 程式驗證來檢索實體時，不需要 API 權限。

在 SharePoint 伺服器中，確定您有：

- 複製您的 SharePoint 執行個體 URL 和網 SharePoint 址的網域名稱。您輸入的主機網址格式為 *https://yourcompany/sites/mysite*。您的網址必須以開頭 https。

Note

(內部預備/伺服器) Amazon Kendra 會檢查中包含的端點資訊 AWS Secrets Manager 是否與資料來源組態詳細資料中指定的端點資訊相同。這有助於防止[混淆的副問題](#)，這是一個安全

性問題，即使用者沒有執行動作的權限，但用 Amazon Kendra 作 Proxy 來存取設定的密碼並執行動作。如果您稍後變更端點資訊，則必須建立新密碼才能同步此資訊。

- 停用您 SharePoint 帳戶中的多重要素驗證 (MFA)，因此不會 Amazon Kendra 封鎖檢索您的內容。SharePoint
- 如果使用 SharePoint 僅應用程式驗證進行存取控制：
 - 複製您在站點級別註冊僅應用程序時生成的 SharePoint 客戶端 ID。用戶端識別碼格式為 ClientId @ TenantId。例如，*F8f89-44e7-b0e4-49670756342c @888d0b57 -69f1-4fb8-957F-E1fT*。
 - 複製您在站點級別註冊僅應用程序時生成的 SharePoint 客戶端密鑰。

注意：由於只有在您註冊 SharePoint 伺服器進行應用程式驗證時，才會為單一網站產生用戶端 ID 和用戶端密碼，因此僅支援一個網站 URL 進行僅 SharePoint 應用程式驗證。

Note

SharePoint SharePoint 2013 版本不支援僅限應用程式驗證。

- 如果使用自訂網域的電子郵件 ID 進行存取控制：
 - *#####Amazon.com##*
- 如果將電子郵件 ID 與 IDP 授權的域名一起使用，請複製您的：
 - LDAP 伺服器端點 (LDAP 伺服器的端點，包括通訊協定和連接埠號碼)。例如：*LDAP###389*。
 - LDAP 搜尋依據 (LDAP 使用者的搜尋基礎)。例如：*CN = ###DC = SharePoint#DC = COM*。
 - LDAP 使用者名稱和 LDAP 密碼。
- 設定的 NTLM 驗證認證，或設定包含使用者名稱 (帳戶使用者名稱) 和密碼 (SharePoint 帳戶密碼) 的 Kerberos 驗證認證。SharePoint

在你的 AWS 帳戶，確保你有：

- [建立 Amazon Kendra 索引](#)，如果使用 API，則會記下索引 ID。
- 為您的[資料來源建立 IAM 角色](#)，如果使用 API，則會記錄 IAM 角色的 ARN。

Note

如果您變更驗證類型和認證，則必須更新 IAM 角色才能存取正確的 AWS Secrets Manager 密碼 ID。

- 將您的 SharePoint 身份驗證憑據存儲在 AWS Secrets Manager 密鑰中，如果使用 API，則記錄密鑰的 ARN。

Note

我們建議您定期重新整理或輪換您的認證和密碼。僅為您自己的安全提供必要的訪問級別。我們不建議您跨資料來源以及連接器 1.0 和 2.0 版 (如果適用) 重複使用認證和密碼。

如果您沒有現有的 IAM 角色或密碼，則可以在將 SharePoint 資料來源連線到時使用主控台建立新 IAM 角色和 Secrets Manager 密碼 Amazon Kendra。如果您使用 API，則必須提供現有 IAM 角色和 Secrets Manager 密碼的 ARN 以及索引 ID。

連接說明

若要連線 Amazon Kendra 到 SharePoint 資料來源，您必須提供 SharePoint 認證的詳細資料，Amazon Kendra 以便能夠存取您的資料。如果您尚未設定「Amazon Kendra 請 SharePoint 參閱[必要條件](#)」。

Console: SharePoint Online

若要連 SharePoint 線 Amazon Kendra 到線上

- 登入 AWS Management Console 並開啟[Amazon Kendra 主控台](#)。
- 在左側導覽窗格中，選擇 [索引]，然後從索引清單中選擇要使用的索引。

Note

您可以選擇在索引設置下配置或編輯您的用戶訪問控制設置。

- 在 [開始使用] 頁面上，選擇 [新增資料來源]。
- 在 [新增資料來源] 頁面上，選擇 [SharePoint 連接器]，然後選擇 [新增連接器]。如果使用版本 2 (如果適用)，請選擇帶有「V2.0」標籤的 SharePoint 連接器。


5. 在 [指定資料來源詳細資訊] 頁面上，輸入下列資訊：
 - a. 在名稱和說明中，對於資料來源名稱 — 輸入資料來源的名稱。您可以包含連字號，但不能包含空格。
 - b. (選擇性) 說明 — 輸入資料來源的選用說明。
 - c. 在預設語言中 — 選擇一種語言來篩選索引的文件。除非另有指定，否則語言預設為英文。文件中繼資料中指定的語言會覆寫選取的語言。
 - d. 在「標籤」中，針對「新增標籤」 — 包含可選標籤以搜尋和篩選資源或追蹤 AWS 成本。
 - e. 選擇下一步。
6. 在 [定義存取和安全性] 頁面上，輸入下列資訊：
 - a. 託管方法 — 選擇「SharePoint 線上」。
 - b. 儲存庫特定的網站 SharePoint URL — 輸入 SharePoint 主機 URL。您輸入的主機網址格式為 *https://yourdomain.sharepoint.com/sites/mysite*。URL 必須以 https 通訊協定開頭。使用新行分隔 URL。您最多可以新增 100 個網址。
 - c. 網域 — 輸入網 SharePoint 域。例如，網址 *https://yourdomain.sharepoint.com/sites/mysite* 中的網域就是####。
 - d. 授權 — 開啟或關閉文件的存取控制清單 (ACL) 資訊 (如果您有 ACL)，且想要將其用於存取控制。ACL 會指定使用者和群組可存取的文件。ACL 資訊可用來根據使用者或使用者對文件的群組存取權來篩選搜尋結果。如需詳細資訊，請參閱[使用者內容篩選](#)。

您也可以選擇使用者識別碼的類型，無論是從 Azure 入口網站擷取的使用者主體名稱或使用者電子郵件。如果未指定，則預設會使用電子郵件。
 - e. 驗證 — 選擇基本、OAuth 2.0、僅限 Azure AD 應用程式驗證、僅應用程式驗證或 OAuth 2.0 重新整理權杖驗證。SharePoint 您可以選擇現有 AWS Secrets Manager 密碼來儲存您的驗證認證，或建立密碼。
 - i. 如果使用基本驗證，您的密碼必須包含密碼名稱、使用 SharePoint 者名稱和密碼。
 - ii. 如果使用 OAuth 2.0 驗證，您的密碼必須包含 SharePoint 租用戶識別碼、密碼名稱、使用 SharePoint 者名稱、密碼、在 Azure AD SharePoint 中註冊時產生的 Azure AD 用戶端識別碼，以及在 Azure AD SharePoint 中註冊時產生的 Azure AD 用戶端密碼。
 - iii. 如果使用僅限 Azure AD 應用程式驗證，您的密鑰必須包含 SharePoint 租用戶識別碼、Azure AD 自我簽署 X.509 憑證、密碼名稱、在 Azure AD SharePoint 中註冊時產生的 Azure AD 用戶端識別碼，以及用來驗證 Azure AD 連接器的私密金鑰。

- iv. 如果使用SharePoint僅應用程式驗證，您的密碼必須包含 SharePoint 租用戶識別碼、密碼名稱、您在租用 SharePoint 戶層級註冊應用程式時產生的用 SharePoint 戶端識別碼、在租用戶層級註冊僅應用程式時產生的用戶端密碼、在 Azure AD SharePoint 中註冊時產生的 Azure AD 用戶端識別碼，以及在 Azure AD 註冊 SharePoint 時產生的 Azure AD 用戶端密碼。


用 SharePoint 戶端 ID 格式為用戶端 `@#TenantId` 例如，`F8f89-44e7-b0e4-49670756342c @888d0b57 -69f1-4fb8-957F- E1fT`。
- v. 如果使用 OAuth 2.0 重新整理權杖驗證，您的密碼必須包含 SharePoint 租用戶識別碼、密碼名稱、在 Azure AD SharePoint 中註冊時產生的唯一 Azure AD 用戶端識別碼、註冊 SharePoint 至 Azure AD 時產生的 Azure AD 用戶端密碼、重新整理 Amazon Kendra 要 SharePoint 連線的權杖。
- f. Virtual Private Cloud (VPC) (VPC) — 您可以選擇使用 VPC。如果是這樣，您必須新增子網路和 VPC 安全性群組。
- g. 識別爬行者程式 — 指定是否要開啟身分識別爬行者 Amazon Kendra 者程式。識別爬行者程式會使用文件的存取控制清單 (ACL) 資訊，根據使用者或使用者對文件的群組存取權來篩選搜尋結果。如果您有文件的 ACL 並選擇使用 ACL，您也可以選擇開啟的身分識別爬行者程式，以設定搜尋結果的使用者環境定義篩選。Amazon Kendra 否則，如果關閉身分搜索器，則可以公開搜索所有文檔。如果您想要對文件使用存取控制，且身分識別編目程式已關閉，您也可以使用 [PutPrincipalMapping](#) API 來上傳使用者和群組存取資訊以進行使用者內容篩選。

您也可以選擇編目本機群組對應或 Azure 作用中目錄群組對應。

 Note

AD 群組對應編目僅適用於 OAuth 2.0、OAuth 2.0 重新整理權杖和僅 SharePoint 應用程式驗證。

- h. IAM role — 選擇現有 IAM 角色或建立新 IAM 角色以存取存放庫認證和索引內容。

 Note

IAM 用於索引的角色不能用於資料來源。如果您不確定索引或常見問題集是否使用現有角色，請選擇 [建立新角色] 以避免發生錯誤。

- i. 選擇下一步。

7. 在 [設定同步設定] 頁面上，輸入下列資訊：
 - a. 在同步範圍中，從下列選項中選擇：
 - i. 選取實體 — 選取您要編目的實體。您可以選取編目 [所有實體] 或 [檔案]、[附件]、[連結頁面]、[事件]、[註解] 和 [清單資料] 的任意組合。
 - ii. 在其他配置中，對於實體正則表達式模式-添加鏈接，頁面和事件的正則表達式模式以包含特定的實體，而不是同步所有文檔。
 - iii. 正則表達式模式-添加正則表達式模式以包含或排除文件通過文件路徑，文件名，文件類型，OneNote 部分名稱和OneNote 頁面名稱，而不是同步所有文檔。您最多可以添加 100。
 - b. 對於同步模式，請選擇資料來源內容變更時要如何更新索引。第一次將資料來源同 Amazon Kendra 步時，依預設會同步所有內容。
 - 完全同步 — 同步所有內容，無論先前的同步狀態為何。
 - 新增或修改的文件同步 — 僅同步新文件或修改過的文件。
 - 新增、修改或刪除的文件同步 — 僅同步新文件、修改過的和已刪除的文件。
 - c. 在同步執行排程中，對於頻率 — 選擇同步資料來源內容和更新索引的頻率。
 - d. 選擇下一步。
8. 在 [設定欄位對映] 頁面上，輸入下列資訊：
 - a. 預設資料來源欄位 — 從 Amazon Kendra 產生的預設資料來源欄位中選取您要對映至索引的資料來源欄位。
 - b. 新增欄位 — 新增自訂資料來源欄位，以建立要對映的索引欄位名稱和欄位資料類型。
 - c. 選擇下一步。
9. 在 [檢閱並建立] 頁面上，檢查您輸入的資訊是否正確，然後選取 [新增資料來源]。您也可以從此頁面選擇編輯您的資訊。成功新增資料來源後，您的資料來源將顯示在 [資料來源] 頁面上。

**Note**

OneNote 爬網僅適用於 OAuth 2.0，OAuth 2.0 刷新令牌和僅 SharePoint 應用程式身份驗證。

Console: SharePoint Server

若要連線 Amazon Kendra 到 SharePoint

1. 登入 AWS Management Console 並開啟 [Amazon Kendra 主控台](#)。
2. 在左側導覽窗格中，選擇 [索引]，然後從索引清單中選擇要使用的索引。

Note

您可以選擇在索引設置下配置或編輯您的用戶訪問控制設置。

3. 在 [開始使用] 頁面上，選擇 [新增資料來源]。
4. 在 [新增資料來源] 頁面上，選擇 [SharePoint 連接器]，然後選擇 [新增連接器]。如果使用版本 2 (如果適用)，請選擇帶有「V2.0」標籤的SharePoint 連接器。
5. 在 [指定資料來源詳細資訊] 頁面上，輸入下列資訊：
 - a. 在名稱和說明中，對於資料來源名稱 — 輸入資料來源的名稱。您可以包含連字號，但不能包含空格。
 - b. (選擇性) 說明 — 輸入資料來源的選用說明。
 - c. 在預設語言中 — 選擇一種語言來篩選索引的文件。除非另有指定，否則語言預設為英文。文件中繼資料中指定的語言會覆寫選取的語言。
 - d. 在「標籤」中，針對「新增標籤」 — 包含可選標籤以搜尋和篩選資源或追蹤 AWS 成本。
 - e. 選擇下一步。
6. 在 [定義存取和安全性] 頁面上，輸入下列資訊：
 - a. 託管方法 — 選擇「SharePoint伺服器」。
 - b. 選擇 SharePoint版本 — 選擇 SharePoint 2013 年、SharePoint 2016 SharePoint 年、2019 年及 SharePoint (訂閱版)。
 - c. 儲存庫特定的網站 SharePoint URL — 輸入 SharePoint 主機 URL。您輸入的主機網址格式為 *https://yourcompany/sites/mysite*。URL 必須以https通訊協定開頭。使用新行分隔 URL。您最多可以新增 100 個網址。
 - d. 網域 — 輸入網 SharePoint 域。例如，網址 *https://yourcompany/sites/mysite* 中的網域就是#的公司
 - e. SSL 憑證位置 — 輸入 SSL 憑證檔案的 Amazon S3 路徑。

- f. (選擇性) 對於 Web Proxy — 輸入主機名稱 (不含http://或通https://訊協定), 以及主機 URL 傳輸通訊協定使用的連接埠號碼。連接埠號碼的數值必須介於 0 到 65535 之間。
- g. 授權 — 開啟或關閉文件的存取控制清單 (ACL) 資訊 (如果您有 ACL), 且想要將其用於存取控制。ACL 會指定使用者和群組可存取的文件。ACL 資訊可用來根據使用者或使用者對文件的群組存取權來篩選搜尋結果。如需詳細資訊, 請參閱[使用者內容篩選](#)。

對於 SharePoint 伺服器, 您可以從下列 ACL 選項中進行選擇:

- i. 來自 IDP 的網域的電子郵件 ID — 使用者 ID 是以電子郵件 ID 為基礎, 其網域是從基礎身分識別提供者 (IDP) 擷取的。您在 Secrets Manager 密碼中提供 IDP 連線詳細資料, 作為驗證的一部分。
- ii. 具有自訂網域的電子郵件 ID — 使用者 ID 是以自訂電子郵件網域值為基礎。例如, "**#****##**". 電子郵件網域將用於建構存取控制的電子郵件 ID。您必須輸入自訂電子郵件網域。
- iii. 具有網域的網域\使用者 — 使用者 ID 是使用網域\使用者識別碼格式建構的。您必須提供有效的網域名稱。例如: **#### 2019#** 來構建訪問控制。
- h. 對於 [驗證], 請選擇 [SharePoint 僅限應用程式驗證]、[NTLM 驗證] 或 [Kerberos 驗證]。您可以選擇現有 AWS Secrets Manager 密碼來儲存您的驗證認證, 或建立密碼。
 - i. 如果使用 NTLM 驗證或 Kerberos 驗證, 則密碼必須包含密碼名稱、使用者名稱和密碼。

如果將電子郵件 ID 與 IDP 的域名一起使用, 請輸入您的:

- LDAP 伺服器端點 — LDAP 伺服器的端點, 包括通訊協定和連接埠號碼。例如: **LDAP####389**。
 - LDAP 搜尋依據 — LDAP 使用者的搜尋基礎。例如: **CN = ###DC = SharePoint#DC = COM**。
 - LDAP 使用者名稱 — 您的 LDAP 使用者名稱。
 - LDAP 密碼 — 您的 LDAP 密碼。
- ii. 如果使用 SharePoint 僅應用程式身份驗證, 則您的密鑰必須包含秘密名稱, 您在站點級別註冊僅應用程式時生成的 SharePoint 客戶端 ID, 在站點級別註冊僅應用程式時生成的客戶端密鑰。


用 SharePoint 戶端 ID 格式為用戶端 **@#TenantId** 例如, **F8f89-44e7-b0e4-49670756342c @888d0b57 -69f1-4fb8-957F- E1fT**。

注意：由於只有在您註冊 SharePoint 伺服器進行應用程式驗證時，才會為單一網站產生用戶端 ID 和用戶端密碼，因此僅支援一個網站 URL 進行僅 SharePoint 應用程式驗證。

如果將電子郵件 ID 與 IDP 的域名一起使用，請輸入您的：


- LDAP 伺服器端點 — LDAP 伺服器的端點，包括通訊協定和連接埠號碼。例如：*LDAP####389*。
 - LDAP 搜尋依據 — LDAP 使用者的搜尋基礎。例如：*CN = ###DC = SharePoint#DC = COM*。
 - LDAP 使用者名稱 — 您的 LDAP 使用者名稱。
 - LDAP 密碼 — 您的 LDAP 密碼。
- i. Virtual Private Cloud (VPC) (VPC) — 您可以選擇使用 VPC。如果是這樣，您必須新增子網路和 VPC 安全性群組。
- j. 識別爬行者程式 — 指定是否要開啟身分識別爬行者程式。識別爬行者程式會使用文件的存取控制清單 (ACL) 資訊，根據使用者或使用者對文件的群組存取權來篩選搜尋結果。如果您有文件的 ACL 並選擇使用 ACL，您也可以選擇開啟的身分識別爬行者程式，以設定搜尋結果的[使用者環境定義篩選](#)。Amazon Kendra 否則，如果關閉身分搜索器，則可以公開搜索所有文檔。如果您想要對文件使用存取控制，且身分識別編目程式已關閉，您也可以使用 [PutPrincipalMapping](#) API 來上傳使用者和群組存取資訊以進行使用者內容篩選。

您也可以選擇編目本機群組對應或 Azure 作用中目錄群組對應。

 Note

AD 群組對應編目僅適用於 SharePoint 應用程式驗證。

- k. IAM role — 選擇現有 IAM 角色或建立新 IAM 角色以存取存放庫認證和索引內容。


 Note

IAM 用於索引的角色不能用於資料來源。如果您不確定索引或常見問題集是否使用現有角色，請選擇 [建立新角色] 以避免發生錯誤。

- l. 選擇下一步。

7. 在 [設定同步設定] 頁面上，輸入下列資訊：

- a. 在同步範圍中，從下列選項中選擇：
 - i. 選取實體 — 選取您要編目的實體。您可以選取編目 [所有實體] 或 [檔案]、[附件]、[連結頁面]、[事件] 和 [清單資料] 的任意組合。
 - ii. 在其他配置中，對於實體正則表達式模式-添加鏈接，頁面和事件的正則表達式模式以包含特定實體，而不是同步所有文檔。
 - iii. 正則表達式模式-添加正則表達式模式以包含或排除文件文件路徑文件名文件類型，OneNote部分名稱和OneNote頁面名稱，而不是同步所有文檔。您最多可以添加100。

 Note

OneNote 搜索僅適 SharePoint 用於僅應用程序身份驗證。


- b. 同步模式 — 選擇資料來源內容變更時要如何更新索引。當您第一次將資料來源同 Amazon Kendra 步處理時，依預設會檢索所有內容並建立索引。如果初始同步失敗，您必須執行資料的完整同步處理，即使您沒有選擇完整同步作為同步模式選項。
 - 完全同步：新鮮索引所有內容，並在每次資料來源與索引同步時取代現有內容。
 - 新增、修改的同步：每次資料來源與索引同步時，僅對新內容和已修改的內容建立索引。Amazon Kendra 可以使用資料來源的機制來追蹤內容變更，並為上次同步後變更的內容建立索引。
 - 新增、修改、刪除的同步：每次資料來源與索引同步時，僅對新內容、已修改和刪除的內容建立索引。Amazon Kendra 可以使用資料來源的機制來追蹤內容變更，並為上次同步後變更的內容建立索引。
 - c. 在同步執行排程中，對於頻率 — 選擇同步資料來源內容和更新索引的頻率。
 - d. 選擇下一步。
8. 在 [設定欄位對映] 頁面上，輸入下列資訊：
 - a. 預設資料來源欄位 — 從 Amazon Kendra 產生的預設資料來源欄位中選取您要對映至索引的資料來源欄位。
 - b. 新增欄位 — 新增自訂資料來源欄位，以建立要對映的索引欄位名稱和欄位資料類型。
 - c. 選擇下一步。
 9. 在 [檢閱並建立] 頁面上，檢查您輸入的資訊是否正確，然後選取 [新增資料來源]。您也可以從此頁面選擇編輯您的資訊。成功新增資料來源後，您的資料來源將顯示在 [資料來源] 頁面上。

API

若要連線 Amazon Kendra 到 SharePoint

您必須使用 [TemplateConfigurationAPI](#) 指定 [資料來源結構描述](#) 的 JSON。您必須提供以下信息：

- 資料來源 — 指定使用 [TemplateConfigurationJSON](#) 結構定義 SHAREPOINTV2 時的資料來源類型。同時將資料來源指定為呼叫 [CreateDataSourceAPI](#) TEMPLATE 時的方式。
- 儲存庫端點中繼資料 — 指定 SharePoint 執行個體 `siteUrls` 的 `tenantIDdomain` 和。
- 同步模式 — 指定資料來源內容變更時 Amazon Kendra 應如何更新索引。當您第一次將資料來源同 Amazon Kendra 步處理時，依預設會檢索所有內容並建立索引。如果初始同步失敗，您必須執行資料的完整同步處理，即使您沒有選擇完整同步作為同步模式選項。您可以選擇：
 - FORCED_FULL_CRAWL 新建索引所有內容，並在每次資料來源與索引同步時取代現有內容。
 - FULL_CRAWL，以在每次資料來源與索引同步時，僅對新的、修改的和刪除的內容建立索引。Amazon Kendra 可以使用資料來源的機制來追蹤內容變更，並為上次同步後變更的內容建立索引。
 - CHANGE_LOG 每次資料來源與索引同步時，僅對新內容和修改的內容建立索引。Amazon Kendra 可以使用資料來源的機制來追蹤內容變更，並為上次同步後變更的內容建立索引。
- 識別爬行者程式 — 指定是否要開啟身分識別爬行者 Amazon Kendra 者程式。識別爬行者程式會使用文件的存取控制清單 (ACL) 資訊，根據使用者或使用者對文件的群組存取權來篩選搜尋結果。如果您有文件的 ACL 並選擇使用 ACL，您也可以選擇開啟的身分識別爬行者程式，以設定搜尋結果的使用 [者環境定義篩選](#)。Amazon Kendra 否則，如果關閉身分搜索器，則可以公開搜索所有文檔。如果您想要對文件使用存取控制，且身分識別編目程式已關閉，您也可以使用 [PutPrincipalMappingAPI](#) 來上傳使用者和群組存取資訊以進行使用者內容篩選。

 Note

只有當您設 `crawlAcl` 定為 `true` 時，才能使用識別爬行者程式。

- 儲存庫其他屬性 — 指定：
 - (適用於 Azure AD) `s3bucketName`，`s3certificateName` 您可以使用來儲存 Azure AD 自我簽署的 X.509 憑證。
 - 您使用的驗證類型 (`auth_Type`) `OAuth20Auth2App`，是 `OAuth2CertificateBasic`、`OAuth2_RefreshToken`、`NTLM`、和 `Kerberos`。
 - 您使用的版本 (`version`)，無論是 `Server` 或 `Online`。如果 `Server` 您使用，則可以進一步指定 `onPremVersion` 為 `20132016`、`2019`、或 `SubscriptionEdition`。

- 秘密 Amazon 資源名稱 (ARN) — 提供包含您在帳戶中建立的身份驗證登入資料的 Secrets Manager 密碼的 Amazon 資源名稱 (ARN)。SharePoint

如果您使用「SharePoint 線上」，則可以選擇「基本」、「OAuth 2.0」、「僅限 Azure AD 應用程式」和「僅限 SharePoint 應用程式」驗證。以下是每個身份驗證選項的密碼中必須包含的最低 JSON 結構：

- 基本驗證

```
{
  "userName": "SharePoint account user name",
  "password": "SharePoint account password"
}
```

- 驗證身份驗證

```
{
  "clientId": "client id generated when registering SharePoint with Azure AD",
  "clientSecret": "client secret generated when registering SharePoint with Azure AD",
  "userName": "SharePoint account user name",
  "password": "SharePoint account password"
}
```

- 僅限 Azure AD 應用程式的驗證

```
{
  "clientId": "client id generated when registering SharePoint with Azure AD",
  "privateKey": "private key to authorize connection with Azure AD"
}
```

- SharePoint 僅應用程式驗證

```
{
  "clientId": "client id generated when registering SharePoint for App Only at Tenant Level",
  "clientSecret": "client secret generated when registering SharePoint for App Only at Tenant Level",
  "adClientId": "client id generated while registering SharePoint with Azure AD",
  "adClientSecret": "client secret generated while registering SharePoint with Azure AD"
}
```



```
}

```

- OAuth 2.0 刷新令牌身份驗證

```
{
  "clientId": "client id generated when registering SharePoint with Azure AD",
  "clientSecret": "client secret generated when registering SharePoint with Azure AD",
  "refreshToken": "refresh token generated to connect to SharePoint"
}
```

如果您使用 SharePoint 伺服器，則可以選擇 SharePoint 僅限應用程式驗證、NTLM 驗證和 Kerberos 驗證。以下是每個身份驗證選項的密碼中必須包含的最低 JSON 結構：

- SharePoint 僅應用程式驗證

```
{
  "siteUrlsHash": "Hash representation of SharePoint site URLs",
  "clientId": "client id generated when registering SharePoint for App Only at Site Level",
  "clientSecret": "client secret generated when registering SharePoint for App Only at Site Level"
}
```

- SharePoint 具有 IDP 授權的域的僅應用程式身份驗證

```
{
  "siteUrlsHash": "Hash representation of SharePoint site URLs",
  "clientId": "client id generated when registering SharePoint for App Only at Site Level",
  "clientSecret": "client secret generated when registering SharePoint for App Only at Site Level",
  "ldapUrl": "LDAP Account url eg. ldap://example.com:389",
  "baseDn": "LDAP Account base dn eg. CN=Users,DC=sharepoint,DC=com",
  "ldapUser": "LDAP account user name",
  "ldapPassword": "LDAP account password"
}
```

- (僅限伺服器) NTLM 或 Kerberos 驗證

```
{
  "siteUrlsHash": "Hash representation of SharePoint site URLs",
  "userName": "SharePoint account user name",

```

```
"password": "SharePoint account password"
}
```

- (僅限伺服器) 透過 IDP 授權的網域進行 NTLM 或 Kerberos 驗證

```
{
  "siteUrlsHash": "Hash representation of SharePoint site URLs",
  "userName": "SharePoint account user name",
  "password": "SharePoint account password",
  "ldapUrl": "ldap://example.com:389",
  "baseDn": "CN=Users,DC=sharepoint,DC=com",
  "ldapUser": "LDAP account user name",
  "ldapPassword": "LDAP account password"
}
```

- IAM role — 指定RoleArn何時呼叫CreateDataSource以提供具有存取 Secrets Manager 密碼之權限的 IAM 角色，以及呼叫 SharePoint 連接器和 Amazon Kendra所需公用 API 的時間。有關詳情，請參閱[SharePoint 料來源的IAM 角色](#)。

您還可以添加以下可選功能：

- Virtual Private Cloud (VPC) — 指定您撥打電話的VpcConfiguration時間。CreateDataSource如需詳細資訊，請參閱[配置 Amazon Kendra 為使用 Amazon VPC](#)。
- 包含和排除篩選器 — 您可以指定是否要包含或排除某些檔案及其他內容。OneNotes

Note

大多數資料來源使用規則運算式模式，這些模式是稱為篩選器的包含或排除模式。如果您指定包含篩選器，則只有符合包含項目篩選器的內容會編製索引。不符合包含篩選器的任何文件都不會建立索引。如果您指定包含和排除篩選器，符合排除篩選器的文件將不會建立索引，即使它們符合包含篩選器也是如此。

- 欄位對映 — 選擇將資 SharePoint 料來源欄位對映至 Amazon Kendra 索引欄位。如需詳細資訊，請參閱[映射資料來源欄位](#)。

Note

您的文件需要文件內文欄位或文件內文對等項目，才能搜尋您的文件。Amazon Kendra 您必須將資料來源中的文件內文欄位名稱對應至索引欄位名稱_document_body。所有其他欄位是選用的。

如需要設定的其他重要 JSON 金鑰清單，請參閱[SharePoint 範本結構定義](#)。

備註

- 連接器僅支援檔案實體的自訂欄位對應。
- 對於所有 SharePoint 伺服器版本，ACL 權杖必須為小寫。針對來自 IDP 的具有網域的電子郵件，以及含有自訂網域 ACL 的電子郵件 ID，例如：*user@sharepoint2019.com*。對於具有網域 ACL 的網域\使用者，例如：*### 2013*使用者。
- 連接器不支援 SharePoint 2013 年的變更記錄模式/新增或修改的內容同步。
- 如果實體名稱的名稱中有%字元，則由於 API 限制，連接器將略過這些檔案。
- OneNote 只能透過使用租用戶識別碼的連接器進行編目，以及針對線上啟用 OAuth 2.0、OAuth 2.0 重新整理權杖或僅 SharePoint 應用程式驗證。SharePoint
- 連接器只會使用其預設名稱來編目 OneNote 文件的第一個區段，即使文件已重新命名也是如此。
- 連接器只會對 SharePoint 2019 年、SharePoint 線上和訂閱版中探索連結，只有在選取頁面和檔案做為要編目的實體時，連接器才會探索連結。
- 如果選取連結做為要編目的實體，則連接器會在 SharePoint 2013 年和 SharePoint 2016 年探索連結。
- 只有在同時選取 [清單資料] 做為要編目的實體時，連接器探索才會列出附件和註解。
- 只有在同時選取「事件」作為要編目的實體時，連接器才會探索事件附件。
- 對於在 SharePoint 線版本，ACL 令牌將以小寫形式顯示。例如，如果 Azure 入口網站中的使用者主體名稱是 *MaryMajor@domain.com*，則 SharePoint 連接器中的 ACL 權杖將是 *marymajor@domain.com*。
- 在 SharePoint 線上和伺服器的身分識別爬行者程式中，如果您想要編目巢狀群組，則必須啟動本機和 AD 群組編目。

- 如果您使用的是 SharePoint 線上，而 Azure 入口網站中的使用者主要名稱是大寫和小寫的組合，SharePoint API 會在內部將其轉換為小寫。因此，Amazon Kendra SharePoint 連接器將 ACL 設定為小寫。

Microsoft SQL Server

Microsoft SQL Server是由 Microsoft 開發的關係數據庫管理系統 (RDBMS)。如果您是使用Microsoft SQL Server者，則可以使用 Amazon Kendra 對資Microsoft SQL Server料來源建立索引。資 Amazon Kendra Microsoft SQL Server料來源連接器支援 MS SQL 伺服器 2019。

您可以使用[Amazon Kendra 主控台](#)和 [TemplateConfiguration](#)API 連線 Amazon Kendra 到Microsoft SQL Server資料來源。

如需疑難排解資 Amazon Kendra Microsoft SQL Server料來源連接器，請參閱[疑難排解資料來](#)。

主題

- [支援的功能](#)
- [必要條件](#)
- [連接說明](#)
- [備註](#)

支援的功能

- 欄位對映
- 使用者內容篩選
- 包含/排除過濾器
- 完整和增量內容同步
- 虛擬私有雲端 (VPC)

必要條件

在您可以用來 Amazon Kendra 為資Microsoft SQL Server料來源建立索引之前，請先在Microsoft SQL Server和 AWS 帳戶中進行這些變更。

在中Microsoft SQL Server，請確定您有：

- 記下您的資料庫使用者名稱和密碼。

⚠ Important

最佳作法是提供 Amazon Kendra 唯讀資料庫認證。

- 複製您的資料庫主機 URL、連接埠和執行個體。
- 已勾選的每個文件在您打算用於相同索引的其他資料來源中 Microsoft SQL Server 和其他資料來源之間都是唯一的。您要用於索引的每個資料來源不得包含跨資料來源的相同文件。文件 ID 對索引來說是全域的，而且每個索引必須是唯一的。

在您的中 AWS 帳戶，請確保您有：

- [建立 Amazon Kendra 索引](#)，如果使用 API，則會記下索引識別碼。
- 為您的[資料來源建立 IAM 角色](#)，如果使用 API，則會記錄 IAM 角色的 ARN。

📘 Note

如果您變更驗證類型和認證，則必須更新 IAM 角色才能存取正確的 AWS Secrets Manager 密碼 ID。

- 將您的 Microsoft SQL Server 身份驗證憑據存儲在 AWS Secrets Manager 密鑰中，如果使用 API，則記錄密鑰的 ARN。

📘 Note

我們建議您定期重新整理或輪換您的認證和密碼。僅為您自己的安全提供必要的訪問級別。我們不建議您跨資料來源以及連接器 1.0 和 2.0 版 (如果適用) 重複使用認證和密碼。

如果您沒有現有的 IAM 角色或密碼，則可以在將 Microsoft SQL Server 資料來源連線到時使用主控台建立新 IAM 角色和 Secrets Manager 密碼 Amazon Kendra。如果您使用 API，則必須提供現有 IAM 角色和 Secrets Manager 密碼的 ARN，以及索引 ID。

連接說明

若要連線 Amazon Kendra 到 Microsoft SQL Server 資料來源，您必須提供 Microsoft SQL Server 認證的詳細資料，Amazon Kendra 以便能夠存取您的資料。如果您尚未設定「Amazon Kendra 請 Microsoft SQL Server 參閱[必要條件](#)」。

Console

若要連線 Amazon Kendra 到 Microsoft SQL Server


1. 登入 AWS Management Console 並開啟 [Amazon Kendra 主控台](#)。
2. 在左側導覽窗格中，選擇 [索引]，然後從索引清單中選擇要使用的索引。

Note

您可以選擇在索引設置下配置或編輯您的用戶訪問控制設置。


3. 在 [開始使用] 頁面上，選擇 [新增資料來源]。
4. 在 [新增資料來源] 頁面上，選擇 [Microsoft SQL Server 連接器]，然後選擇 [新增連接器]。如果使用版本 2 (如果適用)，請選擇帶有「V2.0」標籤的 Microsoft SQL Server 連接器。
5. 在 [指定資料來源詳細資訊] 頁面上，輸入下列資訊：
 - a. 在名稱和說明中，對於資料來源名稱 — 輸入資料來源的名稱。您可以包含連字號，但不能包含空格。
 - b. (選擇性) 說明 — 輸入資料來源的選用說明。
 - c. 在預設語言中 — 選擇一種語言來篩選索引的文件。除非另有指定，否則語言預設為英文。文件中繼資料中指定的語言會覆寫選取的語言。
 - d. 在「標籤」中，針對「新增標籤」 — 包含可選標籤以搜尋和篩選資源或追蹤 AWS 成本。
 - e. 選擇下一步。
6. 在 [定義存取權和安全性] 頁面上，輸入下列資訊：
 - a. 在來源中，輸入下列資訊：
 - b. 主機 — 輸入資料庫主機名稱。
 - c. 連接埠 — 輸入資料庫連接埠。
 - d. 執行處理 — 輸入資料庫執行處理。
 - e. 啟用 SSL 憑證位置 — 選擇此選項可輸入 SSL 憑證檔案的 Amazon S3 路徑。
 - f. 在驗證中 — 輸入下列資訊：
 - AWS Secrets Manager 祕密 — 選擇現有密碼或建立新 Secrets Manager 密碼來儲存您的 Microsoft SQL Server 驗證認證。如果您選擇建立新密碼，則會開啟一個 AWS Secrets Manager 密碼視窗。

- A. 在「建立 AWS Secrets Manager 密碼視窗」中輸入下列資訊：
 - I. 秘密名稱 — 您秘密的名稱。前綴 'AmazonKendraMicrosoft SQL Server-' 會自動添加到您的密碼名稱中。
 - II. 對於資料庫使用者名稱和密碼 — 輸入您從資料庫複製的驗證認證值。
- B. 選擇儲存。
- g. V@@@rtual Private Cloud (VPC) (VPC) — 您可以選擇使用 VPC。如果是這樣，您必須新增子網路和 VPC 安全性群組。
- h. IAM role — 選擇現有 IAM 角色或建立新 IAM 角色以存取存放庫認證和索引內容。

 Note

IAM 用於索引的角色不能用於資料來源。如果您不確定索引或常見問題集是否使用現有角色，請選擇 [建立新角色] 以避免發生錯誤。

- i. 選擇下一步。
7. 在 [設定同步設定] 頁面上，輸入下列資訊：
- a. 在同步範圍中，從下列選項中選擇：
 - SQL 查詢 — 輸入 SQL 查詢陳述式，例如選取和聯結作業。SQL 查詢必須小於 32 KB。Amazon Kendra 會編目符合您查詢的所有資料庫內容。

 Note

如果表格名稱在名稱中包含特殊字元 (非字母數字)，則必須在表格名稱周圍使用方括號。例如，# *[my-database-table]* ### *

- 主索引鍵欄 — 提供資料庫表格的主索引鍵。這標識數據庫中的一個表。
 - 標題欄 — 提供資料庫表格中文件標題欄的名稱。
 - 主體欄 — 提供資料庫表格中文件主體欄的名稱。
- b. 在 [其他設定 — 選用] 中，從下列選項中選擇以同步特定內容，而非同步所有檔案：
 - 變更偵測欄 — 輸入 Amazon Kendra 將用來偵測內容變更的欄名稱。Amazon Kendra 當這些資料行中有任何變更時，會重新建立內容的索引。
 - 使用者 ID 欄 — 輸入包含允許存取內容的使用者 ID 的欄名稱。


- 群組欄 — 輸入包含允許存取內容之群組的欄名稱。
 - 來源 URL 欄 — 輸入包含要編製索引之來源 URL 的資料欄名稱。
 - 時間戳記欄 — 輸入包含時間戳記的欄名稱。Amazon Kendra 使用時間戳記資訊偵測內容中的變更，並僅同步變更的內容。
 - [時區] 欄 — 輸入資料欄的名稱，其中包含要編目之內容的時區。
 - 時間戳記格式 — 輸入包含時間戳記格式的欄名稱，可用來偵測內容變更並重新同步處理內容。
- c. 同步模式 — 選擇資料來源內容變更時要如何更新索引。當您第一次將資料來源同 Amazon Kendra 步處理時，依預設會檢索所有內容並建立索引。如果初始同步失敗，您必須執行資料的完整同步處理，即使您沒有選擇完整同步作為同步模式選項。
- 完全同步：新鮮索引所有內容，並在每次資料來源與索引同步時取代現有內容。
 - 新增、修改的同步：每次資料來源與索引同步時，僅對新內容和已修改的內容建立索引。Amazon Kendra 可以使用資料來源的機制來追蹤內容變更，並為上次同步後變更的內容建立索引。
 - 新增、修改、刪除的同步：每次資料來源與索引同步時，僅對新內容、已修改和刪除的內容建立索引。Amazon Kendra 可以使用資料來源的機制來追蹤內容變更，並為上次同步後變更的內容建立索引。
- d. 在同步執行排程中，對於頻率 — 與資料來源同步的頻率。Amazon Kendra
- e. 選擇下一步。
8. 在 [設定欄位對映] 頁面上，輸入下列資訊：
- a. 從產生的預設資料來源欄位中選取您要對應至 Amazon Kendra 索引的文件 ID、文件標題和來源 URL。
 - b. 新增欄位 — 新增自訂資料來源欄位，以建立要對映的索引欄位名稱和欄位資料類型。
 - c. 選擇下一步。
9. 在 [檢閱並建立] 頁面上，檢查您輸入的資訊是否正確，然後選取 [新增資料來源]。您也可以從此頁面選擇編輯您的資訊。成功新增資料來源後，您的資料來源將顯示在 [資料來源] 頁面上。

API

若要連線 Amazon Kendra 到 Microsoft SQL Server

您必須使用 [TemplateConfiguration](#) API 指定下列項目：


- 資料來源 — 指定使用 [TemplateConfiguration](#) JSON 結構定義 JDBC 時的資料來源類型。同時將資料來源指定為呼叫 [CreateDataSource](#) API TEMPLATE 時的方式。
- 資料庫類型 — 您必須將資料庫類型指定為 `sqlserver`。
- SQL 查詢 — 指定 SQL 查詢陳述式，例如 SELECT 和 JOIN 作業。SQL 查詢必須小於 32 KB。Amazon Kendra 會編目符合您查詢的所有資料庫內容。

 Note

如果表格名稱在名稱中包含特殊字元 (非字母數字)，則必須在表格名稱周圍使用方括號。
例如，`# [my-database-table] ### *`

- 同步模式 — 指定資料來源內容變更時 Amazon Kendra 應如何更新索引。當您第一次將資料來源同 Amazon Kendra 步處理時，依預設會檢索所有內容並建立索引。如果初始同步失敗，您必須執行資料的完整同步處理，即使您沒有選擇完整同步作為同步模式選項。您可以選擇：
 - `FORCED_FULL_CRAWL` 新建索引所有內容，並在每次資料來源與索引同步時取代現有內容。
 - `FULL_CRAWL`，以在每次資料來源與索引同步時，僅對新的、修改的和刪除的內容建立索引。Amazon Kendra 可以使用資料來源的機制來追蹤內容變更，並為上次同步後變更的內容建立索引。
 - `CHANGE_LOG` 每次資料來源與索引同步時，僅對新內容和修改的內容建立索引。Amazon Kendra 可以使用資料來源的機制來追蹤內容變更，並為上次同步後變更的內容建立索引。
- 秘密 Amazon 資源名稱 (ARN) — 提供包含您在帳戶中建立的身份驗證登入資料的 Secrets Manager 密碼的 Amazon 資源名稱 (ARN)。Microsoft SQL Server 密碼會以下列金鑰儲存在 JSON 結構中：

```
{
  "user name": "database user name",
  "password": "password"
}
```


 Note

我們建議您定期重新整理或輪換您的認證和密碼。僅為您自己的安全提供必要的訪問級別。我們不建議您跨資料來源以及連接器 1.0 和 2.0 版 (如果適用) 重複使用認證和密碼。

- IAM role — 指定RoleArn何時呼叫CreateDataSource以提供具有存取 Secrets Manager 密碼之權限的 IAM 角色，以及呼叫Microsoft SQL Server連接器和 Amazon Kendra所需公用 API 的時間。有關詳情，請參閱[Microsoft SQL Server料來源的IAM 角色](#)。

您還可以添加以下可選功能：

- Virtual Private Cloud (VPC) — 指定您撥打電話的VpcConfiguration時間。CreateDataSource如需詳細資訊，請參閱 [配置 Amazon Kendra 為使用 Amazon VPC](#)。
- 包含和排除篩選器 — 您可以指定是否要使用使用者 ID、群組、來源 URL、時間戳記和時區來包含特定內容。
- 使用者前後關聯篩選與存取控制 — Amazon Kendra 探索文件的存取控制清單 (ACL) (如果您有文件的 ACL)。ACL 資訊可用來根據使用者或使用者對文件的群組存取權來篩選搜尋結果。如需詳細資訊，請參閱[使用者內容篩選](#)。
- 欄位對映 — 選擇將Microsoft SQL Server料來源欄位對映至 Amazon Kendra 索引欄位。如需詳細資訊，請參閱[映射資料來源欄位](#)。

 Note

您的文件需要文件內文欄位或文件內文對等項目，才能搜尋您的文件。Amazon Kendra 您必須將資料來源中的文件內文欄位名稱對應至索引欄位名稱_document_body。所有其他欄位是選用的。

如需要設定的其他重要 JSON 金鑰清單，請參閱[Microsoft SQL 服務器模板架構](#)。

備註

- Amazon Kendra 檢查更新的內容時，不會追蹤已刪除的資料庫列。
- 資料庫中一列中欄位名稱和值的大小不得超過 400 KB。
- 如果您的資料庫資料來源中有大量資料，並且不想 Amazon Kendra 在第一次同步之後對所有資料庫內容建立索引，則可以選擇僅同步新文件、修改或刪除的文件。
- 最佳作法是提供 Amazon Kendra 唯讀資料庫認證。
- 最佳做法是避免新增包含敏感資料或個人可識別資訊 (PII) 的表格。

Microsoft Teams

Microsoft 團隊是用於消息傳遞，會議和文件共享的企業協作工具。如果您是 Microsoft 團隊使用者，您可以使 Amazon Kendra 用索引您的 Microsoft 團隊資料來源。

您可以使用[Amazon Kendra 主控台](#)和 [TemplateConfiguration](#)API 連線 Amazon Kendra 到您的 Microsoft 團隊資料來源。

如需疑難排解 Amazon Kendra Microsoft Teams 資料來源連接器，請參閱[疑難排解資料來](#)。

主題

- [支援的功能](#)
- [必要條件](#)
- [連接說明](#)
- [進一步了解](#)

支援的功能

- 欄位對映
- 使用者存取控制
- 包含/排除過濾器
- 完整和增量內容同步
- 虛擬私有雲端 (VPC)

必要條件

在您可以使用 Amazon Kendra 來索引您的 Microsoft 團隊資料來源之前，請先在您的 Microsoft 小組和 AWS 帳戶中進行這些變更。

在 Microsoft 團隊中，請確保您擁有：

- 在辦公室 365 中創建了一個 Microsoft 團隊帳戶。
- 注意到您的 Microsoft 365 租戶 ID。您可以在 Azure 作用中目錄入口網站的內容或 OAuth 應用程式中找到您的租用戶識別碼。
- 在 Azure 入口網站中設定 OAuth 應用程式，並記下用戶端識別碼和用戶端密碼或用戶端認證。如需詳細資訊，請參閱 [Microsoft 教學課程](#)和 [已註冊應用程式](#)

Note

當您在 Azure 入口網站中建立或註冊應用程式時，秘密識別碼代表實際的密碼值。建立密碼和應用程式時，您必須立即記下或儲存實際的密碼值。您可以在 Azure 入口網站中選取應用程式的名稱，然後導覽至憑證和密碼的功能表選項，以存取您的密碼。

您可以在 Azure 入口網站中選取應用程式的名稱，然後導覽至概觀頁面，以存取用戶端識別碼。應用程式 (客戶端) ID 是客戶端 ID。

Note

我們建議您定期重新整理或輪換您的認證和密碼。僅為您自己的安全提供必要的訪問級別。我們不建議您跨資料來源以及連接器 1.0 和 2.0 版 (如果適用) 重複使用認證和密碼。

- 添加了必要的權限。您可以選擇新增所有權限，也可以根據要編目的實體選取較少的權限來限制範圍。下表依對應實體列出應用程式層級權限：

實體	資料同步所需的權限	身分同步所需的權限
頻道郵報	<ul style="list-style-type: none"> • ChannelMessage 閱讀全部 • 群組 閱讀全部 • 使用者. 讀取 • 使用者 .Read. 全部 	TeamMember 閱讀全部
頻道附件	<ul style="list-style-type: none"> • ChannelMessage 閱讀全部 • 群組 閱讀全部 • 使用者. 讀取 • 使用者 .Read. 全部 	TeamMember 閱讀全部
頻道維基	<ul style="list-style-type: none"> • 群組 閱讀全部 • 使用者. 讀取 • 使用者 .Read. 全部 	TeamMember 閱讀全部
聊天訊息	<ul style="list-style-type: none"> • 聊天 閱讀全部 • ChatMessage 閱讀全部 	TeamMember 閱讀全部

實體	資料同步所需的權限	身分同步所需的權限
	<ul style="list-style-type: none"> • ChatMember 閱讀全部 • 使用者. 讀取 • 使用者 .Read. 全部 • 群組 閱讀全部 	
會議聊天	<ul style="list-style-type: none"> • 聊天 閱讀全部 • ChatMessage. 閱讀 • ChatMember 閱讀全部 • 使用者. 讀取 • 使用者 .Read. 全部 • 群組 閱讀全部 	TeamMember 閱讀全部
聊天附件	<ul style="list-style-type: none"> • 聊天 閱讀全部 • ChatMessage. 閱讀 • ChatMember 閱讀全部 • 使用者. 讀取 • 使用者 .Read. 全部 • 群組 閱讀全部 	TeamMember 閱讀全部
會議檔案	<ul style="list-style-type: none"> • 聊天 閱讀全部 • ChatMessage 閱讀全部 • ChatMember 閱讀全部 • 使用者. 讀取 • 使用者 .Read. 全部 • 群組 閱讀全部 • 檔案. 閱讀全部 	TeamMember 閱讀全部

實體	資料同步所需的權限	身分同步所需的權限
行事曆會議	<ul style="list-style-type: none"> 聊天閱讀全部 ChatMessage閱讀全部 ChatMember閱讀全部 使用者. 讀取 使用者 .Read. 全部 群組閱讀全部 檔案. 閱讀全部 	TeamMember閱讀全部
會議筆記	<ul style="list-style-type: none"> 使用者. 讀取 使用者 .Read. 全部 群組閱讀全部 檔案. 閱讀全部 	TeamMember閱讀全部

- 核取每個文件在 Microsoft Teams 中，以及您打算用於相同索引的其他資料來源中都是唯一的。您要用於索引的每個資料來源不得包含跨資料來源的相同文件。文件 ID 對索引來說是全域的，而且每個索引必須是唯一的。

在你的 AWS 帳戶，確保你有：

- [建立 Amazon Kendra 索引](#)，如果使用 API，則會記下索引 ID。
- 為您的[資料來源建立 IAM 角色](#)，如果使用 API，則會記錄 IAM 角色的 ARN。

Note

如果您變更驗證類型和認證，則必須更新 IAM 角色才能存取正確的 AWS Secrets Manager 密碼 ID。

- 將您的 Microsoft 團隊驗證憑據存儲在 AWS Secrets Manager 密鑰中，並且如果使用 API，則記錄密碼的 ARN。

Note

我們建議您定期重新整理或輪換您的認證和密碼。僅為您自己的安全提供必要的訪問級別。我們不建議您跨資料來源以及連接器 1.0 和 2.0 版 (如果適用) 重複使用認證和密碼。

如果您沒有現有的 IAM 角色或密碼，則可以在將 Microsoft Teams 資料來源連線到時，使用主控台建立新 IAM 角色和 Secrets Manager 密碼 Amazon Kendra。如果您使用 API，則必須提供現有 IAM 角色和 Secrets Manager 密碼的 ARN，以及索引 ID。

連接說明

若要連線 Amazon Kendra 到您的 Microsoft Teams 資料來源，您必須提供 Microsoft Teams 資料來源的必要詳細資料，Amazon Kendra 以便能夠存取您的資料。如果您尚未設定的 Microsoft 團隊 Amazon Kendra，請參閱[必要條件](#)。

Console

若要連線 Amazon Kendra 到 Microsoft 團隊

1. 登入 AWS Management Console 並開啟[Amazon Kendra 主控台](#)。
2. 在左側導覽窗格中，選擇 [索引]，然後從索引清單中選擇要使用的索引。

Note

您可以選擇在索引設置下配置或編輯您的用戶訪問控制設置。

3. 在 [開始使用] 頁面上，選擇 [新增資料來源]。
4. 在 [新增資料來源] 頁面上，選擇 [Microsoft Teams 連接器]，然後選擇 [新增連接器]。如果使用版本 2 (如果適用)，請選擇帶有「V2.0」標籤的 Microsoft 團隊連接器。
5. 在 [指定資料來源詳細資訊] 頁面上，輸入下列資訊：
 - a. 在名稱和說明中，對於資料來源名稱 — 輸入資料來源的名稱。您可以包含連字號，但不能包含空格。
 - b. (選擇性) 說明 — 輸入資料來源的選用說明。
 - c. 在預設語言中 — 選擇一種語言來篩選索引的文件。除非另有指定，否則語言預設為英文。文件中繼資料中指定的語言會覆寫選取的語言。

- d. 在「標籤」中，針對「新增標籤」— 包含可選標籤以搜尋和篩選資源或追蹤 AWS 成本。
 - e. 選擇下一步。
6. 在 [定義存取和安全性] 頁面上，輸入下列資訊：
- a. 租用戶識別碼 — 輸入您的 Microsoft 365 租用戶識別碼。您可以在 Azure 作用中目錄入口網站的內容或 OAuth 應用程式中找到您的租用戶識別碼。
 - b. 授權 — 開啟或關閉文件的存取控制清單 (ACL) 資訊 (如果您有 ACL)，且想要將其用於存取控制。ACL 會指定使用者和群組可存取的文件。ACL 資訊可用來根據使用者或使用者對文件的群組存取權來篩選搜尋結果。如需詳細資訊，請參閱[使用者內容篩選](#)。
 - c. AWS Secrets Manager 密碼 — 選擇現有密碼或建立新 Secrets Manager 密碼來儲存您的 Microsoft Teams 驗證認證。如果您選擇建立新密碼，則會開啟一個 AWS Secrets Manager 密碼視窗。
 - i. 在「建立 AWS Secrets Manager 密碼視窗」中輸入下列資訊：
 - A. 秘密名稱 — 您秘密的名稱。前綴 'AmazonKendra-Microsoft 團隊-' 會自動添加到您的密碼名稱中。
 - B. 如果是用戶端識別碼和用戶端密碼，請輸入 Azure 入口網站中 Microsoft Teams 中設定的驗證認證。
 - ii. 保存並添加您的秘密。
 - d. 付款模式 — 您可以為您的 Microsoft 團隊帳戶選擇授權和付款模式。Model A 付款模式僅限於需要符合安全性規範的授權和付款模式。B 型付款模式適用於不需要符合安全性規範的授權和付款模式。
 - e. V@@@ irtual Private Cloud (VPC) (VPC) — 您可以選擇使用 VPC。如果是這樣，您必須新增子網路和 VPC 安全性群組。
 - f. 識別爬行者程式 — 指定是否要開啟身分識別爬行 Amazon Kendra 者程式。識別爬行者程式會使用文件的存取控制清單 (ACL) 資訊，根據使用者或使用者對文件的群組存取權來篩選搜尋結果。如果您有文件的 ACL 並選擇使用 ACL，您也可以選擇開啟的身分識別爬行者程式，以設定搜尋結果的[使用者環境定義篩選](#)。Amazon Kendra 否則，如果關閉身分搜索器，則可以公開搜索所有文檔。如果您想要對文件使用存取控制，且身分識別編目程式已關閉，您也可以使用 [PutPrincipalMapping](#) API 來上傳使用者和群組存取資訊以進行使用者內容篩選。
 - g. IAM role — 選擇現有 IAM 角色或建立新 IAM 角色以存取存放庫認證和索引內容。

Note

IAM 用於索引的角色不能用於資料來源。如果您不確定索引或常見問題集是否使用現有角色，請選擇 [建立新角色] 以避免發生錯誤。

- h. 選擇下一步。
7. 在 [設定同步設定] 頁面上，輸入下列資訊：
 - a. 同步內容 — 選取要編目的內容類型。您可以選擇檢索聊天、團隊和行事曆內容。
 - b. 其他設定 — 指定特定行事曆的開始和結束日期、使用者電子郵件、團隊名稱、頻道名稱、附件和 OneNotes。
 - c. 同步模式 — 選擇資料來源內容變更時要如何更新索引。當您第一次將資料來源同 Amazon Kendra 步處理時，依預設會檢索所有內容並建立索引。如果初始同步失敗，您必須執行資料的完整同步處理，即使您沒有選擇完整同步作為同步模式選項。
 - 完全同步：新鮮索引所有內容，並在每次資料來源與索引同步時取代現有內容。
 - 新增、修改的同步：每次資料來源與索引同步時，僅對新內容和已修改的內容建立索引。Amazon Kendra 可以使用資料來源的機制來追蹤內容變更，並為上次同步後變更的內容建立索引。
 - 新增、修改、刪除的同步：每次資料來源與索引同步時，僅對新內容、已修改和刪除的內容建立索引。Amazon Kendra 可以使用資料來源的機制來追蹤內容變更，並為上次同步後變更的內容建立索引。
 - d. 在同步執行排程中，對於頻率 — 選擇同步資料來源內容和更新索引的頻率。
 - e. 選擇下一步。
 8. 在 [設定欄位對映] 頁面上，輸入下列資訊：
 - a. 預設資料來源欄位 — 從 Amazon Kendra 產生的預設資料來源欄位中選取您要對映至索引的資料來源欄位。
 - b. 新增欄位 — 新增自訂資料來源欄位，以建立要對映的索引欄位名稱和欄位資料類型。
 - c. 選擇下一步。
 9. 在 [檢閱並建立] 頁面上，檢查您輸入的資訊是否正確，然後選取 [新增資料來源]。您也可以從此頁面選擇編輯您的資訊。成功新增資料來源後，您的資料來源將顯示在 [資料來源] 頁面上。

API

若要連線 Amazon Kendra 到 Microsoft 團隊

您必須使用 [TemplateConfiguration](#) API 指定 [資料來源結構描述](#) 的 JSON。您必須提供以下信息：

- 資料來源 — 指定使用 [TemplateConfiguration](#) JSON 結構定義 MSTEAMS 時的資料來源類型。同時指定呼叫 [CreateDataSource](#) API TEMPLATE 時的資料來源。
- 租用戶識別碼 — 您可以在 Azure 作用中目錄入口網站的內容或 OAuth 應用程式中找到您的租用戶識別碼。
- 同步模式 — 指定資料來源內容變更時 Amazon Kendra 應如何更新索引。當您第一次將資料來源同 Amazon Kendra 步處理時，依預設會檢索所有內容並建立索引。如果初始同步失敗，您必須執行資料的完整同步處理，即使您沒有選擇完整同步作為同步模式選項。您可以選擇：
 - FORCED_FULL_CRAWL 新建索引所有內容，並在每次資料來源與索引同步時取代現有內容。
 - FULL_CRAWL，以在每次資料來源與索引同步時，僅對新的、修改的和刪除的內容建立索引。Amazon Kendra 可以使用資料來源的機制來追蹤內容變更，並為上次同步後變更的內容建立索引。
 - CHANGE_LOG 每次資料來源與索引同步時，僅對新內容和修改的內容建立索引。Amazon Kendra 可以使用資料來源的機制來追蹤內容變更，並為上次同步後變更的內容建立索引。
- 秘密 Amazon 資源名稱 (ARN) — 提供包含您 Microsoft 團隊帳戶身份驗證登入資料的 Secrets Manager 秘密的 Amazon 資源名稱 (ARN)。密碼會以下列金鑰儲存在 JSON 結構中：


```
{
  "clientId": "client ID",
  "clientSecret": "client secret"
}
```

- IAM 角色 — 指定 RoleArn 當您呼叫 CreateDataSource 以提供具有存取 Secrets Manager 密碼之權限的 IAM 角色，以及呼叫 Microsoft Teams 連接器和 Amazon Kendra 所需公用 API 的時間。如需詳細資訊，請參閱 [Microsoft 團隊資料來源的 IAM 角色](#)。

您還可以添加以下可選功能：


- V@@@ irtual Private Cloud (VPC) — 指定您撥打電話的 VpcConfiguration 時間。CreateDataSource 如需詳細資訊，請參閱 [配置 Amazon Kendra 為使用 Amazon VPC](#)。
- 文件/內容類型：指定是否要檢索聊天訊息和附件、頻道貼文和附件、頻道 Wiki、行事曆內容、會議聊天以及檔案和備註。

- 行事曆內容 — 指定編目行事曆內容的開始和結束日期-時間。
- 包含和排除篩選器 — 指定是否要在 Microsoft Teams 中包含或排除某些內容。您可以包含或排除團隊名稱、頻道名稱、檔案名稱和檔案類型、使用者電子郵件、OneNote 區段和 OneNote 頁面。

 Note

大多數資料來源使用規則運算式模式，這些模式是稱為篩選器的包含或排除模式。如果您指定包含篩選器，則只有符合包含項目篩選器的內容會編製索引。不符合包含篩選器的任何文件都不會建立索引。如果您指定包含和排除篩選器，符合排除篩選器的文件將不會建立索引，即使它們符合包含篩選器也是如此。

- 識別爬行者程式 — 指定是否要開啟身分識別爬行 Amazon Kendra 者程式。識別爬行者程式會使用文件的存取控制清單 (ACL) 資訊，根據使用者或使用者對文件的群組存取權來篩選搜尋結果。如果您有文件的 ACL 並選擇使用 ACL，您也可以選擇開啟的身分識別爬行者程式，以設定搜尋結果的使用者環境定義篩選。Amazon Kendra 否則，如果關閉身分搜索器，則可以公開搜索所有文檔。如果您想要對文件使用存取控制，且身分識別編目程式已關閉，您也可以使用 [PutPrincipalMapping](#) API 來上傳使用者和群組存取資訊以進行使用者內容篩選。
- 欄位對應 — 選擇將您的 Microsoft Teams 資料來源欄位對應至 Amazon Kendra 索引欄位。如需詳細資訊，請參閱 [映射資料來源欄位](#)。

 Note

您的文件需要文件內文欄位或文件內文對等項目，才能搜尋您的文件。Amazon Kendra 您必須將資料來源中的文件內文欄位名稱對應至索引欄位名稱_document_body。所有其他欄位是選用的。

如需要設定的其他重要 JSON 金鑰清單，請參閱 [Microsoft 團隊範本結構描述](#)。

進一步了解

若要深入了解如何 Amazon Kendra 與您的 Microsoft 團隊資料來源整合，請參閱：

- [使用適用於 Microsoft 團隊的 Amazon Kendra 連接器，智慧地搜尋組織的 Microsoft 團隊資料來源](#)

Microsoft 亞默

Microsoft Yammer 是用於消息傳遞，會議和文件共享的企業協作工具。如果您是 Microsoft Yammer 使用者，您可以使用索引您的 Microsoft Yammer 資料 Amazon Kendra 來源。

您可以使用 [Amazon Kendra 主控台](#) 和 [TemplateConfiguration](#) API 連線 Amazon Kendra 到您的 Microsoft Yammer 資料來源。

如需疑難排解 Amazon Kendra Microsoft Yammer 資料來源連接器，請參閱 [疑難排解資料來](#)。

支援的功能

- 欄位對映
- 使用者存取控制
- 包含/排除過濾器
- 完整和增量內容同步
- 虛擬私有雲端 (VPC)

必要條件

在您可以使用索引您 Amazon Kendra 的 Microsoft Yammer 資料來源之前，請先在您的 Microsoft Yammer 和 AWS 帳戶中進行這些變更。

在 Microsoft Yammer 中，請確保您擁有：

- 創建了一個 Microsoft Yammer 管理帳戶辦公室 365。
- 記下您的 Microsoft Yammer 使用者名稱和密碼。
- 注意到您的 Microsoft 365 租戶 ID。您可以在 Azure 作用中目錄入口網站的內容或 OAuth 應用程式中找到您的租用戶識別碼。
- 在 Azure 入口網站中設定 OAuth 應用程式，並記下用戶端識別碼和用戶端密碼或用戶端認證。如需詳細資訊，請參閱 [Microsoft 教學課程](#) 和 [已註冊應用程式](#)

Note

當您在 Azure 入口網站中建立或註冊應用程式時，秘密識別碼代表實際的密碼值。建立密碼和應用程式時，您必須立即記下或儲存實際的密碼值。您可以在 Azure 入口網站中選取應用程式的名稱，然後導覽至憑證和密碼的功能表選項，以存取您的密碼。

您可以在 Azure 入口網站中選取應用程式的名稱，然後導覽至概觀頁面，以存取用戶端識別碼。應用程式 (客戶端) ID 是客戶端 ID。

Note

我們建議您定期重新整理或輪換您的認證和密碼。僅為您自己的安全提供必要的訪問級別。我們不建議您跨資料來源以及連接器 1.0 和 2.0 版 (如果適用) 重複使用認證和密碼。

- 已核取每個文件在 Microsoft Yammer 以及您打算用於相同索引的其他資料來源中是唯一的。您要用於索引的每個資料來源不得包含跨資料來源的相同文件。文件 ID 對索引來說是全域的，而且每個索引必須是唯一的。

在您的中 AWS 帳戶，請確保您具有：

- [建立 Amazon Kendra 索引](#)，如果使用 API，則會記下索引識別碼。
- 為您的[資料來源建立 IAM 角色](#)，如果使用 API，則會記錄 IAM 角色的 ARN。

Note

如果您變更驗證類型和認證，則必須更新 IAM 角色才能存取正確的 AWS Secrets Manager 密碼 ID。

- 將您的 Microsoft Yammer 身份驗證憑據存儲在 AWS Secrets Manager 密鑰中，並且如果使用 API，則會記錄密鑰的 ARN。

Note

我們建議您定期重新整理或輪換您的認證和密碼。僅為您自己的安全提供必要的訪問級別。我們不建議您跨資料來源以及連接器 1.0 和 2.0 版 (如果適用) 重複使用認證和密碼。

如果您沒有現有的 IAM 角色或密碼，則可以在將 Microsoft Yammer 資料來源連線到時，使用主控台建立新 IAM 角色和 Secrets Manager 密碼。Amazon Kendra 如果您使用 API，則必須提供現有 IAM 角色和 Secrets Manager 密碼的 ARN 以及索引 ID。

連接說明

若要連線 Amazon Kendra 到您的 Microsoft Yammer 資料來源，您必須提供您的 Microsoft Yammer 資料來源的必要詳細資料，Amazon Kendra 以便能夠存取您的資料。如果您尚未設定的 Microsoft Yammer Amazon Kendra，請參閱[必要條件](#)。

Console

若要連線 Amazon Kendra 到 Microsoft Yammer


1. 登入 AWS Management Console 並開啟[Amazon Kendra 主控台](#)。
2. 在左側導覽窗格中，選擇 [索引]，然後從索引清單中選擇要使用的索引。

Note

您可以選擇在索引設置下配置或編輯您的用戶訪問控制設置。

3. 在 [開始使用] 頁面上，選擇 [新增資料來源]。
4. 在 [新增資料來源] 頁面上，選擇 [Microsoft Yammer 連接器]，然後選擇 [新增連接器]。如果使用第 2 版 (如果適用)，請選擇具有「V2.0」標籤的 Microsoft Yammer 連接器。
5. 在 [指定資料來源詳細資訊] 頁面上，輸入下列資訊：
 - a. 在名稱和說明中，對於資料來源名稱 — 輸入資料來源的名稱。您可以包含連字號，但不能包含空格。
 - b. (選擇性) 說明 — 輸入資料來源的選用說明。
 - c. 在預設語言中 — 選擇一種語言來篩選索引的文件。除非另有指定，否則語言預設為英文。文件中繼資料中指定的語言會覆寫選取的語言。
 - d. 在「標籤」中，針對「新增標籤」— 包含可選標籤以搜尋和篩選資源或追蹤 AWS 成本。
 - e. 選擇下一步。
6. 在 [定義存取權和安全性] 頁面上，輸入下列資訊：
 - a. 授權 — 開啟或關閉文件的存取控制清單 (ACL) 資訊 (如果您有 ACL)，且想要將其用於存取控制。ACL 會指定使用者和群組可存取的文件。ACL 資訊可用來根據使用者或使用者對文件的群組存取權來篩選搜尋結果。如需詳細資訊，請參閱[使用者內容篩選](#)。
 - b. AWS Secrets Manager 密碼 — 選擇現有密碼或建立新 Secrets Manager 密碼來儲存您的 Microsoft Yammer 驗證認證。如果您選擇建立新密碼，則會開啟一個 AWS Secrets Manager 密碼視窗。

- i. 在「建立 AWS Secrets Manager 密碼視窗」中輸入下列資訊：
 - A. 秘密名稱 — 您秘密的名稱。前綴 'AmazonKendra-Microsoft Yammer-' 會自動添加到您的密碼名稱中。
 - B. 對於使用者名稱、密碼 — 輸入您的 Microsoft Yammer 使用者名稱和密碼。
 - C. 對於用戶端識別碼，用戶端密碼 — 輸入 Azure 入口網站中設定在 Microsoft Yammer 中的驗證認證。
- ii. 保存並添加您的秘密。
- c. V@@ irtual Private Cloud (VPC) (VPC) — 您可以選擇使用 VPC。如果是這樣，您必須新增子網路和 VPC 安全性群組。
- d. 識別爬行者程式 — 指定是否要開啟身分識別爬行 Amazon Kendra 爬行者程式。識別爬行者程式會使用文件的存取控制清單 (ACL) 資訊，根據使用者或使用者對文件的群組存取權來篩選搜尋結果。如果您有文件的 ACL 並選擇使用 ACL，您也可以選擇開啟的身分識別爬行者程式，以設定搜尋結果的使用者環境定義篩選。Amazon Kendra 否則，如果關閉身分搜索器，則可以公開搜索所有文檔。如果您想要對文件使用存取控制，且身分識別編目程式已關閉，您也可以使用 [PutPrincipalMapping](#) API 來上傳使用者和群組存取資訊以進行使用者內容篩選。
- e. IAM role — 選擇現有 IAM 角色或建立新 IAM 角色以存取存放庫認證和索引內容。

 Note

IAM 用於索引的角色不能用於資料來源。如果您不確定索引或常見問題集是否使用現有角色，請選擇 [建立新角色] 以避免發生錯誤。

- f. 選擇下一步。
7. 在 [設定同步設定] 頁面上，輸入下列資訊：
- a. 自日期 — 指定開始在 Microsoft Yammer 中探索資料的日期。
 - b. 同步內容 — 選取要編目的內容類型。例如，公用訊息、私人訊息和附件。
 - c. 其他配置 — 指定您要編目的某些社群名稱，並使用規則運算式模式來包含或排除某些內容。
 - d. 同步模式 — 選擇資料來源內容變更時要如何更新索引。當您第一次將資料來源同 Amazon Kendra 步處理時，依預設會檢索所有內容並建立索引。如果初始同步失敗，您必須執行資料的完整同步處理，即使您沒有選擇完整同步作為同步模式選項。

- 完全同步：新鮮索引所有內容，並在每次資料來源與索引同步時取代現有內容。
 - 新增、修改的同步：每次資料來源與索引同步時，僅對新內容和已修改的內容建立索引。Amazon Kendra 可以使用資料來源的機制來追蹤內容變更，並為上次同步後變更的內容建立索引。
 - 新增、修改、刪除的同步：每次資料來源與索引同步時，僅對新內容、已修改和刪除的內容建立索引。Amazon Kendra 可以使用資料來源的機制來追蹤內容變更，並為上次同步後變更的內容建立索引。
- e. 在同步執行排程中，對於頻率 — 選擇同步資料來源內容和更新索引的頻率。
 - f. 選擇下一步。
8. 在 [設定欄位對映] 頁面上，輸入下列資訊：
 - a. 預設資料來源欄位 — 從 Amazon Kendra 產生的預設資料來源欄位中選取您要對映至索引的資料來源欄位。
 - b. 新增欄位 — 新增自訂資料來源欄位，以建立要對映的索引欄位名稱和欄位資料類型。
 - c. 選擇下一步。
 9. 在 [檢閱並建立] 頁面上，檢查您輸入的資訊是否正確，然後選取 [新增資料來源]。您也可以從此頁面選擇編輯您的資訊。成功新增資料來源後，您的資料來源將顯示在 [資料來源] 頁面上。

API

若要連線 Amazon Kendra 到 Microsoft Yammer

您必須使用 [TemplateConfiguration](#) API 指定 [資料來源結構描述](#) 的 JSON。您必須提供以下信息：

- 資料來源 — 指定使用 [TemplateConfiguration](#) JSON 結構定義 YAMMER 時的資料來源類型。同時將資料來源指定為呼叫 [CreateDataSource](#) API TEMPLATE 時的方式。
- 同步模式 — 指定資料來源內容變更時 Amazon Kendra 應如何更新索引。當您第一次將資料來源同 Amazon Kendra 步處理時，依預設會檢索所有內容並建立索引。如果初始同步失敗，您必須執行資料的完整同步處理，即使您沒有選擇完整同步作為同步模式選項。您可以選擇：
 - FORCED_FULL_CRAWL 新建索引所有內容，並在每次資料來源與索引同步時取代現有內容。
 - FULL_CRAWL，以在每次資料來源與索引同步時，僅對新的、修改的和刪除的內容建立索引。Amazon Kendra 可以使用資料來源的機制來追蹤內容變更，並為上次同步後變更的內容建立索引。
 - CHANGE_LOG 每次資料來源與索引同步時，僅對新內容和修改的內容建立索引。Amazon Kendra 可以使用資料來源的機制來追蹤內容變更，並為上次同步後變更的內容建立索引。

- 秘密 Amazon 資源名稱 (ARN) — 提供包含您 Microsoft Yammer 帳戶身份驗證登入資料的 Secrets Manager 密碼的 Amazon 資源名稱 (ARN)。密碼會以下列金鑰儲存在 JSON 結構中：

```
{
  "username": "user name",
  "password": "password",
  "clientId": "client ID",
  "clientSecret": "client secret"
}
```

- IAM 角色 — 指定 RoleArn 當您呼叫 CreateDataSource 以提供具有存取 Secrets Manager 密碼之權限的 IAM 角色，以及呼叫 Microsoft Yammer 連接器和所需公用 API 的時間。Amazon Kendra 如需詳細資訊，請參閱 [Microsoft Yammer 資料來源的 IAM 角色](#)。

您還可以添加以下可選功能：

- VPC — 指定您撥打電話的 VpcConfiguration 時間。CreateDataSource 如需詳細資訊，請參閱 [配置 Amazon Kendra 為使用 Amazon VPC](#)。
- 文件/內容類型 — 指定是否編目社群內容、郵件和附件以及私人訊息。
- 包含和排除篩選器 — 指定要包含還是排除特定內容。

Note

大多數資料來源使用規則運算式模式，這些模式是稱為篩選器的包含或排除模式。如果您指定包含篩選器，則只有符合包含項目篩選器的內容會編製索引。不符合包含篩選器的任何文件都不會建立索引。如果您指定包含和排除篩選器，符合排除篩選器的文件將不會建立索引，即使它們符合包含篩選器也是如此。

- 識別爬行者程式 — 指定是否要開啟身分識別爬行 Amazon Kendra 爬行者程式。識別爬行者程式會使用文件的存取控制清單 (ACL) 資訊，根據使用者或使用者對文件的群組存取權來篩選搜尋結果。如果您有文件的 ACL 並選擇使用 ACL，您也可以選擇開啟的身分識別爬行者程式，以設定搜尋結果的使用者環境定義篩選。Amazon Kendra 否則，如果關閉身分搜索器，則可以公開搜索所有文檔。如果您想要對文件使用存取控制，且身分識別編目程式已關閉，您也可以使用 [PutPrincipalMapping](#) API 來上傳使用者和群組存取資訊以進行使用者內容篩選。
- 欄位對應 — 選擇將您的 Microsoft Yammer 資料來源欄位對應至 Amazon Kendra 索引欄位。如需詳細資訊，請參閱 [映射資料來源欄位](#)。

Note

您的文件需要文件內文欄位或文件內文對等項目，才能搜尋您的文件。Amazon Kendra 您必須將資料來源中的文件內文欄位名稱對應至索引欄位名稱_document_body。所有其他欄位是選用的。

如需要設定的其他重要 JSON 金鑰清單，請參閱 [Microsoft Yammer 範本結構描述](#)。

進一步了解

若要深入了解如何 Amazon Kendra 與您的 Microsoft Yammer 資料來源整合，請參閱：

- [宣布 Yammer 連接器 Amazon Kendra](#)

MySQL

MySQL 是一個開源的關係數據庫管理系統。如果您是使用 MySQL 者，則可以使用 Amazon Kendra 對資料來源建立索引。資料來源 Amazon Kendra MySQL 資料來源連接器支援 MySQL 8.0。21。

您可以使用 [Amazon Kendra 主控台](#) 和 [TemplateConfiguration API](#) 連線 Amazon Kendra 到 MySQL 資料來源。

如需疑難排解資料來源 Amazon Kendra MySQL 資料來源連接器，請參閱 [疑難排解資料來](#)。

主題

- [支援的功能](#)
- [必要條件](#)
- [連接說明](#)
- [備註](#)

支援的功能

- 欄位對映
- 使用者內容篩選

- 包含/排除過濾器
- 完整和增量內容同步
- 虛擬私有雲端 (VPC)

必要條件

在您可以用來 Amazon Kendra 為資料來源建立索引之前，請先在 MySQL 和 AWS 帳戶中進行這些變更。

在 MySQL 中，請確定您有：

- 記下您的資料庫使用者名稱和密碼。

Important

最佳作法是提供 Amazon Kendra 唯讀資料庫認證。

- 複製您的資料庫主機 URL、連接埠和執行個體。
- 已勾選的每個文件在您打算用於相同索引的其他資料來源中 MySQL 和其他資料來源之間都是唯一的。您要用於索引的每個資料來源不得包含跨資料來源的相同文件。文件 ID 對索引來說是全域的，而且每個索引必須是唯一的。

在你的 AWS 帳戶，確保你有：

- [建立 Amazon Kendra 索引](#)，如果使用 API，則會記下索引 ID。
- 為您的 [資料來源建立 IAM 角色](#)，如果使用 API，則會記錄 IAM 角色的 ARN。

Note

如果您變更驗證類型和認證，則必須更新 IAM 角色以存取正確的 AWS Secrets Manager 密碼 ID。

- 將您的 MySQL 身份驗證憑據存儲在 AWS Secrets Manager 密鑰中，如果使用 API，則記錄密鑰的 ARN。

Note

我們建議您定期重新整理或輪換您的認證和密碼。僅為您自己的安全提供必要的訪問級別。我們不建議您跨資料來源以及連接器 1.0 和 2.0 版 (如果適用) 重複使用認證和密碼。

如果您沒有現有的 IAM 角色或密碼，則可以在將MySQL資料來源連線到時使用主控台建立新 IAM 角色和 Secrets Manager 密碼 Amazon Kendra。如果您使用 API，則必須提供現有 IAM 角色和 Secrets Manager 密碼的 ARN 以及索引 ID。

連接說明

若要連線 Amazon Kendra 到MySQL資料來源，您必須提供MySQL認證的詳細資料，Amazon Kendra 以便存取您的資料。如果您尚未設定「Amazon Kendra 請MySQL參閱[必要條件](#)」。

Console

若要連線 Amazon Kendra 到 MySQL


1. 登入 AWS Management Console 並開啟[Amazon Kendra 主控台](#)。
2. 在左側導覽窗格中，選擇 [索引]，然後從索引清單中選擇要使用的索引。

Note

您可以選擇在索引設置下配置或編輯用戶訪問控制設置。

3. 在 [開始使用] 頁面上，選擇 [新增資料來源]。
4. 在 [新增資料來源] 頁面上，選擇 [MySQL連接器]，然後選擇 [新增連接器]。如果使用版本 2 (如果適用)，請選擇帶有「V2.0」標籤的MySQL連接器。
5. 在 [指定資料來源詳細資訊] 頁面上，輸入下列資訊：
 - a. 在名稱和說明中，對於資料來源名稱 — 輸入資料來源的名稱。您可以包含連字號，但不能包含空格。
 - b. (選擇性) 說明 — 輸入資料來源的選用說明。
 - c. 在預設語言中 — 選擇一種語言來篩選索引的文件。除非另有指定，否則語言預設為英文。文件中繼資料中指定的語言會覆寫選取的語言。
 - d. 在「標籤」中，針對「新增標籤」 — 包含可選標籤以搜尋和篩選資源或追蹤 AWS 成本。

- e. 選擇下一步。
6. 在 [定義存取權和安全性] 頁面上，輸入下列資訊：
 - a. 在來源中，輸入下列資訊：
 - b. 主機 — 輸入資料庫主機名稱。
 - c. 連接埠 — 輸入資料庫連接埠。
 - d. 執行處理 — 輸入資料庫執行處理。
 - e. 啟用 SSL 憑證位置 — 選擇輸入 SSL 憑證檔案的 Amazon S3 路徑。
 - f. 在驗證中 — 輸入下列資訊：
 - AWS Secrets Manager 祕密 — 選擇現有密碼或建立新 Secrets Manager 密碼來儲存您的MySQL驗證認證。如果您選擇建立新密碼，則會開啟一個 AWS Secrets Manager 密碼視窗。
 - A. 在「建立 AWS Secrets Manager 密碼視窗」中輸入下列資訊：
 - I. 秘密名稱 — 您秘密的名稱。前綴 'AmazonKendraMySQL-' 會自動添加到您的密碼名稱中。
 - II. 對於資料庫使用者名稱和密碼 — 輸入您從資料庫複製的驗證認證值。
 - B. 選擇儲存。
 - g. Virtual Private Cloud (VPC) (VPC) — 您可以選擇使用 VPC。如果是這樣，您必須新增子網路 and VPC 安全性群組。
 - h. IAM role — 選擇現有 IAM 角色或建立新 IAM 角色以存取存放庫認證和索引內容。

 Note

IAM 用於索引的角色不能用於資料來源。如果您不確定索引或常見問題集是否使用現有角色，請選擇 [建立新角色] 以避免發生錯誤。

- i. 選擇下一步。
7. 在 [設定同步設定] 頁面上，輸入下列資訊：
 - a. 在同步範圍中，從下列選項中選擇：
 - SQL 查詢 — 輸入 SQL 查詢陳述式，例如選取和聯結作業。SQL 查詢必須小於 32 KB。Amazon Kendra 會編目符合您查詢的所有資料庫內容。

- 主索引鍵欄 — 提供資料庫表格的主索引鍵。這標識數據庫中的一個表。
 - 標題欄 — 提供資料庫表格中文件標題欄的名稱。
 - 主體欄 — 提供資料庫表格中文件主體欄的名稱。
- b. 在 [其他設定 — 選用] 中，從下列選項中選擇以同步特定內容，而非同步所有檔案：
- 變更偵測欄 — 輸入 Amazon Kendra 將用來偵測內容變更的欄名稱。Amazon Kendra 當這些資料行中有任何變更時，會重新建立內容的索引。
 - 使用者 ID 欄 — 輸入包含允許存取內容的使用者 ID 的欄名稱。
 - 群組欄 — 輸入包含允許存取內容之群組的欄名稱。
 - 來源 URL 欄 — 輸入包含要編製索引之來源 URL 的資料欄名稱。
 - 時間戳記欄 — 輸入包含時間戳記的欄名稱。Amazon Kendra 使用時間戳記資訊偵測內容中的變更，並僅同步變更的內容。
 - [時區] 欄 — 輸入資料欄的名稱，其中包含要編目之內容的時區。
 - 時間戳記格式 — 輸入包含時間戳記格式的欄名稱，可用來偵測內容變更並重新同步內容。
- c. 同步模式 — 選擇資料來源內容變更時要如何更新索引。當您第一次將資料來源同 Amazon Kendra 步處理時，依預設會檢索所有內容並建立索引。如果初始同步失敗，您必須執行資料的完整同步，即使您沒有選擇完整同步作為同步模式選項。
- 完全同步：新鮮索引所有內容，並在每次資料來源與索引同步時取代現有內容。
 - 新增、修改的同步：每次資料來源與索引同步時，僅對新內容和已修改的內容建立索引。Amazon Kendra 可以使用資料來源的機制來追蹤內容變更，並為上次同步後變更的內容建立索引。
 - 新增、修改、刪除的同步：每次資料來源與索引同步時，僅對新內容、已修改和刪除的內容建立索引。Amazon Kendra 可以使用資料來源的機制來追蹤內容變更，並為上次同步後變更的內容建立索引。
- d. 在同步執行排程中，對於頻率 — 與資料來源同步的頻率。Amazon Kendra
- e. 選擇下一步。
8. 在 [設定欄位對映] 頁面上，輸入下列資訊：
- a. 從產生的預設資料來源欄位中選取您要對應至 Amazon Kendra 索引的文件 ID、文件標題和來源 URL。
 - b. 新增欄位 — 新增自訂資料來源欄位以建立要對映的索引欄位名稱和欄位資料類型。
 - c. 選擇下一步。

- 在 [檢閱並建立] 頁面上，檢查您輸入的資訊是否正確，然後選取 [新增資料來源]。您也可以從此頁面選擇編輯您的資訊。成功新增資料來源後，您的資料來源將顯示在 [資料來源] 頁面上。

API

若要連線 Amazon Kendra 到 MySQL

您必須使用 [TemplateConfiguration](#) API 指定下列項目：

- 資料來源 — 指定使用 [TemplateConfiguration](#) JSON 結構定義 JDBC 時的資料來源類型。同時指定呼叫 [CreateDataSource](#) API TEMPLATE 時的資料來源。
- 資料庫類型 — 您必須將資料庫類型指定為 `mysql`。
- SQL 查詢 — 指定 SQL 查詢陳述式，例如 `SELECT` 和 `JOIN` 作業。SQL 查詢必須小於 32 KB。Amazon Kendra 會編目符合您查詢的所有資料庫內容。
- 同步模式 — 指定資料來源內容變更時 Amazon Kendra 應如何更新索引。當您第一次將資料來源同 Amazon Kendra 步處理時，依預設會檢索所有內容並建立索引。如果初始同步失敗，您必須執行資料的完整同步，即使您沒有選擇完整同步作為同步模式選項。您可以選擇：
 - `FORCED_FULL_CRAWL` 新建索引所有內容，並在每次資料來源與索引同步時取代現有內容。
 - `FULL_CRAWL`，以在每次資料來源與索引同步時，僅對新的、修改的和刪除的內容建立索引。Amazon Kendra 可以使用資料來源的機制來追蹤內容變更，並為上次同步後變更的內容建立索引。
 - `CHANGE_LOG` 每次資料來源與索引同步時，僅對新內容和修改的內容建立索引。Amazon Kendra 可以使用資料來源的機制來追蹤內容變更，並為上次同步後變更的內容建立索引。
- 秘密 Amazon 資源名稱 (ARN) — 提供包含您在帳戶中建立的身份驗證登入資料的 `Secrets Manager` 密碼的 Amazon 資源名稱 (ARN)。MySQL 密碼會以下列金鑰儲存在 JSON 結構中：

```
{
  "user name": "database user name",
  "password": "password"
}
```


Note

我們建議您定期重新整理或輪換您的認證和密碼。僅為您自己的安全提供必要的訪問級別。我們不建議您跨資料來源以及連接器 1.0 和 2.0 版 (如果適用) 重複使用認證和密碼。

- IAM role — 指定RoleArn何時呼叫CreateDataSource以提供具有存取 Secrets Manager 密碼之權限的 IAM 角色，以及呼叫MySQL連接器和 Amazon Kendra所需公用 API 的時間。有關詳情，請參閱[MySQL料來源的IAM 角色](#)。

您還可以添加以下可選功能：

- Virtual Private Cloud (VPC) — 指定您呼叫的VpcConfiguration時間。CreateDataSource如需詳細資訊，請參閱 [配置 Amazon Kendra 為使用 Amazon VPC](#)。
- 包含和排除篩選器 — 您可以指定是否要使用使用者 ID、群組、來源 URL、時間戳記和時區來包含特定內容。
- 使用者前後關聯篩選與存取控制 — Amazon Kendra 探索文件的存取控制清單 (ACL) (如果您有文件的 ACL)。ACL 資訊可用來根據使用者或使用者對文件的群組存取來篩選搜尋結果。如需詳細資訊，請參閱[使用者內容篩選](#)。
- 欄位對映 — 選擇將MySQL料來源欄位對映至 Amazon Kendra 索引欄位。如需詳細資訊，請參閱[映射資料來源欄位](#)。

 Note

您的文件需要文件內文欄位或文件內文對等項目，才能搜尋您的文件。Amazon Kendra 您必須將資料來源中的文件內文欄位名稱對應至索引欄位名稱_document_body。所有其他欄位是選用的。

備註

- Amazon Kendra 檢查更新的內容時，不會追蹤已刪除的資料庫列。
- 資料庫中一列中欄位名稱和值的大小不得超過 400 KB。
- 如果您的資料庫資料來源中有大量資料，並且不想 Amazon Kendra 在第一次同步之後對所有資料庫內容建立索引，則可以選擇僅同步新文件、修改或刪除的文件。
- 最佳作法是提供 Amazon Kendra 唯讀資料庫認證。
- 最佳做法是避免新增包含敏感資料或個人可識別資訊 (PII) 的表格。

Oracle Database

Oracle Database 是一個數據庫管理系統。如果您是使用 Oracle Database 者，則可以使用 Amazon Kendra 對資 Oracle Database 料來源建立索引。資 Amazon Kendra Oracle Database 料來源連接器支援 Oracle 資料庫 18c、19c 和 21c。

您可以使用 [Amazon Kendra 主控台](#) 和 [TemplateConfiguration](#) API 連線 Amazon Kendra 到 Oracle Database 資料來源。

如需對資 Amazon Kendra Oracle Database 料來源連接器進行疑難排解，請參 [疑難排解資料來](#)

主題

- [支援的功能](#)
- [必要條件](#)
- [連接說明](#)
- [備註](#)

支援的功能

- 欄位對映
- 使用者內容篩選
- 包含/排除過濾器
- 完整和增量內容同步
- 虛擬私有雲端 (VPC)

必要條件

在您可以用來 Amazon Kendra 為資 Oracle Database 料來源建立索引之前，請先在 Oracle Database 和 AWS 帳戶中進行這些變更。

在中 Oracle Database，請確定您有：

- 記下您的資料庫使用者名稱和密碼。

Important

最佳作法是提供 Amazon Kendra 唯讀資料庫認證。

- 複製您的資料庫主機 URL、連接埠和執行個體。
- 已勾選的每個文件在您打算用於相同索引的其他資料來源中 Oracle Database 和其他資料來源之間都是唯一的。您要用於索引的每個資料來源不得包含跨資料來源的相同文件。文件 ID 對索引來說是全域的，而且每個索引必須是唯一的。

在您的 AWS 帳戶，請確保您有：

- [建立 Amazon Kendra 索引](#)，如果使用 API，則會記下索引識別碼。
- 為您的 [資料來源建立 IAM 角色](#)，如果使用 API，則會記錄 IAM 角色的 ARN。

Note

如果您變更驗證類型和認證，則必須更新 IAM 角色才能存取正確的 AWS Secrets Manager 密碼 ID。

- 將您的 Oracle Database 身份驗證憑據存儲在 AWS Secrets Manager 密鑰中，如果使用 API，則記錄密鑰的 ARN。

Note

我們建議您定期重新整理或輪換您的認證和密碼。僅為您自己的安全提供必要的訪問級別。我們不建議您跨資料來源以及連接器 1.0 和 2.0 版 (如果適用) 重複使用認證和密碼。

如果您沒有現有的 IAM 角色或密碼，則可以在將 Oracle Database 資料來源連線到時使用主控台建立新 IAM 角色和 Secrets Manager 密碼 Amazon Kendra。如果您使用 API，則必須提供現有 IAM 角色和 Secrets Manager 密碼的 ARN，以及索引 ID。

連接說明


若要連線 Amazon Kendra 到 Oracle Database 資料來源，您必須提供 Oracle Database 認證的詳細資料，Amazon Kendra 以便能夠存取您的資料。如果您尚未設定「Amazon Kendra 請 Oracle Database 參閱 [必要條件](#)」。

Console

若要連線 Amazon Kendra 到 Oracle Database

1. 登入 AWS Management Console 並開啟 [Amazon Kendra 主控台](#)。

2. 在左側導覽窗格中，選擇 [索引]，然後從索引清單中選擇要使用的索引。

 Note

您可以選擇在索引設置下配置或編輯您的用戶訪問控制設置。

3. 在 [開始使用] 頁面上，選擇 [新增資料來源]。
4. 在 [新增資料來源] 頁面上，選擇 [Oracle Database 連接器]，然後選擇 [新增連接器]。如果使用版本 2 (如果適用)，請選擇帶有「V2.0」標籤的 Oracle Database 連接器。
5. 在 [指定資料來源詳細資訊] 頁面上，輸入下列資訊：
 - a. 在名稱和說明中，對於資料來源名稱 — 輸入資料來源的名稱。您可以包含連字號，但不能包含空格。
 - b. (選擇性) 說明 — 輸入資料來源的選用說明。
 - c. 在預設語言中 — 選擇一種語言來篩選索引的文件。除非另有指定，否則語言預設為英文。文件中繼資料中指定的語言會覆寫選取的語言。
 - d. 在「標籤」中，針對「新增標籤」— 包含可選標籤以搜尋和篩選資源或追蹤 AWS 成本。
 - e. 選擇下一步。
6. 在 [定義存取權和安全性] 頁面上，輸入下列資訊：
 - a. 在來源中，輸入下列資訊：
 - b. 主機 — 輸入資料庫主機名稱。
 - c. 連接埠 — 輸入資料庫連接埠。
 - d. 執行處理 — 輸入資料庫執行處理。
 - e. 啟用 SSL 憑證位置 — 選擇此選項可輸入 SSL 憑證檔案的 Amazon S3 路徑。
 - f. 在驗證中 — 輸入下列資訊：
 - AWS Secrets Manager 祕密 — 選擇現有密碼或建立新 Secrets Manager 密碼來儲存您的 Oracle Database 驗證認證。如果您選擇建立新密碼，則會開啟一個 AWS Secrets Manager 密碼視窗。
 - A. 在「建立 AWS Secrets Manager 密碼視窗」中輸入下列資訊：
 - I. 祕密名稱 — 您祕密的名稱。前綴 'AmazonKendraOracle Database-' 會自動添加到您的密碼名稱中。
 - II. 對於資料庫使用者名稱和密碼 — 輸入您從資料庫複製的驗證認證值。

B. 選擇儲存。

- g. Virtual Private Cloud (VPC) (VPC) — 您可以選擇使用 VPC。如果是這樣，您必須新增子網路和 VPC 安全性群組。
- h. IAM role — 選擇現有 IAM 角色或建立新 IAM 角色以存取存放庫認證和索引內容。

Note

IAM 用於索引的角色不能用於資料來源。如果您不確定索引或常見問題集是否使用現有角色，請選擇 [建立新角色] 以避免發生錯誤。

- i. 選擇下一步。

7. 在 [設定同步設定] 頁面上，輸入下列資訊：

- a. 在同步範圍中，從下列選項中選擇：

- SQL 查詢 — 輸入 SQL 查詢陳述式，例如 SELECT 和 JOIN 作業。SQL 查詢必須小於 32 KB。Amazon Kendra 會編目符合您查詢的所有資料庫內容。
- 主索引鍵欄 — 提供資料庫表格的主索引鍵。這標識數據庫中的一個表。
- 標題欄 — 提供資料庫表格中文件標題欄的名稱。
- 主體欄 — 提供資料庫表格中文件主體欄的名稱。

- b. 在 [其他設定 — 選用] 中，從下列選項中選擇以同步特定內容，而非同步所有檔案：

- 變更偵測欄 — 輸入 Amazon Kendra 將用來偵測內容變更的欄名稱。Amazon Kendra 當這些資料行中有任何變更時，會重新建立內容的索引。
- 使用者 ID 欄 — 輸入包含允許存取內容的使用者 ID 的欄名稱。
- 群組欄 — 輸入包含允許存取內容之群組的欄名稱。
- 來源 URL 欄 — 輸入包含要編製索引之來源 URL 的資料欄名稱。
- 時間戳記欄 — 輸入包含時間戳記的欄名稱。Amazon Kendra 使用時間戳記資訊偵測內容中的變更，並僅同步變更的內容。
- [時區] 欄 — 輸入資料欄的名稱，其中包含要編目之內容的時區。
- 時間戳記格式 — 輸入包含時間戳記格式的欄名稱，可用來偵測內容變更並重新同步處理內容。

- c. 同步模式 — 選擇資料來源內容變更時要如何更新索引。當您第一次將資料來源同 Amazon Kendra 步處理時，依預設會檢索所有內容並建立索引。如果初始同步失敗，您必須執行資料的完整同步處理，即使您沒有選擇完整同步作為同步模式選項。

- 完全同步：新鮮索引所有內容，並在每次資料來源與索引同步時取代現有內容。
 - 新增、修改的同步：每次資料來源與索引同步時，僅對新內容和已修改的內容建立索引。Amazon Kendra 可以使用資料來源的機制來追蹤內容變更，並為上次同步後變更的內容建立索引。
 - 新增、修改、刪除的同步：每次資料來源與索引同步時，僅對新內容、已修改和刪除的內容建立索引。Amazon Kendra 可以使用資料來源的機制來追蹤內容變更，並為上次同步後變更的內容建立索引。
- d. 在同步執行排程中，對於頻率 — 與資料來源同步的頻率。Amazon Kendra
 - e. 選擇下一步。
8. 在 [設定欄位對映] 頁面上，輸入下列資訊：
- a. 從產生的預設資料來源欄位中選取您要對應至 Amazon Kendra 索引的文件 ID、文件標題和來源 URL。
 - b. 新增欄位 — 新增自訂資料來源欄位，以建立要對映的索引欄位名稱和欄位資料類型。
 - c. 選擇下一步。
9. 在 [檢閱並建立] 頁面上，檢查您輸入的資訊是否正確，然後選取 [新增資料來源]。您也可以從此頁面選擇編輯您的資訊。成功新增資料來源後，您的資料來源將顯示在 [資料來源] 頁面上。

API


若要連線 Amazon Kendra 到 Oracle Database

您必須使用 [TemplateConfiguration](#) API 指定下列項目：

- 資料來源 — 指定使用 [TemplateConfiguration](#) JSON 結構定義 JDBC 時的資料來源類型。同時將資料來源指定為呼叫 [CreateDataSource](#) API TEMPLATE 時的方式。
- 資料庫類型 — 您必須將資料庫類型指定為 `oracle`。
- SQL 查詢 — 指定 SQL 查詢陳述式，例如 SELECT 和 JOIN 作業。SQL 查詢必須小於 32 KB。Amazon Kendra 會編目符合您查詢的所有資料庫內容。
- 同步模式 — 指定資料來源內容變更時 Amazon Kendra 應如何更新索引。當您第一次將資料來源同 Amazon Kendra 步處理時，依預設會檢索所有內容並建立索引。如果初始同步失敗，您必須執行資料的完整同步處理，即使您沒有選擇完整同步作為同步模式選項。您可以選擇：
 - `FORCED_FULL_CRAWL` 新建索引所有內容，並在每次資料來源與索引同步時取代現有內容。

- FULL_CRAWL，以在每次資料來源與索引同步時，僅對新的、修改的和刪除的內容建立索引。Amazon Kendra 可以使用資料來源的機制來追蹤內容變更，並為上次同步後變更的內容建立索引。
- CHANGE_LOG每次資料來源與索引同步時，僅對新內容和修改的內容建立索引。Amazon Kendra 可以使用資料來源的機制來追蹤內容變更，並為上次同步後變更的內容建立索引。
- 秘密 Amazon 資源名稱 (ARN) — 提供包含您在帳戶中建立的身份驗證登入資料的 Secrets Manager 密碼的 Amazon 資源名稱 (ARN)。Oracle Database密碼會以下列金鑰儲存在 JSON 結構中：

```
{  
  "user name": "database user name",  
  "password": "password"  
}
```

 Note

我們建議您定期重新整理或輪換您的認證和密碼。僅為您自己的安全提供必要的訪問級別。我們不建議您跨資料來源以及連接器 1.0 和 2.0 版 (如果適用) 重複使用認證和密碼。

- IAM role — 指定RoleArn何時呼叫CreateDataSource以提供具有存取 Secrets Manager 密碼之權限的 IAM 角色，以及呼叫Oracle Database連接器和 Amazon Kendra所需公用 API 的時間。有關詳情，請參閱[Oracle Database料來源的IAM 角色](#)。

您還可以添加以下可選功能：

- Virtual Private Cloud (VPC) — 指定您撥打電話的VpcConfiguration時間。CreateDataSource如需詳細資訊，請參閱 [配置 Amazon Kendra 為使用 Amazon VPC](#)。
- 包含和排除篩選器 — 您可以指定是否要使用使用者 ID、群組、來源 URL、時間戳記和時區來包含特定內容。
- 使用者前後關聯篩選與存取控制 — Amazon Kendra 探索文件的存取控制清單 (ACL) (如果您有文件的 ACL)。ACL 資訊可用來根據使用者或使用者對文件的群組存取權來篩選搜尋結果。如需詳細資訊，請參閱[使用者內容篩選](#)。
- 欄位對映 — 選擇將Oracle Database料來源欄位對映至 Amazon Kendra 索引欄位。如需詳細資訊，請參閱[映射資料來源欄位](#)。

Note

您的文件需要文件內文欄位或文件內文對等項目，才能搜尋您的文件。Amazon Kendra 您必須將資料來源中的文件內文欄位名稱對應至索引欄位名稱_document_body。所有其他欄位是選用的。

如需要設定的其他重要 JSON 金鑰清單，請參閱[Oracle 資料庫範本綱要](#)。

備註

- Amazon Kendra 檢查更新的內容時，不會追蹤已刪除的資料庫列。
- 資料庫中一系列欄位名稱和值的大小不得超過 400 KB。
- 如果您的資料庫資料來源中有大量資料，並且不想 Amazon Kendra 在第一次同步之後對所有資料庫內容建立索引，則可以選擇僅同步新文件、修改或刪除的文件。
- 最佳作法是提供 Amazon Kendra 唯讀資料庫認證。
- 最佳做法是避免新增包含敏感資料或個人可識別資訊 (PII) 的表格。

PostgreSQL

PostgreSQL 是一個開源數據庫管理系統。如果您是使用 PostgreSQL 者，則可以使用 Amazon Kendra 對 PostgreSQL 資料來源建立索引。Amazon Kendra PostgreSQL 資料來源連接器支援 PostgreSQL 9.6。

您可以使用[Amazon Kendra 主控台](#)和 [TemplateConfiguration](#) API 連線 Amazon Kendra 到 PostgreSQL 資料來源。

如需疑難排解 Amazon Kendra PostgreSQL 資料來源連接器，請參閱[疑難排解資料來](#)。

主題

- [支援的功能](#)
- [必要條件](#)
- [連接說明](#)
- [備註](#)

支援的功能

- 欄位對映
- 使用者內容篩選
- 包含/排除過濾器
- 完整和增量內容同步
- 虛擬私有雲端 (VPC)

必要條件

在您可以用來 Amazon Kendra 為資 PostgreSQL 料來源建立索引之前，請先在 PostgreSQL 和 AWS 帳戶中進行這些變更。

在中 PostgreSQL，請確定您有：

- 記下您的資料庫使用者名稱和密碼。

Important

最佳作法是提供 Amazon Kendra 唯讀資料庫認證。

- 複製您的資料庫主機 URL、連接埠和執行個體。
- 已勾選的每個文件在您打算用於相同索引的其他資料來源中 PostgreSQL 和其他資料來源之間都是唯一的。您要用於索引的每個資料來源不得包含跨資料來源的相同文件。文件 ID 對索引來說是全域的，而且每個索引必須是唯一的。

在你的 AWS 帳戶，確保你有：

- [建立 Amazon Kendra 索引](#)，如果使用 API，則會記下索引 ID。
- 為您的[資料來源建立 IAM 角色](#)，如果使用 API，則會記錄 IAM 角色的 ARN。

Note

如果您變更驗證類型和認證，則必須更新 IAM 角色才能存取正確的 AWS Secrets Manager 密碼 ID。

- 將您的PostgreSQL身份驗證憑據存儲在 AWS Secrets Manager 密鑰中，如果使用 API，則記錄密鑰的 ARN。

Note

我們建議您定期重新整理或輪換您的認證和密碼。僅為您自己的安全提供必要的訪問級別。我們不建議您跨資料來源以及連接器 1.0 和 2.0 版 (如果適用) 重複使用認證和密碼。

如果您沒有現有的 IAM 角色或密碼，則可以在將 PostgreSQL 資料來源連線到時使用主控台建立新 IAM 角色和 Secrets Manager 密碼 Amazon Kendra。如果您使用 API，則必須提供現有 IAM 角色和 Secrets Manager 密碼的 ARN，以及索引 ID。

連接說明

若要連線 Amazon Kendra 到 PostgreSQL 資料來源，您必須提供 PostgreSQL 認證的詳細資料，Amazon Kendra 以便能夠存取您的資料。如果您尚未設定「Amazon Kendra 請 PostgreSQL 參閱 [必要條件](#)」。

Console

若要連線 Amazon Kendra 到 PostgreSQL


1. 登入 AWS Management Console 並開啟 [Amazon Kendra 主控台](#)。
2. 在左側導覽窗格中，選擇 [索引]，然後從索引清單中選擇要使用的索引。

Note

您可以選擇在索引設置下配置或編輯您的用戶訪問控制設置。

3. 在 [開始使用] 頁面上，選擇 [新增資料來源]。
4. 在 [新增資料來源] 頁面上，選擇 [PostgreSQL 連接器]，然後選擇 [新增連接器]。如果使用版本 2 (如果適用)，請選擇帶有「V2.0」標籤的 PostgreSQL 連接器。
5. 在 [指定資料來源詳細資訊] 頁面上，輸入下列資訊：
 - a. 在名稱和說明中，對於資料來源名稱 — 輸入資料來源的名稱。您可以包含連字號，但不能包含空格。
 - b. (選擇性) 說明 — 輸入資料來源的選用說明。

- c. 在預設語言中 — 選擇一種語言來篩選索引的文件。除非另有指定，否則語言預設為英文。文件中繼資料中指定的語言會覆寫選取的語言。
 - d. 在「標籤」中，針對「新增標籤」 — 包含可選標籤以搜尋和篩選資源或追蹤 AWS 成本。
 - e. 選擇下一步。
6. 在 [定義存取和安全性] 頁面上，輸入下列資訊：
- a. 在來源中，輸入下列資訊：
 - b. 主機 — 輸入資料庫主機名稱。
 - c. 連接埠 — 輸入資料庫連接埠。
 - d. 執行處理 — 輸入資料庫執行處理。
 - e. 啟用 SSL 憑證位置 — 選擇此選項可輸入 SSL 憑證檔案的 Amazon S3 路徑。
 - f. 在驗證中 — 輸入下列資訊：
 - AWS Secrets Manager 祕密 — 選擇現有密碼或建立新 Secrets Manager 密碼來儲存您的 PostgreSQL 驗證認證。如果您選擇建立新密碼，則會開啟一個 AWS Secrets Manager 密碼視窗。
 - A. 在「建立 AWS Secrets Manager 密碼視窗」中輸入下列資訊：
 - I. 秘密名稱 — 您秘密的名稱。前綴 'AmazonKendraPostgreSQL-' 會自動添加到您的密碼名稱中。
 - II. 對於資料庫使用者名稱和密碼 — 輸入您從資料庫複製的驗證認證值。
 - B. 選擇儲存。
 - g. V@@@ irtual Private Cloud (VPC) (VPC) — 您可以選擇使用 VPC。如果是這樣，您必須新增子網路和 VPC 安全性群組。
 - h. IAM role — 選擇現有 IAM 角色或建立新 IAM 角色以存取存放庫認證和索引內容。

 Note

IAM 用於索引的角色不能用於資料來源。如果您不確定索引或常見問題集是否使用現有角色，請選擇 [建立新角色] 以避免發生錯誤。

- i. 選擇下一步。
7. 在 [設定同步設定] 頁面上，輸入下列資訊：
- a. 在同步範圍中，從下列選項中選擇：

- SQL 查詢 — 輸入 SQL 查詢陳述式，例如選取和聯結作業。SQL 查詢必須小於 32 KB。Amazon Kendra 會編目符合您查詢的所有資料庫內容。
 - 主索引鍵欄 — 提供資料庫表格的主索引鍵。這標識數據庫中的一個表。
 - 標題欄 — 提供資料庫表格中文件標題欄的名稱。
 - 主體欄 — 提供資料庫表格中文件主體欄的名稱。
- b. 在 [其他設定 — 選用] 中，從下列選項中選擇以同步特定內容，而非同步所有檔案：
- 變更偵測欄 — 輸入 Amazon Kendra 將用來偵測內容變更的欄名稱。Amazon Kendra 當這些資料行中有任何變更時，會重新建立內容的索引。
 - 使用者 ID 欄 — 輸入包含允許存取內容的使用者 ID 的欄名稱。
 - 群組欄 — 輸入包含允許存取內容之群組的欄名稱。
 - 來源 URL 欄 — 輸入包含要編製索引之來源 URL 的資料欄名稱。
 - 時間戳記欄 — 輸入包含時間戳記的欄名稱。Amazon Kendra 使用時間戳記資訊偵測內容中的變更，並僅同步變更的內容。
 - [時區] 欄 — 輸入資料欄的名稱，其中包含要編目之內容的時區。
 - 時間戳記格式 — 輸入包含時間戳記格式的欄名稱，可用來偵測內容變更並重新同步處理內容。
- c. 同步模式 — 選擇資料來源內容變更時要如何更新索引。當您第一次將資料來源同 Amazon Kendra 步處理時，依預設會檢索所有內容並建立索引。如果初始同步失敗，您必須執行資料的完整同步處理，即使您沒有選擇完整同步作為同步模式選項。
- 完全同步：新鮮索引所有內容，並在每次資料來源與索引同步時取代現有內容。
 - 新增、修改的同步：每次資料來源與索引同步時，僅對新內容和已修改的內容建立索引。Amazon Kendra 可以使用資料來源的機制來追蹤內容變更，並為上次同步後變更的內容建立索引。
 - 新增、修改、刪除的同步：每次資料來源與索引同步時，僅對新內容、已修改和刪除的內容建立索引。Amazon Kendra 可以使用資料來源的機制來追蹤內容變更，並為上次同步後變更的內容建立索引。
- d. 在同步執行排程中，對於頻率 — 與資料來源同步的頻率。Amazon Kendra
- e. 選擇下一步。
8. 在 [設定欄位對映] 頁面上，輸入下列資訊：
- a. 從產生的預設資料來源欄位中選取您要對應至 Amazon Kendra 索引的文件 ID、文件標題和來源 URL。

- b. 新增欄位 — 新增自訂資料來源欄位，以建立要對映的索引欄位名稱和欄位資料類型。
 - c. 選擇下一步。
9. 在 [檢閱並建立] 頁面上，檢查您輸入的資訊是否正確，然後選取 [新增資料來源]。您也可以從此頁面選擇編輯您的資訊。成功新增資料來源後，您的資料來源將顯示在 [資料來源] 頁面上。

API

若要連線 Amazon Kendra 到 PostgreSQL

您必須使用 [TemplateConfiguration](#) API 指定下列項目：

- 資料來源 — 指定使用 [TemplateConfiguration](#) JSON 結構定義 JDBC 時的資料來源類型。同時將資料來源指定為呼叫 [CreateDataSource](#) API TEMPLATE 時的方式。
- 資料庫類型 — 您必須將資料庫類型指定為 postgresql。
- SQL 查詢 — 指定 SQL 查詢陳述式，例如 SELECT 和 JOIN 作業。SQL 查詢必須小於 32 KB。Amazon Kendra 會編目符合您查詢的所有資料庫內容。
- 同步模式 — 指定資料來源內容變更時 Amazon Kendra 應如何更新索引。當您第一次將資料來源同 Amazon Kendra 步處理時，依預設會檢索所有內容並建立索引。如果初始同步失敗，您必須執行資料的完整同步處理，即使您沒有選擇完整同步作為同步模式選項。您可以選擇：
 - FORCED_FULL_CRAWL 新建索引所有內容，並在每次資料來源與索引同步時取代現有內容。
 - FULL_CRAWL，以在每次資料來源與索引同步時，僅對新的、修改的和刪除的內容建立索引。Amazon Kendra 可以使用資料來源的機制來追蹤內容變更，並為上次同步後變更的內容建立索引。
 - CHANGE_LOG 每次資料來源與索引同步時，僅對新內容和修改的內容建立索引。Amazon Kendra 可以使用資料來源的機制來追蹤內容變更，並為上次同步後變更的內容建立索引。
- 秘密 Amazon 資源名稱 (ARN) — 提供包含您在帳戶中建立的身份驗證登入資料的 Secrets Manager 密碼的 Amazon 資源名稱 (ARN)。PostgreSQL 密碼會以下列金鑰儲存在 JSON 結構中：

```
{
  "user name": "database user name",
  "password": "password"
}
```

Note

我們建議您定期重新整理或輪換您的認證和密碼。僅為您自己的安全提供必要的訪問級別。我們不建議您跨資料來源以及連接器 1.0 和 2.0 版 (如果適用) 重複使用認證和密碼。

- IAM role — 指定RoleArn何時呼叫CreateDataSource以提供具有存取 Secrets Manager 密碼之權限的 IAM 角色，以及呼叫PostgreSQL連接器和 Amazon Kendra所需公用 API 的時間。有關詳情，請參閱[PostgreSQL料來源的IAM 角色](#)。

您還可以添加以下可選功能：

- VPC — 指定您撥打電話的VpcConfiguration時間。CreateDataSource如需詳細資訊，請參閱 [配置 Amazon Kendra 為使用 Amazon VPC](#)。
- 包含和排除篩選器 — 您可以指定是否要使用使用者 ID、群組、來源 URL、時間戳記和時區來包含特定內容。
- 使用者前後關聯篩選與存取控制 — Amazon Kendra 探索文件的存取控制清單 (ACL) (如果您有文件的 ACL)。ACL 資訊可用來根據使用者或使用者對文件的群組存取權來篩選搜尋結果。如需詳細資訊，請參閱[使用者內容篩選](#)。
- 欄位對映 — 選擇將PostgreSQL料來源欄位對映至 Amazon Kendra 索引欄位。如需詳細資訊，請參閱[映射資料來源欄位](#)。

Note

您的文件需要文件內文欄位或文件內文對等項目，才能搜尋您的文件。Amazon Kendra 您必須將資料來源中的文件內文欄位名稱對應至索引欄位名稱_document_body。所有其他欄位是選用的。

如需要設定的其他重要 JSON 金鑰清單，請參閱[PostgreSQL 架構](#)。

備註

- Amazon Kendra 檢查更新的內容時，不會追蹤已刪除的資料庫列。
- 資料庫中一列中欄位名稱和值的大小不得超過 400 KB。

- 如果您的資料庫資料來源中有大量資料，並且不想 Amazon Kendra 在第一次同步之後對所有資料庫內容建立索引，則可以選擇僅同步新文件、修改或刪除的文件。
- 最佳作法是提供 Amazon Kendra 唯讀資料庫認證。
- 最佳做法是避免新增包含敏感資料或個人可識別資訊 (PII) 的表格。

諷刺語

Quip 是一款協作生產力軟體，提供即時文件撰寫功能。您可以使用 Amazon Kendra 對 Quip 文件夾、文件、文件注解、聊天室和附件進行索引。

您可以使用 [Amazon Kendra 控制台](#) 和 [QuipConfiguration](#) API 連接 Amazon Kendra 到 Quip 數據源。

如需 Amazon Kendra Quip 資料來源連接器的疑難排解，請參閱 [疑難排解資料來](#)。

主題

- [支援的功能](#)
- [必要條件](#)
- [連接說明](#)
- [進一步了解](#)

支援的功能

Amazon Kendra Quip 資料來源連接器支援下列功能：


- 欄位對映
- 使用者存取控制
- 包含/排除過濾器
- 虛擬私有雲端 (VPC)

必要條件

在您可以用來 Amazon Kendra 為 Quip 資料來源建立索引之前，請先在 Quip 和 AWS 帳戶中進行這些變更。

在 Quip 中，請確保您擁有：

- 具有管理權限的 Quip 帳戶。
- 創建了包含個人訪問令牌的 Quip 身份驗證憑據。該令牌用作存儲在 AWS Secrets Manager 密鑰中的身份驗證憑據。如需詳細資訊，請參閱有關驗證的 [Quip 文件](#)。


 Note

我們建議您定期重新整理或輪換您的認證和密碼。僅為您自己的安全提供必要的訪問級別。我們不建議您跨資料來源以及連接器 1.0 和 2.0 版 (如果適用) 重複使用認證和密碼。

- 複製您的 Quip 網站域。例如，<https://quip-company.quipdomain.com/browse>，其中#####。
- 核取的每個文件在 Quip 和您打算用於相同索引的其他資料來源中都是唯一的。您要用於索引的每個資料來源不得包含跨資料來源的相同文件。文件 ID 對索引來說是全域的，而且每個索引必須是唯一的。


在您的中 AWS 帳戶，請確保您具有：

- [建立 Amazon Kendra 索引](#)，如果使用 API，則會記下索引識別碼。
- 為您的[資料來源建立 IAM 角色](#)，如果使用 API，則會記錄 IAM 角色的 ARN。

 Note

如果您變更驗證類型和認證，則必須更新 IAM 角色才能存取正確的 AWS Secrets Manager 密碼 ID。

- 將您的 Quip 身份驗證憑據存儲在 AWS Secrets Manager 密鑰中，如果使用 API，則記錄密鑰的 ARN。

 Note

我們建議您定期重新整理或輪換您的認證和密碼。僅為您自己的安全提供必要的訪問級別。我們不建議您跨資料來源以及連接器 1.0 和 2.0 版 (如果適用) 重複使用認證和密碼。

如果您沒有現有的 IAM 角色或密碼，則可以在將 Quip 資料來源連線到時使用主控台建立新 IAM 角色和 Secrets Manager 密碼。Amazon Kendra 如果您使用 API，則必須提供現有 IAM 角色和 Secrets Manager 密碼的 ARN 以及索引 ID。

連接說明

要連接 Amazon Kendra 到 Quip 數據源，您必須提供 Quip 數據源的必要詳細信息，以便 Amazon Kendra 可以訪問您的數據。如果您尚未為 Quip 設定 Amazon Kendra，請參閱[必要條件](#)。

Console

若要連接 Amazon Kendra 到 Quip


1. 登入 AWS Management Console 並開啟[Amazon Kendra 主控台](#)。
2. 在左側導覽窗格中，選擇 [索引]，然後從索引清單中選擇要使用的索引。

Note

您可以選擇在索引設置下配置或編輯您的用戶訪問控制設置。


3. 在 [開始使用] 頁面上，選擇 [新增資料來源]。
4. 在 [新增資料來源] 頁面上，選擇 Quip 連接器，然後選擇 [新增連接器]。如果使用版本 2 (如果適用)，請選擇帶有「V2.0」標籤的 Quip 連接器。
5. 在 [指定資料來源詳細資訊] 頁面上，輸入下列資訊：
 - a. 在名稱和說明中，對於資料來源名稱 — 輸入資料來源的名稱。您可以包含連字號，但不能包含空格。
 - b. (選擇性) 說明 — 輸入資料來源的選用說明。
 - c. 在預設語言中 — 選擇一種語言來篩選索引的文件。除非另有指定，否則語言預設為英文。文件中繼資料中指定的語言會覆寫選取的語言。
 - d. 在「標籤」中，針對「新增標籤」 — 包含可選標籤以搜尋和篩選資源或追蹤 AWS 成本。
 - e. 選擇下一步。
6. 在 [定義存取權和安全性] 頁面上，輸入下列資訊：
 - a. Quip 網域名稱 — 輸入您從 Quip 帳戶複製的 Quip。
 - b. AWS Secrets Manager 秘密 — 選擇現有密碼或建立新 Secrets Manager 密碼來儲存您的 Quip 驗證認證。如果您選擇建立新密碼，則會開啟一個 AWS Secrets Manager 密碼視窗。
 - i. 在「建立 AWS Secrets Manager 密碼視窗」中輸入下列資訊：

- A. 秘密名稱 — 您秘密的名稱。前綴 'AmazonKendra-Quip-' 會自動添加到您的密碼名稱中。
 - B. Quip 權杖 — 輸入設定的 Quip 個人存取權限。
- ii. 添加並保存您的秘密。
- c. Virtual Private Cloud (VPC) (VPC) — 您可以選擇使用 VPC。如果是這樣，您必須新增子網路和 VPC 安全性群組。
 - d. IAM role — 選擇現有 IAM 角色或建立新 IAM 角色以存取存放庫認證和索引內容。

 Note

IAM 用於索引的角色不能用於資料來源。如果您不確定索引或常見問題集是否使用現有角色，請選擇 [建立新角色] 以避免發生錯誤。

- e. 選擇下一步。
7. 在 [設定同步設定] 頁面上，輸入下列資訊：
- a. 新增 Quip 資料夾 ID 以進行編目 — 您要編目的 Quip 資料夾 ID。

 Note

若要編目根資料夾 (包括其中的所有子資料夾和文件)，請新增根資料夾 ID。若要編目特定子資料夾，請新增特定的子資料夾 ID。

- b. 其他配置 (內容類型) — 輸入您要編目的內容類型。
 - c. 正則表達式模式-包含或排除某些文件的正則表達式模式。您最多可以添加 100 個圖案。
 - d. 在同步執行排程中，針對頻率 — 選擇同步資料來源內容並更新索引的頻率
 - e. 選擇下一步。
8. 在 [設定欄位對映] 頁面上，輸入下列資訊：
- a. 從產生的預設資料來源欄位中選取您要對映至 Amazon Kendra 索引的資料來源欄位。
 - b. 新增欄位 — 新增自訂資料來源欄位，以建立要對映的索引欄位名稱和欄位資料類型。
 - c. 選擇下一步。
9. 在 [檢閱並建立] 頁面上，檢查您輸入的資訊是否正確，然後選取 [新增資料來源]。您也可以從此頁面選擇編輯您的資訊。成功新增資料來源後，您的資料來源將顯示在 [資料來源] 頁面上。

API

若要連接 Amazon Kendra 到 Quip

您必須使用 [QuipConfiguration](#) API 指定下列項目：

- Quip 網站網域 — 例如，<https://quip-company.quipdomain.com/browse>，其中 `quipdomain.com` 是網域。
- 秘密 Amazon 資源名稱 (ARN) — 提供包含 Quip 帳戶身份驗證登入資料的 Secrets Manager 密碼的 Amazon 資源名稱 (ARN)。密碼會以下列金鑰儲存在 JSON 結構中：

```
{
  "accessToken": "token"
}
```

- IAM role — 指定 `RoleArn` 何時呼叫 `CreateDataSource` 以提供具有存取 Secrets Manager 密碼的權限的 IAM 角色，以及呼叫 Quip 連接器和所需公用 API 的時間。Amazon Kendra 有關詳情，請參閱 [Quip 資料來源的 IAM 角色](#)。

您還可以添加以下可選功能：

- Virtual Private Cloud (VPC) — 指定 `VpcConfiguration` 為資料來源組態的一部分。請參閱 [設定 Amazon Kendra 定以使用 VPC](#)。
- 包含和排除篩選器 — 指定要包含還是排除某些檔案。

Note

大多數資料來源使用規則運算式模式，這些模式是稱為篩選器的包含或排除模式。如果您指定包含篩選器，則只有符合包含項目篩選器的內容會編製索引。不符合包含篩選器的任何文件都不會建立索引。如果您指定包含和排除篩選器，符合排除篩選器的文件將不會建立索引，即使它們符合包含篩選器也是如此。

- 資料夾 — 指定您要索引的 Quip 資料夾和子資料夾

Note

若要編目根資料夾 (包括其中的所有子資料夾和文件)，請輸入根資料夾 ID。若要編目特定子資料夾，請新增特定的子資料夾 ID。

- 附件、聊天室、檔案註解 — 選擇是否要包含檢索附件、聊天室內容和檔案註解。
- 使用者前後關聯篩選與存取控制 — Amazon Kendra 探索文件的存取控制清單 (ACL) (如果您有文件的 ACL)。ACL 資訊可用來根據使用者或使用者對文件的群組存取權來篩選搜尋結果。如需詳細資訊，請參閱[使用者內容篩選](#)。
- 欄位對映 — 選擇將 Quip 資料來源欄位對映至 Amazon Kendra 索引欄位。如需詳細資訊，請參閱[映射資料來源欄位](#)。

Note

您的文件需要文件內文欄位或文件內文對等項目，才能搜尋您的文件。Amazon Kendra 您必須將資料來源中的文件內文欄位名稱對應至索引欄位名稱_document_body。所有其他欄位是選用的。

進一步了解

要了解有關 Amazon Kendra 與 Quip 數據源集成的更多信息，請參閱：

- [使用 Quip 連接器使用智慧搜尋來搜尋 Quip 文件中的知識 Amazon Kendra](#)

Salesforce

Salesforce 是一種客戶關係管理 (CRM) 工具，用於管理支持，銷售和營銷團隊。您可以使用 Amazon Kendra 引您的 Salesforce 標準物件，甚至是自訂物件。

您可以使用[Amazon Kendra 主控台](#)、API 或 [TemplateConfiguration](#) API 連線 Amazon Kendra 到 Salesforce 資料來源。[SalesforceConfiguration](#)

Amazon Kendra 有兩個版本的 Salesforce 連接器。每個版本的支援功能包括：

銷售力連接器 1.0 版/應用程式介面 [SalesforceConfiguration](#)

- 欄位對映
- 使用者存取控制
- 包含/排除過濾器

銷售連接器 2.0 版/應用程式介面 [TemplateConfiguration](#)

- 欄位對映
- 使用者存取控制
- 包含/排除過濾器
- 完整和增量內容同步
- 虛擬私有雲端 (VPC)

Note

Support 於 Salesforce 連接器 1.0/ SalesforceConfiguration API 的支援預定於 2023 年結束。我們建議您移轉至或使用 Salesforce 連接器 2.0/ TemplateConfiguration API。

如需 Amazon Kendra Salesforce 資料來源連接器的疑難排解，請參閱[疑難排解資料來](#)。

主題

- [銷售連接器 V1.0](#)
- [銷售連接器 V2.0](#)

銷售連接器 V1.0

Salesforce 是一種客戶關係管理 (CRM) 工具，用於管理支持，銷售和營銷團隊。您可以使用索引 Amazon Kendra 引您的 Salesforce 標準物件，甚至是自訂物件。

Important

Amazon Kendra 使用版本 48 的銷售力量 API。Salesforce API 會限制您每天可發出的要求數量。如果 Salesforce 超過這些要求，它會重試直到能夠繼續。

Note

Support 於 Salesforce 連接器 1.0/ SalesforceConfiguration API 的支援預定於 2023 年結束。我們建議您移轉至或使用 Salesforce 連接器 2.0/ TemplateConfiguration API。

如需 Amazon Kendra Salesforce 資料來源連接器的疑難排解，請參閱[疑難排解資料來](#)。

主題

- [支援的功能](#)
- [必要條件](#)
- [連接說明](#)

支援的功能

Amazon Kendra Salesforce 資料來源連接器支援下列功能：

- 欄位對映
- 使用者存取控制
- 包含/排除過濾器

必要條件

在您可以使用 Amazon Kendra 索引 Salesforce 資料來源之前，請先在 Salesforce 和 AWS 帳戶中進行這些變更。

在「銷售力量」中，請確定您擁有：

- 已建立 Salesforce 帳戶，並記下您用來連線至 Salesforce 的使用者名稱和密碼。
- 建立已啟用 OAuth 的 Salesforce 連線應用程式帳戶，並複製指派給 Salesforce 連線應用程式的消費者金鑰 (用戶端識別碼) 和消費者密碼 (用戶端密碼)。用戶端 ID 和用戶端密碼會用作儲存在 AWS Secrets Manager 密碼中的驗證憑證。如需詳細資訊，請參閱[已連線應用程式的 Salesforce 文件](#)

Note

我們建議您定期重新整理或輪換您的認證和密碼。僅為您自己的安全提供必要的訪問級別。我們不建議您跨資料來源以及連接器 1.0 和 2.0 版 (如果適用) 重複使用認證和密碼。

- 複製與用來連線至 Salesforce 之帳戶相關聯的 Salesforce 安全性權杖。
- 複製您要索引之 Salesforce 執行個體的 URL。<company>通常情況下，這是 **HTTPS:** 伺服器必須執行已連線到 Salesforce 的應用程式。
- 透過複製 ReadOnly 設定檔，然後新增「檢視所有資料」和「管理文章」權限，為具有 Salesforce 唯讀存取權限的使用者新增認證至您的 Salesforce 伺服器。這些認證可識別進行連線的使用者，以及連線到的 Salesforce Amazon Kendra 連線應用程式。

- 核取每個文件在 Salesforce 和您打算用於相同索引的其他資料來源中都是唯一的。您要用於索引的每個資料來源不得包含跨資料來源的相同文件。文件 ID 對索引來說是全域的，而且每個索引必須是唯一的。

在您的中 AWS 帳戶，請確保您有：

- [建立 Amazon Kendra 索引](#)，如果使用 API，則會記下索引識別碼。
- 為您的[資料來源建立 IAM 角色](#)，如果使用 API，則會記錄 IAM 角色的 ARN。

Note

如果您變更驗證類型和認證，則必須更新 IAM 角色以存取正確的 AWS Secrets Manager 密碼 ID。

- 將您的 Salesforce 驗證認證儲存在 AWS Secrets Manager 密碼中，如果使用 API，則會記下密碼的 ARN。

Note

我們建議您定期重新整理或輪換您的認證和密碼。僅為您自己的安全提供必要的訪問級別。我們不建議您跨資料來源以及連接器 1.0 和 2.0 版 (如果適用) 重複使用認證和密碼。

如果您沒有現有的 IAM 角色或密碼，則可以在將 Salesforce 資料來源連線到時，使用主控台建立新 IAM 角色和 Secrets Manager 密碼。Amazon Kendra 如果您使用 API，則必須提供現有 IAM 角色和 Secrets Manager 密碼的 ARN 以及索引 ID。


連接說明

若要連線 Amazon Kendra 到 Salesforce 資料來源，您必須提供 Salesforce 資料來源的必要詳細資料，Amazon Kendra 以便存取您的資料。如果您尚未配置 Salesforce 以查 Amazon Kendra 看[必要條件](#)。

Console


若要連線 Amazon Kendra 至銷售力量

1. 登入 AWS 管理主控台並開啟主[Amazon Kendra 控制台](#)。
2. 在左側導覽窗格中，選擇 [索引]，然後從索引清單中選擇要使用的索引。

 Note

您可以選擇在索引設置下配置或編輯用戶訪問控制設置。


3. 在 [開始使用] 頁面上，選擇 [新增資料來源]。
4. 在 [新增資料來源] 頁面上，選擇 Salesforce 連接器 V1.0，然後選擇 [新增連接器]。
5. 在 [指定資料來源詳細資訊] 頁面上，輸入下列資訊：
 - a. 資料來源名稱 — 輸入資料來源的名稱。您可以包含連字號，但不能包含空格。
 - b. (選擇性) 說明 — 輸入資料來源的選用說明。
 - c. 預設語言 — 用來篩選索引文件的語言。除非另有指定，否則語言預設為英文。中繼資料中指定的語言會覆寫所選語言
 - d. 新增標籤 — 用來搜尋和篩選資源或追蹤共用成本的標籤。
 - e. 選擇下一步。
6. 在 [定義存取權和安全性] 頁面上，輸入下列資訊：
 - a. Salesforce 網址：輸入您要索引之 Salesforce 網站的執行個體 URL。
 - b. 對於驗證類型，請選擇現有和新增來儲存您的 Salesforce 驗證認證。如果您選擇建立新密碼，則會開啟一個 AWS Secrets Manager 密碼視窗。
 - 在「建立 AWS Secrets Manager 密碼視窗」中輸入下列資訊：
 - A. 秘密名稱 — 您秘密的名稱。前綴 'AmazonKendra-Salesforce' 會自動添加到您的密碼名稱中。
 - B. 針對使用者名稱、密碼、安全性權杖、取用者金鑰、取用者密碼和驗證 URL，請輸入您在 Salesforce 帳戶中建立的驗證認證值。
 - C. 選擇 [儲存驗證]。
 - c. IAM role — 選擇現有 IAM 角色或建立新 IAM 角色以存取存放庫認證和索引內容。

 Note

IAM 用於索引的角色不能用於資料來源。如果您不確定索引或常見問題集是否使用現有角色，請選擇 [建立新角色] 以避免發生錯誤。


- d. 選擇下一步。

7. 在 [設定同步設定] 頁面上，輸入下列資訊：
 - a. 針對編目附件 — 選取此選項可編目所有附加的物件、文章和摘要。
 - b. 針對標準物件、知識文章和 Chatter 摘要，請選取您要編目的 Salesforce 實體或內容類型。

 Note

您必須提供組態資訊，以索引至少一個標準物件、知識文章或 chatter 摘要。如果您選擇編目知識文章，您必須指定要索引的知識文章類型、文章的名稱，以及是否要索引所有知識文章的標準欄位，還是僅索引自訂文章類型的欄位。如果您選擇索引自訂文章，您必須指定文章類型的內部名稱。您最多可以指定 10 種文章類型。

- c. 頻率：與資料來源同步的頻率。 Amazon Kendra
 - d. 選擇下一步。
8. 在 [設定欄位對映] 頁面上，輸入下列資訊：
 - a. 對於標準知識文章、標準物件附件和其他建議的欄位對應 — 從 Amazon Kendra 產生的預設資料來源欄位中選取您要對應至索引的預設資料來源欄位。

 Note

需要對映 `_document_body` 的索引。您無法變更欄 Salesforce ID 位與欄位之間的 Amazon Kendra `_document_id` 對應。

- b. 新增欄位 — 新增自訂資料來源欄位以建立要對映的索引欄位名稱和欄位資料類型。
 - c. 選擇下一步。
9. 在 [檢閱並建立] 頁面上，檢查您輸入的資訊是否正確，然後選取 [新增資料來源]。您也可以從此頁面選擇編輯您的資訊。成功新增資料來源後，您的資料來源將顯示在 [資料來源] 頁面上。

API

若要連線 Amazon Kendra 至銷售力量

您必須指定下列 [SalesforceConfigurationAPI](#)：

- 伺服器 URL — 您要索引之 Salesforce 網站的執行個體 URL。

- 秘密 Amazon 資源名稱 (ARN) — 提供機 Secrets Manager 密的 Amazon 資源名稱 (ARN) , 其中包含您的 Salesforce 帳戶的身份驗證登入資料。密碼會以下列金鑰儲存在 JSON 結構中 :

```
{
  "authenticationUrl": "OAUTH endpoint that Amazon Kendra connects to get an OAUTH token",
  "consumerKey": "Application public key generated when you created your Salesforce application",
  "consumerSecret": "Application private key generated when you created your Salesforce application.",
  "password": "Password associated with the user logging in to the Salesforce instance",
  "securityToken": "Token associated with the user account logging in to the Salesforce instance",
  "username": "User name of the user logging in to the Salesforce instance"
}
```

- IAM 角色 — 指定RoleArn當您呼叫CreateDataSource以提供具有存取 Secrets Manager 密碼之權限的 IAM 角色 , 以及呼叫 Salesforce 連接器和所需的公用 API 的時間。 Amazon Kendra 如需詳細資訊 , 請參閱 [Salesforce 資料來源的IAM 角色](#)。
- 您必須提供組態資訊 , 以索引至少一個標準物件、知識文章或 chatter 摘要。
 - 標準物件 — 如果您選擇編目標準物件 , 您必須指定標準物件的名稱 , 以及包含文件內容的標準物件表格中的欄位名稱。
 - 知識文章 — 如果您選擇編目知識文章 , 您必須指定要索引的知識文章類型、要索引的知識文章的狀態 , 以及是否要索引所有知識文章的標準欄位 , 還是只為自訂文章類型的欄位建立索引。
 - Chatter 摘要 — 如果您選擇編目 Chatter 摘要 , 則必須在包含要索引之內容的 Salesforce FeedItem 表格中指定資料行的名稱。

您還可以添加以下可選功能 :

- 包含和排除篩選器 — 指定要包含還是排除某些檔案附件。

Note

大多數資料來源使用規則運算式模式 , 這些模式是稱為篩選器的包含或排除模式。如果您指定包含篩選器 , 則只有符合包含項目篩選器的內容會編製索引。不符合包含篩選器的任

何文件都不會建立索引。如果您指定包含和排除篩選器，符合排除篩選器的文件將不會建立索引，即使它們符合包含篩選器也是如此。

- 欄位對映 — 選擇將 Salesforce 資料來源欄位對映至 Amazon Kendra 索引欄位。如需詳細資訊，請參閱[映射資料來源欄位](#)。

Note

您的文件需要文件內文欄位或文件內文對等項目，才能搜尋您的文件。Amazon Kendra 您必須將資料來源中的文件內文欄位名稱對應至索引欄位名稱_document_body。所有其他欄位是選用的。

- 使用者前後關聯篩選與存取控制 — Amazon Kendra 探索文件的存取控制清單 (ACL) (如果您有文件的 ACL)。ACL 資訊可用來根據使用者或使用者對文件的群組存取來篩選搜尋結果。如需詳細資訊，請參閱[使用者內容篩選](#)。

銷售連接器 V2.0

Salesforce 是一種客戶關係管理 (CRM) 工具，用於管理支持，銷售和營銷團隊。您可以使用 Amazon Kendra 引您的 Salesforce 標準物件，甚至是自訂物件。

S Amazon Kendra Salesforce 資料來源連接器支援下列 Salesforce 版本：開發人員版和企業版。

Note

Support 於 Salesforce 連接器 1.0/ SalesforceConfiguration API 的支援預定於 2023 年結束。我們建議您移轉至或使用 Salesforce 連接器 2.0/ TemplateConfiguration API。

如需 Amazon Kendra Salesforce 資料來源連接器的疑難排解，請參閱[疑難排解資料來](#)。

主題

- [支援的功能](#)
- [必要條件](#)
- [連接說明](#)
- [進一步了解](#)

支援的功能

Amazon Kendra Salesforce 資料來源連接器支援下列功能：

- 欄位對映
- 使用者存取控制
- 包含/排除過濾器
- 完整和增量內容同步
- 虛擬私有雲端 (VPC)

必要條件

在您可以使用 Amazon Kendra 索引 Salesforce 資料來源之前，請先在 Salesforce 和 AWS 帳戶中進行這些變更。

在「銷售力量」中，請確定您擁有：

- 建立 Salesforce 系統管理帳戶，並記下您用來連線至 Salesforce 的使用者名稱和密碼。
- 複製與用來連線至 Salesforce 之帳戶相關聯的 Salesforce 安全性權杖。
- 建立已啟用 OAuth 的 Salesforce 連線應用程式帳戶，並複製指派給 Salesforce 連線應用程式的消費者金鑰 (用戶端識別碼) 和消費者密碼 (用戶端密碼)。用戶端 ID 和用戶端密碼會用作儲存在 AWS Secrets Manager 密碼中的驗證憑證。如需詳細資訊，請參閱[已連線應用程式的 Salesforce 文件](#)

Note

我們建議您定期重新整理或輪換您的認證和密碼。僅為您自己的安全提供必要的訪問級別。我們不建議您跨資料來源以及連接器 1.0 和 2.0 版 (如果適用) 重複使用認證和密碼。

- 複製您要索引之 Salesforce 執行個體的 URL。<company>通常情況下，這是 **HTTPS:** 伺服器必須執行已連線到 Salesforce 的應用程式。
- 透過複製 ReadOnly 設定檔，然後新增「檢視所有資料」和「管理文章」權限，為具有 Salesforce 唯讀存取權限的使用者新增認證至您的 Salesforce 伺服器。這些認證可識別進行連線的使用者，以及連線到的 Salesforce Amazon Kendra 連線應用程式。
- 核取每個文件在 Salesforce 和您打算用於相同索引的其他資料來源中都是唯一的。您要用於索引的每個資料來源不得包含跨資料來源的相同文件。文件 ID 對索引來說是全域的，而且每個索引必須是唯一的。

在您的中 AWS 帳戶，請確保您有：

- [建立 Amazon Kendra 索引](#)，如果使用 API，則會記下索引識別碼。
- 為您的[資料來源建立 IAM 角色](#)，如果使用 API，則會記錄 IAM 角色的 ARN。

Note

如果您變更驗證類型和認證，則必須更新 IAM 角色以存取正確的 AWS Secrets Manager 密碼 ID。

- 將您的 Salesforce 驗證認證儲存在 AWS Secrets Manager 密碼中，如果使用 API，則會記下密碼的 ARN。

Note

我們建議您定期重新整理或輪換您的認證和密碼。僅為您自己的安全提供必要的訪問級別。我們不建議您跨資料來源以及連接器 1.0 和 2.0 版 (如果適用) 重複使用認證和密碼。

如果您沒有現有的 IAM 角色或密碼，則可以在將 Salesforce 資料來源連線到時，使用主控台建立新 IAM 角色和 Secrets Manager 密碼。Amazon Kendra 如果您使用 API，則必須提供現有 IAM 角色和 Secrets Manager 密碼的 ARN 以及索引 ID。

連接說明

若要連線 Amazon Kendra 到 Salesforce 資料來源，您必須提供 Salesforce 資料來源的必要詳細資料，Amazon Kendra 以便存取您的資料。如果您尚未配置 Salesforce 以查 Amazon Kendra 看[必要條件](#)。

Console


若要連線 Amazon Kendra 至銷售力量：

1. 登入 AWS Management Console 並開啟[Amazon Kendra 主控台](#)。
2. 在左側導覽窗格中，選擇 [索引]，然後從索引清單中選擇要使用的索引。

Note

您可以選擇在索引設置下配置或編輯用戶訪問控制設置。


3. 在 [開始使用] 頁面上，選擇 [新增資料來源]。
4. 在 [新增資料來源] 頁面上，選擇 Salesforce 連接器，然後選擇 [新增連接器]。如果使用第 2 版 (如果適用)，請選擇具有「V2.0」標籤的 Salesforce 連接器。
5. 在 [指定資料來源詳細資訊] 頁面上，輸入下列資訊：
 - a. 在名稱和說明中，對於資料來源名稱 — 輸入資料來源的名稱。您可以包含連字號，但不能包含空格。
 - b. (選擇性) 說明 — 輸入資料來源的選用說明。
 - c. 在預設語言中 — 選擇一種語言來篩選索引的文件。除非另有指定，否則語言預設為英文。文件中繼資料中指定的語言會覆寫選取的語言。
 - d. 在「標籤」中，針對「新增標籤」 — 包含可選標籤以搜尋和篩選資源或追蹤 AWS 成本。
 - e. 選擇下一步。
6. 在 [定義存取權和安全性] 頁面上，輸入下列資訊：
 - a. Salesforce URL — 輸入您要索引之 Salesforce 網站的執行個體 URL。
 - b. 授權 — 開啟或關閉文件的存取控制清單 (ACL) 資訊 (如果您有 ACL)，且想要將其用於存取控制。ACL 會指定使用者和群組可存取的文件。ACL 資訊可用來根據使用者或使用者對文件的群組存取來篩選搜尋結果。如需詳細資訊，請參閱[使用者內容篩選](#)。
 - c. 輸入現有密碼，或者如果您建立新密碼，則會開啟一個 AWS Secrets Manager 密碼視窗。
 - 驗證 — 在「建立 AWS Secrets Manager 密碼視窗」中輸入下列資訊：
 - A. 秘密名稱 — 您秘密的名稱。前綴 'AmazonKendra-Salesforce' 會自動添加到您的密碼名稱中。
 - B. 針對使用者名稱、密碼、安全性權杖、取用者金鑰、取用者密碼和驗證 URL，請輸入您從 Salesforce 帳戶產生並下載的驗證認證值。

 Note

如果您使用 Salesforce 開發人員版，請使用 `https://login.salesforce.com/services/oauth2/token` 或「我的網域登入網址」(例如 `#https://MyCompany.my.salesforce.com`) 做為驗證網址。如果您使用 Salesforce 沙箱版本，請使用 `https://test.salesforce.com/services/oauth2/token` 或「我的網域

登入網址」(例如, **MyDomainName-SandboxName .sandbox.my.salesforce.com**) 做為驗證網址。

- C. 選擇 [儲存驗證]。
- d. Virtual Private Cloud (VPC) (VPC) — 您可以選擇使用 VPC。如果是這樣, 您必須新增子網路和 VPC 安全性群組。
- e. 識別爬行者程式 — 指定是否要開啟身分識別爬行者 Amazon Kendra 程式。識別爬行者程式會使用文件的存取控制清單 (ACL) 資訊, 根據使用者或使用者對文件的群組存取權來篩選搜尋結果。如果您有文件的 ACL 並選擇使用 ACL, 您也可以選擇開啟的身分識別爬行者程式, 以設定搜尋結果的使用者環境定義篩選。Amazon Kendra 否則, 如果關閉身分搜索器, 則可以公開搜索所有文檔。如果您想要對文件使用存取控制, 且身分識別編目程式已關閉, 您也可以使用 [PutPrincipalMapping](#) API 來上傳使用者和群組存取資訊以進行使用者內容篩選。
- f. IAM role — 選擇現有 IAM 角色或建立新 IAM 角色以存取存放庫認證和索引內容。

 Note

IAM 用於索引的角色不能用於資料來源。如果您不確定索引或常見問題集是否使用現有角色, 請選擇 [建立新角色] 以避免發生錯誤。

- g. 選擇下一步。
7. 在 [設定同步設定] 頁面上, 輸入下列資訊:
 - a. 針對編目附件 — 選取此選項可編目所有附加的 Salesforce 物件。
 - b. 針對標準物件、含附件的標準物件, 以及不含附件和知識文章的標準物件 — 選取您要編目的 Salesforce 實體或內容類型。
 - c. 您必須提供組態資訊, 以索引至少一個標準物件、知識文章或 chatter 摘要。如果您選擇編目知識文章, 您必須指定要索引的知識文章類型。您可以選擇已發布, 存檔, 草稿和附件。

正則表達式過濾器 — 指定正則表達式模式以包含特定的目錄項

8. 對於其他配置:

- ACL 資訊依預設會包含所有存取控制清單。取消選取存取控制清單後, 該類別中的所有檔案都會公開。

- 正則表達式模式-添加正則表達式模式以包含或排除某些文件。您最多可以添加 100 個圖案。

同步模式 — 選擇資料來源內容變更時要如何更新索引。當您第一次將資料來源同 Amazon Kendra 步處理時，依預設會檢索所有內容並建立索引。如果初始同步失敗，您必須執行資料的完整同步，即使您沒有選擇完整同步作為同步模式選項。

- 完全同步：新鮮索引所有內容，並在每次資料來源與索引同步時取代現有內容。
- 新增、修改的同步：每次資料來源與索引同步時，僅對新內容和已修改的內容建立索引。Amazon Kendra 可以使用資料來源的機制來追蹤內容變更，並為上次同步後變更的內容建立索引。
- 新增、修改、刪除的同步：每次資料來源與索引同步時，僅對新內容、已修改和刪除的內容建立索引。Amazon Kendra 可以使用資料來源的機制來追蹤內容變更，並為上次同步後變更的內容建立索引。

9. 選擇下一步。

10. 在 [設定欄位對映] 頁面上，輸入下列資訊：

- a. 對於標準知識文章、標準物件附件和其他建議的欄位對應 — 從 Amazon Kendra 產生的預設資料來源欄位中選取您要對應至索引的預設資料來源欄位。

Note

需要對映 `_document_body` 的索引。您無法變更欄位 Salesforce ID 位與欄位之間的 Amazon Kendra `_document_id` 對應。您可以將任何 Salesforce 字段映射到文檔標題或文檔正文 Amazon Kendra 保留/默認索引字段。

如果您將任何 Salesforce 欄位對應至 Amazon Kendra 文件標題和文件內文欄位，Amazon Kendra 會在搜尋回應中使用文件標題和內文欄位中的資料。

- b. 新增欄位 — 新增自訂資料來源欄位以建立要對映的索引欄位名稱和欄位資料類型。
- c. 選擇下一步。

11. 在 [檢閱並建立] 頁面上，檢查您輸入的資訊是否正確，然後選取 [新增資料來源]。您也可以從此頁面選擇編輯您的資訊。成功新增資料來源後，您的資料來源將顯示在 [資料來源] 頁面上。

API

若要連線 Amazon Kendra 至銷售力量

您必須使用 [TemplateConfiguration](#) API 指定 [資料來源結構描述](#) 的 JSON。您必須提供以下信息：

- 資料來源 — 指定使用 [TemplateConfiguration](#) JSON 結構描述 SALESFORCEV2 時的資料來源類型。同時指定呼叫 [CreateDataSource](#) API TEMPLATE 時的資料來源。
- 主機 URL — 指定 Salesforce 執行個體主機 URL。
- 同步模式 — 指定資料來源內容變更時 Amazon Kendra 應如何更新索引。當您第一次將資料來源同 Amazon Kendra 步處理時，依預設會檢索所有內容並建立索引。如果初始同步失敗，您必須執行資料的完整同步，即使您沒有選擇完整同步作為同步模式選項。您可以選擇：
 - FORCED_FULL_CRAWL 新建索引所有內容，並在每次資料來源與索引同步時取代現有內容。
 - FULL_CRAWL，以在每次資料來源與索引同步時，僅對新的、修改的和刪除的內容建立索引。Amazon Kendra 可以使用資料來源的機制來追蹤內容變更，並為上次同步後變更的內容建立索引。
 - CHANGE_LOG 每次資料來源與索引同步時，僅對新內容和修改的內容建立索引。Amazon Kendra 可以使用資料來源的機制來追蹤內容變更，並為上次同步後變更的內容建立索引。
- 秘密 Amazon 資源名稱 (ARN) — 提供機 Secrets Manager 密的 Amazon 資源名稱 (ARN)，其中包含您的 Salesforce 帳戶的身份驗證登入資料。密碼會以下列金鑰儲存在 JSON 結構中：

```
{
  "authenticationUrl": "OAUTH endpoint that Amazon Kendra connects to get an OAUTH token",
  "consumerKey": "Application public key generated when you created your Salesforce application",
  "consumerSecret": "Application private key generated when you created your Salesforce application",
  "password": "Password associated with the user logging in to the Salesforce instance",
  "securityToken": "Token associated with the user account logging in to the Salesforce instance",
  "username": "User name of the user logging in to the Salesforce instance"
}
```

- IAM 角色 — 指定 RoleArn 當您呼叫 CreateDataSource 以提供具有存取 Secrets Manager 密碼之權限的 IAM 角色，以及呼叫 Salesforce 連接器和所需的公用 API 的時間。Amazon Kendra 如需詳細資訊，請參閱 [Salesforce 資料來源的 IAM 角色](#)。

您還可以添加以下可選功能：

- V@@@rtual Private Cloud (VPC) — 指定您撥打電話的VpcConfiguration時間。CreateDataSource如需詳細資訊，請參閱 [配置 Amazon Kendra 為使用 Amazon VPC](#)。
- 包含和排除篩選器 — 您可以指定是否要包含或排除特定文件、客戶、促銷活動、案例、連絡人、潛在客戶、商機、解決方案、工作、群組、聊天程式和自訂實體檔案。

Note

大多數資料來源使用規則運算式模式，這些模式是稱為篩選器的包含或排除模式。如果您指定包含篩選器，則只有符合包含項目篩選器的內容會編製索引。不符合包含篩選器的任何文件都不會建立索引。如果您指定包含和排除篩選器，符合排除篩選器的文件將不會建立索引，即使它們符合包含篩選器也是如此。

- 識別爬行者程式 — 指定是否要開啟身分識別爬行 Amazon Kendra 者程式。識別爬行者程式會使用文件的存取控制清單 (ACL) 資訊，根據使用者或使用者對文件的群組存取權來篩選搜尋結果。如果您有文件的 ACL 並選擇使用 ACL，您也可以選擇開啟的身分識別爬行者程式，以設定搜尋結果的使用者環境定義篩選。Amazon Kendra 否則，如果關閉身分搜索器，則可以公開搜索所有文檔。如果您想要對文件使用存取控制，且身分識別編目程式已關閉，您也可以使用 [PutPrincipalMapping](#) API 來上傳使用者和群組存取資訊以進行使用者內容篩選。
- 欄位對映 — 選擇將 Salesforce 資料來源欄位對映至 Amazon Kendra 索引欄位。如需詳細資訊，請參閱 [映射資料來源欄位](#)。

Note

您的文件需要文件內文欄位或文件內文對等項目，才能搜尋您的文件。Amazon Kendra 您必須將資料來源中的文件內文欄位名稱對應至索引欄位名稱_document_body。所有其他欄位是選用的。

Note

需要對映_document_body的索引。您無法變更欄Salesforce ID位與欄位之間的 Amazon Kendra _document_id 對應。您可以將任何 Salesforce 字段映射到文檔標題或文檔正文 Amazon Kendra 保留/默認索引字段。

如果您將任何 Salesforce 欄位對應至 Amazon Kendra 文件標題和文件內文欄位，Amazon Kendra 會在搜尋回應中使用文件標題和內文欄位中的資料。

如需要設定的其他重要 JSON 金鑰清單，請參閱 [Salesforce 範本結構描述](#)。

進一步了解

若要深入瞭解如何 Amazon Kendra 與 Salesforce 資料來源整合，請參閱：

- [宣布更新的銷售力量連接器 \(V2\) Amazon Kendra](#)

ServiceNow

ServiceNow 提供雲端服務管理系統，以建立和管理組織層級的工作流程，例如 IT 服務、票務系統和支援。您可以用 Amazon Kendra 來編製目 ServiceNow 錄、知識文章、事件及其附件的索引。

您可以使用 [Amazon Kendra 主控台](#)、API 或 [TemplateConfiguration](#) API 連線 Amazon Kendra 到 ServiceNow 資料來源。 [ServiceNowConfiguration](#)

Amazon Kendra 有兩個版本的 ServiceNow 連接器。每個版本的支援功能包括：

ServiceNow 連接器 1.0 /API [ServiceNowConfiguration](#)

- 欄位對映
- ServiceNow 執行個體版本：倫敦、其他
- 包含/排除過濾器

ServiceNow 連接器 2.0 版/[TemplateConfiguration](#) API

- 欄位對映
- 使用者存取控制
- 包含/排除過濾器
- 完整和增量內容同步
- ServiceNow 執行個體版本：羅馬、聖地牙哥、東京、其他
- 虛擬私有雲端 (VPC)

Note

對 ServiceNow 連接器 V1.0/ ServiceNowConfiguration API 的 Support 預定於 2023 年結束。我們建議您移轉至或使用 ServiceNow 連接器 V2.0/ TemplateConfiguration API。

如需疑難排解資 Amazon Kendra ServiceNow 料來源連接器，請參閱[疑難排解資料來](#)。

主題

- [ServiceNow 連接器 1.0 版](#)
- [ServiceNow 連接器 2.0 版](#)
- [使用查詢指定要編製索引的文件](#)

ServiceNow 連接器 1.0 版

ServiceNow 提供雲端服務管理系統，以建立和管理組織層級的工作流程，例如 IT 服務、票務系統和支援。您可以使 Amazon Kendra 用編製目 ServiceNow 錄、知識文章及其附件的索引。

Note

對 ServiceNow 連接器 V1.0/ ServiceNowConfiguration API 的 Support 預定於 2023 年結束。我們建議您移轉至或使用 ServiceNow 連接器 V2.0/ TemplateConfiguration API。

如需疑難排解資 Amazon Kendra ServiceNow 料來源連接器，請參閱[疑難排解資料來](#)。

主題

- [支援的功能](#)
- [必要條件](#)
- [連接說明](#)
- [進一步了解](#)

支援的功能

Amazon Kendra ServiceNow 資料來源連接器支援下列功能：

- ServiceNow 執行個體版本：倫敦、其他

- 包含/排除模式：服務目錄、知識文章及其附件

必要條件

在您可以用來 Amazon Kendra 為資料來源建立索引之前，請先在 ServiceNow 和 AWS 帳戶中進行這些變更。

在中 ServiceNow，請確定您有：

- 建立 ServiceNow 管理員帳戶並建立 ServiceNow 執行個體。
- 已複製執行 ServiceNow 個體 URL 的主機。##### *https://your-domain.service-now.com#####*
- 記下您的基本驗證認證，其中包含允許連線 Amazon Kendra 至 ServiceNow 執行個體的使用者名稱和密碼。

Note

我們建議您定期重新整理或輪換您的認證和密碼。僅為您自己的安全提供必要的訪問級別。我們不建議您跨資料來源以及連接器 1.0 和 2.0 版 (如果適用) 重複使用認證和密碼。

- 選用性：設定 OAuth 2.0 認證權杖，可識別 Amazon Kendra 並產生使用者名稱、密碼、用戶端 ID 和用戶端密碼。使用者名稱和密碼必須提供對 ServiceNow 知識庫和服務目錄的存取權。如需詳細資訊，請參閱 [OAuth 2.0 驗證的 ServiceNow 文件](#)。
- 已新增下列權限：
 - KB 類別
 - 知識知識
 - 知識庫
 - kb_uc_cannot_讀取_mtom
 - kb_uc_can_讀取_mtom
 - 目錄
 - 分類
 - 貓項目
 - 系統附件
 - 系統附件文件
 - 系統使用者角色

- 已勾選的每個文件在您打算用於相同索引的其他資料來源中 ServiceNow 和其他資料來源之間都是唯一的。您要用於索引的每個資料來源不得包含跨資料來源的相同文件。文件 ID 對索引來說是全域的，而且每個索引必須是唯一的。

在你的 AWS 帳戶，確保你有：

- [建立 Amazon Kendra 索引](#)，如果使用 API，則會記下索引 ID。
- 為您的[資料來源建立 IAM 角色](#)，如果使用 API，則會記錄 IAM 角色的 ARN。

Note

如果您變更驗證類型和認證，則必須更新 IAM 角色才能存取正確的 AWS Secrets Manager 密碼 ID。

- 將您的 ServiceNow 身份驗證憑據存儲在 AWS Secrets Manager 密鑰中，如果使用 API，則記錄密鑰的 ARN。

Note

我們建議您定期重新整理或輪換您的認證和密碼。僅為您自己的安全提供必要的訪問級別。我們不建議您跨資料來源以及連接器 1.0 和 2.0 版 (如果適用) 重複使用認證和密碼。

如果您沒有現有的 IAM 角色或密碼，則可以在將 ServiceNow 資料來源連線到時使用主控台建立新 IAM 角色和 Secrets Manager 密碼 Amazon Kendra。如果您使用 API，則必須提供現有 IAM 角色和 Secrets Manager 密碼的 ARN，以及索引 ID。

連接說明

若要連線 Amazon Kendra 到 ServiceNow 資料來源，您必須提供資料來源的必要詳細 ServiceNow 資訊，Amazon Kendra 以便能夠存取您的資料。如果您尚未設定「Amazon Kendra 請 ServiceNow 參閱[必要條件](#)」。

Console

若要連線 Amazon Kendra 到 ServiceNow

1. 登入 AWS 管理主控台並開啟主[Amazon Kendra 控制台](#)。
2. 在左側導覽窗格中，選擇 [索引]，然後從索引清單中選擇要使用的索引。

Note

您可以選擇在索引設置下配置或編輯您的用戶訪問控制設置。

3. 在 [開始使用] 頁面上，選擇 [新增資料來源]。
4. 在 [新增資料來源] 頁面上，選擇 [ServiceNow連接器 V1.0]，然後選擇 [新增資料來源]。
5. 在 [指定資料來源詳細資訊] 頁面上，輸入下列資訊：
 - a. 在名稱和說明中，對於資料來源名稱 — 輸入資料來源的名稱。您可以包含連字號，但不能包含空格。
 - b. (選擇性) 說明 — 輸入資料來源的選用說明。
 - c. 在預設語言中 — 選擇一種語言來篩選索引的文件。除非另有指定，否則語言預設為英文。文件中繼資料中指定的語言會覆寫選取的語言。
 - d. 在「標籤」中，針對「新增標籤」 — 包含可選標籤以搜尋和篩選資源或追蹤 AWS 成本。
 - e. 選擇下一步。
6. 在 [定義存取和安全性] 頁面上，輸入下列資訊：
 - a. ServiceNow 主機 — 輸入 ServiceNow主機 URL。
 - b. ServiceNow 版本 — 選取您的 ServiceNow 版本。
 - c. 根據您的使用案例，在基本驗證和 Oauth 2.0 驗證之間進行選擇。
 - d. AWS Secrets Manager 祕密 — 選擇現有密碼或建立新 Secrets Manager 密碼來儲存您的 ServiceNow 驗證認證。如果您選擇建立新密碼，則會開啟一個 AWS Secrets Manager 密碼視窗。
 - i. 祕密名稱 — 您祕密的名稱。前綴 'AmazonKendraServiceNow-' 會自動添加到您的密碼名稱中。
 - ii. 如果使用基本驗證 — 輸入您帳戶的密碼名稱、使用者名稱和密碼。 ServiceNow
如果使用 OAuth2 驗證 — 輸入您在帳戶中建立的密碼名稱、使用者名稱、密碼、用戶端 ID 和用戶端密碼。 ServiceNow
 - iii. 選擇 [儲存並新增密碼]。
 - e. IAM role — 選擇現有 IAM 角色或建立新 IAM 角色以存取存放庫認證和索引內容。

Note

IAM 用於索引的角色不能用於資料來源。如果您不確定索引或常見問題集是否使用現有角色，請選擇 [建立新角色] 以避免發生錯誤。

- f. 選擇下一步。
7. 在 [設定同步設定] 頁面上，輸入下列資訊：
 - a. 包含知識文章 — 選擇索引知識文章。
 - b. 知識文章類型 — 根據您的使用案例，在「僅包含公開文章」和「根據 ServiceNow 篩選器查詢包含文章」之間進行選擇。如果您選取「根據 ServiceNow 篩選器查詢包含文章」，則必須輸入從 ServiceNow 帳戶複製的篩選器查詢。
 - c. 包含知識文章附件 — 選擇索引知識文章附件。您也可以選取要建立索引的特定檔案類型。
 - d. 包含目錄項目 — 選擇索引目錄項目。
 - e. 包含目錄項目附件 — 選擇索引目錄項目附件。您也可以選取要建立索引的特定檔案類型。
 - f. 頻率：與資料來源同步的頻率。 Amazon Kendra
 - g. 選擇下一步。
 8. 在 [設定欄位對映] 頁面上，輸入下列資訊：
 - a. 知識文章和服務目錄 — 從 Amazon Kendra 產生的預設資料來源欄位和其他建議的欄位對應中選取您要對應至索引的其他建議欄位對應。
 - b. 新增欄位 — 新增自訂資料來源欄位，以建立要對映的索引欄位名稱和欄位資料類型。
 - c. 選擇下一步。
 9. 在 [檢閱並建立] 頁面上，檢查您輸入的資訊是否正確，然後選取 [新增資料來源]。您也可以從此頁面選擇編輯您的資訊。成功新增資料來源後，您的資料來源將顯示在 [資料來源] 頁面上。

API

若要連線 Amazon Kendra 到 ServiceNow

您必須使用 [ServiceNowConfiguration API](#) 指定下列項目：

- 資料來源 URL — 指定 ServiceNow URL。主機端點應如下所示：**#**的網域。

- 資料來源主機執行個體 — 將 ServiceNow 主機執行個體版本指定為 LONDON 或 OTHERS。
- 秘密 Amazon 資源名稱 (ARN) — 提供包含您在帳戶中建立的身份驗證登入資料的 Secrets Manager 密碼的 Amazon 資源名稱 (ARN)。ServiceNow

如果您使用的是基本驗證，密碼會以下列金鑰儲存在 JSON 結構中：

```
{
  "username": "user name",
  "password": "password"
}
```

如果您使用的是 OAuth2 驗證，則密碼會以下列金鑰儲存在 JSON 結構中：

```
{
  "username": "user name",
  "password": "password",
  "clientId": "client id",
  "clientSecret": "client secret"
}
```

- IAM role — 指定 RoleArn 何時呼叫 CreateDataSource 以提供具有存取 Secrets Manager 密碼之權限的 IAM 角色，以及呼叫 ServiceNow 連接器和 Amazon Kendra 所需公用 API 的時間。有關詳情，請參閱 [ServiceNow 料來源的 IAM 角色](#)。

您還可以添加以下可選功能：

- 欄位對映 — 選擇將 ServiceNow 料來源欄位對映至 Amazon Kendra 索引欄位。如需詳細資訊，請參閱 [映射資料來源欄位](#)。

Note

您的文件需要文件內文欄位或文件內文對等項目，才能搜尋您的文件。Amazon Kendra 您必須將資料來源中的文件內文欄位名稱對應至索引欄位名稱 `_document_body`。所有其他欄位是選用的。

- 包含和排除篩選器 — 指定是否要包含或排除目錄和知識文章的某些檔案附件。

Note

大多數資料來源使用規則運算式模式，這些模式是稱為篩選器的包含或排除模式。如果您指定包含篩選器，則只有符合包含項目篩選器的內容會編製索引。不符合包含篩選器的任何文件都不會建立索引。如果您指定包含和排除篩選器，符合排除篩選器的文件將不會建立索引，即使它們符合包含篩選器也是如此。

- 索引參數 — 您也可以選擇指定是否要：
 - 索引知識文章和服務目錄，或兩者。如果您選擇索引知識文件和服務目錄項目，則必須提供對應至索引中索引文件內容欄位的 Amazon Kendra 欄位名稱。ServiceNow
 - 為知識文章和目錄項目建立附件的索引。
 - 使用從一個或多個知識庫中選擇文檔的 ServiceNow 查詢。知識庫可以是公共的或私人的。如需詳細資訊，請參閱[使用查詢指定要索引的文件](#)。

進一步了解

若要進一步瞭解 Amazon Kendra 與 ServiceNow 資料來源整合的相關資訊，請參閱：

- [開始使用 Amazon Kendra ServiceNow 線上連接器](#)

ServiceNow 連接器 2.0 版

ServiceNow 提供雲端服務管理系統，以建立和管理組織層級的工作流程，例如 IT 服務、票務系統和支援。您可以用 Amazon Kendra 來編製目 ServiceNow 錄、知識文章、事件及其附件的索引。

如需疑難排解 Amazon Kendra ServiceNow 料來源連接器，請參閱[疑難排解資料來](#)。

主題

- [支援的功能](#)
- [必要條件](#)
- [連接說明](#)
- [進一步了解](#)

支援的功能

Amazon Kendra ServiceNow 資料來源連接器支援下列功能：

- 欄位對映
- 使用者存取控制
- 包含/排除過濾器
- 完整和增量內容同步
- ServiceNow 執行個體版本：羅馬、聖地牙哥、東京、其他
- 虛擬私有雲端 (VPC)

必要條件

在您可以用來 Amazon Kendra 為資料來源建立索引之前，請先在 ServiceNow 和 AWS 帳戶中進行這些變更。

在中 ServiceNow，請確定您有：

- 建立個人或企業開發人員執行個體，並擁有具有系統管理角色的 ServiceNow 執行個體。
- 已複製執行個體 URL 的主機。您輸入的主機網址格式為您的網#。您需要 ServiceNow 執行個體 URL 才能連線到 Amazon Kendra。
- 記下您的使用者名稱和密碼的基本驗證憑證，以允許連線 Amazon Kendra 至您的 ServiceNow 執行個體。

Note

我們建議您定期重新整理或輪換您的認證和密碼。僅為您自己的安全提供必要的訪問級別。我們不建議您跨資料來源以及連接器 1.0 和 2.0 版 (如果適用) 重複使用認證和密碼。

- 可選：已設定 OAuth 2.0 用戶端憑證，可 Amazon Kendra 使用使用者名稱、密碼和產生的用戶端 ID 和用戶端密碼進行識別。如需詳細資訊，請參閱 [OAuth 2.0 驗證的 ServiceNow 文件](#)。
- 已勾選的每個文件在您打算用於相同索引的其他資料來源中 ServiceNow 和其他資料來源之間都是唯一的。您要用於索引的每個資料來源不得包含跨資料來源的相同文件。文件 ID 對索引來說是全域的，而且每個索引必須是唯一的。

在你的 AWS 帳戶，確保你有：

- [建立 Amazon Kendra 索引](#)，如果使用 API，則會記下索引 ID。
- 為您的 [資料來源建立 IAM 角色](#)，如果使用 API，則會記錄 IAM 角色的 ARN。

Note

如果您變更驗證類型和認證，則必須更新 IAM 角色才能存取正確的 AWS Secrets Manager 密碼 ID。

- 將您的 ServiceNow 身份驗證憑據存儲在 AWS Secrets Manager 密鑰中，如果使用 API，則記錄密鑰的 ARN。

Note

我們建議您定期重新整理或輪換您的認證和密碼。僅為您自己的安全提供必要的訪問級別。我們不建議您跨資料來源以及連接器 1.0 和 2.0 版 (如果適用) 重複使用認證和密碼。

如果您沒有現有的 IAM 角色或密碼，則可以在將 ServiceNow 資料來源連線到時使用主控台建立新 IAM 角色和 Secrets Manager 密碼 Amazon Kendra。如果您使用 API，則必須提供現有 IAM 角色和 Secrets Manager 密碼的 ARN，以及索引 ID。

連接說明

若要連線 Amazon Kendra 到 ServiceNow 資料來源，您必須提供資料來源的必要詳細 ServiceNow 資訊，Amazon Kendra 以便能夠存取您的資料。如果您尚未設定「Amazon Kendra 請 ServiceNow 參閱[必要條件](#)」。

Console

若要連線 Amazon Kendra 到 ServiceNow

- 登入 AWS Management Console 並開啟[Amazon Kendra 主控台](#)。
- 在左側導覽窗格中，選擇 [索引]，然後從索引清單中選擇要使用的索引。

Note

您可以選擇在索引設置下配置或編輯您的用戶訪問控制設置。


- 在 [開始使用] 頁面上，選擇 [新增資料來源]。
- 在 [新增資料來源] 頁面上，選擇 [ServiceNow 連接器]，然後選擇 [新增連接器]。如果使用版本 2 (如果適用)，請選擇帶有「V2.0」標籤的 ServiceNow 連接器。

5. 在 [指定資料來源詳細資訊] 頁面上，輸入下列資訊：
 - a. 在名稱和說明中，對於資料來源名稱 — 輸入資料來源的名稱。您可以包含連字號，但不能包含空格。
 - b. (選擇性) 說明 — 輸入資料來源的選用說明。
 - c. 在預設語言中 — 選擇一種語言來篩選索引的文件。除非另有指定，否則語言預設為英文。文件中繼資料中指定的語言會覆寫選取的語言。
 - d. 在「標籤」中，針對「新增標籤」 — 包含可選標籤以搜尋和篩選資源或追蹤 AWS 成本。
 - e. 選擇下一步。
6. 在 [定義存取和安全性] 頁面上，輸入下列資訊：
 - a. ServiceNow 主機 — 輸入 ServiceNow 主機 URL。您輸入的主機網址格式為您的網#。
 - b. ServiceNow 版本 — 選取您的 ServiceNow 執行個體版本。您可以選擇羅馬，聖地牙哥，東京或其他。
 - c. 授權 — 開啟或關閉文件的存取控制清單 (ACL) 資訊 (如果您有 ACL)，且想要將其用於存取控制。ACL 會指定使用者和群組可存取的文件。ACL 資訊可用來根據使用者或使用者對文件的群組存取權來篩選搜尋結果。如需詳細資訊，請參閱[使用者內容篩選](#)。
 - d. 驗證 — 在「基本驗證」和「OAuth 2.0」驗證之間進行選擇。
 - e. AWS Secrets Manager 祕密 — 選擇現有密碼或建立新 Secrets Manager 密碼來儲存您的 ServiceNow 驗證認證。如果您選擇建立新密碼，則會開啟一個 AWS Secrets Manager 密碼視窗。在視窗中輸入下列資訊：
 - i. 祕密名稱 — 您祕密的名稱。前綴 'AmazonKendraServiceNow-' 會自動添加到您的密碼名稱中。
 - ii. 如果使用基本驗證 — 輸入您帳戶的密碼名稱、使用者名稱和密碼。 ServiceNow

如果使用 OAuth2.0 驗證 — 請輸入您在帳戶中建立的密碼名稱、使用者名稱、密碼、用戶端 ID 和用戶端密碼。 ServiceNow
 - iii. 保存並添加您的祕密。
 - f. Virtual Private Cloud (VPC) (VPC) — 您可以選擇使用 VPC。如果是這樣，您必須新增子網路和 VPC 安全性群組。
 - g. 識別爬行者程式 — 指定是否要開啟身分爬行 Amazon Kendra 者程式。識別爬行者程式會使用文件的存取控制清單 (ACL) 資訊，根據使用者或使用者對文件的群組存取權來篩選搜尋結果。如果您有文件的 ACL 並選擇使用 ACL，您也可以選擇開啟的身分識別爬行者程式，以設定搜尋結果的[使用者環境定義篩選](#)。 Amazon Kendra 否則，如果關閉身分搜索

器，則可以公開搜索所有文檔。如果您想要對文件使用存取控制，且身分識別編目程式已關閉，您也可以使用 [PutPrincipalMapping](#) API 來上傳使用者和群組存取資訊以進行使用者內容篩選。

- h. IAM role — 選擇現有 IAM 角色或建立新 IAM 角色以存取存放庫認證和索引內容。

 Note


IAM 用於索引的角色不能用於資料來源。如果您不確定索引或常見問題集是否使用現有角色，請選擇 [建立新角色] 以避免發生錯誤。

- i. 選擇下一步。

7. 在 [設定同步設定] 頁面上，輸入下列資訊：

- a. 對於知識文章，請從下列選項中選擇：

- 知識文章 — 選擇索引知識文章。
- 知識文章附件 — 選擇索引知識文章附件。
- 知識文章類型 — 根據您的使用案例，在僅公開文章和知識文章之間進行 ServiceNow 選擇。如果您選取「根據 ServiceNow 篩選器查詢包含文章」，則必須輸入從 ServiceNow 帳戶複製的篩選器查詢。`##### = ## ^ ####kb_##
_base=dfc19531bf202f072C1ac0739 ## ^ ##### ^ EQ### _ ## = ## ^
= ## ^ EQ#`

 Important

如果您選擇僅編目公開文章，則只會 Amazon Kendra 探索中 ServiceNow 指派公用存取角色的知識文章。

- 包含以簡短描述篩選為基礎的文章：指定規則運算式模式以包含或排除特定文章。

- b. 對於服務目錄項目：

- 服務目錄項目 — 選擇索引服務目錄項目。
- 服務目錄項目附件 — 選擇索引服務目錄項目附件。
- 作用中的服務目錄項目 — 選擇索引作用中的服務目錄項目。
- 非作用中服務目錄項目 — 選擇索引非作用中的服務目錄項目。

- 篩選器查詢 — 根據 ServiceNow 執行個體中定義的篩選器，選擇包含服務目錄項目。#
^ ## =2809952237B13000B6A3549d4^ EQ#####
^ ### = ## ^ EQ#
 - 根據簡短描述篩選包含服務目錄項目 — 指定規則運算式模式以包含特定目錄項目。
- c. 對於事件：
- 未預期事件 — 選擇索引服務事件。
 - 事件附件 — 選擇索引未預期事件附件。
 - 作用中事件 — 選擇索引作用中事件。
 - 非作用中事件 — 選擇索引非作用中事件。
 - 作用中事件類型 — 根據您的使用案例，選擇「所有事件」、「未結事件」、「開啟-未指派的事件」及「已解決的事件」。
 - 篩選器查詢 — 選擇根據 ServiceNow 執行個體中定義的篩選器包含事件。#####
^ ## = 3 ^ ## = 1 ^ EQ#### = 2 ^ ## = ## ^ EQ#
 - 包含以簡短描述篩選為基礎的事件 — 指定規則運算式模式以包含特定事件。
- d. 對於其他配置：
- ACL 資訊 — 依預設會包含您所選圖元的存取控制清單。取消選取存取控制清單後，該類別中的所有檔案都會公開。對於未選取的圖元，ACL 選項會自動停用。針對公開文章，不會套用 ACL。
 - 對於檔案大小上限 — 指定 Amazon Kendra 將抓取的檔案大小限制 (以 MB 為單位)。Amazon Kendra 只會抓取您定義的大小限制內的檔案。預設檔案大小為 50MB。檔案大小上限應該大於 0MB 且小於或等於 50MB。
 - 附件 regex 模式 — 新增規則運算式模式，以包含或排除目錄、知識文章和事件的某些附加檔案。您最多可以添加 100 個圖案。
- e. 同步模式 — 選擇資料來源內容變更時要如何更新索引。當您第一次將資料來源同 Amazon Kendra 步處理時，依預設會檢索所有內容並建立索引。如果初始同步失敗，您必須執行資料的完整同步處理，即使您沒有選擇完整同步作為同步模式選項。
- 完全同步：新鮮索引所有內容，並在每次資料來源與索引同步時取代現有內容。
 - 新增、修改、刪除的同步：每次資料來源與索引同步時，僅對新內容、已修改和刪除的內容建立索引。Amazon Kendra 可以使用資料來源的機制來追蹤內容變更，並為上次同步後變更的內容建立索引。
- f. 在同步執行排程中，對於頻率 — 選擇同步資料來源內容和更新索引的頻率。

- g. 選擇下一步。
8. 在 [設定欄位對映] 頁面上，輸入下列資訊：
 - a. 預設欄位對映 — 從 Amazon Kendra 產生的預設資料來源欄位中選取您要對映至索引的欄位。
 - b. 新增欄位 — 新增自訂資料來源欄位，以建立要對映的索引欄位名稱和欄位資料類型。
 - c. 選擇下一步。
9. 在 [檢閱並建立] 頁面上，檢查您輸入的資訊是否正確，然後選取 [新增資料來源]。您也可以從此頁面選擇編輯您的資訊。成功新增資料來源後，您的資料來源將顯示在 [資料來源] 頁面上。

API

若要連線 Amazon Kendra 到 ServiceNow

您必須使用 [TemplateConfiguration](#) API 指定 [資料來源結構描述](#) 的 JSON。您必須提供以下信息：

- 資料來源 — 指定使用 [TemplateConfiguration](#) JSON 結構定義 SERVICENOWV2 時的資料來源類型。同時指定呼叫 [CreateDataSource](#) API TEMPLATE 時的資料來源。
- 主機 URL — 指定 ServiceNow 主機執行個體版本。例如，`###.####.com`。
- 驗證類型 — 指定您使用的驗證類型 (無論執行個體 basicAuth 或 OAuth2 ServiceNow 執行個體)。
- ServiceNow 例證版本 — 指定您使用的 ServiceNow 實例，無論是 Tokyo、SanDiegoRome、還 Others 是。
- 同步模式 — 指定資料來源內容變更時 Amazon Kendra 應如何更新索引。當您第一次將資料來源同 Amazon Kendra 步處理時，依預設會檢索所有內容並建立索引。如果初始同步失敗，您必須執行資料的完整同步處理，即使您沒有選擇完整同步作為同步模式選項。您可以選擇：
 - FORCED_FULL_CRAWL 新建索引所有內容，並在每次資料來源與索引同步時取代現有內容。
 - FULL_CRAWL，以在每次資料來源與索引同步時，僅對新的、修改的和刪除的內容建立索引。Amazon Kendra 可以使用資料來源的機制來追蹤內容變更，並為上次同步後變更的內容建立索引。
- 秘密 Amazon 資源名稱 (ARN) — 提供包含您在帳戶中建立的身份驗證登入資料的 Secrets Manager 密碼的 Amazon 資源名稱 (ARN)。ServiceNow

如果您使用基本驗證，密碼會以下列金鑰儲存在 JSON 結構中：

```
{
```



```
"username": "user name",  
"password": "password"  
}
```

- 如果您使用 OAuth2 用戶端認證，密碼會以下列金鑰儲存在 JSON 結構中：

```
{  
  "username": "user name",  
  "password": "password",  
  "clientId": "client id",  
  "clientSecret": "client secret"  
}
```

- IAM role — 指定RoleArn何時呼叫CreateDataSource以提供具有存取 Secrets Manager 密碼之權限的 IAM 角色，以及呼叫 ServiceNow 連接器和 Amazon Kendra所需公用 API 的時間。有關詳情，請參閱[ServiceNow 料來源的IAM 角色](#)。

您還可以添加以下可選功能：


- Virtual Private Cloud (VPC) — 指定您呼叫的VpcConfiguration時間。CreateDataSource如需詳細資訊，請參閱[配置 Amazon Kendra 為使用 Amazon VPC](#)。
- 包含和排除篩選器 — 您可以使用檔案名稱和知識文章、服務目錄和事件的檔案類型，指定是否要包含或排除某些附加檔案。

Note

大多數資料來源使用規則運算式模式，這些模式是稱為篩選器的包含或排除模式。如果您指定包含篩選器，則只有符合包含項目篩選器的內容會編製索引。不符合包含篩選器的任何文件都不會建立索引。如果您指定包含和排除篩選器，符合排除篩選器的文件將不會建立索引，即使它們符合包含篩選器也是如此。

- 要索引的特定文件 — 您可以使用 ServiceNow查詢，從一或多個知識庫 (包括私人知識庫) 中指定您想要的文件。知識庫的存取權由您用來連線至 ServiceNow 執行個體的使用者決定。如需詳細資訊，請參閱[使用查詢指定要索引的文件](#)。
- 索引參數 — 您也可以選擇指定是否要：
 - 索引知識文章、服務目錄和事件，或所有這些。如果您選擇索引知識文件、服務目錄項目和事件，則必須提供對應至索引中索引文件內容欄位的 Amazon Kendra 欄位名稱。ServiceNow
 - 將附件索引至知識文章、服務目錄項目和事件。

- 根據short description篩選器模式包含知識文章、服務目錄項目和事件。
- 選擇此選項可篩選作用中和非作用中服務目錄項目與事件
- 選擇此選項可根據事件類型篩選事件。
- 選擇哪些實體應該探索其 ACL。
- 您可以使用 ServiceNow 查詢從一個或多個知識庫 (包括私有知識庫) 中指定所需的文檔。知識庫的存取權由您用來連線至 ServiceNow 執行個體的使用者決定。如需詳細資訊，請參閱[使用查詢指定要索引的文件](#)。
- 識別爬行者程式 — 指定是否要開啟身分爬行 Amazon Kendra 者程式。識別爬行者程式會使用文件的存取控制清單 (ACL) 資訊，根據使用者或使用者對文件的群組存取權來篩選搜尋結果。如果您有文件的 ACL 並選擇使用 ACL，您也可以選擇開啟的身分識別爬行者程式，以設定搜尋結果的使用者環境定義篩選。Amazon Kendra 否則，如果關閉身分搜索器，則可以公開搜索所有文檔。如果您想要對文件使用存取控制，且身分識別編目程式已關閉，您也可以使用 [PutPrincipalMapping](#) API 來上傳使用者和群組存取資訊以進行使用者內容篩選。
- 欄位對映 — 選擇將 ServiceNow 資料來源欄位對映至 Amazon Kendra 索引欄位。如需詳細資訊，請參閱[映射資料來源欄位](#)。

 Note

您的文件需要文件內文欄位或文件內文對等項目，才能搜尋您的文件。Amazon Kendra 您必須將資料來源中的文件內文欄位名稱對應至索引欄位名稱_document_body。所有其他欄位是選用的。

如需要設定的其他重要 JSON 金鑰清單，請參閱[ServiceNow 範本結構定義](#)。

進一步了解

若要進一步瞭解 Amazon Kendra 與 ServiceNow 資料來源整合的相關資訊，請參閱：

- [開始使用 Amazon Kendra 宣布更新的 ServiceNow 連接器 \(V2\) Amazon Kendra](#)

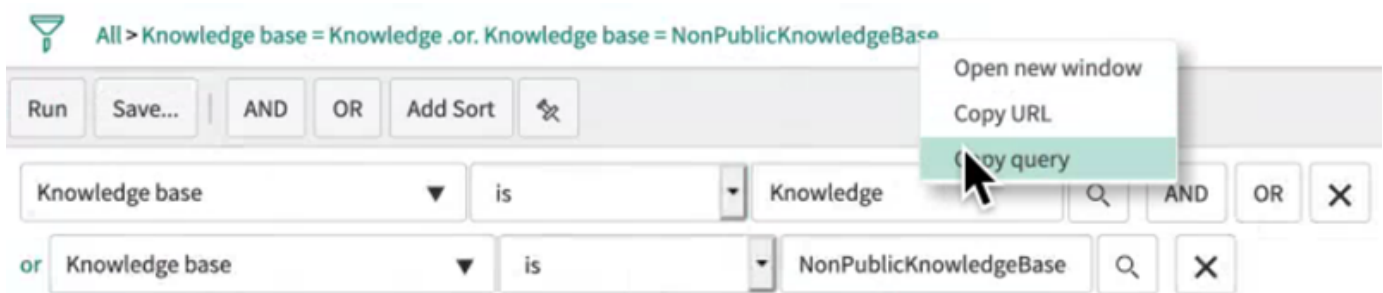
使用查詢指定要編製索引的文件

您可以使用 ServiceNow 查詢來指定要包含在 Amazon Kendra 索引中的文件。使用查詢時，您可以指定多個知識庫，包括私有知識庫。知識庫的存取權由您用來連線至 ServiceNow 執行個體的使用者決定。

若要建立查詢，請使用查 ServiceNow 詢建置器。您可以使用建構器來建立查詢，並測試查詢是否傳回正確的文件清單。

若要使用 ServiceNow 主控台建立查詢

1. 登入 ServiceNow 主控台。
2. 從左側選單中選擇「知識」，然後選擇「文章」，然後選擇「全部」。
3. 在頁面頂端，選擇篩選器圖示。
4. 使用查詢建置器建立查詢。
5. 查詢完成後，請在查詢上按一下滑鼠右鍵，然後選擇「複製查詢」，以從查詢建構器複製查詢。儲存此查詢以在中使用 Amazon Kendra。



複製查詢時，請確定未變更任何查詢參數。如果無法辨識任何查詢參數，請 ServiceNow 將參數視為空，而不會使用它來篩選結果。

Slack

Slack 是一款企業通信應用程序，可讓用戶通過各種公共和私有渠道發送消息和附件。您可以用 Amazon Kendra 來為 Slack 公開和私人通道、機器人和封存訊息、檔案和附件、直接和群組訊息建立索引。您也可以選擇要過濾的特定內容。

Note

Amazon Kendra 現在支援升級的 Slack 連接器。

主機已自動為您升級。您在中建的任何新連接器都會使用升級的架構。如果您使用 API，您現在必須使用 [TemplateConfiguration](#) 物件而非 `SlackConfiguration` 物件來設定連接器。

使用舊版主控台和 API 架構設定的連接器將繼續如設定般運作。但是，您將無法編輯或更新它們。如果您要編輯或更新連接器組態，您必須建立新的連接器。

建議您將連接器工作流程移轉至升級版本。使用舊架構設定的連接器 Support 排程於 2024 年 6 月結束。

您可以使用 [Amazon Kendra 主控台](#) 或 [TemplateConfigurationAPI](#) 連線 Amazon Kendra 到 Slack 資料來源。

如需 Amazon Kendra Slack 資料來源連接器的疑難排解，請參閱 [疑難排解資料來](#)。

主題

- [支援的功能](#)
- [必要條件](#)
- [連接說明](#)
- [進一步了解](#)

支援的功能

Amazon Kendra Slack 資料來源連接器支援下列功能：

- 欄位對映
- 使用者存取控制
- 包含/排除過濾器
- 完整和增量內容同步
- 虛擬私有雲端 (VPC)

必要條件

在您可以用來 Amazon Kendra 為 Slack 資料來源建立索引之前，請先在 Slack 和 AWS 帳戶中進行這些變更。

在 Slack 中，請確定您擁有：

- 配置了鬆弛機器人用戶 OAuth 令牌或鬆弛用戶 OAuth 令牌。您可以選擇任一權杖來連線 Amazon Kendra 至 Slack 資料來源。需要令牌才能用作您的身份驗證憑據。有關更多信息，請參閱有 [關訪問令牌的 Slack 文檔](#)。

Note

如果您將機器人令牌用作 Slack 憑據的一部分，則無法為直接消息和群組消息編制索引，並且必須將機器人令牌添加到要編制索引的渠道中。

Note

我們建議您定期重新整理或輪換您的認證和密碼。僅為您自己的安全提供必要的訪問級別。我們不建議您跨資料來源以及連接器 1.0 和 2.0 版 (如果適用) 重複使用認證和密碼。

- 從 Slack 工作區主頁面網址記下您的 Slack 工作區團隊 ID。舉個例子, <https://app.slack.com/client/T0123456789/...> 其中 *T0123456789* 是群組識別碼。
- 已新增下列 Oauth 範圍/權限：

使用者權杖範圍	機器人令牌範圍
• 頻道:歷史	• 頻道:歷史
• 頻道:讀取	• 通道:管理
• 表情符號:讀取	• 頻道:讀取
• 檔案:讀取	• 交談. 連線:管理
• 群組:歷程	• 對話. 連線:讀取
• 群組:讀取	• 檔案:讀取
• IM: 歷程	• 群組:歷程
• IM: 讀取	• 群組:讀取
• MPIM: 歷程	• IM: 歷程
• MPM: 讀取	• IM: 讀取
• team:read	• MPIM: 歷程
• 使用者. 設定檔:讀取	• MPM: 讀取
• 使用者:讀取	• 反應:讀取
• 使用者:讀取. 電子郵件	• team:read
	• 使用者群組:讀取
	• 使用者. 設定檔:讀取

使用者權杖範圍

機器人令牌範圍

- 使用者:讀取
- 使用者:讀取. 電子郵件

- 已勾選的每個文件在 Slack 和您打算用於相同索引的其他資料來源中都是唯一的。您要用於索引的每個資料來源不得包含跨資料來源的相同文件。文件 ID 對索引來說是全域的，而且每個索引必須是唯一的。

在您的中 AWS 帳戶，請確保您有：

- [建立 Amazon Kendra 索引](#)，如果使用 API，則會記下索引 ID。
- 為您的[資料來源建立 IAM 角色](#)，如果使用 API，則會記錄 IAM 角色的 ARN。

Note

如果您變更驗證類型和認證，則必須更新 IAM 角色才能存取正確的 AWS Secrets Manager 密碼 ID。

- 將您的 Slack 驗證憑證儲存在 AWS Secrets Manager 密碼中，如果使用 API，則會記錄密碼的 ARN。

Note

我們建議您定期重新整理或輪換您的認證和密碼。僅為您自己的安全提供必要的訪問級別。我們不建議您跨資料來源以及連接器 1.0 和 2.0 版 (如果適用) 重複使用認證和密碼。

如果您沒有現有的 IAM 角色或密碼，則可以在將 Slack 資料來源連線至時使用主控台建立新 IAM 角色和 Secrets Manager 密碼。Amazon Kendra 如果您使用 API，則必須提供現有 IAM 角色和 Secrets Manager 密碼的 ARN，以及索引 ID。

連接說明

若要連線 Amazon Kendra 至 Slack 資料來源，您必須提供 Slack 資料來源的必要詳細資訊，Amazon Kendra 以便存取您的資料。如果您尚未為 Slack 設定 Amazon Kendra，請參閱[必要條件](#)。

Console

若要連線 Amazon Kendra 至鬆弛


1. 登入 AWS Management Console 並開啟 [Amazon Kendra 主控台](#)。
2. 在左側導覽窗格中，選擇 [索引]，然後從索引清單中選擇要使用的索引。

Note

您可以選擇在索引設置下配置或編輯您的用戶訪問控制設置。


3. 在 [開始使用] 頁面上，選擇 [新增資料來源]。
4. 在 [新增資料來源] 頁面上，選擇 [Slack 連接器]，然後選擇 [新增連接器]。如果使用第 2 版（如果適用），請選擇帶有「V2.0」標籤的 Slack 連接器。
5. 在 [指定資料來源詳細資訊] 頁面上，輸入下列資訊：
 - a. 在名稱和說明中，對於資料來源名稱 — 輸入資料來源的名稱。您可以包含連字號，但不能包含空格。
 - b. (選擇性) 說明 — 輸入資料來源的選用說明。
 - c. 在預設語言中 — 選擇一種語言來篩選索引的文件。除非另有指定，否則語言預設為英文。文件中繼資料中指定的語言會覆寫選取的語言。
 - d. 在「標籤」中，針對「新增標籤」 — 包含可選標籤以搜尋和篩選資源或追蹤 AWS 成本。
 - e. 選擇下一步。
6. 在 [定義存取和安全性] 頁面上，輸入下列資訊：
 - a. 適用於 Slack 工作區團隊 ID — Slack 工作區的團隊 ID。您可以在 Slack 工作區主頁面 URL 中找到您的團隊 ID。舉個例子，<https://app.slack.com/client/T0123456789/...> 其中 `T0123456789` 是群組識別碼。
 - b. 授權 — 開啟或關閉文件的存取控制清單 (ACL) 資訊 (如果您有 ACL)，且想要將其用於存取控制。ACL 會指定使用者和群組可存取的文件。ACL 資訊可用來根據使用者或使用者對文件的群組存取來篩選搜尋結果。如需詳細資訊，請參閱 [使用者內容篩選](#)。
 - c. AWS Secrets Manager 秘密：選擇現有密碼或建立新 Secrets Manager 密碼來儲存您的 Slack 驗證憑證。如果您選擇建立新密碼，則會開啟一個 AWS Secrets Manager 密碼視窗。
 - i. 在「建立 AWS Secrets Manager 密碼視窗」中輸入下列資訊：

- A. 秘密名稱 — 您秘密的名稱。字首 'AmazonKendra-Slack-' 會自動新增至您的密碼名稱。
 - B. 針對 Slack 權杖 — 輸入您設定 Slack 的驗證認證值。
- ii. 保存並添加您的秘密。
- d. Virtual Private Cloud (VPC) (VPC) — 您可以選擇使用 VPC。如果是這樣，您必須新增子網路和 VPC 安全性群組。
 - e. 識別爬行者程式 — 指定是否要開啟身分爬行 Amazon Kendra 爬行者程式。識別爬行者程式會使用文件的存取控制清單 (ACL) 資訊，根據使用者或使用者對文件的群組存取權來篩選搜尋結果。如果您有文件的 ACL 並選擇使用 ACL，您也可以選擇開啟的身分識別爬行者程式，以設定搜尋結果的使用者環境定義篩選。Amazon Kendra 否則，如果關閉身分搜索器，則可以公開搜索所有文檔。如果您想要對文件使用存取控制，且身分識別編目程式已關閉，您也可以使用 [PutPrincipalMapping](#) API 來上傳使用者和群組存取資訊以進行使用者內容篩選。
 - f. IAM role — 選擇現有 IAM 角色或建立新 IAM 角色以存取存放庫認證和索引內容。

 Note

IAM 用於索引的角色不能用於資料來源。如果您不確定索引或常見問題集是否使用現有角色，請選擇 [建立新角色] 以避免發生錯誤。

- g. 選擇下一步。
7. 在 [設定同步設定] 頁面上，輸入下列資訊：
- a. 選取內容類型 — 選取您要編目的 Slack 實體或內容類型。您可以從所有頻道、公開頻道、私人頻道、群組訊息和私人訊息中進行選擇。
 - b. 選取編目開始日期 — 輸入您要開始檢索內容的日期。
 - c. 對於其他組態 — 選擇包含機器人和封存訊息，並使用規則運算式模式來包含或排除特定內容。

 Note

如果您選擇同時包含通道 ID 和通道名稱，則 Amazon Kendra Slack 連接器會將通道 ID 優先於通道名稱。

如果您選擇包含特定的私人和群組郵件，Amazon Kendra Slack 連接器會忽略所有私人和群組郵件，而且只會編目您指定的私人和群組郵件。

- d. 同步模式 — 選擇資料來源內容變更時要如何更新索引。當您第一次將資料來源同 Amazon Kendra 步處理時，依預設會檢索所有內容並建立索引。如果初始同步失敗，您必須執行資料的完整同步處理，即使您沒有選擇完整同步作為同步模式選項。
 - 完全同步：新鮮索引所有內容，並在每次資料來源與索引同步時取代現有內容。
 - 新增、修改、刪除的同步：每次資料來源與索引同步時，僅對新內容、已修改和刪除的內容建立索引。Amazon Kendra 可以使用資料來源的機制來追蹤內容變更，並為上次同步後變更的內容建立索引。
 - e. 在同步執行排程中，對於頻率 — 選擇同步資料來源內容和更新索引的頻率。
 - f. 選擇下一步。
8. 在 [設定欄位對映] 頁面上，輸入下列資訊：
 - a. 預設資料來源欄位 — 從 Amazon Kendra 產生的預設資料來源欄位中選取您要對映至索引的資料來源欄位。
 - b. 新增欄位 — 新增自訂資料來源欄位，以建立要對映的索引欄位名稱和欄位資料類型。
 - c. 選擇下一步。
 9. 在 [檢閱並建立] 頁面上，檢查您輸入的資訊是否正確，然後選取 [新增資料來源]。您也可以從此頁面選擇編輯您的資訊。成功新增資料來源後，您的資料來源將顯示在 [資料來源] 頁面上。

API

若要連線 Amazon Kendra 至鬆弛

您必須使用 [TemplateConfiguration](#) API 指定 [資料來源結構描述](#) 的 JSON。您必須提供以下信息：

- 資料來源 — 指定使用 [TemplateConfiguration](#) JSON 結構定義 SLACK 時的資料來源類型。同時指定呼叫 [CreateDataSource](#) API TEMPLATE 時的資料來源。
- 鬆弛工作區團隊 ID — 您從 Slack 主頁面 URL 複製的 Slack 團隊 ID。
- 自日期 — 開始從 Slack 工作區團隊檢索資料的日期。日期必須遵循以下格式：yyyy-mm-dd。
- 同步模式 — 指定資料來源內容變更時 Amazon Kendra 應如何更新索引。當您第一次將資料來源同 Amazon Kendra 步處理時，依預設會檢索所有內容並建立索引。如果初始同步失敗，您必須執行資料的完整同步處理，即使您沒有選擇完整同步作為同步模式選項。您可以選擇：
 - FORCED_FULL_CRAWL 新建索引所有內容，並在每次資料來源與索引同步時取代現有內容。

- FULL_CRAWL，以在每次資料來源與索引同步時，僅對新的、修改的和刪除的內容建立索引。Amazon Kendra 可以使用資料來源的機制來追蹤內容變更，並為上次同步後變更的內容建立索引。
- CHANGE_LOG每次資料來源與索引同步時，僅對新內容和修改的內容建立索引。Amazon Kendra 可以使用資料來源的機制來追蹤內容變更，並為上次同步後變更的內容建立索引。
- 識別爬行者程式 — 指定是否要開啟身分爬行者 Amazon Kendra 程式。識別爬行者程式會使用文件的存取控制清單 (ACL) 資訊，根據使用者或使用者對文件的群組存取權來篩選搜尋結果。如果您有文件的 ACL 並選擇使用 ACL，您也可以選擇開啟的身分識別爬行者程式，以設定搜尋結果的使用者環境定義篩選。Amazon Kendra 否則，如果關閉身分搜索器，則可以公開搜索所有文檔。如果您想要對文件使用存取控制，且身分識別編目程式已關閉，您也可以使用 [PutPrincipalMapping](#) API 來上傳使用者和群組存取資訊以進行使用者內容篩選。
- 秘密 Amazon 資源名稱 (ARN) — 提供包含 Slack 帳戶身份驗證登入資料的 Secrets Manager 密碼的 Amazon 資源名稱 (ARN)。密碼會以下列金鑰儲存在 JSON 結構中：

```
{
  "slackToken": "token"
}
```

- IAM role — 指定 RoleArn 當您呼叫 CreateDataSource 以提供具有存取 Secrets Manager 密碼之權限的 IAM 角色，以及呼叫 Slack 連接器和所需的公用 API 的時間。Amazon Kendra 如需詳細資訊，請參閱 [Slack 資料來源的 IAM 角色](#)。

您還可以添加以下可選功能：

- Virtual Private Cloud (VPC) — 指定您呼叫的 VpcConfiguration 時間。CreateDataSource 如需詳細資訊，請參閱 [配置 Amazon Kendra 為使用 Amazon VPC](#)。
- 特定頻道：依公開或私人頻道進行篩選，並依其 ID 指定特定頻道。
- 頻道和訊息類型 — 是否 Amazon Kendra 應為公開和私人頻道、群組和直接訊息，以及機器人和封存訊息建立索引。如果您使用機器人令牌作為 Slack 身份驗證憑據的一部分，則必須將機器人令牌添加到要索引的通道中。您無法使用機器人權杖建立直接訊息和群組訊息的索引。
- 回顧 — 您可以選擇設定 lookBack 參數，讓 Slack 連接器在上次連接器同步之前的指定小時內搜索更新或刪除的內容。
- 包含和排除篩選器：指定要包含還是排除特定 Slack 內容。如果您使用機器人令牌作為 Slack 身份驗證憑據的一部分，則必須將機器人令牌添加到要索引的通道中。您無法使用機器人權杖建立直接訊息和群組訊息的索引。

Note

大多數資料來源使用規則運算式模式，這些模式是稱為篩選器的包含或排除模式。如果您指定包含篩選器，則只有符合包含項目篩選器的內容會編製索引。不符合包含篩選器的任何文件都不會建立索引。如果您指定包含和排除篩選器，符合排除篩選器的文件將不會建立索引，即使它們符合包含篩選器也是如此。

- 欄位對映 — 選擇將 Slack 資料來源欄位對映至 Amazon Kendra 索引欄位。如需詳細資訊，請參閱[映射資料來源欄位](#)。

Note

您的文件需要文件內文欄位或文件內文對等項目，才能搜尋您的文件。Amazon Kendra 您必須將資料來源中的文件內文欄位名稱對應至索引欄位名稱_document_body。所有其他欄位是選用的。

如需要設定的其他重要 JSON 金鑰清單，請參閱[Slack 範本結構定義](#)。

進一步了解

若要深入瞭解如何 Amazon Kendra 與 Slack 資料來源整合，請參閱：

- [使用 Slack 連接器透過智慧型搜尋來解開 Slack 工作區中的知識 Amazon Kendra](#)

Zendesk

Zendesk 是一個客戶關係管理系統，可幫助企業自動化並增強客戶支持互動。您可以用 Amazon Kendra 來為 Zendesk 支援票證、票證註解、票證附件、說明中心文章、文章註解、文章評論附件、指南社群主題、社群貼文和社群貼文註解建立索引。

如果您要索引僅在特定組織內的工單，您可以依組織名稱進行篩選。您也可以選擇設定編目日期，以便開始從 Zendesk 探索資料的時間。

您可以使用[Amazon Kendra 主控台](#)和 [TemplateConfiguration](#) API 連線 Amazon Kendra 至 Zendesk 資料來源。

若要疑難排解 Amazon Kendra Zendesk 資料來源連接器，請參閱[疑難排解資料來](#)。

主題

- [支援的功能](#)
- [必要條件](#)
- [連接說明](#)
- [進一步了解](#)

支援的功能

Amazon Kendra Zendesk 資料來源連接器支援下列功能：

- 欄位對映
- 使用者存取控制
- 包含/排除過濾器
- 更改日誌，完整和增量內容同步
- 虛擬私有雲端 (VPC)

必要條件

在您可以使用 Amazon Kendra 對 Zendesk 資料來源建立索引之前，請先在 Zendesk 和 AWS 帳戶中進行這些變更。

在 ZENDESK 中，請確保您擁有：

- 創建了一個 Zendesk 套件（專業/企業）管理帳戶。
- 記下您的 Zendesk 主機網址。例如：<https://{sub-domain}.zendesk.com/>。

Note

(預備內部/伺服器) Amazon Kendra 會檢查中包含的端點資訊 AWS Secrets Manager 是否與資料來源組態詳細資料中指定的端點資訊相同。這有助於防止[混淆的副問題](#)，這是一個安全性問題，即使用者沒有執行動作的權限，但用 Amazon Kendra 作 Proxy 來存取設定的密碼並執行動作。如果您稍後變更端點資訊，則必須建立新密碼才能同步此資訊。

- 設定包含用戶端 ID、用戶端密碼、使用者名稱和密碼的 OAuth 2.0 權杖。OAuth 2.0 令牌需要用作您的身份驗證憑據。有關更多信息，請參閱有關[配置 OAuth 2.0 令牌的 Zendesk 文檔](#)。

Note

我們建議您定期重新整理或輪換您的認證和密碼。僅為您自己的安全提供必要的訪問級別。我們不建議您跨資料來源以及連接器 1.0 和 2.0 版 (如果適用) 重複使用認證和密碼。

- 已新增下列 OAuth 2.0 範圍：
 - 讀取
- 選用性：安裝允許連線 Amazon Kendra 的 SSL 憑證。
- 核取每個文件在 Zendesk 和您打算用於相同索引的其他資料來源中都是唯一的。您要用於索引的每個資料來源不得包含跨資料來源的相同文件。文件 ID 對索引來說是全域的，而且每個索引必須是唯一的。

在你的 AWS 帳戶，確保你有：

- [建立 Amazon Kendra 索引](#)，如果使用 API，則會記下索引 ID。
- 為您的[資料來源建立 IAM 角色](#)，如果使用 API，則會記錄 IAM 角色的 ARN。

Note

如果您變更驗證類型和認證，則必須更新 IAM 角色才能存取正確的 AWS Secrets Manager 密碼 ID。

- 將您的 Zendesk 驗證憑證儲存在 AWS Secrets Manager 密碼中，如果使用 API，則會記下密碼的 ARN。

Note

我們建議您定期重新整理或輪換您的認證和密碼。僅為您自己的安全提供必要的訪問級別。我們不建議您跨資料來源以及連接器 1.0 和 2.0 版 (如果適用) 重複使用認證和密碼。

如果您沒有現有的 IAM 角色或密碼，則可以在將 Zendesk 資料來源連線至時使用主控台建立新 IAM 角色和 Secrets Manager 密碼。Amazon Kendra 如果您使用 API，則必須提供現有 IAM 角色和 Secrets Manager 密碼的 ARN，以及索引 ID。

連接說明

若要連線 Amazon Kendra 至 Zendesk 資料來源，您必須提供 Zendesk 資料來源的必要詳細資料，Amazon Kendra 以便能夠存取您的資料。如果您尚未為 Zendesk 設定 Amazon Kendra，請參閱[必要條件](#)。

Console

若要連接 Amazon Kendra 至天台


1. 登入 AWS Management Console 並開啟[Amazon Kendra 主控台](#)。
2. 在左側導覽窗格中，選擇 [索引]，然後從索引清單中選擇要使用的索引。

Note

您可以選擇在索引設置下配置或編輯您的用戶訪問控制設置。

3. 在 [開始使用] 頁面上，選擇 [新增資料來源]。
4. 在 [新增資料來源] 頁面上，選擇 [Zendesk 連接器]，然後選擇 [新增連接器]。如果使用第 2 版（如果適用），請選擇帶有「V2.0」標籤的 Zendesk 連接器。
5. 在 [指定資料來源詳細資訊] 頁面上，輸入下列資訊：
 - a. 在名稱和說明中，對於資料來源名稱 — 輸入資料來源的名稱。您可以包含連字號，但不能包含空格。
 - b. (選擇性) 說明 — 輸入資料來源的選用說明。
 - c. 在預設語言中 — 選擇一種語言來篩選索引的文件。除非另有指定，否則語言預設為英文。文件中繼資料中指定的語言會覆寫選取的語言。
 - d. 在「標籤」中，針對「新增標籤」 — 包含可選標籤以搜尋和篩選資源或追蹤 AWS 成本。
 - e. 選擇下一步。
6. 在 [定義存取和安全性] 頁面上，輸入下列資訊：
 - a. Zendesk 網址 — 輸入您的 Zendesk 網址。例如：`https://{sub-domain}.zendesk.com/`。
 - b. 授權 — 開啟或關閉文件的存取控制清單 (ACL) 資訊 (如果您有 ACL)，且想要將其用於存取控制。ACL 會指定使用者和群組可存取的文件。ACL 資訊可用來根據使用者或使用者對文件的群組存取權來篩選搜尋結果。如需詳細資訊，請參閱[使用者內容篩選](#)。

- c. AWS Secrets Manager 密碼 — 選擇現有密碼或建立新 Secrets Manager 密碼來儲存您的 Zendesk 驗證憑證。如果您選擇建立新密碼，則會開啟一個 AWS Secrets Manager 密碼視窗。
 - i. 在「建立 AWS Secrets Manager 密碼視窗」中輸入下列資訊：
 - A. 秘密名稱 — 您秘密的名稱。字首 'AmazonKendra-Zendesk' 會自動新增至您的密碼名稱。
 - B. 針對用戶端 ID、用戶端密碼、使用者名稱、密碼 — 輸入在 Zendesk 中設定的驗證認證值。
 - ii. 保存並添加您的秘密。
- d. V@@@ irtual Private Cloud (VPC) (VPC) — 您可以選擇使用 VPC。如果是這樣，您必須新增子網路和 VPC 安全性群組。
- e. 識別爬行者程式 — 指定是否要開啟身分識別爬行 Amazon Kendra 者程式。識別爬行者程式會使用文件的存取控制清單 (ACL) 資訊，根據使用者或使用者對文件的群組存取權來篩選搜尋結果。如果您有文件的 ACL 並選擇使用 ACL，您也可以選擇開啟的身分識別爬行者程式，以設定搜尋結果的使用者環境定義篩選。Amazon Kendra 否則，如果關閉身分搜索器，則可以公開搜索所有文檔。如果您想要對文件使用存取控制，且身分識別編目程式已關閉，您也可以使用 [PutPrincipalMapping](#) API 來上傳使用者和群組存取資訊以進行使用者內容篩選。
- f. IAM role — 選擇現有 IAM 角色或建立新 IAM 角色以存取存放庫認證和索引內容。

 Note

IAM 用於索引的角色不能用於資料來源。如果您不確定索引或常見問題集是否使用現有角色，請選擇 [建立新角色] 以避免發生錯誤。

- g. 選擇下一步。
7. 在 [設定同步設定] 頁面上，輸入下列資訊：
 - a. 選取內容 — 選取您要從工單編目的內容類型、說明中心文章、社群主題等。
 - b. 組織名稱 — 輸入 Zendesk 組織名稱以篩選內容。
 - c. 同步開始日期：輸入您要開始檢索內容的日期。
 - d. 正則表達式模式-添加正則表達式模式以包含或排除某些文件。您最多可以添加 100 個圖案。

- e. 同步模式 — 選擇資料來源內容變更時要如何更新索引。當您第一次將資料來源同 Amazon Kendra 步處理時，依預設會檢索所有內容並建立索引。如果初始同步失敗，您必須執行資料的完整同步處理，即使您沒有選擇完整同步作為同步模式選項。
 - 完全同步：新鮮索引所有內容，並在每次資料來源與索引同步時取代現有內容。
 - 新增、修改的同步：每次資料來源與索引同步時，僅對新內容和已修改的內容建立索引。Amazon Kendra 可以使用資料來源的機制來追蹤內容變更，並為上次同步後變更的內容建立索引。
 - 新增、修改、刪除的同步：每次資料來源與索引同步時，僅對新內容、已修改和刪除的內容建立索引。Amazon Kendra 可以使用資料來源的機制來追蹤內容變更，並為上次同步後變更的內容建立索引。
 - f. 頻率的同步執行排程 — 選擇同步資料來源內容和更新索引的頻率。
 - g. 選擇下一步。
8. 在 [設定欄位對映] 頁面上，輸入下列資訊：
- a. 預設資料來源欄位 — 從 Amazon Kendra 產生的預設資料來源欄位中選取您要對映至索引的資料來源欄位。
 - b. 新增欄位 — 新增自訂資料來源欄位，以建立要對映的索引欄位名稱和欄位資料類型。
 - c. 選擇下一步。
9. 在 [檢閱並建立] 頁面上，檢查您輸入的資訊是否正確，然後選取 [新增資料來源]。您也可以從此頁面選擇編輯您的資訊。成功新增資料來源後，您的資料來源將顯示在 [資料來源] 頁面上。

API

若要連接 Amazon Kendra 至天台

您必須使用 [TemplateConfiguration](#) API 指定 [資料來源結構描述](#) 的 JSON。您必須提供以下信息：

- 資料來源 — 指定使用 [TemplateConfiguration](#) JSON 結構定義 ZENDESK 時的資料來源類型。同時將資料來源指定為呼叫 [CreateDataSource](#) API TEMPLATE 時的方式。
- 主機 URL — 提供您的 Zendesk 主機 URL 作為連線組態或存放庫端點詳細資訊的一部分。例如：<https://yoursubdomain.zendesk.com>。
- 變更記錄 — 是否 Amazon Kendra 應使用 Zendesk 資料來源變更記錄機制來決定是否必須在索引中更新文件。

Note

如果您不想 Amazon Kendra 掃描所有文檔，請使用更改日誌。如果您的變更記錄很大，掃描 Zendesk 資料來源中的文件所花費的時間可能會比處理變更記錄更 Amazon Kendra 少。如果您是第一次將 Zendesk 資料來源與索引同步，則會掃描所有文件。

- 秘密 Amazon 資源名稱 (ARN) — 提供包含 Zendesk 帳戶身份驗證登入資料的 Secrets Manager 密碼的 Amazon 資源名稱 (ARN)。密碼會以下列金鑰儲存在 JSON 結構中：

```
{
  "hostUrl": "https://yoursubdomain.zendesk.com",
  "clientId": "client ID",
  "clientSecret": "Zendesk client secret",
  "userName": "Zendesk user name",
  "password": "Zendesk password"
}
```

- IAM 角色 — 指定 RoleArn 何時呼叫 CreateDataSource 以提供具有存取 Secrets Manager 密碼之權限的 IAM 角色，以及呼叫 Zendesk 連接器和所需公用 API 的時間。Amazon Kendra 如需詳細資訊，請參閱 [Zendesk 資料來源的 IAM 角色](#)。

您還可以添加以下可選功能：

- Virtual Private Cloud (VPC) — 指定您撥打電話的 VpcConfiguration 時間。CreateDataSource 如需詳細資訊，請參閱 [配置 Amazon Kendra 為使用 Amazon VPC](#)。
- 文件/內容類型 — 指定是否要編目：
 - Support 票，票評論和/或票評論附件
 - 說明中心文章、文章附件和文章註解
 - 引導社群主題、貼文或張貼評論
- 包含和排除篩選器：指定要包含還是排除特定 Slack 內容。如果您使用機器人令牌作為 Slack 身份驗證憑據的一部分，則必須將機器人令牌添加到要索引的通道中。您無法使用機器人權杖建立直接訊息和群組訊息的索引。

Note

大多數資料來源使用規則運算式模式，這些模式是稱為篩選器的包含或排除模式。如果您指定包含篩選器，則只有符合包含項目篩選器的內容會編製索引。不符合包含篩選器的任

何文件都不會建立索引。如果您指定包含和排除篩選器，符合排除篩選器的文件將不會建立索引，即使它們符合包含篩選器也是如此。

- 使用者前後關聯篩選與存取控制 — Amazon Kendra 探索文件的存取控制清單 (ACL) (如果您有文件的 ACL)。ACL 資訊可用來根據使用者或使用者對文件的群組存取權來篩選搜尋結果。如需詳細資訊，請參閱[使用者內容篩選](#)。
- 欄位對映 — 選擇將 Zendesk 資料來源欄位對映至 Amazon Kendra 索引欄位。如需詳細資訊，請參閱[映射資料來源欄位](#)。

Note

您的文件需要文件內文欄位或文件內文對等項目，才能搜尋您的文件。Amazon Kendra 您必須將資料來源中的文件內文欄位名稱對應至索引欄位名稱 `_document_body`。所有其他欄位是選用的。

如需要設定的其他重要 JSON 金鑰清單，請參閱 [Zendesk 範本結構描述](#)。

進一步了解

若要深入瞭解如何 Amazon Kendra 與 Zendesk 資料來源整合，請參閱：

- [透過 Amazon Kendra 智慧型搜尋功能探索 Zendesk 的深入](#)

對映資料來源欄位

Amazon Kendra 資料來源連接器可以將資料來源中的文件或內容欄位對應至 Amazon Kendra 索引中的欄位。依預設，每個連接器都設計為編目特定的資料來源欄位。無法變更或自訂預設資料來源欄位及其屬性。在 Amazon Kendra 控制台上，無法編輯的默認字段和默認字段屬性將顯示為灰色。

Amazon Kendra 連接器也可讓您將資料來源中的自訂文件或內容欄位對應至索引中的自訂欄位。例如，如果您的資料來源中有一個名為「dept」的欄位，其中包含文件的部門資訊，則可以將其對應到名為「Deport」的索引欄位。這樣，您可以在查詢文檔時使用該字段。

您還可以映射 Amazon Kendra 保留或常用字段，例如 `_created_at`。如果您的資料來源有一個名為「creation_date」的欄位，您可以將其對應到名為的對等 Amazon Kendra 保留欄位。`_created_at` 如需有關 Amazon Kendra 保留欄位的詳細資訊，請參閱[文件屬性或欄位](#)。

您可以對映大多數資料來源的欄位。您可以為下列資料來源建立欄位對映：

- 體驗管理器
- 露天
- Aurora 航空 (MySQL)
- Aurora (PostgreSQL)
- Amazon FSx (視窗)
- Amazon FSx (NetApp ONTAP)
- Amazon R/Aurora
- Amazon RDS (Microsoft SQL 服務器)
- Amazon RDS (MySQL)
- Amazon RDS (甲骨文)
- Amazon RDS
- Amazon Kendra 網絡爬蟲
- Amazon WorkDocs
- 立方體
- Confluence
- Dropbox
- Drupal
- GitHub
- 谷歌工作區硬盤
- Gmail
- IBM DB2
- Jira
- Microsoft Exchange
- Microsoft OneDrive
- Microsoft SharePoint
- Microsoft Teams
- Microsoft SQL Server
- Microsoft 亞默
- MySQL

- Oracle Database
- PostgreSQL
- 諷刺語
- Salesforce
- ServiceNow
- Slack
- Zendesk

如果您將文件存放在 S3 儲存貯體或 S3 資料來源中，請使用 JSON 中繼資料檔案指定欄位。如需詳細資訊，請參閱 [S3 資料來源連接器](#)。

將資料來源欄位對應至索引欄位需要三個步驟：

1. 建立索引。如需詳細資訊，請參閱[建立索引](#)。
2. 更新索引以新增欄位。
3. 建立資料來源並包含欄位對應，以將保留欄位和任何自訂欄位對映至 Amazon Kendra 索引欄位。

若要更新索引以新增自訂欄位，請使用主控台編輯資料來源欄位對應並新增自訂欄位或使用 [UpdateIndex](#) API。您總共可以在索引中新增 500 個自訂欄位。

對於資料庫資料來源，如果資料庫欄的名稱與保留欄位的名稱相符，則會自動對應欄位和欄。

使用 [UpdateIndex](#) API，您可以使用 `DocumentMetadataConfigurationUpdates`。

下面的 JSON 示例使 `DocumentMetadataConfigurationUpdates` 用一個名為「部門」的字段添加到索引。

```
"DocumentMetadataConfigurationUpdates": [  
  {  
    "Name": "Department",  
    "Type": "STRING_VALUE"  
  }  
]
```

建立欄位時，您可以選擇設定如何使用欄位進行搜尋。您可以選擇下列項目：

- 可顯示 — 決定是否在查詢回應中傳回欄位。預設值為 `true`。
- 可刻面 (Facetable)-指示欄位可用於建立多面。預設值為 `false`。

- 可搜尋 — 決定是否在搜尋中使用欄位。字串欄位的預設值是 `true`，以及數字和日期欄位的預設值是 `false`。
- 可排序 — 表示欄位可用來排序查詢的回應。只能為日期、數字和字串欄位設定。無法為字串清單欄位設定。

下面的 JSON 示例使用 `DocumentMetadataConfigurationUpdates` 一個名為「部門」的字段添加到索引，並將其標記為可面的。

```
"DocumentMetadataConfigurationUpdates": [  
  {  
    "Name": "Department",  
    "Type": "STRING_VALUE",  
    "Search": {  
      "Facetable": true  
    }  
  }  
]
```

使用 Amazon Kendra 保留或一般文件欄位

使用 [UpdateIndex API](#)，您可以使用 `DocumentMetadataConfigurationUpdates` 並指定保留索引欄位名稱來建立 Amazon Kendra 保留或通用欄位，以對應至對等的文件屬性/欄位名稱。您也可以建立自訂欄位。如果您使用資料來源連接器，大多數都會包含將資料來源文件欄位對映至 Amazon Kendra 索引欄位的欄位對映。如果您使用主控台，您可以透過選取資料來源、選取編輯動作，然後繼續進行欄位對應區段旁邊以配置資料來源來更新欄位。

您可以設定 `Search` 物件以將欄位設定為可顯示、可變更、可搜尋和可排序。您可以將 `Relevance` 物件設定為設定欄位的排名順序、提升持續時間或時段，以套用至提升、新鮮度、重要性值，以及對應至特定欄位值的重要性值。如果您使用控制台，則可以透過選取導覽功能表中的 `Facet` 選項來設定欄位的搜尋設定。若要設定相關性調整，請在導覽功能表中選取搜尋索引的選項、輸入查詢，然後使用側邊面板選項來調整搜尋相關性。建立欄位後，就無法變更欄位類型。

Amazon Kendra 您可以使用下列保留或一般文件欄位：

- `_authors` 負責文件內容的一或多個作者清單。
- `_category` 將文件放置在特定群組中的類別。
- `_created_at` 以 ISO 8601 格式建立文件的日期和時間。例如，`2012-03-25T12:30:10+01:00` 是以 ISO 8601 日期時間格式表示的歐洲中部時間 2012 年 3 月 25 日中午 12:30 (加上 10 秒)。

- `_data_source_id` 包含文件之資料來源的識別碼。
- `_document_body` 文件的內容。
- `_document_id` 文件的唯一識別元。
- `_document_title` 文件的標題。
- `_excerpt_page_number` 顯示文件摘錄的 PDF 檔案中的頁碼。如果您的索引是在 2020 年 9 月 8 日之前建立的，您必須重新建立文件索引，才能使用此屬性。
- `_faq_id` 如果這是問答類型文件 (FAQ)，這是常見問題集的唯一識別碼。
- `_file_type` 文件的檔案類型，例如 pdf 或 doc。
- `_last_updated_at` 上次更新文件的日期和時間 (使用 ISO 8601 格式)。例如，2012-03-25T12:30:10+01:00 是以 ISO 8601 日期時間格式表示的歐洲中部時間 2012 年 3 月 25 日中午 12:30 (加上 10 秒)。
- `_source_uri` 可使用文件的 URI。例如，在公司網站上的文件 URI。
- `_version` 文件特定版本的識別元。
- `_view_count` 檢視文件的次數。
- `_language_code` (字串)-套用至文件之語言的程式碼。如果您未指定語言，則預設為英文。如需支援語言 (包括其代碼) 的詳細資訊，請參閱以 [英文以外的語言新增文件](#)。

對於自訂欄位，您可以使 `DocumentMetadataConfigurationUpdates` 用 `UpdateIndex` API 建立這些欄位，就像建立保留欄位或公用欄位一樣。您必須為自訂欄位設定適當的資料類型。如果您使用主控台，您可以透過選取資料來源、選取編輯動作，然後繼續進行欄位對應區段旁邊以配置資料來源來更新欄位。某些資料來源不支援新增欄位或自訂欄位。建立欄位後，就無法變更欄位類型。

以下是您可以為自訂欄位設定的類型：

- 日期
- Number
- 字串
- 字串清單

如果您使用 [BatchPutDocument](#) API 將文件新增至索引，會 `Attributes` 列出文件的欄位/屬性，並使用物件建立欄位。 `DocumentAttribute`

對於從資 Amazon S3 料來源編製索引的文件，您可以使用包含欄位資訊的 [JSON 中繼資料檔案](#) 建立欄位。

如果您使用支援的資料庫做為資料來源，您可以使用欄位[對應選項來設定欄位](#)。

以英文以外的語言新增文件

您可以編製多種語言的文件索引。如果您未指定語言，則依預設會以英文 Amazon Kendra 編製文件索引。您可以將文件的語言代碼作為欄位包含在文件中繼資料中。如需有關文件欄位的詳細資訊，請參閱 [_language_code](#) 欄位對應和 [自訂屬性](#)。

您可以在呼叫時指定資料來源中所有文件的語言代碼 [CreateDataSource](#)。如果文件沒有在中繼資料欄位中指定的語言代碼，則會使用在資料來源層級為所有文件指定的語言代碼為文件編製索引。在主控台中，您只能在資料來源層級以支援的語言編製文件索引。轉到數據源，然後選擇指定數據源詳細信息頁面，然後從下拉菜單中選擇語言語言。

您也可以使用支援的語言搜尋或查詢文件。如需詳細資訊，請參閱以 [語言搜尋](#)。

支持以下語言及其代碼（如果您未指定語言，則默認支持英語）。en 此表格包含 Amazon Kendra 支援完整語意搜尋的語言，以及僅支援簡單關鍵字比對的語言。支援完整語意搜尋的語言會以星號標示，並在下表中以粗體文字顯示。完整的語義搜索也支持英語（默認語言）。

語言名稱	語言代碼
Arabic	ar
亞美尼亞文	hy
巴斯克文	eu
孟加拉文	bn
保加利亞文	bg
加泰隆尼亞文	ca
中文 — 簡體和繁體 *	zh
捷克文	cs
丹麥文	da
荷蘭文	nl

語言名稱	語言代碼
芬蘭文	fi
法文 — 包括法文 (加拿大) *	fr
加利西亞文	gl
德文 *	de
Greek	el
北印度文	hi
匈牙利文	hu
印尼文	id
愛爾蘭人	ga
義大利文	it
日語 *	ja
韓國 *	ko
拉脫維亞文	lv
立陶宛文	lt
挪威文	no
波斯文	fa
葡萄牙文	pt
葡萄牙文 (巴西) *	pt-BR
羅馬尼亞文	ro
俄文	ru

語言名稱	語言代碼
索拉尼	ckb
西班牙語-包括西班牙語 (墨西哥) *	es
瑞典文	sv
土耳其文	tr

* 語言支持語義搜索。

對於支援語意搜尋的語言，支援下列功能。

- 文件相關性超越簡單的關鍵字比對
- 除了簡單的關鍵字比對之外的
- 根據閱讀理解力從文檔中提取答案。Amazon Kendra
- 搜尋結果的信賴值區 (非常高、高、中和低)。

對於不支援語意搜尋的語言，文件相關性和常見問題集支援簡單的關鍵字比對。

[僅支援英文 \(預設語言\) 的同義字 \(包括自訂同義字\)、漸進式學習與意見反應，以及查詢建議。](#)

配置 Amazon Kendra 為使用 Amazon VPC

Amazon Kendra 可以連線到您使用建立的虛擬私有雲 (VPC)，Amazon Virtual Private Cloud 以索引儲存在私有雲中執行的資料來源中的內容。建立資料來源連接器時，您可以為包含資料來源的子網路提供安全群組和子網路識別碼。使用此資訊，可 Amazon Kendra 建立 elastic network interface，用於與 VPC 中的資料來源進行安全通訊。

若要使用設定 Amazon Kendra 資料來源連接器 Amazon VPC，您可以使用 AWS Management Console 或 [CreateDataSource](#) API 作業。如果您使用主控台，請在連接器設定程序期間連線 VPC。

Note

設定 Amazon Kendra 資料來源連接器時，此 Amazon VPC 功能是選用的。如果您的資料來源可從公用網際網路存取，則無需啟用此 Amazon VPC 功能。並非所有 Amazon Kendra 資料來源連接器都支援 Amazon VPC。

如果您的資料來源未在上執行 Amazon VPC 且無法從公用網際網路存取，則首先使用虛擬私人網路 (VPN) 將資料來源連線到 VPC。然後，您可以使用 Amazon VPC 和的組合將資料來源連接到 Amazon Kendra AWS Virtual Private Network。如需有關設定 VPN 的資訊，請參閱[AWS VPN 文件](#)。

主題

- [設定 Amazon Kendra 連接器的 Amazon VPC 支援](#)
- [設定要連線到的 Amazon Kendra 資料來源 Amazon VPC](#)
- [連接到 VPC 中的數據庫](#)
- [VPC 連線問題疑難排解](#)

設定 Amazon Kendra 連接器的 Amazon VPC 支援

若要設 Amazon VPC 定與 Amazon Kendra 連接器搭配使用，請採取下列步驟。

步驟

- [步驟 1. 建立 Amazon VPC 子網路 Amazon Kendra](#)
- [步驟 2. 建立的 Amazon VPC 安全性群組 Amazon Kendra](#)
- [步驟 3. 設定您的外部資料來源和 Amazon VPC](#)

步驟 1. 建立 Amazon VPC 子網路 Amazon Kendra

建立或選擇 Amazon Kendra 可用來存取資料來源的現有 Amazon VPC 子網路。準備好的子網路必須位於下列 AWS 區域 其中一個可用區域中：

- 美國西部 (奧勒岡)/美國西部-2 美國西部 -2-阿茲 1, 使用 2-az3
- 美國東部 (維吉尼亞北部)/美國東部 -1 使用 1-az1 , 使用 1-az2 , 使用 1-az4
- 美國東部 (俄亥俄州)/美國東部 -2-使用 2-az1 , 使用 2-az2 , 使用 2-az3
- 亞太區域 (東京)/亞太區東北部 -1-阿西 1, 窒息 1-az2

- 亞太區域 (孟買)/亞太區 (孟買)/南方 1, APS1-AZ1, APS1-az3
- 亞太區 (新加坡) /AP-東南部-1-阿西 1, 阿西 1, 阿西 1 號
- 亞太區域 (雪梨) /AP-東南部-2-apse2-az1, apse2-az2, apse2-az3
- 加拿大 (中部) /CA-中央 -1-卡卡 1-AZ1, 可卡 1-az2, 可卡 1-az4
- 歐洲 (愛爾蘭)/歐洲-西部 -1 歐盟 1-az1, 歐盟 1-az3
- 歐洲 (倫敦) /歐洲-西部 -2-英制 2-阿西 1, 我們 2-az3

您的資料來源必須可從您提供給 Amazon Kendra 連接器的子網路存取。

如需有關如何設定 Amazon VPC 子網路的詳細資訊，請參閱 Amazon VPC 使用者指南 Amazon VPC 中的[適用於您的子網路](#)。

如果 Amazon Kendra 必須在兩個或多個子網路之間路由連線，您可以準備多個子網路。例如，包含資料來源的子網路不在 IP 位址中。在這種情況下，您可以提供 Amazon Kendra 具有足夠 IP 位址並連線至第一個子網路的其他子網路的子網路。如果您列出多個子網路，子網路必須能夠彼此通訊。

步驟 2. 建立的 Amazon VPC 安全性群組 Amazon Kendra

若要將 Amazon Kendra 資料來源連接器連線到 Amazon VPC，您必須從 VPC 準備一個或多個要 Amazon Kendra 指派的安全性群組。安全性群組將與建立的 elastic network interface 相關聯 Amazon Kendra。此網路介面可控制存取 Amazon VPC 子網路 Amazon Kendra 時的入站和輸出流量。

請確定安全性群組的輸出規則允許來自 Amazon Kendra 資料來源連接器的流量存取您要同步處理的子網路和資料來源。例如，您可以使用 MySQL 連接器從 MySQL 資料庫同步。如果您使用預設連接埠，安全性群組必須允許 Amazon Kendra 取執行資料庫之主機上的連接埠 3306。

我們建議您使用下列值來設定預設安全性群組，Amazon Kendra 以供使用：

- 輸入規則 — 如果您選擇將此項保留空白，則會封鎖所有入站流量。
- 輸出規則 — 新增一個規則以允許所有輸出流量，Amazon Kendra 以便啟動要求以從資料來源同步處理。
 - IP 版本 — 網絡版本
 - 類型 — 所有流量
 - 通訊協定 — 所有流量
 - 連接埠範圍 — 全部
 - 目的地 — 0.0.0/0

如需如何設定 Amazon VPC 安全群組的詳細資訊，請參閱 Amazon VPC 使用者指南中的[安全群組規則](#)。

步驟 3. 設定您的外部資料來源和 Amazon VPC

請確定您的外部資料來源具有正確的權限組態和網路設定，Amazon Kendra 以便存取外部資料來源。您可以在每個連接器頁面的 [必要條件] 區段中找到有關如何設定資料來源的詳細指示。

此外，請檢查您的 Amazon VPC 設定，並確定可從您要指派的子網路存取外部資料來源 Amazon Kendra。為此，我們建議您在具有相同安全群組的相同子網路中建立 Amazon EC2 執行個體，並測試從此 Amazon EC2 執行個體對資料來源的存取權。如需詳細資訊，請參閱[疑難排解 Amazon VPC 連線](#)。

設定要連線到的 Amazon Kendra 資料來源 Amazon VPC

在中加入新資料來源時 Amazon Kendra，如果選取的資料來源連接器支援此 Amazon VPC 圖徵，則可以使用圖徵。

您可以使用 AWS Management Console 或 Amazon Kendra API 設定 Amazon VPC 已啟用的新 Amazon Kendra 資料來源。具體來說，請使用 [CreateDataSource](#) API 作業，然後使用 `VpcConfiguration` 參數提供下列資訊：

- SubnetIds-子網的標識符列 Amazon VPC 表
- SecurityGroupIds— Amazon VPC 安全群組的識別碼清單

如果您使用主控台，請在連接器組態期間提供必要的 Amazon VPC 資訊。若要使用主控台為連接器啟用 Amazon VPC 功能，請先選擇 Amazon VPC。然後，您可以提供任何 Amazon VPC 子網路的識別碼，以及任何 Amazon VPC 安全群組的識別碼。您可以選擇在[設定 Amazon VPC 中建立的 Amazon VPC 子網路和 Amazon VPC 安全群組](#)，或使用任何現有的子網路和 Amazon VPC 安全群組。

主題

- [檢視 Amazon VPC 識別碼](#)
- [檢查您的資料來源 IAM 角色](#)

檢視 Amazon VPC 識別碼

子網路和安全群組的識別碼是在 Amazon VPC 主控台中設定的。若要檢視識別碼，請使用下列程序。

檢視子網路識別碼

1. 登入 AWS Management Console 並開啟 Amazon VPC 主控台，網址為 <https://console.aws.amazon.com/vpc/>。
2. 在瀏覽窗格中，選擇「子網路」。
3. 從「子網路」清單中，選擇包含資料庫伺服器的子網路。
4. 從「詳細資料」標籤中，記下「子網路 ID」欄位中的識別碼。

若要檢視安全群組識別碼

1. 登入 AWS Management Console 並開啟 Amazon VPC 主控台，網址為 <https://console.aws.amazon.com/vpc/>。
2. 在瀏覽窗格中，選擇 [安全性群組]。
3. 從安全性群組清單中，選擇您想要識別碼的群組。
4. 從「詳細資料」索引標籤中，記下「安全性群組 ID」欄位中的識別碼。

檢查您的資料來源 IAM 角色

請確定您的資料來源連接器 (AWS Identity and Access Management (IAM) 角色) 包含存取 Amazon VPC。

如果您使用主控台為您的角色建立新 IAM 角色，則會代表您 Amazon Kendra 自動將正確的權限新增至您的 IAM 角色。如果您使用 API 或使用現有 IAM 角色，請檢查您的角色是否包含存取權限 Amazon VPC。若要確認您擁有正確的權限，請參閱 [VPC 的 IAM 角色](#)。

您可以修改現有的資料來源以使用不同的 Amazon VPC 子網路。但是，請檢查資料來源的 IAM 角色，並在必要時對其進行修改，以反映 Amazon Kendra 資料來源連接器正常運作的變更。

連接到 VPC 中的數據庫

下列範例顯示如何連線在虛擬私有雲 (VPC) 中執行的 MySQL 資料庫。此範例假設您從預設 VPC 開始，且需要建立 MySQL 資料庫。如果您已經擁有 VPC，請確定其設定如圖所示。如果你有一個 MySQL 數據庫，你可以使用它，而不是創建一個新的。

步驟

- [步驟 1：設定虛擬私人 VPC](#)
- [步驟 2：建立和設定安全群組](#)
- [步驟 3：建立資料庫](#)

• [步驟 4：建立資料來源連接器](#)

步驟 1：設定虛擬私人 VPC

設定您的 VPC，讓您擁有私有子網路和安全群組，以存 Amazon Kendra 取子網路中執行的 MySQL 資料庫。VPC 組態中提供的子網路必須位於美國西部 (奧勒岡) 區域、美國東部 (維吉尼亞北部) 區域或歐洲 (愛爾蘭) 區域。

若要使用設定 VPC Amazon VPC

1. 登入 AWS Management Console 並開啟 Amazon VPC 主控台，網址為 <https://console.aws.amazon.com/vpc/>。
2. 在導覽窗格中，選擇「路由表」，然後選擇「建立路由表」。
3. 在「名稱」欄位中輸入 **Private subnet route table**。從 VPC 下拉式清單中，選取您的 VPC，然後選擇 [建立路由表]。選擇「關閉」以返回路由表清單。
4. 在瀏覽窗格中，選擇 NAT 閘道，然後選擇「建立 NAT 閘道」。
5. 從子網路下拉式清單中，選擇公用子網路的子網路。記下子網路識別碼。
6. 如果您沒有彈性 IP 位址，請選擇 [建立新的 EIP]，選擇 [建立 NAT 閘道]，然後選擇 [關閉]。
7. 在導覽窗格中，選擇「路由表」。
8. 從路由表清單中，選擇您在步驟 3 中建立的私人子網路路由表格。從「動作」中選擇「編輯路由」。
9. 選擇 Add route (新增路由)。對於目的地，請輸入 **0.0.0.0/0** 以允許所有傳出流量連接至網際網路。針對「目標」，選擇「NAT 閘道」，然後選擇您在步驟 4 中建立的閘道。選擇 [儲存變更]，然後選擇 [關閉]。
10. 從動作中，選擇編輯子網路關聯。
11. 選擇您要設為私人的子網路。請勿使用您先前記下的 NAT 閘道來選擇子網路。完成後，選擇「保存關聯」。

步驟 2：建立和設定安全群組

接下來，設定資料庫的安全性群組。

建立和設定安全群組

1. 登入 AWS Management Console 並開啟 Amazon VPC 主控台，網址為 <https://console.aws.amazon.com/vpc/>。

2. 從虛擬私人 VPC 的說明中，記下 IPv4 CIDR。
3. 從功能窗格中，選擇 [安全性群組]，然後選擇 [建立安全性群組]。
4. 針對 Security group name (安全群組名稱)，輸入 **DataSourceInboundSecurityGroup**。提供說明，然後從列表中選擇您的 VPC。選擇建立安全性群組，然後選擇 [關閉]。
5. 選擇 Inbound Rules (傳入規則) 索引標籤。
6. 選擇 [編輯輸入規則]，然後選擇 [新增規則]
7. 對於資料庫，請輸入連接埠範圍的連接埠號碼。例如，MySQL 因為它是和 **3306**，對於 HTTPS，它是 **443**。針對來源，輸入 VPC 的無類別網域間路由 (CIDR)。選擇儲存規則，然後選擇「關閉」。

安全性群組允許 VPC 中的任何人連線到資料庫，並允許對網際網路的輸出連線。

步驟 3：建立資料庫

創建一個數據庫來保存您的文檔，或者您可以使用現有的數據庫。

如需如何建立資MySQL料庫的指示，請參閱[MySQL](#)。

步驟 4：建立資料來源連接器

設定 VPC 並建立資料庫之後，您可以為資料庫建立資料來源連接器。如需支援之資料庫連接器的資訊，請參閱 Amazon Kendra [支援的連接器](#)。

對於您的資料庫，請確定您已設定 VPC、您在 VPC 中建立的私有子網路，以及您在 VPC 中建立的安全性群組。

VPC 連線問題疑難排解

如果您在使用虛擬私有雲端 (VPC) 連線時遇到任何問題，請檢查您的 IAM 權限、安全性群組設定和子網路的路由表是否已正確設定。

資料來源連接器同步失敗的一個潛在原因是資料來源可能無法從您指派的子網路存取資料來 Amazon Kendra 源。若要疑難排解此問題，建議您使用相同的 Amazon VPC 設定建立 Amazon EC2 執行個體。然後，嘗試使用 REST API 呼叫或其他方法（根據資料來源的特定類型）從此 Amazon EC2 執行個體存取資料來源。

如果您從建立的 Amazon EC2 執行個體成功存取資料來源，則表示您可以從此子網路存取您的資料來源。因此，您的同步問題與您的資料來源無法存取無關 Amazon VPC。

如果您無法從 VPC 組態存取 Amazon EC2 執行個體，並使用您建立的 Amazon EC2 執行個體進行驗證，則需要進一步疑難排解。例如，如果您有一個連 Amazon S3 接器，其同步失敗並出現連線問題的錯誤，您可以使用指派給連 Amazon S3 接器的相同 Amazon VPC 組態來設定 Amazon EC2 執行個體。然後，使用此 Amazon EC2 執行個體來測試您 Amazon VPC 的設定是否正確。

以下是設定 Amazon EC2 執行個體以疑難排解與 Amazon S3 資料來源之間的 Amazon VPC 連線問題的範例。

主題

- [步驟 1：啟動 Amazon EC2 執行個體](#)
- [步驟 2：Connect 至 Amazon EC2 執行個體](#)
- [步驟 3：測試 Amazon S3 存取權](#)

步驟 1：啟動 Amazon EC2 執行個體

1. 登入 AWS Management Console 並開啟 Amazon EC2 主控台，網址為 <https://console.aws.amazon.com/ec2/>。
2. 選取啟動執行個體。
3. 選擇 [網路設定]，然後選擇 [編輯]，然後執行下列動作：
 - a. 選擇您指派給的相同 VPC 和子網路。Amazon Kendra
 - b. 對於「防火牆 (安全群組)」，選擇「選取現有安全群組」。然後，選取您指派給的安全性群組 Amazon Kendra。

Note

安全性群組應允許輸出流量至 Amazon S3。

- c. 將自動指派公用 IP 設定為 [停用]。
- d. 在進階詳細資料中，執行下列動作：
 - 對於 IAM 執行個體設定檔，請選取 [建立新的 IAM 設定檔]，以建立 IAM 執行個體設定檔並將其附加到執行。請確定設定檔具有存取權限 Amazon S3。如需詳細資訊，請參閱[如何授與 Amazon EC2 執行個體存取 Amazon S3 值區的權限？](#) 在 AWS re:Post。
 - 保留所有其他設定為預設值。
- e. 檢閱並啟動 Amazon EC2 執行個體。

步驟 2：Connect 至 Amazon EC2 執行個體

執行 Amazon EC2 個體執行後，前往執行個體詳細資料頁面並連線至您的執行個體。若要這麼做，請使用 [Linux 執行個體使用 Amazon EC2 者指南中的 EC2 執行個體 Connect 端點使用 EC2 執行個體 Connect 端點使用公有 IPv4 地址連線到執行個體中的步驟](#)。

步驟 3：測試 Amazon S3 存取權

連線至執行個 Amazon EC2 體終端機之後，請執行 AWS CLI 指令來測試從此私有子網路到 Amazon S3 值區的連線。

若要測試 Amazon S3 存取權，請在中鍵入下列 AWS CLI 命令 `AWS CLI : aws s3 ls`

AWS CLI 命令執行後，請檢閱下列項目：

- 如果您已正確設定必要的 IAM 權限，且 Amazon S3 設定正確無誤，您應該會看到 Amazon S3 值區的清單。
- 如果您看到權限錯誤，例如 `Access Denied`，則您的 VPC 配置可能是正確的，但您的 IAM 權限或 Amazon S3 存儲桶策略有問題。

如果命令逾時，您的連線可能已逾時，因為您的 VPC 設定不正確，且 Amazon EC2 執行個體無法從子網路存取 Amazon S3。重新設定您的 VPC，然後再試一次。

刪除索引、資料來源或批次上傳的文件

本節說明如何刪除索引、索引中文件的資料來源儲存庫或您批次上傳的索引中的文件。

主題

- [刪除索引](#)
- [刪除資料來源](#)
- [刪除批次上傳的文件](#)

刪除索引

您可以從不再使用索引Amazon Kendra時刪除索引。例如，在下列情況下刪除索引：

- 您不再使用索引，並希望減少AWS帳戶的費用。無論您是否對Amazon Kendra索引進行查詢，索引都會在執行時產生費用。
- 您想要重新設定其他版本的Amazon Kendra索引。刪除現有的索引，然後使用不同的版本創建一個新索引。
- 您已達到帳戶中的索引數量上限，並且不想超過配額。刪除現有索引並新增索引。如需可建立之索引數目上限的相關資訊，請參閱[配額](#)。

若要刪除索引，請使用主控台、指AWS CloudFormation令碼或 DeleteIndex API。AWS Command Line Interface刪除索引會移除索引及所有關聯的資料來源和文件資料。刪除索引並不會從儲存空間中移除原始文件。

刪除索引是一項非同步作業。當您開始刪除索引時，索引狀態會變更為DELETING。它會保持狀DELETING態，直到移除與索引相關的所有資訊為止。一旦刪除索引，它就不會再出現在呼叫 [ListIndices](#)API 的結果中。如果您使用已刪除索引的標識符調用 [DescribeIndex](#)API，則會收到並發生ResourceNotFound異常。

若要刪除索引 (主控台)

1. 請登入AWS Management Console並開啟Amazon Kendra主控台，[網址為 https://console.aws.amazon.com/kendra/](https://console.aws.amazon.com/kendra/)。
2. 在功能窗格中，選擇 [索引]，然後選擇要刪除的索引。
3. 選擇刪除以刪除選取的索引。

若要刪除索引 (CLI)

- 在 AWS CLI 中，使用以下命令。此指令已針對 Linux 和 macOS 進行格式化。如果您使用的是 Windows，請使用插入符號 (^) 取代 Unix 行接續字元 (\)。

```
aws kendra delete-index \  
  --id index-id
```

刪除資料來源

當您想要從 Amazon Kendra 索引中移除資料來源中包含的資訊時，可以刪除資料來源。例如，在下列情況下刪除資料來源：

- 資料來源設定不正確。刪除資料來源，等待資料來源完成刪除，然後重新建立資料來源。
- 您將文件從一個資料來源移轉到另一個資料來源。刪除原始資料來源，然後在新位置重新建立該資料來源。
- 您已達到索引資料來源的上限。刪除其中一個現有資料來源，然後新增一個資料來源。如需可建立之資料來源數目的詳細資訊，請參閱[配額](#)。

若要刪除資料來源，請使用主控台、AWS Command Line Interface (AWS CLI)、DeleteDataSource API 或指 AWS CloudFormation 令碼。刪除資料來源會從索引中移除有關資料來源的所有資訊。如果您只想停止同步資料來源，請將資料來源的同步化排程變更為「隨選執行」。

刪除資料來源是一項非同步作業。開始刪除資料來源時，資料來源狀態會變更為 DELETING。它會保持 DELETING 態，直到移除與資料來源相關的資訊為止。刪除資料來源後，該資料來源將不再出現在呼叫 [ListDataSources](#) API 的結果中。如果您使用已刪除資料來源的識別碼呼叫 [DescribeDataSource](#) API，則會收到 ResourceNotFound 例外狀況。

Note

刪除整個資料來源或從資料來源刪除特定文件後重新同步索引可能需要長達一個小時或更長時間，具體取決於您要刪除的文件數目。

若要刪除資料來源 (主控台)

1. 請登入AWS Management Console並開啟Amazon Kendra主控台，網址為 <https://console.aws.amazon.com/kendra/>。
2. 在瀏覽窗格中，選擇 [索引]，然後選擇包含要刪除之資料來源的索引。
3. 在導覽窗格中選擇 Data sources (資料來源)。
4. 選擇要移除的資料來源。
5. 選擇刪除以刪除資料來源。

若要刪除資料來源 (CLI)

- 在 AWS Command Line Interface 中，使用以下命令。此指令已針對 Linux 和 macOS 進行格式化。如果您使用的是 Windows，請使用插入符號 (^) 取代 Unix 行接續字元 (\)。

```
aws kendra delete-data-source \  
  --id data-source-id \  
  --index-id index-id
```

刪除資料來源時，Amazon Kendra會移除有關資料來源的所有已儲存資訊。Amazon Kendra移除索引中儲存的所有文件資料，以及與資料來源相關聯的所有執行歷史記錄和指標。刪除資料來源並不會從儲存裝置中移除原始文件。

Amazon Kendra刪除資料來源時，資料來源中的文件可能會包含在 DescribeIndex API 傳回的文件計數中。Amazon Kendra刪除資料來源時，資料來源的文件可能會出現在搜尋結果中。

Amazon Kendra當您呼叫 DeleteDataSource API 或選擇在主控台中刪除資料來源時，立即釋放資料來源的資源。如果要刪除資料來源以減少超過限制的資料來源數量，則可以立即建立新資料來源。

如果要刪除資料來源，然後為文件資料建立另一個資料來源，請等待第一個資料來源刪除，然後再同步新資料來源。

您可以刪除正在與同步處理的資料來源Amazon Kendra。同步會停止並移除資料來源。如果您在刪除資料來源時嘗試啟動同步，則會收到ConflictException例外狀況。

如果關聯的索引處於DELETING狀態，則無法刪除資料來源。刪除索引會刪除索引的所有資料來源。您可以在該索引的資料來源處於DELETING狀態時開始刪除索引。

如果您有兩個資料來源指向相同的文件，例如指向同一個Amazon S3值區的兩個資料來源，則當刪除其中一個資料來源時，索引中的文件可能會不一致。當兩個資料來源參照相同的文件時，索引中只會儲存一個文件資料副本。移除一個資料來源會移除文件的索引資料。另一個資料來源不知道文件已移除，因此在下次同步時Amazon Kendra無法正確地重新編製文件的索引。當您有兩個資料來源指向相同的文件位置時，您應該刪除這兩個資料來源，然後重新建立一個資料來源。

刪除批次上傳的文件

您可以使用 [BatchDeleteDocument](#) API 直接從索引中刪除文件。您無法直接使用主控台刪除文件。如果使用主控台，則可以從資料來源儲存庫刪除特定文件，然後與索引重新同步，或刪除整個資料來源連接器。

使用從索引中刪除文檔BatchDeleteDocument是一種異步操作。呼叫BatchDeleteDocument API 之後，您可以使用 [BatchGetDocumentStatus](#) API 監視刪除文件的進度。當文檔從索引中刪除時，Amazon Kendra返回NOT_FOUND作為狀態。

Note

使用從索引刪除文件最多BatchDeleteDocument可能需要一個小時或更長時間，具體取決於您要刪除的文件數量。

若要從索引 (CLI) 刪除批次上傳的文件

- 在 AWS Command Line Interface 中，使用以下命令。此指令已針對 Linux 和 macOS 進行格式化。如果您使用的是 Windows，請使用插入符號 (^) 取代 Unix 行接續字元 (\)。

```
aws kendra batch-delete-document \  
  --index-id index-id \  
  --document-id-list 'doc-id-1' 'doc-id-2'
```

擷取期間豐富您的文件

您可以在文件擷取程序期間變更內容和文件中繼資料欄位或屬性。使用Amazon Kendra的自訂文件增強功能，您可以在內嵌文件時建立、修改或刪除文件屬性和內容。Amazon Kendra這意味著您可以根據需要操作和導入數據。

此功能可讓您控制文件的處理和擷取方式Amazon Kendra。例如，您可以在擷取文件時，清除文件中繼資料中的個人識別資訊。Amazon Kendra

您可以使用此功能的另一種方式是叫用中AWS Lambda的 Lambda 函數，對影像執行光學字元辨識 (OCR)、在文字上進行翻譯，以及準備資料以進行搜尋或分析的其他工作。例如，您可以叫用在影像上執行 OCR 的函數。該功能可以解釋圖像中的文本，並將每個圖像視為文本文檔。一家接收郵寄客戶調查問卷並將這些調查存儲為圖像的公司可以將這些圖像作為文本文檔導入。Amazon Kendra然後，該公司可以在中搜索有價值的客戶調查信息Amazon Kendra。

您可以使用基本作業來套用做為資料的第一個剖析，然後使用 Lambda 函數在資料上套用更複雜的作業。例如，您可以使用基本操作簡單地刪除文檔元數據字段「Customer_ID」中的所有值，然後應用 Lambda 函數從文檔中的文本的圖像中提取文本。

自訂文件擴充的運作方式

自訂文件擴充的整體程序如下：

1. 您可以在建立或更新資料來源或將文件直接編入Amazon Kendra索引時，設定「自訂文件擴充」。
2. Amazon Kendra套用內嵌組態或基本邏輯來變更您的資料。如需詳細資訊，請參閱[the section called “更改元數據的基本操作”](#)。
3. 如果您選擇設定進階資料操作，Amazon Kendra可以在原始、原始文件或結構化、剖析的文件上套用此功能。如需詳細資訊，請參閱[the section called “Lambda 函數：擷取和變更中繼資料或內容”](#)。
4. 您修改過的文件會被攝入Amazon Kendra。

在此過程中的任何時候，如果您的配置無效，則Amazon Kendra會引發錯誤。

當您呼叫[CreateDataSourceUpdateDataSource](#)、或 [BatchPutDocument](#) API 時，您會提供自訂文件擴充組態。如果您撥打電話BatchPutDocument，您必須針對每個要求設定自訂文件擴充功能。如果您使用主控台，請選取索引，然後選取 [文件擴充] 以設定 [自訂文件擴充]。

如果您在主控台中使用文件擴充功能，則可以選擇僅設定基本作業，或只設定 Lambda 函數或兩者，就像使用 API 一樣。您可以在主控台步驟中選取 [下一步]，選擇不設定基本作業和僅設定 Lambda 函

數，包括套用至原始 (擷取前) 還是結構化 (擷取後) 資料。您只能透過完成主控台中的所有步驟來儲存設定。如果您未完成所有步驟，則不會儲存您的文件組態。

更改元數據的基本操作

您可以使用基本邏輯來操作文件欄位和內容。這包括移除欄位中的值、使用條件修改欄位中的值或建立欄位。對於超出您可以使用基本邏輯操作的進階操作，請叫用 Lambda 函數。如需詳細資訊，請參閱[the section called “Lambda 函數：擷取和變更中繼資料或內容”](#)。

若要套用基本邏輯，您可以使用 `DocumentAttributeTarget` 物件指定要操作的目標欄位。您提供屬性索引鍵。例如，鍵 '部門' 是一個字段或屬性，它保存與文檔相關的所有部門名稱。如果符合特定條件，您也可以指定要在目標欄位中使用的值。您可以使用物件設定條 `DocumentAttributeCondition` 件。例如，如果「Source_URI」欄位的 URI 值中包含「財務」，則在目標欄位「部門」中預先填入文件的目標值「財務」。您也可以刪除目標文件屬性的值。

若要使用主控台套用基本邏輯，請選取您的索引，然後在導覽功能表中選取 [文件擴充]。轉到配置基本操作以將基本操作應用於文檔字段和內容。

以下是使用基本邏輯刪除名為「Customer_ID」文檔字段中的所有客戶識別號碼的示例。

範例 1：移除與文件相關聯的客戶識別碼

應用基本操作之前的數據。

文件識別碼	本文 _ 文字	客戶識別碼
1	洛雷姆·伊普瑟姆.	CID1234
2	洛雷姆·伊普瑟姆.	CID1235
3	洛雷姆·伊普瑟姆.	CID1236

應用基本操作後的數據。

文件識別碼	本文 _ 文字	客戶識別碼
1	洛雷姆·伊普瑟姆.	
2	洛雷姆·伊普瑟姆.	

文件識別碼	本文_文字	客戶識別碼
3	洛雷姆·伊普瑟姆.	

以下是使用基本邏輯創建一個名為「部門」的字段的示例，並根據「SOURCE_URI」字段中的信息將部門名稱預填此字段。這使用的條件是，如果「Source_URI」字段在其 URI 值中包含「財務」，則將目標字段「部門」預填為文檔的目標值「財務」。

範例 2：建立「部門」欄位，並使用條件預先填入與文件相關聯的部門名稱。

應用基本操作之前的數據。

文件識別碼	本文_文字	來源
1	洛雷姆·伊普瑟姆.	金融/1
2	洛雷姆·伊普瑟姆.	金融/2
3	洛雷姆·伊普瑟姆.	金融/3

應用基本操作後的數據。

文件識別碼	本文_文字	來源	部門
1	洛雷姆·伊普瑟姆.	金融/1	財務
2	洛雷姆·伊普瑟姆.	金融/2	財務
3	洛雷姆·伊普瑟姆.	金融/3	財務

Note

Amazon Kendra 如果目標文件欄位尚未建立為索引欄位，則無法建立該欄位。建立索引欄位之後，您可以使用建立文件欄位 `DocumentAttributeTarget`。Amazon Kendra 然後將新創建的文檔元數據字段映射到索引字段。

下列程式碼是設定基本資料操作，以移除與文件相關聯的客戶識別碼的範例。

Console

設定基本資料操作以移除客戶識別號碼

1. 在左側導覽窗格的 [索引] 下，選取 [文件擴充]，然後選取 [新增文件擴充]。
2. 在 [設定基本作業] 頁面上，從下拉式清單中選擇您要變更文件欄位和內容的資料來源。然後從下拉列表中選擇文檔字段名稱「Customer_ID」，從下拉列表中選擇索引字段名稱「Customer_ID」，然後從下拉列表中選擇目標操作刪除。然後選擇添加基本操作。

CLI

設定基本資料操作以移除客戶識別號碼

```
aws kendra create-data-source \  
  --name data-source-name \  
  --index-id index-id \  
  --role-arn arn:aws:iam::account-id:role/role-name \  
  --type S3 \  
  --configuration '{"S3Configuration":{"BucketName":"S3-bucket-name"}}' \  
  --custom-document-enrichment-configuration '{"InlineConfigurations":[{"Target":  
{"TargetDocumentAttributeKey":"Customer_ID", "TargetDocumentAttributeValueDeletion":  
true}}]}'
```

Python

設定基本資料操作以移除客戶識別號碼

```
import boto3  
from botocore.exceptions import ClientError  
import pprint  
import time  
  
kendra = boto3.client("kendra")  
  
print("Create a data source with customizations")  
  
# Provide the name of the data source  
name = "data-source-name"  
# Provide the index ID for the data source  
index_id = "index-id"
```



```
# Provide the IAM role ARN required for data sources
role_arn = "arn:aws:iam::${account-id}:role/${role-name}"
# Provide the data source connection information
data_source_type = "S3"
S3_bucket_name = "S3-bucket-name"
# Configure the data source with Custom Document Enrichment
configuration = {"S3Configuration":
    {
        "BucketName": S3_bucket_name
    }
}
custom_document_enrichment_configuration = {"InlineConfigurations":[
    {
        "Target":{"TargetDocumentAttributeKey":"Customer_ID",
            "TargetDocumentAttributeValueDeletion": True}
    }
]}

try:
    data_source_response = kendra.create_data_source(
        Name = name,
        IndexId = index_id,
        RoleArn = role_arn,
        Type = data_source_type
        Configuration = configuration
        CustomDocumentEnrichmentConfiguration =
custom_document_enrichment_configuration
    )

    pprint.pprint(data_source_response)

    data_source_id = data_source_response["Id"]

    print("Wait for Amazon Kendra to create the data source with your
customizations.")

    while True:
        # Get the details of the data source, such as the status
        data_source_description = kendra.describe_data_source(
            Id = data_source_id,
            IndexId = index_id
        )
        status = data_source_description["Status"]
        print(" Creating data source. Status: "+status)
```

```
        time.sleep(60)
        if status != "CREATING":
            break

    print("Synchronize the data source.")

    sync_response = kendra.start_data_source_sync_job(
        Id = data_source_id,
        IndexId = index_id
    )

    pprint.pprint(sync_response)

    print("Wait for the data source to sync with the index.")

    while True:

        jobs = kendra.list_data_source_sync_jobs(
            Id= data_source_id,
            IndexId= index_id
        )

        # For this example, there should be one job
        status = jobs["History"][0]["Status"]

        print(" Syncing data source. Status: "+status)
        time.sleep(60)
        if status != "SYNCING":
            break

    except ClientError as e:
        print("%s" % e)

    print("Program ends.")
```

Java

設定基本資料操作以移除客戶識別號碼

```
package com.amazonaws.kendra;

import java.util.concurrent.TimeUnit;
import software.amazon.awssdk.services.kendra.KendraClient;
import software.amazon.awssdk.services.kendra.model.CreateDataSourceRequest;
```

```
import software.amazon.awssdk.services.kendra.model.CreateDataSourceResponse;
import software.amazon.awssdk.services.kendra.model.CreateIndexRequest;
import software.amazon.awssdk.services.kendra.model.CreateIndexResponse;
import software.amazon.awssdk.services.kendra.model.DataSourceConfiguration;
import software.amazon.awssdk.services.kendra.model.DataSourceStatus;
import software.amazon.awssdk.services.kendra.model.DataSourceSyncJob;
import software.amazon.awssdk.services.kendra.model.DataSourceSyncJobStatus;
import software.amazon.awssdk.services.kendra.model.DataSourceType;
import software.amazon.awssdk.services.kendra.model.DescribeDataSourceRequest;
import software.amazon.awssdk.services.kendra.model.DescribeDataSourceResponse;
import software.amazon.awssdk.services.kendra.model.DescribeIndexRequest;
import software.amazon.awssdk.services.kendra.model.DescribeIndexResponse;
import software.amazon.awssdk.services.kendra.model.IndexStatus;
import software.amazon.awssdk.services.kendra.model.ListDataSourceSyncJobsRequest;
import software.amazon.awssdk.services.kendra.model.ListDataSourceSyncJobsResponse;
import software.amazon.awssdk.services.kendra.model.S3DataSourceConfiguration;
import software.amazon.awssdk.services.kendra.model.StartDataSourceSyncJobRequest;
import software.amazon.awssdk.services.kendra.model.StartDataSourceSyncJobResponse;

public class CreateDataSourceWithCustomizationsExample {

    public static void main(String[] args) throws InterruptedException {
        System.out.println("Create a data source with customizations");

        String dataSourceName = "data-source-name";
        String indexId = "index-id";
        String dataSourceRoleArn = "arn:aws:iam::account-id:role/role-name";
        String s3BucketName = "S3-bucket-name"

        KendraClient kendra = KendraClient.builder().build();

        CreateDataSourceRequest createDataSourceRequest = CreateDataSourceRequest
            .builder()
            .name(dataSourceName)
            .description(experienceDescription)
            .roleArn(experienceRoleArn)
            .type(DataSourceType.S3)
            .configuration(
                DataSourceConfiguration
                    .builder()
                    .s3Configuration(
                        S3DataSourceConfiguration
                            .builder()
                            .bucketName(s3BucketName)
```

```
                .build()
            ).build()
        )
        .customDocumentEnrichmentConfiguration(
            CustomDocumentEnrichmentConfiguration
                .builder()
                .inlineConfigurations(Arrays.asList(
                    InlineCustomDocumentEnrichmentConfiguration
                        .builder()
                        .target(
                            DocumentAttributeTarget
                                .builder()
                                .targetDocumentAttributeKey("Customer_ID")
                                .targetDocumentAttributeValueDeletion(true)
                                .build()
                            )
                        .build()
                ))).build();

        CreateDataSourceResponse createDataSourceResponse =
kendra.createDataSource(createDataSourceRequest);
        System.out.println(String.format("Response of creating data source: %s",
createDataSourceResponse));

        String dataSourceId = createDataSourceResponse.id();
        System.out.println(String.format("Waiting for Kendra to create the data
source %s", dataSourceId));
        DescribeDataSourceRequest describeDataSourceRequest =
DescribeDataSourceRequest
            .builder()
            .indexId(indexId)
            .id(dataSourceId)
            .build();

        while (true) {
            DescribeDataSourceResponse describeDataSourceResponse =
kendra.describeDataSource(describeDataSourceRequest);

            DataSourceStatus status = describeDataSourceResponse.status();
            System.out.println(String.format("Creating data source. Status: %s",
status));
            TimeUnit.SECONDS.sleep(60);
            if (status != DataSourceStatus.CREATING) {
                break;
            }
        }
```

```
    }

    System.out.println(String.format("Synchronize the data source %s",
dataSourceId));
    StartDataSourceSyncJobRequest startDataSourceSyncJobRequest =
StartDataSourceSyncJobRequest
        .builder()
        .indexId(indexId)
        .id(dataSourceId)
        .build();
    StartDataSourceSyncJobResponse startDataSourceSyncJobResponse =
kendra.startDataSourceSyncJob(startDataSourceSyncJobRequest);
    System.out.println(String.format("Waiting for the data
source to sync with the index %s for execution ID %s", indexId,
startDataSourceSyncJobResponse.executionId()));

    // For this example, there should be one job
    ListDataSourceSyncJobsRequest listDataSourceSyncJobsRequest =
ListDataSourceSyncJobsRequest
        .builder()
        .indexId(indexId)
        .id(dataSourceId)
        .build();

    while (true) {
        ListDataSourceSyncJobsResponse listDataSourceSyncJobsResponse =
kendra.listDataSourceSyncJobs(listDataSourceSyncJobsRequest);
        DataSourceSyncJob job = listDataSourceSyncJobsResponse.history().get(0);
        System.out.println(String.format("Syncing data source. Status: %s",
job.status()));

        TimeUnit.SECONDS.sleep(60);
        if (job.status() != DataSourceSyncJobStatus.SYNCING) {
            break;
        }
    }

    System.out.println("Data source creation with customizations is complete");
}
}
```

Lambda 函數：擷取和變更中繼資料或內容

您可以使用 Lambda 函數來操作文件欄位和內容。如果您想超越基本邏輯並應用高級數據操作，這非常有用。例如，使用「光學字元辨識」(OCR) 會解譯影像中的文字，並將每個影像視為文字文件。或者，檢索特定時區中的當前日期時間，然後插入日期時間，其中有一個日期字段的空值。

您可以先套用基本邏輯，然後使用 Lambda 函數進一步操作資料，反之亦然。您也可以選擇只套用 Lambda 函數。

Amazon Kendra 可以叫用 Lambda 函數，在擷取程序期間套用進階資料操作，做為

[CustomDocumentEnrichmentConfiguration](#) 您指定的角色包含執行 Lambda 函數和存取儲存 Amazon S3 貯體以存放資料操作輸出的權限，請參閱 [IAM 閱存取角色](#)。

Amazon Kendra 可以在原始、原始文件或結構化、剖析的文件上套用 Lambda 函數。您可以設定 Lambda 函數，以擷取原始或原始資料，並使 [PreExtractionHookConfiguration](#) 用。您也可以設定 Lambda 函數，以接收結構化文件，並使 [PostExtractionHookConfiguration](#) 用。Amazon Kendra 擷取文件中繼資料和文字以建立文件的結構。您的 Lambda 函數必須遵循強制要求和回應結構。如需詳細資訊，請參閱 [the section called “Lambda 函數的資料合約”](#)。

若要在主控台中設定 Lambda 函數，請選取索引，然後在導覽功能表中選取 [文件擴充]。前往設定 Lambda 函數以設定 Lambda 函數。

您只能為 [PreExtractionHookConfiguration](#) 設定一個 Lambda 函數，

且只能設定一個 Lambda 函數 [PostExtractionHookConfiguration](#)。

但是，您的 Lambda 函數可以叫用其所需的其他函數。您可以同時配

置 [PreExtractionHookConfiguration](#) 和 [PostExtractionHookConfiguration](#) 或其中一個。

Lambda 函數的執行時間不 [PreExtractionHookConfiguration](#) 得超過 5 分鐘，且 Lambda

函數的執行時間不 [PostExtractionHookConfiguration](#) 得超過 1 分鐘。設定自訂文件增強功能自

然而需要較長的時間來擷取文 Amazon Kendra 件，而不是設定此項目。

您可以設定 Amazon Kendra 為只有在符合條件時才叫用 Lambda 函數。例如，您可以指定一個條件，如果有空的日期時間值，則 Amazon Kendra 應該調用插入當前日期時間的函數。

以下是使用 Lambda 函數執行 OCR 來解譯影像中的文字，並將此文字儲存在名為「文件影像_文字」的欄位中的範例。

範例 1：從影像擷取文字以建立文字文件

應用高級操作之前的數據。

文件識別碼	文件影像
1	image_1.png
2	image_2.png
3	image_3.png

套用進階操作後的資料。

文件識別碼	文件影像	文件影像文字
1	image_1.png	郵寄調查問卷回覆
2	image_2.png	郵寄調查問卷回覆
3	image_3.png	郵寄調查問卷回覆

以下是使用 Lambda 函數為空白日期值插入目前日期時間的範例。這使用的條件是，如果一個日期字段值為 'null'，然後用當前的日期時間替換它。

範例 2：將「最後一次更新」欄位中的空值取代為目前的日期時間。

應用高級操作之前的數據。

文件識別碼	本文_文字	最後更新
1	洛雷姆·伊普瑟姆.	二零二零年一月一日
2	洛雷姆·伊普瑟姆.	
3	洛雷姆·伊普瑟姆.	2020 年 7 月 1 日

套用進階操作後的資料。

文件識別碼	本文_文字	最後更新
1	洛雷姆·伊普瑟姆.	二零二零年一月一日
2	洛雷姆·伊普瑟姆.	2021 年 12 月 1 日
3	洛雷姆·伊普瑟姆.	2020 年 7 月 1 日

下列程式碼是設定 Lambda 函數以對原始原始資料進行進階資料操作的範例。

Console

若要設定 Lambda 函數，以對原始原始資料進行進階資料操作

1. 在左側導覽窗格的 [索引] 下，選取 [文件擴充]，然後選取 [新增文件擴充]。
2. 在「設定 Lambda 函數」頁面的「用於預先擷取的 Lambda」區段中，從下拉式清單中選取 Lambda 函數 ARN 和儲存貯體。Amazon S3 從下拉式清單中選取建立新角色的選項，以新增您的 IAM 存取角色。這會建立建立文件擴充所需的 Amazon Kendra 權限。

CLI

若要設定 Lambda 函數，以對原始原始資料進行進階資料操作

```
aws kendra create-data-source \
  --name data-source-name \
  --index-id index-id \
  --role-arn arn:aws:iam::account-id:role/role-name \
  --type S3 \
  --configuration '{"S3Configuration":{"BucketName":"S3-bucket-name"}}' \
  --custom-document-enrichment-configuration '{"PreExtractionHookConfiguration":
{"LambdaArn":"arn:aws:iam::account-id:function/function-name", "S3Bucket":"S3-
bucket-name"}, "RoleArn": "arn:aws:iam:account-id:role/cde-role-name"}'
```

Python

若要設定 Lambda 函數，以對原始原始資料進行進階資料操作

```
import boto3
from botocore.exceptions import ClientError
import pprint
```



```
import time

kendra = boto3.client("kendra")

print("Create a data source with customizations.")

# Provide the name of the data source
name = "data-source-name"
# Provide the index ID for the data source
index_id = "index-id"
# Provide the IAM role ARN required for data sources
role_arn = "arn:aws:iam::${account-id}:role/${role-name}"
# Provide the data source connection information
data_source_type = "S3"
S3_bucket_name = "S3-bucket-name"
# Configure the data source with Custom Document Enrichment
configuration = {"S3Configuration":
    {
        "BucketName": S3_bucket_name
    }
}
custom_document_enrichment_configuration = {"PreExtractionHookConfiguration":
    {
        "LambdaArn": "arn:aws:iam::account-id:function/function-name",
        "S3Bucket": "S3-bucket-name"
    }
    "RoleArn": "arn:aws:iam::account-id:role/cde-role-name"
}

try:
    data_source_response = kendra.create_data_source(
        Name = name,
        IndexId = index_id,
        RoleArn = role_arn,
        Type = data_source_type
        Configuration = configuration
        CustomDocumentEnrichmentConfiguration =
custom_document_enrichment_configuration
    )

    pprint.pprint(data_source_response)

    data_source_id = data_source_response["Id"]
```

```
print("Wait for Amazon Kendra to create the data source with your
customizations.")

while True:
    # Get the details of the data source, such as the status
    data_source_description = kendra.describe_data_source(
        Id = data_source_id,
        IndexId = index_id
    )
    status = data_source_description["Status"]
    print(" Creating data source. Status: "+status)
    time.sleep(60)
    if status != "CREATING":
        break

print("Synchronize the data source.")

sync_response = kendra.start_data_source_sync_job(
    Id = data_source_id,
    IndexId = index_id
)

pprint.pprint(sync_response)

print("Wait for the data source to sync with the index.")

while True:

    jobs = kendra.list_data_source_sync_jobs(
        Id = data_source_id,
        IndexId = index_id
    )

    # For this example, there should be one job
    status = jobs["History"][0]["Status"]

    print(" Syncing data source. Status: "+status)
    time.sleep(60)
    if status != "SYNCING":
        break

except ClientError as e:
    print("%s" % e)
```

```
print("Program ends.")
```

Java

若要設定 Lambda 函數，以對原始資料進行進階資料操作

```
package com.amazonaws.kendra;

import java.util.concurrent.TimeUnit;
import software.amazon.awssdk.services.kendra.KendraClient;
import software.amazon.awssdk.services.kendra.model.CreateDataSourceRequest;
import software.amazon.awssdk.services.kendra.model.CreateDataSourceResponse;
import software.amazon.awssdk.services.kendra.model.CreateIndexRequest;
import software.amazon.awssdk.services.kendra.model.CreateIndexResponse;
import software.amazon.awssdk.services.kendra.model.DataSourceConfiguration;
import software.amazon.awssdk.services.kendra.model.DataSourceStatus;
import software.amazon.awssdk.services.kendra.model.DataSourceSyncJob;
import software.amazon.awssdk.services.kendra.model.DataSourceSyncJobStatus;
import software.amazon.awssdk.services.kendra.model.DataSourceType;
import software.amazon.awssdk.services.kendra.model.DescribeDataSourceRequest;
import software.amazon.awssdk.services.kendra.model.DescribeDataSourceResponse;
import software.amazon.awssdk.services.kendra.model.DescribeIndexRequest;
import software.amazon.awssdk.services.kendra.model.DescribeIndexResponse;
import software.amazon.awssdk.services.kendra.model.IndexStatus;
import software.amazon.awssdk.services.kendra.model.ListDataSourceSyncJobsRequest;
import software.amazon.awssdk.services.kendra.model.ListDataSourceSyncJobsResponse;
import software.amazon.awssdk.services.kendra.model.S3DataSourceConfiguration;
import software.amazon.awssdk.services.kendra.model.StartDataSourceSyncJobRequest;
import software.amazon.awssdk.services.kendra.model.StartDataSourceSyncJobResponse;

public class CreateDataSourceWithCustomizationsExample {

    public static void main(String[] args) throws InterruptedException {
        System.out.println("Create a data source with customizations");

        String dataSourceName = "data-source-name";
        String indexId = "index-id";
        String dataSourceRoleArn = "arn:aws:iam::account-id:role/role-name";
        String s3BucketName = "S3-bucket-name"

        KendraClient kendra = KendraClient.builder().build();

        CreateDataSourceRequest createDataSourceRequest = CreateDataSourceRequest
```

```

        .builder()
        .name(dataSourceName)
        .description(experienceDescription)
        .roleArn(experienceRoleArn)
        .type(DataSourceType.S3)
        .configuration(
            DataSourceConfiguration
                .builder()
                .s3Configuration(
                    S3DataSourceConfiguration
                        .builder()
                        .bucketName(s3BucketName)
                        .build()
                ).build()
        )
        .customDocumentEnrichmentConfiguration(
            CustomDocumentEnrichmentConfiguration
                .builder()
                .preExtractionHookConfiguration(
                    HookConfiguration
                        .builder()
                        .lambdaArn("arn:aws:iam::account-id:function/function-
name")
                        .s3Bucket("S3-bucket-name")
                        .build()
                ).roleArn("arn:aws:iam::account-id:role/cde-role-name")
                .build();

        CreateDataSourceResponse createDataSourceResponse =
kendra.createDataSource(createDataSourceRequest);
        System.out.println(String.format("Response of creating data source: %s",
createDataSourceResponse));

        String dataSourceId = createDataSourceResponse.id();
        System.out.println(String.format("Waiting for Kendra to create the data
source %s", dataSourceId));
        DescribeDataSourceRequest describeDataSourceRequest =
DescribeDataSourceRequest
            .builder()
            .indexId(indexId)
            .id(dataSourceId)
            .build();

        while (true) {

```

```
DescribeDataSourceResponse describeDataSourceResponse =
kendra.describeDataSource(describeDataSourceRequest);

DataSourceStatus status = describeDataSourceResponse.status();
System.out.println(String.format("Creating data source. Status: %s",
status));
TimeUnit.SECONDS.sleep(60);
if (status != DataSourceStatus.CREATING) {
    break;
}
}

System.out.println(String.format("Synchronize the data source %s",
dataSourceId));
StartDataSourceSyncJobRequest startDataSourceSyncJobRequest =
StartDataSourceSyncJobRequest
    .builder()
    .indexId(indexId)
    .id(dataSourceId)
    .build();
StartDataSourceSyncJobResponse startDataSourceSyncJobResponse =
kendra.startDataSourceSyncJob(startDataSourceSyncJobRequest);
System.out.println(String.format("Waiting for the data
source to sync with the index %s for execution ID %s", indexId,
startDataSourceSyncJobResponse.executionId()));

// For this example, there should be one job
ListDataSourceSyncJobsRequest listDataSourceSyncJobsRequest =
ListDataSourceSyncJobsRequest
    .builder()
    .indexId(indexId)
    .id(dataSourceId)
    .build();

while (true) {
    ListDataSourceSyncJobsResponse listDataSourceSyncJobsResponse =
kendra.listDataSourceSyncJobs(listDataSourceSyncJobsRequest);
    DataSourceSyncJob job = listDataSourceSyncJobsResponse.history().get(0);
    System.out.println(String.format("Syncing data source. Status: %s",
job.status()));

    TimeUnit.SECONDS.sleep(60);
    if (job.status() != DataSourceSyncJobStatus.SYNCING) {
        break;
    }
}
```

```

        }

    }

    System.out.println("Data source creation with customizations is complete");
}
}

```

Lambda 函數的資料合約

用於進階資料操作的 Lambda 函數會與 Amazon Kendra 資料合約互動。合約是 Lambda 函數的強制要求和回應結構。如果您的 Lambda 函數不遵循這些結構，則 Amazon Kendra 會擲回錯誤。

您的 Lambda 函數 `PreExtractionHookConfiguration` 應該需要下列要求結構：

```

{
  "version": <str>,
  "dataBlobStringEncodedInBase64": <str>, //In the case of a data blob
  "s3Bucket": <str>, //In the case of an S3 bucket
  "s3ObjectKey": <str>, //In the case of an S3 bucket
  "metadata": <Metadata>
}

```

結 metadata 構，其中包括該 `CustomDocumentAttribute` 結構，如下所示：

```

{
  "attributes": [<CustomDocumentAttribute>]
}

CustomDocumentAttribute
{
  "name": <str>,
  "value": <CustomDocumentAttributeValue>
}

CustomDocumentAttributeValue
{
  "stringValue": <str>,
  "integerValue": <int>,
  "longValue": <long>,
  "stringListValue": list<str>,

```

```
"dateValue": <str>
}
```

您的 Lambda 函數 `PreExtractionHookConfiguration` 必須遵守下列回應結構：

```
{
  "version": <str>,
  "dataBlobStringEncodedInBase64": <str>, //In the case of a data blob
  "s3ObjectKey": <str>, //In the case of an S3 bucket
  "metadataUpdates": [<CustomDocumentAttribute>]
}
```

您的 Lambda 函數 `PostExtractionHookConfiguration` 應該需要下列要求結構：

```
{
  "version": <str>,
  "s3Bucket": <str>,
  "s3ObjectKey": <str>,
  "metadata": <Metadata>
}
```

您的 Lambda 函數 `PostExtractionHookConfiguration` 必須遵守下列回應結構：

```
PostExtractionHookConfiguration Lambda Response
{
  "version": <str>,
  "s3ObjectKey": <str>,
  "metadataUpdates": [<CustomDocumentAttribute>]
}
```

您修改過的文件會上傳至 Amazon S3 值區。變更後的文件必須遵循中所示的格式 [the section called “結構化文件格式”](#)。

結構化文件格式

Amazon Kendra 將您的結構化文檔上傳到給定的 Amazon S3 存儲桶。結構化文件遵循以下格式：

```
Kendra document

{
  "textContent": <TextContent>
```

```
}

TextContent
{
  "documentBodyText": <str>
}
```

符合資料合約的 Lambda 函數範例

下列 Python 程式碼是 Lambda 函數的範例，可套用中繼資料欄位的進階操作 `_authors_document_title`，以及原始文件或原始文件上的內文內容。

在 Amazon S3 存儲桶中的正文內容的情況下

```
import json
import boto3

s3 = boto3.client("s3")

# Lambda function for advanced data manipulation
def lambda_handler(event, context):
    # Get the value of "S3Bucket" key name or item from the given event input
    s3_bucket = event.get("s3Bucket")
    # Get the value of "S3ObjectKey" key name or item from the given event input
    s3_object_key = event.get("s3ObjectKey")

    content_object_before_CDE = s3.get_object(Bucket = s3_bucket, Key = s3_object_key)
    content_before_CDE = content_object_before_CDE["Body"].read().decode("utf-8");
    content_after_CDE = "CDEInvolved " + content_before_CDE

    # Get the value of "metadata" key name or item from the given event input
    metadata = event.get("metadata")
    # Get the document "attributes" from the metadata
    document_attributes = metadata.get("attributes")

    s3.put_object(Bucket = s3_bucket, Key = "dummy_updated_kendra_document",
    Body=json.dumps(content_after_CDE))
    return {
        "version": "v0",
        "s3ObjectKey": "dummy_updated_kendra_document",
        "metadataUpdates": [
            {"name": "_document_title", "value":
{"stringValue": "title_from_pre_extraction_lambda"}},
```



```

        {"name": "_authors", "value": {"stringListValue": ["author1", "author2"]}}
    ]
}

```

在駐留在數據 Blob 中的主體內容的情況下

```

import json
import boto3
import base64

# Lambda function for advanced data manipulation
def lambda_handler(event, context):

    # Get the value of "dataBlobStringEncodedInBase64" key name or item from the given
    event input
    data_blob_string_encoded_in_base64 = event.get("dataBlobStringEncodedInBase64")
    # Decode the data blob string in UTF-8
    data_blob_string =
base64.b64decode(data_blob_string_encoded_in_base64).decode("utf-8")
    # Get the value of "metadata" key name or item from the given event input
    metadata = event.get("metadata")
    # Get the document "attributes" from the metadata
    document_attributes = metadata.get("attributes")

    new_data_blob = "This should be the modified data in the document by pre processing
lambda ".encode("utf-8")
    return {
        "version": "v0",
        "dataBlobStringEncodedInBase64":
base64.b64encode(new_data_blob).decode("utf-8"),
        "metadataUpdates": [
            {"name": "_document_title", "value":
{"stringValue": "title_from_pre_extraction_lambda"}},
            {"name": "_authors", "value": {"stringListValue": ["author1", "author2"]}}
        ]
    }
}

```

下列 Python 程式碼是 Lambda 函數的範例，可套用中繼資料欄位的進階操作 `_authors_document_title`，以及結構化或剖析文件上的內文內容。

```

import json
import boto3
import time

```

```
s3 = boto3.client("s3")

# Lambda function for advanced data manipulation
def lambda_handler(event, context):

    # Get the value of "S3Bucket" key name or item from the given event input
    s3_bucket = event.get("s3Bucket")
    # Get the value of "S3ObjectKey" key name or item from the given event input
    s3_key = event.get("s3ObjectKey")
    # Get the value of "metadata" key name or item from the given event input
    metadata = event.get("metadata")
    # Get the document "attributes" from the metadata
    document_attributes = metadata.get("attributes")

    kendra_document_object = s3.get_object(Bucket = s3_bucket, Key = s3_key)
    kendra_document_string = kendra_document_object['Body'].read().decode('utf-8')
    kendra_document = json.loads(kendra_document_string)
    kendra_document["textContent"]["documentBodyText"] = "Changing document body to a
short sentence."

    s3.put_object(Bucket = s3_bucket, Key = "dummy_updated_kendra_document",
Body=json.dumps(kendra_document))

    return {
        "version" : "v0",
        "s3ObjectKey": "dummy_updated_kendra_document",
        "metadataUpdates": [
            {"name": "_document_title", "value":{"stringValue":
"title_from_post_extraction_lambda"}},
            {"name": "_authors", "value":{"stringValue":["author1", "author2"]}}
        ]
    }
```

搜尋索引

若要搜尋 Amazon Kendra 索引，請使用 [查詢](#) API。QueryAPI 會傳回您在應用程式中使用之索引文件的相關資訊。本節說明如何進行查詢、執行篩選器，以及解譯從 Query API 取得的回應。

若要搜尋已編製索引的文件 Amazon Lex，Amazon Kendra 請使用 [AMAZON.KendraSearchIntent](#)。如需 Amazon Kendra 使用配置的範例 Amazon Lex，請參閱 [建立 Amazon Kendra 索引的常見問題集機器人](#)。

主題

- [查詢索引](#)
- [瀏覽索引](#)
- [特色搜尋結果](#)
- [以表格方式搜尋](#)
- [查詢建議](#)
- [查詢拼字檢查](#)
- [篩選和平面搜尋](#)
- [篩選使用者內容](#)
- [查詢回應和回應類型](#)
- [調整和排序回應](#)
- [摺疊/展開查詢結果](#)

查詢索引

當您搜尋索引時，Amazon Kendra 會使用您提供的有關文件的所有資訊來決定與輸入的檢索字詞最相關的文件。Amazon Kendra 考慮的一些項目是：

- 文件的文字或內文。
- 文件的標題。
- 您已標記為可搜尋的自訂文字欄位。
- 應使用您指示的日期欄位來決定文件的「新鮮度」。
- 任何其他可以提供相關資訊的欄位。

Amazon Kendra 還可以根据您為搜索設置的任何字段/屬性過濾器來過濾響應。例如，如果您有一個名為「部門」的自定義字段，則可以過濾響應以僅返回名為「合法」部門的文檔。如需詳細資訊，請參閱[自訂欄位或屬性](#)。

傳回的搜尋結果會依據 Amazon Kendra 決定每個文件的相關性來排序。結果會分頁，以便您可以一次向使用者顯示頁面。

若要搜尋已編製索引的文件 Amazon Lex，Amazon Kendra 請使用 [AMAZON.KendraSearchIntent](#)。如需 Amazon Kendra 使用配置的範例 Amazon Lex，請參閱[建立 Amazon Kendra 索引的常見問題集機器人](#)。

下面的例子演示了如何搜索索引。Amazon Kendra 決定最適合查詢的搜尋結果類型 (答案、文件、問題答案)。您無法設定 Amazon Kendra 為將特定類型的搜尋回應 (回答、文件、問題答案) 傳回查詢。

如需有關查詢回應的資訊，請參閱[查詢回應和回應類型](#)。

必要條件

在使用查詢 [API](#) 查詢索引之前：

- 設定索引所需的權限，並連線至資料來源或批次上傳文件。如需詳細資訊，請參閱[IAM 角色](#)。呼叫 API 建立索引和資料來源連接器或批次上傳文件時，您可以使用角色的 Amazon 資源名稱。
- 設定 AWS Command Line Interface、SDK 或前往 Amazon Kendra 主控台。如需詳細資訊，請參閱[設定 Amazon Kendra](#)。
- 創建索引並連接到文檔的數據源或批量上傳文檔。如需詳細資訊，請參閱[建立索引](#)和[建立資料來源連接器](#)。

搜尋索引 (主控台)

您可以使用主 Amazon Kendra 控制台來搜尋和測試索引。您可以進行查詢並查看結果。

使用主控台搜尋索引

1. 請登入 AWS Management Console 並開啟 Amazon Kendra 主控台，[網址為 http://console.aws.amazon.com/kendra/](http://console.aws.amazon.com/kendra/)。
2. 在導覽窗格中，選擇 [索引]。
3. 選擇您的索引。
4. 在導覽選單中，選擇搜尋索引的選項。

5. 在文字方塊中輸入查詢，然後按 Enter 鍵。
6. Amazon Kendra 返回搜索的結果。

您還可以通過選擇側面板中的燈泡圖標來獲取搜索的查詢 ID。

搜尋索引 (SDK)

若要使用 Python 或 Java 搜尋索引

- 下列範例會搜尋索引。將的值變更query為您的搜尋查詢和index_id或，變更indexId為您要搜尋之索引的索引識別碼。

當您呼叫 Query API 時，您也可以取得搜尋的查詢 ID 做為回應元素的一部分。

Python

```
import boto3
import pprint

kendra = boto3.client("kendra")

# Provide the index ID
index_id = "index-id"
# Provide the query text
query = "query text"

response = kendra.query(
    QueryText = query,
    IndexId = index_id)

print("\nSearch results for query: " + query + "\n")

for query_result in response["ResultItems"]:

    print("-----")
    print("Type: " + str(query_result["Type"]))

    if query_result["Type"]=="ANSWER" or
    query_result["Type"]=="QUESTION_ANSWER":
        answer_text = query_result["DocumentExcerpt"]["Text"]
        print(answer_text)
```

```
if query_result["Type"]=="DOCUMENT":
    if "DocumentTitle" in query_result:
        document_title = query_result["DocumentTitle"]["Text"]
        print("Title: " + document_title)
    document_text = query_result["DocumentExcerpt"]["Text"]
    print(document_text)

print("-----\n\n")
```

Java

```
package com.amazonaws.kendra;

import software.amazon.awssdk.services.kendra.KendraClient;
import software.amazon.awssdk.services.kendra.model.QueryRequest;
import software.amazon.awssdk.services.kendra.model.QueryResponse;
import software.amazon.awssdk.services.kendra.model.QueryResultItem;

public class SearchIndexExample {
    public static void main(String[] args) {
        KendraClient kendra = KendraClient.builder().build();

        String query = "query text";
        String indexId = "index-id";

        QueryRequest queryRequest = QueryRequest
            .builder()
            .queryText(query)
            .indexId(indexId)
            .build();

        QueryResponse queryResponse = kendra.query(queryRequest);

        System.out.println(String.format("\nSearch results for query: %s",
            query));
        for(QueryResultItem item: queryResponse.resultItems()) {
            System.out.println("-----");
            System.out.println(String.format("Type: %s", item.type()));

            switch(item.type()) {
                case QUESTION_ANSWER:
                case ANSWER:
```

```
        String answerText = item.documentExcerpt().text();
        System.out.println(answerText);
        break;
    case DOCUMENT:
        String documentTitle = item.documentTitle().text();
        System.out.println(String.format("Title: %s",
documentTitle));
        String documentExcerpt = item.documentExcerpt().text();
        System.out.println(String.format("Excerpt: %s",
documentExcerpt));
        break;
    default:
        System.out.println(String.format("Unknown query result type:
%s", item.type()));
    }

    System.out.println("-----\n");
}
}
```

搜索索引 (郵遞員)

您可以使用[郵遞員](#)來查詢和測試 Amazon Kendra 索引。

若要使用郵遞員搜尋索引

1. 在郵遞員中創建一個新的集合，並將請求類型設置為 POST。
2. 輸入端點 URL。例如, `https://kendra.<region>`
3. 選取「授權」標籤，然後輸入下列資訊。
 - 類型 — 選取AWS 簽名。
 - AccessKey輸入建立 IAM 使用者時產生的存取金鑰。
 - SecretKey輸入建立 IAM 使用者時產生的密鑰。
 - AWS 區域 — 輸入索引的區域。例如，`us-west-2`。
 - 服務名稱 — 輸入肯德拉。這是區分大小寫的，所以必須是小寫。

⚠ Warning

如果您輸入錯誤的服務名稱或未使用小寫字母，則在您選取「傳送」以傳送要求時，就會擲回錯誤：「認證應設定為正確的服務 'kendra」。您還必須檢查是否輸入了正確的訪問密鑰和密鑰。

4. 選取「標題」標籤，然後輸入下列機碼與值資訊。

- 按鍵：X-目標

價值:是. 阿馬遜. AWSKendraFrontendService. 查詢

- 金鑰：內容編碼

值：阿姆斯特 1.0

5. 選取「本體」頁籤，然後執行下列動作。

- 選擇要求內文的原始 JSON 類型。
- 輸入包含索引 ID 和查詢文字的 JSON。

```
{
  "IndexId": "index-id",
  "QueryText": "enter a query here"
}
```

⚠ Warning

如果您的 JSON 未使用正確的縮排，則會擲回錯誤："" SerializationException。檢查 JSON 中的縮進。

6. 選取 [傳送] (靠近右上角)。

使用進階查詢語法搜尋

您可以使用進階查詢語法或運算子，建立比簡單關鍵字或自然語言查詢更具體的查詢。這包括範圍、布林值、萬用字元等。透過使用運算子，您可以為查詢提供更多內容，並進一步精簡搜尋結果。

Amazon Kendra 支持以下運營商。

- 布林值：限制或擴大搜尋範圍的邏輯。例如，將搜尋amazon AND sports限制為僅搜尋包含這兩個字詞的文件。
- 圓括號：依優先順序讀取巢狀查詢字詞。例如，(amazon AND sports) NOT rainforest讀取(amazon AND sports)之前NOT rainforest。
- 範圍：日期或數值範圍值。範圍可以是包容性、排斥或無界限。例如，您可以搜尋上次在 2020 年 1 月 1 日至 2020 年 12 月 31 日期間更新的文件，包括這些日期。
- 欄位：使用特定欄位來限制搜尋。例如，您可以在「位置」字段中搜索具有「美國」的文檔。
- 萬用字元：部分符合文字字串。例如，Cloud*可以相符 CloudFormation。Amazon Kendra 目前僅支援尾隨萬用字元。
- 精確引號：完全匹配文本字符串。例如，包含"Amazon Kendra" "pricing"。

您可以使用上述任何運營商的組合。

請注意，過度使用運算子或高度複雜的查詢可能會影響查詢延遲。就延遲而言，萬用字元是一些最昂貴的運算子。一般規則是您使用的術語和運算子越多，對延遲的潛在影響就越大。影響延遲的其他因素包括索引文件的平均大小、索引的大小、搜尋結果的篩選，以及索引 Amazon Kendra 的整體負載。

Boolean

您可以使用布林運算子AND、OR來組合或排除單字NOT。

以下是使用布林運算子的範例。

amazon AND sports

返回在文本中包含兩個術語「Amazon」和「運動」的搜索結果，如亞馬遜 Prime 視頻體育或其他類似內容。

sports OR recreation

傳回文字中包含術語「sports」或「娛樂」或兩者的搜尋結果。

amazon NOT rainforest

傳回文字中包含術語「Amazon」但不包含「雨林」一詞的搜尋結果。這是為了搜索有關公司的文件 Amazon，而不是 Amazon 雨林。

括號

您可以使用括號以優先順序查詢巢狀單字。括號表示應該 Amazon Kendra 如何讀取查詢。

以下是使用括號運算子的範例。

(amazon AND sports) NOT rainforest

返回在文本中包含術語「亞馬遜」和「運動」，但不包含術語「雨林」的文檔。這是為了搜索 Amazon Prime 視頻體育或其他類似內容，而不是 Amazon 雨林中的冒險運動。括號有助於表示amazon AND sports應該在之前閱讀NOT rainforest。查詢不應讀取為amazon AND (sports NOT rainforest)。

(amazon AND (sports OR recreation)) NOT rainforest

返回包含術語「體育」或「娛樂」，或兩者兼而有之，以及術語「亞馬遜」的文件。但它不包括「雨林」一詞。這是搜索 Amazon 總理視頻體育或娛樂，而不是冒險運動在 Amazon 雨林。括號有助於表明sports OR recreation應該在與之前閱讀的 '亞馬遜' 結合之前閱讀NOT rainforest。查詢不應讀取為amazon AND (sports OR (recreation NOT rainforest))。

範圍

您可以使用值範圍來篩選搜尋結果。您可以指定屬性和範圍值。這可以是日期或數字類型。

日期範圍必須為下列格式：

- Epoch
- YYYY
- 年毫米
- 年-月-日
- 年-月-日-日

您也可以指定是否要包含或排除範圍的較低值和較高值。

以下是使用範圍運算子的範例。

`_processed_date:>2019-12-31 AND _processed_date:<2021-01-01`

2020 年處理的退貨文件 —— 大於 2019 年 12 月 31 日且少於 2021 年 1 月 1 日。

`_processed_date:>=2020-01-01 AND _processed_date:<=2020-12-31`

2020 年處理的退貨文件 — 大於或等於 2020 年 1 月 1 日，且小於或等於 2020 年 12 月 31 日的退貨文件。

_document_likes:<1

傳回零點讚或沒有使用者意見回饋 (小於 1 讚) 的文件。

您可以指定是否應將範圍視為包含或排除給定範圍值。

包容性

_last_updated_at:[2020-01-01 TO 2020-12-31]

最近更新於 2020 年的退貨文件 — 包括 2020 年 12 月 1 日和 2020 年 12 月 31 日的日期。

獨家

_last_updated_at:{2019-12-31 TO 2021-01-01}

返回最後更新於 2020 年的文件-不包括 2019 年 12 月 31 日和 2021 年 1 月 1 日的日期。

對於既不包含或排斥的無界範圍，只需使用 < and > 運算子即可。例

如：_last_updated_at:>2019-12-31 AND _last_updated_at:<2021-01-01

欄位

您可以將搜尋限制為僅傳回符合特定欄位中值的文件。該字段可以是任何類型的。

以下是使用欄位層級內容運算子的範例。

status:"Incomplete" AND financial_year:2021

傳回 2021 財政年度狀態不完整的文件。

(sports OR recreation) AND country:"United States" AND level:"professional"

傳回討論美國職業運動或娛樂的文件。

萬用字元

您可以使用萬用字元運算子擴大搜尋範圍，以考量字詞和片語的變體。這在搜尋名稱變體時很有用。Amazon Kendra 目前僅支援尾隨萬用字元。尾端萬用字元的前置字元數目必須大於兩個。

以下是使用萬用字元運算子的範例。

Cloud*

傳回包含諸如 CloudFormation 和之類的變體的文件 CloudWatch。

kendra*aws

返回包含變體的文檔，如肯德拉。

kendra*aws*

返回包含變體的文檔，如肯德拉。

精確引號

您可以使用引號來搜尋完全相符的文字。

以下是使用引號的範例。

"Amazon Kendra" "pricing"

傳回同時包含「」和「定價Amazon Kendra」一詞的文件。文件必須同時包含 " 和 '定價' 才能傳回結果。Amazon Kendra

"Amazon Kendra" "pricing" cost

傳回同時包含「」一詞和「定價Amazon Kendra」一詞，以及選擇性地指定「成本」一詞的文件。文件必須同時包含Amazon Kendra" 和 '定價' 才能傳回結果，但不一定包含「成本」。

無效的查詢語法

Amazon Kendra 如果您的查詢語法發生問題，或者您的查詢目前不受支援，則會發出警告 Amazon Kendra。如需詳細資訊，請參閱[查詢警告的 API 文件](#)。

下列查詢是無效查詢語法的範例。

_last_updated_at:<2021-12-32

無效的日期。第 32 天不存在於由使用的公曆中。Amazon Kendra

_view_count:ten

無效的數值。必須使用數字來表示數值。

nonExistentField:123

欄位搜尋無效。此欄位必須存在，才能使用欄位搜尋。

Product:[A TO D]

無效的範圍。數值或日期必須用於範圍。

OR Hello

布林值無效。運算子必須與字詞一起使用，並放置在術語之間。

以語言搜尋

您可以使用支援的語言搜尋文件。您可以在中傳遞語言代碼，[AttributeFilter](#)以您選擇的語言傳回已篩選的文件。您可以使用支援的語言鍵入查詢。

如果您未指定語言，則依預設會以英文 Amazon Kendra 查詢文件。如需支援語言 (包括其代碼) 的詳細資訊，請參閱以[英文以外的語言新增文件](#)。

若要在主控台中搜尋支援語言的文件，請選取您的索引，然後從導覽功能表中選取搜尋索引的選項。選取搜尋設定，然後從下拉式清單中選取語言，以選擇要傳回文件的語言。

下列範例顯示如何以西班牙文搜尋文件。

在主控台中以西班牙文搜尋索引

1. 請登入 AWS Management Console 並開啟 Amazon Kendra 主控台，[網址為 http://console.aws.amazon.com/kendra/](http://console.aws.amazon.com/kendra/)。
2. 在導覽選單中，選擇 [索引]，然後選擇您的索引。
3. 在導覽選單中，選擇搜尋索引的選項。
4. 在搜索設置中，選擇語言下拉列表，然後選擇西班牙語。
5. 在文字方塊中輸入查詢，然後按 Enter 鍵。
6. Amazon Kendra 以西班牙文傳回搜尋結果。

若要使用 CLI、Python 或 Java 以西班牙文搜尋索引

- 下列範例會以西班牙文搜尋索引。searchString將值變更為搜尋查詢，並indexID將值變更為您要搜尋之索引的識別碼。西班牙語的語言代碼為es. 您可以用自己的語言代碼替換它。

CLI

```
{
  "EqualsTo": {
    "Key": "_language_code",
    "Value": {
      "StringValue": "es"
    }
  }
}
```

```
}
```

Python

```
import boto3
import pprint

kendra = boto3.client("kendra")

# Provide the index ID
index_id = "index-id"
# Provide the query text
query = "search-string"

# Includes the index ID, query text, and language attribute filter
response = kendra.query(
    QueryText = query,
    IndexId = index_id,
    AttributeFilter = {
        "EqualsTo": {
            "Key": "_language_code",
            "Value": {
                "StringValue": "es"
            }
        }
    }
)

print ("\nSearch results|Resultados de la búsqueda: " + query + "\n")

for query_result in response["ResultItems"]:

    print("-----")
    print("Type: " + str(query_result["Type"]))

    if query_result["Type"]=="ANSWER" or
query_result["Type"]=="QUESTION_ANSWER":
        answer_text = query_result["DocumentExcerpt"]["Text"]
        print(answer_text)

    if query_result["Type"]=="DOCUMENT":
        if "DocumentTitle" in query_result:
            document_title = query_result["DocumentTitle"]["Text"]
            print("Title: " + document_title)
```

```
document_text = query_result["DocumentExcerpt"]["Text"]
print(document_text)

print("-----\n\n")
```

Java

```
package com.amazonaws.kendra;

import software.amazon.awssdk.services.kendra.KendraClient;
import software.amazon.awssdk.services.kendra.model.QueryRequest;
import software.amazon.awssdk.services.kendra.model.QueryResponse;
import software.amazon.awssdk.services.kendra.model.QueryResultItem;

public class SearchIndexExample {
    public static void main(String[] args) {
        KendraClient kendra = KendraClient.builder().build();

        String query = "searchString";
        String indexId = "indexID";

        QueryRequest queryRequest = QueryRequest.builder()
            .queryText(query)
            .indexId(indexId)
            .attributeFilter(
                AttributeFilter.builder()
                    .withEqualsTo(
                        DocumentAttribute.builder()
                            .withKey("_language_code")
                            .withValue("es")
                            .build())
                    .build())
            .build();

        QueryResponse queryResponse = kendra.query(queryRequest);

        System.out.println(String.format("\nSearch results|
                                         Resultados de la búsqueda: %s",
query));
        for(QueryResultItem item: queryResponse.resultItems()) {
            System.out.println("-----");
        }
    }
}
```

```
        System.out.println(String.format("Type: %s", item.type()));

        switch(item.type()) {
            case QUESTION_ANSWER:
            case ANSWER:
                String answerText = item.documentExcerpt().text();
                System.out.println(answerText);
                break;
            case DOCUMENT:
                String documentTitle = item.documentTitle().text();
                System.out.println(String.format("Title: %s",
documentTitle));
                String documentExcerpt = item.documentExcerpt().text();
                System.out.println(String.format("Excerpt: %s",
documentExcerpt));
                break;
            default:
                System.out.println(String.format("Unknown query result type:
%s", item.type()));
        }

        System.out.println("-----\n");
    }
}
}
```

擷取段落

您可以使用 [RetrieveAPI](#) 作為檢索增強生成 (RAG) 系統的檢索器。

RAG 系統使用生成人工智慧來建置問答應用程式。RAG 系統包括一個檢索器和大型語言模型 (LLM)。給定一個查詢，檢索器從文檔的語料庫中識別最相關的文本塊，並將其提供給 LLM 以提供最有用的答案。然後，LLM 分析相關的文本塊或段落，並為查詢生成全面的響應。

RetrieveAPI 會查看稱為段落的文字區塊或摘錄，並傳回與查詢最相關的頂部段落。

如同 [QueryAPI](#)，RetrieveAPI 也會使用語意搜尋來搜尋相關資訊。語意搜尋會考量搜尋查詢的內容，以及索引文件中的所有可用資訊。但是，默認情況下，QueryAPI 僅返回多達 100 個令牌單詞的摘錄段落。使用 Retrieve API，您可以檢索多達 200 個令牌單詞的較長段落和多達 100 個與語義相關的段落。這不包括索引中的問題答案或常見問題解答類型回應。這些段落是文本摘錄，可以從多個

文檔和同一文檔的多個部分語義中提取。如果在極端情況下，您的文件使用 Retrieve API 產生零段落，您也可以使用 Query API 及其回應類型。

您也可以使用 Retrieve API 執行以下操作：

- 在索引層級覆寫提升
- 根據文件欄位或屬性進行篩選
- 根據使用者或其群組對文件的存取權進行篩選
- 檢視已擷取之通道結果的可信度分數時段。信賴值區會提供相對排名，指出回應與查詢相關的信 Amazon Kendra 心程度。

Note

信心分數值區目前僅適用於英文。

您還可以在響應中包含某些字段，這些字段可能會提供有用的其他信息。

RetrieveAPI 目前不支援 Query API 支援的所有功能。不支援下列功能：使用[進階查詢語法進行查詢](#)、[建議的查詢拼字校正](#)、[Facting](#)、自動完成搜尋[查詢的查詢建議](#)，以及[增量學習](#)。請注意，並非所有功能都適用於 Retrieve API。任何 future 版本的 Retrieve API 都會記錄在本指南中。

RetrieveAPI 會共用您為索引設定的[查詢容量單位](#)數量。如需單一容量單位包含的內容以及索引的預設基本容量的詳細資訊，請參閱[調整容量](#)。

Note

如果您使用的是 Amazon Kendra 開發人員版，則無法新增容量；您只能在使用 Amazon Kendra 企業版時增加容量。如需開發人員和企業版所包含內容的詳細資訊，請參閱[Amazon Kendra 版本](#)。

以下是使用 Retrieve API 從查詢索引中的文件擷取前 100 個最相關段落的範例 "how does amazon kendra work?"

Python

```
import boto3
import pprint
```

```
kendra = boto3.client("kendra")

# Provide the index ID
index_id = "index-id"
# Provide the query text
query = "how does amazon kendra work?"
# You can retrieve up to 100 relevant passages
# You can paginate 100 passages across 10 pages, for example
page_size = 10
page_number = 10

result = kendra.retrieve(
    IndexId = index_id,
    QueryText = query,
    PageSize = page_size,
    PageNumber = page_number)

print("\nRetrieved passage results for query: " + query + "\n")

for retrieve_result in result["ResultItems"]:

    print("-----")
    print("Title: " + str(retrieve_result["DocumentTitle"]))
    print("URI: " + str(retrieve_result["DocumentURI"]))
    print("Passage content: " + str(retrieve_result["Content"]))
    print("-----\n\n")
```

Java

```
package com.amazonaws.kendra;

import software.amazon.awssdk.services.kendra.KendraClient;
import software.amazon.awssdk.services.kendra.model.RetrieveRequest;
import software.amazon.awssdk.services.kendra.model.RetrieveResult;
import software.amazon.awssdk.services.kendra.model.RetrieveResultItem;

public class RetrievePassageExample {
    public static void main(String[] args) {
        KendraClient kendra = KendraClient.builder().build();

        String indxId = "index-id";
        String query = "how does amazon kendra work?";
```

```
Integer pgSize = 10;
Integer pgNumber = 10;

RetrieveRequest retrieveRequest = retrieveRequest
    .builder()
    .indexId(indxId)
    .queryText(query)
    .pageSize(pgSize)
    .pageNumber(pgNumber)
    .build();

RetrieveResult retrieveResult = kendra.retrieve(retrieveRequest);

System.out.println(String.format("\nRetrieved passage results for query:
%s", query));
for(RetrieveResultItem item: retrieveResult.resultItems()) {
    System.out.println("-----");
    System.out.println(String.format("Title: %s", documentTitle));
    System.out.println(String.format("URI: %s", documentURI));
    System.out.println(String.format("Passage content: %s", content));
    System.out.println("-----\n");
}
}
}
```

瀏覽索引

您可以依照文件的屬性或 Facet 瀏覽文件，而不必輸入搜尋查詢。Amazon Kendra 索引瀏覽可以幫助您的用戶通過自由瀏覽索引而不考慮特定查詢來發現文檔。這也有助於您的使用者在搜尋時廣泛地瀏覽索引作為起點。

索引瀏覽只能用於依文件屬性或排序類型的 Facet 進行搜尋。您無法使用「索引瀏覽」搜尋整個索引。如果缺少查詢文字，則 Amazon Kendra 會詢問文件屬性篩選器或 Facet，以及排序類型。

若要允許使用[查詢](#) API 瀏覽索引，您必須包含[AttributeFilter](#)或 [Facet](#) 和[SortingConfiguration](#)。若要允許在主控台中瀏覽索引，請在導覽功能表的 [索引] 底下選取您的索引，然後選取搜尋索引的選項。在搜索框中，按 Enter 鍵兩次。選取下拉式清單 [篩選搜尋結果] 以選擇篩選器，然後選取下拉式清單 [排序] 以選擇排序類型。

以下是以文件建立日期遞減順序瀏覽西班牙文文件索引的範例。

CLI

```
aws kendra query \  
--index-id "index-id" \  
--attribute-filter '{  
  "EqualsTo":{  
    "Key": "_language_code",  
    "Value": {  
      "StringValue": "es"  
    }  
  }  
}' \  
--sorting-configuration '{  
  "DocumentAttributeKey": "_created_at",  
  "SortOrder": "DESC"  
}'
```

Python

```
import boto3  
  
kendra = boto3.client("kendra")  
  
# Must include the index ID, the attribute filter, and sorting configuration  
response = kendra.query(  
    IndexId = "index-id",  
    AttributeFilter = {  
        "EqualsTo": {  
            "Key": "_language_code",  
            "Value": {  
                "StringValue": "es"  
            }  
        }  
    },  
    SortingConfiguration = {  
        "DocumentAttributeKey": "_created_at",  
        "SortOrder": "DESC"})  
  
print("\nSearch results|Resultados de la búsqueda: \n")  
  
for query_result in response["ResultItems"]:  
    print("-----")
```

```
print("Type: " + str(query_result["Type"]))

if query_result["Type"]=="ANSWER" or query_result["Type"]=="QUESTION_ANSWER":
    answer_text = query_result["DocumentExcerpt"]["Text"]
    print(answer_text)

if query_result["Type"]=="DOCUMENT":
    if "DocumentTitle" in query_result:
        document_title = query_result["DocumentTitle"]["Text"]
        print("Title: " + document_title)
    document_text = query_result["DocumentExcerpt"]["Text"]
    print(document_text)

print("-----\n\n")
```

Java

```
package com.amazonaws.kendra;

import software.amazon.awssdk.services.kendra.KendraClient;
import software.amazon.awssdk.services.kendra.model.QueryRequest;
import software.amazon.awssdk.services.kendra.model.QueryResult;
import software.amazon.awssdk.services.kendra.model.QueryResultItem;

public class SearchIndexExample {
    public static void main(String[] args) {
        KendraClient kendra = KendraClient.builder().build();
        QueryRequest queryRequest = QueryRequest.builder()
            .withIndexId("index-id")
            .withAttributeFilter(AttributeFilter.builder()
                .withEqualsTo(DocumentAttribute.builder()
                    .withKey("_language_code")
                    .withValue(DocumentAttributeValue.builder()
                        .withStringValue("es")
                        .build())
                    .build())
                .build())
            .build()
            .withSortingConfiguration(SortingConfiguration.builder()
                .withDocumentAttributeKey("_created_at")
                .withSortOrder("DESC")
                .build())
            .build());
```

```
QueryResult queryResult = kendra.query(queryRequest);
for (QueryResultItem item : queryResult.getResultItems()) {
    System.out.println("-----");
    System.out.println(String.format("Type: %s", item.getType()));

    switch (item.getType()) {
        case QueryResultType.QUESTION_ANSWER:
        case QueryResultType.ANSWER:
            String answerText = item.getDocumentExcerpt().getText();
            System.out.println(answerText);
            break;
        case QueryResultType.DOCUMENT:
            String documentTitle = item.getDocumentTitle().getText();
            System.out.println(String.format("Title: %s", documentTitle));
            String documentExcerpt = item.getDocumentExcerpt().getText();
            System.out.println(String.format("Excerpt: %s",
documentExcerpt));
            break;
        default:
            System.out.println(String.format("Unknown query result type:
%s", item.getType()));
    }
    System.out.println("-----\n");
}
}
```

特色搜尋結果

當您的使用者發出某些查詢時，您可以在搜尋結果中顯示特定文件。這有助於使用者的結果更加明顯和突出。精選結果會與一般的結果清單分開，並顯示在搜尋頁面的頂端。您可以嘗試針對不同的查詢提供不同的文檔，或確保某些文檔獲得應有的可見性。

您可以將特定查詢對映至特定文件，以便在結果中進行特色。如果查詢包含完全相符項目，則會在搜尋結果中顯示一或多個特定文件。

例如，您可以指定如果您的使用者發出「新產品 2023」查詢，請選取標題為「最新消息」和「即將推出」的文件，以顯示在搜尋結果頁面頂端。這有助於確保這些有關新產品的文件獲得應有的可見性。

Amazon Kendra 如果已在搜尋結果頁面頂端選取特色搜尋結果，則不會重複搜尋結果。如果特色結果已經超越所有其他結果，則不會再將其排名為第一個結果。

若要顯示特定結果，您必須指定完全相符的全文檢索查詢，而不是使用查詢中包含的關鍵字或片語來指定查詢的部分相符項目。例如，如果您只在特色結果集中指定查詢「Kendra」，則查詢如「Kendra 如何在語意上對結果進行排名？」不會呈現特色結果。精選結果是針對特定查詢而設計的，而非範圍過於廣泛的查詢。Amazon Kendra 自然地處理關鍵字類型查詢，以在搜索結果中排名最有用的文檔，避免基於簡單關鍵字的結果過度特徵。

如果您的使用者經常使用某些查詢，您可以為精選結果指定這些查詢。例如，如果您使用 [Amazon Kendra Analytics](#) 查看熱門查詢並發現特定查詢，例如「kendra 如何在語義上對結果進行排名？」和 'kendra 語義搜索' 經常使用，那麼這些查詢可能對指定標題為「搜索 101」Amazon Kendra 的文檔有用。

Amazon Kendra 會將特色結果的查詢視為不區分大小寫。Amazon Kendra 將查詢轉換為小寫，並用單個空格替換尾隨空格字符。Amazon Kendra 匹配所有其他字符，因為它們是當你指定你的特色結果查詢。

您可以建立一組精選結果，並使用 [CreateFeaturedResultsSet](#) API 對應至特定查詢。如果您使用主控台，請選取索引，然後在導覽選單中選取「精選結果」，以建立精選結果集。每個索引最多可建立 50 組精選結果，每個索引最多可建立四份文件，每個精選結果集最多可建立 49 個查詢文字。您可以聯絡 [Support](#) 部門，要求提高這些限制。

您可以在多組精選結果中選擇相同的文件。但是，您不得在多個集合中使用相同的完全相符查詢文字。您為精選結果指定的查詢必須是每個索引的每個精選結果集唯一的查詢。

選取最多四個精選文件時，您可以排列文件順序。如果您使用 API，則精選文件的列出順序與精選結果中顯示的順序相同。如果您使用控制台，則可以在選擇要在結果中特色顯示的文件時，只需拖放文件的順序即可。

存取控制 (某些使用者和群組可以存取某些文件，而其他人則無法存取) 在設定精選結果時仍會受到接受。對於使用者內容篩選也是如此。例如，使用者 A 屬於「實習生」公司群組，該群組不應存取有關公司機密的文件。如果使用者 A 輸入包含公司密碼文件的查詢，使用者 A 就不會在其結果中看到此文件。對於搜索結果頁面上的任何其他結果也是如此。您也可以使用標籤來控制對特色結果集的存取，這是您控制其存取權的 Amazon Kendra 資源。

下面是創建一組特色結果的例子，其中包括查詢「新產品 2023」，「可用的新產品」映射到標題為「新功能」(doc-id-1) 和「即將推出」(doc-id-2) 的文檔。

CLI

```
aws kendra create-featured-results-set \  
  --featured-results-set-name 'New product docs to feature' \  
  --query 'kendra 如何在語義上對結果進行排名？' \  
  --query 'kendra 語義搜索'
```

```
--description "Featuring What's new and Coming soon docs" \  
--index-id index-id \  
--query-texts 'new products 2023' 'new products available' \  
--featured-documents '{"Id":"doc-id-1", "Id":"doc-id-2"}'
```

Python

```
import boto3  
from botocore.exceptions import ClientError  
import pprint  
import time  
  
kendra = boto3.client("kendra")  
  
print("Create a featured results set.")  
  
# Provide a name for the featured results set  
featured_results_name = "New product docs to feature"  
# Provide an optional description for the featured results set  
description = "Featuring What's new and Coming soon docs"  
# Provide the index ID for the featured results set  
index = "index-id"  
# Provide a list of query texts for the featured results set  
queries = ['new products 2023', 'new products available']  
# Provide a list of document IDs for the featured results set  
featured_doc_ids = [{"Id":"doc-id-1"}, {"Id":"doc-id-2"}]  
  
try:  
    featured_results_set_response = kendra.create_featured_results_set(  
        FeaturedResultsSetName = featured_results_name,  
        Description = description,  
        Index = index,  
        QueryTexts = queries,  
        FeaturedDocuments = featured_doc_ids  
    )  
  
    pprint.pprint(featured_results_set_response)  
  
    featured_results_set_id = featured_results_set_response["FeaturedResultsSetId"]  
  
    while True:  
        # Get the details of the featured results set, such as the status  
        featured_results_set_description = kendra.describe_featured_results_set(  

```



```
        Id = featured_results_set_id
    )
    status = featured_results_set_description["Status"]
    print(" Featured results set status: "+status)

except ClientError as e:
    print("%s" % e)

print("Program ends.")
```

以表格方式搜尋

Amazon Kendra 的表格搜索功能可以從嵌入在 HTML 文檔中的表中搜索和提取答案。當您搜尋索引時，如果表格摘錄與查詢相關並提供有用的資訊，請 Amazon Kendra 包含表格摘錄。

Amazon Kendra 查看文件內文中的所有資訊，包括表格中的有用資訊。例如，索引包含商業報告，其中包含營運成本、收入和其他財務資訊的表格。對於查詢，「從 2020-2022 年度起的年度運營成本是多少？」，Amazon Kendra 可以傳回包含相關表格欄「營運 (百萬美元)」和「財政年度」的表格摘錄，以及包含 2020 年、2021 年和 2022 年收入值的表格列。結果中會包含表格摘錄，以及文件標題、完整文件的連結，以及您選擇包含的任何其他文件欄位。

無論是在表格的一個儲存格或多個儲存格中找到資訊，都可以在搜尋結果中顯示表格摘錄。例如，Amazon Kendra 可以顯示針對以下每種查詢量身打造的表格摘錄：

- 「2020 年最高利率信用卡」
- 「2020 至 22 年度最高利率信用卡」
- 「2020 至 22 年度前三大最高利率信用卡」
- 「利率低於 10% 的信用卡」
- 「所有可用的低息信用卡」

Amazon Kendra 反白與查詢最相關的表格儲存格。最相關的單元格及其對應的行，列和列名稱顯示在搜索結果中。根據查詢相關的表格儲存格數目，以及原始表格中可用的欄數目，表格摘錄最多會顯示五欄和三列。最重要的儲存格會顯示在表格摘錄中，以及下一個最相關的儲存格。

回應包含信賴值區 (MEDIUM、HIGH、VERY_HIGH)，以顯示資料表回答與查詢的相關性。如果表格儲存格值具有 VERY_HIGH 信心，則會變成「最常見的答案」並反白顯示。對於有 HIGH 信心的表格儲存格值，則會反白顯示它們。對於有 MEDIUM 信心的表格儲存格值，則不會反白顯示它們。表格答案的整體

可信度會在回應中傳回。例如，如果資料表大部分包含有HIGH信心的表格儲存格，則表格答案回應中傳回的整體信HIGH賴度就是信賴度。

根據預設，表格的重要性層級不會比文件的其他元件更高或更重要。在文件中，如果表格僅與查詢稍微相關，但有高度相關的段落，則會 Amazon Kendra 傳回段落的摘錄。搜尋結果會在相同文件或其他文件中顯示提供最佳答案和最有用資訊的內容片段。如果資料表的可信MEDIUM度低於置信度，則回應中不會傳回資料表摘錄。

若要在現有索引上使用表格搜尋，您必須重新建立內容的索引。

Amazon Kendra 表格式搜尋支援[同義字](#) (包括自訂同義字)。Amazon Kendra 僅支援含有表格標籤內之 HTML 表格的英文文件。

下列範例顯示查詢結果中包含的表格摘錄。若要檢視包含查詢回應的範例 JSON (包括資料表摘錄)，請參閱[查詢回應和類型](#)。

Python

```
import boto3
import pprint

kendra = boto3.client("kendra")

# Provide the index ID
index_id = <index-id>
# Provide the query text
query = "search string"

response = kendra.query(
    QueryText = query,
    IndexId = index_id)

print("\nSearch results for query: " + query + "\n")

for query_result in response["ResultItems"]:

    print("-----")
    print("Type: " + str(query_result["Type"]))
    print("Type: " + str(query_result["Format"]))

    if query_result["Type"]=="ANSWER" and query_result["Format"]=="TABLE":
        answer_table = query_result["TableExcerpt"]
        print(answer_table)
```

```
if query_result["Type"]=="ANSWER" and query_result["Format"]=="TEXT":
    answer_text = query_result["DocumentExcerpt"]
    print(answer_text)

if query_result["Type"]=="QUESTION_ANSWER":
    question_answer_text = query_result["DocumentExcerpt"]["Text"]
    print(question_answer_text)

if query_result["Type"]=="DOCUMENT":
    if "DocumentTitle" in query_result:
        document_title = query_result["DocumentTitle"]["Text"]
        print("Title: " + document_title)
    document_text = query_result["DocumentExcerpt"]["Text"]
    print(document_text)

print("-----\n\n")
```

Java

```
package com.amazonaws.kendra;

import software.amazon.awssdk.services.kendra.KendraClient;
import software.amazon.awssdk.services.kendra.model.QueryRequest;
import software.amazon.awssdk.services.kendra.model.QueryResponse;
import software.amazon.awssdk.services.kendra.model.QueryResultItem;

public class SearchIndexExample {
    public static void main(String[] args) {
        KendraClient kendra = KendraClient.builder().build();

        String query = "search string";
        String indexId = "index-id";

        QueryRequest queryRequest = QueryRequest
            .builder()
            .queryText(query)
            .indexId(indexId)
            .build();

        QueryResponse queryResponse = kendra.query(queryRequest);

        System.out.println(String.format("\nSearch results for query: %s", query));
    }
}
```

```
for(QueryResultItem item: queryResponse.resultItems()) {
    System.out.println("-----");
    System.out.println(String.format("Type: %s", item.type()));
    System.out.println(String.format("Format: %s", item.format()));

    switch(item.format()) {
        case TABLE:
            String answerTable = item.TableExcerpt();
            System.out.println(answerTable);
            break;
    }

    switch(item.format()) {
        case TEXT:
            String answerText = item.DocumentExcerpt();
            System.out.println(answerText);
            break;
    }

    switch(item.type()) {
        case QUESTION_ANSWER:
            String questionAnswerText = item.documentExcerpt().text();
            System.out.println(questionAnswerText);
            break;
        case DOCUMENT:
            String documentTitle = item.documentTitle().text();
            System.out.println(String.format("Title: %s", documentTitle));
            String documentExcerpt = item.documentExcerpt().text();
            System.out.println(String.format("Excerpt: %s",
documentExcerpt));
            break;
        default:
            System.out.println(String.format("Unknown query result type:
%s", item.type()));
    }

    System.out.println("-----\n");
}
}
```

查詢建議

Amazon Kendra 查詢建議可以幫助您的用戶更快地輸入搜索查詢並引導他們的搜索。

Amazon Kendra 根據下列其中一項建議與使用者相關的查詢：

- 查詢歷史記錄或查詢日誌中的熱門查詢
- 文檔欄位/屬性的內容

您可以通過設置 `SuggestionTypes` 為 `DOCUMENT_ATTRIBUTES` 和調用來設置使用查詢歷史記錄 `QUERY` 或文檔字段的偏好設置 [GetQuerySuggestions](#)。根據預設，Amazon Kendra 會使用查詢歷史記錄來建議。如果查詢記錄和文件欄位在您呼叫時都已啟動，[UpdateQuerySuggestionsConfig](#) 且您尚未將 `SuggestionTypes` 偏好設定設定為使用文件欄位，則 Amazon Kendra 會使用查詢記錄。

如果您使用控制台，則可以根據查詢歷史記錄或文檔字段進行查詢建議。您首先選取您的索引，然後在導覽功能表中的 [擴充] 下選取 [查詢建議]。然後選取 [設定查詢建議]。設定查詢建議後，系統會將您導向至搜尋主控台，您可以在其中選取右側面板中的 [查詢記錄] 或 [文件] 欄位，然後在搜尋列中輸入搜尋查詢。

根據預設，使用查詢歷史記錄和文件欄位的查詢建議都會啟用，而無需額外付費。您可以隨時使用 `UpdateQuerySuggestionsConfig` API 停用這些類型的查詢建議。若要根據查詢歷史記錄停用查詢建議，請在呼叫 `DISABLED` 時設定 `Mode` 為 `UpdateQuerySuggestionsConfig`。要根據文檔字段停用查詢建議，請 `INACTIVE` 在文檔字段配置中設置 `AttributeSuggestionsMode` 為，然後調用 `UpdateQuerySuggestionsConfig`。如果您使用主控台，您可以在 [查詢建議] 設定中停用查詢建議。

查詢建議不區分大小寫。Amazon Kendra 將查詢前置詞和建議的查詢轉換為小寫，忽略所有單引號和雙引號，並以單一空格取代多個空格字元。Amazon Kendra 匹配所有其他特殊字符，因為他們是。Amazon Kendra 如果使用者輸入少於兩個字元或超過 60 個字元，則不會顯示任何建議。

主題

- [使用查詢歷史查詢建議](#)
- [使用文件欄位查詢建議](#)
- [封鎖建議中的某些查詢或文件欄位內容](#)

使用查詢歷史查詢建議

主題

- [選取建議查詢的設定](#)
- [清除建議，同時保留查詢歷史](#)
- [沒有可用的建議](#)

您可以選擇根據查詢歷史記錄或查詢日誌中的常用查詢建議與使用者相關的查詢。Amazon Kendra 使用您的使用者搜尋並從這些查詢中學習的所有查詢，向您的使用者提供建議。Amazon Kendra 當用戶開始輸入查詢時，向用戶建議流行的查詢。Amazon Kendra 建議查詢，如果查詢的前綴或前幾個字符與用戶開始輸入的查詢相匹配。

例如，用戶開始鍵入查詢「即將發生的事件」。Amazon Kendra 從查詢歷史記錄中了解到，許多用戶多次搜索了「即將發生的事件 2050」。用戶看到「即將發生的事件 2050」直接出現在他們的搜索欄下方，自動完成他們的搜索查詢。使用者選取此查詢建議，搜尋結果中會傳回「新事件：2050 年發生的事件」文件。

您可以指定如何 Amazon Kendra 選取符合資格的查詢，以向使用者建議。例如，您可以指定查詢建議必須由至少 10 個不重複使用者 (預設值為 3 位)、在過去 30 天內搜尋過，且不包含[封鎖清單](#)中的任何字詞或片語。Amazon Kendra 要求查詢至少有一個搜尋結果，且至少包含一個超過四個字元的單字。

選取建議查詢的設定

您可以使用 [UpdateQuerySuggestionsConfig](#) API 設定下列設定，以選取建議的查詢：

- 模式：使用查詢歷史記錄的查詢建議是ENABLED或LEARN_ONLY。Amazon Kendra 預設會啟用查詢建議。LEARN_ONLY關閉查詢建議。如果關閉，則會 Amazon Kendra 繼續學習建議，但不會向使用者提供查詢建議。
- 查詢記錄時間視窗 — 查詢在查詢記錄時間視窗中的最近程度。時間範圍是從當天到過去天數的整數值。
- 不含使用者資訊的查詢 — 設定TRUE為包含所有查詢，或設定FALSE為僅包含使用者資訊的查詢。如果您的搜尋應用程式在使用者發出查詢時包含使用者資訊 (例如使用者 ID)，則可以使用此設定。根據預設，如果沒有與查詢相關聯的特定使用者資訊，此設定不會篩選出查詢。但是，您可以使用此設定，僅根據包含使用者資訊的查詢提出建議。
- 唯一使用者 — 必須在查詢中搜尋查詢才有資格向您的使用者建議的唯一使用者數目下限。這個數字是一個整數值。
- 查詢計數 — 必須搜尋查詢才符合向使用者建議的查詢次數下限。這個數字是一個整數值。

這些設定會影響如何選取查詢做為常用查詢，以向使用者建議。調整設定的方式取決於您的特定需求，例如：

- 如果您的使用者通常每月平均搜尋一次，則您可以將查詢記錄時間視窗中的天數設定為 30 天。透過使用該設定，您可以在使用者在時間範圍中過期之前擷取大多數使用者最近的查詢。
- 如果只有少數查詢包含使用者資訊，而您不想根據較小的範例大小建議查詢，則可以設定查詢以包含所有使用者。
- 如果您將常用查詢定義為由至少 10 個不重複使用者搜尋，並搜尋至少 100 次，則您將唯一使用者設定為 10，而查詢計數為 100。

Warning

您對設定所做的變更可能不會立即生效。您可以使用 [DescribeQuerySuggestionsConfig](#) API 追蹤設定變更。更新設定的生效時間取決於您所做的更新，以及索引中的搜尋查詢數目。Amazon Kendra 在您變更設定後或套用[封鎖清單](#)後，每 24 小時自動更新建議。

CLI

若要擷取查詢建議

```
aws kendra get-query-suggestions \  
  --index-id index-id \  
  --query-text "query-text" \  
  --suggestion-types '["QUERY"]' \  
  --max-suggestions-count 1 // If you want to limit the number of suggestions
```

若要更新查詢建議

例如，若要變更查詢記錄檔時間範圍以及必須搜尋查詢的次數下限：

```
aws kendra update-query-suggestions-config \  
  --index-id index-id \  
  --query-log-look-back-window-in-days 30 \  
  --minimum-query-count 100
```

Python

若要擷取查詢建議

```
import boto3
from botocore.exceptions import ClientError

kendra = boto3.client("kendra")

print("Get query suggestions.")

# Provide the index ID
index_id = "index-id"

# Provide the query text
query_text = "query"

# Provide the query suggestions type
query_suggestions_type = "QUERY"

# If you want to limit the number of suggestions
num_suggestions = 1

try:
    query_suggestions_response = kendra.get_query_suggestions(
        IndexId = index_id,
        QueryText = query_text,
        SuggestionTypes = query_suggestions_type,
        MaxSuggestionsCount = num_suggestions
    )

    # Print out the suggestions you received
    if ("Suggestions" in query_suggestions_response.keys()) {
        for (suggestion: query_suggestions_response["Suggestions"]) {
            print(suggestion["Value"]["Text"]["Text"]);
        }
    }

except ClientError as e:
    print("%s" % e)

print("Program ends.")
```

若要更新查詢建議

例如，若要變更查詢記錄檔時間範圍以及必須搜尋查詢的次數下限：


```
import boto3
from botocore.exceptions import ClientError
import pprint
import time

kendra = boto3.client("kendra")

print("Updating query suggestions settings/configuration for an index.")

# Provide the index ID
index_id = "index-id"

# Configure the settings you want to update
minimum_query_count = 100
query_log_look_back_window_in_days = 30

try:
    kendra.update_query_suggestions_config(
        IndexId = index_id,
        MinimumQueryCount = minimum_query_count,
        QueryLogLookBackWindowInDays = query_log_look_back_window_in_days
    )

    print("Wait for Amazon Kendra to update the query suggestions.")

    while True:
        # Get query suggestions description of settings/configuration
        query_sugg_config_response = kendra.describe_query_suggestions_config(
            IndexId = index_id
        )

        # If status is not UPDATING, then quit
        status = query_sugg_config_response["Status"]
        print(" Updating query suggestions config. Status: " + status)
        if status != "UPDATING":
            break
        time.sleep(60)

except ClientError as e:
    print("%s" % e)

print("Program ends.")
```

清除建議，同時保留查詢歷史

您可以使用 [ClearQuerySuggestions](#) API 清除查詢建議。清除建議只會刪除現有的查詢建議，而不會刪除查詢歷史記錄中的查詢。當您清除建議時，Amazon Kendra 會根據您清除建議之後新增至查詢記錄檔的新查詢來學習新建議。

CLI

若要清除查詢建議

```
aws kendra clear-query-suggestions \  
  --index-id index-id
```

Python

若要清除查詢建議

```
import boto3  
from botocore.exceptions import ClientError  
  
kendra = boto3.client("kendra")  
  
print("Clearing out query suggestions for an index.")  
  
# Provide the index ID  
index_id = "index-id"  
  
try:  
    kendra.clear_query_suggestions(  
        IndexId = index_id  
    )  
  
    # Confirm last cleared date-time and that there are no suggestions  
    query_sugg_config_response = kendra.describe_query_suggestions_config(  
        IndexId = index_id  
    )  
    print("Query Suggestions last cleared at: " +  
          str(query_sugg_config_response["LastClearTime"]));  
    print("Number of suggestions available from the time of clearing: " +  
          str(query_sugg_config_response["TotalSuggestionsCount"]));  
  
except ClientError as e:
```

```
print("%s" % e)

print("Program ends.")
```

沒有可用的建議

如果您沒有看到查詢的建議，可能是下列其中一個原因：

- 索引中沒有足夠的查詢可 Amazon Kendra 供學習。
- 您的查詢建議設定過於嚴格，導致大部分的查詢都會從建議中篩選掉。
- 您最近清除了建議，Amazon Kendra 仍然需要時間來累積新的查詢才能學習新的建議。

您可以使用 [DescribeQuerySuggestionsConfig](#) API 檢查您目前的設定。

使用文件欄位查詢建議

主題

- [選取建議欄位的設定](#)
- [文件欄位中的使用者控制](#)

您可以選擇根據文件欄位的內容建議與使用者相關的查詢。您可以使用文件欄位中包含的資訊來自動完成查詢，而不是使用查詢歷史記錄來建議其他常用的相關查詢。Amazon Kendra 會在設定為 Suggestable 且與使用者查詢密切符合的欄位中尋找相關內容。然後，在您的用戶開始輸入查詢時向用戶 Amazon Kendra 建議此內容。

例如，如果您指定要基於建議的標題字段，並且用戶開始輸入查詢「如何使用 Amazon ken...」，最相關的標題「如何 Amazon Kendra 工作」可以建議自動完成搜索。用戶看到「如何 Amazon Kendra 工作」直接出現在他們的搜索欄下方，自動完成他們的搜索查詢。用戶選擇此查詢建議，並在搜索結果中返回「如何 Amazon Kendra 工作」文檔。

您可以使用 String 和 StringList 類型的任何文件欄位的內容來建議查詢，方法是將欄位設定 Suggestable 為做為欄位組態的一部分，以取得查詢建議。您也可以使用 [封鎖清單](#)，讓包含特定字詞或片語的建議文件欄位不會向您的使用者顯示。您可以使用一個封鎖清單。無論您是將查詢建議設定為使用查詢歷史記錄還是文件欄位，封鎖清單都會套用。

選取建議欄位的設定

您可以設定下列設定，以便使用 [AttributeSuggestionsConfig](#) 和呼叫

[UpdateQuerySuggestionsConfig](#) API 來更新索引層級的設定來選取建議的文件欄位：

- 欄位/屬性建議模式 — 使用文件欄位的查詢建議為或。ACTIVE INACTIVE Amazon Kendra 預設會啟用查詢建議。
- 可建@@ 欄位/屬性 — 欄位名稱或欄位鍵，以建議為基礎。這些欄位必須設定 TRUE 為 Suggestable，作為欄位組態的一部分。您可以在查詢級別覆蓋字段配置，同時保持索引級別的配置。使用 [GetQuerySuggestions](#) API [AttributeSuggestionConfig](#) 在查詢層級進行變更。這個查詢層級的設定對於快速嘗試使用不同的文件欄位非常有用，而不必在索引層級更新組態。
- 其他欄位/屬性 — 您要包含在查詢建議回應中的其他欄位。這些欄位用於在回應中提供額外資訊；但是，它們不會用於建議的基礎。

Warning

您對設定所做的變更可能不會立即生效。您可以使用 [DescribeQuerySuggestionsConfig](#) API 追蹤設定變更。更新的設定生效的時間取決於您所做的更新。Amazon Kendra 在您變更設定後或套用 [封鎖清單](#) 後，每 24 小時自動更新建議。

CLI

在查詢層級擷取查詢建議並覆寫文件欄位組態，而不必在索引層級變更組態。

```
aws kendra get-query-suggestions \  
  --index-id index-id \  
  --query-text "query-text" \  
  --suggestion-types '["DOCUMENT_ATTRIBUTES"]' \  
  --attribute-suggestions-config '{"SuggestionAttributes":["field/attribute key  
1", "field/attribute key 2"]', "AdditionalResponseAttributes":["response field/  
attribute key 1", "response field/attribute key 2"]}' \  
  --max-suggestions-count 1 // If you want to limit the number of suggestions
```

若要更新查詢建議

例如，要在索引級別更改文檔字段配置：

```
aws kendra update-query-suggestions-config \  

```

```
--index-id index-id \  
--attribute-suggestions-config '{"SuggestableConfigList": '[{"SuggestableConfig":  
  "_document_title", "Suggestable": true}]', "AttributeSuggestionsMode": "ACTIVE"}'
```

Python

在查詢層級擷取查詢建議並覆寫文件欄位組態，而不必在索引層級變更組態。

```
import boto3  
from botocore.exceptions import ClientError  
  
kendra = boto3.client("kendra")  
  
print("Get query suggestions.")  
  
# Provide the index ID  
index_id = "index-id"  
  
# Provide the query text  
query_text = "query"  
  
# Provide the query suggestions type  
query_suggestions_type = "DOCUMENT_ATTRIBUTES"  
  
# Override fields/attributes configuration at query level  
configuration = {"SuggestionAttributes":  
  ["field/attribute key 1", "field/attribute key 2"],  
  "AdditionalResponseAttributes":  
    ["response field/attribute key 1", "response field/attribute key 2"]  
}  
  
# If you want to limit the number of suggestions  
num_suggestions = 1  
  
try:  
    query_suggestions_response = kendra.get_query_suggestions(  
        IndexId = index_id,  
        QueryText = query_text,  
        SuggestionTypes = [query_suggestions_type],  
        AttributeSuggestionsConfig = configuration,  
        MaxSuggestionsCount = num_suggestions  
    )  
  
    # Print out the suggestions you received
```

```
    if ("Suggestions" in query_suggestions_response.keys()) {
        for (suggestion: query_suggestions_response["Suggestions"]) {
            print(suggestion["Value"]["Text"]["Text"]);
        }
    }

except ClientError as e:
    print("%s" % e)

print("Program ends.")
```

若要更新查詢建議

例如，要在索引級別更改文檔字段配置：

```
import boto3
from botocore.exceptions import ClientError
import pprint
import time

kendra = boto3.client("kendra")

print("Updating query suggestions settings/configuration for an index.")

# Provide the index ID
index_id = "index-id"

# Configure the settings you want to update at the index level
configuration = {"SuggestableConfigList":
    '[{"SuggestableConfig": "_document_title", "Suggestable": true}]',
    "AttributeSuggestionsMode": "ACTIVE"
}

try:
    kendra.update_query_suggestions_config(
        IndexId = index_id,
        AttributeSuggestionsConfig = configuration
    )

    print("Wait for Amazon Kendra to update the query suggestions.")

    while True:
        # Get query suggestions description of settings/configuration
        query_sugg_config_response = kendra.describe_query_suggestions_config(
```

```
        IndexId = index_id
    )

    # If status is not UPDATING, then quit
    status = query_sugg_config_response["Status"]
    print(" Updating query suggestions config. Status: " + status)
    if status != "UPDATING":
        break
    time.sleep(60)

except ClientError as e:
    print("%s" % e)

print("Program ends.")
```

文件欄位中的使用者控制

您可以將使用者前後關聯篩選套用至您要依據查詢建議的文件欄位。這會根據使用者或其對文件的群組存取權來篩選文件欄位資訊。例如，實習生會搜尋公司的入口網站，但無法存取絕密的公司文件。因此，根據絕密文件標題或任何其他可建議的欄位建議的查詢不會向實習生顯示。

您可以使用存取控制清單 (ACL) 為文件建立索引，以定義哪些使用者和群組被指派給哪些文件的存取權。然後，您可以將使用者內容篩選套用至您的文件欄位，以取得查詢建議。目前針對索引設定的使用者前後關聯篩選與套用至文件欄位的使用者前後關聯篩選相同，以進行查詢建議。使用者前後關聯篩選是文件欄位組態的一部分。您使用 [AttributeSuggestionsGetConfig](#) 並呼叫 [GetQuerySuggestions](#)。

封鎖建議中的某些查詢或文件欄位內容

封鎖清單會停 Amazon Kendra 止向使用者建議某些查詢。封鎖清單是您要從查詢建議中排除的字詞或片語清單。Amazon Kendra 排除包含封鎖清單中字詞或片語完全相符的查詢。

您可以使用封鎖清單來防範通常出現在查詢歷史記錄或文件欄位中且 Amazon Kendra 可以選取做為建議的冒犯性字詞或片語。封鎖清單也可以防 Amazon Kendra 止建議包含尚未準備好公開發行或公佈之資訊的查詢。例如，您的使用者經常會查詢有關潛在新產品的即將發行版本。但是，您不想建議該產品，因為您還沒有準備好發布它。您可以阻止包含產品名稱和建議產品信息的查詢。

您可以使用 [CreateQuerySuggestionsBlockList](#) API 為查詢建立封鎖清單。您可以將每個區塊字或片語放在文字檔案中的個別行上。然後，您將文字檔上傳到 Amazon S3 儲存貯體，並在中提供檔案的路徑或位置 Amazon S3。Amazon Kendra 目前僅支援建立一個封鎖清單。

您可以取代 Amazon S3 值區中封鎖字詞和片語的文字檔案。若要更新中的封鎖清單 Amazon Kendra，請使用 [UpdateQuerySuggestionsBlockListAPI](#)。

使用 [DescribeQuerySuggestionsBlockListAPI](#) 獲取阻止列表的狀態。

[DescribeQuerySuggestionsBlockList](#) 還可以為您提供其他有用的信息，例如：

- 上次更新封鎖清單的時間
- 目前封鎖清單中有多少字或片語
- 建立封鎖清單時有用的錯誤訊息

您也可以使用 [ListQuerySuggestionsBlockListsAPI](#) 取得索引的封鎖清單摘要清單。

若要刪除您的封鎖清單，請使用 [DeleteQuerySuggestionsBlockListAPI](#)。

您對封鎖清單的更新可能不會立即生效。您可以使用 [DescribeQuerySuggestionsBlockList API](#) 追蹤更新。

CLI

建立封鎖清單的步驟

```
aws kendra create-query-suggestions-block-list \  
  --index-id index-id \  
  --name "block-list-name" \  
  --description "block-list-description" \  
  --source-s3-path "Bucket=bucket-name,Key=query-suggestions/block_list.txt" \  
  --role-arn role-arn
```

更新封鎖清單的步驟

```
aws kendra update-query-suggestions-block-list \  
  --index-id index-id \  
  --name "new-block-list-name" \  
  --description "new-block-list-description" \  
  --source-s3-path "Bucket=bucket-name,Key=query-suggestions/new_block_list.txt" \  
  --role-arn role-arn
```

刪除封鎖清單的步驟

```
aws kendra delete-query-suggestions-block-list \  

```



```
--index-id index-id \  
--id block-list-id
```

Python

建立封鎖清單的步驟

```
import boto3  
from botocore.exceptions import ClientError  
import pprint  
import time  
  
kendra = boto3.client("kendra")  
  
print("Create a query suggestions block list.")  
  
# Provide a name for the block list  
block_list_name = "block-list-name"  
# Provide an optional description for the block list  
block_list_description = "block-list-description"  
# Provide the IAM role ARN required for query suggestions block lists  
block_list_role_arn = "role-arn"  
  
# Provide the index ID  
index_id = "index-id"  
  
s3_bucket_name = "bucket-name"  
s3_key = "query-suggestions/block_list.txt"  
source_s3_path = {  
    'Bucket': s3_bucket_name,  
    'Key': s3_key  
}  
  
try:  
    block_list_response = kendra.create_query_suggestions_block_list(  
        Description = block_list_description,  
        Name = block_list_name,  
        RoleArn = block_list_role_arn,  
        IndexId = index_id,  
        SourceS3Path = source_s3_path  
    )  
  
    print(block_list_response)
```

```

block_list_id = block_list_response["Id"]

print("Wait for Amazon Kendra to create the block list.")

while True:
    # Get block list description
    block_list_description = kendra.describe_query_suggestions_block_list(
        Id = block_list_id,
        IndexId = index_id
    )
    # If status is not CREATING, then quit
    status = block_list_description["Status"]
    print("Creating block list. Status: " + status)
    if status != "CREATING":
        break
    time.sleep(60)

except ClientError as e:
    print("%s" % e)

print("Program ends.")

```

更新封鎖清單的步驟

```

import boto3
from botocore.exceptions import ClientError
import pprint
import time

kendra = boto3.client("kendra")

print("Update a block list for query suggestions.")

# Provide the block list name you want to update
block_list_name = "new-block-list-name"
# Provide the block list description you want to update
block_list_description = "new-block-list-description"
# Provide the IAM role ARN required for query suggestions block lists
block_list_role_arn = "role-arn"

# Provide the block list ID
block_list_id = "block-list-id"
# Provide the index ID

```

```
index_id = "index-id"

s3_bucket_name = "bucket-name"
s3_key = "query-suggestions/new_block_list.txt"
source_s3_path = {
    'Bucket': s3_bucket_name,
    'Key': s3_key
}

try:
    kendra.update_query_suggestions_block_list(
        Id = block_list_id,
        IndexId = index_id,
        Description = block_list_description,
        Name = block_list_name,
        RoleArn = block_list_role_arn,
        SourceS3Path = source_s3_path
    )

    print("Wait for Amazon Kendra to update the block list.")

    while True:
        # Get block list description
        block_list_description = kendra.describe_query_suggestions_block_list(
            Id = block_list_id,
            IndexId = index_id
        )
        # If status is not UPDATING, then the update has finished
        status = block_list_description["Status"]
        print("Updating block list. Status: " + status)
        if status != "UPDATING":
            break
        time.sleep(60)

except ClientError as e:
    print("%s" % e)

print("Program ends.")
```

刪除封鎖清單的步驟

```
import boto3
from botocore.exceptions import ClientError
```

```
kendra = boto3.client("kendra")

print("Delete a block list for query suggestions.")

# provide the block list ID
query_suggestions_block_list_id = "query-suggestions-block-list-id"
# Provide the index ID
index_id = "index-id"

try:
    kendra.delete_query_suggestions_block_list(
        Id = query_suggestions_block_list_id,
        IndexId = index_id
    )

except ClientError as e:
    print("%s" % e)

print("Program ends.")
```

查詢拼字檢查

Amazon Kendra 拼字檢查程式會建議查詢的拼字校正。這可以幫助您將搜索結果的出現次數降至最低，並返回相關結果。您的使用者可能會從拼字錯誤的查詢中收到[零搜尋結果](#)，但沒有相符的結果或沒有傳回的文件。或者，您的使用者可能會從拼字錯誤的查詢收到[不相關的搜尋結果](#)。

拼字檢查程式旨在根據索引文件中出現的單字，以及更正的單字與拼錯的單字相符程度，建議更正錯誤的單字。例如，如果編製索引的文件中出現「陳述式」一詞，則這可能會與查詢「年終財務統計」中拼錯的「statments」字詞非常相符。

拼字檢查程式會傳回用來取代原始查詢文字中拼錯字詞的預期或更正文字。例如，「去除 kendre 搜尋」可能會傳回「部署 Kendra 搜尋」。您也可以使用 API 中提供的偏移位置，在前端應用程式中的查詢中反白顯示或斜體顯示傳回的更正字詞。在控制台中，默認情況下突出顯示或斜體更正的單詞。例如，「部署 Kendra 搜索」。

對於出現在索引文件中的企業特定或特殊字詞，拼字檢查程式不會將這些字詞誤解為查詢中的拼字錯誤。例如，「亞馬遜獼猴」未更正為「亞馬遜獼猴」。

對於以連字符連接的單字 (例如「年終」)，拼字檢查程式會將這些字詞視為個別單字來建議更正這些字詞。例如，「yaer-end」的建議修正可能是「年底」。

對於DOCUMENT和QUESTION_ANSWER查詢回應類型，拼字檢查程式會根據文件內文中的單字，建議對拼錯的單字進行更正。文件內文比標題更可靠，用於建議與拼錯字密切相符的更正。對於ANSWER查詢回應類型，拼字檢查程式會根據索引中預設問題和答案文件中的文字建議更正。

您可以使用[SpellCorrectionConfiguration](#)物件啟動拼字檢查程式。您設定IncludeQuerySpellCheckSuggestions為TRUE。默認情況下，控制台中的拼寫檢查器是激活的。默認情況下，它內置在控制台中。

拼字檢查器也可以針對多種語言的查詢建議拼字校正，而不僅僅是英文。如需拼字檢查程式支援的語言清單，請參閱[Amazon Kendra 支援的語言](#)。

使用具有預設限制的查詢拼字檢查程式

拼字檢查器設計有特定的預設值或限制。以下是當您啟動拼字校正建議時所套用的目前限制清單。

- 對於長度少於三個字元或超過 30 個字元的單字，則無法傳回建議的拼字更正。若要允許超過 30 個字元或少於三個字元，請聯絡 Sup [port](#) 部門。
- 建議的拼字更正無法根據使用者存取控制或您的使用[者內容篩選](#)存取控制清單來限制建議。拼字校正正是以索引文件中的所有字詞為基礎，無論文字是否限於特定使用者。如果您想避免某些單詞出現在建議的查詢拼寫更正中，請不要激活SpellCorrectionConfiguration。
- 對於包含數字的單字，則無法傳回建議的拼字校正。例如，「如何 2 不是 br8k unbun2」。
- 建議的拼字校正無法使用未出現在索引文件中的單字。
- 建議的拼字校正無法使用經常在編製索引文件中經常使用低於 0.01% 的單字。若要變更 0.01% 閾值，請聯絡 Sup [port](#) 部門。

篩選和平面搜尋

您可以使用篩選器改善[查詢](#) API 的搜尋結果或回應。篩選器會將回應中的文件限制為直接套用至查詢的文件。若要建立多面向搜尋建議，請使用布林邏輯從回應或不符合特定條件的文件中篩選出特定文件屬性。您可以使用 Query API 中的Facets參數來指定刻面。

若要搜尋已編製索引的文件 Amazon Lex，Amazon Kendra 請使用 [AMAZON.KendraSearchIntent](#)。如需 Amazon Kendra 使用配置的範例 Amazon Lex，請參閱[建立 Amazon Kendra 索引的常見問題集機器人](#)。您也可以使用提供回應的篩選器[AttributeFilter](#)。這是配置時 JSON 中的查詢過濾器AMAZON.KendraSearchIntent。若要在主控台中設定搜尋意圖時提供屬性篩選器，請前任意圖編輯器，然後選擇 Amazon Kendra 查詢以 JSON 提供查詢篩選器。如需相關資訊AMAZON.KendraSearchIntent，請參閱[Amazon Lex 文件指南](#)。

面向

Facet 是一組搜尋結果的範圍檢視。例如，您可以為世界各地的城市提供搜尋結果，文件會根據與其關聯的特定城市進行篩選。或者，您可以建立刻面以顯示特定作者的結果。

您可以使用與文件相關聯的文件屬性或中繼資料欄位做為 Facet，以便您的使用者可以依該 Facet 中的類別或值進行搜尋。您還可以在搜索結果中顯示嵌套 Facet，以便您的用戶不僅可以按類別或字段進行搜索，還可以通過子類別或子字段進行搜索。

下列範例顯示如何取得「城市」自訂屬性的 Facet 資訊。

```
response=kendra.query(  
    QueryText = query,  
    IndexId = index,  
    Facets = [  
        {  
            "DocumentAttributeKey" : "City"  
        }  
    ]  
)
```

您可以使用巢狀刻面來進一步縮小搜尋範圍。例如，文件屬性或多面「城市」包含稱為「西雅圖」的值。此外，文件屬性或 Facet "CityRegion" 包括指派給「西雅圖」之文件的「北」與「南」值。您可以在搜尋結果中顯示巢狀 Facet 及其計數，以便不僅可以依城市搜尋文件，還可以依城市內的區域搜尋文件。

請注意，巢狀 Facet 可能會影響查詢延遲。一般規則是您使用的巢狀 Facet 越多，對延遲的潛在影響就越大。影響延遲的其他因素包括索引文件的平均大小、索引的大小、高度複雜的查詢，以及 Amazon Kendra 引的整體負載。

下列範例顯示如何取得 "CityRegion" 自訂屬性的 Facet 資訊，做為「City」內的巢狀 Facet。

```
response=kendra.query(  
    QueryText = query,  
    IndexId = index,  
    Facets = [  
        {  
            "DocumentAttributeKey" : "City",  
            "Facets": [  
                {  
                    "DocumentAttributeKey" : "CityRegion"  
                }  
            ]  
        }  
    ]  
)
```

```
    ]
  }
]
)
```

Facet 資訊 (例如文件計數) 會在回 FacetResults 應陣列中傳回。您可以使用內容在應用程式中顯示多面搜尋建議。例如，如果文件屬性「City」包含可套用搜尋的城市，請使用該資訊來顯示城市搜尋清單。用戶可以選擇一個城市來過濾他們的搜索結果。若要進行多面搜尋，請呼叫 [Query API](#)，並使用選擇的文件屬性來篩選結果。

查詢的每個 Facet 最多可以顯示 10 個 Facet 值，而一個多面內只能顯示一個巢狀 Facet。如果您想要提高這些限制，請聯絡 [Support](#) 部門。如果您想要將每個 Facet 值的數目限制為小於 10，您可以在物件中指定此值。Facet

下列範例 JSON 回應顯示範圍為「城市」文件屬性的方面。回應包括 Facet 值的文件計數。

```
{
  'FacetResults': [
    {
      'DocumentAttributeKey': 'City',
      'DocumentAttributeValueCountPairs': [
        {
          'Count': 3,
          'DocumentAttributeValue': {
            'StringValue': 'Dubai'
          }
        },
        {
          'Count': 3,
          'DocumentAttributeValue': {
            'StringValue': 'Seattle'
          }
        },
        {
          'Count': 1,
          'DocumentAttributeValue': {
            'StringValue': 'Paris'
          }
        }
      ]
    }
  ]
}
```

您也可以顯示巢狀 Facet (例如城市中的區域) 的刻面資訊，以進一步篩選搜尋結果。

下列範例 JSON 回應顯示範圍為 "CityRegion" 文件屬性的 Facet，做為「City」內的巢狀 Facet。回應包括巢狀 Facet 值的文件計數。

```
{
  'FacetResults': [
    {
      'DocumentAttributeKey': 'City',
      'DocumentAttributeValueCountPairs': [
        {
          'Count': 3,
          'DocumentAttributeValue': {
            'StringValue': 'Dubai'
          },
          'FacetResults': [
            {
              'DocumentAttributeKey': 'CityRegion',
              'DocumentAttributeValueCountPairs': [
                {
                  'Count': 2,
                  'DocumentAttributeValue': {
                    'StringValue': 'Bur Dubai'
                  }
                },
                {
                  'Count': 1,
                  'DocumentAttributeValue': {
                    'StringValue': 'Deira'
                  }
                }
              ]
            }
          ]
        }
      ],
    },
    {
      'Count': 3,
      'DocumentAttributeValue': {
        'StringValue': 'Seattle'
      },
      'FacetResults': [
        {
          'DocumentAttributeKey': 'CityRegion',
          'DocumentAttributeValueCountPairs': [
```



```

        {
            'Count': 1,
            'DocumentAttributeValue': {
                'StringValue': 'North'
            }
        },
        {
            'Count': 2,
            'DocumentAttributeValue': {
                'StringValue': 'South'
            }
        }
    ]
}
],
},
{
    'Count': 1,
    'DocumentAttributeValue': {
        'StringValue': 'Paris'
    },
    'FacetResults': [
        {
            'DocumentAttributeKey': 'CityRegion',
            'DocumentAttributeValueCountPairs': [
                {
                    'Count': 1,
                    'DocumentAttributeValue': {
                        'StringValue': 'City center'
                    }
                }
            ]
        }
    ]
}
]
}
]
}
}

```

當您使用字串清單欄位建立 Facet 時，傳回的 Facet 結果會根據字串清單的內容而定。例如，如果您有一個包含兩個項目的字符串列表字段，其中一個包含「臘腸犬」，「香腸狗」列表和一個值為「赫斯基」，則可以獲得 FacetResults 三個方面。

如需詳細資訊，請參閱 [查詢回應和回應類型](#)。

使用文件屬性篩選搜尋結果

依預設，Query會傳回所有搜尋結果。若要篩選回應，您可以對文件屬性執行邏輯作業。例如，如果您只想要特定城市的文件，您可以篩選「城市」和「州/省」自訂文件屬性。您可[AttributeFilter](#)以使用在您提供的篩選器上建立布林運算。

大多數屬性都可用來篩選所有回[應類型](#)的回應。不過，此_excerpt_page_number屬性只適用於篩選回應時的回ANSWER應類型。

下列範例顯示如何透過篩選特定城市 (西雅圖) 和華盛頓州，來執行邏輯 AND 作業。

```
response=kendra.query(
    QueryText = query,
    IndexId = index,
    AttributeFilter = {'AndAllFilters':
        [
            {"EqualsTo": {"Key": "City","Value": {"StringValue": "Seattle"}}},
            {"EqualsTo": {"Key": "State","Value": {"StringValue": "Washington"}}}
        ]
    }
)
```

下列範例會示範如何在任何Fileformat、Author或SourceURI索引鍵符合指定值時執行邏輯 OR 作業。

```
response=kendra.query(
    QueryText = query,
    IndexId = index,
    AttributeFilter = {'OrAllFilters':
        [
            {"EqualsTo": {"Key": "Fileformat","Value": {"StringValue":
" AUTO_DETECT"}}},
            {"EqualsTo": {"Key": "Author","Value": {"StringValue": "Ana
Carolina"}}},
            {"EqualsTo": {"Key": "SourceURI","Value": {"StringValue": "https://
aws.amazonaws.com/234234242342"}}}
        ]
    }
)
```

對於StringList欄位，請使用ContainsAny或ContainsAll屬性篩選器來傳回具有指定字串的文件。下列範例顯示如何傳回其Locations自訂屬性中具有「Seattle」或「Portland」值的所有文件。

```
response=kendra.query(  
    QueryText = query,  
    IndexId = index,  
    AttributeFilter = {  
        "ContainsAny": { "Key": "Locations", "Value": { "StringListValue":  
[ "Seattle", "Portland" ] }}  
    }  
)
```

篩選搜尋結果中每個文件的屬性

Amazon Kendra 會傳回搜尋結果中每個文件的文件屬性。您可以篩選要包含在回應中作為搜尋結果一部分的某些文件屬性。依預設，指派給文件的所有文件屬性都會在回應中傳回。

在下列範例中，只有_source_uri和_author文件屬性會包含在文件的回應中。

```
response=kendra.query(  
    QueryText = query,  
    IndexId = index,  
    RequestedDocumentAttributes = ["_source_uri", "_author"]  
)
```

篩選使用者內容

您可以根據使用者或使用者對文件的群組存取權來篩選使用者的搜尋結果。您可以使用使用者權杖、使用者 ID 或使用者屬性來篩選文件。Amazon Kendra 也可以將使用者對應至其群組。您可以選擇用 AWS IAM Identity Center 作身分存放區/來源。

使用者前後關聯篩選是一種個人化搜尋，具有控制文件存取權的好處。例如，並非所有在公司入口網站中搜尋資訊的團隊都應該存取絕密的公司文件，這些文件也不應該與所有使用者相關。只有具備絕密文件存取權的特定使用者或專案團隊群組才能在搜尋結果中看到這些文件。

將文件編入索引時 Amazon Kendra，大多數文件都會擷取對應的存取控制清單 (ACL)。ACL 指定允許或拒絕存取文件的使用者名稱和群組名稱。沒有 ACL 的文件是公開文件。

Amazon Kendra 可以為大多數資料來源擷取與每個文件相關聯的使用者或群組資訊。例如，Quip 中的文檔可以包含具有文檔訪問權限的選擇用戶的「共享」列表。如果您使用 S3 儲存貯體做為資料來源，

則為 ACL 提供 [JSON 檔案](#)，並將此檔案的 S3 路徑納入資料來源組態的一部分。如果您直接將文件新增至索引，您可以將[主參與者](#)物件中的 ACL 指定為 [BatchPutDocument](#) API 中文件物件的一部分。

您可以使用 [CreateAccessControlConfiguration](#) API 重新設定現有文件層級存取控制，而無需再次編製所有文件的索引。例如，您的索引包含只有特定員工或使用者應存取的絕密公司文件。其中一位使用者離開公司或切換至應封鎖的小組，無法存取絕密文件。使用者仍然可以存取絕密文件，因為使用者可以存取您的文件先前已編製索引。您可以為具有拒絕存取權的使用者建立特定的存取控制組態。您可以稍後更新存取控制組態，以便在使用者返回公司並重新加入「絕密」小組的情況下允許存取。您可以在情況變更時重新設定文件的存取控制。

若要將存取控制設定套用至特定文件，請呼叫 `AccessControlConfigurationId` 包含在 [Document](#) 物件中的 [BatchPutDocument](#) API。如果您使用 S3 儲存貯體做為資料來源，請使用資料來源 `.metadata.json` 源更新 `AccessControlConfigurationId` 並同步處理資料來源。Amazon Kendra 目前僅支援 S3 資料來源和使用 `BatchPutDocument` API 編製索引的文件的存取控制組態。

按用戶令牌過濾

當您查詢索引時，您可以使用使用者權杖，根據使用者或他們對文件的群組存取權來篩選搜尋結果。當您發出查詢時，Amazon Kendra 擷取和驗證 Token、提取並檢查使用者和群組資訊，然後執行查詢。傳回使用者可存取的所有文件 (包括公用文件)。如需詳細資訊，請參閱以[權杖為基礎的使用者存取控制](#)。

您可以在 [UserContext](#) 對象中提供用戶令牌，並在 [查詢](#) API 中傳遞此令牌。

以下說明如何包含使用者權杖。

```
response = kendra.query(  
    QueryText = query,  
    IndexId = index,  
    UserToken = {  
        Token = "token"  
    })
```

您可以將使用者對應至群組。當您使用使用者內容篩選時，在您發出查詢時，不需要包含使用者所屬的所有群組。使用 [PutPrincipalMapping](#) API，您可以將使用者對應至其群組。如果您不想使用 `PutPrincipalMapping` API，則必須在發出查詢時提供使用者名稱和使用者所屬的所有群組。您也可以使用 [UserGroupResolutionConfiguration](#) 物件擷取 IAM 身分中心身分識別來源中群組和使用者的存取層級。

依使用者 ID 和群組篩選

當您查詢索引時，您可以使用使用者 ID 和群組，根據使用者或他們對文件的群組存取權來篩選搜尋結果。當您發出查詢時，請 Amazon Kendra 檢查使用者和群組資訊並執行查詢。系統會傳回與使用者可存取之查詢相關的所有文件 (包括公用文件)。

您也可以依使用者和群組可存取的資料來源篩選搜尋結果。如果群組與多個資料來源相關聯，但您只希望群組存取特定資料來源的文件，則指定資料來源非常有用。例如，組「研究」，「工程」和「銷售和營銷」都綁定到存儲在數據源匯流和 Salesforce 公司的文檔。不過，「銷售與行銷」團隊只需要存取儲存在 Salesforce 中的客戶相關文件。因此，當銷售和行銷使用者搜尋與客戶相關的文件時，他們可以在搜尋結果中看到 Salesforce 的文件。不從事銷售和行銷工作的使用者在搜尋結果中看不到 Salesforce 文件。

您可以在 [UserContext](#) 物件中提供使用者、群組和資料來源資訊，並在 [Query](#) API 中傳遞此資訊。使用者 ID、群組和資料來源清單應與您在 [Principle](#) 物件中指定的名稱相符，以識別使用者、群組和資料來源。透過 [Principal](#) 物件，您可以將使用者、群組或資料來源新增至用於存取文件的允許清單或拒絕清單。

您必須提供下列其中一項：

- 使用者和群組資訊，以及 (選用) 資料來源資訊。
- 如果您使用 [PutPrincipalMapping](#) API 將使用者對應至群組和資料來源，則只有使用者資訊。您也可以使用 [UserGroupResolutionConfiguration](#) 物件擷取 IAM 身分中心身分識別來源中群組和使用者的存取層級。

如果查詢中未包含此資訊，則會 Amazon Kendra 傳回所有文件。如果您提供此資訊，則只會傳回具有相符使用者 ID、群組和資料來源的文件。

以下說明如何包含使用者 ID、群組和資料來源。

```
response = kendra.query(  
    QueryText = query,  
    IndexId = index,  
    UserId = {  
        UserId = "user1"  
    },  
    Groups = {  
        Groups = ["Sales and Marketing"]  
    },  
    DataSourceGroups = {
```

```
DataSourceGroups = [{"DataSourceId" : "SalesforceCustomerDocsGroup", "GroupId":  
"Sales and Marketing"}]  
})
```

依使用者屬性篩選

當您查詢索引時，您可以使用內建屬性，`_user_id`並根據`_group_id`使用者及其對文件的群組存取權來篩選搜尋結果。您最多可以設定 100 個群組識別碼。當您發出查詢時，請 Amazon Kendra 檢查使用者和群組資訊並執行查詢。系統會傳回與使用者有權存取之查詢相關的所有文件 (包括公用文件)。

您可以在 [AttributeFilter](#) 物件中提供使用者和群組屬性，並在 [查詢](#) API 中傳遞此屬性。

下列範例會顯示根據使用者識別碼以及使用者所屬群組「HR」和「IT」群組來篩選查詢回應的要求。查詢會傳回允許清單中具有使用者或「HR」或「IT」群組的任何文件。如果使用者或其中一個群組位於文件的拒絕清單中，則不會傳回文件。

```
response = kendra.query(  
    QueryText = query,  
    IndexId = index,  
    AttributeFilter = {  
        "OrAllFilters": [  
            {  
                "EqualsTo": {  
                    "Key": "_user_id",  
                    "Value": {  
                        "StringValue": "user1"  
                    }  
                }  
            },  
            {  
                "EqualsTo": {  
                    "Key": "_group_ids",  
                    "Value": {  
                        "StringListValue": ["HR", "IT"]  
                    }  
                }  
            }  
        ]  
    }  
)
```

您也可以指定群組可以在 [Principal](#) 物件中存取的資料來源。

Note

使用者內容篩選不是內容的驗證或授權控制項。它不會對發送到 Query API 的用戶和組進行用戶身份驗證。這取決於您的應用程式，以確保發送到 Query API 的用戶和組信息經過身份驗證和授權。

每個資料來源都有使用者內容篩選的實作。以下部分描述了每個實現。

主題

- [直接新增至索引的文件的使用者前後關聯篩選](#)
- [常見問題集的使用者內容篩選](#)
- [資料來源的使用者內容篩選](#)

直接新增至索引的文件的使用者前後關聯篩選

當您使用 [BatchPutDocument](#) API 直接將文件新增至索引時，Amazon Kendra 會從文件的 `AccessControlList` 欄位中取得使用者和群組資訊。您為文件提供存取控制清單 (ACL)，且 ACL 會隨您的文件一併擷取。

您可以在 [主參與者](#) 物件中指定 ACL 做為 `BatchPutDocument` API 中 [文件物件](#) 的一部分。您提供下列資訊：

- 使用者或群組應具有的存取權。你可以說 `ALLOW` 或 `DENY`。
- 實體的類型。你可以說 `USER` 或 `GROUP`。
- 使用者或群組的名稱。

您最多可以在 `AccessControlList` 欄位中新增 200 個項目。

常見問題集的使用者內容篩選

當您將 [常見問題集](#) 新增至索引時，Amazon Kendra 會從常見問題 JSON 檔案的 `AccessControlList` 物件/欄位取得使用者和群組資訊。您也可以使用具有自訂欄位或屬性的常見問題解答 CSV 檔案進行存取控制。

您提供下列資訊：

- 使用者或群組應具有的存取權。你可以說 `ALLOW` 或 `DENY`。

- 實體的類型。你可以說USER或GROUP。
- 使用者或群組的名稱。

如需詳細資訊，請參閱 [FAQ 檔案](#)。

資料來源的使用者內容篩選

Amazon Kendra 也會從支援的資料來源連接器編目使用者和群組存取控制清單 (ACL) 資訊。這對於使用者前後關聯篩選非常有用，其中搜尋結果會根據使用者或他們對文件的群組存取權進行篩選。

主題

- [Adobe 體驗管理員資料來源的使用者內容篩選](#)
- [適用於露天資料來源的使用者內容篩選](#)
- [Aurora \(MySQL\) 資料來源的使用者內容篩選](#)
- [Aurora \(PostgreSQL\) 資料來源的使用者內容篩選](#)
- [Amazon FSx 資料來源的使用者內容篩選](#)
- [資料庫資料來源的使用者內容篩選](#)
- [Amazon RDS \(Microsoft SQL 伺服器\) 資料來源的使用者內容篩選](#)
- [Amazon RDS \(MySQL\) 資料來源的使用者內容篩選](#)
- [Amazon RDS \(Oracle\) 資料來源的使用者內容篩選](#)
- [Amazon RDS \(PostgreSQL\) 資料來源的使用者內容篩選](#)
- [Amazon S3 資料來源的使用者內容篩選](#)
- [Amazon WorkDocs 資料來源的使用者內容篩選](#)
- [Box 資料來源的使用者內容篩選](#)
- [匯流資料來源的使用者內容篩選](#)
- [Dropbox 資料來源的使用者上下文篩選](#)
- [Drupal 數據源的用戶上下文過濾](#)
- [GitHub 資料來源的使用者內容篩選](#)
- [Gmail 資料來源的使用者內容篩選](#)
- [Google 雲端硬碟資料來源的使用者內容篩選](#)
- [IBM DB2 資料來源的使用者內容篩選](#)
- [Jira 資料來源的使用者內容篩選](#)

- [Microsoft 交換資料來源的使用者內容篩選](#)
- [Microsoft OneDrive 資料來源的使用者內容篩選](#)
- [Microsoft OneDrive 2.0 資料來源的使用者內容篩選](#)
- [Microsoft SharePoint 資料來源的使用者內容篩選](#)
- [Microsoft SQL 伺服器資料來源的使用者內容篩選](#)
- [Microsoft 團隊資料來源的使用者內容篩選](#)
- [Microsoft Yammer 資料來源的使用者內容篩選](#)
- [MySQL 資料來源的使用者內容篩選](#)
- [Oracle 資料庫資料來源的使用者內容篩選](#)
- [PostgreSQL 資料來源的使用者內容篩選](#)
- [Quip 資料來源的使用者內容篩選](#)
- [Salesforce 資料來源的使用者內容篩選](#)
- [ServiceNow 資料來源的使用者內容篩選](#)
- [Slack 資料來源的使用者內容篩選](#)
- [Zendesk 資料來源的使用者內容篩選](#)

Adobe 體驗管理員資料來源的使用者內容篩選

當您使用 Adobe 體驗管理員資料來源時，Amazon Kendra 會從 Adobe 體驗管理員實例取得使用者和群組資訊。

群組和使用者 ID 的對應方式如下：

- `_group_ids` 群組 ID 存在於具有設定存取權限的 Adobe 體驗管理員內容中。它們會從 Adobe 體驗管理員中的群組名稱對應而來。
- `_user_id` 使用者 ID 存在於具有設定存取權限的 Adobe 體驗管理員內容中。它們會從使用者電子郵件對應為 Adobe 體驗管理員中的 ID。

您最多可以在 `AccessControlList` 欄位中新增 200 個項目。

適用於露天資料來源的使用者內容篩選

當您使用 Alfresco 資料來源時，Amazon Kendra 會從 Alfresco 執行個體取得使用者和群組資訊。

群組和使用者 ID 的對應方式如下：

- `_group_ids`在有設置訪問權限的文件上，Alfresco 中存在組 ID。它們是從 Alfresco 中組的系統名稱（而不是顯示名稱）映射的。
- `_user_id`用戶 ID 存在於 Alfresco 中，存在於有設置訪問權限的文件上。它們從用戶電子郵件中映射為 Alfresco 中的 ID。

您最多可以在 `AccessControlList` 欄位中新增 200 個項目。

Aurora (MySQL) 資料來源的使用者內容篩選

當您使用 Aurora (MySQL) 資料來源時，Amazon Kendra 會從來源資料表中的資料行取得使用者和群組資訊。您可以在主控台中指定此欄，或使用 [TemplateConfiguration](#) 物件做為 [CreateDataSourceAPI](#) 的一部分。

Aurora (MySQL) 資料庫資料來源有以下限制：

- 您只能指定資料庫資料來源的允許清單。您無法指定拒絕清單。
- 您只能指定群組。您無法為允許清單指定個別使用者。
- 資料庫欄應該是包含以分號分隔的群組清單的字串。

Aurora (PostgreSQL) 資料來源的使用者內容篩選

當您使用 Aurora (PostgreSQL) 資料來源時，Amazon Kendra 會從來源資料表中的資料行取得使用者和群組資訊。您可以在主控台中指定此欄，或使用 [TemplateConfiguration](#) 物件做為 [CreateDataSourceAPI](#) 的一部分。

A Aurora (PostgreSQL) 資料庫資料來源具有下列限制：

- 您只能指定資料庫資料來源的允許清單。您無法指定拒絕清單。
- 您只能指定群組。您無法為允許清單指定個別使用者。
- 資料庫欄應該是包含以分號分隔的群組清單的字串。

Amazon FSx 資料來源的使用者內容篩選

使用 Amazon FSx 資料來源時，Amazon Kendra 會從 Amazon FSx 執行個體的目錄服務取得使用者和群組資訊。

群 Amazon FSx 組和使用者 ID 對應如下：

- `_group_ids` 群組 ID 存在 Amazon FSx 於具有設定存取權限的檔案中。它們會從的目錄服務中的系統群組名稱對應 Amazon FSx。
- `_user_id` 使用者 ID 存在 Amazon FSx 於具有設定存取權限的檔案中。它們會從的目錄服務中的系統使用者名稱對應 Amazon FSx。

您最多可以在 `AccessControlList` 欄位中新增 200 個項目。

資料庫資料來源的使用者內容篩選

當您使用資料庫資料來源時，例如 Amazon Aurora PostgreSQL，Amazon Kendra 會從來源資料表中的資料行取得使用者和群組資訊。您可以在 [AclConfiguration](#) 物件中將此欄指定為 [CreateDataSource](#) API 中 [DatabaseConfiguration](#) 物件的一部分。

資料庫資料來源有下列限制：

- 您只能指定資料庫資料來源的允許清單。您無法指定拒絕清單。
- 您只能指定群組。您無法為允許清單指定個別使用者。
- 資料庫欄應該是包含以分號分隔的群組清單的字串。

Amazon RDS (Microsoft SQL 伺服器) 資料來源的使用者內容篩選

當您使用 Amazon RDS (Microsoft SQL Server) 資料來源時，Amazon Kendra 會從來源資料表中的資料行取得使用者和群組資訊。您可以在主控台中指定此欄，或使用 [TemplateConfiguration](#) 物件做為 [CreateDataSource](#) API 的一部分。

A Amazon RDS (Microsoft SQL 服務器) 數據庫數據源具有以下限制：

- 您只能指定資料庫資料來源的允許清單。您無法指定拒絕清單。
- 您只能指定群組。您無法為允許清單指定個別使用者。
- 資料庫欄應該是包含以分號分隔的群組清單的字串。

Amazon RDS (MySQL) 資料來源的使用者內容篩選

當您使用 Amazon RDS (MySQL) 資料來源時，Amazon Kendra 會從來源資料表中的資料行取得使用者和群組資訊。您可以在主控台中指定此欄，或使用 [TemplateConfiguration](#) 物件做為 [CreateDataSource](#) API 的一部分。

Amazon RDS (MySQL) 資料庫資料來源有以下限制：

- 您只能指定資料庫資料來源的允許清單。您無法指定拒絕清單。
- 您只能指定群組。您無法為允許清單指定個別使用者。
- 資料庫欄應該是包含以分號分隔的群組清單的字串。

Amazon RDS (Oracle) 資料來源的使用者內容篩選

使用 Amazon RDS (Oracle) 資料來源時，Amazon Kendra 會從來源表格中的欄取得使用者和群組資訊。您可以在主控台中指定此欄，或使用 [TemplateConfiguration](#) 物件做為 [CreateDataSource](#) API 的一部分。

Amazon RDS (Oracle) 資料庫資料來源有下列限制：

- 您只能指定資料庫資料來源的允許清單。您無法指定拒絕清單。
- 您只能指定群組。您無法為允許清單指定個別使用者。
- 資料庫欄應該是包含以分號分隔的群組清單的字串。

Amazon RDS (PostgreSQL) 資料來源的使用者內容篩選

當您使用 Amazon RDS (PostgreSQL) 資料來源時，Amazon Kendra 會從來源資料表中的資料行取得使用者和群組資訊。您可以在主控台中指定此欄，或使用 [TemplateConfiguration](#) 物件做為 [CreateDataSource](#) API 的一部分。

A Amazon RDS (PostgreSQL) 資料庫資料來源具有下列限制：

- 您只能指定資料庫資料來源的允許清單。您無法指定拒絕清單。
- 您只能指定群組。您無法為允許清單指定個別使用者。
- 資料庫欄應該是包含以分號分隔的群組清單的字串。

Amazon S3 資料來源的使用者內容篩選

您可以使用與文件關聯的中繼 Amazon S3 資料檔案，將使用者前後關聯篩選新增至資料來源中的文件。您可以將資訊新增至 JSON 文件中的 `AccessControlList` 欄位。如需將中繼資料新增至從 Amazon S3 料來源編製索引的文件的詳細資訊，請參閱 [S3 文件中繼資料](#)。

您提供三項資訊：

- 該實體應具有的訪問權限。你可以說 ALLOW 或 DENY。

- 實體的類型。你可以說USER或GROUP。
- 實體的名稱。

您最多可以在AccessControlList欄位中新增 200 個項目。

Amazon WorkDocs 資料來源的使用者內容篩選

使用 Amazon WorkDocs 資料來源時，Amazon Kendra 會從 Amazon WorkDocs 執行個體取得使用者和群組資訊。

群組和使用者 ID 對應如下：

- `_group_ids`群組 ID 存在 Amazon WorkDocs 於具有設定存取權限的檔案中。它們會從中的群組名稱對應 Amazon WorkDocs。
- `_user_id`使用者 ID 存在 Amazon WorkDocs 於具有設定存取權限的檔案中。它們會從中的使用者名稱對應 Amazon WorkDocs。

您最多可以在AccessControlList欄位中新增 200 個項目。

Box 資料來源的使用者內容篩選

使用 Box 資料來源時，Amazon Kendra 會從 Box 執行個體取得使用者和群組資訊。

Box 群組和使用者 ID 的對應方式如下：

- `_group_ids`群組 ID 存在於 Box 中，存在於具有設定存取權限的檔案上。它們是從 Box 中的組的名稱映射的。
- `_user_id`在有設定存取權限的檔案上，使用者 ID 存在於 Box 中。它們從用戶電子郵件映射為 Box 中的用戶 ID。

您最多可以在AccessControlList欄位中新增 200 個項目。

匯流資料來源的使用者內容篩選

當您使用匯流資料來源時，Amazon Kendra 會從匯流執行個體取得使用者和群組資訊。

您可以使用空間權限頁面設定使用者和群組對空間的存取權限。對於頁面和博客，您可以使用限制頁面。如需有關空間權限的詳細資訊，請參閱 Confluence Support 網站上的[空間權限概觀](#)。如需有關頁面和部落格限制的詳細資訊，請參閱 Confluence Support 網站上的[頁面限制](#)。

匯流群組和使用者名稱的對應方式如下：

- `_group_ids` 群組名稱會出現在有限制的空間、頁面和部落格上。它們是從匯流組的名稱映射的。群組名稱永遠是小寫。
- `_user_id` 使用者名稱會出現在有限制的空間、頁面或部落格上。它們會根據您正在使用的匯流實例的類型進行映射。

對於匯流連接器 v1.0

- 伺服器-`_user_id` 是使用者名稱。用戶名總是小寫。
- 雲端 — `_user_id` 是使用者的帳戶 ID。

對於匯流連接器 v2.0

- 伺服器-`_user_id` 是使用者名稱。用戶名總是小寫。
- 雲端 — `_user_id` 是使用者的電子郵件 ID。

Important

若要讓使用者內容篩選正確運作您的 Confluence 連接器，您需要確定授與 Confluence 頁面存取權的使用者可見性設定為 [任何人]。如需詳細資訊，請參閱在 Atlassian [開發人員文件中設定電子郵件可見度](#)。

您最多可以在 `AccessControlList` 欄位中新增 200 個項目。

Dropbox 資料來源的使用者上下文篩選

當您使用 Dropbox 資料來源時，Amazon Kendra 會從 Dropbox 執行個體取得使用者和群組資訊。

群組和使用者 ID 的對應方式如下：

- `_group_ids`— 群組 ID 存在於 Dropbox 中，存在於有設定存取權限的檔案上。它們是從 Dropbox 中的群組名稱對應而來。
- `_user_id`— 使用者 ID 存在於 Dropbox 中，存在於有設定存取權限的檔案上。它們從用戶的電子郵件中映射為 Dropbox 中的 ID。

您最多可以在 `AccessControlList` 欄位中新增 200 個項目。

Drupal 數據源的用戶上下文過濾

當你使用一個 Drupal 的數據源，Amazon Kendra 獲取從數據的用戶和組信息。

群組和使用者 ID 的對應方式如下：

- `_group_ids`— 組 ID 存在於 Drupal 中存在於有設置訪問權限的文件上。它們是從 Drupal 的組的名稱映射。
- `_user_id`— 用戶 ID 存在於 Drupal 中存在於有設置訪問權限的文件上。它們從用戶電子郵件中映射為 Drupal 中的 ID。

您最多可以在 `AccessControlList` 欄位中新增 200 個項目。

GitHub 資料來源的使用者內容篩選

使用資 GitHub 料來源時，Amazon Kendra 會從執行個 GitHub 體取得使用者資訊。

GitHub 使用者 ID 的對應方式如下：

- `_user_id` 使用者 ID 存在 GitHub 於具有設定存取權限的檔案中。它們會從使用者電子郵件中對應為中的 ID GitHub。

您最多可以在 `AccessControlList` 欄位中新增 200 個項目。

Gmail 資料來源的使用者內容篩選

當您使用 Gmail 資料來源時，Amazon Kendra 會從 Gmail 執行個體取得使用者資訊。

使用者 ID 對應如下：

- `_user_id`— 在有設置訪問權限的文件上，用戶 ID 存在於 Gmail 中。它們從用戶電子郵件中映射為 Gmail 中的 ID。

您最多可以在 `AccessControlList` 欄位中新增 200 個項目。

Google 雲端硬碟資料來源的使用者內容篩選

Google 工作區雲端硬碟資料來源會傳回 Google 雲端硬碟使用者和群組的使用者和群組資訊。群組和網域成員資格會對應至 `_group_ids` 引欄位。Google 雲端硬碟使用者名稱會對應至 `_user_id` 欄位。

當您在 Query API 中提供一或多個使用者電子郵件地址時，只會傳回與這些電子郵件地址共用的文件。下列 `AttributeFilter` 參數只會傳回與「martha@example.com」共用的文件。

```
"AttributeFilter": {
  "EqualsTo": {
    "Key": "_user_id",
    "Value": {
      "StringValue": "martha@example.com"
    }
  }
}
```

如果您在查詢中提供一或多個群組電子郵件地址，則只會傳回與群組共用的文件。下列 `AttributeFilter` 參數只會傳回與「hr@example.com」群組共用的文件。

```
"AttributeFilter": {
  "EqualsTo": {
    "Key": "_group_ids",
    "Value": {
      "StringListValue": ["hr@example.com"]
    }
  }
}
```

如果您在查詢中提供網域，則會傳回與該網域共用的所有文件。下列 `AttributeFilter` 參數會傳回與「example.com」網域共用的文件。

```
"AttributeFilter": {
  "EqualsTo": {
    "Key": "_group_ids",
    "Value": {
      "StringListValue": ["example.com"]
    }
  }
}
```

您最多可以在 `AccessControlList` 欄位中新增 200 個項目。

IBM DB2 資料來源的使用者內容篩選

當您使用 IBM DB2 資料來源時，Amazon Kendra 會從來源表格中的欄取得使用者和群組資訊。您可以在主控台中指定此欄，或使用 [TemplateConfiguration](#) 物件做為 [CreateDataSourceAPI](#) 的一部分。

IBM DB2 資料庫資料來源具有下列限制：

- 您只能指定資料庫資料來源的允許清單。您無法指定拒絕清單。
- 您只能指定群組。您無法為允許清單指定個別使用者。
- 資料庫欄應該是包含以分號分隔的群組清單的字串。

Jira 資料來源的使用者內容篩選

使用 Jira 資料來源時，Amazon Kendra 會從 Jira 執行個體取得使用者和群組資訊。

Jira 使用者 ID 的對應方式如下：

- `_user_id`在有設定存取權限的檔案上，使用者 ID 存在於 Jira 中。它們從用戶電子郵件中映射為 Jira 中的用戶 ID。

您最多可以在 `AccessControlList` 欄位中新增 200 個項目。

Microsoft 交換資料來源的使用者內容篩選

當您使用 Microsoft 交換資料來源時，Amazon Kendra 會從 Microsoft Exchange 執行個體取得使用者資訊。

Microsoft 交易所使用者識別碼對應如下：

- `_user_id`使用者識別碼存在於 Microsoft Exchange 權限中，可供使用者存取特定內容。它們是從用戶名映射為在 Microsoft 交易所的 ID。

您最多可以在 `AccessControlList` 欄位中新增 200 個項目。

Microsoft OneDrive 資料來源的使用者內容篩選

Amazon Kendra 當 Microsoft 索引網站上的文件 OneDrive 時，會從 Microsoft 擷取使用者和群組資訊。使用者和群組資訊取自主控的基礎 Microsoft SharePoint 網站 OneDrive。

當您使用使用 OneDrive 者或群組篩選搜尋結果時，請依照下列方式計算 ID：

1. 取得網站名稱。例如：`https://host.onmicrosoft.com/sites/siteName`。
2. 取站點名稱的 MD5 哈希值。例如 `430a6b90503eef95c89295c8999c7981`。
3. 透過將 MD5 雜湊與垂直列 (|) 和 ID 連接，以建立使用者電子郵件或群組 ID。例如，如果群組名稱是 "localGroupName"，則群組識別碼會是：

```
"430a6b90503eef95c89295c8999c7981 | localGroupName"
```

Note

在垂直列前後加入空格。垂直條用於localGroupName與它的 MD5 哈希標識。

使用者名稱「someone@host.onmicrosoft.com」的使用者識別碼如下：

```
"430a6b90503eef95c89295c8999c7981 | someone@host.onmicrosoft.com"
```

當您呼叫[查詢](#) API 時，將使用者 `_user_id` 或群組 ID Amazon Kendra 做為或 `_group_id` 屬性傳送至。例如，使用群組篩選搜尋結果的 AWS CLI 指令如下所示：

```
aws kendra query \  
    --index-id index ID  
    --query-text "query text"  
    --attribute-filter '{  
        "EqualsTo":{  
            "Key": "_group_id",  
            "Value": {"StringValue": "430a6b90503eef95c89295c8999c7981 |  
localGroupName"}  
        }  
    }'
```

您最多可以在AccessControlList欄位中新增 200 個項目。

Microsoft OneDrive 2.0 資料來源的使用者內容篩選

Microsoft OneDrive 2.0 資料來源會從 OneDrive 存取控制清單 (ACL) 實體傳回區段和頁面資訊。Amazon Kendra 使用 OneDrive 承租人網域連線至 OneDrive 執行個體，然後可以根據使用者或群組對區段和檔案名稱的存取權限篩選搜尋結果。

對於標準物件，`_user_id`和的使`_group_id`用方式如下：

- `_user_id`— 您的 Microsoft OneDrive 用戶電子郵件 ID 被映射到該 `_user_id` 字段。
- `_group_id`— 您的 Microsoft OneDrive 群組電子郵件已對應至 `_group_id` 欄位。

您最多可以在 `AccessControlList` 欄位中新增 200 個項目。

Microsoft SharePoint 資料來源的使用者內容篩選

Amazon Kendra 當 Microsoft 索引網站文件 SharePoint 時，會從 Microsoft 擷取使用者和群組資訊。若要根據使用者或群組存取權篩選搜尋結果，請在呼叫 Query API 時提供使用者和群組資訊。

若要使用使用者名稱進行篩選，請使用使用者的電子郵件地址。例如，`johnstiles@example.com`。

當您使用 SharePoint 群組篩選搜尋結果時，請依照下列方式計算群組 ID：

對於本地團體

1. 取得網站名稱。例如：`https://host.onmicrosoft.com/sites/siteName`。
2. 採取站點名稱的 SHA256 哈希值。例如 `430a6b90503eef95c89295c8999c7981`。
3. 透過將 SHA256 雜湊與垂直列 (`|`) 和群組名稱相連，以建立群組識別碼。例如，如果群組名稱是 `"localGroupName"`，則群組識別碼會是：

```
"430a6b90503eef95c89295c8999c7981 | localGroupName"
```

Note

在垂直列前後加入空格。垂直條用於 `localGroupName` 與它的 SHA256 哈希標識。

當您呼叫 [查詢 API](#) 時，傳送群組識別碼 Amazon Kendra 做為 `_group_id` 屬性。例如，AWS CLI 命令看起來像這樣：

```
aws kendra query \  
    --index-id index ID  
    --query-text "query text"  
    --attribute-filter '{  
        "EqualsTo":{  
            "Key": "_group_id",  
            "Value": {"StringValue": "430a6b90503eef95c89295c8999c7981 |  
localGroupName"}}
```

```
}}'
```

適用於廣告群組

1. 使用 AD 群組識別碼來設定搜尋結果的篩選。

當您呼叫[查詢](#) API 時，傳送群組識別碼 Amazon Kendra 做為 `_group_id` 屬性。例如，AWS CLI 命令看起來像這樣：

```
aws kendra query \  
    --index-id index ID  
    --query-text "query text"  
    --attribute-filter '{  
        "EqualsTo":{  
            "Key": "_group_id",  
            "Value": {"StringValue": "AD group"}  
        }  
    }'
```

您最多可以在 `AccessControlList` 欄位中新增 200 個項目。

Microsoft SQL 伺服器資料來源的使用者內容篩選

當您使用 Microsoft SQL Server 資料來源時，Amazon Kendra 會從來源資料表中的資料行取得使用者和群組資訊。您可以在主控台中指定此欄，或使用 [TemplateConfiguration](#) 物件做為 [CreateDataSourceAPI](#) 的一部分。

Microsoft SQL 伺服器資料庫資料來源有下列限制：

- 您只能指定資料庫資料來源的允許清單。您無法指定拒絕清單。
- 您只能指定群組。您無法為允許清單指定個別使用者。
- 資料庫欄應該是包含以分號分隔的群組清單的字串。

Microsoft 團隊資料來源的使用者內容篩選

Amazon Kendra 當它為文件編製索引時，會從 Microsoft 小組擷取使用者資訊。使用者資訊取自基礎 Microsoft 團隊執行個體。

您最多可以在 `AccessControlList` 欄位中新增 200 個項目。

Microsoft Yammer 資料來源的使用者內容篩選

Amazon Kendra 當它索引文檔時，會從 Microsoft Yammer 中檢索用戶信息。使用者和群組資訊取自基礎 Microsoft Yammer 執行個體。

Microsoft Yammer 使用者識別碼對應如下：

- `_email_id`— 映射到該 `_user_id`字段的 Microsoft 電子郵件 ID。

您最多可以在 `AccessControlList` 欄位中新增 200 個項目。

MySQL 資料來源的使用者內容篩選

當您使用 MySQL 資料來源時，Amazon Kendra 會從來源資料表中的資料行取得使用者和群組資訊。您可以在主控台中指定此欄，或使用 [TemplateConfiguration](#) 物件做為 [CreateDataSource](#) API 的一部分。

MySQL 資料庫資料來源有以下限制：

- 您只能指定資料庫資料來源的允許清單。您無法指定拒絕清單。
- 您只能指定群組。您無法為允許清單指定個別使用者。
- 資料庫欄應該是包含以分號分隔的群組清單的字串。

Oracle 資料庫資料來源的使用者內容篩選

當您使用「Oracle 資料庫」資料來源時，Amazon Kendra 會從來源表格中的資料欄取得使用者和群組資訊。您可以在主控台中指定此欄，或使用 [TemplateConfiguration](#) 物件做為 [CreateDataSource](#) API 的一部分。

Oracle 資料庫資料來源有下列限制：

- 您只能指定資料庫資料來源的允許清單。您無法指定拒絕清單。
- 您只能指定群組。您無法為允許清單指定個別使用者。
- 資料庫欄應該是包含以分號分隔的群組清單的字串。

PostgreSQL 資料來源的使用者內容篩選

當您使用 PostgreSQL 資料來源時，Amazon Kendra 會從來源資料表中的資料行取得使用者和群組資訊。您可以在主控台中指定此欄，或使用 [TemplateConfiguration](#) 物件做為 [CreateDataSource](#) API 的一部分。

PostgreSQL 資料庫資料來源具有下列限制：

- 您只能指定資料庫資料來源的允許清單。您無法指定拒絕清單。
- 您只能指定群組。您無法為允許清單指定個別使用者。
- 資料庫欄應該是包含以分號分隔的群組清單的字串。

Quip 資料來源的使用者內容篩選

當您使用 Quip 資料來源時，Amazon Kendra 會從 Quip 執行個體取得使用者資訊。

Quip 使用者識別碼的對應方式如下：

- `_user_id` 在有設定存取權限的檔案上，使用者 ID 存在於 Quip 中。它們從用戶電子郵件映射為 Quip 中的 ID。

您最多可以在 `AccessControlList` 欄位中新增 200 個項目。

Salesforce 資料來源的使用者內容篩選

Salesforce 資料來源會從 Salesforce 存取控制清單 (ACL) 實體傳回使用者和群組資訊。您可以將使用者內容篩選套用至 Salesforce 標準物件和聊天程式摘要。Salesforce 知識文章無法使用使用者內容篩選。

如果您將任何 Salesforce 欄位對應至 Amazon Kendra 文件標題和文件內文欄位，Amazon Kendra 會在搜尋回應中使用文件標題和內文欄位中的資料。

對於標準物件，`_user_id` 和 `_group_ids` 的使用方式如下：

- `_user_id`—Salesforce 使用者的使用者名稱。
- `_group_ids`—
 - 銷售隊伍的名稱 Profile
 - 銷售隊伍的名稱 Group
 - 銷售隊伍的名稱 UserRole

- 銷售隊伍的名稱 PermissionSet

對於喋喋不休的摘要，_user_id和的使_group_ids用方式如下：

- _user_idSalesforce 使用者的使用者名稱。只有當項目張貼在使用者的摘要中時才可用。
- _group_ids群組 ID 的使用方式如下。只有在動態消息項目張貼在聊天或協同作業群組時才可使用。
 - 聊天或協同作業群組的名稱。
 - 如果群組是公開的，PUBLIC:ALL.

您最多可以在AccessControlList欄位中新增 200 個項目。

ServiceNow 資料來源的使用者內容篩選

的使用者內容篩選 ServiceNow 僅支援 TemplateConfiguration API 和 ServiceNow 連接器 2.0 版。ServiceNowConfigurationAPI 和 ServiceNow 連接器 1.0。不支持用戶上下文過濾。

使用資 ServiceNow 料來源時，Amazon Kendra 會從 ServiceNow 執行個體取得使用者和群組資訊。

群組和使用者 ID 的對應方式如下：

- _group_ids群組 ID 存在 ServiceNow 於具有設定存取權限的檔案中。它們是從中的角色名稱對應而sys_ids來 ServiceNow。
- _user_id使用者 ID 存在 ServiceNow 於具有設定存取權限的檔案中。它們會從使用者電子郵件中對應為中的 ID ServiceNow。

您最多可以在AccessControlList欄位中新增 200 個項目。

Slack 資料來源的使用者內容篩選

使用 Slack 資料來源時，Amazon Kendra 會從 Slack 執行個體取得使用者資訊。

Slack 使用者 ID 的對應方式如下：

- _user_idSlack 中有使用者 ID 存在於具有設定存取權限的訊息和通道上。它們會從使用者電子郵件對應為 Slack 中的 ID。

您最多可以在AccessControlList欄位中新增 200 個項目。

Zendesk 資料來源的使用者內容篩選

使用 Zendesk 資料來源時，Amazon Kendra 會從 Zendesk 執行個體取得使用者和群組資訊。

群組和使用者 ID 的對應方式如下：

- `_group_ids`群組 ID 存在於有設定存取權限的 Zendesk 票證和文章中。它們是從 Zendesk 中的群組名稱進行對映。
- `_user_id`群組 ID 存在於有設定存取權限的 Zendesk 票證和文章中。它們會從使用者電子郵件對應為 Zendesk 中的 ID。

您最多可以在AccessControlList欄位中新增 200 個項目。

查詢回應和回應類型

Amazon Kendra 支持不同的查詢響應和響應類型。

查詢回應

呼叫查詢 API 會傳回搜尋結果的相關資訊。結果位於[QueryResultItem](#)物件 (ResultItems) 的陣列中。每個都QueryResultItem包括結果的摘要。包括與查詢結果相關聯的文件屬性。

摘要資訊

摘要資訊會根據結果類型而有所不同。在每種情況下，它都包含符合搜尋字詞的文件文字。它還包括反白顯示資訊，您可以使用這些資訊在應用程式輸出中反白顯示搜尋文字。例如，如果搜索詞是太空針塔的高度是多少？，摘要資訊包括字詞高度和太空針的文字位置。有關響應類型的更多內容，敬請參閱[查詢回應和回應類型](#)。

文件屬性

每個結果都包含符合查詢之文件的文件屬性。某些屬性是預先定義的DocumentId，例如DocumentTitle、和DocumentUri。其他則是您定義的自訂屬性。您可以使用文件屬性來篩選 Query API 的回應。例如，您可能只想要由特定作者或文件的特定版本所撰寫的文件。如需詳細資訊，請參閱 [篩選和平面搜尋](#)。當您將文件新增至索引時，您可以指定文件屬性。如需詳細資訊，請參閱[自訂欄位或屬性](#)。

以下是查詢結果的範例 JSON 程式碼。請注意和中的文件屬DocumentAttributes性AdditionalAttributes。


```
{
  "QueryId": "query-id",
  "ResultItems": [
    {
      "Id": "result-id",
      "Type": "ANSWER",
      "AdditionalAttributes": [
        {
          "Key": "AnswerText",
          "ValueType": "TEXT_WITH_HIGHLIGHTS_VALUE",
          "Value": {
            "TextWithHighlightsValue": {
              "Text": "text",
              "Highlights": [
                {
                  "BeginOffset": 55,
                  "EndOffset": 90,
                  "TopAnswer": false
                }
              ]
            }
          }
        }
      ],
      "DocumentId": "document-id",
      "DocumentTitle": {
        "Text": "title"
      },
      "DocumentExcerpt": {
        "Text": "text",
        "Highlights": [
          {
            "BeginOffset": 0,
            "EndOffset": 300,
            "TopAnswer": false
          }
        ]
      },
      "DocumentURI": "uri",
      "DocumentAttributes": [],
      "ScoreAttributes": "score",
      "FeedbackToken": "token"
    },
  ],
}
```

```
{
  "Id": "result-id",
  "Type": "ANSWER",
  "Format": "TABLE",
  "DocumentId": "document-id",
  "DocumentTitle": {
    "Text": "title"
  },
  "TableExcerpt": {
    "Rows": [{
      "Cells": [{
        "Header": true,
        "Highlighted": false,
        "TopAnswer": false,
        "Value": "value"
      }, {
        "Header": true,
        "Highlighted": false,
        "TopAnswer": false,
        "Value": "value"
      }, {
        "Header": true,
        "Highlighted": false,
        "TopAnswer": false,
        "Value": "value"
      }, {
        "Header": true,
        "Highlighted": false,
        "TopAnswer": false,
        "Value": "value"
      }
    ]
  }, {
    "Cells": [{
      "Header": false,
      "Highlighted": false,
      "TopAnswer": false,
      "Value": "value"
    }, {
      "Header": false,
      "Highlighted": false,
      "TopAnswer": false,
      "Value": "value"
    }, {
      "Header": false,
```

```

        "Highlighted": true,
        "TopAnswer": true,
        "Value": "value"
    }, {
        "Header": false,
        "Highlighted": false,
        "TopAnswer": false,
        "Value": "value"
    }
  ]],
  "TotalNumberOfRows": number
},
{
  "DocumentURI": "uri",
  "ScoreAttributes": "score",
  "FeedbackToken": "token"
},
{
  "Id": "result-id",
  "Type": "DOCUMENT",
  "AdditionalAttributes": [],
  "DocumentId": "document-id",
  "DocumentTitle": {
    "Text": "title",
    "Highlights": []
  },
  "DocumentExcerpt": {
    "Text": "text",
    "Highlights": [
      {
        "BeginOffset": 74,
        "EndOffset": 77,
        "TopAnswer": false
      }
    ]
  },
  "DocumentURI": "uri",
  "DocumentAttributes": [
    {
      "Key": "_source_uri",
      "Value": {
        "StringValue": "uri"
      }
    }
  ]
},

```

```
        "ScoreAttributes": "score",
        "FeedbackToken": "token",
    }
],
"FacetResults": [],
"TotalNumberOfResults": number
}
```

回應類型

Amazon Kendra 返回三種類型的查詢響應。

- 答案 (包括表格答案)
- 文件
- 問題和解答

回應類型會在 [QueryResultItem](#) 物件的 `type` 欄位中傳回。

答案

Amazon Kendra 在回應中偵測到一個或多個問題答案。Factoid 是對誰，什麼，何時或在哪裡問題的回應，如哪裡是最近的服務中心給我？Amazon Kendra 會傳回索引中最符合查詢的文字。文字位於 `AnswerText` 欄位中，包含回應文字中搜尋字詞的反白顯示資訊。 `AnswerText` 包括帶有突出顯示文本的完整文檔摘錄，同時 `DocumentExcerpt` 包括帶有突出顯示文本的截斷 (290 個字符) 文檔摘錄。

Amazon Kendra 每個文檔只返回一個答案，這是具有最高信心的答案。若要從文件傳回多個答案，您必須將文件分割成多個文件。

```
{
  'AnswerText': {
    'TextWithHighlights': [
      {
        'BeginOffset': 271,
        'EndOffset': 279,
        'TopAnswer': False
      },
      {
        'BeginOffset': 481,
        'EndOffset': 489,
        'TopAnswer': False
      }
    ]
  }
}
```

```
    },
    {
      'BeginOffset': 547,
      'EndOffset': 555,
      'TopAnswer': False
    },
    {
      'BeginOffset': 764,
      'EndOffset': 772,
      'TopAnswer': False
    }
  ],
  'Text': 'Asynchronousoperationscan\n''alsoprocess
\n''documentsthatareinPDF''format.UsingPDFformatfilesallowsyoutoprocess''multi-
page\n''documents.\n''Forinformationabouthow''AmazonTextextractrepresents
\n''documentsasBlockobjects,
  ''seeDocumentsandBlockObjects.
\n''\n''\n''\n''Forinformationaboutdocument''limits,
  seeLimitsinAmazonTextextract.
\n''\n''\n''\n''TheAmazonTextextractsynchronous''operationscandocumentsthat
\n''S3Bucketoryoucanpass''base64encodedimagebytes.\n''Formoreinformation,
  see''CallingAmazonTextextractSynchronousOperations.''Asynchronousoperationsrequireinputdocuments
\n''tobesuppliedinanAmazon''S3Bucket.'
},
'DocumentExcerpt': {
  'Highlights': [
    {
      'BeginOffset': 0,
      'EndOffset': 300,
      'TopAnswer': False
    }
  ]
},
  'Text': 'Asynchronousoperationscan\n''alsoprocess
\n''documentsthatareinPDF''format.UsingPDFformatfilesallowsyoutoprocess''multi-page
\n''documents.\n''ForinformationabouthowAmazon''Textextractrepresents\n''''
},
'Type': 'ANSWER'
}
```

文件

Amazon Kendra 傳回符合搜尋字詞的排名文件。排名基於對搜索結果準確性的可信度。Amazon Kendra 相符文件的相關資訊會在中傳回 [QueryResultItem](#)。它包括文檔的標題。摘錄包括搜尋文字的反白資訊，以及文件中相符文字的區段。相符文件的 URI 位於文SourceURI件屬性中。下列範例 JSON 顯示相符文件的文件摘要。

```
{
  'DocumentTitle': {
    'Highlights': [
      {
        'BeginOffset': 7,
        'EndOffset': 15,
        'TopAnswer': False
      },
      {
        'BeginOffset': 97,
        'EndOffset': 105,
        'TopAnswer': False
      }
    ],
    'Text': 'AmazonTextractAPIPermissions: Actions,
\n''Permissions,
andResourcesReference-''AmazonTextract'
  },
  'DocumentExcerpt': {
    'Highlights': [
      {
        'BeginOffset': 68,
        'EndOffset': 76,
        'TopAnswer': False
      },
      {
        'BeginOffset': 121,
        'EndOffset': 129,
        'TopAnswer': False
      }
    ],
    'Text': '...LoggingandMonitoring\tMonitoring
\n''\tCloudWatchMetricsforAmazonTextract
\n''\tLoggingAmazonTextractAPICallswithAWScloudTrail\n''\tAPIReference\tActions
\tAnalyzeDocument\n''\tDetectDocumentText\n''\tGetDocumentAnalysis...'
  },
}
```

```
'Type': 'DOCUMENT'  
}
```

問題和解答

當問題與索引中的其中一個常見問題 Amazon Kendra 相符時，就會傳回問題和答案回應。該回應包括字 [QueryResultItem](#) 段中匹配的問題和答案。它也包含在查詢字串中偵測到的查詢字詞的反白顯示資訊。下列 JSON 顯示問題與答案回應。請注意，回覆中包含問題文字。

```
{  
  'AnswerText': {  
    'TextWithHighlights': [  
  
    ],  
    'Text': '605feet'  
  },  
  'DocumentExcerpt': {  
    'Highlights': [  
      {  
        'BeginOffset': 0,  
        'EndOffset': 8,  
        'TopAnswer': False  
      }  
    ],  
    'Text': '605feet'  
  },  
  'Type': 'QUESTION_ANSWER',  
  'QuestionText': {  
    'Highlights': [  
      {  
        'BeginOffset': 12,  
        'EndOffset': 18,  
        'TopAnswer': False  
      },  
      {  
        'BeginOffset': 26,  
        'EndOffset': 31,  
        'TopAnswer': False  
      },  
      {  
        'BeginOffset': 32,  
        'EndOffset': 38,  
        'TopAnswer': False  
      }  
    ]  
  }  
}
```

```
    }  
  ],  
  'Text': 'whatistheheightoftheSpaceNeedle?'  
}  
}
```

如需將問題和答案文字新增至索引的詳細資訊，請參閱[建立常見問題集](#)。

調整和排序回應

您可以透過相關性調整來修改欄位或屬性對搜尋相關性的影響。您還可以按特定屬性或字段對搜索結果進行排序。

主題

- [調整回應](#)
- [排序回應](#)

調整回應

您可以透過相關性調整來修改欄位或屬性對搜尋相關性的影響。若要快速測試相關性調整，請使用 [Query API](#) 在查詢中傳遞調整設定。然後，您可以看到從不同配置獲得的不同搜索結果。主控台不支援在查詢層級進行相關性調整。您也可以僅 `StringList` 在索引層級調整類型的欄位或屬性。如需詳細資訊，請參閱[調整搜尋相關性](#)。

根據預設，查詢回應會依據 Amazon Kendra 決定回應中每個結果的相關性分數排序。

您可以調整下列類型之任何內建或自訂屬性/欄位的結果：

- 日期值
- 長值
- 字串值

您無法排序下列類型的屬性：

- 字串清單值

排名和調整文件結果 (AWS SDK)

將 `Searchable` 參數設定為 `true` 以提升文件中繼資料組態。

若要調整查詢中的屬性，請設定 Query API 的 `DocumentRelevanceOverrideConfigurations` 參數，並指定要調整的屬性名稱。

下列 JSON 範例顯示的 `DocumentRelevanceOverrideConfigurations` 物件會覆寫索引中稱為「部門」之屬性的調整。

```
"DocumentRelevanceOverrideConfigurations" : [  
  "Name": "department",  
  "Relevance": {  
    "Importance": 1,  
    "ValueImportanceMap": {  
      "IT": 3,  
      "HR": 7  
    }  
  }  
]
```

排序回應

Amazon Kendra 使用排序屬性或欄位作為查詢傳回之文件條件的一部分。例如，以「`_created_at`」排序的查詢傳回的結果可能與以「`_version`」排序的查詢所包含的結果不同。

根據預設，查詢回應會依據 Amazon Kendra 決定回應中每個結果的相關性分數排序。若要變更排序順序，請將文件屬性設為可排序，然後配置 Amazon Kendra 為使用該屬性來排序回應。

您可以針對下列類型的任何內建或自訂屬性/欄位排序結果：

- 日期值
- 長值
- 字串值

您無法排序下列類型的屬性：

- 字串清單值

您可以在每個查詢中排序一或多個文件屬性。查詢會傳回 100 個結果。如果已設定排序屬性的文件少於 100 個，則不含排序屬性值的文件會在結果結尾傳回，並依與查詢的相關性排序。

若要排序文件結果 (AWS SDK)

1. 若要使用 [UpdateIndex](#) API 使屬性可排序，請將 `Sortable` 參數設定為 `true`。下面的 JSON 示例使 `DocumentMetadataConfigurationUpdates` 用一個名為「部門」的屬性添加到索引，並使其排序。

```
"DocumentMetadataConfigurationUpdates": [  
  {  
    "Name": "Department",  
    "Type": "STRING_VALUE",  
    "Search": {  
      "Sortable": "true"  
    }  
  }  
]
```

2. 若要在查詢中使用一個可排序屬性，請設定 [查詢](#) API 的 `SortingConfiguration` 參數。指定要排序的屬性名稱，以及是否要以遞增或遞減順序來排序回應。

下列 JSON 範例會顯示您用來依遞增順序依「部門」屬性來排序查詢結果的 `SortingConfiguration` 參數。

```
"SortingConfiguration": {  
  "DocumentAttributeKey": "Department",  
  "SortOrder": "ASC"  
}
```

3. 若要在查詢中使用多個可排序屬性，請設定 [查詢](#) API 的 `SortingConfigurations` 參數。您最多可以設置 3 個 Amazon Kendra 應該對結果進行排序的字段。您也可以指定結果應以遞增或遞減順序排序。排序欄位配額可以增加。

如果您未提供排序設定，則會依據 Amazon Kendra 決定結果的相關性來排序結果。在排序結果的關係的情況下，結果按相關性排序。

下列 JSON 範例會顯示您用來依遞增順序的屬性「名稱」和「價格」來排序查詢結果的 `SortingConfigurations` 參數。

```
"CollapseConfiguration" : {  
  "DocumentAttributeKey": "Name",  
  "SortingConfigurations": [  
    {
```

```
        "DocumentAttributeKey": "Price",
        "SortOrder": "ASC"
    }
],
"MissingAttributeKeyStrategy": "IGNORE"
}
```

若要排序文件結果 (主控台)

Note

目前不支援多屬性排序。AWS Management Console

1. 若要讓屬性在主控台中排序，請在屬性定義中選擇「可排序」。您可以在建立屬性時將屬性設為可排序，也可以稍後修改屬性。
2. 若要在主控台中排序查詢回應，請從「排序」功能表選擇要排序回應的屬性。只有在資料來源組態期間標記為可排序的屬性才會顯示在清單中。

摺疊/展開查詢結果

當您連線 Amazon Kendra 到資料時，它會編目 [文件中繼資料屬性](#) (例如 `_document_title`、`_created_at`、`_document_id`) 並使用這些屬性或欄位在查詢期間提供進階搜尋功能。

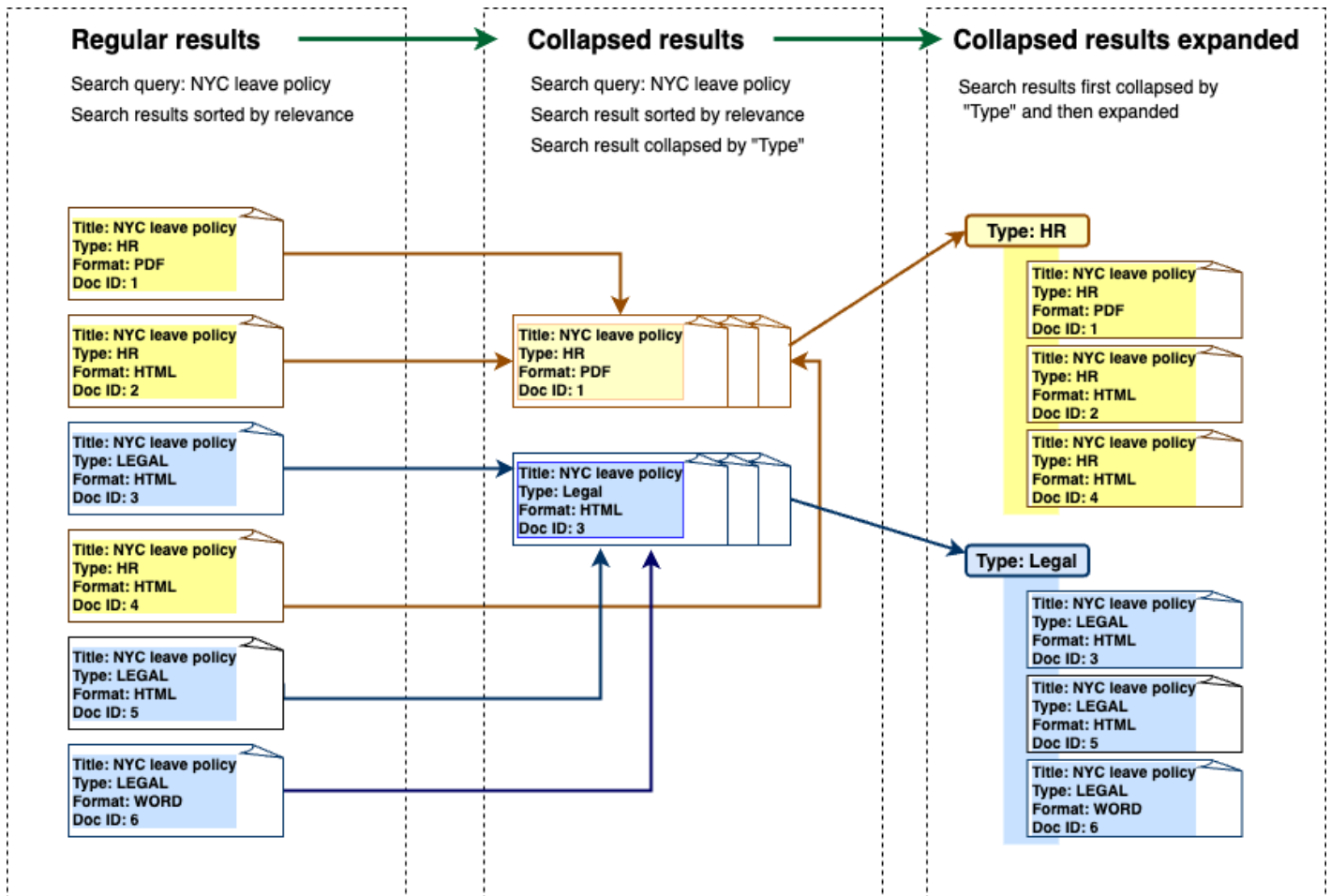
Amazon Kendra 的「摺疊和展開查詢結果」功能可讓您使用通用文件屬性來分組搜尋結果，並在指定的主要文件下顯示搜尋結果 (摺疊或部分展開)。

Note

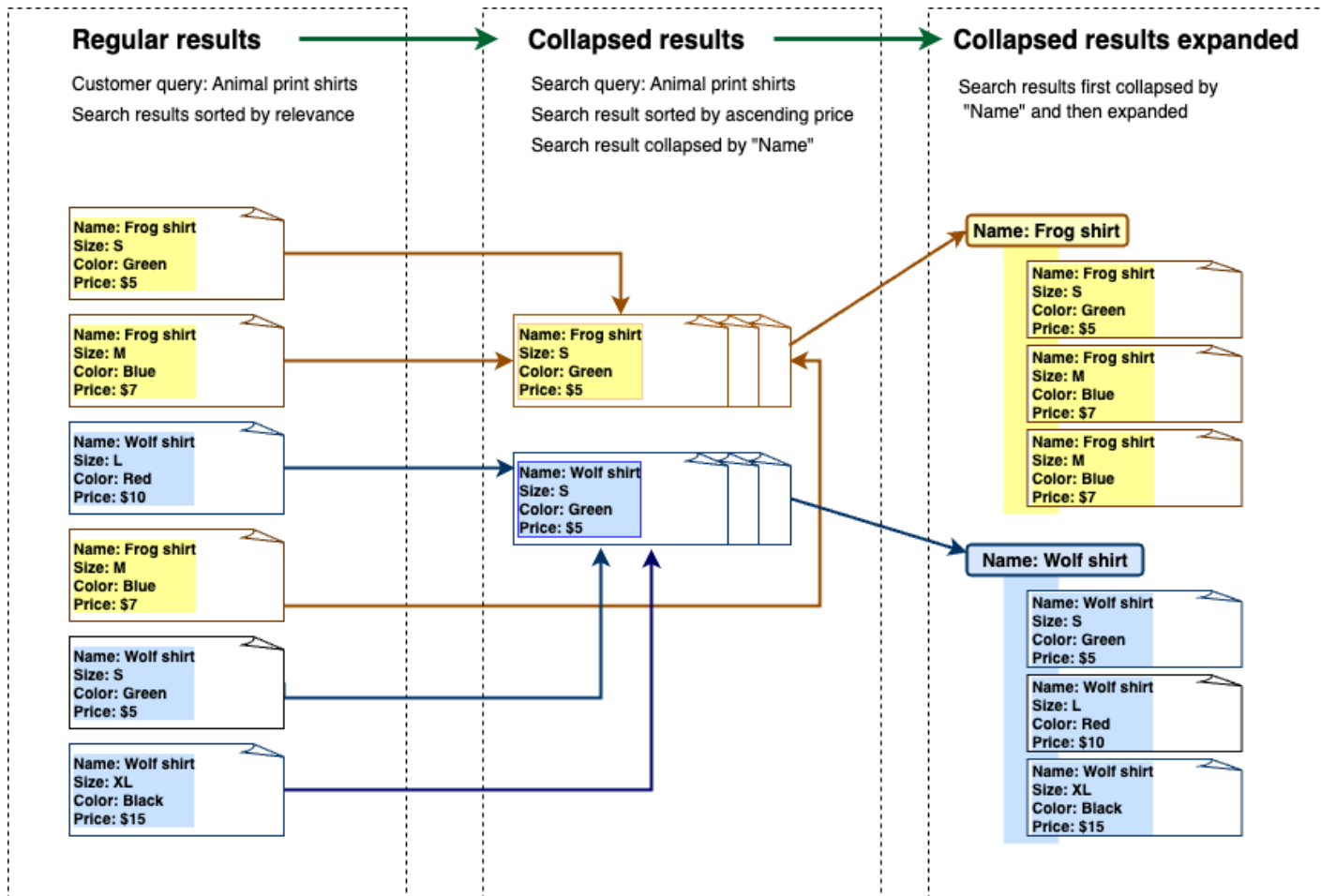
收合和展開查詢結果功能目前只能透過 [Amazon Kendra API](#) 使用。

這在下列類型的搜尋情況下很有用：

- 索引內的文件中存在多個版本的內容。當您的一般使用者查詢索引時，您希望他們看到最相關的文件版本，並隱藏/摺疊重複項目。例如，如果您的索引包含多個名為「NYC 休假政策」的文件版本，您可以選擇使用「類型」屬性/欄位來收合特定群組「HR」和「法律」群組的文件。



- 您的索引包含多個文件，其中包含一種項目或物件的唯一資訊，例如產品庫存。為了方便地擷取和排序項目資訊，您希望最終使用者可以將項目或物件連結的所有文件作為一個搜尋結果存取。在下面的例子中，客戶搜索「動物印花襯衫」返回按名稱分組的結果，並按價格升序排序。



摺疊結果

若要將類似或相關的文件群組在一起，您必須指定要收合的屬性 (例如，您可以依據 `_category` 縮疊/群組文件)。若要執行這項操作，請呼叫 [Query API](#) 並使用 [CollapseConfiguration](#) 物件來指定 `DocumentAttributeKey` 要收合的。 `DocumentAttributeKey` 控制哪些欄位搜尋結果將在收合時。支援的屬性索引鍵欄位包括 `String` 和 `Number`。 `String list` 和 `Date` 類型不受支援。

使用排序順序選擇主要文件

若要配置主要文件以顯示縮疊群組，請使用下的 `SortingConfigurations` 參數 [CollapseConfiguration](#)。例如，若要取得文件的最新版本，您可以依據每個收合的群組來排序 `_version`。您最多可以指定 3 個屬性/欄位進行排序，並使用指定每個屬性/欄位的排序順序。 `SortingConfigurations` 您可以要求增加排序屬性數目的配額。

根據預設，會 Amazon Kendra 依據其針對回應中每個結果所決定的相關性分數來排序查詢回應。若要變更預設排序順序，請將文件屬性設為可排序，然後設定 Amazon Kendra 為使用這些屬性來排序回應。如需詳細資訊，請參閱[排序回覆](#)。

缺少文件金鑰策略

如果您的文件沒有摺疊屬性值，會 Amazon Kendra 提供三個自訂選項：

- 選擇COLLAPSE一個群組中包含 null 或缺少值的所有文件。這是預設組態。
- 選擇具有空值或缺少值的IGNORE文件。忽略的文件將不會出現在查詢結果中。
- 選擇將EXPAND具有 null 或缺少值的文檔放入其自己的一組中。

擴大結果

您可以選擇是否使用[CollapseConfiguration](#)物件中的Expand參數來展開收合的搜尋結果群組。展開的結果會維持用來為群組選取主要文件的排序順序相同。

若要配置要展開的縮疊搜尋結果群組數目，請在[ExpandConfiguration](#)物件中使用MaxResultItemstoExpand參數。例如，如果將此值設定為 10，則只有 100 個結果群組中的前 10 個具有展開功能。

若要配置每個摺疊的主要文件要顯示的展開結果數目，請使用MaxExpandResultsPerItem參數。例如，如果您將此值設定為 3，則每個摺疊群組最多會顯示 3 個結果。

與其他 Amazon Kendra 功能的互動

- 收合和展開結果不會變更刻面數，也不會影響顯示的結果總數。
- Amazon Kendra 即使[精選搜尋結果](#)的欄位值與您設定的收合欄位值相同，也不會收合。
- 收合和展開結果僅適用於類型DOCUMENT的結果。

調整搜尋相關性

Amazon Kendra 查詢會產生依其相關性排名的搜尋結果。索引中的可搜索字段或屬性都有助於此排名。

您可以透過相關性調整來修改欄位或屬性對搜尋相關性的影響。您可以在索引層級手動調整搜尋相關性，也可以在索引層級設定調整組態，或者在查詢層級透過覆寫在索引層級設定的組態來完成。

當您使用相關性調整時，當查詢包含符合欄位或屬性的字詞時，系統會提升回應結果。您也可以指定當有相符項目時，文件會收到多少提升。相關性調整不會導 Amazon Kendra 致在查詢響應中包含文檔，它只是 Amazon Kendra 用於確定文檔相關性的因素之一。

您可以提升索引中的特定欄位或屬性，為特定回應指派更多重要性。例如，當有人搜索「什麼時候是 re：發明？」您可以提高該領域文檔新鮮度的相關 `_last_update_at` 性。或者，在研究報告的索引中，您可以在「源」字段中提升特定數據源。

您還可以根據論壇和其他支持知識庫中常見的投票或查看次數來提高文檔。您可以結合增強功能，例如增強檢視更多、更新的文件。

您可以使用 `Importance` 參數來設定文件接收的提升量。越高 `Importance`，欄位或屬性越多，就會提高文件的相關性。當您在查詢層級調整索引或 `tune` 時，請以較小的遞增方式增加 `Importance` 參數的值，直到您得到想要的效果為止。若要判斷是否要改善搜尋結果，請執行搜尋並將結果與先前的查詢進行比較。

您可以指定日期、數字或字串屬性，以便在查詢層級調整索引或調整。您 `StringList` 只能在索引層級調整類型的欄位或屬性。每個欄位或屬性都有特定條件，以便在提升結果時使用。

- 日期欄位或屬性 — 日期欄位、`DurationFreshness` 和 `RankOrder` 有三個特定條件。
 - `Duration` 設定提升套用至的時間週期。例如，如果您將時間範圍設定為 86400 秒 (即一天)，則增幅會在一天後開始減少。重要性越高，增強效果就越快就會減少。
 - `Freshness` 決定將文件套用至欄位或屬性時的最近程度。如果您套用 `Freshness` 至建立日期或上次更新日期的欄位，則會將最近建立或最後更新的文件視為比較舊的文件「更新」。例如，如果文件 1 是在 11 月 14 日建立的，而文件 2 是在 11 月 5 日建立的，則文件 1 會比文件 2「新鮮」。而且，如果文件 1 上次在 11 月 14 日更新，文件 2 最後更新於 11 月 20 日，則文件 2 比文件 1「更新」。文檔越新鮮，應用的這種提升就越多。您的索引中只能有一個 `Freshness` 欄位。
 - `RankOrder` 以遞增或遞減順序套用提升。如果您指定 `ASCENDING`，則較晚的日期具有優先順序。如果您指定 `DESCENDING`，較早的日期具有優先順序。

- 數字欄位或屬性 — 對於數字欄位或屬性，您可以指定決定欄位或屬性相關性時 Amazon Kendra 應使用的排名順序。如果您指定ASCENDING，則會優先考慮較高的數字。如果您指定DESCENDING，則較低的數字具有優先順序。
- 字串欄位或屬性 — 對於字串欄位或屬性，您可以建立欄位的類別，讓每個類別都有不同的提升。例如，如果您提升名為「部門」的欄位或屬性，您可以對「HR」的文件提供不同的提升，而不是「法律」中的文件。您可以提高類型的字段或屬性String。您只能在索引層級提升StringList欄位。

在索引層級進行相關性調整

您可以使用[主控台](#)在索引詳細資料或 [UpdateIndex](#)API 中設定調整，來調整索引層級的欄位或屬性的相關性。

下列範例會將_last_updated_at欄位設定為文件的Freshness欄位。

```
"DocumentMetadataConfigurationUpdates" : [  
  {  
    "Name": "_last_updated_at",  
    "Type": "DATE_VALUE",  
    "Relevance": {  
      "Freshness": TRUE,  
      "Importance": 2  
    }  
  }  
]
```

下列範例會將不同的重要性套用至「部門」欄位中的不同類別。

```
"DocumentMetadataConfigurationUpdates" : [  
  {  
    "Name": "department",  
    "Type": "STRING_VALUE",  
    "Relevance": {  
      "Importance": 2,  
      "ValueImportanceMap": {  
        "HR": 3,  
        "Legal": 1  
      }  
    }  
  }  
]
```


在查詢層級進行相關性調整

[您可以使用查詢 API 在查詢層級調整欄位或屬性的相關性。](#)

主控台不支援在查詢層級進行相關性調整。

在查詢層級進行調整可以加快測試相關性調整的過程，因為您不需要為每個測試手動更新索引中的調整配置。您可以通過在查詢中傳遞調整配置來調整文檔的相關性。然後，您可以看到從不同配置獲得的不同結果。在查詢中傳遞的組態會覆寫在索引層級設定的組態。

下列範例會覆寫套用至「部門」欄位的重要性，以及在索引層級設定的每個部門類別，如上述範例所示。當用戶輸入搜索查詢時，「部門」字段具有公平的重要性，而法律部門比人力資源部門更重要。

```
"DocumentRelevanceOverrideConfigurations" : [
  {
    "Name": "department",
    "Type": "STRING_VALUE",
    "Relevance": {
      "Importance": 2,
      "ValueImportanceMap": {
        "HR": 2,
        "Legal": 8
      }
    }
  }
]
```

透過搜尋分析獲得洞察

您可以使用 Amazon Kendra 搜尋 Analytics 來深入瞭解搜尋應用程式如何成功或未成功協助使用者尋找資訊。

Amazon Kendra Analytics (分析) 提供使用者如何與搜尋應用程式互動的快照，以及搜尋應用程式設定的有效性。您可以使用 [GetSnapshots](#) API 或在主控台的導覽面板上選取 Analytics 來檢視指標資料。

您可以在自己的定制儀表板 GetSnapshots 上呈現由生成的數據。或者，您可以使用控制台中提供的指標儀表板，其中包括視覺化圖形。透過視覺化儀表板，您可以尋找一段時間內的使用者行為趨勢或模式，或是顯示搜尋應用程式組態的問題。例如，顯示每天查詢數量一致且穩定增加的折線圖可能表示採用率和使用量有所增加。另一方面，突然下降可能表明存在必須調查的問題。

您可以使用指標在不同資料點之間建立連線，以解決使用者如何查詢資訊或發現商機的問題。例如，文檔「AI 如何工作？」是搜尋結果中點擊次數最多的文件，搜尋最多的查詢是「機器學習如何運作？」。這會通知您使用者使用的慣用條款和語言。您可以將這些字詞整合到文件中，或針對這些字詞使用自訂同義詞，讓您的文件更容易搜尋到您的使用者。

搜尋量度

有 10 個指標可用於分析搜尋應用程式的效能或使用者搜尋的資訊。若要擷取指標資料，請指定呼叫時要擷取的測量結果資料的字串名稱 GetSnapshots。

您也必須提供時間間隔或時間範圍，才能檢視測量結果資料。時間間隔會使用索引的時區。您可以在下列時間範圍中檢視資料：

- `THIS_WEEK`: 本週，從星期日開始，在目前日期的前一天結束。
- `ONE_WEEK_AGO`: 前一週，從星期日開始，在下一個星期六結束。
- `TWO_WEEKS_AGO`: 前一週的前一週，從星期日開始，在下一個星期六結束。
- `THIS_MONTH`: 當月，從當月的第一天開始，到目前日期的前一天結束。
- `ONE_MONTH_AGO`: 上個月，從每月的第一天開始，到該月的最後一天結束。
- `TWO_MONTHS_AGO`: 上個月的前一個月，從該月的第一天開始，到該月的最後一天結束。

在控制台中，支持的時間窗口是本週，上週，本月，上個月。

點擊率

在搜尋結果中導致點進至文件的查詢比例。這可協助您瞭解搜尋應用程式組態是否可協助您的使用者尋找與其查詢相關的資訊。對於傳回即時答案的查詢，使用者可能不需要按一下文件以取得更多資訊。如需詳細資訊，請參閱 [the section called “即時答案率”](#)。您必須致電 [SubmitFeedback](#) 以確保收集點擊回饋。

若要使用 GetSnapshots API 擷取點進率的資料，請指定 `metricType` 為 `AGG_QUERY_DOC_METRICS`。您也可以在主控台中選取導覽面板上的 Analytics 來檢視此量度。

零點擊率

在搜尋結果中導致零點擊的查詢比例。這可以幫助您了解內容中的差距，從而提供無關的搜索結果。對於傳回即時答案的查詢，使用者可能不需要按一下文件以取得更多資訊。如需詳細資訊，請參閱 [the section called “即時答案率”](#)。此外，您的搜尋設定 (例如調整組態) 也會影響搜尋結果中傳回文件的方式。

若要使用 GetSnapshots API 擷取零點擊率的資料，請指定 `metricType` 為 `AGG_QUERY_DOC_METRICS`。您也可以在主控台中選取導覽面板上的 Analytics 來檢視此量度。

零搜索結果率

導致搜尋結果為零的查詢比例。這可以幫助您了解內容中的差距，而不會提供相關的搜索結果。

若要使用 GetSnapshots API 擷取搜尋結果率為零的資料，請指定 `metricType` 為 `AGG_QUERY_DOC_METRICS`。您也可以在主控台中選取導覽面板上的 Analytics 來檢視此量度。

即時答案率

返回具有即時答案或常見問題解答的查詢比例。這有助於您了解即時答案在提供信息方面的作用。

若要使用 GetSnapshots API 擷取即時回答率的資料，請指定 `metricType` 為 `AGG_QUERY_DOC_METRICS`。您也可以在主控台中選取導覽面板上的 Analytics 來檢視此量度。

熱門查詢

您的使用者搜尋的前 100 個查詢。這可協助您瞭解哪些查詢最受歡迎，以及使用者最感興趣的資訊種類。

量度包括搜尋查詢的次數、文件點進次數的比例、文件無點進的比例、查詢搜尋結果的平均點按深度、查詢的即時答案比例，以及查詢前 10 個搜尋結果的平均信賴度。

若要使用 GetSnapshots API 擷取常用查詢的資料，請指定 `metricType` 為 `QUERIES_BY_COUNT`。您也可以在主控台中選取導覽面板上的 Analytics，然後選取 [查詢清單] 下的 [常用查詢]，在主控台中檢視此量度。

零點擊的熱門查詢

在搜尋結果中導致零點擊的前 100 名查詢。這可協助您瞭解內容中的任何差距，因為缺少與某些查詢相關的文件，或者您的搜尋應用程式組態會傳回不相關的搜尋結果。對於傳回即時答案的查詢，使用者可能不需要按一下文件以取得更多資訊。如需詳細資訊，請參閱 [the section called “即時答案率”](#)。

指標包括查詢導致零點擊次數的次數、查詢的零點擊比例、查詢的即時答案比例，以及查詢前 10 個搜尋結果的平均信賴度。

若要使用 GetSnapshots API 以零點選的方式擷取熱門查詢的資料，請指定 `metricType` 為 `QUERIES_BY_ZERO_CLICK_RATE`。您也可以在主控台中選取導覽面板上的 Analytics，然後選取 [查詢清單] 下的 [前零點擊查詢]，在主控台中檢視此量度。

搜尋結果為零的熱門查詢

導致搜尋結果為零的前 100 個查詢。這有助於您了解內容中的任何差距，其中沒有與某些查詢相關的文檔。或者，您的使用者可能會使用可能不會導致搜尋結果的特殊字詞進行查詢，並提示您建立 [自訂同義字](#) 來處理此問題。

量度包括查詢導致搜尋結果為零的次數、查詢的搜尋結果為零的比例，以及搜尋查詢與所有查詢相比的次數比例。

若要使用 GetSnapshots API 擷取搜尋結果為零的熱門查詢資料，請指定 `metricType` 為 `QUERIES_BY_ZERO_RESULT_RATE`。您也可以在主控台中選取導覽面板上的 Analytics，然後選取 [查詢清單] 下的 [前零結果查詢]，在主控台中檢視此量度。

點擊頂部的文檔

搜尋結果中點擊次數最多的 100 個文件。這有助於您瞭解哪些文件或搜尋結果在使用者查詢資訊時最相關。

指標包括文件被點擊的次數、文件從使用者收到的喜歡次數 (豎起大拇指)、文件從使用者那裡收到的不喜歡次數 (豎起大拇指)。

要使用 GetSnapshots API 檢索頂部單擊文檔的數據，請指定 `metricType` 為 `DOCS_BY_CLICK_COUNT`。您也可以在主控台中檢視此量度，方法是選取主控台中導覽面板上的 Analytics，然後選取 [查詢清單] 下的 [點選最多的文件]。

查詢總數

您的使用者搜尋的查詢總數。這可協助您瞭解使用者與搜尋應用程式的互動程度。

若要使用 GetSnapshots API 擷取總查詢的資料，請指定 `metricType` 為 `AGG_QUERY_DOC_METRICS`。您也可以在主控台中選取導覽面板上的 Analytics 來檢視此量度。

文件總數

索引中的文件總數。這有助於您將索引的大小與查詢總數進行比較，以檢查查詢量是否有適當數量的文檔。

若要使用 GetSnapshots API 擷取全部文件的資料，請指定 `metricType` 為 `AGG_QUERY_DOC_METRICS`。您也可以在主控台中選取導覽面板上的 Analytics 來檢視此量度。

擷取測量結果資料的範例

下列程式碼是擷取上個月最常用查詢資料的範例。

Console

若要擷取上個月的前幾個查詢

1. 在左側導覽窗格的 [索引] 下，選取您的索引，然後選取 [分析]。
2. 在「分析」頁面上，選擇「本週」按鈕，將用於檢索數據的時間窗口更改為上個月。

3. 在「分析」頁面的「查詢清單」下，選取「熱門查詢」。

CLI

若要擷取上個月的前幾個查詢

```
aws kendra get-snapshots \  
--index-id index-id \  
--interval "ONE_MONTH_AGO" \  
--metric-type "QUERIES_BY_COUNT"
```

Python

若要擷取上個月的前幾個查詢

```
import boto3  
  
kendra = boto3.client("kendra")  
  
index_id = "index-id"  
interval = "ONE_MONTH_AGO"  
metric_type = "QUERIES_BY_COUNT"  
  
snapshots_response = kendra.get_snapshots(  
    IndexId = index_id,  
    Interval = interval,  
    MetricType = metric_type  
)  
  
print("Top queries data: " + snapshots_response["snapshotsData"])
```

Java

若要擷取上個月的前幾個查詢

```
package com.amazonaws.kendra;  
  
import software.amazon.awssdk.services.kendra.KendraClient;  
import software.amazon.awssdk.services.kendra.model.GetSnapshotsRequest;  
import software.amazon.awssdk.services.kendra.model.GetSnapshotsResponse;  
  
public class TopQueriesExample {
```

```
public static void main(String[] args) {
    KendraClient kendra = KendraClient.builder().build();

    String indexId = "indexID";
    String interval = "ONE_MONTH_AGO";
    String metricType = "QUERIES_BY_COUNT";

    GetSnapshotsRequest getSnapshotsRequest = GetSnapshotsRequest
        .builder()
        .indexId(indexId)
        .interval(interval)
        .metricType(metricType)
        .build();

    GetSnapshotsResponse getSnapshotsResponse =
kendra.getSnapshots(GetSnapshotsRequest);

    System.out.println(String.format("Top queries data: ",
getSnapshotsResponse.snapshotsData()))
}
```

從指標到可行的洞察

可操作的見解是從原始數據中提取的有意義的信息片段，用於指導您的行動或決策。要從指標中提取含義並使用它們來推動可行的見解，重要的是不僅要隔離查看指標，還要在指標之間建立連接。

例如，無點擊次數的最佳查詢是「目前有哪些地區可用？」。但是，它也具有 100% 的即時答案率。這表明您的使用者會收到此問題的答案，而不需要按一下搜尋結果或提供可用區域資訊的文件。如果您單獨查看零點擊，則無法獲得完整的故事，並且可能會對搜索應用程序配置在處理此查詢時的成功做出錯誤的結論。

另一個可操作洞察的例子是發現商機。企業通常會尋找通過分析搜索指標來增加客戶的機會。點擊次數最多的文檔是「可用區域」。除此之外，大多數搜尋最熱門的查詢都與 Oceanic 地區產品可用性相關問題，其中 100% 即時回答率和較高的點擊率，以取得有關可用區域的更多資訊，作為答案的一部分。這表明在這個地區對您的產品或服務有興趣和需求。

視覺化和報告搜尋分析

有五個指標包含趨勢資料，供您視覺化並尋找一段時間內的趨勢或模式。如果您使用主控台，則會提供趨勢資料的圖形。如果您使用 API，您可以擷取趨勢資料以建立自己的圖形或視覺效果。控制台中的大多數圖表都會在您選擇的時間範圍內繪製每日數據點。

控制台提供指標的儀表板，您可以在其中選擇您感興趣查看的圖形和頂級列表。您可以選取 Analytics (分析) 首頁上的「匯出」，以 CSV 格式匯出儀表板上顯示的指標。您可以在業務文件或簡報中包含這些報告。

您可以視覺化以下指標：

查詢總計圖表

每天發出的查詢數目的折線圖。此圖表可協助您視覺化日常使用者參與度中的模式。一些示例包括用戶參與度的穩定增加或減少，或者由於搜索應用程序崩潰或網站問題而急劇下降到 0 查詢。

如果您使用 API，您可以透過指定來擷取這些資料TREND_QUERY_DOC_METRICS。您可以使用數據創建自己的圖形，或使用控制台中提供的圖形。

點擊率圖

每日點進比例的折線圖。此圖表可協助您以視覺化方式呈現每日點進率的模式。一些例子包括點擊率穩定增加或下降，或者即時答案的下降可能會影響點擊率的增加。

如果您使用 API，您可以透過指定來擷取這些資料TREND_QUERY_DOC_METRICS。您可以使用數據創建自己的圖形，或使用控制台中提供的圖形。

零點擊率圖

每天零點擊比例的折線圖。該圖可幫助您以每日零點擊率視覺化模式。一些例子包括穩定增加或減少零點擊率，或者即時答案的增加可能會影響零點擊的增加。

如果您使用 API，您可以透過指定來擷取這些資料TREND_QUERY_DOC_METRICS。您可以使用數據創建自己的圖形，或使用控制台中提供的圖形。

零搜尋結果比率圖

每天零搜尋結果比例的折線圖。該圖可幫助您將每日零搜索結果率中的模式視覺化。有些範例包括搜尋結果率穩定增加或減少為零，或索引中的文件數量急劇減少，可能會影響搜尋結果零的增加。

如果您使用 API，您可以透過指定來擷取這些資料TREND_QUERY_DOC_METRICS。您可以使用數據創建自己的圖形，或使用控制台中提供的圖形。

即時答案率圖

返回即時答案或常見問題解答的查詢比例的折線圖。該圖可幫助您以每日即時答案率視覺化模式。一些例子包括問答類型查詢的穩定增加或減少，或者點擊次數的減少可能會影響即時答案的增加。

如果您使用 API，您可以透過指定來擷取這些資料TREND_QUERY_DOC_METRICS。您可以使用數據創建自己的圖形，或使用控制台中提供的圖形。

提交漸進學習的意見反應

Amazon Kendra 使用漸進式學習來改善搜尋結果。使用來自查詢的反饋，增量學習可以改善排名算法並優化搜索結果以提高準確性。

例如，假設您的使用者搜尋「醫療保健福利」一詞。如果用戶始終從列表中選擇第二個結果，則隨著時間的 Amazon Kendra 推移將結果提高到第一名結果。提升會隨著時間的推移而減少，因此，如果用戶停止選擇結果，Amazon Kendra 最終將其刪除並顯示另一個更受歡迎的結果。這有助於根據相關性、年齡和內容 Amazon Kendra 排定結果的優先順序。

會針對所有索引和所有[支援的文件類型](#)啟動增量學習。

Amazon Kendra 只要您提供意見反應，就會立即開始學習，但可能需要超過 24 小時才能看到意見反應的結果。Amazon Kendra 提供三種方法供您提交意見反應：AWS 主控台、可包含在搜尋結果頁面上的 JavaScript 資料庫，以及可使用的 API。

Amazon Kendra 接受兩種類型的用戶反饋：

- 按一下 — 使用者選擇哪個查詢結果的相關資訊。反饋包括結果 ID 和選擇搜索結果的日期和時間的 Unix 時間戳。

要提交點擊反饋，您的應用程式必須從用戶的活動中收集點擊信息，然後將該信息提交給 Amazon Kendra。您可以使用主控台、程式 JavaScript 庫和 Amazon Kendra API 收集點擊資訊。

- 相關性 — 使用者通常會提供的搜尋結果相關性的相關性資訊。意見反應包含結果 ID 和相關性指示器 (RELEVANT 或 NOT_RELEVANT)。使用者決定相關性資訊。

若要提交相關性意見反應，您的應用程式必須提供意見反應機制，讓使用者為查詢結果選擇適當的相關性，然後將該資訊提交給 Amazon Kendra。您只能透過主控台和 Amazon Kendra API 收集相關性資訊。

當索引處於作用中狀態時，會使用回饋。意見反應只會影響提交的索引，不能跨索引或不同帳戶使用。

當您查詢 Amazon Kendra 索引時，您應該提供額外的使用者內容。當您提供使用者內容時，Amazon Kendra 可以判斷意見反應是由單一使用者還是由多位使用者提供，並相應地調整搜尋結果。

當您提供使用者前後關聯時，查詢的意見反應會與前後關聯中提供的特定使用者相關聯。如果您未指定使用者內容，則可以提供用於分組和彙總查詢的訪客 ID。

如果您未提供使用者內容或訪客 ID，則意見反應是匿名的，並與其他匿名意見彙總。

下列程式碼顯示如何將使用者內容包含為權杖或訪客 ID。

```
response = kendra.query(  
  QueryText = query,  
  IndexId = index,  
  UserToken = {  
    Token = "token"  
  })  
  
OR  
  
response = kendra.query(  
  QueryText = query,  
  IndexId = index,  
  VisitorId = "visitor-id")
```

對於 Web 應用程式，您可以使用 Cookie、位置或瀏覽器使用者為每個使用者產生訪客 ID。

對於標頭查詢，提供點擊回饋的查詢量最大可提供足夠的資訊來提高整體準確性。對於尾部查詢，那些罕見的主題專家應提交相關且不相關的回饋，以提高這些查詢的準確性。

除了控制台之外，您還可以使用以下兩種方法之一：JavaScript 庫或 [SubmitFeedbackAPI](#)。你應該只使用其中一種收集信用評價的方法。為了獲得最佳結果，您應該在查詢後的 24 小時內提交回饋。

主題

- [使用圖 Amazon Kendra JavaScript 書館提交意見反應](#)
- [使用 Amazon Kendra API 提交意見反應](#)

使用圖 Amazon Kendra JavaScript 書館提交意見反應

Amazon Kendra 提供一個 JavaScript 資料庫，讓您可以將點擊回饋新增至搜尋結果頁面。若要使用元件庫，請在用戶端程式碼中插入指令碼標記以顯示搜尋結果，然後將資訊新增至結果清單中的每個文件連結。當使用者選擇檢視文件的連結時，按一下資訊會傳送至 Amazon Kendra。

該庫適用於支持 ES6/ES2015 JavaScript 版本的瀏覽器。

步驟 1：在 Amazon Kendra 搜尋應用程式中插入指令碼標記

在呈現 Amazon Kendra 搜尋結果的用戶端程式碼中，插入<script>標籤並將參考新增至程式 JavaScript 庫：

```

<script>
(function(w, d, s, c, g, n) {
  if(!w[n]) {
    w[n] = w[n] || function () {
      (w[n].q = w[n].q || []).push(arguments);
    }
    w[n].st = new Date().getTime();
    w[n].ep = g;
    var e = document.createElement(s),
        j = document.getElementsByTagName(s)[0];
    e.async = 1;
    e.src = c;
    e.type = 'module';
    j.parentNode.insertBefore(e, j);
  }
})(window, document, 'script',
'library download URL',
'feedback endpoint',
'kendraFeedback');
</script>

```

指令碼會以非同步方式從 Amazon Kendra 託管的 CDN 下載程式 JavaScript 庫，並初始化名為的全域變數，可 `kendraFeedback` 讓您設定選擇性參數。

根據託管 Amazon Kendra 索引的地區，將程式 `### URL` 和 `#####` 取代為下表中的識別碼。

區域	下載 URL	反饋端點
us-east-1	https://d2zm0lpns956f8.cloudfront.net/ksf-v1.js	https://ujxwp5s92h.execute-api.us-east-1.amazonaws.com/prod/submit
us-east-2	https://d2crv7fufeg244.cloudfront.net/ksf-v1.js	https://i6h76zwzf3.execute-api.us-east-2.amazonaws.com/prod/submit
us-west-2	https://d2iezfpnpoujy.cloudfront.net/ksf-v1.js	https://wg6nim909c.execute-api.us-west-2.amazonaws.com/prod/submit

區域	下載 URL	反饋端點
ca-central-1	https://d1zbfomowykaq.cloudfront.net/ksf-v1.js	https://budi8txevj.execute-api.ca-central-1.amazonaws.com/prod/submit
eu-west-1	https://d3gptlxtulu4us.cloudfront.net/ksf-v1.js	https://po2b11740b.execute-api.eu-west-1.amazonaws.com/prod/submit
ap-southeast-1	https://d1vvuam7g4taoe.cloudfront.net/ksf-v1	https://9je5uw7t5l.execute-api.ap-southeast-1.amazonaws.com/prod/submit
ap-southeast-2	https://dopqntoe6z0ce.cloudfront.net/ksf-v1.js	https://oovf4nvjj7.execute-api.ap-southeast-2.amazonaws.com/prod/submit
ap-south-1	https://d1ts9ouelsmk3g.cloudfront.net/ksf-v1.js	https://k1abnmd43b.execute-api.ap-south-1.amazonaws.com/prod/submit
ap-northeast-1	https://d3w0ybsa293kb4.cloudfront.net/ksf-v1.js	https://wg7rz0uzjh.execute-api.ap-northeast-1.amazonaws.com/prod/submit
eu-west-2	https://d1tsrujswld1d1.cloudfront.net/ksf-v1.js	https://qi7mct3x7f.execute-api.eu-west-2.amazonaws.com/prod/submit

例如，如果您的索引位於美國東部（維吉尼亞北部），則程式### URL 為<https://d2zm0lpns956f8.cloudfront.net/ksf-v1.js>，##### 為<https://ujxwp5s92h.execute-api.us-east-1.amazonaws.com/prod/submit>。

您可以為程式 Amazon Kendra JavaScript 庫進行兩種選擇性設定：

- `disableCookies`— 默認情況下，Amazon Kendra 設置唯一標識用戶的 cookie。將此項設定 `true` 為以停用 Cookie。

```
kendraFeedback('disableCookie', 'true | false');
```

searchDivClassName-默認情況下，Amazon Kendra 監控您的搜索結果頁面上的點擊所有鏈接。將此項設定為<div>類別名稱，以僅監視指定類別中的連結。

```
kendraFeedback('searchDivClassName', 'class name');
```

步驟 2：將意見反應記號新增至搜尋結果

在結果頁面上，新增名data-kendra-token為錨點標籤的 HTML 屬性，或是包含查詢回應之文件連結的直接父 div 標籤。例如：

```
<a href="document location" data-kendra-token="feedback token value"></a>  
OR  
<div data-url="document location" data-kendra-token="feedback token value"></div>
```

查詢響應在feedbackToken字段中包含令牌。如果使用者選擇回應，Token 會唯一識別回應。將權杖的值指派給data-kendra-token屬性。當用戶選擇結果並將其提交到 Amazon Kendra 端點作為反饋時，Amazon Kendra JavaScript 庫會查找此令牌。

程式 Amazon Kendra JavaScript 庫只會提交意見反應權杖和其他中繼資料，例如選擇結果的時間和唯一訪客 ID。

步驟 3：測試意見反應指令碼

若要確定程式 JavaScript 庫設定正確，並將意見反應傳送至正確的端點，請執行下列動作。這個例子使用 Chrome 瀏覽器。

1. 在瀏覽器中開啟 Web 開發人員工具。在 Chrome 上，打開瀏覽器右上角的 Chrome 菜單，選擇更多工具，然後選擇開發人員工具。
2. 確保控制台選項卡中沒有與 Amazon Kendra JavaScript 庫相關的錯誤。
3. 進行搜索並選擇任何結果。在開發人員工具的「網絡」選項卡中。您應該會看到傳送至意見反應端點的要求、結果的權杖，以及 200 OK 狀態。

使用 Amazon Kendra API 提交意見反應

若要使用 Amazon Kendra API 提交查詢意見反應，請使用 [SubmitFeedback](#) API。若要識別查詢，請提供查詢套用之索引的索引識別碼，並提供查詢 API 回應中傳回的 [查詢 ID](#)。

以下範例顯示如何使用 Amazon Kendra API 提交點擊和相關性意見反應。您可以透過 `ClickFeedbackItems` 和陣列提交多個 `RelevanceFeedbackItems` 組意見反應。此範例會提交一次按一下和單一相關性意見反應項目。意見反應提交會使用目前的時間。

若要提交搜尋的意見反應 (AWS SDK)

1. 您可以將下列範例程式碼與必要值搭配使用：
 - a. `index_id` 套用查詢之索引的 ID。
 - b. `query_id` 您要提供意見反應的查詢。
 - c. `result_id` 您要提供意見反應的查詢結果 ID。查詢回應包含結果 ID。
 - d. `relevance_value` `RELEVANT` (查詢結果相關) 或 `NOT_RELEVANT` (查詢結果不相關)。

Python

```
import boto3
import time

kendra = boto3.client("kendra")

# Provide the index ID
index_id = "index-id"
# Provide the query ID
query_id = "query-id"
# Provide the search result ID
result_id = "result-id"

# Configure the feedback item
feedback_item = {"ClickTime": int(time.time()),
                "ResultId": result_id}

# Configure the relevance value
relevance_value = "RELEVANT"
relevance_item = {"RelevanceValue": relevance_value,
                 "ResultId": result_id}
```

```
    }

    response = kendra.submit_feedback(
        QueryId = query_id,
        IndexId = index_id,
        ClickFeedbackItems = [feedback_item],
        RelevanceFeedbackItems = [relevance_item]
    )

    print("Submitted feedback for query: " + query_id)
```

Java

```
package com.amazonaws.kendra;

import java.time.Instant;
import software.amazon.awssdk.services.kendra.KendraClient;
import software.amazon.awssdk.services.kendra.model.ClickFeedback;
import software.amazon.awssdk.services.kendra.model.RelevanceFeedback;
import software.amazon.awssdk.services.kendra.model.RelevanceType;
import software.amazon.awssdk.services.kendra.model.SubmitFeedbackRequest;
import software.amazon.awssdk.services.kendra.model.SubmitFeedbackResponse;

public class SubmitFeedbackExample {
    public static void main(String[] args) {
        KendraClient kendra = KendraClient.builder().build();

        SubmitFeedbackRequest submitFeedbackRequest = SubmitFeedbackRequest
            .builder()
            .indexId("IndexId")
            .queryId("QueryId")
            .clickFeedbackItems(
                ClickFeedback
                    .builder()
                    .clickTime(Instant.now())
                    .resultId("ResultId")
                    .build()
            )
```



```
        .relevanceFeedbackItems(  
            RelevanceFeedback  
                .builder()  
                .relevanceValue(RelevanceType.RELEVANT)  
                .resultId("ResultId")  
                .build())  
        .build();  
  
        SubmitFeedbackResponse response =  
kendra.submitFeedback(submitFeedbackRequest);  
  
        System.out.println("Feedback is submitted");  
    }  
}
```

2. 執行程式碼。提交意見反應後，程式碼會顯示訊息。

將自訂同義字新增至索引

若要將自訂同義字新增至索引，請在同義字辭典檔案中指定它們。您可以在 Amazon Kendra 使用同義字時包含特定業務或專用術語。一般英文同義詞 (例如 leader, head) 已內建於同義字 Amazon Kendra 辭典檔案中，包括使用連字號的一般同義字。Amazon Kendra 支持所有響應類型的同義詞，包括 DOCUMENT 響應類型和 QUESTION_ANSWER 或 ANSWER 響應類型。Amazon Kendra 目前不支援新增標記為停用字詞的同義字。這將包含在 future 的版本中。

Amazon Kendra 使同義詞之間的相關性。例如，使用同義詞對 Dynamo, Amazon DynamoDB，將 Dynamo Amazon Kendra 與相關聯。Amazon DynamoDB 查詢「什麼是發電機？」然後返回一個文檔，如「什麼是 Amazon DynamoDB？」。使用同義詞，Amazon Kendra 可以更輕鬆地拾取相關性。

索引典檔案是儲存在值區中的文字檔案。Amazon S3 請參閱 [將索引典新增至索引](#)。

同義字檔案使用 [Solr](#) 同義字格式。Amazon Kendra 對每個索引的同義詞庫數量有限制。請參閱 [配額](#)。

在下列情況下，同義字可能很有用：

- 不是傳統英語語言同義詞的專業術語，例如 NLP, Natural Language Processing.
- 具有複雜語義關聯的正確名詞。這些名詞是普通大眾不太可能理解的名詞，例如，在機器學習中，. cost, loss, model performance
- 不同形式的產品名稱，例如，Elastic Compute Cloud, EC2.
- 特定網域或業務特定詞彙，例如產品名稱。例如 Route53, DNS。

請勿在下列情況下使用同義字：

- 通用英語語言同義詞，例如 leader, head. 這些同義字並非網域特有的，在這些案例中使用同義字可能會產生意想不到的影響。
- 印刷錯誤，例如 .teh => the
- 形態變體，例如名詞的複數和所有物，形容詞的比較和最高級形式以及動詞的過去式，過去分詞和漸進形式。比較和最高級形容詞的一個例子是。good, better, best
- 統一圖 (單個字) 停止詞，WHO 例如。同義字辭典中不允許使用 Unigram 停用字詞，且會從搜尋中排除。例如，WHO => World Health Organization 被拒絕。W.H.O. 但是，您可以將其用作同

義詞，並且可以使用停用詞作為多字同義詞的一部分。例如，of不允許，但United States of America被接受。

自訂同義詞可擴展查詢以涵蓋特定業務的同義詞，讓您輕鬆地改善 Amazon Kendra對特定業務術語的理解。儘管同義詞可以提高搜索準確性，但了解同義詞如何影響延遲很重要，以便您可以針對此進行優化。

同義字的一般規則是：查詢中符合和擴充同義字的字詞越多，對延遲的潛在影響就越大。影響延遲的其他因素包括索引文件的平均大小、索引的大小、搜尋結果的篩選，以及索 Amazon Kendra 引的整體負載。不符合任何同義字的查詢不會受到影響。

同義詞如何影響延遲的一般準則：

使用案例	延遲增加 *
典型的自然語言或關鍵字查詢，每個 3 到 5 個單詞	少於百分之十五
1 個查詢詞擴展為 3 個同義詞	
約 50 萬份文件的索引 (每份文件的擷取文字平均為 10.48 KB) 或 30,000 個常見問題/問題對	

* 效能會根據您在索引中對同義字和組態的特定使用情況而有所不同。最好測試搜尋效能，以針對您的特定使用案例取得更準確的基準。

如果您的索引典很大、具有很高的擴充比率，且延遲增加不在可接受的範圍內，您可以嘗試下列其中一種或兩種方法：

- 修剪索引典以降低擴充比例 (每個字詞的同義字數目)。
- 修剪字詞的整體涵蓋範圍 (索引典中的行數)。

或者，您可以增加佈建容量 (虛擬儲存單元)，以抵消延遲增加的情況。

主題

- [建立同義字辭典檔案](#)
- [將索引典新增至索引](#)

- [更新索引典](#)
- [刪除索引典](#)
- [搜尋結果中的亮點](#)

建立同義字辭典檔案

同義 Amazon Kendra 詞字典檔案是 UTF-8 編碼的檔案，其中包含 Solr 同義字清單格式的同義字清單。索引典檔案必須小於 5 MB。

有兩種方法可以指定同義字對映：

- 雙向同義字會指定為以逗號分隔的術語清單。如果您的使用者查詢任何字詞，則清單中的所有字詞都會用來搜尋包含原始查詢字詞的文件。
- 單向同義詞被指定為由它們之間的符號「=>」分隔的術語，以將術語映射到它們的同義詞。如果您的使用者查詢符號「=>」左側的術語，則會將其對應至右側的術語，以使用同義字搜尋文件。它沒有映射反之亦然，使得這是單向的。

同義詞本身是區分大小寫的，但它們映射的術語不區分大小寫。例如，ML => Machine Learning 表示如果您的使用者查詢「ML」或「ml」或使用其他情況，它會對應至「Machine Learning」。如果您要對映此反之亦然 Machine Learning => ML，則「Machine Learning」或「機器學習」或其他案例將映射到「ML」。

同義字不會搜尋特殊字元的完全相符項目。例如，如果您搜尋 "dead-letter-queue「，Amazon Kendra 可以傳回符合「無效字母佇列」(無連字號) 的文件。如果您的文件包含連字號 (例如 "dead-letter-queue「) 會在搜尋期間 Amazon Kendra 處理文件以移除連字號。對於內建 Amazon Kendra 且不應包含在索引典檔案中的一般英文同義字詞，Amazon Kendra 可以同時搜尋字詞的連字號版本和字詞的非連字號版本。例如，如果您搜尋「第三方」和「第三方」，則會 Amazon Kendra 傳回符合這些字詞任一版本的文件。

對於包含停用字詞或常用字詞的同義字，會 Amazon Kendra 傳回符合字詞 (包括停用字詞) 的文件。例如，您可以建立同義字規則來對應「登機」和「上線」。您不能單獨使用停用字詞作為同義字。例如，如果您搜尋「on」，則 Amazon Kendra 無法傳回包含「開啟」的所有文件。

某些同義字規則會被忽略。例如，a => b 這是一個規則，但會 a => a 被忽略，並且不算作規則。

術語計數是 theaurus 檔案中唯一字詞的數目。下面的示例文件包括術語 AWS CodeStar ML Machine Learning, autoscaling group, , ASG, 和更多。

每個同義字辭典有最大數量的同義字規則，而每個字詞的同義字數量上限為上限。如需詳細資訊，請參閱 [的配額 Amazon Kendra](#)。

下列範例顯示具有同義字規則的同義字字典檔案。每一行都包含一個同義字規則。空白行和註釋將被忽略。

```
# Lines starting with pound are comments and blank lines are ignored.

# Synonym relationships can be defined as unidirectional or bidirectional
relationships.

# Unidirection relationships are represented by any term sequence
# on the left hand side (LHS) of "=>" followed by synonyms on the right hand side (RHS)
CodeStar => AWS CodeStar
# This will map CodeStar to AWS CodeStar, but not vice-versa

# To map terms vice versa
ML => Machine Learning
Machine Learning => ML

# Multiple synonym relationships may be defined in one line as well by comma
seperation.
autoscaling group, ASG => Auto Scaling group, autoscaling
# The above is equivalent to:
# autoscaling group => Auto Scaling group, autoscaling
# ASG => Auto Scaling group, autoscaling

# Bi-directional synonyms are comma separated terms with no "=>"
DNS, Route53, Route 53
# DNS, Route53, and Route 53 map to one another and are interchangeable at match time
# The above is equivalent to:
# DNS => Route53, Route 53
# Route53 => DNS, Route 53
# Route 53 => DNS, Route53

# Overlapping LHS terms will be merged
Beta => Alpha
Beta => Gamma
Beta, Delta
# is equivalent to:
# Beta => Alpha, Gamma, Delta
# Delta => Beta
```

```
# Each line contains a single synonym rule.
# Synonym rule count is the total number of lines defining synonym relationships
# Term count is the total number of unique terms for all rules.
# Comments and blanks lines do not count.
```

將索引典新增至索引

下列程序顯示如何將包含同義字的索引典檔案新增至索引。您最多可能需要 30 分鐘才能看到更新的索引典檔案的效果。如需索引典檔案的詳細資訊，請參閱。[建立同義字辭典檔案](#)

Console

若要新增索引典

1. 在左側導覽窗格中，在您要新增同義字清單的索引下，選擇同義詞字典。
2. 在「同義字」頁面上，選擇「新增同義字辭典」。
3. 在定義索引典中，為您的索引典指定名稱和選擇性說明。
4. 在索引典設定中，提供索引典檔案的 Amazon S3 路徑。檔案必須小於 5 MB。
5. 對於 IAM 角色，請選取角色或選取建立新角色並指定角色名稱以建立新角色。Amazon Kendra 使用此角色代表您存取 Amazon S3 資源。IAM 角色的前置詞為「AmazonKendra-」。
6. 選擇 [儲存] 以儲存組態並新增索引典。一旦擷取同義字辭典，它就是作用中的，且同義字會在結果中反白顯示。查看索引典檔案的效果最多可能需要 30 分鐘。

CLI

若要使用新增索引至索引 AWS CLI，請呼叫：`create-thesaurus`

```
aws kendra create-thesaurus \
--index-id index-id \
--name "thesaurus-name" \
--description "thesaurus-description" \
--source-s3-path "Bucket=bucket-name,Key=thesaurus/synonyms.txt" \
--role-arn role-arn
```

呼叫`list-thesauri`以查看索引典清單：

```
aws kendra list-thesauri \
--index-id index-id
```

若要檢視索引典的詳細資料，請呼叫：`describe-thesaurus`

```
aws kendra describe-thesaurus \  
--index-id index-id \  
--index-id thesaurus-id
```

查看索引典檔案的效果最多可能需要 30 分鐘。

Python

```
import boto3  
from botocore.exceptions import ClientError  
import pprint  
import time  
  
kendra = boto3.client("kendra")  
  
print("Create a thesaurus")  
  
thesaurus_name = "thesaurus-name"  
thesaurus_description = "thesaurus-description"  
thesaurus_role_arn = "role-arn"  
  
index_id = "index-id"  
  
s3_bucket_name = "bucket-name"  
s3_key = "thesaurus-file"  
source_s3_path = {  
    'Bucket': s3_bucket_name,  
    'Key': s3_key  
}  
  
try:  
    thesaurus_response = kendra.create_thesaurus(  
        Description = thesaurus_description,  
        Name = thesaurus_name,  
        RoleArn = thesaurus_role_arn,  
        IndexId = index_id,  
        SourceS3Path = source_s3_path  
    )  
  
    pprint.pprint(thesaurus_response)  
  
    thesaurus_id = thesaurus_response["Id"]
```

```
print("Wait for Kendra to create the thesaurus.")

while True:
    # Get thesaurus description
    thesaurus_description = kendra.describe_thesaurus(
        Id = thesaurus_id,
        IndexId = index_id
    )
    # If status is not CREATING quit
    status = thesaurus_description["Status"]
    print("Creating thesaurus. Status: " + status)
    if status != "CREATING":
        break
    time.sleep(60)

except ClientError as e:
    print("%s" % e)

print("Program ends.")
```

Java

```
package com.amazonaws.kendra;

import software.amazon.awssdk.services.kendra.KendraClient;
import software.amazon.awssdk.services.kendra.model.CreateThesaurusRequest;
import software.amazon.awssdk.services.kendra.model.CreateThesaurusResponse;
import software.amazon.awssdk.services.kendra.model.DescribeThesaurusRequest;
import software.amazon.awssdk.services.kendra.model.DescribeThesaurusResponse;
import software.amazon.awssdk.services.kendra.model.S3Path;
import software.amazon.awssdk.services.kendra.model.ThesaurusStatus;

public class CreateThesaurusExample {

    public static void main(String[] args) throws InterruptedException {

        KendraClient kendra = KendraClient.builder().build();

        String thesaurusName = "thesaurus-name";
        String thesaurusDescription = "thesaurus-description";
        String thesaurusRoleArn = "role-arn";
```



```
String s3BucketName = "bucket-name";
String s3Key = "thesaurus-file";
String indexId = "index-id";

System.out.println(String.format("Creating a thesaurus named %s",
thesaurusName));
CreateThesaurusRequest createThesaurusRequest = CreateThesaurusRequest
    .builder()
    .name(thesaurusName)
    .indexId(indexId)
    .description(thesaurusDescription)
    .roleArn(thesaurusRoleArn)
    .sourceS3Path(S3Path.builder()
        .bucket(s3BucketName)
        .key(s3Key)
        .build())
    .build();
CreateThesaurusResponse createThesaurusResponse =
kendra.createThesaurus(createThesaurusRequest);
System.out.println(String.format("Thesaurus response %s",
createThesaurusResponse));

String thesaurusId = createThesaurusResponse.id();

System.out.println(String.format("Waiting until the thesaurus with ID %s is
created.", thesaurusId));

while (true) {
    DescribeThesaurusRequest describeThesaurusRequest =
DescribeThesaurusRequest.builder()
    .id(thesaurusId)
    .indexId(indexId)
    .build();
    DescribeThesaurusResponse describeThesaurusResponse =
kendra.describeThesaurus(describeThesaurusRequest);
    ThesaurusStatus status = describeThesaurusResponse.status();
    if (status != ThesaurusStatus.CREATING) {
        break;
    }

    TimeUnit.SECONDS.sleep(60);
}

System.out.println("Thesaurus creation is complete.");
```

```
}  
}
```

更新索引典

您可以在建立索引典之後變更其組態。您可以變更索引典名稱和 IAM 資訊等詳細資料。您也可以變更索引典檔案 Amazon S3 路徑的位置。如果您變更索引典檔案的路徑，Amazon Kendra 會以更新路徑中指定的索引典取代現有的索引典。

您最多可能需要 30 分鐘才能看到更新的索引典檔案的效果。

Note

如果索引典檔案中有驗證或語法錯誤，則會保留先前上傳的索引典檔案。

下列程序顯示如何修改索引典詳細資料。

Console

若要修改索引典詳細資料

1. 在左側導覽窗格的索引下，選擇 [同義字]。
2. 在「同義字」頁面上，選取您要修改的同義字辭典，然後選擇「編輯」。
3. 在 [更新索引典] 頁面上，更新索引典詳細資料。
4. (選擇性) 選擇 [變更索引典檔案路徑]，然後指定新索引典檔案的 Amazon S3 路徑。您現有的索引典檔案會由您指定的檔案取代。如果您不變更路徑，請從現有路徑 Amazon Kendra 重新載入同義字辭典。

如果您選取「保留目前的索引典檔案」，則 Amazon Kendra 不會重新載入同義字辭典檔案。

5. 選擇 [儲存] 以儲存組態。

您也可以從現有的索引典路徑重新載入索引典。

從既有路徑重新載入同義字辭典

1. 在左側導覽窗格的索引下，選擇 [同義字]。

2. 在「同義字」頁面上，選取您要重新載入的同義字辭典，然後選擇「重新整理」。
3. 在 [重新載入索引典檔案] 頁面上，確認您要重新整理索引典檔案。

CLI

若要更新索引典，請呼叫：`update-thesaurus`

```
aws kendra update-thesaurus \  
--index-id index-id \  
--name "thesaurus-name" \  
--description "thesaurus-description" \  
--source-s3-path "Bucket=bucket-name,Key=thesaurus/synonyms.txt" \  
--role-arn role-arn
```

Python

```
import boto3  
from botocore.exceptions import ClientError  
import pprint  
import time  
  
kendra = boto3.client("kendra")  
  
print("Update a thesaurus")  
  
thesaurus_name = "thesaurus-name"  
thesaurus_description = "thesaurus-description"  
thesaurus_role_arn = "role-arn"  
  
thesaurus_id = "thesaurus-id"  
index_id = "index-id"  
  
s3_bucket_name = "bucket-name"  
s3_key = "thesaurus-file"  
source_s3_path = {  
    'Bucket': s3_bucket_name,  
    'Key': s3_key  
}  
  
try:  
    kendra.update_thesaurus(  
        Id = thesaurus_id,
```

```
        IndexId = index_id,
        Description = thesaurus_description,
        Name = thesaurus_name,
        RoleArn = thesaurus_role_arn,
        SourceS3Path = source_s3_path
    )

    print("Wait for Kendra to update the thesaurus.")

    while True:
        # Get thesaurus description
        thesaurus_description = kendra.describe_thesaurus(
            Id = thesaurus_id,
            IndexId = index_id
        )
        # If status is not UPDATING quit
        status = thesaurus_description["Status"]
        print("Updating thesaurus. Status: " + status)
        if status != "UPDATING":
            break
        time.sleep(60)

    except ClientError as e:
        print("%s" % e)

    print("Program ends.")
```

Java

```
package com.amazonaws.kendra;

import software.amazon.awssdk.services.kendra.KendraClient;
import software.amazon.awssdk.services.kendra.model.UpdateThesaurusRequest;
import software.amazon.awssdk.services.kendra.model.DescribeThesaurusRequest;
import software.amazon.awssdk.services.kendra.model.DescribeThesaurusResponse;
import software.amazon.awssdk.services.kendra.model.S3Path;
import software.amazon.awssdk.services.kendra.model.ThesaurusStatus;

public class UpdateThesaurusExample {

    public static void main(String[] args) throws InterruptedException {

        KendraClient kendra = KendraClient.builder().build();
```

```
String thesaurusName = "thesaurus-name";
String thesaurusDescription = "thesaurus-description";
String thesaurusRoleArn = "role-arn";

String s3BucketName = "bucket-name";
String s3Key = "thesaurus-file";

String thesaurusId = "thesaurus-id";
String indexId = "index-id";

UpdateThesaurusRequest updateThesaurusRequest = UpdateThesaurusRequest
    .builder()
    .id(thesaurusId)
    .indexId(indexId)
    .name(thesaurusName)
    .description(thesaurusDescription)
    .roleArn(thesaurusRoleArn)
    .sourceS3Path(S3Path.builder()
        .bucket(s3BucketName)
        .key(s3Key)
        .build())
    .build();
kendra.updateThesaurus(updateThesaurusRequest);

System.out.println(String.format("Waiting until the thesaurus with ID %s is
updated.", thesaurusId));

// a new source s3 path requires re-consumption by Kendra
// and so can take as long as a Create Thesaurus operation
while (true) {
    DescribeThesaurusRequest describeThesaurusRequest =
DescribeThesaurusRequest.builder()
    .id(thesaurusId)
    .indexId(indexId)
    .build();
    DescribeThesaurusResponse describeThesaurusResponse =
kendra.describeThesaurus(describeThesaurusRequest);
    ThesaurusStatus status = describeThesaurusResponse.status();
    if (status != ThesaurusStatus.UPDATING) {
        break;
    }

    TimeUnit.SECONDS.sleep(60);
}
```

```
    }  
  
    System.out.println("Thesaurus update is complete.");  
  }  
}
```

刪除索引典

下列程序顯示如何刪除索引典。

Console

1. 在左側導覽窗格的索引下，選擇 [同義字]。
2. 在「同義字」頁面上，選取您要刪除的同義字辭典。
3. 在 [索引典詳細資料] 頁面上，選擇 [刪除]，然後確認刪除。

CLI

若要使用刪除索引的索引 AWS CLI，請呼叫：`delete-thesaurus`

```
aws kendra delete-thesaurus \  
--index-id index-id \  
--id thesaurus-id
```

Python

```
import boto3  
from botocore.exceptions import ClientError  
  
kendra = boto3.client("kendra")  
  
print("Delete a thesaurus")  
  
thesaurus_id = "thesaurus-id"  
index_id = "index-id"  
  
try:  
    kendra.delete_thesaurus(  
        Id = thesaurus_id,  
        IndexId = index_id
```

```
)

except ClientError as e:
    print("%s" % e)

print("Program ends.")
```

Java

```
package com.amazonaws.kendra;

import software.amazon.awssdk.services.kendra.KendraClient;
import software.amazon.awssdk.services.kendra.model.DeleteThesaurusRequest;

public class DeleteThesaurusExample {

    public static void main(String[] args) throws InterruptedException {

        KendraClient kendra = KendraClient.builder().build();

        String thesaurusId = "thesaurus-id";
        String indexId = "index-id";

        DeleteThesaurusRequest updateThesaurusRequest = DeleteThesaurusRequest
            .builder()
            .id(thesaurusId)
            .indexId(indexId)
            .build();
        kendra.deleteThesaurus(updateThesaurusRequest);
    }
}
```

搜尋結果中的亮點

依預設，同義字反白顯示處於開啟狀態。突出顯示信息包含在 Amazon Kendra SDK 和 CLI 查詢結果中。如果您與 Amazon Kendra 使用 SDK 或 CLI 進行互動，您將決定如何顯示結果。

同義詞突出顯示將具有突出顯示類型。THESAURUS_SYNONYM如需有關亮顯的詳細資訊，請參閱[反白物件](#)。

教學課程：使用 Amazon Kendra 建置豐富中繼資料的智慧型搜尋解決方案

本教學說明如何使用 [Amazon Kendra](#)、[Amazon Comprehend](#)、[Amazon 簡單儲存服務 \(S3\)](#) 和，為企業資料建立豐富中繼資料的自然語言智慧搜尋解決方案。[AWS CloudShell](#)

Amazon Kendra 是一種智慧型搜尋服務，可為您的非結構化自然語言資料儲存庫建立搜尋索引。為了讓您的客戶更容易找到並篩選相關答案，您可以使用 Amazon Comprehend 從資料擷取中繼資料，並將其導入 Amazon Kendra 搜尋索引中。

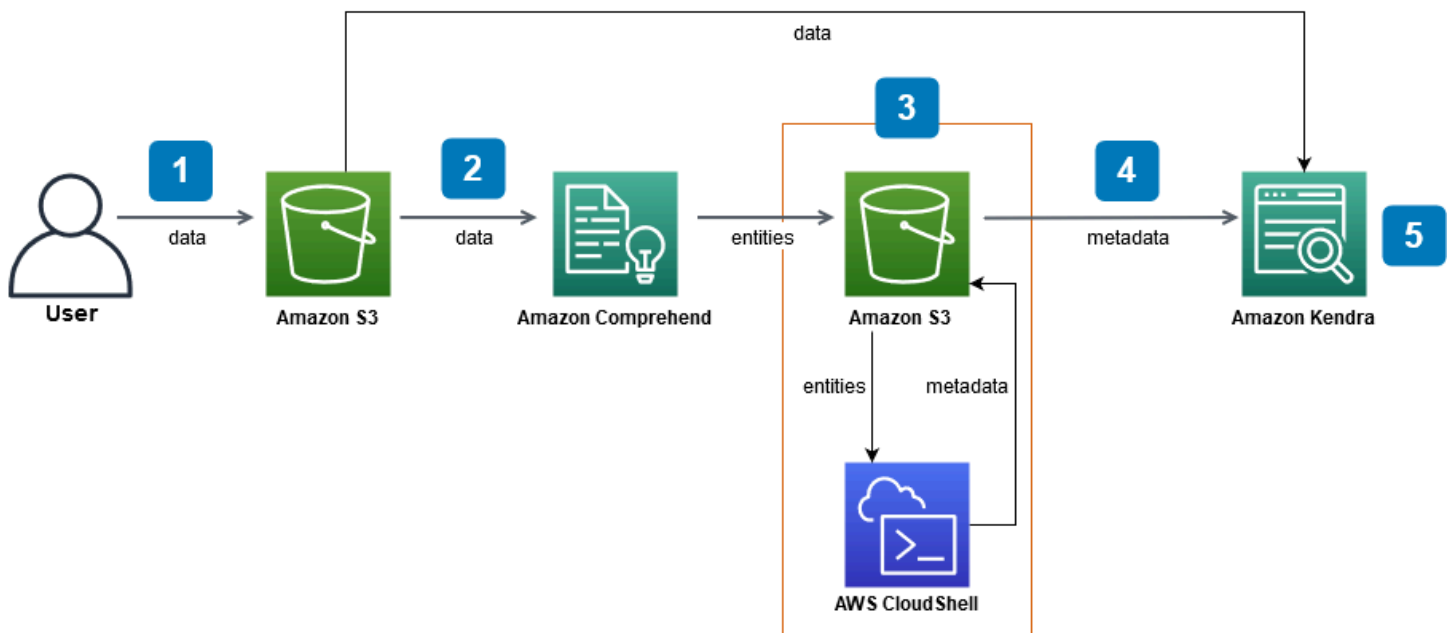
Amazon Comprehend 是一種自然語言處理 (NLP) 服務，可以識別實體。實體是資料中人員、場所、位置、組織和物件的參照。

本教學課程使用新聞文章的範例資料集擷取實體、將其轉換為中繼資料，並將其導入 Amazon Kendra 索引中，以便在其上執行搜尋。新增的中繼資料可讓您使用這些實體的任何子集篩選搜尋結果，並提高搜尋準確性。按照本教程，您將學習如何在沒有任何專門的機器學習知識的情況下為您的企業數據創建搜索解決方案。

本教學課程說明如何使用下列步驟建置搜尋解決方案：

1. 在 Amazon S3 中存放新聞文章的範例資料集。
2. 使用 Amazon Comprehend 從您的資料中擷取實體。
3. 執行 Python 3 指令碼，將實體轉換為 Amazon Kendra 索引中繼資料格式，並將此中繼資料存放在 S3 中。
4. 建立 Amazon Kendra 搜尋索引，並擷取資料和中繼資料。
5. 查詢搜尋索引。

下圖顯示工作流程：



完成此自學課程的預估時間：1 小時

預估費用：本教學課程中的某些動作會對您的 AWS 帳戶產生費用。[如需每項服務成本的詳細資訊，請參閱 Amazon S3、AmazonComprehend 和亞馬 Amazon Kendra 的價格頁面。](#) [AWS CloudShell](#)

主題

- [必要條件](#)
- [第 1 步：將文檔添加到 Amazon S3](#)
- [步驟 2：在 Amazon Comprehend 上執行實體分析任務](#)
- [步驟 3：將實體分析輸出格式化為 Amazon Kendra 中繼資料](#)
- [步驟 4：建立 Amazon Kendra 索引並擷取中繼資料](#)
- [步驟 5：查詢 Amazon Kendra 索引](#)
- [步驟 6：清理](#)

必要條件

若要完成本教學課程，您需要下列資源：

- 一個 AWS 帳戶。如果您沒有 AWS 帳戶，請按照[設定 Amazon Kendra 中的步驟](#)設定您的 AWS 帳戶。

- 執行視窗、macOS 或 Linux 的開發電腦，以存取 AWS 管理主控台。如需詳細資訊，請參閱[設定 AWS 管理主控台](#)。
- 一個 [AWS Identity and Access Management\(IAM\)](#) 使用者。若要了解如何為您的帳戶設定 IAM 使用者和群組，請參閱 IAM 使用者指南中的[入門](#)章節。

如果您使用的是 AWS Command Line Interface，您還需要將下列政策附加到 IAM 使用者，以授予其完成本教學課程所需的基本許可。

如需詳細資訊，請參閱[建立 IAM 政策](#)和[新增和移除 IAM 身分許可](#)。

- [AWS 區域服務清單](#)。為了減少延遲，您應該選擇距離您所在地理位置最近的 AWS 區域，該區域同時受到 Amazon Comprehend 和 Amazon Kendra 支援。
- (選擇性) 一個 [AWS Key Management Service](#)。雖然本教學課程不使用加密，但您可能希望針對特定使用案例使用加密最佳作法。
- (可選) [Amazon Virtual Private Cloud](#)。雖然本教學課程不使用 VPC，但您可能需要使用 VPC 最佳做法來確保特定使用案例的資料安全性。

第 1 步：將文檔添加到 Amazon S3

在您的資料集上執行 Amazon Comprehend 實體分析任務之前，請先建立 Amazon S3 儲存貯體來託管資料、中繼資料和 Amazon Comprehend 實體分析輸出。

主題

- [下載範例資料集](#)
- [建立 Amazon S3 儲存貯體](#)
- [在 S3 儲存貯體中建立資料和中繼資料資料夾](#)
- [上傳輸入數據](#)

下載範例資料集

Amazon Comprehend 才能對您的資料執行實體分析任務，您必須先下載並擷取資料集，然後將其上傳到 S3 儲存貯體。

若要下載並擷取資料集 (主控台)

1. 在您的設備上下載 [tutorial-dataset.zip](#) 文件夾。

2. 解壓縮tutorial-dataset料夾以存取data資料夾。

若要下載並擷取資料集 (終端機)

1. 若要下載tutorial-dataset，請在終端機視窗上執行下列命令：

Linux

```
curl -o path/tutorial-dataset.zip https://docs.aws.amazon.com/kendra/latest/dg/samples/tutorial-dataset.zip
```

其中：

- *path/* 是要保存 zip 文件夾的位置的本地文件路徑。

macOS

```
curl -o path/tutorial-dataset.zip https://docs.aws.amazon.com/kendra/latest/dg/samples/tutorial-dataset.zip
```

其中：

- *path/* 是要保存 zip 文件夾的位置的本地文件路徑。

Windows

```
curl -o path/tutorial-dataset.zip https://docs.aws.amazon.com/kendra/latest/dg/samples/tutorial-dataset.zip
```

其中：

- *path/* 是要保存 zip 文件夾的位置的本地文件路徑。

2. 要從 zip 文件夾中提取數據，請在終端機窗口中運行以下命令：

Linux

```
unzip path/tutorial-dataset.zip -d path/
```

其中：

- `path/` 是保存的 zip 文件夾的本地文件路徑。

macOS

```
unzip path/tutorial-dataset.zip -d path/
```

其中：

- `path/` 是保存的 zip 文件夾的本地文件路徑。

Windows

```
tar -xf path/tutorial-dataset.zip -C path/
```

其中：

- `path/` 是保存的 zip 文件夾的本地文件路徑。

在此步驟結束時，您應該將提取的文件放在名為tutorial-dataset的解壓縮文件夾中。此資料夾包含一個包含 Apache 2.0 開放原始碼歸因的README檔案，以及一個名為包data含本教學課程資料集的資料夾。資料集由 100 個副檔.story名的檔案組成。

建立 Amazon S3 儲存貯體

下載並擷取範例資料資料夾後，您可以將其存放在 Amazon S3 儲存貯體中。

Important

Amazon S3 儲存貯體的名稱在所有儲存貯體中都必須是唯一的 AWS。

若要建立 S3 儲存貯體 (主控台)

1. 登入 AWS Management Console 並開啟 Amazon S3 主控台，網址為 <https://console.aws.amazon.com/s3/>。

2. 在「值區」中選擇「建立值區」。
3. 對於 Bucket name (儲存貯體名稱)，輸入一個唯一名稱。
4. 在「區域」中，選擇您要建立值 AWS 區的區域。

Note

您必須選擇同時支援亞馬遜和亞馬 Amazon Kendra 的區域。建立值區之後，就無法變更該值區的區域。

5. 保留此值區、值區版本控制和標籤的「封鎖公開存取」設定的預設設定。
6. 對於預設加密，請選擇停用。
7. 保留「進階」設定的預設設定。
8. 檢閱值區組態，然後選擇 [建立值區]。

若要建立 S3 儲存貯體 (AWS CLI)

1. 若要建立 S3 儲存貯體，請在下列項目中使用[建立儲存貯體](#)命令：AWS CLI

Linux

```
aws s3api create-bucket \  
    --bucket DOC-EXAMPLE-BUCKET \  
    --region aws-region \  
    --create-bucket-configuration LocationConstraint=aws-region
```

其中：

- 文檔示例桶是您的存儲桶名稱，
- *aws-region* 是您要在其中創建存儲桶的區域。

macOS

```
aws s3api create-bucket \  
    --bucket DOC-EXAMPLE-BUCKET \  
    --region aws-region \  
    --create-bucket-configuration LocationConstraint=aws-region
```

其中：

- 文檔示例桶是您的存儲桶名稱，
- *aws-region* 是您要在其中創建存儲桶的區域。

Windows

```
aws s3api create-bucket ^  
    --bucket DOC-EXAMPLE-BUCKET ^  
    --region aws-region ^  
    --create-bucket-configuration LocationConstraint=aws-region
```

其中：

- 文檔示例桶是您的存儲桶名稱，
- *aws-region* 是您要在其中創建存儲桶的區域。

Note

您必須選擇同時支援亞馬遜和亞馬 Amazon Kendra 的區域。建立值區之後，就無法變更該值區的區域。

2. 若要確保您的儲存貯體已成功建立，請使用 [list](#) 指令：

Linux

```
aws s3 ls
```

macOS

```
aws s3 ls
```

Windows

```
aws s3 ls
```

在 S3 儲存貯體中建立資料和中繼資料資料夾

建立 S3 儲存貯體之後，您可以在其中建立資料和中繼資料夾。

在 S3 儲存貯體中建立資料夾 (主控台)

1. 前往 <https://console.aws.amazon.com/s3/> 開啟的 Amazon Simple Storage Service (Amazon S3) 主控台。
2. 在值區中，按一下值區清單中的值區名稱。
3. 在「物件」標籤中，選擇「建立資料夾」。
4. 對於新資料夾名稱，請輸入 **data**。
5. 對於加密設定，請選擇 [停用]。
6. 選擇 Create folder (建立資料夾)。
7. 重複步驟 3 到 6，建立另一個用於儲存 Amazon Kendra 中繼資料的資料夾，並為步驟 4 **metadata** 中建立的資料夾命名。

在 S3 儲存貯體中建立資料夾 (AWS CLI)

1. 若要在 S3 儲存貯體中建立 data 資料夾，請使用下列指令中的 [put-object](#) 命令：AWS CLI

Linux

```
aws s3api put-object \  
    --bucket DOC-EXAMPLE-BUCKET \  
    --key data/
```

其中：

- 文檔示例桶是您的存儲桶名稱。

macOS

```
aws s3api put-object \  
    --bucket DOC-EXAMPLE-BUCKET \  
    --key data/
```

其中：

- 文檔示例桶是您的存儲桶名稱。

Windows

```
aws s3api put-object ^
    --bucket DOC-EXAMPLE-BUCKET ^
    --key data/
```

其中：

- 文檔示例桶是您的存儲桶名稱。

2. 若要在 S3 儲存貯體中建立metadata資料夾，請使用下列指令中的 [put-object](#) 命令：AWS CLI

Linux

```
aws s3api put-object \  
    --bucket DOC-EXAMPLE-BUCKET \  
    --key metadata/
```

其中：

- 文檔示例桶是您的存儲桶名稱。

macOS

```
aws s3api put-object \  
    --bucket DOC-EXAMPLE-BUCKET \  
    --key metadata/
```

其中：

- 文檔示例桶是您的存儲桶名稱。

Windows

```
aws s3api put-object ^
    --bucket DOC-EXAMPLE-BUCKET ^
```



```
--key metadata/
```

其中：

- 文檔示例桶是您的存儲桶名稱。

3. 若要確保資料夾已成功建立，請使用 [list](#) 指令檢查值區的內容：

Linux

```
aws s3 ls s3://DOC-EXAMPLE-BUCKET/
```

其中：

- 文檔示例桶是您的存儲桶名稱。

macOS

```
aws s3 ls s3://DOC-EXAMPLE-BUCKET/
```

其中：

- 文檔示例桶是您的存儲桶名稱。

Windows

```
aws s3 ls s3://DOC-EXAMPLE-BUCKET/
```

其中：

- 文檔示例桶是您的存儲桶名稱。

上傳輸入數據

建立資料和中繼資料資料夾之後，您可以將範例資料集上傳至資料data夾。

若要將範例資料集上傳至資料資料夾 (主控台)

1. 前往 <https://console.aws.amazon.com/s3/> 開啟的 Amazon Simple Storage Service (Amazon S3) 主控台。
2. 在值區中，按一下值區清單中的值區名稱，然後按一下data。
3. 選擇上傳，然後選擇添加文件。
4. 在對話方塊中，導覽至本機裝置中tutorial-dataset資料data夾內的資料夾，選取所有檔案，然後選擇「開啟」。
5. 保留「目的地」、「權限」和「內容」的預設設定。
6. 選擇上傳。

若要將範例資料集上傳至資料資料夾 (AWS CLI)

1. 若要將範例資料上傳至資料data夾，請使用下列指令中的 [copy](#) 指令 AWS CLI：

Linux

```
aws s3 cp path/tutorial-dataset/data s3://DOC-EXAMPLE-BUCKET/data/ --recursive
```

其中：

- *path/* 是設備上文件tutorial-dataset夾的文件路徑，
- 文檔示例桶是您的存儲桶名稱。

macOS

```
aws s3 cp path/tutorial-dataset/data s3://DOC-EXAMPLE-BUCKET/data/ --recursive
```

其中：

- *path/* 是設備上文件tutorial-dataset夾的文件路徑，
- 文檔示例桶是您的存儲桶名稱。

Windows

```
aws s3 cp path/tutorial-dataset/data s3://DOC-EXAMPLE-BUCKET/data/ --recursive
```

其中：

- *path/* 是設備上文件tutorial-dataset夾的文件路徑，
- 文檔示例桶是您的存儲桶名稱。

2. 若要確保資料集檔案已成功上傳至資料data夾，請使用下列項目中的 [list](#) 指令 AWS CLI：

Linux

```
aws s3 ls s3://DOC-EXAMPLE-BUCKET/data/
```

其中：

- 文檔示例存儲桶是您的 S3 存儲桶的名稱。

macOS

```
aws s3 ls s3://DOC-EXAMPLE-BUCKET/data/
```

其中：

- 文檔示例存儲桶是您的 S3 存儲桶的名稱。

Windows

```
aws s3 ls s3://DOC-EXAMPLE-BUCKET/data/
```

其中：

- 文檔示例存儲桶是您的 S3 存儲桶的名稱。

在此步驟結束時，您會有一個 S3 儲存貯體，其中資料集存放在資料data夾內，以及一個空白資料metadata夾 (用於儲存 Amazon Kendra 中繼資料)。

步驟 2：在 Amazon Comprehend 上執行實體分析任務

將範例資料集儲存在 S3 儲存貯體之後，您可以執行 Amazon Comprehend 實體分析任務，以從文件中擷取實體。這些實體將形成 Amazon Kendra 自訂屬性，並協助您篩選索引上的搜尋結果。如需詳細資訊，請參閱[偵測實體](#)。

主題

- [執行 Amazon Comprehend 實體分析任務](#)

執行 Amazon Comprehend 實體分析任務

若要從資料集擷取實體，請執行 Amazon Comprehend 實體分析任務。

如果您在此步驟中使用 AWS CLI，請先為 Amazon Comprehend 建立並附加 AWS IAM 角色和政策，然後執行實體分析任務。若要對範例資料執行實體分析任務，Amazon Comprehend 需要：

- 將其識別為受信任實體的 AWS Identity and Access Management (IAM) 角色
- 附加到 AWS IAM 角色的 IAM 政策，授予其存取 S3 儲存貯體的許可

如需詳細資訊，請參閱 [Amazon Comprehend 如何與 IAM 和以身分識別為基礎的政策搭配](#) Amazon Comprehend 用。

若要執行 Amazon Comprehend 實體分析任務 (主控台)

1. [在 https://console.aws.amazon.com/comprehend/ 打開 Amazon Comprehend 域控制台。](https://console.aws.amazon.com/comprehend/)

Important

確保您位於建立 Amazon S3 儲存貯體的相同區域。如果您位於其他區域，請從頂端導覽列的 AWS 區域選擇器中選擇您建立 S3 儲存貯體的區域。

2. 選擇啟動 Amazon Comprehend.
3. 在左側導覽窗格中，選擇 [分析工作]。
4. 選擇建立作業。

5. 在 [Job 設定] 區段中，執行下列動作：
 - a. 針對名稱，輸入 **data-entities-analysis**。
 - b. 對於「分析」類型，請選擇實體。
 - c. 選擇「英文」做為「語言」。
 - d. 保持 Job 加密關閉狀態。
6. 在「輸入資料」區段中，執行下列操作：
 - a. 對於資料來源，選擇我的文件。
 - b. 對於 S3 位置，請選擇瀏覽 S3。
 - c. 對於「選擇資源」，請從值區清單中按一下值區的名稱。
 - d. 對於「物件」，請選取選項按鈕，data然後選擇「選擇」。
 - e. 在「輸入格式」中，選擇「每個檔案一個文件」
7. 在「輸出資料」區段中，執行下列操作：
 - a. 對於 S3 位置，請選擇瀏覽 S3，然後從儲存貯體清單中選取儲存貯體的選項方塊，然後選擇 [選擇]。
 - b. 保持加密關閉狀態。
8. 在「存取權限」區段中，執行下列動作：
 - a. 對於 IAM 角色，請選擇建立 IAM 角色。
 - b. 對於存取權限，請選擇輸入和輸出 S3 儲存貯體。
 - c. 對於「名稱尾碼」，輸入**comprehend-role**。此角色可讓您存取 Amazon S3 儲存貯體。
9. 保留預設的 VPC 設定。
10. 選擇建立作業。

若要執行 Amazon Comprehend 實體分析任務 ()AWS CLI

1. 若要為 Amazon Comprehend 建立並附加將其識別為受信任實體的 IAM 角色，請執行以下操作：
 - a. 將下列信任原則儲存為本機裝置上文字編輯器comprehend-trust-policy.json中呼叫的 JSON 檔案。

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

```
{
  "Effect": "Allow",
  "Principal": {
    "Service": "comprehend.amazonaws.com"
  },
  "Action": "sts:AssumeRole"
}
]
```

- b. 若要建立名為的 IAM 角色，comprehend-role並將儲存的comprehend-trust-policy.json檔案附加至該角色，請使用 [create-](#)role 命令：

Linux

```
aws iam create-role \
    --role-name comprehend-role \
    --assume-role-policy-document file://path/comprehend-trust-
policy.json
```

其中：

- *path/* 是本地設備comprehend-trust-policy.json上的文件路徑。

macOS

```
aws iam create-role \
    --role-name comprehend-role \
    --assume-role-policy-document file://path/comprehend-trust-
policy.json
```

其中：

- *path/* 是本地設備comprehend-trust-policy.json上的文件路徑。

Windows

```
aws iam create-role ^
    --role-name comprehend-role ^
```

```
--assume-role-policy-document file://path/comprehend-trust-policy.json
```

其中：

- *path* 是本地設備 `comprehend-trust-policy.json` 上的文件路徑。

- c. 將 Amazon 資源名稱 (ARN) 複製到您的文字編輯器，並將其儲存為 `comprehend-role-arn` 本機。

 Note

ARN 的格式類似於 `arn:aw:IAM::123456789012:##/###色`。您需要儲存的 ARN，才 `comprehend-role-arn` 能執行 Amazon Comprehend 分析任務。

2. 若要建立 IAM 政策並將其附加到 IAM 角色，以授予其存取 S3 儲存貯體的權限，請執行以下操作：

- a. 將下列信任原則儲存為本機裝置上文字編輯器 `comprehend-S3-access-policy.json` 中呼叫的 JSON 檔案。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "s3:GetObject"
      ],
      "Resource": [
        "arn:aws:s3:::DOC-EXAMPLE-BUCKET/*"
      ],
      "Effect": "Allow"
    },
    {
      "Action": [
        "s3:ListBucket"
      ],
      "Resource": [
        "arn:aws:s3:::DOC-EXAMPLE-BUCKET"
      ],
      "Effect": "Allow"
    }
  ]
}
```

```
{
  "Action": [
    "s3:PutObject"
  ],
  "Resource": [
    "arn:aws:s3:::DOC-EXAMPLE-BUCKET/*"
  ],
  "Effect": "Allow"
}
```

- b. 若要建立呼叫 `comprehend-S3-access-policy` 以存取 S3 儲存貯體的 IAM 政策，請使用 [建立政策命令](#)：

Linux

```
aws iam create-policy \
  --policy-name comprehend-S3-access-policy \
  --policy-document file://path/comprehend-S3-access-policy.json
```

其中：

- *path/* 是本地設備 `comprehend-S3-access-policy.json` 上的文件路徑。

macOS

```
aws iam create-policy \
  --policy-name comprehend-S3-access-policy \
  --policy-document file://path/comprehend-S3-access-policy.json
```

其中：

- *path/* 是本地設備 `comprehend-S3-access-policy.json` 上的文件路徑。

Windows

```
aws iam create-policy ^
  --policy-name comprehend-S3-access-policy ^
  --policy-document file://path/comprehend-S3-access-policy.json
```


其中：

- *path/* 是本地設備comprehend-S3-access-policy.json上的文件路徑。

- c. 將 Amazon 資源名稱 (ARN) 複製到您的文字編輯器，並將其儲存為comprehend-S3-access-arn本機。

Note

ARN 的格式類似於 ARN: aw: IAM:: 123456789012###/##-S3-#問策略。您需要另存的 ARN 才comprehend-S3-access-arn能將其附加comprehend-S3-access-policy到 IAM 角色。

- d. 若要附加comprehend-S3-access-policy到您的 IAM 角色，請使用以下[attach-role-policy](#)命令：

Linux

```
aws iam attach-role-policy \  
    --policy-arn policy-arn \  
    --role-name comprehend-role
```

其中：

- *## arn* 是您另存為的 ARN。comprehend-S3-access-arn

macOS

```
aws iam attach-role-policy \  
    --policy-arn policy-arn \  
    --role-name comprehend-role
```

其中：

- *## arn* 是您另存為的 ARN。comprehend-S3-access-arn

Windows

```
aws iam attach-role-policy ^
```

```
--policy-arn policy-arn ^  
--role-name comprehend-role
```

其中：

- **## arn** 是您另存為的 ARN。comprehend-S3-access-arn

3. 若要執行 Amazon Comprehend 實體分析任務，請使用以下 [start-entities-detection-job](#) 命令：

Linux

```
aws comprehend start-entities-detection-job \  
    --input-data-config S3Uri=s3://DOC-EXAMPLE-BUCKET/  
data/,InputFormat=ONE_DOC_PER_FILE \  
    --output-data-config S3Uri=s3://DOC-EXAMPLE-BUCKET/ \  
    --data-access-role-arn role-arn \  
    --job-name data-entities-analysis \  
    --language-code en \  
    --region aws-region
```

其中：

- 文檔示例桶是您的 S3 存儲桶的名稱，
- **## arn** 是您另存為的 ARN，comprehend-role-arn
- **aws-region ### AWS ##**。

macOS

```
aws comprehend start-entities-detection-job \  
    --input-data-config S3Uri=s3://DOC-EXAMPLE-BUCKET/  
data/,InputFormat=ONE_DOC_PER_FILE \  
    --output-data-config S3Uri=s3://DOC-EXAMPLE-BUCKET/ \  
    --data-access-role-arn role-arn \  
    --job-name data-entities-analysis \  
    --language-code en \  
    --region aws-region
```

其中：

- 文檔示例桶是您的 S3 存儲桶的名稱，

- `## arn` 是您另存為的 ARN , comprehend-role-arn
- `aws-region ### AWS ##`。

Windows

```
aws comprehend start-entities-detection-job ^
  --input-data-config S3Uri=s3://DOC-EXAMPLE-BUCKET/
data/,InputFormat=ONE_DOC_PER_FILE ^
  --output-data-config S3Uri=s3://DOC-EXAMPLE-BUCKET/ ^
  --data-access-role-arn role-arn ^
  --job-name data-entities-analysis ^
  --language-code en ^
  --region aws-region
```

其中：

- 文檔示例桶是您的 S3 存儲桶的名稱，
 - `## arn` 是您另存為的 ARN , comprehend-role-arn
 - `aws-region ### AWS ##`。
4. 複製實體分析 JobId 並將其保存在文本編輯器中 comprehend-job-id。可 JobId 協助您追蹤實體分析工作的狀態。
 5. 若要追蹤實體分析工作的進度，請使用以下 [describe-entities-detection-job](#) 指令：

Linux

```
aws comprehend describe-entities-detection-job \  
  --job-id entities-job-id \  
  --region aws-region
```

其中：

- `entities-job-id` 是你的保存 comprehend-job-id，
- `aws-region ### AWS ##`。

macOS

```
aws comprehend describe-entities-detection-job \  
  --job-id entities-job-id \  
  --region aws-region
```

```
--job-id entities-job-id \  
--region aws-region
```

其中：

- *entities-job-id* 是你的保存 comprehend-job-id，
- *aws-region* ### AWS ##。

Windows

```
aws comprehend describe-entities-detection-job ^  
  --job-id entities-job-id ^  
  --region aws-region
```

其中：

- *entities-job-id* 是你的保存 comprehend-job-id，
- *aws-region* ### AWS ##。

變更為可能需 JobStatus 要幾分鐘的時間 COMPLETED。

在此步驟結束時，Amazon Comprehend 會將實體分析結果作為壓縮 `output.tar.gz` 檔案存放在 S3 儲存貯體的自動產生 `output` 資料夾中的資料夾內。在進行下一個步驟之前，請確保分析工作狀態已完成。

步驟 3：將實體分析輸出格式化為 Amazon Kendra 中繼資料

若要將 Amazon Comprehend 擷取的實體轉換為亞馬 Amazon Kendra 索引所需的中繼資料格式，您可以執行 Python 3 指令碼。轉換結果會存放在 Amazon S3 儲存貯體中的 `metadata` 資料夾中。

如需 Amazon Kendra 中繼資料格式和結構的詳細資訊，請參閱 [S3 文件中繼資料](#)。

主題

- [下載和提取 Amazon Comprehend 輸出](#)
- [將輸出上傳到 S3 儲存貯體](#)
- [將輸出轉換為 Amazon Kendra 元數據格式](#)
- [清理你的 Amazon S3 存儲桶](#)

下載和提取 Amazon Comprehend 輸出

若要格式化 Amazon Comprehend 實體分析輸出，您必須先下載 Amazon Comprehend 實體分析 `output.tar.gz` 存檔並擷取實體分析檔案。

下載並解壓縮輸出檔案 (控制台)

1. 在 Amazon Comprehend 主控台導覽窗格中，導覽至分析任務。
2. 選擇您的實體分析工作 `data-entities-analysis`。
3. 在「輸出」下，選擇「輸出資料位置」旁邊顯示的連結。這會將您重新導向至 S3 儲 `output.tar.gz` 存貯體中的存檔。
4. 在「概覽」標籤中，選擇「下載」。

Tip

所有亞馬遜分析任務的輸出都具有相同的名稱。重新命名歸檔可協助您更輕鬆地追蹤檔案。

5. 將下載的 Amazon Comprehend 檔案解壓縮並解壓縮到您的裝置。

下載並解壓縮輸出檔案的步驟 (AWS CLI)

1. 若要存取 S3 儲存貯體中包含實體分析任務結果的 Amazon Comprehend 自動產生資料夾的名稱，請使用以下 [describe-entities-detection-job](#) 命令：

Linux

```
aws comprehend describe-entities-detection-job \  
    --job-id entities-job-id \  
    --region aws-region
```

其中：

- *entities-job-id* 是你保存 comprehend-job-id 的 [the section called “步驟 2：偵測圖元”](#)，
- *aws-region* **### AWS ##**。

macOS

```
aws comprehend describe-entities-detection-job \  
  --job-id entities-job-id \  
  --region aws-region
```

其中：

- *entities-job-id*是你保存comprehend-job-id的[the section called “步驟 2：偵測圖元”](#)，
- *aws-region* ### AWS ##。

Windows

```
aws comprehend describe-entities-detection-job ^  
  --job-id entities-job-id ^  
  --region aws-region
```

其中：

- *entities-job-id*是你保存comprehend-job-id的[the section called “步驟 2：偵測圖元”](#)，
- *aws-region* ### AWS ##。

2. 從實體工作描述中的OutputDataConfig物件中，複製並儲存在文字編輯器comprehend-S3uri上的S3Uri值。

Note

該S3Uri值的格式類似於 *s3://DOC-EXAMPLE-BUCKET/... /output/output.tar.gz*。

3. 要下載實體輸出歸檔，請使用 [copy](#) 命令：

Linux

```
aws s3 cp s3://DOC-EXAMPLE-BUCKET/.../output/output.tar.gz path/output.tar.gz
```

其中：

- `s3://DOC-EXAMPLE-BUCKET/.../output/output.tar.gz` 是您保存為的S3Uri值comprehend-S3uri，
- `path/` 是您希望保存輸出的本地目錄。

macOS

```
aws s3 cp s3://DOC-EXAMPLE-BUCKET/.../output/output.tar.gz path/output.tar.gz
```

其中：

- `s3://DOC-EXAMPLE-BUCKET/.../output/output.tar.gz` 是您保存為的S3Uri值comprehend-S3uri，
- `path/` 是您希望保存輸出的本地目錄。

Windows

```
aws s3 cp s3://DOC-EXAMPLE-BUCKET/.../output/output.tar.gz path/output.tar.gz
```

其中：

- `s3://DOC-EXAMPLE-BUCKET/.../output/output.tar.gz` 是您保存為的S3Uri值comprehend-S3uri，
- `path/` 是您希望保存輸出的本地目錄。

4. 若要擷取實體輸出，請在終端機視窗上執行下列命令：

Linux

```
tar -xf path/output.tar.gz -C path/
```

其中：

- `path/` 是本地設備上下載output.tar.gz存檔的文件路徑。

macOS

```
tar -xf path/output.tar.gz -C path/
```

其中：

- *path*/ 是本地設備上下載output.tar.gz存檔的文件路徑。

Windows

```
tar -xf path/output.tar.gz -C path/
```

其中：

- *path*/ 是本地設備上下載output.tar.gz存檔的文件路徑。

在此步驟結束時，您的裝置上應該有一個檔案，其中output包含 Amazon Comprehend 識別的實體清單。

將輸出上傳到 S3 儲存貯體

下載並擷取 Amazon Comprehend 實體分析檔案後，您可以將擷取的output檔案上傳到 Amazon S3 儲存貯體。

上傳擷取的亞馬遜輸出檔案 (主控台)

1. 前往 <https://console.aws.amazon.com/s3/> 開啟的 Amazon Simple Storage Service (Amazon S3) 主控台。
2. 在「值區」中，按一下值區的名稱，然後選擇「上傳」。
3. 在 [檔案和資料夾] 中選擇 [新增檔案]。
4. 在對話方塊中，導覽至裝置中解壓縮的output檔案，選取該檔案，然後選擇「開啟」。
5. 保留「目的地」、「權限」和「內容」的預設設定。
6. 選擇上傳。

上傳擷取的亞馬遜輸出檔案 ()AWS CLI

1. 要將解壓縮的output文件上傳到存儲桶，請使用 [copy](#) 命令：

Linux

```
aws s3 cp path/output s3://DOC-EXAMPLE-BUCKET/output
```

其中：

- *path/* 是提取output文件的本地文件路徑，
- 文檔示例存儲桶是您的 S3 存儲桶的名稱。

macOS

```
aws s3 cp path/output s3://DOC-EXAMPLE-BUCKET/output
```

其中：

- *path/* 是提取output文件的本地文件路徑，
- 文檔示例存儲桶是您的 S3 存儲桶的名稱。

Windows

```
aws s3 cp path/output s3://DOC-EXAMPLE-BUCKET/output
```

其中：

- *path/* 是提取output文件的本地文件路徑，
- 文檔示例存儲桶是您的 S3 存儲桶的名稱。

2. 若要確保output檔案已成功上傳至 S3 儲存貯體，請使用 [list](#) 指令檢查其內容：

Linux

```
aws s3 ls s3://DOC-EXAMPLE-BUCKET/
```

其中：

- 文檔示例存儲桶是您的 S3 存儲桶的名稱。

macOS

```
aws s3 ls s3://DOC-EXAMPLE-BUCKET/
```

其中：

- 文檔示例存儲桶是您的 S3 存儲桶的名稱。

Windows

```
aws s3 ls s3://DOC-EXAMPLE-BUCKET/
```

其中：

- 文檔示例存儲桶是您的 S3 存儲桶的名稱。

將輸出轉換為 Amazon Kendra 元數據格式

若要將 Amazon Comprehend 輸出轉換為 Amazon Kendra 中繼資料，您可以執行 Python 3 指令碼。如果您使用的是「主控台」，請使 AWS CloudShell 用此步驟。

要運行 Python 3 腳本（控制台）

1. 在您的設備上下載[轉換器 .py.zip 壓縮文件](#)。
2. 解壓縮 Python 3 文件 converter.py。
3. 登入[AWS 管理主控台](#)，確認您的 AWS 區域設定為與 S3 儲存貯體和 Amazon Comprehend 分析任務相同的區域。
4. 選擇 AWS CloudShell 圖示或 AWS CloudShell 在頂端導覽列的 [搜尋] 方塊中輸入以啟動環境。

Note

首次在新瀏覽器視窗中 AWS CloudShell 啟動時，會顯示歡迎面板並列出主要功能。當您關閉此面板並顯示指令提示字元之後，shell 就可以進行互動。

5. 準備好終端機之後，從導覽窗格中選擇 [動作]，然後從功能表中選擇 [上傳檔案]。
6. 在開啟的對話方塊中，選擇 [選取檔案]，然後 converter.py 從您的裝置選擇下載的 Python 3 檔案。選擇上傳。
7. 在 AWS CloudShell 環境中，輸入以下命令：

```
python3 converter.py
```

8. 當殼層介面提示您輸入 S3 儲存貯體的名稱時，請輸入 S3 儲存貯體的名稱，然後按 Enter 鍵。
9. 當殼層介面提示您輸入 Comprehend 輸出檔案的完整檔案路徑時，請輸入 **output** 並按下 Enter 鍵。
10. 當 shell 介面提示您輸入中繼資料資料夾的完整檔案路徑時，請輸入 **metadata/** 並按 Enter 鍵。

Important

若要正確格式化中繼資料，步驟 8-10 中的輸入值必須精確無誤。

若要執行 Python 3 指令碼 (AWS CLI)

1. 若要下載 Python 3 檔案 converter.py，請在終端機視窗上執行下列命令：

Linux

```
curl -o path/converter.py.zip https://docs.aws.amazon.com/kendra/latest/dg/samples/converter.py.zip
```

其中：

- *path/* 是要保存壓縮文件的位置的文件路徑。

macOS

```
curl -o path/converter.py.zip https://docs.aws.amazon.com/kendra/latest/dg/samples/converter.py.zip
```

其中：

- *path/* 是要保存壓縮文件的位置的文件路徑。

Windows

```
curl -o path/converter.py.zip https://docs.aws.amazon.com/kendra/latest/dg/samples/converter.py.zip
```

其中：

- *path/* 是要保存壓縮文件的位置的文件路徑。

2. 若要解壓縮 Python 3 檔案，請在終端機視窗中執行下列命令：

Linux

```
unzip path/converter.py.zip -d path/
```

其中：

- *path/* 是您保存的文件路徑。converter.py.zip

macOS

```
unzip path/converter.py.zip -d path/
```

其中：

- *path/* 是您保存的文件路徑。converter.py.zip

Windows

```
tar -xf path/converter.py.zip -C path/
```

其中：

- *path/* 是您保存的文件路徑。converter.py.zip

3. 通過運行以下命令，確保 Boto3 已安裝在設備上。

Linux

```
pip3 show boto3
```

macOS

```
pip3 show boto3
```

Windows

```
pip3 show boto3
```

Note

如果您沒有安裝 Boto3，請運行 `pip3 install boto3` 以安裝它。

- 若要執行 Python 3 指令碼來轉換 output 檔案，請執行下列命令。

Linux

```
python path/converter.py
```

其中：

- *path/* 是您保存的文件路徑。converter.py.zip

macOS

```
python path/converter.py
```

其中：

- *path/* 是您保存的文件路徑。converter.py.zip

Windows

```
python path/converter.py
```

其中：

- *path/* 是您保存的文件路徑。converter.py.zip
5. 出現 AWS CLI 提示時 Enter the name of your S3 bucket，請輸入 S3 儲存貯體的名稱，然後按 Enter 鍵。
 6. 出現提 AWS CLI 示時 Enter the full filepath to your Comprehend output file，請輸入 **output** 並按 Enter 鍵。
 7. 出現提 AWS CLI 示時 Enter the full filepath to your metadata folder，請輸入 **metadata/** 並按 Enter 鍵。

Important

若要正確格式化中繼資料，必須精確步驟 5-7 中的輸入值。

在此步驟結束時，格式化的中繼資料會存放在 S3 儲存貯體的資料 metadata 夾內。

清理你的 Amazon S3 存儲桶

由於 Amazon Kendra 索引會同步儲存在儲存貯體中的所有檔案，因此建議您清理 Amazon S3 儲存貯體以防止多餘的搜尋結果。

清理您的 Amazon S3 存儲桶（控制台）

1. 前往 <https://console.aws.amazon.com/s3/> 開啟的 Amazon Simple Storage Service (Amazon S3) 主控台。
2. 在值區中，選擇您的儲存貯體，然後選取 Amazon Comprehend 實體分析輸出資料夾、Amazon Comprehend 實體分析.temp 檔案，以及擷取的 Amazon Comprehend 檔案。output
3. 從「概覽」標籤中選擇「刪除」。
4. 在 [刪除物件] 中，選擇 [永久刪除物件？] 並 **permanently delete** 在文字輸入欄位中輸入。
5. 選擇 Delete objects (刪除物件)。

清理您的 Amazon S3 存儲桶 (AWS CLI)

1. 若要刪除 S3 儲存貯體中除了和資料夾以外的所有檔案data和metadata資料夾，請使用以下指令中的 [remove](#) 命令 AWS CLI：

Linux

```
aws s3 rm s3://DOC-EXAMPLE-BUCKET/ --recursive --exclude "data/*" --exclude "metadata/*"
```

其中：

- 文檔示例存儲桶是您的 S3 存儲桶的名稱。

macOS

```
aws s3 rm s3://DOC-EXAMPLE-BUCKET/ --recursive --exclude "data/*" --exclude "metadata/*"
```

其中：

- 文檔示例存儲桶是您的 S3 存儲桶的名稱。

Windows

```
aws s3 rm s3://DOC-EXAMPLE-BUCKET/ --recursive --exclude "data/*" --exclude "metadata/*"
```

其中：

- 文檔示例存儲桶是您的 S3 存儲桶的名稱。

2. 若要確保物件已成功從 S3 儲存貯體中刪除，請使用 [list](#) 指令檢查其內容：

Linux

```
aws s3 ls s3://DOC-EXAMPLE-BUCKET/
```

其中：

- 文檔示例存儲桶是您的 S3 存儲桶的名稱。

macOS

```
aws s3 ls s3://DOC-EXAMPLE-BUCKET/
```

其中：

- 文檔示例存儲桶是您的 S3 存儲桶的名稱。

Windows

```
aws s3 ls s3://DOC-EXAMPLE-BUCKET/
```

其中：

- 文檔示例存儲桶是您的 S3 存儲桶的名稱。

在此步驟結束時，您已將 Amazon Comprehend 實體分析輸出轉換為 Amazon Kendra 中繼資料。您現在已準備好建立 Amazon Kendra 索引。

步驟 4：建立 Amazon Kendra 索引並擷取中繼資料

若要實作智慧型搜尋解決方案，您需要建立 Amazon Kendra 索引，並將 S3 資料和中繼資料導入其中。

在將中繼資料新增至 Amazon Kendra 索引之前，您必須建立與自訂文件屬性對應的自訂索引欄位，這些欄位會對應於 Amazon Comprehend 實體類型。Amazon Kendra 使用您建立的索引欄位和自訂文件屬性來搜尋和篩選文件。

如需詳細資訊，請參閱[索引](#)和[建立自訂文件屬性](#)。

主題

- [創建一個 Amazon Kendra 索引](#)
- [更新 Amazon S3 存取的 IAM 角色](#)
- [創建 Amazon Kendra 自定義搜索索引字段](#)

- [將 Amazon S3 儲存貯體新增為索引的資料來源](#)
- [同步 Amazon Kendra 索引](#)

創建一個 Amazon Kendra 索引

若要查詢來源文件，請建立 Amazon Kendra 索引。

如果您在此步驟 AWS CLI 中使用，請建立並附加 AWS IAM 角色和政策，讓 Amazon Kendra 在建立索引之前存取 CloudWatch 日誌。如需詳細資訊，請參閱[先決條件](#)。

若要建立 Amazon Kendra 索引 (主控台)

1. 在 <https://console.aws.amazon.com/kendra/> 上打開 Amazon Kendra 控制台。

Important

確保您位於建立 Amazon Comprehend 實體分析任務和 Amazon S3 儲存貯體所在的區域中。如果您位於其他區域，請從頂端導覽列的 AWS 區域選擇器中選擇建立 Amazon S3 儲存貯體的區域。

2. 選擇 [建立索引]。
3. 如需 [指定索引詳細資訊] 頁面的索引詳細資訊，請執行下列動作
 - a. 對於 Index name (索引名稱)，輸入 **kendra-index**。
 - b. 請將「描述」欄位保持空白。
 - c. 對於 IAM 角色，選擇建立新角色。此角色可讓您存取 Amazon S3 儲存貯體。
 - d. 在角色名稱中，輸入 **kendra-role**。IAM 角色將具有前置詞AmazonKendra-。
 - e. 保留「加密」和「標籤」的預設設定，然後選擇「下
4. 對於 [設定使用者存取控制] 頁面上的存取控制設定，請選擇否，然後選擇 [下一步]。
5. 對於佈建詳細資料頁面上的佈建版本，選擇開發人員版本，然後選擇建立。

若要建立 Amazon Kendra 索引 (AWS CLI)

1. 若要為 Amazon Kendra 建立並附加將其識別為受信任實體的 IAM 角色，請執行以下操作：
 - a. 將下列信任原則儲存為本機裝置上文字編輯器kendra-trust-policy.json中呼叫的 JSON 檔案。

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

- b. 若要建立名為的 IAM 角色，`kendra-role`並將儲存的`kendra-trust-policy.json`檔案附加至該角色，請使用 `create-role` 命令：

Linux

```
aws iam create-role \
  --role-name kendra-role \
  --assume-role-policy-document file://path/kendra-trust-policy.json
```

其中：

- *path/* 是本地設備`kendra-trust-policy.json`上的文件路徑。

macOS

```
aws iam create-role \
  --role-name kendra-role \
  --assume-role-policy-document file://path/kendra-trust-policy.json
```

其中：

- *path/* 是本地設備`kendra-trust-policy.json`上的文件路徑。


Windows

```
aws iam create-role ^
  --role-name kendra-role ^
  --assume-role-policy-document file://path/kendra-trust-policy.json
```

其中：

- `path/` 是本地設備 `kendra-trust-policy.json` 上的文件路徑。

- c. 將 Amazon 資源名稱 (ARN) 複製到您的文字編輯器，並將其儲存為 `kendra-role-arn` 本機。

 Note

ARN 的格式類似於 `arn:aw:IAM::123456789012:##/#####`。您需要儲存的 ARN 才 `kendra-role-arn` 能執行 Amazon Kendra 任務。

2. 在建立索引之前，您 `kendra-role` 必須提供寫入 CloudWatch 記錄檔的權限。若要執行此動作，請執行下列步驟。
 - a. 將下列信任原則儲存為本機裝置上文字編輯器 `kendra-cloudwatch-policy.json` 中呼叫的 JSON 檔案。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "cloudwatch:PutMetricData",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "cloudwatch:namespace": "Kendra"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": "logs:DescribeLogGroups",
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": "logs:CreateLogGroup",
      "Resource": "arn:aws:logs:aws-region:aws-account-id:log-group:/aws/kendra/*"
    }
  ],
}
```

```
{
  "Effect": "Allow",
  "Action": [
    "logs:DescribeLogStreams",
    "logs:CreateLogStream",
    "logs:PutLogEvents"
  ],
  "Resource": "arn:aws:logs:aws-region:aws-account-id:log-group:/aws/kendra/*:log-stream:*"
}
```

將 *aws-region* ##### AWS 區，並 *aws-account-id* 使用您的 12 位數 AWS 帳戶 ID。

- b. 若要建立存取 CloudWatch 記錄的 IAM 政策，請使用 [建立](#) 政策命令：

Linux

```
aws iam create-policy \
  --policy-name kendra-cloudwatch-policy \
  --policy-document file://path/kendra-cloudwatch-policy.json
```

其中：

- *path/* 是本地設備 `kendra-cloudwatch-policy.json` 上的文件路徑。

macOS

```
aws iam create-policy \
  --policy-name kendra-cloudwatch-policy \
  --policy-document file://path/kendra-cloudwatch-policy.json
```

其中：

- *path/* 是本地設備 `kendra-cloudwatch-policy.json` 上的文件路徑。

Windows

```
aws iam create-policy ^
```

```
--policy-name kendra-cloudwatch-policy ^  
--policy-document file://path/kendra-cloudwatch-policy.json
```

其中：

- *path* 是本地設備 `kendra-cloudwatch-policy.json` 上的文件路徑。

- c. 將 Amazon 資源名稱 (ARN) 複製到您的文字編輯器，並將其儲存為 `kendra-cloudwatch-arn` 本機。

Note

ARN 的格式類似於 `ARN: AW: IAM:: 12345678 9012: ##/`。 `kendra-cloudwatch-policy` 您需要另存的 ARN 才 `kendra-cloudwatch-arn` 能將其附加 `kendra-cloudwatch-policy` 到 IAM 角色。

- d. 若要附加 `kendra-cloudwatch-policy` 到您的 IAM 角色，請使用以下 [attach-role-policy](#) 命令：

Linux

```
aws iam attach-role-policy \  
    --policy-arn policy-arn \  
    --role-name kendra-role
```

其中：

- *####* 是你保存的。 `kendra-cloudwatch-arn`

macOS

```
aws iam attach-role-policy \  
    --policy-arn policy-arn \  
    --role-name kendra-role
```

其中：

- *####* 是你保存的。 `kendra-cloudwatch-arn`

Windows

```
aws iam attach-role-policy ^
    --policy-arn policy-arn ^
    --role-name kendra-role
```

其中：

- *####*是你保存的。kendra-cloudwatch-arn

3. 若要建立索引，請使用[建立索引](#)指令：

Linux

```
aws kendra create-index \  
    --name kendra-index \  
    --edition DEVELOPER_EDITION \  
    --role-arn role-arn \  
    --region aws-region
```

其中：

- *## arn* 是你保存的，kendra-role-arn
- *aws-region ### AWS ##*。

macOS

```
aws kendra create-index \  
    --name kendra-index \  
    --edition DEVELOPER_EDITION \  
    --role-arn role-arn \  
    --region aws-region
```

其中：

- *## arn* 是你保存的，kendra-role-arn
- *aws-region ### AWS ##*。

Windows

```
aws kendra create-index ^
  --name kendra-index ^
  --edition DEVELOPER_EDITION ^
  --role-arn role-arn ^
  --region aws-region
```

其中：

- *## arn* 是你保存的，*kendra-role-arn*
 - *aws-region ### AWS ##*。
4. 複製索引Id並將其儲存在文字編輯器中*kendra-index-id*。可Id協助您追蹤索引建立的狀態。
 5. 若要追蹤索引建立工作的進度，請使用[描述](#)索引指令：

Linux

```
aws kendra describe-index \  
  --id kendra-index-id \  
  --region aws-region
```

其中：

- *kendra-index-id*是你的保存*kendra-index-id*，
- *aws-region ### AWS ##*。

macOS

```
aws kendra describe-index \  
  --id kendra-index-id \  
  --region aws-region
```

其中：

- *kendra-index-id*是你的保存*kendra-index-id*，
- *aws-region ### AWS ##*。

Windows

```
aws kendra describe-index ^  
    --id kendra-index-id ^  
    --region aws-region
```

其中：

- *kendra-index-id* 是你的保存 `kendra-index-id`，
- *aws-region ### AWS ##*。

索引建立過程平均需要 15 分鐘，但可能需要更長的時間。當索引的狀態處於作用中狀態時，您的索引就可以使用了。建立索引時，您可以開始下一個步驟。

如果您在此步驟 AWS CLI 中使用，您可以建立 IAM 政策並將其附加到 Amazon Kendra IAM 角色，以便為您提供存取 S3 儲存貯體的索引許可。

更新 Amazon S3 存取的 IAM 角色

建立索引時，您可以更新 Amazon Kendra IAM 角色，以允許您建立的索引從 Amazon S3 儲存貯體讀取資料。如需詳細資訊，請參閱 [適用於 Amazon Kendra 的 IAM 存取角色](#)。

更新您的 IAM 角色 (主控台)

1. 前往 <https://console.aws.amazon.com/iam/> 開啟 IAM 主控台。
2. 在左側導覽窗格中，選擇 [角色]，並 `kendra-role` 在 [角色名稱] 上方的 [搜尋] 方塊中輸入。
3. 從建議的選項中，單擊 `kendra-role`。
4. 在 [摘要] 中選擇 [附加原則]。
5. 在 [附加權限] 的 [搜尋] 方塊中，輸入 `S3` 並從建議選項中選取 `AmazonS3 ReadOnlyAccess` 政策旁邊的核取方塊。
6. 選擇連接政策。在 [摘要] 頁面上，您現在會看到兩個附加至 IAM 角色的政策。
7. 返回 Amazon Kendra 主控台，網址為 <https://console.aws.amazon.com/kendra/>，等待索引狀態從「建立」變更為「作用中」，然後再繼續進行下一個步驟。

若要更新您的 IAM 角色 (AWS CLI)

1. 將下列文字儲存在本機裝置上的文字編輯器 `kendra-S3-access-policy.json` 中稱為的 JSON 檔案中。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "s3:GetObject"
      ],
      "Resource": [
        "arn:aws:s3:::DOC-EXAMPLE-BUCKET/*"
      ],
      "Effect": "Allow"
    },
    {
      "Action": [
        "s3:ListBucket"
      ],
      "Resource": [
        "arn:aws:s3:::DOC-EXAMPLE-BUCKET"
      ],
      "Effect": "Allow"
    },
    {
      "Effect": "Allow",
      "Action": [
        "kendra:BatchPutDocument",
        "kendra:BatchDeleteDocument",
        "kendra:ListDataSourceSyncJobs"
      ],
      "Resource": [
        "arn:aws:kendra:aws-region:aws-account-id:index/kendra-index-id"
      ]
    }
  ]
}
```

使用您的 S3 儲存貯體名稱取代 DOC/EXAMPLE 儲存貯體，將 *aws-region* 取代為您的區域，並使用您 AWS 儲存 *aws-account-id* 的 12 位數 AWS 帳戶 ID 取代。 *kendra-index-id* `kendra-index-id`

- 若要建立 IAM 政策以存取 S3 儲存貯體，請使用建 [立](#) 政策命令：

Linux

```
aws iam create-policy \  
    --policy-name kendra-S3-access-policy \  
    --policy-document file://path/kendra-S3-access-policy.json
```

其中：

- *path/* 是本地設備 `kendra-S3-access-policy.json` 上的文件路徑。

macOS

```
aws iam create-policy \  
    --policy-name kendra-S3-access-policy \  
    --policy-document file://path/kendra-S3-access-policy.json
```

其中：

- *path/* 是本地設備 `kendra-S3-access-policy.json` 上的文件路徑。

Windows

```
aws iam create-policy ^  
    --policy-name kendra-S3-access-policy ^  
    --policy-document file://path/kendra-S3-access-policy.json
```

其中：

- *path/* 是本地設備 `kendra-S3-access-policy.json` 上的文件路徑。

- 將 Amazon 資源名稱 (ARN) 複製到您的文字編輯器，並將其儲存為 `kendra-S3-access-arn` 本機。

Note

ARN 的格式類似於 ARN: aw: IAM:: 123456789012: **##/###-S3-#**問策略。您需要另存的 ARN 才 `kendra-S3-access-arn` 能將其附加 `kendra-S3-access-policy` 到 IAM 角色。

4. 若要附加 `kendra-S3-access-policy` 到您的 Amazon Kendra IAM 角色，請使用以下 [attach-role-policy](#) 命令：

Linux

```
aws iam attach-role-policy \  
    --policy-arn policy-arn \  
    --role-name kendra-role
```

其中：

- **###**是你保存的。 `kendra-S3-access-arn`

macOS

```
aws iam attach-role-policy \  
    --policy-arn policy-arn \  
    --role-name kendra-role
```

其中：

- **###**是你保存的。 `kendra-S3-access-arn`

Windows

```
aws iam attach-role-policy ^  
    --policy-arn policy-arn ^  
    --role-name kendra-role
```

其中：

- **###**是你保存的。 `kendra-S3-access-arn`

創建 Amazon Kendra 自定義搜索索引字段

若要準備 Amazon Kendra 將中繼資料識別為自訂文件屬性，您可以建立與 Amazon Comprehend 實體類型對應的自訂欄位。您輸入下列九個 Amazon Comprehend 類型做為自訂欄位：

- 商業項目
- DATE
- EVENT
- LOCATION
- 組織
- OTHER
- 人
- 數量
- 標題

Important

拼錯的實體類型將不會被索引識別。

若要為您的 Amazon Kendra 索引 (主控台) 建立自訂欄位

1. 在 <https://console.aws.amazon.com/kendra/> 上打開 Amazon Kendra 控制台。
2. 從「索引」清單中，按一下 `kendra-index`。
3. 從左側導覽面板的 [資料管理] 下，選擇 [Facet 定義]。
4. 從 [索引欄位] 功能表中，選擇 [新增欄位]。
5. 在 [新增索引欄位] 對話方塊中，執行下列動作：
 - a. 在欄位名稱中，輸入 **COMMERCIAL_ITEM**。
 - b. 在 [資料類型] 中選擇 [字串清單]。
 - c. 在「使用情況類型」中，選取「可刻面」、「可搜尋」及「可顯示」，然後選擇「新增」。
 - d. 針對每個 Amazon Comprehend 實體類型重複步驟 a 到 c：商業項目、日期、事件、地點、組織、其他、人員、數量、標題。

主控台會顯示成功的欄位新增訊息。您可以選擇關閉它們，然後再繼續進行下一個步驟。

若要為您的 Amazon Kendra 索引建立自訂欄位 ()AWS CLI

1. 將下列文字儲存為本機裝置上文字編輯器custom-attributes.json中呼叫的 JSON 檔案。

```
[
  {
    "Name": "COMMERCIAL_ITEM",
    "Type": "STRING_LIST_VALUE",
    "Search": {
      "Facetable": true,
      "Searchable": true,
      "Displayable": true
    }
  },
  {
    "Name": "DATE",
    "Type": "STRING_LIST_VALUE",
    "Search": {
      "Facetable": true,
      "Searchable": true,
      "Displayable": true
    }
  },
  {
    "Name": "EVENT",
    "Type": "STRING_LIST_VALUE",
    "Search": {
      "Facetable": true,
      "Searchable": true,
      "Displayable": true
    }
  },
  {
    "Name": "LOCATION",
    "Type": "STRING_LIST_VALUE",
    "Search": {
      "Facetable": true,
      "Searchable": true,
      "Displayable": true
    }
  },
  {
```

```
    "Name": "ORGANIZATION",
    "Type": "STRING_LIST_VALUE",
    "Search": {
      "Facetable": true,
      "Searchable": true,
      "Displayable": true
    }
  },
  {
    "Name": "OTHER",
    "Type": "STRING_LIST_VALUE",
    "Search": {
      "Facetable": true,
      "Searchable": true,
      "Displayable": true
    }
  },
  {
    "Name": "PERSON",
    "Type": "STRING_LIST_VALUE",
    "Search": {
      "Facetable": true,
      "Searchable": true,
      "Displayable": true
    }
  },
  {
    "Name": "QUANTITY",
    "Type": "STRING_LIST_VALUE",
    "Search": {
      "Facetable": true,
      "Searchable": true,
      "Displayable": true
    }
  },
  {
    "Name": "TITLE",
    "Type": "STRING_LIST_VALUE",
    "Search": {
      "Facetable": true,
      "Searchable": true,
      "Displayable": true
    }
  }
}
```

]

2. 要在索引中創建自定義字段，請使用[更新索引](#)命令：

Linux

```
aws kendra update-index \  
    --id kendra-index-id \  
    --document-metadata-configuration-updates file://path/custom-  
attributes.json \  
    --region aws-region
```

其中：

- *kendra-index-id* 是你的保存 `kendra-index-id`，
- *path/* 是本地設備 `custom-attributes.json` 上的文件路徑，
- *aws-region* ### AWS ##。

macOS

```
aws kendra update-index \  
    --id kendra-index-id \  
    --document-metadata-configuration-updates file://path/custom-  
attributes.json \  
    --region aws-region
```

其中：

- *kendra-index-id* 是你的保存 `kendra-index-id`，
- *path/* 是本地設備 `custom-attributes.json` 上的文件路徑，
- *aws-region* ### AWS ##。

Windows

```
aws kendra update-index ^  
    --id kendra-index-id ^  
    --document-metadata-configuration-updates file://path/custom-  
attributes.json ^
```

```
--region aws-region
```

其中：

- *kendra-index-id* 是你的保存 `kendra-index-id`，
- *path/* 是本地設備 `custom-attributes.json` 上的文件路徑，
- *aws-region ### AWS ##*。

3. 若要確認自訂屬性是否已新增至索引，請使用 [describe-index](#) 指令：

Linux

```
aws kendra describe-index \  
    --id kendra-index-id \  
    --region aws-region
```

其中：

- *kendra-index-id* 是你的保存 `kendra-index-id`，
- *aws-region ### AWS ##*。

macOS

```
aws kendra describe-index \  
    --id kendra-index-id \  
    --region aws-region
```

其中：

- *kendra-index-id* 是你的保存 `kendra-index-id`，
- *aws-region ### AWS ##*。

Windows

```
aws kendra describe-index ^  
    --id kendra-index-id ^  
    --region aws-region
```


其中：

- *kendra-index-id* 是你的保存 `kendra-index-id`，
- *aws-region ### AWS ##*。

將 Amazon S3 儲存貯體新增為索引的資料來源

在您可以同步索引之前，您必須先將 S3 資料來源連線到索引。

將 S3 儲存貯體連接到您的 Amazon Kendra 索引 (控制台)

1. 在 <https://console.aws.amazon.com/kendra/> 上打開 Amazon Kendra 控制台。
2. 從「索引」清單中，按一下 `kendra-index`。
3. 從左側導覽功能表的 [資料管理] 下，選擇 [資料來源]。
4. 在「選取資料來源連接器類型」區段下，導覽至 Amazon S3，然後選擇「新增連接器」。
5. 在 [指定資料來源詳細資訊] 頁面中，執行下列動作：
 - a. 在「名稱和說明」下，對於「資料來源名稱」，輸入 **S3-data-source**。
 - b. 將 [說明] 區段保持空白。
 - c. 保留「標籤」的預設設定。
 - d. 選擇下一步。
6. 在 [設定同步設定] 頁面的 [同步範圍] 區段中，執行下列動作：
 - a. 在 [輸入資料來源位置] 中，選擇 [瀏覽 S3]。
 - b. 在 [選擇資源] 中，選取 S3 儲存貯體，然後選擇 [選擇]。
 - c. 在中繼資料檔案前置詞資料夾位置中，選擇瀏覽 S3。
 - d. 在 [選擇資源] 中，按一下值區清單中的值區名稱。
 - e. 對於「物件」，請選取選項方塊，`metadata` 然後選擇「選擇」。位置字段現在應該說 `metadata/`。
 - f. 保留存取控制清單組態檔案位置、選取解密金鑰和其他組態的預設設定。
7. 對於 IAM 角色，在 [設定同步設定] 頁面上，選擇 `kendra-role`。
8. 在 [設定同步設定] 頁面的 [同步執行排程] 下，針對 [頻率] 選擇 [視需求執行]，然後選擇 [下一步]。
9. 在「檢閱並建立」頁面上，檢閱您對資料來源詳細資訊的選擇，然後選擇「新增資料來源」。

將 S3 存儲桶連接到 Amazon Kendra 索引 () AWS CLI

1. 將下列文字儲存為本機裝置上文字編輯器 `S3-data-connector.json` 中呼叫的 JSON 檔案。

```
{
  "S3Configuration":{
    "BucketName":"DOC-EXAMPLE-BUCKET",
    "DocumentsMetadataConfiguration":{
      "S3Prefix":"metadata"
    }
  }
}
```

將文件範例儲存貯體取代為 S3 儲存貯體的名稱。

2. 要將 S3 存儲桶連接到索引，請使用以下 [create-data-source](#) 命令：

Linux

```
aws kendra create-data-source \
  --index-id kendra-index-id \
  --name S3-data-source \
  --type S3 \
  --configuration file://path/S3-data-connector.json \
  --role-arn role-arn \
  --region aws-region
```

其中：

- *kendra-index-id* 是你的保存 `kendra-index-id`，
- *path/* 是本地設備 `S3-data-connector.json` 上的文件路徑，
- *## arn* 是你保存的，`kendra-role-arn`
- *aws-region ### AWS ##*。

macOS

```
aws kendra create-data-source \
  --index-id kendra-index-id \
  --name S3-data-source \
  --type S3 \
```

```
--configuration file://path/S3-data-connector.json \  
--role-arn role-arn \  
--region aws-region
```

其中：

- *kendra-index-id* 是你的保存 `kendra-index-id`，
- *path/* 是本地設備 `S3-data-connector.json` 上的文件路徑，
- *## arn* 是你保存的，`kendra-role-arn`
- *aws-region ### AWS ##*。

Windows

```
aws kendra create-data-source ^  
  --index-id kendra-index-id ^  
  --name S3-data-source ^  
  --type S3 ^  
  --configuration file://path/S3-data-connector.json ^  
  --role-arn role-arn ^  
  --region aws-region
```

其中：

- *kendra-index-id* 是你的保存 `kendra-index-id`，
- *path/* 是本地設備 `S3-data-connector.json` 上的文件路徑，
- *## arn* 是你保存的，`kendra-role-arn`
- *aws-region ### AWS ##*。

3. 複製連接器 Id 並將其儲存在文字編輯器中 `S3-connector-id`。可 Id 協助您追蹤資料連線程序的狀態。
4. 若要確保 S3 資料來源已成功連線，請使用以下 [describe-data-source](#) 指令：

Linux

```
aws kendra describe-data-source \  
  --id S3-connector-id \  
  --index-id kendra-index-id \  
  --region aws-region
```

其中：

- *S3 ### ID ###* 存的，S3-connector-id
- *kendra-index-id* 是你的保存kendra-index-id，
- *aws-region ### AWS ##*。

macOS

```
aws kendra describe-data-source \  
  --id S3-connector-id \  
  --index-id kendra-index-id \  
  --region aws-region
```

其中：

- *S3 ### ID ###* 存的，S3-connector-id
- *kendra-index-id* 是你的保存kendra-index-id，
- *aws-region ### AWS ##*。

Windows

```
aws kendra describe-data-source ^  
  --id S3-connector-id ^  
  --index-id kendra-index-id ^  
  --region aws-region
```

其中：

- *S3 ### ID ###* 存的，S3-connector-id
- *kendra-index-id* 是你的保存kendra-index-id，
- *aws-region ### AWS ##*。

在此步驟結束時，您的 Amazon S3 資料來源會連接到索引。

同步 Amazon Kendra 索引

新增了 Amazon S3 資料來源後，您現在可以將 Amazon Kendra 索引同步到該資料來源。

同步您的 Amazon Kendra 索引 (控制台)

1. 在 <https://console.aws.amazon.com/kendra/> 上打開 Amazon Kendra 控制台。
2. 從「索引」清單中，按一下kendra-index。
3. 從左側導覽功能表中，選擇 [資料來源]。
4. 在資料來源中，選取S3-data-source。
5. 在頂端導覽列中，選擇 [立即同步處理]。

同步您的 Amazon Kendra 索引 () AWS CLI

1. 若要同步您的索引，請使用 [start-data-source-sync-job](#) 指令：

Linux

```
aws kendra start-data-source-sync-job \  
    --id S3-connector-id \  
    --index-id kendra-index-id \  
    --region aws-region
```

其中：

- *S3 ### ID ###* 存的，S3-connector-id
- *kendra-index-id* 是你的保存kendra-index-id，
- *aws-region ### AWS ##*。

macOS

```
aws kendra start-data-source-sync-job \  
    --id S3-connector-id \  
    --index-id kendra-index-id \  
    --region aws-region
```

其中：

- *S3 ### ID ###* 存的, S3-connector-id
- *kendra-index-id* 是你的保存kendra-index-id ,
- *aws-region ### AWS ##*。

Windows

```
aws kendra start-data-source-sync-job ^
  --id S3-connector-id ^
  --index-id kendra-index-id ^
  --region aws-region
```

其中：

- *S3 ### ID ###* 存的, S3-connector-id
- *kendra-index-id* 是你的保存kendra-index-id ,
- *aws-region ### AWS ##*。

2. 若要檢查索引同步的狀態，請使用 [list-data-source-sync-jobs](#) 指令：

Linux

```
aws kendra list-data-source-sync-jobs \  
  --id S3-connector-id \  
  --index-id kendra-index-id \  
  --region aws-region
```

其中：

- *S3 ### ID ###* 存的, S3-connector-id
- *kendra-index-id* 是你的保存kendra-index-id ,
- *aws-region ### AWS ##*。

macOS

```
aws kendra list-data-source-sync-jobs \  
  --id S3-connector-id \  
  --index-id kendra-index-id \  
  --region aws-region
```

```
--region aws-region
```

其中：

- *S3 ### ID ###* 存的，S3-connector-id
- *kendra-index-id* 是你的保存kendra-index-id，
- *aws-region ### AWS ##*。

Windows

```
aws kendra list-data-source-sync-jobs ^  
  --id S3-connector-id ^  
  --index-id kendra-index-id ^  
  --region aws-region
```

其中：

- *S3 ### ID ###* 存的，S3-connector-id
- *kendra-index-id* 是你的保存kendra-index-id，
- *aws-region ### AWS ##*。

在此步驟結束時，您已為資料集建立可搜尋且可篩選的 Amazon Kendra 索引。

步驟 5：查詢 Amazon Kendra 索引

您的 Amazon Kendra 索引現在已準備好進行自然語言查詢。當您搜尋索引時，Amazon Kendra 會使用您提供的所有資料和中繼資料，為您的搜尋查詢傳回最準確的答案。

Amazon Kendra 可以回答三種類型的查詢：

- Factoid 查詢 (「誰」，「什麼」，「何時」或「在哪裡」問題)
- 描述性查詢 (「如何」問題)
- 關鍵字搜尋 (意圖和範圍不清楚的問題)

主題

- [查詢您的 Amazon Kendra 索引](#)

- [篩選搜尋結果](#)

查詢您的 Amazon Kendra 索引

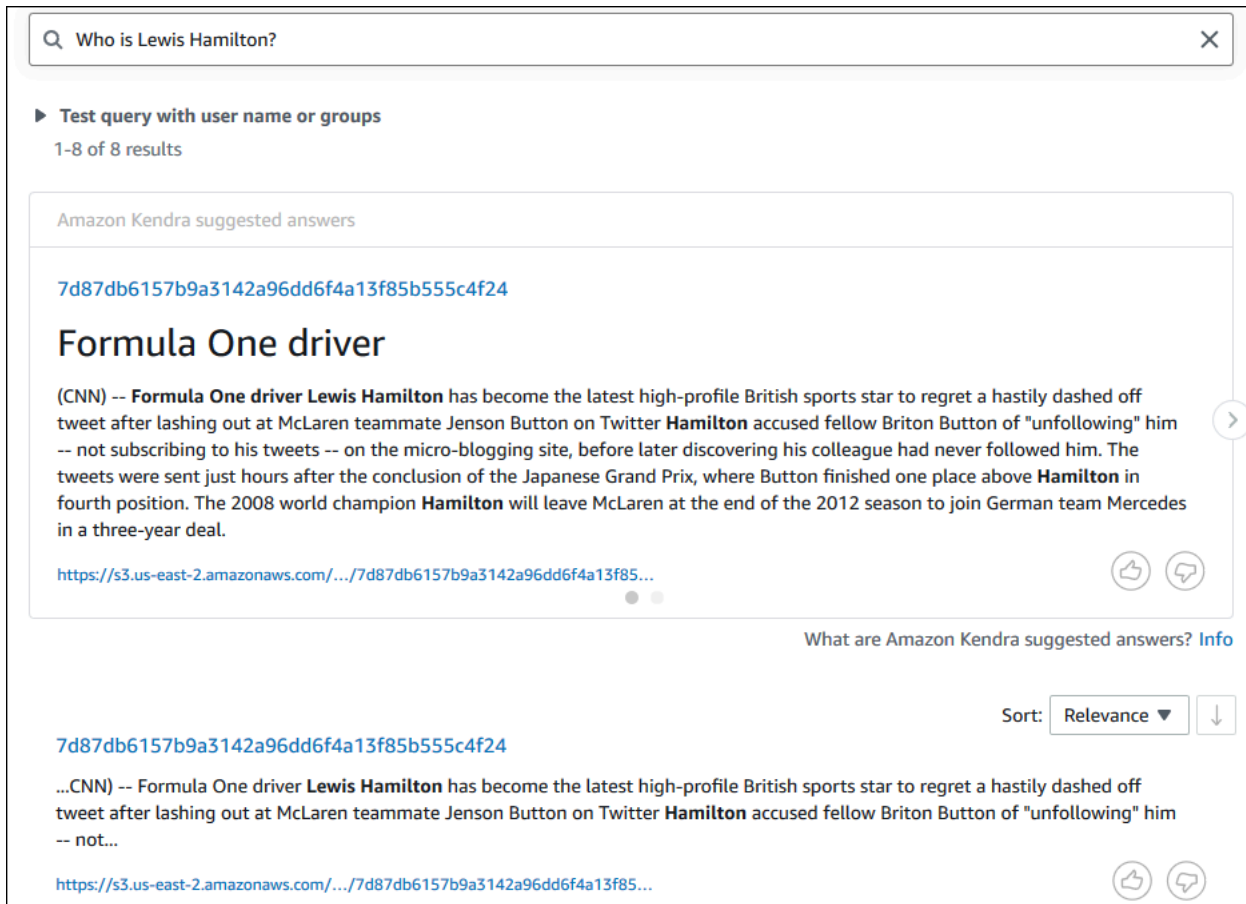
您可以使用與 Amazon Kendra 支援的三種查詢類型相對應的問題來查詢 Amazon Kendra 索引。如需詳細資訊，請參閱[查詢](#)。

本節中的範例問題已根據範例資料集選擇。

查詢您的 Amazon Kendra 索引（控制台）

1. 在 <https://console.aws.amazon.com/kendra/> 上打開 Amazon Kendra 控制台。
2. 從「索引」清單中，按一下 `kendra-index`。
3. 從左側導覽選單中，選擇搜尋索引的選項。
4. 若要執行範例 factoid 查詢，請 **Who is Lewis Hamilton?** 在搜尋方塊中輸入，然後按 Enter 鍵。

第一個傳回的結果是 Amazon Kendra 建議的答案，以及包含答案的資料檔案。結果的其餘部分構成了一組推薦的文件。



Q Who is Lewis Hamilton? ✕

▶ Test query with user name or groups
1-8 of 8 results

Amazon Kendra suggested answers

[7d87db6157b9a3142a96dd6f4a13f85b555c4f24](#)

Formula One driver

(CNN) -- **Formula One driver Lewis Hamilton** has become the latest high-profile British sports star to regret a hastily dashed off tweet after lashing out at McLaren teammate Jenson Button on Twitter **Hamilton** accused fellow Briton Button of "unfollowing" him -- not subscribing to his tweets -- on the micro-blogging site, before later discovering his colleague had never followed him. The tweets were sent just hours after the conclusion of the Japanese Grand Prix, where Button finished one place above **Hamilton** in fourth position. The 2008 world champion **Hamilton** will leave McLaren at the end of the 2012 season to join German team Mercedes in a three-year deal.

<https://s3.us-east-2.amazonaws.com/.../7d87db6157b9a3142a96dd6f4a13f85...>

What are Amazon Kendra suggested answers? [Info](#)

Sort: Relevance ▼ ↓

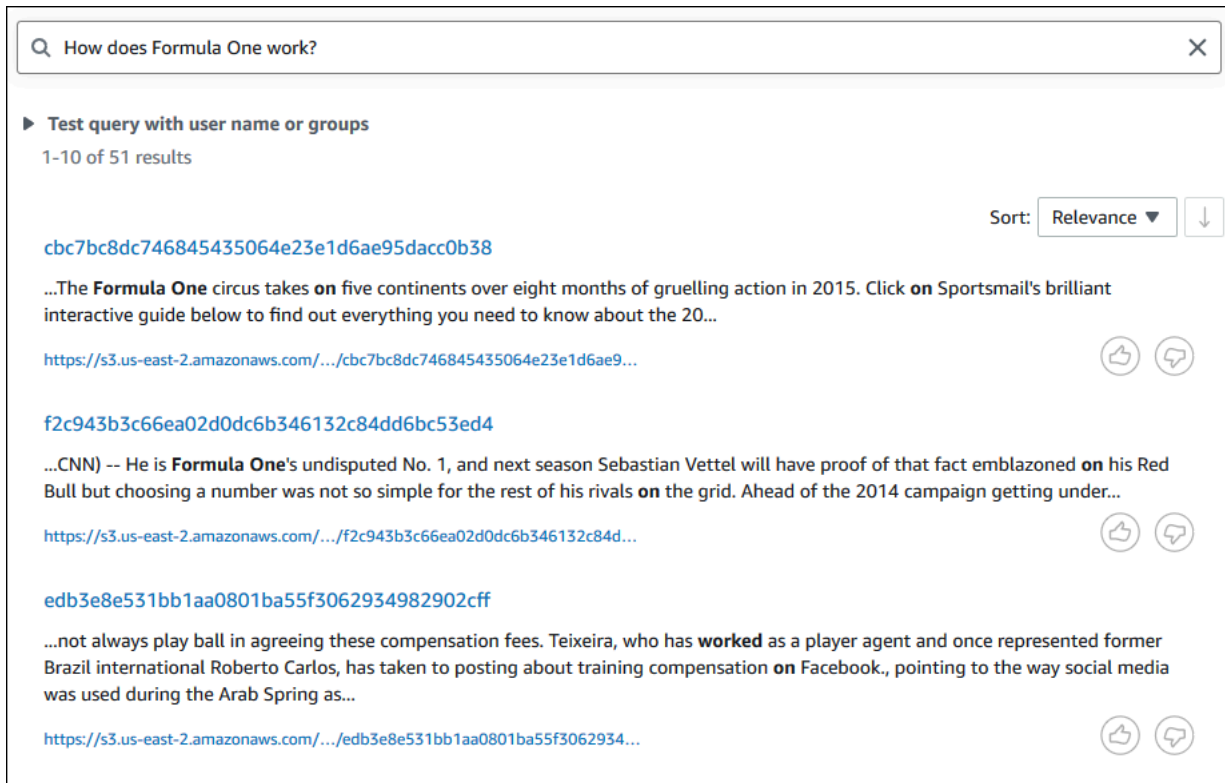
[7d87db6157b9a3142a96dd6f4a13f85b555c4f24](#)

...CNN) -- Formula One driver **Lewis Hamilton** has become the latest high-profile British sports star to regret a hastily dashed off tweet after lashing out at McLaren teammate Jenson Button on Twitter **Hamilton** accused fellow Briton Button of "unfollowing" him -- not...

<https://s3.us-east-2.amazonaws.com/.../7d87db6157b9a3142a96dd6f4a13f85...>

5. 若要執行描述性查詢，請 **How does Formula One work?** 在搜尋方塊中輸入，然後按 Enter。

您會看到 Amazon Kendra 主控台傳回的另一個結果，這次會反白顯示相關片語。



Q How does Formula One work? X

► Test query with user name or groups
1-10 of 51 results

Sort: Relevance ▼ ↓

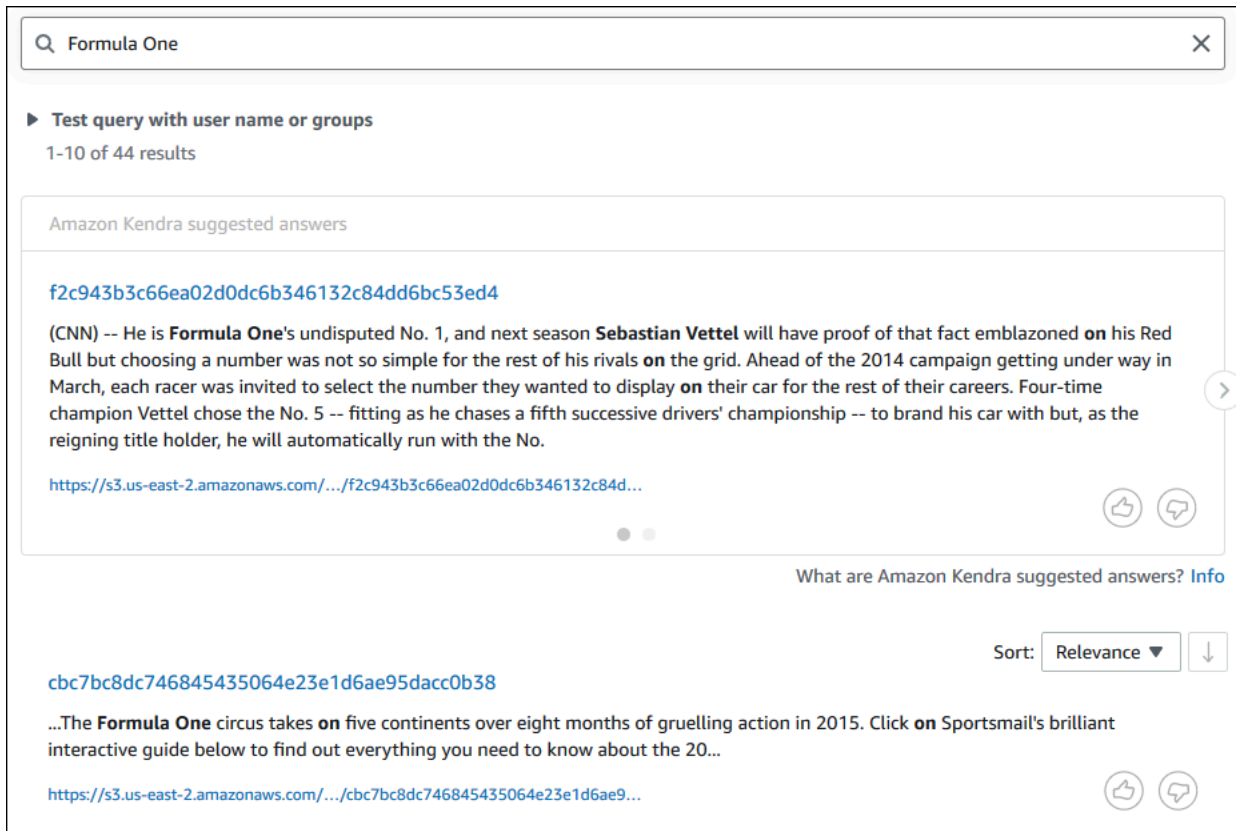
[cbc7bc8dc746845435064e23e1d6ae95dacc0b38](#)
...The **Formula One** circus takes **on** five continents over eight months of gruelling action in 2015. Click **on** Sportsmail's brilliant interactive guide below to find out everything you need to know about the 20...
<https://s3.us-east-2.amazonaws.com/.../cbc7bc8dc746845435064e23e1d6ae9...>

[f2c943b3c66ea02d0dc6b346132c84dd6bc53ed4](#)
...CNN) -- He is **Formula One**'s undisputed No. 1, and next season Sebastian Vettel will have proof of that fact emblazoned **on** his Red Bull but choosing a number was not so simple for the rest of his rivals **on** the grid. Ahead of the 2014 campaign getting under...
<https://s3.us-east-2.amazonaws.com/.../f2c943b3c66ea02d0dc6b346132c84d...>

[edb3e8e531bb1aa0801ba55f3062934982902cff](#)
...not always play ball in agreeing these compensation fees. Teixeira, who has **worked** as a player agent and once represented former Brazil international Roberto Carlos, has taken to posting about training compensation **on** Facebook., pointing to the way social media was used during the Arab Spring as...
<https://s3.us-east-2.amazonaws.com/.../edb3e8e531bb1aa0801ba55f3062934...>

6. 若要執行關鍵字搜尋，請**Formula One**在搜尋方塊中輸入，然後按 Enter 鍵。

您會看到 Amazon Kendra 主控台傳回的另一個結果，接著是資料集中所有其他提及片語的結果。



查詢您的 Amazon Kendra 索引 () AWS CLI

- 若要執行範例 factoid 查詢，請使用查詢指令：

Linux

```
aws kendra query \
  --index-id kendra-index-id \
  --query-text "Who is Lewis Hamilton?" \
  --region aws-region
```

其中：

- *kendra-index-id* 是你的保存 `kendra-index-id`，
- *aws-region* ### AWS ##。

macOS

```
aws kendra query \  
  --index-id kendra-index-id \  
  --query-text "Who is Lewis Hamilton?" \  
  --region aws-region
```

其中：

- *kendra-index-id* 是你的保存 `kendra-index-id`，
- *aws-region* ### AWS ##。

Windows

```
aws kendra query ^  
  --index-id kendra-index-id ^  
  --query-text "Who is Lewis Hamilton?" ^  
  --region aws-region
```

其中：

- *kendra-index-id* 是你的保存 `kendra-index-id`，
- *aws-region* ### AWS ##。

會 AWS CLI 顯示查詢的結果。

2. 若要執行範例描述性查詢，請使用 [query](#) 指令：

Linux

```
aws kendra query \  
  --index-id kendra-index-id \  
  --query-text "How does Formula One work?" \  
  --region aws-region
```

其中：

- *kendra-index-id* 是你的保存 `kendra-index-id`，

- *aws-region ### AWS ##*。

macOS

```
aws kendra query \  
  --index-id kendra-index-id \  
  --query-text "How does Formula One work?" \  
  --region aws-region
```

其中：

- *kendra-index-id*是你的保存kendra-index-id，
- *aws-region ### AWS ##*。

Windows

```
aws kendra query ^  
  --index-id kendra-index-id ^  
  --query-text "How does Formula One work?" ^  
  --region aws-region
```

其中：

- *kendra-index-id*是你的保存kendra-index-id，
- *aws-region ### AWS ##*。

會 AWS CLI 顯示查詢的結果。

3. 若要執行範例關鍵字搜尋，請使用 [query](#) 指令：

Linux

```
aws kendra query \  
  --index-id kendra-index-id \  
  --query-text "Formula One" \  
  --region aws-region
```

其中：

- *kendra-index-id* 是你的保存 `kendra-index-id` ,
- *aws-region ### AWS ##*。

macOS

```
aws kendra query \  
  --index-id kendra-index-id \  
  --query-text "Formula One" \  
  --region aws-region
```

其中：

- *kendra-index-id* 是你的保存 `kendra-index-id` ,
- *aws-region ### AWS ##*。

Windows

```
aws kendra query ^  
  --index-id kendra-index-id ^  
  --query-text "Formula One" ^  
  --region aws-region
```

其中：

- *kendra-index-id* 是你的保存 `kendra-index-id` ,
- *aws-region ### AWS ##*。

會 AWS CLI 顯示您查詢的傳回回答。

篩選搜尋結果

您可以使用 Amazon Kendra 主控台自訂文件屬性篩選和排序搜尋結果。如需 Amazon Kendra 如何處理查詢的詳細資訊，請參閱 [篩選查詢](#)。

若要篩選搜尋結果 (主控台)

1. 在 <https://console.aws.amazon.com/kendra/> 上打開 Amazon Kendra 控制台。
2. 從「索引」清單中，按一下 `kendra-index`。
3. 從左側導覽選單中，選擇搜尋索引的選項。
4. 在搜尋方塊中，輸入 **Soccer matches** 為查詢，然後按 Enter 鍵。
5. 從左側導覽功能表中選擇 [篩選搜尋結果]，以查看可用來篩選搜尋的 Facet 清單。
6. 勾選 EVENT 副標題下方的「歐洲冠軍聯賽」核取方塊，即可查看僅依含有「歐洲冠軍聯賽」的結果篩選搜尋結果。

The screenshot displays the Amazon Kendra search interface. At the top, a search bar contains the query "Soccer matches". Below the search bar, there are several facets for filtering results:

- LOCATION:** Hanover (1), Europe (1), Rome (1)
- OTHER:** Brazilian (2), European (1)
- ORGANIZATION:** Borussia Dortmund (1), UEFA (1), FIFA (1)
- DATE:** four years later (1), 2004 (1), Sunday (1)
- PERSON:** Manuel Neuer (1), Teixeira (1), Queen Elizabeth II (1)
- QUANTITY:** over 300 million people (1), 20% (1), 19 points (1)
- TITLE:** Universal Declaration of Human Rights (1)
- EVENT:** Champions League (3) (selected)

The main content area shows "Test query with user name or groups" with "1-4 of 4 results". Below this, there are "Amazon Kendra suggested answers" with the following results:

- 7e5db27742008942b2f9cf6ac41826f86148d1f**: Saturday's **match** will see one of the teams claim their fourth European title, overtaking the beaten finalist in the all-time winners' table. The wonder of Wembley To much national debate, Wembley Stadium, the recognized home of **soccer** in England -- the country where the sport originated -- was closed in 2000, ahead of a controversial proposal to raze it to the ground before building a new arena on the same site. Football cathedral prepares for final The stadium's dramatic opening in 1923 set the trend for 77 years of iconic images. <https://s3.us-east-2.amazonaws.com/.../7e5db27742008942b2f9cf6ac41826...>
- 7e5db27742008942b2f9cf6ac41826f86148d1f**: ...Saturday's **match** will see one of the teams claim their fourth European title, overtaking the beaten finalist in the all-time winners' table. The wonder of Wembley To much national debate, Wembley Stadium, the recognized home of **soccer** in England -- the country where the... <https://s3.us-east-2.amazonaws.com/.../7e5db27742008942b2f9cf6ac41826...>
- eabeaab06e62ca309bfc8c5fcac21d99d864ba2c**: ...We started well and had the **match** under control for the first 20 minutes, but Hoffenheim ran hard, showed lots of fighting spirit and seized the initiative," he said. "The draw's... <https://s3.us-east-2.amazonaws.com/.../eabeaab06e62ca309bfc8c5fcac21d99...>
- edb3e8e531bb1aa0801ba55f3062934982902cff**: ...da Gama, and that the Brazilian footballer confirms he had been at Botafogo for four years since the age of 12 from 2004. The gambling game: **Soccer's** battle with betting "The claim is for Botafogo and has nothing to do with Ceregatti," added Teixeira, after CNN asked to interview the player... <https://s3.us-east-2.amazonaws.com/.../edb3e8e531bb1aa0801ba55f3062934...>

At the bottom right, there is a "Sort: Relevance" dropdown and a "What are Amazon Kendra suggested answers? Info" link.

若要篩選搜尋結果 (AWS CLI)

1. 若要查看可用於搜尋的特定類型 (例如EVENT) 的實體，請使用 [query](#) 指令：

Linux

```
aws kendra query \  
  --index-id kendra-index-id \  
  --query-text "Soccer matches" \  
  --facets '[{"DocumentAttributeKey":"EVENT"}]' \  
  --region aws-region
```

其中：

- *kendra-index-id* 是你的保存kendra-index-id，
- *aws-region* ### AWS ##。

macOS

```
aws kendra query \  
  --index-id kendra-index-id \  
  --query-text "Soccer matches" \  
  --facets '[{"DocumentAttributeKey":"EVENT"}]' \  
  --region aws-region
```

其中：

- *kendra-index-id* 是你的保存kendra-index-id，
- *aws-region* ### AWS ##。

Windows

```
aws kendra query ^  
  --index-id kendra-index-id ^  
  --query-text "Soccer matches" ^  
  --facets '[{"DocumentAttributeKey":"EVENT"}]' ^  
  --region aws-region
```

其中：

- *kendra-index-id* 是你的保存 *kendra-index-id* ,
- *aws-region ### AWS ##*。

會 AWS CLI 顯示搜尋結果。若要取得類型的 Facet 清單 EVENT，請瀏覽至 AWS CLI 輸出的「FacetResults」區段，以查看可篩選 Facet 及其計數的清單。例如，其中一個方面是「冠軍聯賽」。

Note

而不是 EVENT，您可以選擇在中 [the section called “創建一個 Amazon Kendra 索引”](#) 為 DocumentAttributeKey 值建立的任何索引欄位。

2. 要運行相同的搜索，但僅通過包含「歐洲冠軍聯賽」的結果進行過濾，請使用 [查詢](#) 命令：

Linux

```
aws kendra query \  
  --index-id kendra-index-id \  
  --query-text "Soccer matches" \  
  --attribute-filter '{"ContainsAny":{"Key":"EVENT","Value":  
{"StringListValue":["Champions League"]}}}' \  
  --region aws-region
```

其中：

- *kendra-index-id* 是你的保存 *kendra-index-id* ,
- *aws-region ### AWS ##*。

macOS

```
aws kendra query \  
  --index-id kendra-index-id \  
  --query-text "Soccer matches" \  
  --attribute-filter '{"ContainsAny":{"Key":"EVENT","Value":  
{"StringListValue":["Champions League"]}}}' \  
  --region aws-region
```

其中：

- *kendra-index-id* 是你的保存 *kendra-index-id* ,
- *aws-region ### AWS ##*。

Windows

```
aws kendra query ^
  --index-id kendra-index-id ^
  --query-text "Soccer matches" ^
  --attribute-filter '{"ContainsAny":{"Key":"EVENT","Value":
{"StringListValue":["Champions League"]}}}' ^
  --region aws-region
```

其中：

- *kendra-index-id* 是你的保存 *kendra-index-id* ,
- *aws-region ### AWS ##*。

AWS CLI 會顯示篩選的搜尋結果。

步驟 6：清理

清理您的文件

若要在完成本教學課程後停止在 AWS 帳戶中產生費用，您可以執行下列步驟：

1. 刪除您的 Amazon S3 存儲桶

如需刪除值區的詳細資訊，請參閱[刪除值區](#)。

2. 刪除您的 Amazon Kendra 索引

如需刪除 Amazon Kendra 索引的相關資訊，請參閱[刪除索引](#)。

3. 刪除 **converter.py**

- 對於主控台：請前往 [AWS CloudShell](#)，並確認區域已設定為您的 AWS 地區。在 bash 殼層載入之後，在環境中鍵入下列命令，然後按回車鍵。

```
rm converter.py
```

- For AWS CLI：在終端機視窗上執行下列命令。

Linux

```
rm file/converter.py
```

其中：

- *file/* 是本地設備converter.py上的文件路徑。

macOS

```
rm file/converter.py
```

其中：

- *file/* 是本地設備converter.py上的文件路徑。

Windows

```
rm file/converter.py
```

其中：

- *file/* 是本地設備converter.py上的文件路徑。

進一步了解

若要進一步了解如何將 Amazon Kendra 整合到您的工作流程中，您可以查看下列部落格文章：

- [用於增強搜尋的內容中繼資料](#)
- [利用自動化內容豐富建置智慧型搜尋解決方案](#)

要了解有關亞馬遜的更多信息，您可以查看 [Amazon Comprehend](#) 開發人員指南。

Amazon Kendra 的監控與記錄

主題

- [監視您的索引 \(控制台\)](#)
- [使用 記錄 Amazon Kendra API 呼叫AWS CloudTrail日誌](#)
- [記錄 Amazon Kendra 智慧排名 API 呼叫AWS CloudTrail日誌](#)
- [Amazon Kendra 監控與 Amazon Kendra CloudWatch](#)
- [Amazon Kendra 監控與 Amazon Kendra CloudWatch 日誌](#)

監視您的索引 (控制台)

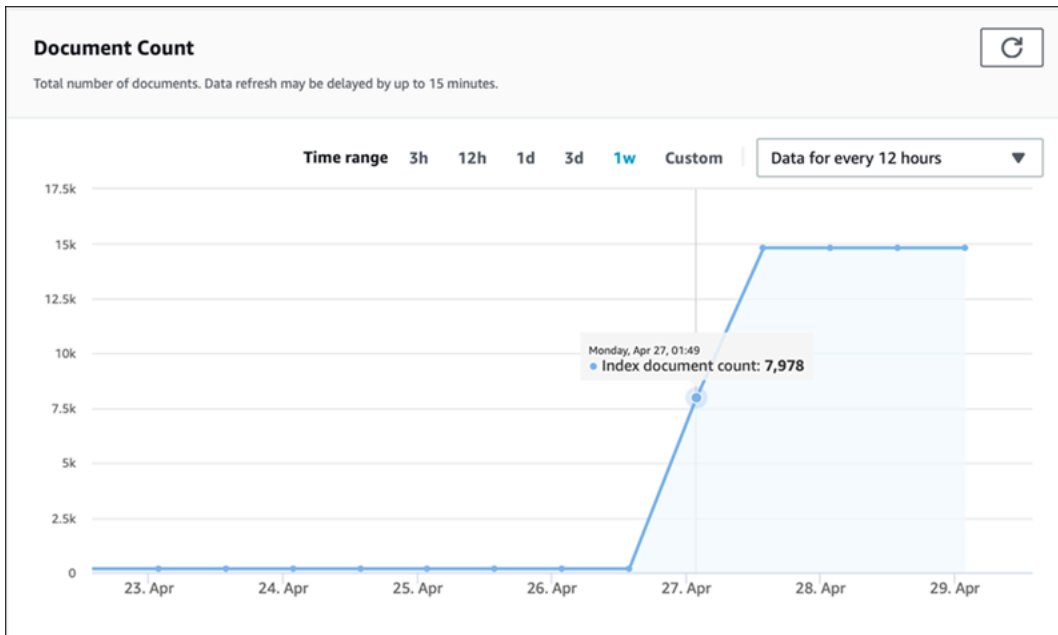
使用 Amazon Kendra 主控台監控索引和資料來源的狀態。您可以使用此資訊來追蹤索引的大小和儲存需求，以及監視索引和資料來源之間同步處理的進度和成功。

若要檢視索引測量結果 (主控台)

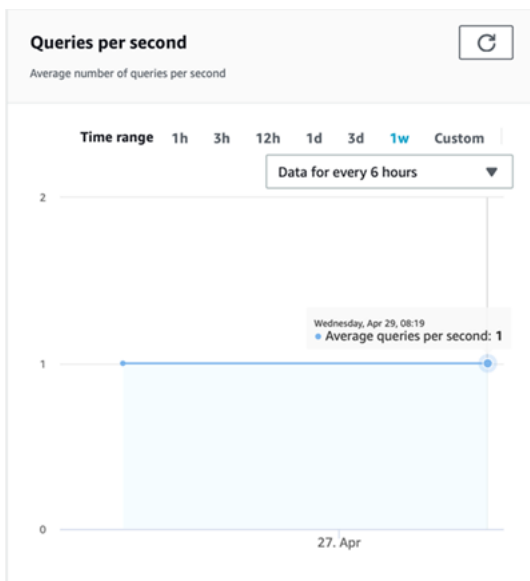
1. 登錄AWS Management Console並在以下位置打開亞馬遜肯德拉控制台 <https://console.aws.amazon.com/kendra/home>。
2. 從索引清單中，選擇要檢視的索引。
3. 捲動畫面以查看索引量度。

您可以看到有關索引的以下指標。

- 文件計數 — 編製索引的文件總數。這包括來自所有資料來源的所有文件。使用此指標來判斷您是否需要為索引購買更多或更少的儲存單位。



- **每秒查詢次數** — 每秒要求的索引查詢數目。使用此量度來判斷您是否需要為索引購買更多或更少的查詢單位。



若要監控索引和資料來源之間同步的進度和成功情況，請使用 Amazon Kendra 主控台。使用此資訊可協助判斷資料來源的健全狀況。

檢視同步化測量結果 (主控台)

1. 登錄AWS Management Console並在以下位置打開亞馬遜肯德拉控制台 <https://console.aws.amazon.com/kendra/home>。

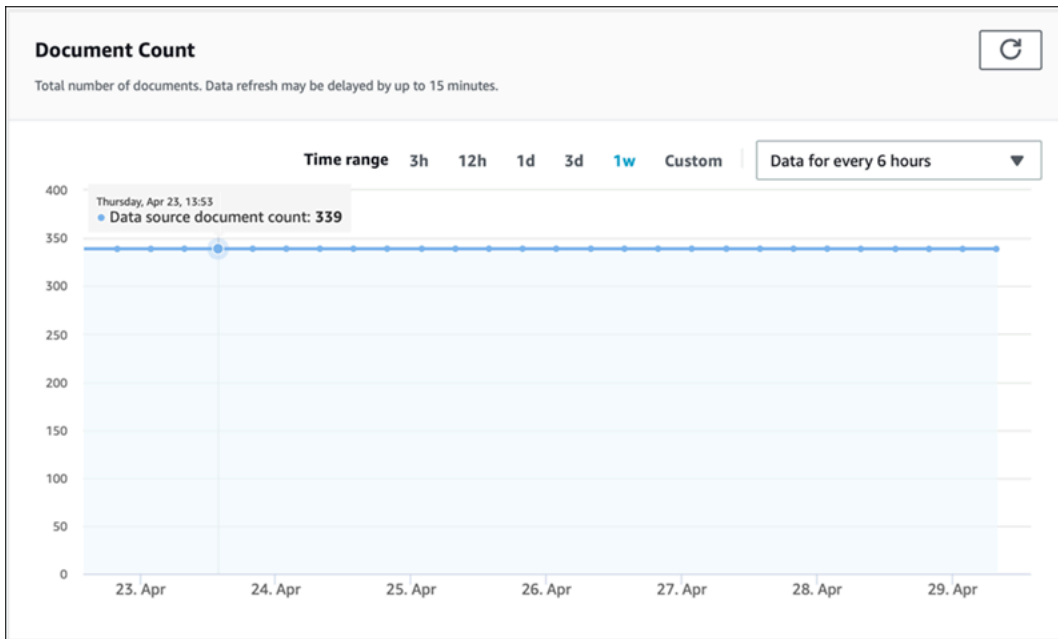
2. 從索引清單中，選擇要檢視其同步化測量結果的索引。
3. 從左側功能表中選擇 [資料來源]。
4. 從資料來源清單中，選擇要檢視的資料來源。
5. 捲動畫面以查看同步執行指標。

您可以看到以下信息。

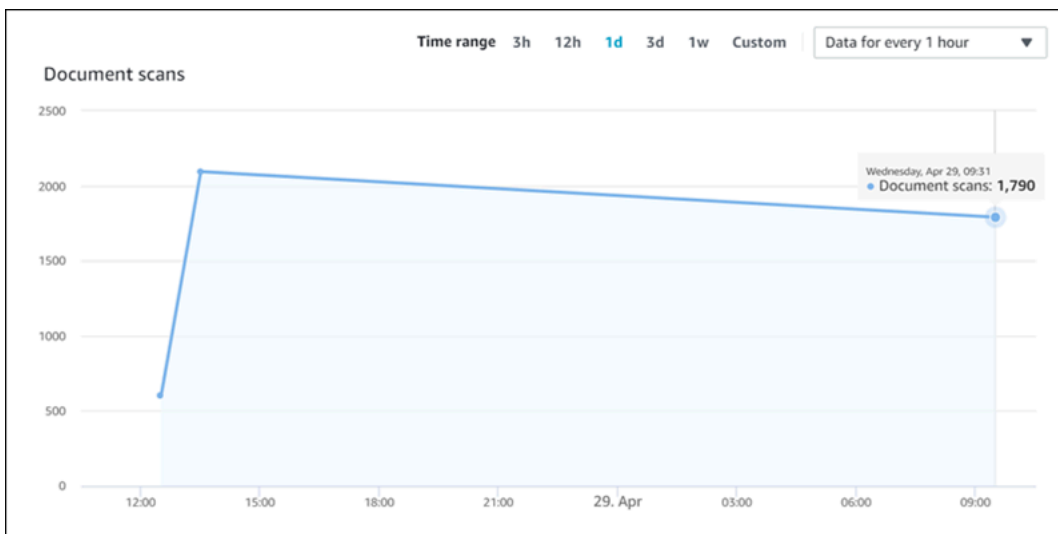
- 同步執行歷程記錄 — 有關同步執行的統計資料，包括開始和結束時間、新增、刪除和失敗的文件數目。如果同步執行失敗，則會有一個包含更多資訊的CloudWatch記錄檔連結。選擇左上角的設定圖示，以變更歷史記錄中顯示的欄。使用此資訊可判斷資料來源的一般健康狀況。

Sync run history (5)						
Status / Summary	Start time	End time	Added / Modified	Deleted	Failed	Details ↗
◀ Syncing - indexing	Apr 29, 2020, 9:53 AM PDT	Apr 29, 2020, 9:54 AM PDT	◀	◀	◀	View in CloudWatch
✔ Succeeded	Apr 28, 2020, 1:35 PM PDT	Apr 28, 2020, 1:37 PM PDT	1484	0	2	Service is operating normally ↗
✔ Succeeded	Apr 28, 2020, 1:32 PM PDT	Apr 28, 2020, 1:32 PM PDT	0	0	0	Service is operating normally ↗
✔ Succeeded	Apr 28, 2020, 1:05 PM PDT	Apr 28, 2020, 1:06 PM PDT	5	0	0	Service is operating normally ↗
✔ Succeeded	Apr 28, 2020, 1:05 PM PDT	Apr 28, 2020, 1:05 PM PDT	298	0	1	Service is operating normally ↗

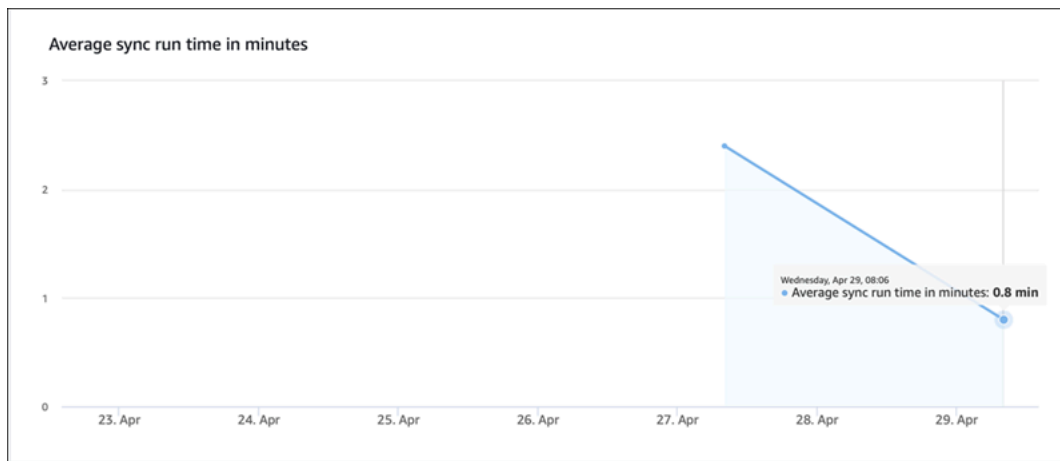
- 文件計數 — 從此資料來源編製索引的文件總數。這是新增至資料來源的所有文件總數，減去從資料來源刪除的所有文件總數。使用此資訊可判斷索引中包含此資料來源的文件數目。



- **文件掃描** — 同步執行期間掃描的文件總數。這包括資料來源中的所有文件，包括新增、更新、刪除或未變更的文件。使用此資訊判斷 Amazon Kendra 是否正在掃描資料來源中的所有文件。掃描的文件數量會影響服務的收費金額。



- **平均同步執行時間 (分鐘)** — 完成同步執行所需的平均時間長度。同步處理資料來源所需的時間會影響服務的費用。



使用記錄 Amazon Kendra API 呼叫AWS CloudTrail日誌

Amazon Kendra 集成AWS CloudTrail，提供使用者、角色或角色所採取之動作之記錄的服務AWS Amazon Kendra 的服務。CloudTrail 擷取 Amazon Kendra 的所有 API 呼叫作為事件，包括 Amazon Kendra 主控台的呼叫，以及 Amazon Kendra API 的呼叫。如果您建立追蹤，您可以啟動持續傳送 CloudTrail 到 Amazon S3 儲存貯體的事件，包括 Amazon Kendra 的活動。如果您未設定追蹤，您仍然可以在 CloudTrail 主控與事件歷史。使用所收集的資訊 CloudTrail，您可以決定向 Amazon Kendra 發出的請求、提出請求的 IP 地址、提出請求的人、提出請求的時間以及其他詳細資訊。

進一步了解 CloudTrail，包括如何配置和激活它，請參閱[AWS CloudTrail使用者金鑰](#)。

Amazon Kendra 的資訊 CloudTrail

CloudTrail 在您的激活AWS建立金鑰 Amazon Kendra 中發生活動時，此活動會記錄在 CloudTrail 與其他事件一起AWS service events in the CloudTrail 事件歷史。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 事件歷程記錄檢視事件](#)。

Amazon Kendra 的記錄AWS帳戶，包括 Amazon Kendra 的事件，創建一個跟踪。一個線索是允許的配置 CloudTrail 以日誌檔的形式傳送事件到指定的 S3 儲存貯體。根據預設，當您在主控台建立追蹤記錄時，追蹤記錄會套用到所有 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 S3 儲存貯體。此外，您可以設定AWS進一步分析和處理收集到的事件數據的服務 CloudTrail 日誌。如需詳細資訊，請參閱：

- [建立追蹤的概觀](#)
- [CloudTrail 支援的服務和整合](#)
- [設定的 Amazon SNS 通知 CloudTrail](#)

- [接收 CloudTrail 來自多個區域的記錄](#)和[接收 CloudTrail 來自多個記錄](#)

CloudTrail 記錄所有 Amazon Kendra 動作，這些動作記錄在[API Kendra](#)。例如，呼叫 `CreateIndex`, `CreateDataSource`，以及 `Query` 作業會產生項目 CloudTrail 記錄

每一筆事件或日誌項目都會包含產生請求者的資訊。如需詳細資訊，請參閱 [CloudTrail 使用者身分元素](#)。

Amazon Kendra 的記錄

一個線索是允許將事件作為日誌檔傳送到指定 S3 儲存貯體的組態。CloudTrail 記錄檔包含一或多個記錄項目。一個事件代表來自任何來源的單一要求，並包含有關請求的動作、動作的日期和時間、請求參數等的資訊。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的順序顯示。

呼叫到 `Query` 作業的記錄

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "AssumedRole | FederatedUser | IAMUser | Root | SAMLUser | WebIdentityUser",
    "principalId": "principal ID",
    "arn": "ARN",
    "accountId": "account ID",
    "accessKeyId": "access key ID",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "principal Id",
        "arn": "ARN",
        "accountId": "account ID",
        "userName": "user name"
      },
      "webIdFederationData": {

    },
    "attributes": {
      "mfaAuthenticated": false,
      "creationDate": "timestamp"
    }
  }
}
```

```
    },
    "eventTime": "timestamp",
    "eventSource": "kendra.amazonaws.com",
    "eventName": "Query",
    "awsRegion": "region",
    "sourceIPAddress": "source IP address",
    "userAgent": "user agent",
    "requestParameters": {
      "indexId": "index ID"
    },
    "responseElements": null,
    "requestID": "request ID",
    "eventID": "event ID",
    "eventType": "AwsApiCall",
    "recipientAccountId": "account ID"
  },
```

記錄 Amazon Kendra 智慧排名 API 呼叫AWS CloudTrail日誌

Amazon Kendra 智慧排名與AWS CloudTrail，提供使用者、角色或角色所採取之動作之記錄的服務AWS Amazon Kendra 智慧排名中的服務。CloudTrail 擷取 Amazon Kendra 智慧排名的所有 API 呼叫作為事件，包括 Amazon Kendra Api 的程式碼呼叫。如果您建立追蹤，您可以啟動持續傳送 CloudTrail 到 Amazon S3 儲存貯體的事件，包括 Amazon Kendra 智慧排名的活動。如果您未設定追蹤，您仍然可以在 CloudTrail 主控與事件歷史。使用所收集的資訊 CloudTrail，您可以判斷 Amazon Kendra 智慧排名的請求、提出請求的 IP 位址、提出請求的人、提出要求的時間和其他詳細資訊。

進一步了解 CloudTrail，包括如何配置和激活它，請參閱[AWS CloudTrail使用者金鑰](#)。

Amazon Kendra 智慧排名資訊 CloudTrail

CloudTrail 在您的激活AWS建立金鑰 Amazon Kendra 智慧排名中發生活動時，此活動會記錄在 CloudTrail與其他事件一起AWS service events in the CloudTrail 事件歷史。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[檢控與 CloudTrail 事件歷史](#)。

Amazon Kendra 的記錄AWS帳戶，包括 Amazon Kendra 智能排名的事件，可以創建一個跟踪。一個線索是允許的配置 CloudTrail 以日誌檔的形式傳送事件到指定的 S3 儲存貯體。根據預設，當您在主控台建立追蹤記錄時，追蹤記錄會套用到所有 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 S3 儲存貯體。此外，您可以設定AWS進一步分析和處理收集到的事件數據的服務 CloudTrail 日誌。如需詳細資訊，請參閱：

- [建立追蹤的概觀](#)

- [CloudTrail 支援的服務和整合](#)
- [設定的 Amazon SNS 通知 CloudTrail](#)
- [接收 CloudTrail 來自多個區域的記錄](#)和[接收 CloudTrail 來自多個記錄](#)

CloudTrail 記錄所有 Amazon Kendra 智慧排名動作，這些動作記錄在[API Kendra](#)。例如，呼叫 `CreateRescoreExecutionPlan` 產生項目 CloudTrail 記錄

每一筆事件或日誌項目都會包含產生請求者的資訊。如需詳細資訊，請參閱 [CloudTrail 使用者身分元素](#)。

範例：Amazon Kendra 智慧排名記錄檔項目

一個線索是允許將事件作為日誌檔傳送到指定 S3 儲存貯體的組態。CloudTrail 記錄檔包含一或多個記錄項目。一個事件代表來自任何來源的單一要求，並包含有關請求的動作、動作的日期和時間、請求參數等的資訊。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的順序顯示。

呼叫到 `CreateRescoreExecutionPlan` 作業的記錄

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "principal ID",
    "arn": "ARN",
    "accountId": "account ID",
    "accessKeyId": "access key ID",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "principal ID",
        "arn": "ARN",
        "accountId": "account ID",
        "userName": "user name"
      },
      "webIdFederationData": {},
      "attributes": {
        "creationDate": "yyyy-mm-ddThh:mm:ssZ",
        "mfaAuthenticated": "false"
      }
    }
  }
}
```

```
    },
    "eventTime": "yyyy-mm-ddThh:mm:ssZ",
    "eventSource": "kendra-ranking.amazonaws.com",
    "eventName": "CreateRescoreExecutionPlan",
    "awsRegion": "region",
    "sourceIPAddress": "source IP address",
    "userAgent": "user agent",
    "requestParameters": {
      "name": "name",
      "description": "description",
      "clientToken": "client token"
    },
    "responseElements": {
      "id": "rescore execution plan ID",
      "arn": "rescore execution plan ARN"
    },
    "requestID": "request ID",
    "eventID": "event ID",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "account ID",
    "eventCategory": "Management",
    "tlsDetails": {
      "tlsVersion": "TLS version",
      "cipherSuite": "cipher suite",
      "clientProvidedHostHeader": "kendra-ranking.[region].api.aws"
    }
  }
}
```

Amazon Kendra 監控與 Amazon Kendra CloudWatch

要跟踪索引的運行狀態，請使用亞馬遜 CloudWatch。同 CloudWatch，您可以取得索引文件同步處理的指標。您也可以設定 CloudWatch 警示會在一或多個測量結果超過您定義的臨界值時收到通知。例如，您可以監視提交要編製索引的文件數目，或無法編製索引的文件數目。

您必須擁有相應的 CloudWatch 監控 Amazon Kendra 的許可 CloudWatch。如需詳細資訊，請參閱[Amazon 的身份驗證和訪問控制 CloudWatch](#)在亞馬遜 CloudWatch 使用者金鑰。

Amazon Kendra 的檢控

Amazon Kendra 的 Amazon Kendra CloudWatch 控制台

若要檢控與記錄CloudWatch 控制台

1. 登入AWS Management Console與記錄 CloudWatch 主控與<https://console.aws.amazon.com/cloudwatch/>。
2. 選擇度量，選擇所有量度然後選擇Kendra。
3. 選擇維度、選擇指標名稱，再選擇 Add to graph (新增至圖形)。
4. 選擇日期範圍的值。所選日期範圍的指標計數會顯示在圖形中。

建立警示

一個 CloudWatch alarm 會監視指定時段內的單一指標，並執行一或多個動作:傳送通知到 Amazon SAuto Scaling 政策。此動作或動作是根據您指定的期間內，相對於指定臨界值的測量結果值。CloudWatch 此外，還可以在警報狀態變更時傳送 Amazon SNS 訊息。

CloudWatch 警報只有在狀態變更且您指定的期間內持續存在時，才會呼叫動作。

設定警示

1. 登入AWS Management Console與記錄 CloudWatch 主控與<https://console.aws.amazon.com/cloudwatch/>。
2. 選擇警報然後選擇建立警示。
3. 選取量度。選擇Kendra索引和資料來源的量度。還可以將時間設置為設置的小時，天數，週數或自定義數。
4. 選擇您的統計資料。例如：平均。還可以將鬧鐘觸發時間段選擇為設定的分鐘數、小時數、每天或自訂。
5. 選擇您的閾值以觸發警報，無論是使用靜態值還是頻段，以及符合閾值的條件。
6. 選擇觸發器的警示狀態，指標是否必須超出您設定的閾值，還是其他狀態。選取要傳送警示通知給誰/哪個電子郵件。
7. 如果您對警報感到滿意，請選擇建立警示。

Note

您必須提供您的名稱 CloudWatch 警控與記錄

CloudWatch 索引同步工作的測量結果

下表說明 Amazon Kendra 指標，適用於資料來源同步任務。

如果您使用 API 或 CLI，您必須指定 Namespace 作為 'AWS / 肯德拉' 除了 MetricName 您在使用時的選擇 [GetMetricStatistics](#) API。

指標	描述
DocumentsCrawled	<p>執行期間掃描或探索的同步化工作的文件數目。</p> <p>維度：</p> <ul style="list-style-type: none"> • IndexId • DataSourceId <p>單位：計數</p>
DocumentsSubmittedForIndexing	<p>同步化工作提交至索引的文件數目。</p> <p>維度：</p> <ul style="list-style-type: none"> • IndexId • DataSourceId <p>單位：計數</p>
DocumentsSubmittedForIndexingFailed	<p>編製索引失敗的文件數目。檢控與記錄 CloudWatch 記錄同步化工作以取得詳細資訊。</p> <p>維度：</p> <ul style="list-style-type: none"> • IndexId • DataSourceId <p>單位：計數</p>
DocumentsSubmittedForDeletion	<p>同步處理工作要求從索引中移除的文件數目。</p>

指標	描述
	維度： <ul style="list-style-type: none"> • IndexId • DataSourceId 單位：計數
DocumentsSubmittedForDeletionFailed	無法刪除的文件數目。檢控與記錄 CloudWatch 記錄同步化工作以取得詳細資訊。 維度： <ul style="list-style-type: none"> • IndexId • DataSourceId 單位：計數

Amazon Kendra 的指標

下表說明 Amazon Kendra 指標，適用於資料來源同步任務。標有星號 (*) 的指標僅用於 Amazon S3 資料來源。

如果您使用 API 或 CLI，您必須指定 Namespace 作為 'AWS /肯德拉' 除了 MetricName 您在使用時的選擇 [GetMetricStatistics](#) API。

指標	描述
DocumentsSkippedNoChange *	已檢查且發現沒有變更的文件數量，因此不會提交以進行索引。 維度： <ul style="list-style-type: none"> • IndexId • DataSourceId

指標	描述
	單位：計數
DocumentsSkippedInvalidMetadata*	<p>因為關聯的中繼資料檔案發生問題，所以略過的文件數目。檢控與記錄 CloudWatch 記錄同步運行以獲取詳細信息。</p> <p>維度：</p> <ul style="list-style-type: none">• IndexId• DataSourceId <p>單位：計數</p>
DocumentsCrawled	<p>檢查的文件檔案數目。</p> <p>維度：</p> <ul style="list-style-type: none">• IndexId• DataSourceId <p>單位：計數</p>
DocumentsSubmittedForDeletion	<p>已從資料來源刪除並提交刪除的已檢查文件數目。</p> <p>維度：</p> <ul style="list-style-type: none">• IndexId• DataSourceId <p>單位：計數</p>

指標	描述
DocumentsSubmittedForDeletionFailed	<p>從資料來源刪除失敗的文件數目。</p> <p>維度：</p> <ul style="list-style-type: none"> • IndexId • DataSourceId <p>單位：計數</p>
DocumentsSubmittedForIndexing	<p>檢查並提交以供索引使用的文件數目。</p> <p>維度：</p> <ul style="list-style-type: none"> • IndexId • DataSourceId <p>單位：計數</p>
DocumentsSubmittedForIndexingFailed	<p>無法編製索引的提交進行理想的文件數目。</p> <p>維度：</p> <ul style="list-style-type: none"> • IndexId • DataSourceId <p>單位：計數</p>

索引文件的量度

下表說明索引文件的 Amazon Kendra 指標。對於使用編製索引的文件 [BatchPutDocument](#) 操作，只有 IndexId 支援維度。

如果您使用 API 或 CLI，您必須指定 Namespace 作為 'AWS / 肯德拉' 除了 MetricName 您在使用時的選擇 [GetMetricStatistics](#) API。

指標	描述
DocumentsIndexed	<p>已編製索引的文件數目。</p> <p>維度：</p> <ul style="list-style-type: none"> • IndexId • DataSourceId <p>單位：計數</p>
DocumentsFailedToIndex	<p>無法編製索引的文件數目。檢控與記錄 CloudWatch 記錄</p> <p>維度：</p> <ul style="list-style-type: none"> • IndexId • DataSourceId <p>單位：計數</p>
IndexQueryCount	<p>每分鐘的索引查詢數目。</p> <p>維度：</p> <ul style="list-style-type: none"> • IndexId <p>單位：計數</p>

Amazon Kendra 監控與 Amazon Kendra CloudWatch 日誌

Amazon Kendra CloudWatch 記錄可讓您深入瞭解資料來源的運作。Amazon Kendra 會在文件編製索引時，處理文件的詳細資訊。它會記錄在文件編製索引時發生的資料來源錯誤。您使用 CloudWatch 日誌來監視，存儲和訪問日誌文件。

CloudWatch 記錄檔會將記錄事件儲存在屬於記錄群組一部分的記錄資料流中。Amazon Kendra 使用這些功能如下：

- 日誌群組 — Amazon Kendra 會將所有日誌串流存放在每個索引的單一日誌群組中。Amazon Kendra 會在建立索引時建立日誌群組。記錄群組識別碼一律以「aws/kendra/」開頭。
- 日誌串流 — Amazon Kendra 會為您執行的每個索引同步任務，在日誌群組中建立新的資料來源日誌串流。當串流達到大約 500 個項目時，它也會建立新的文件記錄資料流。
- 日誌項目 — Amazon Kendra 會在編製文件索引時，在日誌串流中建立日誌項目。每個項目都提供有關處理文件或遇到的任何錯誤的資訊。

Amazon Kendra 的詳細資訊 CloudWatch 記錄檔，請參閱[什麼是亞馬遜雲觀察日誌](#)在亞馬遜雲觀察日誌使用者指南。

Amazon Kendra 會建立兩種類型的日誌串流：

- [資料來源日誌串流](#)
- [記錄](#)

資料來源日誌串流

資料來源記錄會串流有關索引同步化工作的發佈項目。每個同步處理工作都會建立一個用來發佈項目的新記錄資料流。記錄

```
data source id/YYYY-MM-DD-HH/data source sync job ID
```

系統會為每個同步化工作執行建立新的記錄資料流。

發佈至資料來源記錄串流的記錄訊息有三種類型：

- 無法傳送以進行索引的文件的記錄訊息。以下是 S3 資料來源中文件的此訊息範例：

```
{
  "DocumentId": "document ID",
  "S3Path": "s3://bucket/prefix/object",
  "Message": "Failed to ingest document via BatchPutDocument.",
  "ErrorCode": "InvalidRequest",
  "ErrorMessage": "No document metadata configuration found for document attribute
key city."
}
```

- 無法傳送刪除之文件的記錄訊息。以下是此訊息的範例：

```
{
  "DocumentId": "document ID",
  "Message": "Failed to delete document via BatchDeleteDocument.",
  "ErrorCode": "InvalidRequest",
  "ErrorMessage": "Document can't be deleted because it doesn't exist."
}
```

- 在 Amazon S3 儲存貯體中找到文件的無效中繼資料檔案時顯示日誌訊息。以下是此訊息的範例。

```
{
  "Message": "Found invalid metadata
file bucket/prefix/filename.extension.metadata.json."
}
```

- 對於 SharePoint 和資料庫連接器，Amazon Kendra 只會在文件無法編製索引時，才會將訊息寫入日誌串流。以下是 Amazon Kendra 記錄的錯誤訊息範例。

```
{
  "DocumentID": "document ID",
  "IndexID": "index ID",
  "SourceURI": "",
  "CrawlStatus": "FAILED",
  "ErrorCode": "403",
  "ErrorMessage": "Access Denied",
  "DataSourceErrorCode": "403"
}
```

記錄

Amazon Kendra 會在文件編製索引時記錄有關處理文件的資訊。此功能會針對 Amazon S3 資料來源中存放的文件記錄一組訊息。它僅記錄存儲在 Microsoft 中的文檔錯誤 SharePoint 或資料金鑰

如果使用將文件新增至索引 [BatchPutDocument](#) 操作時，日誌流命名如下：

```
YYYY-MM-DD-HH/UUID
```

如果使用數據源將文檔添加到索引中，則日誌流的命名如下：

```
dataSourceId/YYYY-MM-DD-HH/UUID
```

每個記錄串流最多可包含 500 則訊息。

如果索引文檔失敗，此消息將輸出到日誌流：

```
{
  "DocumentId": "document ID",
  "IndexName": "index name",
  "IndexId": "index ID"
  "SourceURI": "source URI"
  "IndexingStatus": "DocumentFailedToIndex",
  "ErrorCode": "400 | 500",
  "ErrorMessage": "message"
}
```

Amazon Kendra 中的安全性

雲安全 AWS 是最高的優先級。身為 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 AWS 與您之間共同承擔的責任。[共同責任模型](#)將其描述為雲端的安全性和雲端中的安全性：

- 雲端的安全性 — AWS 負責保護在 AWS 雲端中執行 AWS 服務的基礎架構。AWS 還為您提供可以安全使用的服務。若要了解適用於 Amazon Kendra 的合規計劃，請參閱合規計劃[AWS 服務範圍內的合規計劃](#) AWS 服務。
- 雲端中的安全性 — 您的責任取決於您使用的 AWS 服務。您也必須對其他因素負責，包括資料的機密性、您的公司的要求和適用法律和法規。

本文件可協助您了解如何在使用 Amazon Kendra 時套用共同的責任模型。下列主題說明如何設定 Amazon Kendra 以符合安全性和合規目標。您也會學到如何使用其他可 AWS 協助您監控和保護 Amazon Kendra 資源的服務。

主題

- [Amazon Kendra 的資料保護](#)
- [Amazon Kendra Amazon Kendra 智能排名和接口 VPC 端點 \(\) AWS PrivateLink](#)
- [Amazon Kendra 的身分和存取管理](#)
- [安全最佳實務](#)
- [在 Amazon Kendra 中進行記錄和監控](#)
- [Amazon Kendra 的合規驗證](#)
- [Amazon Kendra 的韌性](#)
- [Amazon Kendra 的基礎設施安全](#)
- [中的配置和漏洞分析 AWS Identity and Access Management](#)

Amazon Kendra 的資料保護

AWS [共同責任模型](#)適用於 Amazon Kendra 中的資料保護。如此模型中所述，AWS 負責保護執行所有 AWS 雲端。您負責維護在此基礎設施上託管內容的控制權。您也同時負責所使用 AWS 服務的安全組態和管理任務。如需資料隱私權的詳細資訊，請參閱[資料隱私權常見問答集](#)。如需有關歐洲資料保護的相關資訊，請參閱 AWS 安全性部落格上的 [AWS 共同的責任模型和 GDPR](#) 部落格文章。

基於資料保護目的，我們建議您使用 AWS IAM Identity Center 或 AWS Identity and Access Management (IAM) 保護 AWS 帳戶 登入資料並設定個別使用者。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：

- 每個帳戶均要使用多重要素驗證 (MFA)。
- 使用 SSL/TLS 與 AWS 資源進行通訊。我們需要 TLS 1.2 並建議使用 TLS 1.3。
- 使用設定 API 和使用者活動記錄 AWS CloudTrail。
- 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。
- 如果您在透過命令列介面或 API 存取時需要經 AWS 過 FIPS 140-2 驗證的加密模組，請使用 FIPS 端點。如需有關 FIPS 和 FIPS 端點的更多相關資訊，請參閱[聯邦資訊處理標準 \(FIPS\) 140-2 概觀](#)。

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 AWS 服務 使用主控台、API 或 AWS 開發套件與 Amazon Kendra 或其他人合作時。AWS CLI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。如果您提供外部伺服器的 URL，我們強烈建議請勿在驗證您對該伺服器請求的 URL 中包含憑證資訊。

靜態加密

Amazon Kendra 會使用您選擇的加密金鑰來加密靜態資料。您可以選擇下列其中之一：

- AWS擁有的 AWS KMS 金鑰。如果您未指定加密金鑰，預設情況下，您的資料會使用此金鑰加密。
- 您帳戶中的 AWS受管 KMS 金鑰。此金鑰是由 Amazon Kendra 代表您建立、管理和使用的。金鑰名稱為aws/kendra。
- 客戶管理的金鑰。您可以提供您在帳戶中建立的加密金鑰的 ARN。當您使用客戶管理的 KMS 金鑰時，您必須提供金鑰一個金鑰政策，以允許 Amazon Kendra 使用金鑰。選取對稱加密客戶管理的 KMS 金鑰，Amazon Kendra 不支援非對稱 KMS 金鑰。如需詳細資訊，請參閱[金鑰管理](#)。

傳輸中加密

Amazon Kendra 使用 HTTPS 通訊協定與您的用戶端應用程式進行通訊。它使用 HTTPS 和 AWS 簽名代表您的應用程序與其他服務進行通信。如果您使用虛擬私人雲端，您可以使 AWS PrivateLink 用在 VPC 和 Amazon Kendra 之間建立私人連線。

金鑰管理

Amazon Kendra 會使用三種金鑰類型的其中一種來加密索引的內容。您可以選擇下列其中之一：

- AWS擁有的 AWS KMS。此為預設值。
- AWS受管理的 KMS 金鑰。此金鑰是在您的帳戶中建立的，並由 Amazon Kendra 代表您管理和使用。
- 客戶管理的 KMS 金鑰。您可以在建立 Amazon Kendra 索引或資料來源時建立金鑰，也可以使用 AWS KMS 主控台建立金鑰。選取客戶管理的 KMS 金鑰對稱加密。Amazon Kendra 不支援非對稱 KMS 金鑰。如需詳細資訊，請參閱《AWS Key Management Service 開發人員指南》中的[使用對稱和非對稱金鑰](#)。

Amazon Kendra Amazon Kendra 智能排名和接口 VPC 端點

() AWS PrivateLink

您可以透過建立介面 VPC 端點，在虛擬私人雲端和 Amazon Kendra 之間建立私有連線。介面端點採用這種技術 [AWS PrivateLink](#)，可讓您在沒有網際網路閘道、NAT 裝置、VPN 連線或 AWS 直 Connect 連線的情況下私有存取 Amazon Kendra API。VPC 中的執行個體不需要公有 IP 地址即可與 Amazon Kendra API 進行通訊。您的 VPC 和 Amazon Kendra 之間的流量不會離開 Amazon 網絡。

每個介面端點都是由您子網路中的一或多個[彈性網路介面](#)表示。

亞馬遜肯德拉和亞馬遜肯德拉智慧排名 VPC 端點的注意事項

在為 Amazon Kendra 或 Amazon Kendra 智慧型排名設定介面 VPC 端點之前，請務必檢閱 Amazon VPC 使用者指南中的[先決條件](#)。

Amazon Kendra 和 Amazon Kendra 智慧排名支援從您的 VPC 呼叫其所有 API 動作。

為亞馬遜肯德拉和 Amazon Kendra 智能排名創建接口 VPC 端點

您可以使用 Amazon Kendra VPC 主控台或 () 為 Amazon 肯德拉或亞馬遜肯德拉智慧排名服務建立 VPC 端點。AWS Command Line Interface AWS CLI

使用下列服務名稱為 Amazon Kendra 建立 VPC 端點：

- `com.amazonaws.region.kendra`

使用下列服務名稱為 Amazon Kendra 智慧型排名建立 VPC 端點：

- `aws.api.region.kendra-ranking`

建立 VPC 端點後，您可以使用下列範例 AWS CLI 命令，該命令使用該 `endpoint-url` 參數將介面端點指定給 Amazon Kendra API：

```
aws kendra list-indices --endpoint-url https://VPC endpoint
```

`VPC ##` 是建立介面端點時產生的 DNS 名稱。此名稱包括 VPC 端點識別碼，以及 Amazon Kendra 服務名稱，其中包括該區域。例如 `vpce-1234-abcdef.kendra.us-west-2.vpce.amazonaws.com`。

如果您為端點啟用私有 DNS，則可以使用該區域的預設 DNS 名稱向 Amazon Kendra 發出 API 請求。例如 `kendra.us-east-1.amazonaws.com`。

如需詳細資訊，請參閱《Amazon VPC 使用者指南》中的 [建立介面端點](#)。

為亞馬遜肯德拉和 Amazon Kendra 智慧排名建立 VPC 端點政策

您可以將端點政策附加到 VPC 端點，以控制對 Amazon Kendra 或亞馬 Amazon Kendra 智慧排名的存取。

亞馬遜肯德拉或亞馬遜肯德拉智慧排名政策指定了以下資訊：

- 可以執行動作的主要/授權使用者。
- 可執行的動作。
- 可供執行動作的資源。

範例：適用於 Amazon Kendra 動作的 VPC 端點政策

以下是適用於 Amazon Kendra 的端點政策範例。連接到端點時，此政策會授予所有資源上所有主理/授權使用者所有可用 Amazon Kendra 動作的存取權。

```
{
  "Statement": [
    {
      "Principal": "*",
      "Effect": "Allow",
```

```
    "Action":[
      "kendra:*"
    ],
    "Resource": "*"
  }
]
```

範例：適用於 Amazon Kendra 智慧排名動作的 VPC 端點政策

以下是 Amazon Kendra 智慧排名的端點政策範例。連接到端點時，此政策會授予所有資源上所有主管/授權使用者的所有可用 Amazon Kendra 智慧排名動作的存取權。

```
{
  "Statement": [
    {
      "Principal": "*",
      "Effect": "Allow",
      "Action": [
        "kendra-ranking:*"
      ],
      "Resource": "*"
    }
  ]
}
```

如需詳細資訊，請參閱 Amazon VPC 使用者指南中的使用端點政策控制對 VPC [端點的存取](#)。

Amazon Kendra 的身分和存取管理

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通過身份驗證 (登入) 和授權 (具有許可) 來使用 Amazon Kendra 資源。IAM 是您可以使用的 AWS 服務，無需額外付費。

主題

- [物件](#)
- [使用身分驗證](#)
- [使用政策管理存取權](#)
- [亞馬遜肯德拉如何與 IAM 合作](#)

- [Amazon Kendra 身份識別政策範例](#)
- [AWS Amazon Kendra 的受管政策](#)
- [疑難排解 Amazon Kendra 身分和存取](#)

物件

您使用 AWS Identity and Access Management (IAM) 的方式會有所不同，具體取決於您在 Amazon Kendra 中所做的工作。

服務使用者 — 如果您使用 Amazon Kendra 服務執行工作，則管理員會為您提供所需的登入資料和許可。當您使用更多 Amazon Kendra 功能完成工作時，您可能需要額外的許可。了解存取許可的管理方式可協助您向管理員請求正確的許可。如果您無法在 Amazon Kendra 中存取某項功能，請參閱[疑難排解 Amazon Kendra 身分和存取](#)。

服務管理員 — 如果您負責公司的 Amazon Kendra 資源，您可能擁有 Amazon Kendra 的完整存取權。您的任務是判斷服務使用者應存取哪些 Amazon Kendra 功能和資源。接著，您必須將請求提交給您的 IAM 管理員，來變更您服務使用者的許可。檢閱此頁面上的資訊，了解 IAM 的基本概念。若要進一步了解貴公司如何將 IAM 與 Amazon Kendra 搭配使用，請參閱[亞馬遜肯德拉如何與 IAM 合作](#)。

IAM 管理員 — 如果您是 IAM 管理員，您可能想要了解如何撰寫政策以管理 Amazon Kendra 存取權的詳細資訊。若要檢視您可以在 IAM 中使用的 Amazon Kendra 身分型政策範例，請參閱[Amazon Kendra 身份識別政策範例](#)

使用身分驗證

驗證是您 AWS 使用身分認證登入的方式。您必須以 IAM 使用者身分或假設 IAM 角色進行驗證 (登入 AWS)。AWS 帳戶根使用者

您可以使用透過 AWS 身分識別來源提供的認證，以聯合身分識別身分登入。AWS IAM Identity Center (IAM 身分中心) 使用者、貴公司的單一登入身分驗證，以及您的 Google 或 Facebook 登入資料都是聯合身分識別的範例。您以聯合身分登入時，您的管理員先前已設定使用 IAM 角色的聯合身分。當您使 AWS 用同盟存取時，您會間接擔任角色。

根據您的使用者類型，您可以登入 AWS Management Console 或 AWS 存取入口網站。如需有關登入的詳細資訊 AWS，請參閱《AWS 登入 使用指南》AWS 帳戶中的[如何登入](#)您的。

如果您 AWS 以程式設計方式存取，請 AWS 提供軟體開發套件 (SDK) 和命令列介面 (CLI)，以使用您的認證以加密方式簽署要求。如果您不使用 AWS 工具，則必須自行簽署要求。如需使用建議的方法自行簽署請求的詳細資訊，請參閱 IAM 使用者指南中的[簽署 AWS API 請求](#)。

無論您使用何種身分驗證方法，您可能都需要提供額外的安全性資訊。例如，AWS 建議您使用多重要素驗證 (MFA) 來增加帳戶的安全性。如需更多資訊，請參閱 AWS IAM Identity Center 使用者指南中的 [多重要素驗證](#) 和 IAM 使用者指南中的 [在 AWS 中使用多重要素驗證 \(MFA\)](#)。

AWS 帳戶 根使用者

當您建立時 AWS 帳戶，您會從一個登入身分開始，該身分可完整存取該帳戶中的所有資源 AWS 服務和資源。此身分稱為 AWS 帳戶 root 使用者，可透過使用您用來建立帳戶的電子郵件地址和密碼登入來存取。強烈建議您不要以根使用者處理日常任務。保護您的根使用者憑證，並將其用來執行只能由根使用者執行的任務。如需這些任務的完整清單，了解需以根使用者登入的任務，請參閱《IAM 使用者指南》中的 [需要根使用者憑證的任務](#)。

IAM 使用者和群組

[IAM 使用者](#) 是您內部的身分，具 AWS 帳戶 有單一人員或應用程式的特定許可。建議您盡可能依賴暫時憑證，而不是擁有建立長期憑證 (例如密碼和存取金鑰) 的 IAM 使用者。但是如果特定使用案例需要擁有長期憑證的 IAM 使用者，建議您輪換存取金鑰。如需更多資訊，請參閱 [IAM 使用者指南](#) 中的為需要長期憑證的使用案例定期輪換存取金鑰。

[IAM 群組](#) 是一種指定 IAM 使用者集合的身分。您無法以群組身分簽署。您可以使用群組來一次為多名使用者指定許可。群組可讓管理大量使用者許可的程序變得更為容易。例如，您可以擁有一個名為 IAMAdmins 的群組，並給予該群組管理 IAM 資源的許可。

使用者與角色不同。使用者只會與單一人員或應用程式建立關聯，但角色的目的是在由任何需要它的人員取得。使用者擁有永久的長期憑證，但角色僅提供暫時憑證。如需進一步了解，請參閱 IAM 使用者指南中的 [建立 IAM 使用者 \(而非角色\) 的時機](#)。

IAM 角色

[IAM 角色](#) 是您 AWS 帳戶 內部具有特定許可的身分。它類似 IAM 使用者，但不與特定的人員相關聯。您可以 [切換角色，在中暫時擔任 IAM 角色](#)。AWS Management Console 您可以透過呼叫 AWS CLI 或 AWS API 作業或使用自訂 URL 來擔任角色。如需使用角色的方法詳細資訊，請參閱 IAM 使用者指南中的 [使用 IAM 角色](#)。

使用暫時憑證的 IAM 角色在下列情況中非常有用：

- 聯合身分使用者存取 — 如需向聯合身分指派許可，請建立角色，並為角色定義許可。當聯合身分進行身分驗證時，該身分會與角色建立關聯，並獲授予由角色定義的許可。如需有關聯合角色的相關資訊，請參閱 [IAM 使用者指南](#) 中的為第三方身分提供者建立角色。如果您使用 IAM Identity Center，則需要設定許可集。為控制身分驗證後可以存取的內容，IAM Identity Center 將許可集與 IAM 中的角色相關聯。如需有關許可集的資訊，請參閱 AWS IAM Identity Center 使用者指南中的 [許可集](#)。

- 暫時 IAM 使用者許可 – IAM 使用者或角色可以擔任 IAM 角色來暫時針對特定任務採用不同的許可。
- 跨帳戶存取權：您可以使用 IAM 角色，允許不同帳戶中的某人 (信任的主體) 存取您帳戶的資源。角色是授予跨帳戶存取權的主要方式。但是，對於某些策略 AWS 服務，您可以將策略直接附加到資源 (而不是使用角色作為代理)。若要了解跨帳戶存取角色和以資源為基礎的政策之間的差異，請參閱 IAM 使用者指南中的 [IAM 中的跨帳戶資源存取](#)。
- 跨服務訪問 — 有些 AWS 服務使用其他 AWS 服務功能。例如，當您在服務中進行呼叫時，該服務通常會在 Amazon EC2 中執行應用程式或將物件儲存在 Amazon Simple Storage Service (Amazon S3) 中。服務可能會使用呼叫主體的許可、使用服務角色或使用服務連結角色來執行此作業。
- 轉寄存取工作階段 (FAS) — 當您使用 IAM 使用者或角色在中執行動作時 AWS，您會被視為主體。使用某些服務時，您可能會執行某個動作，進而在不同服務中啟動另一個動作。FAS 會使用主體呼叫的權限 AWS 服務，並結合要求 AWS 服務 向下游服務發出要求。只有當服務收到需要與其 AWS 服務 他資源互動才能完成的請求時，才會發出 FAS 請求。在此情況下，您必須具有執行這兩個動作的許可。如需提出 FAS 請求時的策略詳細資訊，請參閱 [《轉發存取工作階段》](#)。
- 服務角色 – 服務角色是服務擔任的 [IAM 角色](#)，可代表您執行動作。IAM 管理員可以從 IAM 內建立、修改和刪除服務角色。如需詳細資訊，請參閱 IAM 使用者指南中的 [建立角色以委派許可給 AWS 服務服務](#)。
- 服務連結角色 — 服務連結角色是連結至 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，但不能編輯服務連結角色的許可。
- 在 Amazon EC2 上執行的應用程式 — 您可以使用 IAM 角色來管理在 EC2 執行個體上執行的應用程式以及發出 AWS CLI 或 AWS API 請求的臨時登入資料。這是在 EC2 執行個體內儲存存取金鑰的較好方式。若要將 AWS 角色指派給 EC2 執行個體並提供給其所有應用程式，請建立連接至執行個體的執行個體設定檔。執行個體設定檔包含該角色，並且可讓 EC2 執行個體上執行的程式取得暫時憑證。如需詳細資訊，請參閱 IAM 使用者指南中的 [利用 IAM 角色來授予許可給 Amazon EC2 執行個體上執行的應用程式](#)。

如需了解是否要使用 IAM 角色或 IAM 使用者，請參閱 IAM 使用者指南中的 [建立 IAM 角色 \(而非使用者\) 的時機](#)。

使用政策管理存取權

您可以透 AWS 過建立原則並將其附加至 AWS 身分識別或資源來控制中的存取。原則是一個物件 AWS，當與身分識別或資源相關聯時，會定義其權限。AWS 當主參與者 (使用者、root 使用者或角色工作階段) 提出要求時，評估這些原則。政策中的許可決定是否允許或拒絕請求。大多數原則會 AWS 以 JSON 文件的形式儲存在中。如需 JSON 政策文件結構和內容的詳細資訊，請參閱 IAM 使用者指南中的 [JSON 政策概觀](#)。

管理員可以使用 AWS JSON 政策來指定誰可以存取哪些內容。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。

預設情況下，使用者和角色沒有許可。若要授予使用者對其所需資源執行動作的許可，IAM 管理員可以建立 IAM 政策。然後，管理員可以將 IAM 政策新增至角色，使用者便能擔任這些角色。

IAM 政策定義該動作的許可，無論您使用何種方法來執行操作。例如，假設您有一個允許 `iam:GetRole` 動作的政策。具有該原則的使用者可以從 AWS Management Console AWS CLI、或 AWS API 取得角色資訊。

身分型政策

身分型政策是可以附加到身分 (例如 IAM 使用者、使用者群組或角色) 的 JSON 許可政策文件。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。若要了解如何建立身分類型政策，請參閱 IAM 使用者指南中的[建立 IAM 政策](#)。

身分型政策可進一步分類成內嵌政策或受管政策。內嵌政策會直接內嵌到單一使用者、群組或角色。受管理的策略是獨立策略，您可以將其附加到您的 AWS 帳戶。受管政策包括 AWS 受管政策和客戶管理的策略。如需了解如何在受管政策及內嵌政策間選擇，請參閱 IAM 使用者指南中的[在受管政策和內嵌政策間選擇](#)。

資源型政策

資源型政策是連接到資源的 JSON 政策文件。資源型政策的最常見範例是 IAM 角色信任政策和 Amazon S3 儲存貯體政策。在支援資源型政策的服務中，服務管理員可以使用它們來控制對特定資源的存取權限。對於附加政策的資源，政策會定義指定的主體可以對該資源執行的動作以及在何種條件下執行的動作。您必須在資源型政策中[指定主體](#)。主參與者可以包括帳戶、使用者、角色、同盟使用者或。AWS 服務

資源型政策是位於該服務中的內嵌政策。您無法在以資源為基礎的政策中使用 IAM 的 AWS 受管政策。

存取控制清單 (ACL)

存取控制清單 (ACL) 可控制哪些主體 (帳戶成員、使用者或角色) 擁有存取某資源的許可。ACL 類似於資源型政策，但它們不使用 JSON 政策文件格式。

Amazon S3 和 Amazon VPC 是支援 ACL 的服務範例。AWS WAF 如需進一步了解 ACL，請參閱 Amazon Simple Storage Service 開發人員指南中的[存取控制清單 \(ACL\) 概觀](#)。

其他政策類型

AWS 支援其他較不常見的原則類型。這些政策類型可設定較常見政策類型授予您的最大許可。

- **許可界限** – 許可範圍是一種進階功能，可供您設定身分型政策能授予 IAM 實體 (IAM 使用者或角色) 的最大許可。您可以為實體設定許可界限。所產生的許可會是實體的身分型政策和其許可界限的交集。會在 Principal 欄位中指定使用者或角色的資源型政策則不會受到許可界限限制。所有這類政策中的明確拒絕都會覆寫該允許。如需許可界限的詳細資訊，請參閱 IAM 使用者指南中的 [IAM 實體許可界限](#)。
- **服務控制策略 (SCP)** — SCP 是 JSON 策略，用於指定中組織或組織單位 (OU) 的最大權限。AWS Organizations 是一種用於分組和集中管理您企業擁有的多個 AWS 帳戶的服務。若您啟用組織中的所有功能，您可以將服務控制策略 (SCP) 套用到任何或所有帳戶。SCP 限制成員帳戶中實體的權限，包括每個 AWS 帳戶根使用者帳戶。如需 Organizations 和 SCP 的詳細資訊，請參閱 AWS Organizations 使用者指南中的 [SCP 運作方式](#)。
- **工作階段政策** – 工作階段政策是一種進階政策，您可以在透過編寫程式的方式建立角色或聯合使用者的暫時工作階段時，作為參數傳遞。所產生工作階段的許可會是使用者或角色的身分型政策和工作階段政策的交集。許可也可以來自資源型政策。所有這類政策中的明確拒絕都會覆寫該允許。如需詳細資訊，請參閱 IAM 使用者指南中的 [工作階段政策](#)。

多種政策類型

將多種政策類型套用到請求時，其結果形成的許可會更為複雜、更加難以理解。要了解如何在涉及多個政策類型時 AWS 確定是否允許請求，請參閱《IAM 使用者指南》中的 [政策評估邏輯](#)。

亞馬遜肯德拉如何與 IAM 合作

在您使用 IAM 管理 Amazon Kendra 的存取權限之前，您應該了解哪些 IAM 功能可與 Amazon Kendra 搭配使用。若要深入瞭解 Amazon Kendra 和其他 AWS 服務如何與 IAM 搭配使用，請參閱 IAM 使用者指南中的與 IAM 搭配使用的 [AWS 服務](#)。

主題

- [Amazon Kendra 基於身份的政策](#)
- [Amazon Kendra 基於資源的政策](#)
- [存取控制清單 \(ACL\)](#)
- [基於 Amazon Kendra 標籤的授權](#)
- [Amazon Kendra IAM 角色](#)

Amazon Kendra 基於身份的政策

使用 IAM 身分型政策，您可以指定允許或拒絕的動作和資源，以及在何種條件下允許或拒絕動作。Amazon Kendra 支援特定動作、資源和條件金鑰。若要了解您在 JSON 政策中使用的所有元素，請參閱 IAM 使用者指南中的 [JSON 政策元素參考](#)。

動作

管理員可以使用 AWS JSON 政策來指定誰可以存取哪些內容。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。

JSON 政策的 Action 元素描述您可以用來允許或拒絕政策中存取的動作。原則動作通常與關聯的 AWS API 作業具有相同的名稱。有一些例外狀況，例如沒有相符的 API 操作的僅限許可動作。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。

Amazon Kendra 中的政策動作會在動作前使用下列前置詞：kendra: 例如，若要授與某人使用 [ListIndices](#) API 作業列出 Amazon Kendra 索引的權限，您可以在他們的政策中包含該kendra:ListIndices動作。政策陳述式必須包含 Action 或 NotAction 元素。Amazon Kendra 會定義自己的一組動作，說明您可以使用此服務執行的任務。

若要在單一陳述式中指定多個動作，請用逗號分隔，如下所示：

```
"Action": [
  "kendra:action1",
  "kendra:action2"
```

您也可以使用萬用字元 (*) 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": "kendra:Describe*"
```

若要查看 Amazon Kendra 動作清單，請參閱 [IAM 使用者指南中的 Amazon Kendra 定義](#) 的動作。

資源

管理員可以使用 AWS JSON 政策來指定誰可以存取哪些內容。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。

Resource JSON 政策元素可指定要套用動作的物件。陳述式必須包含 Resource 或 NotResource 元素。最佳實務是使用其 [Amazon Resource Name \(ARN\)](#) 來指定資源。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 Kendra 索引資源具有以下 ARN：

```
arn:${Partition}:kendra:${Region}:${Account}:index/${IndexId}
```

如需 ARN 格式的詳細資訊，請參閱 [Amazon 資源名稱 \(ARN\) 和 AWS 服務命名空間](#)。

例如，若要在陳述式中指定索引，請在下列 ARN 中使用索引的 GUID：

```
"Resource": "arn:aws:kendra:${Region}:${Account}:index/${GUID}"
```

若要指定屬於特定帳戶的所有索引，請使用萬用字元 (*)：

```
"Resource": "arn:aws:${Region}:${Account}:index/*"
```

某些 Amazon Kendra 動作 (例如用於建立資源的動作) 無法在特定資源上執行。在這些情況下，您必須使用萬用字元 (*)。

```
"Resource": "*"
```

若要查看 Amazon Kendra 資源類型及其 ARN 的清單，請參閱 IAM 使用者指南中的 [Amazon Kendra 定義的資源](#)。若要了解可以使用哪些動作指定每個資源的 ARN，請參閱 [Amazon Kendra 定義的動作](#)。

條件索引鍵

管理員可以使用 AWS JSON 政策來指定誰可以存取哪些內容。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。

您也可以指定條件時使用預留位置變數。例如，您可以只在使用者使用其 IAM 使用者名稱標記時，將存取資源的許可授予該 IAM 使用者。如需更多資訊，請參閱 IAM 使用者指南中的 [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 全域條件金鑰，請參閱《IAM 使用者指南》中的 [AWS 全域條件內容金鑰](#)。

Amazon Kendra 不提供任何服務特定條件金鑰，但確實支援使用某些全域條件金鑰。若要查看所有 AWS 全域條件金鑰，請參閱 IAM 使用者指南中的 [AWS 全域條件內容金鑰](#)。

範例

若要檢視 Amazon Kendra 身分識別型政策的範例，請參閱 [Amazon Kendra 身分識別政策範例](#)

Amazon Kendra 基於資源的政策

Amazon Kendra 不支援以資源為基礎的政策。

存取控制清單 (ACL)

Amazon Kendra 不支援存取控制清單 (ACL) 以存取 AWS 服務和資源。

基於 Amazon Kendra 標籤的授權

您可以將標籤與特定類型的 Amazon Kendra 資源相關聯，以授權存取這些資源。若要根據標籤控制存取，請使用、或條件索引鍵 `aws:RequestTag/key-name`，在原則的條 `aws:TagKeys` 元素中提供標籤資訊。

下表列出以標籤為基礎的存取控制的動作、對應的資源類型和條件索引鍵。每個動作都會根據與對應資源類型相關聯的標籤進行授權。

動作	資源類型	條件索引鍵
CreateData來源		<code>aws:RequestTag</code> , <code>aws:TagKeys</code>

動作	資源類型	條件索引鍵
CreateFaq		aws:RequestTag , aws:TagKeys
CreateIndex		aws:RequestTag , aws:TagKeys
API_ListTagsForResource	資料來源, 常見問題集, 索引	
TagResource	資料來源, 常見問題集, 索引	aws:RequestTag , aws:TagKeys
UntagResource	資料來源, 常見問題集, 索引	aws:TagKeys

如需標記 Amazon Kendra 資源的相關資訊，請參閱[標籤](#)。如需根據資源標籤限制資源存取權的識別型政策範例，請參閱。[標籤型政策範例](#)如需有關使用標籤限制資源存取權的詳細資訊，請參閱 [IAM 使用者指南中的使用標籤控制存取](#)。

Amazon Kendra IAM 角色

[IAM 角色](#)是您 AWS 帳戶中具有特定許可的實體。

使用臨時登入資料與 Amazon Kendra

您可以搭配聯合使用暫時憑證、擔任 IAM 角色，或是擔任跨帳戶角色。您可以透過呼叫[AssumeRole](#)或[GetFederation權杖](#)等 AWS STS API 作業來取得臨時安全登入資料。

Amazon Kendra 支援使用臨時登入資料。

服務角色

此功能可讓服務代表您擔任[服務角色](#)。此角色可讓服務存取其他服務中的資源，以代表您完成動作。服務角色會出現在您的 IAM 帳戶中，且由該帳戶所擁有。這表示 IAM 管理員可以變更此角色的許可。不過，這樣可能會破壞此服務的功能。

Amazon Kendra 支援服務角色。

在 Amazon Kendra 中選擇 IAM 角色

當您建立索引、呼叫BatchPutDocument作業、建立資料來源或建立常見問題集時，必須提供 Amazon Kendra 用來代表您存取所需資源的存取角色 Amazon 資源名稱 (ARN)。如果您先前已建立角色，Amazon Kendra 主控台會提供可供您選擇的角色清單。選擇一個允許訪問所需資源的角色非常重要。如需詳細資訊，請參閱 [IAM 存取角色 Amazon Kendra](#)。

Amazon Kendra 身份識別政策範例

依預設，使用者和角色沒有建立或修改 Amazon Kendra 資源的權限。他們也無法使用 AWS Management Console AWS CLI、或 AWS API 執行工作。IAM 管理員必須建立 IAM 政策，授予使用者和角色在指定資源上執行特定 API 操作的所需許可。管理員接著必須將這些政策連接至需要這些許可的使用者或群組。

若要了解如何使用這些範例 JSON 政策文件建立 IAM 身分型政策，請參閱 IAM 使用者指南中的 [在 JSON 索引標籤上建立政策](#)。

主題

- [政策最佳實務](#)
- [AWS Amazon Kendra 的受管 \(預先定義\) 政策](#)
- [允許使用者檢視他們自己的許可](#)
- [訪問一個 Amazon Kendra 索引](#)
- [標籤型政策範例](#)

政策最佳實務

以身份識別為基礎的政策決定某人是否可以在您的帳戶中建立、存取或刪除 Amazon Kendra 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 — 若要開始將權限授與使用者和工作負載，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。如需更多資訊，請參閱 IAM 使用者指南中的 [AWS 受管政策](#)或[任務職能的AWS 受管政策](#)。
- 套用最低權限許可 – 設定 IAM 政策的許可時，請僅授予執行任務所需的許可。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。如需使用 IAM 套用許可的更多相關資訊，請參閱 IAM 使用者指南中的 [IAM 中的政策和許可](#)。

- 使用 IAM 政策中的條件進一步限制存取權 – 您可以將條件新增至政策，以限制動作和資源的存取。例如，您可以撰寫政策條件，指定必須使用 SSL 傳送所有請求。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 使用者指南中的 [IAM JSON 政策元素：條件](#)。
- 使用 IAM Access Analyzer 驗證 IAM 政策，確保許可安全且可正常運作 – IAM Access Analyzer 驗證新政策和現有政策，確保這些政策遵從 IAM 政策語言 (JSON) 和 IAM 最佳實務。IAM Access Analyzer 提供 100 多項政策檢查及切實可行的建議，可協助您編寫安全且實用的政策。如需更多資訊，請參閱 IAM 使用者指南中的 [IAM Access Analyzer 政策驗證](#)。
- 需要多因素身份驗證 (MFA) — 如果您的案例需要 IAM 使用者或根使用者 AWS 帳戶，請開啟 MFA 以獲得額外的安全性。如需在呼叫 API 操作時請求 MFA，請將 MFA 條件新增至您的政策。如需更多資訊，請參閱 [IAM 使用者指南](#) 中的設定 MFA 保護的 API 存取。

如需 IAM 中最佳實務的相關資訊，請參閱 IAM 使用者指南中的 [IAM 安全最佳實務](#)。

AWS Amazon Kendra 的受管 (預先定義) 政策

AWS 透過提供由建立和管理的獨立 IAM 政策來解決許多常見使用案例 AWS。這些原則稱為 AWS 受管理的原則。AWS 受管理的策略可讓您更輕鬆地將權限指派給使用者、群組和角色，而不是必須自行撰寫原則。如需詳細資訊，請參閱《IAM 使用者指南》中的 [新增許可到使用者](#)。

Amazon Kendra 專用的下列 AWS 受管政策 (您可以附加到帳戶中的群組和角色)：

- AmazonKendraReadOnly— 授予對 Amazon Kendra 資源的唯讀存取權。
- AmazonKendraFullAccess— 授予建立、讀取、更新、刪除、標記和執行所有 Amazon Kendra 資源的完整存取權。

對於主控台，您的角色也必須具

有 `iam:CreateRole`、`iam:CreatePolicy`、`iam:AttachRolePolicy`、和 `s3:ListBucket` 權限。

Note

您可以登入 IAM 主控台並搜尋特定政策，以檢閱這些許可。

您也可以建立自己的自訂政策，以允許 Amazon Kendra API 動作執行許可。您可以將這些自訂政策附加至需要這些許可的 IAM 角色或群組。如需 Amazon Kendra 的 IAM 政策範例，請參閱 [Amazon Kendra 身份識別政策範例](#)。

允許使用者檢視他們自己的許可

此範例會示範如何建立政策，允許 IAM 使用者檢視附加到他們使用者身分的內嵌及受管政策。此原則包含在主控台上或以程式設計方式使用 AWS CLI 或 AWS API 完成此動作的權限。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ViewOwnUserInfo",
      "Effect": "Allow",
      "Action": [
        "iam:GetUserPolicy",
        "iam:ListGroupsWithUser",
        "iam:ListAttachedUserPolicies",
        "iam:ListUserPolicies",
        "iam:GetUser"
      ],
      "Resource": ["arn:aws:iam::*:user/${aws:username}"]
    },
    {
      "Sid": "NavigateInConsole",
      "Effect": "Allow",
      "Action": [
        "iam:GetGroupPolicy",
        "iam:GetPolicyVersion",
        "iam:GetPolicy",
        "iam:ListAttachedGroupPolicies",
        "iam:ListGroupPolicies",
        "iam:ListPolicyVersions",
        "iam:ListPolicies",
        "iam:ListUsers"
      ],
      "Resource": "*"
    }
  ]
}
```

訪問一個 Amazon Kendra 索引

在此範例中，您想要授與 AWS 帳戶中的使用者以查詢索引的存取權。

```
{
```

```
"Version": "2012-10-17",
"Statement": [
  {
    "Sid": "QueryIndex",
    "Effect": "Allow",
    "Action": [
      "kendra:Query"
    ],
    "Resource": "arn:aws:kendra:${Region}:${Account}:index/${Index ID}"
  }
]
```

標籤型政策範例

以標籤為基礎的原則是 JSON 政策文件，可指定主參與者可對標記資源執行的動作。

範例：使用標籤存取資源

此範例策略授予 AWS 帳號中的使用者或角色權限，以便將Query作業與任何標記為索引鍵`department`和值的資源搭配使用`finance`。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "kendra:Query"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/department": "finance"
        }
      }
    }
  ]
}
```

範例：使用標籤啟用 Amazon Kendra 操作

此範例政策授予 AWS 帳戶中的使用者或角色使用任何 Amazon Kendra 操作的權限，但對任何標有金鑰 **department** 和值 **finance** 的資源進 TagResource 行操作除外。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "kendra:*",
      "Resource": "*"
    },
    {
      "Effect": "Deny",
      "Action": [
        "kendra:TagResource"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/department": "finance"
        }
      }
    }
  ]
}
```

範例：使用標籤來限制對作業的存取

此範例原則會限制 AWS 帳戶中的使用者或角色使用該 CreateIndex 作業的存取權，除非使用者提供標 **department** 籤，且其具有允許的值 **finance** 和 **IT**。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "kendra:CreateIndex",
      "Resource": "*"
    },
    {
      "Effect": "Deny",
```



```
    "Action": "kendra:CreateIndex",
    "Resource": "*",
    "Condition": {
      "Null": {
        "aws:RequestTag/department": "true"
      }
    }
  },
  {
    "Effect": "Deny",
    "Action": "kendra:CreateIndex",
    "Resource": "*",
    "Condition": {
      "ForAnyValue:StringNotEquals": {
        "aws:RequestTag/department": [
          "finance",
          "IT"
        ]
      }
    }
  }
]
```

AWS Amazon Kendra 的受管政策

若要新增使用者、群組和角色的權限，使用 AWS 受管理的原則比自己撰寫原則更容易。建立 [IAM 客戶受管政策](#) 需要時間和專業知識，而受管政策可為您的團隊提供其所需的許可。若要快速開始使用，您可以使用我們的 AWS 受管政策。這些政策涵蓋常見使用案例，並可在您的 AWS 帳戶中使用。如需 AWS 受管政策的詳細資訊，請參閱 IAM 使用者指南中的 [AWS 受管政策](#)。

AWS 服務會維護和更新 AWS 受管理的策略。您無法變更 AWS 受管理原則中的權限。服務偶爾會在 AWS 受管政策中新增其他許可以支援新功能。此類型的更新會影響已連接政策的所有身分識別 (使用者、群組和角色)。當新功能啟動或新操作可用時，服務很可能會更新 AWS 受管政策。服務不會從 AWS 受管理的政策移除權限，因此政策更新不會破壞您現有的權限。

此外，還 AWS 支援跨多個服務之工作職能的受管理原則。例如，ReadOnly 存取 AWS 管理原則會提供所有 AWS 服務和資源的唯讀存取權。當服務啟動新功能時，會為新作業和資源新 AWS 增唯讀權限。如需任務職能政策的清單和說明，請參閱 IAM 使用者指南中 [有關任務職能的 AWS 受管政策](#)。

AWS 受管理策略：AmazonKendraReadOnly

授予對 Amazon Kendra 資源的唯讀存取權。此政策包含以下許可。

- kendra— 允許使用者執行傳回項目清單或項目詳細資訊的動作。這包括以 Describe、ListQuery、BatchGetDocumentStatus 或開頭的 API 作業 GetSnapshots、GetQuerySuggestions

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "kendra:Describe*",
        "kendra:List*",
        "kendra:Query",
        "kendra:BatchGetDocumentStatus",
        "kendra:GetQuerySuggestions",
        "kendra:GetSnapshots"
      ],
      "Effect": "Allow",
      "Resource": "*"
    }
  ]
}
```

AWS 受管理策略：AmazonKendraFullAccess

授予建立、讀取、更新、刪除、標記和執行所有 Amazon Kendra 資源的完整存取權。此政策包含以下許可。

- kendra 允許主體對 Amazon Kendra 中的所有動作進行讀取和寫入存取。
- s3— 允許主體取得 Amazon S3 儲存貯體位置並列出儲存貯體。
- iam 允許主參與者傳遞和列出角色。
- kms 允許主參與者描述及列出 AWS KMS 索引鍵和別名。
- secretsmanager 允許主參與者建立、描述和列出密碼。

- ec2允許主體描述安全性群組、vCP (虛擬私人雲端) 和子網路。
- cloudwatch— 允許主參與者檢視雲端監控量度。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "iam:PassRole",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "iam:PassedToService": "kendra.amazonaws.com"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": [
        "iam:ListRoles"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "kms:ListKeys",
        "kms:ListAliases",
        "kms:DescribeKey"
      ],
      "Resource": "*"
    }
  ]
}
```

```

    "Effect": "Allow",
    "Action": [
      "s3:ListAllMyBuckets",
      "s3:GetBucketLocation"
    ],
    "Resource": "*"
  },
  {
    "Effect": "Allow",
    "Action": [
      "secretsmanager:ListSecrets"
    ],
    "Resource": "*"
  },
  {
    "Effect": "Allow",
    "Action": [
      "cloudwatch:GetMetricData"
    ],
    "Resource": "*"
  },
  {
    "Effect": "Allow",
    "Action": [
      "secretsmanager:CreateSecret",
      "secretsmanager:DescribeSecret"
    ],
    "Resource": "arn:aws:secretsmanager:*:*:secret:AmazonKendra-*"
  },
  {
    "Effect": "Allow",
    "Action": "kendra:*",
    "Resource": "*"
  }
]
}

```

Amazon Kendra 更新 AWS 受管政策

檢視 Amazon Kendra AWS 受管政策更新的詳細資訊，因為此服務開始追蹤這些變更。如需有關此頁面變更的自動警示，請訂閱 Amazon Kendra 文件歷史記錄頁面上的 RSS 摘要。

變更	描述	日期
AmazonKendraReadOnly- 添加對支持 GetSnapshots , BatchGetDocumentStatus API 的權限	Amazon Kendra 添加了新的 API GetSnapshots 和BatchGetDocumentStatus .GetSnapshots 提供顯示使用者如何與您的搜尋應用程式互動的資料。BatchGetDocumentStatus 監控文件編製索引的進度。	2022 年 1 月 3 日
AmazonKendraReadOnly— 添加權限以支持 GetQuerySuggestions 操作	Amazon Kendra 新增了一個新的 API , GetQuerySuggestions 可讓您存取熱門搜尋查詢的查詢建議，協助引導使用者的搜尋。當用戶鍵入他們的搜索查詢，建議的查詢有助於自動完成他們的搜索。	2021 年 5 月 27 日
Amazon Kendra 開始跟踪更改	Amazon Kendra 開始追蹤其 AWS 受管政策的變更。	2021 年 5 月 27 日

疑難排解 Amazon Kendra 身分和存取

使用下列資訊可協助您診斷和修正使用 Amazon Kendra 和 IAM 時可能會遇到的常見問題。

主題

- [我沒有授權在 Amazon Kendra 執行操作](#)
- [我沒有授權執行 iam : PassRole](#)
- [我是管理員，我想允許其他人訪問 Amazon Kendra](#)
- [我想要允許我 AWS 帳戶以外的人員存取我的 Amazon Kendra 資源](#)

我沒有授權在 Amazon Kendra 執行操作

如果 AWS Management Console 告訴您您沒有執行動作的授權，則您必須聯絡您的管理員以尋求協助。您的管理員是為您提供簽署憑證的人員。

當使用mateojackson者嘗試使用主控台來檢視索引的詳細資料，但沒有kendra:*DescribeIndex*權限時，就會發生下列範例錯誤。

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
kendra:DescribeIndex on resource: index ARN
```

在此情況下，Mateo 會請求管理員更新他的政策，允許他使用 index 動作存取 kendra:*DescribeIndex* 資源。

我沒有授權執行 iam : PassRole

如果您收到未獲授權執行iam:PassRole動作的錯誤訊息，則必須更新您的政策以允許您將角色傳遞給 Amazon Kendra。

有些 AWS 服務 允許您將現有角色傳遞給該服務，而不是建立新的服務角色或服務連結角色。如需執行此作業，您必須擁有將角色傳遞至該服務的許可。

當名為的 IAM 使用者marymajor嘗試使用主控台在 Amazon Kendra 中執行動作時，會發生下列範例錯誤。但是，動作請求服務具備服務角色授予的許可。Mary 沒有將角色傳遞至該服務的許可。

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
iam:PassRole
```

在這種情況下，Mary 的政策必須更新，允許她執行 iam:PassRole 動作。

如果您需要協助，請聯絡您的 AWS 系統管理員。您的管理員提供您的簽署憑證。

我是管理員，我想允許其他人訪問 Amazon Kendra

若要允許其他人存取 Amazon Kendra，您必須為需要存取的人員或應用程式建立 IAM 實體 (使用者或角色)。他們將使用該實體的憑證來存取 AWS。然後，您必須將政策附加到實體，以便在 Amazon Kendra 中授予他們正確許可。

若要立即開始使用，請參閱《IAM 使用者指南》中的[建立您的第一個 IAM 委派使用者及群組](#)。

我想要允許我 AWS 帳戶以外的人員存取我的 Amazon Kendra 資源

您可以建立一個角色，讓其他帳戶中的使用者或您組織外部的人員存取您的資源。您可以指定要允許哪些信任物件取得該角色。針對支援基於資源的政策或存取控制清單 (ACL) 的服務，您可以使用那些政策來授予人員存取您的資源的許可。

如需進一步了解，請參閱以下內容：

- 若要了解 Amazon Kendra 是否支援這些功能，請參閱[亞馬遜肯德拉如何與 IAM 合作](#)。
- 若要了解如何提供對您所擁有資源 AWS 帳戶的存取權，請參閱《IAM 使用者指南》中您擁有的另一 [AWS 帳戶 個 IAM 使用者提供存取權限](#)。
- 若要了解如何將資源存取權提供給第三方 AWS 帳戶，請參閱 IAM 使用者指南中的[提供第三方 AWS 帳戶 擁有的存取權](#)。
- 如需了解如何透過聯合身分提供存取權，請參閱 IAM 使用者指南中的[將存取權提供給在外部進行身分驗證的使用者 \(聯合身分\)](#)。
- 若要了解跨帳戶存取使用角色和以資源為基礎的政策之間的差異，請參閱 IAM 使用者指南中的 [IAM 中的跨帳戶資源存取](#)。

安全最佳實務

Amazon Kendra 提供許多安全功能，可在您開發和實作自己的安全政策時考慮。以下最佳實務為一般準則，並不代表完整的安全解決方案。這些最佳實務可能不適用或無法滿足您的環境需求，因此請將其視為實用建議就好，而不要當作是指示。

套用最低權限準則

Amazon Kendra 為使用 IAM 角色的應用程式提供精細的存取政策。建議您只將工作所需的最低權限集授與角色，例如涵蓋您的應用程式和記錄目的地的存取權限。我們還建議定期以及在應用程式發生變更時審核作業許可。

角色型存取控制 (RBAC) 許可

管理員應嚴格控制 Amazon Kendra 應用程式的角色型存取控制 (RBAC) 許可。

在 Amazon Kendra 中進行記錄和監控

監控是維護 Amazon Kendra 應用程式的可靠性、可用性和效能的重要組成部分。若要監控 Amazon Kendra API 呼叫，您可以使用 AWS CloudTrail。若要監控任務的狀態，請使用 Amazon CloudWatch 日誌。

- Amazon CloudWatch 警示 — 使用 CloudWatch 警示，您可以在指定的時間段內觀看單一指標。如果測量結果超過原則。CloudWatch 當測量結果處於特定狀態時，警示不會叫用動作。必須是狀態已變更並維持了所指定的時間長度，才會呼叫動作。如需詳細資訊，請參閱 [Amazon Kendra 監控與 Amazon Kendra CloudWatch](#)。
- AWS CloudTrail 日誌 — CloudTrail 提供使用者、角色或 AWS 服務在 Amazon Kendra 或亞馬遜 KenAmazon Kendra 智慧排名中所採取的動作記錄。使用收集的資訊 CloudTrail，您可以判斷向 Amazon Kendra 發出的請求、提出請求的 IP 地址、提出請求的人員、提出請求的時間以及其他詳細資訊。如需詳細資訊，請參閱 [使用記錄 Amazon Kendra API 呼叫AWS CloudTrail日誌](#) 及 [記錄 Amazon Kendra 智慧排名 API 呼叫AWS CloudTrail日誌](#)。

Amazon Kendra 的合規驗證

第三方稽核員會在多個 Amazon Kendra 合規計劃中，評估 Amazon Kendra 的安全性和合規性。Amazon Kendra 符合以下規定：

- 美國健康保險流通與責任法案 (HIPAA)
- 系統與組織控制 (SOC) 2
- 資訊保安註冊評審員計劃 (IRAP)
- 美國東部/西部地區的聯邦風險與授權管理計畫 (FedRAMP) 溫和
- AWS (美國西部) 區域的聯邦風險與授權管理計畫 GovCloud (FedRAMP) 高

如需特定規範計劃範圍內的 AWS 服務清單，請參閱 [合規計劃AWS 服務範圍](#) 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 AWS 人工因素下載人工因素 Ar AWS](#)。

使用 Amazon Kendra 時的合規責任取決於資料的敏感度、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：

- [安全性與合規快速入門指南](#) — 這些部署指南討論架構考量，並提供在上部署以安全性和法規遵循為重點的基準環境的步驟。AWS
- [建構 HIPAA 安全性與合規性白皮書](#) — 本白皮書說明公司如何使用建立符合 HIPAA 標準的應用程式。AWS
- [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。
- [使用AWS Config 開發人員指南中的規則評估資源](#) — 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](#) — 此 AWS 服務提供安全狀態的全面檢視，協助您檢查您 AWS 是否符合安全性產業標準和最佳做法。

Amazon Kendra 的韌性

AWS 全球基礎架構是圍繞區 AWS 域和可用區域建立的。AWS 區域提供多個實體分離和隔離的可用區域，這些區域透過低延遲、高輸送量和高度備援的網路連線。透過可用區域，您可以設計與操作的應用程式和資料庫，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、容錯能力和擴展能力，均較單一或多個資料中心的傳統基礎設施還高。

如需區域和可用區域的相關 AWS 資訊，請參閱[AWS 全域基礎結構](#)。

透過 AWS 全球基礎設施，Amazon Kendra 企業版具備容錯能力、可擴展性和高可用性。目前不支援復原至先前版本的索引，但是您可以透過[刪除](#)現有資料來源並將現有資料來源重新[加入](#)索引，以重新整理或重新建立索引的部分。

Amazon Kendra 的基礎設施安全

作為受管服務，Amazon Kendra 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 Kendra。使用者端必須支援下列專案：

- Transport Layer Security (TLS)。我們需要 TLS 1.2 並建議使用 TLS 1.3。
- 具備完美轉送私密(PFS)的密碼套件，例如 DHE (Ephemeral Diffie-Hellman)或 ECDHE (Elliptic Curve Ephemeral Diffie-Hellman)。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 主體相關聯的私密存取金鑰來簽署。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。

中的配置和漏洞分析 AWS Identity and Access Management

AWS 處理基本安全性工作，例如客體作業系統 (OS) 和資料庫修補、防火牆組態和嚴重損壞修復。這些程序已由適當的第三方進行檢閱並認證。如需詳細資訊，請參閱以下資源：

- [共同的責任模型](#)
- AWS：[安全性程序概觀](#) (白皮書)

下列資源也會解決 AWS Identity and Access Management (IAM) 中的組態和弱點分析問題：

- [符合性驗證 AWS Identity and Access Management](#)
- 中的[安全性最佳做法和使用 AWS Identity and Access Management 案例](#)

的配額 Amazon Kendra

支援的 區域

如需可用 AWS 區域的 Amazon Kendra 清單，請參閱 Amazon Web Services 一般參考中的 [Amazon Kendra 區域和端點](#)。

配額

服務配額 (也稱為限制) 是您 AWS 帳戶的服務資源數目上限。如需詳細資訊，請參閱 AWS 一般參考中的 [Amazon Kendra 服務配額](#)。

索引配額

描述	預設	版本	可調整
每個帳號的最大索引數	10	開發人員, 企業	是
為單一單位中的索引擷取的文字數量 (開發人員)。您無法為開發人員版添加額外的單位來提取文本。	3 GB	開發人員	否
為單一單位 (企業) 的索引擷取的文字數量。您最多可以新增 100 個額外單位來擷取企業版的文字，或直接聯絡 Support 部門。	30 GB	Enterprise	是

資料來源連接器配額

描述	預設	版本	可調整
每個索引的資料來源連接器數目上限 (開發人員)	5	開發人員	否
每個索引的資料來源連接器數目上限 (企業)	50	Enterprise	是
使用資料來源連接器時，單一文件或原始檔案的大小上限	50 MB	開發人員, 企業	是
Amazon S3 資料來源連接器中所包含的存取控制清單組態檔案中 S3 首碼的最大數目	100	開發人員, 企業	否
Amazon S3 資料來源連接器中包含的存取控制清單組態檔案大小上限	50 MB	開發人員, 企業	是

常見問題集

描述	預設	版本	可調整
每個索引最多常見問題	30	開發人員, 企業	是
1 個常見問題的最大尺寸	5 MB	開發人員, 企業	是
針對常見問題集傳回的最大結果數	4	開發人員, 企業	是

描述	預設	版本	可調整
常見問題解答問題允許的最大字符數	300	開發人員, 企業	否
常見問題解答中的最大字元數	2000	開發人員, 企業	否

索引典配額

描述	預設	版本	可調整
每個索引的最大同義詞數	1	開發人員, 企業	否
索引典檔案的大小上限	5 MB	開發人員, 企業	是
每個索引典的同義字規則數目上限	10,000	開發人員, 企業	是
索引中所有同義詞中每個字詞的同義字數上限	10	開發人員, 企業	否

Amazon Kendra 體驗配額

描述	預設	版本	可調整
每個索引的最大 Amazon Kendra 體驗數	50	開發人員, 企業	是

查詢和搜尋結果配額

描述	預設	版本	可調整
單一單位中索引的每秒查詢量 (開發人員)。您無法為開發人員版的查詢添加額外的單位。	0.05	開發人員	否
單一單位 (企業) 中索引的每秒查詢量。您最多可以新增 100 個額外單位來查詢企業版，或直接聯絡 Support 部門。	0.1	Enterprise	是
每個查詢文字的最大字元數	1000	開發人員, 企業	是
每個查詢的搜尋結果數目上限。預設值為 100。若要允許超過 100 個結果，只要聯絡 Support 部門即可。	100	開發人員, 企業	是
每頁最大搜尋結果數	100	開發人員, 企業	是
截斷前每個查詢文字的 Token 字數上限。預設值為 30。若要允許超過 30 個字，只要聯絡 Support 部門即可。	30	開發人員, 企業	是
每個查詢屬性使用者群組清單大小上限	1000	開發人員, 企業	是

描述	預設	版本	可調整
每個查詢屬性的字串清單大小上限	10	開發人員, 企業	是

查詢建議配額

描述	預設	版本	可調整
每個建議呼叫傳回的查詢建議數目上限	10	開發人員, 企業	是
每GetQuery個建議呼叫的查詢建議的欄位/屬性數目上限	10	開發人員, 企業	是
每GetQuery個建議呼叫的查詢建議額外欄位/屬性數目上限	5	開發人員, 企業	是
每個索引的封鎖清單數目上限	1	開發人員, 企業	否
封鎖清單文字檔的大小上限	2 MB	開發人員, 企業	是
封鎖清單中的項目數目上限 (單字或片語)	20,000	開發人員, 企業	是
QueryAPI 呼叫中所傳回的拼字校正查詢建議數目上限。	1	開發人員, 企業	是

文件配額

描述	預設	版本	可調整
為單一單位中的索引擷取的文字數量 (開發人員)。您無法為開發人員版添加額外的單位來提取文本。	3 GB	開發人員	否
為單一單位 (企業) 的索引擷取的文字數量。您最多可以新增 100 個額外單位來擷取企業版的文字，或直接聯絡 Sup port 部門。	30 GB	Enterprise	是
使用資料來源連接器時，單一文件或原始檔案的大小上限	50 MB	開發人員, 企業	是
使用 BatchPutDocument API 時，單一文件或原始檔案的大小上限	5 MB	開發人員, 企業	是
從單個文檔中提取的最大文本量	5 MB	開發人員, 企業	否
每個索引的自定義字段/屬性的最大數量	500	開發人員, 企業	否

特色搜尋結果配額

描述	預設	版本	可調整
每個精選結果集的精選文件數目上限	4	Enterprise	是
每個精選結果集的查詢文字數目上限	49	Enterprise	否
特色結果集中每個查詢文字的字元數目上限	1000	Enterprise	是
每個索引的最大特色結果集數	50	Enterprise	是

重新核心/重新排名搜尋結果額度

描述	預設	版本	可調整
重新評分執行計畫或單一容量單位的每秒Rescore要求數目上限。您最多可以添加1000個額外單位。	0.01	Enterprise	否
每個帳戶重新評分執行計畫的最大數目。	50	Enterprise	是
Rescore請求中Title文檔的最大令牌數量。	100	Enterprise	否
Rescore請求中Body文檔的最大令牌數量。	200	Enterprise	否

描述	預設	版本	可調整
Rescore請求中的最大文檔數量。	25	Enterprise	否
Rescore請求中每個群組的文件數目上限。	3	Enterprise	否

如需 Amazon Kendra Service Quotas 和要求增加配額的詳細資訊，請參閱[服務配額](#)。

故障診斷

本節可協助您解決使用時可能會發現的常見問題 Amazon Kendra。

主題

- [疑難排解資料來](#)
- [文件搜尋結果的疑難](#)
- [疑難排解一般問題](#)

疑難排解資料來

本節可協助您解決設定和使用 Amazon Kendra 資料來源連接器時的常見問題。

我的文件沒有編製索引

當您將 Amazon Kendra 索引與資料來源同步處理時，可能會遇到阻止文件編製索引的問題。索引是一個兩個步驟的過程。首先，檢查資料來源是否有要建立索引的新文件和更新文件，並尋找要從索引中移除的文件。其次，在文檔級別，每個文檔被訪問和索引。

在這些步驟之一中都可能發生錯誤。資料來源詳細資料頁面的 [同步執行歷程記錄] 區段的主控台中會報告資料來源層級錯誤。同步化工作的狀態可以是「成功」、「未完成」或「失敗」。您也可以查看工作期間編製索引和刪除的文件數目。如果狀態為「失敗」，則「詳細資料」欄中會顯示訊息。

在中報告文件層級錯誤 Amazon CloudWatch Logs。您可以使用 CloudWatch 控制台看到錯誤。

若要產生文件同步狀態報告，請參閱[我想要產生文件的同步狀態報告](#)。

我的同步工作失敗

當索引或資料來源中發生組態錯誤時，同步化工作通常會失敗。在主控台中，您可以在資料來源詳細資料頁面的 [詳細資料] 欄下的 [同步執行歷程記錄] 區段中找到錯誤訊息。在中報告文件層級錯誤 Amazon CloudWatch Logs。錯誤消息提供了有關出錯的信息。問題通常是索引或資料來源沒有適當的 IAM 權限。錯誤訊息會描述遺失的權限。以下是您可以收到的一些錯誤訊息：

```
Failed to create log group for job. Please make sure that the IAM role provided has sufficient permissions.
```

如果您的索引角色沒有使用權限 CloudWatch，則資料來源將無法建立 CloudWatch 記錄檔。如果您收到這個錯誤，您必須新增索引角色的 CloudWatch 權限。

```
Failed to access Amazon S3 file prefix (bucket name) while trying to crawl your metadata files. Please make sure the IAM role (ARN) provided has sufficient permissions.
```

使用 Amazon S3 資料來源時，Amazon Kendra 必須具有存取包含文件之值區的權限。您需要新增權限，才 Amazon Kendra 能將值區讀取至資料來源 IAM 角色。

```
The provided IAM role (ARN) could not be assumed. Please make sure Amazon Kendra is a trusted entity that is allowed to assume the role.
```

Amazon Kendra 需要具有索引和資料來源 IAM 角色的權限。您需要將信任原則新增至具有 `sts:AssumeRole` 動作權限的角色。

有關 Amazon Kendra 需要為資料來源編製索引的 IAM 策略，請參閱[IAM 角色](#)。

若要產生文件同步狀態報告，請參閱[我想要產生文件的同步狀態報告](#)。

我的同步工作不完整

工作通常在完成資料來源層級程序後不完整，但在文件層級處理期間出現一些錯誤。當工作不完整時，某些文件可能未成功編製索引。對於 Amazon S3 資料來源，不完整的工作通常是由下列原因造成的：

- 一或多個文件的中繼資料無效。
- 提交文件進行索引，但至少有一份文件未提交時。
- 提交要從索引中刪除的文件，但至少有一份文件未提交時。

若要疑難排解不完整的同步處理工作，請先查看您的 CloudWatch 記錄檔。

1. 從詳細資訊欄中，選擇檢視詳細資料於 CloudWatch。
2. 檢閱錯誤訊息以查看導致文件失敗的原因。

若要產生文件同步狀態報告，請參閱[我想要產生文件的同步狀態報告](#)。

我的同步處理工作成功，但沒有編製索引的文件

有時候，索引同步處理工作執行會標示為「成功」，但沒有新文件或更新的文件在您預期的情況下編製索引。可能的原因包括：

- 檢查 CloudWatch DocumentsSubmittedForIndexingFailed 量度以查看是否有任何文件無法同步處理。如需詳細資訊，請檢查 CloudWatch 記錄。
- 對於資料來源 Amazon S3，您可能提供了錯誤 Amazon Kendra 的值區名稱或前置詞。請確定正在使用的值區 Amazon Kendra 是包含要編製索引之文件的值區。
- 重新索引未能在較早的工作中建立索引的文件時，除非您已變更文件或其關聯的中繼資料檔案，否則 Amazon Kendra 不會對其建立索引。

若要產生文件同步狀態報告，請參閱[我想要產生文件的同步狀態報告](#)。

我在同步資料來源時遇到檔案格式問題

如果您在將檔案新增至資料來源或同步資料來源時遇到檔案格式問題，請確定 Amazon Kendra 支援您的文件類型。如需支援的文件類型清單，Amazon Kendra 請參閱[文件類型或格式](#)。

如果您將 BatchPutDocument API 與純文字檔案搭配使用，請指定 PLAIN_TEXT 為內容類型。

我想要為我的文件產生同步記錄報告

同步資料來源 Amazon Kendra 料來源連接器時，Amazon Kendra 可以為資料來源中的每個文件產生同步狀態報告，並將其複製到 Amazon S3 值區。在此過程中，您的數據使用密 AWS KMS 鑰進行加密，並且只能由您查看。報告的文件狀態可以是下列其中一種：「失敗」、「已完成」或「成功但有錯誤」。

您必須先執行下列動作，才能產生同步狀態報告：

- 將下列 Amazon Kendra 服務主體新增至您的 Amazon S3 存取原則

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "KendraS3Access",
      "Effect": "Allow",
      "Principal": {
        "Service": "kendra.amazonaws.com"
      },
      "Action": "s3:PutObject",
      "Resource": "arn:aws:s3:::your-manifest-bucket-name/*"
    }
  ]
}
```

- 建立具有 Amazon S3 存取權限的值區 Amazon Kendra

如果您使用主控台，若要產生同步狀態報告，請從 [資料來源詳細資料] 頁面選擇啟動同步歷史記錄產生選項。然後，輸入 Amazon S3 值區位置，並從可用的配置選項中進行選擇。啟動產生報告後，將從下次同步處理產生報告。

如果刪除 Amazon S3 值區，您將遺失記錄資料，而且必須設定新值區才能儲存新的同步報告。

目前僅支援[Amazon S3 連接器](#)的產生同步報告狀態。

同步資料來源需要多少時間？

如果文件沒有更新，Amazon Kendra 索引的同步時間會隨文件數目成線性比例增加。例如，1,000 份沒有任何更新的文件大約需要 5 分鐘才能同步處理，而 2,000 份文件而沒有任何更新則大約需要 10 分鐘。如果文件有任何更新，則同步時間會根據更新的文件數量而增加。

同步資料來源的費用為何？

當您同步索引時，需要兩分鐘的時間來預熱並啟動，Amazon EC2 以建立必要的連線。在此過程中，您不會收取任何費用。您的使用量計量器只會在同步工作開始後開始。如需 Amazon Kendra 定價的詳細資訊，請參閱[Amazon Kendra 定價](#)。

我收到 Amazon EC2 授權錯誤

如果在同步虛擬私有雲 (VPC) 資料來源期間發生 Amazon EC2 未經授權的作業錯誤，則可能是您的 VPC IAM 角色缺少必要的權限。請檢查您用於資料來源的 IAM 角色是否具有附加的權限。如需詳細資訊，請參閱[虛擬私有雲 IAM 角色](#)。

我無法使用搜索索引鏈接打開我的 Amazon S3 對象

您的 Amazon Kendra 索引只能存取 Amazon S3 資料來源授予其存取權限的檔案。例如，Amazon Kendra 無法修改決 Amazon S3 物件應為公用還是加密的權限。Amazon Kendra 也沒有為 Amazon S3 物件建立或傳回已簽署連結的預設權限。如果您想要啟動 Amazon Kendra 索引中 Amazon S3 物件的已簽署連結，您有兩個選項：

- 在將結果傳回至搜尋頁面之前，您可以使用來源 uri 物件來簽署索引查詢結果。如需此程序的 step-by-step 逐步解說，請參閱[使用預先簽署的 URL 共用物件](#)。
- 您可以覆寫 Amazon S3 物件中繼資料來源 uri，並透過連線至 Amazon S3 值區的 CloudFront 內容傳遞網路 (CDN) 提供服務。或者，您可以使用 API Gateway 代理端點返回預先簽署的 URL 並重定向到該端點。

我收到「使用 SSL 憑證檔案AccessDenied 時」錯誤訊息

如果您在將 SSL 憑證與資料來源搭配使用時遇到存取遭拒的錯誤，請確定您的 IAM 角色具有存取其指定位置中的 SSL 憑證檔案的權限。如果憑證使用 AWS KMS 金鑰加密，您的 IAM 角色也應具有使用 AWS KMS 金鑰解密的權限。如需詳細資訊，請參閱的[驗證和存取控制 AWS KMS](#)。

我在使用 SharePoint 資料來源時收到授權錯誤

如果您在同步索引與 SharePoint 資料來源時收到授權錯誤，請確認您在中指派了網站管理員角色 SharePoint。

我的索引不會從我的匯合資料來源抓取文件

如果您的 Amazon Kendra 索引未在同步處理過程中從 Confluence 資料來源探索文件，請確認您是 Confluence 中的系統管理員群組的一部分。

文件搜尋結果的疑難

本節可協助您修正 Amazon Kendra 搜尋結果中的問題。

我的搜尋結果與我的搜尋條件不相關

如果您的搜尋結果看起來無關緊要，可能原因如下：

- 結果中包含有LOW信心的結果。您可以使用的ScoreAttributes欄位來排除任何值為的[QueryResultItem](#)結果，有LOW信心地篩選出結果LOW。 Amazon Kendra 為每個結果指派VERY_HIGH、HIGHMEDIUM和的信賴值區值LOW。這些值表示結果與查詢相關的可信度等級。此外，無論置信桶如何，都會按以下順序 Amazon Kendra 返回三種類型的結果：ANSWER（建議的答案摘錄），QUESTION_ANSWER（FAQ）和DOCUMENT（文檔摘錄）。因此，可以將置LOW信度QUESTION_ANSWER結果定位在置VERY_HIGH信度DOCUMENT結果之上。但是，信心比LOW信心更好的結果並不總QUESTION_ANSWER是如此DOCUMENT。VERY_HIGH
- 某些中繼資料欄位或屬性會提升至非常高的值，從而影響結果的排名。 Amazon Kendra 使用多個參數（例如文件標題、文字、日期和自訂文字欄位或屬性）來搜尋索引。您可以嘗試使用不同的提升值，以在所有查詢中獲得最佳結果。您也可以查詢層級使用動態[相關性調整](#)，為每個查詢使用不同的提升值。
- 您的使用者在查詢資訊時使用專用術語，而且沒有為您的索引設定自訂同義詞來處理這些特殊字詞。如需如何及何時使用同義字的詳細資訊，請參閱[將自訂同義字新增至索引](#)。

為什麼我只看到 100 個結果？

Amazon Kendra 傳回相關文件的總數。依預設，每個查詢都會傳回前 100 名。結果會分頁。您可以使用 PageNumber 訪問不同的頁面。

您可以設定 Amazon Kendra 為每個查詢最多傳回 1,000 個文件或搜尋結果，每頁最多可傳回 100 個結果。若要傳回 100 個以上的結果，您可以聯絡 [配額 Support](#) 要求。增加搜尋結果的數量可能會影響延遲。

為什麼我希望看到的文檔丟失？

Amazon Kendra 支援以使用者和群組為基礎的存取控制清單 (ACL)。Amazon Kendra 透過連接器擷取 ACL 原則。如果索引未配置 ACL，則只會顯示符合使用者和群組之屬性篩選器的文件。如果提供使用者或群組屬性篩選器，則不會顯示沒有 ACL 的文件。

如果您使用權杖型存取控制，則會顯示沒有 ACL 原則的文件以及符合使用者和群組的文件。

為什麼我會看到具有 ACL 政策的文件？

如果索引未設定存取控制原則，則篩選器可以提供使用者和群組。如果未套用使用者和群組篩選，則會傳回所有相關文件。任何 ACL 政策都將被忽略。

疑難排解一般問題

Amazon Kendra 使用 CloudWatch 指標和日誌來提供有關同步資料來源的見解。您可以使用指標和記錄來判斷同步處理執行發生了什麼問題，以及如何修正它。

對於一般疑難排解，請從您的 CloudWatch 指標開始。

- 檢查 DocumentsCrawled 指標以查看您的資料來源檢查了多少文件。對於 Amazon S3 值區，如果數字小於您預期的數字，請檢查資料來源是否指向正確的值區。
- 檢查 DocumentsSkippedNoChange 量度以查看有多少文檔被跳過，因為自上次同步以來沒有更改。如果數字與您預期的不符，請檢查您的儲存庫是否已正確更新。
- 檢查 DocumentsSkippedInvalidMetadata 量度以查看有多少文件具有無效的中繼資料。檢查您的 CloudWatch 日誌以查看發生的特定錯誤。
- 檢查 DocumentsSubmittedForIndexingFailed 量度以查看有多少文件從資料來源傳送至索引，但無法編製索引。例如，如果您在尚未定義為自訂索引欄位的 Amazon S3 資料來源中使用 metadata 屬性，則不會對文件進行索引。檢查您的 CloudWatch 日誌以查看發生的特定錯誤。

- 檢查 DocumentsSubmittedForDeletionFailed 量度，以查看資料來源嘗試從索引中移除的文件數目無法從索引中刪除。檢查您的 CloudWatch 日誌以查看發生的特定錯誤。

您可以查看特定同步處理執行的 CloudWatch 記錄檔，以取得執行期間發生錯誤的詳細資訊。如需有關 CloudWatch 記錄的詳細資訊 Amazon Kendra，請參閱 [CloudWatch Logs](#)。

Amazon Kendra 智慧排名

Amazon Kendra 智慧排名使用 Amazon Kendra 語意搜尋功能，聰明地重新排名搜尋服務的結果。

主題

- [Amazon Kendra 自我管理的智慧排名 OpenSearch](#)
- [語義上對搜索服務的結果進行排名](#)

Amazon Kendra 自我管理的智慧排名 OpenSearch

您可以利用 Amazon Kendra 語意搜尋功能來改善以 Apache 2.0 授權為基礎的自我管理開放原始碼搜尋服務的搜尋結果。[OpenSearch](#) Amazon Kendra 智能排名插件在語義上使用重新排名 OpenSearch 的結果。Amazon Kendra 它透過使用預設 OpenSearch 搜尋結果中的特定欄位 (例如文件內文或標題) 瞭解搜尋查詢的意義和前後關聯來達成此目的。

以此查詢為例：「主要主題演講地址」。由於「地址」具有多種含義，因此 Amazon Kendra 可以推斷查詢背後的含義，以返回與預期含義一致的相關信息。在這種情況下，這是一個會議主題演講。例如，較簡單的搜尋服務可能無法將意圖列入考量，而且可能會傳回 Main Street 上街道地址的結果。

的智慧排名外掛程式 OpenSearch 適用於 OpenSearch (自我管理) 2.4.0 及更高版本。您可以使用快速啟動 Bash 腳本安裝插件，以構建一個新的 Docker 形象 OpenSearch 與智能排名插件包括在內。請參閱 [設定智慧型搜尋外掛程式](#) — 這是一個讓您快速啟動和運行的設置示例。

智能搜索插件的工作原理

OpenSearch (自我管理) 的智能排名插件的整體過程如下：

1. OpenSearch 使用者發出查詢，並 OpenSearch 提供查詢回應或與查詢相關的文件清單。
2. 智能排名插件獲取查詢響應並從文檔中提取信息。
3. 智能排名插件調用 Amazon Kendra 智能排名的 [重分](#) API。
4. 該 Rescore API 從文檔中獲取提取的信息，並在語義上重新排名搜索結果。
5. 該 Rescore API 將重新排名的搜索結果發送回插件。該插件在搜索響應中重新排列搜 OpenSearch 索結果，以反映新的語義排名。

智能排名插件使用「正文」和「標題」字段重新排名結果。這些外掛程式欄位可以對應至 OpenSearch 索引中最符合文件內文和標題定義的欄位。例如，如果您的索引包含帶有「chapter_title」和

「chapter_contents」等字段的書籍章節，則可以將前者對應到「標題」，而後者對應到「正文」以獲得最佳結果。

設定智慧型搜尋外掛程式

以下概述了如何使用智能排名插件快速設置 OpenSearch（自我管理）。

設置 OpenSearch（自我管理）與智能排名插件（快速設置）

如果您已經在使用 Docker 圖像 `opensearch:2.4.0`，則可以使用此 [Dockerfile 使用智能排名插件](#) 構建 OpenSearch 2.4.0 的新圖像。您可以在 [碼頭工具組成 .yaml 文件或打開搜索 .yaml 文件中包含新圖像](#) 的容器。您還可以通過創建重新評分執行計劃以及您的區域和端點信息包含生成的重新評分執行計劃 ID，請參閱有關創建重新評分執行計劃的步驟 2。

如果您之前下載的 `opensearch` Docker 映像版本早於 2.4.0，則必須使用 Docker 映像 `opensearch:2.4.0` 或更高版本，並使用包含智能排名插件構建新圖像。

1. 下載並安裝 [Docker 桌面](#) 為您的操作系統。碼頭桌面包括碼頭構成和碼頭引擎。建議您檢查您的電腦是否符合 Docker 安裝詳細資料中提到的系統需求。

您還可以在 Docker 桌面的設置中增加內存使用需求。除了 Docker 服務的免費使用限制以外，您必須對 Docker 的使用需求負責。請參閱 [泊塢視窗訂閱](#)。

檢查碼頭桌面狀態是否「正在運行」。

2. 提供 Amazon Kendra 智能排名和您的 [容量](#) 需求。佈建 Amazon Kendra 智慧排名後，系統會根據您設定的容量單位，每小時向您收費。請參閱 [免費方案和定價資訊](#)。

您可以使用 [CreateRescoreExecutionPlan](#) API 來佈建 Rescore API。如果您不需要超過單一單位預設的容量單位，請不要新增更多單位，而且只提供重新評分執行計畫的名稱。您也可以使用 [UpdateRescoreExecutionPlan](#) API 更新容量需求。如需詳細資訊，請參閱以 [語意方式排名搜尋服務的結果](#)。

或者，您可以在執行快速啟動 Bash 指令碼時，移至步驟 3 建立預設的重新分數執行計畫。

請注意步驟 4 回應中包含的重新評分執行計畫 ID。

CLI

```
aws kendra-ranking create-rescore-execution-plan \  
  --name MyRescoreExecutionPlan \  
  --region us-east-1
```

```
--capacity-units '{"RescoreCapacityUnits':<integer number of additional capacity units>}'
```

Response:

```
{
  "Id": "<rescore execution plan ID>",
  "Arn": "arn:aws:kendra-ranking:<region>:<account-id>:rescore-execution-plan/
<rescore-execution-plan-id>"
}
```

Python

```
import boto3
from botocore.exceptions import ClientError
import pprint
import time

kendra_ranking = boto3.client("kendra-ranking")

print("Create a rescore execution plan.")

# Provide a name for the rescore execution plan
name = "MyRescoreExecutionPlan"
# Set your required additional capacity units
# Don't set capacity units if you don't require more than 1 unit given by
# default
capacity_units = 1

try:
    rescore_execution_plan_response =
    kendra_ranking.create_rescore_execution_plan(
        Name = name,
        CapacityUnits = {"RescoreCapacityUnits":capacity_units}
    )

    pprint.pprint(rescore_execution_plan_response)

    rescore_execution_plan_id = rescore_execution_plan_response["Id"]

    print("Wait for Amazon Kendra to create the rescore execution plan.")

    while True:
```

```
# Get the details of the rescore execution plan, such as the status
rescore_execution_plan_description =
kendra_ranking.describe_rescore_execution_plan(
    Id = rescore_execution_plan_id
)
# When status is not CREATING quit.
status = rescore_execution_plan_description["Status"]
print(" Creating rescore execution plan. Status: "+status)
time.sleep(60)
if status != "CREATING":
    break

except ClientError as e:
    print("%s" % e)

print("Program ends.")
```

3. OpenSearch 通過從主分支下拉列表中 GitHub 選擇版本分支，從您的版本下載 [快速啟動 Bash 腳本](#)。

此指令碼會使用您在指令碼 GitHub 存放庫中選取的本來使用 Docker 映像 OpenSearch 和 OpenSearch 儀表板。它下載了智能排名插件的 zip 文件，並生成一個 Dockerfile 個構建包括插件 OpenSearch 的新 Docker 圖像。它還創建了一個 [碼頭組成 .yaml](#) 文件，其中包括與智能排名插件和儀表板 OpenSearch 的容器。OpenSearch 此指令碼會將您的重新評分執行計劃 ID、區域資訊和端點 (使用區域) 新增至停駐端工具組成 .yaml 檔案。然後執行指令碼 `docker-compose up` 以啟動包 OpenSearch 含智慧排名和 OpenSearch 儀表板的容器。要停止容器而不刪除它們，請運行 `docker-compose stop`。若要移除容器，請執行 `docker-compose down`。

4. 打開終端，然後在 Bash 腳本的目錄中運行以下命令。

```
bash search_processing_kendra_quickstart.sh -p <execution-plan-id> -r <region>
```

當您執行此命令時，請提供您佈建 Amazon Kendra 智慧排名時在步驟 2 中記下的重新評分執行計畫 ID，以及您的區域資訊。或者，您可以使用 `--create-execution-plan` 選項來佈建「Amazon Kendra 智慧排名」。這會建立具有預設名稱和預設容量的重新評分執行計畫。

若要在移除預設暫時容器時不會遺失索引，您可以透過使用選項提供資料磁碟區名稱，讓索引在執行間持續存在。`--volume-name` 如果您先前已建立索引，您可以在碼頭組成 .yaml 或 `opensearch.yaml` 檔案中指定磁碟區。要保持卷不變，請不要運行 `docker-compose down -v`。

快速啟動 Bash 腳本在 OpenSearch 密鑰庫中配置您的 AWS 憑據以連接到 Amazon Kendra 智能排名。若要提供您的 AWS 認證給指令碼，請使用 `--profile` 選項來指定 AWS 設定檔。如果未指定該 `--profile` 選項，則快速啟動 Bash 腳本會嘗試從環境變量中讀取 AWS 憑據（訪問/秘密密鑰，可選會話令牌），然後從默認 AWS 配置文件中讀取憑據。如果未指定 `--profile` 選項且找不到認證，則指令碼不會將認證傳遞至 OpenSearch 金鑰儲存庫。如果 OpenSearch 金鑰儲存庫中未指定認證，外掛程式仍會檢查[預設認證提供者鏈結中的認證](#)，包括透過中 Amazon EC2 繼資料服務傳送的 Amazon ECS 容器認證或執行個體設定檔認證。

請確定您已建立具有呼叫 Amazon Kendra 智慧排名所需權限的 IAM 角色。以下是授與將 Rescore API 用於特定重新評分執行計劃之權限的 IAM 政策範例：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "kendra-ranking:Rescore",
      "Resource": "arn:aws:kendra-ranking:${Region}:${Account}:rescore-execution-plan/${RescoreExecutionPlanId}"
    }
  ]
}
```

碼頭工具組成 .yml 的示例

使用 2.4.0 或更新版本搭配智慧排名外掛程式和儀表板 OpenSearch 2.4.0 或更新版本的碼頭工具組成 .yml 檔案範例。OpenSearch

```
version: '3'
networks:
  opensearch-net:
volumes:
  <volume-name>:
services:
  opensearch-node:
    image: <Docker image tag name of OpenSearch with Intelligent Ranking plugin>
    container_name: opensearch-node
    environment:
      - cluster.name=opensearch-cluster
      - node.name=opensearch-node
```

```

- discovery.type=single-node
- kendra_intelligent_ranking.service.endpoint=https://kendra-
ranking.<region>.api.aws
- kendra_intelligent_ranking.service.region=<region>
- kendra_intelligent_ranking.service.execution_plan_id=<rescore-execution-plan-
id>
ulimits:
  memlock:
    soft: -1
    hard: -1
  nofile:
    soft: 65536
    hard: 65536
ports:
- 9200:9200
- 9600:9600
networks:
- opensearch-net
volumes:
  <docker-volume-name>:/usr/share/opensearch/data
opensearch-dashboard:
  image: opensearchproject/opensearch-dashboards:<your-version>
  container_name: opensearch-dashboards
  ports:
    - 5601:5601
  environment:
    OPENSEARCH_HOSTS: '["https://opensearch-node:9200"]'
  networks:
    - opensearch-net

```

碼頭文件和構建圖像的示例

使用 OpenSearch 2.4.0 或更新版本與智慧排名外掛程式的範例。Dockerfile

```

FROM opensearchproject/opensearch:<your-version>
RUN /usr/share/opensearch/bin/opensearch-plugin install --batch https://github.com/
opensearch-project/search-processor/releases/download/<your-version>/search-
processor.zip

```

OpenSearch 使用智能排名插件構建 Docker 圖像。

```
docker build --tag=<Docker image tag name of OpenSearch with Intelligent Ranking plugin>
```

與智慧型搜尋外掛程式互動

使用智能排名插件設置 OpenSearch (自我管理) 後, 您可以使用 curl 命令或 OpenSearch 客戶端庫與插件進行交互。使用智能排名插件訪問 OpenSearch 的默認憑據是用戶名「管理員」和密碼「管理員」。

若要將智慧排名外掛程式設定套用至 OpenSearch 索引：

Curl

```
curl -XPUT "https://localhost:9200/<your-docs-index>/_settings" -u 'admin:admin' --insecure -H 'Content-Type: application/json' -d'
{
  "index": {
    "plugin" : {
      "searchrelevance" : {
        "result_transformer" : {
          "kendra_intelligent_ranking": {
            "order": 1,
            "properties": {
              "title_field": "title_field_name_here",
              "body_field": "body_field_name_here"
            }
          }
        }
      }
    }
  }
}
```

Python

```
pip install opensearch-py

from opensearchpy import OpenSearch
host = 'localhost'
port = 9200
```



```
auth = ('admin', 'admin')

client = OpenSearch(
    hosts = [{'host': host, 'port': port}],
    http_compress = True, # enables gzip compression for request bodies
    http_auth = auth,
    # client_cert = client_cert_path,
    # client_key = client_key_path,
    use_ssl = True,
    verify_certs = False,
    ssl_assert_hostname = False,
    ssl_show_warn = False,
    ca_certs = ca_certs_path
)

setting_body = {
    "index": {
        "plugin" : {
            "searchrelevance" : {
                "result_transformer" : {
                    "kendra_intelligent_ranking": {
                        "order": 1,
                        "properties": {
                            "title_field": "title_field_name_here",
                            "body_field": "body_field_name_here"
                        }
                    }
                }
            }
        }
    }
}

response = client.indices.put_settings(index_name, body=setting_body)
```

您必須包含要用來重新排名的主要文字欄位的名稱，例如文件內文或文件內容欄位。您也可以包含其他文字欄位，例如文件標題或文件摘要。

現在，您可以發出任何查詢，並使用智能排名插件對結果進行排名。

Curl

```
curl -XGET "https://localhost:9200/<your-docs-index>/_search?pretty" -u
'admin:admin' --insecure -H 'Content-Type: application/json' -d'
{
  "query" : {
    "match" : {
      "body_field_name_here": "intelligent systems"
    }
  }
}
```

Python

```
from opensearchpy import OpenSearch
host = 'localhost'
port = 9200
auth = ('admin', 'admin')

client = OpenSearch(
    hosts = [{'host': host, 'port': port}],
    http_compress = True, # enables gzip compression for request bodies
    http_auth = auth,
    # client_cert = client_cert_path,
    # client_key = client_key_path,
    use_ssl = True,
    verify_certs = False,
    ssl_assert_hostname = False,
    ssl_show_warn = False,
    ca_certs = ca_certs_path
)

query = {
    'size': 10,
    "query" : {
        "match" : {
            "body_field_name_here": "intelligent systems"
        }
    }
}

response = client.search(
```

```
        body = query,
        index = index_name
    )

print('\nSearch results:')
print(response)
```

若要移除索引 OpenSearch 的智慧排名外掛程式設定：

Curl

```
curl -XPUT "http://localhost:9200/<your-docs-index>/_settings" -H 'Content-Type:
application/json' -d'
{
  "index": {
    "plugin": {
      "searchrelevance": {
        "result_transformer": {
          "kendra_intelligent_ranking.*": null
        }
      }
    }
  }
}
```

Python

```
from opensearchpy import OpenSearch
host = 'localhost'
port = 9200
auth = ('admin', 'admin')

client = OpenSearch(
    hosts = [{'host': host, 'port': port}],
    http_compress = True, # enables gzip compression for request bodies
    http_auth = auth,
    # client_cert = client_cert_path,
    # client_key = client_key_path,
    use_ssl = True,
    verify_certs = False,
    ssl_assert_hostname = False,
```

```

    ssl_show_warn = False,
    ca_certs = ca_certs_path
)

setting_body = {
  "index": {
    "plugin": {
      "searchrelevance": {
        "result_transformer": {
          "kendra_intelligent_ranking.*": null
        }
      }
    }
  }
}

response = client.indices.put_settings(index_name, body=setting_body)

```

若要在特定查詢上測試智慧排名外掛程式，或測試某些內文和標題欄位：

Curl

```

curl -XGET "https://localhost:9200/<your-docs-index>/_search?pretty" -u
'admin:admin' --insecure -H 'Content-Type: application/json' -d'
{
  "query": {
    "multi-match": {
      "query": "intelligent systems",
      "fields": ["body_field_name_here", "title_field_name_here"]
    }
  },
  "size": 25,
  "ext": {
    "search_configuration": {
      "result_transformer": {
        "kendra_intelligent_ranking": {
          "order": 1,
          "properties": {
            "title_field": "title_field_name_here",
            "body_field": "body_field_name_here"
          }
        }
      }
    }
  }
}

```

```
    }  
  }  
}  
,
```

Python

```
from opensearchpy import OpenSearch  
host = 'localhost'  
port = 9200  
auth = ('admin', 'admin')  
  
client = OpenSearch(  
    hosts = [{'host': host, 'port': port}],  
    http_compress = True, # enables gzip compression for request bodies  
    http_auth = auth,  
    # client_cert = client_cert_path,  
    # client_key = client_key_path,  
    use_ssl = True,  
    verify_certs = False,  
    ssl_assert_hostname = False,  
    ssl_show_warn = False,  
    ca_certs = ca_certs_path  
)  
  
# Index settings null for kendra_intelligent_ranking  
  
query = {  
    "query": {  
        "multi_match": {  
            "query": "intelligent systems",  
            "fields": ["body_field_name_here", "title_field_name_here"]  
        }  
    },  
    "size": 25,  
    "ext": {  
        "search_configuration": {  
            "result_transformer": {  
                "kendra_intelligent_ranking": {  
                    "order": 1,  
                    "properties": {  
                        "title_field": "title_field_name_here",
```

```
        "body_field": "body_field_name_here"
    }
}
}
}
}

response = client.search(
    body = query,
    index = index_name
)

print('\nSearch results:')
print(response)
```

比較 OpenSearch 結果與 Amazon Kendra 結果

您可以將 side-by-side OpenSearch (自我管理) 排名結果與重新排名 Amazon Kendra 的結果進行比較。OpenSearch 儀表板 2.4.0 版及更高版本提供 side-by-side 結果，以便您可以比較文檔與如 OpenSearch 何 Amazon Kendra 或插件對搜索查詢文檔進行排名的排名。

在將排名結果與 Amazon Kendra 重新排名的結果進行比較 OpenSearch 之前，請確保您的 OpenSearch 儀表板由具有智慧排名外掛程式的 OpenSearch 伺服器提供支援。您可以使用 Docker 和快速啟動 Bash 腳本進行設置。請參閱[設定智慧型搜尋外掛程式](#)。

以下概述了如何在 OpenSearch 儀表板中比較 OpenSearch 和 Amazon Kendra 搜尋結果。如需詳細資訊，請參閱[OpenSearch 文件](#)。

比較 OpenSearch 儀表板中的搜尋結果

1. 開啟 `http://localhost:5601` 並登入 OpenSearch 儀表板。預設憑證為使用者名稱「admin」和密碼「管理員」。
2. 從導覽選單中的 OpenSearch 外掛程式中選取 [搜尋相關性]。
3. 在搜尋列中輸入搜尋文字。
4. 選取查詢 1 的索引，然後在查詢 DSL 中輸入 OpenSearch 查詢。您可以使用 `%SearchText%` 變數來參照您在搜尋列中輸入的搜尋文字。如需此查詢的範例，請參閱[OpenSearch 文件](#)。此查詢返回的結 OpenSearch 果是不使用智能排名插件的結果。

5. 為查詢 2 選取相同的索引，然後在查詢 DSL 中輸入相同的 OpenSearch 查詢。此外，包括擴展名，`kendra_intelligent_ranking`並指定強制性`body_field`的排名。您也可以指定標題欄位，但是主體欄位是必填欄位。如需此查詢的範例，請參閱[OpenSearch 文件](#)。此查詢返回的結果是使用智能排名插件 Amazon Kendra 重新排名的結果。該插件最多排名 25 結果。
6. 選取「搜尋」以傳回並比較結果。

語義上對搜索服務的結果進行排名

Amazon Kendra 智能排名使用 Amazon Kendra 的語義搜索功能來重新排名搜索服務的結果。它會考慮到搜尋查詢的前後關聯，以及搜尋服務文件中的所有可用資訊來達成此目的。Amazon Kendra 智能排名可以改善簡單的關鍵字匹配。

[CreateRescoreExecutionPlan](#) API 會建立用於佈建 [重新分數](#) API 的 Amazon Kendra 智慧排名資源。Rescore API 會重新排列搜尋服務的搜尋結果，例如 [OpenSearch \(自我管理\)](#)。

打電話時 [CreateRescoreExecutionPlan](#)，您可以設定所需的容量單位，以重新排名搜尋服務的結果。如果您不需要超出單一單位預設值的更多容量單位，請勿變更預設值。僅提供重新評分執行計劃的名稱。您最多可以設置 1000 個額外單位。如需單一容量單位所包含項目的資訊，請參閱 [調整容量](#)。佈建 Amazon Kendra 智慧排名後，系統會根據您設定的容量單位，每小時向您收取費用。請參閱 [免費方案和定價資訊](#)。

重新評分執行計劃 ID 會產生，並在您呼叫 [CreateRescoreExecutionPlan](#) 時傳回回應中。Rescore API 會使用重新評分執行計畫 ID，使用您設定的容量來重新排名搜尋服務的結果。您可以在搜尋服務的組態檔案中包含重新評分執行計畫 ID。例如，如果您使用 [OpenSearch \(自我管理\)](#)，您可以將重新評分執行計畫識別碼納入您的碼頭組成 `.yaml` 或 `opensearch.yaml` 檔案中 — 請參閱 [智慧排名 \(自助服務\) 結果](#)。 [OpenSearch](#)

當您調用 [CreateRescoreExecutionPlan](#) 用 Amazon 資源名稱 (ARN) 也會在響應中生成。您可以使用此 ARN 在 AWS Identity and Access Management (IAM) 中建立權限原則，以限制使用者對特定重新評分執行計畫之特定 ARN 的存取。如需授與針對特定重新評分執行計畫使用 Rescore API 之權限的 IAM 原則範例，請參閱 [自我 OpenSearch 管理的 Amazon Kendra 智慧排名](#)。

以下是建立容量單位設為 1 的重新評分執行計畫的範例。

CLI

```
aws kendra-ranking create-rescore-execution-plan \
  --name MyRescoreExecutionPlan \
  --capacity-units '{"RescoreCapacityUnits":1}'
```

Response:

```
{
  "Id": "<rescore execution plan ID>",
  "Arn": "arn:aws:kendra-ranking:<region>:<account-id>:rescore-execution-plan/
<rescore-execution-plan-id>"
}
```

Python

```
import boto3
from botocore.exceptions import ClientError
import pprint
import time

kendra_ranking = boto3.client("kendra-ranking")

print("Create a rescore execution plan.")

# Provide a name for the rescore execution plan
name = "MyRescoreExecutionPlan"
# Set your required additional capacity units
# Don't set capacity units if you don't require more than 1 unit given by default
capacity_units = 1

try:
    rescore_execution_plan_response = kendra_ranking.create_rescore_execution_plan(
        Name = name,
        CapacityUnits = {"RescoreCapacityUnits":capacity_units}
    )

    pprint.pprint(rescore_execution_plan_response)

    rescore_execution_plan_id = rescore_execution_plan_response["Id"]

    print("Wait for Amazon Kendra to create the rescore execution plan.")

    while True:
        # Get the details of the rescore execution plan, such as the status
        rescore_execution_plan_description =
kendra_ranking.describe_rescore_execution_plan(
            Id = rescore_execution_plan_id
```



```
    )
    # When status is not CREATING quit.
    status = rescore_execution_plan_description["Status"]
    print(" Creating rescore execution plan. Status: "+status)
    time.sleep(60)
    if status != "CREATING":
        break

except ClientError as e:
    print("%s" % e)

print("Program ends.")
```

Java

```
import java.util.concurrent.TimeUnit;

import software.amazon.awssdk.services.kendraranking.KendraRankingClient;
import
    software.amazon.awssdk.services.kendraranking.model.CapacityUnitsConfiguration;
import
    software.amazon.awssdk.services.kendraranking.model.CreateRescoreExecutionPlanRequest;
import
    software.amazon.awssdk.services.kendraranking.model.CreateRescoreExecutionPlanResponse;
import
    software.amazon.awssdk.services.kendraranking.model.DescribeRescoreExecutionPlanRequest;
import
    software.amazon.awssdk.services.kendraranking.model.DescribeRescoreExecutionPlanResponse;
import
    software.amazon.awssdk.services.kendraranking.model.RescoreExecutionPlanStatus;

public class CreateRescoreExecutionPlanExample {

    public static void main(String[] args) throws InterruptedException {

        String rescoreExecutionPlanName = "MyRescoreExecutionPlan";
        int capacityUnits = 1;

        KendraRankingClient kendraRankingClient = KendraRankingClient.builder().build();

        System.out.println(String.format("Creating a rescore execution plan named %s",
            rescoreExecutionPlanName));
```

```

    CreateRescoreExecutionPlanResponse createResponse =
kendraRankingClient.createRescoreExecutionPlan(
    CreateRescoreExecutionPlanRequest.builder()
        .name(rescoreExecutionPlanName)
        .capacityUnits(
            CapacityUnitsConfiguration.builder()
                .rescoreCapacityUnits(capacityUnits)
                .build()
        )
        .build()
    );

    String rescoreExecutionPlanId = createResponse.id();
    System.out.println(String.format("Waiting for rescore execution plan with id %s
to finish creating.", rescoreExecutionPlanId));
    while (true) {
        DescribeRescoreExecutionPlanResponse describeResponse =
kendraRankingClient.describeRescoreExecutionPlan(
            DescribeRescoreExecutionPlanRequest.builder()
                .id(rescoreExecutionPlanId)
                .build()
        );
        RescoreExecutionPlanStatus rescoreExecutionPlanStatus =
describeResponse.status();
        if (rescoreExecutionPlanStatus != RescoreExecutionPlanStatus.CREATING) {
            break;
        }
        TimeUnit.SECONDS.sleep(60);
    }

    System.out.println("Rescore execution plan creation is complete.");
}
}

```

以下是更新重新評分執行計畫以將容量單位設定為 2 的範例。

CLI

```

aws kendra-ranking update-rescore-execution-plan \
  --id <rescore execution plan ID> \
  --capacity-units '{"RescoreCapacityUnits":2}'

```

Python

```
import boto3
from botocore.exceptions import ClientError
import pprint
import time

kendra_ranking = boto3.client("kendra-ranking")

print("Update a rescore execution plan.")

# Provide the ID of the rescore execution plan
id = <rescore execution plan ID>
# Re-set your required additional capacity units
capacity_units = 2

try:
    kendra_ranking.update_rescore_execution_plan(
        Id = id,
        CapacityUnits = {"RescoreCapacityUnits":capacity_units}
    )

    print("Wait for Amazon Kendra to update the rescore execution plan.")

    while True:
        # Get the details of the rescore execution plan, such as the status
        rescore_execution_plan_description =
kendra_ranking.describe_rescore_execution_plan(
            Id = id
        )
        # When status is not UPDATING quit.
        status = rescore_execution_plan_description["Status"]
        print(" Updating rescore execution plan. Status: "+status)
        time.sleep(60)
        if status != "UPDATING":
            break

except ClientError as e:
    print("%s" % e)

print("Program ends.")
```

Java

```
import java.util.concurrent.TimeUnit;

import software.amazon.awssdk.services.kendraranking.KendraRankingClient;
import
    software.amazon.awssdk.services.kendraranking.model.CapacityUnitsConfiguration;
import
    software.amazon.awssdk.services.kendraranking.model.DescribeRescoreExecutionPlanRequest;
import
    software.amazon.awssdk.services.kendraranking.model.DescribeRescoreExecutionPlanResponse;
import
    software.amazon.awssdk.services.kendraranking.model.RescoreExecutionPlanStatus;
import
    software.amazon.awssdk.services.kendraranking.model.UpdateRescoreExecutionPlanRequest;
import
    software.amazon.awssdk.services.kendraranking.model.UpdateRescoreExecutionPlanResponse;

public class UpdateRescoreExecutionPlanExample {

    public static void main(String[] args) throws InterruptedException {

        String rescoreExecutionPlanId = <rescore execution plan ID>;
        int newCapacityUnits = 2;

        KendraRankingClient kendraRankingClient = KendraRankingClient.builder().build();

        System.out.println(String.format("Updating a rescore execution plan named %s",
            rescoreExecutionPlanId));

        UpdateRescoreExecutionPlanResponse updateResponse =
            kendraRankingClient.updateRescoreExecutionPlan(
                UpdateRescoreExecutionPlanRequest.builder()
                    .id(rescoreExecutionPlanId)
                    .capacityUnits(
                        CapacityUnitsConfiguration.builder()
                            .rescoreCapacityUnits(newCapacityUnits)
                            .build()
                    )
                    .build()
            );

        System.out.println(String.format("Waiting for rescore execution plan with id %s
            to finish updating.", rescoreExecutionPlanId));
```

```

while (true) {
    DescribeRescoreExecutionPlanResponse describeResponse =
kendraRankingClient.describeRescoreExecutionPlan(
        DescribeRescoreExecutionPlanRequest.builder()
            .id(rescoreExecutionPlanId)
            .build()
    );
    RescoreExecutionPlanStatus rescoreExecutionPlanStatus =
describeResponse.status();
    if (rescoreExecutionPlanStatus != RescoreExecutionPlanStatus.UPDATING) {
        break;
    }
    TimeUnit.SECONDS.sleep(60);
}

System.out.println("Rescore execution plan update is complete.");
}
}

```

以下是使用 Rescore API 的範例。

CLI

```

aws kendra-ranking rescore \
  --rescore-execution-plan-id <rescore execution plan ID> \
  --search-query "intelligent systems" \
  --documents "[{"Id": "DocId1", "Title": "Smart systems", "Body":
  "intelligent systems in everyday life", "OriginalScore": 2.0}, {"Id":
  "DocId2", "Title": "Smarter systems", "Body": "living with intelligent
  systems", "OriginalScore": 1.0}]"

```

Python

```

import boto3
from botocore.exceptions import ClientError
import pprint

kendra_ranking = boto3.client("kendra-ranking")

print("Use the Rescore API.")

# Provide the ID of the rescore execution plan

```

```
id = <rescore execution plan ID>
# The search query from the search service
query = "intelligent systems"
# The list of documents for Intelligent Ranking to rescore
document_list = [
    {"Id": "DocId1", "Title": "Smart systems", "Body": "intelligent systems in
everyday life", "OriginalScore": 2.0},
    {"Id": "DocId2", "Title": "Smarter systems", "Body": "living with intelligent
systems", "OriginalScore": 1.0}
]

try:
    rescore_response = kendra_ranking.rescore(
        rescore_execution_plan_id = id,
        search_query = query,
        documents = document_list
    )

    print(rescore_response["RescoreId"])
    print(rescore_resposne["ResultItems"])

except ClientError as e:
    print("%s" % e)

print("Program ends.")
```

Java

```
import java.util.ArrayList;
import java.util.List;

import software.amazon.awssdk.services.kendraranking.KendraRankingClient;
import software.amazon.awssdk.services.kendraranking.model.RescoreRequest;
import software.amazon.awssdk.services.kendraranking.model.RescoreResponse;
import software.amazon.awssdk.services.kendraranking.model.Document;

public class RescoreExample {

    public static void main(String[] args) {

        String rescoreExecutionPlanId = <rescore execution plan ID>;
        String query = "intelligent systems";
```

```
List<Document> documentList = new ArrayList<>();
documentList.add(
    Document.builder()
        .id("DocId1")
        .originalScore(2.0F)
        .body("intelligent systems in everyday life")
        .title("Smart systems")
        .build()
);
documentList.add(
    Document.builder()
        .id("DocId2")
        .originalScore(1.0F)
        .body("living with intelligent systems")
        .title("Smarter systems")
        .build()
);

KendraRankingClient kendraRankingClient = KendraRankingClient.builder().build();

RescoreResponse rescoreResponse = kendraRankingClient.rescore(
    RescoreRequest.builder()
        .rescoreExecutionPlanId(rescoreExecutionPlanId)
        .searchQuery(query)
        .documents(documentList)
        .build()
);

System.out.println(rescoreResponse.rescoreId());
System.out.println(rescoreResponse.resultItems());
}
}
```

的文件歷史記錄 Amazon Kendra

- 最新文件更新：2024 年 2 月 27 日

下表說明每個發行版本中的重要變更 Amazon Kendra。如需有關此文件更新的通知，您可以訂閱 [RSS 摘要](#)。

變更	描述	日期
新功能	Amazon Kendra 現在支援資 GitHub 料來源連接器的更新 版本。如需詳細資訊，請參 閱 GitHub 。	2024年2月27日
新功能	Amazon Kendra 現在支援資 Amazon FSx 料來源連接器的 更新版本。如需詳細資訊， 請參閱 Amazon FSx (視窗) 和 Amazon FSx (NetAppON TAP) 。	2024年2月8日
新功能	Amazon Kendra 現在支援 Slack 資料來源連接器的更新 版本。如需詳細資訊，請參閱 Slack 。	2024年1月11日
新功能	Amazon Kendra 現在支持折疊 和擴展您的搜索結果。如需詳 細資訊，請參閱 縮疊/展開搜尋 結果 。	2023 年 10 月 19 日
新功能	Amazon Kendra 現在支援 Aurora (MySQL) 資料來源連 接器。如需詳細資訊，請參閱 Aurora (MySQL) 。	2023 年 9 月 28 日

新功能	Amazon Kendra 現在支援 Aurora (PostgreSQL) 資料來源連接器。如需詳細資訊，請參閱 Aurora (PostgreSQL) 。	2023 年 9 月 28 日
新功能	Amazon Kendra 現在支援 Amazon RDS (MySQL) 資料來源連接器。如需詳細資訊，請參閱 Amazon RDS (MySQL) 。	2023 年 9 月 28 日
新功能	Amazon Kendra 現在支援 Amazon RDS (Microsoft SQL 伺服器) 資料來源連接器。如需詳細資訊，請參閱 Amazon RDS (Microsoft SQL 伺服器) 。	2023 年 9 月 28 日
新功能	Amazon Kendra 現在支援 Amazon RDS (Oracle) 資料來源連接器。如需詳細資訊，請參閱 Amazon RDS (Oracle) 。	2023 年 9 月 28 日
新功能	Amazon Kendra 現在支援 Amazon RDS (PostgreSQL) 資料來源連接器。如需詳細資訊，請參閱 Amazon RDS (PostgreSQL) 。	2023 年 9 月 28 日
新功能	Amazon Kendra 現在支援 IBM DB2 資料來源連接器。如需詳細資訊，請參閱 IBM DB2 。	2023 年 9 月 28 日
新功能	Amazon Kendra 現在支援 Microsoft SQL 伺服器資料來源連接器。如需詳細資訊，請參閱 Microsoft SQL 伺服器 。	2023 年 9 月 28 日

新功能	Amazon Kendra 現在支援 MySQL 資料來源連接器。如需詳細資訊，請參閱 MySQL 。	2023 年 9 月 28 日
新功能	Amazon Kendra 現在支援「Oracle 資料庫」資料來源連接器。如需詳細資訊，請參閱 Oracle 資料庫 。	2023 年 9 月 28 日
新功能	Amazon Kendra 現在支援 PostgreSQL 資料來源連接器。如需詳細資訊，請參閱 PostgreSQL 。	2023 年 9 月 28 日
新功能	Amazon Kendra 現在為 Drupal 提供了一個數據源連接器。如需詳細資訊，請參閱 Drupal 。	2023 年 9 月 6 日
新功能	使用擷取 API Amazon Kendra 擷取擴增產生 (RAG) 系統 的語義相關段落。	2023 年 6 月 22 日
新功能	Amazon Kendra 現在支援 Amazon Kendra Web 爬行者程式資料來源連接器的更新版本。如需詳細資訊，請參閱 Amazon Kendra 網路爬行者程式 2.0 版 。	2023 年 6 月 21 日
區域擴展	Amazon Kendra 現已在歐洲 (倫敦) (歐洲-西部 -2) 推出。	2023 年 6 月 5 日
新功能	Amazon Kendra 現在支援 Alfresco 資料來源連接器的更新版本。如需詳細資訊，請參閱 露天 。	2023 年 5 月 16 日

新功能	Amazon Kendra 現在為 Adobe 體驗管理員提供資料來源連接器。如需詳細資訊，請參閱 Adobe 體驗管理員 。	2023 年 5 月 11 日
新功能	Amazon Kendra 現在支援在您呼叫時設定文件欄位/屬性。 GetQuerySuggestions 您現在可以根據文件欄位的內容進行查詢建議。如需詳細資訊，請參閱 查詢建議 。	2023 年 5 月 2 日
新功能	Amazon Kendra 現在提供 Gmail 的資料來源連接器。如需詳細資訊，請參閱 Gmail 。	2023 年 4 月 13 日
新功能	Amazon Kendra 現在支援 Microsoft OneDrive 資料來源連接器的更新版本。如需詳細資訊，請參閱 Microsoft OneDrive 2.0 版 。	2023 年 4 月 3 日
新功能	當您的使用者使用精選 結果輸入特定查詢時 ，改善新文件的 可見度或宣傳特定文件 。	2023 年 3 月 30 日
新功能	Amazon Kendra 現在支援 Microsoft 的更新資料來源連接器 SharePoint。如需詳細資訊，請參閱 Microsoft SharePoint 。	2023 年 3 月 2 日
新功能	Amazon Kendra 現在支援匯流資料來源連接器的更新版本。若要取得更多資訊，請參閱 〈匯合〉 。	2023 年 3 月 1 日

區域擴展	Amazon Kendra 現已於亞太區域 (東京) (ap-東北-1) 推出。	2023 年 2 月 7 日
新功能	Amazon Kendra 現在為 Microsoft 交換提供資料來源連接器。如需詳細資訊，請參閱 Microsoft 交換 。	2023 年 1 月 12 日
新功能	Amazon Kendra 現在為 Microsoft Yammer 提供資料來源連接器。如需詳細資訊，請參閱 Microsoft Yammer 。	2023 年 1 月 12 日
新功能	Amazon Kendra 現在支援建立 RTF、XML、XSLT、MS_EXCEL、CSV、JSON 和 MD 文件類型的索引。如需詳細資訊，請參閱 文件類型 。	2023 年 1 月 11 日
新功能	Amazon Kendra 現在支援 Amazon S3 料來源連接器的更新版本。如需詳細資訊，請參閱 Amazon S3 。	2023 年 1 月 10 日
新功能	OpenSearch (自我管理) 搜索結果可以使用 Amazon Kendra 智能排名進行語義排名 。	2023 年 1 月 9 日
新功能	Amazon Kendra 現在為 Microsoft 團隊提供資料來源連接器。如需詳細資訊，請參閱 Microsoft 團隊 。	2023 年 1 月 5 日
新功能	Amazon Kendra 具有用於 Google 雲端硬碟的更新數據源連接器。如需詳細資訊，請參閱 Google 雲端硬碟 。	2023 年 1 月 5 日

新功能	Amazon Kendra 具有的更新資料來源連接器 ServiceNow。如需詳細資訊，請參閱 ServiceNow 。	2022 年 12 月 21 日
新功能	Amazon Kendra 具有適用於 Salesforce 的更新資料來源連接器。如需詳細資訊，請參閱 銷售力量 。	2022 年 12 月 21 日
區域擴展	Amazon Kendra 現已於亞太區域 (孟買) (AI-南 -1) 推出。	2022 年 12 月 14 日
新功能	Amazon Kendra 的 表格搜索功能 可以從嵌入在 HTML 文檔中的表中搜索和提取答案。	2022 年 11 月 27 日
新功能	Amazon Kendra 支持 語義搜索一組選擇的語言 。	2022 年 11 月 27 日
新功能	Amazon Kendra 現在為 Dropbox 提供了一個數據源連接器。如需詳細資訊，請參閱 Dropbox 。	2022 年 9 月 27 日
新功能	Amazon Kendra 現在為 Zendesk 提供了一個資料來源連接器。如需詳細資訊，請參閱 Zendesk 。	2022 年 8 月 17 日
新功能	文件層級存取控制現在可以在編製文件索引之後重新設定。如需詳細資訊，請參閱 存取控制組態 。	2022 年 7 月 14 日
新功能	Amazon Kendra 現在為露天提供資料來源連接器。如需詳細資訊，請參閱 露天 。	2022 年 6 月 30 日

新功能	Amazon Kendra 現在提供的資料來源連接器 GitHub。如需詳細資訊，請參閱 GitHub 。	2022 年 6 月 2 日
新功能	Amazon Kendra 現在提供 Jira 的資料來源連接器。如需詳細資訊，請參閱 Jira 。	2022 年 5 月 12 日
新功能	多面內的巢狀多面可以顯示在搜尋結果中。如需詳細資訊，請參閱 剖面 。	2022 年 5 月 5 日
新功能	Amazon Kendra 現在提供 Quip 的資料來源連接器。如需詳細資訊，請參閱 Quip 。	2022 年 4 月 19 日
新功能	Amazon Kendra 現在提供 Box 的資料來源連接器。如需詳細資訊，請參閱 Box 。	2022 年 4 月 6 日
新功能	Amazon Kendra 現在提供 Slack 的資料來源連接器。如需詳細資訊，請參閱 Slack 。	2022 年 3 月 14 日
新功能	Amazon Kendra 現在提供的資料來源連接器 Amazon FSx。如需詳細資訊，請參閱 Amazon FSx 。	2022 年 2 月 8 日
AWS 受管策略更新-新策略	Amazon Kendra 增加了新的 AWS 受管理策略。如需詳細資訊，請參閱的 AWS 受管理政策 Amazon Kendra 。	2022 年 1 月 3 日

新功能	Amazon Kendra 搜索應用程式可以在點擊幾下，而無需任何前端代碼進行部署。如需詳細資訊，請參閱 部署不含程式碼的搜尋應用程式 。	2021 年 12 月 1 日
新功能	在文件擷取過程中，可以豐富文件中繼資料和內容。如需詳細資訊，請參閱 在擷取過程中自訂文件中繼資料 。	2021 年 12 月 1 日
新功能	Amazon Kendra 提供搜尋分析，以取得搜尋應用程式的實用見解。如需詳細資訊，請參閱 透過搜尋分析取得深入分析 。	2021 年 12 月 1 日
區域擴展	Amazon Kendra 目前可在 AWS GovCloud (美國西部) (us-gov-west-1) 中使用。	2021 年 10 月 13 日
新功能	Amazon Kendra 現在可以索引多種語言的文件，並依語言篩選搜尋結果。請參閱以 英文以外的語言新增文件 和以 語言搜尋 。	2021 年 10 月 7 日
新功能	Amazon Kendra 現在與 Identity Center 目錄整合，以擷取群組和使用者的存取層級以進行 使用者內容篩選 。請參閱 IAM 身分中心的使用者群組組態 。	2021 年 10 月 6 日

新增教學	Amazon Kendra 現在提供教學課程，逐步引導您如何建立豐富中繼資料的搜尋解決方案。請參閱 建置智慧型搜尋解決方案 。	2021 年 8 月 13 日
新功能	Amazon Kendra 現在提供的資料來源連接器 Amazon WorkDocs。如需詳細資訊，請參閱 Amazon WorkDocs 。	2021 年 7 月 20 日
新功能	Amazon Kendra 現在提供了一個用於爬網和索引網頁的 Web 爬蟲。如需詳細資訊，請參閱 網路爬行者程式 。	2021 年 6 月 17 日
區域擴展	Amazon Kendra 現已在加拿大 (中部) (CA-中央 -1) 推出。	2021 年 6 月 16 日
區域擴展	Amazon Kendra 現已在美國東部 (俄亥俄州) (us-east-2) 推出。	2021 年 6 月 7 日
新功能	Amazon Kendra 現在支援查詢建議，建議使用者與其搜尋相關的熱門查詢。如需詳細資訊，請參閱 建議熱門搜尋查詢 。	2021 年 5 月 27 日
AWS 受管策略更新-新策略	Amazon Kendra 增加了新的 AWS 受管理策略。如需詳細資訊，請參閱的 AWS 受管理政策 Amazon Kendra 。	2021 年 5 月 27 日
區域擴展	Amazon Kendra 現已於亞太區域 (新加坡) (ap-東南 -1) 推出。	2021 年 5 月 5 日

新功能	Amazon Kendra 現在支援透過覆寫索引層級設定的調整組態來調整查詢中的搜尋相關性。如需詳細資訊，請參閱 調整搜尋相關性 和 調整回應 。	2021 年 4 月 20 日
新功能	Amazon Kendra 現在支援 OAuth 2.0 驗證，並使用 ServiceNow 查詢來選取要編製索引的文件。如需詳細資訊，請參閱 ServiceNow 。	2021 年 4 月 1 日
新功能	Amazon Kendra 現在支援常見問題集文件的增量學習。如需詳細資訊，請參閱 提交漸進式學習的意見反應 。	2021 年 2 月 17 日
新功能	Amazon Kendra 現在支援索引同義字。如需詳細資訊，請參閱 將同義字新增至索引 。	2020 年 12 月 10 日
新功能	Amazon Kendra 現在為 Google 工作區驅動器提供了一個數據庫連接器。如需詳細資訊，請參閱 使用 Google Workspace Drive 資料來源 。	2020 年 12 月 8 日
新功能	Amazon Kendra 現在提供了一個 JavaScript 資源庫，可讓您更輕鬆地向其提供查詢回饋 Amazon Kendra。如需詳細資訊，請參閱 提交意見反應 。	2020 年 12 月 8 日
新功能	Amazon Kendra 現在支援以權杖為基礎的使用者存取控制。如需詳細資訊，請參閱 控制索引中文件的存取 。	2020 年 11 月 5 日

新功能	Amazon Kendra 匯流數據源連接器現在可以與匯流雲工作。如需詳細資訊，請參閱 使用 Confluence 資料來源 。	2020 年 11 月 5 日
區域擴展	Amazon Kendra 現已於亞太區域 (雪梨) (ap-東南-2) 推出。	2020 年 11 月 2 日
新功能	Amazon Kendra 現在為匯流伺服器提供資料來源連接器。如需詳細資訊，請參閱 使用 Confluence 資料來源 。	2020 年 10 月 26 日
新功能	Amazon Kendra 現在提供可用於產生自訂連接器統計資料的資料來源。有關詳情，請參閱 使用自訂資料來源 。	2020 年 10 月 21 日
新功能	Amazon Kendra 現在支援常見問題集的自訂屬性。如需詳細資訊，請參閱 新增問題和答案 。	2020 年 9 月 17 日
新功能	Amazon Kendra 現在會傳回查詢結果的可信度分數。如需詳細資訊，請參閱 QueryResultItem 。	2020 年 9 月 15 日
新功能	AWS CloudFormation 現在支持 Amazon Kendra。如需詳細資訊，請參閱 Amazon Kendra 資源類型參考- AWS CloudFormation 。	2020 年 9 月 10 日

新功能

Amazon Kendra 增加了對 AWS PrivateLink。如需詳細資訊，請參閱 [Amazon Kendra 和介面 VPC 端點 \(AWS PrivateLink\)](#)。

2020 年 7 月 7 日

新的指南

這是《Amazon Kendra 開發人員指南》的第一版。

2020 年 5 月 11 日

API 參考

[API 參考文檔](#)現在是一個單獨的指南。

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。