aws

Panduan Developer

Amazon Kendra

Amazon Kendra: Panduan Developer

Table of Contents

Apakah Amazon Kendra itu?

Amazon Kendraadalah layanan pencarian cerdas yang menggunakan pemrosesan bahasa alami dan algoritma pembelajaran mesin canggih untuk mengembalikan jawaban spesifik untuk mencari pertanyaan dari data Anda.

Tidak seperti pencarian berbasis kata kunci tradisional, Amazon Kendra menggunakan kemampuan pemahaman semantik dan kontekstual untuk memutuskan apakah dokumen relevan dengan permintaan pencarian. Amazon Kendra mengembalikan jawaban spesifik atas pertanyaan, menghadirkan sebuah pengalaman interaksi yang mendekati seorang ahli.

> **Note**
>
> Anda juga dapat menggunakan Amazon Kendra kemampuan pencarian semantik untuk memberi peringkat ulang hasil layanan pencarian lain. Lihat Peringkat Amazon Kendra Cerdas untuk detail selengkapnya.

DenganAmazon Kendra, Anda dapat membuat pengalaman pencarian terpadu dengan menghubungkan beberapa repositori data ke indeks dan menelan dan merangkak dokumen. Anda dapat menggunakan metadata dokumen untuk membuat pengalaman pencarian yang kaya fitur dan disesuaikan untuk pengguna Anda, membantu mereka menemukan jawaban yang tepat untuk kueri mereka secara efisien.

Apa itu Amazon Kendra?

Mengkueri Amazon Kendra

Anda dapat Amazon Kendra menanyakan jenis kueri berikut:

Pertanyaan factoid —Sederhana siapa, apa, kapan, atau di mana pertanyaan, seperti Di mana pusat layanan terdekat ke Seattle? Pertanyaan factoid memiliki jawaban berdasarkan fakta yang dapat dikembalikan sebagai satu kata atau frasa. Jawabannya diambil dari FAQ atau dari dokumen Anda yang diindeks.

Pertanyaan deskriptif —Pertanyaan di mana jawabannya bisa berupa kalimat, bagian, atau keseluruhan dokumen. Misalnya, Bagaimana cara menghubungkan Echo Plus saya ke jaringan saya? Atau, Bagaimana cara mendapatkan manfaat pajak untuk keluarga berpenghasilan rendah?

Pertanyaan kata kunci dan bahasa alami —Pertanyaan yang mencakup konten percakapan yang kompleks di mana maknanya mungkin tidak jelas. Misalnya, alamat keynote. Ketika Amazon Kendra menemukan kata seperti “alamat”, yang memiliki beberapa makna kontekstual, itu benar menyimpulkan makna di balik permintaan pencarian dan mengembalikan informasi yang relevan.

Manfaat dari Amazon Kendra

Amazon Kendrasangat terukur, mampu memenuhi tuntutan kinerja, terintegrasi erat dengan AWS layanan lain seperti Amazon S3dan Amazon Lex, dan menawarkan keamanan tingkat perusahaan. Beberapa manfaat menggunakan Amazon Kendra meliputi:

Simplicity — Amazon Kendra menyediakan konsol dan API untuk mengelola dokumen yang ingin Anda cari. Anda dapat menggunakan API pencarian sederhana untuk mengintegrasikan Amazon Kendra ke dalam aplikasi klien Anda, seperti situs web atau aplikasi seluler.

Konektivitas — Amazon Kendra dapat terhubung ke repositori data pihak ketiga atau sumber data seperti Microsoft. SharePoint Anda dapat dengan mudah mengindeks dan mencari dokumen Anda menggunakan sumber data Anda.

Akurasi —Tidak seperti layanan pencarian tradisional yang menggunakan pencarian kata kunci, Amazon Kendra mencoba memahami konteks pertanyaan dan mengembalikan kata, cuplikan, atau dokumen yang paling relevan untuk kueri Anda. Amazon Kendramenggunakan pembelajaran mesin untuk meningkatkan hasil pencarian dari waktu ke waktu.

Keamanan - Amazon Kendra memberikan pengalaman pencarian perusahaan yang sangat aman. Hasil pencarian Anda mencerminkan model keamanan organisasi Anda dan dapat difilter berdasarkan akses pengguna atau grup ke dokumen. Pelanggan bertanggung jawab untuk mengautentikasi dan mengotorisasi akses pengguna.

Amazon KendraEdisi

Amazon Kendramemiliki dua versi: Developer Edition dan Enterprise Edition. Tabel berikut menguraikan fitur mereka dan perbedaan antara keduanya.

Amazon KendraEdisi Pengembang

Amazon KendraDeveloper Edition menyediakan semua fitur dengan Amazon Kendra biaya lebih rendah.

Kasus penggunaan yang ideal

- Menjelajahi bagaimana Amazon Kendra mengindeks dokumen Anda
- Mencoba fitur
- Mengembangkan aplikasi yang menggunakan Amazon Kendra

Fitur

- Tingkat gratis dengan 750 jam penggunaan disertakan
- Hingga 5 indeks dengan hingga 5 sumber data masing-masing
- 10.000 dokumen atau 3 GB teks yang diekstraksi
- Sekitar 4.000 kueri per hari atau 0,05 kueri per detik
- Berjalan di 1 Availability Zone (AZ) —lihat Availability Zone (pusat data di AWS wilayah)

Keterbatasan

- Bukan untuk aplikasi produksi
- Tidak ada jaminan latensi atau ketersediaan

Amazon KendraEdisi Perusahaan

Amazon KendraEnterprise Edition menyediakan semua fitur Amazon Kendra dan dirancang untuk konteks produksi.

Kasus penggunaan yang ideal

- Mengindeks seluruh pustaka dokumen perusahaan Anda
- Menerapkan aplikasi Anda di lingkungan produksi

Fitur

- Hingga 5 indeks dengan hingga 50 sumber data masing-masing
- 100.000 dokumen atau 30 GB teks yang diekstraksi
- Sekitar 8.000 kueri per hari atau 0,1 kueri per detik
- Berjalan di 3 Availability Zone (AZ) —lihat Availability Zone (pusat data di AWS wilayah)

> **Note**
>
> Anda dapat meningkatkan kuota ini menggunakan Konsol Service Quotas.

Keterbatasan

- Tidak ada

> **Note**
>
> Untuk daftar wilayah, titik akhir, dan kuota layanan yang didukung olehAmazon Kendra, lihat Amazon Kendratitik akhir dan kuota.

Harga untuk Amazon Kendra

Anda dapat memulai secara gratis dengan Amazon Kendra Developer Edition yang menyediakan penggunaan hingga 750 jam untuk 30 hari pertama.

Setelah uji coba berakhir, Anda dikenai biaya untuk semua indeks yang disediakan, meskipun Amazon Kendra indeks kosong dan tidak ada kueri yang dijalankan. Setelah uji coba berakhir, ada biaya tambahan untuk memindai dan menyinkronkan dokumen menggunakan sumber data. Amazon Kendra

Untuk daftar lengkap biaya dan harga, lihat Amazon Kendraharga.

Apakah Anda pengguna Amazon Kendra baru?

Jika Anda adalah pengguna pertama kaliAmazon Kendra, kami sarankan Anda membaca bagian berikut secara berurutan:

1	2	3	4	5	6
Cara kerja Amazon Kendra	Memulai	Membuat indeks	Menambahkan dokumen langsung ke indeks dengan batch upload	Membuat konektor sumber data	Mencari indeks
Memperkenalkan Amazon Kendra komponen dan	Menjelaskan cara menyiapkan akun Anda dan menguji API Amazon	Menjelaskan cara menggunakan Amazon Kendra untuk membuat	Menjelaskan cara menambahkan dokumen langsung ke Amazon	Menjelaskan cara menambahkan dokumen dari repositori data Anda ke	Menjelaskan cara menggunakan API Amazon Kendra

1	2	3	4	5	6
Cara kerja Amazon Kendra	Memulai	Membuat indeks	Menambahkan dokumen langsung ke indeks dengan batch upload	Membuat konektor sumber data	Mencari indeks
menjelaskan cara Anda menggunakannya untuk membuat solusi pencarian.	Kendra pencarian.	indeks pencarian dan menambahkan sumber data untuk menyinkronkan dokumen Anda.	Kendra indeks.	indeksAmazon Kendra.	pencarian untuk mencari indeks.

Cara kerja Amazon Kendra

Amazon Kendra menyediakan fungsionalitas pencarian untuk aplikasi Anda. Ini mengindeks dokumen Anda secara langsung atau dari repositori dokumen pihak ketiga Anda dan secara cerdas menyajikan informasi yang relevan kepada pengguna Anda. Anda dapat menggunakan Amazon Kendra untuk membuat indeks dokumen yang dapat diperbarui dari berbagai jenis. Untuk daftar jenis dokumen yang didukung oleh Amazon Kendra lihat Jenis dokumen.

Amazon Kendra terintegrasi dengan layanan lain. Misalnya, Anda dapat mengaktifkan bot Amazon Lex obrolan dengan Amazon Kendra pencarian untuk memberikan jawaban yang berguna atas pertanyaan pengguna. Anda dapat menggunakan Amazon Simple Storage Service bucket sebagai sumber data Amazon Kendra untuk menghubungkan dan mengindeks dokumen Anda. Dan Anda dapat mengatur kebijakan akses atau izin ke sumber daya menggunakan AWS Identity and Access Management.

Amazon Kendra memiliki komponen-komponen berikut:

- Indeks yang menyimpan dokumen Anda dan membuatnya dapat dicari.
- Sumber data yang menyimpan dokumen Anda dan Amazon Kendra terhubung ke. Anda dapat secara otomatis menyinkronkan sumber data dengan Amazon Kendra indeks sehingga indeks Anda tetap diperbarui dengan repositori sumber Anda.
- API penambahan dokumen yang menambahkan dokumen langsung ke indeks.

Anda dapat menggunakan Amazon Kendra melalui konsol atau API. Anda dapat membuat, memperbarui, dan menghapus indeks. Menghapus indeks akan menghapus semua konektor sumber datanya dan secara permanen menghapus semua informasi dokumen Anda. Amazon Kendra

Topik

- Indeks
- Dokumen
- Sumber data
- Kueri
- Tag

Indeks

Indeks menyimpan isi dokumen Anda dan disusun sedemikian rupa untuk membuat dokumen dapat dicari. Cara Anda menambahkan dokumen ke indeks tergantung pada bagaimana Anda menyimpan dokumen Anda.

- Jika Anda menyimpan dokumen di beberapa jenis repositori, seperti Amazon S3 bucket atau SharePoint situs Microsoft, Anda menggunakan konektor sumber data untuk mengindeks dokumen Anda dari repositori Anda.
- Jika Anda tidak menyimpan dokumen Anda dalam repositori, Anda menggunakan BatchPutDocumentAPI untuk langsung mengindeks dokumen Anda.
- Untuk pertanyaan dan jawaban FAQ, yang harus disimpan dalam bucket Amazon Kendra (Amazon S3), Anda mengunggahnya dari bucket

Anda dapat membuat indeks dengan Amazon Kendra konsol, SDK AWS CLI, atau AWS SDK. Untuk informasi tentang jenis dokumen yang dapat diindeks, lihat Jenis dokumen.

Menggunakan bidang dokumen yang Amazon Kendra dicadangkan atau umum

Dengan UpdateIndex API, Anda dapat membuat kolom cadangan atau umum menggunakan `DocumentMetadataConfigurationUpdates` dan menentukan nama bidang indeks Amazon Kendra cadangan untuk dipetakan ke atribut/nama bidang dokumen yang setara. Anda juga dapat membuat bidang khusus. Jika Anda menggunakan konektor sumber data, sebagian besar menyertakan pemetaan bidang yang memetakan bidang dokumen sumber data Anda ke bidang Amazon Kendra indeks. Jika Anda menggunakan konsol, Anda memperbarui bidang dengan memilih sumber data, memilih tindakan edit, dan kemudian melanjutkan di sebelah bagian pemetaan bidang untuk mengonfigurasi sumber data.

Anda dapat mengonfigurasi `Search` objek untuk menetapkan bidang sebagai dapat ditampilkan, facetable, dapat dicari, dan dapat diurutkan. Anda dapat mengonfigurasi `Relevance` objek untuk mengatur urutan peringkat bidang, durasi peningkatan, atau periode waktu untuk diterapkan pada peningkatan, kesegaran, nilai kepentingan, dan nilai kepentingan yang dipetakan ke nilai bidang tertentu. Jika Anda menggunakan konsol, Anda dapat mengatur pengaturan pencarian untuk bidang dengan memilih opsi facet di menu navigasi. Untuk mengatur penyetelan relevansi, pilih opsi untuk mencari indeks Anda di menu navigasi, masukkan kueri, dan gunakan opsi panel samping untuk

menyetel relevansi pencarian. Anda tidak dapat mengubah jenis bidang setelah Anda membuat bidang.

Amazon Kendra memiliki bidang dokumen cadangan atau umum berikut yang dapat Anda gunakan:

- `_authors`Daftar satu atau lebih penulis yang bertanggung jawab atas isi dokumen.
- `_category`Sebuah kategori yang menempatkan dokumen dalam kelompok tertentu.
- `_created_at`Tanggal dan waktu dalam format ISO 8601 bahwa dokumen itu dibuat. Misalnya, 2012-03-25T 12:30:10 +01:00 adalah format tanggal-waktu ISO 8601 untuk 25 Maret 2012 pukul 12:30 (ditambah 10 detik) di Waktu Eropa Tengah.
- `_data_source_id`—Pengidentifikasi sumber data yang berisi dokumen.
- `_document_body`—Isi dokumen.
- `_document_id`—Pengenal unik untuk dokumen.
- `_document_title`—Judul dokumen.
- `_excerpt_page_number`—Nomor halaman dalam file PDF tempat kutipan dokumen muncul. Jika indeks Anda dibuat sebelum 8 September 2020, Anda harus mengindeks ulang dokumen sebelum dapat menggunakan atribut ini.
- `_faq_id`—Jika ini adalah dokumen tipe tanya jawab (FAQ), pengenal unik untuk FAQ.
- `_file_type`—Jenis file dokumen, seperti pdf atau doc.
- `_last_updated_at`Tanggal dan waktu dalam format ISO 8601 bahwa dokumen terakhir diperbarui. Misalnya, 2012-03-25T 12:30:10 +01:00 adalah format tanggal-waktu ISO 8601 untuk 25 Maret 2012 pukul 12:30 (ditambah 10 detik) di Waktu Eropa Tengah.
- `_source_uri`—URI tempat dokumen tersedia. Misalnya, URI dokumen di situs web perusahaan.
- `_version`—Pengidentifikasi untuk versi dokumen tertentu.
- `_view_count`—Berapa kali dokumen telah dilihat.
- `_language_code`(String) —Kode untuk bahasa yang berlaku untuk dokumen. Ini default ke bahasa Inggris jika Anda tidak menentukan bahasa. Untuk informasi selengkapnya tentang bahasa yang didukung, termasuk kodenya, lihat Menambahkan dokumen dalam bahasa selain bahasa Inggris.

Untuk bidang kustom, Anda membuat bidang ini menggunakan `DocumentMetadataConfigurationUpdates` `UpdateIndex` API, seperti yang Anda lakukan saat membuat bidang cadangan atau umum. Anda harus mengatur tipe data yang sesuai untuk bidang kustom Anda. Jika Anda menggunakan konsol, Anda memperbarui bidang dengan memilih sumber

data, memilih tindakan edit, dan kemudian melanjutkan di sebelah bagian pemetaan bidang untuk mengonfigurasi sumber data. Beberapa sumber data tidak mendukung penambahan bidang baru atau bidang khusus. Anda tidak dapat mengubah jenis bidang setelah Anda membuat bidang.

Berikut ini adalah jenis yang dapat Anda atur untuk bidang khusus:

- Tanggal
- Angka
- String
- Daftar string

Jika Anda menambahkan dokumen ke indeks menggunakan BatchPutDocumentAPI, `Attributes` daftar bidang/atribut dokumen Anda dan Anda membuat bidang menggunakan objek. `DocumentAttribute`

Untuk dokumen yang diindeks dari sumber Amazon S3 data, Anda membuat bidang menggunakan file metadata JSON yang menyertakan informasi bidang.

Jika Anda menggunakan database yang didukung sebagai sumber data, Anda dapat mengonfigurasi bidang menggunakan opsi pemetaan bidang.

Indeks pencarian

Setelah Anda membuat indeks, Anda dapat mulai mencari dokumen Anda. Untuk informasi selengkapnya, lihat Mencari indeks.

Dokumen

Bagian ini menjelaskan bagaimana Amazon Kendra mengindeks banyak format dokumen yang didukungnya dan bidang/atribut dokumen yang berbeda.

Topik

- Jenis atau format dokumen
- Atribut atau bidang dokumen

Jenis atau format dokumen

Amazon Kendra mendukung jenis atau format dokumen populer seperti PDF, HTML, Word PowerPoint, dan banyak lagi. Indeks dapat berisi beberapa format dokumen.

Amazon Kendra mengekstrak konten di dalam dokumen untuk membuat dokumen dapat dicari. Dokumen diuraikan dengan cara mengoptimalkan pencarian pada teks yang diekstraksi dan konten tabular apa pun (tabel HTML) di dalam dokumen. Ini berarti menyusun dokumen ke dalam bidang atau atribut yang digunakan untuk pencarian. Metadata dokumen, seperti tanggal modifikasi terakhir, dapat menjadi bidang yang berguna untuk pencarian.

Dokumen dapat diatur ke dalam baris dan kolom. Misalnya, setiap dokumen adalah baris dan setiap bidang/atribut dokumen, seperti judul dan isi isi, adalah kolom. Misalnya, jika Anda menggunakan database sebagai sumber data Anda, data harus terstruktur atau diatur ke dalam baris dan kolom.

Anda dapat menambahkan dokumen ke indeks Anda melalui cara-cara berikut:

- API BatchPutDocument
- Konektor sumber data

Jika Anda ingin menambahkan file FAQ, Anda menggunakan CreateFaqAPI untuk menambahkan file yang disimpan dalam Amazon S3 bucket. Anda dapat memilih antara format CSV dasar, format CSV yang menyertakan bidang/atribut pabean di header, dan format JSON yang menyertakan bidang khusus. Format defaultnya adalah CSV dasar.

Berikut ini memberikan informasi tentang setiap format dokumen yang didukung dan bagaimana Amazon Kendra memperlakukan setiap format saat mengindeks dokumen.

Format dokumen	Diperlakukan sebagai	Bagaimana dokumen diperlakukan	Struktur asli
Format Dokumen Portabel (PDF)	HTML	Dikonversi ke HTML, maka konten diekstraksi.	Tidak terstruktur
HyperText Bahasa Markup (HTML)	HTML	Tag HTML disaring untuk mengekstrak konten. Konten harus	Semi-terstruktur

Format dokumen	Diperlakukan sebagai	Bagaimana dokumen diperlakukan	Struktur asli
		antara tag HTML awal dan penutup utama (<HTML>content</HTML>).	
Bahasa Markup yang Dapat Diperluas (XHTML)	XML	Tag XHTML disaring untuk mengekstrak konten.	Semi-terstruktur
Transformasi Bahasa Stylesheet yang Dapat Diperluas (XSLT)	XSLT	Tag disaring untuk mengekstrak konten.	Semi-terstruktur
MarkDown (MD)	Teks biasa	Konten diekstraksi dengan MarkDown sintaks disertakan.	Semi-terstruktur
Nilai Terpisah Koma (CSV)	CSV	Konten diekstrak si dari setiap sel, dengan satu file diperlakukan sebagai hasil dokumen tunggal.	Terstruktur untuk file FAQ, jika tidak semi-terstruktur
Microsoft Excel (XLS dan XLSX)	XLS dan XLSX	Konten diekstrak si dari setiap sel, dengan satu file diperlakukan sebagai hasil dokumen tunggal.	Semi-terstruktur
JavaScript Notasi Objek (JSON)	Teks biasa	Konten diekstraksi dengan sintaks JSON disertakan.	Semi-terstruktur

Format dokumen	Diperlakukan sebagai	Bagaimana dokumen diperlakukan	Struktur asli
Format Teks Kaya (RTF)	RTF	Sintaks RTF disaring untuk mengekstrak konten.	Semi-terstruktur
Microsoft PowerPoint (PPT)	PPT	Hanya konten teks yang diekstraksi dari PowerPoint slide untuk pencarian. Gambar dan konten lainnya tidak diekstraksi.	Tidak terstruktur
Microsoft Word (DOCX)	DOCX	Hanya konten teks yang diekstraksi dari halaman Word untuk pencarian. Gambar dan konten lainnya tidak diekstraksi.	Tidak terstruktur
Teks biasa (TXT)	TXT	Semua teks dalam dokumen teks diekstraksi.	Tidak terstruktur

Atribut atau bidang dokumen

Dokumen memiliki atribut atau bidang yang terkait dengannya. Bidang dokumen adalah properti dokumen atau apa yang terkandung dalam struktur dokumen. Misalnya, setiap dokumen Anda mungkin berisi judul, teks badan, dan penulis. Anda juga dapat menambahkan bidang khusus untuk dokumen khusus Anda. Misalnya, jika indeks Anda mencari dokumen pajak, Anda dapat menentukan bidang khusus untuk jenis dokumen pajak seperti W-2, 1099, dan sebagainya.

Sebelum Anda dapat menggunakan bidang dokumen dalam kueri, itu harus dipetakan ke bidang indeks. Misalnya, bidang judul dapat dipetakan ke bidang `_document_title`. Untuk informasi selengkapnya, lihat Bidang pemetaan. Untuk menambahkan bidang baru, Anda harus membuat

bidang indeks untuk memetakan bidang tersebut. Anda membuat kolom indeks menggunakan konsol atau dengan menggunakan UpdateIndexAPI.

Anda dapat menggunakan bidang dokumen untuk memfilter tanggapan dan untuk membuat hasil pencarian segi. Misalnya, Anda dapat memfilter respons untuk hanya mengembalikan versi dokumen tertentu, atau Anda dapat memfilter pencarian untuk hanya mengembalikan 1099 jenis dokumen pajak yang cocok dengan istilah pencarian. Untuk informasi selengkapnya, lihat Memfilter dan pencarian faset.

Anda juga dapat menggunakan bidang dokumen untuk menyetel respons kueri secara manual. Misalnya, Anda dapat memilih untuk meningkatkan pentingnya bidang judul untuk menambah bobot yang diberikan ke Amazon Kendra bidang saat menentukan dokumen mana yang akan dikembalikan dalam respons. Untuk informasi selengkapnya, lihat Menyetel relevansi penelusuran.

Jika Anda menambahkan dokumen secara langsung ke indeks, Anda menentukan bidang dalam parameter input Dokumen ke BatchPutDocumentAPI. Anda menentukan nilai bidang kustom dalam array DocumentAttributeobjek. Jika Anda menggunakan sumber data, metode yang Anda gunakan untuk menambahkan bidang dokumen tergantung pada sumber data. Untuk informasi lebih lanjut, lihat Memetakan bidang sumber data.

Menggunakan bidang dokumen yang Amazon Kendra dicadangkan atau umum

Dengan UpdateIndex API, Anda dapat membuat kolom cadangan atau umum menggunakan `DocumentMetadataConfigurationUpdates` dan menentukan nama bidang indeks Amazon Kendra cadangan untuk dipetakan ke atribut/nama bidang dokumen yang setara. Anda juga dapat membuat bidang khusus. Jika Anda menggunakan konektor sumber data, sebagian besar menyertakan pemetaan bidang yang memetakan bidang dokumen sumber data Anda ke bidang Amazon Kendra indeks. Jika Anda menggunakan konsol, Anda memperbarui bidang dengan memilih sumber data, memilih tindakan edit, dan kemudian melanjutkan di sebelah bagian pemetaan bidang untuk mengonfigurasi sumber data.

Anda dapat mengonfigurasi `Search` objek untuk menetapkan bidang sebagai dapat ditampilkan, facetable, dapat dicari, dan dapat diurutkan. Anda dapat mengonfigurasi `Relevance` objek untuk mengatur urutan peringkat bidang, durasi peningkatan, atau periode waktu untuk diterapkan pada peningkatan, kesegaran, nilai kepentingan, dan nilai kepentingan yang dipetakan ke nilai bidang tertentu. Jika Anda menggunakan konsol, Anda dapat mengatur pengaturan pencarian untuk bidang dengan memilih opsi facet di menu navigasi. Untuk mengatur penyetelan relevansi, pilih opsi untuk mencari indeks Anda di menu navigasi, masukkan kueri, dan gunakan opsi panel samping untuk

menyetel relevansi pencarian. Anda tidak dapat mengubah jenis bidang setelah Anda membuat bidang.

Amazon Kendra memiliki bidang dokumen cadangan atau umum berikut yang dapat Anda gunakan:

- `_authors`Daftar satu atau lebih penulis yang bertanggung jawab atas isi dokumen.
- `_category`Sebuah kategori yang menempatkan dokumen dalam kelompok tertentu.
- `_created_at`Tanggal dan waktu dalam format ISO 8601 bahwa dokumen itu dibuat. Misalnya, 2012-03-25T 12:30:10 +01:00 adalah format tanggal-waktu ISO 8601 untuk 25 Maret 2012 pukul 12:30 (ditambah 10 detik) di Waktu Eropa Tengah.
- `_data_source_id`—Pengidentifikasi sumber data yang berisi dokumen.
- `_document_body`—Isi dokumen.
- `_document_id`—Pengenal unik untuk dokumen.
- `_document_title`—Judul dokumen.
- `_excerpt_page_number`—Nomor halaman dalam file PDF tempat kutipan dokumen muncul. Jika indeks Anda dibuat sebelum 8 September 2020, Anda harus mengindeks ulang dokumen sebelum dapat menggunakan atribut ini.
- `_faq_id`—Jika ini adalah dokumen tipe tanya jawab (FAQ), pengenal unik untuk FAQ.
- `_file_type`—Jenis file dokumen, seperti pdf atau doc.
- `_last_updated_at`Tanggal dan waktu dalam format ISO 8601 bahwa dokumen terakhir diperbarui. Misalnya, 2012-03-25T 12:30:10 +01:00 adalah format tanggal-waktu ISO 8601 untuk 25 Maret 2012 pukul 12:30 (ditambah 10 detik) di Waktu Eropa Tengah.
- `_source_uri`—URI tempat dokumen tersedia. Misalnya, URI dokumen di situs web perusahaan.
- `_version`—Pengidentifikasi untuk versi dokumen tertentu.
- `_view_count`—Berapa kali dokumen telah dilihat.
- `_language_code`(String) —Kode untuk bahasa yang berlaku untuk dokumen. Ini default ke bahasa Inggris jika Anda tidak menentukan bahasa. Untuk informasi selengkapnya tentang bahasa yang didukung, termasuk kodenya, lihat Menambahkan dokumen dalam bahasa selain bahasa Inggris.

Untuk bidang kustom, Anda membuat bidang ini menggunakan `DocumentMetadataConfigurationUpdates` `UpdateIndex` API, seperti yang Anda lakukan saat membuat bidang cadangan atau umum. Anda harus mengatur tipe data yang sesuai untuk bidang kustom Anda. Jika Anda menggunakan konsol, Anda memperbarui bidang dengan memilih sumber

data, memilih tindakan edit, dan kemudian melanjutkan di sebelah bagian pemetaan bidang untuk mengonfigurasi sumber data. Beberapa sumber data tidak mendukung penambahan bidang baru atau bidang khusus. Anda tidak dapat mengubah jenis bidang setelah Anda membuat bidang.

Berikut ini adalah jenis yang dapat Anda atur untuk bidang khusus:

- Tanggal
- Angka
- String
- Daftar string

Jika Anda menambahkan dokumen ke indeks menggunakan BatchPutDocumentAPI, `Attributes` daftar bidang/atribut dokumen Anda dan Anda membuat bidang menggunakan objek. `DocumentAttribute`

Untuk dokumen yang diindeks dari sumber Amazon S3 data, Anda membuat bidang menggunakan file metadata JSON yang menyertakan informasi bidang.

Jika Anda menggunakan database yang didukung sebagai sumber data, Anda dapat mengonfigurasi bidang menggunakan opsi pemetaan bidang.

Sumber data

Sumber data adalah repositori data atau lokasi yang Amazon Kendra menghubungkan dan mengindeks dokumen atau konten Anda. Misalnya, Anda dapat mengonfigurasi Amazon Kendra untuk terhubung ke Microsoft SharePoint untuk merayapi dan mengindeks dokumen yang disimpan di sumber ini. Anda juga dapat mengindeks halaman web dengan menyediakan URL Amazon Kendra untuk di-crawl. Anda dapat secara otomatis menyinkronkan sumber data dengan Amazon Kendra indeks sehingga dokumen yang ditambahkan, diperbarui, atau dihapus dalam sumber data juga ditambahkan, diperbarui, atau dihapus dalam indeks.

Sumber data yang didukung adalah:

- Manajer Pengalaman Adobe
- Alfresco
- Aurora (MySQL)
- Aurora (PostgreSQL)

- Amazon FSx (Jendela)
- Amazon FSx (NetApp ONTAP)
- Sumber data basis data
- Amazon RDS (Server Microsoft SQL)
- Amazon RDS (MySQL)
- Amazon RDS (Oracle)
- Amazon RDS (PostgreSQL)
- Amazon S3 ember
- Amazon Kendra Perayap Web
- Amazon WorkDocs
- Kotak
- Pertemuan
- Sumber data khusus
- Dropbox
- Drupal
- GitHub
- Gmail
- Drive Google Workspace
- IBM DB2
- Jira
- Microsoft Exchange
- Microsoft OneDrive
- Microsoft SharePoint
- Tim Microsoft
- Microsoft SQL Server
- Microsoft Yammer
- MySQL
- Database Oracle
- PostgreSQL

- Menyindir
- Salesforce
- ServiceNow
- Kendur
- Zendesk

Untuk daftar jenis dokumen atau format yang didukung oleh Amazon Kendra lihat Jenis dokumen. Anda harus terlebih dahulu membuat indeks sebelum membuat konektor sumber data untuk mengindeks dokumen Anda dari sumber data Anda.

> **Note**
>
> Untuk membuat indeks dokumen, Anda tidak perlu menggunakan sumber data. Anda dapat menambahkan dokumen langsung ke indeks dengan unggahan batch. Untuk informasi selengkapnya, lihat Menambahkan dokumen langsung ke indeks.

Untuk panduan tentang penggunaan Amazon Kendra konsol, AWS CLI, atau SDK, lihat Memulai.

Kueri

Untuk mendapatkan jawaban, pengguna melakukan kueri indeks. Pengguna dapat menggunakan bahasa alami dalam kueri mereka. Respons berisi informasi, seperti judul, kutipan teks, dan lokasi dokumendalam indeks yang memberikan jawaban terbaik.

Amazon Kendra menggunakan semua informasi yang Anda berikan tentang dokumen Anda, bukan hanya isi dokumen, untuk menentukan apakah suatu dokumen relevan dengan kueri. Misalnya, jika indeks Anda berisi informasi tentang kapan dokumen terakhir diperbarui, Anda dapat memberi tahu Amazon Kendra untuk menetapkan relevansi yang lebih tinggi ke dokumen yang diperbarui baru-baru ini.

Kueri juga dapat berisi kriteria untuk cara memfilter respons sehingga hanya Amazon Kendra mengembalikan dokumen yang memenuhi kriteria filter. Misalnya, jika Anda membuat sebuah bidang indeks yang disebutdepartemen, Anda dapat menyaring respons sehingga hanya dokumen dengan bidang departemen yang diatur ke hukum yang dikembalikan. Untuk informasi selengkapnya, lihat Memfilter pencarian.

Anda dapat mempengaruhi hasil kueri dengan penyetelan relevansi masing-masing bidang dalam indeks. Tuning mengubah pentingnya bidang pada hasil. Misalnya, jika Anda meningkatkan pentingnya dokumen dengan kategori baru, dokumen dengan kategori ini lebih cenderung dimasukkan dalam respons. Untuk informasi selengkapnya, lihat Menyetel relevansi penelusuran.

Untuk informasi selengkapnya tentang menggunakan kueri, lihat Mencari indeks.

Tag

Kelola indeks, sumber data, dan FAQ Anda dengan menetapkan tag atau label. Anda dapat menggunakan tag untuk mengkategorikan Amazon Kendra sumber daya Anda dengan berbagai cara. Misalnya, dengan tujuan, pemilik, atau aplikasi, atau kombinasi apa pun. Setiap tag terdiri atas sebuah kunci dan sebuah nilai, yang keduanya Anda tentukan.

Tanda membantu Anda untuk:

- Identifikasi dan atur AWS sumber daya Anda. Banyak AWS layanan mendukung penandaan, sehingga Anda dapat menetapkan tag yang sama ke sumber daya di layanan yang berbeda untuk menunjukkan bahwa sumber daya terkait. Misalnya, Anda dapat menandai indeks dan Amazon Lex bot yang menggunakan indeks dengan tag yang sama.
- Alokasikan biaya. Anda mengaktifkan tag di AWS Billing and Cost Management dasbor. AWS menggunakan tag untuk mengkategorikan biaya Anda dan mengirimkan laporan alokasi biaya bulanan kepada Anda. Untuk informasi selengkapnya, lihat Alokasi Biaya dan Penandaan di Tentang AWS Billing and Cost Management.
- Mengendalikan akses ke sumber daya Anda. Anda dapat menggunakan tag dalam AWS Identity and Access Management (IAM) kebijakan yang mengontrol akses ke Amazon Kendra sumber daya. Anda dapat melampirkan kebijakan ini ke IAM peran atau pengguna untuk mengaktifkan kontrol akses berbasis tag. Untuk informasi selengkapnya, lihat Otorisasi berdasarkan tag.

Anda dapat membuat dan mengelola tag menggunakan AWS Management Console, the AWS Command Line Interface (AWS CLI), atau Amazon Kendra API.

Pemberian tag pada sumber daya

Jika menggunakan Amazon Kendra konsol, Anda dapat menandai sumber daya saat membuatnya atau menambahkannya nanti. Anda juga dapat menggunakan konsol untuk memperbarui atau menghapus tanda.

Jika Anda menggunakan AWS Command Line Interface (AWS CLI) atau Amazon Kendra API, gunakan operasi berikut untuk mengelola tag untuk sumber daya Anda:

- CreateDataSource—Terapkan tag saat Anda membuat sumber data.
- CreateFaq—Terapkan tag saat Anda membuat FAQ.
- CreateIndex—Terapkan tag saat Anda membuat indeks.
- ListTagsForResource—Lihat tag yang terkait dengan sumber daya.
- TagResource—Menambahkan dan memodifikasi tag untuk sumber daya.
- UntagResource—Hapus tag dari sumber daya.

Batasan tanda

Pembatasan berikut berlaku untuk tag pada Amazon Kendra sumber daya:

- Jumlah maksimum tag—50
- Panjang kunci maksimum—128 karakter
- Panjang nilai maksimum—256 karakter
- Karakter yang valid untuk kunci dan nilai—a—z, A—Z, spasi, dan karakter berikut: _.:/= + - dan @
- Kunci dan nilai peka huruf besar dan kecil
- Jangan gunakan `aws:` sebagai prefiks untuk kunci; ini dicadangkan untuk penggunaan AWS

Menyiapkan Amazon Kendra

Sebelum menggunakan Amazon Kendra, Anda harus memiliki akun Amazon Web Services (AWS). Setelah memiliki AWS akun, Anda dapat mengakses Amazon Kendra melalui konsol Amazon Kendra, AWS CLI (), AWS Command Line Interface atau SDK. AWS

Panduan ini mencakup contoh untuk AWS CLI, Java, dan Python.

Topik

Mendaftar untuk AWS

Saat Anda mendaftar ke Amazon Web Services (AWS), akun Anda secara otomatis mendaftar untuk semua layanan AWS, termasuk Amazon Kendra. Anda hanya membayar biaya layanan yang Anda gunakan.

Jika Anda sudah memiliki AWS akun, lompat ke tugas berikutnya. Jika Anda belum memiliki akun AWS , gunakan prosedur berikut untuk membuatnya.

Untuk mendaftar AWS

1. Buka https://aws.amazon.com, lalu pilih Buat AWS Akun.
2. Ikuti petunjuk di layar untuk menyelesaikan pembuatan akun. Catat nomor AWS rekening 12 digit Anda. Bagian dari prosedur pendaftaran melibatkan menerima panggilan telepon dan memasukkan PIN menggunakan keypad telepon.
3. Buat pengguna admin AWS Identity and Access Management (IAM). Lihat Membuat Grup dan Pengguna IAM Pertama Anda dalam AWS Identity and Access Management Panduan Pengguna untuk melihat instruksi.

Wilayah dan titik akhir

Titik akhir adalah URL yang merupakan titik masuk untuk layanan web. Setiap titik akhir dikaitkan dengan AWS wilayah tertentu. Jika Anda menggunakan kombinasi konsol Amazon Kendra, SDK Amazon Kendra AWS CLI, dan Amazon Kendra, perhatikan wilayah defaultnya karena semua komponen Amazon Kendra dari kampanye tertentu (indeks, kueri, dll.) Harus dibuat di wilayah yang sama. Untuk wilayah dan titik akhir yang didukung oleh Amazon Kendra, lihat Wilayah dan Titik Akhir.

Menyiapkan AWS CLI

AWS Command Line Interface (AWS CLI) adalah alat pengembang terpadu untuk mengelola AWS layanan, termasuk Amazon Kendra. Kami menyarankan Anda menginstalnya.

1. Untuk menginstal AWS CLI, ikuti petunjuk dalam Menginstal Antarmuka Baris AWS Perintah di Panduan Pengguna Antarmuka Baris AWS Perintah.
2. Untuk mengkonfigurasi AWS CLI dan mengatur profil untuk memanggil AWS CLI, ikuti petunjuk dalam Mengkonfigurasi dalam Panduan Pengguna Antarmuka Baris AWS Perintah. AWS CLI
3. Untuk mengonfirmasi bahwa AWS CLI profil dikonfigurasi dengan benar, jalankan perintah berikut:

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

   Jika profil Anda telah dikonfigurasi dengan benar, Anda akan melihat output yang serupa dengan yang berikut ini:

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

4. Untuk memverifikasi bahwa AWS CLI dikonfigurasi untuk digunakan dengan Amazon Kendra, jalankan perintah berikut:

   ```
   aws kendra help
   ```

   Jika AWS CLI dikonfigurasi dengan benar, Anda akan melihat daftar AWS CLI perintah yang didukung untuk Amazon Kendra, Amazon Kendra runtime, dan Amazon Kendra event.

Menyiapkan AWS SDK

Unduh dan instal AWS SDK yang ingin Anda gunakan. Panduan ini memberikan contoh untuk Python. Untuk informasi tentang AWS SDK lain, lihat Alat untuk Amazon Web Services.

Paket untuk Python SDK disebut Boto3.

Sebelum Anda menjalankan perintah Python di bawah ini, Anda harus terlebih dahulu mengunduh dan menginstal Python 3.6 atau yang lebih baru untuk sistem operasi Anda. Support untuk Python 3.5 dan sebelumnya tidak digunakan lagi. Jika Anda tidak memiliki pip yang disertakan dalam direktori Skrip Python Anda, Anda dapat mengunduh get-pip.py dan menyimpannya di direktori Scripts Anda. Anda juga dapat mengatur direktori Python Anda sebagai Path atau variabel lingkungan menggunakan program terminal.

```
# 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
```

Untuk menggunakan Boto3, Anda harus menyiapkan kredensi otentikasi untuk AWS akun Anda menggunakan konsol IAM.

IAM peran akses untuk Amazon Kendra

Saat Anda membuat indeks, sumber data, atau FAQ, Amazon Kendra memerlukan akses ke AWS sumber daya yang diperlukan untuk membuat Amazon Kendra sumber daya. Anda harus membuat kebijakan AWS Identity and Access Management (IAM) sebelum membuat Amazon Kendra sumber daya. Ketika Anda memanggil operasi, Anda menyediakan Amazon Resource Name (ARN) dari peran dengan kebijakan yang dilampirkan. Misalnya, jika Anda memanggil BatchPutDocumentAPI untuk menambahkan dokumen dari Amazon S3 bucket, Anda menyediakan peran Amazon Kendra dengan kebijakan yang memiliki akses ke bucket.

Anda dapat membuat IAM peran baru di Amazon Kendra konsol atau memilih peran yang IAM ada untuk digunakan. Konsol tersebut menampilkan peran yang memiliki string “kendra” atau “Kendra” dalam nama peran.

Topik berikut memberikan detail untuk kebijakan yang diperlukan. Jika Anda membuat IAM peran menggunakan Amazon Kendra konsol, kebijakan ini dibuat untuk Anda.

Topik

IAM peran untuk indeks

Ketika Anda membuat indeks, Anda harus memberikan IAM peran dengan izin untuk menulis ke Amazon CloudWatch. Anda juga harus memberikan kebijakan kepercayaan yang memungkinkan Amazon Kendra untuk mengambil peran. Berikut ini adalah kebijakan yang harus disediakan.

IAM peran untuk indeks

Kebijakan peran Amazon Kendra untuk mengizinkan mengakses CloudWatch log.

```
{
    "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:*"
        }
    ]
}
```

Kebijakan peran untuk Amazon Kendra memungkinkan akses AWS Secrets Manager. Jika Anda menggunakan konteks pengguna Secrets Manager sebagai lokasi utama, Anda dapat menggunakan kebijakan berikut.

```
{
   "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"
               ]
            }
         }
      }
   ]
}
```

Kebijakan kepercayaan untuk memungkinkan Amazon Kendra untuk mengambil peran.

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

IAM peran untuk BatchPutDocument API

> **Warning**
>
> Amazon Kendra tidak menggunakan kebijakan bucket yang memberikan izin kepada Amazon Kendra kepala sekolah untuk berinteraksi dengan bucket S3. Sebaliknya, ia menggunakan IAM peran. Pastikan itu Amazon Kendra tidak disertakan sebagai anggota tepercaya dalam kebijakan bucket Anda untuk menghindari masalah keamanan data dalam pemberian izin secara tidak sengaja kepada prinsipal arbitrer. Namun, Anda dapat menambahkan kebijakan bucket untuk menggunakan Amazon S3 bucket di berbagai akun. Untuk informasi selengkapnya, lihat Kebijakan untuk digunakan Amazon S3 di seluruh akun. Untuk informasi tentang IAM peran untuk sumber data S3, lihat IAM peran.

Saat Anda menggunakan BatchPutDocumentAPI untuk mengindeks dokumen dalam Amazon S3 bucket, Anda harus menyediakan IAM peran Amazon Kendra dengan akses ke bucket. Anda juga harus memberikan kebijakan kepercayaan yang memungkinkan Amazon Kendra untuk mengambil peran. Jika dokumen dalam bucket dienkripsi, Anda harus memberikan izin untuk menggunakan AWS KMS customer master key (CMK) untuk mendekripsi dokumen.

IAM peran untuk BatchPutDocument API

Kebijakan peran yang diperlukan Amazon Kendra untuk memungkinkan mengakses Amazon S3 bucket.

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

Kebijakan kepercayaan untuk memungkinkan Amazon Kendra untuk mengambil peran.

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

Disarankan agar Anda memasukkan `aws:sourceAccount` dan `aws:sourceArn` dalam kebijakan kepercayaan. Ini membatasi izin dan memeriksa dengan aman apakah `aws:sourceAccount` dan sama seperti yang `aws:sourceArn` disediakan dalam kebijakan IAM peran untuk tindakan tersebut`sts:AssumeRole`. Ini mencegah entitas yang tidak sah mengakses IAM peran Anda dan izinnya. Untuk informasi lebih lanjut, lihat AWS Identity and Access Management panduan tentang masalah wakil yang bingung.

```
{
    "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/
*"
                }
            }
```

```
        }
    ]
}
```

Kebijakan peran opsional Amazon Kendra untuk memungkinkan penggunaan kunci master AWS KMS pelanggan (CMK) untuk mendekripsi dokumen dalam bucket. Amazon S3

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

IAM peran untuk sumber data

Saat Anda menggunakan CreateDataSourceAPI, Anda harus memberikan Amazon Kendra IAM peran yang memiliki izin untuk mengakses sumber daya. Izin khusus yang diperlukan tergantung pada sumber data.

IAM peran untuk sumber data Adobe Experience Manager

Saat Anda menggunakan Adobe Experience Manager, Anda memberikan peran dengan kebijakan berikut.

- Izin untuk mengakses AWS Secrets Manager rahasia Anda untuk mengautentikasi Adobe Experience Manager Anda.
- Izin untuk memanggil API publik yang diperlukan untuk konektor Adobe Experience Manager.
- Izin untuk memanggil `BatchPutDocumentBatchDeleteDocument`,,`PutPrincipalMapping`,`DeletePrincipalMapping`,`D` dan `ListGroupsOlderThanOrderingId` API.

> **Note**
>
> Anda dapat menghubungkan sumber data Adobe Experience Manager ke Amazon Kendra through Amazon VPC. Jika Anda menggunakan Amazon VPC, Anda perlu menambahkan izin tambahan.

```
{
  "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}}"
  }]
}
```

Kebijakan kepercayaan untuk memungkinkan Amazon Kendra untuk mengambil peran.

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

IAM peran untuk sumber data Alfresco

Saat Anda menggunakan Alfresco, Anda memberikan peran dengan kebijakan berikut.

- Izin untuk mengakses AWS Secrets Manager rahasia Anda untuk mengautentikasi Alfresco Anda.
- Izin untuk memanggil API publik yang diperlukan untuk konektor Alfresco.
- Izin untuk memanggil `BatchPutDocumentBatchDeleteDocument`,,`PutPrincipalMapping`,`DeletePrincipalMapping`,`D` dan `ListGroupsOlderThanOrderingId` API.

> **Note**
>
> Anda dapat menghubungkan sumber data Alfresco ke through. Amazon Kendra Amazon VPC Jika Anda menggunakan Amazon VPC, Anda perlu menambahkan izin tambahan.

```
{
  "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}}"
  }]
}
```

Kebijakan kepercayaan untuk memungkinkan Amazon Kendra untuk mengambil peran.

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

IAM peran untuk sumber Aurora data (MySQL)

Saat Anda menggunakan Aurora (MySQL), Anda memberikan peran dengan kebijakan berikut.

- Izin untuk mengakses AWS Secrets Manager rahasia Anda untuk mengautentikasi Aurora (MySQL) Anda.
- Izin untuk memanggil API publik yang diperlukan untuk konektor Aurora (MySQL).
- Izin untuk memanggil `BatchPutDocumentBatchDeleteDocument`,,`PutPrincipalMapping`,`DeletePrincipalMapping`,D dan `ListGroupsOlderThanOrderingId` API.

> **Note**
>
> Anda dapat menghubungkan sumber data Aurora (MySQL) ke through. Amazon Kendra Amazon VPC Jika Anda menggunakan Amazon VPC, Anda perlu menambahkan izin tambahan.

```
{
  "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:ListGroupsOlderThanOrderingId",
        "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}}"
  }]
}
```

Kebijakan kepercayaan untuk memungkinkan Amazon Kendra untuk mengambil peran.

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

IAM peran untuk sumber Aurora data (PostgreSQL)

Saat Anda menggunakan Aurora (PostgreSQL), Anda memberikan peran dengan kebijakan berikut.

- Izin untuk mengakses AWS Secrets Manager rahasia Anda untuk mengautentikasi Aurora (PostgreSQL) Anda.
- Izin untuk memanggil API publik yang diperlukan untuk konektor Aurora (PostgreSQL).
- Izin untuk memanggil `BatchPutDocumentBatchDeleteDocument`,,`PutPrincipalMapping`,`DeletePrincipalMapping`,`D` dan `ListGroupsOlderThanOrderingId` API.

> **Note**
>
> Anda dapat menghubungkan sumber data Aurora (PostgreSQL) ke through. Amazon Kendra Amazon VPC Jika Anda menggunakan Amazon VPC, Anda perlu menambahkan izin tambahan.

```
{
  "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:ListGroupsOlderThanOrderingId",
        "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}}"
  }]
}
```

Kebijakan kepercayaan untuk memungkinkan Amazon Kendra untuk mengambil peran.

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

IAM peran untuk sumber Amazon FSx data

Saat Anda menggunakan Amazon FSx, Anda memberikan peran dengan kebijakan berikut.

- Izin untuk mengakses AWS Secrets Manager rahasia Anda untuk mengautentikasi sistem Amazon FSx file Anda.
- Izin untuk mengakses Amazon Virtual Private Cloud (VPC) di mana sistem Amazon FSx file Anda berada.
- Izin untuk mendapatkan nama domain Direktori Aktif Anda untuk sistem Amazon FSx file Anda.
- Izin untuk memanggil API publik yang diperlukan untuk Amazon FSx konektor.

- Izin untuk memanggil `BatchPutDocument` dan `BatchDeleteDocument` API untuk memperbarui indeks.

```
{
    "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}}"
        }
        ]
}
```

Kebijakan kepercayaan untuk memungkinkan Amazon Kendra untuk mengambil peran.

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

IAM peran untuk sumber data database

Bila Anda menggunakan database sebagai sumber data, Anda memberikan peran Amazon Kendra yang memiliki izin yang diperlukan untuk menghubungkan ke. Ini termasuk:

- Izin untuk mengakses AWS Secrets Manager rahasia yang berisi nama pengguna dan kata sandi untuk situs. Untuk informasi lebih lanjut tentang isi rahasia, lihat sumber data.
- Izin untuk menggunakan kunci master AWS KMS pelanggan (CMK) untuk mendekripsi nama pengguna dan rahasia kata sandi yang disimpan oleh. Secrets Manager
- Izin untuk menggunakan operasi `BatchPutDocument` dan `BatchDeleteDocument` untuk memperbarui indeks.
- Izin untuk mengakses Amazon S3 bucket yang berisi sertifikat SSL yang digunakan untuk berkomunikasi dengan situs.

> **Note**
>
> Anda dapat menghubungkan sumber data database ke Amazon Kendra through Amazon VPC. Jika Anda menggunakan Amazon VPC, Anda perlu menambahkan izin tambahan.

```
{
    "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/*"
            ]
        }
    ]
}
```

Ada dua kebijakan opsional yang mungkin Anda gunakan dengan sumber data.

Jika Anda telah mengenkripsi Amazon S3 bucket yang berisi sertifikat SSL yang digunakan untuk berkomunikasi dengan, berikan kebijakan untuk memberikan Amazon Kendra akses ke kunci.

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

```
}
```

Jika Anda menggunakan VPC, berikan kebijakan yang memberikan Amazon Kendra akses ke sumber daya yang diperlukan. Lihat IAM peran untuk sumber data, VPC untuk kebijakan yang diperlukan.

Kebijakan kepercayaan untuk memungkinkan Amazon Kendra untuk mengambil peran.

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

IAM peran untuk Amazon RDS sumber data (Microsoft SQL Server)

Bila Anda menggunakan konektor sumber data Amazon RDS (Microsoft SQL Server), Anda memberikan peran dengan kebijakan berikut.

- Izin untuk mengakses AWS Secrets Manager rahasia Anda untuk mengautentikasi instance sumber data Amazon RDS (Microsoft SQL Server) Anda.
- Izin untuk memanggil API publik yang diperlukan untuk konektor sumber data Amazon RDS (Microsoft SQL Server).
- Izin untuk memanggil `BatchPutDocumentBatchDeleteDocument`,,`PutPrincipalMapping`,`DeletePrincipalMapping`,`D` dan `ListGroupsOlderThanOrderingId` API.

> **Note**
>
> Anda dapat menghubungkan sumber data Amazon RDS (Microsoft SQL Server) ke Amazon Kendra through Amazon VPC. Jika Anda menggunakan Amazon VPC, Anda perlu menambahkan izin tambahan.

```
{
  "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:ListGroupsOlderThanOrderingId",
        "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}}"
  }]
}
```

Kebijakan kepercayaan untuk memungkinkan Amazon Kendra untuk mengambil peran.

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

IAM peran untuk sumber Amazon RDS data (MySQL)

Bila Anda menggunakan konektor sumber data Amazon RDS (MySQL), Anda memberikan peran dengan kebijakan berikut.

- Izin untuk mengakses AWS Secrets Manager rahasia Anda untuk mengautentikasi instance Amazon RDS sumber data (MySQL) Anda.
- Izin untuk memanggil API publik yang diperlukan untuk konektor Amazon RDS sumber data (MySQL).
- Izin untuk memanggil `BatchPutDocumentBatchDeleteDocument`,,`PutPrincipalMapping`,`DeletePrincipalMapping`,`D` dan `ListGroupsOlderThanOrderingId` API.

> **Note**
>
> Anda dapat menghubungkan sumber data Amazon RDS (MySQL) ke through. Amazon Kendra Amazon VPC Jika Anda menggunakan Amazon VPC, Anda perlu menambahkan izin tambahan.

```
{
  "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:ListGroupsOlderThanOrderingId",
        "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}}"
  }]
}
```

Kebijakan kepercayaan untuk memungkinkan Amazon Kendra untuk mengambil peran.

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

IAM peran untuk Amazon RDS sumber data (Oracle)

Bila Anda menggunakan konektor sumber data Amazon RDS Oracle, Anda memberikan peran dengan kebijakan berikut.

- Izin untuk mengakses AWS Secrets Manager rahasia Anda untuk mengautentikasi instance sumber data Amazon RDS (Oracle) Anda.
- Izin untuk memanggil API publik yang diperlukan untuk konektor sumber data Amazon RDS (Oracle).
- Izin untuk memanggil `BatchPutDocumentBatchDeleteDocument`,,`PutPrincipalMapping`,`DeletePrincipalMapping`,D dan `ListGroupsOlderThanOrderingId` API.

> **Note**
>
> Anda dapat menghubungkan sumber data Amazon RDS Oracle ke Amazon Kendra through Amazon VPC. Jika Anda menggunakan Amazon VPC, Anda perlu menambahkan izin tambahan.

```
{
  "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:ListGroupsOlderThanOrderingId",
        "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}}"
  }]
}
```

Kebijakan kepercayaan untuk memungkinkan Amazon Kendra untuk mengambil peran.

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

IAM peran untuk sumber Amazon RDS data (PostgreSQL)

Bila Anda menggunakan konektor sumber data Amazon RDS (PostgreSQL), Anda memberikan peran dengan kebijakan berikut.

- Izin untuk mengakses AWS Secrets Manager rahasia Anda untuk mengautentikasi instance sumber Amazon RDS data (PostgreSQL) Anda.
- Izin untuk memanggil API publik yang diperlukan untuk konektor sumber Amazon RDS data (PostgreSQL).
- Izin untuk memanggil `BatchPutDocumentBatchDeleteDocument`,,`PutPrincipalMapping`,`DeletePrincipalMapping`,`D` dan `ListGroupsOlderThanOrderingId` API.

> **Note**
>
> Anda dapat menghubungkan sumber data Amazon RDS (PostgreSQL) ke through. Amazon Kendra Amazon VPC Jika Anda menggunakan Amazon VPC, Anda perlu menambahkan izin tambahan.

```
{
  "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:ListGroupsOlderThanOrderingId",
        "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}}"
  }]
}
```

Kebijakan kepercayaan untuk memungkinkan Amazon Kendra untuk mengambil peran.

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

IAM peran untuk sumber Amazon S3 data

> **Warning**
>
> Amazon Kendra tidak menggunakan kebijakan bucket yang memberikan izin kepada Amazon Kendra kepala sekolah untuk berinteraksi dengan bucket S3. Sebaliknya, ia menggunakan IAM peran. Pastikan itu Amazon Kendra tidak disertakan sebagai anggota tepercaya dalam kebijakan bucket Anda untuk menghindari masalah keamanan data dalam pemberian izin secara tidak sengaja kepada prinsipal arbitrer. Namun, Anda dapat menambahkan kebijakan bucket untuk menggunakan Amazon S3 bucket di berbagai akun. Untuk informasi selengkapnya, lihat Kebijakan untuk digunakan Amazon S3 di seluruh akun (gulir ke bawah).

Bila Anda menggunakan Amazon S3 bucket sebagai sumber data, Anda menyediakan peran yang memiliki izin untuk mengakses bucket, serta untuk menggunakan `BatchPutDocument` dan `BatchDeleteDocument` operasi. Jika dokumen dalam Amazon S3 bucket dienkripsi, Anda harus memberikan izin untuk menggunakan AWS KMS customer master key (CMK) untuk mendekripsi dokumen.

Kebijakan peran berikut harus memungkinkan Amazon Kendra untuk mengambil peran. Gulir lebih jauh ke bawah untuk melihat kebijakan kepercayaan untuk mengambil peran.

Kebijakan peran yang diperlukan Amazon Kendra untuk memungkinkan penggunaan Amazon S3 bucket sebagai sumber data.

```
{
    "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"
            ]
        }
```

```
    ]
}
```

Kebijakan peran opsional Amazon Kendra untuk memungkinkan penggunaan kunci master AWS KMS pelanggan (CMK) untuk mendekripsi dokumen dalam bucket. Amazon S3

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

Kebijakan peran opsional Amazon Kendra untuk memungkinkan mengakses Amazon S3 bucket, saat menggunakan Amazon VPC, dan tanpa mengaktifkan AWS KMS atau berbagi AWS KMS izin.

```
{
  "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-accoount-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: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}}"
    }
  ]
}
```

Kebijakan peran opsional Amazon Kendra untuk memungkinkan mengakses Amazon S3 bucket saat menggunakan Amazon VPC, dan dengan AWS KMS izin diaktifkan.

```
{
  "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: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}}"
    }
  ]
}
```

Kebijakan kepercayaan untuk memungkinkan Amazon Kendra untuk mengambil peran.

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

Kebijakan untuk digunakan Amazon S3 di seluruh akun

Jika Amazon S3 bucket Anda berada di akun yang berbeda dengan akun yang Anda gunakan untuk Amazon Kendra indeks, Anda dapat membuat kebijakan untuk menggunakannya di seluruh akun.

Kebijakan peran untuk menggunakan Amazon S3 bucket sebagai sumber data saat bucket berada di akun yang berbeda dengan Amazon Kendra indeks Anda. Perhatikan bahwa `s3:PutObject` dan `s3:PutObjectAcl` bersifat opsional, dan Anda menggunakan ini jika Anda ingin menyertakan file konfigurasi untuk daftar kontrol akses Anda.

```
{
```

```
    "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/*"
        }
    ]
}
```

Kebijakan bucket untuk mengizinkan peran sumber Amazon S3 data mengakses Amazon S3 bucket di seluruh akun. Perhatikan bahwa `s3:PutObject` dan `s3:PutObjectAcl` bersifat opsional, dan Anda menggunakan ini jika Anda ingin menyertakan file konfigurasi untuk daftar kontrol akses Anda.

```
{
    "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"
        }
    ]
}
```

Kebijakan kepercayaan untuk memungkinkan Amazon Kendra untuk mengambil peran.

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

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

IAM peran untuk sumber data Amazon Kendra Web Crawler

Saat Anda menggunakan Amazon Kendra Web Crawler, Anda memberikan peran dengan kebijakan berikut:

- Izin untuk mengakses AWS Secrets Manager rahasia yang berisi kredensil untuk terhubung ke situs web atau server proxy web yang didukung oleh otentikasi dasar. Untuk informasi selengkapnya tentang konten rahasia, lihat Menggunakan sumber data crawler web.
- Izin untuk menggunakan kunci master AWS KMS pelanggan (CMK) untuk mendekripsi nama pengguna dan rahasia kata sandi yang disimpan oleh. Secrets Manager
- Izin untuk menggunakan operasi `BatchPutDocument` dan `BatchDeleteDocument` untuk memperbarui indeks.
- Jika Anda menggunakan Amazon S3 bucket untuk menyimpan daftar URL benih atau peta situs, sertakan izin untuk mengakses bucket. Amazon S3

> **Note**
>
> Anda dapat menghubungkan sumber data Amazon Kendra Web Crawler ke Amazon Kendra through Amazon VPC. Jika Anda menggunakan Amazon VPC, Anda perlu menambahkan izin tambahan.

```
{
  "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"
  }]
}
```

Jika menyimpan URL benih atau peta situs dalam Amazon S3 bucket, Anda harus menambahkan izin ini ke peran tersebut.

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

Kebijakan kepercayaan untuk memungkinkan Amazon Kendra untuk mengambil peran.

```
{
```

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

IAM peran untuk sumber Amazon WorkDocs data

Saat Anda menggunakan Amazon WorkDocs, Anda memberikan peran dengan kebijakan berikut

- Izin untuk memverifikasi ID direktori (ID organisasi) yang sesuai dengan repositori Amazon WorkDocs situs Anda.
- Izin untuk mendapatkan nama domain Direktori Aktif Anda yang berisi direktori Amazon WorkDocs situs Anda.
- Izin untuk memanggil API publik yang diperlukan untuk Amazon WorkDocs konektor.
- Izin untuk memanggil `BatchPutDocument` dan `BatchDeleteDocument` API untuk memperbarui indeks.

```
{
  "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"
      ]
    }
  ]
}
```

Kebijakan kepercayaan untuk memungkinkan Amazon Kendra untuk mengambil peran.

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

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

IAM peran untuk sumber data Kotak

Saat Anda menggunakan Box, Anda memberikan peran dengan kebijakan berikut.

- Izin untuk mengakses AWS Secrets Manager rahasia Anda untuk mengautentikasi Slack Anda.
- Izin untuk memanggil API publik yang diperlukan untuk konektor Box.
- Izin untuk memanggil `BatchPutDocument`,`BatchDeleteDocument`,`PutPrincipalMapping`,`DeletePrincipalMapping`,`D` dan `ListGroupsOlderThanOrderingId` API.

> **Note**
>
> Anda dapat menghubungkan sumber data Box ke Amazon Kendra through Amazon VPC. Jika Anda menggunakan Amazon VPC, Anda perlu menambahkan izin tambahan.

```
{
  "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-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}}"
  }]
}
```

Kebijakan kepercayaan untuk memungkinkan Amazon Kendra untuk mengambil peran.

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

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

IAM peran untuk sumber data Confluence

IAM peran untuk Confluence Connector v1.0

Ketika Anda menggunakan server Confluence sebagai sumber data, Anda memberikan peran dengan kebijakan berikut:

- Izin untuk mengakses AWS Secrets Manager rahasia yang berisi kredensyal yang diperlukan untuk terhubung ke Confluence. Untuk informasi lebih lanjut tentang isi rahasia, lihat Sumber data pertemuan.
- Izin untuk menggunakan kunci master AWS KMS pelanggan (CMK) untuk mendekripsi nama pengguna dan rahasia kata sandi yang disimpan oleh. Secrets Manager
- Izin untuk menggunakan operasi `BatchPutDocument` dan `BatchDeleteDocument` untuk memperbarui indeks.

> **Note**
>
> Anda dapat menghubungkan sumber data Confluence ke Amazon Kendra through. Amazon VPC Jika Anda menggunakan Amazon VPC, Anda perlu menambahkan izin tambahan.

```
{
  "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"
  }]
}
```

Jika Anda menggunakan VPC, berikan kebijakan yang memberikan Amazon Kendra akses ke sumber daya yang diperlukan. Lihat IAM peran untuk sumber data, VPC untuk kebijakan yang diperlukan.

Kebijakan kepercayaan untuk memungkinkan Amazon Kendra untuk mengambil peran.

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

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

IAM peran untuk Confluence Connector v2.0

Untuk sumber data konektor Confluence v2.0, Anda memberikan peran dengan kebijakan berikut.

- Izin untuk mengakses AWS Secrets Manager rahasia yang berisi kredensi otentikasi untuk Confluence. Untuk informasi lebih lanjut tentang isi rahasia, lihat Sumber data pertemuan.
- Izin untuk menggunakan kunci master AWS KMS pelanggan (CMK) untuk mendekripsi nama pengguna dan rahasia kata sandi yang disimpan oleh. AWS Secrets Manager
- Izin untuk menggunakan operasi `BatchPutDocument` dan `BatchDeleteDocument` untuk memperbarui indeks.

Anda juga harus melampirkan kebijakan kepercayaan yang memungkinkan Amazon Kendra untuk mengambil peran.

> **Note**
>
> Anda dapat menghubungkan sumber data Confluence ke Amazon Kendra through. Amazon VPC Jika Anda menggunakan Amazon VPC, Anda perlu menambahkan izin tambahan.

Kebijakan peran untuk memungkinkan terhubung Amazon Kendra ke Confluence.

```
{
  "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"
    }
  ]
}
```

Kebijakan kepercayaan untuk memungkinkan Amazon Kendra untuk mengambil peran.

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

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

IAM peran untuk sumber data Dropbox

Saat Anda menggunakan Dropbox, Anda memberikan peran dengan kebijakan berikut.

- Izin untuk mengakses AWS Secrets Manager rahasia Anda untuk mengautentikasi Dropbox Anda.
- Izin untuk memanggil API publik yang diperlukan untuk konektor Dropbox.
- Izin untuk memanggil `BatchPutDocumentBatchDeleteDocument`,,`PutPrincipalMapping`,`DeletePrincipalMapping`,`D` dan `ListGroupsOlderThanOrderingId` API.

> **Note**
>
> Anda dapat menghubungkan sumber data Dropbox ke Amazon Kendra melalui Amazon VPC. Jika Anda menggunakan Amazon VPC, Anda perlu menambahkan izin tambahan.

```
{
"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}}"
  }]
}
```

Kebijakan kepercayaan untuk memungkinkan Amazon Kendra untuk mengambil peran.

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

```
    ]
}
```

IAM peran untuk sumber data Drupal

Ketika Anda menggunakan Drupal, Anda memberikan peran dengan kebijakan berikut.

- Izin untuk mengakses AWS Secrets Manager rahasia Anda untuk mengotentikasi Drupal Anda.
- Izin untuk memanggil API publik yang diperlukan untuk konektor Drupal.
- Izin untuk memanggil `BatchPutDocumentBatchDeleteDocument`,,`PutPrincipalMapping`,`DeletePrincipalMapping`,`D` dan `ListGroupsOlderThanOrderingId` API.

> **Note**
>
> Anda dapat menghubungkan sumber data Drupal ke Amazon Kendra through Amazon VPC. Jika Anda menggunakan Amazon VPC, Anda perlu menambahkan izin tambahan.

```
{
  "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:ListGroupsOlderThanOrderingId",
        "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}}"
  }]
}
```

Kebijakan kepercayaan untuk memungkinkan Amazon Kendra untuk mengambil peran.

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

IAM peran untuk sumber GitHub data

Saat Anda menggunakan GitHub, Anda memberikan peran dengan kebijakan berikut.

- Izin untuk mengakses AWS Secrets Manager rahasia Anda untuk mengautentikasi Anda GitHub.
- Izin untuk memanggil API publik yang diperlukan untuk GitHub konektor.
- Izin untuk memanggil `BatchPutDocument`,`BatchDeleteDocument`,`PutPrincipalMapping`,`DeletePrincipalMapping`,`D` dan `ListGroupsOlderThanOrderingId` API.

> **Note**
>
> Anda dapat menghubungkan sumber GitHub data ke Amazon Kendra through Amazon VPC. Jika Anda menggunakan Amazon VPC, Anda perlu menambahkan izin tambahan.

```
{
  "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}}"
  }]
}
```

Kebijakan kepercayaan untuk memungkinkan Amazon Kendra untuk mengambil peran.

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

IAM peran untuk sumber data Gmail

Saat Anda menggunakan Gmail, Anda memberikan peran dengan kebijakan berikut.

- Izin untuk mengakses AWS Secrets Manager rahasia Anda untuk mengautentikasi Gmail Anda.
- Izin untuk memanggil API publik yang diperlukan untuk Gmailconnector.
- Izin untuk memanggil `BatchPutDocumentBatchDeleteDocument`,,`PutPrincipalMapping`,`DeletePrincipalMapping`,`D` dan `ListGroupsOlderThanOrderingId` API.

> **Note**
>
> Anda dapat menghubungkan sumber data Gmail ke Amazon Kendra melalui Amazon VPC. Jika Anda menggunakan Amazon VPC, Anda perlu menambahkan izin tambahan.

```
{
"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}}"
  }]
}
```

Kebijakan kepercayaan untuk memungkinkan Amazon Kendra untuk mengambil peran.

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

IAM peran untuk sumber data Google Drive

Saat Anda menggunakan sumber data Google Workspace Drive, Anda Amazon Kendra memberikan peran yang memiliki izin yang diperlukan untuk menyambung ke situs. Ini termasuk:

- Izin untuk mendapatkan dan mendekripsi AWS Secrets Manager rahasia yang berisi email akun klien, email akun admin, dan kunci pribadi yang diperlukan untuk terhubung ke situs Google Drive. Untuk informasi selengkapnya tentang isi rahasia, lihat sumber data Google Drive.
- Izin untuk menggunakan BatchPutDocumentdan BatchDeleteDocumentAPI.

> **Note**
>
> Anda dapat menghubungkan sumber data Google Drive ke Amazon Kendra through Amazon VPC. Jika Anda menggunakan Amazon VPC, Anda perlu menambahkan izin tambahan.

IAM Kebijakan berikut memberikan izin yang diperlukan:

```
{
  "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"
  }]
}
```

Kebijakan kepercayaan untuk memungkinkan Amazon Kendra untuk mengambil peran.

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

IAM peran untuk sumber data IBM DB2

Bila Anda menggunakan konektor sumber data IBM DB2, Anda memberikan peran dengan kebijakan berikut.

- Izin untuk mengakses AWS Secrets Manager rahasia Anda untuk mengautentikasi contoh sumber data IBM DB2 Anda.
- Izin untuk memanggil API publik yang diperlukan untuk konektor sumber data IBM DB2.
- Izin untuk memanggil `BatchPutDocumentBatchDeleteDocument`,,`PutPrincipalMapping`,`DeletePrincipalMapping`,`D` dan `ListGroupsOlderThanOrderingId` API.

> **Note**
>
> Anda dapat menghubungkan sumber data IBM DB2 ke through. Amazon Kendra Amazon VPC Jika Anda menggunakan Amazon VPC, Anda perlu menambahkan izin tambahan.

```
{
  "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:ListGroupsOlderThanOrderingId",
        "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}}"
  }]
}
```

Kebijakan kepercayaan untuk memungkinkan Amazon Kendra untuk mengambil peran.

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

IAM peran untuk sumber data Jira

Saat Anda menggunakan Jira, Anda memberikan peran dengan kebijakan berikut.

- Izin untuk mengakses AWS Secrets Manager rahasia Anda untuk mengotentikasi Jira Anda.
- Izin untuk memanggil API publik yang diperlukan untuk konektor Jira.
- Izin untuk memanggil `BatchPutDocumentBatchDeleteDocument`,,`PutPrincipalMapping`,`DeletePrincipalMapping`,`D` dan `ListGroupsOlderThanOrderingId` API.

> **Note**
>
> Anda dapat menghubungkan sumber data Jira ke Amazon Kendra through Amazon VPC. Jika Anda menggunakan Amazon VPC, Anda perlu menambahkan izin tambahan.

```
{
  "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}}"
  }]
}
```

Kebijakan kepercayaan untuk memungkinkan Amazon Kendra untuk mengambil peran.

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

IAM peran untuk sumber data Microsoft Exchange

Saat Anda menggunakan sumber data Microsoft Exchange, Anda memberikan Amazon Kendra peran yang memiliki izin yang diperlukan untuk menghubungkan ke situs. Ini termasuk:

- Izin untuk mendapatkan dan mendekripsi AWS Secrets Manager rahasia yang berisi ID aplikasi dan kunci rahasia yang diperlukan untuk terhubung ke situs Microsoft Exchange. Untuk informasi selengkapnya tentang isi rahasia, lihat sumber data Microsoft Exchange.
- Izin untuk menggunakan BatchPutDocumentdan BatchDeleteDocumentAPI.

> **Note**
>
> Anda dapat menghubungkan sumber data Microsoft Exchange ke Amazon Kendra through Amazon VPC. Jika Anda menggunakan Amazon VPC, Anda perlu menambahkan izin tambahan.

IAM Kebijakan berikut memberikan izin yang diperlukan:

```
{
  "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"
  }]
}
```

Jika Anda menyimpan daftar pengguna untuk diindeks dalam Amazon S3 bucket, Anda juga harus memberikan izin untuk menggunakan `GetObject` operasi S3. IAM Kebijakan berikut memberikan izin yang diperlukan:

```
{
  "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"
  }]
}
```

Kebijakan kepercayaan untuk memungkinkan Amazon Kendra untuk mengambil peran.

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

IAM peran untuk sumber OneDrive data Microsoft

Saat Anda menggunakan sumber OneDrive data Microsoft, Anda Amazon Kendra memberikan peran yang memiliki izin yang diperlukan untuk menghubungkan ke situs. Ini termasuk:

- Izin untuk mendapatkan dan mendekripsi AWS Secrets Manager rahasia yang berisi ID aplikasi dan kunci rahasia yang diperlukan untuk terhubung ke situs. OneDrive Untuk informasi selengkapnya tentang isi rahasia, lihat Sumber OneDrive data Microsoft.
- Izin untuk menggunakan BatchPutDocumentdan BatchDeleteDocumentAPI.

> **Note**
>
> Anda dapat menghubungkan sumber OneDrive data Microsoft ke Amazon Kendra through Amazon VPC. Jika Anda menggunakan Amazon VPC, Anda perlu menambahkan izin tambahan.

IAM Kebijakan berikut memberikan izin yang diperlukan:

```
{
  "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"
  }]
}
```

Jika Anda menyimpan daftar pengguna untuk diindeks dalam Amazon S3 bucket, Anda juga harus memberikan izin untuk menggunakan `GetObject` operasi S3. IAM Kebijakan berikut memberikan izin yang diperlukan:

```
{
  "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"
  }]
}
```

Kebijakan kepercayaan untuk memungkinkan Amazon Kendra untuk mengambil peran.

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

IAM peran untuk sumber SharePoint data Microsoft

IAM peran untuk SharePoint Connector v1.0

Untuk sumber data SharePoint konektor Microsoft v1.0, Anda memberikan peran dengan kebijakan berikut.

- Izin untuk mengakses AWS Secrets Manager rahasia yang berisi nama pengguna dan kata sandi untuk SharePoint situs. Untuk informasi selengkapnya tentang isi rahasia, lihat Sumber SharePoint data Microsoft.
- Izin untuk menggunakan kunci master AWS KMS pelanggan (CMK) untuk mendekripsi nama pengguna dan rahasia kata sandi yang disimpan oleh. AWS Secrets Manager

- Izin untuk menggunakan operasi `BatchPutDocument` dan `BatchDeleteDocument` untuk memperbarui indeks.
- Izin untuk mengakses Amazon S3 bucket yang berisi sertifikat SSL yang digunakan untuk berkomunikasi dengan SharePoint situs.

Anda juga harus melampirkan kebijakan kepercayaan yang memungkinkan Amazon Kendra untuk mengambil peran.

> **Note**
>
> Anda dapat menghubungkan sumber SharePoint data Microsoft ke Amazon Kendra through Amazon VPC. Jika Anda menggunakan Amazon VPC, Anda perlu menambahkan izin tambahan.

```
{
    "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/*"
            ]
        }
    ]
}
```

Jika Anda telah mengenkripsi Amazon S3 bucket yang berisi sertifikat SSL yang digunakan untuk berkomunikasi dengan SharePoint situs, berikan kebijakan untuk memberikan Amazon Kendra akses ke kunci tersebut.

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

```
}
```

Kebijakan kepercayaan untuk memungkinkan Amazon Kendra untuk mengambil peran.

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

IAM peran untuk SharePoint Connector v2.0

Untuk sumber data SharePoint konektor Microsoft v2.0, Anda memberikan peran dengan kebijakan berikut.

- Izin untuk mengakses AWS Secrets Manager rahasia yang berisi kredensyal otentikasi untuk situs. SharePoint Untuk informasi selengkapnya tentang isi rahasia, lihat Sumber SharePoint data Microsoft.
- Izin untuk menggunakan kunci master AWS KMS pelanggan (CMK) untuk mendekripsi nama pengguna dan rahasia kata sandi yang disimpan oleh. AWS Secrets Manager
- Izin untuk menggunakan operasi `BatchPutDocument` dan `BatchDeleteDocument` untuk memperbarui indeks.
- Izin untuk mengakses Amazon S3 bucket yang berisi sertifikat SSL yang digunakan untuk berkomunikasi dengan SharePoint situs.

Anda juga harus melampirkan kebijakan kepercayaan yang memungkinkan Amazon Kendra untuk mengambil peran.

> **Note**
>
> Anda dapat menghubungkan sumber SharePoint data Microsoft ke Amazon Kendra through Amazon VPC. Jika Anda menggunakan Amazon VPC, Anda perlu menambahkan izin tambahan.

```
{
  "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/*"
      ]
    },
    {
      "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": "*"
    }
  ]
}
```

Jika Anda telah mengenkripsi Amazon S3 bucket yang berisi sertifikat SSL yang digunakan untuk berkomunikasi dengan SharePoint situs, berikan kebijakan untuk memberikan Amazon Kendra akses ke kunci tersebut.

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

Kebijakan kepercayaan untuk memungkinkan Amazon Kendra untuk mengambil peran.

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

IAM peran untuk sumber data Microsoft SQL Server

Bila Anda menggunakan Microsoft SQL Server, Anda memberikan peran dengan kebijakan berikut.

- Izin untuk mengakses AWS Secrets Manager rahasia Anda untuk mengautentikasi instance Microsoft SQL Server Anda.
- Izin untuk memanggil API publik yang diperlukan untuk konektor Microsoft SQL Server.

- Izin untuk memanggil `BatchPutDocument`,`BatchDeleteDocument`,`PutPrincipalMapping`,`DeletePrincipalMapping`,D dan `ListGroupsOlderThanOrderingId` API.

> **Note**
>
> Anda dapat menghubungkan sumber data Microsoft SQL Server ke Amazon Kendra through Amazon VPC. Jika Anda menggunakan Amazon VPC, Anda perlu menambahkan izin tambahan.

```
{
  "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:ListGroupsOlderThanOrderingId",
        "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}}"
  }]
}
```

Kebijakan kepercayaan untuk memungkinkan Amazon Kendra untuk mengambil peran.

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

IAM peran untuk sumber data Microsoft Teams

Saat Anda menggunakan sumber data Microsoft Teams, Anda memberikan Amazon Kendra peran yang memiliki izin yang diperlukan untuk menghubungkan ke situs. Ini termasuk:

- Izin untuk mendapatkan dan mendekripsi AWS Secrets Manager rahasia yang berisi ID klien dan rahasia klien yang diperlukan untuk terhubung ke Microsoft Teams. Untuk informasi selengkapnya tentang isi rahasia, lihat Sumber data Microsoft Teams.

> **Note**
>
> Anda dapat menghubungkan sumber data Microsoft Teams ke Amazon Kendra through Amazon VPC. Jika Anda menggunakan Amazon VPC, Anda perlu menambahkan izin tambahan.

IAM Kebijakan berikut memberikan izin yang diperlukan:

```
{
  "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"
  }]
}
```

Kebijakan kepercayaan untuk memungkinkan Amazon Kendra untuk mengambil peran.

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

IAM peran untuk sumber data Microsoft Yammer

Saat Anda menggunakan sumber data Microsoft Yammer, Anda Amazon Kendra memberikan peran yang memiliki izin yang diperlukan untuk menghubungkan ke situs. Ini termasuk:

- Izin untuk mendapatkan dan mendekripsi AWS Secrets Manager rahasia yang berisi ID aplikasi dan kunci rahasia yang diperlukan untuk terhubung ke situs Microsoft Yammer. Untuk informasi selengkapnya tentang isi rahasia, lihat Sumber data Microsoft Yammer.
- Izin untuk menggunakan BatchPutDocumentdan BatchDeleteDocumentAPI.

> **Note**
>
> Anda dapat menghubungkan sumber data Microsoft Yammer ke Amazon Kendra through Amazon VPC. Jika Anda menggunakan Amazon VPC, Anda perlu menambahkan izin tambahan.

IAM Kebijakan berikut memberikan izin yang diperlukan:

```
{
  "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"
  }]
}
```

Jika Anda menyimpan daftar pengguna untuk diindeks dalam Amazon S3 bucket, Anda juga harus memberikan izin untuk menggunakan `GetObject` operasi S3. IAM Kebijakan berikut memberikan izin yang diperlukan:

```
{
  "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"
  }]
}
```

Kebijakan kepercayaan untuk memungkinkan Amazon Kendra untuk mengambil peran.

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

IAM peran untuk sumber data MySQL

Bila Anda menggunakan konektor sumber data SQL Saya, Anda memberikan peran dengan kebijakan berikut.

- Izin untuk mengakses AWS Secrets Manager rahasia Anda untuk mengautentikasi instance sumber data SQL Saya.
- Izin untuk memanggil API publik yang diperlukan untuk konektor sumber data SQL Saya.
- Izin untuk memanggil `BatchPutDocumentBatchDeleteDocument`,,`PutPrincipalMapping`,`DeletePrincipalMapping`,`D` dan `ListGroupsOlderThanOrderingId` API.

> **Note**
>
> Anda dapat menghubungkan sumber data MySQL ke through. Amazon Kendra Amazon VPC Jika Anda menggunakan Amazon VPC, Anda perlu menambahkan izin tambahan.

```
{
```

```
  "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:ListGroupsOlderThanOrderingId",
        "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}}"
  }]
}
```

Kebijakan kepercayaan untuk memungkinkan Amazon Kendra untuk mengambil peran.

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

IAM peran untuk sumber data Oracle

Bila Anda menggunakan konektor sumber data Oracle, Anda memberikan peran dengan kebijakan berikut.

- Izin untuk mengakses AWS Secrets Manager rahasia Anda untuk mengautentikasi instance sumber data Oracle Anda.
- Izin untuk memanggil API publik yang diperlukan untuk konektor sumber data Oracle.
- Izin untuk memanggil `BatchPutDocumentBatchDeleteDocument`,,`PutPrincipalMapping`,`DeletePrincipalMapping`,`D` dan `ListGroupsOlderThanOrderingId` API.

> **Note**
>
> Anda dapat menghubungkan sumber data Oracle ke Amazon Kendra through Amazon VPC. Jika Anda menggunakan Amazon VPC, Anda perlu menambahkan izin tambahan.

```
{
  "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:ListGroupsOlderThanOrderingId",
        "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}}"
```

```
  }]
}
```

Kebijakan kepercayaan untuk memungkinkan Amazon Kendra untuk mengambil peran.

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

IAM peran untuk sumber data PostgreSQL

Bila Anda menggunakan konektor sumber data PostgreSQL, Anda memberikan peran dengan kebijakan berikut.

- Izin untuk mengakses AWS Secrets Manager rahasia Anda untuk mengautentikasi instance sumber data PostgreSQL Anda.
- Izin untuk memanggil API publik yang diperlukan untuk konektor sumber data PostgreSQL.
- Izin untuk memanggil `BatchPutDocument`,`BatchDeleteDocument`,`PutPrincipalMapping`,`DeletePrincipalMapping`,`D` dan `ListGroupsOlderThanOrderingId` API.

> **Note**
>
> Anda dapat menghubungkan sumber data PostgreSQL ke through. Amazon Kendra Amazon VPC Jika Anda menggunakan Amazon VPC, Anda perlu menambahkan izin tambahan.

```
{
  "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:ListGroupsOlderThanOrderingId",
        "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}}"
  }]
```

```
}
```

Kebijakan kepercayaan untuk memungkinkan Amazon Kendra untuk mengambil peran.

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

IAM peran untuk sumber data Quip

Saat Anda menggunakan Quip, Anda memberikan peran dengan kebijakan berikut.

- Izin untuk mengakses AWS Secrets Manager rahasia Anda untuk mengautentikasi Quip Anda.
- Izin untuk memanggil API publik yang diperlukan untuk konektor Quip.
- Izin untuk memanggil `BatchPutDocument`,`BatchDeleteDocument`,`PutPrincipalMapping`,`DeletePrincipalMapping`,`D` dan `ListGroupsOlderThanOrderingId` API.

> **Note**
>
> Anda dapat menghubungkan sumber data Quip ke Amazon Kendra through Amazon VPC. Jika Anda menggunakan Amazon VPC, Anda perlu menambahkan izin tambahan.

```
{
  "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}}:{{yoour-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/{{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}}"
  }]
}
```

Kebijakan kepercayaan untuk memungkinkan Amazon Kendra untuk mengambil peran.

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

IAM peran untuk sumber data Salesforce

Ketika Anda menggunakan Salesforce sebagai sumber data, Anda memberikan peran dengan kebijakan berikut:

- Izin untuk mengakses AWS Secrets Manager rahasia yang berisi nama pengguna dan kata sandi untuk situs Salesforce. Untuk informasi selengkapnya tentang isi rahasia, lihat Sumber data Salesforce.
- Izin untuk menggunakan kunci master AWS KMS pelanggan (CMK) untuk mendekripsi nama pengguna dan rahasia kata sandi yang disimpan oleh. Secrets Manager
- Izin untuk menggunakan operasi `BatchPutDocument` dan `BatchDeleteDocument` untuk memperbarui indeks.

> **Note**
>
> Anda dapat menghubungkan sumber data Salesforce ke Amazon Kendra through. Amazon VPC Jika Anda menggunakan Amazon VPC, Anda perlu menambahkan izin tambahan.

```
{
  "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"
  }]
}
```

Kebijakan kepercayaan untuk memungkinkan Amazon Kendra untuk mengambil peran.

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

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

IAM peran untuk sumber ServiceNow data

Bila Anda menggunakan ServiceNow sebagai sumber data, Anda memberikan peran dengan kebijakan berikut:

- Izin untuk mengakses Secrets Manager rahasia yang berisi nama pengguna dan kata sandi untuk ServiceNow situs. Untuk informasi lebih lanjut tentang isi rahasia, lihat sumber ServiceNow data.
- Izin untuk menggunakan kunci master AWS KMS pelanggan (CMK) untuk mendekripsi nama pengguna dan rahasia kata sandi yang disimpan oleh. Secrets Manager
- Izin untuk menggunakan operasi `BatchPutDocument` dan `BatchDeleteDocument` untuk memperbarui indeks.

> **Note**
>
> Anda dapat menghubungkan sumber ServiceNow data ke Amazon Kendra through Amazon VPC. Jika Anda menggunakan Amazon VPC, Anda perlu menambahkan izin tambahan.

```
{
  "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"
  }]
}
```

Kebijakan kepercayaan untuk memungkinkan Amazon Kendra untuk mengambil peran.

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

IAM peran untuk sumber data Slack

Saat Anda menggunakan Slack, Anda memberikan peran dengan kebijakan berikut.

- Izin untuk mengakses AWS Secrets Manager rahasia Anda untuk mengautentikasi Slack Anda.

- Izin untuk memanggil API publik yang diperlukan untuk konektor Slack.
- Izin untuk memanggil `BatchPutDocumentBatchDeleteDocument`,,`PutPrincipalMapping`,`DeletePrincipalMapping`,`D` dan `ListGroupsOlderThanOrderingId` API.

> **Note**
>
> Anda dapat menghubungkan sumber data Slack ke Amazon Kendra through Amazon VPC. Jika Anda menggunakan Amazon VPC, Anda perlu menambahkan izin tambahan.

```
{
  "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: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}}"
  }]
}
```

Kebijakan kepercayaan untuk memungkinkan Amazon Kendra untuk mengambil peran.

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

IAM peran untuk sumber data Zendesk

Saat Anda menggunakan Zendesk, Anda memberikan peran dengan kebijakan berikut.

- Izin untuk mengakses AWS Secrets Manager rahasia Anda untuk mengautentikasi Zendesk Suite Anda.
- Izin untuk memanggil API publik yang diperlukan untuk konektor Zendesk.

- Izin untuk memanggil `BatchPutDocumentBatchDeleteDocument`,,`PutPrincipalMapping`,`DeletePrincipalMapping`,`D` dan `ListGroupsOlderThanOrderingId` API.

> **Note**
>
> Anda dapat menghubungkan sumber data Zendesk ke Amazon Kendra through Amazon VPC. Jika Anda menggunakan Amazon VPC, Anda perlu menambahkan izin tambahan.

```
{
  "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}}"
  }]
}
```

Kebijakan kepercayaan untuk memungkinkan Amazon Kendra untuk mengambil peran.

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

Peran cloud pribadi virtual (VPC) IAM

Jika Anda menggunakan virtual private cloud (VPC) untuk terhubung ke sumber data Anda, Anda harus memberikan izin tambahan berikut.

Peran VPC IAM

```
{
      "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": "*"
    }
}
```

Kebijakan kepercayaan untuk memungkinkan Amazon Kendra untuk mengambil peran.

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

IAM peran untuk pertanyaan yang sering diajukan (FAQ)

Saat menggunakan CreateFaqAPI untuk memuat pertanyaan dan jawaban ke dalam indeks, Anda harus menyediakan IAM peran Amazon Kendra dengan akses ke Amazon S3 bucket yang berisi file

sumber. Jika file sumber dienkripsi, Anda harus memberikan izin untuk menggunakan kunci master AWS KMS pelanggan (CMK) untuk mendekripsi file.

IAM peran untuk FAQ

Kebijakan peran yang diperlukan Amazon Kendra untuk memungkinkan mengakses Amazon S3 bucket.

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

Kebijakan peran opsional Amazon Kendra untuk memungkinkan penggunaan kunci master AWS KMS pelanggan (CMK) untuk mendekripsi file dalam bucket. Amazon S3

```
{
    "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"
                    ]
                }
```

```
            }
        }
    ]
}
```

Kebijakan kepercayaan untuk memungkinkan Amazon Kendra untuk mengambil peran.

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

IAM peran untuk saran kueri

Saat Anda menggunakan Amazon S3 file sebagai daftar blokir saran kueri, Anda menyediakan peran yang memiliki izin untuk mengakses Amazon S3 file dan Amazon S3 bucket. Jika file teks daftar blokir (Amazon S3 file) di Amazon S3 bucket dienkripsi, Anda harus memberikan izin untuk menggunakan kunci master AWS KMS pelanggan (CMK) untuk mendekripsi dokumen.

IAM peran untuk saran kueri

Kebijakan peran yang diperlukan Amazon Kendra untuk mengizinkan penggunaan Amazon S3 file sebagai daftar blokir saran kueri Anda.

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

```
            ]
        }
    ]
}
```

Kebijakan peran opsional Amazon Kendra untuk memungkinkan penggunaan kunci master AWS KMS pelanggan (CMK) untuk mendekripsi dokumen dalam bucket. Amazon S3

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

Kebijakan kepercayaan untuk memungkinkan Amazon Kendra untuk mengambil peran.

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

IAM peran untuk pemetaan utama pengguna dan grup

Saat Anda menggunakan PutPrincipalMappingAPI untuk memetakan pengguna ke grup mereka untuk memfilter hasil penelusuran berdasarkan konteks pengguna, Anda perlu memberikan daftar

pengguna atau sub grup yang termasuk dalam grup. Jika daftar Anda lebih dari 1000 pengguna atau sub grup untuk grup, Anda harus menyediakan peran yang memiliki izin untuk mengakses Amazon S3 file daftar dan Amazon S3 bucket Anda. Jika file teks (Amazon S3 file) dari daftar dalam Amazon S3 bucket dienkripsi, Anda harus memberikan izin untuk menggunakan kunci master AWS KMS pelanggan (CMK) untuk mendekripsi dokumen.

IAM peran untuk pemetaan utama

Kebijakan peran yang diperlukan Amazon Kendra untuk mengizinkan penggunaan Amazon S3 file sebagai daftar pengguna dan sub grup milik grup.

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

Kebijakan peran opsional Amazon Kendra untuk memungkinkan penggunaan kunci master AWS KMS pelanggan (CMK) untuk mendekripsi dokumen dalam bucket. Amazon S3

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

Kebijakan kepercayaan untuk memungkinkan Amazon Kendra untuk mengambil peran.

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

Disarankan agar Anda memasukkan `aws:sourceAccount` dan `aws:sourceArn` dalam kebijakan kepercayaan. Ini membatasi izin dan memeriksa dengan aman apakah `aws:sourceAccount` dan sama seperti yang `aws:sourceArn` disediakan dalam kebijakan IAM peran untuk tindakan tersebut`sts:AssumeRole`. Ini mencegah entitas yang tidak sah mengakses IAM peran Anda dan izinnya. Untuk informasi lebih lanjut, lihat AWS Identity and Access Management panduan tentang masalah wakil yang bingung.

```
{
    "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 peran untuk AWS IAM Identity Center

Saat Anda menggunakan UserGroupResolutionConfigurationobjek untuk mengambil tingkat akses grup dan pengguna dari sumber AWS IAM Identity Center identitas, Anda perlu menyediakan peran yang memiliki izin untuk mengakses IAM Identity Center.

IAM peran untuk AWS IAM Identity Center

Kebijakan peran yang diperlukan untuk Amazon Kendra memungkinkan akses IAM Identity Center.

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

```
    ]
}
```

Kebijakan kepercayaan untuk memungkinkan Amazon Kendra untuk mengambil peran.

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

IAM peran untuk Amazon Kendra pengalaman

Saat Anda menggunakan UpdateExperienceAPI CreateExperienceatau untuk membuat atau memperbarui aplikasi pencarian, Anda harus menyediakan peran yang memiliki izin untuk mengakses operasi yang diperlukan dan Pusat Identitas IAM.

IAM peran untuk pengalaman Amazon Kendra pencarian

Kebijakan peran yang diperlukan Amazon Kendra untuk memungkinkan mengakses `Query` operasi, operasi, `QuerySuggestions` `SubmitFeedback` operasi, dan Pusat Identitas IAM yang menyimpan informasi pengguna dan grup Anda.

```
{
  "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:ListGroupsForUser",
        "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"
          ]
        }
```

```
      }
    }
  ]
}
```

Kebijakan kepercayaan untuk memungkinkan Amazon Kendra untuk mengambil peran.

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

Disarankan agar Anda memasukkan `aws:sourceAccount` dan `aws:sourceArn` dalam kebijakan kepercayaan. Ini membatasi izin dan memeriksa dengan aman apakah `aws:sourceAccount` dan sama seperti yang `aws:sourceArn` disediakan dalam kebijakan IAM peran untuk tindakan tersebut`sts:AssumeRole`. Ini mencegah entitas yang tidak sah mengakses IAM peran Anda dan izinnya. Untuk informasi lebih lanjut, lihat AWS Identity and Access Management panduan tentang masalah wakil yang bingung.

```
{
    "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 peran untuk Pengayaan Dokumen Kustom

Saat Anda menggunakan CustomDocumentEnrichmentConfigurationobjek untuk menerapkan perubahan lanjutan dari metadata dan konten dokumen Anda, Anda harus menyediakan peran yang memiliki izin yang diperlukan untuk dijalankan dan/atau. `PreExtractionHookConfiguration` `PostExtractionHookConfiguration` Anda mengonfigurasi fungsi Lambda `PostExtractionHookConfiguration` untuk `PreExtractionHookConfiguration` dan/atau menerapkan perubahan lanjutan dari metadata dan konten dokumen Anda selama proses konsumsi. Jika Anda memilih untuk mengaktifkan Enkripsi Sisi Server untuk Amazon S3 bucket Anda, Anda harus memberikan izin untuk menggunakan kunci master AWS KMS pelanggan (CMK) untuk mengenkripsi dan mendekripsi objek yang disimpan di bucket Anda. Amazon S3

IAM peran untuk Pengayaan Dokumen Kustom

Kebijakan peran yang diperlukan Amazon Kendra untuk memungkinkan menjalankan `PreExtractionHookConfiguration` dan `PostExtractionHookConfiguration` dengan enkripsi untuk Amazon S3 bucket Anda.

```
{
  "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"
  }]
}
```

Kebijakan peran opsional Amazon Kendra untuk memungkinkan menjalankan `PreExtractionHookConfiguration` dan `PostExtractionHookConfiguration` tanpa enkripsi untuk Amazon S3 bucket Anda.

```
{
  "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"
  }]
}
```

Kebijakan kepercayaan untuk memungkinkan Amazon Kendra untuk mengambil peran.

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

Disarankan agar Anda memasukkan `aws:sourceAccount` dan `aws:sourceArn` dalam kebijakan kepercayaan. Ini membatasi izin dan memeriksa dengan aman apakah `aws:sourceAccount` dan sama seperti yang `aws:sourceArn` disediakan dalam kebijakan IAM peran untuk tindakan tersebut`sts:AssumeRole`. Ini mencegah entitas yang tidak sah mengakses IAM peran Anda dan izinnya. Untuk informasi lebih lanjut, lihat AWS Identity and Access Management panduan tentang masalah wakil yang bingung.

```
{
```

```
    "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/*"
                }
            }
        }
    ]
}
```

Penerapan Amazon Kendra

Ketika tiba saatnya untuk menyebarkanAmazon KendraCari di situs web Anda, kami menyediakan kode sumber yang dapat Anda gunakan dengan React untuk memulai aplikasi Anda. Kode sumber disediakan tanpa biaya di bawah lisensi MIT yang dimodifikasi. Anda dapat menggunakannya apa adanya atau mengubahnya untuk kebutuhan Anda sendiri. Aplikasi React yang disediakan adalah contoh. Ini bukan aplikasi siap produksi.

Untuk menerapkan aplikasi penelusuran tanpa kode dan menghasilkan URL titik akhir ke halaman pencarian Anda dengan kontrol akses, lihatAmazon KendraPembangun Pengalaman.

Kode contoh berikut menambahkanAmazon Kendracari aplikasi web React yang ada:

- https://kendrasamples.s3.amazonaws.com/kendrasamples-react-app.zip—Contoh file yang dapat digunakan pengembang untuk membangun pengalaman pencarian fungsional ke dalam aplikasi web React yang ada.

Contoh tersebut dimodelkan setelah halaman pencarianAmazon Kendrakonsol. Mereka memiliki fitur yang sama untuk mencari dan menampilkan hasil pencarian. Anda dapat menggunakan seluruh contoh, atau Anda dapat memilih salah satu fitur untuk Anda gunakan sendiri.

Untuk melihat tiga komponen halaman pencarian diAmazon Kendrakonsol, pilih ikon kode (</>) dari menu yang tepat. Arahkan kursor ke setiap bagian untuk melihat deskripsi singkat komponen dan untuk mendapatkan URL sumber komponen.

Topik

Gambaran Umum

Anda menambahkan kode contoh ke aplikasi web React yang ada untuk mengaktifkan pencarian. Kode contoh menyertakan file Readme dengan langkah-langkah untuk menyiapkan lingkungan pengembangan React baru. Contoh data dalam contoh kode dapat digunakan untuk menunjukkan pencarian. File dan penjelasan dalam kode contoh disusun sebagai berikut:

- Halaman pencarian utama (`Search.tsx`) —Ini adalah halaman utama. Berikut ini adalah tempat Anda mengintegrasikan aplikasi Anda denganAmazon KendraAPI.
- Bilah penelusuran—Ini adalah komponen di mana pengguna memasukkan istilah pencarian dan memanggil fungsi pencarian.
- Hasil-Ini adalah komponen yang menampilkan hasilAmazon Kendra. Ini memiliki tiga komponen: jawaban yang disarankan, hasil FAQ, dan dokumen yang direkomendasikan.
- Aspek — Ini adalah komponen yang menunjukkan aspek dalam hasil pencarian dan memungkinkan Anda memilih aspek untuk mempersempit pencarian.
- Paginasi—Ini adalah komponen yang menentukan responsAmazon Kendra.

Prasyarat

Sebelum memulai, Anda perlu melakukan hal berikut:

- Node.js dan npmterpasang. Diperlukan Node.js versi 19 atau yang lebih lama.
- Python 3 atau Python 2diunduh dan diinstal.
- SDK for JavaatauAWS SDK for JavaScriptuntuk melakukan panggilan APIAmazon Kendra.
- Aplikasi web React yang ada. Kode contoh menyertakan file Readme dengan langkah-langkah tentang cara menyiapkan lingkungan pengembangan React baru, termasuk menggunakan kerangka kerja/pustaka yang diperlukan. Anda juga dapat mengikuti petunjuk mulai cepat diDokumentasi React tentang membuat aplikasi web React.
- Pustaka dan dependensi yang diperlukan dikonfigurasi di lingkungan pengembangan Anda. Kode contoh menyertakan file Readme yang mencantumkan pustaka dan dependensi paket yang diperlukan. Perhatikan bahwa`sass`diperlukan, sepertinode-sasssudah usang. Jika sebelumnya Anda menginstalnode-sass, hapus instalan ini dan instal`sass`.

Menyiapkan contoh

Prosedur lengkap untuk menambahkanAmazon Kendrapencarian ke aplikasi React ada di file Readme yang disertakan dalam contoh kode.

Untuk mulai menggunakan kendrasamples-react-app.zip

1. Pastikan Anda telah menyelesaikanPrasyarat, termasuk mengunduh dan menginstal Node.js dan npm.
2. Unduh kendrasamples-react-app.zip dan unzip.
3. Buka terminal Anda dan pergi ke`aws-kendra-example-react-app/src/services/`. Buka`local-dev-credentials.json`dan berikan kredensialnya. Jangan menambahkan file ini ke repositori publik apa pun.
4. Pergi ke`aws-kendra-example-react-app`dan instal dependensi di`package.json`. Jalankan `npm install`.
5. Luncurkan versi demo aplikasi Anda di server lokal. Jalankan `npm start`. Anda dapat menghentikan server lokal dengan memasukkan pada keyboard Anda`Cmd/Ctrl + C`.
6. Anda dapat mengubah port atau host (misalnya, alamat IP) dengan membuka`package.json`dan perbarui host dan port:`"start": "HOST=[host] PORT=[port] react-scripts start"`. Jika Anda menggunakan Windows:`"start": "set HOST=[host] && set PORT=[port] && react-scripts start"`.
7. Jika Anda memiliki domain situs web terdaftar, Anda dapat menentukan ini di`package.json`setelah nama aplikasi Anda. Sebagai contoh, `"homepage": "https://mywebsite.com"`. Anda harus larinpm installlagi untuk memperbarui dependensi baru, dan kemudian jalankannpm start.
8. Untuk membangun aplikasi, jalankannpm build. Unggah konten direktori build ke penyedia hosting Anda.

> **Warning**
>
> Aplikasi React adalahtidakproduksi siap. Ini adalah contoh penerapan aplikasi untukAmazon Kendrapencarian.

Halaman pencarian utama

Halaman pencarian utama (`Search.tsx`) berisi semua komponen pencarian contoh. Ini termasuk komponen bilah pencarian untuk output, komponen hasil untuk menampilkan respons dariPermintaanAPI, dan komponen pagination untuk paging melalui respons.

Komponen pencarian

Komponen pencarian menyediakan kotak teks untuk memasukkan teks kueri. Theon`Search`fungsi adalah hook yang memanggil fungsi utama di`Search.tsx`untuk membuatAmazon Kendra PermintaanPanggilan API.

Komponen hasil

Komponen hasil menunjukkan respons`Query`API. Hasilnya ditunjukkan di tiga area terpisah.

- Jawaban yang disarankan — Ini adalah hasil teratas yang dikembalikan`Query`API. Ini berisi hingga tiga jawaban yang disarankan. Dalam respon, mereka mempunyai jenis hasil `ANSWER`.
- Jawaban FAQ—Ini adalah hasil pertanyaan yang sering diajukan yang dikembalikan oleh jawaban. FAQ ditambahkan ke indeks secara terpisah. Dalam respon, mereka mempunyai jenis hasil `QUESTION_ANSWER`. Untuk informasi selengkapnya, lihatPertanyaan dan jawaban.
- Dokumen yang direkomendasikan—Ini adalah dokumen tambahan yangAmazon Kendrakembali dalam respon. Dalam tanggapan dari`Query`API, mereka memiliki tipe`DOCUMENT`.

Komponen hasil berbagi satu set komponen untuk fitur seperti penjelasan, penjelasan, penjelasan, penjelasan, dan lainnya. Komponen bersama harus hadir agar komponen hasil bisa bekerja.

Komponen faset

Komponen faset mencantumkan faset yang tersedia di hasil pencarian. Setiap faset mengklasifikasikan respon di sepanjang dimensi tertentu, seperti penulis. Anda dapat memperbaiki pencarian ke faset tertentu dengan memilih salah satu dari daftar.

Setelah Anda memilih sebuah facet, komponen akan memanggil`Query`dengan filter atribut yang membatasi pencarian ke dokumen yang cocok dengan faset.

Komponen paginasi

Komponen pagination memungkinkan Anda untuk menampilkan hasil pencarian`Query`API di beberapa halaman. Ini memanggil`Query`API dengan`PageSize`dan`PageNumber`parameter untuk mendapatkan halaman hasil tertentu.

Membangun pengalaman pencarian tanpa kode

Anda dapat membangun dan menerapkanAmazon Kendracari aplikasi tanpa perlu kode front-end apa pun.Amazon Kendra Pembangun Pengalamanmembantu Anda membangun dan menyebarkan aplikasi pencarian yang berfungsi penuh dalam beberapa klik sehingga Anda dapat segera mulai mencari. Anda dapat mendesain halaman pencarian Anda dan menyesuaikan pencarian Anda untuk menyesuaikan pengalaman dengan kebutuhan pengguna Anda.Amazon Kendramenghasilkan URL titik akhir yang unik dan sepenuhnya dihosting dari halaman pencarian Anda untuk mulai mencari dokumen dan FAQ Anda. Anda dapat dengan cepat membangun bukti konsep pengalaman pencarian Anda dan membagikannya dengan orang lain.

Anda menggunakan template pengalaman pencarian yang tersedia di builder untuk menyesuaikan pencarian Anda. Anda dapat mengundang orang lain untuk berkolaborasi dalam membangun pengalaman penelusuran Anda, atau mengevaluasi hasil penelusuran untuk tujuan penyetelan. Setelah pengalaman pencarian Anda siap bagi pengguna Anda untuk mulai mencari, Anda cukup membagikan URL endpoint yang aman.

Cara kerja Experience Builder pencarian

Keseluruhan proses membangun pengalaman pencarian adalah sebagai berikut:

1. Anda membuat pengalaman pencarian dengan memberinya nama, deskripsi, dan memilih sumber data yang ingin Anda gunakan untuk pengalaman pencarian Anda.
2. Anda mengonfigurasi daftar pengguna dan grup AndaAWS IAM Identity Centerdan kemudian berikan mereka hak akses ke pengalaman pencarian Anda. Anda termasuk diri Anda sebagai pemilik pengalaman. Untuk informasi selengkapnya, lihat the section called “Menyediakan akses ke halaman pencarian”.
3. Anda membukaAmazon KendraExperience Builder untuk merancang dan menyetel halaman pencarian Anda. Anda dapat membagikan URL titik akhir pengalaman penelusuran Anda dengan orang lain yang Anda tetapkan sendiri hak akses edit atau hak akses lihat-penelusuran.

Anda memanggilCreateExperienceAPI untuk membuat dan mengonfigurasi pengalaman penelusuran Anda. Jika Anda menggunakan konsol, Anda memilih indeks Anda dan kemudian pilihPengalamandi menu navigasi untuk mengonfigurasi pengalaman Anda.

Rancang dan sesuaikan pengalaman pencarian Anda

Setelah membuat dan mengonfigurasi pengalaman penelusuran, Anda membuka pengalaman penelusuran menggunakan URL titik akhir untuk mulai menyesuaikan pencarian Anda sebagai pemilik dengan hak akses editor. Anda mengetik kueri Anda ke dalam kotak pencarian, lalu menyesuaikan pencarian Anda menggunakan opsi pengeditan di panel samping untuk melihat bagaimana penerapannya ke halaman Anda. Ketika Anda siap untuk mempublikasikan, pilihPublikasikan. Anda juga dapat beralihBeralih ke tampilan langsung, untuk melihat versi terbaru yang diterbitkan dari halaman pencarian Anda, danBeralih ke mode build, untuk mengedit atau menyesuaikan halaman pencarian Anda.

Berikut ini adalah cara Anda dapat menyesuaikan pengalaman pencarian Anda.

Filter

Tambahkan pencarian segi atau filter berdasarkan atribut dokumen. Berikut ini termasuk atribut yang disesuaikan. Anda dapat menambahkan filter menggunakan bidang metadata yang dikonfigurasi sendiri. Misalnya, untuk pencarian segi menurut setiap kategori kota, gunakan`_category`atribut dokumen kustom yang berisi semua kategori kota.

Jawaban yang disarankan

Tambahkan jawaban yang dihasilkan pembelajaran mesin ke kueri pengguna Anda. Sebagai contoh,“Seberapa sulit kursus ini?”.Amazon Kendradapat mengambil teks yang paling relevan di semua dokumen yang mengacu pada kesulitan kursus dan menyarankan jawaban yang paling relevan.

Pertanyaan yang Sering Diajukan

Tambahkan dokumen FAQ untuk memberikan jawaban atas pertanyaan yang sering diajukan. Sebagai contoh,“Berapa jam untuk menyelesaikan kursus ini?”.Amazon Kendradapat menggunakan dokumen FAQ yang berisi jawaban atas pertanyaan ini dan memberikan jawaban yang benar.

Urutkan

Tambahkan penyortiran hasil pencarian sehingga pengguna Anda dapat mengatur hasil berdasarkan relevansi, waktu yang dibuat, waktu terakhir diperbarui, dan kriteria penyortiran lainnya.

Dokumen

Konfigurasikan bagaimana dokumen atau hasil pencarian ditampilkan di halaman pencarian Anda. Anda dapat mengonfigurasi berapa banyak hasil yang ditampilkan pada halaman, menyertakan pagination seperti nomor halaman, mengaktifkan tombol umpan balik pengguna, dan mengatur bagaimana bidang metadata dokumen ditampilkan dalam hasil pencarian.

Bahasa

Pilih bahasa untuk memfilter hasil pencarian atau dokumen dalam bahasa yang dipilih.

Kotak pencarian

Konfigurasikan ukuran dan teks placeholder kotak pencarian Anda, serta izinkan saran kueri.

Penyetelan relevansi

Tambahkan boosting ke bidang metadata dokumen untuk memberi bobot lebih pada bidang ini saat pengguna Anda mencari dokumen. Anda dapat menambahkan bobot yang dimulai dari 1 dan secara bertahap meningkat menjadi 10. Anda dapat meningkatkan teks, tanggal, dan jenis bidang numerik. Misalnya, untuk memberi`_last_updated_at`dan`_created_at`lebih berat atau penting daripada bidang lain, berikan bidang ini bobot 1 hingga 10, tergantung pada kepentingannya. Anda dapat menerapkan konfigurasi penyetelan relevansi yang berbeda untuk setiap aplikasi atau pengalaman pencarian.

Menyediakan akses ke halaman pencarian

Akses ke pengalaman pencarian Anda adalah melalui IAM Identity Center. Saat mengonfigurasi pengalaman penelusuran, Anda memberi orang lain yang terdaftar di direktori Pusat Identitas Anda akses keAmazon Kendrahalaman pencarian. Mereka menerima email yang mengarahkan mereka untuk masuk menggunakan kredensialnya di IAM Identity Center untuk mengakses halaman pencarian. Anda harus menyiapkan Pusat Identitas IAM di tingkat organisasi atau tingkat pemegang akun diAWS Organizations. Untuk informasi lebih lanjut tentang pengaturan Pusat Identitas IAM, lihatMemulai Pusat Identitas IAM.

Anda mengaktifkan identitas pengguna di IAM Identity Center dengan pengalaman pencarian Anda dan menetapkanPenampilatauPemilikakses izin menggunakan API atau konsol.

- Penampil: Diizinkan untuk mengeluarkan pertanyaan, menerima jawaban yang disarankan yang relevan dengan pencarian mereka, dan menyumbangkan umpan balik merekaAmazon Kendrasehingga terus meningkatkan pencarian.
- Pemilik: Diizinkan untuk menyesuaikan desain halaman pencarian, menyetel pencarian, dan menggunakan aplikasi pencarian sebagaiPenampil. Menonaktifkan akses ke pemirsa di konsol saat ini tidak didukung.

Untuk menetapkan akses orang lain ke pengalaman penelusuran Anda, pertama-tama Anda mengaktifkan identitas pengguna di Pusat Identitas IAM denganAmazon KendraPengalaman dengan menggunakanExperienceConfigurationobjek. Anda menentukan nama bidang yang berisi pengidentifikasi pengguna Anda seperti nama pengguna atau alamat email. Anda kemudian memberikan daftar pengguna akses ke pengalaman penelusuran Anda menggunakanAssociateEntitiesToExperienceAPI dan tentukan izinnya sebagaiPenampilatauPemilikmenggunakanAssociatePersonasToEntitiesAPI. Anda menentukan setiap pengguna atau grup menggunakanEntityConfigurationobjek dan apakah pengguna atau grup itu adalahPenampilatauPemilikmenggunakanEntityPersonaConfiguratonobjek.

Untuk menetapkan akses orang lain ke pengalaman pencarian Anda menggunakan konsol, Anda harus terlebih dahulu membuat pengalaman dan mengonfirmasi identitas Anda dan bahwa Anda adalah pemilik. Kemudian Anda dapat menetapkan pengguna atau grup lain sebagai pemirsa atau pemilik. Di konsol, pilih indeks Anda dan kemudian pilihPengalamanDi menu navigasi. Setelah Anda membuat pengalaman Anda, Anda dapat memilih pengalaman Anda dari daftar. Pergi keManajemen aksesuntuk menetapkan pengguna atau grup sebagai pemirsa atau pemilik.

Mengonfigurasi pengalaman penelusuran

Berikut ini adalah contoh pengalaman pencarian.

Console

Untuk membuatAmazon Kendrapengalaman pencarian

1. Di panel navigasi kiri, di bawahIndeks, pilihPengalamandan kemudian pilihCiptakan pengalaman.
2. PadaKonfigurasikan pengalamanHalaman, masukkan nama dan penjelasan untuk pengalaman Anda, pilih sumber konten, lalu pilih peran IAM untuk pengalaman Anda. Untuk informasi lebih lanjut tentang peran IAM, lihatPeran IAM untukAmazon Kendrapengalaman.

3. PadaKonfirmasikan identitas Anda dari direktori Pusat Identitashalaman, pilih ID pengguna Anda seperti email Anda. Jika Anda tidak memiliki direktori Pusat Identitas, cukup masukkan nama lengkap dan email Anda untuk membuat direktori Pusat Identitas. Ini termasuk Anda sebagai pengguna pengalaman dan secara otomatis memberi Anda hak akses pemilik.
4. PadaTinjau untuk membuka Experience Builderhalaman, tinjau detail konfigurasi AndaCiptakan pengalaman dan buka Experience Builderuntuk mulai mengedit halaman pencarian Anda.

CLI

Untuk membuatAmazon Kendrapengalaman

```
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

Untuk membuatAmazon Kendrapengalaman

```
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

Untuk membuatAmazon 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.");
    }
}
```

Menyesuaikan kapasitas

Amazon Kendra menyediakan sumber daya untuk indeks Anda dalam unit kapasitas. Setiap unit kapasitas menyediakan sumber daya tambahan untuk indeks Anda. Ada unit kapasitas terpisah untuk penyimpanan dokumen dan untuk kueri. Anda hanya dapat menambahkan unit kapasitas ke indeks Amazon Kendra Enterprise Edition. Anda tidak dapat menambahkan kapasitas ke indeks Edisi Pengembang.

Unit kapasitas penyimpanan dokumen menyediakan penyimpanan tambahan berikut untuk indeks Anda.

- 100.000 dokumen atau penyimpanan 30 GB.

Satu unit kapasitas kueri menyediakan kueri tambahan berikut untuk indeks Anda.

- 0,1 kueri per detik atau sekitar 8.000 kueri per hari.

Setiap indeks dilengkapi dengan kapasitas dasar sama dengan 1 unit kapasitas (penyimpanan 30 GB dan 0,1 kueri per detik). Ada biaya tambahan untuk setiap unit kapasitas tambahan. Untuk detailnya, lihat Amazon Kendra harga.

Anda dapat menambahkan hingga 100 unit kapasitas tambahan ke penyimpanan dan sumber daya kueri untuk indeks. Jika Anda membutuhkan lebih banyak unit, cukup hubungi Support.

Anda dapat menyesuaikan unit kapasitas hingga 5 kali per hari agar sesuai dengan kebutuhan penggunaan Anda. Anda tidak dapat mengurangi kapasitas penyimpanan dokumen di bawah jumlah dokumen yang disimpan dalam indeks Anda. Misalnya, jika Anda menyimpan 150.000 dokumen, Anda tidak dapat mengurangi kapasitas penyimpanan di bawah 1 unit tambahan.

Anda dapat melihat sumber daya yang digunakan indeks di konsol dengan memilih nama indeks untuk membuka setelan indeks dan informasi lainnya, atau Anda dapat menggunakan DescribeIndexAPI.

Amazon Kendra juga mengembalikan pengecualian ketika Anda melebihi kapasitas indeks. Anda mendapatkan `ServiceQuotaExceededException` ketika ukuran total yang diekstraksi dari semua dokumen melebihi batas untuk indeks. Anda mendapatkan `InvalidRequest` untuk setiap dokumen ketika jumlah dokumen melebihi batas untuk indeks. Anda mendapatkan `ThrottlingException`

ketika jumlah kueri per detik melebihi batas. Untuk informasi lebih lanjut tentang batasan, lihat Kuota untuk Amazon Kendra.

Akumulasi kueri akan bertahan hingga 24 jam.

Kapasitas penayangan

Lihat sumber daya yang digunakan indeks Anda dengan Amazon Kendra konsol dengan memilih nama indeks Anda untuk mengakses detailnya. Konsol juga menyediakan grafik penggunaan sehingga Anda dapat menentukan berapa banyak penyimpanan dan kapasitas kueri yang digunakan indeks Anda. Anda dapat menggunakan informasi ini untuk membantu merencanakan kapan harus menambahkan kapasitas tambahan.

Untuk melihat penyimpanan dokumen dan penggunaan kueri (konsol)

1. Masuk ke AWS Management Console dan buka Amazon Kendra konsol di https://console.aws.amazon.com/kendra/home.
2. Dari daftar indeks, pilih indeks yang ingin Anda akses.
3. Gulir ke bagian pengaturan untuk melihat total penyimpanan dokumen dan kapasitas kueri saat ini.

Untuk melihat kapasitas menggunakan Amazon Kendra API, gunakan `CapacityUnits` parameter di DescribeIndexAPI.

Menambahkan dan menghapus kapasitas

Jika Anda membutuhkan kapasitas tambahan untuk indeks Anda, Anda dapat menambahkannya menggunakan konsol atau Amazon Kendra API.

Untuk menambah atau menghapus kapasitas penyimpanan atau kueri (konsol)

1. Masuk ke AWS Management Console dan buka Amazon Kendra konsol di https://console.aws.amazon.com/kendra/home.
2. Dari daftar indeks, pilih indeks yang ingin Anda akses.
3. Pilih Edit, atau pilih Edit dari dropdown Tindakan.
4. Pilih Berikutnya untuk pergi ke halaman detail penyediaan.

5. Menambah atau menghapus penyimpanan dokumen dan/atau unit kapasitas kueri.
6. Lanjutkan untuk memilih Berikutnya untuk pergi ke halaman ulasan dan kemudian pilih Perbarui untuk menyimpan perubahan Anda.

Setelah Anda memperbarui kapasitas indeks Anda, perlu beberapa menit agar perubahan diterapkan.

Untuk menambah atau menghapus kapasitas menggunakan Amazon Kendra API, gunakan `CapacityUnits` parameter di UpdateIndexAPI.

Amazon Kendra Kapasitas Peringkat Cerdas

Unit kapasitas menyediakan permintaan skor ulang tambahan berikut per detik untuk rencana eksekusi skor ulang. Rencana eksekusi rescore adalah sumber daya yang digunakan untuk menyediakan API Rescore.

- 0,01 permintaan per detik.

Setiap rencana eksekusi rescore dilengkapi dengan kapasitas dasar sama dengan 1 unit kapasitas (0,01 permintaan per detik). Ada biaya tambahan untuk setiap unit kapasitas tambahan. Untuk detailnya, lihat Amazon Kendra harga.

Anda dapat menambahkan hingga 1000 unit kapasitas tambahan untuk rencana eksekusi skor ulang. Jika Anda membutuhkan lebih banyak unit, cukup hubungi Support.

Kapasitas saran kueri

Saat menggunakan saran kueri, ada kapasitas kueri dasar 2,5 GetQuerySuggestionspanggilan per detik. Kapasitas `GetQuerySuggestions` lima kali lebih banyak dibanding kapasitas kueri yang ditetapkan untuk indeks, atau kapasitas dasar sebanyak 2,5 panggilan per detik, mana pun yang lebih tinggi. Sebagai contoh, kapasitas dasar untuk indeks adalah 0,1 kueri per detik, dan kapasitas `GetQuerySuggestions` memiliki dasar 2,5 panggilan per detik. Jika Anda menambahkan 0,1 kueri per detik lainnya ke total 0,2 kueri per detik untuk satu indeks, kapasitas `GetQuerySuggestions` adalah 2,5 panggilan per detik (lebih tinggi dari lima kali 0,2 kueri per detik).

Amazon Kendra kapasitas pengalaman

Kapasitas pengalaman pencarian

Amazon Kendra mulai membatasi`Query`,`QuerySuggestions`, `SubmitFeedback` untuk Amazon Kendra pengalaman Anda pada 15 permintaan per detik dan 40 permintaan per detik untuk ledakan kueri. Untuk indeks dengan lebih dari 150 unit kapasitas kueri, batasan ini masih berlaku.

Misalnya, unit kapasitas kueri untuk indeks Anda adalah 150, sehingga aplikasi pengalaman penelusuran Anda dapat menangani 15 permintaan per detik. Namun, jika Anda menskalakan hingga 200 unit kapasitas kueri, maka aplikasi pengalaman penelusuran Anda hanya akan menangani 15 permintaan per detik. Jika Anda membatasi indeks hingga 100 unit kapasitas kueri, maka aplikasi pengalaman penelusuran Anda hanya akan menangani 10 permintaan per detik.

Pemecahan kueri adaptif

Amazon Kendra memiliki kapasitas dasar yang disediakan 1 unit kapasitas kueri. Anda dapat menggunakan hingga 8.000 kueri per hari dengan throughput minimum 0,1 kueri per detik (per unit kapasitas kueri). Akumulasi kueri akan bertahan hingga 24 jam dan dapat mengakomodasi semburan lalu lintas. Jumlah burst yang diizinkan bervariasi karena tergantung pada beban cluster pada waktu tertentu. Menyediakan unit kapasitas kueri yang cukup untuk menangani tingkat beban puncak Anda.

Pendekatan adaptif untuk menangani semburan lalu lintas yang tidak terduga di luar throughput yang disediakan adalah ledakan kueri adaptif bawaan Amazon Kendra. Ledakan kueri adaptif tersedia di Edisi Perusahaan. Amazon Kendra

Ledakan kueri adaptif adalah kemampuan bawaan yang memungkinkan Anda menerapkan kapasitas kueri yang tidak digunakan untuk menangani lalu lintas yang tidak terduga. Amazon Kendra mengakumulasi kueri yang tidak terpakai pada kueri yang disediakan per detik, setiap detik, hingga jumlah kueri maksimum yang telah Anda berikan untuk indeks Anda. Amazon Kendra Kueri akumulasi ini digunakan untuk lalu lintas tak terduga di atas kapasitas yang dialokasikan. Performa optimal pemecahan kueri adaptif dapat bervariasi, tergantung pada beberapa faktor seperti ukuran indeks total, kompleksitas kueri, akumulasi kueri yang tidak terpakai, dan beban keseluruhan pada indeks Anda. Sebaiknya lakukan tes beban Anda sendiri untuk mengukur kapasitas pemecahan secara akurat.

Memulai

Bagian ini menunjukkan cara membuat sumber data dan menambahkan dokumen Anda ke Amazon Kendra indeks. Instruksi disediakan untuk AWS konsol,AWS CLI, program Python menggunakanAWS SDK for Python (Boto3), dan program Java menggunakan. AWS SDK for Java

Topik

Prasyarat

Langkah-langkah berikut adalah prasyarat untuk memulai latihan. Langkah-langkah tersebut menunjukkan cara mengatur akun, membuat IAM peran yang memberikan Amazon Kendra izin untuk melakukan panggilan atas nama Anda, dan mengindeks dokumen dari Amazon S3 bucket. Bucket S3 digunakan sebagai contoh, tetapi Anda dapat menggunakan sumber data lain yang Amazon Kendra mendukung. Lihat Sumber data.

Daftar Akun AWS

Jika Anda tidak memiliki Akun AWS, selesaikan langkah-langkah berikut untuk membuatnya.

Untuk mendaftar Akun AWS

1. Buka https://portal.aws.amazon.com/billing/signup.
2. Ikuti petunjuk secara online.

   Anda akan diminta untuk menerima panggilan telepon dan memasukkan kode verifikasi pada keypad telepon sebagai bagian dari prosedur pendaftaran.

Saat Anda mendaftar Akun AWS, Pengguna root akun AWS dibuat. Pengguna root memiliki akses ke semua Layanan AWS dan sumber daya dalam akun. Sebagai praktik terbaik keamanan, tetapkan akses administratif ke pengguna administratif, dan hanya gunakan pengguna root untuk melakukan tugas yang memerlukan akses pengguna root.

AWS akan mengirimkan email konfirmasi kepada Anda setelah proses pendaftaran selesai. Anda dapat melihat aktivitas akun saat ini dan mengelola akun dengan mengunjungi https://aws.amazon.com/ dan memilih Akun Saya.

Membuat pengguna administratif

Setelah Anda mendaftarAkun AWS, amankanPengguna root akun AWS, aktifkanAWS IAM Identity Center, dan buat pengguna administratif sehingga Anda tidak menggunakan pengguna root untuk tugas sehari-hari.

Mengamankan Pengguna root akun AWS Anda

1. Masuk ke AWS Management Console sebagai pemilik akun dengan memilih Pengguna root dan memasukkan alamat email Akun AWS Anda. Pada halaman berikutnya, masukkan kata sandi Anda.

   Untuk bantuan masuk menggunakan pengguna root, lihat Masuk sebagai pengguna root dalam Panduan Pengguna AWS Sign-In.

2. Mengaktifkan autentikasi multi-faktor (MFA) untuk pengguna root Anda.

   Untuk petunjuk, lihat Mengaktifkan perangkat MFA virtual untuk pengguna root Akun AWS Anda (konsol) dalam Panduan Pengguna IAM.

Membuat pengguna administratif

1. Aktifkan Pusat Identitas IAM.

   Untuk petunjuk, lihat Mengaktifkan AWS IAM Identity Center di Panduan AWS IAM Identity Center Pengguna.

2. Di Pusat Identitas IAM, berikan akses administratif ke pengguna administratif.

Untuk tutorial tentang menggunakan Direktori Pusat Identitas IAM sebagai sumber identitas Anda, lihat Mengkonfigurasi akses pengguna dengan default Direktori Pusat Identitas IAM di Panduan AWS IAM Identity Center Pengguna.

Masuk sebagai pengguna administratif

- Untuk masuk dengan pengguna Pusat Identitas IAM, gunakan URL masuk yang dikirim ke alamat email Anda saat Anda membuat pengguna Pusat Identitas IAM.

  Untuk bantuan masuk menggunakan pengguna Pusat Identitas IAM, lihat Masuk ke portal akses AWS dalam Panduan Pengguna AWS Sign-In.

- Jika Anda menggunakan bucket S3 yang berisi dokumen untuk mengujiAmazon Kendra, buat bucket S3 di wilayah yang sama dengan yang Anda gunakan. Amazon Kendra Untuk petunjuknya, lihat Membuat dan Mengonfigurasi Bucket S3 di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.

  Unggah dokumen ke bucket S3 Anda. Untuk petunjuk, lihat Mengunggah, Mengunduh, dan Mengelola Objek di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.

  Jika Anda menggunakan sumber data lain, Anda harus memiliki situs aktif dan kredensialnya untuk terhubung ke sumber data.

Jika Anda menggunakan konsol untuk memulai, mulailah denganMemulai dengan Amazon Kendra konsol.

Amazon Kendrasumber daya:AWS CLI, SDK, konsol

Ada izin tertentu yang diperlukan jika Anda menggunakan CLI, SDK, atau konsol.

Amazon KendraUntuk menggunakan CLI, SDK, atau konsol, Anda harus memiliki izin Amazon Kendra untuk memungkinkan membuat dan mengelola sumber daya atas nama Anda. Bergantung pada kasus penggunaan Anda, izin ini mencakup akses ke Amazon Kendra API itu sendiri, AWS KMS keys jika Anda ingin mengenkripsi data Anda melalui CMK kustom, direktori Pusat Identitas jika Anda ingin mengintegrasikan dengan AWS IAM Identity Center atau membuat Pengalaman Pencarian. Untuk daftar lengkap izin untuk kasus penggunaan yang berbeda, lihat IAMperan.

Pertama, Anda harus melampirkan izin di bawah ini ke pengguna IAM Anda.

```
{
  "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": "*"
    }
  ]
}
```

Kedua, jika Anda menggunakan CLI atau SDK, Anda juga harus membuat IAM peran dan kebijakan untuk mengakses. Amazon CloudWatch Logs Jika Anda menggunakan konsol, Anda tidak perlu membuat IAM peran dan kebijakan untuk ini. Anda membuat ini sebagai bagian dari prosedur konsol.

Untuk membuat IAM peran dan kebijakan untuk SDK AWS CLI dan SDK yang Amazon Kendra memungkinkan Anda Amazon CloudWatch Logs mengakses.

1. Masuk ke AWS Management Console dan buka konsol IAM di https://console.aws.amazon.com/iam/.
2. Pada menu kiri, pilih Kebijakan, lalu pilih Buat kebijakan.
3. Pilih JSON dan ganti kebijakan default dengan hal berikut:

```
{
    "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. Pilih Tinjau kebijakan.
5. Beri nama kebijakan"KendraPolicyForGettingStartedIndex", lalu pilih Buat kebijakan.
6. Pada menu kiri, pilih Peran, lalu pilih Buat peran.
7. Pilih AWSAkun lain, lalu ketik ID akun Anda di ID Akun. Pilih Next: Permissions (Selanjutnya: Izin).
8. Pilih kebijakan yang Anda buat di atas lalu pilih Berikutnya: Tag
9. Jangan tambahkan tag apa pun. Pilih Next: Review (Selanjutnya: Tinjauan).
10. Beri nama peran "KendraRoleForGettingStartedIndex" dan kemudian pilih Buat peran.

11. Pilih peran yang baru Anda buat. Pilih nama peran untuk membuka ringkasan. Pilih Hubungan kepercayaan kemudian pilih Sunting hubungan kepercayaan.
12. Ganti hubungan kepercayaan yang ada dengan hal berikut:

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

13. Pilih Perbarui Kebijakan Kepercayaan.

Ketiga, jika Anda menggunakan file Amazon S3 untuk menyimpan dokumen atau menggunakan S3 untuk mengujiAmazon Kendra, Anda juga harus membuat IAM peran dan kebijakan untuk mengakses bucket Anda. Jika Anda menggunakan sumber data lain, lihat IAMperan untuk sumber data.

Untuk membuat IAM peran dan kebijakan yang memungkinkan Amazon Kendra untuk mengakses dan mengindeks Amazon S3 bucket Anda.

1. Masuk ke AWS Management Console dan buka konsol IAM di https://console.aws.amazon.com/iam/.
2. Pada menu kiri, pilih Kebijakan, lalu pilih Buat kebijakan.
3. Pilih JSON dan ganti kebijakan default dengan hal berikut:

```
{
    "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. Pilih Tinjau kebijakan.
5. Beri nama kebijakan "KendraPolicyForGettingStartedDataSource" dan kemudian pilih Buat kebijakan.
6. Pada menu kiri, pilih Peran, lalu pilih Buat peran.
7. Pilih AWSAkun lain, lalu ketik ID akun Anda di ID Akun. Pilih Next: Permissions (Selanjutnya: Izin).
8. Pilih kebijakan yang Anda buat di atas lalu pilih Berikutnya: Tag
9. Jangan tambahkan tag apa pun. Pilih Next: Review (Selanjutnya: Tinjauan).
10. Beri nama peran "KendraRoleForGettingStartedDataSource" dan kemudian pilih Buat peran.
11. Pilih peran yang baru Anda buat. Pilih nama peran untuk membuka ringkasan. Pilih Hubungan kepercayaan kemudian pilih Sunting hubungan kepercayaan.
12. Ganti hubungan kepercayaan yang ada dengan hal berikut:

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

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

13. Pilih Perbarui Kebijakan Kepercayaan.

Bergantung pada bagaimana Anda ingin menggunakan Amazon Kendra API, lakukan salah satu hal berikut.

- Memulai (AWS CLI)
- Memulai (AWS SDK for Java)
- Memulai (AWS SDK for Python (Boto3))

Memulai dengan Amazon Kendra konsol

Prosedur berikut menunjukkan cara membuat dan menguji Amazon Kendra indeks dengan menggunakan AWS konsol. Dalam prosedur Anda membuat indeks dan sumber data untuk indeks. Terakhir, Anda menguji indeks Anda dengan membuat permintaan pencarian.

Langkah 1: Untuk membuat indeks (konsol)

1. Masuk ke Konsol AWS Manajemen dan buka Amazon Kendra konsol di https://console.aws.amazon.com/kendra/.
2. Pilih Buat indeks di bagian Indeks.
3. Di halaman Tentukan detail indeks, beri indeks Anda nama dan deskripsi.
4. Dalam IAMperan, pilih Buat peran baru dan kemudian beri nama peran. IAMPeran akan memiliki awalan "AmazonKendra-”.
5. Biarkan bidang lain dengan defaultnya. Pilih Selanjutnya.
6. Di halaman Konfigurasikan kontrol akses pengguna, pilih Selanjutnya.
7. Di halaman Detail penyediaan, pilih Edisi Developer.

8. Pilih Buat untuk membuat indeks Anda.
9. Tunggu indeks Anda dibuat. Amazon Kendramenyediakan perangkat keras untuk indeks Anda. Operasi ini dapat memakan waktu lama.

Langkah 2: Untuk menambahkan sumber data ke indeks (konsol)

1. Lihat sumber data yang tersedia untuk menghubungkan dan Amazon Kendra mengindeks dokumen Anda.
2. Di panel navigasi, pilih Sumber data lalu pilih Tambahkan sumber data untuk sumber data pilihan Anda.
3. Ikuti langkah-langkah untuk mengkonfigurasi sumber data.

Langkah 3: Untuk mencari indeks (konsol)

1. Di panel navigasi, pilih opsi untuk mencari indeks Anda.
2. Masukkan istilah penelusuran yang sesuai untuk indeks Anda. hasil teratas dan hasil dokumen teratas ditampilkan.

Memulai (AWS CLI)

Prosedur berikut menunjukkan cara membuat Amazon Kendra indeks menggunakanAWS CLI. Prosedur menciptakan sumber data, indeks, dan menjalankan kueri pada indeks.

Untuk membuat Amazon Kendra indeks (CLI)

1. Lakukan Prasyarat.
2. Masukkan perintah berikut untuk membuat indeks.

```
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. Tunggu Amazon Kendra untuk membuat indeks. Periksa progres dengan menggunakan perintah berikut. Ketika bidang status `ACTIVE`, lanjutkan ke langkah berikutnya.

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

```
 --id index id
```

4. Pada prompt perintah, masukkan perintah berikut untuk membuat sumber data.

```
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"}}'
```

   Jika Anda terhubung ke sumber data menggunakan skema templat, konfigurasikan skema templat.

```
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. Butuh Amazon Kendra beberapa saat untuk membuat sumber data. Masukkan perintah berikut untuk memeriksa progres. Ketika bidang status `ACTIVE`, lanjutkan ke langkah berikutnya.

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

6. Masukkan perintah berikut untuk menyinkronkan sumber data.

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

7. Amazon Kendraakan mengindeks sumber data Anda. Jumlah waktu yang dibutuhkan tergantung pada jumlah dokumen. Anda dapat memeriksa status tugas sinkron menggunakan perintah berikut. Ketika bidang status `ACTIVE`, lanjutkan ke langkah berikutnya.

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

8. Masukkan perintah berikut untuk membuat kueri.

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

Hasil pencarian ditampilkan dalam format JSON.

Memulai (AWS SDK for Python (Boto3))

Program berikut adalah contoh penggunaan Amazon Kendra dalam program Python. Program melakukan tugas berikut:

1. Menciptakan indeks baru menggunakan operasi CreateIndex.
2. Menunggu pembuatan indeks selesai. Menggunakan metode operasi DescribeIndex untuk memantau status indeks.
3. Setelah indeks aktif, itu menciptakan sumber data menggunakan operasi CreateDataSource.
4. Menunggu pembuatan sumber data selesai. Menggunakan metode operasi DescribeDataSource untuk memantau status sumber data.
5. Ketika sumber data aktif, itu akan menyinkronkan indeks dengan isi sumber data menggunakan operasi StartDataSourceSyncJob.

```
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.")
```

Memulai (AWS SDK for Java)

Program berikut adalah contoh penggunaan Amazon Kendra dalam program Java. Program melakukan tugas berikut:

1. Menciptakan indeks baru menggunakan operasi CreateIndex.
2. Menunggu pembuatan indeks selesai. Menggunakan metode operasi DescribeIndex untuk memantau status indeks.
3. Setelah indeks aktif, itu menciptakan sumber data menggunakan operasi CreateDataSource.
4. Menunggu pembuatan sumber data selesai. Menggunakan metode operasi DescribeDataSource untuk memantau status sumber data.
5. Ketika sumber data aktif, itu akan menyinkronkan indeks dengan isi sumber data menggunakan operasi StartDataSourceSyncJob.

```
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");
    }
}
```

Memulai dengan sumber Amazon S3 data (konsol)

Anda dapat menggunakan Amazon Kendra konsol untuk mulai menggunakan Amazon S3 bucket sebagai penyimpanan data. Bila Anda menggunakan konsol tersebut, Anda menentukan informasi koneksi yang Anda butuhkan untuk mengindeks isi bucket. Untuk informasi selengkapnya, lihat Amazon S3.

Gunakan prosedur berikut untuk membuat sumber data bucket S3 dasar menggunakan konfigurasi default. Prosedur ini mengasumsikan bahwa Anda telah membuat indeks mengikuti langkah-langkah di langkah 1 dari Memulai dengan Amazon Kendra konsol.

Untuk membuat sumber data bucket S3 menggunakan konsol Amazon Kendra

1. Masuk ke AWS Management Console dan buka Amazon Kendra konsol di https://console.aws.amazon.com/kendra/home.
2. Dari daftar indeks, pilih indeks yang ingin Anda tambahkan sumber data.
3. Pilih Tambah sumber data.
4. Dari daftar konektor sumber data, pilih Amazon S3.
5. Pada halaman Tentukan atribut, berikan nama sumber data dan jika perlu, tambahkan deskripsi. Kosongkan bidang Tag. Pilih Selanjutnya untuk melanjutkan.
6. Di bidang Masukkan lokasi sumber data, masukkan nama bucket S3 yang berisi dokumen Anda. Anda dapat memasukkan nama secara langsung, atau Anda dapat menelusuri nama dengan memilih Telusuri. Bucket harus berada di Wilayah yang sama dengan indeks.
7. Dalam IAMperan pilih Buat peran baru, lalu ketik nama peran. Untuk informasi selengkapnya, lihat IAMperan untuk sumber Amazon S3 data.
8. Di bagian Atur jadwal jalan sinkronisasi, pilih Jalankan sesuai permintaan.
9. Pilih Selanjutnya untuk melanjutkan.
10. Pada halaman Tinjau dan buat, tinjau pengaturan untuk sumber data S3 Anda. Jika Anda ingin melakukan perubahan, pilih tombol Edit di samping item yang ingin Anda ubah. Bila Anda puas dengan pilihan Anda, pilih Buat untuk membuat sumber data S3.

Setelah Anda memilih Buat, Amazon Kendra mulailah membuat sumber data. Ini akan memerlukan beberapa menit hingga sumber data dibuat. Setelah selesai, status sumber data berubah dari Membuat menjadi Aktif.

Setelah membuat sumber data, Anda perlu menyinkronkan Amazon Kendra indeks dengan sumber data. Pilih Sinkronkan sekarang untuk memulai proses sinkronisasi. Diperlukan beberapa menit hingga beberapa jam untuk menyinkronkan sumber data, tergantung pada jumlah dan ukuran dokumen.

Memulai dengan sumber data database MySQL (konsol)

Anda dapat menggunakan Amazon Kendra konsol untuk memulai menggunakan database MySQL sebagai sumber data. Bila Anda menggunakan konsol tersebut, Anda menentukan informasi koneksi yang Anda butuhkan untuk mengindeks isi basis data MySQL. Untuk informasi lebih lanjut, lihat Menggunakan sumber data basis data.

Anda harus terlebih dahulu membuat basis data MySQL, maka Anda dapat membuat sumber data untuk basis data.

Gunakan prosedur berikut untuk membuat basis data MySQL dasar. Prosedur ini mengasumsikan bahwa Anda telah membuat indeks mengikuti langkah 1 dari Memulai dengan Amazon Kendra konsol.

Untuk membuat basis data MySQL

1. Masuk ke AWS Management Console dan buka konsol Amazon RDS di https://console.aws.amazon.com/rds/.
2. Di panel navigasi, pilih Grup subnet, kemudian pilih Buat Grup Subnet DB.
3. Beri nama grup dan pilih Virtual Private Cloud (VPC) Anda. Untuk informasi selengkapnya tentang mengonfigurasi VPC, lihat Mengkonfigurasi Amazon Kendra untuk menggunakan VPC.
4. Tambahkan subnet pribadi VPC Anda. Subnet pribadi Anda adalah orang-orang yang tidak terhubung ke NAT Anda. Pilih Create (Buat).
5. Di panel navigasi, pilih Basis data, lalu pilih Buat basis data.
6. Gunakan parameter berikut untuk membuat basis data. Biarkan parameter lain dalam posisi default.

   - Opsi mesin —MySQL
   - Template —Tingkat gratis
   - Pengaturan Kredensi —Masukkan dan konfirmasikan kata sandi
   - Dalam Konektivitas, pilih Konfigurasi konektivitas tambahan. Lakukan pilihan berikut.
     - Grup subnet —Pilih grup subnet yang Anda buat pada langkah 4.
     - Grup keamanan VPC —Pilih grup yang berisi aturan masuk dan keluar yang Anda buat di VPC Anda. Sebagai contoh, **`DataSourceSecurityGroup`**. Untuk informasi selengkapnya tentang mengonfigurasi VPC, lihat Mengkonfigurasi Amazon Kendra untuk menggunakan VPC.
   - Di bawah Konfigurasi tambahan, atur Nama basis data awal ke **`content`**.
7. Pilih Buat basis data.
8. Dari daftar basis data, pilih basis data baru Anda. Buat catatan tentang titik akhir basis data.
9. Setelah Anda membuat basis data Anda, Anda harus membuat tabel untuk menyimpan dokumen Anda. Membuat tabel ada di luar lingkup petunjuk ini. Saat membuat tabel Anda, perhatikan hal berikut ini:

- Nama database— **`content`**
- Nama tabel— **`documents`**
- Columns—**`ID`**,**`Title`**,**`Body`**, dan**`LastUpdate`**. Anda dapat menyertakan kolom tambahan jika Anda ingin.

Sekarang Anda telah membuat basis data MySQL, maka Anda dapat membuat sumber data untuk basis data.

Untuk membuat basis data MySQL

1. Masuk ke AWS Management Console dan buka Amazon Kendra konsol di https://console.aws.amazon.com/kendra/home.
2. Di panel navigasi, pilih indeks lalu pilih indeks Anda.
3. Pilih Tambahkan sumber data lalu pilih Amazon RDS.
4. Ketik nama dan deskripsi untuk sumber data kemudian pilih Selanjutnya.
5. Pilih MySQL.
6. Di bawah Akses koneksi, masukkan informasi berikut:
   - Endpoint —Titik akhir dari database yang Anda buat sebelumnya.
   - Port —Nomor port untuk database. Untuk MySQL, default-nya adalah 3306.
   - Jenis otentikasi —Pilih Baru.
   - Nama kontainer rahasia baru —Sebuah nama untuk Secrets Manager wadah untuk kredenial database.
   - Nama pengguna —Nama pengguna dengan akses administratif ke database.
   - Kata Sandi —Kata sandi untuk pengguna, lalu pilih Simpan otentikasi.
   - Nama database —**`content`**.
   - Nama tabel —**`documents`**.
   - Peran IAM —Pilih Buat peran baru, lalu ketik nama untuk peran tersebut.
7. Dalam Konfigurasi kolom masukkan hal berikut:
   - Nama kolom ID dokumen — **`ID`**
   - Nama kolom judul dokumen - **`Title`**
   - Nama kolom data dokumen - **`Body`**

8. Dalam Deteksi perubahan kolom masukkan perintah berikut:
   - Ubah kolom pendeteksian - **`LastUpdate`**
9. Dalam Konfigurasi VPC & grup keamanan berikan perintah berikut:
   - Dalam Virtual Private Cloud (VPC) Pilih VPC Anda.
   - Dalam Subnet, Pilih subnet privat yang sudah Anda buat di VPC Anda.
   - Dalam Grup keamanan VPC, pilih grup keamanan yang berisi aturan inbound dan outbound yang Anda buat di VPC untuk basis data MySQL Anda. Sebagai contoh, **`DataSourceSecurityGroup`**.
10. Dalam Atur jadwal pelaksanaan sinkronisasi pilih Jalankan sesuai permintaan lalu pilih Selanjutnya.
11. Dalam Pemetaan bidang sumber data pilih Selanjutnya.
12. Tinjau konfigurasi sumber data Anda untuk memastikan bahwa itu benar. Ketika Anda puas bahwa semuanya sudah benar, pilih Buat.

Memulai dengan sumber AWS IAM Identity Center identitas (konsol)

Sumber AWS IAM Identity Center identitas berisi informasi tentang pengguna dan grup Anda. Ini berguna untuk menyiapkan pemfilteran konteks pengguna, di mana Amazon Kendra memfilter hasil pencarian untuk pengguna yang berbeda berdasarkan akses pengguna atau grup mereka ke dokumen.

Untuk membuat sumber identitas Pusat Identitas IAM, Anda harus mengaktifkan Pusat Identitas IAM dan membuat organisasi di. AWS Organizations Ketika Anda mengaktifkan IAM Identity Center dan membuat organisasi untuk pertama kalinya, secara otomatis default ke direktori Pusat Identitas sebagai sumber identitas. Anda dapat mengubah ke Active Directory (Amazon dikelola atau dikelola sendiri) atau penyedia identitas eksternal sebagai sumber identitas Anda. Anda harus mengikuti panduan yang benar untuk ini — lihat Mengubah sumber identitas Pusat Identitas IAM Anda. Anda hanya dapat memiliki satu sumber identitas per organisasi.

Agar pengguna dan grup Anda diberi tingkat akses yang berbeda ke dokumen, Anda harus menyertakan pengguna dan grup Anda dalam daftar kontrol akses saat Anda memasukkan dokumen ke dalam indeks Anda. Ini memungkinkan pengguna dan grup Anda untuk mencari dokumen sesuai

dengan tingkat akses mereka. Amazon Kendra Saat Anda mengeluarkan kueri, ID pengguna harus sama persis dengan nama pengguna di Pusat Identitas IAM.

Anda juga harus memberikan izin yang diperlukan untuk menggunakan Pusat Identitas IAM dengan. Amazon Kendra Untuk informasi selengkapnya, lihat IAM peran untuk Pusat Identitas IAM.

Untuk menyiapkan sumber identitas Pusat Identitas IAM

1. Buka konsol Pusat Identitas IAM.
2. Pilih Aktifkan Pusat Identitas IAM, lalu pilih Buat AWS organisasi.

   Direktori Pusat Identitas dibuat secara default, dan email dikirimkan kepada Anda untuk memverifikasi alamat email yang terkait dengan organisasi.
3. Untuk menambahkan grup ke AWS organisasi Anda, di panel navigasi, pilih Grup.
4. Pada halaman Grup, pilih Buat grup dan masukkan nama dan deskripsi grup di kotak dialog. Pilih Buat.
5. Untuk menambahkan pengguna ke Organizations Anda, di panel navigasi, pilih Pengguna.
6. Pada halaman Pengguna, pilih Tambah pengguna. Di bawah Rincian pengguna, tentukan semua bidang yang diperlukan. Untuk Kata Sandi, pilih Kirim email ke pengguna. Pilih Berikutnya.
7. Untuk menambahkan pengguna ke grup, pilih Grup dan pilih grup.
8. Pada halaman Detail, di bawah Anggota grup, pilih Tambah pengguna.
9. Pada halaman Tambahkan pengguna ke grup, pilih pengguna yang ingin Anda tambahkan sebagai anggota grup. Anda dapat memilih beberapa pengguna untuk ditambahkan ke grup.
10. Untuk menyinkronkan daftar pengguna dan grup Anda dengan IAM Identity Center, ubah sumber identitas Anda menjadi Active Directory atau penyedia identitas eksternal.

    Direktori Pusat Identitas adalah sumber identitas default dan mengharuskan Anda menambahkan pengguna dan grup secara manual menggunakan sumber ini jika Anda tidak memiliki daftar sendiri yang dikelola oleh penyedia. Untuk mengubah sumber identitas Anda, Anda harus mengikuti panduan yang benar untuk ini—lihat Mengubah sumber identitas Pusat Identitas IAM Anda.

> **Note**
>
> Jika menggunakan Active Directory atau penyedia identitas eksternal sebagai sumber identitas Anda, Anda harus memetakan alamat email pengguna Anda ke nama pengguna IAM Identity Center saat Anda menentukan protokol System for Cross-domain Identity Management (SCIM). Untuk informasi lebih lanjut, lihat panduan Pusat Identitas IAM di SCIM untuk mengaktifkan Pusat Identitas IAM.

Setelah Anda mengatur sumber identitas Pusat Identitas IAM Anda, Anda dapat mengaktifkannya di konsol saat Anda membuat atau mengedit indeks Anda. Buka Kontrol akses pengguna di pengaturan indeks Anda dan edit pengaturan Anda untuk memungkinkan pengambilan informasi grup pengguna dari Pusat Identitas IAM.

Anda juga dapat mengaktifkan IAM Identity Center menggunakan UserGroupResolutionConfigurationobjek. Anda memberikan `UserGroupResolutionMode` as `AWS_SSO` dan membuat IAM peran yang memberikan izin untuk meneleponsso:ListDirectoryAssociations,sso-directory:SearchUsers,sso-directory:ListGroupsForUser,sso-directory:DescribeGroups.

> **Warning**
>
> Amazon Kendra saat ini tidak mendukung penggunaan `UserGroupResolutionConfiguration` dengan akun anggota AWS organisasi untuk sumber identitas Pusat Identitas IAM Anda. Anda harus membuat indeks Anda di akun manajemen untuk organisasi agar dapat digunakan`UserGroupResolutionConfiguration`.

Berikut ini adalah ikhtisar tentang cara mengatur sumber data dengan `UserGroupResolutionConfiguration` dan kontrol akses pengguna untuk memfilter hasil pencarian pada konteks pengguna. Ini mengasumsikan Anda telah membuat indeks dan IAM peran untuk indeks. Anda membuat indeks dan memberikan IAM peran menggunakan CreateIndexAPI.

Menyiapkan sumber data dengan **`UserGroupResolutionConfiguration`** dan pemfilteran konteks pengguna

1. Buat IAM peran yang memberikan izin untuk mengakses sumber identitas Pusat Identitas IAM Anda.
2. Konfigurasikan `UserGroupResolutionConfiguration`dengan mengatur mode ke `AWS_SSO` dan panggil UpdateIndexuntuk memperbarui indeks Anda untuk menggunakan IAM Identity Center.
3. Jika Anda ingin menggunakan kontrol akses pengguna berbasis token untuk memfilter hasil penelusuran pada konteks pengguna, setel UserContextPolicyke `USER_TOKEN` saat Anda menelepon. `UpdateIndex` Jika tidak, Amazon Kendra crawl daftar kontrol akses untuk setiap dokumen Anda untuk sebagian besar konektor sumber data. Anda juga dapat memfilter hasil penelusuran pada konteks pengguna di Query API dengan memberikan informasi pengguna dan grup di`UserContext`. Anda juga dapat memetakan pengguna ke grup mereka PutPrincipalMappingsehingga Anda hanya perlu memberikan ID pengguna saat mengeluarkan kueri.
4. Buat IAM peran yang memberikan izin untuk mengakses sumber data Anda.
5. Konfigurasikan sumber data Anda. Anda harus memberikan informasi koneksi yang diperlukan untuk terhubung ke sumber data Anda.
6. Buat sumber data menggunakan CreateDataSourceAPI. Berikan `DataSourceConfiguration` objek, yang mencakup`TemplateConfiguration`, ID indeks Anda, IAM peran untuk sumber data Anda, tipe sumber data, dan beri nama sumber data Anda. Anda juga dapat memperbarui sumber data Anda.

Mengubah sumber identitas Pusat Identitas IAM

> **Warning**
>
> Mengubah sumber identitas Anda di Pengaturan Pusat Identitas IAM dapat memengaruhi pelestarian informasi pengguna dan grup. Untuk melakukan ini dengan aman, disarankan Anda meninjau Pertimbangan untuk mengubah sumber identitas Anda. Saat Anda mengubah sumber identitas Anda, ID sumber identitas baru akan dihasilkan. Periksa Anda menggunakan ID yang benar sebelum Anda mengatur mode ke `AWS_SSO` in UserGroupResolutionConfiguration.

Untuk mengubah sumber identitas Pusat Identitas IAM

1. Buka Pusat Identitas IAM> konsol.
2. Pilih Pengaturan.
3. Pada halaman Pengaturan, di bawah Sumber identitas, pilih Ubah.
4. Pada halaman Ubah sumber identitas, pilih sumber identitas pilihan Anda, lalu pilih Berikutnya.

Membuat indeks

Anda dapat membuat indeks menggunakan konsol, atau dengan memanggil CreateIndexAPI. Anda dapat menggunakan AWS Command Line Interface (AWS CLI) atau SDK dengan API. Setelah Anda membuat indeks Anda, Anda dapat menambahkan dokumen langsung ke sana atau dari sumber data.

Untuk membuat indeks, Anda harus memberikan Amazon Resource Name (ARN) peran AWS Identity and Access Management (IAM) agar indeks dapat diakses. CloudWatch Untuk informasi selengkapnya, lihat IAM peran untuk indeks.

Tab berikut menyediakan prosedur untuk membuat indeks dengan menggunakan, dan contoh kode untuk menggunakan AWS Management Console, dan Python dan Java SDK. AWS CLI

Console

Untuk membuat indeks

1. Masuk ke Konsol AWS Manajemen dan buka Amazon Kendra konsol di https://console.aws.amazon.com/kendra/.
2. Pilih Buat indeks di bagian Indeks.
3. Pada Tentukan detail indeks, beri indeks Anda nama dan deskripsi.
4. Dalam IAM peran memberikan IAM peran. Untuk menemukan peran, pilih dari peran di akun Anda yang berisi kata “kendra” atau masukkan nama peran lain. Untuk informasi selengkapnya tentang izin yang diperlukan peran, lihat IAM peran untuk indeks.
5. Pilih Berikutnya.
6. Di halaman Konfigurasikan kontrol akses pengguna, pilih Selanjutnya. Anda dapat memperbarui indeks untuk menggunakan token untuk kontrol akses setelah membuat indeks. Untuk informasi selengkapnya, lihat Mengontrol akses ke dokumen.
7. Pada halaman Detail penyediaan, pilih Buat.
8. Mungkin perlu beberapa waktu untuk membuat indeks. Periksa daftar indeks untuk melihat kemajuan pembuatan indeks Anda. Ketika status indeks `ACTIVE`, indeks Anda siap digunakan.

AWS CLI

Untuk membuat indeks

1. Gunakan perintah berikut ini untuk membuat indeks. `role-arn`Harus berupa Nama Sumber Daya Amazon (ARN) dari IAM peran yang dapat menjalankan Amazon Kendra tindakan. Untuk informasi selengkapnya, lihat IAM peran.

   Perintah ini diformat untuk Linux dan macOS. Jika menggunakan Windows, ganti karakter kelanjutan baris Unix (\) dengan caret (^).

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

2. Mungkin perlu beberapa waktu untuk membuat indeks. Untuk memeriksa status indeks Anda, gunakan ID indeks yang dikembalikan `create-index` dengan perintah berikut. Ketika status indeks `ACTIVE`, indeks Anda siap digunakan.

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

Python

Untuk membuat indeks

- Berikan nilai untuk variabel berikut dalam contoh kode berikut:
  - `description`—Deskripsi indeks yang Anda buat. Ini bersifat opsional.
  - `index_name`—Nama indeks yang Anda buat.
  - `role_arn`—Nama Sumber Daya Amazon (ARN) dari peran yang dapat Amazon Kendra menjalankan API. Untuk informasi selengkapnya, lihat IAM peran.

  ```
  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

Untuk membuat indeks

- Berikan nilai untuk variabel berikut dalam contoh kode berikut:
  - `description`—Deskripsi indeks yang Anda buat. Ini bersifat opsional.
  - `index_name`—Nama indeks yang Anda buat.
  - `role_arn`—Nama Sumber Daya Amazon (ARN) dari peran yang dapat Amazon Kendra menjalankan API. Untuk informasi selengkapnya, lihat IAM peran.

```
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.");
    }
}
```

Setelah Anda membuat indeks Anda, Anda menambahkan dokumen ke dalamnya. Anda dapat menambahkannya secara langsung atau membuat sumber data yang memperbarui indeks Anda pada jadwal reguler.

Topik

- Menambahkan dokumen langsung ke indeks dengan batch upload
- Menambahkan pertanyaan yang sering diajukan (FAQ) ke indeks
- Membuat bidang dokumen kustom
- Mengontrol akses pengguna ke dokumen dengan token

Menambahkan dokumen langsung ke indeks dengan batch upload

Anda dapat menambahkan dokumen langsung ke indeks menggunakan BatchPutDocumentAPI. Anda tidak dapat menambahkan dokumen secara langsung menggunakan konsol tersebut. Jika Anda menggunakan konsol, Anda terhubung ke sumber data untuk menambahkan dokumen ke indeks Anda. Dokumen dapat ditambahkan dari bucket S3 atau disediakan sebagai data biner. Untuk daftar jenis dokumen yang didukung oleh Amazon Kendra lihat Jenis dokumen.

Menambahkan dokumen ke indeks menggunakan `BatchPutDocument` adalah operasi asinkron. Setelah Anda memanggil `BatchPutDocument` API, Anda menggunakan BatchGetDocumentStatusAPI untuk memantau kemajuan pengindeksan dokumen Anda. Ketika Anda memanggil `BatchGetDocumentStatus` API dengan daftar ID dokumen, ia mengembalikan status dokumen. Ketika status dokumen menjadi `INDEXED` atau `FAILED`, pemrosesan dokumen selesai. Ketika statusnya`FAILED`, `BatchGetDocumentStatus` API mengembalikan alasan bahwa dokumen tidak dapat diindeks.

Jika Anda ingin mengubah bidang atau atribut metadata konten dan dokumen selama proses penyerapan dokumen, lihat Pengayaan Dokumen Kustom. Amazon Kendra Jika Anda ingin menggunakan sumber data kustom, setiap dokumen yang Anda kirimkan menggunakan `BatchPutDocument` API memerlukan ID sumber data dan ID eksekusi sebagai atribut atau bidang. Untuk informasi selengkapnya, lihat Atribut yang diperlukan untuk sumber data kustom.

> **Note**
>
> Setiap ID dokumen harus unik per indeks. Anda tidak dapat membuat sumber data untuk mengindeks dokumen Anda dengan ID uniknya dan kemudian menggunakan `BatchPutDocument` API untuk mengindeks dokumen yang sama, atau sebaliknya. Anda dapat menghapus sumber data dan kemudian menggunakan `BatchPutDocument` API untuk mengindeks dokumen yang sama, atau sebaliknya. Menggunakan `BatchPutDocument` dan `BatchDeleteDocument` API dalam kombinasi dengan konektor sumber Amazon Kendra data untuk kumpulan dokumen yang sama dapat menyebabkan ketidakkonsistenan dengan data Anda. Sebagai gantinya, sebaiknya gunakan konektor sumber data Amazon Kendra khusus.

Dokumen panduan pengembang berikut menunjukkan cara menambahkan dokumen langsung ke indeks.

Topik

Menambahkan dokumen dengan BatchPutDocument API

Contoh berikut menambahkan gumpalan teks ke indeks dengan memanggil BatchPutDocument. Anda dapat menggunakan `BatchPutDocument` API untuk menambahkan dokumen langsung ke indeks Anda. Untuk daftar jenis dokumen yang didukung oleh Amazon Kendra lihat Jenis dokumen.

Untuk contoh membuat indeks menggunakan AWS CLI dan SDK, lihat Membuat indeks. Untuk mengatur CLI dan SDK, lihat Menyiapkan. Amazon Kendra

> **Note**
>
> File yang ditambahkan ke indeks harus dalam pengaliran byte yang dikodekan dengan UTF-8.

Dalam contoh berikut, teks yang dikodekan UTF-8 ditambahkan ke indeks.

CLI

Dalam AWS Command Line Interface, gunakan perintah berikut. Perintah ini diformat untuk Linux dan macOS. Jika menggunakan Windows, ganti karakter kelanjutan baris Unix (\) dengan caret (^).

```
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));
    }
}
```

Menambahkan dokumen dari bucket S3

Anda dapat menambahkan dokumen langsung ke indeks Anda dari Amazon S3 bucket menggunakan BatchPutDocumentAPI. Anda dapat menambahkan hingga 10 dokumen dalam panggilan yang sama. Saat menggunakan bucket S3, Anda harus memberikan IAM peran dengan izin untuk mengakses bucket yang berisi dokumen Anda. Anda menentukan peran dalam parameter `RoleArn`.

Menggunakan BatchPutDocumentAPI untuk menambahkan dokumen dari Amazon S3 bucket adalah operasi satu kali. Agar indeks tetap disinkronkan dengan isi bucket, buat sumber Amazon S3 data. Untuk informasi selengkapnya, lihat sumber Amazon S3 data.

Untuk contoh membuat indeks menggunakan AWS CLI dan SDK, lihat Membuat indeks. Untuk mengatur CLI dan SDK, lihat Menyiapkan. Amazon Kendra Untuk informasi tentang membuat bucket S3, lihat Amazon Simple Storage Service dokumentasi.

Dalam contoh berikut, dua dokumen Microsoft Word ditambahkan ke indeks menggunakan `BatchPutDocument` API.

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::${acccountID}:policy/${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));
    }
}
```

Menambahkan pertanyaan yang sering diajukan (FAQ) ke indeks

Anda dapat menambahkan pertanyaan umum (FAQ) langsung ke indeks Anda menggunakan konsol atau API. CreateFaq Menambahkan FAQ ke indeks adalah operasi asinkron. Anda meletakkan data untuk FAQ dalam file yang Anda simpan dalam Amazon Simple Storage Service ember. Anda dapat menggunakan file CSV atau JSON sebagai masukan untuk FAQ Anda:

- CSV dasar—File CSV di mana setiap baris berisi pertanyaan, jawaban, dan URI sumber opsional.
- CSV kustom—File CSV yang berisi pertanyaan, jawaban, dan header untuk bidang/atribut khusus yang dapat Anda gunakan untuk memfaksi, menampilkan, atau mengurutkan respons FAQ. Anda juga dapat menentukan bidang kontrol akses untuk membatasi respons FAQ untuk pengguna dan grup tertentu yang diizinkan untuk melihat respons FAQ.
- JSON—File JSON yang berisi pertanyaan, jawaban, dan bidang/atribut khusus yang dapat Anda gunakan untuk memfaksikan, menampilkan, atau mengurutkan tanggapan FAQ. Anda juga dapat menentukan bidang kontrol akses untuk membatasi respons FAQ untuk pengguna dan grup tertentu yang diizinkan untuk melihat respons FAQ.

Misalnya, berikut ini adalah file CSV dasar yang memberikan jawaban atas pertanyaan tentang klinik gratis di Spokane, Washington AS dan Mountain View, Missouri, AS.

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

> **Note**
>
> File FAQ harus berupa file yang dikodekan UTF-8.

Topik

Membuat kolom indeks untuk file FAQ

Saat Anda menggunakan file CSV atau JSON khusus untuk masukan, Anda dapat mendeklarasikan bidang khusus untuk pertanyaan FAQ Anda. Misalnya, Anda dapat membuat bidang kustom yang menetapkan setiap pertanyaan FAQ departemen bisnis. Ketika FAQ dikembalikan sebagai tanggapan, Anda dapat menggunakan departemen sebagai aspek untuk mempersempit pencarian menjadi “SDM” atau “Keuangan” saja, misalnya.

Bidang kustom harus dipetakan ke bidang indeks. Di konsol, Anda menggunakan halaman definisi Facet untuk membuat bidang indeks. Saat menggunakan API, Anda harus terlebih dahulu membuat bidang indeks menggunakan UpdateIndexAPI.

Jenis bidang/atribut dalam file FAQ harus cocok dengan jenis bidang indeks terkait. Misalnya, bidang “Departemen” adalah bidang `STRING_LIST` tipe. Jadi, Anda harus memberikan nilai untuk bidang departemen sebagai daftar string di file FAQ Anda. Anda dapat memeriksa jenis bidang indeks menggunakan halaman definisi Facet di konsol atau dengan menggunakan DescribeIndexAPI.

Ketika membuat bidang indeks yang dipetakan ke atribut kustom, Anda dapat menandainya sebagai dapat ditampilkan, dapat dibuat faset, atau dapat diurutkan. Anda tidak dapat menjadikan atribut kustom dapat dicari.

Selain atribut kustom, Anda juga dapat menggunakan bidang Amazon Kendra cadangan atau umum dalam file CSV atau JSON kustom. Untuk informasi selengkapnya, lihat Atribut atau bidang dokumen.

File CSV dasar

Gunakan file CSV dasar saat Anda ingin menggunakan struktur sederhana untuk FAQ Anda. Dalam file CSV dasar, setiap baris memiliki dua atau tiga bidang: pertanyaan, jawaban, dan URI sumber opsional yang menunjuk ke dokumen dengan informasi lebih lanjut.

Isi file harus mengikuti RFC 4180 Common Format dan MIME Type for Comma-Separated Values (CSV) File.

Berikut ini adalah file FAQ dalam format CSV dasar.

```
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
```

File CSV kustom

Gunakan file CSV khusus saat Anda ingin menambahkan bidang/atribut khusus ke pertanyaan FAQ Anda. Untuk file CSV kustom, Anda menggunakan baris header dalam file CSV Anda untuk menentukan atribut tambahan.

File CSV harus berisi dua bidang wajib berikut:

- `_question`Pertanyaan yang sering diajukan
- `_answer`Jawaban atas pertanyaan yang sering diajukan

File Anda dapat berisi bidang Amazon Kendra cadangan dan bidang khusus. Berikut ini adalah contoh file CSV kustom.

```
_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
```

Isi file kustom harus mengikuti RFC 4180 Common Format dan MIME Type for Comma-Separated Values (CSV) File.

Berikut ini mencantumkan jenis bidang kustom:

- Tanggal — ISO 8601 yang dikodekan tanggal dan nilai waktu.

  Misalnya, 2012-03-25T 12:30:10 +01:00 adalah format tanggal-waktu ISO 8601 untuk 25 Maret 2012, pukul 12:30 (ditambah 10 detik) di zona waktu Eropa Tengah.
- Long—Angka, seperti. `1234`
- Nilai string — String. Jika string Anda berisi koma, lampirkan seluruh nilai dalam tanda kutip ganda (“) (misalnya,). `"custom attribute, and more"`
- Daftar String — daftar nilai string. Buat daftar nilai dalam daftar dipisahkan koma yang diapit tanda kutip (“) (misalnya,). `"item1, item2, item3"` Jika daftar hanya berisi satu entri, Anda dapat menghilangkan tanda kutip (misalnya,`item1`).

File CSV khusus dapat berisi bidang kontrol akses pengguna. Anda dapat menggunakan bidang ini untuk membatasi akses ke FAQ untuk pengguna dan grup tertentu. Untuk memfilter konteks pengguna, pengguna harus memberikan informasi pengguna dan grup dalam kueri. Jika tidak, semua Pertanyaan yang Sering Diajukan yang relevan dikembalikan. Untuk informasi selengkapnya, lihat Pemfilteran konteks pengguna.

Berikut daftar filter konteks pengguna untuk FAQ:

- `_acl_user_allow`—Pengguna dalam daftar izinkan dapat melihat FAQ dalam respons kueri. Pertanyaan yang Sering Diajukan tidak dikembalikan ke pengguna lain.
- `_acl_user_deny`—Pengguna dalam daftar tolak tidak dapat melihat FAQ dalam respons kueri. FAQ dikembalikan ke semua pengguna lain jika relevan dengan kueri.
- `_acl_group_allow`—Pengguna yang merupakan anggota grup yang diizinkan dapat melihat FAQ dalam respons kueri. Pertanyaan yang Sering Diajukan tidak dikembalikan ke pengguna yang merupakan anggota grup lain.
- `_acl_group_deny`Pengguna yang merupakan anggota grup yang ditolak tidak dapat melihat FAQ dalam respons kueri. FAQ dikembalikan ke grup lain jika relevan dengan kueri.

Berikan nilai untuk daftar izinkan dan tolak dalam daftar yang dipisahkan koma yang diapit tanda kutip (misalnya,). `"user1,user2,user3"` Anda dapat menyertakan pengguna atau grup dalam daftar izinkan atau daftar penolakan, tetapi tidak keduanya di mana pengguna yang sama diizinkan secara individual tetapi juga grup ditolak. Jika menyertakan pengguna atau grup dalam keduanya, Anda akan menerima kesalahan.

Berikut ini adalah contoh file CSV kustom dengan informasi konteks pengguna.

```
_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
```

File JSON

Anda dapat menggunakan file JSON untuk memberikan pertanyaan, jawaban, dan bidang untuk indeks Anda. Anda dapat menambahkan salah satu bidang yang Amazon Kendra dicadangkan atau bidang khusus ke FAQ.

Berikut ini adalah skema untuk file JSON.

```
{
    "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
    ]
}
```

Contoh file JSON berikut menunjukkan dua dokumen FAQ. Salah satu dokumen hanya memiliki pertanyaan dan jawaban yang diperlukan. Dokumen lainnya juga mencakup bidang tambahan dan konteks pengguna atau informasi kontrol akses.

```
{
```

```
    "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"
               }
            ]
        }
    ]
}
```

Berikut ini mencantumkan jenis bidang kustom:

- Tanggal — Nilai string JSON dengan nilai tanggal dan waktu yang dikodekan ISO 8601. Misalnya, 2012-03-25T 12:30:10 +01:00 adalah format tanggal-waktu ISO 8601 untuk 25 Maret 2012, pukul 12:30 (ditambah 10 detik) di zona waktu Eropa Tengah.
- Panjang — Nilai nomor JSON, seperti. `1234`
- String—Nilai string JSON (misalnya,). `"custom attribute"`
- Daftar String-sebuah array JSON dari nilai string (misalnya,). `["item1,item2,item3"]`

File JSON dapat berisi bidang kontrol akses pengguna. Anda dapat menggunakan bidang ini untuk membatasi akses ke FAQ untuk pengguna dan grup tertentu. Untuk memfilter konteks

pengguna, pengguna harus memberikan informasi pengguna dan grup dalam kueri. Jika tidak, semua Pertanyaan yang Sering Diajukan yang relevan dikembalikan. Untuk informasi selengkapnya, lihat Pemfilteran konteks pengguna.

Anda dapat menyertakan pengguna atau grup dalam daftar izinkan atau daftar penolakan, tetapi tidak keduanya di mana pengguna yang sama diizinkan secara individual tetapi juga grup ditolak. Jika menyertakan pengguna atau grup dalam keduanya, Anda akan menerima kesalahan.

Berikut ini adalah contoh termasuk kontrol akses pengguna ke FAQ JSON.

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

Menggunakan file Pertanyaan yang Sering Diajukan

Setelah menyimpan file input FAQ Anda dalam bucket S3, Anda menggunakan konsol atau `CreateFaq` API untuk memasukkan pertanyaan dan jawaban ke dalam indeks Anda. Jika Anda ingin memperbarui FAQ, hapus FAQ dan buat lagi. Anda menggunakan `DeleteFaq` API untuk menghapus FAQ.

Anda harus memberikan IAM peran yang memiliki akses ke bucket S3 yang berisi file sumber Anda. Tentukan peran di konsol tersebut, atau di parameter `RoleArn`. Berikut ini adalah contoh menambahkan file FAQ ke indeks.

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));

    }
}
```

File FAQ dalam bahasa selain bahasa Inggris

Anda dapat mengindeks FAQ dalam bahasa yang didukung. Amazon Kendra mengindeks FAQ dalam bahasa Inggris secara default jika Anda tidak menentukan bahasa. Anda menentukan kode bahasa ketika Anda memanggil CreateFaqoperasi atau Anda dapat menyertakan kode bahasa untuk FAQ dalam metadata FAQ sebagai bidang. Jika FAQ tidak memiliki kode bahasa dalam metadatanya yang ditentukan dalam bidang metadata, FAQ diindeks menggunakan kode bahasa yang ditentukan saat Anda memanggil operasi. `CreateFAQ` Untuk mengindeks dokumen FAQ dalam bahasa yang didukung di konsol, buka FAQ dan pilih Tambah FAQ. Anda memilih bahasa dari Bahasa dropdown.

Membuat bidang dokumen kustom

Anda dapat membuat atribut atau bidang khusus untuk dokumen Anda di indeks Amazon Kendra Anda. Misalnya, Anda dapat membuat bidang atau atribut khusus yang disebut “Departemen” dengan nilai “HR”, “Penjualan”, dan “Manufaktur”. Jika Anda memetakan bidang atau atribut khusus ini ke indeks Amazon Kendra Anda, Anda dapat menggunakannya untuk memfilter hasil pencarian untuk menyertakan dokumen dengan atribut departemen “HR”, misalnya.

Sebelum Anda dapat menggunakan bidang atau atribut khusus, Anda harus terlebih dahulu membuat bidang dalam indeks. Gunakan konsol untuk mengedit pemetaan bidang sumber data untuk menambahkan bidang khusus atau menggunakan UpdateIndexAPI untuk membuat bidang indeks. Anda tidak dapat mengubah tipe data bidang setelah Anda membuat bidang.

Untuk sebagian besar sumber data, Anda memetakan bidang di sumber data eksternal ke bidang yang sesuai Amazon Kendra. Untuk informasi lebih lanjut, lihat Memetakan bidang sumber data. Untuk sumber data S3, Anda dapat membuat bidang atau atribut khusus menggunakan file metadata JSON.

Anda dapat membuat hingga 500 bidang atau atribut khusus.

Anda juga dapat menggunakan bidang yang Amazon Kendra dipesan atau umum. Untuk informasi selengkapnya, lihat Atribut atau bidang dokumen.

Topik

- Memperbarui bidang dokumen kustom

Memperbarui bidang dokumen kustom

Dengan `UpdateIndex` API, Anda menambahkan bidang atau atribut khusus menggunakan `DocumentMetadataConfigurationUpdates` parameter.

Contoh JSON berikut digunakan `DocumentMetadataConfigurationUpdates` untuk menambahkan bidang yang disebut “Departemen” ke indeks.

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

Bagian berikut mencakup contoh untuk menambahkan atribut atau bidang khusus menggunakan BatchPutDocumentdan untuk sumber data Amazon S3.

Topik

- Menambahkan atribut atau bidang khusus dengan BatchPutDocument API
- Menambahkan atribut atau bidang khusus ke sumber Amazon S3 data

Menambahkan atribut atau bidang khusus dengan BatchPutDocument API

Saat Anda menggunakan BatchPutDocumentAPI untuk menambahkan dokumen ke indeks, Anda menentukan bidang atau atribut khusus sebagai bagian dari`Attributes`. Anda dapat menambahkan beberapa bidang atau atribut saat memanggil API. Anda dapat membuat hingga 500 bidang atau atribut khusus. Contoh berikut adalah bidang atau atribut khusus yang menambahkan “Departemen” ke dokumen.

```
"Attributes":
```

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

Menambahkan atribut atau bidang khusus ke sumber Amazon S3 data

Saat Anda menggunakan bucket S3 sebagai sumber data untuk indeks Anda, Anda menambahkan metadata ke dokumen dengan file metadata pendamping. Letakkan file JSON metadata dalam struktur direktori yang paralel dengan dokumen Anda. Untuk informasi selengkapnya, lihat metadata dokumen S3.

Anda menentukan bidang kustom atau atribut dalam struktur `Attributes` JSON. Anda dapat membuat hingga 500 bidang atau atribut khusus. Misalnya, contoh berikut digunakan `Attributes` untuk menentukan tiga bidang atau atribut khusus dan satu bidang cadangan.

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

Langkah-langkah berikut memandu Anda untuk menambahkan atribut khusus ke sumber data Amazon S3.

Topik

- Langkah 1: Buat indeks Amazon Kendra
- Langkah 2: Perbarui indeks untuk menambahkan bidang dokumen khusus
- Langkah 3: Buat sumber data Amazon S3 dan petakan bidang sumber data ke atribut khusus

Langkah 1: Buat indeks Amazon Kendra

Ikuti langkah-langkah Membuat indeks untuk membuat indeks Amazon Kendra Anda.

Langkah 2: Perbarui indeks untuk menambahkan bidang dokumen khusus

Setelah membuat indeks, Anda menambahkan bidang ke dalamnya. Prosedur berikut menunjukkan cara menambahkan bidang ke indeks menggunakan konsol dan CLI.

Console

Untuk membuat bidang indeks

1. Pastikan Anda telah membuat indeks.
2. Kemudian, dari menu navigasi kiri, dari Manajemen data, pilih Definisi Facet.
3. Di Panduan pengaturan bidang Indeks, dari bidang Indeks, pilih Tambahkan bidang untuk menambahkan bidang khusus.
4. Dalam kotak dialog Add index field, lakukan hal berikut:
   - Nama bidang - Tambahkan nama bidang.
   - Tipe data - Pilih tipe data, apakah String, daftar String, atau Tanggal.
   - Jenis penggunaan — Pilih jenis penggunaan, apakah Facetable, Searchable, Displayable, dan Sortable.

     Kemudian, pilih Tambah.

   Ulangi langkah terakhir untuk bidang lain yang ingin Anda petakan.

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
        }
    }
...
]"
```

Langkah 3: Buat sumber data Amazon S3 dan petakan bidang sumber data ke atribut khusus

Untuk membuat sumber data Amazon S3 dan memetakan bidang ke sana, ikuti petunjuk di. Amazon S3

Jika Anda menggunakan API, gunakan `fieldMappings` atribut di bawah `configuration` saat Anda menggunakan CreateDataSourceAPI.

Untuk gambaran umum tentang cara bidang sumber data dipetakan, lihatMemetakan bidang sumber data.

Mengontrol akses pengguna ke dokumen dengan token

Anda dapat mengontrol pengguna atau grup mana yang dapat mengakses dokumen tertentu dalam indeks Anda atau melihat dokumen tertentu dalam hasil pencarian mereka. Ini disebut pemfilteran konteks pengguna. Ini adalah semacam pencarian yang dipersonalisasi dengan manfaat mengendalikan akses ke dokumen. Misalnya, tidak semua tim yang mencari informasi di portal perusahaan harus mengakses dokumen perusahaan rahasia, juga dokumen-dokumen ini tidak relevan untuk semua pengguna. Hanya pengguna atau grup tim tertentu yang diberi akses ke dokumen rahasia yang harus melihat dokumen-dokumen ini di hasil pencarian mereka.

Amazon Kendramendukung kontrol akses pengguna berbasis token menggunakan jenis token berikut:

- ID terbuka
- JWT dengan rahasia bersama
- JWT dengan kunci publik
- JSON

Amazon Kendramemberikan pencarian perusahaan yang sangat aman untuk aplikasi pencarian Anda. Hasil pencarian Anda mencerminkan model keamanan organisasi Anda. Pelanggan bertanggung jawab untuk mengautentikasi dan mengotorisasi pengguna untuk mendapatkan akses ke aplikasi pencariannya. Pada waktu pencarian,Amazon Kendrafilter layanan hasil pencarian berdasarkan ID pengguna yang disediakan oleh aplikasi pencarian pelanggan, dan daftar kontrol akses dokumen (ACL) yang dikumpulkan olehAmazon Kendrakonektor selama waktu merangkak/pengindeksan. Hasil pencarian mengembalikan URL yang mengarah kembali ke repositori dokumen asli ditambah kutipan singkat. Akses ke dokumen lengkap masih diberlakukan oleh repositori asli.

Topik

Menggunakan OpenID

Untuk mengonfigurasi Amazon Kendra indeks untuk menggunakan token OpenID untuk kontrol akses, Anda memerlukan URL JWKS (JSON Web Key Set) dari penyedia OpenID. Dalam kebanyakan kasus, URL JWKS dalam format berikut (jika mereka mengikuti penemuan OpenID). `https://domain-name/.well_known/jwks.json`

Contoh berikut menunjukkan cara menggunakan token OpenID untuk kontrol akses pengguna saat Anda membuat indeks.

Console

1. Pilih Buat indeks untuk mulai membuat indeks baru.
2. Pada Tentukan detail indeks, beri indeks Anda nama dan deskripsi.
3. Untuk IAM peran, pilih peran atau pilih Buat peran baru dan tentukan nama peran untuk membuat peran baru. Peran IAM akan memiliki awalan "AmazonKendra-”.
4. Biarkan bidang lain dengan defaultnya. Pilih Berikutnya.
5. Di halaman Konfigurasikan kontrol akses pengguna, di bawah Pengaturan kontrol akses, pilih Ya untuk menggunakan token untuk kontrol akses.
6. Di bawah Konfigurasi token, pilih OpenID sebagai Jenis token.

7. Menentukan URL kunci penandatanganan. URL harus mengarah ke satu set kunci web JSON.
8. Opsional Pada Konfigurasi lanjutan:
    a. Tentukan Nama pengguna untuk digunakan dalam pemeriksaan ACL.
    b. Tentukan satu atau lebih Grup untuk digunakan dalam pemeriksaan ACL.
    c. Tentukan Penerbit yang akan memvalidasi penerbit token.
    d. Tentukan Id Klien. Anda harus menentukan ekspresi reguler yang sesuai dengan audiens di JWT.
9. Di halaman Detail penyediaan, pilih Edisi Developer.
10. Pilih Buat untuk membuat indeks Anda.
11. Tunggu indeks Anda dibuat. Amazon Kendra menyediakan perangkat keras untuk indeks Anda. Operasi ini dapat memakan waktu lama.

CLI

Untuk membuat indeks dengan AWS CLI menggunakan file input JSON, pertama buat file JSON dengan parameter yang Anda inginkan:

```
{
    "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"
}
```

Anda dapat mengganti nama bidang pengguna dan grup default. Nilai default untuk `UserNameAttributeField` adalah "user". Nilai default untuk `GroupAttributeField` adalah "groups".

Selanjutnya, panggil `create-index` menggunakan file input. Misalnya, jika nama file JSON Anda adalah `create-index-openid.json`, Anda dapat menggunakan yang berikut ini:

```
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'
)
```

Menggunakan JSON Web Token (JWT) dengan rahasia bersama

Contoh berikut menunjukkan cara menggunakan JSON Web Token (JWT) dengan token rahasia bersama untuk kontrol akses pengguna saat Anda membuat indeks.

Console

1. Pilih Buat indeks untuk mulai membuat indeks baru.
2. Pada Tentukan detail indeks, beri indeks Anda nama dan deskripsi.

3. Untuk IAM role, pilih peran atau pilih Buat peran baru dan tentukan nama peran untuk membuat peran baru. IAM Peran akan memiliki awalan "AmazonKendra-”.
4. Biarkan bidang lain dengan defaultnya. Pilih Berikutnya.
5. Di halaman Konfigurasikan kontrol akses pengguna, di bawah Pengaturan kontrol akses, pilih Ya untuk menggunakan token untuk kontrol akses.
6. Di bawah Konfigurasi token, pilih JWT dengan rahasia bersama sebagai Jenis token.
7. Di bawah Parameter untuk menandatangani rahasia bersama, pilih Jenis rahasia. Anda dapat menggunakan rahasia bersama AWS Secrets Manager atau membuat rahasia bersama baru.

   Untuk membuat rahasia bersama baru, pilih Baru, lalu ikuti langkah-langkah ini:

   a. Di bawah AWS Secrets Manager Rahasia baru, tentukan nama Rahasia. Awalan `AmazonKendra-` akan ditambahkan saat Anda menyimpan kunci publik.
   b. Tentukan ID kunci. Kunci tersebut adalah petunjuk yang menunjukkan kunci yang digunakan untuk mengamankan tanda tangan web JSON (JWS) token.
   c. Pilih Algoritme penandatanganan untuk token. Ini adalah algoritme kriptografi yang digunakan untuk mengamankan token ID. Untuk informasi selengkapnya tentang RSA, lihat Kriptografi RSA.
   d. Tentukan rahasia Bersama dengan memasukkan rahasia yang dikodekan URL base64. Anda juga dapat memilih Hasilkan rahasia untuk membuat rahasia untuk Anda. Anda harus memastikan rahasianya adalah rahasia yang dikodekan URL base64.
   e. (Opsional) Tentukan kapan rahasia bersama valid. Anda dapat menentukan tanggal dan waktu berlaku atau berakhirnya rahasia, atau keduanya. Rahasia akan berlaku dalam interval yang ditentukan.
   f. Pilih Simpan rahasia untuk menyimpan rahasia baru.
8. (Opsional) Di bawah Konfigurasi lanjutan:

   a. Tentukan Nama pengguna untuk digunakan dalam pemeriksaan ACL.
   b. Tentukan satu atau lebih Grup untuk digunakan dalam pemeriksaan ACL.
   c. Tentukan Penerbit yang akan memvalidasi penerbit token.
   d. Tentukan ID Klaim. Anda harus menentukan ekspresi reguler yang cocok dengan audiens di JWT.
9. Di halaman Detail penyediaan, pilih Edisi Developer.
10. Pilih Buat untuk membuat indeks Anda.

11. Tunggu indeks Anda dibuat. Amazon Kendra menyediakan perangkat keras untuk indeks Anda. Operasi ini dapat memakan waktu lama.

CLI

Anda dapat menggunakan token JWT dengan rahasia bersama di dalamnya. AWS Secrets Manager Rahasianya harus berupa rahasia yang dikodekan URL base64. Anda memerlukan Secrets Manager ARN, dan Amazon Kendra peran Anda harus memiliki akses ke sumber `GetSecretValue` daya. Secrets Manager Jika Anda mengenkripsi Secrets Manager sumber daya dengan AWS KMS, peran juga harus memiliki akses ke tindakan dekripsi.

Untuk membuat indeks dengan AWS CLI menggunakan file input JSON, pertama buat file JSON dengan parameter yang Anda inginkan:

```
{
    "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"
}
```

Anda dapat mengganti nama bidang pengguna dan grup default. Nilai default untuk `UserNameAttributeField` adalah "user". Nilai default untuk `GroupAttributeField` adalah "groups".

Selanjutnya, panggil `create-index` menggunakan file input. Misalnya, jika nama file JSON Anda adalah `create-index-openid.json`, Anda dapat menggunakan yang berikut ini:

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

Rahasianya harus memiliki format berikut di 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"
    }
  ]
}
```

Untuk informasi selengkapnya tentang JWT, lihat jwt.io.

Python

Anda dapat menggunakan token JWT dengan rahasia bersama di dalamnya. AWS Secrets Manager Rahasianya harus berupa rahasia yang dikodekan URL base64. Anda memerlukan Secrets Manager ARN, dan Amazon Kendra peran Anda harus memiliki akses ke sumber `GetSecretValue` daya. Secrets Manager Jika Anda mengenkripsi Secrets Manager sumber daya dengan AWS KMS, peran juga harus memiliki akses ke tindakan dekripsi.

```
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'
)
```

Menggunakan JSON Web Token (JWT) dengan kunci publik

Contoh berikut menunjukkan cara menggunakan JSON Web Token (JWT) dengan kunci publik untuk kontrol akses pengguna saat Anda membuat indeks. Untuk informasi selengkapnya tentang JWT, lihat jwt.io.

Console

1. Pilih Buat indeks untuk mulai membuat indeks baru.
2. Pada Tentukan detail indeks, beri indeks Anda nama dan deskripsi.
3. Untuk IAM role, pilih peran atau pilih Buat peran baru dan tentukan nama peran untuk membuat peran baru. IAM Peran akan memiliki awalan "AmazonKendra-”.
4. Biarkan bidang lain dengan defaultnya. Pilih Berikutnya.
5. Di halaman Konfigurasikan kontrol akses pengguna, di bawah Pengaturan kontrol akses, pilih Ya untuk menggunakan token untuk kontrol akses.
6. Pada Konfigurasi token, pilih JWT dengan kunci publik sebagai Jenis token.
7. Di bawah Parameter untuk menandatangani kunci publik, pilih Jenis rahasia. Anda dapat menggunakan rahasia AWS Secrets Manager yang ada atau membuat rahasia bersama baru.

   Untuk membuat rahasia baru, pilih Baru, lalu ikuti langkah-langkah ini:

   a. Di bawah AWS Secrets Manager Rahasia baru, tentukan nama Rahasia. Awalan `AmazonKendra-` akan ditambahkan saat Anda menyimpan kunci publik.

   b. Tentukan ID kunci. Kunci tersebut adalah petunjuk yang menunjukkan kunci yang digunakan untuk mengamankan tanda tangan web JSON (JWS) token.

   c. Pilih Algoritme penandatanganan untuk token. Ini adalah algoritme kriptografi yang digunakan untuk mengamankan token ID. Untuk informasi selengkapnya tentang RSA, lihat Kriptografi RSA.

d. Pada Atribut sertifikat, tentukan Rangkaian sertifikat opsional. Rangkaian sertifikat terdiri dari daftar beberapa sertifikat. Rangkaian ini dimulai dengan sertifikat server dan berakhir dengan sertifikat akar.

e. Opsional Tentukan Sidik jari jempol atau sidik jari. Ini harus berupa hash sertifikat, dikomputasi atas semua data sertifikat dan tanda tangannya.

f. Tentukan Eksponen. Ini adalah nilai eksponen untuk kunci publik RSA. Hal ini direpresentasikan sebagai nilai yang dikodekan dengan Base64urlUInt.

g. Tentukan Modulus. Ini adalah nilai eksponen untuk kunci publik RSA. Hal ini direpresentasikan sebagai nilai yang dikodekan dengan Base64urlUInt.

h. Pilih Simpan kunci untuk menyimpan kunci baru.

8. Opsional Pada Konfigurasi lanjutan:

   a. Tentukan Nama pengguna untuk digunakan dalam pemeriksaan ACL.

   b. Tentukan satu atau lebih Grup untuk digunakan dalam pemeriksaan ACL.

   c. Tentukan Penerbit yang akan memvalidasi penerbit token.

   d. Tentukan Id Klien. Anda harus menentukan ekspresi reguler yang sesuai dengan audiens di JWT.

9. Di halaman Detail penyediaan, pilih Edisi Developer.

10. Pilih Buat untuk membuat indeks Anda.

11. Tunggu indeks Anda dibuat. Amazon Kendra menyediakan perangkat keras untuk indeks Anda. Operasi ini dapat memakan waktu lama.

CLI

Anda dapat menggunakan JWT dengan kunci publik di dalam AWS Secrets Manager. Anda memerlukan Secrets Manager ARN, dan Amazon Kendra peran Anda harus memiliki akses ke sumber `GetSecretValue` daya. Secrets Manager Jika Anda mengenkripsi Secrets Manager sumber daya dengan AWS KMS, peran juga harus memiliki akses ke tindakan dekripsi.

Untuk membuat indeks dengan AWS CLI menggunakan file input JSON, pertama buat file JSON dengan parameter yang Anda inginkan:

```
{
    "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"
}
```

Anda dapat mengganti nama bidang pengguna dan grup default. Nilai default untuk `UserNameAttributeField` adalah "user". Nilai default untuk `GroupAttributeField` adalah "groups".

Selanjutnya, panggil `create-index` menggunakan file input. Misalnya, jika nama file JSON Anda adalah `create-index-openid.json`, Anda dapat menggunakan yang berikut ini:

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

Rahasianya harus memiliki format berikut di 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 thumprint for x.509 cert",
      "x5c": [
        "certificate chain"
      ]
    }
  ]
```

```
}
```

Untuk informasi selengkapnya tentang JWT, lihat 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'
)
```

Menggunakan JSON

Contoh berikut menunjukkan cara menggunakan JSON untuk kontrol akses pengguna saat Anda membuat indeks.

> **Warning**
>
> Token JSON adalah muatan yang tidak divalidasi. Ini hanya boleh digunakan ketika permintaan Amazon Kendra datang dari server tepercaya dan tidak pernah dari browser.

Console

1. Pilih Buat indeks untuk mulai membuat indeks baru.
2. Pada Tentukan detail indeks, beri indeks Anda nama dan deskripsi.

3. Untuk IAM peran, pilih peran atau pilih Buat peran baru dan tentukan nama peran untuk membuat peran baru. IAM Peran akan memiliki awalan "AmazonKendra-".
4. Biarkan bidang lain dengan defaultnya. Pilih Berikutnya.
5. Di halaman Konfigurasikan kontrol akses pengguna, di bawah Pengaturan kontrol akses, pilih Ya untuk menggunakan token untuk kontrol akses.
6. Di bawah Konfigurasi token, pilih JSON sebagai Jenis token.
7. Tentukan nama Pengguna yang akan digunakan dalam pemeriksaan ACL.
8. Tentukan satu atau lebih Grup untuk digunakan dalam pemeriksaan ACL.
9. Pilih Berikutnya.
10. Di halaman Detail penyediaan, pilih Edisi Developer.
11. Pilih Buat untuk membuat indeks Anda.
12. Tunggu indeks Anda dibuat. Amazon Kendra menyediakan perangkat keras untuk indeks Anda. Operasi ini dapat memakan waktu lama.

CLI

Untuk membuat indeks dengan AWS CLI menggunakan file input JSON, pertama buat file JSON dengan parameter yang Anda inginkan:

```
{
    "Name": "user-context",
    "Edition": "ENTERPRISE_EDITION",
    "RoleArn": "arn:aws:iam::account-id:role:/my-role",
    "UserTokenConfigurations": [
        {
            "JsonTokenTypeConfiguration": {
                "UserNameAttributeField": "user",
                "GroupAttributeField": "group"
            }
        }
    ],
    "UserContextPolicy": "USER_TOKEN"
}
```

Selanjutnya, panggil `create-index` menggunakan file input. Misalnya, jika nama file JSON Anda adalah `create-index-openid.json`, Anda dapat menggunakan yang berikut ini:

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

Jika Anda tidak menggunakan Open ID untuk AWS IAM Identity Center, Anda dapat mengirimkan token dalam format JSON kepada kami. Jika demikian, Anda harus menentukan bidang mana dalam token JSON yang berisi nama pengguna dan bidang mana yang berisi grup. Nilai bidang grup harus berupa array string JSON. Misalnya, jika menggunakan SAML, token Anda akan seperti berikut:

```
{
     "username" : "user1",
     "groups": [
        "group1",
        "group2"
     ]
}
```

`TokenConfiguration` akan menentukan nama pengguna dan nama bidang grup:

```
{
    "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'
)
```

Membuat konektor sumber data

Anda dapat membuat konektor sumber data Amazon Kendra untuk menghubungkan dan mengindeks dokumen Anda. Amazon Kendra dapat terhubung ke Microsoft SharePoint, Google Drive, dan banyak penyedia lainnya. Saat Anda membuat konektor sumber data, Anda memberikan informasi konfigurasi Amazon Kendra yang diperlukan untuk terhubung ke repositori sumber Anda. Tidak seperti menambahkan dokumen langsung ke indeks, Anda dapat memindai sumber data secara berkala untuk memperbarui indeks.

Misalnya, katakanlah Anda memiliki gudang dokumen pajak yang disimpan dalam ember. Amazon S3 Dari waktu ke waktu, dokumen yang ada diubah dan dokumen baru ditambahkan ke repositori. Jika Anda menambahkan repositori Amazon Kendra sebagai sumber data, Anda dapat memperbarui indeks Anda dengan mengatur sinkronisasi berkala antara sumber data dan indeks Anda.

Anda dapat memilih untuk memperbarui indeks secara manual menggunakan konsol atau StartDataSourceSyncJobAPI. Jika tidak, Anda mengatur jadwal untuk memperbarui indeks dan menyinkronkannya dengan sumber data Anda.

Indeks dapat memiliki lebih dari satu sumber data. Setiap sumber data dapat memiliki jadwal pembaruannya sendiri. Misalnya, Anda dapat memperbarui indeks dokumen kerja Anda setiap hari, atau bahkan per jam, sembari memperbarui dokumen yang diarsipkan secara manual kapan pun arsip berubah.

Jika Anda ingin mengubah metadata dokumen atau atribut dan konten selama proses konsumsi dokumen, lihat Pengayaan Dokumen Kustom. Amazon Kendra

> **Note**
>
> Setiap ID dokumen harus unik per indeks. Anda tidak dapat membuat sumber data untuk mengindeks dokumen Anda dengan ID uniknya dan kemudian menggunakan `BatchPutDocument` API untuk mengindeks dokumen yang sama, atau sebaliknya. Anda dapat menghapus sumber data dan kemudian menggunakan `BatchPutDocument` API untuk mengindeks dokumen yang sama, atau sebaliknya. Menggunakan `BatchPutDocument` dan `BatchDeleteDocument` API dalam kombinasi dengan konektor sumber Amazon Kendra data untuk kumpulan dokumen yang sama dapat menyebabkan ketidakkonsistenan dengan data Anda. Sebagai gantinya, sebaiknya gunakan konektor sumber data Amazon Kendra khusus.

> **Note**
>
> File yang ditambahkan ke indeks harus dalam pengaliran byte yang dikodekan dengan UTF-8. Untuk informasi selengkapnya tentang dokumen di Amazon Kendra, lihat Dokumen.

Mengatur jadwal pembaruan

Konfigurasikan sumber data Anda untuk diperbarui secara berkala dengan konsol tersebut atau menggunakan parameter `Schedule` saat membuat atau memperbarui sumber data. Isi parameter adalah string yang menyimpan string jadwal `cron` -format atau string kosong untuk menunjukkan bahwa indeks diperbarui sesuai permintaan. Untuk format ekspresi cron, lihat Menjadwalkan Ekspresi untuk Aturan di Panduan Amazon CloudWatch Events Pengguna. Amazon Kendra hanya mendukung ekspresi cron. Itu tidak mendukung ekspresi tingkat.

Mengatur bahasa

Anda dapat mengindeks semua dokumen Anda dalam sumber data dalam bahasa yang didukung. Anda menentukan kode bahasa untuk semua dokumen Anda di sumber data Anda saat Anda menelepon CreateDataSource. Jika dokumen tidak memiliki kode bahasa yang ditentukan dalam bidang metadata, dokumen diindeks menggunakan kode bahasa yang ditentukan untuk semua dokumen di tingkat sumber data. Jika Anda tidak menentukan bahasa, Amazon Kendra indeks dokumen dalam sumber data dalam bahasa Inggris secara default. Untuk informasi selengkapnya tentang bahasa yang didukung, termasuk kodenya, lihat Menambahkan dokumen dalam bahasa selain bahasa Inggris.

Anda mengindeks semua dokumen dalam sumber data dalam bahasa yang didukung menggunakan konsol. Buka Sumber data dan edit sumber data Anda atau Tambahkan sumber data jika Anda menambahkan sumber data baru. Pada halaman Tentukan detail sumber data, pilih bahasa dari Bahasa tarik-turun. Anda memilih Perbarui atau terus memasukkan informasi konfigurasi untuk terhubung ke sumber data Anda.

Konektor sumber data

Bagian ini menunjukkan kepada Anda cara menghubungkan Amazon Kendra ke database yang didukung dan repositori sumber data menggunakan Amazon Kendra dalam AWS Management Console dan API. Amazon Kendra

Topik

- Microsoft SQL Server
- Tim Microsoft
- Microsoft Yammer
- MySQL
- Oracle Database
- PostgreSQL
- Menyindir
- Salesforce
- ServiceNow
- Kendur
- Zendesk

Skema templat sumber data

Berikut ini adalah skema template untuk sumber data di mana template didukung.

Topik

- Adobe Experience Managerskema templat
- Amazon FSx Skema templat (Windows)
- Amazon FSx Skema templat (NetApp ONTAP)
- Alfrescoskema templat
- Aurora Skema templat (MySQL)
- Aurora (PostgreSQL) skema templat
- Amazon RDS Skema templat (Microsoft SQL Server)
- Amazon RDS Skema templat (MySQL)
- Amazon RDS Skema templat (Oracle)
- Amazon RDS (PostgreSQL) skema templat
- Amazon S3 skema templat
- Amazon Kendra Skema Templat Perayap Web
- Skema templat pertemuan
- Skema templat Dropbox

- Skema template Drupal
- GitHub skema templat
- Skema template Gmail
- Skema templat Google Drive
- Skema Templat IBM DB2
- Skema templat Microsoft Exchange
- OneDrive Skema templat Microsoft
- SharePoint Skema templat Microsoft
- Skema templat Microsoft SQL Server
- Skema templat Microsoft Teams
- Skema templat Microsoft Yammer
- Skema templat MySQL
- Skema templat Oracle Database
- Skema Templat PostgreSQL
- Skema templat Salesforce
- ServiceNow skema templat
- Skema template kendur
- Skema template Zendesk

Adobe Experience Managerskema templat

Anda menyertakan JSON yang berisi skema sumber data sebagai bagian dari objek. TemplateConfiguration Anda memberikan URL Adobe Experience Manager host, jenis otentikasi, dan apakah Anda menggunakan Adobe Experience Manager (AEM) sebagai Layanan Cloud atau AEM On-Premise sebagai bagian dari konfigurasi koneksi atau detail titik akhir repositori. Juga, tentukan jenis sumber data sebagai`AEM`, rahasia untuk kredensyal otentikasi Anda, dan konfigurasi lain yang diperlukan. Anda kemudian menentukan `TEMPLATE` sebagai `Type` saat Anda menelepon CreateDataSource.

Anda dapat menggunakan template yang disediakan dalam panduan pengembang ini. Untuk informasi selengkapnya, lihat Adobe Experience ManagerSkema JSON.

Tabel berikut menjelaskan parameter skema AEM JSON.

Konfigurasi	Deskripsi
ConnectionConfiguration	Informasi konfigurasi untuk titik akhir untuk sumber data.
repositoryEndpointMetadata	Informasi titik akhir untuk sumber data.
AEMurl	URL Adobe Experience Manager host. Misalnya, jika Anda menggunakan AEM On-Premise, Anda menyertakan nama host dan port:. https://hostname:port Atau, jika Anda menggunakan AEM sebagai Layanan Cloud, Anda dapat menggunakan URL penulis: https://author-xxxxxx-xxxxxxx.adobeaemcloud.com.
authType	Jenis otentikasi yang Anda gunakan, apakah `Basic` atau`OAuth2`.
deploymentType	Jenis Adobe Experience Manager yang Anda gunakan, baik `CLOUD` atau`ON_PREMISE` .
RepositoryConfigurations	Informasi konfigurasi untuk konten sumber data. Misalnya, mengonfigurasi jenis konten dan pemetaan bidang tertentu.
• halaman • aset	Daftar objek yang memetakan atribut atau nama bidang Adobe Experience Manager halaman dan aset Anda untuk Amazon Kendra mengindeks nama bidang. Untuk informasi lebih lanjut, lihat Memetakan bidang sumber data.
AdditionalProperties	Opsi konfigurasi tambahan untuk konten Anda di sumber data Anda.
timeZoneId	Jika Anda menggunakan AEM On-Premise dan zona waktu server Anda berbeda dari zona waktu konektor atau indeks Amazon Kendra AEM, Anda dapat menentukan zona

Konfigurasi	Deskripsi
	waktu server agar sejajar dengan konektor atau indeks AEM. Zona waktu default untuk AEM On-Premis e adalah zona waktu konektor atau indeks Amazon Kendra AEM. Zona waktu default untuk AEM sebagai Layanan Cloud adalah Greenwich Mean Time.
• pageRootPaths • assetRootPaths	Daftar jalur root untuk halaman dan aset. Misalnya, jalur root untuk halaman bisa / content/sub dan jalur root untuk aset bisa / content/sub/asset1.
CrawlAssets	`true`untuk merayapi aset.
CrawlPages	`true`untuk merayapi halaman.
• pagePathInclusionPola • pageNameInclusionPola • assetPathInclusionPola • assetTypeInclusionPola • assetNameInclusionPola	Daftar pola ekspresi reguler untuk menyertak an halaman dan aset tertentu dalam sumber Adobe Experience Manager data Anda. Halaman dan aset yang cocok dengan pola disertakan dalam indeks. Halaman dan aset yang tidak cocok dengan pola dikecualikan dari indeks. Jika halaman atau aset cocok dengan pola inklusi dan pengecualian, pola pengecualian akan diutamakan, dan konten tidak disertakan dalam indeks.

Konfigurasi	Deskripsi
• pagePathExclusionPola • pageNameExclusionPola • assetPathExclusionPola • assetTypeInclusionPola • assetNameInclusionPola	Daftar pola ekspresi reguler untuk mengecualikan halaman dan aset tertentu di sumber Adobe Experience Manager data Anda. Halaman dan aset yang cocok dengan pola dikecualikan dari indeks. Halaman dan aset yang tidak cocok dengan pola disertakan dalam indeks. Jika halaman atau aset cocok dengan pola inklusi dan pengecualian, pola pengecualian akan diutamakan, dan konten tidak disertakan dalam indeks.
PageComponents	Daftar nama untuk komponen halaman tertentu yang ingin Anda indeks.
contentFragmentVariations	Daftar nama untuk variasi spesifik yang disimpan dari Fragmen Adobe Experience Manager Konten yang ingin Anda indeks.
jenis	Jenis sumber data. Tentukan `AEM` sebagai tipe sumber data Anda.
enableIdentityCrawler	`true`untuk menggunakan Amazon Kendra crawler identitas untuk menyinkronkan identitas /informasi utama pada pengguna dan grup dengan akses ke dokumen tertentu. Jika perayap identitas dimatikan, semua dokumen dapat dicari secara publik. Jika Anda ingin menggunakan kontrol akses untuk dokumen dan crawler identitas dimatikan, Anda dapat menggunakan PutPrincipalMappingAPI untuk mengunggah informasi akses pengguna dan grup.

Konfigurasi	Deskripsi
SyncMode	Tentukan bagaimana Amazon Kendra seharusnya memperbarui indeks Anda saat konten sumber data Anda berubah. Anda dapat memilih antara: • `FORCED_FULL_CRAWL` untuk mengindeks semua konten baru, mengganti konten yang ada setiap kali sumber data Anda disinkron kan dengan indeks Anda. • `FULL_CRAWL` untuk mengindeks hanya konten baru, dimodifikasi, dan dihapus setiap kali sumber data Anda disinkronkan dengan indeks Anda. Amazon Kendra dapat menggunakan mekanisme sumber data Anda untuk melacak perubahan konten dan mengindeks konten yang berubah sejak sinkronisasi terakhir. • `CHANGE_LOG` untuk mengindeks hanya konten baru dan yang dimodifikasi setiap kali sumber data Anda disinkronkan dengan indeks Anda. Amazon Kendra dapat menggunakan mekanisme sumber data Anda untuk melacak perubahan konten dan mengindeks konten yang berubah sejak sinkronisasi terakhir.
Sekretarn	Nama Sumber Daya Amazon (ARN) dari AWS Secrets Manager rahasia yang berisi pasangan kunci-nilai yang diperlukan untuk terhubung ke Adobe Experience Manager Anda. Untuk informasi tentang pasangan nilai kunci ini, lihat Petunjuk koneksi untuk Adobe Experience Manager.
versi	Versi template ini yang saat ini didukung.

Adobe Experience ManagerSkema JSON

```
{
  "$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/Fakaofo",
            "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 Skema templat (Windows)

Anda menyertakan JSON yang berisi skema sumber data sebagai bagian dari objek. TemplateConfiguration Anda memberikan ID sistem file sebagai bagian dari konfigurasi koneksi atau detail titik akhir repositori. Anda juga harus menentukan jenis sumber data sebagaiFSX, rahasia

untuk kredensyal otentikasi Anda, dan konfigurasi lain yang diperlukan. Anda kemudian menentukan `TEMPLATE` sebagai `Type` saat Anda menelepon CreateDataSource.

Anda dapat menggunakan template yang disediakan dalam panduan pengembang ini. Lihat Amazon FSx (Windows) Skema JSON.

Tabel berikut menjelaskan parameter skema JSON Amazon FSx (Windows).

Konfigurasi	Deskripsi
ConnectionConfiguration	Informasi konfigurasi untuk titik akhir untuk sumber data.
repositoryEndpointMetadata	Informasi titik akhir untuk sumber data.
fileSystemId	Pengidentifikasi sistem Amazon FSx file. Anda dapat menemukan ID sistem file Anda di dasbor Sistem File di Amazon FSx konsol.
fileSystemType	Jenis sistem Amazon FSx file. Untuk digunakan Windows File Server sebagai jenis sistem file Anda, tentukan`WINDOWS`.
RepositoryConfigurations	Informasi konfigurasi untuk konten sumber data. Misalnya, mengonfigurasi jenis konten dan pemetaan bidang tertentu.
Semua	Daftar objek yang memetakan atribut atau nama bidang file Anda di sumber Amazon FSx data Anda untuk Amazon Kendra mengindeks nama bidang. Untuk informasi lebih lanjut, lihat Memetakan bidang sumber data.
AdditionalProperties	Opsi konfigurasi tambahan untuk konten Anda di sumber data Anda.
isCrawlAcl	`true`untuk merayapi informasi daftar kontrol akses (ACL) untuk dokumen Anda, jika Anda memiliki ACL dan ingin menggunakannya untuk kontrol akses. ACL menentukan dokumen

Konfigurasi	Deskripsi
	mana yang dapat diakses pengguna dan grup. Informasi ACL digunakan untuk memfilter hasil pencarian berdasarkan pengguna atau akses grup mereka ke dokumen. Untuk informasi selengkapnya, lihat Pemfilteran konteks pengguna.
Pola Inklusi	Daftar pola ekspresi reguler untuk menyertakan file tertentu dalam sumber Amazon FSx data Anda. File yang cocok dengan pola disertakan dalam indeks. File yang tidak cocok dengan pola dikecualikan dari indeks. Jika file cocok dengan pola inklusi dan pengecualian, pola pengecualian akan diutamakan dan file tidak disertakan dalam indeks.
Pola Pengecualian	Daftar pola ekspresi reguler untuk mengecualikan file tertentu di sumber Amazon FSx data Anda. File yang cocok dengan pola dikecualikan dari indeks. File yang tidak cocok dengan pola disertakan dalam indeks. Jika file cocok dengan pola pengecualian dan inklusi, pola pengecualian akan diutamakan dan file tidak disertakan dalam indeks.

Konfigurasi	Deskripsi
enableIdentityCrawler	`true`untuk menggunakan Amazon Kendra crawler identitas untuk menyinkronkan identitas /informasi utama pada pengguna dan grup dengan akses ke dokumen tertentu. Jika perayap identitas dimatikan, semua dokumen dapat dicari secara publik. Jika Anda ingin menggunakan kontrol akses untuk dokumen dan crawler identitas dimatikan, Anda dapat menggunakan PutPrincipalMappingAPI untuk mengunggah informasi akses pengguna dan grup.
SyncMode	Tentukan bagaimana Amazon Kendra seharusnya memperbarui indeks Anda saat konten sumber data Anda berubah. Anda dapat memilih antara: • `FORCED_FULL_CRAWL` untuk mengindeks semua konten baru, mengganti konten yang ada setiap kali sumber data Anda disinkron kan dengan indeks Anda. • `FULL_CRAWL` untuk mengindeks hanya konten baru, dimodifikasi, dan dihapus setiap kali sumber data Anda disinkronkan dengan indeks Anda. Amazon Kendra dapat menggunakan mekanisme sumber data Anda untuk melacak perubahan konten dan mengindeks konten yang berubah sejak sinkronisasi terakhir.
jenis	Jenis sumber data. Untuk sumber data sistem file Windows, tentukan`FSX`.

Amazon FSx (Windows) Skema JSON

```
{
  "$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 Skema templat (NetApp ONTAP)

Anda menyertakan JSON yang berisi skema sumber data sebagai bagian dari objek. TemplateConfiguration Anda memberikan ID sistem file dan mesin virtual penyimpanan (SVM) sebagai bagian dari konfigurasi koneksi atau detail titik akhir repositori. Anda juga harus menentukan jenis sumber data sebagai`FSXONTAP`, rahasia untuk kredensyal otentikasi Anda, dan konfigurasi lain yang diperlukan. Anda kemudian menentukan `TEMPLATE` sebagai `Type` saat Anda menelepon CreateDataSource.

Anda dapat menggunakan template yang disediakan dalam panduan pengembang ini. Lihat Amazon FSx (NetApp ONTAP) Skema JSON.

Tabel berikut menjelaskan parameter skema JSON Amazon FSx (NetApp ONTAP).

Konfigurasi	Deskripsi
ConnectionConfiguration	Informasi konfigurasi untuk titik akhir untuk sumber data.
repositoryEndpointMetadata	Informasi titik akhir untuk sumber data.
fileSystemId	Pengidentifikasi sistem Amazon FSx file. Anda dapat menemukan ID sistem file Anda di dasbor Sistem File di Amazon FSx konsol. Untuk informasi tentang cara membuat sistem file di Amazon FSx konsol untuk NetApp ONTAP, lihat Panduan Memulai untuk NetApp ONTAP di Panduan FSx for ONTAP Pengguna.
fileSystemType	Jenis sistem Amazon FSx file. Untuk digunakan NetApp ONTAP sebagai jenis sistem file Anda, tentukan`ONTAP`.
SVMid	Pengidentifikasi mesin virtual penyimpanan (SVM) yang digunakan dengan sistem Amazon FSx file Anda untuk. NetApp ONTAP Anda dapat menemukan ID SVM Anda dengan membuka dasbor Sistem File di Amazon FSx konsol, memilih ID sistem file Anda, dan kemudian memilih mesin virtual Penyimpanan. Untuk informasi tentang cara membuat sistem file di Amazon FSx konsolNetApp ONTAP, lihat Panduan Memulai NetApp ONTAP di Panduan FSx for ONTAP Pengguna.
ProtocolType	Apakah Anda menggunakan protokol Common Internet File System (CIFS) untuk Windows,

Konfigurasi	Deskripsi
	atau protokol Network File System (NFS) untuk Linux.
RepositoryConfigurations	Informasi konfigurasi untuk konten sumber data. Misalnya, mengonfigurasi jenis konten dan pemetaan bidang tertentu.
file	Daftar objek yang memetakan atribut atau nama bidang file Anda di sumber Amazon FSx data Anda untuk Amazon Kendra mengindeks nama bidang. Untuk informasi lebih lanjut, lihat Memetakan bidang sumber data. Nama bidang sumber data harus ada di metadata kustom file Anda.
AdditionalProperties	Opsi konfigurasi tambahan untuk konten Anda di sumber data Anda.
CrawlaCl	`true`untuk merayapi informasi daftar kontrol akses (ACL) untuk dokumen Anda, jika Anda memiliki ACL dan ingin menggunakannya untuk kontrol akses. ACL menentukan dokumen mana yang dapat diakses pengguna dan grup. Informasi ACL digunakan untuk memfilter hasil pencarian berdasarkan pengguna atau akses grup mereka ke dokumen. Untuk informasi selengkapnya, lihat Pemfilteran konteks pengguna.

Konfigurasi	Deskripsi
Pola Inklusi	Daftar pola ekspresi reguler untuk menyertakan file tertentu dalam sumber Amazon FSx data Anda. File yang cocok dengan pola disertakan dalam indeks. File yang tidak cocok dengan pola dikecualikan dari indeks. Jika file cocok dengan pola inklusi dan pengecualian, pola pengecualian akan diutamakan dan file tidak disertakan dalam indeks.
Pola Pengecualian	Daftar pola ekspresi reguler untuk mengecualikan file tertentu di sumber Amazon FSx data Anda. File yang cocok dengan pola dikecualikan dari indeks. File yang tidak cocok dengan pola disertakan dalam indeks. Jika file cocok dengan pola pengecualian dan inklusi, pola pengecualian akan diutamakan dan file tidak disertakan dalam indeks.
jenis	Jenis sumber data. Untuk sumber data sistem NetApp ONTAP file, tentukan`FSXONTAP`.

Konfigurasi	Deskripsi
SyncMode	Tentukan bagaimana Amazon Kendra seharusnya memperbarui indeks Anda saat konten sumber data Anda berubah. Anda dapat memilih antara: • `FORCED_FULL_CRAWL` untuk mengindeks semua konten baru, mengganti konten yang ada setiap kali sumber data Anda disinkron kan dengan indeks Anda. • `FULL_CRAWL` untuk mengindeks hanya konten baru, dimodifikasi, dan dihapus setiap kali sumber data Anda disinkronkan dengan indeks Anda. Amazon Kendra dapat menggunakan mekanisme sumber data Anda untuk melacak perubahan konten dan mengindeks konten yang berubah sejak sinkronisasi terakhir.

Konfigurasi	Deskripsi

Sekretarn	Nama Sumber Daya Amazon (ARN) dari AWS Secrets Manager rahasia yang berisi pasangan kunci-nilai yang diperlukan untuk terhubung ke sistem file Anda. Amazon FSx Rahasiany a harus berisi struktur JSON dengan kunci berikut:
	
	`{ "username": " user@corp.example. com ", "password": " password" }`
	
	Jika Anda menggunakan protokol NFS untuk sistem Amazon FSx file Anda, rahasianya disimpan dalam struktur JSON dengan kunci berikut:
	
	`{ "leftId": "left ID", "rightId": " right ID", "preSharedKey": " pre-shared key " }`

Amazon FSx (NetApp ONTAP) Skema JSON

```
{
  "$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"
  ]
}
```

Alfrescoskema templat

Anda menyertakan JSON yang berisi skema sumber data sebagai bagian dari objek. TemplateConfiguration Anda memberikan ID Alfresco situs, URL repositori, URL antarmuka pengguna, jenis autentikasi, apakah Anda menggunakan cloud atau lokal, dan jenis konten yang ingin dirayapi. Anda memberikan ini sebagai bagian dari konfigurasi koneksi atau detail titik akhir repositori. Juga tentukan jenis sumber data sebagai`ALFRESCO`, rahasia untuk kredensyal otentikasi Anda, dan konfigurasi lain yang diperlukan. Anda kemudian menentukan `TEMPLATE` sebagai `Type` saat Anda menelepon CreateDataSource.

Anda dapat menggunakan template yang disediakan dalam panduan pengembang ini. Lihat AlfrescoSkema JSON.

Tabel berikut menjelaskan parameter skema Alfresco JSON.

Konfigurasi	Deskripsi
ConnectionConfiguration	Informasi konfigurasi untuk titik akhir untuk sumber data.
repositoryEndpointMetadata	Informasi titik akhir untuk sumber data.
SiteID	Pengidentifikasi situs Alfresco.
Repourl	URL Alfresco repositori Anda. Anda bisa mendapatkan URL repositori dari administrator AndaAlfresco. Misalnya, jika Anda menggunakan Alfresco Cloud (PaaS), URL repositori bisa jadi. https://company.alfrescocloud.com Atau, jika Anda menggunakan Alfresco Lokal, URL repositori bisa jadi. https://company-alfresco-instance.company-domain.suffix:port
webAppUrl	URL antarmuka Alfresco pengguna Anda. Anda bisa mendapatkan URL antarmuka Alfresco pengguna dari Alfresco administrator Anda. Misalnya, URL antarmuka pengguna dapat berupa https://example.com.

Konfigurasi	Deskripsi
repositoryAdditionalProperties	Properti tambahan untuk terhubung dengan titik akhir repositori/sumber data.
authType	Jenis otentikasi yang Anda gunakan, apakah `OAuth2` atau`Basic`.
jenis (penyebaran)	Jenis Alfresco yang Anda gunakan, apakah `PAAS` atau`ON-PREM`.
CrawlType	Jenis konten yang ingin dirayapi, baik `ASPECT` (konten yang ditandai dengan 'Aspek' diAlfresco), `SITE_ID` (konten dalam Alfresco situs tertentu), atau `ALL_SITES` (konten di semua Alfresco situs Anda).
RepositoryConfigurations	Informasi konfigurasi untuk konten sumber data. Misalnya, mengonfigurasi jenis konten dan pemetaan bidang tertentu.
• dokumen • komentar	Daftar objek yang memetakan atribut atau nama bidang dokumen Alfresco Anda dan komentar untuk Amazon Kendra mengindeks nama bidang. Untuk informasi lebih lanjut, lihat Memetakan bidang sumber data.
AdditionalProperties	Opsi konfigurasi tambahan untuk konten Anda di sumber data Anda.
AspectName	Nama 'Aspek' tertentu yang ingin Anda indeks.
AspectProperties	Daftar properti konten 'Aspek' tertentu yang ingin Anda indeks.
enableFineGrainedPengendalian	`true`untuk merangkak 'Aspek'.
isCrawlComment	`true`untuk merayapi komentar.

Konfigurasi	Deskripsi
• inclusionFileNamePola • inclusionFileTypePola • inclusionFilePathPola	Daftar pola ekspresi reguler untuk menyertakan file tertentu dalam sumber Alfresco data Anda. File yang cocok dengan pola disertakan dalam indeks. File yang tidak cocok dengan pola dikecualikan dari indeks. Jika file cocok dengan pola inklusi dan pengecualian, pola pengecualian akan diutamakan, dan file tidak disertakan dalam indeks.
• exclusionFileNamePola • exclusionFileTypePola • exclusionFilePathPola	Daftar pola ekspresi reguler untuk mengecualikan file tertentu di sumber Alfresco data Anda. File yang cocok dengan pola dikecualikan dari indeks. File yang tidak cocok dengan pola disertakan dalam indeks. Jika file cocok dengan pola inklusi dan pengecualian, pola pengecualian akan diutamakan, dan file tidak disertakan dalam indeks.
jenis	Jenis sumber data. Tentukan `ALFRESCO` sebagai tipe sumber data Anda.

Konfigurasi	Deskripsi

Sekretarn	Nama Sumber Daya Amazon (ARN) dari AWS Secrets Manager rahasia yang berisi pasangan kunci-nilai yang diperlukan untuk terhubung ke Anda. Alfresco Rahasianya harus berisi struktur JSON dengan kunci berikut:
	
	Jika menggunakan otentikasi dasar:
	
	`{ "username": " user name", "password": " password" }`
	
	Jika menggunakan otentikasi OAuth 2.0:
	
	`{ "clientId": " client ID", "clientSecret": " client secret", "tokenUrl": " token URL" }`

Konfigurasi	Deskripsi
SyncMode	Tentukan bagaimana Amazon Kendra seharusnya memperbarui indeks Anda saat konten sumber data Anda berubah. Anda dapat memilih antara: • `FORCED_FULL_CRAWL` untuk mengindeks semua konten baru, mengganti konten yang ada setiap kali sumber data Anda disinkron kan dengan indeks Anda. • `FULL_CRAWL` untuk mengindeks hanya konten baru, dimodifikasi, dan dihapus setiap kali sumber data Anda disinkronkan dengan indeks Anda. Amazon Kendra dapat menggunakan mekanisme sumber data Anda untuk melacak perubahan konten dan mengindeks konten yang berubah sejak sinkronisasi terakhir.
enableIdentityCrawler	`true`untuk menggunakan Amazon Kendra crawler identitas untuk menyinkronkan identitas /informasi utama pada pengguna dan grup dengan akses ke dokumen tertentu. Jika perayap identitas dimatikan, semua dokumen dapat dicari secara publik. Jika Anda ingin menggunakan kontrol akses untuk dokumen dan crawler identitas dimatikan, Anda dapat menggunakan PutPrincipalMappingAPI untuk mengunggah informasi akses pengguna dan grup.
versi	Versi template ini yang saat ini didukung.

AlfrescoSkema JSON

```
{
```

```
"$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 Skema templat (MySQL)

Anda menyertakan JSON yang berisi skema sumber data sebagai bagian dari objek. TemplateConfiguration Tentukan jenis sumber data sebagai`JDBC`, tipe database sebagai`mysql`, rahasia untuk kredensyal otentikasi Anda, dan konfigurasi lain yang diperlukan. Anda kemudian menentukan `TEMPLATE` sebagai `Type` saat Anda menelepon CreateDataSource.

Anda dapat menggunakan template yang disediakan dalam panduan pengembang ini. Lihat Aurora (MySQL) skema JSON.

Tabel berikut menjelaskan parameter skema Aurora (MySQL) JSON.

Konfigurasi	Deskripsi
ConnectionConfiguration	Informasi konfigurasi untuk titik akhir untuk sumber data.
repositoryEndpointMetadata	Informasi konfigurasi yang diperlukan untuk menghubungkan sumber data Anda. • DBType—jenis database Java yang Anda gunakan, apakah,,, `mysql`db2, `postgresq l` atau. `oracle` `sqlserver` • DBhost — nama host database. • DBport — port database. • DBinstance—contoh database.
RepositoryConfigurations	Informasi konfigurasi untuk konten sumber data. Misalnya, mengonfigurasi jenis konten dan pemetaan bidang tertentu. Tentukan jenis sumber data dan ARN rahasia.
dokumen	Daftar objek yang memetakan atribut atau nama bidang konten database Anda untuk Amazon Kendra mengindeks nama bidang. Untuk informasi lebih lanjut, lihat Memetakan bidang sumber data.

Konfigurasi	Deskripsi
AdditionalProperties	Opsi konfigurasi tambahan untuk konten Anda di sumber data Anda. Gunakan untuk menyertakan atau mengecualikan konten tertentu dalam sumber data database Anda.
PrimaryKey	Berikan kunci utama untuk tabel database. Ini mengidentifikasi tabel dalam database Anda.
Judul Kolom	Berikan nama kolom judul dokumen dalam tabel database Anda.
BodyColumn	Berikan nama kolom judul dokumen dalam tabel database Anda.
SqlQuery	Masukkan pernyataan kueri SQL seperti operasi SELECT dan JOIN. Kueri SQL harus kurang dari 32KB. Amazon Kendra akan merayapi semua konten database yang cocok dengan kueri Anda.
TimestampColumn	Masukkan nama kolom yang berisi stempel waktu. Amazon Kendra menggunakan informasi cap waktu untuk mendeteksi perubahan dalam konten Anda dan hanya menyinkronkan konten yang diubah.
TimestampFormat	Masukkan nama kolom yang berisi format cap waktu yang akan digunakan untuk mendeteksi perubahan konten dan menyinkronkan ulang konten Anda.
timezone	Masukkan nama kolom yang berisi zona waktu untuk konten yang akan dirayapi.

Konfigurasi	Deskripsi
changeDetectingColumns	Masukkan nama kolom yang Amazon Kendra akan digunakan untuk mendeteksi perubahan konten. Amazon Kendra akan mengindeks ulang konten ketika ada perubahan di salah satu kolom ini
allowedUsersColumns	Masukkan nama kolom yang berisi ID Pengguna untuk diizinkan mengakses konten.
allowedGroupsColumn	Masukkan nama kolom yang berisi ID Pengguna untuk diizinkan mengakses konten.
Sourceuricolumn	Masukkan nama kolom yang berisi URL Sumber yang akan diindeks.
isSslEnabled	Masukkan pernyataan kueri SQL seperti operasi SELECT dan JOIN. Kueri SQL harus kurang dari 32KB. Amazon Kendra akan merayapi semua konten database yang cocok dengan kueri Anda.
jenis	Jenis sumber data. Tentukan `JDBC` sebagai tipe sumber data Anda.

Konfigurasi	Deskripsi
SyncMode	Tentukan bagaimana Amazon Kendra seharusnya memperbarui indeks Anda saat konten sumber data Anda berubah. Anda dapat memilih antara: • `FORCED_FULL_CRAWL` untuk mengindeks semua konten baru, mengganti konten yang ada setiap kali sumber data Anda disinkron kan dengan indeks Anda. • `FULL_CRAWL` untuk mengindeks hanya konten baru, dimodifikasi, dan dihapus setiap kali sumber data Anda disinkronkan dengan indeks Anda. Amazon Kendra dapat menggunakan mekanisme sumber data Anda untuk melacak perubahan konten dan mengindeks konten yang berubah sejak sinkronisasi terakhir. • `CHANGE_LOG` untuk mengindeks hanya konten baru dan yang dimodifikasi setiap kali sumber data Anda disinkronkan dengan indeks Anda. Amazon Kendra dapat menggunakan mekanisme sumber data Anda untuk melacak perubahan konten dan mengindeks konten yang berubah sejak sinkronisasi terakhir.

Konfigurasi	Deskripsi
Sekretarn	Nama Sumber Daya Amazon (ARN) dari rahasia Secrets Manager yang berisi nama pengguna dan kata sandi yang diperlukan untuk terhubung ke database Anda. Rahasiany a harus berisi struktur JSON dengan kunci berikut: `{ "user name": "database user name", "password": " password" }`
versi	Versi template yang saat ini didukung.

Aurora (MySQL) skema JSON

```
{
  "$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"
  ]
}
```

Aurora (PostgreSQL) skema templat

Anda menyertakan JSON yang berisi skema sumber data sebagai bagian dari objek. TemplateConfiguration Tentukan jenis sumber data sebagai`JDBC`, tipe database sebagai`postgresql`, rahasia untuk kredensyal otentikasi Anda, dan konfigurasi lain yang diperlukan. Anda kemudian menentukan `TEMPLATE` sebagai `Type` saat Anda menelepon CreateDataSource.

Anda dapat menggunakan template yang disediakan dalam panduan pengembang ini. Lihat Aurora (PostgreSQL) Skema JSON.

Tabel berikut menjelaskan parameter skema JSON Aurora (PostgreSQL).

Konfigurasi	Deskripsi
ConnectionConfiguration	Informasi konfigurasi untuk titik akhir untuk sumber data.
repositoryEndpointMetadata	Informasi konfigurasi yang diperlukan untuk menghubungkan sumber data Anda. • DBType—jenis database Java yang Anda gunakan, apakah,,, `mysql`db2, `postgresql` atau. `oracle` `sqlserver` • DBhost — nama host database. • DBport — port database. • DBinstance—contoh database.
RepositoryConfigurations	Informasi konfigurasi untuk konten sumber data. Misalnya, mengonfigurasi jenis konten

Konfigurasi	Deskripsi
	dan pemetaan bidang tertentu. Tentukan jenis sumber data dan ARN rahasia.
dokumen	Daftar objek yang memetakan atribut atau nama bidang konten database Anda untuk Amazon Kendra mengindeks nama bidang. Untuk informasi lebih lanjut, lihat Memetakan bidang sumber data.
AdditionalProperties	Opsi konfigurasi tambahan untuk konten Anda di sumber data Anda. Gunakan untuk menyertakan atau mengecualikan konten tertentu dalam sumber data database Anda.
PrimaryKey	Berikan kunci utama untuk tabel database. Ini mengidentifikasi tabel dalam database Anda.
Judul Kolom	Berikan nama kolom judul dokumen dalam tabel database Anda.
BodyColumn	Berikan nama kolom judul dokumen dalam tabel database Anda.
SqlQuery	Masukkan pernyataan kueri SQL seperti operasi SELECT dan JOIN. Kueri SQL harus kurang dari 32KB. Amazon Kendra akan merayapi semua konten database yang cocok dengan kueri Anda.
TimestampColumn	Masukkan nama kolom yang berisi stempel waktu. Amazon Kendra menggunakan informasi cap waktu untuk mendeteksi perubahan dalam konten Anda dan hanya menyinkronkan konten yang diubah.

Konfigurasi	Deskripsi
TimestampFormat	Masukkan nama kolom yang berisi format cap waktu yang akan digunakan untuk mendeteksi perubahan konten dan menyinkronkan ulang konten Anda.
timezone	Masukkan nama kolom yang berisi zona waktu untuk konten yang akan dirayapi.
changeDetectingColumns	Masukkan nama kolom yang Amazon Kendra akan digunakan untuk mendeteksi perubahan konten. Amazon Kendra akan mengindeks ulang konten ketika ada perubahan di salah satu kolom ini
allowedUsersColumns	Masukkan nama kolom yang berisi ID Pengguna untuk diizinkan mengakses konten.
allowedGroupsColumn	Masukkan nama kolom yang berisi ID Pengguna untuk diizinkan mengakses konten.
Sourceuricolumn	Masukkan nama kolom yang berisi URL Sumber yang akan diindeks.
isSslEnabled	Masukkan pernyataan kueri SQL seperti operasi SELECT dan JOIN. Kueri SQL harus kurang dari 32KB. Amazon Kendra akan merayapi semua konten database yang cocok dengan kueri Anda.
jenis	Jenis sumber data. Tentukan `JDBC` sebagai tipe sumber data Anda.

Konfigurasi	Deskripsi
SyncMode	Tentukan bagaimana Amazon Kendra seharusnya memperbarui indeks Anda saat konten sumber data Anda berubah. Anda dapat memilih antara: • `FORCED_FULL_CRAWL` untuk mengindeks semua konten baru, mengganti konten yang ada setiap kali sumber data Anda disinkron kan dengan indeks Anda. • `FULL_CRAWL` untuk mengindeks hanya konten baru, dimodifikasi, dan dihapus setiap kali sumber data Anda disinkronkan dengan indeks Anda. Amazon Kendra dapat menggunakan mekanisme sumber data Anda untuk melacak perubahan konten dan mengindeks konten yang berubah sejak sinkronisasi terakhir. • `CHANGE_LOG` untuk mengindeks hanya konten baru dan yang dimodifikasi setiap kali sumber data Anda disinkronkan dengan indeks Anda. Amazon Kendra dapat menggunakan mekanisme sumber data Anda untuk melacak perubahan konten dan mengindeks konten yang berubah sejak sinkronisasi terakhir.

Konfigurasi	Deskripsi
Sekretarn	Nama Sumber Daya Amazon (ARN) dari rahasia Secrets Manager yang berisi nama pengguna dan kata sandi yang diperlukan untuk terhubung ke database Anda. Rahasiany a harus berisi struktur JSON dengan kunci berikut: `{ "user name": "database user name", "password": " password" }`
versi	Versi template yang saat ini didukung.

Aurora (PostgreSQL) Skema JSON

```
{
  "$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 Skema templat (Microsoft SQL Server)

Anda menyertakan JSON yang berisi skema sumber data sebagai bagian dari objek. TemplateConfiguration Tentukan jenis sumber data sebagai`JDBC`, tipe database sebagai`sqlserver`, rahasia untuk kredensyal otentikasi Anda, dan konfigurasi lain yang diperlukan. Anda kemudian menentukan `TEMPLATE` sebagai `Type` saat Anda menelepon CreateDataSource.

Anda dapat menggunakan template yang disediakan dalam panduan pengembang ini. Lihat Amazon RDS (Microsoft SQL Server) Skema JSON.

Tabel berikut menjelaskan parameter skema JSON Amazon RDS (Microsoft SQL Server).

Konfigurasi	Deskripsi
ConnectionConfiguration	Informasi konfigurasi untuk titik akhir untuk sumber data.
repositoryEndpointMetadata	Informasi konfigurasi yang diperlukan untuk menghubungkan sumber data Anda. • DBType—jenis database Java yang Anda gunakan, apakah,,, `mysql`db2, `postgresql` atau. `oracle` `sqlserver` • DBhost — nama host database. • DBport — port database. • DBinstance—contoh database.
RepositoryConfigurations	Informasi konfigurasi untuk konten sumber data. Misalnya, mengonfigurasi jenis konten

Konfigurasi	Deskripsi
	dan pemetaan bidang tertentu. Tentukan jenis sumber data dan ARN rahasia.
dokumen	Daftar objek yang memetakan atribut atau nama bidang konten database Anda untuk Amazon Kendra mengindeks nama bidang. Untuk informasi lebih lanjut, lihat Memetakan bidang sumber data.
AdditionalProperties	Opsi konfigurasi tambahan untuk konten Anda di sumber data Anda. Gunakan untuk menyertakan atau mengecualikan konten tertentu dalam sumber data database Anda.
PrimaryKey	Berikan kunci utama untuk tabel database. Ini mengidentifikasi tabel dalam database Anda.
Judul Kolom	Berikan nama kolom judul dokumen dalam tabel database Anda.
BodyColumn	Berikan nama kolom judul dokumen dalam tabel database Anda.
SqlQuery	Masukkan pernyataan kueri SQL seperti operasi SELECT dan JOIN. Kueri SQL harus kurang dari 32KB. Amazon Kendra akan merayapi semua konten database yang cocok dengan kueri Anda.
TimestampColumn	Masukkan nama kolom yang berisi stempel waktu. Amazon Kendra menggunakan informasi cap waktu untuk mendeteksi perubahan dalam konten Anda dan hanya menyinkronkan konten yang diubah.

Konfigurasi	Deskripsi
TimestampFormat	Masukkan nama kolom yang berisi format cap waktu yang akan digunakan untuk mendeteksi perubahan konten dan menyinkronkan ulang konten Anda.
timezone	Masukkan nama kolom yang berisi zona waktu untuk konten yang akan dirayapi.
changeDetectingColumns	Masukkan nama kolom yang Amazon Kendra akan digunakan untuk mendeteksi perubahan konten. Amazon Kendra akan mengindeks ulang konten ketika ada perubahan di salah satu kolom ini
allowedUsersColumns	Masukkan nama kolom yang berisi ID Pengguna untuk diizinkan mengakses konten.
allowedGroupsColumn	Masukkan nama kolom yang berisi ID Pengguna untuk diizinkan mengakses konten.
Sourceuricolumn	Masukkan nama kolom yang berisi URL Sumber yang akan diindeks.
isSslEnabled	Masukkan pernyataan kueri SQL seperti operasi SELECT dan JOIN. Kueri SQL harus kurang dari 32KB. Amazon Kendra akan merayapi semua konten database yang cocok dengan kueri Anda.
jenis	Jenis sumber data. Tentukan `JDBC` sebagai tipe sumber data Anda.

Konfigurasi	Deskripsi
SyncMode	Tentukan bagaimana Amazon Kendra seharusnya memperbarui indeks Anda saat konten sumber data Anda berubah. Anda dapat memilih antara: • `FORCED_FULL_CRAWL` untuk mengindeks semua konten baru, mengganti konten yang ada setiap kali sumber data Anda disinkron kan dengan indeks Anda. • `FULL_CRAWL` untuk mengindeks hanya konten baru, dimodifikasi, dan dihapus setiap kali sumber data Anda disinkronkan dengan indeks Anda. Amazon Kendra dapat menggunakan mekanisme sumber data Anda untuk melacak perubahan konten dan mengindeks konten yang berubah sejak sinkronisasi terakhir. • `CHANGE_LOG` untuk mengindeks hanya konten baru dan yang dimodifikasi setiap kali sumber data Anda disinkronkan dengan indeks Anda. Amazon Kendra dapat menggunakan mekanisme sumber data Anda untuk melacak perubahan konten dan mengindeks konten yang berubah sejak sinkronisasi terakhir.

Konfigurasi	Deskripsi
Sekretarn	Nama Sumber Daya Amazon (ARN) dari rahasia Secrets Manager yang berisi nama pengguna dan kata sandi yang diperlukan untuk terhubung ke database Anda. Rahasiany a harus berisi struktur JSON dengan kunci berikut: `{ "user name": "database user name", "password": " password" }`
versi	Versi template yang saat ini didukung.

Amazon RDS (Microsoft SQL Server) Skema JSON

```
{
  "$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 Skema templat (MySQL)

Anda menyertakan JSON yang berisi skema sumber data sebagai bagian dari objek. TemplateConfiguration Tentukan jenis sumber data sebagai`JDBC`, tipe database sebagai`mysql`, rahasia untuk kredensyal otentikasi Anda, dan konfigurasi lain yang diperlukan. Anda kemudian menentukan `TEMPLATE` sebagai `Type` saat Anda menelepon CreateDataSource.

Anda dapat menggunakan template yang disediakan dalam panduan pengembang ini. Lihat Amazon RDS (MySQL) skema JSON.

Tabel berikut menjelaskan parameter skema Amazon RDS (MySQL) JSON.

Konfigurasi	Deskripsi
ConnectionConfiguration	Informasi konfigurasi untuk titik akhir untuk sumber data.
repositoryEndpointMetadata	Informasi konfigurasi yang diperlukan untuk menghubungkan sumber data Anda. • DBType—jenis database Java yang Anda gunakan, apakah,,, `mysql`db2, `postgresql` atau. `oracle` `sqlserver` • DBhost — nama host database. • DBport — port database. • DBinstance—contoh database.
RepositoryConfigurations	Informasi konfigurasi untuk konten sumber data. Misalnya, mengonfigurasi jenis konten

Konfigurasi	Deskripsi
	dan pemetaan bidang tertentu. Tentukan jenis sumber data dan ARN rahasia.
dokumen	Daftar objek yang memetakan atribut atau nama bidang konten database Anda untuk Amazon Kendra mengindeks nama bidang. Untuk informasi lebih lanjut, lihat Memetakan bidang sumber data.
AdditionalProperties	Opsi konfigurasi tambahan untuk konten Anda di sumber data Anda. Gunakan untuk menyertakan atau mengecualikan konten tertentu dalam sumber data database Anda.
PrimaryKey	Berikan kunci utama untuk tabel database. Ini mengidentifikasi tabel dalam database Anda.
Judul Kolom	Berikan nama kolom judul dokumen dalam tabel database Anda.
BodyColumn	Berikan nama kolom judul dokumen dalam tabel database Anda.
SqlQuery	Masukkan pernyataan kueri SQL seperti operasi SELECT dan JOIN. Kueri SQL harus kurang dari 32KB. Amazon Kendra akan merayapi semua konten database yang cocok dengan kueri Anda.
TimestampColumn	Masukkan nama kolom yang berisi stempel waktu. Amazon Kendra menggunakan informasi cap waktu untuk mendeteksi perubahan dalam konten Anda dan hanya menyinkronkan konten yang diubah.

Konfigurasi	Deskripsi
TimestampFormat	Masukkan nama kolom yang berisi format cap waktu yang akan digunakan untuk mendeteksi perubahan konten dan menyinkronkan ulang konten Anda.
timezone	Masukkan nama kolom yang berisi zona waktu untuk konten yang akan dirayapi.
changeDetectingColumns	Masukkan nama kolom yang Amazon Kendra akan digunakan untuk mendeteksi perubahan konten. Amazon Kendra akan mengindeks ulang konten ketika ada perubahan di salah satu kolom ini
allowedUsersColumns	Masukkan nama kolom yang berisi ID Pengguna untuk diizinkan mengakses konten.
allowedGroupsColumn	Masukkan nama kolom yang berisi ID Pengguna untuk diizinkan mengakses konten.
Sourceuricolumn	Masukkan nama kolom yang berisi URL Sumber yang akan diindeks.
isSslEnabled	Masukkan pernyataan kueri SQL seperti operasi SELECT dan JOIN. Kueri SQL harus kurang dari 32KB. Amazon Kendra akan merayapi semua konten database yang cocok dengan kueri Anda.
jenis	Jenis sumber data. Tentukan `JDBC` sebagai tipe sumber data Anda.

Konfigurasi	Deskripsi
SyncMode	Tentukan bagaimana Amazon Kendra seharusnya memperbarui indeks Anda saat konten sumber data Anda berubah. Anda dapat memilih antara: • `FORCED_FULL_CRAWL` untuk mengindeks semua konten baru, mengganti konten yang ada setiap kali sumber data Anda disinkron kan dengan indeks Anda. • `FULL_CRAWL` untuk mengindeks hanya konten baru, dimodifikasi, dan dihapus setiap kali sumber data Anda disinkronkan dengan indeks Anda. Amazon Kendra dapat menggunakan mekanisme sumber data Anda untuk melacak perubahan konten dan mengindeks konten yang berubah sejak sinkronisasi terakhir. • `CHANGE_LOG` untuk mengindeks hanya konten baru dan yang dimodifikasi setiap kali sumber data Anda disinkronkan dengan indeks Anda. Amazon Kendra dapat menggunakan mekanisme sumber data Anda untuk melacak perubahan konten dan mengindeks konten yang berubah sejak sinkronisasi terakhir.

Konfigurasi	Deskripsi
Sekretarn	Nama Sumber Daya Amazon (ARN) dari rahasia Secrets Manager yang berisi nama pengguna dan kata sandi yang diperlukan untuk terhubung ke database Anda. Rahasiany a harus berisi struktur JSON dengan kunci berikut: `{ "user name": "database user name", "password": " password" }`
versi	Versi template yang saat ini didukung.

Amazon RDS (MySQL) skema JSON

```
{
  "$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 Skema templat (Oracle)

Anda menyertakan JSON yang berisi skema sumber data sebagai bagian dari objek. TemplateConfiguration Tentukan jenis sumber data sebagai`JDBC`, tipe database sebagai`oracle`, rahasia untuk kredensyal otentikasi Anda, dan konfigurasi lain yang diperlukan. Anda kemudian menentukan `TEMPLATE` sebagai `Type` saat Anda menelepon CreateDataSource.

Anda dapat menggunakan template yang disediakan dalam panduan pengembang ini. Lihat Amazon RDS (Oracle) Skema JSON.

Tabel berikut menjelaskan parameter skema Amazon RDS (Oracle) JSON.

Konfigurasi	Deskripsi
ConnectionConfiguration	Informasi konfigurasi untuk titik akhir untuk sumber data.
repositoryEndpointMetadata	Informasi konfigurasi yang diperlukan untuk menghubungkan sumber data Anda. • DBType—jenis database Java yang Anda gunakan, apakah,,, `mysql` `db2`, `postgresql` atau. `oracle` `sqlserver` • DBhost — nama host database. • DBport — port database. • DBinstance—contoh database.
RepositoryConfigurations	Informasi konfigurasi untuk konten sumber data. Misalnya, mengonfigurasi jenis konten

Konfigurasi	Deskripsi
	dan pemetaan bidang tertentu. Tentukan jenis sumber data dan ARN rahasia.
dokumen	Daftar objek yang memetakan atribut atau nama bidang konten database Anda untuk Amazon Kendra mengindeks nama bidang. Untuk informasi lebih lanjut, lihat Memetakan bidang sumber data.
AdditionalProperties	Opsi konfigurasi tambahan untuk konten Anda di sumber data Anda. Gunakan untuk menyertakan atau mengecualikan konten tertentu dalam sumber data database Anda.
PrimaryKey	Berikan kunci utama untuk tabel database. Ini mengidentifikasi tabel dalam database Anda.
Judul Kolom	Berikan nama kolom judul dokumen dalam tabel database Anda.
BodyColumn	Berikan nama kolom judul dokumen dalam tabel database Anda.
SqlQuery	Masukkan pernyataan kueri SQL seperti operasi SELECT dan JOIN. Kueri SQL harus kurang dari 32KB. Amazon Kendra akan merayapi semua konten database yang cocok dengan kueri Anda.
TimestampColumn	Masukkan nama kolom yang berisi stempel waktu. Amazon Kendra menggunakan informasi cap waktu untuk mendeteksi perubahan dalam konten Anda dan hanya menyinkronkan konten yang diubah.

Konfigurasi	Deskripsi
TimestampFormat	Masukkan nama kolom yang berisi format cap waktu yang akan digunakan untuk mendeteksi perubahan konten dan menyinkronkan ulang konten Anda.
timezone	Masukkan nama kolom yang berisi zona waktu untuk konten yang akan dirayapi.
changeDetectingColumns	Masukkan nama kolom yang Amazon Kendra akan digunakan untuk mendeteksi perubahan konten. Amazon Kendra akan mengindeks ulang konten ketika ada perubahan di salah satu kolom ini
allowedUsersColumns	Masukkan nama kolom yang berisi ID Pengguna untuk diizinkan mengakses konten.
allowedGroupsColumn	Masukkan nama kolom yang berisi ID Pengguna untuk diizinkan mengakses konten.
Sourceuricolumn	Masukkan nama kolom yang berisi URL Sumber yang akan diindeks.
isSslEnabled	Masukkan pernyataan kueri SQL seperti operasi SELECT dan JOIN. Kueri SQL harus kurang dari 32KB. Amazon Kendra akan merayapi semua konten database yang cocok dengan kueri Anda.
jenis	Jenis sumber data. Tentukan `JDBC` sebagai tipe sumber data Anda.

Konfigurasi	Deskripsi
SyncMode	Tentukan bagaimana Amazon Kendra seharusnya memperbarui indeks Anda saat konten sumber data Anda berubah. Anda dapat memilih antara: • `FORCED_FULL_CRAWL` untuk mengindeks semua konten baru, mengganti konten yang ada setiap kali sumber data Anda disinkron kan dengan indeks Anda. • `FULL_CRAWL` untuk mengindeks hanya konten baru, dimodifikasi, dan dihapus setiap kali sumber data Anda disinkronkan dengan indeks Anda. Amazon Kendra dapat menggunakan mekanisme sumber data Anda untuk melacak perubahan konten dan mengindeks konten yang berubah sejak sinkronisasi terakhir. • `CHANGE_LOG` untuk mengindeks hanya konten baru dan yang dimodifikasi setiap kali sumber data Anda disinkronkan dengan indeks Anda. Amazon Kendra dapat menggunakan mekanisme sumber data Anda untuk melacak perubahan konten dan mengindeks konten yang berubah sejak sinkronisasi terakhir.

Konfigurasi	Deskripsi
Sekretarn	Nama Sumber Daya Amazon (ARN) dari rahasia Secrets Manager yang berisi nama pengguna dan kata sandi yang diperlukan untuk terhubung ke database Anda. Rahasiany a harus berisi struktur JSON dengan kunci berikut: `{ "user name": "database user name", "password": " password" }`
versi	Versi template yang saat ini didukung.

Amazon RDS (Oracle) Skema JSON

```
{
  "$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 (PostgreSQL) skema templat

Anda menyertakan JSON yang berisi skema sumber data sebagai bagian dari objek. TemplateConfiguration Tentukan jenis sumber data sebagai`JDBC`, tipe database sebagai`postgresql`, rahasia untuk kredensyal otentikasi Anda, dan konfigurasi lain yang diperlukan. Anda kemudian menentukan `TEMPLATE` sebagai `Type` saat Anda menelepon CreateDataSource.

Anda dapat menggunakan template yang disediakan dalam panduan pengembang ini. Lihat Amazon RDS (PostgreSQL) Skema JSON.

Tabel berikut menjelaskan parameter skema JSON Amazon RDS (PostgreSQL).

Konfigurasi	Deskripsi
ConnectionConfiguration	Informasi konfigurasi untuk titik akhir untuk sumber data.
repositoryEndpointMetadata	Informasi konfigurasi yang diperlukan untuk menghubungkan sumber data Anda. • DBType—jenis database Java yang Anda gunakan, apakah,,, `mysql`db2, `postgresql` atau. `oracle` `sqlserver` • DBhost — nama host database. • DBport — port database. • DBinstance—contoh database.
RepositoryConfigurations	Informasi konfigurasi untuk konten sumber data. Misalnya, mengonfigurasi jenis konten

Konfigurasi	Deskripsi
	dan pemetaan bidang tertentu. Tentukan jenis sumber data dan ARN rahasia.
dokumen	Daftar objek yang memetakan atribut atau nama bidang konten database Anda untuk Amazon Kendra mengindeks nama bidang. Untuk informasi lebih lanjut, lihat Memetakan bidang sumber data.
AdditionalProperties	Opsi konfigurasi tambahan untuk konten Anda di sumber data Anda. Gunakan untuk menyertakan atau mengecualikan konten tertentu dalam sumber data database Anda.
PrimaryKey	Berikan kunci utama untuk tabel database. Ini mengidentifikasi tabel dalam database Anda.
Judul Kolom	Berikan nama kolom judul dokumen dalam tabel database Anda.
BodyColumn	Berikan nama kolom judul dokumen dalam tabel database Anda.
SqlQuery	Masukkan pernyataan kueri SQL seperti operasi SELECT dan JOIN. Kueri SQL harus kurang dari 32KB. Amazon Kendra akan merayapi semua konten database yang cocok dengan kueri Anda.
TimestampColumn	Masukkan nama kolom yang berisi stempel waktu. Amazon Kendra menggunakan informasi cap waktu untuk mendeteksi perubahan dalam konten Anda dan hanya menyinkronkan konten yang diubah.

Konfigurasi	Deskripsi
TimestampFormat	Masukkan nama kolom yang berisi format cap waktu yang akan digunakan untuk mendeteksi perubahan konten dan menyinkronkan ulang konten Anda.
timezone	Masukkan nama kolom yang berisi zona waktu untuk konten yang akan dirayapi.
changeDetectingColumns	Masukkan nama kolom yang Amazon Kendra akan digunakan untuk mendeteksi perubahan konten. Amazon Kendra akan mengindeks ulang konten ketika ada perubahan di salah satu kolom ini
allowedUsersColumns	Masukkan nama kolom yang berisi ID Pengguna untuk diizinkan mengakses konten.
allowedGroupsColumn	Masukkan nama kolom yang berisi ID Pengguna untuk diizinkan mengakses konten.
Sourceuricolumn	Masukkan nama kolom yang berisi URL Sumber yang akan diindeks.
isSslEnabled	Masukkan pernyataan kueri SQL seperti operasi SELECT dan JOIN. Kueri SQL harus kurang dari 32KB. Amazon Kendra akan merayapi semua konten database yang cocok dengan kueri Anda.
jenis	Jenis sumber data. Tentukan `JDBC` sebagai tipe sumber data Anda.

Konfigurasi	Deskripsi
SyncMode	Tentukan bagaimana Amazon Kendra seharusnya memperbarui indeks Anda saat konten sumber data Anda berubah. Anda dapat memilih antara: • `FORCED_FULL_CRAWL` untuk mengindeks semua konten baru, mengganti konten yang ada setiap kali sumber data Anda disinkron kan dengan indeks Anda. • `FULL_CRAWL` untuk mengindeks hanya konten baru, dimodifikasi, dan dihapus setiap kali sumber data Anda disinkronkan dengan indeks Anda. Amazon Kendra dapat menggunakan mekanisme sumber data Anda untuk melacak perubahan konten dan mengindeks konten yang berubah sejak sinkronisasi terakhir. • `CHANGE_LOG` untuk mengindeks hanya konten baru dan yang dimodifikasi setiap kali sumber data Anda disinkronkan dengan indeks Anda. Amazon Kendra dapat menggunakan mekanisme sumber data Anda untuk melacak perubahan konten dan mengindeks konten yang berubah sejak sinkronisasi terakhir.

Konfigurasi	Deskripsi
Sekretarn	Nama Sumber Daya Amazon (ARN) dari rahasia Secrets Manager yang berisi nama pengguna dan kata sandi yang diperlukan untuk terhubung ke database Anda. Rahasiany a harus berisi struktur JSON dengan kunci berikut: `{ "user name": "database user name", "password": " password" }`
versi	Versi template yang saat ini didukung.

Amazon RDS (PostgreSQL) Skema JSON

```
{
  "$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 skema templat

Anda menyertakan JSON yang berisi skema sumber data sebagai bagian dari konfigurasi template. Anda memberikan nama bucket S3 sebagai bagian dari konfigurasi koneksi atau detail titik akhir repositori. Juga tentukan jenis sumber data sebagai`S3`, dan konfigurasi lain yang diperlukan. Anda kemudian menentukan `TEMPLATE` sebagai `Type` saat Anda menelepon CreateDataSource.

Anda dapat menggunakan template yang disediakan dalam panduan pengembang ini. Lihat Skema S3 JSON.

Tabel berikut menjelaskan parameter skema Amazon S3 JSON.

Konfigurasi	Deskripsi
ConnectionConfiguration	Informasi konfigurasi untuk titik akhir untuk sumber data.
repositoryEndpointMetadata	Informasi titik akhir untuk sumber data.
BucketName	Nama Amazon S3 ember Anda.
RepositoryConfigurations	Informasi konfigurasi untuk konten sumber data. Misalnya, mengonfigurasi jenis konten dan pemetaan bidang tertentu.
AdditionalProperties	Opsi konfigurasi tambahan untuk konten Anda di sumber data Anda
• Pola Inklusi • Pola Pengecualian • Inklusi Prefixes	Daftar pola ekspresi reguler untuk menyertak an atau mengecualikan file tertentu dalam sumber Amazon S3 data Anda. File yang cocok

Konfigurasi	Deskripsi
• PengecualianAwalan	dengan pola disertakan dalam indeks. File yang tidak cocok dengan pola dikecualikan dari indeks. Jika file cocok dengan pola inklusi dan pengecualian, pola pengecualian akan diutamakan dan file tidak disertakan dalam indeks.
aclConfigurationFileJalan	Jalur file yang mengontrol akses ke dokumen dalam Amazon Kendra indeks.
metadataFilesPrefix	Lokasi dalam bucket Anda untuk file metadata.
SyncMode	Tentukan bagaimana Amazon Kendra seharusnya memperbarui indeks Anda saat konten sumber data Anda berubah. Anda dapat memilih antara: • `FORCED_FULL_CRAWL` untuk mengindeks semua konten baru, mengganti konten yang ada setiap kali sumber data Anda disinkron kan dengan indeks Anda. • `FULL_CRAWL` untuk mengindeks hanya konten baru, dimodifikasi, dan dihapus setiap kali sumber data Anda disinkronkan dengan indeks Anda. Amazon Kendra dapat menggunakan mekanisme sumber data Anda untuk melacak perubahan konten dan mengindeks konten yang berubah sejak sinkronisasi terakhir.
jenis	Jenis sumber data. Tentukan `S3` sebagai tipe sumber data Anda.
versi	Versi template yang didukung.

Skema S3 JSON

```
{
  "$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"
      ]
    },
    "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 Skema Templat Perayap Web

Anda menyertakan JSON yang berisi skema sumber data sebagai bagian dari objek. TemplateConfiguration

Anda memberikan URL seed atau titik awal, atau Anda dapat memberikan URL peta situs, sebagai bagian dari konfigurasi koneksi atau detail titik akhir repositori. Alih-alih mencantumkan semua URL Anda secara manual, Anda dapat memberikan jalur ke Amazon S3 bucket yang menyimpan file teks untuk daftar URL benih atau file XHTML peta situs, yang dapat Anda gabungkan bersama dalam file ZIP di S3.

Anda juga menentukan jenis sumber data sebagai`WEBCRAWLERV2`, kredensi otentikasi situs web dan jenis otentikasi jika situs web Anda memerlukan otentikasi, dan konfigurasi lain yang diperlukan.

Anda kemudian menentukan `TEMPLATE` sebagai `Type` saat Anda menelepon CreateDataSource.

> **Important**
>
> Pembuatan konektor Web Crawler v2.0 tidak didukung oleh. AWS CloudFormation Gunakan konektor Web Crawler v1.0 jika Anda memerlukan AWS CloudFormation dukungan.

Saat memilih situs web untuk diindeks, Anda harus mematuhi Kebijakan Penggunaan yang Diterima Amazon dan semua syarat Amazon lainnya. Ingat bahwa Anda hanya harus menggunakan Amazon Kendra Web Crawler untuk mengindeks halaman web Anda sendiri, atau halaman web yang Anda memiliki otorisasi untuk indeks. Untuk mempelajari cara menghentikan Amazon Kendra Web Crawler dari mengindeks situs web Anda, lihat. Mengkonfigurasi *`robots.txt`* file untuk Amazon Kendra Web Crawler

Anda dapat menggunakan template yang disediakan dalam panduan pengembang ini. Lihat Amazon Kendra Skema JSON Web Crawler.

Tabel berikut menjelaskan parameter skema Amazon Kendra Web Crawler JSON.

Konfigurasi	Deskripsi
ConnectionConfiguration	Informasi konfigurasi untuk titik akhir untuk sumber data.
repositoryEndpointMetadata	Informasi titik akhir untuk sumber data.
siteMapUrls	Daftar URL peta situs untuk situs web yang ingin Anda jelajahi. Anda dapat mencantumkan hingga tiga URL peta situs.
s3 SeedUrl	Jalur S3 ke file teks yang menyimpan daftar URL benih atau titik awal. Misalnya, s3://bucket-name/directory/. Setiap URL dalam file teks harus diformat pada baris terpisah. Anda dapat

Konfigurasi	Deskripsi
	mencantumkan hingga 100 URL benih dalam satu file.
s3 SiteMapUrl	Jalur S3 ke file XMLpeta situs. Misalnya, s3://bucket-name/directory/. Anda dapat membuat daftar hingga tiga file XHTML sitemap. Anda dapat menggabungkan beberapa file peta situs ke dalam file ZIP dan menyimpan file ZIP di bucket Anda Amazon S3 .
seedUrlConnections	Daftar URL benih atau titik awal untuk situs web yang ingin Anda jelajahi. Anda dapat mencantumkan hingga 100 URL benih.
SeedURL	URL benih atau titik awal.
autentikasi	Jenis otentikasi jika situs web Anda memerlukan otentikasi yang sama, jika tidak, tentukan. `NoAuthentication`
RepositoryConfigurations	Informasi konfigurasi untuk konten sumber data. Misalnya, mengonfigurasi jenis konten dan pemetaan bidang tertentu.
• Halaman Web • lampiran	Daftar objek yang memetakan atribut atau nama bidang halaman web dan file halaman web Anda untuk Amazon Kendra mengindeks nama bidang. Misalnya, tag judul halaman web HTML dapat dipetakan ke bidang `_document_title` indeks. Untuk informasi lebih lanjut, lihat Memetakan bidang sumber data.

Konfigurasi	Deskripsi
SyncMode	Tentukan bagaimana Amazon Kendra seharusnya memperbarui indeks Anda saat konten sumber data Anda berubah. Anda dapat memilih antara: • `FORCED_FULL_CRAWL` untuk mengindeks semua konten baru, mengganti konten yang ada setiap kali sumber data Anda disinkron kan dengan indeks Anda. • `FULL_CRAWL` untuk mengindeks hanya konten baru, dimodifikasi, dan dihapus setiap kali sumber data Anda disinkronkan dengan indeks Anda. Amazon Kendra dapat menggunakan mekanisme sumber data Anda untuk melacak perubahan konten dan mengindeks konten yang berubah sejak sinkronisasi terakhir.
AdditionalProperties	Opsi konfigurasi tambahan untuk konten Anda di sumber data Anda.
RateLimit	Jumlah maksimum URL yang dirayapi per host situs web per menit.
maxFileSize	Ukuran maksimum (dalam MB) halaman web atau lampiran untuk dirayapi.
CrawlDepth	Jumlah level dari URL seed yang akan dirayapi. Misalnya, halaman URL benih adalah kedalaman 1 dan hyperlink apa pun di halaman ini yang juga dirayapi adalah kedalaman 2.

Konfigurasi	Deskripsi
maxLinksPerUrl	Jumlah maksimum URL pada halaman web yang akan disertakan saat merayapi situs web. Nomor ini per halaman web. Saat halaman web situs web dirayapi, URL apa pun yang ditautkan ke halaman web juga dirayapi. URL pada halaman web dirayapi sesuai urutan tampilan.
crawlSubDomain	`true`untuk merayapi domain situs web dengan subdomain. Misalnya, jika URL benih adalah "abc.example.com“, maka" "dana.abc.example.com" b.abc.example.com "juga dirayapi. Jika Anda tidak menyetel `crawlSubDomain` atau `crawlAllDomain` ke`true`, maka Amazon Kendra hanya merayapi domain situs web yang ingin Anda jelajahi.
crawlAllDomain	`true`untuk merayapi domain situs web dengan subdomain dan domain lain yang ditautkan halaman web. Jika Anda tidak menyetel `crawlSubDomain` atau `crawlAllDomain` ke`true`, maka Amazon Kendra hanya merayapi domain situs web yang ingin Anda jelajahi.
HonorRobots	`true`untuk menghormati arahan robots.txt dari situs web yang ingin Anda jelajahi. Arahan ini mengontrol cara Amazon Kendra Web Crawler merayapi situs web, apakah hanya Amazon Kendra dapat merayapi konten tertentu atau tidak merayapi konten apa pun.
CrawlatTachments	`true`untuk merayapi file yang ditautkan ke halaman web.

Konfigurasi	Deskripsi
• Inklusi URL CrawlPatterns • Inklusi URL IndexPatterns	Daftar pola ekspresi reguler untuk menyertakan crawling URL tertentu dan mengindeks hyperlink apa pun di halaman web URL ini. URL yang cocok dengan pola disertakan dalam indeks. URL yang tidak cocok dengan pola dikecualikan dari indeks. Jika URL cocok dengan pola inklusi dan pengecualian, pola pengecualian akan diutamakan, dan halaman web URL/situs web tidak disertakan dalam indeks.
• URL PengecualianURL CrawlPatterns • URL PengecualianURL IndexPatterns	Daftar pola ekspresi reguler untuk mengecualikan perayapan URL tertentu dan mengindeks hyperlink apa pun di halaman web URL ini. URL yang cocok dengan pola dikecualikan dari indeks. URL yang tidak cocok dengan pola disertakan dalam indeks. Jika URL cocok dengan pola inklusi dan pengecualian, pola pengecualian akan diutamakan, dan halaman web URL/situs web tidak disertakan dalam indeks.
inclusionFileIndexPola	Daftar pola ekspresi reguler untuk menyertakan file halaman web tertentu. File yang cocok dengan pola disertakan dalam indeks. File yang tidak cocok dengan pola dikecualikan dari indeks. Jika file cocok dengan pola inklusi dan pengecualian, pola pengecualian akan diutamakan, dan file tidak disertakan dalam indeks.

Konfigurasi	Deskripsi
exclusionFileIndexPola	Daftar pola ekspresi reguler untuk mengecual ikan file halaman web tertentu. File yang cocok dengan pola dikecualikan dari indeks. File yang tidak cocok dengan pola disertakan dalam indeks. Jika file cocok dengan pola inklusi dan pengecualian, pola pengecualian akan diutamakan, dan file tidak disertakan dalam indeks.
proxy	Informasi konfigurasi diperlukan untuk terhubung ke situs web internal Anda melalui proxy web.
host	Nama host dari proxy sever yang ingin Anda gunakan untuk terhubung ke situs web internal. Misalnya, nama host https://a.example.com/page1.htmladalah "a.example.com”.
port	Nomor port dari pemutus proxy yang ingin Anda gunakan untuk terhubung ke situs web internal. Misalnya, 443 adalah port standar untuk HTTPS.
sekretarn (proxy)	Jika kredensyal proxy web diperlukan untuk terhubung ke host situs web, Anda dapat membuat AWS Secrets Manager rahasia yang menyimpan kredensialnya. Berikan Nama Sumber Daya Amazon (ARN) rahasia tersebut.
jenis	Jenis sumber data. Tentukan `WEBCRAWLERV2` sebagai tipe sumber data Anda.

Konfigurasi	Deskripsi
Sekretarn	Nama Sumber Daya Amazon (ARN) dari AWS Secrets Manager rahasia yang digunakan jika situs web Anda memerlukan otentikasi untuk mengakses situs web. Anda menyimpan kredensi otentikasi untuk situs web dalam rahasia yang berisi pasangan nilai kunci JSON. Jika Anda menggunakan dasar, atau NTML/KerberOS, masukkan nama pengguna dan kata sandi. Kunci JSON dalam rahasia harus `userName` dan`password`. Protokol otentikasi NTLM mencakup hashing kata sandi, dan protokol otentikasi Kerberos mencakup enkripsi kata sandi. Jika Anda menggunakan SAFL atau otentikasi formulir, masukkan nama pengguna dan kata sandi, XPath untuk bidang nama pengguna (dan tombol nama pengguna jika menggunakan SALL), XPaths untuk bidang dan tombol kata sandi, dan URL halaman login. Kunci JSON dalam rahasia harus`userName`,,, `passworduserNameFieldXpath` ,`userNameButtonXpath` , `passwordFieldXpath` `passwordButtonXpath` , dan`loginPageUrl` . Anda dapat menemukan elemen XPaths (XMLPath Language) menggunakan alat pengembang browser web Anda. XPaths biasanya mengikuti format ini:`//tagname[@Attribute='Value']` . Amazon Kendra juga memeriksa apakah informasi titik akhir (URL benih) yang disertakan dalam rahasia sama dengan informasi titik

Konfigurasi	Deskripsi
	akhir yang ditentukan dalam detail konfigurasi titik akhir sumber data Anda.
versi	Versi template ini yang saat ini didukung.

Amazon Kendra Skema JSON Web Crawler

```
{
  "$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"
  ]
}
```

Skema templat pertemuan

Anda menyertakan JSON yang berisi skema sumber data sebagai bagian dari objek. TemplateConfiguration Anda memberikan URL host Confluence, metode hosting, dan jenis otentikasi sebagai bagian dari konfigurasi koneksi atau detail titik akhir repositori. Juga tentukan jenis sumber data sebagai`CONFLUENCEV2`, rahasia untuk kredensyal otentikasi Anda, dan konfigurasi lain yang diperlukan. Anda kemudian menentukan `TEMPLATE` sebagai `Type` saat Anda menelepon CreateDataSource.

Anda dapat menggunakan template yang disediakan dalam panduan pengembang ini. Lihat Skema Confluence JSON.

Tabel berikut menjelaskan parameter skema Confluence JSON.

Konfigurasi	Deskripsi
ConnectionConfiguration	Informasi konfigurasi untuk titik akhir untuk sumber data.
repositoryEndpointMetadata	Informasi titik akhir untuk sumber data.
HostURL	URL untuk instance Confluence Anda. Misalnya, *https://example.confluence.com* .
jenis	Metode hosting untuk instance Confluence Anda, apakah `SAAS` dan. `ON_PREM`
authType	Metode otentikasi untuk instance Confluence Anda, apakah`Basic`, `OAuth2` atau. `Personal-token`
RepositoryConfigurations	Informasi konfigurasi untuk konten sumber data. Misalnya, mengonfigurasi jenis konten dan pemetaan bidang tertentu.
• yang lebih besar • halaman • blog • komentar • lampiran	Daftar objek yang memetakan atribut atau nama bidang ruang Confluence Anda, halaman, blog, komentar, dan lampiran untuk Amazon Kendra mengindeks nama bidang. Untuk informasi lebih lanjut, lihat Memetakan bidang sumber data. Nama bidang sumber data Confluence harus ada di metadata kustom Confluence Anda.
AdditionalProperties	Opsi konfigurasi tambahan untuk konten Anda di sumber data Anda.
isCrawlAcl	`true`untuk merayapi informasi daftar kontrol akses (ACL) untuk dokumen Anda, jika Anda memiliki ACL dan ingin menggunakannya untuk kontrol akses. ACL menentukan dokumen mana yang dapat diakses pengguna dan grup.

Konfigurasi	Deskripsi
	Informasi ACL digunakan untuk memfilter hasil pencarian berdasarkan pengguna atau akses grup mereka ke dokumen. Untuk informasi selengkapnya, lihat Pemfilteran konteks pengguna.
fieldForUserId	Tentukan `email` apakah Anda ingin menggunakan email pengguna untuk ID pengguna. `email`digunakan secara default dan saat ini satu-satunya tipe ID pengguna yang didukung.
• inclusionSpaceKeyFilter • exclusionSpaceKeyFilter • pageTitleRegMANTAN • blogTitleRegMANTAN • commentTitleRegMANTAN • attachmentTitleRegMANTAN • inclusionFileTypePola • exclusionFileTypePola • inclusionUrlPatterns • exclusionUrlPatterns	Daftar pola ekspresi reguler untuk menyertakan dan/atau mengecualikan file tertentu dalam sumber data Confluence Anda. File yang cocok dengan pola disertakan dalam indeks. File yang tidak cocok dengan pola dikecualikan dari indeks. Jika file cocok dengan pola inklusi dan pengecualian, pola pengecualian akan diutamakan dan file tidak disertakan dalam indeks.
ProxyHost	Nama host dari proxy web yang Anda gunakan, tanpa `https://` protokol `http://` atau.
ProxyPort	Nomor port yang digunakan oleh protokol transport URL host. Harus berupa nilai numerik antara 0 dan 65535.

Konfigurasi	Deskripsi
• isCrawlPersonalRuang • isCrawlArchivedRuang • isCrawlArchivedHalaman • isCrawlPage • isCrawlBlog • isCrawlPageKomentar • isCrawlPageLampiran • isCrawlBlogKomentar • isCrawlBlogLampiran	`true`untuk merayapi file di ruang pribadi Confluence Anda, halaman, blog, komentar halaman, lampiran halaman, komentar blog, dan lampiran blog.
maxFileSizeInMegaBytes	Tentukan batas ukuran file di MB yang Amazon Kendra dapat dirayapi. Amazon Kendra hanya merayapi file dalam batas ukuran yang Anda tentukan. Ukuran file default adalah 50MB. Ukuran file maksimum harus lebih besar dari 0MB dan kurang dari atau sama dengan 50MB.
jenis	Jenis sumber data. Tentukan `CONFLUENCEV2` sebagai tipe sumber data Anda.
enableIdentityCrawler	`true`untuk menggunakan Amazon Kendra crawler identitas untuk menyinkronkan identitas /informasi utama pada pengguna dan grup dengan akses ke dokumen tertentu. Jika perayap identitas dimatikan, semua dokumen dapat dicari secara publik. Jika Anda ingin menggunakan kontrol akses untuk dokumen dan crawler identitas dimatikan, Anda dapat menggunakan PutPrincipalMappingAPI untuk mengunggah informasi akses pengguna dan grup.

Konfigurasi	Deskripsi
SyncMode	Tentukan bagaimana Amazon Kendra seharusnya memperbarui indeks Anda saat konten sumber data Anda berubah. Anda dapat memilih antara: • `FORCED_FULL_CRAWL` untuk mengindeks semua konten baru, mengganti konten yang ada setiap kali sumber data Anda disinkron kan dengan indeks Anda. • `FULL_CRAWL` untuk mengindeks hanya konten baru, dimodifikasi, dan dihapus setiap kali sumber data Anda disinkronkan dengan indeks Anda. Amazon Kendra dapat menggunakan mekanisme sumber data Anda untuk melacak perubahan konten dan mengindeks konten yang berubah sejak sinkronisasi terakhir.
Sekretarn	Nama Sumber Daya Amazon (ARN) dari AWS Secrets Manager rahasia yang berisi pasangan kunci-nilai yang diperlukan untuk terhubung ke Confluence Anda. Untuk informasi tentang pasangan nilai kunci ini, lihat Instruksi koneksi untuk Confluence.
versi	Versi template ini yang saat ini didukung.

Skema Confluence JSON

```
{
  "$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"
  ]
```

```
}
```

Skema templat Dropbox

Anda menyertakan JSON yang berisi skema sumber data sebagai bagian dari objek. TemplateConfiguration Anda memberikan kunci aplikasi Dropbox, rahasia aplikasi, dan token akses sebagai bagian dari rahasia Anda yang menyimpan kredensi otentikasi Anda. Juga tentukan jenis sumber data sebagai`DROPBOX`, jenis token akses yang ingin Anda gunakan (sementara atau permanen), dan konfigurasi lain yang diperlukan. Anda kemudian menentukan `TEMPLATE` sebagai `Type` saat Anda menelepon CreateDataSource.

Anda dapat menggunakan template yang disediakan dalam panduan pengembang ini. Lihat Skema Dropbox JSON.

Tabel berikut menjelaskan parameter skema Dropbox JSON.

Konfigurasi	Deskripsi
ConnectionConfiguration	Informasi konfigurasi untuk titik akhir untuk sumber data.
repositoryEndpointMetadata	Informasi titik akhir untuk sumber data. Sumber data ini tidak menentukan titik akhir di`repositoryEndpointMetadata` . Sebaliknya, informasi koneksi termasuk dalam AWS Secrets Manager rahasia yang Anda berikan`secretArn` .
RepositoryConfigurations	Informasi konfigurasi untuk konten sumber data. Misalnya, mengonfigurasi jenis konten dan pemetaan bidang tertentu.
• file • paper • kertas • jalan pintas	Daftar objek yang memetakan atribut atau nama bidang file Dropbox, Dropbox Paper, dan pintasan untuk Amazon Kendra mengindeks nama bidang. Untuk informasi lebih lanjut, lihat Memetakan bidang sumber data.

Konfigurasi	Deskripsi
Sekretarn	Nama Sumber Daya Amazon (ARN) dari AWS Secrets Manager rahasia yang berisi pasangan nilai kunci yang diperlukan untuk terhubung ke Dropbox Anda. Rahasianya harus berisi struktur JSON dengan kunci berikut: `{ "appKey": "Dropbox app key", "appSecret": " Dropbox app secret", "accesstoken": " temporary access token or refresh access token" }`
AdditionalProperties	Opsi konfigurasi tambahan untuk konten Anda di sumber data Anda.
• inclusionFileNamePola • inclusionFileTypePola	Daftar pola ekspresi reguler untuk menyertak an nama dan jenis file tertentu di sumber data Dropbox Anda. File yang cocok dengan pola disertakan dalam indeks. File yang tidak cocok dengan pola dikecualikan dari indeks. Jika file cocok dengan pola inklusi dan pengecualian, pola pengecualian akan diutamakan dan file tidak disertakan dalam indeks.
• exclusionFileNamePola • exclusionFileTypePola	Daftar pola ekspresi reguler untuk mengecual ikan nama dan jenis file tertentu di sumber data Dropbox Anda. File yang cocok dengan pola dikecualikan dari indeks. File yang tidak cocok dengan pola disertakan dalam indeks. Jika file cocok dengan pola pengecualian dan inklusi, pola pengecualian akan diutamakan dan file tidak disertakan dalam indeks.

Konfigurasi	Deskripsi
• CrawlFile • CrawlPaper • CrawlPapert • CrawlShortcut	`true`untuk merayapi file di Dropbox, dokumen Dropbox Paper, templat Dropbox Paper, dan pintasan halaman web yang disimpan di Dropbox Anda.
jenis	Jenis sumber data. Tentukan `DROPBOX` sebagai tipe sumber data Anda.
useChangeLog	`true`untuk menggunakan log perubahan Dropbox untuk menentukan dokumen mana yang perlu ditambahkan, diperbarui, atau dihapus dalam indeks. Bergantung pada ukuran log perubahan, mungkin perlu waktu lebih lama Amazon Kendra untuk menggunak an log perubahan daripada memindai semua dokumen Anda di Dropbox Anda.
TokenType	Tentukan jenis token akses Anda: token akses permanen atau sementara. Anda disarankan untuk membuat token akses penyegaran yang tidak pernah kedaluwarsa di Dropbox daripada mengandalkan token akses satu kali yang kedaluwarsa setelah 4 jam. Anda membuat aplikasi dan token akses refresh di konsol pengembang Dropbox dan menyediakan token akses dalam rahasia Anda.
versi	Versi template ini yang saat ini didukung.

Skema Dropbox JSON

```
{
  "$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"
```

```
                    }
                  },
                  "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"
        ]
      }
    }
  },
  "secretArn": {
    "type": "string"
  },
  "additionalProperties": {
    "type": "object",
    "properties": {
      "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"
    },
    "useChangeLog": {
      "type": "string",
      "enum": [
        "true",
        "false"
      ]
    },
    "tokenType": {
      "type": "string",
      "enum": [
        "PERMANENT",
        "TEMPORARY"
      ]
    },
    "version": {
      "type": "string",
      "anyOf": [
        {
          "pattern": "1.0.0"
        }
      ]
    }
  },
  "additionalProperties": false,
  "required": [
    "connectionConfiguration",
    "repositoryConfigurations",
    "additionalProperties",
    "useChangeLog",
    "secretArn",
    "type",
    "tokenType"
  ]
```

```
}
```

Skema template Drupal

Anda menyertakan JSON yang berisi skema sumber data sebagai bagian dari objek. TemplateConfiguration Anda memberikan URL host Drupal dan jenis otentikasi sebagai bagian dari konfigurasi koneksi atau detail titik akhir repositori. Juga tentukan jenis sumber data sebagai DRUPAL, rahasia untuk kredensi otentikasi Anda, dan konfigurasi lain yang diperlukan. Anda kemudian menentukan `TEMPLATE` sebagai `Type` saat Anda menelepon CreateDataSource.

Anda dapat menggunakan template yang disediakan dalam panduan pengembang ini. Lihat Skema JSON Drupal.

Tabel berikut menjelaskan parameter skema JSON Drupal.

Konfigurasi	Deskripsi
ConnectionConfiguration	Informasi konfigurasi untuk titik akhir untuk sumber data.
repositoryEndpointMetadata	Informasi titik akhir untuk sumber data.
HostURL	URL host situs web Drupal Anda. <drupalsi tename>Misalnya, *https:///* <hostname>.
RepositoryConfigurations	Informasi konfigurasi untuk konten sumber data.
• content • komentar • lampiran	Daftar objek yang memetakan atribut atau nama bidang file Drupal Anda. Untuk informasi lebih lanjut, lihat Memetakan bidang sumber data. Nama bidang sumber data Drupal harus ada di metadata kustom Drupal Anda.
AdditionalProperties	Opsi konfigurasi tambahan untuk konten Anda di sumber data Anda.
• inclusionFileNamePola • articleTitleInclusionPola	Daftar pola ekspresi reguler untuk menyertakan file tertentu dalam sumber data Drupal Anda. File yang cocok dengan pola disertakan dalam

Konfigurasi	Deskripsi
• pageTitleInclusionPola • customContentTitleInclusionPatterns • basicBlockTitleInclusionPatterns • customBlockTitleInclusionPatterns	indeks. File yang tidak cocok dengan pola dikecualikan dari indeks. Jika file cocok dengan pola inklusi dan pengecualian, pola pengecual ian akan diutamakan dan file tidak disertakan dalam indeks.
• exclusionFileNamePola • articleTitleExclusionPola • pageTitleExclusionPola • customContentTitleExclusionPatterns • basicBlockTitleExclusionPatterns • customBlockTitleExclusionPatterns	Daftar pola ekspresi reguler untuk mengecual ikan file tertentu di sumber data Drupal Anda. File yang cocok dengan pola dikecualikan dari indeks. File yang tidak cocok dengan pola disertakan dalam indeks. Jika file cocok dengan pola pengecualian dan inklusi, pola pengecual ian akan diutamakan dan file tidak disertakan dalam indeks.
ContentDefinitions • ContentType • FieldDefinition • isCrawlComments • isCrawlFiles • isCrawlArticle • isCrawlBasicHalaman • isCrawlBasicBlok • isCrawlCustomContentTypesList	Tentukan jenis konten yang akan dirayapi dan apakah akan merayapi komentar dan lampiran untuk jenis konten yang Anda pilih.
jenis	Jenis sumber data. Tentukan `DRUPAL` sebagai tipe sumber data Anda.
authType	Jenis otentikasi yang Anda gunakan, apakah `BASIC-AUTH` atau`OAUTH2`.

Konfigurasi	Deskripsi
SyncMode	Tentukan bagaimana Amazon Kendra seharusnya memperbarui indeks Anda saat konten sumber data Anda berubah. Anda dapat memilih antara: • `FORCED_FULL_CRAWL` untuk mengindeks semua konten baru, mengganti konten yang ada setiap kali sumber data Anda disinkron kan dengan indeks Anda. • `FULL_CRAWL` untuk mengindeks hanya konten baru, dimodifikasi, dan dihapus setiap kali sumber data Anda disinkronkan dengan indeks Anda. Amazon Kendra dapat menggunakan mekanisme sumber data Anda untuk melacak perubahan konten dan mengindeks konten yang berubah sejak sinkronisasi terakhir. • `CHANGE_LOG` untuk mengindeks hanya konten baru dan yang dimodifikasi setiap kali sumber data Anda disinkronkan dengan indeks Anda. Amazon Kendra dapat menggunakan mekanisme sumber data Anda untuk melacak perubahan konten dan mengindeks konten yang berubah sejak sinkronisasi terakhir.

Konfigurasi	Deskripsi
enableIdentityCrawler	`true`untuk menggunakan Amazon Kendra crawler identitas untuk menyinkronkan identitas /informasi utama pada pengguna dan grup dengan akses ke dokumen tertentu. Jika perayap identitas dimatikan, semua dokumen dapat dicari secara publik. Jika Anda ingin menggunakan kontrol akses untuk dokumen dan crawler identitas dimatikan, Anda dapat menggunakan PutPrincipalMappingAPI untuk mengunggah informasi akses pengguna dan grup.

Sekretarn	Nama Sumber Daya Amazon (ARN) dari AWS Secrets Manager rahasia yang berisi pasangan kunci-nilai yang diperlukan untuk terhubung ke Drupal Anda. Rahasianya harus berisi struktur JSON dengan kunci berikut:
	
	Jika menggunakan otentikasi dasar:
	
	`{ "username": "user name", "passwords": "password" }`
	
	Jika menggunakan otentikasi OAuth 2.0:
	
	`{ "username": "user name", "password": "password" , "clientId": "client id", "clientSecret": "client secret" }`

versi	Versi template ini yang saat ini didukung.

Skema JSON Drupal

```
{
 "$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 skema templat

Anda menyertakan JSON yang berisi skema sumber data sebagai bagian dari objek. TemplateConfiguration Anda memberikan URL GitHub host, nama organisasi, dan apakah Anda menggunakan GitHub GitHub cloud atau lokal sebagai bagian dari konfigurasi koneksi atau detail titik akhir repositori. Juga tentukan jenis sumber data sebagai`GITHUB`, rahasia untuk kredensyal otentikasi Anda, dan konfigurasi lain yang diperlukan. Anda kemudian menentukan `TEMPLATE` sebagai `Type` saat Anda menelepon CreateDataSource.

Anda dapat menggunakan template yang disediakan dalam panduan pengembang ini. Lihat GitHub Skema JSON.

Tabel berikut menjelaskan parameter skema GitHub JSON.

Konfigurasi	Deskripsi
ConnectionConfiguration	Informasi konfigurasi untuk titik akhir untuk sumber data.
repositoryEndpointMetadata	Informasi titik akhir untuk sumber data.
jenis	Tentukan jenisnya sebagai salah satu `SAAS` atau`ON_PREMISE` .
HostURL	URL GitHub host. Misalnya, jika Anda menggunakan GitHub SaaS/Enterprise Cloud:. https://api.github.com Atau, jika Anda menggunakan GitHub On-Premises/Enterprise Server:. https://on-prem-host-url/api/v3/
Nama Organisasi	Anda dapat menemukan nama organisasi Anda ketika Anda masuk ke GitHub desktop dan pergi ke Organisasi Anda di bawah dropdown gambar profil Anda.
RepositoryConfigurations	Informasi konfigurasi untuk konten sumber data. Misalnya, mengonfigurasi jenis konten dan pemetaan bidang tertentu.

Konfigurasi	Deskripsi
• GHRepositori • GHKomit • ghIssueDocument • ghIssueComment • ghIssueAttachment • GHPRDocument • GHPRKomentar • GHPRLampiran	Daftar objek yang memetakan atribut atau nama bidang GitHub konten Anda untuk Amazon Kendra mengindeks nama bidang. Untuk informasi lebih lanjut, lihat Memetakan bidang sumber data.
AdditionalProperties	Opsi konfigurasi tambahan untuk konten Anda di sumber data Anda.
isCrawlAcl	`true`untuk merayapi informasi daftar kontrol akses (ACL) untuk dokumen Anda, jika Anda memiliki ACL dan ingin menggunakannya untuk kontrol akses. ACL menentukan dokumen mana yang dapat diakses dan dicari oleh pengguna dan grup. Informasi ACL digunakan untuk memfilter hasil pencarian berdasark an pengguna atau akses grup mereka ke dokumen. Untuk informasi selengkapnya, lihat Pemfilteran konteks pengguna.
fieldForUserId	Tentukan jenis ID pengguna yang ingin Anda gunakan untuk perayapan ACL. Tentukan `email` apakah Anda ingin menggunakan email pengguna untuk ID pengguna, atau `username` jika Anda ingin menggunakan nama pengguna untuk ID pengguna. Jika Anda tidak menentuka n opsi maka `email` digunakan secara default.
RepositoryFilter	Daftar nama repositori tertentu dan nama cabang yang ingin Anda indeks.

Konfigurasi	Deskripsi
CrawlRepository	`true`untuk merayapi repositori.
crawlRepositoryDocuments	`true`untuk merayapi dokumen repositori.
CrawlIssue	`true`untuk merayapi masalah.
crawlIssueComment	`true`untuk merayapi komentar masalah.
crawlIssueCommentLampiran	`true`untuk merayapi lampiran komentar masalah.
crawlPullRequest	`true`untuk merayapi permintaan tarik.
crawlPullRequestKomentar	`true`untuk merayapi komentar permintaan tarik.
crawlPullRequestCommentAttachment	`true`untuk merayapi lampiran komentar permintaan tarik.
• inclusionFolderNamePola • inclusionFileTypePola • inclusionFileNamePola	Daftar pola ekspresi reguler untuk menyertakan konten tertentu dalam sumber GitHub data Anda. Konten yang cocok dengan pola disertakan dalam indeks. Konten yang tidak cocok dengan pola dikecualikan dari indeks. Jika ada konten yang cocok dengan pola inklusi dan pengecualian, pola pengecualian akan diutamakan, dan konten tidak disertakan dalam indeks.

Konfigurasi	Deskripsi
• exclusionFolderNamePola • exclusionFileTypePola • exclusionFileNamePola	Daftar pola ekspresi reguler untuk mengecual ikan konten tertentu dalam sumber GitHub data Anda. Konten yang cocok dengan pola dikecualikan dari indeks. Konten yang tidak cocok dengan pola disertakan dalam indeks. Jika ada konten yang cocok dengan pola inklusi dan pengecualian, pola pengecualian akan diutamakan, dan konten tidak disertakan dalam indeks.
jenis	Jenis sumber data. Tentukan `GITHUB` sebagai tipe sumber data Anda.
enableIdentityCrawler	`true`untuk menggunakan Amazon Kendra crawler identitas untuk menyinkronkan identitas /informasi utama pada pengguna dan grup dengan akses ke dokumen tertentu. Jika perayap identitas dimatikan, semua dokumen dapat dicari secara publik. Jika Anda ingin menggunakan kontrol akses untuk dokumen dan crawler identitas dimatikan, Anda dapat menggunakan PutPrincipalMappingAPI untuk mengunggah informasi akses pengguna dan grup.

Konfigurasi	Deskripsi
SyncMode	Tentukan bagaimana Amazon Kendra seharusnya memperbarui indeks Anda saat konten sumber data Anda berubah. Anda dapat memilih antara: • `FORCED_FULL_CRAWL` untuk mengindeks semua konten baru, mengganti konten yang ada setiap kali sumber data Anda disinkron kan dengan indeks Anda. • `FULL_CRAWL` untuk mengindeks hanya konten baru, dimodifikasi, dan dihapus setiap kali sumber data Anda disinkronkan dengan indeks Anda. Amazon Kendra dapat menggunakan mekanisme sumber data Anda untuk melacak perubahan konten dan mengindeks konten yang berubah sejak sinkronisasi terakhir. • `CHANGE_LOG` untuk mengindeks hanya konten baru dan yang dimodifikasi setiap kali sumber data Anda disinkronkan dengan indeks Anda. Amazon Kendra dapat menggunakan mekanisme sumber data Anda untuk melacak perubahan konten dan mengindeks konten yang berubah sejak sinkronisasi terakhir.

Konfigurasi	Deskripsi
Sekretarn	Nama Sumber Daya Amazon (ARN) dari AWS Secrets Manager rahasia yang berisi pasangan kunci-nilai yang diperlukan untuk terhubung ke Anda. GitHub Rahasianya harus berisi struktur JSON dengan kunci berikut: `{ "personalToken": " token" }`
versi	Versi template ini yang saat ini didukung.

GitHub Skema JSON

Berikut ini adalah skema GitHub JSON:

```
{
    "$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"
    ]
}
```

Skema template Gmail

Anda menyertakan JSON yang berisi skema sumber data sebagai bagian dari objek. TemplateConfiguration Tentukan jenis sumber data sebagai`GMAIL`, rahasia untuk kredensi otentikasi Anda, dan konfigurasi lain yang diperlukan. Anda kemudian menentukan `TEMPLATE` sebagai `Type` saat Anda menelepon CreateDataSource.

Anda dapat menggunakan template yang disediakan dalam panduan pengembang ini. Lihat Skema JSON Gmail.

Tabel berikut menjelaskan parameter skema JSON Gmail.

Konfigurasi	Deskripsi
ConnectionConfiguration	Informasi konfigurasi untuk titik akhir untuk sumber data.
RepositoryConfigurations	Informasi konfigurasi untuk konten sumber data. Misalnya, mengonfigurasi jenis konten dan pemetaan bidang tertentu. Tentukan jenis sumber data dan ARN rahasia.
• pesan • lampiran	Daftar objek yang memetakan atribut atau nama bidang pesan dan lampiran Gmail Anda ke nama bidang Amazon Kendra indeks. Untuk informasi lebih lanjut, lihat Memetakan bidang sumber data.
AdditionalProperties	Opsi konfigurasi tambahan untuk konten Anda di sumber data Anda.
• inclusionLabelNamePola • exclusionLabelNamePola • inclusionAttachmentTypePola • exclusionAttachmentTypePola • inclusionAttachmentNamePola • exclusionAttachmentNamePola • inclusionSubjectFilter • exclusionSubjectFilter • isSubjectAnd • inclusionFromFilter • exclusionFromFilter • inclusionToFilter • exclusionToFilter • inclusionCcFilter • exclusionCcFilter	Daftar pola ekspresi reguler untuk menyertakan atau mengecualikan pesan dengan nama subjek tertentu di sumber data Gmail Anda. File yang cocok dengan pola disertakan dalam indeks. Jika file cocok dengan pola inklusi dan pengecualian, pola pengecualian akan diutamakan, dan file tersebut tidak disertakan dalam indeks.

Konfigurasi	Deskripsi
• inclusionBccFilter • exclusionBccFilter	
beforeDateFilter	Tentukan pesan dan lampiran yang akan disertakan sebelum tanggal tertentu.
afterDateFilter	Tentukan pesan dan lampiran yang akan disertakan setelah tanggal tertentu.
isCrawlAttachment	Nilai Boolean untuk memilih apakah Anda ingin meng-crawl lampiran. Pesan dirayapi secara otomatis.
jenis	Jenis sumber data. Tentukan `GMAIL` sebagai tipe sumber data Anda.
shouldCrawlDraftPesan	Nilai Boolean untuk memilih apakah Anda ingin merayapi pesan draf.

Konfigurasi	Deskripsi
SyncMode	Tentukan bagaimana Amazon Kendra seharusnya memperbarui indeks Anda saat konten sumber data Anda berubah. Anda dapat memilih antara: • `FORCED_FULL_CRAWL` untuk mengindeks semua konten baru, mengganti konten yang ada setiap kali sumber data Anda disinkron kan dengan indeks Anda. • `FULL_CRAWL` untuk mengindeks hanya konten baru, dimodifikasi, dan dihapus setiap kali sumber data Anda disinkronkan dengan indeks Anda. Amazon Kendra dapat menggunakan mekanisme sumber data Anda untuk melacak perubahan konten dan mengindeks konten yang berubah sejak sinkronisasi terakhir. **Important** Karena tidak ada API untuk memperbar ui pesan Gmail yang dihapus secara permanen, sinkronisasi konten baru, dimodifikasi, atau dihapus: • Tidak akan menghapus pesan yang dihapus secara permanen dari Gmail dari Amazon Kendra indeks Anda • Tidak akan menyinkronkan perubahan pada label email Gmail Untuk menyinkronkan perubahan label sumber data Gmail dan pesan email yang dihapus secara permanen ke

Konfigurasi	Deskripsi
	Amazon Kendra indeks, Anda harus menjalankan crawl penuh secara berkala.
Sekretarn	Nama Sumber Daya Amazon (ARN) dari rahasia Secrets Manager yang berisi pasangan nilai kunci yang diperlukan untuk terhubung ke Gmail Anda. Rahasianya harus berisi struktur JSON dengan kunci berikut: `{ "adminAccountEmailId": " service account email", "clientEmailId": " user account email", "privateKey": " private key" }`
versi	Versi template yang saat ini didukung.

Skema JSON Gmail

```
{
  "$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"
  ]
}
```

Skema templat Google Drive

Anda menyertakan JSON yang berisi skema sumber data sebagai bagian dari objek. TemplateConfiguration Tentukan jenis sumber data sebagai`GOOGLEDRIVE2`, rahasia untuk kredensi otentikasi Anda, dan konfigurasi lain yang diperlukan. Anda kemudian menentukan `TEMPLATE` sebagai `Type` saat Anda menelepon CreateDataSource.

Anda dapat menggunakan template yang disediakan dalam panduan pengembang ini. Lihat Skema Google Drive JSON.

Tabel berikut menjelaskan parameter skema Google Drive JSON.

Konfigurasi	Deskripsi
ConnectionConfiguration	Informasi konfigurasi untuk sumber data.
repositoryEndpointMetadata	Informasi titik akhir untuk sumber data. Sumber data ini tidak menentukan titik akhir. Anda memilih jenis otentikasi Anda: `serviceAccount` dan`OAuth2`. Informasi koneksi termasuk dalam AWS Secrets Manager rahasia yang Anda berikan`secretArn` .
authType	Pilih antara `serviceAccount` dan `OAuth2` berdasarkan kasus penggunaan Anda.

Konfigurasi	Deskripsi
RepositoryConfigurations	Informasi konfigurasi untuk konten sumber data. Misalnya, mengonfigurasi jenis konten dan pemetaan bidang tertentu.
• file • komentar	Daftar objek yang memetakan atribut atau nama bidang Google Drive Anda untuk Amazon Kendra mengindeks nama bidang. Untuk informasi lebih lanjut, lihat Memetakan bidang sumber data.
AdditionalProperties	Opsi konfigurasi tambahan untuk konten Anda di sumber data Anda
• maxFileSizeInMegaBytes	Tentukan batas ukuran file di MB yang Amazon Kendra harus dirayapi.
• ISCrawlKomentar	`true`untuk merayapi komentar di sumber data Google Drive Anda.
• isCrawlMyDriveAndSharedWithMe	`true`untuk meng-crawl MyDrive dan Shared With Me Drive di sumber data Google Drive Anda.
• isCrawlSharedDrive	`true`untuk merayapi Drive Bersama di sumber data Google Drive Anda.
isCrawlAcl	`true`untuk merayapi informasi daftar kontrol akses (ACL) untuk dokumen Anda, jika Anda memiliki ACL dan ingin menggunakannya untuk kontrol akses. ACL menentukan dokumen mana yang dapat diakses dan dicari oleh pengguna dan grup. Informasi ACL digunakan untuk memfilter hasil pencarian berdasark an pengguna atau akses grup mereka ke dokumen. Untuk informasi selengkapnya, lihat Pemfilteran konteks pengguna.

Konfigurasi	Deskripsi
• excludeUserAccounts • excludeSharedDrives • excludeMimeTypes • exclusionFileTypePola • exclusionFileNamePola • exclusionFilePathFilter	Daftar pola ekspresi reguler untuk mengecualikan file tertentu di sumber data Google Drive Anda. File yang cocok dengan pola dikecualikan dari indeks. File yang tidak cocok dengan pola disertakan dalam indeks. Jika file cocok dengan pola pengecualian dan inklusi, pola pengecualian akan diutamakan, dan file tidak disertakan dalam indeks.
• includeUserAccounts • includeSharedDrives • includeMimeTypes • inclusionFileTypePola • inclusionFileNamePola • inclusionFilePathFilter	Daftar pola ekspresi reguler untuk menyertakan file tertentu di sumber data Google Drive Anda. File yang cocok dengan pola disertakan dalam indeks. File yang tidak cocok dengan pola dikecualikan dari indeks. Jika file cocok dengan pola inklusi dan pengecualian, pola pengecualian akan diutamakan, dan file tidak disertakan dalam indeks.
jenis	Jenis sumber data. Tentukan `GOOGLEDRIVEV2` sebagai tipe sumber data Anda.
enableIdentityCrawler	`true`untuk menggunakan Amazon Kendra crawler identitas untuk menyinkronkan identitas /informasi utama pada pengguna dan grup dengan akses ke dokumen tertentu. Jika perayap identitas dimatikan, semua dokumen dapat dicari secara publik. Jika Anda ingin menggunakan kontrol akses untuk dokumen dan crawler identitas dimatikan, Anda dapat menggunakan PutPrincipalMappingAPI untuk mengunggah informasi akses pengguna dan grup.

Konfigurasi	Deskripsi
SyncMode	Tentukan bagaimana Amazon Kendra seharusnya memperbarui indeks Anda saat konten sumber data Anda berubah. Anda dapat memilih antara: • `FORCED_FULL_CRAWL` untuk mengindeks semua konten baru, mengganti konten yang ada setiap kali sumber data Anda disinkron kan dengan indeks Anda. • `FULL_CRAWL` untuk mengindeks hanya konten baru, dimodifikasi, dan dihapus setiap kali sumber data Anda disinkronkan dengan indeks Anda. Amazon Kendra dapat menggunakan mekanisme sumber data Anda untuk melacak perubahan konten dan mengindeks konten yang berubah sejak sinkronisasi terakhir. • `CHANGE_LOG` untuk mengindeks hanya konten baru dan yang dimodifikasi setiap kali sumber data Anda disinkronkan dengan indeks Anda. Amazon Kendra dapat menggunakan mekanisme sumber data Anda untuk melacak perubahan konten dan mengindeks konten yang berubah sejak sinkronisasi terakhir.

Konfigurasi	Deskripsi

Sekretarn	Nama Sumber Daya Amazon (ARN) dari AWS Secrets Manager rahasia yang berisi pasangan kunci-nilai yang diperlukan untuk terhubung ke Google Drive Anda. Rahasianya harus berisi struktur JSON dengan kunci berikut:
	
	Jika menggunakan otentikasi Akun Layanan Google:
	
	`{ "clientEmail": " user account email", "adminAccountEmail": " service account email", "privateKey": " private key" }`
	
	Jika menggunakan otentikasi OAuth 2.0:
	
	`{ "clientID": " OAuth client ID", "clientSecret": " client secret", "refreshToken": " refresh token" }`

versi	Versi template ini yang saat ini didukung.

Skema Google Drive JSON

```
{
  "$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"
  ]
}
```

Skema Templat IBM DB2

Anda menyertakan JSON yang berisi skema sumber data sebagai bagian dari objek. TemplateConfiguration Tentukan jenis sumber data sebagai`JDBC`, tipe database sebagai`db2`, rahasia untuk kredensyal otentikasi Anda, dan konfigurasi lain yang diperlukan. Anda kemudian menentukan `TEMPLATE` sebagai `Type` saat Anda menelepon CreateDataSource.

Anda dapat menggunakan template yang disediakan dalam panduan pengembang ini. Lihat IBM DB2 JSON skema.

Tabel berikut menjelaskan parameter skema IBM DB2 JSON.

Konfigurasi	Deskripsi
ConnectionConfiguration	Informasi konfigurasi untuk titik akhir untuk sumber data.

Konfigurasi	Deskripsi
repositoryEndpointMetadata	Informasi konfigurasi yang diperlukan untuk menghubungkan sumber data Anda. • DBType—jenis database Java yang Anda gunakan, apakah,,, `mysqldb2`, `postgresql` atau. `oracle` `sqlserver` • DBhost — nama host database. • DBport — port database. • DBinstance—contoh database.
RepositoryConfigurations	Informasi konfigurasi untuk konten sumber data. Misalnya, mengonfigurasi jenis konten dan pemetaan bidang tertentu. Tentukan jenis sumber data dan ARN rahasia.
dokumen	Daftar objek yang memetakan atribut atau nama bidang konten database Anda untuk Amazon Kendra mengindeks nama bidang. Untuk informasi lebih lanjut, lihat Memetakan bidang sumber data.
AdditionalProperties	Opsi konfigurasi tambahan untuk konten Anda di sumber data Anda. Gunakan untuk menyertakan atau mengecualikan konten tertentu dalam sumber data database Anda.
PrimaryKey	Berikan kunci utama untuk tabel database. Ini mengidentifikasi tabel dalam database Anda.
Judul Kolom	Berikan nama kolom judul dokumen dalam tabel database Anda.
BodyColumn	Berikan nama kolom judul dokumen dalam tabel database Anda.

Konfigurasi	Deskripsi
SqlQuery	Masukkan pernyataan kueri SQL seperti operasi SELECT dan JOIN. Kueri SQL harus kurang dari 32KB. Amazon Kendra akan merayapi semua konten database yang cocok dengan kueri Anda.
TimestampColumn	Masukkan nama kolom yang berisi stempel waktu. Amazon Kendra menggunakan informasi cap waktu untuk mendeteksi perubahan dalam konten Anda dan hanya menyinkronkan konten yang diubah.
TimestampFormat	Masukkan nama kolom yang berisi format cap waktu yang akan digunakan untuk mendeteks i perubahan konten dan menyinkronkan ulang konten Anda.
timezone	Masukkan nama kolom yang berisi zona waktu untuk konten yang akan dirayapi.
changeDetectingColumns	Masukkan nama kolom yang Amazon Kendra akan digunakan untuk mendeteksi perubahan konten. Amazon Kendra akan mengindeks ulang konten ketika ada perubahan di salah satu kolom ini
allowedUsersColumns	Masukkan nama kolom yang berisi ID Pengguna untuk diizinkan mengakses konten.
allowedGroupsColumn	Masukkan nama kolom yang berisi ID Pengguna untuk diizinkan mengakses konten.
Sourceuricolumn	Masukkan nama kolom yang berisi URL Sumber yang akan diindeks.

Konfigurasi	Deskripsi
isSslEnabled	Masukkan pernyataan kueri SQL seperti operasi SELECT dan JOIN. Kueri SQL harus kurang dari 32KB. Amazon Kendra akan merayapi semua konten database yang cocok dengan kueri Anda.
jenis	Jenis sumber data. Tentukan `JDBC` sebagai tipe sumber data Anda.
SyncMode	Tentukan bagaimana Amazon Kendra seharusnya memperbarui indeks Anda saat konten sumber data Anda berubah. Anda dapat memilih antara: • `FORCED_FULL_CRAWL` untuk mengindeks semua konten baru, mengganti konten yang ada setiap kali sumber data Anda disinkron kan dengan indeks Anda. • `FULL_CRAWL` untuk mengindeks hanya konten baru, dimodifikasi, dan dihapus setiap kali sumber data Anda disinkronkan dengan indeks Anda. Amazon Kendra dapat menggunakan mekanisme sumber data Anda untuk melacak perubahan konten dan mengindeks konten yang berubah sejak sinkronisasi terakhir. • `CHANGE_LOG` untuk mengindeks hanya konten baru dan yang dimodifikasi setiap kali sumber data Anda disinkronkan dengan indeks Anda. Amazon Kendra dapat menggunakan mekanisme sumber data Anda untuk melacak perubahan konten dan mengindeks konten yang berubah sejak sinkronisasi terakhir.

Konfigurasi	Deskripsi
Sekretarn	Nama Sumber Daya Amazon (ARN) dari rahasia Secrets Manager yang berisi nama pengguna dan kata sandi yang diperlukan untuk terhubung ke database Anda. Rahasiany a harus berisi struktur JSON dengan kunci berikut: `{ "user name": "database user name", "password": " password" }`
versi	Versi template yang saat ini didukung.

IBM DB2 JSON skema

```
{
  "$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"
  ]
}
```

Skema templat Microsoft Exchange

Anda menyertakan JSON yang berisi skema sumber data sebagai bagian dari objek. TemplateConfiguration Anda memberikan ID penyewa sebagai bagian dari konfigurasi koneksi atau detail titik akhir repositori. Juga tentukan jenis sumber data sebagai`MSEXCHANGE`, rahasia untuk kredensyal otentikasi Anda, dan konfigurasi lain yang diperlukan. Anda kemudian menentukan `TEMPLATE` sebagai `Type` saat Anda menelepon CreateDataSource.

Anda dapat menggunakan template yang disediakan dalam panduan pengembang ini. Lihat Skema Microsoft Exchange JSON.

Tabel berikut menjelaskan parameter skema Microsoft Exchange JSON.

Konfigurasi	Deskripsi
ConnectionConfiguration	Informasi konfigurasi untuk titik akhir untuk sumber data.
repositoryEndpointMetadata	Informasi titik akhir untuk sumber data.
TenanID	ID penyewa Microsoft 365. Anda dapat menemukan ID penyewa Anda di Properti Portal Direktori Aktif Azure Anda atau di aplikasi OAuth Anda.
RepositoryConfigurations	Informasi konfigurasi untuk konten sumber data. Misalnya, mengonfigurasi jenis konten dan pemetaan bidang tertentu.
• Email • lampiran	Daftar objek yang memetakan atribut atau nama bidang sumber data Microsoft Exchange

Konfigurasi	Deskripsi
• kalender • kontak • catatan	Anda ke bidang Amazon Kendra indeks. Untuk informasi lebih lanjut, lihat Memetakan bidang sumber data.
AdditionalProperties	Opsi konfigurasi tambahan untuk konten di sumber data Anda
Pola Inklusi	Daftar pola ekspresi reguler untuk menyertakan file tertentu di sumber data Microsoft Exchange Anda. File yang cocok dengan pola disertaka n dalam indeks. File yang tidak cocok dengan pola dikecualikan dari indeks. Jika file cocok dengan pola inklusi dan pengecualian, pola pengecualian akan diutamakan dan file tidak disertakan dalam indeks.
Pola Pengecualian	Daftar pola ekspresi reguler untuk mengecual ikan file tertentu di sumber data Microsoft Exchange Anda. File yang cocok dengan pola dikecualikan dari indeks. File yang tidak cocok dengan pola disertakan dalam indeks. Jika file cocok dengan pola pengecualian dan inklusi, pola pengecualian akan diutamakan dan file tidak disertakan dalam indeks.
• inclusionUsersList • inclusionUsersFileNama • inclusionDomainUsers	Daftar pola ekspresi reguler untuk menyertakan pengguna dan file pengguna tertentu di sumber data Microsofot Exchange Anda. Pengguna yang cocok dengan pola disertakan dalam indeks. Pengguna yang tidak cocok dengan pola dikecualikan dari indeks. Jika pengguna cocok dengan pola inklusi dan pengecual ian, pola pengecualian akan diutamakan dan pengguna tidak disertakan dalam indeks.

Konfigurasi	Deskripsi
• exclusionUsersList • exclusionUsersFileNama • exclusionDomainUsers	Daftar pola ekspresi reguler untuk mengecualikan pengguna dan file pengguna tertentu di sumber data Microsoft Exchange Anda. Pengguna yang cocok dengan pola dikecualikan dari indeks. Pengguna yang tidak cocok dengan pola disertakan dalam indeks. Jika pengguna cocok dengan pola pengecualian dan inklusi, pola pengecualian akan diutamakan dan pengguna tidak disertakan dalam indeks.
S3BucketName	Nama bucket S3 Anda jika ingin Anda gunakan.
• CrawlKalender • CrawlNotes • CrawlContacts • crawlFolderAcl	`true`untuk merayapi jenis konten ini dan informasi kontrol akses sumber data Microsoft Exchange Anda.
startCalendarDateWaktu	Anda dapat mengonfigurasi tanggal-waktu mulai tertentu untuk konten kalender Anda.
endCalendarDateWaktu	Anda dapat mengonfigurasi tanggal-waktu akhir tertentu untuk konten kalender.
subjek	Anda dapat mengonfigurasi baris subjek tertentu untuk konten email Anda.
EmailDari	Anda dapat mengonfigurasi email tertentu untuk konten email 'Dari' atau pengirim.
EmailTo	Anda dapat mengonfigurasi email tertentu untuk konten email 'Kepada' atau penerima.

Konfigurasi	Deskripsi
SyncMode	Tentukan bagaimana Amazon Kendra seharusnya memperbarui indeks Anda saat konten sumber data Anda berubah. Anda dapat memilih antara: • `FORCED_FULL_CRAWL` untuk mengindeks semua konten baru, mengganti konten yang ada setiap kali sumber data Anda disinkron kan dengan indeks Anda. • `FULL_CRAWL` untuk mengindeks hanya konten baru, dimodifikasi, dan dihapus setiap kali sumber data Anda disinkronkan dengan indeks Anda. Amazon Kendra dapat menggunakan mekanisme sumber data Anda untuk melacak perubahan konten dan mengindeks konten yang berubah sejak sinkronisasi terakhir. • `CHANGE_LOG` untuk mengindeks hanya konten baru dan yang dimodifikasi setiap kali sumber data Anda disinkronkan dengan indeks Anda. Amazon Kendra dapat menggunakan mekanisme sumber data Anda untuk melacak perubahan konten dan mengindeks konten yang berubah sejak sinkronisasi terakhir.
jenis	Jenis sumber data. Tentukan `MSEXCHANGE` sebagai tipe sumber data Anda.

Konfigurasi	Deskripsi
Sekretarn	Nama Sumber Daya Amazon (ARN) dari AWS Secrets Manager rahasia yang berisi pasangan kunci-nilai yang diperlukan untuk terhubung ke Microsoft Exchange Anda. Ini termasuk ID klien Anda dan rahasia klien Anda yang dihasilkan saat Anda membuat aplikasi OAuth di portal Azure.
versi	Versi template ini yang saat ini didukung.

Skema Microsoft Exchange JSON

```
{
  "$schema": "http://json-schema.org/draft-04/schema#",
  "type": "object",
  "properties": {
    "connectionConfiguration": {
      "type": "object",
      "properties": {
        "repositoryEndpointMetadata": {
          "type": "object",
          "properties": {
            "tenantId": {
              "type": "string",
              "pattern": "^[0-9a-f]{8}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]
{12}$",
              "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"
  ]
}
```

OneDrive Skema templat Microsoft

Anda menyertakan JSON yang berisi skema sumber data sebagai bagian dari objek. TemplateConfiguration Anda memberikan ID penyewa sebagai bagian dari konfigurasi koneksi atau detail titik akhir repositori. Juga tentukan jenis sumber data sebagai`ONEDRIVEV2`, dan rahasia untuk kredensyal otentikasi Anda, dan konfigurasi lain yang diperlukan. Anda kemudian menentukan `TEMPLATE` sebagai `Type` saat Anda menelepon CreateDataSource.

Anda dapat menggunakan template yang disediakan dalam panduan pengembang ini. Lihat Microsoft OneDrive JSON skema.

Tabel berikut menjelaskan parameter skema Microsoft OneDrive JSON.

Konfigurasi	Deskripsi
ConnectionConfiguration	Informasi konfigurasi untuk titik akhir untuk sumber data.

Konfigurasi	Deskripsi
repositoryEndpointMetadata	Informasi titik akhir untuk sumber data.
TenanID	ID penyewa Microsoft 365. Anda dapat menemukan ID penyewa Anda di Properti Portal Direktori Aktif Azure Anda atau di aplikasi OAuth Anda.
RepositoryConfigurations	Informasi konfigurasi untuk konten sumber data. Misalnya, mengonfigurasi jenis konten dan pemetaan bidang tertentu.
file	Daftar objek yang memetakan atribut atau nama bidang OneDrive file Microsoft Anda untuk Amazon Kendra mengindeks nama bidang. Untuk informasi lebih lanjut, lihat Memetakan bidang sumber data.
AdditionalProperties	Opsi konfigurasi tambahan untuk konten Anda di sumber data Anda
• userNameFilter • userFilterPath • inclusionFileTypePola • exclusionFileTypePola • inclusionFileNamePola • exclusionFileNamePola • inclusionFilePathPola • exclusionFilePathPola • inclusionOneNoteSectionNamePatterns • exclusionOneNoteSectionNamePatterns • inclusionOneNotePageNamePatterns • exclusionOneNotepageNamePatterns	Anda dapat memilih untuk mengindeks file, OneNote bagian, OneNote halaman, dan filter tertentu berdasarkan nama pengguna.

Konfigurasi	Deskripsi
isUserNameOnS3	`true`untuk memberikan daftar nama pengguna dalam file yang disimpan dalam file Amazon S3.
jenis	Jenis sumber data. Tentukan `ONEDRIVEV2` sebagai tipe sumber data Anda.
enableIdentityCrawler	`true`untuk menggunakan Amazon Kendra crawler identitas untuk menyinkronkan identitas /informasi utama pada pengguna dan grup dengan akses ke dokumen tertentu. Jika perayap identitas dimatikan, semua dokumen dapat dicari secara publik. Jika Anda ingin menggunakan kontrol akses untuk dokumen dan crawler identitas dimatikan, Anda dapat menggunakan PutPrincipalMappingAPI untuk mengunggah informasi akses pengguna dan grup.
jenis	Jenis sumber data. Tentukan `ONEDRIVEV2` sebagai tipe sumber data Anda.

Konfigurasi	Deskripsi
SyncMode	Tentukan bagaimana Amazon Kendra seharusnya memperbarui indeks Anda saat konten sumber data Anda berubah. Anda dapat memilih antara: • `FORCED_FULL_CRAWL` untuk mengindeks semua konten baru, mengganti konten yang ada setiap kali sumber data Anda disinkron kan dengan indeks Anda. • `FULL_CRAWL` untuk mengindeks hanya konten baru, dimodifikasi, dan dihapus setiap kali sumber data Anda disinkronkan dengan indeks Anda. Amazon Kendra dapat menggunakan mekanisme sumber data Anda untuk melacak perubahan konten dan mengindeks konten yang berubah sejak sinkronisasi terakhir. • `CHANGE_LOG` untuk mengindeks hanya konten baru dan yang dimodifikasi setiap kali sumber data Anda disinkronkan dengan indeks Anda. Amazon Kendra dapat menggunakan mekanisme sumber data Anda untuk melacak perubahan konten dan mengindeks konten yang berubah sejak sinkronisasi terakhir.

Konfigurasi	Deskripsi
Sekretarn	Nama Sumber Daya Amazon (ARN) dari AWS Secrets Manager rahasia yang berisi pasangan kunci-nilai yang diperlukan untuk terhubung ke Microsoft Anda. OneDrive Rahasianya harus berisi struktur JSON dengan kunci berikut: `{ "clientId": " client ID", "clientSecret": " client secret" }`
versi	Versi template ini yang saat ini didukung.

Microsoft OneDrive JSON skema

```
{
 "$schema": "http://json-schema.org/draft-04/schema#",
 "type": "object",
 "properties": {
  "connectionConfiguration": {
   "type": "object",
   "properties": {
    "repositoryEndpointMetadata": {
     "type": "object",
     "properties": {
      "tenantId": {
       "type": "string",
       "pattern": "^[0-9a-f]{8}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{12}$",
       "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"
           ]
          },
          "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"
 ]
}
```

SharePoint Skema templat Microsoft

Anda menyertakan JSON yang berisi skema sumber data sebagai bagian dari objek. TemplateConfiguration Anda memberikan URL/URL SharePoint situs, domain, dan juga ID penyewa jika diperlukan sebagai bagian dari konfigurasi koneksi atau detail titik akhir repositori. Juga tentukan jenis sumber data sebagai`SHAREPOINTV2`, rahasia untuk kredensyal otentikasi Anda, dan konfigurasi

lain yang diperlukan. Anda kemudian menentukan `TEMPLATE` sebagai Tipe saat Anda memanggil CreateDataSource.

Anda dapat menggunakan template yang disediakan dalam panduan pengembang ini. Lihat SharePoint Skema JSON.

Tabel berikut menjelaskan parameter skema Microsoft SharePoint JSON.

Konfigurasi	Deskripsi
ConnectionConfiguration	Informasi konfigurasi untuk titik akhir untuk sumber data
repositoryEndpointMetadata	Informasi titik akhir untuk sumber data
TenanID	ID penyewa SharePoint akun Anda.
domain	Domain SharePoint akun Anda.
SiteURLS	URL host SharePoint akun Anda.
repositoryAdditionalProperties	Properti tambahan untuk terhubung dengan titik akhir repositori/sumber data.
S3BucketName	Nama Amazon S3 bucket yang menyimpan sertifikat X.509 yang ditandatangani sendiri Azure AD Anda.
S3CertificateName	Nama sertifikat X.509 yang ditandatangani sendiri Azure AD disimpan di bucket Anda. Amazon S3
authType	Jenis otentikasi yang Anda gunakan, apakah,`OAuth2`,`OAuth2Certificate` ,`OAuth2App` ,`Basic`, `OAuth2_RefreshToken` `NTLM`, atau`Kerberos`.
versi	SharePoint Versi yang Anda gunakan, apakah `Server` atau`Online`.

Konfigurasi	Deskripsi
onPremVersion	Versi SharePoint Server yang Anda gunakan, apakah `2013` `20162019`, atau`Subscript ionEdition` .
RepositoryConfigurations	Informasi konfigurasi untuk konten sumber data. Misalnya, mengonfigurasi jenis konten dan pemetaan bidang tertentu.
• kejadian • halaman • file • link • lampiran • komentar	Daftar objek yang memetakan atribut atau nama bidang SharePoint konten Anda untuk Amazon Kendra mengindeks nama bidang. Untuk informasi lebih lanjut, lihat Memetakan bidang sumber data.
AdditionalProperties	Opsi konfigurasi tambahan untuk konten Anda di sumber data Anda.
• eventTitleFilterRegEx • pageTitleFilterRegEx • linkTitleFilterRegEx • inclusionFilePath • exclusionFilePath • inclusionFileTypePola • exclusionFileTypePola • inclusionFileNamePola • exclusionFileNamePola • inclusionOneNoteSectionNamePatterns • exclusionOneNoteSectionNamePatterns • inclusionOneNotePageNamePatterns • exclusionOneNotePageNamePatterns	Daftar pola ekspresi reguler untuk menyertakan/mengecualikan konten tertentu dalam sumber data Anda SharePoint . Item konten yang cocok dengan pola inklusi disertakan dalam indeks. Item konten yang tidak cocok dengan pola inklusi dikecualikan dari indeks. Jika file cocok dengan pola inklusi dan pengecualian, pola pengecualian akan diutamakan, dan file tidak disertakan dalam indeks.

Konfigurasi	Deskripsi
• CrawlFiles • CrawlPages • CrawleVents • CrawlKomentar • CrawlLinks • CrawlatTachments	`true`untuk merayapi jenis konten ini.
CrawlaCl	`true`untuk merayapi informasi daftar kontrol akses (ACL) untuk dokumen Anda, jika Anda memiliki ACL dan ingin menggunakannya untuk kontrol akses. ACL menentukan dokumen mana yang dapat diakses dan dicari oleh pengguna dan grup. Informasi ACL digunakan untuk memfilter hasil pencarian berdasark an pengguna atau akses grup mereka ke dokumen. Untuk informasi selengkapnya, lihat Pemfilteran konteks pengguna.
fieldForUserId	Tentukan `email` apakah Anda ingin menggunakan email pengguna untuk ID pengguna, atau `userPrincipalName` jika Anda ingin menggunakan nama pengguna untuk ID pengguna. Jika Anda tidak menentuka n opsi maka `email` digunakan secara default.
ACLkonfigurasi	Tentukan salah satu `ACLWithLDAPEmailFm t ACLWithManualEmailFmt` ,, atau`ACLWithUsernameFmtM` .
EmailDomain	Domain email. Misalnya, "*`amazon.com`* ".
• isCrawlLocalGroupMapping • isCrawlAdGroupMapping	`true`untuk merayapi informasi pemetaan grup.

Konfigurasi	Deskripsi
ProxyHost	Nama host dari proxy web yang Anda gunakan, tanpa protokol http://atau https://.
ProxyPort	Nomor port yang digunakan oleh protokol transport URL host. Harus berupa nilai numerik antara 0 dan 65535.
jenis	Tentukan `SHAREPOINTV2` sebagai tipe sumber data Anda
enableIdentityCrawler	`true`untuk menggunakan Amazon Kendra crawler identitas untuk menyinkronkan identitas /informasi utama pada pengguna dan grup dengan akses ke dokumen tertentu. Jika perayap identitas dimatikan, semua dokumen dapat dicari secara publik. Jika Anda ingin menggunakan kontrol akses untuk dokumen dan crawler identitas dimatikan, Anda dapat menggunakan PutPrincipalMappingAPI untuk mengunggah informasi akses pengguna dan grup.

Konfigurasi	Deskripsi
SyncMode	Tentukan bagaimana Amazon Kendra seharusnya memperbarui indeks Anda saat konten sumber data Anda berubah. Anda dapat memilih antara: • `FORCED_FULL_CRAWL` untuk mengindeks semua konten baru, mengganti konten yang ada setiap kali sumber data Anda disinkron kan dengan indeks Anda. • `FULL_CRAWL` untuk mengindeks hanya konten baru, dimodifikasi, dan dihapus setiap kali sumber data Anda disinkronkan dengan indeks Anda. Amazon Kendra dapat menggunakan mekanisme sumber data Anda untuk melacak perubahan konten dan mengindeks konten yang berubah sejak sinkronisasi terakhir. • `CHANGE_LOG` untuk mengindeks hanya konten baru dan yang dimodifikasi setiap kali sumber data Anda disinkronkan dengan indeks Anda. Amazon Kendra dapat menggunakan mekanisme sumber data Anda untuk melacak perubahan konten dan mengindeks konten yang berubah sejak sinkronisasi terakhir.
Sekretarn	Nama Sumber Daya Amazon (ARN) dari AWS Secrets Manager rahasia yang berisi pasangan kunci-nilai yang diperlukan untuk terhubung ke Anda. SharePoint Untuk informasi tentang pasangan nilai kunci ini, lihat Petunjuk koneksi untuk SharePoint Online dan SharePoint Server.
versi	Versi template ini yang saat ini didukung.

SharePoint Skema JSON

```
{
 "$schema": "http://json-schema.org/draft-04/schema#",
 "type": "object",
 "properties": {
  "connectionConfiguration": {
   "type": "object",
   "properties": {
    "repositoryEndpointMetadata": {
     "type": "object",
     "properties": {
      "tenantId": {
       "type": "string",
       "pattern": "^[0-9a-f]{8}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{12}$",
       "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"
 ]
}
```

Skema templat Microsoft SQL Server

Anda menyertakan JSON yang berisi skema sumber data sebagai bagian dari objek. TemplateConfiguration Tentukan jenis sumber data sebagai`JDBC`, tipe database sebagai`sqlserver`, rahasia untuk kredensyal otentikasi Anda, dan konfigurasi lain yang diperlukan. Anda kemudian menentukan `TEMPLATE` sebagai `Type` saat Anda menelepon CreateDataSource.

Anda dapat menggunakan template yang disediakan dalam panduan pengembang ini. Lihat Skema Microsoft SQL Server JSON.

Tabel berikut menjelaskan parameter skema Micorosft SQL Server JSON.

Konfigurasi	Deskripsi
ConnectionConfiguration	Informasi konfigurasi untuk titik akhir untuk sumber data.

Konfigurasi	Deskripsi
repositoryEndpointMetadata	Informasi konfigurasi yang diperlukan untuk menghubungkan sumber data Anda. • DBType—jenis database Java yang Anda gunakan, apakah,,, `mysqldb2`, `postgresql` atau. `oracle` `sqlserver` • DBhost — nama host database. • DBport — port database. • DBinstance—contoh database.
RepositoryConfigurations	Informasi konfigurasi untuk konten sumber data. Misalnya, mengonfigurasi jenis konten dan pemetaan bidang tertentu. Tentukan jenis sumber data dan ARN rahasia.
dokumen	Daftar objek yang memetakan atribut atau nama bidang konten database Anda untuk Amazon Kendra mengindeks nama bidang. Untuk informasi lebih lanjut, lihat Memetakan bidang sumber data.
AdditionalProperties	Opsi konfigurasi tambahan untuk konten Anda di sumber data Anda. Gunakan untuk menyertakan atau mengecualikan konten tertentu dalam sumber data database Anda.
PrimaryKey	Berikan kunci utama untuk tabel database. Ini mengidentifikasi tabel dalam database Anda.
Judul Kolom	Berikan nama kolom judul dokumen dalam tabel database Anda.
BodyColumn	Berikan nama kolom judul dokumen dalam tabel database Anda.

Konfigurasi	Deskripsi
SqlQuery	Masukkan pernyataan kueri SQL seperti operasi SELECT dan JOIN. Kueri SQL harus kurang dari 32KB. Amazon Kendra akan merayapi semua konten database yang cocok dengan kueri Anda.
TimestampColumn	Masukkan nama kolom yang berisi stempel waktu. Amazon Kendra menggunakan informasi cap waktu untuk mendeteksi perubahan dalam konten Anda dan hanya menyinkronkan konten yang diubah.
TimestampFormat	Masukkan nama kolom yang berisi format cap waktu yang akan digunakan untuk mendeteks i perubahan konten dan menyinkronkan ulang konten Anda.
timezone	Masukkan nama kolom yang berisi zona waktu untuk konten yang akan dirayapi.
changeDetectingColumns	Masukkan nama kolom yang Amazon Kendra akan digunakan untuk mendeteksi perubahan konten. Amazon Kendra akan mengindeks ulang konten ketika ada perubahan di salah satu kolom ini
allowedUsersColumns	Masukkan nama kolom yang berisi ID Pengguna untuk diizinkan mengakses konten.
allowedGroupsColumn	Masukkan nama kolom yang berisi ID Pengguna untuk diizinkan mengakses konten.
Sourceuricolumn	Masukkan nama kolom yang berisi URL Sumber yang akan diindeks.

Konfigurasi	Deskripsi
isSslEnabled	Masukkan pernyataan kueri SQL seperti operasi SELECT dan JOIN. Kueri SQL harus kurang dari 32KB. Amazon Kendra akan merayapi semua konten database yang cocok dengan kueri Anda.
jenis	Jenis sumber data. Tentukan `JDBC` sebagai tipe sumber data Anda.
SyncMode	Tentukan bagaimana Amazon Kendra seharusnya memperbarui indeks Anda saat konten sumber data Anda berubah. Anda dapat memilih antara: • `FORCED_FULL_CRAWL` untuk mengindeks semua konten baru, mengganti konten yang ada setiap kali sumber data Anda disinkron kan dengan indeks Anda. • `FULL_CRAWL` untuk mengindeks hanya konten baru, dimodifikasi, dan dihapus setiap kali sumber data Anda disinkronkan dengan indeks Anda. Amazon Kendra dapat menggunakan mekanisme sumber data Anda untuk melacak perubahan konten dan mengindeks konten yang berubah sejak sinkronisasi terakhir. • `CHANGE_LOG` untuk mengindeks hanya konten baru dan yang dimodifikasi setiap kali sumber data Anda disinkronkan dengan indeks Anda. Amazon Kendra dapat menggunakan mekanisme sumber data Anda untuk melacak perubahan konten dan mengindeks konten yang berubah sejak sinkronisasi terakhir.

Konfigurasi	Deskripsi
Sekretarn	Nama Sumber Daya Amazon (ARN) dari rahasia Secrets Manager yang berisi nama pengguna dan kata sandi yang diperlukan untuk terhubung ke database Anda. Rahasiany a harus berisi struktur JSON dengan kunci berikut: `{ "user name": "database user name", "password": " password" }`
versi	Versi template yang saat ini didukung.

Skema Microsoft SQL Server JSON

```
{
  "$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"
  ]
}
```

Skema templat Microsoft Teams

Anda menyertakan JSON yang berisi skema sumber data sebagai bagian dari objek. TemplateConfiguration Anda memberikan ID penyewa sebagai bagian dari konfigurasi koneksi atau detail titik akhir repositori. Juga tentukan jenis sumber data sebagai`MSTEAMS`, rahasia untuk kredensyal otentikasi Anda, dan konfigurasi lain yang diperlukan. Anda kemudian menentukan `TEMPLATE` sebagai `Type` saat Anda menelepon CreateDataSource.

Anda dapat menggunakan template yang disediakan dalam panduan pengembang ini. Lihat Microsoft Teams JSON skema.

Tabel berikut menjelaskan parameter skema Microsoft Teams JSON.

Konfigurasi	Deskripsi
ConnectionConfiguration	Informasi konfigurasi untuk titik akhir untuk sumber data.
repositoryEndpointMetadata	Informasi titik akhir untuk sumber data.
TenanID	ID penyewa Microsoft 365. Anda dapat menemukan ID penyewa Anda di Properti Portal Direktori Aktif Azure Anda atau di aplikasi OAuth Anda.
RepositoryConfigurations	Informasi konfigurasi untuk konten sumber data. Misalnya, mengonfigurasi jenis konten dan pemetaan bidang tertentu.
• ChatMessage • Lampiran Obrolan	Daftar objek yang memetakan atribut atau nama bidang konten Microsoft Teams Anda

Konfigurasi	Deskripsi
• ChannelPost • ChannelWiki • Lampiran Saluran • MeetingChat • MeetingFile • MeetingNote • Kalender Pertemuan	untuk Amazon Kendra mengindeks nama bidang. Untuk informasi lebih lanjut, lihat Memetakan bidang sumber data.
AdditionalProperties	Opsi konfigurasi tambahan untuk konten Anda di sumber data Anda.
Model Pembayaran	Menentukan jenis model pembayaran yang akan digunakan dengan sumber data Microsoft Teams Anda. Model pembayaran Model A dibatasi untuk model lisensi dan pembayara n yang memerlukan kepatuhan keamanan. Model pembayaran Model B cocok untuk model lisensi dan pembayaran yang tidak memerlukan kepatuhan keamanan.
• inclusionTeamNameFilter • inclusionChannelNameFilter • inclusionFileNamePola • inclusionFileTypePola • inclusionUserEmailFilter • inclusionOneNoteSectionNamePatterns • inclusionOneNotePageNamePatterns	Daftar pola ekspresi reguler untuk menyertak an konten tertentu di sumber data Microsoft Teams Anda. Konten yang cocok dengan pola disertakan dalam indeks. Konten yang tidak cocok dengan pola dikecualikan dari indeks. Jika konten cocok dengan pola inklusi dan pengecualian, pola pengecualian akan diutamakan, dan konten tidak disertakan dalam indeks.

Konfigurasi	Deskripsi
• exclusionTeamNameFilter • exclusionChannelNameFilter • exclusionFileNamePola • exclusionFileTypePola • exclusionUserEmailFilter • exclusionOneNoteSectionNamePatterns • exclusionOneNotePageNamePatterns	Daftar pola ekspresi reguler untuk mengecual ikan konten tertentu di sumber data Microsoft Teams Anda. Konten yang cocok dengan pola dikecualikan dari indeks. Konten yang tidak cocok dengan pola disertakan dalam indeks. Jika konten cocok dengan pola inklusi dan pengecualian, pola pengecualian akan diutamakan, dan konten tidak disertakan dalam indeks.
• isCrawlChatPesan • isCrawlChatLampiran • isCrawlChannelPosting • isCrawlChannelLampiran • isCrawlChannelWiki • isCrawlCalendarRapat • isCrawlMeetingObrolan • isCrawlMeetingBerkas • isCrawlMeetingCatatan	`true`untuk merayapi jenis konten ini di sumber data Microsoft Teams Anda.
startCalendarDateWaktu	Anda dapat mengonfigurasi tanggal-waktu mulai tertentu untuk konten kalender Anda.
endCalendarDateWaktu	Anda dapat mengonfigurasi tanggal-waktu akhir tertentu untuk konten kalender.
jenis	Jenis sumber data. Tentukan `MSTEAMS` sebagai tipe sumber data Anda.

Konfigurasi	Deskripsi
enableIdentityCrawler	`true`untuk menggunakan Amazon Kendra crawler identitas untuk menyinkronkan identitas /informasi utama pada pengguna dan grup dengan akses ke dokumen tertentu. Jika perayap identitas dimatikan, semua dokumen dapat dicari secara publik. Jika Anda ingin menggunakan kontrol akses untuk dokumen dan crawler identitas dimatikan, Anda dapat menggunakan PutPrincipalMappingAPI untuk mengunggah informasi akses pengguna dan grup.

Konfigurasi	Deskripsi
SyncMode	Tentukan bagaimana Amazon Kendra seharusnya memperbarui indeks Anda saat konten sumber data Anda berubah. Anda dapat memilih antara: • `FORCED_FULL_CRAWL` untuk mengindeks semua konten baru, mengganti konten yang ada setiap kali sumber data Anda disinkron kan dengan indeks Anda. • `FULL_CRAWL` untuk mengindeks hanya konten baru, dimodifikasi, dan dihapus setiap kali sumber data Anda disinkronkan dengan indeks Anda. Amazon Kendra dapat menggunakan mekanisme sumber data Anda untuk melacak perubahan konten dan mengindeks konten yang berubah sejak sinkronisasi terakhir. • `CHANGE_LOG` untuk mengindeks hanya konten baru dan yang dimodifikasi setiap kali sumber data Anda disinkronkan dengan indeks Anda. Amazon Kendra dapat menggunakan mekanisme sumber data Anda untuk melacak perubahan konten dan mengindeks konten yang berubah sejak sinkronisasi terakhir.
Sekretarn	Nama Sumber Daya Amazon (ARN) dari AWS Secrets Manager rahasia yang berisi pasangan nilai kunci yang diperlukan untuk terhubung ke Tim Microsoft Anda. Ini termasuk ID klien dan rahasia klien Anda yang dihasilkan saat Anda membuat aplikasi OAuth di portal Azure.
versi	Versi template ini yang saat ini didukung.

Microsoft Teams JSON skema

```
{
  "$schema": "http://json-schema.org/draft-04/schema#",
  "type": "object",
  "properties": {
    "connectionConfiguration": {
      "type": "object",
      "properties": {
        "repositoryEndpointMetadata": {
          "type": "object",
          "properties": {
            "tenantId": {
              "type": "string",
              "pattern": "^[0-9a-f]{8}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]
{12}$",
              "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"
  ]
}
```

Skema templat Microsoft Yammer

Anda menyertakan JSON yang berisi skema sumber data sebagai bagian dari objek. TemplateConfiguration Tentukan jenis sumber data sebagai`YAMMER`, rahasia untuk kredensyal otentikasi Anda, dan konfigurasi lain yang diperlukan. Anda kemudian menentukan `TEMPLATE` sebagai Tipe saat Anda memanggil CreateDataSource.

Anda dapat menggunakan template yang disediakan dalam panduan pengembang ini.

Tabel berikut menjelaskan parameter skema Microsoft Yammer JSON.

Konfigurasi	Deskripsi
ConnectionConfiguration	Informasi konfigurasi untuk sumber data.
repositoryEndpointMetadata	Informasi titik akhir untuk sumber data. Sumber data ini tidak menentukan titik akhir di`repositoryEndpointMetadata` . Sebaliknya, informasi koneksi termasuk dalam AWS Secrets Manager rahasia yang Anda beri`secretArn` .
RepositoryConfigurations	Informasi konfigurasi untuk konten sumber data. Misalnya, mengonfigurasi jenis konten dan pemetaan bidang tertentu.
• komunitas • pengguna • pesan	Daftar objek yang memetakan atribut atau nama bidang konten Microsoft Yammer ke nama bidang indeks Amazon Kendra. Untuk

Konfigurasi	Deskripsi
• lampiran	informasi lebih lanjut, lihat Memetakan bidang sumber data.
AdditionalProperties	Opsi konfigurasi tambahan untuk konten Anda di sumber data Anda
Pola Inklusi	Daftar pola ekspresi reguler untuk menyertakan file tertentu di sumber data Microsoft Yammer Anda. File yang cocok dengan pola disertaka n dalam indeks. File yang tidak cocok dengan pola dikecualikan dari indeks. Jika file cocok dengan pola inklusi dan pengecualian, pola pengecualian akan diutamakan dan file tidak disertakan dalam indeks.
Pola Pengecualian	Daftar pola ekspresi reguler untuk mengecual ikan file tertentu di sumber data Microsoft Yammer Anda. File yang cocok dengan pola dikecualikan dari indeks. File yang tidak cocok dengan pola disertakan dalam indeks. Jika file cocok dengan pola pengecualian dan inklusi, pola pengecualian akan diutamakan dan file tidak disertakan dalam indeks.
sejakDate	Anda dapat memilih untuk mengonfigurasi `sinceDate` parameter sehingga konektor Microsoft Yammer merayapi konten berdasark an spesifik. `sinceDate`
communityNameFilter	Anda dapat memilih untuk mengindeks konten komunitas tertentu.
• isCrawlMessage • isCrawlAttachment • isCrawlPrivatePesan	`true`untuk merayapi pesan, lampiran pesan, dan pesan pribadi.

Konfigurasi	Deskripsi
jenis	Tentukan `YAMMER` sebagai tipe sumber data Anda.
Sekretarn	Nama Sumber Daya Amazon (ARN) dari AWS Secrets Manager rahasia yang berisi pasangan kunci-nilai yang diperlukan untuk terhubung ke Microsoft Yammer Anda. Ini termasuk nama pengguna dan kata sandi Microsoft Yammer Anda, serta ID klien dan rahasia klien yang dihasilkan saat Anda membuat aplikasi OAuth di portal Azure.
useChangeLog	`true`untuk menggunakan log perubahan Microsoft Yammer untuk menentukan dokumen mana yang perlu diperbarui dalam indeks.

Konfigurasi	Deskripsi
SyncMode	Tentukan bagaimana Amazon Kendra seharusnya memperbarui indeks Anda saat konten sumber data Anda berubah. Anda dapat memilih antara: • `FORCED_FULL_CRAWL` untuk mengindeks semua konten baru, mengganti konten yang ada setiap kali sumber data Anda disinkron kan dengan indeks Anda. • `FULL_CRAWL` untuk mengindeks hanya konten baru, dimodifikasi, dan dihapus setiap kali sumber data Anda disinkronkan dengan indeks Anda. Amazon Kendra dapat menggunakan mekanisme sumber data Anda untuk melacak perubahan konten dan mengindeks konten yang berubah sejak sinkronisasi terakhir. • `CHANGE_LOG` untuk mengindeks hanya konten baru dan yang dimodifikasi setiap kali sumber data Anda disinkronkan dengan indeks Anda. Amazon Kendra dapat menggunakan mekanisme sumber data Anda untuk melacak perubahan konten dan mengindeks konten yang berubah sejak sinkronisasi terakhir.

Konfigurasi	Deskripsi
enableIdentityCrawler	`true`untuk menggunakan Amazon Kendra crawler identitas untuk menyinkronkan identitas /informasi utama pada pengguna dan grup dengan akses ke dokumen tertentu. Jika perayap identitas dimatikan, semua dokumen dapat dicari secara publik. Jika Anda ingin menggunakan kontrol akses untuk dokumen dan crawler identitas dimatikan, Anda dapat menggunakan PutPrincipalMappingAPI untuk mengunggah informasi akses pengguna dan grup.

Microsoft Yammer JSON skema

```
{
  "$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"
  ]
}
```

Skema templat MySQL

Anda menyertakan JSON yang berisi skema sumber data sebagai bagian dari objek. TemplateConfiguration Tentukan jenis sumber data sebagai`JDBC`, tipe database sebagai`mysql`, rahasia untuk kredensyal otentikasi Anda, dan konfigurasi lain yang diperlukan. Anda kemudian menentukan `TEMPLATE` sebagai `Type` saat Anda menelepon CreateDataSource.

Anda dapat menggunakan template yang disediakan dalam panduan pengembang ini. Lihat MySQL JSON skema.

Tabel berikut menjelaskan parameter skema MySQL JSON.

Konfigurasi	Deskripsi
ConnectionConfiguration	Informasi konfigurasi untuk titik akhir untuk sumber data.
repositoryEndpointMetadata	Informasi konfigurasi yang diperlukan untuk menghubungkan sumber data Anda. • DBType—jenis database Java yang Anda gunakan, apakah,,, `mysql` `db2`, `postgresql` atau. `oracle` `sqlserver` • DBhost — nama host database. • DBport — port database. • DBinstance—contoh database.
RepositoryConfigurations	Informasi konfigurasi untuk konten sumber data. Misalnya, mengonfigurasi jenis konten dan pemetaan bidang tertentu. Tentukan jenis sumber data dan ARN rahasia.
dokumen	Daftar objek yang memetakan atribut atau nama bidang konten database Anda untuk Amazon Kendra mengindeks nama bidang. Untuk informasi lebih lanjut, lihat Memetakan bidang sumber data.
AdditionalProperties	Opsi konfigurasi tambahan untuk konten Anda di sumber data Anda. Gunakan untuk menyertakan atau mengecualikan konten tertentu dalam sumber data database Anda.
PrimaryKey	Berikan kunci utama untuk tabel database. Ini mengidentifikasi tabel dalam database Anda.
Judul Kolom	Berikan nama kolom judul dokumen dalam tabel database Anda.

Konfigurasi	Deskripsi
BodyColumn	Berikan nama kolom judul dokumen dalam tabel database Anda.
SqlQuery	Masukkan pernyataan kueri SQL seperti operasi SELECT dan JOIN. Kueri SQL harus kurang dari 32KB. Amazon Kendra akan merayapi semua konten database yang cocok dengan kueri Anda.
TimestampColumn	Masukkan nama kolom yang berisi stempel waktu. Amazon Kendra menggunakan informasi cap waktu untuk mendeteksi perubahan dalam konten Anda dan hanya menyinkronkan konten yang diubah.
TimestampFormat	Masukkan nama kolom yang berisi format cap waktu yang akan digunakan untuk mendeteks i perubahan konten dan menyinkronkan ulang konten Anda.
timezone	Masukkan nama kolom yang berisi zona waktu untuk konten yang akan dirayapi.
changeDetectingColumns	Masukkan nama kolom yang Amazon Kendra akan digunakan untuk mendeteksi perubahan konten. Amazon Kendra akan mengindeks ulang konten ketika ada perubahan di salah satu kolom ini
allowedUsersColumns	Masukkan nama kolom yang berisi ID Pengguna untuk diizinkan mengakses konten.
allowedGroupsColumn	Masukkan nama kolom yang berisi ID Pengguna untuk diizinkan mengakses konten.
Sourceuricolumn	Masukkan nama kolom yang berisi URL Sumber yang akan diindeks.

Konfigurasi	Deskripsi
isSslEnabled	Masukkan pernyataan kueri SQL seperti operasi SELECT dan JOIN. Kueri SQL harus kurang dari 32KB. Amazon Kendra akan merayapi semua konten database yang cocok dengan kueri Anda.
jenis	Jenis sumber data. Tentukan `JDBC` sebagai tipe sumber data Anda.
SyncMode	Tentukan bagaimana Amazon Kendra seharusnya memperbarui indeks Anda saat konten sumber data Anda berubah. Anda dapat memilih antara: • `FORCED_FULL_CRAWL` untuk mengindeks semua konten baru, mengganti konten yang ada setiap kali sumber data Anda disinkron kan dengan indeks Anda. • `FULL_CRAWL` untuk mengindeks hanya konten baru, dimodifikasi, dan dihapus setiap kali sumber data Anda disinkronkan dengan indeks Anda. Amazon Kendra dapat menggunakan mekanisme sumber data Anda untuk melacak perubahan konten dan mengindeks konten yang berubah sejak sinkronisasi terakhir. • `CHANGE_LOG` untuk mengindeks hanya konten baru dan yang dimodifikasi setiap kali sumber data Anda disinkronkan dengan indeks Anda. Amazon Kendra dapat menggunakan mekanisme sumber data Anda untuk melacak perubahan konten dan mengindeks konten yang berubah sejak sinkronisasi terakhir.

Konfigurasi	Deskripsi
Sekretarn	Nama Sumber Daya Amazon (ARN) dari rahasia Secrets Manager yang berisi nama pengguna dan kata sandi yang diperlukan untuk terhubung ke database Anda. Rahasiany a harus berisi struktur JSON dengan kunci berikut: `{ "user name": "database user name", "password": " password" }`
versi	Versi template yang saat ini didukung.

MySQL JSON skema

```
{
  "$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"
  ]
}
```

Skema templat Oracle Database

Anda menyertakan JSON yang berisi skema sumber data sebagai bagian dari objek. TemplateConfiguration Tentukan jenis sumber data sebagai`JDBC`, tipe database sebagai`oracle`, rahasia untuk kredensyal otentikasi Anda, dan konfigurasi lain yang diperlukan. Anda kemudian menentukan `TEMPLATE` sebagai `Type` saat Anda menelepon CreateDataSource.

Anda dapat menggunakan template yang disediakan dalam panduan pengembang ini. Lihat Skema JSON Database Oracle.

Tabel berikut menjelaskan parameter skema Oracle Database JSON.

Konfigurasi	Deskripsi
ConnectionConfiguration	Informasi konfigurasi untuk titik akhir untuk sumber data.
repositoryEndpointMetadata	Informasi konfigurasi yang diperlukan untuk menghubungkan sumber data Anda. • DBType—jenis database Java yang Anda gunakan, apakah,,, `mysql` `db2`, `postgresql` atau. `oracle` `sqlserver` • DBhost — nama host database. • DBport — port database. • DBinstance—contoh database.
RepositoryConfigurations	Informasi konfigurasi untuk konten sumber data. Misalnya, mengonfigurasi jenis konten

Konfigurasi	Deskripsi
	dan pemetaan bidang tertentu. Tentukan jenis sumber data dan ARN rahasia.
dokumen	Daftar objek yang memetakan atribut atau nama bidang konten database Anda untuk Amazon Kendra mengindeks nama bidang. Untuk informasi lebih lanjut, lihat Memetakan bidang sumber data.
AdditionalProperties	Opsi konfigurasi tambahan untuk konten Anda di sumber data Anda. Gunakan untuk menyertakan atau mengecualikan konten tertentu dalam sumber data database Anda.
PrimaryKey	Berikan kunci utama untuk tabel database. Ini mengidentifikasi tabel dalam database Anda.
Judul Kolom	Berikan nama kolom judul dokumen dalam tabel database Anda.
BodyColumn	Berikan nama kolom judul dokumen dalam tabel database Anda.
SqlQuery	Masukkan pernyataan kueri SQL seperti operasi SELECT dan JOIN. Kueri SQL harus kurang dari 32KB. Amazon Kendra akan merayapi semua konten database yang cocok dengan kueri Anda.
TimestampColumn	Masukkan nama kolom yang berisi stempel waktu. Amazon Kendra menggunakan informasi cap waktu untuk mendeteksi perubahan dalam konten Anda dan hanya menyinkronkan konten yang diubah.

Konfigurasi	Deskripsi
TimestampFormat	Masukkan nama kolom yang berisi format cap waktu yang akan digunakan untuk mendeteksi perubahan konten dan menyinkronkan ulang konten Anda.
timezone	Masukkan nama kolom yang berisi zona waktu untuk konten yang akan dirayapi.
changeDetectingColumns	Masukkan nama kolom yang Amazon Kendra akan digunakan untuk mendeteksi perubahan konten. Amazon Kendra akan mengindeks ulang konten ketika ada perubahan di salah satu kolom ini
allowedUsersColumns	Masukkan nama kolom yang berisi ID Pengguna untuk diizinkan mengakses konten.
allowedGroupsColumn	Masukkan nama kolom yang berisi ID Pengguna untuk diizinkan mengakses konten.
Sourceuricolumn	Masukkan nama kolom yang berisi URL Sumber yang akan diindeks.
isSslEnabled	Masukkan pernyataan kueri SQL seperti operasi SELECT dan JOIN. Kueri SQL harus kurang dari 32KB. Amazon Kendra akan merayapi semua konten database yang cocok dengan kueri Anda.
jenis	Jenis sumber data. Tentukan `JDBC` sebagai tipe sumber data Anda.

Konfigurasi	Deskripsi
SyncMode	Tentukan cara Amazon Kendra memperbarui indeks Anda saat konten sumber data Anda berubah. Anda dapat memilih antara: • `FORCED_FULL_CRAWL` untuk mengindeks semua konten baru, mengganti konten yang ada setiap kali sumber data Anda disinkron kan dengan indeks Anda. • `FULL_CRAWL` untuk mengindeks hanya konten baru, dimodifikasi, dan dihapus setiap kali sumber data Anda disinkronkan dengan indeks Anda. Amazon Kendra dapat menggunakan mekanisme sumber data Anda untuk melacak perubahan konten dan mengindeks konten yang berubah sejak sinkronisasi terakhir. • `CHANGE_LOG` untuk mengindeks hanya konten baru dan yang dimodifikasi setiap kali sumber data Anda disinkronkan dengan indeks Anda. Amazon Kendra dapat menggunakan mekanisme sumber data Anda untuk melacak perubahan konten dan mengindeks konten yang berubah sejak sinkronisasi terakhir.

Konfigurasi	Deskripsi
Sekretarn	Nama Sumber Daya Amazon (ARN) dari rahasia Secrets Manager yang berisi nama pengguna dan kata sandi yang diperlukan untuk terhubung ke database Anda. Rahasiany a harus berisi struktur JSON dengan kunci berikut: `{ "user name": "database user name", "password": " password" }`
versi	Versi template yang saat ini didukung.

Skema JSON Database Oracle

```
{
  "$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"
  ]
}
```

Skema Templat PostgreSQL

Anda menyertakan JSON yang berisi skema sumber data sebagai bagian dari objek. TemplateConfiguration Tentukan jenis sumber data sebagai`JDBC`, tipe database sebagai`postgresql`, rahasia untuk kredensyal otentikasi Anda, dan konfigurasi lain yang diperlukan. Anda kemudian menentukan `TEMPLATE` sebagai `Type` saat Anda menelepon CreateDataSource.

Anda dapat menggunakan template yang disediakan dalam panduan pengembang ini. Lihat PostgreSQL JSON skema.

Tabel berikut menjelaskan parameter skema PostgreSQL JSON.

Konfigurasi	Deskripsi
ConnectionConfiguration	Informasi konfigurasi untuk titik akhir untuk sumber data.
repositoryEndpointMetadata	Informasi konfigurasi yang diperlukan untuk menghubungkan sumber data Anda. • DBType—jenis database Java yang Anda gunakan, apakah,,, `mysql`, `db2`, `postgresql` atau. `oracle` `sqlserver` • DBhost — nama host database. • DBport — port database. • DBinstance—contoh database.
RepositoryConfigurations	Informasi konfigurasi untuk konten sumber data. Misalnya, mengonfigurasi jenis konten

Konfigurasi	Deskripsi
	dan pemetaan bidang tertentu. Tentukan jenis sumber data dan ARN rahasia.
dokumen	Daftar objek yang memetakan atribut atau nama bidang konten database Anda untuk Amazon Kendra mengindeks nama bidang. Untuk informasi lebih lanjut, lihat Memetakan bidang sumber data.
AdditionalProperties	Opsi konfigurasi tambahan untuk konten Anda di sumber data Anda. Gunakan untuk menyertakan atau mengecualikan konten tertentu dalam sumber data database Anda.
PrimaryKey	Berikan kunci utama untuk tabel database. Ini mengidentifikasi tabel dalam database Anda.
Judul Kolom	Berikan nama kolom judul dokumen dalam tabel database Anda.
BodyColumn	Berikan nama kolom judul dokumen dalam tabel database Anda.
SqlQuery	Masukkan pernyataan kueri SQL seperti operasi SELECT dan JOIN. Kueri SQL harus kurang dari 32KB. Amazon Kendra akan merayapi semua konten database yang cocok dengan kueri Anda.
TimestampColumn	Masukkan nama kolom yang berisi stempel waktu. Amazon Kendra menggunakan informasi cap waktu untuk mendeteksi perubahan dalam konten Anda dan hanya menyinkronkan konten yang diubah.

Konfigurasi	Deskripsi
TimestampFormat	Masukkan nama kolom yang berisi format cap waktu yang akan digunakan untuk mendeteksi perubahan konten dan menyinkronkan ulang konten Anda.
timezone	Masukkan nama kolom yang berisi zona waktu untuk konten yang akan dirayapi.
changeDetectingColumns	Masukkan nama kolom yang Amazon Kendra akan digunakan untuk mendeteksi perubahan konten. Amazon Kendra akan mengindeks ulang konten ketika ada perubahan di salah satu kolom ini
allowedUsersColumns	Masukkan nama kolom yang berisi ID Pengguna untuk diizinkan mengakses konten.
allowedGroupsColumn	Masukkan nama kolom yang berisi ID Pengguna untuk diizinkan mengakses konten.
Sourceuricolumn	Masukkan nama kolom yang berisi URL Sumber yang akan diindeks.
isSslEnabled	Masukkan pernyataan kueri SQL seperti operasi SELECT dan JOIN. Kueri SQL harus kurang dari 32KB. Amazon Kendra akan merayapi semua konten database yang cocok dengan kueri Anda.
jenis	Jenis sumber data. Tentukan `JDBC` sebagai tipe sumber data Anda.

Konfigurasi	Deskripsi
SyncMode	Tentukan cara Amazon Kendra memperbarui indeks Anda saat konten sumber data Anda berubah. Anda dapat memilih antara: • `FORCED_FULL_CRAWL` untuk mengindeks semua konten baru, mengganti konten yang ada setiap kali sumber data Anda disinkronkan dengan indeks Anda. • `FULL_CRAWL` untuk mengindeks hanya konten baru, dimodifikasi, dan dihapus setiap kali sumber data Anda disinkronkan dengan indeks Anda. Amazon Kendra dapat menggunakan mekanisme sumber data Anda untuk melacak perubahan konten dan mengindeks konten yang berubah sejak sinkronisasi terakhir. • `CHANGE_LOG` untuk mengindeks hanya konten baru dan yang dimodifikasi setiap kali sumber data Anda disinkronkan dengan indeks Anda. Amazon Kendra dapat menggunakan mekanisme sumber data Anda untuk melacak perubahan konten dan mengindeks konten yang berubah sejak sinkronisasi terakhir.

Konfigurasi	Deskripsi
Sekretarn	Nama Sumber Daya Amazon (ARN) dari rahasia Secrets Manager yang berisi nama pengguna dan kata sandi yang diperlukan untuk terhubung ke database Anda. Rahasiany a harus berisi struktur JSON dengan kunci berikut: `{ "user name": "database user name", "password": " password" }`
versi	Versi template yang saat ini didukung.

PostgreSQL JSON skema

```
{
  "$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"
  ]
}
```

Skema templat Salesforce

Anda menyertakan JSON yang berisi skema sumber data sebagai bagian dari objek. TemplateConfiguration Anda memberikan URL host Salesforce sebagai bagian dari konfigurasi koneksi atau detail titik akhir repositori. Juga tentukan jenis sumber data sebagai`SALESFORCEV2`, rahasia untuk kredensyal otentikasi Anda, dan konfigurasi lain yang diperlukan. Anda kemudian menentukan `TEMPLATE` sebagai `Type` saat Anda menelepon CreateDataSource.

Anda dapat menggunakan template yang disediakan dalam panduan pengembang ini. Lihat Skema JSON Salesforce.

Tabel berikut menjelaskan parameter skema JSON Salesforce.

Konfigurasi	Deskripsi
ConnectionConfiguration	Informasi konfigurasi untuk titik akhir untuk sumber data.
repositoryEndpointMetadata	Informasi titik akhir untuk sumber data.
HostURL	URL instance Salesforce yang akan diindeks.
RepositoryConfigurations	Informasi konfigurasi untuk konten sumber data. Misalnya, mengonfigurasi jenis konten dan pemetaan bidang tertentu.
• akun • kontak • kampanye • kasus	Daftar objek yang memetakan atribut atau nama bidang entitas Salesforce Anda untuk Amazon Kendra mengindeks nama bidang. Untuk informasi lebih lanjut, lihat Memetakan bidang sumber data.

Konfigurasi	Deskripsi
• produk • timbal • kontrak • pasangan • profile • gagasan • buku harga • tugas • solusi • lampiran • pengguna • dokumen • Artikel Pengetahuan • grup • peluang • obrolan • KustomentITAS	

Konfigurasi	Deskripsi
Sekretarn	Nama Sumber Daya Amazon (ARN) dari AWS Secrets Manager rahasia yang berisi pasangan kunci-nilai yang diperlukan untuk terhubung ke Salesforce Anda. Rahasianya harus berisi struktur JSON dengan kunci berikut: `{ "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" }`
AdditionalProperties	Opsi konfigurasi tambahan untuk konten Anda di sumber data Anda

Konfigurasi	Deskripsi
• Filter Akun • Filter Kontak • CaseFilter • CampaignFilter • KontrakFilter • GroupFilter • LeadFilter • Filter Produk • Peluang Filter • PartnerFilter • PricebookFilter • IdeaFilter • Filter Profil • Filter Tugas • Filter Solusi • UserFilter • Filter obrolan • DocumentFilter • knowledgeArticleFilter • Kustomentitas	Kumpulan string yang menentukan entitas mana yang akan difilter.

Konfigurasi	Deskripsi
Pola Inklusi • inclusionDocumentFileTypePatterns • inclusionDocumentFileNamePatterns • inclusionAccountFileTypePatterns • inclusionCampaignFileTypePatterns • inclusionDocumentFileNamePatterns • inclusionCampaignFileNamePatterns • inclusionCaseFileTypePatterns • inclusionCaseFileNamePatterns • inclusionContactFileTypePatterns • inclusionContractFileNamePatterns • inclusionLeadFileTypePatterns • inclusionLeadFileNamePatterns • inclusionOpportunityFileTypePatterns • inclusionOpportunityFileNamePatterns • inclusionSolutionFileTypePatterns • inclusionSolutionFileNamePatterns • inclusionTaskFileTypePatterns • inclusionTaskFileNamePatterns • inclusionGroupFileTypePatterns • inclusionGroupFileNamePatterns • inclusionChatterFileTypePatterns • inclusionChatterFileNamePatterns • inclusionCustomEntityFileTypePatterns • inclusionCustomEntityFileNamePatterns	Daftar pola ekspresi reguler untuk menyertakan file tertentu dalam sumber data Salesforce Anda. File yang cocok dengan pola disertakan dalam indeks. File yang tidak cocok dengan pola dikecualikan dari indeks. Jika file cocok dengan pola inklusi dan pengecualian, pola pengecualian akan diutamakan dan file tidak disertakan dalam indeks.

Konfigurasi	Deskripsi
Pola Pengecualian • exclusionDocumentFileTypePatterns • exclusionDocumentFileNamePatterns • exclusionAccountFileTypePatterns • exclusionCampaignFileTypePatterns • exclusionCampaignFileNamePatterns • exclusionCaseFileTypePatterns • exclusionCaseFileNamePatterns • exclusionContactFileTypePatterns • exclusionContractFileNamePatterns • exclusionLeadFileTypePatterns • exclusionLeadFileNamePatterns • exclusionOpportunityFileTypePatterns • exclusionOpportunityFileNamePatterns • exclusionSolutionFileTypePatterns • exclusionSolutionFileNamePatterns • exclusionTaskFileTypePatterns • exclusionTaskFileNamePatterns • exclusionGroupFileTypePatterns • exclusionGroupFileNamePatterns • exclusionChatterFileTypePatterns • exclusionChatterFileNamePatterns • exclusionCustomEntityFileTypePatterns • exclusionCustomEntityFileNamePatterns	Daftar pola ekspresi reguler untuk mengecual ikan file tertentu di sumber data Salesforce Anda. File yang cocok dengan pola dikecuali kan dari indeks. File yang tidak cocok dengan pola disertakan dalam indeks. Jika file cocok dengan pola pengecualian dan inklusi, pola pengecualian akan diutamakan dan file tidak disertakan dalam indeks.

Konfigurasi	Deskripsi
• isCrawlAccount • isCrawlContact • isCrawlCase • isCrawlCampaign • isCrawlProduct • isCrawlLead • isCrawlContract • isCrawlPartner • isCrawlProfile • isCrawlIdea • isCrawlPricebook • isCrawlDocument • crawlSharedDocument • isCrawlGroup • isCrawlOpportunity • isCrawlChatter • isCrawlUser • isCrawlSolution • isCrawlTask • isCrawlAccountLampiran • isCrawlContactLampiran • isCrawlCaseLampiran • isCrawlCampaignLampiran • isCrawlLeadLampiran • isCrawlContractLampiran • isCrawlGroupLampiran • isCrawlOpportunityLampiran • isCrawlChatterLampiran • isCrawlSolutionLampiran	`true`untuk merayapi jenis file ini di akun Salesforce Anda.

Konfigurasi	Deskripsi

• isCrawlTaskLampiran
• isCrawlCustomEntityAttachments
• isCrawlKnowledgeArtikel
  • isCrawlDraft
  • isCrawlPublish
  • isCrawlArchived	

jenis	Jenis sumber data. Tentukan `SALESFORCEV2` sebagai tipe sumber data Anda.
enableIdentityCrawler	`true`untuk menggunakan Amazon Kendra crawler identitas untuk menyinkronkan identitas /informasi utama pada pengguna dan grup dengan akses ke dokumen tertentu. Jika perayap identitas dimatikan, semua dokumen dapat dicari secara publik. Jika Anda ingin menggunakan kontrol akses untuk dokumen dan crawler identitas dimatikan, Anda dapat menggunakan PutPrincipalMappingAPI untuk mengunggah informasi akses pengguna dan grup.

Konfigurasi	Deskripsi
SyncMode	Tentukan cara Amazon Kendra memperbarui indeks Anda saat konten sumber data Anda berubah. Anda dapat memilih antara: • `FORCED_FULL_CRAWL` untuk mengindeks semua konten baru, mengganti konten yang ada setiap kali sumber data Anda disinkron kan dengan indeks Anda. • `FULL_CRAWL` untuk mengindeks hanya konten baru, dimodifikasi, dan dihapus setiap kali sumber data Anda disinkronkan dengan indeks Anda. Amazon Kendra dapat menggunakan mekanisme sumber data Anda untuk melacak perubahan konten dan mengindeks konten yang berubah sejak sinkronisasi terakhir. • `CHANGE_LOG` untuk mengindeks hanya konten baru dan yang dimodifikasi setiap kali sumber data Anda disinkronkan dengan indeks Anda. Amazon Kendra dapat menggunakan mekanisme sumber data Anda untuk melacak perubahan konten dan mengindeks konten yang berubah sejak sinkronisasi terakhir.
versi	Versi template ini yang saat ini didukung.

Skema JSON Salesforce

```
{
  "$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"
          }
        },
        "inclusionCustomEntityFileTypePatterns":{
          "type": "array",
          "items":
          {
            "type": "string"
          }
        },
        "exclusionCustomEntityFileTypePatterns":{
          "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 skema templat

Anda menyertakan JSON yang berisi skema sumber data sebagai bagian dari objek. TemplateConfiguration Anda memberikan URL ServiceNow host, jenis otentikasi, dan versi instans sebagai bagian dari konfigurasi koneksi atau detail titik akhir repositori. Juga tentukan jenis sumber data sebagai`SERVICENOWV2`, rahasia untuk kredensyal otentikasi Anda, dan konfigurasi lain yang diperlukan. Anda kemudian menentukan `TEMPLATE` sebagai `Type` saat Anda menelepon CreateDataSource.

Anda dapat menggunakan template yang disediakan dalam panduan pengembang ini. Lihat ServiceNow Skema JSON.

Tabel berikut menjelaskan parameter skema ServiceNow JSON.

Konfigurasi	Deskripsi
ConnectionConfiguration	Informasi konfigurasi untuk titik akhir untuk sumber data.
repositoryEndpointMetadata	Informasi titik akhir untuk sumber data.
HostURL	URL ServiceNow host. Misalnya, *your-domain.service-now.com* .
authType	Jenis otentikasi yang Anda gunakan, apakah `basicAuth` atau`OAuth2`.
servicenowInstanceVersion	ServiceNow Versi yang Anda gunakan. Anda dapat memilih antara`Tokyo`,`Sandiego`,`Rome`, dan`Others`.
RepositoryConfigurations	Informasi konfigurasi untuk konten sumber data. Misalnya, mengonfigurasi jenis konten dan pemetaan bidang tertentu.

Konfigurasi	Deskripsi
• Pengetahuan Artikel • lampiran • ServiceCatalog • insiden	Daftar objek yang memetakan atribut atau nama bidang artikel ServiceNow pengetahuan Anda, lampiran, katalog layanan, dan insiden untuk Amazon Kendra me ngindeks nama bidang. Untuk informasi lebih lanjut, lihat Memetakan bidang sumber data. Nama bidang sumber ServiceNow data harus ada di metadata ServiceNow kustom Anda.
properti tambahan	Opsi konfigurasi tambahan untuk konten Anda di sumber data Anda.
maxFileSizeInMegaBytes	Tentukan batas ukuran file di MB yang akan dirayapi Amazon Kendra. Amazon Kendra hanya akan merayapi file dalam batas ukuran yang Anda tentukan. Ukuran file default adalah 50MB. Ukuran file maksimum harus lebih besar dari 0MB dan kurang dari atau sama dengan 50MB.
• knowledgeArticleFilter • incidentQueryFilter • serviceCatalogQueryFilter • knowledgeArticleTitleRegExp • serviceCatalogTitleRegExp • incidentTitleRegExp • inclusionFileTypePola • exclusionFileTypePola • inclusionFileNamePola • exclusionFileNamePola • incidentStateType	Daftar pola ekspresi reguler untuk menyertakan dan/atau mengecualikan file tertentu dalam sumber ServiceNo w data Anda. File yang cocok dengan pola disertaka n dalam indeks. File yang tidak cocok dengan pola dikecualikan dari indeks. Jika file cocok dengan pola inklusi dan pengecualian, pola pengecualian akan diutamakan dan file tidak disertakan dalam indeks.

Konfigurasi	Deskripsi
• isCrawlKnowledgeArtikel • isCrawlKnowledgeArticleAttachment • includePublicArticlesHanya • isCrawlServiceKatalog • isCrawlServiceCatalogAttachment • isCrawlActiveServiceCatalog • isCrawlInactiveServiceCatalog • isCrawlIncident • isCrawlIncidentLampiran • isCrawlActiveInsiden • isCrawlInactiveInsiden • TerapkanACL ForKnowledgeArticle • TerapkanACL ForServiceCatalog • TerapkanACL ForIncident	`true`untuk merayapi artikel ServiceNow pengetahuan, katalog layanan, insiden, dan lampiran.
jenis	Jenis sumber data. Tentukan `SERVICENOWV2` sebagai tipe sumber data Anda.
enableIdentityCrawler	`true`untuk menggunakan Amazon Kendra crawler identitas untuk menyinkronkan identitas/informasi utama pada pengguna dan grup dengan akses ke dokumen tertentu. Jika perayap identitas dimatikan, semua dokumen dapat dicari secara publik. Jika Anda ingin menggunakan kontrol akses untuk dokumen dan crawler identitas dimatikan, Anda dapat menggunakan PutPrincipalMappingAPI untuk mengunggah informasi akses pengguna dan grup.

Konfigurasi	Deskripsi
SyncMode	Tentukan cara Amazon Kendra memperbarui indeks Anda saat konten sumber data Anda berubah. Anda dapat memilih antara: • `FORCED_FULL_CRAWL` untuk mengindeks semua konten baru, mengganti konten yang ada setiap kali sumber data Anda disinkronkan dengan indeks Anda. • `FULL_CRAWL` untuk mengindeks hanya konten baru, dimodifikasi, dan dihapus setiap kali sumber data Anda disinkronkan dengan indeks Anda. Amazon Kendra dapat menggunakan mekanisme sumber data Anda untuk melacak perubahan konten dan mengindeks konten yang berubah sejak sinkronisasi terakhir.

Sekretarn	Nama Sumber Daya Amazon (ARN) dari AWS Secrets Manager rahasia yang berisi pasangan kunci-nilai yang diperlukan untuk terhubung ke Anda. ServiceNo w Rahasianya harus berisi struktur JSON dengan kunci berikut:
	`{ "username": " user name", "password": " password" }`
	Jika Anda menggunakan otentikasi OAuth2, rahasia Anda harus berisi struktur JSON dengan kunci berikut:
	`{ "username": " user name", "password": " password", "clientId": " client id", "clientSecret": " client secret" }`

Konfigurasi	Deskripsi
versi	Versi template yang saat ini didukung.

ServiceNow Skema JSON

```
{
  "$schema": "http://json-schema.org/draft-04/schema#",
  "type": "object",
  "properties": {
    "connectionConfiguration": {
      "type": "object",
      "properties": {
        "repositoryEndpointMetadata": {
          "type": "object",
          "properties": {
            "hostUrl": {
              "type": "string",
              "pattern": "^(?!(^(https?|ftp|file):\/\/))[a-z0-9-]+(.service-
now.com|.servicenowservices.com)$",
              "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"
  ]
}
```

Skema template kendur

Anda menyertakan JSON yang berisi skema sumber data sebagai bagian dari objek. TemplateConfiguration Anda memberikan URL host sebagai bagian dari konfigurasi koneksi atau detail titik akhir repositori. Juga tentukan jenis sumber data sebagai`SLACK`, rahasia untuk kredensyal otentikasi Anda, dan konfigurasi lain yang diperlukan. Anda kemudian menentukan `TEMPLATE` sebagai `Type` saat Anda menelepon CreateDataSource.

Anda dapat menggunakan template yang disediakan dalam panduan pengembang ini. Lihat Slack JSON skema.

Tabel berikut menjelaskan parameter skema Slack JSON.

Konfigurasi	Deskripsi
ConnectionConfiguration	Informasi konfigurasi untuk titik akhir untuk sumber data.
repositoryEndpointMetadata	Informasi titik akhir untuk sumber data.
TeamID	ID tim Slack yang Anda salin dari URL halaman utama Slack Anda.
RepositoryConfigurations	Informasi konfigurasi untuk konten sumber data. Misalnya, mengonfigurasi jenis konten dan pemetaan bidang tertentu.

Konfigurasi	Deskripsi
Semua	Daftar objek yang memetakan atribut atau nama bidang Slack konten Anda untuk Amazon Kendra mengindeks nama bidang.
AdditionalProperties	Opsi konfigurasi tambahan untuk konten Anda di sumber data Anda.
Pola Inklusi	Daftar pola ekspresi reguler untuk menyertakan konten tertentu dalam sumber Slack data Anda. Konten yang cocok dengan pola disertakan dalam indeks. Konten yang tidak cocok dengan pola dikecualikan dari indeks. Jika ada konten yang cocok dengan pola inklusi dan pengecualian, pola pengecualian akan diutamakan, dan konten tidak disertakan dalam indeks.
Pola Pengecualian	Daftar pola ekspresi reguler untuk mengecualikan konten tertentu di sumber Slack data Anda. Konten yang cocok dengan pola dikecualikan dari indeks. Konten yang tidak cocok dengan pola disertakan dalam indeks. Jika ada konten yang cocok dengan pola inklusi dan pengecualian, pola pengecualian akan diutamakan, dan konten tidak disertakan dalam indeks.
crawlBotMessages	`true`untuk merayapi pesan bot.
ExcludeDiarsipkan	`true`untuk mengecualikan perayapan pesan yang diarsipkan.
ConversationType	Jenis percakapan yang ingin Anda indeks apakah`PUBLIC_CHANNEL` ,`PRIVATE_CHANNEL` , `GROUP_MESSAGE` dan`DIRECT_MESSAGE` .

Konfigurasi	Deskripsi
Filter Saluran	Jenis saluran yang ingin Anda indeks apakah `private_channel` atau `public_channel` .
sejakDate	Anda dapat memilih untuk mengonfigurasi `sinceDate` parameter sehingga Slack konektor merayapi konten berdasarkan spesifik `sinceDate` .
Lookback	Anda dapat memilih untuk mengonfigurasi `lookBack` parameter sehingga Slack konektor merayapi konten yang diperbarui atau dihapus hingga jumlah jam tertentu sebelum sinkronis asi konektor terakhir Anda.

Konfigurasi	Deskripsi
SyncMode	Tentukan cara Amazon Kendra memperbarui indeks Anda saat konten sumber data Anda berubah. Anda dapat memilih antara: • `FORCED_FULL_CRAWL` untuk mengindeks semua konten baru, mengganti konten yang ada setiap kali sumber data Anda disinkron kan dengan indeks Anda. • `FULL_CRAWL` untuk mengindeks hanya konten baru, dimodifikasi, dan dihapus setiap kali sumber data Anda disinkronkan dengan indeks Anda. Amazon Kendra dapat menggunakan mekanisme sumber data Anda untuk melacak perubahan konten dan mengindeks konten yang berubah sejak sinkronisasi terakhir. • `CHANGE_LOG` untuk mengindeks hanya konten baru dan yang dimodifikasi setiap kali sumber data Anda disinkronkan dengan indeks Anda. Amazon Kendra dapat menggunakan mekanisme sumber data Anda untuk melacak perubahan konten dan mengindeks konten yang berubah sejak sinkronisasi terakhir.
jenis	Jenis sumber data. Tentukan `SLACK` sebagai tipe sumber data Anda.

Konfigurasi	Deskripsi
enableIdentityCrawler	`true`untuk menggunakan Amazon Kendra crawler identitas untuk menyinkronkan identitas /informasi utama pada pengguna dan grup dengan akses ke dokumen tertentu. Jika perayap identitas dimatikan, semua dokumen dapat dicari secara publik. Jika Anda ingin menggunakan kontrol akses untuk dokumen dan crawler identitas dimatikan, Anda dapat menggunakan PutPrincipalMappingAPI untuk mengunggah informasi akses pengguna dan grup.
Sekretarn	Nama Sumber Daya Amazon (ARN) dari AWS Secrets Manager rahasia yang berisi pasangan kunci-nilai yang diperlukan untuk terhubung ke Anda. Slack Rahasianya harus berisi struktur JSON dengan kunci berikut: `{ "slackToken": " token" }`
versi	Versi template ini yang saat ini didukung.

Slack JSON skema

```
{
  "$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": [
    ]
  },
  "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"
  ]
}
```

Skema template Zendesk

Anda menyertakan JSON yang berisi skema sumber data sebagai bagian dari objek. TemplateConfiguration Anda memberikan URL host sebagai bagian dari konfigurasi koneksi atau detail titik akhir repositori. Juga tentukan jenis sumber data sebagai`ZENDESK`, rahasia untuk kredensyal otentikasi Anda, dan konfigurasi lain yang diperlukan. Anda kemudian menentukan `TEMPLATE` sebagai `Type` saat Anda menelepon CreateDataSource.

Anda dapat menggunakan template yang disediakan dalam panduan pengembang ini. Lihat Skema Zendesk JSON.

Tabel berikut menjelaskan parameter skema Zendesk JSON.

Konfigurasi	Deskripsi
ConnectionConfiguration	Informasi konfigurasi untuk titik akhir untuk sumber data.
repositoryEndpointMetadata	Informasi titik akhir untuk sumber data.
HostURL	URL host Zendesk. Misalnya, https://yoursubdomain.zendesk.com.
RepositoryConfigurations	Informasi konfigurasi untuk konten sumber data. Misalnya, mengonfigurasi jenis konten dan pemetaan bidang tertentu.
• karcis • TicketKomentar • ticketCommentAttachment • artikel • ArtikelKomentar • ArtikelLampiran • KomunitasTopik • communityPostComment	Daftar objek yang memetakan atribut atau nama bidang tiket Zendesk ke nama bidang indeks Amazon Kendra. Untuk informasi lebih lanjut, lihat Memetakan bidang sumber data.
Sekretarn	Nama Sumber Daya Amazon (ARN) dari AWS Secrets Manager rahasia yang berisi pasangan kunci-nilai yang diperlukan untuk terhubung ke Zendesk Anda. Rahasia harus berisi struktur JSON dengan kunci berikut: URL host, ID klien, rahasia klien, nama pengguna, dan kata sandi.
AdditionalProperties	Opsi konfigurasi tambahan untuk konten Anda di sumber data Anda

Konfigurasi	Deskripsi
organizationNameFilter	Anda dapat memilih untuk mengindeks tiket yang ada dalam Organisasi tertentu.
sejakDate	Anda dapat memilih untuk mengonfigurasi `sinceDate` parameter sehingga konektor Zendesk merayapi konten berdasarkan spesifik. `sinceDate`
Pola Inklusi	Daftar pola ekspresi reguler untuk menyertakan file tertentu dalam sumber data Zendesk Anda. File yang cocok dengan pola disertakan dalam indeks. File yang tidak cocok dengan pola dikecualikan dari indeks. Jika file cocok dengan pola inklusi dan pengecualian, pola pengecualian akan diutamakan, dan file tidak disertakan dalam indeks.
Pola Pengecualian	Daftar pola ekspresi reguler untuk mengecualikan file tertentu di sumber data Zendesk Anda. File yang cocok dengan pola dikecualikan dari indeks. File yang tidak cocok dengan pola disertakan dalam indeks. Jika file cocok dengan pola pengecualian dan inklusi, pola pengecualian akan diutamakan, dan file tidak disertakan dalam indeks.

Konfigurasi	Deskripsi
• isCrawlTicket • isCrawlTicketKomentar • isCrawlTicketCommentAttachment • isCrawlArticle • isCrawlArticleKomentar • isCrawlArticleLampiran • isCrawlCommunityTopik • isCrawlCommunityPosting • isCrawlCommunityPostComment	Masukkan "`true`" untuk merayapi jenis konten ini.
jenis	Tentukan `ZENDESK` sebagai tipe sumber data Anda.
useChangeLog	Masukkan "`true`" untuk menggunakan log perubahan Zendesk untuk menentukan dokumen mana yang perlu diperbarui dalam indeks. Tergantung pada ukuran log perubahan , mungkin lebih cepat untuk memindai dokumen di Zendesk. Jika Anda menyinkronkan sumber data Zendesk Anda dengan indeks Anda untuk pertama kalinya, semua dokumen dipindai.

Skema Zendesk JSON

```
{
  "$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"
                    }
                  },
                  "required": [
                    "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"
                  }
                },
                "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"
                      }
                    },
                    "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"
```

```
        },
        "isCrawTicket": {
          "type": "string"
        },
        "isCrawTicketComment": {
          "type": "string"
        },
        "isCrawTicketCommentAttachment": {
          "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 Manageradalah sistem manajemen konten yang digunakan untuk membuat konten situs web atau aplikasi seluler. Anda dapat menggunakan Amazon Kendra untuk menghubungkan Adobe Experience Manager dan mengindeks halaman dan aset konten Anda.

Amazon Kendra mendukung Adobe Experience Manager (AEM) sebagai instance penulis Layanan Cloud dan penulis Adobe Experience Manager On-Premise dan menerbitkan instance.

Anda dapat terhubung Amazon Kendra ke sumber Adobe Experience Manager data menggunakan Amazon Kendra konsol atau TemplateConfigurationAPI.

Untuk memecahkan masalah konektor sumber data Amazon Kendra Adobe Experience Manager, lihat. Mengatasi masalah sumber data

Topik

- Fitur yang didukung
- Prasyarat
- Instruksi koneksi

Fitur yang didukung

Adobe Experience Managerkonektor sumber data mendukung fitur-fitur berikut:

- Pemetaan lapangan

- Pemfilteran konteks pengguna
- Filter inklusi/pengecualian
- Sinkronisasi konten penuh dan tambahan
- OAuth 2.0 dan otentikasi dasar
- Cloud privat virtual (VPC)

Prasyarat

Sebelum Anda dapat menggunakan Amazon Kendra untuk mengindeks sumber Adobe Experience Manager data Anda, buat perubahan ini di akun Adobe Experience Manager dan AWS akun Anda.

DiAdobe Experience Manager, pastikan Anda memiliki:

- Akses ke akun dengan hak administratif, atau pengguna admin.
- Menyalin URL Adobe Experience Manager host Anda.

> **Note**
>
> (On-premise/server) Amazon Kendra memeriksa apakah informasi titik akhir yang disertakan sama dengan informasi titik akhir yang AWS Secrets Manager ditentukan dalam detail konfigurasi sumber data Anda. Ini membantu melindungi dari masalah wakil yang membingungkan, yang merupakan masalah keamanan di mana pengguna tidak memiliki izin untuk melakukan tindakan tetapi menggunakan Amazon Kendra sebagai proxy untuk mengakses rahasia yang dikonfigurasi dan melakukan tindakan. Jika nanti Anda mengubah informasi titik akhir Anda, Anda harus membuat rahasia baru untuk menyinkronkan informasi ini.

- Mencatat kredensi otentikasi dasar Anda dari nama pengguna dan kata sandi admin.
- Opsional: Kredensi OAuth 2.0 yang dihasilkan di Adobe Experience Manager (AEM) sebagai Layanan Cloud atau AEM On-Premise. Jika Anda menggunakan AEM On-Premise, kredensialnya mencakup ID klien, rahasia klien, dan kunci pribadi. Jika Anda menggunakan AEM sebagai Layanan Cloud, kredensialnya mencakup ID klien, rahasia klien, kunci pribadi, ID organisasi, ID akun teknis, dan host Adobe Identity Management System (IMS). Untuk informasi selengkapnya tentang cara membuat kredensil ini untuk AEM sebagai Layanan Cloud, lihat dokumentasi. Adobe Experience Manager Untuk AEM On-Premise, implementasi server Adobe Granite OAuth 2.0 (com.adobe.granite.oauth.server) menyediakan dukungan untuk fungsi server OAuth 2.0 di AEM.

- Memeriksa setiap dokumen unik di Adobe Experience Manager dan di seluruh sumber data lain yang Anda rencanakan untuk digunakan untuk indeks yang sama. Setiap sumber data yang ingin Anda gunakan untuk indeks tidak boleh berisi dokumen yang sama di seluruh sumber data. ID dokumen bersifat global untuk indeks dan harus unik per indeks.

Di dalam Anda Akun AWS, pastikan Anda memiliki:

- Membuat Amazon Kendra indeks dan, jika menggunakan API, mencatat ID indeks.
- Membuat IAM peran untuk sumber data Anda dan, jika menggunakan API, catat ARN peran tersebut IAM .

> **Note**
>
> Jika Anda mengubah jenis otentikasi dan kredensialnya, Anda harus memperbarui IAM peran Anda untuk mengakses ID rahasia yang benar AWS Secrets Manager .

- Menyimpan kredensi otentikasi Adobe Experience Manager Anda AWS Secrets Manager secara rahasia dan, jika menggunakan API, catat ARN rahasianya.

> **Note**
>
> Kami menyarankan Anda secara teratur menyegarkan atau memutar kredensil dan rahasia Anda. Berikan hanya tingkat akses yang diperlukan untuk keamanan Anda sendiri. Kami tidak menyarankan Anda menggunakan kembali kredensil dan rahasia di seluruh sumber data, dan konektor versi 1.0 dan 2.0 (jika berlaku).

Jika Anda tidak memiliki IAM peran atau rahasia yang ada, Anda dapat menggunakan konsol untuk membuat IAM peran dan Secrets Manager rahasia baru saat Anda menghubungkan sumber data Adobe Experience Manager Amazon Kendra. Jika Anda menggunakan API, Anda harus memberikan ARN IAM peran dan Secrets Manager rahasia yang ada, dan ID indeks.

Instruksi koneksi

Untuk terhubung Amazon Kendra ke sumber Adobe Experience Manager data Anda, Anda harus memberikan rincian yang diperlukan dari sumber Adobe Experience Manager data Anda sehingga Amazon Kendra dapat mengakses data Anda. Jika Anda belum mengkonfigurasi Adobe Experience Manager untuk Amazon Kendra, lihatPrasyarat.

Console

Untuk terhubung Amazon Kendra ke Adobe Experience Manager

1. Masuk ke AWS Management Console dan buka Amazon Kendra konsol.
2. Dari panel navigasi kiri, pilih Indeks dan kemudian pilih indeks yang ingin Anda gunakan dari daftar indeks.

> **Note**
>
> Anda dapat memilih untuk mengonfigurasi atau mengedit pengaturan kontrol akses Pengguna Anda di bawah Pengaturan indeks.

3. Pada halaman Memulai, pilih Tambahkan sumber data.
4. Pada halaman Tambah sumber data, pilih konektor Adobe Experience Manager, lalu pilih Tambah konektor.
5. Pada halaman Tentukan detail sumber data, masukkan informasi berikut:
   a. Di Nama dan deskripsi, untuk Nama sumber data —Masukkan nama untuk sumber data Anda. Anda dapat memasukkan tanda hubung tetapi bukan spasi.
   b. (Opsional) Deskripsi —Masukkan deskripsi opsional untuk sumber data Anda.
   c. Dalam Bahasa default —Pilih bahasa untuk memfilter dokumen Anda untuk indeks. Kecuali Anda menentukan sebaliknya, bahasa default ke bahasa Inggris. Bahasa yang ditentukan dalam metadata dokumen mengesampingkan bahasa yang dipilih.
   d. Di Tag, untuk Tambahkan tag baru —Sertakan tag opsional untuk mencari dan memfilter sumber daya Anda atau melacak AWS biaya Anda.
   e. Pilih Berikutnya.
6. Pada halaman Tentukan akses dan keamanan, masukkan informasi berikut:
   a. Sumber —Pilih AEM On-Premise atau AEM sebagai Layanan Cloud.

      Masukkan URL Adobe Experience Manager host Anda. Misalnya, jika Anda menggunakan AEM On-Premise, Anda menyertakan nama host dan port:. https://hostname:port Atau, jika Anda menggunakan AEM sebagai Layanan Cloud, Anda dapat menggunakan URL penulis: https://author-xxxxxx-xxxxxxx.adobeaemcloud.com.

b. Lokasi sertifikat SSL —Masukkan jalur ke sertifikat SSL yang disimpan dalam bucket. Amazon S3 Anda menggunakan ini untuk terhubung ke AEM On-Premise dengan koneksi SSL yang aman.

c. Otorisasi — Aktifkan atau nonaktifkan informasi daftar kontrol akses (ACL) untuk dokumen Anda, jika Anda memiliki ACL dan ingin menggunakannya untuk kontrol akses. ACL menentukan dokumen mana yang dapat diakses pengguna dan grup. Informasi ACL digunakan untuk memfilter hasil pencarian berdasarkan pengguna atau akses grup mereka ke dokumen. Untuk informasi selengkapnya, lihat Pemfilteran konteks pengguna.

d. Otentikasi —Pilih otentikasi dasar atau otentikasi OAuth 2.0. Kemudian pilih AWS Secrets Manager rahasia yang ada atau buat rahasia baru untuk menyimpan Adobe Experience Manager kredensil Anda. Jika Anda memilih untuk membuat rahasia baru, jendela AWS Secrets Manager rahasia terbuka.

   Jika Anda memilih otentikasi dasar, masukkan nama untuk rahasia, nama pengguna Adobe Experience Manager situs dan kata sandi. Pengguna harus memiliki izin admin atau menjadi pengguna admin.

   Jika Anda memilih otentikasi OAuth 2.0 dan Anda menggunakan AEM On-Premise, masukkan nama untuk rahasia, ID klien, rahasia klien, dan kunci pribadi. Jika Anda menggunakan AEM sebagai Layanan Cloud, masukkan nama untuk rahasia, ID klien, rahasia klien, kunci pribadi, ID organisasi, ID akun teknis, dan host Adobe Identity Management System (IMS).

   Pilih Simpan.

e. Virtual Private Cloud (VPC) —Anda dapat memilih untuk menggunakan VPC. Jika demikian, Anda harus menambahkan Subnet dan grup keamanan VPC.

f. Perayap identitas —Tentukan apakah akan mengaktifkan crawler Amazon Kendra identitas. Perayap identitas menggunakan informasi daftar kontrol akses (ACL) untuk dokumen Anda untuk memfilter hasil penelusuran berdasarkan akses pengguna atau grup mereka ke dokumen. Jika Anda memiliki ACL untuk dokumen Anda dan memilih untuk menggunakan ACL Anda, Anda juga dapat memilih untuk mengaktifkan crawler Amazon Kendra identitas untuk mengonfigurasi pemfilteran konteks pengguna dari hasil pencarian. Jika tidak, jika crawler identitas dimatikan, semua dokumen dapat dicari secara publik. Jika Anda ingin menggunakan kontrol akses untuk dokumen dan crawler identitas dimatikan, Anda dapat menggunakan PutPrincipalMappingAPI untuk mengunggah informasi akses pengguna dan grup untuk pemfilteran konteks pengguna.

g. IAM peran —Pilih peran yang sudah ada atau buat IAM IAM peran baru untuk mengakses kredensi repositori dan mengindeks konten Anda.

> **Note**
>
> IAM peran yang digunakan untuk indeks tidak dapat digunakan untuk sumber data. Jika Anda tidak yakin apakah peran yang ada digunakan untuk indeks atau FAQ, pilih Buat peran baru untuk menghindari kesalahan.

h. Pilih Berikutnya.

7. Pada halaman Konfigurasi pengaturan sinkronisasi, masukkan informasi berikut:

a. Sinkronisasi cakupan —Tetapkan batas untuk merayapi jenis konten tertentu, komponen halaman, dan jalur akar, dan filter konten menggunakan pola ekspresi regex.

i. Jenis konten —Pilih apakah hanya akan merayapi halaman atau aset, atau keduanya.

ii. (Opsional) Konfigurasi tambahan —Konfigurasikan pengaturan berikut:

- Komponen halaman —Nama spesifik komponen halaman. Komponen Halaman adalah komponen halaman yang dapat diperluas yang dirancang untuk bekerja dengan editor Adobe Experience Manager template dan memungkinkan header halaman/footer dan komponen struktur dirakit dengan editor template.
- Variasi fragmen konten —Nama spesifik variasi fragmen konten. Fragmen Konten memungkinkan Anda mendesain, membuat, mengkurasi, dan mempublikasikan konten yang tidak bergantung pada halaman. Adobe Experience Manager Mereka memungkinkan Anda menyiapkan konten yang siap digunakan di beberapa lokasi/ melalui beberapa saluran.
- Jalur root —Jalur root ke konten tertentu.
- Pola Regex —Pola ekspresi reguler untuk menyertakan atau mengecualikan halaman dan aset tertentu.

b. Mode sinkronisasi —Pilih cara memperbarui indeks saat konten sumber data berubah. Saat Anda menyinkronkan sumber data Amazon Kendra untuk pertama kalinya, semua konten dirayapi dan diindeks secara default. Anda harus menjalankan sinkronisasi penuh data Anda jika sinkronisasi awal Anda gagal, bahkan jika Anda tidak memilih sinkronisasi penuh sebagai opsi mode sinkronisasi Anda.

- Sinkronisasi penuh: Indeks baru semua konten, ganti konten yang ada setiap kali sumber data Anda disinkronkan dengan indeks Anda.
- Sinkronisasi baru yang dimodifikasi: Indeks hanya konten baru dan yang dimodifikasi setiap kali sumber data Anda disinkronkan dengan indeks Anda. Amazon Kendra dapat menggunakan mekanisme sumber data Anda untuk melacak perubahan konten dan mengindeks konten yang berubah sejak sinkronisasi terakhir.
- Sinkronisasi baru, dimodifikasi, dihapus: Indeks hanya konten baru, dimodifikasi, dan dihapus setiap kali sumber data Anda disinkronkan dengan indeks Anda. Amazon Kendra dapat menggunakan mekanisme sumber data Anda untuk melacak perubahan konten dan mengindeks konten yang berubah sejak sinkronisasi terakhir.

c. ID zona waktu —Jika Anda menggunakan AEM On-Premise dan zona waktu server Anda berbeda dari zona waktu konektor atau indeks Amazon Kendra AEM, Anda dapat menentukan zona waktu server agar sejajar dengan konektor atau indeks AEM. Zona waktu default untuk AEM On-Premise adalah zona waktu konektor atau indeks Amazon Kendra AEM. Zona waktu default untuk AEM sebagai Layanan Cloud adalah Greenwich Mean Time.

d. Sinkronkan jadwal berjalan —Untuk Frekuensi, pilih seberapa sering Amazon Kendra akan disinkronkan dengan sumber data Anda.

e. Pilih Berikutnya.

8. Pada halaman Setel pemetaan bidang, masukkan informasi berikut:

   a. Pilih dari bidang sumber data default yang Amazon Kendra dihasilkan yang ingin Anda petakan ke indeks Anda. Untuk menambahkan bidang sumber data kustom, buat nama bidang indeks untuk dipetakan dan tipe data bidang.

   b. Pilih Berikutnya.

9. Pada halaman Tinjau dan buat, periksa apakah informasi yang Anda masukkan sudah benar dan kemudian pilih Tambahkan sumber data. Anda juga dapat memilih untuk mengedit informasi Anda dari halaman ini. Sumber data Anda akan muncul di halaman Sumber data setelah sumber data berhasil ditambahkan.

API

Untuk terhubung Amazon Kendra ke Adobe Experience Manager

Anda harus menentukan JSON dari skema sumber data menggunakan API. TemplateConfiguration Anda harus memberikan informasi berikut ini:

- Sumber data —Tentukan tipe sumber data seperti `AEM` saat Anda menggunakan skema TemplateConfigurationJSON. Tentukan juga sumber data seperti `TEMPLATE` saat Anda memanggil CreateDataSourceAPI.
- URL host AEM —Tentukan URL Adobe Experience Manager host. Misalnya, jika Anda menggunakan AEM On-Premise, Anda menyertakan nama host dan port:. https://hostname:port Atau, jika Anda menggunakan AEM sebagai Layanan Cloud, Anda dapat menggunakan URL penulis: https://author-xxxxxx-xxxxxxx.adobeaemcloud.com.
- Mode sinkronisasi —Tentukan cara Amazon Kendra memperbarui indeks Anda saat konten sumber data Anda berubah. Saat Anda menyinkronkan sumber data Amazon Kendra untuk pertama kalinya, semua konten dirayapi dan diindeks secara default. Anda harus menjalankan sinkronisasi penuh data Anda jika sinkronisasi awal Anda gagal, bahkan jika Anda tidak memilih sinkronisasi penuh sebagai opsi mode sinkronisasi Anda. Anda dapat memilih antara:
  - `FORCED_FULL_CRAWL`untuk mengindeks semua konten baru, mengganti konten yang ada setiap kali sumber data Anda disinkronkan dengan indeks Anda.
  - `FULL_CRAWL`untuk mengindeks hanya konten baru, dimodifikasi, dan dihapus setiap kali sumber data Anda disinkronkan dengan indeks Anda. Amazon Kendra dapat menggunakan mekanisme sumber data Anda untuk melacak perubahan konten dan mengindeks konten yang berubah sejak sinkronisasi terakhir.
  - `CHANGE_LOG`untuk mengindeks hanya konten baru dan yang dimodifikasi setiap kali sumber data Anda disinkronkan dengan indeks Anda. Amazon Kendra dapat menggunakan mekanisme sumber data Anda untuk melacak perubahan konten dan mengindeks konten yang berubah sejak sinkronisasi terakhir.
- Jenis otentikasi —Tentukan jenis otentikasi yang ingin Anda gunakan, salah satu atau. `Basic` `OAuth2`
- Jenis AEM —Tentukan jenis yang Adobe Experience Manager Anda gunakan, salah satu atau`CLOUD`. `ON_PREMISE`
- Rahasia Nama Sumber Daya Amazon (ARN) —Jika Anda ingin menggunakan otentikasi dasar untuk AEM On-Premise atau Cloud, Anda memberikan rahasia yang menyimpan kredensi otentikasi nama pengguna dan kata sandi Anda. Anda memberikan Nama Sumber Daya Amazon (ARN) dari sebuah AWS Secrets Manager rahasia. Rahasianya disimpan dalam struktur JSON dengan kunci berikut:

```
{
    "aemUrl": "Adobe Experience Manager On-Premise host URL",
    "username": "user name with admin permissions",
    "password": "password with admin permissions"
}
```

Jika Anda ingin menggunakan otentikasi OAuth 2.0 untuk AEM On-Premise, rahasianya disimpan dalam struktur JSON dengan kunci berikut:

```
{
    "aemUrl": "Adobe Experience Manager host URL",
    "clientId": "client ID",
    "clientSecret": "client secret",
    "privateKey": "private key"
}
```

Jika Anda ingin menggunakan otentikasi OAuth 2.0 untuk AEM sebagai Layanan Cloud, rahasianya disimpan dalam struktur JSON dengan kunci berikut:

```
{
    "clientId": "client ID",
    "clientSecret": "client secret",
    "privateKey": "private key",
    "orgId": "organization ID",
    "technicalAccountId": "technical account ID",
    "imsHost": "Adobe Identity Management System (IMS) host"
}
```

- IAM peran —Tentukan `RoleArn` kapan Anda menelepon `CreateDataSource` untuk memberikan IAM peran dengan izin untuk mengakses Secrets Manager rahasia Anda dan memanggil API publik yang diperlukan untuk konektor Adobe Experience Manager dan. Amazon Kendra Untuk informasi selengkapnya, lihat IAM peran untuk sumber data Adobe Experience Manager.

Anda juga dapat menambahkan fitur opsional berikut:

- Virtual Private Cloud (VPC) **`VpcConfiguration`** —Tentukan kapan Anda menelepon. `CreateDataSource` Untuk informasi selengkapnya, lihat Mengkonfigurasi Amazon Kendra untuk menggunakan Amazon VPC.

- ID zona waktu —Jika Anda menggunakan AEM On-Premise dan zona waktu server Anda berbeda dari zona waktu konektor atau indeks Amazon Kendra AEM, Anda dapat menentukan zona waktu server agar sejajar dengan konektor atau indeks AEM.

  Zona waktu default untuk AEM On-Premise adalah zona waktu konektor atau indeks Amazon Kendra AEM. Zona waktu default untuk AEM sebagai Layanan Cloud adalah Greenwich Mean Time.

  Untuk informasi tentang ID zona waktu yang didukung, lihat skema Adobe Experience Manager JSON.
- Filter inklusi dan pengecualian —Tentukan apakah akan menyertakan atau mengecualikan halaman dan aset tertentu.

  > **Note**
  >
  > Sebagian besar sumber data menggunakan pola ekspresi reguler, yang merupakan pola inklusi atau pengecualian yang disebut sebagai filter. Jika Anda menentukan filter inklusi, hanya konten yang cocok dengan filter inklusi yang diindeks. Dokumen apa pun yang tidak cocok dengan filter inklusi tidak diindeks. Jika Anda menentukan filter inklusi dan pengecualian, dokumen yang cocok dengan filter pengecualian tidak akan diindeks, meskipun sesuai dengan filter inklusi.
- Perayap identitas —Tentukan apakah akan mengaktifkan crawler Amazon Kendra identitas. Perayap identitas menggunakan informasi daftar kontrol akses (ACL) untuk dokumen Anda untuk memfilter hasil penelusuran berdasarkan akses pengguna atau grup mereka ke dokumen. Jika Anda memiliki ACL untuk dokumen Anda dan memilih untuk menggunakan ACL Anda, Anda juga dapat memilih untuk mengaktifkan crawler Amazon Kendra identitas untuk mengonfigurasi pemfilteran konteks pengguna dari hasil pencarian. Jika tidak, jika crawler identitas dimatikan, semua dokumen dapat dicari secara publik. Jika Anda ingin menggunakan kontrol akses untuk dokumen dan crawler identitas dimatikan, Anda dapat menggunakan PutPrincipalMappingAPI untuk mengunggah informasi akses pengguna dan grup untuk pemfilteran konteks pengguna.
- Pemetaan bidang —Pilih untuk memetakan bidang sumber data Adobe Experience Manager Anda ke bidang indeks Anda Amazon Kendra . Untuk informasi lebih lanjut, lihat Memetakan bidang sumber data.

> **Note**
>
> Bidang badan dokumen atau badan dokumen yang setara untuk dokumen Anda diperlukan Amazon Kendra untuk mencari dokumen Anda. Anda harus memetakan nama bidang badan dokumen Anda di sumber data Anda ke nama bidang indeks_`document_body`. Semua kolom lain bersifat opsional.

Untuk daftar kunci JSON penting lainnya untuk dikonfigurasi, lihat skema Adobe Experience Manager template.

Alfresco

Alfrescoadalah layanan manajemen konten yang membantu pelanggan menyimpan dan mengelola konten mereka. Anda dapat menggunakan Amazon Kendra untuk mengindeks pustaka Alfresco Dokumen, Wiki, dan Blog Anda.

Amazon Kendra mendukung Alfresco On-Premise dan Alfresco Cloud (Platform as a Service).

Anda dapat terhubung Amazon Kendra ke sumber Alfresco data menggunakan Amazon Kendra konsol atau TemplateConfigurationAPI.

Untuk memecahkan masalah konektor sumber data Amazon Kendra Alfresco, lihat. Mengatasi masalah sumber data

Topik

- Fitur yang didukung
- Prasyarat
- Instruksi koneksi
- Pelajari selengkapnya

Fitur yang didukung

Amazon Kendra Alfrescokonektor sumber data mendukung fitur-fitur berikut:

- Pemetaan lapangan
- Filter inklusi/pengecualian

- Sinkronisasi konten penuh dan tambahan
- Cloud privat virtual (VPC)
- Pemfilteran konteks pengguna
- OAuth 2.0 dan otentikasi dasar

Prasyarat

Sebelum Anda dapat menggunakan Amazon Kendra untuk mengindeks sumber data Alfresco Anda, buat perubahan ini pada sumber data Anda dan. Alfresco Akun AWS

DiAlfresco, pastikan Anda memiliki:

- Menyalin URL Alfresco repositori dan URL aplikasi web Anda. Jika Anda hanya ingin mengindeks Alfresco situs tertentu, maka salin juga ID situs.
- Mencatat kredensi Alfresco otentikasi Anda, yang mencakup nama pengguna dan kata sandi dengan setidaknya izin baca. Jika Anda ingin menggunakan otentikasi OAuth 2.0, Anda harus menambahkan pengguna ke grup administrator. Alfresco
- Opsional: Kredensi OAuth 2.0 yang dihasilkan di. Alfresco Kredensialnya termasuk ID klien, rahasia klien, dan URL token. Untuk informasi selengkapnya tentang cara mengonfigurasi klien untuk Alfresco Lokal, lihat dokumentasi Alfresco. Jika Anda menggunakan Alfresco Cloud (PaaS), Anda harus menghubungi dukungan Hyland untuk Alfresco otentikasi OAuth 2.0.
- Memeriksa setiap dokumen unik di Alfresco dan di seluruh sumber data lain yang Anda rencanakan untuk digunakan untuk indeks yang sama. Setiap sumber data yang ingin Anda gunakan untuk indeks tidak boleh berisi dokumen yang sama di seluruh sumber data. ID dokumen bersifat global untuk indeks dan harus unik per indeks.

Di dalam Anda Akun AWS, pastikan Anda memiliki:

- Membuat Amazon Kendra indeks dan, jika menggunakan API, mencatat ID indeks.
- Membuat IAM peran untuk sumber data Anda dan, jika menggunakan API, catat ARN peran tersebut IAM .

> **Note**
>
> Jika Anda mengubah jenis otentikasi dan kredensialnya, Anda harus memperbarui IAM peran Anda untuk mengakses ID rahasia yang benar AWS Secrets Manager .

- Menyimpan kredensi otentikasi Alfresco Anda secara AWS Secrets Manager rahasia dan, jika menggunakan API, catat ARN rahasianya.

> **Note**
>
> Kami menyarankan Anda secara teratur menyegarkan atau memutar kredensil dan rahasia Anda. Berikan hanya tingkat akses yang diperlukan untuk keamanan Anda sendiri. Kami tidak menyarankan Anda menggunakan kembali kredensil dan rahasia di seluruh sumber data, dan konektor versi 1.0 dan 2.0 (jika berlaku).

Jika Anda tidak memiliki IAM peran atau rahasia yang ada, Anda dapat menggunakan konsol untuk membuat IAM peran dan Secrets Manager rahasia baru saat menghubungkan sumber data Alfresco Anda. Amazon Kendra Jika Anda menggunakan API, Anda harus memberikan ARN IAM peran dan Secrets Manager rahasia yang ada, dan ID indeks.

Instruksi koneksi

Untuk terhubung Amazon Kendra ke sumber data Alfresco Anda, Anda harus memberikan rincian yang diperlukan dari sumber data Alfresco Anda sehingga dapat mengakses data Anda. Amazon Kendra Jika Anda belum mengkonfigurasi Alfresco untuk Amazon Kendra, lihat. Prasyarat

Console

Untuk terhubung Amazon Kendra ke Alfresco

1. Masuk ke AWS Management Console dan buka Amazon Kendra konsol.
2. Dari panel navigasi kiri, pilih Indeks dan kemudian pilih indeks yang ingin Anda gunakan dari daftar indeks.

> **Note**
>
> Anda dapat memilih untuk mengonfigurasi atau mengedit pengaturan kontrol akses Pengguna Anda di bawah Pengaturan indeks.

3. Pada halaman Memulai, pilih Tambahkan sumber data.
4. Pada halaman Tambahkan sumber data, pilih konektor Alfresco, lalu pilih Tambah konektor.
5. Pada halaman Tentukan detail sumber data, masukkan informasi berikut:

a. Di Nama dan deskripsi, untuk Nama sumber data —Masukkan nama untuk sumber data Anda. Anda dapat memasukkan tanda hubung tetapi bukan spasi.

b. (Opsional) Deskripsi —Masukkan deskripsi opsional untuk sumber data Anda.

c. Dalam Bahasa default —Pilih bahasa untuk memfilter dokumen Anda untuk indeks. Kecuali Anda menentukan sebaliknya, bahasa default ke bahasa Inggris. Bahasa yang ditentukan dalam metadata dokumen menggantikan bahasa yang dipilih.

d. Di Tag, untuk Tambahkan tag baru —Sertakan tag opsional untuk mencari dan memfilter sumber daya Anda atau melacak AWS biaya Anda.

e. Pilih Berikutnya.

6. Pada halaman Tentukan akses dan keamanan, masukkan informasi berikut:

a. Alfrescoketik —Pilih apakah Anda menggunakan Alfresco Lokal atau Alfresco Cloud (Platform sebagai Layanan).

b. URL repositori alfresco —Masukkan URL repositori Alfresco Anda. Misalnya, jika Anda menggunakan Alfresco Cloud (PaaS), URL repositori bisa jadi. https://company.alfrescocloud.com Atau, jika Anda menggunakan Alfresco On-Premises, URL repositori bisa jadi. https://company-alfresco-instance.company-domain.suffix:port

c. Aplikasi pengguna alfresco. URL —Masukkan URL antarmuka Alfresco pengguna Anda. Anda bisa mendapatkan URL repositori dari administrator AndaAlfresco. Misalnya, URL antarmuka pengguna dapat berupa https://example.com.

d. Lokasi sertifikat SSL —Masukkan jalur ke sertifikat SSL yang disimpan dalam bucket. Amazon S3 Anda menggunakan ini untuk terhubung ke Alfresco Lokal dengan koneksi SSL yang aman.

e. Otorisasi — Aktifkan atau nonaktifkan informasi daftar kontrol akses (ACL) untuk dokumen Anda, jika Anda memiliki ACL dan ingin menggunakannya untuk kontrol akses. ACL menentukan dokumen mana yang dapat diakses pengguna dan grup. Informasi ACL digunakan untuk memfilter hasil pencarian berdasarkan pengguna atau akses grup mereka ke dokumen. Untuk informasi selengkapnya, lihat Pemfilteran konteks pengguna.

f. Otentikasi —Pilih otentikasi dasar atau otentikasi OAuth 2.0. Kemudian pilih Secrets Manager rahasia yang ada atau buat rahasia baru untuk menyimpan Alfresco kredensil Anda. Jika Anda memilih untuk membuat rahasia baru, jendela AWS Secrets Manager rahasia terbuka.

Jika Anda memilih otentikasi Dasar, masukkan nama untuk rahasia, nama Alfresco pengguna, dan kata sandi.

Jika Anda memilih otentikasi OAuth 2.0, masukkan nama untuk rahasia, ID klien, rahasia klien, dan URL token.

g. Virtual Private Cloud (VPC) —Anda dapat memilih untuk menggunakan VPC. Jika demikian, Anda harus menambahkan Subnet dan grup keamanan VPC.

h. Perayap identitas —Tentukan apakah akan mengaktifkan crawler Amazon Kendra identitas. Perayap identitas menggunakan informasi daftar kontrol akses (ACL) untuk dokumen Anda untuk memfilter hasil penelusuran berdasarkan akses pengguna atau grup mereka ke dokumen. Jika Anda memiliki ACL untuk dokumen Anda dan memilih untuk menggunakan ACL Anda, Anda juga dapat memilih untuk mengaktifkan crawler Amazon Kendra identitas untuk mengonfigurasi pemfilteran konteks pengguna dari hasil pencarian. Jika tidak, jika crawler identitas dimatikan, semua dokumen dapat dicari secara publik. Jika Anda ingin menggunakan kontrol akses untuk dokumen dan crawler identitas dimatikan, Anda dapat menggunakan PutPrincipalMappingAPI untuk mengunggah informasi akses pengguna dan grup untuk pemfilteran konteks pengguna.

i. IAM peran —Pilih peran yang ada atau buat IAM IAM peran baru untuk mengakses kredensi repositori dan mengindeks konten Anda.

> **Note**
>
> IAM peran yang digunakan untuk indeks tidak dapat digunakan untuk sumber data. Jika Anda tidak yakin apakah peran yang ada digunakan untuk indeks atau FAQ, pilih Buat peran baru untuk menghindari kesalahan.

j. Pilih Berikutnya.

7. Pada halaman Konfigurasi pengaturan sinkronisasi, masukkan informasi berikut:

a. Lingkup sinkronisasi —Tetapkan batas untuk merayapi konten tertentu dan memfilter konten menggunakan pola ekspresi regex.

b. i. Konten —Pilih apakah akan merayapi konten yang ditandai dengan 'Aspek'Alfresco, konten dalam Alfresco situs tertentu, atau konten di semua situs AndaAlfresco.

ii. (Opsional) Konfigurasi tambahan —Atur pengaturan berikut:

- Sertakan komentar —Pilih untuk menyertakan komentar di pustaka Alfresco Dokumen dan Blog.
- Pola Regex —Pola ekspresi reguler untuk menyertakan atau mengecualikan file tertentu.

c. Mode sinkronisasi —Pilih cara memperbarui indeks saat konten sumber data berubah. Saat Anda menyinkronkan sumber data Amazon Kendra untuk pertama kalinya, semua konten dirayapi dan diindeks secara default. Anda harus menjalankan sinkronisasi penuh data Anda jika sinkronisasi awal Anda gagal, bahkan jika Anda tidak memilih sinkronisasi penuh sebagai opsi mode sinkronisasi Anda.

- Sinkronisasi penuh: Indeks baru semua konten, ganti konten yang ada setiap kali sumber data Anda disinkronkan dengan indeks Anda.
- Sinkronisasi baru, dimodifikasi, dihapus: Indeks hanya konten baru, dimodifikasi, dan dihapus setiap kali sumber data Anda disinkronkan dengan indeks Anda. Amazon Kendra dapat menggunakan mekanisme sumber data Anda untuk melacak perubahan konten dan mengindeks konten yang berubah sejak sinkronisasi terakhir.

d. Di Jadwal lari Sinkronisasi, untuk Frekuensi —Pilih seberapa sering Amazon Kendra akan disinkronkan dengan sumber data Anda.

e. Pilih Berikutnya.

8. Pada halaman Setel pemetaan bidang, masukkan informasi berikut:

a. Pilih dari bidang sumber data default yang Amazon Kendra dihasilkan yang ingin Anda petakan ke indeks Anda.

b. Untuk menambahkan bidang sumber data kustom, buat nama bidang indeks untuk dipetakan dan tipe data bidang.

c. Pilih Berikutnya.

9. Pada halaman Tinjau dan buat, periksa apakah informasi yang Anda masukkan sudah benar dan kemudian pilih Tambahkan sumber data. Anda juga dapat memilih untuk mengedit informasi Anda dari halaman ini. Sumber data Anda akan muncul di halaman Sumber data setelah sumber data berhasil ditambahkan.

API

Untuk terhubung Amazon Kendra ke Alfresco

Anda harus menentukan JSON dari skema sumber data menggunakan API. TemplateConfiguration Anda harus memberikan informasi berikut ini:

- Sumber data —Tentukan tipe sumber data seperti `ALFRESCO` saat Anda menggunakan skema TemplateConfigurationJSON. Tentukan juga sumber data seperti `TEMPLATE` saat Anda memanggil CreateDataSourceAPI.
- AlfrescoID situs —Tentukan ID situs Alfresco.
- AlfrescoURL repositori —Tentukan URL repositori. Alfresco Anda bisa mendapatkan URL repositori dari administrator AndaAlfresco. Misalnya, jika Anda menggunakan Alfresco Cloud (PaaS), URL repositori bisa jadi. https://company.alfrescocloud.com Atau, jika Anda menggunakan Alfresco On-Premises, URL repositori bisa jadi. https://company-alfresco-instance.company-domain.suffix:port
- AlfrescoURL aplikasi web —Tentukan URL antarmuka Alfresco pengguna. Anda bisa mendapatkan URL repositori dari administrator AndaAlfresco. Misalnya, URL antarmuka pengguna dapat berupa https://example.com.
- Jenis otentikasi —Tentukan jenis otentikasi yang ingin Anda gunakan, apakah atau. `OAuth2` `Basic`
- Alfrescotype —Tentukan jenis yang Alfresco Anda gunakan, apakah `PAAS` (Cloud/Platform sebagai Layanan) atau `ON_PREM` (Lokal).
- Rahasia Nama Sumber Daya Amazon (ARN) —Jika Anda ingin menggunakan otentikasi dasar, Anda memberikan rahasia yang menyimpan kredensi otentikasi nama pengguna dan kata sandi Anda. Anda memberikan Nama Sumber Daya Amazon (ARN) rahasia. AWS Secrets Manager Rahasianya disimpan dalam struktur JSON dengan kunci berikut:

```
{
    "username": "user name",
    "password": "password"
}
```

Jika Anda ingin menggunakan otentikasi OAuth 2.0, rahasianya disimpan dalam struktur JSON dengan kunci berikut:

```
{
    "clientId": "client ID",
    "clientSecret": "client secret",
    "tokenUrl": "token URL"
```

```
}
```

- IAM peran —Tentukan `RoleArn` kapan Anda menelepon `CreateDataSource` untuk memberikan IAM peran dengan izin untuk mengakses Secrets Manager rahasia Anda dan memanggil API publik yang diperlukan untuk konektor Alfresco dan. Amazon Kendra Untuk informasi selengkapnya, lihat IAM peran untuk sumber data Alfresco.

Anda juga dapat menambahkan fitur opsional berikut:

- Virtual Private Cloud (VPC) **`VpcConfiguration`** —Tentukan kapan Anda menelepon. `CreateDataSource` Untuk informasi selengkapnya, lihat Mengkonfigurasi Amazon Kendra untuk menggunakan Amazon VPC.
- Jenis konten —Jenis konten yang ingin dirayapi, apakah konten yang ditandai dengan 'Aspek'Alfresco, konten dalam Alfresco situs tertentu, atau konten di semua situs AndaAlfresco. Anda juga dapat membuat daftar konten 'Aspek' tertentu.
- Filter inklusi dan pengecualian —Tentukan apakah akan menyertakan atau mengecualikan file tertentu.

> **Note**
>
> Sebagian besar sumber data menggunakan pola ekspresi reguler, yang merupakan pola inklusi atau pengecualian yang disebut sebagai filter. Jika Anda menentukan filter inklusi, hanya konten yang cocok dengan filter inklusi yang diindeks. Dokumen apa pun yang tidak cocok dengan filter inklusi tidak diindeks. Jika Anda menentukan filter inklusi dan pengecualian, dokumen yang cocok dengan filter pengecualian tidak akan diindeks, meskipun sesuai dengan filter inklusi.

- Mode sinkronisasi —Tentukan cara Amazon Kendra memperbarui indeks Anda saat konten sumber data Anda berubah. Saat Anda menyinkronkan sumber data Amazon Kendra untuk pertama kalinya, semua konten dirayapi dan diindeks secara default. Anda harus menjalankan sinkronisasi penuh data Anda jika sinkronisasi awal Anda gagal, bahkan jika Anda tidak memilih sinkronisasi penuh sebagai opsi mode sinkronisasi Anda. Anda dapat memilih antara:
  - `FORCED_FULL_CRAWL`untuk mengindeks semua konten baru, mengganti konten yang ada setiap kali sumber data Anda disinkronkan dengan indeks Anda.
  - `FULL_CRAWL`untuk mengindeks hanya konten baru, dimodifikasi, dan dihapus setiap kali sumber data Anda disinkronkan dengan indeks Anda. Amazon Kendra dapat menggunakan

mekanisme sumber data Anda untuk melacak perubahan konten dan mengindeks konten yang berubah sejak sinkronisasi terakhir.

- Perayap identitas —Tentukan apakah akan mengaktifkan crawler Amazon Kendra identitas. Perayap identitas menggunakan informasi daftar kontrol akses (ACL) untuk dokumen Anda untuk memfilter hasil penelusuran berdasarkan akses pengguna atau grup mereka ke dokumen. Jika Anda memiliki ACL untuk dokumen Anda dan memilih untuk menggunakan ACL Anda, Anda juga dapat memilih untuk mengaktifkan crawler Amazon Kendra identitas untuk mengonfigurasi pemfilteran konteks pengguna dari hasil pencarian. Jika tidak, jika crawler identitas dimatikan, semua dokumen dapat dicari secara publik. Jika Anda ingin menggunakan kontrol akses untuk dokumen dan crawler identitas dimatikan, Anda dapat menggunakan PutPrincipalMappingAPI untuk mengunggah informasi akses pengguna dan grup untuk pemfilteran konteks pengguna.
- Pemetaan bidang —Pilih untuk memetakan bidang sumber data Alfresco Anda ke bidang indeks Anda. Amazon Kendra Untuk informasi lebih lanjut, lihat Memetakan bidang sumber data.

> **Note**
>
> Bidang badan dokumen atau badan dokumen yang setara untuk dokumen Anda diperlukan Amazon Kendra untuk mencari dokumen Anda. Anda harus memetakan nama bidang badan dokumen Anda di sumber data Anda ke nama bidang indeks_`document_body`. Semua kolom lain bersifat opsional.

Untuk daftar kunci JSON penting lainnya untuk dikonfigurasi, lihat skema Alfresco template.

Pelajari selengkapnya

Untuk mempelajari lebih lanjut tentang mengintegrasikan Amazon Kendra dengan sumber data Alfresco Anda, lihat:

- Cerdas mencari konten menggunakan AlfrescoAmazon Kendra

Aurora (MySQL)

Aurora adalah sistem manajemen basis data relasional (RDBMS) yang dibangun untuk cloud. Jika Anda adalah Aurora pengguna, Anda dapat menggunakan Amazon Kendra untuk mengindeks sumber Aurora (MySQL) data Anda. Konektor sumber Amazon Kendra Aurora (MySQL) data mendukung Aurora MySQL 3 dan MySQL 8.0 Tanpa Aurora Server.

Anda dapat terhubung Amazon Kendra ke sumber Aurora (MySQL) data menggunakan Amazon Kendra konsol dan TemplateConfigurationAPI.

Untuk memecahkan masalah konektor sumber Amazon Kendra Aurora (MySQL) data Anda, lihat. Mengatasi masalah sumber data

Topik

- Fitur yang didukung
- Prasyarat
- Instruksi koneksi
- Catatan

Fitur yang didukung

- Pemetaan lapangan
- Pemfilteran konteks pengguna
- Filter inklusi/pengecualian
- Sinkronisasi konten penuh dan tambahan
- Cloud privat virtual (VPC)

Prasyarat

Sebelum Anda dapat menggunakan Amazon Kendra untuk mengindeks sumber Aurora (MySQL) data Anda, buat perubahan ini di akun Aurora (MySQL) dan AWS akun Anda.

DiAurora (MySQL), pastikan Anda memiliki:

- Mencatat nama pengguna dan kata sandi database Anda.

> **Important**
>
> Sebagai praktik terbaik, sediakan Amazon Kendra kredensil basis data hanya-baca.

- Menyalin url, port, dan instance host database Anda. Anda dapat menemukan informasi ini di Amazon RDS konsol.
- Memeriksa setiap dokumen unik di dalam Aurora (MySQL) dan di seluruh sumber data lain yang Anda rencanakan untuk digunakan untuk indeks yang sama. Setiap sumber data yang ingin Anda gunakan untuk indeks tidak boleh berisi dokumen yang sama di seluruh sumber data. ID dokumen bersifat global untuk indeks dan harus unik per indeks.

Di dalam Anda Akun AWS, pastikan Anda memiliki:

- Membuat Amazon Kendra indeks dan, jika menggunakan API, mencatat ID indeks.
- Membuat IAM peran untuk sumber data Anda dan, jika menggunakan API, catat ARN peran tersebut IAM .

> **Note**
>
> Jika Anda mengubah jenis otentikasi dan kredensyal, Anda harus memperbarui IAM peran Anda untuk mengakses ID rahasia yang benar AWS Secrets Manager .

- Menyimpan kredensyal Aurora (MySQL) otentikasi Anda AWS Secrets Manager secara rahasia dan, jika menggunakan API, catat ARN rahasia tersebut.

> **Note**
>
> Kami menyarankan Anda secara teratur menyegarkan atau memutar kredensil dan rahasia Anda. Berikan hanya tingkat akses yang diperlukan untuk keamanan Anda sendiri. Kami tidak menyarankan Anda menggunakan kembali kredensyal dan rahasia di seluruh sumber data, dan konektor versi 1.0 dan 2.0 (jika berlaku).

Jika Anda tidak memiliki IAM peran atau rahasia yang ada, Anda dapat menggunakan konsol untuk membuat IAM peran dan Secrets Manager rahasia baru saat menghubungkan sumber Aurora

(MySQL) data Amazon Kendra. Jika Anda menggunakan API, Anda harus memberikan ARN IAM peran dan Secrets Manager rahasia yang ada, dan ID indeks.

Instruksi koneksi

Untuk terhubung Amazon Kendra ke sumber Aurora (MySQL) data Anda, Anda harus memberikan rincian Aurora (MySQL) kredensyal Anda sehingga Amazon Kendra dapat mengakses data Anda. Jika Anda belum mengkonfigurasi Aurora (MySQL) untuk Amazon Kendra lihatPrasyarat.

Console

Untuk terhubung Amazon Kendra ke Aurora (MySQL)

1. Masuk ke AWS Management Console dan buka Amazon Kendra konsol.
2. Dari panel navigasi kiri, pilih Indeks dan kemudian pilih indeks yang ingin Anda gunakan dari daftar indeks.

> **Note**
>
> Anda dapat memilih untuk mengonfigurasi atau mengedit pengaturan kontrol akses Pengguna Anda di bawah Pengaturan indeks.

3. Pada halaman Memulai, pilih Tambahkan sumber data.
4. Pada halaman Tambahkan sumber data, pilih Aurora (MySQL)konektor, lalu pilih Tambah konektor.
5. Pada halaman Tentukan detail sumber data, masukkan informasi berikut:
   a. Di Nama dan deskripsi, untuk Nama sumber data —Masukkan nama untuk sumber data Anda. Anda dapat memasukkan tanda hubung tetapi bukan spasi.
   b. (Opsional) Deskripsi —Masukkan deskripsi opsional untuk sumber data Anda.
   c. Dalam Bahasa default —Pilih bahasa untuk memfilter dokumen Anda untuk indeks. Kecuali Anda menentukan sebaliknya, bahasa default ke bahasa Inggris. Bahasa yang ditentukan dalam metadata dokumen menggantikan bahasa yang dipilih.
   d. Di Tag, untuk Tambahkan tag baru —Sertakan tag opsional untuk mencari dan memfilter sumber daya Anda atau melacak AWS biaya Anda.
   e. Pilih Berikutnya.
6. Pada halaman Tentukan akses dan keamanan, masukkan informasi berikut:

a. Di Sumber, masukkan informasi berikut:

b. Host — Masukkan URL host database, misalnya:`http://instance URL.region.rds.amazonaws.com`.

c. Port — Masukkan port database, misalnya,`5432`.

d. Instance - Masukkan instance database.

e. Dalam Otentikasi —masukkan informasi berikut:

- AWS Secrets Manager rahasia —Pilih rahasia yang ada atau buat Secrets Manager rahasia baru untuk menyimpan kredensyal Aurora (MySQL) otentikasi Anda. Jika Anda memilih untuk membuat rahasia baru, jendela AWS Secrets Manager rahasia terbuka.

  A. Masukkan informasi berikut di jendela Buat AWS Secrets Manager rahasia:

     I. Nama rahasia —Nama untuk rahasiamu. Awalan 'AmazonKendra- Aurora (MySQL) -' secara otomatis ditambahkan ke nama rahasia Anda.

     II. Untuk nama pengguna Database, dan Kata Sandi —Masukkan nilai kredensi otentikasi yang Anda salin dari database Anda.

  B. Pilih Simpan.

f. Virtual Private Cloud (VPC) —Anda dapat memilih untuk menggunakan VPC. Jika demikian, Anda harus menambahkan Subnet dan grup keamanan VPC.

g. IAM peran —Pilih peran yang ada atau buat IAM IAM peran baru untuk mengakses kredensi repositori dan mengindeks konten Anda.

> **Note**
>
> IAM peran yang digunakan untuk indeks tidak dapat digunakan untuk sumber data. Jika Anda tidak yakin apakah peran yang ada digunakan untuk indeks atau FAQ, pilih Buat peran baru untuk menghindari kesalahan.

h. Pilih Berikutnya.

7. Pada halaman Konfigurasi pengaturan sinkronisasi, masukkan informasi berikut:

a. Dalam lingkup Sinkronisasi, pilih dari opsi berikut:

- Kueri SQL —Masukkan pernyataan kueri SQL seperti operasi SELECT dan JOIN. Kueri SQL harus kurang dari 32KB Kueri SQL harus kurang dari 32KB dan tidak mengandung semi-titik dua (;). Amazon Kendra akan merayapi semua konten database yang cocok dengan kueri Anda.
- Kolom kunci primer —Berikan kunci utama untuk tabel database. Ini mengidentifikasi tabel dalam database Anda.
- Judul kolom —Berikan nama kolom judul dokumen dalam tabel database Anda.
- Kolom tubuh —Berikan nama kolom badan dokumen dalam tabel database Anda.

b. Dalam Konfigurasi tambahan — opsional, pilih dari opsi berikut untuk menyinkronkan konten tertentu alih-alih menyinkronkan semua file:

- Kolom pendeteksi perubahan —Masukkan nama kolom yang Amazon Kendra akan digunakan untuk mendeteksi perubahan konten. Amazon Kendra akan mengindeks ulang konten ketika ada perubahan di salah satu kolom ini.
- Kolom ID Pengguna —Masukkan nama kolom yang berisi ID Pengguna agar diizinkan mengakses konten.
- Kolom Grup —Masukkan nama kolom yang berisi grup untuk diizinkan mengakses konten.
- Kolom URL sumber —Masukkan nama kolom yang berisi URL Sumber yang akan diindeks.
- Kolom stempel waktu —Masukkan nama kolom yang berisi stempel waktu. Amazon Kendra menggunakan informasi cap waktu untuk mendeteksi perubahan dalam konten Anda dan hanya menyinkronkan konten yang diubah.
- Kolom zona waktu —Masukkan nama kolom yang berisi zona waktu untuk konten yang akan dirayapi.
- Format stempel waktu —Masukkan nama kolom yang berisi format cap waktu yang akan digunakan untuk mendeteksi perubahan konten dan menyinkronkan ulang konten Anda.

c. Mode sinkronisasi —Pilih cara memperbarui indeks saat konten sumber data berubah. Saat Anda menyinkronkan sumber data Amazon Kendra untuk pertama kalinya, semua konten dirayapi dan diindeks secara default. Anda harus menjalankan sinkronisasi penuh data Anda jika sinkronisasi awal Anda gagal, bahkan jika Anda tidak memilih sinkronisasi penuh sebagai opsi mode sinkronisasi Anda.

- Sinkronisasi penuh: Indeks baru semua konten, ganti konten yang ada setiap kali sumber data Anda disinkronkan dengan indeks Anda.
- Sinkronisasi baru yang dimodifikasi: Indeks hanya konten baru dan yang dimodifikasi setiap kali sumber data Anda disinkronkan dengan indeks Anda. Amazon Kendra dapat menggunakan mekanisme sumber data Anda untuk melacak perubahan konten dan mengindeks konten yang berubah sejak sinkronisasi terakhir.
- Sinkronisasi baru, dimodifikasi, dihapus: Indeks hanya konten baru, dimodifikasi, dan dihapus setiap kali sumber data Anda disinkronkan dengan indeks Anda. Amazon Kendra dapat menggunakan mekanisme sumber data Anda untuk melacak perubahan konten dan mengindeks konten yang berubah sejak sinkronisasi terakhir.

d. Dalam jadwal berjalan Sinkronisasi, untuk Frekuensi —Seberapa sering Amazon Kendra akan disinkronkan dengan sumber data Anda.

e. Pilih Berikutnya.

8. Pada halaman Setel pemetaan bidang, masukkan informasi berikut:

   a. Pilih dari bidang sumber data default yang dihasilkan - ID dokumen, judul dokumen, dan URL Sumber - yang ingin Anda petakan ke Amazon Kendra indeks.

   b. Tambahkan bidang —Untuk menambahkan bidang sumber data kustom untuk membuat nama bidang indeks untuk dipetakan dan tipe data bidang.

   c. Pilih Berikutnya.

9. Pada halaman Tinjau dan buat, periksa apakah informasi yang Anda masukkan sudah benar dan kemudian pilih Tambahkan sumber data. Anda juga dapat memilih untuk mengedit informasi Anda dari halaman ini. Sumber data Anda akan muncul di halaman Sumber data setelah sumber data berhasil ditambahkan.

API

Untuk terhubung Amazon Kendra ke Aurora (MySQL)

Anda harus menentukan yang berikut menggunakan TemplateConfigurationAPI:

- Sumber data —Tentukan tipe sumber data seperti `JDBC` saat Anda menggunakan skema TemplateConfigurationJSON. Tentukan juga sumber data seperti `TEMPLATE` saat Anda memanggil CreateDataSourceAPI.
- Jenis database —Anda harus menentukan jenis database sebagai`mySql`.

- Kueri SQL —Tentukan pernyataan kueri SQL seperti operasi SELECT dan JOIN. Kueri SQL harus kurang dari 32KB. Amazon Kendra akan merayapi semua konten database yang cocok dengan kueri Anda.
- Mode sinkronisasi —Tentukan cara Amazon Kendra memperbarui indeks Anda saat konten sumber data Anda berubah. Saat Anda menyinkronkan sumber data Amazon Kendra untuk pertama kalinya, semua konten dirayapi dan diindeks secara default. Anda harus menjalankan sinkronisasi penuh data Anda jika sinkronisasi awal Anda gagal, bahkan jika Anda tidak memilih sinkronisasi penuh sebagai opsi mode sinkronisasi Anda. Anda dapat memilih antara:
  - `FORCED_FULL_CRAWL`untuk mengindeks semua konten baru, mengganti konten yang ada setiap kali sumber data Anda disinkronkan dengan indeks Anda.
  - `FULL_CRAWL`untuk mengindeks hanya konten baru, dimodifikasi, dan dihapus setiap kali sumber data Anda disinkronkan dengan indeks Anda. Amazon Kendra dapat menggunakan mekanisme sumber data Anda untuk melacak perubahan konten dan mengindeks konten yang berubah sejak sinkronisasi terakhir.
  - `CHANGE_LOG`untuk mengindeks hanya konten baru dan yang dimodifikasi setiap kali sumber data Anda disinkronkan dengan indeks Anda. Amazon Kendra dapat menggunakan mekanisme sumber data Anda untuk melacak perubahan konten dan mengindeks konten yang berubah sejak sinkronisasi terakhir.
- Rahasia Nama Sumber Daya Amazon (ARN) —Berikan Nama Sumber Daya Amazon (ARN) Secrets Manager rahasia yang berisi kredensyal otentikasi yang Anda buat di akun Anda. Aurora (MySQL) Rahasianya disimpan dalam struktur JSON dengan kunci berikut:

```
{
    "user name": "database user name",
    "password": "password"
}
```

> **Note**
>
> Kami menyarankan Anda secara teratur menyegarkan atau memutar kredensil dan rahasia Anda. Berikan hanya tingkat akses yang diperlukan untuk keamanan Anda sendiri. Kami tidak menyarankan Anda menggunakan kembali kredensyal dan rahasia di seluruh sumber data, dan konektor versi 1.0 dan 2.0 (jika berlaku).

- IAM peran —Tentukan `RoleArn` kapan Anda menelepon `CreateDataSource` untuk memberikan IAM peran dengan izin untuk mengakses Secrets Manager rahasia Anda dan

memanggil API publik yang diperlukan untuk Aurora (MySQL) konektor dan. Amazon Kendra Untuk informasi selengkapnya, lihat IAM peran untuk sumber Aurora (MySQL) data.

Anda juga dapat menambahkan fitur opsional berikut:

- Virtual Private Cloud (VPC) **`VpcConfiguration`** —Tentukan kapan Anda menelepon. `CreateDataSource` Untuk informasi selengkapnya, lihat Mengkonfigurasi Amazon Kendra untuk menggunakan Amazon VPC.
- Filter penyertaan dan pengecualian —Anda dapat menentukan apakah akan menyertakan konten tertentu menggunakan ID pengguna, grup, URL sumber, stempel waktu, dan zona waktu.
- Pemfilteran konteks pengguna dan kontrol akses —Amazon Kendra meng-crawl daftar kontrol akses (ACL) untuk dokumen Anda, jika Anda memiliki ACL untuk dokumen Anda. Informasi ACL digunakan untuk memfilter hasil pencarian berdasarkan pengguna atau akses grup mereka ke dokumen. Untuk informasi selengkapnya, lihat Pemfilteran konteks pengguna.
- Pemetaan bidang —Pilih untuk memetakan bidang sumber Aurora (MySQL) data Anda ke bidang indeks Anda Amazon Kendra . Untuk informasi lebih lanjut, lihat Memetakan bidang sumber data.

> **Note**
>
> Bidang badan dokumen atau badan dokumen yang setara untuk dokumen Anda diperlukan Amazon Kendra untuk mencari dokumen Anda. Anda harus memetakan nama bidang badan dokumen Anda di sumber data Anda ke nama bidang indeks_`document_body`. Semua kolom lain bersifat opsional.

Untuk daftar kunci JSON penting lainnya untuk dikonfigurasi, lihatAurora Skema templat (MySQL).

Catatan

- Baris database yang dihapus tidak akan dilacak saat Amazon Kendra memeriksa konten yang diperbarui.
- Ukuran nama bidang dan nilai dalam deretan database Anda tidak dapat melebihi 400KB.

- Jika Anda memiliki sejumlah besar data dalam sumber data database Anda, dan tidak Amazon Kendra ingin mengindeks semua konten database Anda setelah sinkronisasi pertama, Anda dapat memilih untuk menyinkronkan hanya dokumen baru, dimodifikasi, atau dihapus.
- Sebagai praktik terbaik, sediakan Amazon Kendra kredensil basis data hanya-baca.
- Sebagai praktik terbaik, hindari menambahkan tabel dengan data sensitif atau informasi identitas pribadi (PII).

Aurora (PostgreSQL)

Aurora adalah sistem manajemen basis data relasional (RDBMS) yang dibangun untuk cloud. Jika Anda adalah Aurora pengguna, Anda dapat menggunakan Amazon Kendra untuk mengindeks sumber Aurora (PostgreSQL) data Anda. Konektor sumber Amazon Kendra Aurora (PostgreSQL) data mendukung Aurora PostgreSQL 1.

Anda dapat terhubung Amazon Kendra ke sumber Aurora (PostgreSQL) data menggunakan Amazon Kendra konsol dan TemplateConfigurationAPI.

Untuk memecahkan masalah konektor sumber Amazon Kendra Aurora (PostgreSQL) data Anda, lihat. Mengatasi masalah sumber data

Topik

- Fitur yang didukung
- Prasyarat
- Instruksi koneksi
- Catatan

Fitur yang didukung

- Pemetaan lapangan
- Pemfilteran konteks pengguna
- Filter inklusi/pengecualian
- Sinkronisasi konten penuh dan tambahan
- Cloud privat virtual (VPC)

Prasyarat

Sebelum Anda dapat menggunakan Amazon Kendra untuk mengindeks sumber Aurora (PostgreSQL) data Anda, buat perubahan ini di akun Aurora (PostgreSQL) dan AWS akun Anda.

DiAurora (PostgreSQL), pastikan Anda memiliki:

- Mencatat nama pengguna dan kata sandi database Anda.

> **Important**
>
> Sebagai praktik terbaik, sediakan Amazon Kendra kredensil basis data hanya-baca.

- Menyalin url, port, dan instance host database Anda.
- Memeriksa setiap dokumen unik di dalam Aurora (PostgreSQL) dan di seluruh sumber data lain yang Anda rencanakan untuk digunakan untuk indeks yang sama. Setiap sumber data yang ingin Anda gunakan untuk indeks tidak boleh berisi dokumen yang sama di seluruh sumber data. ID dokumen bersifat global untuk indeks dan harus unik per indeks.

Di dalam Anda Akun AWS, pastikan Anda memiliki:

- Membuat Amazon Kendra indeks dan, jika menggunakan API, mencatat ID indeks.
- Membuat IAM peran untuk sumber data Anda dan, jika menggunakan API, catat ARN peran tersebut IAM .

> **Note**
>
> Jika Anda mengubah jenis otentikasi dan kredensyal, Anda harus memperbarui IAM peran Anda untuk mengakses ID rahasia yang benar AWS Secrets Manager .

- Menyimpan kredensyal Aurora (PostgreSQL) otentikasi Anda AWS Secrets Manager secara rahasia dan, jika menggunakan API, catat ARN rahasia tersebut.

> **Note**
>
> Kami menyarankan Anda secara teratur menyegarkan atau memutar kredensil dan rahasia Anda. Berikan hanya tingkat akses yang diperlukan untuk keamanan Anda sendiri. Kami

tidak menyarankan Anda menggunakan kembali kredensyal dan rahasia di seluruh sumber data, dan konektor versi 1.0 dan 2.0 (jika berlaku).

Jika Anda tidak memiliki IAM peran atau rahasia yang ada, Anda dapat menggunakan konsol untuk membuat IAM peran dan Secrets Manager rahasia baru saat menghubungkan sumber Aurora (PostgreSQL) data Amazon Kendra. Jika Anda menggunakan API, Anda harus memberikan ARN IAM peran dan Secrets Manager rahasia yang ada, dan ID indeks.

Instruksi koneksi

Untuk terhubung Amazon Kendra ke sumber Aurora (PostgreSQL) data Anda, Anda harus memberikan rincian Aurora (PostgreSQL) kredensyal Anda sehingga Amazon Kendra dapat mengakses data Anda. Jika Anda belum mengkonfigurasi Aurora (PostgreSQL) untuk Amazon Kendra lihatPrasyarat.

Console

Untuk terhubung Amazon Kendra ke Aurora (PostgreSQL)

1. Masuk ke AWS Management Console dan buka Amazon Kendra konsol.
2. Dari panel navigasi kiri, pilih Indeks dan kemudian pilih indeks yang ingin Anda gunakan dari daftar indeks.

   > **Note**
   >
   > Anda dapat memilih untuk mengonfigurasi atau mengedit pengaturan kontrol akses Pengguna Anda di bawah Pengaturan indeks.

3. Pada halaman Memulai, pilih Tambahkan sumber data.
4. Pada halaman Tambahkan sumber data, pilih Aurora (PostgreSQL)konektor, lalu pilih Tambah konektor.
5. Pada halaman Tentukan detail sumber data, masukkan informasi berikut:

   a. Di Nama dan deskripsi, untuk Nama sumber data —Masukkan nama untuk sumber data Anda. Anda dapat memasukkan tanda hubung tetapi bukan spasi.

   b. (Opsional) Deskripsi —Masukkan deskripsi opsional untuk sumber data Anda.

c. Dalam Bahasa default —Pilih bahasa untuk memfilter dokumen Anda untuk indeks. Kecuali Anda menentukan sebaliknya, bahasa default ke bahasa Inggris. Bahasa yang ditentukan dalam metadata dokumen mengesampingkan bahasa yang dipilih.

d. Di Tag, untuk Tambahkan tag baru —Sertakan tag opsional untuk mencari dan memfilter sumber daya Anda atau melacak AWS biaya Anda.

e. Pilih Berikutnya.

6. Pada halaman Tentukan akses dan keamanan, masukkan informasi berikut:

a. Di Sumber, masukkan informasi berikut:

b. Host — Masukkan URL host database, misalnya:`http://`*`instance URL`*`.`*`region`*`.rds.amazonaws.com`.

c. Port — Masukkan port database, misalnya,`5432`.

d. Instance — Masukkan contoh database, misalnya`postgres`.

e. Aktifkan lokasi sertifikat SSL —Pilih untuk memasukkan Amazon S3 jalur ke file sertifikat SSL Anda.

f. Dalam Otentikasi —masukkan informasi berikut:

- AWS Secrets Manager rahasia —Pilih rahasia yang ada atau buat Secrets Manager rahasia baru untuk menyimpan kredensyal Aurora (PostgreSQL) otentikasi Anda. Jika Anda memilih untuk membuat rahasia baru, jendela AWS Secrets Manager rahasia terbuka.

  A. Masukkan informasi berikut di jendela Buat AWS Secrets Manager rahasia:

     I. Nama rahasia —Nama untuk rahasiamu. Awalan 'AmazonKendra- Aurora (PostgreSQL) -' secara otomatis ditambahkan ke nama rahasia Anda.

     II. Untuk nama pengguna Database, dan Kata Sandi —Masukkan nilai kredensi otentikasi yang Anda salin dari database Anda.

  B. Pilih Simpan.

g. Virtual Private Cloud (VPC) —Anda dapat memilih untuk menggunakan VPC. Jika demikian, Anda harus menambahkan Subnet dan grup keamanan VPC.

h. IAM peran —Pilih peran yang sudah ada atau buat IAM IAM peran baru untuk mengakses kredensi repositori dan mengindeks konten Anda.

> **Note**
>
> IAM peran yang digunakan untuk indeks tidak dapat digunakan untuk sumber data. Jika Anda tidak yakin apakah peran yang ada digunakan untuk indeks atau FAQ, pilih Buat peran baru untuk menghindari kesalahan.

i. Pilih Berikutnya.

7. Pada halaman Konfigurasi pengaturan sinkronisasi, masukkan informasi berikut:

   a. Dalam lingkup Sinkronisasi, pilih dari opsi berikut:

      - Kueri SQL —Masukkan pernyataan kueri SQL seperti operasi SELECT dan JOIN. Kueri SQL harus kurang dari 32KB Kueri SQL harus kurang dari 32KB dan tidak mengandung semi-titik dua (;). Amazon Kendra akan merayapi semua konten database yang cocok dengan kueri Anda.
      - Kolom kunci primer —Menyediakan kunci utama untuk tabel database. Ini mengidentifikasi tabel dalam database Anda.
      - Judul kolom —Berikan nama kolom judul dokumen dalam tabel database Anda.
      - Kolom tubuh —Berikan nama kolom badan dokumen dalam tabel database Anda.

   b. Dalam Konfigurasi tambahan — opsional, pilih dari opsi berikut untuk menyinkronkan konten tertentu alih-alih menyinkronkan semua file:

      - Kolom pendeteksi perubahan —Masukkan nama kolom yang Amazon Kendra akan digunakan untuk mendeteksi perubahan konten. Amazon Kendra akan mengindeks ulang konten ketika ada perubahan di salah satu kolom ini.
      - Kolom ID Pengguna —Masukkan nama kolom yang berisi ID Pengguna agar diizinkan mengakses konten.
      - Kolom Grup —Masukkan nama kolom yang berisi grup untuk diizinkan mengakses konten.
      - Kolom URL sumber —Masukkan nama kolom yang berisi URL Sumber yang akan diindeks.
      - Kolom stempel waktu —Masukkan nama kolom yang berisi stempel waktu. Amazon Kendra menggunakan informasi cap waktu untuk mendeteksi perubahan dalam konten Anda dan hanya menyinkronkan konten yang diubah.

- Kolom zona waktu —Masukkan nama kolom yang berisi zona waktu untuk konten yang akan dirayapi.
- Format stempel waktu —Masukkan nama kolom yang berisi format cap waktu yang akan digunakan untuk mendeteksi perubahan konten dan menyinkronkan ulang konten Anda.

c. Mode sinkronisasi —Pilih cara memperbarui indeks saat konten sumber data berubah. Saat Anda menyinkronkan sumber data Amazon Kendra untuk pertama kalinya, semua konten dirayapi dan diindeks secara default. Anda harus menjalankan sinkronisasi penuh data Anda jika sinkronisasi awal Anda gagal, bahkan jika Anda tidak memilih sinkronisasi penuh sebagai opsi mode sinkronisasi Anda.

- Sinkronisasi penuh: Indeks baru semua konten, ganti konten yang ada setiap kali sumber data Anda disinkronkan dengan indeks Anda.
- Sinkronisasi baru yang dimodifikasi: Indeks hanya konten baru dan yang dimodifikasi setiap kali sumber data Anda disinkronkan dengan indeks Anda. Amazon Kendra dapat menggunakan mekanisme sumber data Anda untuk melacak perubahan konten dan mengindeks konten yang berubah sejak sinkronisasi terakhir.
- Sinkronisasi baru, dimodifikasi, dihapus: Indeks hanya konten baru, dimodifikasi, dan dihapus setiap kali sumber data Anda disinkronkan dengan indeks Anda. Amazon Kendra dapat menggunakan mekanisme sumber data Anda untuk melacak perubahan konten dan mengindeks konten yang berubah sejak sinkronisasi terakhir.

d. Dalam jadwal berjalan Sinkronisasi, untuk Frekuensi —Seberapa sering Amazon Kendra akan disinkronkan dengan sumber data Anda.

e. Pilih Berikutnya.

8. Pada halaman Setel pemetaan bidang, masukkan informasi berikut:

a. Pilih dari bidang sumber data default yang dihasilkan - ID dokumen, judul dokumen, dan URL Sumber - yang ingin Anda petakan ke Amazon Kendra indeks.

b. Tambahkan bidang —Untuk menambahkan bidang sumber data kustom untuk membuat nama bidang indeks untuk dipetakan dan tipe data bidang.

c. Pilih Berikutnya.

9. Pada halaman Tinjau dan buat, periksa apakah informasi yang Anda masukkan sudah benar dan kemudian pilih Tambahkan sumber data. Anda juga dapat memilih untuk mengedit informasi Anda dari halaman ini. Sumber data Anda akan muncul di halaman Sumber data setelah sumber data berhasil ditambahkan.

API

Untuk terhubung Amazon Kendra ke Aurora (PostgreSQL)

Anda harus menentukan yang berikut menggunakan TemplateConfigurationAPI:

- Sumber data —Tentukan tipe sumber data seperti `JDBC` saat Anda menggunakan skema TemplateConfigurationJSON. Tentukan juga sumber data seperti `TEMPLATE` saat Anda memanggil CreateDataSourceAPI.
- Jenis database —Anda harus menentukan jenis database sebagai`postgresql`.
- Kueri SQL —Tentukan pernyataan kueri SQL seperti operasi SELECT dan JOIN. Kueri SQL harus kurang dari 32KB. Amazon Kendra akan merayapi semua konten database yang cocok dengan kueri Anda.
- Mode sinkronisasi —Tentukan cara Amazon Kendra memperbarui indeks Anda saat konten sumber data Anda berubah. Saat Anda menyinkronkan sumber data Amazon Kendra untuk pertama kalinya, semua konten dirayapi dan diindeks secara default. Anda harus menjalankan sinkronisasi penuh data Anda jika sinkronisasi awal Anda gagal, bahkan jika Anda tidak memilih sinkronisasi penuh sebagai opsi mode sinkronisasi Anda. Anda dapat memilih antara:
  - `FORCED_FULL_CRAWL`untuk mengindeks semua konten baru, mengganti konten yang ada setiap kali sumber data Anda disinkronkan dengan indeks Anda.
  - `FULL_CRAWL`untuk mengindeks hanya konten baru, dimodifikasi, dan dihapus setiap kali sumber data Anda disinkronkan dengan indeks Anda. Amazon Kendra dapat menggunakan mekanisme sumber data Anda untuk melacak perubahan konten dan mengindeks konten yang berubah sejak sinkronisasi terakhir.
  - `CHANGE_LOG`untuk mengindeks hanya konten baru dan yang dimodifikasi setiap kali sumber data Anda disinkronkan dengan indeks Anda. Amazon Kendra dapat menggunakan mekanisme sumber data Anda untuk melacak perubahan konten dan mengindeks konten yang berubah sejak sinkronisasi terakhir.
- Rahasia Nama Sumber Daya Amazon (ARN) —Berikan Nama Sumber Daya Amazon (ARN) Secrets Manager rahasia yang berisi kredensyal otentikasi yang Anda buat di akun Anda. Aurora (PostgreSQL) Rahasianya disimpan dalam struktur JSON dengan kunci berikut:

```
{
    "user name": "database user name",
    "password": "password"
}
```

> **Note**
>
> Kami menyarankan Anda secara teratur menyegarkan atau memutar kredensil dan rahasia Anda. Berikan hanya tingkat akses yang diperlukan untuk keamanan Anda sendiri. Kami tidak menyarankan Anda menggunakan kembali kredensyal dan rahasia di seluruh sumber data, dan konektor versi 1.0 dan 2.0 (jika berlaku).

- IAM peran —Tentukan `RoleArn` kapan Anda menelepon `CreateDataSource` untuk memberikan IAM peran dengan izin untuk mengakses Secrets Manager rahasia Anda dan memanggil API publik yang diperlukan untuk Aurora (PostgreSQL) konektor dan. Amazon Kendra Untuk informasi selengkapnya, lihat IAM peran untuk sumber Aurora (PostgreSQL) data.

Anda juga dapat menambahkan fitur opsional berikut:

- Virtual Private Cloud (VPC) **`VpcConfiguration`** —Tentukan kapan Anda menelepon. `CreateDataSource` Untuk informasi selengkapnya, lihat Mengkonfigurasi Amazon Kendra untuk menggunakan Amazon VPC.
- Filter penyertaan dan pengecualian —Anda dapat menentukan apakah akan menyertakan konten tertentu menggunakan ID pengguna, grup, URL sumber, stempel waktu, dan zona waktu.
- Pemfilteran konteks pengguna dan kontrol akses —Amazon Kendra meng-crawl daftar kontrol akses (ACL) untuk dokumen Anda, jika Anda memiliki ACL untuk dokumen Anda. Informasi ACL digunakan untuk memfilter hasil pencarian berdasarkan pengguna atau akses grup mereka ke dokumen. Untuk informasi selengkapnya, lihat Pemfilteran konteks pengguna.
- Pemetaan bidang —Pilih untuk memetakan bidang sumber Aurora (PostgreSQL) data Anda ke bidang indeks Anda Amazon Kendra . Untuk informasi lebih lanjut, lihat Memetakan bidang sumber data.

> **Note**
>
> Bidang badan dokumen atau badan dokumen yang setara untuk dokumen Anda diperlukan Amazon Kendra untuk mencari dokumen Anda. Anda harus memetakan nama bidang badan dokumen Anda di sumber data Anda ke nama bidang indeks_`document_body`. Semua kolom lain bersifat opsional.

Untuk daftar kunci JSON penting lainnya untuk dikonfigurasi, lihatAurora (PostgreSQL) skema templat.

Catatan

- Baris database yang dihapus tidak akan dilacak saat Amazon Kendra memeriksa konten yang diperbarui.
- Ukuran nama bidang dan nilai dalam deretan database Anda tidak dapat melebihi 400KB.
- Jika Anda memiliki sejumlah besar data dalam sumber data database Anda, dan tidak Amazon Kendra ingin mengindeks semua konten database Anda setelah sinkronisasi pertama, Anda dapat memilih untuk menyinkronkan hanya dokumen baru, dimodifikasi, atau dihapus.
- Sebagai praktik terbaik, sediakan Amazon Kendra kredensil basis data hanya-baca.
- Sebagai praktik terbaik, hindari menambahkan tabel dengan data sensitif atau informasi identitas pribadi (PII).

Amazon FSx (Jendela)

Amazon FSx (Windows) adalah sistem server file berbasis cloud yang dikelola sepenuhnya yang menawarkan kemampuan penyimpanan bersama. Jika Anda pengguna Amazon FSx (Windows), Anda dapat menggunakan Amazon Kendra untuk mengindeks sumber data Amazon FSx (Windows) Anda.

> **Note**
>
> Amazon Kendra sekarang mendukung konektor Amazon FSx (Windows) yang ditingkatkan. Konsol telah ditingkatkan secara otomatis untuk Anda. Konektor baru apa pun yang Anda buat di konsol akan menggunakan arsitektur yang ditingkatkan. Jika Anda menggunakan API, Anda sekarang harus menggunakan TemplateConfigurationobjek alih-alih `FSxConfiguration` objek untuk mengonfigurasi konektor Anda.
> Konektor yang dikonfigurasi menggunakan konsol lama dan arsitektur API akan terus berfungsi seperti yang dikonfigurasi. Namun, Anda tidak akan dapat mengedit atau memperbaruinya. Jika Anda ingin mengedit atau memperbarui konfigurasi konektor Anda, Anda harus membuat konektor baru.

Kami merekomendasikan untuk memigrasikan alur kerja konektor Anda ke versi yang ditingkatkan. Support untuk konektor yang dikonfigurasi menggunakan arsitektur lama dijadwalkan berakhir pada Juni 2024.

Anda dapat terhubung Amazon Kendra ke sumber data Amazon FSx (Windows) menggunakan Amazon Kendra konsol, atau TemplateConfigurationAPI.

Untuk memecahkan masalah konektor sumber data Amazon Kendra Amazon FSx (Windows) Anda, lihat. Mengatasi masalah sumber data

Topik

- Fitur yang didukung
- Prasyarat
- Instruksi koneksi
- Pelajari selengkapnya

Fitur yang didukung

Amazon Kendra Amazon FSx (Windows) konektor sumber data mendukung fitur-fitur berikut:

- Pemetaan lapangan
- Kontrol akses pengguna
- Perayapan identitas pengguna
- Filter inklusi dan pengecualian
- Sinkronisasi konten penuh dan tambahan
- Cloud privat virtual (VPC)

Prasyarat

Sebelum Anda dapat menggunakan Amazon Kendra untuk mengindeks sumber data Amazon FSx (Windows) Anda, periksa detail Amazon FSx (Windows) Anda dan Akun AWS.

Untuk Amazon FSx (Windows), pastikan Anda memiliki:

- Siapkan Amazon FSx (Windows) dengan izin baca dan pemasangan.

- Mencatat ID sistem file Anda. Anda dapat menemukan ID sistem file Anda di dasbor Sistem File di konsol Amazon FSx (Windows).
- Mengonfigurasi cloud pribadi virtual menggunakan Amazon VPC tempat sistem file Amazon FSx (Windows) Anda berada.
- Mencatat kredensi otentikasi Amazon FSx (Windows) Anda untuk akun Active Directory pengguna. Ini termasuk nama pengguna Active Directory Anda dengan nama domain DNS Anda (misalnya, user@corp.example.com) dan kata sandi.

> **Note**
>
> Gunakan hanya kredensil yang diperlukan agar konektor berfungsi. Jangan gunakan kredensil istimewa seperti admin domain.

- Memeriksa setiap dokumen unik di Amazon FSx (Windows) dan di seluruh sumber data lain yang Anda rencanakan untuk digunakan untuk indeks yang sama. Setiap sumber data yang ingin Anda gunakan untuk indeks tidak boleh berisi dokumen yang sama di seluruh sumber data. ID dokumen bersifat global untuk indeks dan harus unik per indeks.

Di dalam Anda Akun AWS, pastikan Anda memiliki:

- Membuat Amazon Kendra indeks dan, jika menggunakan API, mencatat ID indeks.
- Membuat IAM peran untuk sumber data Anda dan, jika menggunakan API, catat ARN peran tersebut IAM .

> **Note**
>
> Jika Anda mengubah jenis otentikasi dan kredensialnya, Anda harus memperbarui IAM peran Anda untuk mengakses ID rahasia yang benar AWS Secrets Manager .

- Menyimpan kredensi otentikasi Amazon FSx (Windows) Anda AWS Secrets Manager secara rahasia dan, jika menggunakan API, catat ARN rahasia tersebut.

> **Note**
>
> Kami menyarankan Anda secara teratur menyegarkan atau memutar kredensil dan rahasia Anda. Berikan hanya tingkat akses yang diperlukan untuk keamanan Anda sendiri. Kami

tidak menyarankan Anda menggunakan kembali kredensil dan rahasia di seluruh sumber data, dan konektor versi 1.0 dan 2.0 (jika berlaku).

Jika Anda tidak memiliki IAM peran atau rahasia yang ada, Anda dapat menggunakan konsol untuk membuat IAM peran dan Secrets Manager rahasia baru saat Anda menghubungkan sumber data Amazon FSx (Windows) Anda Amazon Kendra. Jika Anda menggunakan API, Anda harus memberikan ARN IAM peran dan Secrets Manager rahasia yang ada, dan ID indeks.

Instruksi koneksi

Untuk terhubung Amazon Kendra ke sumber data Amazon FSx (Windows) Anda, Anda harus memberikan rincian yang diperlukan dari sumber data Amazon FSx (Windows) Anda sehingga Amazon Kendra dapat mengakses data Anda. Jika Anda belum mengkonfigurasi Amazon FSx (Windows) untuk Amazon Kendra, lihatPrasyarat.

Console

Untuk terhubung Amazon Kendra ke sistem file Amazon FSx (Windows) Anda

1. Masuk ke AWS Management Console dan buka Amazon Kendra konsol.
2. Dari panel navigasi kiri, pilih Indeks dan kemudian pilih indeks yang ingin Anda gunakan dari daftar indeks.

   > **Note**
   >
   > Anda dapat memilih untuk mengonfigurasi atau mengedit pengaturan kontrol akses Pengguna Anda di bawah Pengaturan indeks.

3. Pada halaman Memulai, pilih Tambahkan sumber data.
4. Pada halaman Tambahkan sumber data, pilih konektor Amazon FSx (Windows), lalu pilih Tambah konektor.
5. Pada halaman Tentukan detail sumber data, masukkan informasi berikut:

   a. Di Nama dan deskripsi, untuk Nama sumber data —Masukkan nama untuk sumber data Anda. Anda dapat memasukkan tanda hubung tetapi bukan spasi.

   b. (Opsional) Deskripsi —Masukkan deskripsi opsional untuk sumber data Anda.

c. Dalam Bahasa default —Pilih bahasa untuk memfilter dokumen Anda untuk indeks. Kecuali Anda menentukan sebaliknya, bahasa default ke bahasa Inggris. Bahasa yang ditentukan dalam metadata dokumen mengesampingkan bahasa yang dipilih.

d. Di Tag, untuk Tambahkan tag baru —Sertakan tag opsional untuk mencari dan memfilter sumber daya Anda atau melacak AWS biaya Anda.

e. Pilih Berikutnya.

6. Pada halaman Tentukan akses dan keamanan, masukkan informasi berikut:

a. Amazon FSx (Windows) ID sistem file —Pilih dari dropdown ID sistem file Anda yang ada, diambil dari Amazon FSx (Windows). Atau, buat sistem file Amazon FSx (Windows). Anda dapat menemukan ID sistem file Anda di dasbor Sistem File di konsol Amazon FSx (Windows).

b. Otorisasi — Aktifkan atau nonaktifkan informasi daftar kontrol akses (ACL) untuk dokumen Anda, jika Anda memiliki ACL dan ingin menggunakannya untuk kontrol akses. ACL menentukan dokumen mana yang dapat diakses pengguna dan grup. Informasi ACL digunakan untuk memfilter hasil pencarian berdasarkan pengguna atau akses grup mereka ke dokumen. Untuk informasi selengkapnya, lihat Pemfilteran konteks pengguna.

c. Otentikasi —Pilih AWS Secrets Manager rahasia yang ada, atau buat rahasia baru untuk menyimpan kredensi sistem file Anda. Jika Anda memilih untuk membuat rahasia baru, jendela AWS Secrets Manager rahasia terbuka.

   Berikan rahasia yang menyimpan kredensi otentikasi Anda atas nama pengguna dan kata sandi Anda. Nama pengguna harus menyertakan nama domain DNS Anda. Misalnya, user@corp.example.com.

   Simpan dan tambahkan rahasia Anda.

d. Virtual Private Cloud (VPC) —Anda harus memilih Amazon VPC tempat (Windows) Anda Amazon FSx berada. Anda menyertakan subnet VPC dan grup keamanan. Lihat Mengkonfigurasi file. Amazon VPC

e. IAM peran —Pilih peran yang sudah ada atau buat IAM IAM peran baru untuk mengakses kredensi repositori dan mengindeks konten Anda.

> **Note**
>
> IAM peran yang digunakan untuk indeks tidak dapat digunakan untuk sumber data. Jika Anda tidak yakin apakah peran yang ada digunakan untuk indeks atau FAQ, pilih Buat peran baru untuk menghindari kesalahan.

f. Pilih Berikutnya.

7. Pada halaman Konfigurasi pengaturan sinkronisasi, masukkan informasi berikut:

   a. Lingkup sinkronisasi, pola Regex —Tambahkan pola ekspresi reguler untuk menyertakan atau mengecualikan file tertentu.

   b. Mode sinkronisasi —Pilih cara memperbarui indeks saat konten sumber data berubah. Saat Anda menyinkronkan sumber data Amazon Kendra untuk pertama kalinya, semua konten dirayapi dan diindeks secara default. Anda harus menjalankan sinkronisasi penuh data Anda jika sinkronisasi awal Anda gagal, bahkan jika Anda tidak memilih sinkronisasi penuh sebagai opsi mode sinkronisasi Anda.

      - Sinkronisasi penuh: Indeks baru semua konten, ganti konten yang ada setiap kali sumber data Anda disinkronkan dengan indeks Anda.
      - Sinkronisasi baru, dimodifikasi, dihapus: Indeks hanya konten baru, dimodifikasi, dan dihapus setiap kali sumber data Anda disinkronkan dengan indeks Anda. Amazon Kendra dapat menggunakan mekanisme sumber data Anda untuk melacak perubahan konten dan mengindeks konten yang berubah sejak sinkronisasi terakhir.

   c. Sinkronkan jadwal berjalan —Untuk Frekuensi, pilih seberapa sering menyinkronkan konten sumber data Anda dan memperbarui indeks Anda.

   d. Pilih Berikutnya.

8. Pada halaman Setel pemetaan bidang, masukkan informasi berikut:

   a. Pilih dari bidang default Amazon Kendra yang dihasilkan dari file Anda yang ingin Anda petakan ke indeks Anda. Untuk menambahkan bidang sumber data kustom, buat nama bidang indeks untuk dipetakan dan tipe data bidang.

   b. Pilih Berikutnya.

9. Pada halaman Tinjau dan buat, periksa apakah informasi yang Anda masukkan sudah benar dan kemudian pilih Tambahkan sumber data. Anda juga dapat memilih untuk mengedit

informasi Anda dari halaman ini. Sumber data Anda akan muncul di halaman Sumber data setelah sumber data berhasil ditambahkan.

API

Untuk terhubung Amazon Kendra ke sistem file Amazon FSx (Windows) Anda

Anda harus menentukan JSON dari skema sumber data menggunakan API. TemplateConfiguration Anda harus memberikan informasi berikut ini:

- Sumber data —Tentukan tipe sumber data seperti `FSX` saat Anda menggunakan skema TemplateConfigurationJSON. Juga tentukan sumber data seperti `TEMPLATE` saat Anda memanggil CreateDataSourceAPI.
- ID sistem file —Pengidentifikasi sistem file Amazon FSx (Windows). Anda dapat menemukan ID sistem file Anda di dasbor Sistem File di konsol Amazon FSx (Windows).
- Jenis sistem file —Tentukan jenis sistem file sebagai`WINDOWS`.
- Virtual Private Cloud (VPC) **`VpcConfiguration`** —Tentukan kapan Anda menelepon. `CreateDataSource` Untuk informasi selengkapnya, lihat Mengkonfigurasi Amazon Kendra untuk menggunakan Amazon VPC.

  > **Note**
  >
  > Anda harus memilih Amazon VPC tempat Amazon FSx (Windows) Anda berada. Anda menyertakan subnet VPC dan grup keamanan.

- Mode sinkronisasi —Tentukan cara Amazon Kendra memperbarui indeks Anda saat konten sumber data Anda berubah. Saat Anda menyinkronkan sumber data Amazon Kendra untuk pertama kalinya, semua konten dirayapi dan diindeks secara default. Anda harus menjalankan sinkronisasi penuh data Anda jika sinkronisasi awal Anda gagal, bahkan jika Anda tidak memilih sinkronisasi penuh sebagai opsi mode sinkronisasi Anda. Anda dapat memilih antara:
  - `FORCED_FULL_CRAWL`untuk mengindeks semua konten baru, mengganti konten yang ada setiap kali sumber data Anda disinkronkan dengan indeks Anda.
  - `FULL_CRAWL`untuk mengindeks hanya konten baru, dimodifikasi, dan dihapus setiap kali sumber data Anda disinkronkan dengan indeks Anda. Amazon Kendra dapat menggunakan mekanisme sumber data Anda untuk melacak perubahan konten dan mengindeks konten yang berubah sejak sinkronisasi terakhir.

- Perayap identitas —Tentukan apakah akan mengaktifkan crawler Amazon Kendra identitas. Perayap identitas menggunakan informasi daftar kontrol akses (ACL) untuk dokumen Anda untuk memfilter hasil penelusuran berdasarkan akses pengguna atau grup mereka ke dokumen. Jika Anda memiliki ACL untuk dokumen Anda dan memilih untuk menggunakan ACL Anda, Anda juga dapat memilih untuk mengaktifkan crawler Amazon Kendra identitas untuk mengonfigurasi pemfilteran konteks pengguna dari hasil pencarian. Jika tidak, jika crawler identitas dimatikan, semua dokumen dapat dicari secara publik. Jika Anda ingin menggunakan kontrol akses untuk dokumen dan crawler identitas dimatikan, Anda dapat menggunakan PutPrincipalMappingAPI untuk mengunggah informasi akses pengguna dan grup untuk pemfilteran konteks pengguna.
- Rahasia Nama Sumber Daya Amazon (ARN) —Berikan Nama Sumber Daya Amazon (ARN) Secrets Manager rahasia yang berisi kredensi otentikasi untuk akun (Windows) Anda. Amazon FSx Rahasianya disimpan dalam struktur JSON dengan kunci berikut:

```
{
    "username": "user@corp.example.com",
    "password": "password"
}
```

- IAM peran —Tentukan `RoleArn` kapan Anda menelepon `CreateDataSource` untuk memberikan IAM peran dengan izin untuk mengakses Secrets Manager rahasia Anda dan memanggil API publik yang diperlukan untuk konektor Amazon FSx (Windows) dan. Amazon Kendra Untuk informasi selengkapnya, lihat IAM peran untuk sumber data Amazon FSx (Windows).

Anda juga dapat menambahkan fitur opsional berikut:

- Filter inklusi dan pengecualian —Tentukan apakah akan menyertakan atau mengecualikan file tertentu.

> **Note**
>
> Sebagian besar sumber data menggunakan pola ekspresi reguler, yang merupakan pola inklusi atau pengecualian yang disebut sebagai filter. Jika Anda menentukan filter inklusi, hanya konten yang cocok dengan filter inklusi yang diindeks. Dokumen apa pun yang tidak cocok dengan filter inklusi tidak diindeks. Jika Anda menentukan filter inklusi

dan pengecualian, dokumen yang cocok dengan filter pengecualian tidak akan diindeks, meskipun sesuai dengan filter inklusi.

- Daftar kontrol akses (ACL) —Tentukan apakah akan merayapi informasi ACL untuk dokumen Anda, jika Anda memiliki ACL dan ingin menggunakannya untuk kontrol akses. ACL menentukan dokumen mana yang dapat diakses pengguna dan grup. Informasi ACL digunakan untuk memfilter hasil pencarian berdasarkan pengguna atau akses grup mereka ke dokumen. Untuk informasi selengkapnya, lihat Pemfilteran konteks pengguna.

  > **Note**
  >
  > Untuk menguji pemfilteran konteks pengguna pada pengguna, Anda harus menyertakan nama domain DNS sebagai bagian dari nama pengguna saat Anda mengeluarkan kueri. Anda harus memiliki izin administratif dari domain Active Directory. Anda juga dapat menguji pemfilteran konteks pengguna pada nama grup.

- Pemetaan bidang —Pilih untuk memetakan bidang sumber data Amazon FSx (Windows) Anda ke bidang indeks Anda Amazon Kendra . Untuk informasi lebih lanjut, lihat Memetakan bidang sumber data.

  > **Note**
  >
  > Bidang badan dokumen atau badan dokumen yang setara untuk dokumen Anda diperlukan Amazon Kendra untuk mencari dokumen Anda. Anda harus memetakan nama bidang badan dokumen Anda di sumber data Anda ke nama bidang indeks_`document_body`. Semua kolom lain bersifat opsional.

Untuk daftar kunci JSON penting lainnya untuk dikonfigurasi, lihat skema templat Amazon FSx (Windows).

Pelajari selengkapnya

Untuk mempelajari lebih lanjut tentang mengintegrasikan Amazon Kendra dengan sumber data Amazon FSx (Windows) Anda, lihat:

- Cari data tidak terstruktur dengan aman pada sistem file Windows dengan Amazon Kendra konektor untuk Amazon FSx (Windows) untuk. Windows File Server

Amazon FSx (NetApp ONTAP)

Amazon FSx (NetApp ONTAP) adalah sistem server file berbasis cloud yang dikelola sepenuhnya yang menawarkan kemampuan penyimpanan bersama. Jika Anda pengguna Amazon FSx (NetApp ONTAP), Anda dapat menggunakan Amazon Kendra untuk mengindeks sumber data Amazon FSx (NetApp ONTAP) Anda.

Anda dapat terhubung Amazon Kendra ke sumber data Amazon FSx (NetApp ONTAP) menggunakan Amazon Kendra konsol, atau TemplateConfigurationAPI.

Untuk memecahkan masalah konektor sumber data Amazon Kendra Amazon FSx (NetApp ONTAP) Anda, lihat. Mengatasi masalah sumber data

Topik

- Fitur yang didukung
- Prasyarat
- Instruksi koneksi

Fitur yang didukung

Amazon Kendra Amazon FSx (NetApp ONTAP) konektor sumber data mendukung fitur-fitur berikut:

- Pemetaan lapangan
- Kontrol akses pengguna
- Filter inklusi dan pengecualian
- Sinkronisasi konten penuh dan inkremental
- Cloud privat virtual (VPC)

Prasyarat

Sebelum Anda dapat menggunakan Amazon Kendra untuk mengindeks sumber data Amazon FSx (NetApp ONTAP) Anda, periksa detail Amazon FSx (NetApp ONTAP) Anda dan. Akun AWS

Untuk Amazon FSx (NetApp ONTAP), pastikan Anda memiliki:

- Siapkan Amazon FSx (NetApp ONTAP) dengan izin baca dan pemasangan.

- Mencatat ID sistem file Anda. Anda dapat menemukan ID sistem file Anda di dasbor Sistem File di konsol Amazon FSx (NetApp ONTAP).
- Mencatat ID mesin virtual penyimpanan (SVM) yang digunakan dengan sistem file Anda. Anda dapat menemukan ID SVM Anda dengan membuka dasbor Sistem File di konsol Amazon FSx (NetApp ONTAP), memilih ID sistem file Anda, dan kemudian memilih mesin virtual Penyimpanan.
- Mengonfigurasi cloud pribadi virtual menggunakan Amazon VPC tempat sistem file Amazon FSx (NetApp ONTAP) Anda berada.
- Mencatat kredensi autentikasi Amazon FSx (NetApp ONTAP) Anda untuk akun pengguna. Active Directory Ini termasuk nama pengguna Active Directory Anda dengan nama domain DNS Anda (misalnya, user@corp.example.com) dan kata sandi. Jika Anda menggunakan protokol Network File System (NFS) untuk sistem file Amazon FSx (NetApp ONTAP) Anda, kredensi otentikasi mencakup ID kiri, ID kanan, dan kunci yang telah dibagikan sebelumnya.

  > **Note**
  >
  > Gunakan hanya kredensil yang diperlukan agar konektor berfungsi. Jangan gunakan kredensil istimewa seperti admin domain.

- Memeriksa setiap dokumen unik di Amazon FSx (NetApp ONTAP) dan di seluruh sumber data lain yang Anda rencanakan untuk digunakan untuk indeks yang sama. Setiap sumber data yang ingin Anda gunakan untuk indeks tidak boleh berisi dokumen yang sama di seluruh sumber data. ID dokumen bersifat global untuk indeks dan harus unik per indeks.

Di dalam Anda Akun AWS, pastikan Anda memiliki:

- Membuat Amazon Kendra indeks dan, jika menggunakan API, mencatat ID indeks.
- Membuat IAM peran untuk sumber data Anda dan, jika menggunakan API, catat ARN peran tersebut IAM .

  > **Note**
  >
  > Jika Anda mengubah jenis otentikasi dan kredensialnya, Anda harus memperbarui IAM peran Anda untuk mengakses ID rahasia yang benar AWS Secrets Manager .

- Menyimpan kredensi otentikasi Amazon FSx (NetApp ONTAP) Anda AWS Secrets Manager secara rahasia dan, jika menggunakan API, catat ARN rahasia tersebut.

> **Note**
>
> Kami menyarankan Anda secara teratur menyegarkan atau memutar kredensil dan rahasia Anda. Berikan hanya tingkat akses yang diperlukan untuk keamanan Anda sendiri. Kami tidak menyarankan Anda menggunakan kembali kredensil dan rahasia di seluruh sumber data, dan konektor versi 1.0 dan 2.0 (jika berlaku).

Jika Anda tidak memiliki IAM peran atau rahasia yang ada, Anda dapat menggunakan konsol untuk membuat IAM peran dan Secrets Manager rahasia baru saat menghubungkan sumber data Amazon FSx (NetApp ONTAP) ke Amazon Kendra. Jika Anda menggunakan API, Anda harus memberikan ARN IAM peran dan Secrets Manager rahasia yang ada, dan ID indeks.

Instruksi koneksi

Untuk terhubung Amazon Kendra ke sumber data Amazon FSx (NetApp ONTAP) Anda, Anda harus memberikan rincian yang diperlukan dari sumber data Amazon FSx (NetApp ONTAP) Anda sehingga Amazon Kendra dapat mengakses data Anda. Jika Anda belum mengkonfigurasi Amazon FSx (NetApp ONTAP) untuk Amazon Kendra, lihatPrasyarat.

Console

Untuk terhubung Amazon Kendra ke sistem file Amazon FSx (NetApp ONTAP)

1. Masuk ke AWS Management Console dan buka Amazon Kendra konsol.
2. Dari panel navigasi kiri, pilih Indeks dan kemudian pilih indeks yang ingin Anda gunakan dari daftar indeks.

   > **Note**
   >
   > Anda dapat memilih untuk mengonfigurasi atau mengedit pengaturan kontrol akses Pengguna di bawah Pengaturan indeks.

3. Pada halaman Memulai, pilih Tambahkan sumber data.
4. Pada halaman Tambahkan sumber data, pilih konektor Amazon FSx (NetApp ONTAP), lalu pilih Tambah konektor.
5. Pada halaman Tentukan detail sumber data, masukkan informasi berikut:

a. Dalam Nama dan deskripsi, untuk Nama sumber data —Masukkan nama untuk sumber data Anda. Anda dapat memasukkan tanda hubung tetapi bukan spasi.

b. (Opsional) Deskripsi —Masukkan deskripsi opsional untuk sumber data Anda.

c. Dalam Bahasa default —Pilih bahasa untuk memfilter dokumen Anda untuk indeks. Kecuali Anda menentukan sebaliknya, bahasa default ke bahasa Inggris. Bahasa yang ditentukan dalam metadata dokumen mengesampingkan bahasa yang dipilih.

d. Di Tag, untuk Tambahkan tag baru —Sertakan tag opsional untuk mencari dan memfilter sumber daya Anda atau melacak AWS biaya Anda.

e. Pilih Berikutnya.

6. Pada halaman Tentukan akses dan keamanan, masukkan informasi berikut:

a. Sumber —Berikan informasi sistem file Anda.

- Protokol sistem file —Pilih protokol sistem file Amazon FSx (NetApp ONTAP) Anda. Anda dapat memilih protokol Common Internet File System (CIFS), atau protokol Network File System (NFS) untuk Linux.
- Amazon FSx (NetApp ONTAP) ID sistem file —Pilih dari dropdown ID sistem file Anda yang ada, diambil dari (ONTAP). Amazon FSx NetApp Atau, buat sistem file Amazon FSx (NetApp ONTAP). Anda dapat menemukan ID sistem file Anda di dasbor Sistem File di konsol Amazon FSx (NetApp ONTAP).
- ID SVM (Amazon FSx (NetApp ONTAP) NetApp ONTAP hanya untuk) —Berikan ID mesin virtual penyimpanan (SVM) Anda Amazon FSx (ONTAP). NetApp NetApp ONTAP Anda dapat menemukan ID SVM Anda dengan membuka dasbor Sistem File di konsol Amazon FSx (NetApp ONTAP), memilih ID sistem file Anda, dan memilih mesin virtual Penyimpanan.

b. Otorisasi — Aktifkan atau nonaktifkan informasi daftar kontrol akses (ACL) untuk dokumen Anda, jika Anda memiliki ACL dan ingin menggunakannya untuk kontrol akses. ACL menentukan dokumen mana yang dapat diakses pengguna dan grup. Informasi ACL digunakan untuk memfilter hasil pencarian berdasarkan pengguna atau akses grup mereka ke dokumen. Untuk informasi selengkapnya, lihat Pemfilteran konteks pengguna.

c. Otentikasi —Pilih AWS Secrets Manager rahasia yang ada, atau buat rahasia baru untuk menyimpan kredensi sistem file Anda. Jika Anda memilih untuk membuat rahasia baru, jendela AWS Secrets Manager rahasia terbuka.

Berikan rahasia yang menyimpan kredensi otentikasi Anda atas nama pengguna dan kata sandi Anda. Nama pengguna harus menyertakan nama domain DNS Anda. Misalnya, user@corp.example.com.

Jika Anda menggunakan protokol NFS untuk sistem file Amazon FSx (NetApp ONTAP) Anda, berikan rahasia yang menyimpan kredensi otentikasi Anda dari ID kiri, ID kanan, dan kunci yang telah dibagikan sebelumnya.

Simpan dan tambahkan rahasia Anda.

d. Virtual Private Cloud (VPC) —Anda harus memilih lokasi (ONTAP) Anda Amazon VPC Amazon FSx berada. NetApp Anda menyertakan subnet VPC dan grup keamanan. Lihat Mengkonfigurasi file. Amazon VPC

e. IAM peran —Pilih peran yang ada atau buat IAM IAM peran baru untuk mengakses kredensi repositori dan mengindeks konten.

> **Note**
>
> IAM peran yang digunakan untuk indeks tidak dapat digunakan untuk sumber data. Jika Anda tidak yakin apakah peran yang ada digunakan untuk indeks atau FAQ, pilih Buat peran baru untuk menghindari kesalahan.

f. Pilih Berikutnya.

7. Pada halaman Konfigurasi pengaturan sinkronisasi, masukkan informasi berikut:

a. Lingkup sinkronisasi, pola Regex —Tambahkan pola ekspresi reguler untuk menyertakan atau mengecualikan file tertentu.

b. Mode sinkronisasi —Pilih cara memperbarui indeks saat konten sumber data berubah. Saat Anda menyinkronkan sumber data Amazon Kendra untuk pertama kalinya, semua konten dirayapi dan diindeks secara default. Anda harus menjalankan sinkronisasi penuh data Anda jika sinkronisasi awal Anda gagal, bahkan jika Anda tidak memilih sinkronisasi penuh sebagai opsi mode sinkronisasi Anda.

- Sinkronisasi penuh: Indeks baru semua konten, ganti konten yang ada setiap kali sumber data Anda disinkronkan dengan indeks Anda.
- Sinkronisasi baru, dimodifikasi, dihapus: Indeks hanya konten baru, dimodifikasi, dan dihapus setiap kali sumber data Anda disinkronkan dengan indeks Anda. Amazon

Kendra dapat menggunakan mekanisme sumber data Anda untuk melacak perubahan konten dan mengindeks konten yang berubah sejak sinkronisasi terakhir.

c. Sinkronkan jadwal berjalan —Untuk Frekuensi, pilih seberapa sering menyinkronkan konten sumber data Anda dan memperbarui indeks Anda.

d. Pilih Berikutnya.

8. Pada halaman Setel pemetaan bidang, masukkan informasi berikut:

a. Pilih dari bidang default Amazon Kendra yang dihasilkan dari file Anda yang ingin Anda petakan ke indeks Anda. Untuk menambahkan bidang sumber data kustom, buat nama bidang indeks untuk dipetakan dan tipe data bidang.

b. Pilih Berikutnya.

9. Pada halaman Tinjau dan buat, periksa apakah informasi yang Anda masukkan sudah benar dan kemudian pilih Tambahkan sumber data. Anda juga dapat memilih untuk mengedit informasi Anda dari halaman ini. Sumber data Anda akan muncul di halaman Sumber data setelah sumber data berhasil ditambahkan.

API

Untuk terhubung Amazon Kendra ke sistem file Amazon FSx (NetApp ONTAP)

Anda harus menentukan JSON dari skema sumber data menggunakan API. TemplateConfiguration Anda harus memberikan informasi berikut ini:

- Sumber data —Tentukan tipe sumber data seperti `FSXONTAP` saat Anda menggunakan skema TemplateConfigurationJSON. Tentukan juga sumber data seperti `TEMPLATE` saat Anda memanggil CreateDataSourceAPI.
- ID sistem file —Pengidentifikasi sistem file Amazon FSx (NetApp ONTAP). Anda dapat menemukan ID sistem file Anda di dasbor Sistem File di konsol Amazon FSx (NetApp ONTAP).
- ID SVM —ID mesin virtual penyimpanan (SVM) yang digunakan dengan sistem file Anda. Anda dapat menemukan ID SVM Anda dengan membuka dasbor Sistem File di konsol Amazon FSx (NetApp ONTAP), memilih ID sistem file Anda, dan kemudian memilih mesin virtual Penyimpanan.
- Jenis protokol —Tentukan apakah Anda menggunakan protokol Common Internet File System (CIFS), atau protokol Network File System (NFS) untuk Linux.
- Jenis sistem file —Tentukan jenis sistem file sebagai keduanya`FSXONTAP`.

- Virtual Private Cloud (VPC) **`VpcConfiguration`** —Tentukan kapan Anda menelepon. `CreateDataSource` Untuk informasi selengkapnya, lihat Mengkonfigurasi Amazon Kendra untuk menggunakan Amazon VPC.

  > **Note**
  >
  > Anda harus memilih Amazon VPC tempat Amazon FSx (NetApp ONTAP) Anda berada. Anda menyertakan subnet VPC dan grup keamanan.

- Rahasia Nama Sumber Daya Amazon (ARN) —Berikan Nama Sumber Daya Amazon (ARN) Secrets Manager rahasia yang berisi kredensi otentikasi untuk akun (ONTAP) Anda. Amazon FSx NetApp Rahasianya disimpan dalam struktur JSON dengan kunci berikut:

  ```
  {
      "username": "user@corp.example.com",
      "password": "password"
  }
  ```

  Jika Anda menggunakan protokol NFS untuk sistem file Amazon FSx (NetApp ONTAP) Anda, rahasianya disimpan dalam struktur JSON dengan kunci berikut:

  ```
  {
      "leftId": "left ID",
      "rightId": "right ID",
      "preSharedKey": "pre-shared key"
  }
  ```

- IAM peran —Tentukan `RoleArn` kapan Anda menelepon `CreateDataSource` untuk memberikan IAM peran dengan izin untuk mengakses Secrets Manager rahasia Anda dan memanggil API publik yang diperlukan untuk konektor Amazon FSx (NetApp ONTAP) dan. Amazon Kendra Untuk informasi selengkapnya, lihat IAM peran untuk sumber data Amazon FSx (NetApp ONTAP).

Anda juga dapat menambahkan fitur opsional berikut:

- Mode sinkronisasi —Tentukan cara Amazon Kendra memperbarui indeks Anda saat konten sumber data Anda berubah. Saat Anda menyinkronkan sumber data Amazon Kendra untuk pertama kalinya, semua konten dirayapi dan diindeks secara default. Anda harus menjalankan

sinkronisasi penuh data Anda jika sinkronisasi awal Anda gagal, bahkan jika Anda tidak memilih sinkronisasi penuh sebagai opsi mode sinkronisasi Anda. Anda dapat memilih antara:

- `FORCED_FULL_CRAWL`untuk mengindeks semua konten baru, mengganti konten yang ada setiap kali sumber data Anda disinkronkan dengan indeks Anda.
- `FULL_CRAWL`untuk mengindeks hanya konten baru, dimodifikasi, dan dihapus setiap kali sumber data Anda disinkronkan dengan indeks Anda. Amazon Kendra dapat menggunakan mekanisme sumber data Anda untuk melacak perubahan konten dan mengindeks konten yang berubah sejak sinkronisasi terakhir.

- Filter inklusi dan pengecualian —Tentukan apakah akan menyertakan atau mengecualikan file tertentu.

  > **Note**
  >
  > Sebagian besar sumber data menggunakan pola ekspresi reguler, yang merupakan pola inklusi atau pengecualian yang disebut sebagai filter. Jika Anda menentukan filter inklusi, hanya konten yang cocok dengan filter inklusi yang diindeks. Dokumen apa pun yang tidak cocok dengan filter inklusi tidak diindeks. Jika Anda menentukan filter inklusi dan pengecualian, dokumen yang cocok dengan filter pengecualian tidak akan diindeks, meskipun sesuai dengan filter inklusi.

- Daftar kontrol akses (ACL) —Tentukan apakah akan merayapi informasi ACL untuk dokumen Anda, jika Anda memiliki ACL dan ingin menggunakannya untuk kontrol akses. ACL menentukan dokumen mana yang dapat diakses pengguna dan grup. Informasi ACL digunakan untuk memfilter hasil pencarian berdasarkan pengguna atau akses grup mereka ke dokumen. Untuk informasi selengkapnya, lihat Pemfilteran konteks pengguna.

  > **Note**
  >
  > Untuk menguji pemfilteran konteks pengguna pada pengguna, Anda harus menyertakan nama domain DNS sebagai bagian dari nama pengguna saat mengeluarkan kueri. Anda harus memiliki izin administratif dari domain Active Directory. Anda juga dapat menguji pemfilteran konteks pengguna pada nama grup.

- Pemetaan bidang —Pilih untuk memetakan bidang sumber data Amazon FSx (NetApp ONTAP) Anda ke bidang indeks Anda. Amazon Kendra Untuk informasi lebih lanjut, lihat Memetakan bidang sumber data.

> **Note**
>
> Bidang badan dokumen atau badan dokumen yang setara untuk dokumen Anda diperlukan Amazon Kendra untuk mencari dokumen Anda. Anda harus memetakan nama bidang badan dokumen Anda di sumber data Anda ke nama bidang indeks_`document_body`. Semua kolom lain bersifat opsional.

Untuk daftar kunci JSON penting lainnya untuk dikonfigurasi, lihat skema templat Amazon FSx (NetApp ONTAP).

Amazon RDS/Aurora

Anda dapat mengindeks dokumen yang disimpan dalam database menggunakan sumber data database. Setelah Anda memberikan informasi koneksi untuk database, Amazon Kendra menghubungkan dan mengindeks dokumen.

Amazon Kendra mendukung database berikut:

- Amazon Aurora MySQL
- Amazon Aurora PostgreSQL
- Amazon RDS untuk MySQL
- Amazon RDS untuk PostgreSQL

> **Note**
>
> Database Aurora tanpa server tidak didukung.

> **Important**
>
> Konektor Amazon RDS/Aurora ini dijadwalkan untuk penghentian pada akhir 2023. Amazon Kendra sekarang mendukung konektor sumber data database baru. Untuk pengalaman yang lebih baik, kami sarankan Anda memilih dari konektor baru berikut untuk kasus penggunaan Anda:

- Aurora (MySQL)
- Aurora (PostgreSQL)
- Amazon RDS (MySQL)
- Amazon RDS (Server Microsoft SQL)
- Amazon RDS (Oracle)
- Amazon RDS (PostgreSQL)
- IBM DB2
- Microsoft SQL Server
- MySQL
- Database Oracle
- PostgreSQL

Anda dapat terhubung Amazon Kendra ke sumber data database Anda menggunakan Amazon Kendra konsol dan DatabaseConfigurationAPI.

Untuk memecahkan masalah konektor sumber data Amazon Kendra database Anda, lihat. Mengatasi masalah sumber data

Topik

- Fitur yang didukung
- Prasyarat
- Instruksi koneksi

Fitur yang didukung

Amazon Kendra konektor sumber data database mendukung fitur-fitur berikut:

- Pemetaan lapangan
- Pemfilteran konteks pengguna
- Cloud privat virtual (VPC)

Prasyarat

Sebelum Anda dapat menggunakan Amazon Kendra untuk mengindeks sumber data database Anda, buat perubahan ini di database dan AWS akun Anda.

Dalam database Anda, pastikan Anda memiliki:

- Mencatat kredensi otentikasi dasar Anda dari nama pengguna dan kata sandi untuk database Anda.
- Menyalin nama host, nomor port, alamat host, nama database, dan nama tabel data yang berisi data dokumen. Untuk PostgreSQL, tabel data harus berupa tabel publik atau skema publik.

> **Note**
>
> Host dan port memberi tahu Amazon Kendra di mana menemukan server database di internet. Nama database dan nama tabel memberi tahu Amazon Kendra di mana menemukan data dokumen di server database.

- Menyalin nama kolom dalam tabel data yang berisi data dokumen. Anda harus menyertakan ID dokumen, badan dokumen, kolom untuk mendeteksi apakah dokumen telah berubah (misalnya, kolom terakhir diperbarui), dan kolom tabel data opsional yang dipetakan ke bidang indeks kustom. Anda juga dapat memetakan salah satu nama bidang yang Amazon Kendra dicadangkan ke kolom tabel.
- Menyalin informasi jenis mesin database seperti apakah Anda menggunakan Amazon RDS untuk MySQL atau jenis lain.
- Memeriksa setiap dokumen unik dalam database dan di seluruh sumber data lain yang Anda rencanakan untuk digunakan untuk indeks yang sama. Setiap sumber data yang ingin Anda gunakan untuk indeks tidak boleh berisi dokumen yang sama di seluruh sumber data. ID dokumen bersifat global untuk indeks dan harus unik per indeks.

Di dalam Anda Akun AWS, pastikan Anda memiliki:

- Membuat Amazon Kendra indeks dan, jika menggunakan API, mencatat ID indeks.
- Membuat IAM peran untuk sumber data Anda dan, jika menggunakan API, catat ARN peran tersebut IAM .

> **Note**
>
> Jika Anda mengubah jenis otentikasi dan kredensyal, Anda harus memperbarui IAM peran Anda untuk mengakses ID rahasia yang benar AWS Secrets Manager .

- Menyimpan kredensi otentikasi database Anda AWS Secrets Manager secara rahasia dan, jika menggunakan API, catat ARN rahasia tersebut.

> **Note**
>
> Kami menyarankan Anda secara teratur menyegarkan atau memutar kredensil dan rahasia Anda. Berikan hanya tingkat akses yang diperlukan untuk keamanan Anda sendiri. Kami tidak menyarankan Anda menggunakan kembali kredensyal dan rahasia di seluruh sumber data, dan konektor versi 1.0 dan 2.0 (jika berlaku).

Jika Anda tidak memiliki IAM peran atau rahasia yang ada, Anda dapat menggunakan konsol untuk membuat IAM peran dan Secrets Manager rahasia baru saat Anda menghubungkan sumber data database Anda Amazon Kendra. Jika Anda menggunakan API, Anda harus memberikan ARN IAM peran dan Secrets Manager rahasia yang ada, dan ID indeks.

Instruksi koneksi

Untuk terhubung Amazon Kendra ke sumber data database Anda, Anda harus memberikan rincian yang diperlukan dari sumber data database Anda sehingga Amazon Kendra dapat mengakses data Anda. Jika Anda belum mengkonfigurasi database untuk Amazon Kendra, lihatPrasyarat.

Console

Untuk terhubung Amazon Kendra ke database

1. Masuk ke AWS Management Console dan buka Amazon Kendra konsol.
2. Dari panel navigasi kiri, pilih Indeks dan kemudian pilih indeks yang ingin Anda gunakan dari daftar indeks.

> **Note**
>
> Anda dapat memilih untuk mengonfigurasi atau mengedit pengaturan kontrol akses Pengguna Anda di bawah Pengaturan indeks.

3. Pada halaman Memulai, pilih Tambahkan sumber data.
4. Pada halaman Tambah sumber data, pilih konektor database, lalu pilih Tambah konektor.
5. Pada halaman Tentukan detail sumber data, masukkan informasi berikut:

   a. Dalam Nama dan deskripsi, untuk Nama sumber data —Masukkan nama untuk sumber data Anda. Anda dapat memasukkan tanda hubung tetapi bukan spasi.

   b. (Opsional) Deskripsi —Masukkan deskripsi opsional untuk sumber data Anda.

   c. Dalam Bahasa default —Pilih bahasa untuk memfilter dokumen Anda untuk indeks. Kecuali Anda menentukan sebaliknya, bahasa default ke bahasa Inggris. Bahasa yang ditentukan dalam metadata dokumen mengesampingkan bahasa yang dipilih.

   d. Di Tag, untuk Tambahkan tag baru —Sertakan tag opsional untuk mencari dan memfilter sumber daya Anda atau melacak AWS biaya Anda.

   e. Pilih Berikutnya.

6. Pada halaman Tentukan akses dan keamanan, masukkan informasi berikut:

   a. Endpoint — Nama host DNS, alamat IPv4, atau alamat IPv6.

   b. Port —Nomor port.

   c. Database —Nama database.

   d. Nama tabel —Nama tabel.

   e. Untuk Jenis otentikasi, pilih antara Existing dan New untuk menyimpan kredensyal otentikasi database Anda. Jika Anda memilih untuk membuat rahasia baru, jendela AWS Secrets Manager rahasia terbuka.

      - Masukkan informasi berikut di jendela Buat AWS Secrets Manager rahasia:

        A. Nama rahasia —Nama untuk rahasiamu. Awalan 'AmazonKendra-database-' secara otomatis ditambahkan ke nama rahasia Anda.

        B. Untuk Nama Pengguna dan Kata Sandi —Masukkan nilai kredensi otentikasi dari akun database Anda.

        C. Pilih Simpan otentikasi.

f. Virtual Private Cloud (VPC) —Anda dapat memilih untuk menggunakan VPC. Jika demikian, Anda harus menambahkan Subnet dan grup keamanan VPC.

> **Note**
>
> Anda harus menggunakan subnet pribadi. Jika instans RDS Anda berada di subnet publik di VPC Anda, Anda dapat membuat subnet pribadi yang memiliki akses keluar ke gateway NAT di subnet publik. Subnet yang disediakan dalam konfigurasi VPC harus berada di AS Barat (Oregon), AS Timur (Virginia N.), UE (Irlandia).

g. IAM peran —Pilih peran yang sudah ada atau buat IAM IAM peran baru untuk mengakses kredensi repositori dan mengindeks konten Anda.

> **Note**
>
> IAM peran yang digunakan untuk indeks tidak dapat digunakan untuk sumber data. Jika Anda tidak yakin apakah peran yang ada digunakan untuk indeks atau FAQ, pilih Buat peran baru untuk menghindari kesalahan.

h. Pilih Berikutnya.

7. Pada halaman Konfigurasi pengaturan sinkronisasi, masukkan informasi berikut:

   a. Pilih antara Aurora MySQL, MySQL, Aurora PostgreSQL, dan PostgreSQL berdasarkan kasus penggunaan Anda.

   b. Lampirkan pengidentifikasi SQL dengan tanda kutip ganda —Pilih untuk melampirkan pengidentifikasi SQL dalam tanda kutip ganda. Misalnya, “ColumnName”.

   c. Kolom ACL dan Ubah kolom pendeteksi —Konfigurasikan kolom yang Amazon Kendra digunakan untuk deteksi perubahan (misalnya, kolom yang terakhir diperbarui) dan daftar kontrol akses Anda.

   d. Di Jadwal berjalan Sinkronisasi, untuk Frekuensi —Pilih seberapa sering Amazon Kendra akan disinkronkan dengan sumber data Anda.

   e. Pilih Berikutnya.

8. Pada halaman Setel pemetaan bidang, masukkan informasi berikut:

a. Amazon Kendra pemetaan bidang default —Pilih dari bidang sumber data default Amazon Kendra yang dihasilkan yang ingin Anda petakan ke indeks Anda. Anda harus menambahkan nilai kolom Database untuk `document_id` dan `document_body`

b. Pemetaan bidang kustom —Untuk menambahkan bidang sumber data kustom untuk membuat nama bidang indeks untuk dipetakan dan tipe data bidang.

c. Pilih Berikutnya.

9. Pada halaman Tinjau dan buat, periksa apakah informasi yang Anda masukkan sudah benar dan kemudian pilih Tambahkan sumber data. Anda juga dapat memilih untuk mengedit informasi Anda dari halaman ini. Sumber data Anda akan muncul di halaman Sumber data setelah sumber data berhasil ditambahkan.

API

Untuk terhubung Amazon Kendra ke database

Anda harus menentukan DatabaseConfigurationAPI berikut ini:

- ColumnConfiguration—Informasi tentang di mana indeks harus mendapatkan informasi dokumen dari database. Untuk detail selengkapnya, lihat ColumnConfiguration. Anda harus menentukan bidang `DocumentDataColumnName` (badan dokumen atau teks utama) dan`DocumentIdColumnName`, dan `ChangeDetectingColumn` (misalnya, kolom yang diperbarui terakhir). Kolom yang dipetakan ke bidang `DocumentIdColumnName` harus berupa kolom integer. Contoh berikut menunjukkan konfigurasi kolom sederhana untuk sumber data database:

```
"ColumnConfiguration": {
    "ChangeDetectingColumns": [
        "LastUpdateDate",
        "LastUpdateTime"
    ],
    "DocumentDataColumnName": "TextColumn",
    "DocumentIdColumnName": "IdentifierColumn",
    "DocoumentTitleColumnName": "TitleColumn",
    "FieldMappings": [
        {
            "DataSourceFieldName": "AbstractColumn",
            "IndexFieldName": "Abstract"
        }
```

```
    ]
}
```

- ConnectionConfigurationKonfigurasi informasi yang diperlukan untuk terhubung ke database. Untuk detail selengkapnya, lihat ConnectionConfiguration.
- DatabaseEngineType—Jenis mesin database yang menjalankan database. `DatabaseHost`Bidang untuk `ConnectionConfiguration` harus berupa titik akhir instance Amazon Relational Database Service (Amazon RDS) untuk database. Jangan gunakan titik akhir klaster.
- Rahasia Nama Sumber Daya Amazon (ARN) —Berikan Nama Sumber Daya Amazon (ARN) Secrets Manager rahasia yang berisi kredensyal otentikasi untuk akun database Anda. Rahasianya disimpan dalam struktur JSON dengan kunci berikut:

```
{
    "username": "user name",
    "password": "password"
}
```

Contoh berikut menunjukkan konfigurasi database, termasuk ARN rahasia.

```
"DatabaseConfiguration": {
"ConnectionConfiguration": {
"DatabaseHost": "host.subdomain.domain.tld",
        "DatabaseName": "DocumentDatabase",
        "DatabasePort": 3306,
        "SecretArn": "arn:aws:secretmanager:region:account ID:secret/secret name",
        "TableName": "DocumentTable"
    }
}
```

> **Note**
>
> Kami menyarankan Anda secara teratur menyegarkan atau memutar kredensil dan rahasia Anda. Berikan hanya tingkat akses yang diperlukan untuk keamanan Anda sendiri. Kami tidak menyarankan Anda menggunakan kembali kredensyal dan rahasia di seluruh sumber data, dan konektor versi 1.0 dan 2.0 (jika berlaku).

- IAM peran —Tentukan `RoleArn` kapan Anda memanggil `CreateDataSource` untuk memberikan IAM peran dengan izin untuk mengakses Secrets Manager rahasia Anda dan memanggil API publik yang diperlukan untuk konektor database dan. Amazon Kendra Untuk informasi selengkapnya, lihat IAM peran untuk sumber data database.

Anda juga dapat menambahkan fitur opsional berikut:

- Virtual Private Cloud (VPC) —Tentukan `VpcConfiguration` sebagai bagian dari konfigurasi sumber data. Lihat Mengkonfigurasi Amazon Kendra untuk menggunakan VPC.

> **Note**
>
> Anda hanya perlu menggunakan subnet pribadi. Jika instans RDS Anda berada di subnet publik di VPC Anda, Anda dapat membuat subnet pribadi yang memiliki akses keluar ke gateway NAT di subnet publik. Subnet yang disediakan dalam konfigurasi VPC harus berada di AS Barat (Oregon), AS Timur (Virginia N.), UE (Irlandia).

- Pemetaan bidang —Pilih untuk memetakan bidang sumber data database Anda ke bidang indeks Anda Amazon Kendra . Untuk informasi lebih lanjut, lihat Memetakan bidang sumber data.

> **Note**
>
> Bidang badan dokumen atau badan dokumen yang setara untuk dokumen Anda diperlukan Amazon Kendra untuk mencari dokumen Anda. Anda harus memetakan nama bidang badan dokumen Anda di sumber data Anda ke nama bidang `indeks_document_body`. Semua kolom lain bersifat opsional.

- Pemfilteran konteks pengguna dan kontrol akses —Amazon Kendra meng-crawl daftar kontrol akses (ACL) untuk dokumen Anda, jika Anda memiliki ACL untuk dokumen Anda. Informasi ACL digunakan untuk memfilter hasil pencarian berdasarkan pengguna atau akses grup mereka ke dokumen. Untuk informasi selengkapnya, lihat Pemfilteran konteks pengguna.

Amazon RDS (Microsoft SQL Server)

SQL Server adalah sistem manajemen basis data yang dikembangkan oleh Microsoft. Amazon RDS untuk SQL Server memudahkan untuk mengatur, mengoperasikan, dan menskalakan penyebaran

SQL Server di cloud. Jika Anda adalah pengguna Amazon RDS (Microsoft SQL Server), Anda dapat menggunakan Amazon Kendra untuk mengindeks sumber data Amazon RDS (Microsoft SQL Server) Anda. Konektor sumber data Amazon Kendra JDBC mendukung Microsoft SQL Server 2019.

Anda dapat terhubung Amazon Kendra ke sumber data Amazon RDS (Microsoft SQL Server) menggunakan Amazon Kendra konsol dan TemplateConfigurationAPI.

Untuk memecahkan masalah konektor sumber data (Amazon Kendra Amazon RDS Microsoft SQL Server), lihat. Mengatasi masalah sumber data

Topik

Fitur yang didukung

- Pemetaan lapangan
- Pemfilteran konteks pengguna
- Filter inklusi/pengecualian
- Sinkronisasi konten penuh dan tambahan
- Cloud privat virtual (VPC)

Prasyarat

Sebelum Anda dapat menggunakan Amazon Kendra untuk mengindeks sumber data Amazon RDS (Microsoft SQL Server) Anda, buat perubahan ini di Amazon RDS (Microsoft SQL Server) dan AWS akun Anda.

Di Amazon RDS (Microsoft SQL Server), pastikan Anda memiliki:

- Mencatat nama pengguna dan kata sandi database Anda.

> **Important**
>
> Sebagai praktik terbaik, sediakan Amazon Kendra kredensil basis data hanya-baca.

- Menyalin url, port, dan instance host database Anda.
- Memeriksa setiap dokumen unik di Amazon RDS (Microsoft SQL Server) dan di seluruh sumber data lain yang Anda rencanakan untuk digunakan untuk indeks yang sama. Setiap sumber data yang ingin Anda gunakan untuk indeks tidak boleh berisi dokumen yang sama di seluruh sumber data. ID dokumen bersifat global untuk indeks dan harus unik per indeks.

Di dalam Anda Akun AWS, pastikan Anda memiliki:

- Membuat Amazon Kendra indeks dan, jika menggunakan API, mencatat ID indeks.
- Membuat IAM peran untuk sumber data Anda dan, jika menggunakan API, catat ARN peran tersebut IAM .

> **Note**
>
> Jika Anda mengubah jenis otentikasi dan kredensyal, Anda harus memperbarui IAM peran Anda untuk mengakses ID rahasia yang benar AWS Secrets Manager .

- Menyimpan kredensi otentikasi Amazon RDS (Microsoft SQL Server) Anda secara AWS Secrets Manager rahasia dan, jika menggunakan API, catat ARN rahasianya.

> **Note**
>
> Kami menyarankan Anda secara teratur menyegarkan atau memutar kredensil dan rahasia Anda. Berikan hanya tingkat akses yang diperlukan untuk keamanan Anda sendiri. Kami tidak menyarankan Anda menggunakan kembali kredensyal dan rahasia di seluruh sumber data, dan konektor versi 1.0 dan 2.0 (jika berlaku).

Jika Anda tidak memiliki IAM peran atau rahasia yang ada, Anda dapat menggunakan konsol untuk membuat IAM peran dan Secrets Manager rahasia baru saat menghubungkan sumber data Amazon RDS (Microsoft SQL Server) ke Amazon Kendra. Jika Anda menggunakan API, Anda harus memberikan ARN IAM peran dan Secrets Manager rahasia yang ada, dan ID indeks.

Instruksi koneksi

Untuk terhubung Amazon Kendra ke sumber data Amazon RDS (Microsoft SQL Server) Anda harus memberikan rincian kredensyal Amazon RDS (Microsoft SQL Server) Anda sehingga Amazon Kendra dapat mengakses data Anda. Jika Anda belum mengkonfigurasi Amazon RDS (Microsoft SQL Server) untuk Amazon Kendra lihatPrasyarat.

Console

Untuk terhubung Amazon Kendra ke Amazon RDS (Microsoft SQL Server)

1. Masuk ke AWS Management Console dan buka Amazon Kendra konsol.
2. Dari panel navigasi kiri, pilih Indeks dan kemudian pilih indeks yang ingin Anda gunakan dari daftar indeks.

> **Note**
>
> Anda dapat memilih untuk mengonfigurasi atau mengedit pengaturan kontrol akses Pengguna Anda di bawah Pengaturan indeks.

3. Pada halaman Memulai, pilih Tambahkan sumber data.
4. Pada halaman Tambah sumber data, pilih konektor Amazon RDS (Microsoft SQL Server), lalu pilih Tambah konektor.
5. Pada halaman Tentukan detail sumber data, masukkan informasi berikut:
   a. Di Nama dan deskripsi, untuk Nama sumber data —Masukkan nama untuk sumber data Anda. Anda dapat memasukkan tanda hubung tetapi bukan spasi.
   b. (Opsional) Deskripsi —Masukkan deskripsi opsional untuk sumber data Anda.
   c. Dalam Bahasa default —Pilih bahasa untuk memfilter dokumen Anda untuk indeks. Kecuali Anda menentukan sebaliknya, bahasa default ke bahasa Inggris. Bahasa yang ditentukan dalam metadata dokumen mengesampingkan bahasa yang dipilih.
   d. Di Tag, untuk Tambahkan tag baru —Sertakan tag opsional untuk mencari dan memfilter sumber daya Anda atau melacak AWS biaya Anda.
   e. Pilih Berikutnya.
6. Pada halaman Tentukan akses dan keamanan, masukkan informasi berikut:
   a. Di Sumber, masukkan informasi berikut:

b. Host — Masukkan nama host database.

c. Port — Masukkan port database.

d. Instance - Masukkan instance database.

e. Aktifkan lokasi sertifikat SSL —Pilih untuk memasukkan Amazon S3 jalur ke file sertifikat SSL Anda.

f. Dalam Otentikasi —masukkan informasi berikut:

- AWS Secrets Manager rahasia —Pilih rahasia yang ada atau buat Secrets Manager rahasia baru untuk menyimpan kredensyal otentikasi Amazon RDS (Microsoft SQL Server) Anda. Jika Anda memilih untuk membuat rahasia baru, jendela AWS Secrets Manager rahasia terbuka.

  A. Masukkan informasi berikut di jendela Buat AWS Secrets Manager rahasia:

     I. Nama rahasia —Nama untuk rahasiamu. Awalan 'AmazonKendra-Amazon RDS (Microsoft SQL Server) -' secara otomatis ditambahkan ke nama rahasia Anda.

     II. Untuk nama pengguna Database, dan Kata Sandi —Masukkan nilai kredensi otentikasi yang Anda salin dari database Anda.

  B. Pilih Simpan.

g. Virtual Private Cloud (VPC) —Anda dapat memilih untuk menggunakan VPC. Jika demikian, Anda harus menambahkan Subnet dan grup keamanan VPC.

h. IAM peran —Pilih peran yang sudah ada atau buat IAM IAM peran baru untuk mengakses kredensi repositori dan mengindeks konten Anda.

> **Note**
>
> IAM peran yang digunakan untuk indeks tidak dapat digunakan untuk sumber data. Jika Anda tidak yakin apakah peran yang ada digunakan untuk indeks atau FAQ, pilih Buat peran baru untuk menghindari kesalahan.

i. Pilih Berikutnya.

7. Pada halaman Konfigurasi pengaturan sinkronisasi, masukkan informasi berikut:

   a. Dalam lingkup Sinkronisasi, pilih dari opsi berikut:

- Kueri SQL —Masukkan pernyataan kueri SQL seperti operasi SELECT dan JOIN. Kueri SQL harus kurang dari 32KB. Amazon Kendra akan merayapi semua konten database yang cocok dengan kueri Anda.

  > **Note**
  >
  > Jika nama tabel menyertakan karakter khusus (non alfanumerik) dalam nama, Anda harus menggunakan tanda kurung siku di sekitar nama tabel. Misalnya, *pilih * dari [my-database-table]*

- Kolom kunci primer —Berikan kunci utama untuk tabel database. Ini mengidentifikasi tabel dalam database Anda.
- Judul kolom —Berikan nama kolom judul dokumen dalam tabel database Anda.
- Kolom tubuh —Berikan nama kolom badan dokumen dalam tabel database Anda.

b. Dalam Konfigurasi tambahan — opsional, pilih dari opsi berikut untuk menyinkronkan konten tertentu alih-alih menyinkronkan semua file:

- Kolom pendeteksi perubahan —Masukkan nama kolom yang Amazon Kendra akan digunakan untuk mendeteksi perubahan konten. Amazon Kendra akan mengindeks ulang konten ketika ada perubahan di salah satu kolom ini.
- Kolom ID Pengguna —Masukkan nama kolom yang berisi ID Pengguna agar diizinkan mengakses konten.
- Kolom Grup —Masukkan nama kolom yang berisi grup untuk diizinkan mengakses konten.
- Kolom URL sumber —Masukkan nama kolom yang berisi URL Sumber yang akan diindeks.
- Kolom stempel waktu —Masukkan nama kolom yang berisi stempel waktu. Amazon Kendra menggunakan informasi cap waktu untuk mendeteksi perubahan dalam konten Anda dan hanya menyinkronkan konten yang diubah.
- Kolom zona waktu —Masukkan nama kolom yang berisi zona waktu untuk konten yang akan dirayapi.
- Format stempel waktu —Masukkan nama kolom yang berisi format cap waktu yang akan digunakan untuk mendeteksi perubahan konten dan menyinkronkan ulang konten Anda.

c. Mode sinkronisasi —Pilih cara Anda ingin memperbarui indeks saat konten sumber data Anda berubah. Saat Anda menyinkronkan sumber data Amazon Kendra untuk pertama kalinya, semua konten dirayapi dan diindeks secara default. Anda harus menjalankan sinkronisasi penuh data Anda jika sinkronisasi awal Anda gagal, bahkan jika Anda tidak memilih sinkronisasi penuh sebagai opsi mode sinkronisasi Anda.

   - Sinkronisasi penuh: Indeks baru semua konten, ganti konten yang ada setiap kali sumber data Anda disinkronkan dengan indeks Anda.
   - Sinkronisasi baru yang dimodifikasi: Indeks hanya konten baru dan yang dimodifikasi setiap kali sumber data Anda disinkronkan dengan indeks Anda. Amazon Kendra dapat menggunakan mekanisme sumber data Anda untuk melacak perubahan konten dan mengindeks konten yang berubah sejak sinkronisasi terakhir.
   - Sinkronisasi baru, dimodifikasi, dihapus: Indeks hanya konten baru, dimodifikasi, dan dihapus setiap kali sumber data Anda disinkronkan dengan indeks Anda. Amazon Kendra dapat menggunakan mekanisme sumber data Anda untuk melacak perubahan konten dan mengindeks konten yang berubah sejak sinkronisasi terakhir.

d. Dalam jadwal berjalan Sinkronisasi, untuk Frekuensi —Seberapa sering Amazon Kendra akan disinkronkan dengan sumber data Anda.

e. Pilih Berikutnya.

8. Pada halaman Setel pemetaan bidang, masukkan informasi berikut:

   a. Pilih dari bidang sumber data default yang dihasilkan - ID dokumen, judul dokumen, dan URL Sumber - yang ingin Anda petakan ke Amazon Kendra indeks.

   b. Tambahkan bidang —Untuk menambahkan bidang sumber data kustom untuk membuat nama bidang indeks untuk dipetakan dan tipe data bidang.

   c. Pilih Berikutnya.

9. Pada halaman Tinjau dan buat, periksa apakah informasi yang Anda masukkan sudah benar dan kemudian pilih Tambahkan sumber data. Anda juga dapat memilih untuk mengedit informasi Anda dari halaman ini. Sumber data Anda akan muncul di halaman Sumber data setelah sumber data berhasil ditambahkan.

API

Untuk terhubung Amazon Kendra ke Amazon RDS (Microsoft SQL Server)

Anda harus menentukan yang berikut menggunakan TemplateConfigurationAPI:

- Sumber data —Tentukan tipe sumber data seperti `JDBC` saat Anda menggunakan skema TemplateConfigurationJSON. Tentukan juga sumber data seperti `TEMPLATE` saat Anda memanggil CreateDataSourceAPI.
- Jenis database —Anda harus menentukan jenis database sebagai`sqlserver`.
- Kueri SQL —Tentukan pernyataan kueri SQL seperti operasi SELECT dan JOIN. Kueri SQL harus kurang dari 32KB. Amazon Kendra akan merayapi semua konten database yang cocok dengan kueri Anda.

  > **Note**
  >
  > Jika nama tabel menyertakan karakter khusus (non alfanumerik) dalam nama, Anda harus menggunakan tanda kurung siku di sekitar nama tabel. Misalnya, *`pilih * dari [my-database-table]`*

- Mode sinkronisasi —Tentukan cara Amazon Kendra memperbarui indeks Anda saat konten sumber data Anda berubah. Saat Anda menyinkronkan sumber data Amazon Kendra untuk pertama kalinya, semua konten dirayapi dan diindeks secara default. Anda harus menjalankan sinkronisasi penuh data Anda jika sinkronisasi awal Anda gagal, bahkan jika Anda tidak memilih sinkronisasi penuh sebagai opsi mode sinkronisasi Anda. Anda dapat memilih antara:
  - `FORCED_FULL_CRAWL`untuk mengindeks semua konten baru, mengganti konten yang ada setiap kali sumber data Anda disinkronkan dengan indeks Anda.
  - `FULL_CRAWL`untuk mengindeks hanya konten baru, dimodifikasi, dan dihapus setiap kali sumber data Anda disinkronkan dengan indeks Anda. Amazon Kendra dapat menggunakan mekanisme sumber data Anda untuk melacak perubahan konten dan mengindeks konten yang berubah sejak sinkronisasi terakhir.
  - `CHANGE_LOG`untuk mengindeks hanya konten baru dan yang dimodifikasi setiap kali sumber data Anda disinkronkan dengan indeks Anda. Amazon Kendra dapat menggunakan mekanisme sumber data Anda untuk melacak perubahan konten dan mengindeks konten yang berubah sejak sinkronisasi terakhir.
- Rahasia Nama Sumber Daya Amazon (ARN) —Berikan Nama Sumber Daya Amazon (ARN) Secrets Manager rahasia yang berisi kredensyal otentikasi yang Anda buat di akun (Microsoft SQL Server) Anda Amazon RDS . Rahasianya disimpan dalam struktur JSON dengan kunci berikut:

```
{
    "user name": "database user name",
```

```
    "password": "password"
}
```

> **Note**
>
> Kami menyarankan Anda secara teratur menyegarkan atau memutar kredensil dan rahasia Anda. Berikan hanya tingkat akses yang diperlukan untuk keamanan Anda sendiri. Kami tidak menyarankan Anda menggunakan kembali kredensyal dan rahasia di seluruh sumber data, dan konektor versi 1.0 dan 2.0 (jika berlaku).

- IAM peran —Tentukan `RoleArn` kapan Anda memanggil `CreateDataSource` untuk memberikan IAM peran dengan izin untuk mengakses Secrets Manager rahasia Anda dan memanggil API publik yang diperlukan untuk konektor (Amazon RDS Microsoft SQL Server) dan. Amazon Kendra Untuk informasi selengkapnya, lihat IAM peran untuk sumber data Amazon RDS (Microsoft SQL Server).

Anda juga dapat menambahkan fitur opsional berikut:

- Virtual Private Cloud (VPC) **`VpcConfiguration`** —Tentukan kapan Anda menelepon. `CreateDataSource` Untuk informasi selengkapnya, lihat Mengkonfigurasi Amazon Kendra untuk menggunakan Amazon VPC.
- Filter penyertaan dan pengecualian —Anda dapat menentukan apakah akan menyertakan konten tertentu menggunakan ID pengguna, grup, URL sumber, stempel waktu, dan zona waktu.
- Pemfilteran konteks pengguna dan kontrol akses —Amazon Kendra meng-crawl daftar kontrol akses (ACL) untuk dokumen Anda, jika Anda memiliki ACL untuk dokumen Anda. Informasi ACL digunakan untuk memfilter hasil pencarian berdasarkan pengguna atau akses grup mereka ke dokumen. Untuk informasi selengkapnya, lihat Pemfilteran konteks pengguna.
- Pemetaan bidang —Pilih untuk memetakan bidang sumber data (Amazon RDS Microsoft SQL Server) Anda ke bidang indeks Anda. Amazon Kendra Untuk informasi lebih lanjut, lihat Memetakan bidang sumber data.

> **Note**
>
> Bidang badan dokumen atau badan dokumen yang setara untuk dokumen Anda diperlukan Amazon Kendra untuk mencari dokumen Anda. Anda harus memetakan

nama bidang badan dokumen Anda di sumber data Anda ke nama bidang indeks_`document_body`. Semua kolom lain bersifat opsional.

Untuk daftar kunci JSON penting lainnya untuk dikonfigurasi, lihatAmazon RDS Skema templat (Microsoft SQL Server).

Catatan

- Baris database yang dihapus tidak akan dilacak saat Amazon Kendra memeriksa konten yang diperbarui.
- Ukuran nama bidang dan nilai dalam deretan database Anda tidak dapat melebihi 400KB.
- Jika Anda memiliki sejumlah besar data dalam sumber data database Anda, dan tidak Amazon Kendra ingin mengindeks semua konten database Anda setelah sinkronisasi pertama, Anda dapat memilih untuk menyinkronkan hanya dokumen baru, dimodifikasi, atau dihapus.
- Sebagai praktik terbaik, sediakan Amazon Kendra kredensil basis data hanya-baca.
- Sebagai praktik terbaik, hindari menambahkan tabel dengan data sensitif atau informasi identitas pribadi (PII).

Amazon RDS (MySQL)

Amazon RDS (Amazon Relational Database Service) adalah layanan web yang memudahkan pengaturan, pengoperasian, dan skala database relasional di AWS Cloud. Jika Anda adalah Amazon RDS pengguna, Anda dapat menggunakan Amazon Kendra untuk mengindeks sumber Amazon RDS (MySQL) data Anda. Konektor sumber Amazon Kendra data mendukung Amazon RDS MySql 5.6, 5.7, dan 8.0.

Anda dapat terhubung Amazon Kendra ke sumber Amazon RDS (MySQL) data menggunakan Amazon Kendra konsol dan TemplateConfigurationAPI.

Untuk memecahkan masalah konektor sumber Amazon Kendra Amazon RDS (MySQL) data Anda, lihat. Mengatasi masalah sumber data

Topik

- Fitur yang didukung
- Prasyarat

- Instruksi koneksi
- Catatan

Fitur yang didukung

- Pemetaan lapangan
- Pemfilteran konteks pengguna
- Filter inklusi/pengecualian
- Sinkronisasi konten penuh dan tambahan
- Cloud privat virtual (VPC)

Prasyarat

Sebelum Anda dapat menggunakan Amazon Kendra untuk mengindeks sumber Amazon RDS (MySQL) data Anda, buat perubahan ini di akun Amazon RDS (MySQL) dan AWS akun Anda.

DiAmazon RDS (MySQL), pastikan Anda memiliki:

- Mencatat nama pengguna dan kata sandi database Anda.

> **Important**
>
> Sebagai praktik terbaik, sediakan Amazon Kendra kredensil basis data hanya-baca.

- Menyalin url, port, dan instance host database Anda. Anda dapat menemukan informasi ini di Amazon RDS konsol.
- Memeriksa setiap dokumen unik di dalam Amazon RDS (MySQL) dan di seluruh sumber data lain yang Anda rencanakan untuk digunakan untuk indeks yang sama. Setiap sumber data yang ingin Anda gunakan untuk indeks tidak boleh berisi dokumen yang sama di seluruh sumber data. ID dokumen bersifat global untuk indeks dan harus unik per indeks.

Di dalam Anda Akun AWS, pastikan Anda memiliki:

- Membuat Amazon Kendra indeks dan, jika menggunakan API, mencatat ID indeks.
- Membuat IAM peran untuk sumber data Anda dan, jika menggunakan API, catat ARN peran tersebut IAM .

> **Note**
>
> Jika Anda mengubah jenis otentikasi dan kredensyal, Anda harus memperbarui IAM peran Anda untuk mengakses ID rahasia yang benar AWS Secrets Manager .

- Menyimpan kredensyal Amazon RDS (MySQL) otentikasi Anda AWS Secrets Manager secara rahasia dan, jika menggunakan API, catat ARN rahasia tersebut.

> **Note**
>
> Kami menyarankan Anda secara teratur menyegarkan atau memutar kredensil dan rahasia Anda. Berikan hanya tingkat akses yang diperlukan untuk keamanan Anda sendiri. Kami tidak menyarankan Anda menggunakan kembali kredensyal dan rahasia di seluruh sumber data, dan konektor versi 1.0 dan 2.0 (jika berlaku).

Jika Anda tidak memiliki IAM peran atau rahasia yang ada, Anda dapat menggunakan konsol untuk membuat IAM peran dan Secrets Manager rahasia baru saat Anda menghubungkan sumber Amazon RDS (MySQL) data Anda Amazon Kendra. Jika Anda menggunakan API, Anda harus memberikan ARN IAM peran dan Secrets Manager rahasia yang ada, dan ID indeks.

Instruksi koneksi

Untuk terhubung Amazon Kendra ke sumber Amazon RDS (MySQL) data Anda, Anda harus memberikan rincian Amazon RDS (MySQL) kredensyal Anda sehingga Amazon Kendra dapat mengakses data Anda. Jika Anda belum mengkonfigurasi Amazon RDS (MySQL) untuk Amazon Kendra lihatPrasyarat.

Console

Untuk terhubung Amazon Kendra ke Amazon RDS (MySQL)

1. Masuk ke AWS Management Console dan buka Amazon Kendra konsol.
2. Dari panel navigasi kiri, pilih Indeks dan kemudian pilih indeks yang ingin Anda gunakan dari daftar indeks.

> **Note**
>
> Anda dapat memilih untuk mengonfigurasi atau mengedit pengaturan kontrol akses Pengguna Anda di bawah Pengaturan indeks.

3. Pada halaman Memulai, pilih Tambahkan sumber data.
4. Pada halaman Tambahkan sumber data, pilih Amazon RDS (MySQL)konektor, lalu pilih Tambah konektor.
5. Pada halaman Tentukan detail sumber data, masukkan informasi berikut:
   a. Di Nama dan deskripsi, untuk Nama sumber data —Masukkan nama untuk sumber data Anda. Anda dapat memasukkan tanda hubung tetapi bukan spasi.
   b. (Opsional) Deskripsi —Masukkan deskripsi opsional untuk sumber data Anda.
   c. Dalam Bahasa default —Pilih bahasa untuk memfilter dokumen Anda untuk indeks. Kecuali Anda menentukan sebaliknya, bahasa default ke bahasa Inggris. Bahasa yang ditentukan dalam metadata dokumen mengesampingkan bahasa yang dipilih.
   d. Di Tag, untuk Tambahkan tag baru —Sertakan tag opsional untuk mencari dan memfilter sumber daya Anda atau melacak AWS biaya Anda.
   e. Pilih Berikutnya.
6. Pada halaman Tentukan akses dan keamanan, masukkan informasi berikut:
   a. Di Sumber, masukkan informasi berikut:
   b. Host — Masukkan URL host database, misalnya:`http://`*`instance URL`*`.`*`region`*`.rds.amazonaws.com`.
   c. Port — Masukkan port database, misalnya,`5432`.
   d. Instance — Masukkan contoh database, misalnya`postgres`.
   e. Aktifkan lokasi sertifikat SSL —Pilih untuk memasukkan Amazon S3 jalur ke file sertifikat SSL Anda.
   f. Dalam Otentikasi —masukkan informasi berikut:
      - AWS Secrets Manager rahasia —Pilih rahasia yang ada atau buat Secrets Manager rahasia baru untuk menyimpan kredensyal Amazon RDS (MySQL) otentikasi Anda. Jika Anda memilih untuk membuat rahasia baru, jendela AWS Secrets Manager rahasia terbuka.

A. Masukkan informasi berikut di jendela Buat AWS Secrets Manager rahasia:

I. Nama rahasia —Nama untuk rahasiamu. Awalan 'AmazonKendra- Amazon RDS (MySQL) -' secara otomatis ditambahkan ke nama rahasia Anda.

II. Untuk nama pengguna Database, dan Kata Sandi —Masukkan nilai kredensi otentikasi yang Anda salin dari database Anda.

B. Pilih Simpan.

g. Virtual Private Cloud (VPC) —Anda dapat memilih untuk menggunakan VPC. Jika demikian, Anda harus menambahkan Subnet dan grup keamanan VPC.

h. IAM peran —Pilih peran yang sudah ada atau buat IAM IAM peran baru untuk mengakses kredensi repositori dan mengindeks konten Anda.

> **Note**
>
> IAM peran yang digunakan untuk indeks tidak dapat digunakan untuk sumber data. Jika Anda tidak yakin apakah peran yang ada digunakan untuk indeks atau FAQ, pilih Buat peran baru untuk menghindari kesalahan.

i. Pilih Berikutnya.

7. Pada halaman Konfigurasi pengaturan sinkronisasi, masukkan informasi berikut:

a. Dalam lingkup Sinkronisasi, pilih dari opsi berikut:

- Kueri SQL —Masukkan pernyataan kueri SQL seperti operasi SELECT dan JOIN. Kueri SQL harus kurang dari 32KB Kueri SQL harus kurang dari 32KB dan tidak mengandung semi-titik dua (;). Amazon Kendra akan merayapi semua konten database yang cocok dengan kueri Anda.
- Kolom kunci primer —Menyediakan kunci utama untuk tabel database. Ini mengidentifikasi tabel dalam database Anda.
- Judul kolom —Berikan nama kolom judul dokumen dalam tabel database Anda.
- Kolom tubuh —Berikan nama kolom badan dokumen dalam tabel database Anda.

b. Dalam Konfigurasi tambahan — opsional, pilih dari opsi berikut untuk menyinkronkan konten tertentu alih-alih menyinkronkan semua file:

- Kolom pendeteksi perubahan —Masukkan nama kolom yang Amazon Kendra akan digunakan untuk mendeteksi perubahan konten. Amazon Kendra akan mengindeks ulang konten ketika ada perubahan di salah satu kolom ini.
- Kolom ID Pengguna —Masukkan nama kolom yang berisi ID Pengguna agar diizinkan mengakses konten.
- Kolom Grup —Masukkan nama kolom yang berisi grup untuk diizinkan mengakses konten.
- Kolom URL sumber —Masukkan nama kolom yang berisi URL Sumber yang akan diindeks.
- Kolom stempel waktu —Masukkan nama kolom yang berisi stempel waktu. Amazon Kendra menggunakan informasi cap waktu untuk mendeteksi perubahan dalam konten Anda dan hanya menyinkronkan konten yang diubah.
- Kolom zona waktu —Masukkan nama kolom yang berisi zona waktu untuk konten yang akan dirayapi.
- Format stempel waktu —Masukkan nama kolom yang berisi format cap waktu yang akan digunakan untuk mendeteksi perubahan konten dan menyinkronkan ulang konten Anda.

c. Mode sinkronisasi —Pilih cara memperbarui indeks saat konten sumber data berubah. Saat Anda menyinkronkan sumber data Amazon Kendra untuk pertama kalinya, semua konten dirayapi dan diindeks secara default. Anda harus menjalankan sinkronisasi penuh data Anda jika sinkronisasi awal Anda gagal, bahkan jika Anda tidak memilih sinkronisasi penuh sebagai opsi mode sinkronisasi Anda.

- Sinkronisasi penuh: Indeks baru semua konten, ganti konten yang ada setiap kali sumber data Anda disinkronkan dengan indeks Anda.
- Sinkronisasi baru yang dimodifikasi: Indeks hanya konten baru dan yang dimodifikasi setiap kali sumber data Anda disinkronkan dengan indeks Anda. Amazon Kendra dapat menggunakan mekanisme sumber data Anda untuk melacak perubahan konten dan mengindeks konten yang berubah sejak sinkronisasi terakhir.
- Sinkronisasi baru, dimodifikasi, dihapus: Indeks hanya konten baru, dimodifikasi, dan dihapus setiap kali sumber data Anda disinkronkan dengan indeks Anda. Amazon Kendra dapat menggunakan mekanisme sumber data Anda untuk melacak perubahan konten dan mengindeks konten yang berubah sejak sinkronisasi terakhir.

d. Dalam jadwal berjalan Sinkronisasi, untuk Frekuensi —Seberapa sering Amazon Kendra akan disinkronkan dengan sumber data Anda.

e. Pilih Berikutnya.

8. Pada halaman Setel pemetaan bidang, masukkan informasi berikut:

a. Pilih dari bidang sumber data default yang dihasilkan— ID Dokumen, Judul dokumen, dan URL Sumber —yang ingin Anda petakan ke Amazon Kendra indeks.

b. Tambahkan bidang —Untuk menambahkan bidang sumber data kustom untuk membuat nama bidang indeks untuk dipetakan dan tipe data bidang.

c. Pilih Berikutnya.

9. Pada halaman Tinjau dan buat, periksa apakah informasi yang Anda masukkan sudah benar dan kemudian pilih Tambahkan sumber data. Anda juga dapat memilih untuk mengedit informasi Anda dari halaman ini. Sumber data Anda akan muncul di halaman Sumber data setelah sumber data berhasil ditambahkan.

API

Untuk terhubung Amazon Kendra ke Amazon RDS (MySQL)

Anda harus menentukan yang berikut menggunakan TemplateConfigurationAPI:

- Sumber data —Tentukan tipe sumber data seperti `JDBC` saat Anda menggunakan skema TemplateConfigurationJSON. Tentukan juga sumber data seperti `TEMPLATE` saat Anda memanggil CreateDataSourceAPI.
- Jenis database —Anda harus menentukan jenis database sebagai`mySql`.
- Kueri SQL —Tentukan pernyataan kueri SQL seperti operasi SELECT dan JOIN. Kueri SQL harus kurang dari 32KB. Amazon Kendra akan merayapi semua konten database yang cocok dengan kueri Anda.
- Mode sinkronisasi —Tentukan cara Amazon Kendra memperbarui indeks Anda saat konten sumber data Anda berubah. Saat Anda menyinkronkan sumber data Amazon Kendra untuk pertama kalinya, semua konten dirayapi dan diindeks secara default. Anda harus menjalankan sinkronisasi penuh data Anda jika sinkronisasi awal Anda gagal, bahkan jika Anda tidak memilih sinkronisasi penuh sebagai opsi mode sinkronisasi Anda. Anda dapat memilih antara:
  - `FORCED_FULL_CRAWL`untuk mengindeks semua konten baru, mengganti konten yang ada setiap kali sumber data Anda disinkronkan dengan indeks Anda.

  - `FULL_CRAWL`untuk mengindeks hanya konten baru, dimodifikasi, dan dihapus setiap kali sumber data Anda disinkronkan dengan indeks Anda. Amazon Kendra dapat menggunakan mekanisme sumber data Anda untuk melacak perubahan konten dan mengindeks konten yang berubah sejak sinkronisasi terakhir.
  - `CHANGE_LOG`untuk mengindeks hanya konten baru dan yang dimodifikasi setiap kali sumber data Anda disinkronkan dengan indeks Anda. Amazon Kendra dapat menggunakan mekanisme sumber data Anda untuk melacak perubahan konten dan mengindeks konten yang berubah sejak sinkronisasi terakhir.
- Rahasia Nama Sumber Daya Amazon (ARN) —Berikan Nama Sumber Daya Amazon (ARN) Secrets Manager rahasia yang berisi kredensyal otentikasi yang Anda buat di akun Anda. Amazon RDS (MySQL) Rahasianya disimpan dalam struktur JSON dengan kunci berikut:

```
{
    "user name": "database user name",
    "password": "password"
}
```

> **Note**
>
> Kami menyarankan Anda secara teratur menyegarkan atau memutar kredensil dan rahasia Anda. Berikan hanya tingkat akses yang diperlukan untuk keamanan Anda sendiri. Kami tidak menyarankan Anda menggunakan kembali kredensyal dan rahasia di seluruh sumber data, dan konektor versi 1.0 dan 2.0 (jika berlaku).

- IAM peran —Tentukan `RoleArn` kapan Anda menelepon `CreateDataSource` untuk memberikan IAM peran dengan izin untuk mengakses Secrets Manager rahasia Anda dan memanggil API publik yang diperlukan untuk Amazon RDS (MySQL) konektor dan. Amazon Kendra Untuk informasi selengkapnya, lihat IAM peran untuk sumber Amazon RDS (MySQL) data.

Anda juga dapat menambahkan fitur opsional berikut:

- Virtual Private Cloud (VPC) **`VpcConfiguration`** —Tentukan kapan Anda menelepon. `CreateDataSource` Untuk informasi selengkapnya, lihat Mengkonfigurasi Amazon Kendra untuk menggunakan Amazon VPC.

- Filter penyertaan dan pengecualian —Anda dapat menentukan apakah akan menyertakan konten tertentu menggunakan ID pengguna, grup, URL sumber, stempel waktu, dan zona waktu.
- Pemetaan bidang —Pilih untuk memetakan bidang sumber Amazon RDS (MySQL) data Anda ke bidang indeks Anda Amazon Kendra . Untuk informasi lebih lanjut, lihat Memetakan bidang sumber data.

> **Note**
>
> Bidang badan dokumen atau badan dokumen yang setara untuk dokumen Anda diperlukan Amazon Kendra untuk mencari dokumen Anda. Anda harus memetakan nama bidang badan dokumen Anda di sumber data Anda ke nama bidang indeks`_document_body`. Semua kolom lain bersifat opsional.

- Pemfilteran konteks pengguna dan kontrol akses —Amazon Kendra meng-crawl daftar kontrol akses (ACL) untuk dokumen Anda, jika Anda memiliki ACL untuk dokumen Anda. Informasi ACL digunakan untuk memfilter hasil pencarian berdasarkan pengguna atau akses grup mereka ke dokumen. Untuk informasi selengkapnya, lihat Pemfilteran konteks pengguna.

Untuk daftar kunci JSON penting lainnya untuk dikonfigurasi, lihatAmazon RDS Skema templat (MySQL).

Catatan

- Baris database yang dihapus tidak akan dilacak saat Amazon Kendra memeriksa konten yang diperbarui.
- Ukuran nama bidang dan nilai dalam deretan database Anda tidak dapat melebihi 400KB.
- Jika Anda memiliki sejumlah besar data dalam sumber data database Anda, dan tidak Amazon Kendra ingin mengindeks semua konten database Anda setelah sinkronisasi pertama, Anda dapat memilih untuk menyinkronkan hanya dokumen baru, dimodifikasi, atau dihapus.
- Sebagai praktik terbaik, sediakan Amazon Kendra kredensil basis data hanya-baca.
- Sebagai praktik terbaik, hindari menambahkan tabel dengan data sensitif atau informasi identitas pribadi (PII).

Amazon RDS (Oracle)

Amazon RDS (Amazon Relational Database Service) adalah layanan web yang membuatnya lebih mudah untuk mengatur, mengoperasikan, dan menskalakan database relasional di AWS Cloud. Jika Anda adalah Amazon RDS (Oracle) pengguna, Anda dapat menggunakan Amazon Kendra untuk mengindeks sumber Amazon RDS (Oracle) data Anda. Konektor sumber Amazon Kendra Amazon RDS (Oracle) data mendukung Amazon RDS Oracle Database 21c, Oracle Database 19c, Oracle Database 12c.

Anda dapat terhubung Amazon Kendra ke sumber Amazon RDS (Oracle) data menggunakan Amazon Kendra konsol dan TemplateConfigurationAPI.

Untuk memecahkan masalah konektor sumber Amazon Kendra Amazon RDS (Oracle) data Anda, lihat. Mengatasi masalah sumber data

Topik

Fitur yang didukung

- Pemetaan lapangan
- Pemfilteran konteks pengguna
- Filter inklusi/pengecualian
- Sinkronisasi konten penuh dan tambahan
- Cloud privat virtual (VPC)

Prasyarat

Sebelum Anda dapat menggunakan Amazon Kendra untuk mengindeks sumber Amazon RDS (Oracle) data Anda, buat perubahan ini di akun Amazon RDS (Oracle) dan AWS akun Anda.

DiAmazon RDS (Oracle), pastikan Anda memiliki:

- Mencatat nama pengguna dan kata sandi database Anda.

> **Important**
>
> Sebagai praktik terbaik, sediakan Amazon Kendra kredensil basis data hanya-baca.

- Menyalin url, port, dan instance host database Anda.
- Memeriksa setiap dokumen unik di dalam Amazon RDS (Oracle) dan di seluruh sumber data lain yang Anda rencanakan untuk digunakan untuk indeks yang sama. Setiap sumber data yang ingin Anda gunakan untuk indeks tidak boleh berisi dokumen yang sama di seluruh sumber data. ID dokumen bersifat global untuk indeks dan harus unik per indeks.

Di dalam Anda Akun AWS, pastikan Anda memiliki:

- Membuat Amazon Kendra indeks dan, jika menggunakan API, mencatat ID indeks.
- Membuat IAM peran untuk sumber data Anda dan, jika menggunakan API, catat ARN peran tersebut IAM .

> **Note**
>
> Jika Anda mengubah jenis otentikasi dan kredensialnya, Anda harus memperbarui IAM peran Anda untuk mengakses ID rahasia yang benar AWS Secrets Manager .

- Menyimpan kredensyal Amazon RDS (Oracle) otentikasi Anda AWS Secrets Manager secara rahasia dan, jika menggunakan API, catat ARN rahasia tersebut.

> **Note**
>
> Kami menyarankan Anda secara teratur menyegarkan atau memutar kredensil dan rahasia Anda. Berikan hanya tingkat akses yang diperlukan untuk keamanan Anda sendiri. Kami tidak menyarankan Anda menggunakan kembali kredensyal dan rahasia di seluruh sumber data, dan konektor versi 1.0 dan 2.0 (jika berlaku).

Jika Anda tidak memiliki IAM peran atau rahasia yang ada, Anda dapat menggunakan konsol untuk membuat IAM peran dan Secrets Manager rahasia baru saat Anda menghubungkan sumber Amazon RDS (Oracle) data Anda Amazon Kendra. Jika Anda menggunakan API, Anda harus memberikan ARN IAM peran dan Secrets Manager rahasia yang ada, dan ID indeks.

Instruksi koneksi

Untuk terhubung Amazon Kendra ke sumber Amazon RDS (Oracle) data Anda, Anda harus memberikan rincian Amazon RDS (Oracle) kredensyal Anda sehingga Amazon Kendra dapat mengakses data Anda. Jika Anda belum mengkonfigurasi Amazon RDS (Oracle) untuk Amazon Kendra lihatPrasyarat.

Console

Untuk terhubung Amazon Kendra ke Amazon RDS (Oracle)

1. Masuk ke AWS Management Console dan buka Amazon Kendra konsol.
2. Dari panel navigasi kiri, pilih Indeks dan kemudian pilih indeks yang ingin Anda gunakan dari daftar indeks.

> **Note**
>
> Anda dapat memilih untuk mengonfigurasi atau mengedit pengaturan kontrol akses Pengguna Anda di bawah Pengaturan indeks.

3. Pada halaman Memulai, pilih Tambahkan sumber data.
4. Pada halaman Tambahkan sumber data, pilih Amazon RDS (Oracle)konektor, lalu pilih Tambah konektor.
5. Pada halaman Tentukan detail sumber data, masukkan informasi berikut:
   a. Di Nama dan deskripsi, untuk Nama sumber data —Masukkan nama untuk sumber data Anda. Anda dapat memasukkan tanda hubung tetapi bukan spasi.
   b. (Opsional) Deskripsi —Masukkan deskripsi opsional untuk sumber data Anda.
   c. Dalam Bahasa default —Pilih bahasa untuk memfilter dokumen Anda untuk indeks. Kecuali Anda menentukan sebaliknya, bahasa default ke bahasa Inggris. Bahasa yang ditentukan dalam metadata dokumen mengesampingkan bahasa yang dipilih.
   d. Di Tag, untuk Tambahkan tag baru —Sertakan tag opsional untuk mencari dan memfilter sumber daya Anda atau melacak AWS biaya Anda.
   e. Pilih Berikutnya.
6. Pada halaman Tentukan akses dan keamanan, masukkan informasi berikut:
   a. Di Sumber, masukkan informasi berikut:

b. Host — Masukkan nama host database.

c. Port — Masukkan port database.

d. Instance - Masukkan instance database.

e. Aktifkan lokasi sertifikat SSL —Pilih untuk memasukkan Amazon S3 jalur ke file sertifikat SSL Anda.

f. Dalam Otentikasi —masukkan informasi berikut:

- AWS Secrets Manager rahasia —Pilih rahasia yang ada atau buat Secrets Manager rahasia baru untuk menyimpan kredensyal Amazon RDS (Oracle) otentikasi Anda. Jika Anda memilih untuk membuat rahasia baru, jendela AWS Secrets Manager rahasia terbuka.

  A. Masukkan informasi berikut di jendela Buat AWS Secrets Manager rahasia:

     I. Nama rahasia —Nama untuk rahasiamu. Awalan 'AmazonKendra- Amazon RDS (Oracle) -' secara otomatis ditambahkan ke nama rahasia Anda.

     II. Untuk nama pengguna Database, dan Kata Sandi —Masukkan nilai kredensi otentikasi yang Anda salin dari database Anda.

  B. Pilih Simpan.

g. Virtual Private Cloud (VPC) —Anda dapat memilih untuk menggunakan VPC. Jika demikian, Anda harus menambahkan Subnet dan grup keamanan VPC.

h. IAM peran —Pilih peran yang sudah ada atau buat IAM IAM peran baru untuk mengakses kredensi repositori dan mengindeks konten Anda.

> **Note**
>
> IAM peran yang digunakan untuk indeks tidak dapat digunakan untuk sumber data. Jika Anda tidak yakin apakah peran yang ada digunakan untuk indeks atau FAQ, pilih Buat peran baru untuk menghindari kesalahan.

i. Pilih Berikutnya.

7. Pada halaman Konfigurasi pengaturan sinkronisasi, masukkan informasi berikut:

a. Dalam lingkup Sinkronisasi, pilih dari opsi berikut:

- Kueri SQL —Masukkan pernyataan kueri SQL seperti operasi SELECT dan JOIN. Kueri SQL harus kurang dari 32KB. Amazon Kendra akan merayapi semua konten database yang cocok dengan kueri Anda.
- Kolom kunci primer —Berikan kunci utama untuk tabel database. Ini mengidentifikasi tabel dalam database Anda.
- Judul kolom —Berikan nama kolom judul dokumen dalam tabel database Anda.
- Kolom tubuh —Berikan nama kolom badan dokumen dalam tabel database Anda.

b. Dalam Konfigurasi tambahan — opsional, pilih dari opsi berikut untuk menyinkronkan konten tertentu alih-alih menyinkronkan semua file:

- Kolom pendeteksi perubahan —Masukkan nama kolom yang Amazon Kendra akan digunakan untuk mendeteksi perubahan konten. Amazon Kendra akan mengindeks ulang konten ketika ada perubahan di salah satu kolom ini.
- Kolom ID Pengguna —Masukkan nama kolom yang berisi ID Pengguna agar diizinkan mengakses konten.
- Kolom Grup —Masukkan nama kolom yang berisi grup untuk diizinkan mengakses konten.
- Kolom URL sumber —Masukkan nama kolom yang berisi URL Sumber yang akan diindeks.
- Kolom stempel waktu —Masukkan nama kolom yang berisi stempel waktu. Amazon Kendra menggunakan informasi cap waktu untuk mendeteksi perubahan dalam konten Anda dan hanya menyinkronkan konten yang diubah.
- Kolom zona waktu —Masukkan nama kolom yang berisi zona waktu untuk konten yang akan dirayapi.
- Format stempel waktu —Masukkan nama kolom yang berisi format cap waktu yang akan digunakan untuk mendeteksi perubahan konten dan menyinkronkan ulang konten Anda.

c. Mode sinkronisasi —Pilih cara Anda ingin memperbarui indeks saat konten sumber data Anda berubah. Saat Anda menyinkronkan sumber data Amazon Kendra untuk pertama kalinya, semua konten dirayapi dan diindeks secara default. Anda harus menjalankan sinkronisasi penuh data Anda jika sinkronisasi awal Anda gagal, bahkan jika Anda tidak memilih sinkronisasi penuh sebagai opsi mode sinkronisasi Anda.

- Sinkronisasi penuh: Indeks baru semua konten, ganti konten yang ada setiap kali sumber data Anda disinkronkan dengan indeks Anda.
- Sinkronisasi baru yang dimodifikasi: Indeks hanya konten baru dan yang dimodifikasi setiap kali sumber data Anda disinkronkan dengan indeks Anda. Amazon Kendra dapat menggunakan mekanisme sumber data Anda untuk melacak perubahan konten dan mengindeks konten yang berubah sejak sinkronisasi terakhir.
- Sinkronisasi baru, dimodifikasi, dihapus: Indeks hanya konten baru, dimodifikasi, dan dihapus setiap kali sumber data Anda disinkronkan dengan indeks Anda. Amazon Kendra dapat menggunakan mekanisme sumber data Anda untuk melacak perubahan konten dan mengindeks konten yang berubah sejak sinkronisasi terakhir.

d. Dalam jadwal berjalan Sinkronisasi, untuk Frekuensi —Seberapa sering Amazon Kendra akan disinkronkan dengan sumber data Anda.

e. Pilih Berikutnya.

8. Pada halaman Setel pemetaan bidang, masukkan informasi berikut:

   a. Pilih dari bidang sumber data default yang dihasilkan— ID Dokumen, Judul dokumen, dan URL Sumber —yang ingin Anda petakan ke Amazon Kendra indeks.

   b. Tambahkan bidang —Untuk menambahkan bidang sumber data kustom untuk membuat nama bidang indeks untuk dipetakan dan tipe data bidang.

   c. Pilih Berikutnya.

9. Pada halaman Tinjau dan buat, periksa apakah informasi yang Anda masukkan sudah benar dan kemudian pilih Tambahkan sumber data. Anda juga dapat memilih untuk mengedit informasi Anda dari halaman ini. Sumber data Anda akan muncul di halaman Sumber data setelah sumber data berhasil ditambahkan.

API

Untuk terhubung Amazon Kendra ke Amazon RDS (Oracle)

Anda harus menentukan yang berikut menggunakan TemplateConfigurationAPI:

- Sumber data —Tentukan tipe sumber data seperti `JDBC` saat Anda menggunakan skema TemplateConfigurationJSON. Tentukan juga sumber data seperti `TEMPLATE` saat Anda memanggil CreateDataSourceAPI.
- Jenis database —Anda harus menentukan jenis database sebagai`oracle`.

- Kueri SQL —Tentukan pernyataan kueri SQL seperti operasi SELECT dan JOIN. Kueri SQL harus kurang dari 32KB. Amazon Kendra akan merayapi semua konten database yang cocok dengan kueri Anda.
- Mode sinkronisasi —Tentukan cara Amazon Kendra memperbarui indeks Anda saat konten sumber data Anda berubah. Saat Anda menyinkronkan sumber data Amazon Kendra untuk pertama kalinya, semua konten dirayapi dan diindeks secara default. Anda harus menjalankan sinkronisasi penuh data Anda jika sinkronisasi awal Anda gagal, bahkan jika Anda tidak memilih sinkronisasi penuh sebagai opsi mode sinkronisasi Anda. Anda dapat memilih antara:
  - `FORCED_FULL_CRAWL`untuk mengindeks semua konten baru, mengganti konten yang ada setiap kali sumber data Anda disinkronkan dengan indeks Anda.
  - `FULL_CRAWL`untuk mengindeks hanya konten baru, dimodifikasi, dan dihapus setiap kali sumber data Anda disinkronkan dengan indeks Anda. Amazon Kendra dapat menggunakan mekanisme sumber data Anda untuk melacak perubahan konten dan mengindeks konten yang berubah sejak sinkronisasi terakhir.
  - `CHANGE_LOG`untuk mengindeks hanya konten baru dan yang dimodifikasi setiap kali sumber data Anda disinkronkan dengan indeks Anda. Amazon Kendra dapat menggunakan mekanisme sumber data Anda untuk melacak perubahan konten dan mengindeks konten yang berubah sejak sinkronisasi terakhir.
- Rahasia Nama Sumber Daya Amazon (ARN) —Berikan Nama Sumber Daya Amazon (ARN) Secrets Manager rahasia yang berisi kredensyal otentikasi yang Anda buat di akun Anda. Amazon RDS (Oracle) Rahasianya disimpan dalam struktur JSON dengan kunci berikut:

```
{
    "user name": "database user name",
    "password": "password"
}
```

> **Note**
>
> Kami menyarankan Anda secara teratur menyegarkan atau memutar kredensil dan rahasia Anda. Berikan hanya tingkat akses yang diperlukan untuk keamanan Anda sendiri. Kami tidak menyarankan Anda menggunakan kembali kredensyal dan rahasia di seluruh sumber data, dan konektor versi 1.0 dan 2.0 (jika berlaku).

- IAM peran —Tentukan `RoleArn` kapan Anda menelepon `CreateDataSource` untuk memberikan IAM peran dengan izin untuk mengakses Secrets Manager rahasia Anda dan

memanggil API publik yang diperlukan untuk Amazon RDS (Oracle) konektor dan. Amazon Kendra Untuk informasi selengkapnya, lihat IAM peran untuk sumber Amazon RDS (Oracle) data.

Anda juga dapat menambahkan fitur opsional berikut:

- Virtual Private Cloud (VPC) **`VpcConfiguration`** —Tentukan kapan Anda menelepon. `CreateDataSource` Untuk informasi selengkapnya, lihat Mengkonfigurasi Amazon Kendra untuk menggunakan Amazon VPC.
- Filter penyertaan dan pengecualian —Anda dapat menentukan apakah akan menyertakan konten tertentu menggunakan ID pengguna, grup, URL sumber, stempel waktu, dan zona waktu.
- Pemfilteran konteks pengguna dan kontrol akses —Amazon Kendra meng-crawl daftar kontrol akses (ACL) untuk dokumen Anda, jika Anda memiliki ACL untuk dokumen Anda. Informasi ACL digunakan untuk memfilter hasil pencarian berdasarkan pengguna atau akses grup mereka ke dokumen. Untuk informasi selengkapnya, lihat Pemfilteran konteks pengguna.
- Pemetaan bidang —Pilih untuk memetakan bidang sumber Amazon RDS (Oracle) data Anda ke bidang indeks Anda Amazon Kendra . Untuk informasi lebih lanjut, lihat Memetakan bidang sumber data.

> **Note**
>
> Bidang badan dokumen atau badan dokumen yang setara untuk dokumen Anda diperlukan Amazon Kendra untuk mencari dokumen Anda. Anda harus memetakan nama bidang badan dokumen Anda di sumber data Anda ke nama bidang indeks_`document_body`. Semua kolom lain bersifat opsional.

Untuk daftar kunci JSON penting lainnya untuk dikonfigurasi, lihatAmazon RDS Skema templat (Oracle).

Catatan

- Baris database yang dihapus tidak akan dilacak saat Amazon Kendra memeriksa konten yang diperbarui.
- Ukuran nama bidang dan nilai dalam deretan database Anda tidak dapat melebihi 400KB.

- Jika Anda memiliki sejumlah besar data dalam sumber data database Anda, dan tidak Amazon Kendra ingin mengindeks semua konten database Anda setelah sinkronisasi pertama, Anda dapat memilih untuk menyinkronkan hanya dokumen baru, dimodifikasi, atau dihapus.
- Sebagai praktik terbaik, sediakan Amazon Kendra kredensil basis data hanya-baca.
- Sebagai praktik terbaik, hindari menambahkan tabel dengan data sensitif atau informasi identitas pribadi (PII).

Amazon RDS (PostgreSQL)

Amazon RDS adalah layanan web yang membuatnya lebih mudah untuk mengatur, mengoperasikan, dan menskalakan database relasional di AWS Cloud. Jika Anda adalah Amazon RDS pengguna, Anda dapat menggunakan Amazon Kendra untuk mengindeks sumber Amazon RDS (PostgreSQL) data Anda. Konektor sumber Amazon Kendra Amazon RDS (PostgreSQL) data mendukung PostgreSQL 9.6.

Anda dapat terhubung Amazon Kendra ke sumber Amazon RDS (PostgreSQL) data menggunakan Amazon Kendra konsol dan TemplateConfigurationAPI.

Untuk memecahkan masalah konektor sumber Amazon Kendra Amazon RDS (PostgreSQL) data Anda, lihat. Mengatasi masalah sumber data

Topik

- Fitur yang didukung
- Prasyarat
- Instruksi koneksi
- Catatan

Fitur yang didukung

- Pemetaan lapangan
- Pemfilteran konteks pengguna
- Filter inklusi/pengecualian
- Sinkronisasi konten penuh dan tambahan
- Cloud privat virtual (VPC)

Prasyarat

Sebelum Anda dapat menggunakan Amazon Kendra untuk mengindeks sumber Amazon RDS (PostgreSQL) data Anda, buat perubahan ini di akun Amazon RDS (PostgreSQL) dan AWS akun Anda.

DiAmazon RDS (PostgreSQL), pastikan Anda memiliki:

- Mencatat nama pengguna dan kata sandi database Anda.

> **Important**
>
> Sebagai praktik terbaik, sediakan Amazon Kendra kredensil basis data hanya-baca.

- Menyalin url, port, dan instance host database Anda. Anda dapat menemukan informasi ini di Amazon RDS konsol.
- Memeriksa setiap dokumen unik di dalam Amazon RDS (PostgreSQL) dan di seluruh sumber data lain yang Anda rencanakan untuk digunakan untuk indeks yang sama. Setiap sumber data yang ingin Anda gunakan untuk indeks tidak boleh berisi dokumen yang sama di seluruh sumber data. ID dokumen bersifat global untuk indeks dan harus unik per indeks.

Di dalam Anda Akun AWS, pastikan Anda memiliki:

- Membuat Amazon Kendra indeks dan, jika menggunakan API, mencatat ID indeks.
- Membuat IAM peran untuk sumber data Anda dan, jika menggunakan API, catat ARN peran tersebut IAM .

> **Note**
>
> Jika Anda mengubah jenis otentikasi dan kredensyal, Anda harus memperbarui IAM peran Anda untuk mengakses ID rahasia yang benar AWS Secrets Manager .

- Menyimpan kredensyal Amazon RDS (PostgreSQL) otentikasi Anda AWS Secrets Manager secara rahasia dan, jika menggunakan API, catat ARN rahasia tersebut.

> **Note**
>
> Kami menyarankan Anda secara teratur menyegarkan atau memutar kredensil dan rahasia Anda. Berikan hanya tingkat akses yang diperlukan untuk keamanan Anda sendiri. Kami tidak menyarankan Anda menggunakan kembali kredensyal dan rahasia di seluruh sumber data, dan konektor versi 1.0 dan 2.0 (jika berlaku).

Jika Anda tidak memiliki IAM peran atau rahasia yang ada, Anda dapat menggunakan konsol untuk membuat IAM peran dan Secrets Manager rahasia baru saat Anda menghubungkan sumber Amazon RDS (PostgreSQL) data Anda Amazon Kendra. Jika Anda menggunakan API, Anda harus memberikan ARN IAM peran dan Secrets Manager rahasia yang ada, dan ID indeks.

Instruksi koneksi

Untuk terhubung Amazon Kendra ke sumber Amazon RDS (PostgreSQL) data Anda, Anda harus memberikan rincian Amazon RDS (PostgreSQL) kredensyal Anda sehingga Amazon Kendra dapat mengakses data Anda. Jika Anda belum mengkonfigurasi Amazon RDS (PostgreSQL) untuk Amazon Kendra lihatPrasyarat.

Console

Untuk terhubung Amazon Kendra ke Amazon RDS (PostgreSQL)

1. Masuk ke AWS Management Console dan buka Amazon Kendra konsol.
2. Dari panel navigasi kiri, pilih Indeks dan kemudian pilih indeks yang ingin Anda gunakan dari daftar indeks.

   > **Note**
   >
   > Anda dapat memilih untuk mengonfigurasi atau mengedit pengaturan kontrol akses Pengguna Anda di bawah Pengaturan indeks.

3. Pada halaman Memulai, pilih Tambahkan sumber data.
4. Pada halaman Tambahkan sumber data, pilih Amazon RDS (PostgreSQL)konektor, lalu pilih Tambah konektor.
5. Pada halaman Tentukan detail sumber data, masukkan informasi berikut:

a. Di Nama dan deskripsi, untuk Nama sumber data —Masukkan nama untuk sumber data Anda. Anda dapat memasukkan tanda hubung tetapi bukan spasi.

b. (Opsional) Deskripsi —Masukkan deskripsi opsional untuk sumber data Anda.

c. Dalam Bahasa default —Pilih bahasa untuk memfilter dokumen Anda untuk indeks. Kecuali Anda menentukan sebaliknya, bahasa default ke bahasa Inggris. Bahasa yang ditentukan dalam metadata dokumen mengesampingkan bahasa yang dipilih.

d. Di Tag, untuk Tambahkan tag baru —Sertakan tag opsional untuk mencari dan memfilter sumber daya Anda atau melacak AWS biaya Anda.

e. Pilih Berikutnya.

6. Pada halaman Tentukan akses dan keamanan, masukkan informasi berikut:

a. Di Sumber, masukkan informasi berikut:

b. Host — Masukkan URL host database, misalnya:`http://`*`instance URL`*`.`*`region`*`.rds.amazonaws.com`.

c. Port — Masukkan port database, misalnya,`5432`.

d. Instance — Masukkan contoh database, misalnya`postgres`.

e. Aktifkan lokasi sertifikat SSL —Pilih untuk memasukkan Amazon S3 jalur ke file sertifikat SSL Anda.

f. Dalam Otentikasi —masukkan informasi berikut:

- AWS Secrets Manager rahasia —Pilih rahasia yang ada atau buat Secrets Manager rahasia baru untuk menyimpan kredensyal Amazon RDS (PostgreSQL) otentikasi Anda. Jika Anda memilih untuk membuat rahasia baru, jendela AWS Secrets Manager rahasia terbuka.

  A. Masukkan informasi berikut di jendela Buat AWS Secrets Manager rahasia:

     I. Nama rahasia —Nama untuk rahasiamu. Awalan 'AmazonKendra- Amazon RDS (PostgreSQL) -' secara otomatis ditambahkan ke nama rahasia Anda.

     II. Untuk nama pengguna Database, dan Kata Sandi —Masukkan nilai kredensi otentikasi yang Anda salin dari database Anda.

  B. Pilih Simpan.

g. Virtual Private Cloud (VPC) —Anda dapat memilih untuk menggunakan VPC. Jika demikian, Anda harus menambahkan Subnet dan grup keamanan VPC.

h. IAM peran —Pilih peran yang sudah ada atau buat IAM IAM peran baru untuk mengakses kredensi repositori dan mengindeks konten Anda.

> **Note**
>
> IAM peran yang digunakan untuk indeks tidak dapat digunakan untuk sumber data. Jika Anda tidak yakin apakah peran yang ada digunakan untuk indeks atau FAQ, pilih Buat peran baru untuk menghindari kesalahan.

i. Pilih Berikutnya.

7. Pada halaman Konfigurasi pengaturan sinkronisasi, masukkan informasi berikut:

   a. Dalam lingkup Sinkronisasi, pilih dari opsi berikut:

   - Kueri SQL —Masukkan pernyataan kueri SQL seperti operasi SELECT dan JOIN. Kueri SQL harus kurang dari 32KB Kueri SQL harus kurang dari 32KB dan tidak mengandung semi-titik dua (;). Amazon Kendra akan merayapi semua konten database yang cocok dengan kueri Anda.
   - Kolom kunci primer —Menyediakan kunci utama untuk tabel database. Ini mengidentifikasi tabel dalam database Anda.
   - Judul kolom —Berikan nama kolom judul dokumen dalam tabel database Anda.
   - Kolom tubuh —Berikan nama kolom badan dokumen dalam tabel database Anda.

   b. Dalam Konfigurasi tambahan — opsional, pilih dari opsi berikut untuk menyinkronkan konten tertentu alih-alih menyinkronkan semua file:

   - Kolom pendeteksi perubahan —Masukkan nama kolom yang Amazon Kendra akan digunakan untuk mendeteksi perubahan konten. Amazon Kendra akan mengindeks ulang konten ketika ada perubahan di salah satu kolom ini.
   - Kolom ID Pengguna —Masukkan nama kolom yang berisi ID Pengguna agar diizinkan mengakses konten.
   - Kolom Grup —Masukkan nama kolom yang berisi grup untuk diizinkan mengakses konten.
   - Kolom URL sumber —Masukkan nama kolom yang berisi URL Sumber yang akan diindeks.

- Kolom stempel waktu —Masukkan nama kolom yang berisi stempel waktu. Amazon Kendra menggunakan informasi cap waktu untuk mendeteksi perubahan dalam konten Anda dan hanya menyinkronkan konten yang diubah.
- Kolom zona waktu —Masukkan nama kolom yang berisi zona waktu untuk konten yang akan dirayapi.
- Format stempel waktu —Masukkan nama kolom yang berisi format cap waktu yang akan digunakan untuk mendeteksi perubahan konten dan menyinkronkan ulang konten Anda.

c. Mode sinkronisasi —Pilih cara Anda ingin memperbarui indeks saat konten sumber data Anda berubah. Saat Anda menyinkronkan sumber data Amazon Kendra untuk pertama kalinya, semua konten dirayapi dan diindeks secara default. Anda harus menjalankan sinkronisasi penuh data Anda jika sinkronisasi awal Anda gagal, bahkan jika Anda tidak memilih sinkronisasi penuh sebagai opsi mode sinkronisasi Anda.

- Sinkronisasi penuh: Indeks baru semua konten, ganti konten yang ada setiap kali sumber data Anda disinkronkan dengan indeks Anda.
- Sinkronisasi baru yang dimodifikasi: Indeks hanya konten baru dan yang dimodifikasi setiap kali sumber data Anda disinkronkan dengan indeks Anda. Amazon Kendra dapat menggunakan mekanisme sumber data Anda untuk melacak perubahan konten dan mengindeks konten yang berubah sejak sinkronisasi terakhir.
- Sinkronisasi baru, dimodifikasi, dihapus: Indeks hanya konten baru, dimodifikasi, dan dihapus setiap kali sumber data Anda disinkronkan dengan indeks Anda. Amazon Kendra dapat menggunakan mekanisme sumber data Anda untuk melacak perubahan konten dan mengindeks konten yang berubah sejak sinkronisasi terakhir.

d. Dalam jadwal berjalan Sinkronisasi, untuk Frekuensi —Seberapa sering Amazon Kendra akan disinkronkan dengan sumber data Anda.

e. Pilih Berikutnya.

8. Pada halaman Setel pemetaan bidang, masukkan informasi berikut:

a. Pilih dari bidang sumber data default yang dihasilkan— ID Dokumen, Judul dokumen, dan URL Sumber —yang ingin Anda petakan ke Amazon Kendra indeks.

b. Tambahkan bidang —Untuk menambahkan bidang sumber data kustom untuk membuat nama bidang indeks untuk dipetakan dan tipe data bidang.

c. Pilih Berikutnya.

9. Pada halaman Tinjau dan buat, periksa apakah informasi yang Anda masukkan sudah benar dan kemudian pilih Tambahkan sumber data. Anda juga dapat memilih untuk mengedit informasi Anda dari halaman ini. Sumber data Anda akan muncul di halaman Sumber data setelah sumber data berhasil ditambahkan.

API

Untuk terhubung Amazon Kendra ke Amazon RDS (PostgreSQL)

Anda harus menentukan yang berikut menggunakan TemplateConfigurationAPI:

- Sumber data —Tentukan tipe sumber data seperti `JDBC` saat Anda menggunakan skema TemplateConfigurationJSON. Tentukan juga sumber data seperti `TEMPLATE` saat Anda memanggil CreateDataSourceAPI.
- Jenis database —Anda harus menentukan jenis database sebagai`postgresql`.
- Kueri SQL —Tentukan pernyataan kueri SQL seperti operasi SELECT dan JOIN. Kueri SQL harus kurang dari 32KB. Amazon Kendra akan merayapi semua konten database yang cocok dengan kueri Anda.
- Mode sinkronisasi —Tentukan cara Amazon Kendra memperbarui indeks Anda saat konten sumber data Anda berubah. Saat Anda menyinkronkan sumber data Amazon Kendra untuk pertama kalinya, semua konten dirayapi dan diindeks secara default. Anda harus menjalankan sinkronisasi penuh data Anda jika sinkronisasi awal Anda gagal, bahkan jika Anda tidak memilih sinkronisasi penuh sebagai opsi mode sinkronisasi Anda. Anda dapat memilih antara:
  - `FORCED_FULL_CRAWL`untuk mengindeks semua konten baru, mengganti konten yang ada setiap kali sumber data Anda disinkronkan dengan indeks Anda.
  - `FULL_CRAWL`untuk mengindeks hanya konten baru, dimodifikasi, dan dihapus setiap kali sumber data Anda disinkronkan dengan indeks Anda. Amazon Kendra dapat menggunakan mekanisme sumber data Anda untuk melacak perubahan konten dan mengindeks konten yang berubah sejak sinkronisasi terakhir.
  - `CHANGE_LOG`untuk mengindeks hanya konten baru dan yang dimodifikasi setiap kali sumber data Anda disinkronkan dengan indeks Anda. Amazon Kendra dapat menggunakan mekanisme sumber data Anda untuk melacak perubahan konten dan mengindeks konten yang berubah sejak sinkronisasi terakhir.
- Rahasia Nama Sumber Daya Amazon (ARN) —Berikan Nama Sumber Daya Amazon (ARN) Secrets Manager rahasia yang berisi kredensyal otentikasi yang Anda buat di akun Anda. Amazon RDS (PostgreSQL) Rahasianya disimpan dalam struktur JSON dengan kunci berikut:

```
{
    "user name": "database user name",
    "password": "password"
}
```

> **Note**
>
> Kami menyarankan Anda secara teratur menyegarkan atau memutar kredensil dan rahasia Anda. Berikan hanya tingkat akses yang diperlukan untuk keamanan Anda sendiri. Kami tidak menyarankan Anda menggunakan kembali kredensyal dan rahasia di seluruh sumber data, dan konektor versi 1.0 dan 2.0 (jika berlaku).

- IAM peran —Tentukan `RoleArn` kapan Anda menelepon `CreateDataSource` untuk memberikan IAM peran dengan izin untuk mengakses Secrets Manager rahasia Anda dan memanggil API publik yang diperlukan untuk Amazon RDS (PostgreSQL) konektor dan. Amazon Kendra Untuk informasi selengkapnya, lihat IAM peran untuk sumber Amazon RDS (PostgreSQL) data.

Anda juga dapat menambahkan fitur opsional berikut:

- Virtual Private Cloud (VPC) **`VpcConfiguration`** —Tentukan kapan Anda menelepon. `CreateDataSource` Untuk informasi selengkapnya, lihat Mengkonfigurasi Amazon Kendra untuk menggunakan Amazon VPC.
- Filter penyertaan dan pengecualian —Anda dapat menentukan apakah akan menyertakan konten tertentu menggunakan ID pengguna, grup, URL sumber, stempel waktu, dan zona waktu.
- Pemfilteran konteks pengguna dan kontrol akses —Amazon Kendra meng-crawl daftar kontrol akses (ACL) untuk dokumen Anda, jika Anda memiliki ACL untuk dokumen Anda. Informasi ACL digunakan untuk memfilter hasil pencarian berdasarkan pengguna atau akses grup mereka ke dokumen. Untuk informasi selengkapnya, lihat Pemfilteran konteks pengguna.
- Pemetaan bidang —Pilih untuk memetakan bidang sumber Amazon RDS (PostgreSQL) data Anda ke bidang indeks Anda Amazon Kendra . Untuk informasi lebih lanjut, lihat Memetakan bidang sumber data.

> **Note**
>
> Bidang badan dokumen atau badan dokumen yang setara untuk dokumen Anda diperlukan Amazon Kendra untuk mencari dokumen Anda. Anda harus memetakan nama bidang badan dokumen Anda di sumber data Anda ke nama bidang indeks_`document_body`. Semua kolom lain bersifat opsional.

Untuk daftar kunci JSON penting lainnya untuk dikonfigurasi, lihatAmazon RDS (PostgreSQL) skema templat.

Catatan

- Baris database yang dihapus tidak akan dilacak saat Amazon Kendra memeriksa konten yang diperbarui.
- Ukuran nama bidang dan nilai dalam deretan database Anda tidak dapat melebihi 400KB.
- Jika Anda memiliki sejumlah besar data dalam sumber data database Anda, dan tidak Amazon Kendra ingin mengindeks semua konten database Anda setelah sinkronisasi pertama, Anda dapat memilih untuk menyinkronkan hanya dokumen baru, dimodifikasi, atau dihapus.
- Sebagai praktik terbaik, sediakan Amazon Kendra kredensil basis data hanya-baca.
- Sebagai praktik terbaik, hindari menambahkan tabel dengan data sensitif atau informasi identitas pribadi (PII).

Amazon S3

Amazon S3 adalah layanan penyimpanan objek yang menyimpan data sebagai objek di dalam ember. Anda dapat menggunakan Amazon Kendra untuk mengindeks repositori Amazon S3 bucket dokumen Anda.

> **Warning**
>
> Amazon Kendra tidak menggunakan kebijakan bucket yang memberikan izin kepada Amazon Kendra kepala sekolah untuk berinteraksi dengan bucket S3. Sebaliknya, ia menggunakan IAM peran. Pastikan itu Amazon Kendra tidak disertakan sebagai anggota tepercaya dalam kebijakan bucket Anda untuk menghindari masalah keamanan data dalam pemberian

izin secara tidak sengaja kepada prinsipal arbitrer. Namun, Anda dapat menambahkan kebijakan bucket untuk menggunakan Amazon S3 bucket di berbagai akun. Untuk informasi selengkapnya, lihat Kebijakan untuk digunakan Amazon S3 di seluruh akun (dalam tab IAM peran S3, di bawah IAM peran untuk sumber data). Untuk informasi tentang IAM peran untuk sumber data S3, lihat IAM peran.

> **Note**
>
> Amazon Kendra sekarang mendukung Amazon S3 konektor yang ditingkatkan. Konsol telah ditingkatkan secara otomatis untuk Anda. Konektor baru apa pun yang Anda buat di konsol akan menggunakan arsitektur yang ditingkatkan. Jika Anda menggunakan API, Anda sekarang harus menggunakan TemplateConfigurationobjek alih-alih `S3DataSourceConfiguration` objek untuk mengonfigurasi konektor Anda. Konektor yang dikonfigurasi menggunakan konsol lama dan arsitektur API akan terus berfungsi seperti yang dikonfigurasi. Namun, Anda tidak akan dapat mengedit atau memperbaruinya. Jika Anda ingin mengedit atau memperbarui konfigurasi konektor Anda, Anda harus membuat konektor baru.
> Kami merekomendasikan untuk memigrasikan alur kerja konektor Anda ke versi yang ditingkatkan. Support untuk konektor yang dikonfigurasi menggunakan arsitektur lama dijadwalkan berakhir pada Juni 2024.

Anda dapat terhubung ke sumber Amazon S3 data menggunakan Amazon Kendra konsol atau TemplateConfigurationAPI.

> **Note**
>
> Untuk membuat laporan status sinkronisasi untuk sumber Amazon S3 data Anda, lihat Memecahkan masalah sumber data.

Untuk memecahkan masalah konektor sumber data Amazon Kendra S3, lihat. Mengatasi masalah sumber data

Topik

- Fitur yang didukung

- Prasyarat
- Instruksi koneksi
- Membuat sumber Amazon S3 data
- Amazon S3 metadata dokumen
- Kontrol akses untuk sumber Amazon S3 data
- Menggunakan Amazon VPC dengan sumber Amazon S3 data

Fitur yang didukung

- Pemetaan lapangan
- Pemfilteran konteks pengguna
- Filter inklusi/pengecualian
- Sinkronisasi konten penuh dan inkremental
- Cloud privat virtual (VPC)

Prasyarat

Sebelum Anda dapat menggunakan Amazon Kendra untuk mengindeks sumber data S3 Anda, buat perubahan ini di S3 dan AWS akun Anda.

Di S3, pastikan Anda memiliki:

- Menyalin nama nama Amazon S3 ember Anda.

  > **Note**
  >
  > Bucket Anda harus berada di wilayah yang sama dengan Amazon Kendra indeks Anda dan indeks Anda harus memiliki izin untuk mengakses bucket yang berisi dokumen Anda.

- Memeriksa setiap dokumen unik di S3 dan di seluruh sumber data lain yang Anda rencanakan untuk digunakan untuk indeks yang sama. Setiap sumber data yang ingin Anda gunakan untuk indeks tidak boleh berisi dokumen yang sama di seluruh sumber data. ID dokumen bersifat global untuk indeks dan harus unik per indeks.

Di AWS akun Anda, pastikan Anda memiliki:

- Membuat Amazon Kendra indeks dan, jika menggunakan API, mencatat ID indeks.
- Membuat IAM peran untuk sumber data Anda dan, jika menggunakan API, catat ARN peran tersebut IAM .

Jika tidak memiliki IAM peran yang ada, Anda dapat menggunakan konsol untuk membuat IAM peran baru saat menghubungkan sumber data S3. Amazon Kendra Jika Anda menggunakan API, Anda harus memberikan ARN IAM peran yang ada dan ID indeks.

Instruksi koneksi

Untuk terhubung Amazon Kendra ke sumber data S3 Anda, Anda harus memberikan rincian yang diperlukan dari sumber data S3 Anda sehingga Amazon Kendra dapat mengakses data Anda. Jika Anda belum mengkonfigurasi S3 untuk Amazon Kendra, lihatPrasyarat.

Console

Untuk terhubung Amazon Kendra ke Amazon S3

1. Masuk ke AWS Management Console dan buka Amazon Kendra konsol.
2. Dari panel navigasi kiri, pilih Indeks dan kemudian pilih indeks yang ingin Anda gunakan dari daftar indeks.

> **Note**
>
> Anda dapat memilih untuk mengonfigurasi atau mengedit pengaturan kontrol akses Pengguna Anda di bawah Pengaturan indeks.

3. Pada halaman Memulai, pilih Tambahkan sumber data.
4. Pada halaman Tambahkan sumber data, pilih konektor S3, lalu pilih Tambah konektor.
5. Pada halaman Tentukan detail sumber data, masukkan informasi berikut:

   a. Dalam Nama dan deskripsi, untuk Nama sumber data —Masukkan nama untuk sumber data Anda. Anda dapat memasukkan tanda hubung tetapi bukan spasi.

   b. (Opsional) Deskripsi —Masukkan deskripsi opsional untuk sumber data Anda.

   c. Dalam Bahasa default —Pilih bahasa untuk memfilter dokumen Anda untuk indeks. Kecuali Anda menentukan sebaliknya, bahasa default ke bahasa Inggris. Bahasa yang ditentukan dalam metadata dokumen mengesampingkan bahasa yang dipilih.

d. Di Tag, untuk Tambahkan tag baru —Sertakan tag opsional untuk mencari dan memfilter sumber daya Anda atau melacak AWS biaya Anda.

e. Pilih Berikutnya.

6. Pada halaman Tentukan akses dan keamanan, masukkan informasi opsional berikut:

a. IAM peran —Pilih peran yang ada atau buat IAM IAM peran baru untuk mengakses kredensi repositori dan mengindeks konten.

> **Note**
>
> IAM peran yang digunakan untuk indeks tidak dapat digunakan untuk sumber data. Jika Anda tidak yakin apakah peran yang ada digunakan untuk indeks atau FAQ, pilih Buat peran baru untuk menghindari kesalahan.

b. Virtual Private Cloud (VPC) —Anda dapat memilih untuk menggunakan Amazon S3 bucket Amazon VPC untuk Anda jika tidak dapat diakses dari Internet publik. Jika demikian, Anda harus menambahkan Subnet dan Grup Amazon VPC Keamanan.

> **Important**
>
> Pastikan Anda memiliki:
>
> - Menambahkan Amazon S3 titik akhir ke Anda Amazon VPC sesuai dengan langkah-langkah di titik akhir Gateway untuk. Amazon S3
> - Memilih subnet pribadi di zona ketersediaan yang Amazon Kendra didukung. Lihat Mengkonfigurasi Amazon Kendra untuk menggunakan untuk detail selengkapnya. Amazon VPC
> - Mengonfigurasi grup keamanan Anda Amazon Kendra untuk memungkinkan mengakses Amazon S3 titik akhir. Lihat Mengkonfigurasi Amazon Kendra untuk digunakan Amazon VPC untuk detail selengkapnya.

c. Pilih Berikutnya.

7. Pada halaman Konfigurasi pengaturan sinkronisasi, masukkan informasi berikut:

a. Dalam lingkup Sinkronisasi, untuk lokasi sumber data —Jalur ke Amazon S3 bucket tempat data Anda disimpan. Pilih Browse S3 untuk memilih bucket Anda.

b. (Opsional) File metadata awalan lokasi folder —Jalur ke folder tempat metadata Anda disimpan. Pilih Browse S3 untuk menemukan folder metadata Anda.

c. (Opsional) Lokasi file konfigurasi daftar kontrol akses —Jalur ke lokasi file yang berisi struktur JSON yang menentukan pengaturan akses untuk file yang disimpan di sumber data S3 Anda. Pilih Browse S3 untuk menemukan file ACL Anda.

d. (Opsional) Pilih kunci dekripsi —Pilih untuk menggunakan kunci dekripsi. Anda dapat memilih untuk menggunakan AWS KMS kunci yang ada.

e. (Opsional) Dalam konfigurasi tambahan, untuk Pola —Tambahkan pola untuk menyertakan atau mengecualikan dokumen dari indeks Anda. Semua jalur relatif terhadap bucket S3 lokasi sumber data. Anda dapat menambahkan hingga 100 pola.

f. Mode sinkronisasi —Pilih cara Anda ingin memperbarui indeks saat konten sumber data Anda berubah. Saat Anda menyinkronkan sumber data Amazon Kendra untuk pertama kalinya, semua konten dirayapi dan diindeks secara default. Anda harus menjalankan sinkronisasi penuh data Anda jika sinkronisasi awal Anda gagal, bahkan jika Anda tidak memilih sinkronisasi penuh sebagai opsi mode sinkronisasi Anda.

   - Sinkronisasi penuh: Indeks baru semua konten, ganti konten yang ada setiap kali sumber data Anda disinkronkan dengan indeks Anda.
   - Sinkronisasi baru, dimodifikasi, dihapus: Indeks hanya konten baru, dimodifikasi, dan dihapus setiap kali sumber data Anda disinkronkan dengan indeks Anda. Amazon Kendra dapat menggunakan mekanisme sumber data Anda untuk melacak perubahan konten dan mengindeks konten yang berubah sejak sinkronisasi terakhir.

g. Di Jadwal berjalan Sinkronisasi, untuk Frekuensi —Pilih seberapa sering Amazon Kendra akan disinkronkan dengan sumber data Anda.

h. Pilih Berikutnya.

8. Pada halaman Setel pemetaan bidang, masukkan informasi opsional berikut:

   a. Pemetaan bidang S3 —Pilih dari bidang sumber data default Amazon Kendra yang dihasilkan yang ingin Anda petakan ke indeks Anda.

   b. Tambahkan bidang —Pilih untuk menambahkan bidang sumber data khusus untuk membuat nama bidang indeks untuk dipetakan dan tipe data bidang.

   c. Pilih Berikutnya.

9. Pada halaman Tinjau dan buat, periksa apakah informasi yang Anda masukkan sudah benar dan kemudian pilih Tambahkan sumber data. Anda juga dapat memilih untuk mengedit

informasi Anda dari halaman ini. Sumber data Anda akan muncul di halaman Sumber data setelah sumber data berhasil ditambahkan.

API

Untuk terhubung Amazon Kendra ke Amazon S3

Anda harus menentukan JSON dari skema sumber data menggunakan API. TemplateConfiguration Anda harus memberikan informasi berikut ini:

- BucketName—Nama ember yang berisi dokumen.
- Mode sinkronisasi —Tentukan cara Amazon Kendra memperbarui indeks Anda saat konten sumber data Anda berubah. Saat Anda menyinkronkan sumber data Amazon Kendra untuk pertama kalinya, semua konten dirayapi dan diindeks secara default. Anda harus menjalankan sinkronisasi penuh data Anda jika sinkronisasi awal Anda gagal, bahkan jika Anda tidak memilih sinkronisasi penuh sebagai opsi mode sinkronisasi Anda. Anda dapat memilih antara:
  - `FORCED_FULL_CRAWL`untuk mengindeks semua konten baru, mengganti konten yang ada setiap kali sumber data Anda disinkronkan dengan indeks Anda.
  - `FULL_CRAWL`untuk mengindeks hanya konten baru, dimodifikasi, dan dihapus setiap kali sumber data Anda disinkronkan dengan indeks Anda. Amazon Kendra dapat menggunakan mekanisme sumber data Anda untuk melacak perubahan konten dan mengindeks konten yang berubah sejak sinkronisasi terakhir.
- IAM role —Tentukan `RoleArn` kapan Anda menelepon `CreateDataSource` untuk memberikan IAM peran dengan izin untuk mengakses Secrets Manager rahasia Anda dan memanggil API publik yang diperlukan untuk konektor S3 dan. Amazon Kendra Untuk informasi selengkapnya, lihat IAM peran untuk sumber data S3.

Anda juga dapat menambahkan fitur opsional berikut:

- Virtual Private Cloud (VPC) **`VpcConfiguration`** —Tentukan kapan Anda menelepon. `CreateDataSource` Untuk informasi selengkapnya, lihat Mengkonfigurasi Amazon Kendra untuk menggunakan Amazon VPC.
- Filter inklusi dan pengecualian —Tentukan apakah akan menyertakan atau mengecualikan nama file tertentu, jenis file, jalur file. Anda menggunakan pola glob (pola yang dapat memperluas pola wildcard ke dalam daftar nama jalur yang cocok dengan pola yang diberikan).

Sebagai contoh, lihat Penggunaan Kecualikan dan Sertakan Filter di Referensi Perintah AWS CLI.

- Konfigurasi metadata dokumen —Tambahkan file metadata dokumen yang berisi informasi seperti informasi kontrol akses dokumen, URI sumber, penulis dokumen, dan atribut kustom. Setiap file metadata berisi metadata tentang satu dokumen.
- Pemetaan bidang —Pilih untuk memetakan bidang sumber data S3 Anda ke bidang indeks Anda. Amazon Kendra Untuk informasi lebih lanjut, lihat Memetakan bidang sumber data.

> **Note**
>
> Bidang badan dokumen atau badan dokumen yang setara untuk dokumen Anda diperlukan Amazon Kendra untuk mencari dokumen Anda. Anda harus memetakan nama bidang badan dokumen Anda di sumber data Anda ke nama bidang indeks `_document_body`. Semua kolom lain bersifat opsional.

Untuk daftar kunci JSON penting lainnya untuk dikonfigurasi, lihatAmazon S3 skema templat.

Pelajari selengkapnya

Untuk mempelajari lebih lanjut tentang mengintegrasikan Amazon Kendra dengan sumber data S3 Anda, lihat:

- Cari jawaban secara akurat menggunakan Konektor Amazon Kendra S3 dengan dukungan VPC

Membuat sumber Amazon S3 data

Contoh berikut menunjukkan pembuatan sumber Amazon S3 data. Contoh mengasumsikan bahwa Anda telah membuat indeks dan IAM peran dengan izin untuk membaca data dari indeks. Untuk informasi selengkapnya tentang IAM peran, lihat peran IAM akses. Untuk informasi selengkapnya tentang membuat indeks, lihat Membuat indeks.

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

Cuplikan kode Python berikut menciptakan sumber data. Amazon S3 Untuk contoh lengkap, lihat Memulai (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 soource 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
    )
```

Proses pembuatan sumber data dapat memakan waktu lama. Anda dapat memantau kemajuan dengan menggunakan DescribeDataSourceAPI. Jika status sumber data adalah `ACTIVE`, sumber data siap digunakan.

Contoh berikut menunjukkan proses mendapatkan status sumber data.

CLI

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

Python

Cuplikan kode Python berikut ini mendapatkan informasi tentang sumber data S3. Untuk contoh lengkap, lihat Memulai (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
```

Sumber data ini tidak memiliki jadwal, sehingga tidak berjalan secara otomatis. Untuk mengindeks sumber data, Anda memanggil StartDataSourceSyncJobuntuk menyinkronkan indeks dengan sumber data.

Contoh berikut menunjukkan proses sinkronisasi sumber data.

CLI

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

Python

Cuplikan kode Python berikut menyinkronkan sumber data. Amazon S3 Untuk contoh lengkap, lihat Memulai (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 metadata dokumen

Anda dapat menambahkan metadata, informasi tambahan tentang dokumen, ke dokumen dalam Amazon S3 bucket menggunakan file metadata. Setiap file metadata terkait dengan dokumen yang diindeks.

File metadata harus disimpan dalam bucket yang sama dengan file yang diindeks. Anda dapat menentukan lokasi dalam bucket untuk file metadata menggunakan konsol atau `S3Prefix` bidang `DocumentsMetadataConfiguration` parameter saat membuat sumber Amazon S3 data. Jika Anda tidak menentukan Amazon S3 awalan, file metadata Anda harus disimpan di lokasi yang sama dengan dokumen yang diindeks.

Jika Anda menentukan Amazon S3 awalan untuk file metadata Anda, mereka berada dalam struktur direktori paralel dengan dokumen yang diindeks. Amazon Kendra terlihat hanya di direktori yang ditentukan untuk metadata Anda. Jika metadata tidak terbaca, periksa apakah lokasi direktori sesuai dengan lokasi metadata.

Contoh berikut menunjukkan bagaimana lokasi dokumen yang diindeks dipetakan ke lokasi file metadata. Perhatikan bahwa Amazon S3 kunci dokumen ditambahkan ke Amazon S3 awalan metadata dan kemudian diakhiran `.metadata.json` untuk membentuk jalur file metadata. Amazon S3 Amazon S3 Kunci gabungan, dengan Amazon S3 awalan dan `.metadata.json` akhiran metadata harus tidak lebih dari total 1024 karakter. Disarankan agar Anda menyimpan Amazon S3 kunci Anda di bawah 1000 karakter untuk memperhitungkan karakter tambahan saat menggabungkan kunci Anda dengan awalan dan akhiran.

```
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
```

Metadata dokumen ditentukan dalam file JSON. File harus berupa file teks UTF-8 tanpa penanda BOM. Nama file dari file JSON harus`<document>.<extension>.metadata.json`. Dalam contoh ini, “dokumen” adalah nama dokumen yang digunakan metadata dan “ekstensi” adalah ekstensi file untuk dokumen tersebut. ID dokumen harus unik di`<document>.<extension>.metadata.json`.

Isi dari file JSON mengikuti templat berikut ini. Semua atribut/bidang bersifat opsional, jadi tidak perlu menyertakan semua atribut. Anda harus memberikan nilai untuk setiap atribut yang ingin Anda sertakan; nilainya tidak boleh kosong. Jika Anda tidak menentukan`_source_uri`, maka tautan yang dikembalikan oleh Amazon Kendra dalam hasil pencarian mengarah ke Amazon S3 bucket yang berisi dokumen. `DocumentId`dipetakan ke bidang `s3_document_id` dan merupakan jalur absolut ke dokumen di S3.

```
{
    "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."
}
```

Bidang metadata `_created_at` dan `_last_updated_at` adalah tanggal yang dikodekan dengan ISO 8601. Misalnya, 2012-03-25T 12:30:10 +01:00 adalah format tanggal-waktu ISO 8601 untuk 25 Maret 2012, pukul 12:30 (ditambah 10 detik) di zona waktu Eropa Tengah.

Anda dapat menambahkan informasi ke bidang `Attributes` tentang dokumen yang digunakan untuk memfilter kueri atau respons kueri grup. Untuk informasi selengkapnya, lihat Membuat bidang dokumen kustom.

Anda dapat menggunakan `AccessControlList` bidang untuk memfilter respons dari kueri. Dengan cara ini, hanya pengguna dan grup tertentu yang memiliki akses ke dokumen. Untuk informasi selengkapnya, lihat Penyaringan pada konteks pengguna.

Kontrol akses untuk sumber Amazon S3 data

Anda dapat mengontrol akses ke dokumen dalam sumber Amazon S3 data menggunakan file konfigurasi. Anda menentukan file di konsol atau sebagai `AccessControlListConfiguration` parameter saat Anda memanggil CreateDataSourceatau UpdateDataSourceAPI.

File konfigurasi berisi struktur JSON yang mengidentifikasi prefiks S3 dan mencantumkan pengaturan akses untuk prefiks. Prefiks dapat berupa jalur, atau file individual. Jika prefiks berupa jalur, pengaturan akses berlaku untuk semua file di jalur tersebut. Ada jumlah maksimum awalan S3 dalam file konfigurasi JSON dan ukuran file maksimum default. Lihat informasi yang lebih lengkap di Kuota untuk Amazon Kendra

Anda dapat menentukan pengguna dan grup dalam pengaturan akses. Saat melakukan kueri indeks, Anda menentukan informasi pengguna dan grup. Untuk informasi selengkapnya, lihat Pemfilteran berdasarkan atribut.

Struktur JSON untuk file konfigurasi harus dalam format berikut:

```
[
    {
```

```
        "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"
            }
        ]
    }
]
```

Menggunakan Amazon VPC dengan sumber Amazon S3 data

Topik ini memberikan step-by-step contoh yang menunjukkan cara menyambung ke bucket Amazon S3 dengan menggunakan konektor Amazon S3 melalui Amazon VPC. Contohnya mengasumsikan bahwa Anda memulai dengan bucket S3 yang ada. Kami menyarankan Anda mengunggah hanya beberapa dokumen ke bucket S3 Anda untuk menguji contoh.

Anda dapat terhubung Amazon Kendra ke Amazon S3 ember Anda melalui Amazon VPC. Untuk melakukannya, Anda harus menentukan Amazon VPC subnet dan grup Amazon VPC keamanan saat membuat konektor sumber Amazon S3 data Anda.

> **Important**
>
> Agar Amazon Kendra Amazon S3 konektor dapat mengakses Amazon S3 bucket Anda, pastikan Anda telah menetapkan Amazon S3 titik akhir ke virtual private cloud (VPC) Anda.

Amazon Kendra Untuk menyinkronkan dokumen dari Amazon S3 bucket Anda Amazon VPC, Anda harus menyelesaikan langkah-langkah berikut:

- Siapkan Amazon S3 titik akhir untuk Amazon VPC. Untuk informasi selengkapnya tentang cara menyiapkan Amazon S3 titik akhir, lihat titik akhir Gateway Amazon S3 di AWS PrivateLink Panduan.
- (Opsional) Memeriksa kebijakan Amazon S3 bucket Anda untuk memastikan Amazon S3 bucket dapat diakses dari virtual private cloud (VPC) yang Anda tetapkan. Amazon KendraUntuk informasi selengkapnya, lihat Mengontrol akses dari titik akhir VPC dengan kebijakan bucket di Panduan Pengguna Amazon S3

Langkah-langkah

- Langkah 1: Konfigurasikan Amazon VPC
- (Opsional) Langkah 2: Konfigurasikan kebijakan Amazon S3 bucket
- Langkah 3: Buat konektor sumber Amazon S3 data uji

Langkah 1: Konfigurasikan Amazon VPC

Buat jaringan VPC termasuk subnet pribadi dengan titik akhir Amazon S3 gateway dan grup keamanan untuk Amazon Kendra digunakan nanti.

Untuk mengonfigurasi VPC dengan subnet pribadi, titik akhir S3, dan grup keamanan

1. Masuk ke AWS Management Console dan buka Amazon VPC konsol dihttps://console.aws.amazon.com/vpc/.
2. Buat VPC dengan subnet pribadi dan titik akhir S3 untuk digunakan: Amazon Kendra

Dari panel navigasi, pilih VPC Anda, lalu pilih Buat VPC.

a. Agar Sumber Daya dapat dibuat, pilih VPC dan lainnya.

b. Untuk tag Nama, aktifkan Auto-generate, lalu masukkan**`kendra-s3-example`**.

c. Untuk blok IPv4/IPv6 CIDR, pertahankan nilai default.

d. Untuk Jumlah Availability Zones (AZ), pilih nomor 1.

e. Pilih Sesuaikan AZ, lalu pilih Availability Zone dari daftar zona ketersediaan pertama.

   Amazon Kendra hanya mendukung satu set Availability Zone tertentu.

f. Untuk Jumlah subnet publik, pilih nomor 0.

g. Untuk Jumlah subnet pribadi, pilih nomor 1.

h. Untuk gateway NAT, pilih None.

i. Untuk titik akhir VPC, pilih gateway.Amazon S3 .

j. Biarkan sisa nilai pada pengaturan defaultnya.

k. Pilih Buat VPC.

   Tunggu hingga alur kerja Create VPC selesai. Kemudian, pilih Lihat VPC untuk memeriksa VPC yang baru saja Anda buat.

Anda sekarang telah membuat jaringan VPC dengan subnet pribadi, yang tidak memiliki akses ke internet publik.

3. Salin ID titik akhir VPC Anda dari titik akhir Amazon S3 Anda:

   a. Dari panel navigasi, pilih Titik akhir.

   b. Dalam daftar Endpoints, temukan endpoint Amazon S3 `kendra-s3-example-vpce-s3` yang baru saja Anda buat bersama dengan VPC Anda.

   c. Catat ID titik akhir VPC.

   Anda sekarang telah membuat titik akhir gateway Amazon S3 untuk mengakses bucket Amazon S3 Anda melalui subnet.

4. Buat Grup Keamanan Amazon Kendra untuk digunakan:

   a. Dari panel navigasi, pilih Grup Keamanan, lalu pilih Buat grup keamanan.

   b. Untuk Nama grup keamanan, masukkan **`s3-data-source-security-group`**.

c. Pilih VPC Anda dari daftar. Amazon VPC

d. Biarkan aturan masuk dan aturan keluar sebagai default.

e. Pilih Buat grup keamanan.

Anda sekarang telah membuat grup keamanan VPC.

Anda menetapkan subnet dan grup keamanan yang Anda buat ke konektor sumber data Amazon S3 selama proses konfigurasi konektor. Amazon Kendra

(Opsional) Langkah 2: Konfigurasikan kebijakan Amazon S3 bucket

Pada langkah opsional ini, pelajari cara mengonfigurasi kebijakan bucket Amazon S3 sehingga bucket Amazon S3 Anda hanya dapat diakses dari VPC yang Anda tetapkan. Amazon Kendra

Amazon Kendra menggunakan peran IAM untuk mengakses bucket Amazon S3 Anda dan tidak mengharuskan Anda mengonfigurasi kebijakan bucket Amazon S3. Namun, Anda mungkin merasa berguna untuk membuat kebijakan bucket jika ingin mengonfigurasi Amazon S3 konektor menggunakan bucket Amazon S3 yang memiliki kebijakan yang membatasi aksesnya dari internet publik.

Untuk mengonfigurasi kebijakan Amazon S3 bucket

1. Buka konsol Amazon S3 di. https://console.aws.amazon.com/s3/
2. Dari panel navigasi, pilih Bucket.
3. Pilih nama bucket Amazon S3 yang ingin Anda sinkronkan. Amazon Kendra
4. Pilih tab Izin, gulir ke bawah ke kebijakan Bucket, lalu klik Edit.
5. Tambahkan atau ubah kebijakan bucket Anda untuk mengizinkan akses hanya dari titik akhir VPC yang Anda buat.

   Berikut ini adalah contoh kebijakan bucket. Ganti *bucket-name*dan *vpce-id*dengan nama bucket Amazon S3 dan ID endpoint Amazon S3 yang Anda catat sebelumnya.

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

```
      "Action": "s3:*",
      "Resource": "arn:aws:s3:::bucket-name/*",
      "Condition": {
        "StringNotEquals": {
          "aws:SourceVpce": "vpce-id"
        }
      }
    }
  ]
}
```

6. Pilih Simpan perubahan.

Bucket S3 Anda sekarang hanya dapat diakses dari VPC tertentu yang Anda buat.

Langkah 3: Buat konektor sumber Amazon S3 data uji

Untuk menguji Amazon VPC konfigurasi Anda, buat Amazon S3 konektor. Kemudian, konfigurasikan dengan VPC yang Anda buat dengan mengikuti langkah-langkah yang diuraikan. Amazon S3

Untuk nilai Amazon VPC konfigurasi, pilih nilai yang Anda buat selama contoh ini:

- Amazon VPC(VPC) — `kendra-s3-example-vpc`
- Subnet — `kendra-s3-example-subnet-private1-[availability zone]`
- Kelompok keamanan - `s3-data-source-security-group`

Tunggu konektor Anda selesai dibuat. Setelah Amazon S3 konektor dibuat, pilih Sinkronkan sekarang untuk memulai sinkronisasi.

Mungkin perlu beberapa menit hingga beberapa jam untuk menyelesaikan sinkronisasi, tergantung pada berapa banyak dokumen yang ada di Amazon S3 ember Anda. Untuk menguji contoh, sebaiknya Anda mengunggah beberapa dokumen saja ke bucket S3 Anda. Jika konfigurasi Anda benar, pada akhirnya Anda akan melihat status Sinkronisasi Selesai.

Jika Anda menemukan kesalahan, lihat Memecahkan masalah koneksi Amazon VPC.

Amazon Kendra Perayap Web

Anda dapat menggunakan Amazon Kendra Web Crawler untuk merayapi dan mengindeks halaman web.

Anda hanya dapat merayapi situs web publik atau situs web perusahaan internal yang menggunakan protokol komunikasi aman Hypertext Transfer Protocol Secure (HTTPS). Jika Anda menerima kesalahan saat merayapi situs web, bisa jadi situs web tersebut diblokir dari perayapan. Untuk merayapi situs web internal, Anda dapat mengatur proxy web. Proxy web harus menghadap publik. Anda juga dapat menggunakan otentikasi untuk mengakses dan merayapi situs web.

Saat memilih situs web untuk diindeks, Anda harus mematuhi Kebijakan Penggunaan yang Diterima Amazon dan semua syarat Amazon lainnya. Ingat bahwa Anda hanya harus menggunakan Amazon Kendra Web Crawler untuk mengindeks halaman web Anda sendiri, atau halaman web yang Anda memiliki otorisasi untuk indeks. Untuk mempelajari cara menghentikan Amazon Kendra Web Crawler dari mengindeks situs web Anda, silakan lihat. Mengkonfigurasi *robots.txt* file untuk Amazon Kendra Web Crawler

> **Note**
>
> Menyalahgunakan Amazon Kendra Web Crawler untuk secara agresif merayapi situs web atau halaman web yang tidak Anda miliki dianggap penggunaan yang dapat diterima.

Amazon Kendra memiliki dua versi web crawler konektor. Fitur yang didukung dari setiap versi meliputi:

Amazon Kendra Konektor Web Crawler v1.0 /API WebCrawlerConfiguration

- Proksi web
- Filter inklusi/pengecualian

Amazon Kendra Konektor Web Crawler v2.0/API TemplateConfiguration

- Pemetaan lapangan
- Filter inklusi/pengecualian
- Sinkronisasi konten penuh dan tambahan
- Proksi web
- Dasar, NTLM/Kerberos, SAMP, dan otentikasi formulir untuk situs web Anda
- Cloud privat virtual (VPC)

> **Important**
>
> Pembuatan konektor Web Crawler v2.0 tidak didukung oleh. AWS CloudFormation Gunakan konektor Web Crawler v1.0 jika Anda memerlukan AWS CloudFormation dukungan.

Untuk memecahkan masalah konektor sumber data crawler Amazon Kendra web Anda, lihat. Mengatasi masalah sumber data

Topik

- Amazon Kendra Konektor Web Crawler v1.0
- Amazon Kendra Konektor Web Crawler v2.0
- Mengkonfigurasi robots.txt file untuk Amazon Kendra Web Crawler

Amazon Kendra Konektor Web Crawler v1.0

Anda dapat menggunakan Amazon Kendra Web Crawler untuk merayapi dan mengindeks halaman web.

Anda hanya dapat merayapi situs web dan situs web yang menghadap publik yang menggunakan protokol komunikasi aman Hypertext Transfer Protocol Secure (HTTPS). Jika Anda menerima kesalahan saat merayapi situs web, bisa jadi situs web tersebut diblokir dari perayapan. Untuk merayapi situs web internal, Anda dapat mengatur proxy web. Proxy web harus menghadap publik.

Saat memilih situs web untuk diindeks, Anda harus mematuhi Kebijakan Penggunaan yang Diterima Amazon dan semua syarat Amazon lainnya. Ingat bahwa Anda hanya harus menggunakan Amazon Kendra Web Crawler untuk mengindeks halaman web Anda sendiri, atau halaman web yang Anda memiliki otorisasi untuk indeks. Untuk mempelajari cara menghentikan Amazon Kendra Web Crawler dari mengindeks situs web Anda, silakan lihat. Mengkonfigurasi *robots.txt* file untuk Amazon Kendra Web Crawler

> **Note**
>
> Menyalahgunakan Amazon Kendra Web Crawler untuk secara agresif merayapi situs web atau halaman web yang tidak Anda miliki dianggap penggunaan yang dapat diterima.

Untuk memecahkan masalah konektor sumber data crawler Amazon Kendra web Anda, lihat. Mengatasi masalah sumber data

Topik

- Fitur yang didukung
- Prasyarat
- Instruksi koneksi
- Pelajari selengkapnya

Fitur yang didukung

- Proksi web
- Filter inklusi/pengecualian

Prasyarat

Sebelum Anda dapat menggunakan Amazon Kendra untuk mengindeks situs web Anda, periksa detail situs web dan AWS akun Anda.

Untuk situs web Anda, pastikan Anda memiliki:

- Menyalin URL benih atau peta situs dari situs web yang ingin Anda indeks.
- Untuk situs web yang memerlukan otentikasi dasar: Mencatat nama pengguna dan kata sandi, dan menyalin nama host situs web dan nomor port.
- Opsional: Menyalin nama host situs web dan nomor port jika Anda ingin menggunakan proxy web untuk terhubung ke situs web internal yang ingin dirayapi. Proxy web harus menghadap publik. Amazon Kendra mendukung koneksi ke server proxy web yang didukung oleh otentikasi dasar atau Anda dapat terhubung tanpa otentikasi.
- Memeriksa setiap dokumen halaman web yang ingin Anda indeks adalah unik dan di seluruh sumber data lain yang Anda rencanakan untuk digunakan untuk indeks yang sama. Setiap sumber data yang ingin Anda gunakan untuk indeks tidak boleh berisi dokumen yang sama di seluruh sumber data. ID dokumen bersifat global untuk indeks dan harus unik per indeks.

Di AWS akun Anda, pastikan Anda memiliki:

- Membuat Amazon Kendra indeks dan, jika menggunakan API, mencatat ID indeks.

- Membuat IAM peran untuk sumber data Anda dan, jika menggunakan API, catat ARN peran tersebut IAM .

> **Note**
>
> Jika Anda mengubah jenis otentikasi dan kredensialnya, Anda harus memperbarui IAM peran Anda untuk mengakses ID rahasia yang benar AWS Secrets Manager .

- Untuk situs web yang memerlukan otentikasi, atau jika menggunakan proxy web dengan otentikasi, menyimpan kredensyal otentikasi Anda secara AWS Secrets Manager rahasia dan, jika menggunakan API, catat ARN rahasia tersebut.

> **Note**
>
> Kami menyarankan Anda secara teratur menyegarkan atau memutar kredensyal dan rahasia Anda. Berikan hanya tingkat akses yang diperlukan untuk keamanan Anda sendiri. Kami tidak menyarankan Anda menggunakan kembali kredensyal dan rahasia di seluruh sumber data, dan konektor versi 1.0 dan 2.0 (jika berlaku).

Jika Anda tidak memiliki IAM peran atau rahasia yang ada, Anda dapat menggunakan konsol untuk membuat IAM peran dan Secrets Manager rahasia baru saat Anda menghubungkan sumber web crawler data Anda Amazon Kendra. Jika Anda menggunakan API, Anda harus memberikan ARN IAM peran dan Secrets Manager rahasia yang ada, dan ID indeks.

Instruksi koneksi

Untuk terhubung Amazon Kendra ke sumber web crawler data Anda, Anda harus memberikan rincian yang diperlukan dari sumber web crawler data Anda sehingga Amazon Kendra dapat mengakses data Anda. Jika Anda belum mengkonfigurasi web crawler untuk Amazon Kendra lihatPrasyarat.

Console

Untuk terhubung Amazon Kendra ke web crawler

1. Masuk ke AWS Management Console dan buka Amazon Kendra konsol.
2. Dari panel navigasi kiri, pilih Indeks dan kemudian pilih indeks yang ingin Anda gunakan dari daftar indeks.

> **Note**
>
> Anda dapat memilih untuk mengonfigurasi atau mengedit pengaturan kontrol akses Pengguna Anda di bawah Pengaturan indeks.

3. Pada halaman Memulai, pilih Tambahkan sumber data.
4. Pada halaman Tambah sumber data, pilih konektor web crawler, lalu pilih Tambah konektor.
5. Pada halaman Tentukan detail sumber data, masukkan informasi berikut:

   a. Di Nama dan deskripsi, untuk Nama sumber data —Masukkan nama untuk sumber data Anda. Anda dapat memasukkan tanda hubung tetapi bukan spasi.

   b. (Opsional) Deskripsi —Masukkan deskripsi opsional untuk sumber data Anda.

   c. Dalam Bahasa default —Pilih bahasa untuk memfilter dokumen Anda untuk indeks. Kecuali Anda menentukan sebaliknya, bahasa default ke bahasa Inggris. Bahasa yang ditentukan dalam metadata dokumen mengesampingkan bahasa yang dipilih.

   d. Di Tag, untuk Tambahkan tag baru —Sertakan tag opsional untuk mencari dan memfilter sumber daya Anda atau melacak AWS biaya Anda.

   e. Pilih Berikutnya.

6. Pada halaman Tentukan akses dan keamanan, masukkan informasi berikut:

   a. Untuk Sumber, pilih antara URL Sumber dan peta situs Sumber tergantung pada kasus penggunaan Anda dan masukkan nilai untuk masing-masing.

      Anda dapat menambahkan hingga 10 URL sumber dan tiga peta situs.

      > **Note**
      >
      > Jika Anda ingin merayapi peta situs, periksa apakah URL dasar atau root sama dengan URL yang tercantum di halaman peta situs Anda. Misalnya, jika URL peta situs Anda https://example.com/sitemap-page.html, URL yang tercantum di halaman peta situs ini juga harus menggunakan URL dasar "". https://example.com/

   b. (Opsional) Untuk proxy Web — masukkan informasi berikut:

      i. Nama host —Nama host tempat proxy web diperlukan.

ii. Nomor port —Port yang digunakan oleh protokol transport URL host. Nomor port harus berupa nilai numerik antara 0 dan 65535.

iii. Untuk kredensyal proxy Web —Jika koneksi proxy web Anda memerlukan otentikasi, pilih rahasia yang ada atau buat rahasia baru untuk menyimpan kredensyal otentikasi Anda. Jika Anda memilih untuk membuat rahasia baru, jendela AWS Secrets Manager rahasia terbuka.

iv. Masukkan informasi berikut di jendela Buat AWS Secrets Manager Secrets Manager rahasia:

A. Nama rahasia —Nama untuk rahasiamu. Awalan 'AmazonKendra-WebCrawler-' secara otomatis ditambahkan ke nama rahasia Anda.

B. Untuk Nama Pengguna dan Kata Sandi —Masukkan kredensyal otentikasi dasar ini untuk situs web Anda.

C. Pilih Simpan.

c. (Opsional) Host dengan otentikasi —Pilih untuk menambahkan host tambahan dengan otentikasi.

d. IAM peran —Pilih peran yang sudah ada atau buat IAM IAM peran baru untuk mengakses kredensi repositori dan mengindeks konten Anda.

> **Note**
>
> IAM peran yang digunakan untuk indeks tidak dapat digunakan untuk sumber data. Jika Anda tidak yakin apakah peran yang ada digunakan untuk indeks atau FAQ, pilih Buat peran baru untuk menghindari kesalahan.

e. Pilih Berikutnya.

7. Pada halaman Konfigurasi pengaturan sinkronisasi, masukkan informasi berikut:

a. Rentang perayapan —Pilih jenis halaman web yang ingin dirayapi.

b. Kedalaman perayapan —Pilih jumlah level dari URL seed yang Amazon Kendra seharusnya di-crawl.

c. Pengaturan crawl lanjutan dan Konfigurasi tambahan masukkan informasi berikut:

i. Ukuran file maksimum —Halaman web maksimum atau ukuran lampiran untuk dirayapi. Minimum 0,000001 MB (1 byte). Maksimal 50 MB.

ii. Tautan maksimum per halaman —Jumlah maksimum tautan yang dirayapi per halaman. Tautan dirayapi sesuai urutan penampilan. Minimal 1 tautan/halaman. Maksimal 1000 tautan/halaman.

iii. Pelambatan maksimum —Jumlah maksimum URL yang dirayapi per nama host per menit. Minimal 1 URL/nama host-/menit. Maksimal 300 URL/nama host-/menit.

iv. Pola Regex —Tambahkan pola ekspresi reguler untuk menyertakan atau mengecualikan URL tertentu. Anda dapat menambahkan hingga 100 pola.

d. Di Jadwal lari Sinkronisasi, untuk Frekuensi —Pilih seberapa sering Amazon Kendra akan disinkronkan dengan sumber data Anda.

e. Pilih Berikutnya.

8. Pada halaman Tinjau dan buat, periksa apakah informasi yang Anda masukkan sudah benar dan kemudian pilih Tambahkan sumber data. Anda juga dapat memilih untuk mengedit informasi Anda dari halaman ini. Sumber data Anda akan muncul di halaman Sumber data setelah sumber data berhasil ditambahkan.

API

Untuk terhubung Amazon Kendra ke web crawler

Anda harus menentukan yang berikut menggunakan WebCrawlerConfigurationAPI:

- URL —Tentukan URL benih atau titik awal situs web atau URL peta situs situs web yang ingin Anda jelajahi menggunakan dan. SeedUrlConfigurationSiteMapsConfiguration

> **Note**
>
> Jika Anda ingin merayapi peta situs, periksa apakah URL dasar atau root sama dengan URL yang tercantum di halaman peta situs Anda. Misalnya, jika URL peta situs Anda https://example.com/sitemap-page.html, URL yang tercantum di halaman peta situs ini juga harus menggunakan URL dasar "". https://example.com/

- Rahasia Nama Sumber Daya Amazon (ARN) —Jika sebuah situs web memerlukan otentikasi dasar, Anda memberikan nama host, nomor port, dan rahasia yang menyimpan kredensyal otentikasi dasar nama pengguna dan kata sandi Anda. Anda memberikan ARN rahasia menggunakan API. AuthenticationConfiguration Rahasianya disimpan dalam struktur JSON dengan kunci berikut:

```
{
    "username": "user name",
    "password": "password"
}
```

Anda juga dapat memberikan kredensyal proxy web menggunakan rahasia. AWS Secrets Manager Anda menggunakan ProxyConfigurationAPI untuk memberikan nama host situs web dan nomor port, dan secara opsional rahasia yang menyimpan kredensyal proxy web Anda.

- IAM peran —Tentukan `RoleArn` kapan Anda menelepon `CreateDataSource` untuk memberikan IAM peran dengan izin untuk mengakses Secrets Manager rahasia Anda dan memanggil API publik yang diperlukan untuk konektor perayap web dan. Amazon Kendra Untuk informasi selengkapnya, lihat IAM peran untuk sumber data perayap web.

Anda juga dapat menambahkan fitur opsional berikut:

- Mode perayapan —Pilih apakah akan merayapi nama host situs web saja, atau nama host dengan subdomain, atau juga merayapi domain lain yang ditautkan ke halaman web.
- 'Kedalaman' atau jumlah level dari tingkat benih hingga merangkak. Misalnya, halaman URL benih adalah kedalaman 1 dan hyperlink apa pun di halaman ini yang juga dirayapi adalah kedalaman 2.
- Jumlah maksimum URL pada satu halaman web untuk dirayapi.
- Ukuran maksimum dalam MB halaman web untuk dirayapi.
- Jumlah maksimum URL yang dirayapi per host situs web per menit.
- Host proxy web dan nomor port untuk terhubung ke dan merayapi situs web internal. Misalnya, nama host https://a.example.com/page1.htmladalah "a.example.com" dan nomor port adalah 443, port standar untuk HTTPS. Jika kredensyal proxy web diperlukan untuk terhubung ke host situs web, Anda dapat membuat AWS Secrets Manager yang menyimpan kredensialnya.
- Informasi autentikasi untuk mengakses dan merayapi situs web yang memerlukan autentikasi pengguna.
- Anda dapat mengekstrak tag meta HTML sebagai bidang menggunakan alat Pengayaan Dokumen Kustom. Untuk informasi selengkapnya, lihat Menyesuaikan metadata dokumen selama proses konsumsi. Untuk contoh mengekstrak tag meta HTML, lihat contoh CDE.
- Filter inklusi dan pengecualian —Tentukan apakah akan menyertakan atau mengecualikan URL tertentu.

> **Note**
>
> Sebagian besar sumber data menggunakan pola ekspresi reguler, yang merupakan pola inklusi atau pengecualian yang disebut sebagai filter. Jika Anda menentukan filter inklusi, hanya konten yang cocok dengan filter inklusi yang diindeks. Dokumen apa pun yang tidak cocok dengan filter inklusi tidak diindeks. Jika Anda menentukan filter inklusi dan pengecualian, dokumen yang cocok dengan filter pengecualian tidak akan diindeks, meskipun sesuai dengan filter inklusi.

Pelajari selengkapnya

Untuk mempelajari lebih lanjut tentang mengintegrasikan Amazon Kendra dengan sumber web crawler data Anda, lihat:

- Bayangkan kembali penemuan pengetahuan menggunakan Web Amazon Kendra Crawler

Amazon Kendra Konektor Web Crawler v2.0

Anda dapat menggunakan Amazon Kendra Web Crawler untuk merayapi dan mengindeks halaman web.

Anda hanya dapat merayapi situs web publik atau situs web perusahaan internal yang menggunakan protokol komunikasi aman Hypertext Transfer Protocol Secure (HTTPS). Jika Anda menerima kesalahan saat merayapi situs web, bisa jadi situs web tersebut diblokir dari perayapan. Untuk merayapi situs web internal, Anda dapat mengatur proxy web. Proxy web harus menghadap publik. Anda juga dapat menggunakan otentikasi untuk mengakses dan merayapi situs web.

Amazon Kendra Web Crawler v2.0 menggunakan paket perayap web Selenium dan driver Chromium. Amazon Kendra secara otomatis memperbarui versi Selenium dan driver Chromium menggunakan Continuous Integration (CI).

Saat memilih situs web untuk diindeks, Anda harus mematuhi Kebijakan Penggunaan yang Diterima Amazon dan semua syarat Amazon lainnya. Ingat bahwa Anda hanya harus menggunakan Amazon Kendra Web Crawler untuk mengindeks halaman web Anda sendiri, atau halaman web yang Anda memiliki otorisasi untuk indeks. Untuk mempelajari cara menghentikan Amazon Kendra Web Crawler dari mengindeks situs web Anda, silakan lihat. Mengkonfigurasi *robots.txt* file untuk Amazon Kendra Web Crawler . Menyalahgunakan Amazon Kendra Web Crawler untuk secara agresif

merayapi situs web atau halaman web yang tidak Anda miliki dianggap penggunaan yang dapat diterima.

Untuk memecahkan masalah konektor sumber data crawler Amazon Kendra web Anda, lihat. Mengatasi masalah sumber data

> **Note**
>
> Konektor Web Crawler v2.0 tidak mendukung crawling daftar situs web dari AWS KMS bucket terenkripsi. Amazon S3 Ini hanya mendukung enkripsi sisi server dengan Amazon S3 kunci terkelola.

> **Important**
>
> Pembuatan konektor Web Crawler v2.0 tidak didukung oleh. AWS CloudFormation Gunakan konektor Web Crawler v1.0 jika Anda memerlukan AWS CloudFormation dukungan.

Topik

Fitur yang didukung

- Pemetaan lapangan
- Filter inklusi/pengecualian
- Sinkronisasi konten penuh dan tambahan
- Proksi web
- Dasar, NTLM/Kerberos, SAMP, dan otentikasi formulir untuk situs web Anda
- Cloud privat virtual (VPC)

Prasyarat

Sebelum Anda dapat menggunakan Amazon Kendra untuk mengindeks situs web Anda, periksa detail situs web dan AWS akun Anda.

Untuk situs web Anda, pastikan Anda memiliki:

- Menyalin URL benih atau peta situs dari situs web yang ingin Anda indeks. Anda dapat menyimpan URL dalam file teks dan mengunggahnya ke Amazon S3 bucket. Setiap URL dalam file teks harus diformat pada baris terpisah. Jika Anda ingin menyimpan peta situs Anda dalam sebuah Amazon S3 bucket, pastikan Anda telah menyalin XMLsitemap dan menyimpannya dalam file XML.5. Anda juga dapat memasukkan beberapa file XMLpeta situs ke dalam file ZIP.

  > **Note**
  >
  > (On-premise/server) Amazon Kendra memeriksa apakah informasi titik akhir yang disertakan sama dengan informasi titik akhir yang AWS Secrets Manager ditentukan dalam detail konfigurasi sumber data Anda. Ini membantu melindungi dari masalah wakil yang membingungkan, yang merupakan masalah keamanan di mana pengguna tidak memiliki izin untuk melakukan tindakan tetapi menggunakan Amazon Kendra sebagai proxy untuk mengakses rahasia yang dikonfigurasi dan melakukan tindakan. Jika nanti Anda mengubah informasi titik akhir Anda, Anda harus membuat rahasia baru untuk menyinkronkan informasi ini.

- Untuk situs web yang memerlukan otentikasi dasar, NTLM, atau Kerberos:
  - Mencatat kredensi otentikasi situs web Anda, yang mencakup nama pengguna dan kata sandi.

    > **Note**
    >
    > Amazon Kendra Web Crawler v2.0 mendukung protokol otentikasi NTLM yang mencakup hashing kata sandi, dan protokol otentikasi Kerberos yang mencakup enkripsi kata sandi.

- Untuk situs web yang memerlukan SAMP atau otentikasi formulir login:
  - Mencatat kredensi otentikasi situs web Anda, yang mencakup nama pengguna dan kata sandi.
  - Menyalin XPaths (XMLPath Language) dari bidang nama pengguna (dan tombol nama pengguna jika menggunakan SAMP), bidang kata sandi dan tombol, dan menyalin URL halaman

login. Anda dapat menemukan elemen XPaths menggunakan alat pengembang browser web Anda. XPaths biasanya mengikuti format ini:`//tagname[@Attribute='Value']`.

> **Note**
>
> Amazon Kendra Web Crawler v2.0 menggunakan browser Chrome tanpa kepala dan informasi dari formulir untuk mengautentikasi dan mengotorisasi akses dengan URL yang dilindungi OAuth 2.0.

- Opsional: Menyalin nama host dan nomor port server proxy web jika Anda ingin menggunakan proxy web untuk terhubung ke situs web internal yang ingin dirayapi. Proxy web harus menghadap publik. Amazon Kendra mendukung koneksi ke server proxy web yang didukung oleh otentikasi dasar atau Anda dapat terhubung tanpa otentikasi.
- Opsional: Menyalin ID subnet virtual private cloud (VPC) jika Anda ingin menggunakan VPC untuk terhubung ke situs web internal yang ingin dirayapi. Untuk informasi selengkapnya, lihat Mengonfigurasi file Amazon VPC.
- Memeriksa setiap dokumen halaman web yang ingin Anda indeks adalah unik dan di seluruh sumber data lain yang Anda rencanakan untuk digunakan untuk indeks yang sama. Setiap sumber data yang ingin Anda gunakan untuk indeks tidak boleh berisi dokumen yang sama di seluruh sumber data. ID dokumen bersifat global untuk indeks dan harus unik per indeks.

Di AWS akun Anda, pastikan Anda memiliki:

- Membuat Amazon Kendra indeks dan, jika menggunakan API, mencatat ID indeks.
- Membuat IAM peran untuk sumber data Anda dan, jika menggunakan API, catat ARN peran tersebut IAM .

> **Note**
>
> Jika Anda mengubah jenis otentikasi dan kredensialnya, Anda harus memperbarui IAM peran Anda untuk mengakses ID rahasia yang benar AWS Secrets Manager .

- Untuk situs web yang memerlukan otentikasi, atau jika menggunakan proxy web dengan otentikasi, menyimpan kredensyal otentikasi Anda secara AWS Secrets Manager rahasia dan, jika menggunakan API, catat ARN rahasia tersebut.

> **Note**
>
> Kami menyarankan Anda secara teratur menyegarkan atau memutar kredensyal dan rahasia Anda. Berikan hanya tingkat akses yang diperlukan untuk keamanan Anda sendiri. Kami tidak menyarankan Anda menggunakan kembali kredensyal dan rahasia di seluruh sumber data, dan konektor versi 1.0 dan 2.0 (jika berlaku).

Jika Anda tidak memiliki IAM peran atau rahasia yang ada, Anda dapat menggunakan konsol untuk membuat IAM peran dan Secrets Manager rahasia baru saat Anda menghubungkan sumber web crawler data Anda Amazon Kendra. Jika Anda menggunakan API, Anda harus memberikan ARN IAM peran dan Secrets Manager rahasia yang ada, dan ID indeks.

Instruksi koneksi

Untuk terhubung Amazon Kendra ke sumber web crawler data Anda, Anda harus memberikan rincian yang diperlukan dari sumber web crawler data Anda sehingga Amazon Kendra dapat mengakses data Anda. Jika Anda belum mengkonfigurasi web crawler untuk Amazon Kendra lihatPrasyarat.

Console

Untuk terhubung Amazon Kendra ke web crawler

1. Masuk ke AWS Management Console dan buka Amazon Kendra konsol.
2. Dari panel navigasi kiri, pilih Indeks dan kemudian pilih indeks yang ingin Anda gunakan dari daftar indeks.

   > **Note**
   >
   > Anda dapat memilih untuk mengonfigurasi atau mengedit pengaturan kontrol akses Pengguna Anda di bawah Pengaturan indeks.

3. Pada halaman Memulai, pilih Tambahkan sumber data.
4. Pada halaman Tambah sumber data, pilih konektor web crawler, lalu pilih Tambah konektor.
5. Pada halaman Tentukan detail sumber data, masukkan informasi berikut:

   a. Di Nama dan deskripsi, untuk Nama sumber data —Masukkan nama untuk sumber data Anda. Anda dapat memasukkan tanda hubung tetapi bukan spasi.

b. (Opsional) Deskripsi —Masukkan deskripsi opsional untuk sumber data Anda.

c. Dalam Bahasa default —Pilih bahasa untuk memfilter dokumen Anda untuk indeks. Kecuali Anda menentukan sebaliknya, bahasa default ke bahasa Inggris. Bahasa yang ditentukan dalam metadata dokumen mengesampingkan bahasa yang dipilih.

d. Di Tag, untuk Tambahkan tag baru —Sertakan tag opsional untuk mencari dan memfilter sumber daya Anda atau melacak AWS biaya Anda.

e. Pilih Berikutnya.

6. Pada halaman Tentukan akses dan keamanan, masukkan informasi berikut:

a. Sumber —Pilih URL Sumber, Peta Situs Sumber, File URL Sumber, File peta situs Sumber. Jika Anda memilih untuk menggunakan file teks yang menyertakan daftar hingga 100 URL benih, Anda menentukan jalur ke Amazon S3 bucket tempat file Anda disimpan. Jika Anda memilih untuk menggunakan file XMLpeta situs, Anda menentukan path ke Amazon S3 bucket tempat file Anda disimpan. Anda juga dapat memasukkan beberapa file XMLpeta situs ke dalam file ZIP. Jika tidak, Anda dapat memasukkan hingga 10 URL benih atau titik awal secara manual, dan hingga tiga URL peta situs.

> **Note**
>
> Jika Anda ingin merayapi peta situs, periksa apakah URL dasar atau root sama dengan URL yang tercantum di halaman peta situs Anda. Misalnya, jika URL peta situs Anda https://example.com/sitemap-page.html, URL yang tercantum di halaman peta situs ini juga harus menggunakan URL dasar "". https://example.com/

Jika situs web Anda memerlukan otentikasi untuk mengakses situs web, Anda dapat memilih ether basic, NTLM/Kerberos, SAMP, atau otentikasi formulir. Jika tidak, pilih opsi untuk tidak ada otentikasi.

> **Note**
>
> Jika Anda ingin mengedit sumber data nanti untuk mengubah URL benih Anda dengan otentikasi ke peta situs, Anda harus membuat sumber data baru. Amazon Kendra mengonfigurasi sumber data menggunakan informasi titik akhir

URL benih dalam Secrets Manager rahasia untuk otentikasi, dan oleh karena itu tidak dapat mengonfigurasi ulang sumber data saat mengubah ke peta situs.

- AWS Secrets Manager Jika situs web Anda memerlukan otentikasi yang sama untuk mengakses situs web, pilih rahasia yang ada atau buat Secrets Manager rahasia baru untuk menyimpan kredensyal situs web Anda. Jika Anda memilih untuk membuat rahasia baru, jendela AWS Secrets Manager rahasia terbuka.

  Jika Anda memilih otentikasi Dasar atau NTML/KerberOS, masukkan nama untuk rahasia, ditambah nama pengguna dan kata sandi. Protokol otentikasi NTLM mencakup hashing kata sandi, dan protokol otentikasi Kerberos mencakup enkripsi kata sandi.

  Jika Anda memilih SAMP atau otentikasi Formulir, masukkan nama untuk rahasia, ditambah nama pengguna dan kata sandi. Gunakan XPath untuk bidang nama pengguna (dan XPath untuk tombol nama pengguna jika menggunakan SAFL). Gunakan XPaths untuk bidang kata sandi dan tombol, dan URL halaman login. Anda dapat menemukan elemen XPaths (XMLPath Language) menggunakan alat pengembang browser web Anda. XPaths biasanya mengikuti format ini:`//tagname[@Attribute='Value']`.

b. (Opsional) Web proxy —Masukkan nama host dan nomor port dari proxy sever yang ingin Anda gunakan untuk terhubung ke situs web internal. Misalnya, nama host https://a.example.com/page1.htmladalah "a.example.com" dan nomor port adalah 443, port standar untuk HTTPS. Jika kredensyal proxy web diperlukan untuk terhubung ke host situs web, Anda dapat membuat AWS Secrets Manager yang menyimpan kredensialnya.

c. Virtual Private Cloud (VPC) —Anda dapat memilih untuk menggunakan VPC. Jika demikian, Anda harus menambahkan Subnet dan grup keamanan VPC.

d. IAM peran —Pilih peran yang sudah ada atau buat IAM IAM peran baru untuk mengakses kredensi repositori dan mengindeks konten Anda.

> **Note**
>
> IAM peran yang digunakan untuk indeks tidak dapat digunakan untuk sumber data. Jika Anda tidak yakin apakah peran yang ada digunakan untuk indeks atau FAQ, pilih Buat peran baru untuk menghindari kesalahan.

e. Pilih Berikutnya.

7. Pada halaman Konfigurasi pengaturan sinkronisasi, masukkan informasi berikut:

   a. Lingkup sinkronisasi —Tetapkan batas untuk merayapi halaman web termasuk domain, ukuran file, dan tautannya; dan filter URL menggunakan pola regex.

      i. (Opsional) Rentang domain crawl —Pilih apakah akan merayapi domain situs web saja, domain dengan subdomain, atau juga merayapi domain lain yang ditautkan oleh halaman web. Secara default, Amazon Kendra hanya merayapi domain situs web yang ingin Anda jelajahi.

      ii. (Opsional) Konfigurasi tambahan —Atur pengaturan berikut:

         - Kedalaman merangkak —' Kedalaman 'atau jumlah level dari tingkat benih hingga merangkak. Misalnya, halaman URL benih adalah kedalaman 1 dan hyperlink apa pun di halaman ini yang juga dirayapi adalah kedalaman 2.
         - Ukuran file maksimum —Ukuran maksimum dalam MB halaman web atau lampiran untuk dirayapi.
         - Tautan maksimum per halaman —Jumlah maksimum URL pada satu halaman web untuk di-crawl.
         - Pelambatan maksimum kecepatan crawling —Jumlah maksimum URL yang dirayapi per host situs web per menit.
         - File —Pilih untuk merayapi file yang ditautkan ke halaman web.
         - Merayapi dan mengindeks URL —Tambahkan pola ekspresi reguler untuk menyertakan atau mengecualikan perayapan URL tertentu, dan mengindeks hyperlink apa pun di halaman web URL ini.

   b. Mode sinkronisasi —Pilih cara Anda ingin memperbarui indeks saat konten sumber data Anda berubah. Saat Anda menyinkronkan sumber data Amazon Kendra untuk pertama kalinya, semua konten dirayapi dan diindeks secara default. Anda harus menjalankan sinkronisasi penuh data Anda jika sinkronisasi awal Anda gagal, bahkan jika Anda tidak memilih sinkronisasi penuh sebagai opsi mode sinkronisasi Anda.

      - Sinkronisasi penuh: Indeks baru semua konten, ganti konten yang ada setiap kali sumber data Anda disinkronkan dengan indeks Anda.
      - Sinkronisasi baru, dimodifikasi, dihapus: Indeks hanya konten baru, dimodifikasi, dan dihapus setiap kali sumber data Anda disinkronkan dengan indeks Anda. Amazon

Kendra dapat menggunakan mekanisme sumber data Anda untuk melacak perubahan konten dan mengindeks konten yang berubah sejak sinkronisasi terakhir.

c. Sinkronkan jadwal berjalan —Untuk Frekuensi, pilih seberapa sering Amazon Kendra akan disinkronkan dengan sumber data Anda.

d. Pilih Berikutnya.

8. Pada halaman Setel pemetaan bidang, masukkan informasi berikut:

a. Pilih dari bidang default Amazon Kendra yang dihasilkan dari halaman web dan file yang ingin Anda petakan ke indeks Anda.

b. Pilih Berikutnya.

9. Pada halaman Tinjau dan buat, periksa apakah informasi yang Anda masukkan sudah benar dan kemudian pilih Tambahkan sumber data. Anda juga dapat memilih untuk mengedit informasi Anda dari halaman ini. Sumber data Anda akan muncul di halaman Sumber data setelah sumber data berhasil ditambahkan.

API

Untuk terhubung Amazon Kendra ke web crawler

Anda harus menentukan JSON dari skema sumber data menggunakan API. TemplateConfiguration Anda harus memberikan informasi berikut ini:

- Sumber data —Tentukan tipe sumber data seperti `WEBCRAWLERV2` saat Anda menggunakan skema TemplateConfigurationJSON. Juga tentukan sumber data seperti `TEMPLATE` saat Anda memanggil CreateDataSourceAPI.
- URL —Tentukan URL benih atau titik awal situs web atau URL peta situs situs web yang ingin dirayapi. Anda dapat menentukan jalur ke Amazon S3 bucket yang menyimpan daftar URL seed Anda. Setiap URL dalam file teks untuk URL benih harus diformat pada baris terpisah. Anda juga dapat menentukan path ke Amazon S3 bucket yang menyimpan file XHTML sitemap Anda. Anda dapat menggabungkan beberapa file peta situs ke dalam file ZIP dan menyimpan file ZIP di bucket Anda Amazon S3 .

> **Note**
>
> Jika Anda ingin merayapi peta situs, periksa apakah URL dasar atau root sama dengan URL yang tercantum di halaman peta situs Anda. Misalnya, jika URL peta situs Anda

https://example.com/sitemap-page.html, URL yang tercantum di halaman peta situs ini juga harus menggunakan URL dasar "". https://example.com/

- Mode sinkronisasi —Tentukan cara Amazon Kendra memperbarui indeks Anda saat konten sumber data Anda berubah. Saat Anda menyinkronkan sumber data Amazon Kendra untuk pertama kalinya, semua konten dirayapi dan diindeks secara default. Anda harus menjalankan sinkronisasi penuh data Anda jika sinkronisasi awal Anda gagal, bahkan jika Anda tidak memilih sinkronisasi penuh sebagai opsi mode sinkronisasi Anda. Anda dapat memilih antara:
  - `FORCED_FULL_CRAWL`untuk mengindeks semua konten baru, mengganti konten yang ada setiap kali sumber data Anda disinkronkan dengan indeks Anda.
  - `FULL_CRAWL`untuk mengindeks hanya konten baru, dimodifikasi, dan dihapus setiap kali sumber data Anda disinkronkan dengan indeks Anda. Amazon Kendra dapat menggunakan mekanisme sumber data Anda untuk melacak perubahan konten dan mengindeks konten yang berubah sejak sinkronisasi terakhir.
- Otentikasi — Jika situs web Anda memerlukan otentikasi yang sama, tentukan salah satu,, `BasicAuth` `NTLM_Kerberos`SAML, atau otentikasi. `Form` Jika situs web Anda tidak memerlukan otentikasi, tentukan`NoAuthentication`.
- Rahasia Nama Sumber Daya Amazon (ARN) —Jika situs web Anda memerlukan otentikasi dasar, NTLM, atau Kerberos, Anda memberikan rahasia yang menyimpan kredensyal otentikasi nama pengguna dan kata sandi Anda. Anda memberikan Nama Sumber Daya Amazon (ARN) dari sebuah AWS Secrets Manager rahasia. Rahasianya disimpan dalam struktur JSON dengan kunci berikut:

```
{
    "seedUrlsHash": "Hash representation of all seed URLs",
    "userName": "user name",
    "password": "password"
}
```

Jika situs web Anda memerlukan otentikasi SAMP, rahasianya disimpan dalam struktur JSON dengan kunci berikut:

```
{
    "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"
}
```

Jika situs web Anda memerlukan otentikasi formulir, rahasianya disimpan dalam struktur JSON dengan kunci berikut:

```
{
    "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"
}
```

Anda dapat menemukan elemen XPaths (XMLPath Language) menggunakan alat pengembang browser web Anda. XPaths biasanya mengikuti format ini:`//tagname[@Attribute='Value']`.

Anda juga dapat memberikan kredensyal proxy web menggunakan dan AWS Secrets Manager rahasia.

- IAM peran —Tentukan `RoleArn` kapan Anda menelepon `CreateDataSource` untuk memberikan IAM peran dengan izin untuk mengakses Secrets Manager rahasia Anda dan memanggil API publik yang diperlukan untuk konektor perayap web dan. Amazon Kendra Untuk informasi selengkapnya, lihat IAM peran untuk sumber data perayap web.

Anda juga dapat menambahkan fitur opsional berikut:

- Virtual Private Cloud (VPC) **`VpcConfiguration`** —Tentukan kapan Anda menelepon. `CreateDataSource` Untuk informasi selengkapnya, lihat Mengkonfigurasi Amazon Kendra untuk menggunakan Amazon VPC.
- Rentang domain —Pilih apakah akan merayapi domain situs web dengan subdomain saja, atau juga merayapi domain lain yang ditautkan ke halaman web. Secara default, Amazon Kendra hanya merayapi domain situs web yang ingin Anda jelajahi.

- 'Kedalaman' atau jumlah level dari tingkat benih hingga merangkak. Misalnya, halaman URL benih adalah kedalaman 1 dan hyperlink apa pun di halaman ini yang juga dirayapi adalah kedalaman 2.
- Jumlah maksimum URL pada satu halaman web untuk dirayapi.
- Ukuran maksimum dalam MB halaman web atau lampiran untuk dirayapi.
- Jumlah maksimum URL yang dirayapi per host situs web per menit.
- Host proxy web dan nomor port untuk terhubung ke dan merayapi situs web internal. Misalnya, nama host https://a.example.com/page1.htmladalah "a.example.com" dan nomor port adalah 443, port standar untuk HTTPS. Jika kredensyal proxy web diperlukan untuk terhubung ke host situs web, Anda dapat membuat AWS Secrets Manager yang menyimpan kredensialnya.
- Filter inklusi dan pengecualian —Tentukan apakah akan menyertakan atau mengecualikan crawling URL tertentu dan mengindeks hyperlink apa pun di halaman web URL ini.

  > **Note**
  >
  > Sebagian besar sumber data menggunakan pola ekspresi reguler, yang merupakan pola inklusi atau pengecualian yang disebut sebagai filter. Jika Anda menentukan filter inklusi, hanya konten yang cocok dengan filter inklusi yang diindeks. Dokumen apa pun yang tidak cocok dengan filter inklusi tidak diindeks. Jika Anda menentukan filter inklusi dan pengecualian, dokumen yang cocok dengan filter pengecualian tidak akan diindeks, meskipun sesuai dengan filter inklusi.

- Pemetaan bidang —Pilih untuk memetakan bidang halaman web dan file halaman web ke bidang indeks Anda Amazon Kendra . Untuk informasi lebih lanjut, lihat Memetakan bidang sumber data.

Untuk daftar kunci JSON penting lainnya untuk dikonfigurasi, lihat Skema template Amazon Kendra Web Crawler.

Mengkonfigurasi **`robots.txt`** file untuk Amazon Kendra Web Crawler

Amazon Kendra adalah layanan pencarian cerdas yang digunakan AWS pelanggan untuk mengindeks dan mencari dokumen pilihan mereka. Untuk mengindeks dokumen di web, pelanggan dapat menggunakan Amazon Kendra Web Crawler, yang menunjukkan URL mana yang harus diindeks dan parameter operasional lainnya. Amazon Kendra pelanggan diharuskan untuk mendapatkan otorisasi sebelum mengindeks situs web tertentu.

Amazon Kendra Web Crawler menghormati arahan robots.txt standar seperti dan. `Allow` `Disallow` Anda dapat memodifikasi `robots.txt` file situs web Anda untuk mengontrol bagaimana Amazon Kendra Web Crawler merayapi situs web Anda.

Mengkonfigurasi bagaimana Amazon Kendra Web Crawler mengakses situs web Anda

Anda dapat mengontrol bagaimana Amazon Kendra Web Crawler mengindeks situs web Anda menggunakan `Allow` dan `Disallow` arahan. Anda juga dapat mengontrol halaman web mana yang diindeks dan halaman web mana yang tidak dirayapi.

Untuk mengizinkan Amazon Kendra Web Crawler merayapi semua halaman web kecuali halaman web yang tidak diizinkan, gunakan arahan berikut:

```
User-agent: amazon-kendra    # Amazon Kendra Web Crawler
Disallow: /credential-pages/ # disallow access to specific pages
```

Untuk mengizinkan Amazon Kendra Web Crawler merayapi hanya halaman web tertentu, gunakan arahan berikut:

```
User-agent: amazon-kendra    # Amazon Kendra Web Crawler
Allow: /pages/ # allow access to specific pages
```

Untuk memungkinkan Amazon Kendra Web Crawler merayapi semua konten situs web dan melarang perayapan untuk robot lain, gunakan arahan berikut:

```
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
```

Menghentikan Amazon Kendra Web Crawler dari merayapi situs web Anda

Anda dapat menghentikan Amazon Kendra Web Crawler dari mengindeks situs web Anda menggunakan arahan. `Disallow` Anda juga dapat mengontrol halaman web mana yang dirayapi dan mana yang tidak.

Untuk menghentikan Amazon Kendra Web Crawler merayapi situs web, gunakan arahan berikut:

```
User-agent: amazon-kendra # Amazon Kendra Web Crawler
Disallow: / # disallow access to any pages
```

Amazon Kendra Web Crawler juga mendukung robot `noindex` dan `nofollow` arahan dalam meta tag di halaman HTML. Arahan ini menghentikan perayap web dari mengindeks halaman web dan berhenti mengikuti tautan apa pun di halaman web. Letakkan tanda meta di bagian dokumen untuk menentukan aturan robot.

Misalnya, halaman web di bawah ini mencakup arahan robot `noindex` dan`nofollow`:

```
<html>
<head>
    <meta name="robots" content="noindex, nofollow"/>
    ...
</head>
<body>...</body>
</html>
```

Jika Anda memiliki pertanyaan atau kekhawatiran tentang Amazon Kendra Web Crawler, Anda dapat menghubungi tim AWS dukungan.

Amazon WorkDocs

Amazon WorkDocs adalah layanan kolaborasi konten yang aman untuk membuat, mengedit, menyimpan, dan berbagi konten. Anda dapat menggunakan Amazon Kendra untuk mengindeks sumber Amazon WorkDocs data Anda.

Anda dapat terhubung Amazon Kendra ke sumber Amazon WorkDocs data menggunakan Amazon Kendra konsol dan WorkDocsConfigurationAPI.

Amazon WorkDocs tersedia di wilayah Oregon, Virginia Utara, Sydney, Singapura, dan Irlandia.

Untuk memecahkan masalah konektor sumber Amazon Kendra WorkDocs data Anda, lihat. Mengatasi masalah sumber data

Topik

- Fitur yang didukung
- Prasyarat
- Instruksi koneksi
- Pelajari selengkapnya

Fitur yang didukung

Amazon Kendra WorkDocs konektor sumber data mendukung fitur-fitur berikut:

- Ubah log
- Pemetaan lapangan
- Pemfilteran konteks pengguna
- Filter inklusi/pengecualian

Prasyarat

Sebelum Anda dapat menggunakan Amazon Kendra untuk mengindeks sumber WorkDocs data Anda, buat perubahan ini di akun WorkDocs dan AWS akun Anda.

Di WorkDocs, pastikan Anda memiliki:

- Mencatat ID Amazon WorkDocs direktori (ID organisasi) untuk Amazon WorkDocs repositori Anda.
- Memeriksa setiap dokumen unik di dalam WorkDocs dan di seluruh sumber data lain yang Anda rencanakan untuk digunakan untuk indeks yang sama. Setiap sumber data yang ingin Anda gunakan untuk indeks tidak boleh berisi dokumen yang sama di seluruh sumber data. ID dokumen bersifat global untuk indeks dan harus unik per indeks.

Di AWS akun Anda, pastikan Anda memiliki:

- Membuat Amazon Kendra indeks dan, jika menggunakan API, mencatat ID indeks.
- Membuat IAM peran untuk sumber data Anda dan, jika menggunakan API, catat ARN peran tersebut IAM .

Jika Anda tidak memiliki IAM peran yang ada, Anda dapat menggunakan konsol untuk membuat IAM peran baru saat Anda menghubungkan sumber WorkDocs data Anda Amazon Kendra. Jika Anda menggunakan API, Anda harus memberikan ARN IAM peran yang ada dan ID indeks.

Instruksi koneksi

Untuk terhubung Amazon Kendra ke sumber WorkDocs data Anda, Anda harus memberikan rincian yang diperlukan dari sumber WorkDocs data Anda sehingga Amazon Kendra dapat mengakses data Anda. Jika Anda belum mengkonfigurasi WorkDocs untuk Amazon Kendra, lihatPrasyarat.

Console

Untuk terhubung Amazon Kendra ke Amazon WorkDocs

1. Masuk ke AWS Management Console dan buka Amazon Kendra konsol.
2. Dari panel navigasi kiri, pilih Indeks dan kemudian pilih indeks yang ingin Anda gunakan dari daftar indeks.

> **Note**
>
> Anda dapat memilih untuk mengonfigurasi atau mengedit pengaturan kontrol akses Pengguna Anda di bawah Pengaturan indeks.

3. Pada halaman Memulai, pilih Tambahkan sumber data.
4. Pada halaman Tambahkan sumber data, pilih WorkDocs konektor, lalu pilih Tambah konektor.
5. Pada halaman Tentukan detail sumber data, masukkan informasi berikut:
   a. Di Nama dan deskripsi, untuk Nama sumber data —Masukkan nama untuk sumber data Anda. Anda dapat memasukkan tanda hubung tetapi bukan spasi.
   b. (Opsional) Deskripsi —Masukkan deskripsi opsional untuk sumber data Anda.
   c. Dalam Bahasa default —Pilih bahasa untuk memfilter dokumen Anda untuk indeks. Kecuali Anda menentukan sebaliknya, bahasa default ke bahasa Inggris. Bahasa yang ditentukan dalam metadata dokumen mengesampingkan bahasa yang dipilih.
   d. Di Tag, untuk Tambahkan tag baru —Sertakan tag opsional untuk mencari dan memfilter sumber daya Anda atau melacak AWS biaya Anda.
   e. Pilih Berikutnya.
6. Pada halaman Tentukan akses dan keamanan, masukkan informasi berikut:
   a. ID Organisasi khusus untuk Amazon WorkDocs situs Anda —Pilih ID Amazon WorkDocs situs yang ingin Anda indeks. Anda harus sudah membuat situs.
   b. IAM peran —Pilih peran yang ada atau buat IAM IAM peran baru untuk mengakses kredensyal repositori dan mengindeks konten Anda.

> **Note**
>
> IAM peran yang digunakan untuk indeks tidak dapat digunakan untuk sumber data. Jika Anda tidak yakin apakah peran yang ada digunakan untuk indeks atau FAQ, pilih Buat peran baru untuk menghindari kesalahan.

c. Pilih Berikutnya.

7. Pada halaman Konfigurasi pengaturan sinkronisasi, masukkan informasi berikut:

   a. Merayapi komentar dokumen Amazon WorkDocs —Entitas atau jenis konten yang ingin dirayapi.

   b. Gunakan log perubahan —Pilih untuk memperbarui indeks Anda hanya dengan konten baru atau yang dimodifikasi alih-alih menyinkronkan semua file Anda.

   c. Pola Regex —Pola ekspresi reguler untuk menyertakan atau mengecualikan file tertentu. Anda dapat menambahkan hingga 100 pola.

   d. Di Sinkronkan jadwal lari untuk Frekuensi —Pilih seberapa sering Amazon Kendra akan disinkronkan dengan sumber data Anda.

   e. Pilih Berikutnya.

8. Pada halaman Setel pemetaan bidang, masukkan informasi berikut:

   a. Bidang sumber data default —Pilih dari bidang sumber data default yang Amazon Kendra dihasilkan yang ingin Anda petakan ke indeks Anda.

   b. Tambahkan bidang —Untuk menambahkan bidang sumber data kustom untuk membuat nama bidang indeks untuk dipetakan dan tipe data bidang.

   c. Pilih Berikutnya.

9. Pada halaman Tinjau dan buat, periksa apakah informasi yang Anda masukkan sudah benar dan kemudian pilih Tambahkan sumber data. Anda juga dapat memilih untuk mengedit informasi Anda dari halaman ini. Sumber data Anda akan muncul di halaman Sumber data setelah sumber data berhasil ditambahkan.

API

Untuk terhubung Amazon Kendra ke Amazon WorkDocs

Anda harus menentukan yang berikut menggunakan WorkDocsConfigurationAPI:

- Amazon WorkDocs ID direktori —Tentukan ID organisasi Amazon WorkDocs direktori Anda. Anda dapat menemukan ID organisasi di AWS Directory Service dengan membuka Active Directory dan kemudian Direktori.
- Peran IAM —Tentukan `RoleArn` kapan Anda memanggil `CreateDataSource` untuk memberikan IAM peran dengan izin untuk mengakses WorkDocs dirtectory dan memanggil API publik yang diperlukan untuk konektor dan. WorkDocs Amazon Kendra Untuk informasi selengkapnya, lihat peran IAM untuk sumber WorkDocs data.

Anda juga dapat menambahkan fitur opsional berikut:

- Ubah log —Apakah Amazon Kendra harus menggunakan mekanisme log perubahan sumber WorkDocs data untuk menentukan apakah dokumen harus diperbarui dalam indeks.

  > **Note**
  >
  > Gunakan log perubahan jika Anda tidak Amazon Kendra ingin memindai semua dokumen. Jika log perubahan Anda besar, mungkin perlu waktu Amazon Kendra lebih sedikit untuk memindai dokumen di sumber WorkDocs data daripada memproses log perubahan. Jika Anda menyinkronkan sumber WorkDocs data Anda dengan indeks Anda untuk pertama kalinya, semua dokumen dipindai.

- Filter inklusi dan pengecualian —Tentukan apakah akan menyertakan atau mengecualikan dokumen dan komentar dokumen tertentu. Setiap komentar diindeks sebagai dokumen terpisah.

  > **Note**
  >
  > Sebagian besar sumber data menggunakan pola ekspresi reguler, yang merupakan pola inklusi atau pengecualian yang disebut sebagai filter. Jika Anda menentukan filter inklusi, hanya konten yang cocok dengan filter inklusi yang diindeks. Dokumen apa pun yang tidak cocok dengan filter inklusi tidak diindeks. Jika Anda menentukan filter inklusi dan pengecualian, dokumen yang cocok dengan filter pengecualian tidak akan diindeks, meskipun sesuai dengan filter inklusi.

- Pemfilteran konteks pengguna dan kontrol akses —Amazon Kendra meng-crawl daftar kontrol akses (ACL) untuk dokumen Anda, jika Anda memiliki ACL untuk dokumen Anda. Informasi

ACL digunakan untuk memfilter hasil pencarian berdasarkan pengguna atau akses grup mereka ke dokumen. Untuk informasi selengkapnya, lihat Pemfilteran konteks pengguna.

- Pemetaan bidang —Pilih untuk memetakan bidang sumber WorkDocs data Anda ke bidang indeks Anda Amazon Kendra . Untuk informasi lebih lanjut, lihat Memetakan bidang sumber data.

> **Note**
>
> Bidang badan dokumen atau badan dokumen yang setara untuk dokumen Anda diperlukan Amazon Kendra untuk mencari dokumen Anda. Anda harus memetakan nama bidang badan dokumen Anda di sumber data Anda ke nama bidang indeks_`document_body`. Semua kolom lain bersifat opsional.

Pelajari selengkapnya

Untuk mempelajari lebih lanjut tentang mengintegrasikan Amazon Kendra dengan sumber WorkDocs data Anda, lihat:

- Memulai dengan WorkDocs konektor Amazon Kendra Amazon

Kotak

Box adalah layanan penyimpanan cloud yang menawarkan kemampuan hosting file. Anda dapat menggunakan Amazon Kendra untuk mengindeks konten dalam konten Box Anda, termasuk komentar, tugas, dan tautan web.

Anda dapat terhubung Amazon Kendra ke sumber data Box menggunakan Amazon Kendra konsol dan BoxConfigurationAPI.

Untuk memecahkan masalah konektor sumber data Amazon Kendra Box, lihat. Mengatasi masalah sumber data

Topik

- Fitur yang didukung
- Prasyarat
- Instruksi koneksi

- Pelajari selengkapnya

Fitur yang didukung

Amazon Kendra Konektor sumber data kotak mendukung fitur-fitur berikut:

- Ubah log
- Pemetaan lapangan
- Pemfilteran konteks pengguna
- Filter inklusi/pengecualian
- Cloud privat virtual (VPC)

Prasyarat

Sebelum Anda dapat menggunakan Amazon Kendra untuk mengindeks sumber data Box Anda, buat perubahan ini di Kotak dan AWS akun Anda.

Di Box, pastikan Anda memiliki:

- Akun Box Enterprise atau Box Enterprise Plus.
- Membuat aplikasi kustom Box di Box Developer Console dan mengonfigurasinya untuk menggunakan Server Authentication (dengan JWT).
- Setel Level Akses Aplikasi Anda ke App + Enterprise Access dan izinkan melakukan panggilan API menggunakan header as-user.
- Menggunakan pengguna admin untuk menambahkan Lingkup Aplikasi berikut di aplikasi Box Anda:
  - Menulis semua file dan folder yang disimpan dalam Kotak
  - Mengelola pengguna
  - Kelola grup
  - Kelola properti perusahaan
- Dihasilkan dan diunduh Public/Private key pair termasuk ID klien, rahasia klien, ID kunci publik, ID kunci pribadi, frasa lulus, dan ID perusahaan untuk digunakan sebagai kredensyal otentikasi. Lihat Keypair publik dan pribadi untuk detail selengkapnya.
- Menyalin ID perusahaan Box Anda baik dari pengaturan Box Developer Console atau dari aplikasi Box Anda. Misalnya, *801234567*.

- Memeriksa setiap dokumen unik di Box dan di seluruh sumber data lain yang Anda rencanakan untuk digunakan untuk indeks yang sama. Setiap sumber data yang ingin Anda gunakan untuk indeks tidak boleh berisi dokumen yang sama di seluruh sumber data. ID dokumen bersifat global untuk indeks dan harus unik per indeks.

Di dalam Anda Akun AWS, pastikan Anda memiliki:

- Membuat Amazon Kendra indeks dan, jika menggunakan API, mencatat ID indeks.
- Membuat IAM peran untuk sumber data Anda dan, jika menggunakan API, catat ARN peran tersebut IAM .

> **Note**
>
> Jika Anda mengubah jenis otentikasi dan kredensyal, Anda harus memperbarui IAM peran Anda untuk mengakses ID rahasia yang benar AWS Secrets Manager .

- Menyimpan kredensi otentikasi Box Anda AWS Secrets Manager secara rahasia dan, jika menggunakan API, catat ARN rahasia tersebut.

> **Note**
>
> Kami menyarankan Anda secara teratur menyegarkan atau memutar kredensil dan rahasia Anda. Berikan hanya tingkat akses yang diperlukan untuk keamanan Anda sendiri. Kami tidak menyarankan Anda menggunakan kembali kredensyal dan rahasia di seluruh sumber data, dan konektor versi 1.0 dan 2.0 (jika berlaku).

Jika Anda tidak memiliki IAM peran atau rahasia yang ada, Anda dapat menggunakan konsol untuk membuat IAM peran dan Secrets Manager rahasia baru saat menghubungkan sumber data Box Amazon Kendra. Jika Anda menggunakan API, Anda harus memberikan ARN IAM peran dan Secrets Manager rahasia yang ada, dan ID indeks.

Instruksi koneksi

Untuk terhubung Amazon Kendra ke sumber data Box Anda, Anda harus memberikan rincian yang diperlukan dari sumber data Box Anda sehingga Amazon Kendra dapat mengakses data Anda. Jika Anda belum mengkonfigurasi Box for Amazon Kendra, lihatPrasyarat.

Console

Untuk terhubung Amazon Kendra ke Box

1. Masuk ke AWS Management Console dan buka Amazon Kendra konsol.
2. Dari panel navigasi kiri, pilih Indeks dan kemudian pilih indeks yang ingin Anda gunakan dari daftar indeks.

> **Note**
>
> Anda dapat memilih untuk mengonfigurasi atau mengedit pengaturan kontrol akses Pengguna Anda di bawah Pengaturan indeks.

3. Pada halaman Memulai, pilih Tambahkan sumber data.
4. Pada halaman Tambahkan sumber data, pilih Konektor kotak, lalu pilih Tambah konektor.
5. Pada halaman Tentukan detail sumber data, masukkan informasi berikut:
   a. Dalam Nama dan deskripsi, untuk Nama sumber data —Masukkan nama untuk sumber data Anda. Anda dapat memasukkan tanda hubung tetapi bukan spasi.
   b. (Opsional) Deskripsi —Masukkan deskripsi opsional untuk sumber data Anda.
   c. Dalam Bahasa default —Pilih bahasa untuk memfilter dokumen Anda untuk indeks. Kecuali Anda menentukan sebaliknya, bahasa default ke bahasa Inggris. Bahasa yang ditentukan dalam metadata dokumen mengesampingkan bahasa yang dipilih.
   d. Di Tag, untuk Tambahkan tag baru —Sertakan tag opsional untuk mencari dan memfilter sumber daya Anda atau melacak AWS biaya Anda.
   e. Pilih Berikutnya.
6. Pada halaman Tentukan akses dan keamanan, masukkan informasi berikut:
   a. Kotak ID perusahaan —Masukkan ID Kotak Perusahaan Anda.
   b. AWS Secrets Manager rahasia —Pilih rahasia yang ada atau buat Secrets Manager rahasia baru untuk menyimpan kredensyal otentikasi Kotak Anda. Jika Anda memilih untuk membuat rahasia baru, jendela AWS Secrets Manager rahasia terbuka.
      i. Nama rahasia —Nama untuk rahasiamu. Awalan 'AmazonKendra-Box-' secara otomatis ditambahkan ke nama rahasia Anda.

ii. Untuk ID Klien, Rahasia Klien, ID Kunci Publik, ID Kunci Pribadi, dan Frasa Lulus —Masukkan nilai dari Kunci Publik/Pribadi yang Anda buat di akun Box Anda dan unduh dari akun Box Anda.

iii. Pilih Simpan.

c. Virtual Private Cloud (VPC) —Anda dapat memilih untuk menggunakan VPC. Jika demikian, Anda harus menambahkan Subnet dan grup keamanan VPC.

d. IAM peran —Pilih peran yang sudah ada atau buat IAM IAM peran baru untuk mengakses kredensi repositori dan mengindeks konten Anda.

> **Note**
>
> IAM peran yang digunakan untuk indeks tidak dapat digunakan untuk sumber data. Jika Anda tidak yakin apakah peran yang ada digunakan untuk indeks atau FAQ, pilih Buat peran baru untuk menghindari kesalahan.

e. Pilih Berikutnya.

7. Pada halaman Konfigurasi pengaturan sinkronisasi, masukkan informasi berikut:

a. Pilih entitas atau jenis konten —Entitas Kotak atau jenis konten yang ingin dirayapi. Setiap komentar diindeks sebagai dokumen terpisah.

b. Ubah log —Pilih untuk memperbarui indeks Anda hanya untuk konten baru atau yang dimodifikasi alih-alih menyinkronkan semua file Anda.

c. Pola Regex —Pola ekspresi reguler untuk menyertakan atau mengecualikan file tertentu. Anda dapat menambahkan hingga 100 pola.

d. Di Jadwal berjalan Sinkronisasi, untuk Frekuensi —Pilih seberapa sering Amazon Kendra akan disinkronkan dengan sumber data Anda.

e. Pilih Berikutnya.

8. Pada halaman Setel pemetaan bidang, masukkan informasi berikut:

a. Untuk File dan folder, Komentar, Tugas, dan Tautan Web —Pilih dari bidang sumber data default yang Amazon Kendra dihasilkan yang ingin Anda petakan ke indeks Anda.

b. Tambahkan bidang —Untuk menambahkan bidang sumber data kustom untuk membuat nama bidang indeks untuk dipetakan dan tipe data bidang.

c. Pilih Berikutnya.

9. Pada halaman Tinjau dan buat, periksa apakah informasi yang Anda masukkan sudah benar dan kemudian pilih Tambahkan sumber data. Anda juga dapat memilih untuk mengedit informasi Anda dari halaman ini. Sumber data Anda akan muncul di halaman Sumber data setelah sumber data berhasil ditambahkan.

API

Untuk terhubung Amazon Kendra ke Box

Anda harus menentukan yang berikut menggunakan BoxConfigurationAPI:

ID perusahaan kotak —Berikan ID Perusahaan Kotak Anda. Anda dapat menemukan ID perusahaan di setelan Box Developer Console atau saat Anda membuat aplikasi di Box.

- Rahasia Nama Sumber Daya Amazon (ARN) —Berikan Nama Sumber Daya Amazon (ARN) Secrets Manager rahasia yang berisi kredensyal otentikasi untuk akun Box Anda. Rahasianya disimpan dalam struktur JSON dengan kunci berikut:

```
{
    "clientID": "client-id",
    "clientSecret": "client-secret",
    "publicKeyID": "public-key-id",
    "privateKey": "private-key",
    "passphrase": "pass-phrase"
}
```

> **Note**
>
> Kami menyarankan Anda secara teratur menyegarkan atau memutar kredensil dan rahasia Anda. Berikan hanya tingkat akses yang diperlukan untuk keamanan Anda sendiri. Kami tidak menyarankan Anda menggunakan kembali kredensyal dan rahasia di seluruh sumber data, dan konektor versi 1.0 dan 2.0 (jika berlaku).

- IAM peran —Tentukan `RoleArn` kapan Anda menelepon `CreateDataSource` untuk memberikan IAM peran dengan izin untuk mengakses Secrets Manager rahasia Anda dan memanggil API publik yang diperlukan untuk konektor Box dan. Amazon Kendra Untuk informasi selengkapnya, lihat IAM peran untuk Sumber data Kotak.

Anda juga dapat menambahkan fitur opsional berikut:

- Virtual Private Cloud (VPC) —Tentukan `VpcConfiguration` sebagai bagian dari konfigurasi sumber data. Lihat Mengkonfigurasi Amazon Kendra untuk menggunakan VPC.
- Ubah log —Apakah Amazon Kendra harus menggunakan mekanisme log perubahan sumber data Kotak untuk menentukan apakah dokumen harus diperbarui dalam indeks.

  > **Note**
  >
  > Gunakan log perubahan jika Anda tidak Amazon Kendra ingin memindai semua dokumen. Jika log perubahan Anda besar, mungkin perlu waktu Amazon Kendra lebih sedikit untuk memindai dokumen di sumber data Kotak daripada memproses log perubahan. Jika Anda menyinkronkan sumber data Box Anda dengan indeks Anda untuk pertama kalinya, semua dokumen dipindai.

- Komentar, tugas, tautan web —Tentukan apakah akan merayapi jenis konten ini.

  > **Note**
  >
  > Sebagian besar sumber data menggunakan pola ekspresi reguler, yang merupakan pola inklusi atau pengecualian yang disebut sebagai filter. Jika Anda menentukan filter inklusi, hanya konten yang cocok dengan filter inklusi yang diindeks. Dokumen apa pun yang tidak cocok dengan filter inklusi tidak diindeks. Jika Anda menentukan filter inklusi dan pengecualian, dokumen yang cocok dengan filter pengecualian tidak akan diindeks, meskipun sesuai dengan filter inklusi.

- Filter inklusi dan pengecualian —Tentukan apakah akan menyertakan atau mengecualikan file dan folder Kotak tertentu.

  > **Note**
  >
  > Sebagian besar sumber data menggunakan pola ekspresi reguler, yang merupakan pola inklusi atau pengecualian yang disebut sebagai filter. Jika Anda menentukan filter inklusi, hanya konten yang cocok dengan filter inklusi yang diindeks. Dokumen apa pun yang tidak cocok dengan filter inklusi tidak diindeks. Jika Anda menentukan filter inklusi dan pengecualian, dokumen yang cocok dengan filter pengecualian tidak akan diindeks, meskipun sesuai dengan filter inklusi.

- Pemfilteran konteks pengguna dan kontrol akses —Amazon Kendra meng-crawl daftar kontrol akses (ACL) untuk dokumen Anda, jika Anda memiliki ACL untuk dokumen Anda. Informasi

ACL digunakan untuk memfilter hasil pencarian berdasarkan pengguna atau akses grup mereka ke dokumen. Untuk informasi selengkapnya, lihat Pemfilteran konteks pengguna.

- Pemetaan bidang —Pilih untuk memetakan bidang sumber data Kotak Anda ke bidang indeks Anda Amazon Kendra . Untuk informasi lebih lanjut, lihat Memetakan bidang sumber data.

> **Note**
>
> Bidang badan dokumen atau badan dokumen yang setara untuk dokumen Anda diperlukan Amazon Kendra untuk mencari dokumen Anda. Anda harus memetakan nama bidang badan dokumen Anda di sumber data Anda ke nama bidang indeks_`document_body`. Semua kolom lain bersifat opsional.

Pelajari selengkapnya

Untuk mempelajari lebih lanjut tentang mengintegrasikan Amazon Kendra dengan sumber data Box Anda, lihat:

- Memulai dengan konektor Amazon Kendra Box

Confluence

Confluence adalah alat manajemen kerja kolaboratif yang dirancang untuk berbagi, menyimpan, dan mengerjakan perencanaan proyek, pengembangan perangkat lunak, dan manajemen produk. Anda dapat menggunakan Amazon Kendra untuk mengindeks ruang Confluence Anda, halaman (termasuk halaman bersarang), blog, dan komentar dan lampiran ke halaman dan blog yang diindeks.

Amazon Kendra mendukung Confluence Server dan Confluence Cloud.

> **Note**
>
> Secara default, Amazon Kendra tidak mengindeks arsip Confluence dan ruang pribadi. Anda dapat memilih untuk mengindeksnya ketika membuat sumber data. Jika Anda tidak ingin Amazon Kendra mengindeks spasi, tandai secara pribadi di Confluence.

Anda dapat terhubung Amazon Kendra ke sumber data Confluence menggunakan Amazon Kendra konsol, TemplateConfigurationAPI, atau API. ConfluenceConfiguration

Amazon Kendra memiliki dua versi konektor Confluence. Fitur yang didukung dari setiap versi meliputi:

Konektor pertemuan V1.0 /API ConfluenceConfiguration

- Pemetaan lapangan
- Pemfilteran konteks pengguna
- Filter inklusi/pengecualian
- (Hanya untuk Server Confluence) Virtual private cloud (VPC)

Konektor pertemuan V2.0 /API TemplateConfiguration

- Pemetaan lapangan
- Pemfilteran konteks pengguna
- Cloud privat virtual (VPC)
- Sinkronkan semua dokumen/Sinkronkan hanya dokumen baru, dimodifikasi, atau dihapus
- Pola inklusi/pengecualian

> **Note**
>
> Support untuk konektor Confluence V1.0/ ConfluenceConfiguration API dijadwalkan berakhir pada tahun 2023. Kami merekomendasikan untuk bermigrasi ke atau menggunakan konektor Confluence V2.0/API. TemplateConfiguration

Untuk memecahkan masalah konektor sumber data Amazon Kendra Confluence, lihat. Mengatasi masalah sumber data

Topik

Konektor pertemuan V1.0

Confluence adalah alat manajemen kerja kolaboratif yang dirancang untuk berbagi, menyimpan, dan mengerjakan perencanaan proyek, pengembangan perangkat lunak, dan manajemen produk. Anda

dapat menggunakan Amazon Kendra untuk mengindeks ruang Confluence Anda, halaman (termasuk halaman bersarang), blog, dan komentar dan lampiran ke halaman dan blog yang diindeks.

> **Note**
>
> Support untuk konektor Confluence V1.0/ ConfluenceConfiguration API dijadwalkan berakhir pada tahun 2023. Kami merekomendasikan untuk bermigrasi ke atau menggunakan konektor Confluence V2.0/API. TemplateConfiguration

Untuk memecahkan masalah konektor sumber data Amazon Kendra Confluence, lihat. Mengatasi masalah sumber data

Topik

- Fitur yang didukung
- Prasyarat
- Instruksi koneksi
- Pelajari selengkapnya

Fitur yang didukung

Amazon Kendra Konektor sumber data pertemuan mendukung fitur-fitur berikut:

- Pemetaan lapangan
- Pemfilteran konteks pengguna
- Filter inklusi/pengecualian
- (Hanya untuk Server Confluence) Virtual private cloud (VPC)

Prasyarat

Sebelum Anda dapat menggunakan Amazon Kendra untuk mengindeks sumber data Confluence Anda, buat perubahan ini di Confluence dan akun Anda. AWS

Di Confluence, pastikan Anda memiliki:

- Memberikan Amazon Kendra izin untuk melihat semua konten dalam instance Confluence Anda dengan:

  - Amazon Kendra Membuat anggota `confluence-administrators` kelompok.
  - Memberikan izin situs-admin untuk semua ruang, blog, dan halaman yang ada.
- Menyalin URL instance Confluence Anda.
- Untuk pengguna SSO (Single Sign-On): Mengaktifkan halaman Show on login untuk nama pengguna dan kata sandi saat Anda mengonfigurasi metode Confluence Authentication di Confluence Data Center.
- Untuk Server Confluence
  - Mencatat kredensi otentikasi dasar Anda yang berisi nama pengguna dan kata sandi akun administratif Confluence Anda untuk terhubung. Amazon Kendra
  - Opsional: Membuat token akses pribadi di akun Confluence Anda untuk terhubung. Amazon Kendra Untuk informasi selengkapnya, lihat Dokumentasi pertemuan tentang pembuatan token akses pribadi.
- Untuk Confluence Cloud
  - Mencatat kredensi otentikasi dasar Anda yang berisi nama pengguna dan kata sandi akun administratif Confluence Anda untuk terhubung. Amazon Kendra
- Memeriksa setiap dokumen unik di Confluence dan di seluruh sumber data lain yang Anda rencanakan untuk digunakan untuk indeks yang sama. Setiap sumber data yang ingin Anda gunakan untuk indeks tidak boleh berisi dokumen yang sama di seluruh sumber data. ID dokumen bersifat global untuk indeks dan harus unik per indeks.

Di dalam Anda Akun AWS, pastikan Anda memiliki:

- Membuat Amazon Kendra indeks dan, jika menggunakan API, mencatat ID indeks.
- Membuat IAM peran untuk sumber data Anda dan, jika menggunakan API, catat ARN peran tersebut IAM .

> **Note**
>
> Jika Anda mengubah jenis otentikasi dan kredensialnya, Anda harus memperbarui IAM peran Anda untuk mengakses ID rahasia yang benar AWS Secrets Manager .

- Menyimpan kredensi otentikasi Confluence Anda secara AWS Secrets Manager rahasia dan, jika menggunakan API, catat ARN rahasia tersebut.

> **Note**
>
> Kami menyarankan Anda secara teratur menyegarkan atau memutar kredensil dan rahasia Anda. Berikan hanya tingkat akses yang diperlukan untuk keamanan Anda sendiri. Kami tidak menyarankan Anda menggunakan kembali kredensil dan rahasia di seluruh sumber data, dan konektor versi 1.0 dan 2.0 (jika berlaku).

Jika Anda tidak memiliki IAM peran atau rahasia yang ada, Anda dapat menggunakan konsol untuk membuat IAM peran dan Secrets Manager rahasia baru saat menghubungkan sumber data Confluence. Amazon Kendra Jika Anda menggunakan API, Anda harus memberikan ARN IAM peran dan Secrets Manager rahasia yang ada, dan ID indeks.

Instruksi koneksi

Untuk terhubung Amazon Kendra ke sumber data Confluence Anda, Anda harus memberikan rincian kredenal Confluence Anda sehingga dapat mengakses data Anda. Amazon Kendra Jika Anda belum mengkonfigurasi Confluence untuk Amazon Kendra lihat. Prasyarat

Console

Untuk terhubung Amazon Kendra ke Confluence

1. Masuk ke Konsol AWS Manajemen dan buka Amazon Kendra konsol.
2. Dari panel navigasi kiri, pilih Indeks dan kemudian pilih indeks yang ingin Anda gunakan dari daftar indeks.

   > **Note**
   >
   > Anda dapat memilih untuk mengonfigurasi atau mengedit pengaturan kontrol akses Pengguna di bawah Pengaturan indeks.

3. Pada halaman Memulai, pilih Tambahkan sumber data.
4. Pada halaman Tambahkan sumber data, pilih Konektor Confluence V1.0, lalu pilih Tambahkan sumber data.
5. Pada halaman Tentukan detail sumber data, masukkan informasi berikut:

a. Di Nama dan deskripsi, untuk Nama sumber data —Masukkan nama untuk sumber data Anda. Anda dapat memasukkan tanda hubung tetapi bukan spasi.

b. (Opsional) Deskripsi —Masukkan deskripsi opsional untuk sumber data Anda.

c. Dalam Bahasa default —Pilih bahasa untuk memfilter dokumen Anda untuk indeks. Kecuali Anda menentukan sebaliknya, bahasa default ke bahasa Inggris. Bahasa yang ditentukan dalam metadata dokumen mengesampingkan bahasa yang dipilih.

d. Di Tag, untuk Tambahkan tag baru —Sertakan tag opsional untuk mencari dan memfilter sumber daya Anda atau melacak AWS biaya Anda.

e. Pilih Berikutnya.

6. Pada halaman Tentukan akses dan keamanan, masukkan informasi berikut:

a. Pilih antara Confluence cloud dan server Confluence berdasarkan kasus penggunaan Anda.

b. Jika Anda memilih Confluence cloud, masukkan informasi berikut:

i. URL Confluence —URL Pertemuan Anda.

ii. AWS Secrets Manager rahasia —Pilih rahasia yang ada atau buat Secrets Manager rahasia baru untuk menyimpan kredensi otentikasi Confluence Anda. Jika Anda memilih untuk membuat rahasia baru, jendela AWS Secrets Manager rahasia terbuka.

- Masukkan informasi berikut di jendela Buat AWS Secrets Manager rahasia:

I. Nama rahasia —Nama untuk rahasiamu. Awalan 'AmazonKendra-Confluence-' secara otomatis ditambahkan ke nama rahasia Anda.

II. Untuk Nama Pengguna dan Kata Sandi —Masukkan nama pengguna Confluence dan token API Confluence Anda sebagai kata sandi.

III. Pilih Simpan otentikasi.

c. Jika Anda memilih server Confluence, masukkan informasi berikut:

i. URL Confluence —Nama pengguna dan kata sandi Confluence Anda.

ii. (Opsional) Untuk proxy Web masukkan informasi berikut:

A. Nama host —Nama host untuk akun Confluence Anda.

B. Nomor port —Port yang digunakan oleh protokol transport URL host.

iii. Pilih antara otentikasi Dasar dan Token Akses Pribadi.

iv. AWS Secrets Manager rahasia —Pilih rahasia yang ada atau buat Secrets Manager rahasia baru untuk menyimpan kredensi otentikasi Confluence Anda. Jika Anda memilih untuk membuat rahasia baru, jendela AWS Secrets Manager rahasia terbuka.

- Masukkan informasi berikut di jendela Buat AWS Secrets Manager rahasia:

I. Nama rahasia —Nama untuk rahasiamu. Awalan 'AmazonKendra-Confluence-' secara otomatis ditambahkan ke nama rahasia Anda.

II. Untuk Nama Pengguna dan Kata Sandi —Masukkan nilai kredensi otentikasi yang Anda buat dan unduh dari akun Confluence Anda. Jika menggunakan otentikasi dasar, gunakan nama pengguna dan kata sandi Confluence Anda sebagai kredensi otentikasi Anda. Jika menggunakan token akses pribadi, masukkan detail Token Akses Pribadi yang Anda buat di akun Confluence Anda.

III. Pilih Simpan otentikasi.

d. IAM peran —Pilih peran yang ada atau buat IAM IAM peran baru untuk mengakses kredensi repositori dan mengindeks konten.

> **Note**
>
> IAM peran yang digunakan untuk indeks tidak dapat digunakan untuk sumber data. Jika Anda tidak yakin apakah peran yang ada digunakan untuk indeks atau FAQ, pilih Buat peran baru untuk menghindari kesalahan.

e. Pilih Berikutnya.

7. Pada halaman Konfigurasi pengaturan sinkronisasi, masukkan informasi berikut:

a. Untuk Sertakan ruang pribadi dan Sertakan ruang yang diarsipkan —Pilih jenis ruang opsional untuk disertakan dalam sumber data ini.

b. Untuk konfigurasi tambahan —Tentukan pola ekspresi reguler untuk menyertakan atau mengecualikan konten tertentu. Anda dapat menambahkan hingga 100 pola.

c. Anda juga dapat memilih untuk Merayapi lampiran dalam ruang yang dipilih.

d. Di Jadwal berjalan Sinkronisasi, untuk Frekuensi —Pilih seberapa sering Amazon Kendra akan disinkronkan dengan sumber data Anda.

e. Pilih Berikutnya.

8. Pada halaman Setel pemetaan bidang, masukkan informasi berikut:

   a. Untuk Spasi, Halaman, Blog —Pilih dari bidang sumber data default Amazon Kendra yang dihasilkan atau Pemetaan bidang yang disarankan tambahan untuk menambahkan bidang indeks.

   b. Tambahkan bidang —Untuk menambahkan bidang sumber data kustom untuk membuat nama bidang indeks untuk dipetakan dan tipe data bidang.

   c. Pilih Berikutnya.

9. Pada halaman Tinjau dan buat, periksa apakah informasi yang Anda masukkan sudah benar dan kemudian pilih Tambahkan sumber data. Anda juga dapat memilih untuk mengedit informasi Anda dari halaman ini. Sumber data Anda akan muncul di halaman Sumber data setelah sumber data berhasil ditambahkan.

API

Untuk terhubung Amazon Kendra ke Confluence

Anda harus menentukan yang berikut menggunakan ConfluenceConfigurationAPI:

- Versi Confluence —Tentukan versi instance Confluence yang Anda gunakan sebagai atau. `CLOUD` `SERVER`
- Rahasia Nama Sumber Daya Amazon (ARN) —Berikan Nama Sumber Daya Amazon (ARN) Secrets Manager rahasia yang berisi kredensyal otentikasi yang Anda buat di akun Confluence Anda.

  Jika Anda menggunakan Confluence Server, Anda dapat menggunakan nama pengguna dan kata sandi Confluence Anda, atau token akses pribadi Anda sebagai kredensil.

  Saat Anda menggunakan nama pengguna dan kata sandi Confluence sebagai kredensyal otentikasi, Anda menyimpan kredensyal berikut sebagai struktur JSON dalam rahasia Anda: Secrets Manager

```
{
    "username": "user name",
    "password": "password"
}
```

Jika Anda menggunakan token akses pribadi untuk menghubungkan Confluence Server Amazon Kendra, Anda menyimpan kredensyal berikut sebagai struktur JSON dalam rahasia Anda: Secrets Manager

```
{
    "patToken": "personal access token"
}
```

Jika Anda menggunakan Confluence Cloud sebagai sumber Amazon Kendra data, Anda menggunakan nama pengguna Confluence dan token API yang dihasilkan di akun Confluence sebagai kata sandi Anda. Anda menyimpan kredensil berikut sebagai struktur JSON dalam rahasia Anda: Secrets Manager

```
{
    "username": "user name",
    "password": "API token"
}
```

> **Note**
>
> Kami menyarankan Anda secara teratur menyegarkan atau memutar kredensil dan rahasia Anda. Berikan hanya tingkat akses yang diperlukan untuk keamanan Anda sendiri. Kami tidak menyarankan Anda menggunakan kembali kredensil dan rahasia di seluruh sumber data, dan konektor versi 1.0 dan 2.0 (jika berlaku).

- IAM peran —Tentukan `RoleArn` kapan Anda menelepon `CreateDataSource` untuk memberikan IAM peran dengan izin untuk mengakses Secrets Manager rahasia Anda dan memanggil API publik yang diperlukan untuk konektor Confluence dan. Amazon Kendra Untuk informasi selengkapnya, lihat IAM peran untuk sumber data Confluence.

Anda juga dapat menambahkan fitur opsional berikut:

- Web proxy —Apakah akan terhubung ke instans URL Confluence Anda melalui proxy web. Anda dapat menggunakan opsi ini untuk Confluence Server.
- (Hanya untuk Confluence Server) Virtual Private Cloud (VPC) `VpcConfiguration` — Tentukan sebagai bagian dari konfigurasi sumber data. Lihat Mengkonfigurasi Amazon Kendra untuk menggunakan VPC.

- Filter inklusi dan pengecualian —Tentukan pola ekspresi reguler untuk menyertakan atau mengecualikan spasi, posting blog, halaman, spasi, dan lampiran tertentu. Jika Anda memilih untuk mengindeks lampiran, hanya lampiran ke halaman dan blog terindeks yang akan diindeks.

  > **Note**
  >
  > Sebagian besar sumber data menggunakan pola ekspresi reguler, yang merupakan pola inklusi atau pengecualian yang disebut sebagai filter. Jika Anda menentukan filter inklusi, hanya konten yang cocok dengan filter inklusi yang diindeks. Dokumen apa pun yang tidak cocok dengan filter inklusi tidak diindeks. Jika Anda menentukan filter inklusi dan pengecualian, dokumen yang cocok dengan filter pengecualian tidak akan diindeks, meskipun sesuai dengan filter inklusi.

- Pemetaan bidang —Pilih untuk memetakan bidang sumber data Confluence Anda ke bidang indeks Anda. Amazon Kendra Untuk informasi lebih lanjut, lihat Memetakan bidang sumber data.

  > **Note**
  >
  > Bidang badan dokumen atau badan dokumen yang setara untuk dokumen Anda diperlukan Amazon Kendra untuk mencari dokumen Anda. Anda harus memetakan nama bidang badan dokumen Anda di sumber data Anda ke nama bidang indeks_`document_body`. Semua kolom lain bersifat opsional.

- Pemfilteran konteks pengguna dan kontrol akses —Amazon Kendra meng-crawl daftar kontrol akses (ACL) untuk dokumen Anda, jika Anda memiliki ACL untuk dokumen Anda. Informasi ACL digunakan untuk memfilter hasil pencarian berdasarkan pengguna atau akses grup mereka ke dokumen. Untuk informasi selengkapnya, lihat Pemfilteran konteks pengguna.

Pelajari selengkapnya

Untuk mempelajari lebih lanjut tentang mengintegrasikan Amazon Kendra dengan sumber data Confluence Anda, lihat:

- Mengkonfigurasi konektor Amazon Kendra Confluence Server Anda

Konektor pertemuan V2.0

Confluence adalah alat manajemen kerja kolaboratif yang dirancang untuk berbagi, menyimpan, dan mengerjakan perencanaan proyek, pengembangan perangkat lunak, dan manajemen produk. Anda dapat menggunakan Amazon Kendra untuk mengindeks ruang Confluence Anda, halaman (termasuk halaman bersarang), blog, dan komentar dan lampiran ke halaman dan blog yang diindeks.

Untuk memecahkan masalah konektor sumber data Amazon Kendra Confluence, lihat. Mengatasi masalah sumber data

Topik

Fitur yang didukung

Amazon Kendra Konektor sumber data pertemuan mendukung fitur-fitur berikut:

- Pemetaan lapangan
- Pemfilteran konteks pengguna
- Pola inklusi/pengecualian
- Sinkronisasi konten penuh dan tambahan
- Cloud privat virtual (VPC)

Prasyarat

Sebelum Anda dapat menggunakan Amazon Kendra untuk mengindeks sumber data Confluence Anda, buat perubahan ini di Confluence dan akun Anda. AWS

Di Confluence, pastikan Anda memiliki:

- Menyalin URL instans Confluence Anda. Misalnya: *`https://example.confluence.com`*, atau *`https://www.example.confluence.com/`*, atau *`https://atlassian.net/`*. Anda memerlukan URL instans Confluence untuk terhubung. Amazon Kendra

  `Jika Anda menggunakan Confluence Cloud, url host Anda harus diakhiri dengan atlassian.net/.`

> **Note**
>
> Format URL berikut tidak didukung:
>
> - *https://example.confluence.com/xyz*
> - *https://www.example.confluence.com//wiki/spacekey/xxx*
> - *https://atlassian.net/xyz*

> **Note**
>
> (On-premise/server) Amazon Kendra memeriksa apakah informasi titik akhir yang disertakan sama dengan informasi titik akhir yang AWS Secrets Manager ditentukan dalam detail konfigurasi sumber data Anda. Ini membantu melindungi dari masalah wakil yang membingungkan, yang merupakan masalah keamanan di mana pengguna tidak memiliki izin untuk melakukan tindakan tetapi menggunakan Amazon Kendra sebagai proxy untuk mengakses rahasia yang dikonfigurasi dan melakukan tindakan. Jika nanti Anda mengubah informasi titik akhir Anda, Anda harus membuat rahasia baru untuk menyinkronkan informasi ini.

- Kredensyal otentikasi dasar yang dikonfigurasi yang berisi nama pengguna (ID email yang digunakan untuk masuk ke Confluence) dan kata sandi (kata sandi server Confluence) untuk memungkinkan Amazon Kendra Anda terhubung ke instans Confluence Anda. Untuk informasi tentang cara membuat token Confluence API, lihat Mengelola token API untuk akun Atlassian Anda.
- Opsional: Kredensyal OAuth 2.0 yang dikonfigurasi yang berisi kunci aplikasi Confluence, rahasia aplikasi Confluence, token akses Confluence, dan token penyegaran Confluence untuk memungkinkan Anda terhubung ke instans Confluence Anda. Amazon Kendra Jika token akses Anda kedaluwarsa, Anda dapat menggunakan token penyegaran untuk membuat ulang token akses dan menyegarkan pasangan token. Atau, Anda dapat mengulangi proses otorisasi. Untuk informasi selengkapnya tentang token akses, lihat Mengelola token akses OAuth.
- (Hanya untuk Server Confluence) Opsional: Mengkonfigurasi Token Akses Pribadi (PAT) yang berisi token Confluence untuk memungkinkan terhubung Amazon Kendra ke instance Confluence Anda. Untuk informasi tentang cara membuat token PAT, lihat Menggunakan Token Akses Pribadi.

Di dalam Anda Akun AWS, pastikan Anda memiliki:

- Membuat Amazon Kendra indeks dan, jika menggunakan API, mencatat ID indeks.
- Membuat IAM peran untuk sumber data Anda dan, jika menggunakan API, catat ARN peran tersebut IAM .

> **Note**
>
> Jika Anda mengubah jenis otentikasi dan kredensialnya, Anda harus memperbarui IAM peran Anda untuk mengakses ID rahasia yang benar AWS Secrets Manager .

- Menyimpan kredensi otentikasi Confluence Anda secara AWS Secrets Manager rahasia dan, jika menggunakan API, catat ARN rahasia tersebut.

> **Note**
>
> Kami menyarankan Anda secara teratur menyegarkan atau memutar kredensil dan rahasia Anda. Berikan hanya tingkat akses yang diperlukan untuk keamanan Anda sendiri. Kami tidak menyarankan Anda menggunakan kembali kredensil dan rahasia di seluruh sumber data, dan konektor versi 1.0 dan 2.0 (jika berlaku).

Jika Anda tidak memiliki IAM peran atau rahasia yang ada, Anda dapat menggunakan konsol untuk membuat IAM peran dan Secrets Manager rahasia baru saat menghubungkan sumber data Confluence. Amazon Kendra Jika Anda menggunakan API, Anda harus memberikan ARN IAM peran dan Secrets Manager rahasia yang ada, dan ID indeks.

Instruksi koneksi

Untuk terhubung Amazon Kendra ke sumber data Confluence Anda, Anda harus memberikan rincian kredenal Confluence Anda sehingga dapat mengakses data Anda. Amazon Kendra Jika Anda belum mengkonfigurasi Confluence untuk Amazon Kendra lihat. Prasyarat

Console

Untuk terhubung Amazon Kendra ke Confluence

1. Masuk ke Konsol AWS Manajemen dan buka Amazon Kendra konsol.
2. Dari panel navigasi kiri, pilih Indeks dan kemudian pilih indeks yang ingin Anda gunakan dari daftar indeks.

> **Note**
>
> Anda dapat memilih untuk mengonfigurasi atau mengedit pengaturan kontrol akses Pengguna di bawah Pengaturan indeks.

3. Pada halaman Memulai, pilih Tambahkan sumber data.
4. Pada halaman Tambah sumber data, pilih Konektor Confluence V2.0, lalu pilih Tambah konektor.
5. Pada halaman Tentukan detail sumber data, masukkan informasi berikut:
   a. Di Nama dan deskripsi, untuk Nama sumber data —Masukkan nama untuk sumber data Anda. Anda dapat memasukkan tanda hubung tetapi bukan spasi.
   b. (Opsional) Deskripsi —Masukkan deskripsi opsional untuk sumber data Anda.
   c. Dalam Bahasa default —Pilih bahasa untuk memfilter dokumen Anda untuk indeks. Kecuali Anda menentukan sebaliknya, bahasa default ke bahasa Inggris. Bahasa yang ditentukan dalam metadata dokumen mengesampingkan bahasa yang dipilih.
   d. Di Tag, untuk Tambahkan tag baru —Sertakan tag opsional untuk mencari dan memfilter sumber daya Anda atau melacak AWS biaya Anda.
   e. Pilih Berikutnya.
6. Pada halaman Tentukan akses dan keamanan, masukkan informasi berikut:
   a. Di Source, pilih antara Confluence Cloud dan Confluence Server berdasarkan metode hosting sumber data Confluence Anda.
   b. URL Confluence —Masukkan URL host Confluence. Format untuk URL host yang Anda masukkan adalah *`https://example.confluence.com`*.
   c. (Hanya untuk Confluence Server) Lokasi sertifikat SSL - opsional —Masukkan Amazon S3 jalur ke file sertifikat SSL Anda untuk Confluence Server.
   d. (Hanya untuk Confluence Server) Proxy web - opsional —Masukkan nama host proxy web (tanpa `https://` protokol `http://` atau) dan nomor Port (port yang digunakan oleh protokol transport URL host). Nomor port harus berupa nilai numerik antara 0 dan 65535.
   e. (Hanya untuk Confluence Server) Otorisasi —Pilih untuk mengaktifkan Access Control List (ACL). Kemudian, pilih antara Nama Pengguna dan Email untuk memilih bidang yang ingin Anda gunakan untuk kontrol akses.

f. Pilih antara otentikasi Dasar, otentikasi Oauth 2.0 dan (Hanya untuk server Confluence) otentikasi Token Akses Pribadi berdasarkan kasus penggunaan Anda.

g. AWS Secrets Manager rahasia —Pilih rahasia yang ada atau buat Secrets Manager rahasia baru untuk menyimpan kredensi otentikasi Confluence Anda. Jika Anda memilih untuk membuat rahasia baru, jendela AWS Secrets Manager rahasia terbuka. Masukkan informasi berikut di jendela:

   i. Nama rahasia —Nama untuk rahasiamu. Awalan 'AmazonKendra-Confluence-' secara otomatis ditambahkan ke nama rahasia Anda.

   ii. Jika menggunakan Otentikasi Dasar —Masukkan nama Rahasia Nama pengguna, dan Kata Sandi (kata sandi Server Confluence) yang Anda buat dan unduh dari akun Confluence Anda.

   Jika menggunakan OAuth2.0 Autentikasi —Masukkan nama Rahasia, Kunci aplikasi, Rahasia aplikasi, Token akses, dan token Refresh yang Anda buat di akun Confluence Anda.

   (Hanya server Confluence) Jika menggunakan otentikasi Token Akses Pribadi — Masukkan nama Rahasia dan token Confluence yang Anda buat di akun Confluence Anda.

   iii. Pilih Simpan dan tambahkan rahasia.

h. Di Konfigurasi VPC dan grup keamanan - opsional, untuk Virtual Private Cloud (VPC) —Anda dapat memilih untuk menggunakan VPC. Jika demikian, Anda harus menambahkan Subnet dan grup keamanan VPC.

i. Perayap identitas —Tentukan apakah akan mengaktifkan crawler Amazon Kendra identitas. Perayap identitas menggunakan informasi daftar kontrol akses (ACL) untuk dokumen Anda untuk memfilter hasil penelusuran berdasarkan akses pengguna atau grup mereka ke dokumen. Jika Anda memiliki ACL untuk dokumen Anda dan memilih untuk menggunakan ACL Anda, Anda juga dapat memilih untuk mengaktifkan crawler Amazon Kendra identitas untuk mengonfigurasi pemfilteran konteks pengguna dari hasil pencarian. Jika tidak, jika crawler identitas dimatikan, semua dokumen dapat dicari secara publik. Jika Anda ingin menggunakan kontrol akses untuk dokumen dan crawler identitas dimatikan, Anda dapat menggunakan PutPrincipalMappingAPI untuk mengunggah informasi akses pengguna dan grup untuk pemfilteran konteks pengguna.

j. IAM peran —Pilih peran yang ada atau buat IAM IAM peran baru untuk mengakses kredensi repositori dan mengindeks konten.

> **Note**
>
> IAM peran yang digunakan untuk indeks tidak dapat digunakan untuk sumber data. Jika Anda tidak yakin apakah peran yang ada digunakan untuk indeks atau FAQ, pilih Buat peran baru untuk menghindari kesalahan.

k. Pilih Berikutnya.

7. Pada halaman Konfigurasi pengaturan sinkronisasi, masukkan informasi berikut:

a. Dalam lingkup Sinkronisasi, untuk konten sinkronisasi, pilih untuk menyinkronkan dari jenis entitas berikut: Halaman, Komentar halaman, Lampiran halaman, Blog, Komentar Blog, Lampiran Blog, Ruang pribadi, dan Ruang yang diarsipkan.

> **Note**
>
> Komentar halaman dan lampiran Halaman hanya dapat dipilih jika Anda memilih untuk menyinkronkan Halaman. Komentar blog dan lampiran blog hanya dapat dipilih jika Anda memilih untuk menyinkronkan Blog.

> **Important**
>
> Jika Anda tidak menentukan pola regex kunci Spasi dalam konfigurasi Tambahan, semua Halaman dan Blog akan dirayapi secara default.

b. Dalam Konfigurasi tambahan untuk pola regex Spaces, tentukan apakah akan menyertakan atau mengecualikan spasi tertentu dalam indeks Anda menggunakan:

- Tombol spasi —Misalnya, *my-space-123*.

> **Note**
>
> Jika Anda tidak menentukan pola regex kunci Spasi dalam konfigurasi Tambahan, semua Halaman dan Blog akan dirayapi secara default.

- URL —*Misalnya,. *//MySiteMyDocuments/*.
- Jenis file —Misalnya, *.*\ .pdf, .*\ .txt*.

- Untuk Ukuran file Maksimum - Tentukan batas ukuran file di MB yang akan dirayapi Amazon Kendra. Amazon Kendra hanya akan merayapi file dalam batas ukuran yang Anda tentukan. Ukuran file default adalah 50MB. Ukuran file maksimum harus lebih besar dari 0MB dan kurang dari atau sama dengan 50MB.

- Untuk pola regex judul Entitas —Tentukan pola ekspresi reguler untuk menyertakan atau mengecualikan Blog, Halaman, Komentar, dan Lampiran tertentu berdasarkan judul.

> **Note**
>
> Jika Anda ingin merayapi halaman atau subhalaman tertentu, Anda dapat menggunakan pola regex judul halaman untuk menyertakan atau mengecualikan halaman ini.

c. Mode sinkronisasi —Pilih cara Anda ingin memperbarui indeks saat konten sumber data Anda berubah. Saat Anda menyinkronkan sumber data Amazon Kendra untuk pertama kalinya, semua konten dirayapi dan diindeks secara default. Anda harus menjalankan sinkronisasi penuh data Anda jika sinkronisasi awal Anda gagal, bahkan jika Anda tidak memilih sinkronisasi penuh sebagai opsi mode sinkronisasi Anda.

   - Sinkronisasi penuh: Indeks baru semua konten, ganti konten yang ada setiap kali sumber data Anda disinkronkan dengan indeks Anda.
   - Sinkronisasi baru, dimodifikasi, dihapus: Indeks hanya konten baru, dimodifikasi, dan dihapus setiap kali sumber data Anda disinkronkan dengan indeks Anda. Amazon Kendra dapat menggunakan mekanisme sumber data Anda untuk melacak perubahan konten dan mengindeks konten yang berubah sejak sinkronisasi terakhir.

d. Dalam jadwal berjalan Sinkronisasi, untuk Frekuensi —Seberapa sering Amazon Kendra akan disinkronkan dengan sumber data Anda.

e. Pilih Berikutnya.

8. Pada halaman Setel pemetaan bidang, masukkan informasi berikut:

   a. Untuk Spasi, Halaman, Blog, Komentar, dan Lampiran —Pilih dari bidang sumber data default yang Amazon Kendra dihasilkan yang ingin Anda petakan ke indeks Anda.

b. Tambahkan bidang —Untuk menambahkan bidang sumber data kustom untuk membuat nama bidang indeks untuk dipetakan dan tipe data bidang.

c. Pilih Berikutnya.

9. Pada halaman Tinjau dan buat, periksa apakah informasi yang Anda masukkan sudah benar dan kemudian pilih Tambahkan sumber data. Anda juga dapat memilih untuk mengedit informasi Anda dari halaman ini. Sumber data Anda akan muncul di halaman Sumber data setelah sumber data berhasil ditambahkan.

API

Untuk terhubung Amazon Kendra ke Confluence

Anda harus menentukan JSON dari skema sumber data menggunakan API. TemplateConfiguration Anda harus memberikan informasi berikut ini:

- Sumber data —Tentukan tipe sumber data seperti `CONFLUENCEV2` saat Anda menggunakan skema TemplateConfigurationJSON. Tentukan juga sumber data seperti `TEMPLATE` saat Anda memanggil CreateDataSourceAPI.
- URL Host —Tentukan versi instans host Confluence. Misalnya, *`https://example.confluence.com`*.
- Mode sinkronisasi —Tentukan cara Amazon Kendra memperbarui indeks Anda saat konten sumber data Anda berubah. Saat Anda menyinkronkan sumber data Amazon Kendra untuk pertama kalinya, semua konten dirayapi dan diindeks secara default. Anda harus menjalankan sinkronisasi penuh data Anda jika sinkronisasi awal Anda gagal, bahkan jika Anda tidak memilih sinkronisasi penuh sebagai opsi mode sinkronisasi Anda. Anda dapat memilih antara:
  - `FORCED_FULL_CRAWL`untuk mengindeks semua konten baru, mengganti konten yang ada setiap kali sumber data Anda disinkronkan dengan indeks Anda.
  - `FULL_CRAWL`untuk mengindeks hanya konten baru, dimodifikasi, dan dihapus setiap kali sumber data Anda disinkronkan dengan indeks Anda. Amazon Kendra dapat menggunakan mekanisme sumber data Anda untuk melacak perubahan konten dan mengindeks konten yang berubah sejak sinkronisasi terakhir.
- Jenis autentikasi —Tentukan jenis otentikasi, apakah `BasicOAuth2`, `Personal-token` untuk instance Confluence Anda.
- (Opsional—Hanya untuk Confluence Server) Lokasi sertifikat SSL —Khususnya dan Anda gunakan untuk menyimpan sertifikat SSL Anda. `S3bucketName` `s3certificateName`

- Rahasia Nama Sumber Daya Amazon (ARN) —Berikan Nama Sumber Daya Amazon (ARN) Secrets Manager rahasia yang berisi kredensyal otentikasi yang Anda buat di akun Confluence Anda. Jika Anda menggunakan otentikasi akun dasar, rahasia disimpan dalam struktur JSON dengan kunci berikut:

```
{
    "username": "Confluence account user name",
    "password": "Confluence API token"
}
```

Jika Anda menggunakan otentikasi OAuth 2.0, rahasia disimpan dalam struktur JSON dengan kunci berikut:

```
{
    "confluenceAppKey": "app key for your Confluence account",
    "confluenceAppSecret": "app secret from your Confluence token",
    "confluenceAccessToken": "access token created in Confluence",
    "confluenceRefreshToken": "refresh token created in Confluence"
}
```

(Hanya untuk Confluence Server) Jika Anda menggunakan otentikasi dasar, rahasia disimpan dalam struktur JSON dengan kunci berikut:

```
{
    "hostUrl": "Confluence Server host URL",
    "username": "Confluence Server user name",
    "password": "Confluence Server password"
}
```

(Hanya untuk Server Confluence) Jika Anda menggunakan otentikasi Token Akses Pribadi, rahasia disimpan dalam struktur JSON dengan kunci berikut:

```
{
    "hostUrl": "Confluence Server host URL",
    "patToken": "Confluence token"
}
```

> **Note**
>
> Kami menyarankan Anda secara teratur menyegarkan atau memutar kredensil dan rahasia Anda. Berikan hanya tingkat akses yang diperlukan untuk keamanan Anda sendiri. Kami tidak menyarankan Anda menggunakan kembali kredensil dan rahasia di seluruh sumber data, dan konektor versi 1.0 dan 2.0 (jika berlaku).

- IAM peran —Tentukan `RoleArn` kapan Anda menelepon `CreateDataSource` untuk memberikan IAM peran dengan izin untuk mengakses Secrets Manager rahasia Anda dan memanggil API publik yang diperlukan untuk konektor Confluence dan. Amazon Kendra Untuk informasi selengkapnya, lihat IAM peran untuk sumber data Confluence.

Anda juga dapat menambahkan fitur opsional berikut:

- Virtual Private Cloud (VPC) **`VpcConfiguration`** —Tentukan kapan Anda menelepon. `CreateDataSource` Untuk informasi selengkapnya, lihat Mengkonfigurasi Amazon Kendra untuk menggunakan Amazon VPC.
- Filter inklusi dan pengecualian —Anda dapat menentukan apakah akan menyertakan atau mengecualikan spasi, halaman, blog, serta komentar dan lampirannya tertentu.

> **Note**
>
> Sebagian besar sumber data menggunakan pola ekspresi reguler, yang merupakan pola inklusi atau pengecualian yang disebut sebagai filter. Jika Anda menentukan filter inklusi, hanya konten yang cocok dengan filter inklusi yang diindeks. Dokumen apa pun yang tidak cocok dengan filter inklusi tidak diindeks. Jika Anda menentukan filter inklusi dan pengecualian, dokumen yang cocok dengan filter pengecualian tidak akan diindeks, meskipun sesuai dengan filter inklusi.

- Perayap identitas —Tentukan apakah akan mengaktifkan crawler Amazon Kendra identitas. Perayap identitas menggunakan informasi daftar kontrol akses (ACL) untuk dokumen Anda untuk memfilter hasil penelusuran berdasarkan akses pengguna atau grup mereka ke dokumen. Jika Anda memiliki ACL untuk dokumen Anda dan memilih untuk menggunakan ACL Anda, Anda juga dapat memilih untuk mengaktifkan crawler Amazon Kendra identitas untuk mengonfigurasi pemfilteran konteks pengguna dari hasil pencarian. Jika tidak, jika crawler identitas dimatikan, semua dokumen dapat dicari secara publik. Jika Anda ingin menggunakan

kontrol akses untuk dokumen dan crawler identitas dimatikan, Anda dapat menggunakan PutPrincipalMappingAPI untuk mengunggah informasi akses pengguna dan grup untuk pemfilteran konteks pengguna.

- Pemetaan bidang —Pilih untuk memetakan bidang sumber data Confluence Anda ke bidang indeks Anda. Amazon Kendra Untuk informasi lebih lanjut, lihat Memetakan bidang sumber data.

> **Note**
>
> Bidang badan dokumen atau badan dokumen yang setara untuk dokumen Anda diperlukan Amazon Kendra untuk mencari dokumen Anda. Anda harus memetakan nama bidang badan dokumen Anda di sumber data Anda ke nama bidang indeks_`document_body`. Semua kolom lain bersifat opsional.

Untuk daftar kunci JSON penting lainnya untuk dikonfigurasi, lihatSkema templat pertemuan.

Catatan

- Token Akses Pribadi (PAT) tidak tersedia untuk Confluence Cloud.

Konektor sumber data kustom

Gunakan sumber data kustom ketika Anda memiliki repositori yang Amazon Kendra belum menyediakan konektor sumber data untuk. Anda dapat menggunakannya untuk melihat metrik riwayat proses yang sama yang disediakan sumber Amazon Kendra data bahkan ketika Anda tidak dapat menggunakan Amazon Kendra sumber data untuk menyinkronkan repositori Anda. Gunakan ini untuk membuat pengalaman pemantauan sinkronisasi yang konsisten antara sumber Amazon Kendra data dan sumber khusus. Secara khusus, gunakan sumber data khusus untuk melihat metrik sinkronisasi untuk konektor sumber data yang Anda buat menggunakan BatchPutDocumentdan BatchDeleteDocumentAPI.

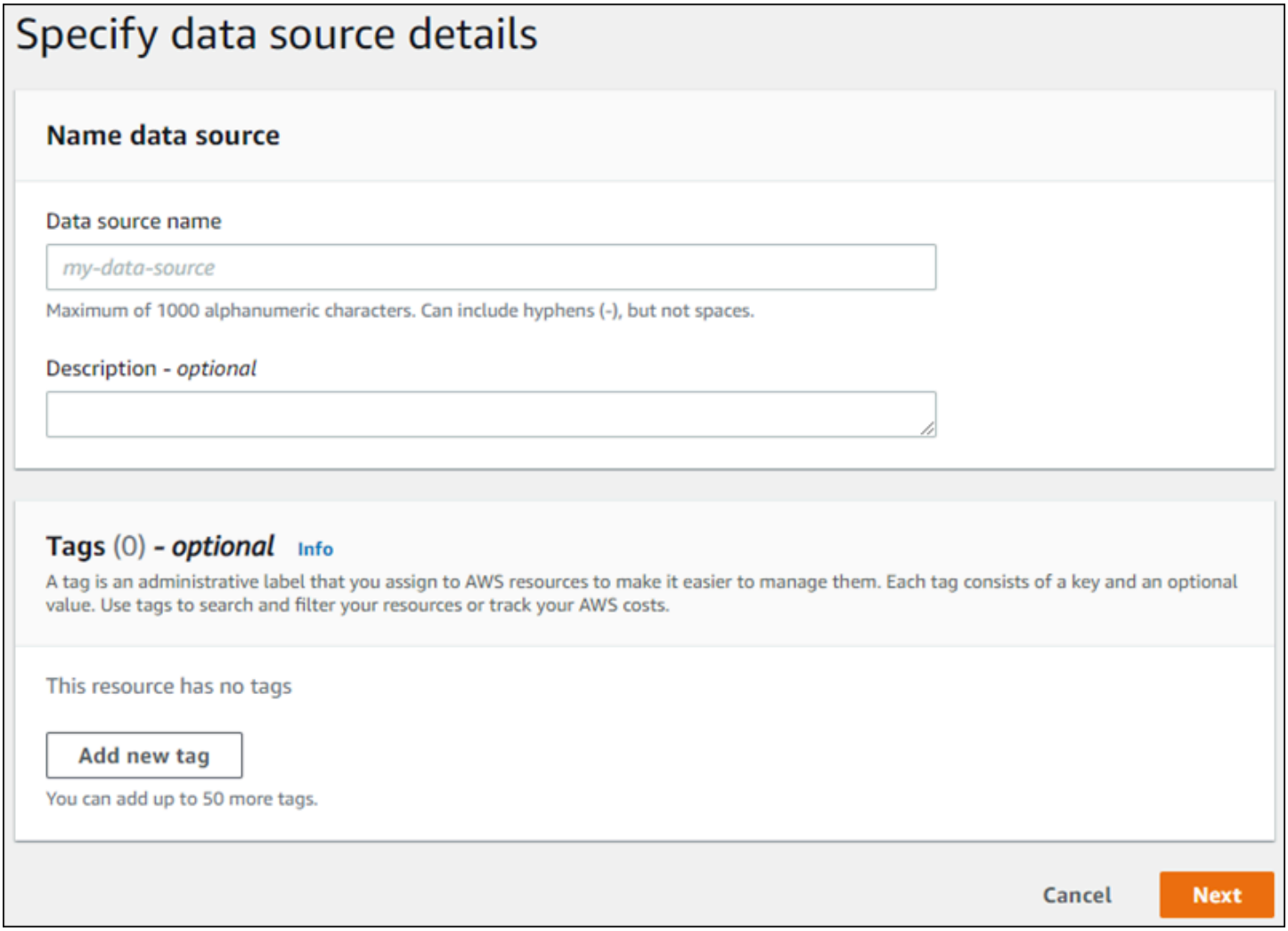
Untuk memecahkan masalah konektor sumber data kustom Amazon Kendra, lihat. Mengatasi masalah sumber data

Saat Anda membuat sumber data kustom, Anda memiliki kontrol penuh atas bagaimana dokumen yang akan diindeks dipilih. Amazon Kendrahanya menyediakan informasi metrik yang dapat Anda

gunakan untuk memantau pekerjaan sinkronisasi sumber data Anda. Anda harus membuat dan menjalankan crawler yang menentukan dokumen yang diindeks sumber data Anda.

Anda harus menentukan judul utama dokumen Anda menggunakan objek Dokumen, dan `_source_uri` untuk memiliki `DocumentTitle` dan `DocumentURI` termasuk dalam respons `Query` hasil. DocumentAttribute

Anda membuat pengenal untuk sumber data kustom Anda menggunakan konsol atau dengan menggunakan CreateDataSourceAPI. Untuk menggunakan konsol tersebut, beri nama sumber data Anda, serta deskripsi dan tanda sumber daya, jika perlu. Setelah sumber data dibuat, ID sumber data ditampilkan. Salin ID ini untuk digunakan saat Anda menyinkronkan sumber data dengan indeks.



Anda juga dapat membuat sumber data kustom menggunakan `CreateDataSource` API. API mengembalikan ID yang akan digunakan saat Anda menyinkronkan sumber data. Bila Anda menggunakan `CreateDataSource` API untuk membuat sumber data kustom, Anda tidak dapat

mengaturConfiguration, RoleArn atau Schedule parameter. Jika Anda mengatur parameter ini, Amazon Kendra mengembalikan ValidationException pengecualian.

Untuk menggunakan sumber data khusus, buat aplikasi yang bertanggung jawab untuk memperbarui Amazon Kendra indeks. Aplikasi tersebut bergantung pada crawler yang Anda buat. Crawler membaca dokumen di repositori Anda dan menentukan mana yang harus dikirim. Amazon Kendra Aplikasi Anda harus melakukan langkah-langkah berikut:

1. Crawl repositori Anda dan buat daftar dokumen di repositori Anda yang ditambahkan, diperbarui, atau dihapus.
2. Panggil StartDataSourceSyncJobAPI untuk memberi sinyal bahwa pekerjaan sinkronisasi dimulai. Anda memberikan ID sumber data untuk mengidentifikasi sumber data yang disinkronkan. Amazon Kendramengembalikan ID eksekusi untuk mengidentifikasi pekerjaan sinkronisasi tertentu.
3. Panggil BatchDeleteDocumentAPI untuk menghapus dokumen dari indeks. Berikan ID sumber data dan ID eksekusi untuk mengidentifikasi sumber data yang sedang disinkronkan dan tugas yang terkait dengan pembaruan ini.
4. Panggil StopDataSourceSyncJobAPI untuk memberi sinyal akhir dari pekerjaan sinkronisasi. Setelah Anda memanggil StopDataSourceSyncJob API, ID eksekusi terkait tidak lagi valid.
5. Panggil ListDataSourceSyncJobsAPI dengan pengenal indeks dan sumber data untuk mencantumkan pekerjaan sinkronisasi sumber data dan untuk melihat metrik untuk pekerjaan sinkronisasi.

Setelah menyelesaikan tugas sinkronisasi, Anda dapat memulai tugas sinkronisasi baru. Mungkin perlu waktu beberapa lama sebelum semua dokumen yang dikirim ditambahkan ke indeks. Gunakan ListDataSourceSyncJobs API untuk melihat status pekerjaan sinkronisasi. Jika Status yang dikembalikan untuk tugas sinkronisasi adalah SYNCING_INDEXING, beberapa dokumen masih diindeks. Anda dapat memulai pekerjaan sinkronisasi baru ketika status pekerjaan sebelumnya adalah FAILED atauSUCCEEDED.

Setelah memanggil StopDataSourceSyncJob API, Anda tidak dapat menggunakan pengenal pekerjaan sinkronisasi dalam panggilan ke BatchPutDocument atau BatchDeleteDocument API. Jika Anda melakukannya, semua dokumen yang dikirimkan akan dikembalikan dalam pesan FailedDocuments respons dari API.

Atribut yang diperlukan

Saat Anda mengirimkan dokumen untuk Amazon Kendra menggunakan `BatchPutDocument` API, setiap dokumen memerlukan dua atribut untuk mengidentifikasi sumber data dan menjalankan sinkronisasi yang dimilikinya. Anda harus memberikan dua atribut berikut untuk memetakan dokumen dari sumber data kustom Anda dengan benar ke Amazon Kendra indeks:

- `_data_source_id`—Pengidentifikasi sumber data. Ini dikembalikan saat Anda membuat sumber data dengan konsol atau `CreateDataSource` API.
- `_data_source_sync_job_execution_id`—Pengidentifikasi dari proses sinkronisasi. Ini dikembalikan saat Anda memulai sinkronisasi indeks dengan `StartDataSourceSyncJob` API.

Berikut ini adalah JSON yang diperlukan untuk indeks dokumen menggunakan sumber data kustom.

```
{
    "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"
}
```

Saat Anda menghapus dokumen dari indeks menggunakan `BatchDeleteDocument` API, Anda perlu menentukan dua bidang berikut dalam `DataSourceSyncJobMetricTarget` parameter:

- `DataSourceId`—Pengidentifikasi sumber data. Ini dikembalikan saat Anda membuat sumber data dengan konsol atau `CreateDataSource` API.
- `DataSourceSyncJobId`—Pengidentifikasi dari proses sinkronisasi. Ini dikembalikan saat Anda memulai sinkronisasi indeks dengan `StartDataSourceSyncJob` API.

Berikut ini adalah JSON yang diperlukan untuk menghapus dokumen dari indeks menggunakan `BatchDeleteDocument` API.

```
{
    "DataSourceSyncJobMetricTarget": {
        "DataSourceId": "data source identifier",
        "DataSourceSyncJobId": "sync job identifier"
    },
    "DocumentIdList": [
        "document identifier"
    ],
    "IndexId": "index identifier"
}
```

Melihat metrik

Setelah pekerjaan sinkronisasi selesai, Anda dapat menggunakan DataSourceSyncJobMetricsAPI untuk mendapatkan metrik yang terkait dengan pekerjaan sinkronisasi. Gunakan ini untuk memantau sinkronisasi sumber data kustom Anda.

Jika Anda mengirimkan dokumen yang sama beberapa kali, baik sebagai bagian dari `BatchPutDocument` API, `BatchDeleteDocument` API, atau jika dokumen dikirimkan untuk penambahan dan penghapusan, dokumen hanya dihitung satu kali dalam metrik.

- `DocumentsAdded`—Jumlah dokumen yang dikirimkan menggunakan `BatchPutDocument` API yang terkait dengan pekerjaan sinkronisasi ini ditambahkan ke indeks untuk pertama kalinya. Jika dokumen dikirimkan untuk penambahan lebih dari sekali dalam sinkronisasi, dokumen hanya dihitung satu kali dalam metrik.
- `DocumentsDeleted`—Jumlah dokumen yang dikirimkan menggunakan `BatchDeleteDocument` API yang terkait dengan pekerjaan sinkronisasi ini dihapus dari indeks. Jika dokumen dikirimkan

untuk penghapusan lebih dari sekali dalam sinkronisasi, dokumen hanya dihitung satu kali dalam metrik.

- `DocumentsFailed`—Jumlah dokumen yang terkait dengan pekerjaan sinkronisasi ini yang gagal dalam pengindeksan. Ini adalah dokumen yang diterima oleh Amazon Kendra untuk pengindeksan tetapi tidak dapat diindeks atau dihapus. Jika dokumen tidak diterima olehAmazon Kendra, pengenal untuk dokumen dikembalikan dalam properti `FailedDocuments` respon `BatchDeleteDocument` API `BatchPutDocument` dan.
- `DocumentsModified`—Jumlah dokumen yang dimodifikasi yang dikirimkan menggunakan `BatchPutDocument` API yang terkait dengan pekerjaan sinkronisasi ini yang dimodifikasi dalam Amazon Kendra indeks.

Amazon Kendrajuga memancarkan Amazon CloudWatch metrik saat mengindeks dokumen. Untuk informasi selengkapnya, lihat Memantau Amazon Kendra dengan Amazon CloudWatch.

Amazon Kendratidak mengembalikan `DocumentsScanned` metrik untuk sumber data khusus. Ini juga memancarkan CloudWatch metrik yang tercantum dalam dokumen Metrik untuk Amazon Kendra sumber data.

Pelajari selengkapnya

Untuk mempelajari lebih lanjut tentang mengintegrasikan Amazon Kendra dengan sumber data kustom Anda, lihat:

- Menambahkan sumber data kustom ke Amazon Kendra

Sumber data kustom (Java)

Kode berikut memberikan contoh implementasi sumber data kustom menggunakan Java. Program pertama membuat sumber data kustom dan kemudian menyinkronkan dokumen yang baru ditambahkan ke indeks dengan sumber data kustom.

Kode berikut menunjukkan pembuatan dan penggunaan sumber data kustom. Bila Anda menggunakan sumber data kustom dalam aplikasi Anda, Anda tidak perlu membuat sumber data baru (proses satu kali) setiap kali Anda menyinkronkan indeks Anda dengan sumber data Anda. Anda menggunakan ID indeks dan ID sumber data untuk menyinkronkan data Anda.

```
package com.amazonaws.kendra;
```

```
import java.util.concurrent.TimeUnit;
import software.amazon.awssdk.services.kendra.KendraClient;
import csoftware.amazon.awssdk.services.kendra.model.BatchPutDocumentRequest;
import csoftware.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 yor 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();

    // 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));

    // Wait for the sync job status to succeed
    // If the sync job status is SYNCING_INDEXING, documents are still being indexed
    // If the sync job status is SYNCING, sync job has started
    System.out.println(String.format("Waiting for the data
source to sync with the index %s for execution ID %s", indexId,
startDataSourceSyncJobResponse.executionId()));
    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("Syncing data source. Status: %s",
job.status()));
```

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

        TimeUnit.SECONDS.sleep(60);

    }

    // Once custom data source synced, stop the sync job using the
 StopDataSourceSyncJob API
    StopDataSourceSyncJobResponse stopDataSourceSyncJobResponse =
 kendra.stopDataSourceSyncJob(
        StopDataSourceSyncJobRequest()
            .indexId(myIndexId)
            .id(dataSourceId)
    );
  }
}
```

Dropbox

Dropbox adalah layanan hosting file yang menawarkan penyimpanan cloud, organisasi dokumen, dan layanan template dokumen. Jika Anda pengguna Dropbox, Anda dapat menggunakannya Amazon Kendra untuk mengindeks file Dropbox, Dropbox Paper, Template Dropbox Paper, dan pintasan tersimpan ke halaman web. Anda juga dapat mengonfigurasi Amazon Kendra untuk mengindeks file Dropbox tertentu, Dropbox Paper, Template Dropbox Paper, dan pintasan tersimpan ke halaman web.

Amazon Kendra mendukung Dropbox dan Dropbox Advanced untuk Dropbox Business.

Anda dapat terhubung Amazon Kendra ke sumber data Dropbox menggunakan Amazon Kendra konsol dan TemplateConfigurationAPI.

Untuk mengatasi masalah konektor sumber data Amazon Kendra Dropbox Anda, lihat. Mengatasi masalah sumber data

Topik

- Fitur yang didukung
- Prasyarat
- Instruksi koneksi

- Pelajari selengkapnya

Fitur yang didukung

Amazon Kendra Konektor sumber data Dropbox mendukung fitur-fitur berikut:

- Ubah log
- Pemetaan lapangan
- Pemfilteran konteks pengguna
- Filter inklusi/pengecualian
- Cloud privat virtual (VPC)

Prasyarat

Sebelum dapat digunakan Amazon Kendra untuk mengindeks sumber data Dropbox Anda, lakukan perubahan ini di Dropbox dan AWS akun Anda.

Di Dropbox, pastikan Anda memiliki:

- Membuat akun Dropbox Advanced dan menyiapkan pengguna admin.
- Membuat aplikasi Dropbox dengan nama Aplikasi unik, mengaktifkan Scoped Access. Lihat dokumentasi Dropbox tentang membuat aplikasi.
- Aktifkan izin Dropbox Lengkap di konsol Dropbox dan menambahkan izin berikut:
  - file.content.read
  - files.metadata.read
  - berbagi.baca
  - file_requests.read
  - kelompok.baca
  - team_info.read
  - team_data.content.read
- Mencatat kunci aplikasi Dropbox Anda, rahasia aplikasi Dropbox, dan token akses Dropbox untuk kredensyal otentikasi dasar.
- Membuat dan menyalin token akses Oauth 2.0 sementara untuk aplikasi Dropbox Anda. Token ini bersifat sementara dan kedaluwarsa setelah 4 jam. Lihat dokumentasi Dropbox tentang autentikasi OAuth.

> **Note**
>
> Anda disarankan untuk membuat token akses penyegaran Dropbox yang tidak pernah kedaluwarsa, alih-alih mengandalkan token akses satu kali yang kedaluwarsa setelah 4 jam. Token akses penyegaran bersifat permanen dan tidak pernah kedaluwarsa sehingga Anda dapat terus menyinkronkan sumber data Anda di masa mendatang.

- Direkomendasikan: Mengonfigurasi token penyegaran permanen Dropbox yang tidak pernah kedaluwarsa untuk memungkinkan Amazon Kendra untuk terus menyinkronkan sumber data Anda tanpa gangguan apa pun. Lihat dokumentasi Dropbox tentang token penyegaran.
- Memeriksa setiap dokumen unik di Dropbox dan di seluruh sumber data lain yang Anda rencanakan untuk digunakan untuk indeks yang sama. Setiap sumber data yang ingin Anda gunakan untuk indeks tidak boleh berisi dokumen yang sama di seluruh sumber data. ID dokumen bersifat global untuk indeks dan harus unik per indeks.

Di dalam Anda Akun AWS, pastikan Anda memiliki:

- Membuat Amazon Kendra indeks dan, jika menggunakan API, mencatat ID indeks.
- Membuat IAM peran untuk sumber data Anda dan, jika menggunakan API, catat ARN peran tersebut IAM .

> **Note**
>
> Jika Anda mengubah jenis otentikasi dan kredensyal, Anda harus memperbarui IAM peran Anda untuk mengakses ID rahasia yang benar AWS Secrets Manager .

- Menyimpan kredensi otentikasi Dropbox Anda secara AWS Secrets Manager rahasia dan, jika menggunakan API, catat ARN rahasianya.

> **Note**
>
> Kami menyarankan Anda secara teratur menyegarkan atau memutar kredensi dan rahasia Anda. Berikan hanya tingkat akses yang diperlukan untuk keamanan Anda sendiri. Kami tidak menyarankan Anda menggunakan kembali kredensyal dan rahasia di seluruh sumber data, dan konektor versi 1.0 dan 2.0 (jika berlaku).

Jika Anda tidak memiliki IAM peran atau rahasia yang ada, Anda dapat menggunakan konsol untuk membuat IAM peran dan Secrets Manager rahasia baru saat Anda menghubungkan sumber data Dropbox Anda. Amazon Kendra Jika Anda menggunakan API, Anda harus memberikan ARN IAM peran dan Secrets Manager rahasia yang ada, dan ID indeks.

Instruksi koneksi

Untuk terhubung Amazon Kendra ke sumber data Dropbox Anda, Anda harus memberikan rincian yang diperlukan dari sumber data Dropbox Anda sehingga Amazon Kendra dapat mengakses data Anda. Jika Anda belum mengonfigurasi Dropbox Amazon Kendra, lihatPrasyarat.

Console

Untuk terhubung Amazon Kendra ke Dropbox

1. Masuk ke AWS Management Console dan buka Amazon Kendra konsol.
2. Dari panel navigasi kiri, pilih Indeks dan kemudian pilih indeks yang ingin Anda gunakan dari daftar indeks.

> **Note**
>
> Anda dapat memilih untuk mengonfigurasi atau mengedit pengaturan kontrol akses Pengguna Anda di bawah Pengaturan indeks.

3. Pada halaman Memulai, pilih Tambahkan sumber data.
4. Pada halaman Tambah sumber data, pilih konektor Dropbox, lalu pilih Tambah konektor.
5. Pada halaman Tentukan detail sumber data, masukkan informasi berikut:
   a. Dalam Nama dan deskripsi, untuk Nama sumber data —Masukkan nama untuk sumber data Anda. Anda dapat memasukkan tanda hubung tetapi bukan spasi.
   b. (Opsional) Deskripsi —Masukkan deskripsi opsional untuk sumber data Anda.
   c. Dalam Bahasa default —Pilih bahasa untuk memfilter dokumen Anda untuk indeks. Kecuali Anda menentukan sebaliknya, bahasa default ke bahasa Inggris. Bahasa yang ditentukan dalam metadata dokumen mengesampingkan bahasa yang dipilih.
   d. Di Tag, untuk Tambahkan tag baru —Sertakan tag opsional untuk mencari dan memfilter sumber daya Anda atau melacak AWS biaya Anda.
   e. Pilih Berikutnya.
6. Pada halaman Tentukan akses dan keamanan, masukkan informasi berikut:

a. Jenis token otentikasi —Pilih antara Token Permanen (disarankan) dan Token Akses (penggunaan sementara) berdasarkan kasus penggunaan Anda.

b. AWS Secrets Manager rahasia —Pilih rahasia yang ada atau buat Secrets Manager rahasia baru untuk menyimpan kredensyal otentikasi Dropbox Anda. Jika Anda memilih untuk membuat rahasia baru, jendela AWS Secrets Manager rahasia terbuka.

   i. Masukkan informasi berikut di jendela Buat AWS Secrets Manager rahasia:

      A. Nama rahasia —Nama untuk rahasiamu. Awalan 'AmazonKendra-Dropbox-' secara otomatis ditambahkan ke nama rahasia Anda.

      B. Untuk kunci Aplikasi, Rahasia aplikasi, dan informasi token (permanen atau sementara) —Masukkan nilai kredensi otentikasi yang Anda hasilkan dari akun Dropbox Anda.

   ii. Pilih Simpan.

c. Virtual Private Cloud (VPC) —Anda dapat memilih untuk menggunakan VPC. Jika demikian, Anda harus menambahkan Subnet dan grup keamanan VPC.

d. IAM peran —Pilih peran yang sudah ada atau buat IAM IAM peran baru untuk mengakses kredensi repositori dan mengindeks konten Anda.

> **Note**
>
> IAM peran yang digunakan untuk indeks tidak dapat digunakan untuk sumber data. Jika Anda tidak yakin apakah peran yang ada digunakan untuk indeks atau FAQ, pilih Buat peran baru untuk menghindari kesalahan.

e. Pilih Berikutnya.

7. Pada halaman Konfigurasi pengaturan sinkronisasi, masukkan informasi berikut:

a. Untuk Pilih entitas atau tipe konten —Pilih entitas atau jenis konten yang ingin dirayapi.

b. Ubah mode log —Pilih untuk memperbarui indeks Anda hanya dengan konten baru dan yang dimodifikasi alih-alih menyinkronkan semua file.

c. Dalam konfigurasi tambahan untuk pola Regex —Tambahkan pola ekspresi reguler untuk menyertakan atau mengecualikan file tertentu.

d. Dalam jadwal berjalan Sinkronisasi, untuk Frekuensi — Pilih seberapa sering Amazon Kendra akan disinkronkan dengan sumber data Anda.

e. Pilih Berikutnya.

8. Pada halaman Setel pemetaan bidang, masukkan informasi berikut:

   a. Templat file, Dropbox Paper, dan Dropbox Paper —Pilih dari bidang sumber data default Amazon Kendra yang dihasilkan yang ingin Anda petakan ke indeks Anda.

   b. Tambahkan bidang —Untuk menambahkan bidang sumber data kustom untuk membuat nama bidang indeks untuk dipetakan dan tipe data bidang.

   c. Pilih Berikutnya.

9. Pada halaman Tinjau dan buat, periksa apakah informasi yang Anda masukkan sudah benar dan kemudian pilih Tambahkan sumber data. Anda juga dapat memilih untuk mengedit informasi Anda dari halaman ini. Sumber data Anda akan muncul di halaman Sumber data setelah sumber data berhasil ditambahkan.

API

Untuk terhubung Amazon Kendra ke Dropbox

Anda harus menentukan JSON dari skema sumber data menggunakan API. TemplateConfiguration Anda harus memberikan informasi berikut ini:

- Sumber data —Tentukan tipe sumber data seperti `DROPBOX` saat Anda menggunakan skema TemplateConfigurationJSON. Tentukan juga sumber data seperti `TEMPLATE` saat Anda memanggil CreateDataSourceAPI.
- Ubah log —Apakah Amazon Kendra harus menggunakan mekanisme log perubahan sumber data Dropbox untuk menentukan apakah dokumen harus diperbarui dalam indeks.

  > **Note**
  >
  > Gunakan log perubahan jika Anda tidak Amazon Kendra ingin memindai semua dokumen. Jika log perubahan Anda berukuran besar, mungkin perlu waktu Amazon Kendra lebih sedikit untuk memindai dokumen di sumber data Dropbox daripada memproses log perubahan. Jika Anda menyinkronkan sumber data Dropbox dengan indeks untuk pertama kalinya, semua dokumen dipindai.

- Rahasia Nama Sumber Daya Amazon (ARN) —Berikan Nama Sumber Daya Amazon (ARN) Secrets Manager rahasia yang berisi kredensi otentikasi untuk akun Dropbox Anda. Rahasianya disimpan dalam struktur JSON dengan kunci berikut:

```
{
    "appKey": "Dropbox app key",
    "appSecret": "Dropbox app secret",
    "accesstoken": "temporary access token or refresh access token"
}
```

> **Note**
>
> Kami menyarankan Anda secara teratur menyegarkan atau memutar kredensi dan rahasia Anda. Berikan hanya tingkat akses yang diperlukan untuk keamanan Anda sendiri. Kami tidak menyarankan Anda menggunakan kembali kredensyal dan rahasia di seluruh sumber data, dan konektor versi 1.0 dan 2.0 (jika berlaku).

- IAM peran —Tentukan `RoleArn` kapan Anda menelepon `CreateDataSource` untuk memberikan IAM peran dengan izin untuk mengakses Secrets Manager rahasia Anda dan memanggil API publik yang diperlukan untuk konektor Dropbox dan. Amazon Kendra Untuk informasi selengkapnya, lihat IAM peran untuk sumber data Dropbox.

Anda juga dapat menambahkan fitur opsional berikut:

- Virtual Private Cloud (VPC) **`VpcConfiguration`** —Tentukan kapan Anda menelepon. `CreateDataSource` Untuk informasi selengkapnya, lihat Mengkonfigurasi Amazon Kendra untuk menggunakan Amazon VPC.
- Filter inklusi dan pengecualian —Tentukan apakah akan menyertakan atau mengecualikan file tertentu.

> **Note**
>
> Sebagian besar sumber data menggunakan pola ekspresi reguler, yang merupakan pola inklusi atau pengecualian yang disebut sebagai filter. Jika Anda menentukan filter inklusi, hanya konten yang cocok dengan filter inklusi yang diindeks. Dokumen apa pun yang tidak cocok dengan filter inklusi tidak diindeks. Jika Anda menentukan filter inklusi dan pengecualian, dokumen yang cocok dengan filter pengecualian tidak akan diindeks, meskipun sesuai dengan filter inklusi.

- Pemfilteran konteks pengguna dan kontrol akses —Amazon Kendra meng-crawl daftar kontrol akses (ACL) untuk dokumen Anda, jika Anda memiliki ACL untuk dokumen Anda. Informasi

ACL digunakan untuk memfilter hasil pencarian berdasarkan pengguna atau akses grup mereka ke dokumen. Untuk informasi selengkapnya, lihat Pemfilteran konteks pengguna.

- Pemetaan bidang —Pilih untuk memetakan bidang sumber data Dropbox Anda ke bidang indeks Anda. Amazon Kendra Untuk informasi lebih lanjut, lihat Memetakan bidang sumber data.

> **Note**
>
> Bidang badan dokumen atau badan dokumen yang setara untuk dokumen Anda diperlukan Amazon Kendra untuk mencari dokumen Anda. Anda harus memetakan nama bidang badan dokumen Anda di sumber data Anda ke nama bidang indeks_`document_body`. Semua kolom lain bersifat opsional.

Untuk daftar kunci JSON penting lainnya untuk dikonfigurasi, lihatSkema templat Dropbox.

Pelajari selengkapnya

Untuk mempelajari lebih lanjut tentang mengintegrasikan Amazon Kendra dengan sumber data Dropbox Anda, lihat:

- Indeks konten Dropbox Anda menggunakan konektor Dropbox untuk Amazon Kendra

Drupal

Drupal adalah sistem manajemen konten open-source (CMS) yang dapat Anda gunakan untuk membuat situs web dan aplikasi web. Anda dapat menggunakan Amazon Kendra untuk mengindeks berikut ini di Drupal:

- Konten—Artikel, Halaman dasar, Blok dasar, Jenis konten yang ditentukan pengguna, Jenis blok yang ditentukan pengguna, Jenis konten khusus, Jenis blok kustom
- Komentar—Untuk semua jenis Konten dan jenis Blok
- Lampiran—Untuk semua jenis Konten dan jenis Blok

Anda dapat terhubung Amazon Kendra ke sumber data Drupal Anda menggunakan Amazon Kendra konsol atau TemplateConfigurationAPI.

Untuk memecahkan masalah konektor sumber data Amazon Kendra Drupal Anda, lihat. Mengatasi masalah sumber data

Topik

Fitur yang didukung

Amazon Kendra Konektor sumber data Drupal mendukung fitur-fitur berikut:

- Pemetaan lapangan
- Pemfilteran konteks pengguna
- Filter inklusi/pengecualian
- Sinkronisasi konten penuh dan tambahan
- Cloud privat virtual (VPC)

Prasyarat

Sebelum Anda dapat menggunakan Amazon Kendra untuk mengindeks sumber data Drupal Anda, buat perubahan ini di Drupal dan AWS akun Anda.

Di Drupal, pastikan Anda memiliki:

- Membuat akun Drupal (Standard) Suite dan pengguna dengan peran administrator.
- Menyalin nama situs Drupal Anda dan mengkonfigurasi url host. <drupalsitename>Misalnya, *https:///*<hostname>.
- Kredensial otentikasi dasar yang dikonfigurasi yang berisi nama pengguna (nama pengguna login situs web Drupal) dan kata sandi (kata sandi situs web Drupal).
- Direkomendasikan: Mengonfigurasi token kredensi OAuth 2.0. Gunakan token ini bersama dengan pemberian kata sandi Drupal Anda, id klien, rahasia klien, nama pengguna (nama pengguna login situs web Drupal) dan kata sandi (kata sandi situs web Drupal) untuk terhubung. Amazon Kendra
- Menambahkan izin berikut di akun Drupal Anda menggunakan peran administrator:

- mengelola blok
- mengelola tampilan block_content
- mengelola bidang block_content
- mengelola tampilan formulir block_content
- mengelola pandangan
- melihat alamat email pengguna
- melihat konten yang tidak dipublikasikan sendiri
- lihat revisi halaman
- lihat revisi artikel
- lihat semua revisi
- melihat tema administrasi
- mengakses konten
- akses ikhtisar konten
- akses komentar
- konten pencarian
- ikhtisar file akses
- mengakses tautan kontekstual

> **Note**
>
> Jika ada jenis konten yang ditentukan pengguna atau jenis blok yang ditentukan pengguna, atau tampilan dan blok apa pun ditambahkan ke situs web Drupal, mereka harus dilengkapi dengan akses administrator.

Di dalam Anda Akun AWS, pastikan Anda memiliki:

- Membuat Amazon Kendra indeks dan, jika menggunakan API, mencatat ID indeks.
- Membuat IAM peran untuk sumber data Anda dan, jika menggunakan API, catat ARN peran tersebut IAM .

> **Note**
>
> Jika Anda mengubah jenis otentikasi dan kredensialnya, Anda harus memperbarui IAM peran Anda untuk mengakses ID rahasia yang benar AWS Secrets Manager .

- Menyimpan kredensi otentikasi Drupal Anda secara AWS Secrets Manager rahasia dan, jika menggunakan API, catat ARN rahasianya.

> **Note**
>
> Kami menyarankan Anda secara teratur menyegarkan atau memutar kredensil dan rahasia Anda. Berikan hanya tingkat akses yang diperlukan untuk keamanan Anda sendiri. Kami tidak menyarankan Anda menggunakan kembali kredensil dan rahasia di seluruh sumber data, dan konektor versi 1.0 dan 2.0 (jika berlaku).

Jika Anda tidak memiliki IAM peran atau rahasia yang ada, Anda dapat menggunakan konsol untuk membuat IAM peran dan Secrets Manager rahasia baru saat Anda menghubungkan sumber data Drupal Anda. Amazon Kendra Jika Anda menggunakan API, Anda harus memberikan ARN IAM peran dan Secrets Manager rahasia yang ada, dan ID indeks.

Instruksi koneksi

Untuk terhubung Amazon Kendra ke sumber data Drupal Anda, Anda harus memberikan rincian kredenal Drupal Anda sehingga Amazon Kendra dapat mengakses data Anda. Jika Anda belum mengkonfigurasi Drupal untuk Amazon Kendra lihatPrasyarat.

Console

Untuk terhubung Amazon Kendra ke Drupal

1. Masuk ke AWS Management Console dan buka Amazon Kendra konsol.
2. Dari panel navigasi kiri, pilih Indeks dan kemudian pilih indeks yang ingin Anda gunakan dari daftar indeks.

> **Note**
>
> Anda dapat memilih untuk mengonfigurasi atau mengedit pengaturan kontrol akses Pengguna Anda di bawah Pengaturan indeks.

3. Pada halaman Memulai, pilih Tambahkan sumber data.
4. Pada halaman Tambah sumber data, pilih konektor Drupal, dan kemudian pilih Tambah konektor.
5. Pada halaman Tentukan detail sumber data, masukkan informasi berikut:
   a. Di Nama dan deskripsi, untuk Nama sumber data —Masukkan nama untuk sumber data Anda. Anda dapat memasukkan tanda hubung tetapi bukan spasi.
   b. (Opsional) Deskripsi —Masukkan deskripsi opsional untuk sumber data Anda.
   c. Dalam Bahasa default —Pilih bahasa untuk memfilter dokumen Anda untuk indeks. Kecuali Anda menentukan sebaliknya, bahasa default ke bahasa Inggris. Bahasa yang ditentukan dalam metadata dokumen mengesampingkan bahasa yang dipilih.
   d. Di Tag, untuk Tambahkan tag baru —Sertakan tag opsional untuk mencari dan memfilter sumber daya Anda atau melacak AWS biaya Anda.
   e. Pilih Berikutnya.
6. Pada halaman Tentukan akses dan keamanan, masukkan informasi berikut:
   a. Di Sumber, untuk URL Host —URL host situs Drupal Anda. <drupalsitename>Misalnya, *https:///*<hostname>.
   b. Untuk lokasi sertifikat SSL —Masukkan jalur ke sertifikat SSL yang disimpan di bucket Anda. Amazon S3
   c. Otorisasi — Aktifkan atau nonaktifkan informasi daftar kontrol akses (ACL) untuk dokumen Anda, jika Anda memiliki ACL dan ingin menggunakannya untuk kontrol akses. ACL menentukan dokumen mana yang dapat diakses pengguna dan grup. Informasi ACL digunakan untuk memfilter hasil pencarian berdasarkan pengguna atau akses grup mereka ke dokumen. Untuk informasi selengkapnya, lihat Pemfilteran konteks pengguna.
   d. Untuk Otentikasi —Pilih antara otentikasi Dasar dan otentikasi OAuth 2.0 berdasarkan kasus penggunaan Anda.

e. AWS Secrets Manager rahasia —Pilih rahasia yang ada atau buat Secrets Manager rahasia baru untuk menyimpan kredensi otentikasi Drupal Anda. Jika Anda memilih untuk membuat rahasia baru, jendela AWS Secrets Manager rahasia terbuka.

   i. Masukkan informasi berikut di jendela Buat AWS Secrets Manager rahasia:

      A. Jika Anda memilih otentikasi Dasar, masukkan Nama Rahasia, Nama Pengguna, (nama pengguna situs Drupal), dan Kata Sandi (kata sandi situs Drupal) yang Anda salin dan pilih Simpan dan tambahkan rahasia.

      B. Jika Anda memilih otentikasi OAuth 2.0, masukkan Nama Rahasia, Nama pengguna (nama pengguna situs Drupal), Kata Sandi (kata sandi situs Drupal), ID Klien, dan rahasia Klien yang dihasilkan di akun Drupal Anda dan pilih Simpan dan tambahkan rahasia.

   ii. Pilih Simpan.

f. Virtual Private Cloud (VPC) —Anda dapat memilih untuk menggunakan VPC. Jika demikian, Anda harus menambahkan Subnet dan grup keamanan VPC.

g. Perayap identitas —Tentukan apakah akan mengaktifkan crawler Amazon Kendra identitas. Perayap identitas menggunakan informasi daftar kontrol akses (ACL) untuk dokumen Anda untuk memfilter hasil penelusuran berdasarkan akses pengguna atau grup mereka ke dokumen. Jika Anda memiliki ACL untuk dokumen Anda dan memilih untuk menggunakan ACL Anda, Anda juga dapat memilih untuk mengaktifkan crawler Amazon Kendra identitas untuk mengonfigurasi pemfilteran konteks pengguna dari hasil pencarian. Jika tidak, jika crawler identitas dimatikan, semua dokumen dapat dicari secara publik. Jika Anda ingin menggunakan kontrol akses untuk dokumen dan crawler identitas dimatikan, Anda dapat menggunakan PutPrincipalMappingAPI untuk mengunggah informasi akses pengguna dan grup untuk pemfilteran konteks pengguna.

h. IAM peran —Pilih peran yang ada atau buat IAM IAM peran baru untuk mengakses kredensi repositori dan mengindeks konten.

> **Note**
>
> IAM peran yang digunakan untuk indeks tidak dapat digunakan untuk sumber data. Jika Anda tidak yakin apakah peran yang ada digunakan untuk indeks atau FAQ, pilih Buat peran baru untuk menghindari kesalahan.

i. Pilih Berikutnya.

7. Pada halaman Konfigurasi pengaturan sinkronisasi, masukkan informasi berikut:

   a. Untuk cakupan Sinkronisasi, pilih dari opsi berikut:

   > **Note**
   >
   > Saat Anda memilih untuk merayapi Artikel, halaman Dasar, dan blok Dasar, bidang defaultnya akan disinkronkan secara otomatis. Anda juga dapat memilih untuk menyinkronkan komentar, lampiran, bidang khusus, dan entitas kustom lainnya.

   - Untuk entitas Pilih:
     - Artikel —Pilih apakah akan merayapi Artikel, komentar mereka Komentar, dan Lampirannya.
     - Halaman dasar —Pilih apakah akan merayapi halaman Dasar, Komentar, dan Lampirannya.
     - Blok dasar —Pilih apakah akan merayapi blok Dasar, Komentar, dan Lampirannya.
     - Anda juga dapat memilih untuk menambahkan jenis konten Kustom dan Blok Kustom.

   b. Untuk konfigurasi Tambahan - opsional:

   - Untuk pola Regex —Tambahkan pola ekspresi reguler untuk menyertakan atau mengecualikan judul entitas dan nama file tertentu. Anda dapat menambahkan hingga 100 pola.

   c. Mode sinkronisasi —Pilih cara Anda ingin memperbarui indeks saat konten sumber data Anda berubah. Saat Anda menyinkronkan sumber data Amazon Kendra untuk pertama kalinya, semua konten dirayapi dan diindeks secara default. Anda harus menjalankan sinkronisasi penuh data Anda jika sinkronisasi awal Anda gagal, bahkan jika Anda tidak memilih sinkronisasi penuh sebagai opsi mode sinkronisasi Anda.

   - Sinkronisasi penuh: Indeks baru semua konten, ganti konten yang ada setiap kali sumber data Anda disinkronkan dengan indeks Anda.
   - Sinkronisasi baru, dimodifikasi, dihapus: Indeks hanya konten baru, dimodifikasi, dan dihapus setiap kali sumber data Anda disinkronkan dengan indeks Anda. Amazon

Kendra dapat menggunakan mekanisme sumber data Anda untuk melacak perubahan konten dan mengindeks konten yang berubah sejak sinkronisasi terakhir.

d. Dalam jadwal berjalan Sync, Frekuensi —Seberapa sering Amazon Kendra akan disinkronkan dengan sumber data Anda.

e. Pilih Berikutnya.

8. Pada halaman Setel pemetaan bidang, masukkan informasi berikut:

a. Untuk Isi, Komentar, dan Lampiran —Pilih dari bidang sumber data default Amazon Kendra yang dihasilkan yang ingin Anda petakan ke indeks Anda.

b. Tambahkan bidang —Untuk menambahkan bidang sumber data kustom untuk membuat nama bidang indeks untuk dipetakan dan tipe data bidang.

c. Pilih Berikutnya.

9. Pada halaman Tinjau dan buat, periksa apakah informasi yang Anda masukkan sudah benar dan kemudian pilih Tambahkan sumber data. Anda juga dapat memilih untuk mengedit informasi Anda dari halaman ini. Sumber data Anda akan muncul di halaman Sumber data setelah sumber data berhasil ditambahkan.

API

Untuk terhubung Amazon Kendra ke Drupal

Anda harus menentukan JSON dari skema sumber data menggunakan API. TemplateConfiguration Anda harus memberikan informasi berikut ini:

- Sumber data —Tentukan tipe sumber data seperti `DRUPAL` saat Anda menggunakan skema TemplateConfigurationJSON. Tentukan juga sumber data seperti `TEMPLATE` saat Anda memanggil CreateDataSourceAPI.
- Mode sinkronisasi —Tentukan cara Amazon Kendra memperbarui indeks Anda saat konten sumber data Anda berubah. Saat Anda menyinkronkan sumber data Amazon Kendra untuk pertama kalinya, semua konten dirayapi dan diindeks secara default. Anda harus menjalankan sinkronisasi penuh data Anda jika sinkronisasi awal Anda gagal, bahkan jika Anda tidak memilih sinkronisasi penuh sebagai opsi mode sinkronisasi Anda. Anda dapat memilih antara:
  - `FORCED_FULL_CRAWL`untuk mengindeks semua konten baru, mengganti konten yang ada setiap kali sumber data Anda disinkronkan dengan indeks Anda.
  - `FULL_CRAWL`untuk mengindeks hanya konten baru, dimodifikasi, dan dihapus setiap kali sumber data Anda disinkronkan dengan indeks Anda. Amazon Kendra dapat menggunakan

mekanisme sumber data Anda untuk melacak perubahan konten dan mengindeks konten yang berubah sejak sinkronisasi terakhir.

- `CHANGE_LOG`untuk mengindeks hanya konten baru dan yang dimodifikasi setiap kali sumber data Anda disinkronkan dengan indeks Anda. Amazon Kendra dapat menggunakan mekanisme sumber data Anda untuk melacak perubahan konten dan mengindeks konten yang berubah sejak sinkronisasi terakhir.

- Rahasia Nama Sumber Daya Amazon (ARN) —Berikan Nama Sumber Daya Amazon (ARN) Secrets Manager rahasia yang berisi kredensi otentikasi yang Anda buat di akun Drupal Anda.

  Jika Anda menggunakan otentikasi dasar, rahasia disimpan dalam struktur JSON dengan kunci berikut:

  ```
  {
      "username": "user name",
      "password": "password"
  }
  ```

  Jika Anda menggunakan otentikasi OAuth 2.0, rahasia disimpan dalam struktur JSON dengan kunci berikut:

  ```
  {
      "username": "user name",
      "password": "password",
      "clientId": "client id",
      "clientSecret": "client secret"
  }
  ```

  Note

  Note

  Kami menyarankan Anda secara teratur menyegarkan atau memutar kredensil dan rahasia Anda. Berikan hanya tingkat akses yang diperlukan untuk keamanan Anda sendiri. Kami tidak menyarankan Anda menggunakan kembali kredensil dan rahasia di seluruh sumber data, dan konektor versi 1.0 dan 2.0 (jika berlaku).

- IAM peran —Tentukan `RoleArn` kapan Anda menelepon `CreateDataSource` untuk memberikan IAM peran dengan izin untuk mengakses Secrets Manager rahasia Anda dan memanggil API publik yang diperlukan untuk konektor Drupal dan. Amazon Kendra Untuk informasi selengkapnya, lihat IAM peran untuk sumber data Drupal.

Anda juga dapat menambahkan fitur opsional berikut:

- Virtual Private Cloud (VPC) **`VpcConfiguration`** —Tentukan kapan Anda menelepon. `CreateDataSource` Untuk informasi selengkapnya, lihat Mengkonfigurasi Amazon Kendra untuk menggunakan Amazon VPC.
- Filter inklusi dan pengecualian —Anda dapat menentukan apakah akan menyertakan konten, komentar, dan lampiran. Anda juga dapat menentukan pola ekspresi reguler untuk menyertakan atau mengecualikan konten, komentar, dan lampiran.

  > **Note**
  >
  > Sebagian besar sumber data menggunakan pola ekspresi reguler, yang merupakan pola inklusi atau pengecualian yang disebut sebagai filter. Jika Anda menentukan filter inklusi, hanya konten yang cocok dengan filter inklusi yang diindeks. Dokumen apa pun yang tidak cocok dengan filter inklusi tidak diindeks. Jika Anda menentukan filter inklusi dan pengecualian, dokumen yang cocok dengan filter pengecualian tidak akan diindeks, meskipun sesuai dengan filter inklusi.

- Perayap identitas —Tentukan apakah akan mengaktifkan crawler Amazon Kendra identitas. Perayap identitas menggunakan informasi daftar kontrol akses (ACL) untuk dokumen Anda untuk memfilter hasil penelusuran berdasarkan akses pengguna atau grup mereka ke dokumen. Jika Anda memiliki ACL untuk dokumen Anda dan memilih untuk menggunakan ACL Anda, Anda juga dapat memilih untuk mengaktifkan crawler Amazon Kendra identitas untuk mengonfigurasi pemfilteran konteks pengguna dari hasil pencarian. Jika tidak, jika crawler identitas dimatikan, semua dokumen dapat dicari secara publik. Jika Anda ingin menggunakan kontrol akses untuk dokumen dan crawler identitas dimatikan, Anda dapat menggunakan PutPrincipalMappingAPI untuk mengunggah informasi akses pengguna dan grup untuk pemfilteran konteks pengguna.
- Pemetaan bidang —Pilih untuk memetakan bidang sumber data Drupal Anda ke bidang indeks Anda. Amazon Kendra Untuk informasi lebih lanjut, lihat Memetakan bidang sumber data.

> **Note**
>
> Bidang badan dokumen atau badan dokumen yang setara untuk dokumen Anda diperlukan Amazon Kendra untuk mencari dokumen Anda. Anda harus memetakan nama bidang badan dokumen Anda di sumber data Anda ke nama bidang indeks_`document_body`. Semua kolom lain bersifat opsional.

Untuk daftar kunci JSON penting lainnya untuk dikonfigurasi, lihatSkema template Drupal.

Catatan

- API Drupal tidak memiliki batas pembatasan resmi.
- SDK Java tidak tersedia untuk Drupal.
- Data Drupal dapat diambil hanya menggunakan JSON API asli.
- Jenis konten yang tidak terkait dengan Tampilan Drupal tidak dapat dirayapi.
- Anda memerlukan akses administrator untuk merayapi data dari Blok Drupal.
- Tidak ada JSON API yang tersedia untuk membuat tipe konten yang ditentukan pengguna menggunakan kata kerja HTTP.
- Badan dokumen dan komentar untuk Artikel, halaman Dasar, Blok dasar, jenis konten yang ditentukan pengguna, dan jenis blok yang ditentukan pengguna, ditampilkan dalam format HTML. Jika konten HTML tidak terbentuk dengan baik, maka tag terkait HTML akan muncul di badan dokumen dan komentar dan akan terlihat di hasil Amazon Kendra pencarian.
- Jenis konten dan jenis Blok tanpa deskripsi atau isi tidak akan dicerna Amazon Kendra. Hanya Komentar dan Lampiran dari jenis Konten atau Blok tersebut yang akan dicerna ke dalam indeks Anda Amazon Kendra .

GitHub

GitHub adalah layanan hosting berbasis web untuk pengembangan perangkat lunak yang menyediakan penyimpanan kode dan layanan manajemen dengan kontrol versi. Anda dapat menggunakan Amazon Kendra untuk mengindeks file repositori GitHub Enterprise Cloud (SaaS) dan GitHub Enterprise Server (On Prem), mengeluarkan dan menarik permintaan, mengeluarkan

dan menarik komentar permintaan, serta mengeluarkan dan menarik lampiran komentar permintaan. Anda juga dapat memilih untuk menyertakan atau mengecualikan file tertentu.

> **Note**
>
> Amazon Kendra sekarang mendukung GitHub konektor yang ditingkatkan.
> Konsol telah ditingkatkan secara otomatis untuk Anda. Konektor baru apa pun yang Anda buat di konsol akan menggunakan arsitektur yang ditingkatkan. Jika Anda menggunakan API, Anda sekarang harus menggunakan TemplateConfigurationobjek alih-alih `GitHubConfiguration` objek untuk mengonfigurasi konektor Anda.
> Konektor yang dikonfigurasi menggunakan konsol lama dan arsitektur API akan terus berfungsi seperti yang dikonfigurasi. Namun, Anda tidak akan dapat mengedit atau memperbaruinya. Jika Anda ingin mengedit atau memperbarui konfigurasi konektor Anda, Anda harus membuat konektor baru.
> Kami merekomendasikan untuk memigrasikan alur kerja konektor Anda ke versi yang ditingkatkan. Support untuk konektor yang dikonfigurasi menggunakan arsitektur lama dijadwalkan berakhir pada Juni 2024.

Anda dapat terhubung Amazon Kendra ke sumber GitHub data menggunakan Amazon Kendra konsol dan TemplateConfigurationAPI.

Untuk memecahkan masalah konektor sumber Amazon Kendra GitHub data Anda, lihat. Mengatasi masalah sumber data

Topik

- Fitur yang didukung
- Prasyarat
- Instruksi koneksi
- Pelajari selengkapnya

Fitur yang didukung

Amazon Kendra GitHub konektor sumber data mendukung fitur-fitur berikut:

- Pemetaan lapangan
- Pemfilteran konteks pengguna

- Perayapan identitas pengguna
- Filter inklusi/pengecualian
- Sinkronisasi konten penuh dan inkremental
- Cloud privat virtual (VPC)

Prasyarat

Sebelum Anda dapat menggunakan Amazon Kendra untuk mengindeks sumber GitHub data Anda, buat perubahan ini di akun GitHub dan AWS akun Anda.

Di GitHub, pastikan Anda memiliki:

- Membuat GitHub pengguna dengan izin administratif untuk GitHub organisasi.
- Membuat token akses pribadi klasik untuk kredensi otentikasi. Lihat GitHub dokumentasi tentang membuat token akses pribadi.
- Direkomendasikan: Membuat token OAuth untuk kredensi otentikasi. Gunakan token OAuth untuk batas throttle API dan kinerja konektor yang lebih baik. Lihat GitHub dokumentasi tentang otorisasi OAuth.
- Mencatat URL GitHub host untuk jenis GitHub layanan yang Anda gunakan. Misalnya, URL host untuk GitHub cloud dapat berupa *`https://api.github.com`* dan URL host untuk GitHub server dapat berupa *`https://on-prem-host-url/api/v3/`*.
- Mencatat nama organisasi Anda untuk GitHub akun GitHub Enterprise Cloud (SaaS) atau akun Server GitHub Perusahaan (lokal) yang ingin Anda sambungkan. Anda dapat menemukan nama organisasi Anda dengan masuk ke GitHub desktop dan memilih Organisasi Anda di bawah dropdown gambar profil Anda.
- Opsional (hanya server): Menghasilkan sertifikat SSL dan menyalin jalur ke sertifikat yang disimpan dalam bucket. Amazon S3 Anda menggunakan ini untuk terhubung GitHub jika Anda memerlukan koneksi SSL yang aman. Anda cukup membuat sertifikat X509 yang ditandatangani sendiri di komputer mana pun menggunakan OpenSSL. Untuk contoh menggunakan OpenSSL untuk membuat sertifikat X509, lihat Membuat dan menandatangani sertifikat X509.
- Menambahkan izin berikut:

  Untuk GitHub Enterprise Cloud (SaaS)

  - repo:status
  - public_repo

- repo:mengundang
- baca:org
- pengguna:email
- baca:pengguna

Untuk Server GitHub Perusahaan (Di Prem)

- repo:status
- public_repo
- repo:mengundang
- baca:org
- pengguna:email
- baca:pengguna
- site_admin

- Memeriksa setiap dokumen unik di dalam GitHub dan di seluruh sumber data lain yang Anda rencanakan untuk digunakan untuk indeks yang sama. Setiap sumber data yang ingin Anda gunakan untuk indeks tidak boleh berisi dokumen yang sama di seluruh sumber data. ID dokumen bersifat global untuk indeks dan harus unik per indeks.

Di dalam Anda Akun AWS, pastikan Anda memiliki:

- Membuat Amazon Kendra indeks dan, jika menggunakan API, mencatat ID indeks.
- Membuat IAM peran untuk sumber data Anda dan, jika menggunakan API, catat ARN peran tersebut IAM .

> **Note**
>
> Jika Anda mengubah jenis otentikasi dan kredensialnya, Anda harus memperbarui IAM peran Anda untuk mengakses ID rahasia yang benar AWS Secrets Manager .

- Menyimpan kredensi GitHub otentikasi Anda AWS Secrets Manager secara rahasia dan, jika menggunakan API, catat ARN rahasia tersebut.

> **Note**
>
> Kami menyarankan Anda secara teratur menyegarkan atau memutar kredensil dan rahasia Anda. Berikan hanya tingkat akses yang diperlukan untuk keamanan Anda sendiri. Kami tidak menyarankan Anda menggunakan kembali kredensil dan rahasia di seluruh sumber data, dan konektor versi 1.0 dan 2.0 (jika berlaku).

Jika Anda tidak memiliki IAM peran atau rahasia yang ada, Anda dapat menggunakan konsol untuk membuat IAM peran dan Secrets Manager rahasia baru saat Anda menghubungkan sumber GitHub data Anda Amazon Kendra. Jika Anda menggunakan API, Anda harus memberikan ARN IAM peran dan Secrets Manager rahasia yang ada, dan ID indeks.

Instruksi koneksi

Untuk terhubung Amazon Kendra ke sumber GitHub data Anda, Anda harus memberikan rincian yang diperlukan dari sumber GitHub data Anda sehingga Amazon Kendra dapat mengakses data Anda. Jika Anda belum mengkonfigurasi GitHub untuk Amazon Kendra, lihatPrasyarat.

Console

Untuk terhubung Amazon Kendra ke GitHub

1. Masuk ke AWS Management Console dan buka Amazon Kendra konsol.
2. Dari panel navigasi kiri, pilih Indeks dan kemudian pilih indeks yang ingin Anda gunakan dari daftar indeks.

   > **Note**
   >
   > Anda dapat memilih untuk mengonfigurasi atau mengedit pengaturan kontrol akses Pengguna Anda di bawah Pengaturan indeks.

3. Pada halaman Memulai, pilih Tambahkan sumber data.
4. Pada halaman Tambahkan sumber data, pilih GitHub konektor, lalu pilih Tambah konektor.
5. Pada halaman Tentukan detail sumber data, masukkan informasi berikut:

   a. Di Nama dan deskripsi, untuk Nama sumber data —Masukkan nama untuk sumber data Anda. Anda dapat memasukkan tanda hubung tetapi bukan spasi.

b. (Opsional) Deskripsi —Masukkan deskripsi opsional untuk sumber data Anda.

c. Dalam Bahasa default —Pilih bahasa untuk memfilter dokumen Anda untuk indeks. Kecuali Anda menentukan sebaliknya, bahasa default ke bahasa Inggris. Bahasa yang ditentukan dalam metadata dokumen mengesampingkan bahasa yang dipilih.

d. Di Tag, untuk Tambahkan tag baru —Sertakan tag opsional untuk mencari dan memfilter sumber daya Anda atau melacak AWS biaya Anda.

e. Pilih Berikutnya.

6. Pada halaman Tentukan akses dan keamanan, masukkan informasi berikut:

a. GitHubsumber —Pilih antara GitHub Enterprise Cloud dan GitHubEnterprise Server.

b. GitHub URL host —Masukkan nama GitHub host Anda.

c. GitHub nama organisasi —Masukkan nama GitHub organisasi Anda. Anda dapat menemukan informasi organisasi Anda di GitHub akun Anda.

d. Otorisasi — Aktifkan atau nonaktifkan informasi daftar kontrol akses (ACL) untuk dokumen Anda, jika Anda memiliki ACL dan ingin menggunakannya untuk kontrol akses. ACL menentukan dokumen mana yang dapat diakses pengguna dan grup. Informasi ACL digunakan untuk memfilter hasil pencarian berdasarkan pengguna atau akses grup mereka ke dokumen. Untuk informasi selengkapnya, lihat Pemfilteran konteks pengguna.

e. AWS Secrets Manager rahasia —Pilih rahasia yang ada atau buat Secrets Manager rahasia baru untuk menyimpan kredensi GitHub otentikasi Anda. Jika Anda memilih untuk membuat rahasia baru, jendela AWS Secrets Manager rahasia terbuka.

i. Masukkan informasi berikut di jendela Buat AWS Secrets Manager rahasia:

A. Nama rahasia —Nama untuk rahasiamu. Awalan 'AmazonKendra- GitHub -' secara otomatis ditambahkan ke nama rahasia Anda.

B. Untuk GitHubtoken —Masukkan nilai kredensi otentikasi yang Anda buat di akun Anda. GitHub

ii. Pilih Simpan.

f. Virtual Private Cloud (VPC) —Anda dapat memilih untuk menggunakan VPC. Jika demikian, Anda harus menambahkan Subnet dan grup keamanan VPC.

g. Perayap identitas —Tentukan apakah akan mengaktifkan crawler Amazon Kendra identitas. Perayap identitas menggunakan informasi daftar kontrol akses (ACL) untuk dokumen Anda untuk memfilter hasil penelusuran berdasarkan akses pengguna atau grup mereka ke dokumen. Jika Anda memiliki ACL untuk dokumen Anda dan memilih

untuk menggunakan ACL Anda, Anda juga dapat memilih untuk mengaktifkan crawler Amazon Kendra identitas untuk mengonfigurasi pemfilteran konteks pengguna dari hasil pencarian. Jika tidak, jika crawler identitas dimatikan, semua dokumen dapat dicari secara publik. Jika Anda ingin menggunakan kontrol akses untuk dokumen dan crawler identitas dimatikan, Anda dapat menggunakan PutPrincipalMappingAPI untuk mengunggah informasi akses pengguna dan grup untuk pemfilteran konteks pengguna.

h. IAM peran —Pilih peran yang sudah ada atau buat IAM IAM peran baru untuk mengakses kredensi repositori dan mengindeks konten Anda.

> **Note**
>
> IAM peran yang digunakan untuk indeks tidak dapat digunakan untuk sumber data. Jika Anda tidak yakin apakah peran yang ada digunakan untuk indeks atau FAQ, pilih Buat peran baru untuk menghindari kesalahan.

i. Pilih Berikutnya.

7. Pada halaman Konfigurasi pengaturan sinkronisasi, masukkan informasi berikut:

   a. Pilih repositori untuk dirayapi —Pilih antara crawling Semua repositori atau Pilih repositori.

      Jika Anda memilih Pilih repositori, tambahkan nama untuk repositori di Nama repositori dan, secara opsional, nama cabang tertentu di Nama cabang.

   b. Jenis konten —Pilih jenis konten yang ingin Anda sertakan.

   c. Pola Regex —Pola ekspresi reguler untuk menyertakan atau mengecualikan file tertentu. Anda dapat menambahkan hingga 100 pola.

   d. Dalam jadwal berjalan Sinkronisasi, untuk Frekuensi —Seberapa sering Amazon Kendra akan disinkronkan dengan sumber data Anda.

   e. Pilih Berikutnya.

8. Mode sinkronisasi —Pilih cara Anda ingin memperbarui indeks saat konten sumber data Anda berubah. Saat Anda menyinkronkan sumber data Amazon Kendra untuk pertama kalinya, semua konten dirayapi dan diindeks secara default. Anda harus menjalankan sinkronisasi penuh data Anda jika sinkronisasi awal Anda gagal, bahkan jika Anda tidak memilih sinkronisasi penuh sebagai opsi mode sinkronisasi Anda.

   - Sinkronisasi penuh: Indeks baru semua konten, ganti konten yang ada setiap kali sumber data Anda disinkronkan dengan indeks Anda.

- Sinkronisasi baru yang dimodifikasi: Indeks hanya konten baru dan yang dimodifikasi setiap kali sumber data Anda disinkronkan dengan indeks Anda. Amazon Kendra dapat menggunakan mekanisme sumber data Anda untuk melacak perubahan konten dan mengindeks konten yang berubah sejak sinkronisasi terakhir.
- Sinkronisasi baru, dimodifikasi, dihapus: Indeks hanya konten baru, dimodifikasi, dan dihapus setiap kali sumber data Anda disinkronkan dengan indeks Anda. Amazon Kendra dapat menggunakan mekanisme sumber data Anda untuk melacak perubahan konten dan mengindeks konten yang berubah sejak sinkronisasi terakhir.

9. Dalam jadwal berjalan Sinkronisasi, untuk Frekuensi —Seberapa sering Amazon Kendra akan disinkronkan dengan sumber data Anda.
10. Pilih Berikutnya.
11. Pada halaman Setel pemetaan bidang, masukkan informasi berikut:

    a. Untuk Repositori, Komit Respositori, Dokumen Masalah, Komentar Masalah, Lampiran Masalah, Komentar Permintaan Tarik, Dokumen Permintaan Tarik, Lampiran Permintaan Tarik —Pilih dari bidang sumber data default Amazon Kendra yang dihasilkan yang ingin Anda petakan ke indeks Anda.

    b. Tambahkan bidang —Untuk menambahkan bidang sumber data kustom untuk membuat nama bidang indeks untuk dipetakan dan tipe data bidang.

    c. Pilih Berikutnya.

12. Pada halaman Tinjau dan buat, periksa apakah informasi yang Anda masukkan sudah benar dan kemudian pilih Tambahkan sumber data. Anda juga dapat memilih untuk mengedit informasi Anda dari halaman ini. Sumber data Anda akan muncul di halaman Sumber data setelah sumber data berhasil ditambahkan.

API

Untuk terhubung Amazon Kendra ke GitHub

Anda harus menentukan JSON dari skema sumber data menggunakan API. TemplateConfiguration Anda harus memberikan informasi berikut ini:

- Sumber data —Tentukan tipe sumber data seperti `GITHUB` saat Anda menggunakan skema TemplateConfigurationJSON. Tentukan juga sumber data seperti `TEMPLATE` saat Anda memanggil CreateDataSourceAPI.
- GitHubtype —Tentukan tipe sebagai salah satu `SAAS` atau`ON_PREMISE`.

- URL Host —Tentukan URL GitHub host atau URL titik akhir API. Misalnya, jika Anda menggunakan GitHub SaaS/Enterprise Cloud, URL host bisa jadi`https://api.github.com`, dan untuk Server GitHub On-premis/Enterprise URL host bisa. `https://on-prem-host-url/api/v3/`
- Nama organisasi —Tentukan nama organisasi GitHub akun. Anda dapat menemukan nama organisasi Anda dengan masuk ke GitHub desktop dan memilih Organisasi Anda di bawah dropdown gambar profil Anda.
- Mode sinkronisasi —Tentukan cara Amazon Kendra memperbarui indeks Anda saat konten sumber data Anda berubah. Saat Anda menyinkronkan sumber data Amazon Kendra untuk pertama kalinya, semua konten dirayapi dan diindeks secara default. Anda harus menjalankan sinkronisasi penuh data Anda jika sinkronisasi awal Anda gagal, bahkan jika Anda tidak memilih sinkronisasi penuh sebagai opsi mode sinkronisasi Anda. Anda dapat memilih antara:
  - `FORCED_FULL_CRAWL`untuk mengindeks semua konten baru, mengganti konten yang ada setiap kali sumber data Anda disinkronkan dengan indeks Anda.
  - `FULL_CRAWL`untuk mengindeks hanya konten baru, dimodifikasi, dan dihapus setiap kali sumber data Anda disinkronkan dengan indeks Anda. Amazon Kendra dapat menggunakan mekanisme sumber data Anda untuk melacak perubahan konten dan mengindeks konten yang berubah sejak sinkronisasi terakhir.
  - `CHANGE_LOG`untuk mengindeks hanya konten baru dan yang dimodifikasi setiap kali sumber data Anda disinkronkan dengan indeks Anda. Amazon Kendra dapat menggunakan mekanisme sumber data Anda untuk melacak perubahan konten dan mengindeks konten yang berubah sejak sinkronisasi terakhir.
- Perayap identitas —Tentukan apakah akan mengaktifkan crawler Amazon Kendra identitas. Perayap identitas menggunakan informasi daftar kontrol akses (ACL) untuk dokumen Anda untuk memfilter hasil penelusuran berdasarkan akses pengguna atau grup mereka ke dokumen. Jika Anda memiliki ACL untuk dokumen Anda dan memilih untuk menggunakan ACL Anda, Anda juga dapat memilih untuk mengaktifkan crawler Amazon Kendra identitas untuk mengonfigurasi pemfilteran konteks pengguna dari hasil pencarian. Jika tidak, jika crawler identitas dimatikan, semua dokumen dapat dicari secara publik. Jika Anda ingin menggunakan kontrol akses untuk dokumen dan crawler identitas dimatikan, Anda dapat menggunakan PutPrincipalMappingAPI untuk mengunggah informasi akses pengguna dan grup untuk pemfilteran konteks pengguna.
- Rahasia Nama Sumber Daya Amazon (ARN) —Berikan Nama Sumber Daya Amazon (ARN) Secrets Manager rahasia yang berisi kredensi otentikasi untuk akun Anda. GitHub Rahasianya disimpan dalam struktur JSON dengan kunci berikut:

```
{
    "personalToken": "token"
}
```

> **Note**
>
> Kami menyarankan Anda secara teratur menyegarkan atau memutar kredensil dan rahasia Anda. Berikan hanya tingkat akses yang diperlukan untuk keamanan Anda sendiri. Kami tidak menyarankan Anda menggunakan kembali kredensil dan rahasia di seluruh sumber data, dan konektor versi 1.0 dan 2.0 (jika berlaku).

- IAM peran —Tentukan `RoleArn` kapan Anda menelepon `CreateDataSource` untuk memberikan IAM peran dengan izin untuk mengakses Secrets Manager rahasia Anda dan memanggil API publik yang diperlukan untuk GitHub konektor dan. Amazon Kendra Untuk informasi selengkapnya, lihat IAM peran untuk sumber GitHub data.

Anda juga dapat menambahkan fitur opsional berikut:

- Virtual Private Cloud (VPC) **`VpcConfiguration`** —Tentukan kapan Anda menelepon. `CreateDataSource` Untuk informasi selengkapnya, lihat Mengkonfigurasi Amazon Kendra untuk menggunakan Amazon VPC.

> **Note**
>
> Jika Anda menggunakan GitHub server, Anda harus menggunakan file Amazon VPC untuk terhubung ke GitHub server Anda.

- Filter repositori —Filter repositori dengan nama dan nama cabangnya.
- Jenis dokumen/konten —Tentukan apakah akan merayapi dokumen repositori, masalah, mengeluarkan komentar, mengeluarkan lampiran komentar, permintaan tarik, komentar permintaan tarik, lampiran komentar permintaan tarik.
- Filter inklusi dan pengecualian —Tentukan apakah akan menyertakan atau mengecualikan file dan folder tertentu.

> **Note**
>
> Sebagian besar sumber data menggunakan pola ekspresi reguler, yang merupakan pola inklusi atau pengecualian yang disebut sebagai filter. Jika Anda menentukan filter inklusi, hanya konten yang cocok dengan filter inklusi yang diindeks. Dokumen apa pun yang tidak cocok dengan filter inklusi tidak diindeks. Jika Anda menentukan filter inklusi dan pengecualian, dokumen yang cocok dengan filter pengecualian tidak akan diindeks, meskipun sesuai dengan filter inklusi.

- Daftar kontrol akses (ACL) —Tentukan apakah akan merayapi informasi ACL untuk dokumen Anda, jika Anda memiliki ACL dan ingin menggunakannya untuk kontrol akses. ACL menentukan dokumen mana yang dapat diakses pengguna dan grup. Informasi ACL digunakan untuk memfilter hasil pencarian berdasarkan pengguna atau akses grup mereka ke dokumen. Untuk informasi selengkapnya, lihat Pemfilteran konteks pengguna.
- Pemetaan bidang —Pilih untuk memetakan bidang sumber GitHub data Anda ke bidang indeks Anda Amazon Kendra . Anda dapat menyertakan bidang dokumen, komit, masalah, lampiran masalah, mengeluarkan komentar, permintaan tarik, lampiran permintaan tarik, komentar permintaan tarik. Untuk informasi lebih lanjut, lihat Memetakan bidang sumber data.

> **Note**
>
> Bidang badan dokumen atau badan dokumen yang setara untuk dokumen Anda diperlukan agar Amazon Kendra dapat mencari dokumen Anda. Anda harus memetakan nama bidang badan dokumen Anda di sumber data Anda ke nama bidang indeks _document_body. Semua kolom lain bersifat opsional.

Untuk daftar kunci JSON penting lainnya untuk dikonfigurasi, lihat skema GitHub template.

Pelajari selengkapnya

Untuk mempelajari lebih lanjut tentang mengintegrasikan Amazon Kendra dengan sumber GitHub data Anda, lihat:

- Bayangkan kembali pencarian di GitHub repositori dengan kekuatan konektor Amazon Kendra GitHub

Gmail

Gmail adalah klien email yang dikembangkan oleh Google di mana Anda dapat mengirim pesan email dengan lampiran file. Pesan Gmail dapat diurutkan dan disimpan di dalam kotak masuk email Anda menggunakan folder dan label. Anda dapat menggunakan Amazon Kendra untuk mengindeks pesan email dan lampiran pesan Anda. Anda juga dapat mengonfigurasi Amazon Kendra untuk menyertakan atau mengecualikan pesan email tertentu, lampiran pesan, dan label untuk pengindeksan.

Anda dapat terhubung Amazon Kendra ke sumber data Gmail Anda menggunakan Amazon Kendra konsol dan TemplateConfigurationAPI.

Untuk mengatasi masalah konektor sumber data Amazon Kendra Gmail, lihat. Mengatasi masalah sumber data

Topik

Fitur yang didukung

- Pemetaan lapangan
- Pemfilteran konteks pengguna
- Filter inklusi/pengecualian
- Sinkronisasi konten penuh dan inkremental
- Cloud privat virtual (VPC)

Prasyarat

Sebelum Anda dapat menggunakan Amazon Kendra untuk mengindeks sumber data Gmail Anda, buat perubahan ini di Gmail dan AWS akun Anda.

Di Gmail, pastikan Anda memiliki:

- Membuat akun admin Google Cloud Platform dan telah membuat proyek Google Cloud.
- Diaktifkan API Gmail dan Admin SDK API di akun admin Anda.
- Membuat akun layanan dan mengunduh kunci pribadi JSON untuk Gmail Anda. Untuk informasi tentang cara membuat dan mengakses kunci pribadi Anda, lihat dokumentasi Google Cloud tentang cara membuat kunci akun layanan dan kredensyal akun Layanan.
- Menyalin email akun admin Anda, email akun layanan Anda, dan kunci pribadi Anda untuk digunakan untuk otentikasi.
- Menambahkan cakupan Oauth berikut (menggunakan peran admin) untuk pengguna Anda dan direktori bersama yang ingin Anda indeks:
  - https://www.googleapis.com/auth/admin.directory.user.readonly
  - https://www.googleapis.com/auth/gmail.readonly
- Memeriksa setiap dokumen unik di Gmail dan di seluruh sumber data lain yang Anda rencanakan untuk digunakan untuk indeks yang sama. Setiap sumber data yang ingin Anda gunakan untuk indeks tidak boleh berisi dokumen yang sama di seluruh sumber data. ID dokumen bersifat global untuk indeks dan harus unik per indeks.

Di dalam Anda Akun AWS, pastikan Anda memiliki:

- Membuat Amazon Kendra indeks dan, jika menggunakan API, mencatat ID indeks.
- Membuat IAM peran untuk sumber data Anda dan, jika menggunakan API, catat ARN peran tersebut IAM .

> **Note**
>
> Jika Anda mengubah jenis otentikasi dan kredensyal, Anda harus memperbarui IAM peran Anda untuk mengakses ID rahasia yang benar AWS Secrets Manager .

- Menyimpan kredensyal otentikasi Gmail Anda AWS Secrets Manager secara rahasia dan, jika menggunakan API, catat ARN rahasianya.

> **Note**
>
> Kami menyarankan Anda secara teratur menyegarkan atau memutar kredensi dan rahasia Anda. Berikan hanya tingkat akses yang diperlukan untuk keamanan Anda sendiri. Kami

tidak menyarankan Anda menggunakan kembali kredensyal dan rahasia di seluruh sumber data, dan konektor versi 1.0 dan 2.0 (jika berlaku).

Jika Anda tidak memiliki IAM peran atau rahasia yang ada, Anda dapat menggunakan konsol untuk membuat IAM peran dan Secrets Manager rahasia baru saat Anda menghubungkan sumber data Gmail Anda Amazon Kendra. Jika Anda menggunakan API, Anda harus memberikan ARN IAM peran dan Secrets Manager rahasia yang ada, dan ID indeks.

Instruksi koneksi

Untuk terhubung Amazon Kendra ke sumber data Gmail Anda, Anda harus memberikan detail kredensyal Gmail Anda sehingga Amazon Kendra dapat mengakses data Anda. Jika Anda belum mengkonfigurasi Gmail untuk Amazon Kendra, lihatPrasyarat.

Console

Untuk terhubung Amazon Kendra ke Gmail

1. Masuk ke AWS Management Console dan buka Amazon Kendra konsol.
2. Dari panel navigasi kiri, pilih Indeks dan kemudian pilih indeks yang ingin Anda gunakan dari daftar indeks.

   > **Note**
   >
   > Anda dapat memilih untuk mengonfigurasi atau mengedit pengaturan kontrol akses Pengguna Anda di bawah Pengaturan indeks.

3. Pada halaman Memulai, pilih Tambahkan sumber data.
4. Pada halaman Tambah sumber data, pilih konektor Gmail, lalu pilih Tambah konektor.
5. Pada halaman Tentukan detail sumber data, masukkan informasi berikut:

   a. Di Nama dan deskripsi, untuk Nama sumber data —Masukkan nama untuk sumber data Anda. Anda dapat memasukkan tanda hubung tetapi bukan spasi.

   b. (Opsional) Deskripsi —Masukkan deskripsi opsional untuk sumber data Anda.

   c. Dalam Bahasa default —Pilih bahasa untuk memfilter dokumen Anda untuk indeks. Kecuali Anda menentukan sebaliknya, bahasa default ke bahasa Inggris. Bahasa yang ditentukan dalam metadata dokumen mengesampingkan bahasa yang dipilih.

d. Di Tag, untuk Tambahkan tag baru —Sertakan tag opsional untuk mencari dan memfilter sumber daya Anda atau melacak AWS biaya Anda.

e. Pilih Berikutnya.

6. Pada halaman Tentukan akses dan keamanan, masukkan informasi berikut:

a. Dalam Otentikasi untuk AWS Secrets Manager rahasia —Pilih rahasia yang ada atau buat Secrets Manager rahasia baru untuk menyimpan kredensi otentikasi Gmail Anda. Jika Anda memilih untuk membuat rahasia baru, jendela AWS Secrets Manager rahasia terbuka.

- Masukkan informasi berikut di jendela Buat AWS Secrets Manager rahasia:

A. Nama Rahasia — Nama untuk rahasiamu.

B. Email klien —Email klien yang Anda salin dari akun layanan Google Anda.

C. Email akun admin —Email akun admin yang ingin Anda gunakan.

D. Kunci pribadi —Kunci pribadi yang Anda salin dari akun layanan Google Anda.

E. Pilih Simpan.

b. Virtual Private Cloud (VPC) —Anda dapat memilih untuk menggunakan VPC. Jika demikian, Anda harus menambahkan Subnet dan grup keamanan VPC.

c. IAM peran —Pilih peran yang sudah ada atau buat IAM IAM peran baru untuk mengakses kredensi repositori dan mengindeks konten Anda.

> **Note**
>
> IAM peran yang digunakan untuk indeks tidak dapat digunakan untuk sumber data. Jika Anda tidak yakin apakah peran yang ada digunakan untuk indeks atau FAQ, pilih Buat peran baru untuk menghindari kesalahan.

d. Pilih Berikutnya.

7. Pada halaman Konfigurasi pengaturan sinkronisasi, masukkan informasi berikut:

a. Dalam lingkup Sinkronisasi, untuk tipe Entitas —Pilih lampiran Pesan untuk menyinkronkan lampiran pesan. Pesan akan disinkronkan secara default.

b. (Opsional) Untuk konfigurasi tambahan, masukkan informasi berikut:

i. Rentang tanggal —Masukkan rentang tanggal untuk menentukan tanggal mulai dan akhir email yang akan dirayapi.

ii. Domain email —Sertakan atau kecualikan email berdasarkan domain.

iii. Kata kunci dalam subjek —Sertakan atau kecualikan email berdasarkan kata kunci dalam subjek mereka.

> **Note**
>
> Anda juga dapat memilih untuk menyertakan dokumen apa pun yang cocok dengan semua kata kunci subjek yang telah Anda masukkan.

iv. Label —Tambahkan pola ekspresi reguler untuk menyertakan atau mengecualikan label tertentu. Anda dapat menambahkan hingga 100 pola.

v. Lampiran —Tambahkan pola ekspresi reguler untuk menyertakan atau mengecualikan lampiran tertentu. Anda dapat menambahkan hingga 100 pola.

c. Mode sinkronisasi —Pilih cara memperbarui indeks saat konten sumber data berubah. Saat Anda menyinkronkan sumber data Amazon Kendra untuk pertama kalinya, semua konten dirayapi dan diindeks secara default. Anda harus menjalankan sinkronisasi penuh data Anda jika sinkronisasi awal Anda gagal, bahkan jika Anda tidak memilih sinkronisasi penuh sebagai opsi mode sinkronisasi Anda.

- Sinkronisasi penuh: Indeks baru semua konten, ganti konten yang ada setiap kali sumber data Anda disinkronkan dengan indeks Anda.
- Sinkronisasi baru, dimodifikasi, dihapus: Indeks hanya konten baru, dimodifikasi, dan dihapus setiap kali sumber data Anda disinkronkan dengan indeks Anda. Amazon Kendra dapat menggunakan mekanisme sumber data Anda untuk melacak perubahan konten dan mengindeks konten yang berubah sejak sinkronisasi terakhir.

> **Important**
>
> Karena tidak ada API untuk memperbarui pesan Gmail yang dihapus secara permanen, sinkronisasi konten baru, dimodifikasi, atau dihapus:
>
> - Tidak akan menghapus pesan yang dihapus secara permanen dari Gmail dari Amazon Kendra indeks Anda

- Tidak akan menyinkronkan perubahan pada label email Gmail

Untuk menyinkronkan perubahan label sumber data Gmail dan pesan email yang dihapus secara permanen ke Amazon Kendra indeks, Anda harus menjalankan crawl penuh secara berkala.

d. Dalam jadwal berjalan Sinkronisasi, untuk Frekuensi —Seberapa sering Amazon Kendra akan disinkronkan dengan sumber data Anda.

e. Pilih Berikutnya.

8. Pada halaman Setel pemetaan bidang, masukkan informasi berikut:

a. Untuk lampiran Pesan dan Pesan —Pilih dari bidang sumber data default Amazon Kendra yang dihasilkan yang ingin Anda petakan ke indeks Anda.

> **Note**
>
> Amazon Kendra Konektor sumber data Gmail tidak mendukung pembuatan bidang indeks khusus karena keterbatasan API.

b. Pilih Berikutnya.

9. Pada halaman Tinjau dan buat, periksa apakah informasi yang Anda masukkan sudah benar dan kemudian pilih Tambahkan sumber data. Anda juga dapat memilih untuk mengedit informasi Anda dari halaman ini. Sumber data Anda akan muncul di halaman Sumber data setelah sumber data berhasil ditambahkan.

API

Untuk terhubung Amazon Kendra ke Gmail

Anda harus menentukan JSON dari skema sumber data menggunakan API. TemplateConfiguration Anda harus memberikan informasi berikut ini:

- Sumber data —Tentukan tipe sumber data seperti `GMAIL` saat Anda menggunakan skema TemplateConfigurationJSON. Tentukan juga sumber data seperti `TEMPLATE` saat Anda memanggil CreateDataSourceAPI.
- Mode sinkronisasi —Tentukan cara Amazon Kendra memperbarui indeks Anda saat konten sumber data Anda berubah. Saat Anda menyinkronkan sumber data Amazon Kendra untuk

pertama kalinya, semua konten dirayapi dan diindeks secara default. Anda harus menjalankan sinkronisasi penuh data Anda jika sinkronisasi awal Anda gagal, bahkan jika Anda tidak memilih sinkronisasi penuh sebagai opsi mode sinkronisasi Anda. Anda dapat memilih antara:

- `FORCED_FULL_CRAWL`untuk mengindeks semua konten baru, mengganti konten yang ada setiap kali sumber data Anda disinkronkan dengan indeks Anda.
- `FULL_CRAWL`untuk mengindeks hanya konten baru, dimodifikasi, dan dihapus setiap kali sumber data Anda disinkronkan dengan indeks Anda. Amazon Kendra dapat menggunakan mekanisme sumber data Anda untuk melacak perubahan konten dan mengindeks konten yang berubah sejak sinkronisasi terakhir.

> **Important**
>
> Karena tidak ada API untuk memperbarui pesan Gmail yang dihapus secara permanen, sinkronisasi konten baru, dimodifikasi, atau dihapus:
>
> - Tidak akan menghapus pesan yang dihapus secara permanen dari Gmail dari Amazon Kendra indeks Anda
> - Tidak akan menyinkronkan perubahan pada label email Gmail
>
> Untuk menyinkronkan perubahan label sumber data Gmail dan pesan email yang dihapus secara permanen ke Amazon Kendra indeks, Anda harus menjalankan crawl penuh secara berkala.

- Rahasia Nama Sumber Daya Amazon (ARN) —Berikan Nama Sumber Daya Amazon (ARN) Secrets Manager rahasia yang berisi kredensyal otentikasi untuk akun Gmail Anda. Rahasianya disimpan dalam struktur JSON dengan kunci berikut:

```
{
    "adminAccountEmailId": "service account email",
    "clientEmailId": "user account email",
    "privateKey": "private key"
}
```

> **Note**
>
> Kami menyarankan Anda secara teratur menyegarkan atau memutar kredensi dan rahasia Anda. Berikan hanya tingkat akses yang diperlukan untuk keamanan Anda

sendiri. Kami tidak menyarankan Anda menggunakan kembali kredensyal dan rahasia di seluruh sumber data, dan konektor versi 1.0 dan 2.0 (jika berlaku).

- IAM peran —Tentukan `RoleArn` kapan Anda menelepon `CreateDataSource` untuk memberikan IAM peran dengan izin untuk mengakses Secrets Manager rahasia Anda dan memanggil API publik yang diperlukan untuk konektor Gmail dan. Amazon Kendra Untuk informasi selengkapnya, lihat IAM peran untuk sumber data Gmail.

Anda juga dapat menambahkan fitur opsional berikut:

- Virtual Private Cloud (VPC) **`VpcConfiguration`** —Tentukan kapan Anda menelepon. `CreateDataSource` Untuk informasi selengkapnya, lihat Mengkonfigurasi Amazon Kendra untuk menggunakan Amazon VPC.
- Filter inklusi dan pengecualian —Anda dapat menentukan apakah akan menyertakan atau mengecualikan pesan dan lampiran.

> **Note**
>
> Sebagian besar sumber data menggunakan pola ekspresi reguler, yang merupakan pola inklusi atau pengecualian yang disebut sebagai filter. Jika Anda menentukan filter inklusi, hanya konten yang cocok dengan filter inklusi yang diindeks. Dokumen apa pun yang tidak cocok dengan filter inklusi tidak diindeks. Jika Anda menentukan filter inklusi dan pengecualian, dokumen yang cocok dengan filter pengecualian tidak akan diindeks, meskipun sesuai dengan filter inklusi.

- Pemfilteran konteks pengguna dan kontrol akses —Amazon Kendra meng-crawl daftar kontrol akses (ACL) untuk dokumen Anda, jika Anda memiliki ACL untuk dokumen Anda. Informasi ACL digunakan untuk memfilter hasil pencarian berdasarkan pengguna atau akses grup mereka ke dokumen. Untuk informasi selengkapnya, lihat Pemfilteran konteks pengguna.
- Pemetaan bidang —Pilih untuk memetakan bidang sumber data Gmail Anda ke bidang indeks Anda Amazon Kendra . Untuk informasi lebih lanjut, lihat Memetakan bidang sumber data.

> **Note**
>
> Bidang badan dokumen atau badan dokumen yang setara untuk dokumen Anda diperlukan Amazon Kendra untuk mencari dokumen Anda. Anda harus memetakan

nama bidang badan dokumen Anda di sumber data Anda ke nama bidang indeks_document_body. Semua kolom lain bersifat opsional.

> **Note**
>
> Amazon Kendra Konektor sumber data Gmail tidak mendukung pembuatan bidang indeks khusus karena keterbatasan API.

Pelajari selengkapnya

Untuk mempelajari lebih lanjut tentang mengintegrasikan Amazon Kendra dengan sumber data Gmail Anda, lihat:

- Lakukan pencarian cerdas di seluruh email di ruang kerja Google Anda menggunakan konektor Gmail untuk Amazon Kendra.

Catatan

- Karena tidak ada API untuk memperbarui pesan Gmail yang dihapus secara permanen, sinkronisasi konten**FULL_CRAWL**/Baru, dimodifikasi, atau dihapus:
  - Tidak akan menghapus pesan yang dihapus secara permanen dari Gmail dari Amazon Kendra indeks Anda
  - Tidak akan menyinkronkan perubahan pada label email Gmail

  Untuk menyinkronkan perubahan label sumber data Gmail dan pesan email yang dihapus secara permanen ke Amazon Kendra indeks, Anda harus menjalankan crawl penuh secara berkala.
- Amazon Kendra Konektor sumber data Gmail tidak mendukung pembuatan bidang indeks khusus karena keterbatasan API.

Google Drive

Google Drive adalah layanan penyimpanan file berbasis cloud. Anda dapat menggunakan Amazon Kendra untuk mengindeks dokumen yang disimpan di drive bersama, My Drives, dan Shared with me folder di sumber data Google Drive Anda. Anda dapat mengindeks dokumen Google Workspace

serta dokumen yang tercantum dalam Jenis dokumentasi. Anda juga dapat menggunakan filter inklusi dan pengecualian untuk mengindeks konten berdasarkan nama file, jenis file, dan jalur file.

Anda dapat terhubung Amazon Kendra ke sumber data Google Drive menggunakan Amazon Kendra konsol, TemplateConfigurationAPI, atau GoogleDriveConfigurationAPI.

Amazon Kendra memiliki dua versi konektor Google Drive. Fitur yang didukung dari setiap versi meliputi:

Konektor Google Drive V1.0/API GoogleDriveConfiguration

- Pemetaan lapangan
- Kontrol akses pengguna
- Filter inklusi/pengecualian

Konektor Google Drive V2.0 /API TemplateConfiguration

- Pemetaan lapangan
- Kontrol akses pengguna
- Filter inklusi/pengecualian
- Sinkronisasi konten penuh dan tambahan
- Cloud privat virtual (VPC)

> **Note**
>
> Support untuk konektor Google Drive V1.0/Google DriveConfiguration API dijadwalkan berakhir pada 2023. Kami merekomendasikan migrasi ke atau menggunakan konektor Google Drive V2.0/ TemplateConfiguration API.

Untuk memecahkan masalah konektor sumber data Amazon Kendra Google Drive, lihat. Mengatasi masalah sumber data

Topik

- Konektor Google Drive V1.0
- Konektor Google Drive V2.0

Konektor Google Drive V1.0

Google Drive adalah layanan penyimpanan file berbasis cloud. Anda dapat menggunakan Amazon Kendra untuk mengindeks dokumen dan komentar yang disimpan di drive bersama, My Drives, dan Shared with me folder di sumber data Google Drive Anda. Anda dapat mengindeks dokumen Google Workspace, serta dokumen yang tercantum dalam Jenis dokumentasi. Anda juga dapat menggunakan filter inklusi dan pengecualian untuk mengindeks konten berdasarkan nama file, jenis file, dan jalur file.

> **Note**
>
> Support untuk konektor Google Drive V1.0/Google DriveConfiguration API dijadwalkan berakhir pada 2023. Kami merekomendasikan migrasi ke atau menggunakan konektor Google Drive V2.0/ TemplateConfiguration API.

Untuk memecahkan masalah konektor sumber data Amazon Kendra Google Drive, lihat. Mengatasi masalah sumber data

Topik

- Fitur yang didukung
- Prasyarat
- Instruksi koneksi
- Pelajari selengkapnya

Fitur yang didukung

- Pemetaan lapangan
- Kontrol akses pengguna
- Filter inklusi/pengecualian

Prasyarat

Sebelum Anda dapat menggunakan Amazon Kendra untuk mengindeks sumber data Google Drive Anda, buat perubahan ini di Google Drive dan AWS akun Anda.

Di Google Drive, pastikan Anda memiliki:

- Entah telah diberikan akses oleh peran admin super atau pengguna dengan hak administratif. Anda tidak memerlukan peran admin super untuk diri sendiri jika Anda telah diberikan akses oleh peran admin super.
- Membuat akun layanan dengan Aktifkan Delegasi Seluruh Domain G Suite diaktifkan dan kunci JSON sebagai kunci pribadi menggunakan akun.
- Menyalin email akun pengguna Anda dan email akun layanan Anda. Saat Amazon Kendra Anda terhubung, masukkan email akun pengguna Anda sebagai email akun admin dan email akun layanan Anda sebagai email klien dalam Secrets Manager rahasia Anda.
- Menambahkan Admin SDK API dan Google Drive API di akun Anda.
- Menambahkan (atau meminta pengguna dengan peran admin super untuk menambahkan) izin berikut ke akun layanan Anda menggunakan peran admin super:
  - 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
- Memeriksa setiap dokumen unik di Google Drive dan di seluruh sumber data lain yang Anda rencanakan untuk digunakan untuk indeks yang sama. Setiap sumber data yang ingin Anda gunakan untuk indeks tidak boleh berisi dokumen yang sama di seluruh sumber data. ID dokumen bersifat global untuk indeks dan harus unik per indeks.

Di dalam Anda Akun AWS, pastikan Anda memiliki:

- Membuat Amazon Kendra indeks dan, jika menggunakan API, mencatat ID indeks.
- Membuat IAM peran untuk sumber data Anda dan, jika menggunakan API, catat ARN peran tersebut IAM .

> **Note**
>
> Jika Anda mengubah jenis otentikasi dan kredensialnya, Anda harus memperbarui IAM peran Anda untuk mengakses ID rahasia yang benar AWS Secrets Manager .

- Menyimpan kredensi otentikasi Google Drive Anda secara AWS Secrets Manager rahasia dan, jika menggunakan API, catat ARN rahasianya.

> **Note**
>
> Kami menyarankan Anda secara teratur menyegarkan atau memutar kredensil dan rahasia Anda. Berikan hanya tingkat akses yang diperlukan untuk keamanan Anda sendiri. Kami tidak menyarankan Anda menggunakan kembali kredensyal dan rahasia di seluruh sumber data, dan konektor versi 1.0 dan 2.0 (jika berlaku).

Jika Anda tidak memiliki IAM peran atau rahasia yang ada, Anda dapat menggunakan konsol untuk membuat IAM peran dan Secrets Manager rahasia baru saat Anda menghubungkan sumber data Google Drive Anda Amazon Kendra. Jika Anda menggunakan API, Anda harus memberikan ARN IAM peran dan Secrets Manager rahasia yang ada, dan ID indeks.

Instruksi koneksi

Untuk terhubung Amazon Kendra ke sumber data Google Drive Anda, Anda harus memberikan rincian yang diperlukan dari sumber data Google Drive Anda sehingga Amazon Kendra dapat mengakses data Anda. Jika Anda belum mengkonfigurasi Google Drive untuk Amazon Kendra lihatPrasyarat.

Console

Untuk terhubung Amazon Kendra ke Google Drive

1. Masuk ke Konsol AWS Manajemen dan buka Amazon Kendra konsol.
2. Dari panel navigasi kiri, pilih Indeks dan kemudian pilih indeks yang ingin Anda gunakan dari daftar indeks.

   > **Note**
   >
   > Anda dapat memilih untuk mengonfigurasi atau mengedit pengaturan kontrol akses Pengguna Anda di bawah Pengaturan indeks.

3. Pada halaman Memulai, pilih Tambahkan sumber data.
4. Pada halaman Tambah sumber data, pilih konektor Google Drive V1.0, lalu pilih Tambah konektor.
5. Pada halaman Tentukan detail sumber data, masukkan informasi berikut:

a. Di Nama dan deskripsi, untuk Nama sumber data —Masukkan nama untuk sumber data Anda. Anda dapat memasukkan tanda hubung tetapi bukan spasi.

b. (Opsional) Deskripsi —Masukkan deskripsi opsional untuk sumber data Anda.

c. Dalam Bahasa default —Pilih bahasa untuk memfilter dokumen Anda untuk indeks. Kecuali Anda menentukan sebaliknya, bahasa default ke bahasa Inggris. Bahasa yang ditentukan dalam metadata dokumen menggantikan bahasa yang dipilih.

d. Di Tag, untuk Tambahkan tag baru —Sertakan tag opsional untuk mencari dan memfilter sumber daya Anda atau melacak AWS biaya Anda.

e. Pilih Berikutnya.

6. Pada halaman Tentukan akses dan keamanan, masukkan informasi berikut:

a. Untuk Jenis otentikasi —Pilih antara yang Ada dan Baru. Jika Anda memilih untuk menggunakan rahasia yang ada, gunakan Select secret untuk memilih rahasia Anda.

b. Jika Anda memilih untuk membuat rahasia baru, opsi AWS Secrets Manager rahasia terbuka.

- Masukkan informasi berikut di jendela Buat AWS Secrets Manager rahasia:

A. Nama rahasia —Nama untuk rahasiamu. Awalan 'AmazonKendra-Google Drive-' secara otomatis ditambahkan ke nama rahasia Anda.

B. Untuk email akun Admin, email Klien, dan Kunci pribadi —Masukkan nilai kredensi autentikasi yang Anda buat dan unduh dari akun Google Drive Anda.

C. Pilih Simpan otentikasi.

c. IAM peran —Pilih peran yang sudah ada atau buat IAM IAM peran baru untuk mengakses kredensi repositori dan mengindeks konten Anda.

> **Note**
>
> IAM peran yang digunakan untuk indeks tidak dapat digunakan untuk sumber data. Jika Anda tidak yakin apakah peran yang ada digunakan untuk indeks atau FAQ, pilih Buat peran baru untuk menghindari kesalahan.

d. Pilih Berikutnya.

7. Pada halaman Konfigurasi pengaturan sinkronisasi, masukkan informasi berikut:

a. Kecualikan akun pengguna —Pengguna Google Drive yang ingin Anda kecualikan dari indeks. Anda dapat menambahkan hingga 100 akun pengguna.

b. Kecualikan drive bersama —Drive bersama Google Drive yang ingin Anda kecualikan dari indeks Anda. Anda dapat menambahkan hingga 100 drive bersama.

c. Kecualikan jenis file drive —Jenis file Google Drive yang ingin Anda kecualikan dari indeks Anda. Anda juga dapat memilih untuk mengedit pilihan tipe MIME.

d. Konfigurasi tambahan —Pola ekspresi reguler untuk menyertakan atau mengecualikan konten tertentu. Anda dapat menambahkan hingga 100 pola.

e. Frekuensi —Seberapa sering Amazon Kendra akan disinkronkan dengan sumber data Anda.

f. Pilih Berikutnya.

8. Pada halaman Setel pemetaan bidang, masukkan informasi berikut:

a. Untuk nama GoogleDrive bidang dan Pemetaan bidang yang disarankan tambahan — Pilih dari bidang sumber data default Amazon Kendra yang dihasilkan yang ingin Anda petakan ke indeks Anda.

b. Tambahkan bidang —Untuk menambahkan bidang sumber data kustom untuk membuat nama bidang indeks untuk dipetakan dan tipe data bidang.

c. Pilih Berikutnya.

9. Pada halaman Tinjau dan buat, periksa apakah informasi yang Anda masukkan sudah benar dan kemudian pilih Tambahkan sumber data. Anda juga dapat memilih untuk mengedit informasi Anda dari halaman ini. Sumber data Anda akan muncul di halaman Sumber data setelah sumber data berhasil ditambahkan.

API

Untuk terhubung Amazon Kendra ke Google Drive

Anda harus menentukan yang berikut menggunakan GoogleDriveConfigurationAPI:

- Rahasia Nama Sumber Daya Amazon (ARN) —Berikan Nama Sumber Daya Amazon (ARN) Secrets Manager rahasia yang berisi kredensyal otentikasi untuk akun Google Drive Anda. Rahasianya disimpan dalam struktur JSON dengan kunci berikut:

```
{
    "clientAccount": "service account email",
```

```
    "adminAccount": "user account email"",
    "privateKey": "private key"
}
```

> **Note**
>
> Kami menyarankan Anda secara teratur menyegarkan atau memutar kredensil dan rahasia Anda. Berikan hanya tingkat akses yang diperlukan untuk keamanan Anda sendiri. Kami tidak menyarankan Anda menggunakan kembali kredensyal dan rahasia di seluruh sumber data, dan konektor versi 1.0 dan 2.0 (jika berlaku).

- IAM peran —Tentukan `RoleArn` kapan Anda menelepon `CreateDataSource` untuk memberikan IAM peran dengan izin untuk mengakses Secrets Manager rahasia Anda dan memanggil API publik yang diperlukan untuk konektor Google Drive dan. Amazon Kendra Untuk informasi selengkapnya, lihat IAM peran untuk sumber data Google Drive.

Anda juga dapat menambahkan fitur opsional berikut:

- Filter inklusi dan pengecualian —Secara default Amazon Kendra mengindeks semua dokumen di Google Drive. Anda dapat menentukan apakah akan menyertakan atau mengecualikan konten tertentu dalam drive bersama, akun pengguna, jenis MIME dokumen, dan file. Jika Anda memilih untuk mengecualikan akun pengguna, tidak ada file di Drive Saya yang dimiliki oleh akun yang diindeks. File yang dibagikan dengan pengguna diindeks, kecuali pemilik file juga dikecualikan.

> **Note**
>
> Sebagian besar sumber data menggunakan pola ekspresi reguler, yang merupakan pola inklusi atau pengecualian yang disebut sebagai filter. Jika Anda menentukan filter inklusi, hanya konten yang cocok dengan filter inklusi yang diindeks. Dokumen apa pun yang tidak cocok dengan filter inklusi tidak diindeks. Jika Anda menentukan filter inklusi dan pengecualian, dokumen yang cocok dengan filter pengecualian tidak akan diindeks, meskipun sesuai dengan filter inklusi.

- Pemetaan bidang —Pilih untuk memetakan bidang sumber data Google Drive Anda ke bidang indeks Anda Amazon Kendra . Untuk informasi lebih lanjut, lihat Memetakan bidang sumber data.

> **Note**
>
> Bidang badan dokumen atau badan dokumen yang setara untuk dokumen Anda diperlukan Amazon Kendra untuk mencari dokumen Anda. Anda harus memetakan nama bidang badan dokumen Anda di sumber data Anda ke nama bidang indeks_`document_body`. Semua kolom lain bersifat opsional.

- Pemfilteran konteks pengguna dan kontrol akses —Amazon Kendra meng-crawl daftar kontrol akses (ACL) untuk dokumen Anda, jika Anda memiliki ACL untuk dokumen Anda. Informasi ACL digunakan untuk memfilter hasil pencarian berdasarkan pengguna atau akses grup mereka ke dokumen. Untuk informasi selengkapnya, lihat Pemfilteran konteks pengguna.

Pelajari selengkapnya

Untuk mempelajari lebih lanjut tentang mengintegrasikan Amazon Kendra dengan sumber data Google Drive Anda, lihat:

- Memulai dengan konektor Amazon Kendra Google Drive

Konektor Google Drive V2.0

Google Drive adalah layanan penyimpanan file berbasis cloud. Anda dapat menggunakan Amazon Kendra untuk mengindeks dokumen dan komentar yang disimpan di drive bersama, My Drives, dan Shared with me folder di sumber data Google Drive Anda. Anda dapat mengindeks dokumen Google Workspace, serta dokumen yang tercantum dalam Jenis dokumentasi. Anda juga dapat menggunakan filter inklusi dan pengecualian untuk mengindeks konten berdasarkan nama file, jenis file, dan jalur file.

> **Note**
>
> Support untuk konektor Google Drive V1.0/Google DriveConfiguration API dijadwalkan berakhir pada 2023. Kami merekomendasikan migrasi ke atau menggunakan konektor Google Drive V2.0/ TemplateConfiguration API.

Untuk memecahkan masalah konektor sumber data Amazon Kendra Google Drive, lihat. Mengatasi masalah sumber data

Topik

Fitur yang didukung

- Pemetaan lapangan
- Kontrol akses pengguna
- Filter inklusi/pengecualian
- Sinkronisasi konten penuh dan tambahan
- Cloud privat virtual (VPC)

Prasyarat

Sebelum Anda dapat menggunakan Amazon Kendra untuk mengindeks sumber data Google Drive Anda, buat perubahan ini di Google Drive dan AWS akun Anda.

Di Google Drive, pastikan Anda memiliki:

- Entah telah diberikan akses oleh peran admin super atau pengguna dengan hak administratif. Anda tidak memerlukan peran admin super untuk diri sendiri jika Anda telah diberikan akses oleh peran admin super.
- Kredensyal koneksi Akun Layanan Google Drive yang dikonfigurasi yang berisi email akun admin, email klien (email akun layanan), dan kunci pribadi Anda. Lihat dokumentasi Google Cloud tentang membuat dan menghapus kunci akun layanan.
- Membuat Akun Layanan Google Cloud (akun dengan otoritas yang didelegasikan untuk mengambil identitas pengguna) dengan Aktifkan Delegasi Seluruh Domain G Suite diaktifkan untuk server-to-server autentikasi, lalu buat kunci pribadi JSON menggunakan akun tersebut.

> **Note**
>
> Kunci pribadi harus dibuat setelah pembuatan akun layanan.

- Menambahkan Admin SDK API dan Google Drive API di akun pengguna Anda.
- Opsional: Kredensyal koneksi Google Drive OAuth 2.0 yang dikonfigurasi yang berisi ID klien, rahasia klien, dan token penyegaran sebagai kredensyal koneksi untuk pengguna tertentu. Anda memerlukan ini untuk merayapi data akun individual. Lihat dokumentasi Google tentang penggunaan OAuth 2.0 untuk mengakses API.
- Menambahkan (atau meminta pengguna dengan peran admin super untuk menambahkan) cakupan OAuth berikut ke akun layanan Anda menggunakan peran admin super. Cakupan API ini diperlukan untuk merayapi semua dokumen, dan informasi kontrol akses (ACL) untuk semua pengguna di domain Google Workspace:
  - https://www.googleapis.com/auth/drive.readonly—View dan unduh semua file Google Drive Anda
  - https://www.googleapis.com/auth/drive.metadata.readonly—View metadata untuk file di Google Drive Anda
  - https://www.googleapis.com/auth/admin.directory.group.readonly—Scope hanya untuk mengambil grup, alias grup, dan informasi anggota. Ini diperlukan untuk Amazon Kendra Identity Crawler.
  - https://www.googleapis.com/auth/admin.directory.user.readonly—Scope hanya untuk mengambil pengguna atau alias pengguna. Ini diperlukan untuk mencantumkan pengguna di Amazon Kendra Identity Crawler dan untuk menyetel ACL.
  - https://www.googleapis.com/auth/cloud-platform—Scope untuk menghasilkan token akses untuk mengambil konten file Google Drive besar.
  - https://www.googleapis.com/auth/forms.body.readonly—Scope untuk mengambil data dari Google Formulir.

  Untuk mendukung API Formulir, tambahkan cakupan tambahan berikut:
  - https://www.googleapis.com/auth/forms.body.readonly
- Memeriksa setiap dokumen unik di Google Drive dan di seluruh sumber data lain yang Anda rencanakan untuk digunakan untuk indeks yang sama. Setiap sumber data yang ingin Anda gunakan untuk indeks tidak boleh berisi dokumen yang sama di seluruh sumber data. ID dokumen bersifat global untuk indeks dan harus unik per indeks.

Di dalam Anda Akun AWS, pastikan Anda memiliki:

- Membuat Amazon Kendra indeks dan, jika menggunakan API, mencatat ID indeks.
- Membuat IAM peran untuk sumber data Anda dan, jika menggunakan API, catat ARN peran tersebut IAM .

> **Note**
>
> Jika Anda mengubah jenis otentikasi dan kredensialnya, Anda harus memperbarui IAM peran Anda untuk mengakses ID rahasia yang benar AWS Secrets Manager .

- Menyimpan kredensi otentikasi Google Drive Anda secara AWS Secrets Manager rahasia dan, jika menggunakan API, catat ARN rahasianya.

> **Note**
>
> Kami menyarankan Anda secara teratur menyegarkan atau memutar kredensil dan rahasia Anda. Berikan hanya tingkat akses yang diperlukan untuk keamanan Anda sendiri. Kami tidak menyarankan Anda menggunakan kembali kredensyal dan rahasia di seluruh sumber data, dan konektor versi 1.0 dan 2.0 (jika berlaku).

Jika Anda tidak memiliki IAM peran atau rahasia yang ada, Anda dapat menggunakan konsol untuk membuat IAM peran dan Secrets Manager rahasia baru saat Anda menghubungkan sumber data Google Drive Anda Amazon Kendra. Jika Anda menggunakan API, Anda harus memberikan ARN IAM peran dan Secrets Manager rahasia yang ada, dan ID indeks.

Instruksi koneksi

Untuk terhubung Amazon Kendra ke sumber data Google Drive Anda, Anda harus memberikan rincian yang diperlukan dari sumber data Google Drive Anda sehingga Amazon Kendra dapat mengakses data Anda. Jika Anda belum mengkonfigurasi Google Drive untuk Amazon Kendra lihatPrasyarat.

Console

Untuk terhubung Amazon Kendra ke Google Drive

1. Masuk ke AWS Management Console dan buka Amazon Kendra konsol.
2. Dari panel navigasi kiri, pilih Indeks dan kemudian pilih indeks yang ingin Anda gunakan dari daftar indeks.

> **Note**
>
> Anda dapat memilih untuk mengonfigurasi atau mengedit pengaturan kontrol akses Pengguna Anda di bawah Pengaturan indeks.

3. Pada halaman Memulai, pilih Tambahkan sumber data.
4. Pada halaman Tambah sumber data, pilih konektor Google Drive, lalu pilih Tambah konektor.
5. Pada halaman Tentukan detail sumber data, masukkan informasi berikut:

    a. Di Nama dan deskripsi, untuk Nama sumber data —Masukkan nama untuk sumber data Anda. Anda dapat memasukkan tanda hubung tetapi bukan spasi.

    b. (Opsional) Deskripsi —Masukkan deskripsi opsional untuk sumber data Anda.

    c. Dalam Bahasa default —Pilih bahasa untuk memfilter dokumen Anda untuk indeks. Kecuali Anda menentukan sebaliknya, bahasa default ke bahasa Inggris. Bahasa yang ditentukan dalam metadata dokumen menggantikan bahasa yang dipilih.

    d. Di Tag, untuk Tambahkan tag baru —Sertakan tag opsional untuk mencari dan memfilter sumber daya Anda atau melacak AWS biaya Anda.

    e. Pilih Berikutnya.

6. Pada halaman Tentukan akses dan keamanan, masukkan informasi berikut:

    a. Otorisasi — Aktifkan atau nonaktifkan informasi daftar kontrol akses (ACL) untuk dokumen Anda, jika Anda memiliki ACL dan ingin menggunakannya untuk kontrol akses. ACL menentukan dokumen mana yang dapat diakses pengguna dan grup. Informasi ACL digunakan untuk memfilter hasil pencarian berdasarkan pengguna atau akses grup mereka ke dokumen. Untuk informasi selengkapnya, lihat Pemfilteran konteks pengguna.

    b. Untuk Otentikasi —Pilih antara akun layanan Google dan otentikasi OAuth 2.0 berdasarkan kasus penggunaan Anda.

    c. AWS Secrets Manager Rahasia —Pilih rahasia yang ada, atau buat Secrets Manager rahasia baru untuk menyimpan kredensyal otentikasi Google Drive Anda. Jika Anda memilih untuk membuat rahasia baru, jendela AWS Secrets Manager rahasia terbuka.

        i. Jika Anda memilih akun layanan Google, masukkan nama untuk rahasia Anda, ID email pengguna admin atau “Pengguna Akun Layanan” dalam konfigurasi akun layanan Anda (email admin), ID email akun layanan (email klien), dan kunci pribadi yang Anda buat di akun layanan Anda.

Simpan dan tambahkan rahasia Anda

ii. Jika Anda memilih otentikasi OAuth 2.0, masukkan nama untuk rahasia, ID klien, rahasia klien, dan token penyegaran yang Anda buat di akun OAuth Anda.

Simpan dan tambahkan rahasia Anda.

d. Virtual Private Cloud (VPC) —Anda dapat memilih untuk menggunakan VPC. Jika demikian, Anda harus menambahkan Subnet dan grup keamanan VPC.

e. (Hanya untuk pengguna otentikasi akun layanan Google)

Perayap identitas —Tentukan apakah akan mengaktifkan crawler Amazon Kendra identitas. Perayap identitas menggunakan informasi daftar kontrol akses (ACL) untuk dokumen Anda untuk memfilter hasil penelusuran berdasarkan akses pengguna atau grup mereka ke dokumen. Jika Anda memiliki ACL untuk dokumen Anda dan memilih untuk menggunakan ACL Anda, Anda juga dapat memilih untuk mengaktifkan crawler Amazon Kendra identitas untuk mengonfigurasi pemfilteran konteks pengguna dari hasil pencarian. Jika tidak, jika crawler identitas dimatikan, semua dokumen dapat dicari secara publik. Jika Anda ingin menggunakan kontrol akses untuk dokumen dan crawler identitas dimatikan, Anda dapat menggunakan PutPrincipalMappingAPI untuk mengunggah informasi akses pengguna dan grup untuk pemfilteran konteks pengguna.

f. IAM peran —Pilih peran yang sudah ada atau buat IAM IAM peran baru untuk mengakses kredensi repositori dan mengindeks konten Anda.

> **Note**
>
> IAM peran yang digunakan untuk indeks tidak dapat digunakan untuk sumber data. Jika Anda tidak yakin apakah peran yang ada digunakan untuk indeks atau FAQ, pilih Buat peran baru untuk menghindari kesalahan.

g. Pilih Berikutnya.

7. Pada halaman Konfigurasi pengaturan sinkronisasi, masukkan informasi berikut:

a. Sinkronkan konten —Pilih opsi atau konten mana yang ingin dirayapi. Anda dapat memilih untuk merayapi Drive Saya (folder pribadi), Drive Bersama (folder yang dibagikan dengan Anda), atau keduanya. Anda juga dapat menyertakan komentar file.

b. Dalam Konfigurasi tambahan - opsional Anda juga dapat memasukkan informasi opsional berikut:

i. Target audiens —Tambahkan audiens target tertentu untuk dokumen yang ingin dirayapi.

ii. Ukuran file maksimum —Tetapkan batas ukuran maksimum dalam MB file untuk dirayapi.

iii. Email pengguna —Tambahkan email pengguna yang ingin Anda sertakan atau kecualikan.

iv. Drive bersama —Tambahkan nama drive bersama yang ingin Anda sertakan atau kecualikan.

v. Jenis mime —Tambahkan tipe MIME yang ingin Anda sertakan atau kecualikan.

vi. Pola regex entitas —Tambahkan pola ekspresi reguler untuk menyertakan atau mengecualikan lampiran tertentu untuk semua entitas yang didukung. Anda dapat menambahkan hingga 100 pola.

c. Mode sinkronisasi —Pilih cara memperbarui indeks saat konten sumber data berubah. Saat Anda menyinkronkan sumber data Amazon Kendra untuk pertama kalinya, semua konten dirayapi dan diindeks secara default. Anda harus menjalankan sinkronisasi penuh data Anda jika sinkronisasi awal Anda gagal, bahkan jika Anda tidak memilih sinkronisasi penuh sebagai opsi mode sinkronisasi Anda.

- Sinkronisasi penuh: Indeks baru semua konten, ganti konten yang ada setiap kali sumber data Anda disinkronkan dengan indeks Anda.
- Sinkronisasi baru yang dimodifikasi: Indeks hanya konten baru dan yang dimodifikasi setiap kali sumber data Anda disinkronkan dengan indeks Anda. Amazon Kendra dapat menggunakan mekanisme sumber data Anda untuk melacak perubahan konten dan mengindeks konten yang berubah sejak sinkronisasi terakhir.
- Sinkronisasi baru, dimodifikasi, dihapus: Indeks hanya konten baru, dimodifikasi, dan dihapus setiap kali sumber data Anda disinkronkan dengan indeks Anda. Amazon Kendra dapat menggunakan mekanisme sumber data Anda untuk melacak perubahan konten dan mengindeks konten yang berubah sejak sinkronisasi terakhir.

> **Important**
>
> Google Drive API tidak mendukung pengambilan komentar dari file yang dihapus secara permanen. Komentar dari file yang dibuang dapat diambil kembali. Ketika file dibuang, konektor akan menghapus komentar dari indeks. Amazon Kendra

d. Di Jadwal lari Sinkronisasi, untuk Frekuensi —pilih seberapa sering menyinkronkan konten sumber data Anda dan memperbarui indeks Anda.

e. Di Sync run history, pilih untuk menyimpan laporan yang dibuat secara otomatis Amazon S3 saat menyinkronkan sumber data Anda. Ini berguna untuk melacak masalah saat menyinkronkan sumber data Anda.

f. Pilih Berikutnya.

8. Pada halaman Setel pemetaan bidang, masukkan informasi berikut:

a. Untuk File —Pilih dari bidang sumber data default yang Amazon Kendra dihasilkan yang ingin Anda petakan ke indeks Anda.

> **Note**
>
> Google Drive API tidak mendukung pembuatan bidang khusus. Pemetaan bidang khusus tidak tersedia untuk konektor Google Drive.

b. Pilih Berikutnya.

9. Pada halaman Tinjau dan buat, periksa apakah informasi yang Anda masukkan sudah benar dan kemudian pilih Tambahkan sumber data. Anda juga dapat memilih untuk mengedit informasi Anda dari halaman ini. Sumber data Anda akan muncul di halaman Sumber data setelah sumber data berhasil ditambahkan.

API

Untuk terhubung Amazon Kendra ke Google Drive

Anda harus menentukan JSON dari skema sumber data menggunakan API. TemplateConfiguration Anda harus memberikan informasi berikut ini:

- Sumber data —Tentukan tipe sumber data seperti `GOOGLEDRIVEV2` saat Anda menggunakan skema TemplateConfigurationJSON. Tentukan juga sumber data seperti `TEMPLATE` saat Anda memanggil CreateDataSourceAPI.
- Jenis otentikasi —Tentukan apakah akan menggunakan otentikasi akun layanan atau otentikasi OAuth 2.0.
- Mode sinkronisasi —Tentukan cara Amazon Kendra memperbarui indeks Anda saat konten sumber data Anda berubah. Saat Anda menyinkronkan sumber data Amazon Kendra untuk pertama kalinya, semua konten dirayapi dan diindeks secara default. Anda harus menjalankan

sinkronisasi penuh data Anda jika sinkronisasi awal Anda gagal, bahkan jika Anda tidak memilih sinkronisasi penuh sebagai opsi mode sinkronisasi Anda. Anda dapat memilih antara:

- `FORCED_FULL_CRAWL`untuk mengindeks semua konten baru, mengganti konten yang ada setiap kali sumber data Anda disinkronkan dengan indeks Anda.
- `FULL_CRAWL`untuk mengindeks hanya konten baru, dimodifikasi, dan dihapus setiap kali sumber data Anda disinkronkan dengan indeks Anda. Amazon Kendra dapat menggunakan mekanisme sumber data Anda untuk melacak perubahan konten dan mengindeks konten yang berubah sejak sinkronisasi terakhir.
- `CHANGE_LOG`untuk mengindeks hanya konten baru dan yang dimodifikasi setiap kali sumber data Anda disinkronkan dengan indeks Anda. Amazon Kendra dapat menggunakan mekanisme sumber data Anda untuk melacak perubahan konten dan mengindeks konten yang berubah sejak sinkronisasi terakhir.

> **Important**
>
> Google Drive API tidak mendukung pengambilan komentar dari file yang dihapus secara permanen. Komentar dari file yang dibuang dapat diambil kembali. Ketika file dibuang, konektor akan menghapus komentar dari indeks. Amazon Kendra

- Rahasia Nama Sumber Daya Amazon (ARN) —Berikan Nama Sumber Daya Amazon (ARN) Secrets Manager rahasia yang berisi kredensyal otentikasi yang Anda buat di akun Google Drive Anda. Jika Anda menggunakan otentikasi akun layanan Google, rahasia disimpan dalam struktur JSON dengan kunci berikut:

```
{
    "clientEmail": "user account email",
    "adminAccountEmail": "service account email",
    "privateKey": "private key"
}
```

Jika Anda menggunakan otentikasi OAuth 2.0, rahasia disimpan dalam struktur JSON dengan kunci berikut:

```
{
    "clientID": "OAuth client ID",
    "clientSecret": "client secret",
    "refreshToken": "refresh token"
```

```
}
```

> **Note**
>
> Kami menyarankan Anda secara teratur menyegarkan atau memutar kredensil dan rahasia Anda. Berikan hanya tingkat akses yang diperlukan untuk keamanan Anda sendiri. Kami tidak menyarankan Anda menggunakan kembali kredensyal dan rahasia di seluruh sumber data, dan konektor versi 1.0 dan 2.0 (jika berlaku).

- IAM peran —Tentukan `RoleArn` kapan Anda menelepon `CreateDataSource` untuk memberikan IAM peran dengan izin untuk mengakses Secrets Manager rahasia Anda dan memanggil API publik yang diperlukan untuk konektor Google Drive dan. Amazon Kendra Untuk informasi selengkapnya, lihat IAM peran untuk sumber data Google Drive.

Anda juga dapat menambahkan fitur opsional berikut:

- Virtual Private Cloud (VPC) **`VpcConfiguration`** —Tentukan kapan Anda menelepon. `CreateDataSource` Untuk informasi selengkapnya, lihat Mengkonfigurasi Amazon Kendra untuk menggunakan Amazon VPC.
- Drive Saya, Drive Bersama, Komentar —Anda dapat menentukan apakah akan merayapi jenis konten ini.
- Filter penyertaan dan pengecualian —Anda dapat menentukan apakah akan menyertakan atau mengecualikan akun pengguna tertentu, drive bersama, dan tipe MIME.

> **Note**
>
> Sebagian besar sumber data menggunakan pola ekspresi reguler, yang merupakan pola inklusi atau pengecualian yang disebut sebagai filter. Jika Anda menentukan filter inklusi, hanya konten yang cocok dengan filter inklusi yang diindeks. Dokumen apa pun yang tidak cocok dengan filter inklusi tidak diindeks. Jika Anda menentukan filter inklusi dan pengecualian, dokumen yang cocok dengan filter pengecualian tidak akan diindeks, meskipun sesuai dengan filter inklusi.

- Daftar kontrol akses (ACL) —Tentukan apakah akan merayapi informasi ACL untuk dokumen Anda, jika Anda memiliki ACL dan ingin menggunakannya untuk kontrol akses. ACL menentukan dokumen mana yang dapat diakses pengguna dan grup. Informasi ACL digunakan

untuk memfilter hasil pencarian berdasarkan pengguna atau akses grup mereka ke dokumen. Untuk informasi selengkapnya, lihat Pemfilteran konteks pengguna.

- Perayap identitas —Tentukan apakah akan mengaktifkan crawler Amazon Kendra identitas. Perayap identitas menggunakan informasi daftar kontrol akses (ACL) untuk dokumen Anda untuk memfilter hasil penelusuran berdasarkan akses pengguna atau grup mereka ke dokumen. Jika Anda memiliki ACL untuk dokumen Anda dan memilih untuk menggunakan ACL Anda, Anda juga dapat memilih untuk mengaktifkan crawler Amazon Kendra identitas untuk mengonfigurasi pemfilteran konteks pengguna dari hasil pencarian. Jika tidak, jika crawler identitas dimatikan, semua dokumen dapat dicari secara publik. Jika Anda ingin menggunakan kontrol akses untuk dokumen dan crawler identitas dimatikan, Anda dapat menggunakan PutPrincipalMappingAPI untuk mengunggah informasi akses pengguna dan grup untuk pemfilteran konteks pengguna.
- Pemetaan bidang —Pilih untuk memetakan bidang sumber data Google Drive Anda ke bidang indeks Anda Amazon Kendra . Untuk informasi lebih lanjut, lihat Memetakan bidang sumber data.

> **Note**
>
> Bidang badan dokumen atau badan dokumen yang setara untuk dokumen Anda diperlukan Amazon Kendra untuk mencari dokumen Anda. Anda harus memetakan nama bidang badan dokumen Anda di sumber data Anda ke nama bidang indeks_`document_body`. Semua kolom lain bersifat opsional.

Untuk daftar kunci JSON penting lainnya untuk dikonfigurasi, lihat skema template Google Drive.

Catatan

- Pemetaan bidang khusus tidak tersedia untuk konektor Google Drive karena UI Google Drive tidak mendukung pembuatan bidang khusus.
- Google Drive API tidak mendukung pengambilan komentar dari file yang dihapus secara permanen. Komentar dapat diambil kembali, bagaimanapun, untuk file yang dibuang. Ketika file dibuang, Amazon Kendra konektor akan menghapus komentar dari indeks. Amazon Kendra
- Google Drive API tidak mengembalikan komentar yang ada dalam file.docx.

IBM DB2

IBM DB2adalah sistem manajemen basis data relasional yang dikembangkan olehIBM. Jika Anda adalah IBM DB2 pengguna, Anda dapat menggunakan Amazon Kendra untuk mengindeks sumber IBM DB2 data Anda. Konektor sumber Amazon Kendra IBM DB2 data mendukung DB2 11.5.7.

Anda dapat terhubung Amazon Kendra ke sumber IBM DB2 data menggunakan Amazon Kendra konsol dan TemplateConfigurationAPI.

Untuk memecahkan masalah konektor sumber Amazon Kendra IBM DB2 data Anda, lihat. Mengatasi masalah sumber data

Topik

Fitur yang didukung

- Pemetaan lapangan
- Pemfilteran konteks pengguna
- Filter inklusi/pengecualian
- Sinkronisasi konten penuh dan inkremental
- Cloud privat virtual (VPC)

Prasyarat

Sebelum dapat digunakan Amazon Kendra untuk mengindeks sumber IBM DB2 data Anda, buat perubahan ini di akun IBM DB2 dan AWS akun Anda.

DiIBM DB2, pastikan Anda memiliki:

- Mencatat nama pengguna dan kata sandi database Anda.

> **Important**
>
> Sebagai praktik terbaik, sediakan Amazon Kendra kredensil basis data hanya-baca.

- Menyalin url, port, dan instance host database Anda.
- Memeriksa setiap dokumen unik di dalam IBM DB2 dan di seluruh sumber data lain yang Anda rencanakan untuk digunakan untuk indeks yang sama. Setiap sumber data yang ingin Anda gunakan untuk indeks tidak boleh berisi dokumen yang sama di seluruh sumber data. ID dokumen bersifat global untuk indeks dan harus unik per indeks.

Di dalam Anda Akun AWS, pastikan Anda memiliki:

- Membuat Amazon Kendra indeks dan, jika menggunakan API, mencatat ID indeks.
- Membuat IAM peran untuk sumber data Anda dan, jika menggunakan API, catat ARN peran tersebut IAM .

> **Note**
>
> Jika Anda mengubah jenis otentikasi dan kredensyal, Anda harus memperbarui IAM peran Anda untuk mengakses ID rahasia yang benar AWS Secrets Manager .

- Menyimpan kredensyal IBM DB2 otentikasi Anda AWS Secrets Manager secara rahasia dan, jika menggunakan API, catat ARN rahasia tersebut.

> **Note**
>
> Kami menyarankan Anda secara teratur menyegarkan atau memutar kredensil dan rahasia Anda. Berikan hanya tingkat akses yang diperlukan untuk keamanan Anda sendiri. Kami tidak menyarankan Anda menggunakan kembali kredensyal dan rahasia di seluruh sumber data, dan konektor versi 1.0 dan 2.0 (jika berlaku).

Jika Anda tidak memiliki IAM peran atau rahasia yang ada, Anda dapat menggunakan konsol untuk membuat IAM peran dan Secrets Manager rahasia baru saat menghubungkan sumber IBM DB2 data Amazon Kendra. Jika Anda menggunakan API, Anda harus memberikan ARN IAM peran dan Secrets Manager rahasia yang ada, dan ID indeks.

Instruksi koneksi

Untuk terhubung Amazon Kendra ke sumber IBM DB2 data Anda, Anda harus memberikan rincian IBM DB2 kredensyal Anda sehingga Amazon Kendra dapat mengakses data Anda. Jika Anda belum mengkonfigurasi IBM DB2 untuk Amazon Kendra lihatPrasyarat.

Console

Untuk terhubung Amazon Kendra ke IBM DB2

1. Masuk ke AWS Management Console dan buka Amazon Kendra konsol.
2. Dari panel navigasi kiri, pilih Indeks dan kemudian pilih indeks yang ingin Anda gunakan dari daftar indeks.

> **Note**
>
> Anda dapat memilih untuk mengonfigurasi atau mengedit pengaturan kontrol akses Pengguna di bawah Pengaturan indeks.

3. Pada halaman Memulai, pilih Tambahkan sumber data.
4. Pada halaman Tambahkan sumber data, pilih IBM DB2konektor, lalu pilih Tambah konektor.
5. Pada halaman Tentukan detail sumber data, masukkan informasi berikut:
   a. Di Nama dan deskripsi, untuk Nama sumber data —Masukkan nama untuk sumber data Anda. Anda dapat memasukkan tanda hubung tetapi bukan spasi.
   b. (Opsional) Deskripsi —Masukkan deskripsi opsional untuk sumber data Anda.
   c. Dalam Bahasa default —Pilih bahasa untuk memfilter dokumen Anda untuk indeks. Kecuali Anda menentukan sebaliknya, bahasa default ke bahasa Inggris. Bahasa yang ditentukan dalam metadata dokumen mengesampingkan bahasa yang dipilih.
   d. Di Tag, untuk Tambahkan tag baru —Sertakan tag opsional untuk mencari dan memfilter sumber daya Anda atau melacak AWS biaya Anda.
   e. Pilih Berikutnya.
6. Pada halaman Tentukan akses dan keamanan, masukkan informasi berikut:
   a. Di Sumber, masukkan informasi berikut:
   b. Host — Masukkan nama host database.
   c. Port — Masukkan port database.

d. Instance - Masukkan instance database.

e. Aktifkan lokasi sertifikat SSL —Pilih untuk memasukkan Amazon S3 jalur ke file sertifikat SSL Anda.

f. Dalam Otentikasi —masukkan informasi berikut:

- AWS Secrets Manager rahasia —Pilih rahasia yang ada atau buat Secrets Manager rahasia baru untuk menyimpan kredensyal IBM DB2 otentikasi Anda. Jika Anda memilih untuk membuat rahasia baru, jendela AWS Secrets Manager rahasia terbuka.

  A. Masukkan informasi berikut di jendela Buat AWS Secrets Manager rahasia:

     I. Nama rahasia —Nama untuk rahasiamu. Awalan 'AmazonKendra- IBM DB2 -' secara otomatis ditambahkan ke nama rahasia Anda.

     II. Untuk nama pengguna Database, dan Kata Sandi —Masukkan nilai kredensi otentikasi yang Anda salin dari database Anda.

  B. Pilih Simpan.

g. Virtual Private Cloud (VPC) —Anda dapat memilih untuk menggunakan VPC. Jika demikian, Anda harus menambahkan Subnet dan grup keamanan VPC.

h. IAM peran —Pilih peran yang ada atau buat IAM IAM peran baru untuk mengakses kredensi repositori dan mengindeks konten Anda.

> **Note**
>
> IAM peran yang digunakan untuk indeks tidak dapat digunakan untuk sumber data. Jika Anda tidak yakin apakah peran yang ada digunakan untuk indeks atau FAQ, pilih Buat peran baru untuk menghindari kesalahan.

i. Pilih Berikutnya.

7. Pada halaman Konfigurasi pengaturan sinkronisasi, masukkan informasi berikut:

a. Dalam lingkup Sinkronisasi, pilih dari opsi berikut:

- Kueri SQL —Masukkan pernyataan kueri SQL seperti operasi SELECT dan JOIN. Kueri SQL harus kurang dari 32KB. Amazon Kendra akan merayapi semua konten database yang cocok dengan kueri Anda.

- Kolom kunci primer —Menyediakan kunci utama untuk tabel database. Ini mengidentifikasi tabel dalam database Anda.
- Judul kolom —Berikan nama kolom judul dokumen dalam tabel database Anda.
- Kolom tubuh —Berikan nama kolom badan dokumen dalam tabel database Anda.

b. Dalam Konfigurasi tambahan — opsional, pilih dari opsi berikut untuk menyinkronkan konten tertentu alih-alih menyinkronkan semua file:

- Kolom pendeteksi perubahan —Masukkan nama kolom yang Amazon Kendra akan digunakan untuk mendeteksi perubahan konten. Amazon Kendra akan mengindeks ulang konten ketika ada perubahan di salah satu kolom ini.
- Kolom ID Pengguna —Masukkan nama kolom yang berisi ID Pengguna agar diizinkan mengakses konten.
- Kolom Grup —Masukkan nama kolom yang berisi grup untuk diizinkan mengakses konten.
- Kolom URL sumber —Masukkan nama kolom yang berisi URL Sumber yang akan diindeks.
- Kolom stempel waktu —Masukkan nama kolom yang berisi stempel waktu. Amazon Kendra menggunakan informasi cap waktu untuk mendeteksi perubahan dalam konten Anda dan hanya menyinkronkan konten yang diubah.
- Kolom zona waktu —Masukkan nama kolom yang berisi zona waktu untuk konten yang akan dirayapi.
- Format stempel waktu —Masukkan nama kolom yang berisi format cap waktu yang akan digunakan untuk mendeteksi perubahan konten dan menyinkronkan ulang konten Anda.

c. Mode sinkronisasi —Pilih cara memperbarui indeks saat konten sumber data berubah. Saat Anda menyinkronkan sumber data Amazon Kendra untuk pertama kalinya, semua konten dirayapi dan diindeks secara default. Anda harus menjalankan sinkronisasi penuh data Anda jika sinkronisasi awal Anda gagal, bahkan jika Anda tidak memilih sinkronisasi penuh sebagai opsi mode sinkronisasi Anda.

- Sinkronisasi penuh: Indeks baru semua konten, ganti konten yang ada setiap kali sumber data Anda disinkronkan dengan indeks Anda.
- Sinkronisasi baru yang dimodifikasi: Indeks hanya konten baru dan yang dimodifikasi setiap kali sumber data Anda disinkronkan dengan indeks Anda. Amazon Kendra

dapat menggunakan mekanisme sumber data Anda untuk melacak perubahan konten dan mengindeks konten yang berubah sejak sinkronisasi terakhir.

- Sinkronisasi baru, dimodifikasi, dihapus: Indeks hanya konten baru, dimodifikasi, dan dihapus setiap kali sumber data Anda disinkronkan dengan indeks Anda. Amazon Kendra dapat menggunakan mekanisme sumber data Anda untuk melacak perubahan konten dan mengindeks konten yang berubah sejak sinkronisasi terakhir.

d. Dalam jadwal berjalan Sinkronisasi, untuk Frekuensi —Seberapa sering Amazon Kendra akan disinkronkan dengan sumber data Anda.

e. Pilih Berikutnya.

8. Pada halaman Setel pemetaan bidang, masukkan informasi berikut:

a. Pilih dari bidang sumber data default yang dihasilkan - ID dokumen, judul dokumen, dan URL Sumber - yang ingin Anda petakan ke Amazon Kendra indeks.

b. Tambahkan bidang —Untuk menambahkan bidang sumber data kustom untuk membuat nama bidang indeks untuk dipetakan dan tipe data bidang.

c. Pilih Berikutnya.

9. Pada halaman Tinjau dan buat, periksa apakah informasi yang Anda masukkan sudah benar dan kemudian pilih Tambahkan sumber data. Anda juga dapat memilih untuk mengedit informasi Anda dari halaman ini. Sumber data Anda akan muncul di halaman Sumber data setelah sumber data berhasil ditambahkan.

API

Untuk terhubung Amazon Kendra ke IBM DB2

Anda harus menentukan yang berikut menggunakan TemplateConfigurationAPI:

- Sumber data —Tentukan tipe sumber data seperti `JDBC` saat Anda menggunakan skema TemplateConfigurationJSON. Juga tentukan sumber data seperti `TEMPLATE` saat Anda memanggil CreateDataSourceAPI.
- Jenis database —Anda harus menentukan jenis database sebagai`db2`.
- Kueri SQL —Tentukan pernyataan kueri SQL seperti operasi SELECT dan JOIN. Kueri SQL harus kurang dari 32KB. Amazon Kendra akan merayapi semua konten database yang cocok dengan kueri Anda.
- Mode sinkronisasi —Tentukan cara Amazon Kendra memperbarui indeks Anda saat konten sumber data Anda berubah. Saat Anda menyinkronkan sumber data Amazon Kendra untuk

pertama kalinya, semua konten dirayapi dan diindeks secara default. Anda harus menjalankan sinkronisasi penuh data Anda jika sinkronisasi awal Anda gagal, bahkan jika Anda tidak memilih sinkronisasi penuh sebagai opsi mode sinkronisasi Anda. Anda dapat memilih antara:

- `FORCED_FULL_CRAWL`untuk mengindeks semua konten baru, mengganti konten yang ada setiap kali sumber data Anda disinkronkan dengan indeks Anda.
- `FULL_CRAWL`untuk mengindeks hanya konten baru, dimodifikasi, dan dihapus setiap kali sumber data Anda disinkronkan dengan indeks Anda. Amazon Kendra dapat menggunakan mekanisme sumber data Anda untuk melacak perubahan konten dan mengindeks konten yang berubah sejak sinkronisasi terakhir.
- `CHANGE_LOG`untuk mengindeks hanya konten baru dan yang dimodifikasi setiap kali sumber data Anda disinkronkan dengan indeks Anda. Amazon Kendra dapat menggunakan mekanisme sumber data Anda untuk melacak perubahan konten dan mengindeks konten yang berubah sejak sinkronisasi terakhir.

- Rahasia Nama Sumber Daya Amazon (ARN) —Berikan Nama Sumber Daya Amazon (ARN) Secrets Manager rahasia yang berisi kredensyal otentikasi yang Anda buat di akun Anda. IBM DB2 Rahasianya disimpan dalam struktur JSON dengan kunci berikut:

```
{
    "user name": "database user name",
    "password": "password"
}
```

> **Note**
>
> Kami menyarankan Anda secara teratur menyegarkan atau memutar kredensil dan rahasia Anda. Berikan hanya tingkat akses yang diperlukan untuk keamanan Anda sendiri. Kami tidak menyarankan Anda menggunakan kembali kredensyal dan rahasia di seluruh sumber data, dan konektor versi 1.0 dan 2.0 (jika berlaku).

- IAM peran —Tentukan `RoleArn` kapan Anda menelepon `CreateDataSource` untuk memberikan IAM peran dengan izin untuk mengakses Secrets Manager rahasia Anda dan memanggil API publik yang diperlukan untuk IBM DB2 konektor dan. Amazon Kendra Untuk informasi selengkapnya, lihat IAM peran untuk sumber IBM DB2 data.

Anda juga dapat menambahkan fitur opsional berikut:

- Virtual Private Cloud (VPC) **`VpcConfiguration`** —Tentukan kapan Anda menelepon. `CreateDataSource` Untuk informasi selengkapnya, lihat Mengkonfigurasi Amazon Kendra untuk menggunakan Amazon VPC.
- Filter penyertaan dan pengecualian —Anda dapat menentukan apakah akan menyertakan konten tertentu menggunakan ID pengguna, grup, URL sumber, stempel waktu, dan zona waktu.
- Pemfilteran konteks pengguna dan kontrol akses —Amazon Kendra meng-crawl daftar kontrol akses (ACL) untuk dokumen Anda, jika Anda memiliki ACL untuk dokumen Anda. Informasi ACL digunakan untuk memfilter hasil pencarian berdasarkan pengguna atau akses grup mereka ke dokumen. Untuk informasi selengkapnya, lihat Pemfilteran konteks pengguna.
- Pemetaan bidang —Pilih untuk memetakan bidang sumber IBM DB2 data Anda ke bidang indeks Anda Amazon Kendra . Untuk informasi lebih lanjut, lihat Memetakan bidang sumber data.

> **Note**
>
> Bidang badan dokumen atau badan dokumen yang setara untuk dokumen Anda diperlukan Amazon Kendra untuk mencari dokumen Anda. Anda harus memetakan nama bidang badan dokumen Anda di sumber data Anda ke nama bidang indeks_`document_body`. Semua kolom lain bersifat opsional.

Untuk daftar kunci JSON penting lainnya untuk dikonfigurasi, lihatSkema Templat IBM DB2.

Catatan

- Baris database yang dihapus tidak akan dilacak saat Amazon Kendra memeriksa konten yang diperbarui.
- Ukuran nama bidang dan nilai dalam deretan database Anda tidak dapat melebihi 400KB.
- Jika Anda memiliki sejumlah besar data dalam sumber data database Anda, dan tidak Amazon Kendra ingin mengindeks semua konten database Anda setelah sinkronisasi pertama, Anda dapat memilih untuk menyinkronkan hanya dokumen baru, dimodifikasi, atau dihapus.
- Sebagai praktik terbaik, sediakan Amazon Kendra kredensil basis data hanya-baca.
- Sebagai praktik terbaik, hindari menambahkan tabel dengan data sensitif atau informasi identitas pribadi (PII).

Jira

Jira adalah alat manajemen proyek untuk pengembangan perangkat lunak, manajemen produk, dan pelacakan bug. Anda dapat menggunakan Amazon Kendra untuk mengindeks proyek, masalah, komentar, lampiran, worklog, dan status Jira Anda.

Amazon Kendra Saat ini hanya mendukung Jira Cloud.

Anda dapat terhubung Amazon Kendra ke sumber data Jira Anda menggunakan Amazon Kendra konsol atau JiraConfiguration API. Untuk daftar fitur yang didukung oleh masing-masing fitur, lihatFitur yang didukung.

Untuk memecahkan masalah konektor sumber data Amazon Kendra Jira Anda, lihat. Mengatasi masalah sumber data

Topik

- Fitur yang didukung
- Prasyarat
- Instruksi koneksi
- Pelajari selengkapnya

Fitur yang didukung

Amazon Kendra Konektor sumber data Jira mendukung fitur-fitur berikut:

- Ubah log
- Pemetaan lapangan
- Pemfilteran konteks pengguna
- Filter inklusi/pengecualian
- Cloud privat virtual (VPC)

Prasyarat

Sebelum Anda dapat menggunakan Amazon Kendra untuk mengindeks sumber data Jira Anda, buat perubahan ini di Jira dan AWS akun Anda.

Di Jira, pastikan Anda memiliki:

- Kredensyal otentikasi token Jira API dibuat yang menyertakan ID Jira (nama pengguna atau email) dan kredensi Jira (token API Jira). Lihat dokumentasi Atlassian tentang pengelolaan token API.
- Mencatat URL akun Jira dari pengaturan akun Jira Anda. Misalnya, *https://company.atlassian.net/*.
- Memeriksa setiap dokumen unik di Jira dan di seluruh sumber data lain yang Anda rencanakan untuk digunakan untuk indeks yang sama. Setiap sumber data yang ingin Anda gunakan untuk indeks tidak boleh berisi dokumen yang sama di seluruh sumber data. ID dokumen bersifat global untuk indeks dan harus unik per indeks.

Di dalam Anda Akun AWS, pastikan Anda memiliki:

- Membuat Amazon Kendra indeks dan, jika menggunakan API, mencatat ID indeks.
- Membuat IAM peran untuk sumber data Anda dan, jika menggunakan API, catat ARN peran tersebut IAM .

> **Note**
>
> Jika Anda mengubah jenis otentikasi dan kredensyal, Anda harus memperbarui IAM peran Anda untuk mengakses ID rahasia yang benar AWS Secrets Manager .

- Menyimpan kredensi otentikasi Jira Anda secara AWS Secrets Manager rahasia dan, jika menggunakan API, catat ARN rahasianya.

> **Note**
>
> Kami menyarankan Anda secara teratur menyegarkan atau memutar kredensi dan rahasia Anda. Berikan hanya tingkat akses yang diperlukan untuk keamanan Anda sendiri. Kami tidak menyarankan Anda menggunakan kembali kredensyal dan rahasia di seluruh sumber data, dan konektor versi 1.0 dan 2.0 (jika berlaku).

Jika Anda tidak memiliki IAM peran atau rahasia yang ada, Anda dapat menggunakan konsol untuk membuat IAM peran dan Secrets Manager rahasia baru saat Anda menghubungkan sumber data Jira Anda. Amazon Kendra Jika Anda menggunakan API, Anda harus memberikan ARN IAM peran dan Secrets Manager rahasia yang ada, dan ID indeks.

Instruksi koneksi

Untuk terhubung Amazon Kendra ke sumber data Jira Anda, Anda harus memberikan rincian yang diperlukan dari sumber data Jira Anda sehingga Amazon Kendra dapat mengakses data Anda. Jika Anda belum mengkonfigurasi Jira untuk Amazon Kendra, lihatPrasyarat.

Console

Untuk terhubung Amazon Kendra ke Jira

1. Masuk ke AWS Management Console dan buka Amazon Kendra konsol.
2. Dari panel navigasi kiri, pilih Indeks dan kemudian pilih indeks yang ingin Anda gunakan dari daftar indeks.

> **Note**
>
> Anda dapat memilih untuk mengonfigurasi atau mengedit pengaturan kontrol akses Pengguna di bawah Pengaturan indeks.

3. Pada halaman Memulai, pilih Tambahkan sumber data.
4. Pada halaman Tambahkan sumber data, pilih konektor Jira, lalu pilih Tambah konektor.
5. Pada halaman Tentukan detail sumber data, masukkan informasi berikut:
   a. Di Nama dan deskripsi, untuk Nama sumber data —Masukkan nama untuk sumber data Anda. Anda dapat memasukkan tanda hubung tetapi bukan spasi.
   b. (Opsional) Deskripsi —Masukkan deskripsi opsional untuk sumber data Anda.
   c. Dalam Bahasa default —Pilih bahasa untuk memfilter dokumen Anda untuk indeks. Kecuali Anda menentukan sebaliknya, bahasa default ke bahasa Inggris. Bahasa yang ditentukan dalam metadata dokumen mengesampingkan bahasa yang dipilih.
   d. Di Tag, untuk Tambahkan tag baru —Sertakan tag opsional untuk mencari dan memfilter sumber daya Anda atau melacak AWS biaya Anda.
   e. Pilih Berikutnya.
6. Pada halaman Tentukan akses dan keamanan, masukkan informasi berikut:
   a. URL Akun JIRA —Masukkan URL Akun Jira Anda. Misalnya: *https://company.atlassian.net/*.

b. AWS Secrets Manager rahasia —Pilih rahasia yang ada atau buat Secrets Manager rahasia baru untuk menyimpan kredensyal otentikasi Jira Anda. Jika Anda memilih untuk membuat rahasia baru, jendela AWS Secrets Manager rahasia terbuka.

   i. Masukkan informasi berikut di jendela Buat AWS Secrets Manager rahasia:

      A. Nama rahasia —Nama untuk rahasiamu. Awalan 'AmazonKendra-Jira-' secara otomatis ditambahkan ke nama rahasia Anda.

      B. Untuk ID JIRA —Masukkan nama pengguna atau email Jira.

      C. Untuk Kata Sandi/Token —Masukkan token API Jira yang Anda buat dari akun Jira Anda.

   ii. Pilih Simpan.

c. Virtual Private Cloud (VPC) —Anda dapat memilih untuk menggunakan VPC. Jika demikian, Anda harus menambahkan Subnet dan grup keamanan VPC.

d. IAM peran —Pilih peran yang ada atau buat IAM IAM peran baru untuk mengakses kredensyal repositori dan mengindeks konten Anda.

> **Note**
>
> IAM peran yang digunakan untuk indeks tidak dapat digunakan untuk sumber data. Jika Anda tidak yakin apakah peran yang ada digunakan untuk indeks atau FAQ, pilih Buat peran baru untuk menghindari kesalahan.

e. Pilih Berikutnya.

7. Pada halaman Konfigurasi pengaturan sinkronisasi, masukkan informasi berikut:

   a. Pilih proyek Jira mana yang akan diindeks —Entitas Jira atau jenis konten yang ingin dirayapi.

   b. Status, elemen tambahan, dan jenis Masalah —Pilih konten untuk memperbaiki cakupan indeks Anda.

   c. Ubah log —Pilih untuk memperbarui indeks Anda hanya dengan konten baru atau yang dimodifikasi alih-alih menyinkronkan semua file Anda.

   d. Pola Regex —Pola ekspresi reguler untuk menyertakan atau mengecualikan file tertentu. Anda dapat menambahkan hingga 100 pola.

   e. Dalam jadwal berjalan Sinkronisasi, untuk Frekuensi —Pilih seberapa sering Amazon Kendra akan disinkronkan dengan sumber data Anda.

f. Pilih Berikutnya.

8. Pada halaman Setel pemetaan bidang, masukkan informasi berikut:

   a. Untuk Proyek, Masalah, Komentar, Lampiran, Worklog —Pilih dari bidang sumber data default yang Amazon Kendra dihasilkan yang ingin Anda petakan ke indeks Anda.

   b. Tambahkan bidang —Untuk menambahkan bidang sumber data kustom untuk membuat nama bidang indeks untuk dipetakan dan tipe data bidang.

   c. Pilih Berikutnya.

9. Pada halaman Tinjau dan buat, periksa apakah informasi yang Anda masukkan sudah benar dan kemudian pilih Tambahkan sumber data. Anda juga dapat memilih untuk mengedit informasi Anda dari halaman ini. Sumber data Anda akan muncul di halaman Sumber data setelah sumber data berhasil ditambahkan.

API

Untuk terhubung Amazon Kendra ke Jira

Anda harus menentukan yang berikut menggunakan JiraConfiguration API:

- URL sumber data —Tentukan URL akun Jira Anda. Misalnya, *company.atlassian.net*.
- Rahasia Nama Sumber Daya Amazon (ARN) —Berikan Nama Sumber Daya Amazon (ARN) Secrets Manager rahasia yang berisi kredensyal otentikasi untuk akun Jira Anda. Rahasianya disimpan dalam struktur JSON dengan kunci berikut:

```
{
    "jiraId": "Jira user name or email",
    "jiraCredential": "Jira API token"
}
```

> **Note**
>
> Kami menyarankan Anda secara teratur menyegarkan atau memutar kredensi dan rahasia Anda. Berikan hanya tingkat akses yang diperlukan untuk keamanan Anda sendiri. Kami tidak menyarankan Anda menggunakan kembali kredensyal dan rahasia di seluruh sumber data, dan konektor versi 1.0 dan 2.0 (jika berlaku).

- IAM peran —Tentukan `RoleArn` kapan Anda menelepon `CreateDataSource` untuk memberikan IAM peran dengan izin untuk mengakses Secrets Manager rahasia Anda dan memanggil API publik yang diperlukan untuk konektor Jira dan. Amazon Kendra Untuk informasi selengkapnya, lihat IAM peran untuk sumber data Jira.

Anda juga dapat menambahkan fitur opsional berikut:

- Virtual Private Cloud (VPC) —Tentukan `VpcConfiguration` sebagai bagian dari konfigurasi sumber data. Lihat Mengkonfigurasi Amazon Kendra untuk menggunakan VPC.
- Ubah log —Apakah Amazon Kendra harus menggunakan mekanisme log perubahan sumber data JIRA untuk menentukan apakah dokumen harus diperbarui dalam indeks.

> **Note**
>
> Gunakan log perubahan jika Anda tidak Amazon Kendra ingin memindai semua dokumen. Jika log perubahan Anda besar, mungkin perlu waktu Amazon Kendra lebih sedikit untuk memindai dokumen di sumber data Jira daripada memproses log perubahan. Jika Anda menyinkronkan sumber data Jira Anda dengan indeks Anda untuk pertama kalinya, semua dokumen dipindai.

- Filter inklusi dan pengecualian —Anda dapat menentukan apakah akan menyertakan atau mengecualikan file tertentu.

> **Note**
>
> Sebagian besar sumber data menggunakan pola ekspresi reguler, yang merupakan pola inklusi atau pengecualian yang disebut sebagai filter. Jika Anda menentukan filter inklusi, hanya konten yang cocok dengan filter inklusi yang diindeks. Dokumen apa pun yang tidak cocok dengan filter inklusi tidak diindeks. Jika Anda menentukan filter inklusi dan pengecualian, dokumen yang cocok dengan filter pengecualian tidak akan diindeks, meskipun sesuai dengan filter inklusi.

- Komentar, lampiran, dan log kerja —Anda dapat menentukan apakah akan merayapi komentar, lampiran, dan log pekerjaan tertentu dari masalah.
- Proyek, Masalah, Status —Anda dapat menentukan apakah akan merayapi ID proyek, jenis masalah, dan status tertentu.

- Pemfilteran konteks pengguna dan kontrol akses —Amazon Kendra meng-crawl daftar kontrol akses (ACL) untuk dokumen Anda, jika Anda memiliki ACL untuk dokumen Anda. Informasi ACL digunakan untuk memfilter hasil pencarian berdasarkan pengguna atau akses grup mereka ke dokumen. Untuk informasi selengkapnya, lihat Pemfilteran konteks pengguna.
- Pemetaan bidang —Pilih untuk memetakan bidang sumber data Jira Anda ke bidang indeks Anda. Amazon Kendra Untuk informasi lebih lanjut, lihat Memetakan bidang sumber data.

> **Note**
>
> Bidang badan dokumen atau badan dokumen yang setara untuk dokumen Anda diperlukan Amazon Kendra untuk mencari dokumen Anda. Anda harus memetakan nama bidang badan dokumen Anda di sumber data Anda ke nama bidang indeks `_document_body`. Semua kolom lain bersifat opsional.

Pelajari selengkapnya

Untuk mempelajari lebih lanjut tentang mengintegrasikan Amazon Kendra dengan sumber data Jira Anda, lihat:

- Cari proyek Jira Anda dengan cerdas dengan Amazon Kendra konektor Jira Cloud

Microsoft Exchange

Microsoft Exchange adalah alat kolaborasi perusahaan untuk pengiriman pesan, rapat, dan berbagi file. Jika Anda adalah pengguna Microsoft Exchange, Anda dapat menggunakan Amazon Kendra untuk mengindeks sumber data Microsoft Exchange Anda.

Anda dapat terhubung Amazon Kendra ke sumber data Microsoft Exchange menggunakan Amazon Kendra konsol dan TemplateConfigurationAPI.

Untuk memecahkan masalah konektor sumber data Amazon Kendra Microsoft Exchange, lihat. Mengatasi masalah sumber data

Fitur yang didukung

- Pemetaan lapangan
- Pemfilteran konteks pengguna

- Filter inklusi/pengecualian
- Sinkronisasi konten penuh dan tambahan
- Cloud privat virtual (VPC)

Prasyarat

Sebelum Anda dapat menggunakan Amazon Kendra untuk mengindeks sumber data Microsoft Exchange Anda, buat perubahan ini di Microsoft Exchange dan AWS akun Anda.

Di Microsoft Exchange, pastikan Anda memiliki:

- Membuat akun Microsoft Exchange di Office 365.
- Mencatat ID penyewa Microsoft 365 Anda. Anda dapat menemukan ID penyewa Anda di Properti Portal Direktori Aktif Azure Anda atau di aplikasi OAuth Anda.
- Membuat aplikasi OAuth di portal Azure dan mencatat ID klien dan rahasia klien atau kredensi klien. Lihat tutorial Microsoft dan contoh aplikasi Terdaftar untuk informasi selengkapnya.

> **Note**
>
> Saat Anda membuat atau mendaftarkan aplikasi di portal Azure, ID rahasia mewakili nilai rahasia yang sebenarnya. Anda harus mencatat atau menyimpan nilai rahasia yang sebenarnya segera saat membuat rahasia dan aplikasi. Anda dapat mengakses rahasia Anda dengan memilih nama aplikasi Anda di portal Azure dan kemudian menavigasi ke opsi menu pada sertifikat dan rahasia.
> Anda dapat mengakses ID klien Anda dengan memilih nama aplikasi Anda di portal Azure dan kemudian menavigasi ke halaman ikhtisar. ID Aplikasi (klien) adalah ID klien.

- Menambahkan izin berikut untuk aplikasi konektor:

Grafik Microsoft	Pertukaran Office 365 Online
• Mail.Read (Aplikasi) • Surat. ReadBasic (Aplikasi) • Surat. ReadBasic.Semua (Aplikasi) • Kalender.Baca (Aplikasi) • User.Read.All (Aplikasi)	full_access_as_app (Aplikasi)

Grafik Microsoft	Pertukaran Office 365 Online
• Kontak.Baca (Aplikasi) • Catatan.Read.All (Aplikasi) • Directory.Read.All (Aplikasi) • EWS. AccessAsUser.Semua (Delegasi)	

- Memeriksa setiap dokumen unik di Microsoft Exchange dan di seluruh sumber data lain yang Anda rencanakan untuk digunakan untuk indeks yang sama. Setiap sumber data yang ingin Anda gunakan untuk indeks tidak boleh berisi dokumen yang sama di seluruh sumber data. ID dokumen bersifat global untuk indeks dan harus unik per indeks.

Di dalam Anda Akun AWS, pastikan Anda memiliki:

- Membuat Amazon Kendra indeks dan, jika menggunakan API, mencatat ID indeks.
- Membuat IAM peran untuk sumber data Anda dan, jika menggunakan API, catat ARN peran tersebut IAM .

> **Note**
>
> Jika Anda mengubah jenis otentikasi dan kredensialnya, Anda harus memperbarui IAM peran Anda untuk mengakses ID rahasia yang benar AWS Secrets Manager .

- Menyimpan kredensi otentikasi Microsoft Exchange Anda AWS Secrets Manager secara rahasia dan, jika menggunakan API, catat ARN rahasianya.

> **Note**
>
> Kami menyarankan Anda secara teratur menyegarkan atau memutar kredensil dan rahasia Anda. Berikan hanya tingkat akses yang diperlukan untuk keamanan Anda sendiri. Kami tidak menyarankan Anda menggunakan kembali kredensyal dan rahasia di seluruh sumber data, dan konektor versi 1.0 dan 2.0 (jika berlaku).

Jika Anda tidak memiliki IAM peran atau rahasia yang ada, Anda dapat menggunakan konsol untuk membuat IAM peran dan Secrets Manager rahasia baru saat Anda menghubungkan sumber data

Microsoft Exchange Anda Amazon Kendra. Jika Anda menggunakan API, Anda harus memberikan ARN IAM peran dan Secrets Manager rahasia yang ada, dan ID indeks.

Instruksi koneksi

Untuk menyambung Amazon Kendra ke sumber data Microsoft Exchange, Anda harus memberikan rincian yang diperlukan dari sumber data Microsoft Exchange agar Amazon Kendra dapat mengakses data Anda. Jika Anda belum mengonfigurasi Microsoft Exchange untuk Amazon Kendra, lihatPrasyarat.

Console

Untuk terhubung Amazon Kendra ke Microsoft Exchange

1. Masuk ke AWS Management Console dan buka Amazon Kendra konsol.
2. Dari panel navigasi kiri, pilih Indeks dan kemudian pilih indeks yang ingin Anda gunakan dari daftar indeks.

> **Note**
>
> Anda dapat memilih untuk mengonfigurasi atau mengedit pengaturan kontrol akses Pengguna Anda di bawah Pengaturan indeks.

3. Pada halaman Memulai, pilih Tambahkan sumber data.
4. Pada halaman Tambah sumber data, pilih konektor Microsoft Exchange, lalu pilih Tambah konektor.
5. Pada halaman Tentukan detail sumber data, masukkan informasi berikut:
   a. Di Nama dan deskripsi, untuk Nama sumber data —Masukkan nama untuk sumber data Anda. Anda dapat memasukkan tanda hubung tetapi bukan spasi.
   b. (Opsional) Deskripsi —Masukkan deskripsi opsional untuk sumber data Anda.
   c. Dalam Bahasa default —Pilih bahasa untuk memfilter dokumen Anda untuk indeks. Kecuali Anda menentukan sebaliknya, bahasa default ke bahasa Inggris. Bahasa yang ditentukan dalam metadata dokumen menggantikan bahasa yang dipilih.
   d. Di Tag, untuk Tambahkan tag baru —Sertakan tag opsional untuk mencari dan memfilter sumber daya Anda atau melacak AWS biaya Anda.
   e. Pilih Berikutnya.

6. Pada halaman Tentukan akses dan keamanan, masukkan informasi berikut:

   a. Sumber —Masukkan ID penyewa Microsoft 365 Anda. Anda dapat menemukan ID penyewa Anda di Properti Portal Direktori Aktif Azure Anda atau di aplikasi OAuth Anda.

   b. Otorisasi — Aktifkan atau nonaktifkan informasi daftar kontrol akses (ACL) untuk dokumen Anda, jika Anda memiliki ACL dan ingin menggunakannya untuk kontrol akses. ACL menentukan dokumen mana yang dapat diakses pengguna dan grup. Informasi ACL digunakan untuk memfilter hasil pencarian berdasarkan pengguna atau akses grup mereka ke dokumen. Untuk informasi selengkapnya, lihat Pemfilteran konteks pengguna.

   c. AWS Secrets Manager rahasia —Pilih rahasia yang ada atau buat Secrets Manager rahasia baru untuk menyimpan kredensyal otentikasi Microsoft Exchange Anda. Jika Anda memilih untuk membuat rahasia baru, jendela AWS Secrets Manager rahasia terbuka.

      i. Masukkan informasi berikut di jendela Buat AWS Secrets Manager rahasia:

         A. Nama rahasia —Nama untuk rahasiamu. Awalan 'AmazonKendra-Microsoft Exchange

         B. Untuk ID Klien — Masukkan ID Klien.

         C. Untuk Rahasia Klien —Masukkan nilai kredensi otentikasi yang Anda buat di akun Microsoft Exchange Anda di portal Azure.

      ii. Pilih Simpan.

   d. Virtual Private Cloud (VPC) —Anda dapat memilih untuk menggunakan VPC. Jika demikian, Anda harus menambahkan Subnet dan grup keamanan VPC.

   e. IAM peran —Pilih peran yang sudah ada atau buat IAM IAM peran baru untuk mengakses kredensi repositori dan mengindeks konten Anda.

      > **Note**
      >
      > IAM peran yang digunakan untuk indeks tidak dapat digunakan untuk sumber data. Jika Anda tidak yakin apakah peran yang ada digunakan untuk indeks atau FAQ, pilih Buat peran baru untuk menghindari kesalahan.

   f. Pilih Berikutnya.

7. Pada halaman Konfigurasi pengaturan sinkronisasi, masukkan informasi berikut:

   a. Sinkronkan konten —Pilih konten untuk disinkronkan.

b. Konfigurasi tambahan —Anda dapat secara opsional mengindeks konten berikut alih-alih menyinkronkan semua dokumen.

- Jenis entitas — Pilih entitas yang ingin Anda sinkronkan. Anda dapat memilih antara Kalender, OneNotesdan Kontak.
- Perayapan kalender — Masukkan tanggal mulai dan berakhir untuk sinkronisasi kalender Anda.
- Sertakan email — Masukkan Email dari dan Email ke domain, dan baris Subjek apa pun yang ingin Anda sertakan atau kecualikan dalam indeks Anda.
- Regex untuk domain — Tambahkan pola untuk menyertakan dan mengecualikan domain email tertentu dari indeks Anda.
- Pola Regex - Tambahkan pola ekspresi reguler untuk menyertakan atau mengecualikan file tertentu. Anda dapat menambahkan hingga 100 pola.

c. Mode sinkronisasi —Pilih cara Anda ingin memperbarui indeks saat konten sumber data Anda berubah. Saat Anda menyinkronkan sumber data Amazon Kendra untuk pertama kalinya, semua konten dirayapi dan diindeks secara default. Anda harus menjalankan sinkronisasi penuh data Anda jika sinkronisasi awal Anda gagal, bahkan jika Anda tidak memilih sinkronisasi penuh sebagai opsi mode sinkronisasi Anda.

- Sinkronisasi penuh: Indeks baru semua konten, ganti konten yang ada setiap kali sumber data Anda disinkronkan dengan indeks Anda.
- Sinkronisasi baru yang dimodifikasi: Indeks hanya konten baru dan yang dimodifikasi setiap kali sumber data Anda disinkronkan dengan indeks Anda. Amazon Kendra dapat menggunakan mekanisme sumber data Anda untuk melacak perubahan konten dan mengindeks konten yang berubah sejak sinkronisasi terakhir.
- Sinkronisasi baru, dimodifikasi, dihapus: Indeks hanya konten baru, dimodifikasi, dan dihapus setiap kali sumber data Anda disinkronkan dengan indeks Anda. Amazon Kendra dapat menggunakan mekanisme sumber data Anda untuk melacak perubahan konten dan mengindeks konten yang berubah sejak sinkronisasi terakhir.

8. Pada halaman Setel pemetaan bidang, masukkan informasi berikut:

a. Bidang sumber data default —Pilih dari bidang sumber data default yang Amazon Kendra dihasilkan yang ingin Anda petakan ke indeks Anda.

> **Note**
>
> Konektor sumber data Amazon Kendra Microsoft Exchange tidak mendukung pemetaan bidang kustom.

b. Pilih Berikutnya.

9. Pada halaman Tinjau dan buat, periksa apakah informasi yang Anda masukkan sudah benar dan kemudian pilih Tambahkan sumber data. Anda juga dapat memilih untuk mengedit informasi Anda dari halaman ini. Sumber data Anda akan muncul di halaman Sumber data setelah sumber data berhasil ditambahkan.

API

Untuk terhubung Amazon Kendra ke Microsoft Exchange

Anda harus menentukan JSON dari skema sumber data menggunakan API. TemplateConfiguration Anda harus memberikan informasi berikut ini:

- Sumber data —Tentukan tipe sumber data seperti `MSEXCHANGE` saat Anda menggunakan skema TemplateConfigurationJSON. Tentukan juga sumber data seperti `TEMPLATE` saat Anda memanggil CreateDataSourceAPI.
- ID Penyewa —Anda dapat menemukan ID penyewa Anda di Properti Portal Direktori Aktif Azure Anda atau di aplikasi OAuth Anda.
- Mode sinkronisasi —Tentukan cara Amazon Kendra memperbarui indeks Anda saat konten sumber data Anda berubah. Saat Anda menyinkronkan sumber data Amazon Kendra untuk pertama kalinya, semua konten dirayapi dan diindeks secara default. Anda harus menjalankan sinkronisasi penuh data Anda jika sinkronisasi awal Anda gagal, bahkan jika Anda tidak memilih sinkronisasi penuh sebagai opsi mode sinkronisasi Anda. Anda dapat memilih antara:
  - `FORCED_FULL_CRAWL`untuk mengindeks semua konten baru, mengganti konten yang ada setiap kali sumber data Anda disinkronkan dengan indeks Anda.
  - `FULL_CRAWL`untuk mengindeks hanya konten baru, dimodifikasi, dan dihapus setiap kali sumber data Anda disinkronkan dengan indeks Anda. Amazon Kendra dapat menggunakan mekanisme sumber data Anda untuk melacak perubahan konten dan mengindeks konten yang berubah sejak sinkronisasi terakhir.
  - `CHANGE_LOG`untuk mengindeks hanya konten baru dan yang dimodifikasi setiap kali sumber data Anda disinkronkan dengan indeks Anda. Amazon Kendra dapat menggunakan

mekanisme sumber data Anda untuk melacak perubahan konten dan mengindeks konten yang berubah sejak sinkronisasi terakhir.

- Rahasia Nama Sumber Daya Amazon (ARN) —Berikan Nama Sumber Daya Amazon (ARN) Secrets Manager rahasia yang berisi kredensyal otentikasi untuk akun Microsoft Exchange Anda. Rahasianya disimpan dalam struktur JSON dengan kunci berikut:

```
{
    "clientId": "client ID",
    "clientSecret": "client secret"
}
```

> **Note**
>
> Kami menyarankan Anda secara teratur menyegarkan atau memutar kredensil dan rahasia Anda. Berikan hanya tingkat akses yang diperlukan untuk keamanan Anda sendiri. Kami tidak menyarankan Anda menggunakan kembali kredensyal dan rahasia di seluruh sumber data, dan konektor versi 1.0 dan 2.0 (jika berlaku).

- IAM peran —Tentukan `RoleArn` kapan Anda memanggil `CreateDataSource` untuk memberikan IAM peran dengan izin untuk mengakses Secrets Manager rahasia Anda dan memanggil API publik yang diperlukan untuk konektor Microsoft Exchange dan. Amazon Kendra Untuk informasi selengkapnya, lihat IAM peran untuk sumber data Microsoft Exchange.

Anda juga dapat menambahkan fitur opsional berikut:

- Virtual Private Cloud (VPC) **`VpcConfiguration`** —Tentukan kapan Anda menelepon. `CreateDataSource` Untuk informasi selengkapnya, lihat Mengkonfigurasi Amazon Kendra untuk menggunakan Amazon VPC.
- Filter inklusi dan pengecualian —Tentukan apakah akan menyertakan atau mengecualikan halaman dan aset tertentu.

> **Note**
>
> Sebagian besar sumber data menggunakan pola ekspresi reguler, yang merupakan pola inklusi atau pengecualian yang disebut sebagai filter. Jika Anda menentukan filter inklusi, hanya konten yang cocok dengan filter inklusi yang diindeks. Dokumen apa pun yang tidak cocok dengan filter inklusi tidak diindeks. Jika Anda menentukan filter inklusi

dan pengecualian, dokumen yang cocok dengan filter pengecualian tidak akan diindeks, meskipun sesuai dengan filter inklusi.

- Pemfilteran konteks pengguna dan kontrol akses —Amazon Kendra meng-crawl daftar kontrol akses (ACL) untuk dokumen Anda, jika Anda memiliki ACL untuk dokumen Anda. Informasi ACL digunakan untuk memfilter hasil pencarian berdasarkan pengguna atau akses grup mereka ke dokumen. Untuk informasi selengkapnya, lihat Pemfilteran konteks pengguna.
- Pemetaan bidang —Pilih untuk memetakan bidang sumber data Microsoft Exchange Anda ke bidang indeks Anda Amazon Kendra . Untuk informasi lebih lanjut, lihat Memetakan bidang sumber data.

> **Note**
>
> Bidang badan dokumen atau badan dokumen yang setara untuk dokumen Anda diperlukan Amazon Kendra untuk mencari dokumen Anda. Anda harus memetakan nama bidang badan dokumen Anda di sumber data Anda ke nama bidang indeks_`document_body`. Semua kolom lain bersifat opsional.

Pelajari selengkapnya

Untuk mempelajari lebih lanjut tentang mengintegrasikan Amazon Kendra dengan sumber data Microsoft Exchange Anda, lihat:

- Indeks konten Microsoft Exchange Anda menggunakan konektor Exchange untuk Amazon Kendra

Microsoft OneDrive

Microsoft OneDrive adalah layanan penyimpanan berbasis cloud yang dapat Anda gunakan untuk menyimpan, berbagi, dan meng-host konten Anda. Anda dapat menggunakan Amazon Kendra untuk mengindeks sumber OneDrive data Anda.

Anda dapat terhubung Amazon Kendra ke sumber OneDrive data menggunakan Amazon Kendra konsol dan OneDriveConfigurationAPI.

Amazon Kendra memiliki dua versi OneDrive konektor. Fitur yang didukung dari setiap versi meliputi:

OneDrive Konektor Microsoft V1.0 /API OneDriveConfiguration

- Pemetaan lapangan
- Filter inklusi/pengecualian

OneDrive Konektor Microsoft V2.0 /API TemplateConfiguration

- Pemfilteran konteks pengguna
- Perayap identitas pengguna
- Filter inklusi/pengecualian
- Sinkronisasi konten penuh dan tambahan
- Cloud privat virtual (VPC)

> **Note**
>
> Support untuk OneDrive konektor V1.0/ OneDriveConfiguration API dijadwalkan berakhir pada Juni 2023. Kami merekomendasikan menggunakan OneDrive konektor V2.0/ TemplateConfigurationAPI.

Untuk memecahkan masalah konektor sumber Amazon Kendra OneDrive data Anda, lihat. Mengatasi masalah sumber data

Topik

- OneDrive Konektor Microsoft V1.0
- OneDrive Konektor Microsoft V2.0
- Pelajari selengkapnya

OneDrive Konektor Microsoft V1.0

Microsoft OneDrive adalah layanan penyimpanan berbasis cloud yang dapat Anda gunakan untuk menyimpan, berbagi, dan meng-host konten Anda. Anda dapat menggunakan Amazon Kendra untuk mengindeks sumber OneDrive data Microsoft Anda.

> **Note**
>
> Support untuk OneDrive konektor V1.0/Microsft OneDrive API dijadwalkan berakhir pada Juni 2023. Kami merekomendasikan menggunakan OneDrive konektor V2.0/ TemplateConfiguration API.

Untuk memecahkan masalah konektor sumber Amazon Kendra OneDrive data Anda, lihat. Mengatasi masalah sumber data

Topik

- Fitur yang didukung
- Prasyarat
- Instruksi koneksi

Fitur yang didukung

- Pemetaan lapangan
- Filter inklusi/pengecualian

Prasyarat

Sebelum Anda dapat menggunakan Amazon Kendra untuk mengindeks sumber OneDrive data Anda, buat perubahan ini di akun OneDrive dan AWS akun Anda.

Di Azure Active Directory (AD) Anda, pastikan Anda memiliki:

- Membuat aplikasi Azure Active Directory (AD).
- Menggunakan ID aplikasi AD untuk mendaftarkan kunci rahasia untuk aplikasi di situs AD. Kunci rahasia harus berisi ID aplikasi dan kunci rahasia.
- Menyalin domain AD organisasi.
- Menambahkan izin aplikasi berikut ke aplikasi AD Anda pada opsi Microsoft Graph:
  - Membaca file di semua koleksi situs (File.Read.All)
  - Membaca profil lengkap semua pengguna (User.Read.All)
  - Membaca data direktori (Directory.Read.All)

  - Membaca semua grup (Group.Read.All)
  - Membaca item di semua koleksi situs (Site.Read.All)
- Menyalin daftar pengguna yang dokumennya harus diindeks. Anda dapat memilih untuk memberikan daftar nama pengguna, atau Anda dapat memberikan nama pengguna dalam file yang disimpan dalam file Amazon S3. Setelah membuat sumber data, Anda dapat:
  - Mengubah daftar pengguna.
  - Ubah dari daftar pengguna ke daftar yang disimpan dalam Amazon S3 bucket.
  - Ubah lokasi Amazon S3 bucket daftar pengguna. Jika Anda mengubah lokasi bucket, Anda juga harus memperbarui IAM peran untuk sumber data agar memiliki akses ke bucket.

    > **Note**
    >
    > Jika Anda menyimpan daftar nama pengguna dalam Amazon S3 bucket, IAM kebijakan untuk sumber data harus menyediakan akses ke bucket dan akses ke kunci yang dienkripsi bucket, jika ada.
- Memeriksa setiap dokumen unik di dalam OneDrive dan di seluruh sumber data lain yang Anda rencanakan untuk digunakan untuk indeks yang sama. Setiap sumber data yang ingin Anda gunakan untuk indeks tidak boleh berisi dokumen yang sama di seluruh sumber data. ID dokumen bersifat global untuk indeks dan harus unik per indeks.

Di dalam Anda Akun AWS, pastikan Anda memiliki:

- Membuat Amazon Kendra indeks dan, jika menggunakan API, mencatat ID indeks.
- Membuat IAM peran untuk sumber data Anda dan, jika menggunakan API, catat ARN peran tersebut IAM .

  > **Note**
  >
  > Jika Anda mengubah jenis otentikasi dan kredensialnya, Anda harus memperbarui IAM peran Anda untuk mengakses ID rahasia yang benar AWS Secrets Manager .
- Menyimpan kredensyal OneDrive otentikasi Anda AWS Secrets Manager secara rahasia dan, jika menggunakan API, catat ARN rahasia tersebut.

> **Note**
>
> Kami menyarankan Anda secara teratur menyegarkan atau memutar kredensyal dan rahasia Anda. Berikan hanya tingkat akses yang diperlukan untuk keamanan Anda sendiri. Kami tidak menyarankan Anda menggunakan kembali kredensyal dan rahasia di seluruh sumber data, dan konektor versi 1.0 dan 2.0 (jika berlaku).

Jika Anda tidak memiliki IAM peran atau rahasia yang ada, Anda dapat menggunakan konsol untuk membuat IAM peran dan Secrets Manager rahasia baru saat Anda menghubungkan sumber OneDrive data Anda Amazon Kendra. Jika Anda menggunakan API, Anda harus memberikan ARN IAM peran dan Secrets Manager rahasia yang ada, dan ID indeks.

Instruksi koneksi

Untuk terhubung Amazon Kendra ke sumber OneDrive data Anda, Anda harus memberikan rincian OneDrive kredensyal Anda sehingga Amazon Kendra dapat mengakses data Anda. Jika Anda belum mengkonfigurasi OneDrive untuk Amazon Kendra lihatPrasyarat.

Console

Untuk terhubung Amazon Kendra ke OneDrive

1. Masuk ke AWS Management Console dan buka Amazon Kendra konsol.
2. Dari panel navigasi kiri, pilih Indeks dan kemudian pilih indeks yang ingin Anda gunakan dari daftar indeks.

   > **Note**
   >
   > Anda dapat memilih untuk mengonfigurasi atau mengedit pengaturan kontrol akses Pengguna Anda di bawah Pengaturan indeks.

3. Pada halaman Memulai, pilih Tambahkan sumber data.
4. Pada halaman Tambahkan sumber data, pilih OneDrive konektor, lalu pilih Tambah konektor.
5. Pada halaman Tentukan detail sumber data, masukkan informasi berikut:

   a. Dalam Nama dan deskripsi, untuk Nama sumber data —Masukkan nama untuk sumber data Anda. Anda dapat memasukkan tanda hubung tetapi bukan spasi.

b. (Opsional) Deskripsi —Masukkan deskripsi opsional untuk sumber data Anda.

c. Dalam Bahasa default —Pilih bahasa untuk memfilter dokumen Anda untuk indeks. Kecuali Anda menentukan sebaliknya, bahasa default ke bahasa Inggris. Bahasa yang ditentukan dalam metadata dokumen mengesampingkan bahasa yang dipilih.

d. Di Tag, untuk Tambahkan tag baru —Sertakan tag opsional untuk mencari dan memfilter sumber daya Anda atau melacak AWS biaya Anda.

e. Pilih Berikutnya.

6. Pada halaman Tentukan akses dan keamanan, masukkan informasi berikut:

a. OneDrive ID penyewa —Masukkan ID OneDrive penyewa tanpa protokol.

b. Jenis otentikasi —Pilih antara Baru dan yang Ada.

c. i. Jika Anda memilih Existing, pilih rahasia yang ada untuk Select secret.

ii. Jika Anda memilih Baru, masukkan informasi berikut di bagian AWS Secrets Manager Rahasia baru:

A. Nama rahasia —Nama untuk rahasiamu. Awalan 'AmazonKendra- OneDrive -' secara otomatis ditambahkan ke nama rahasia Anda.

B. Untuk ID Aplikasi dan kata sandi Aplikasi —Masukkan nilai kredensi otentikasi dari OneDrive akun Anda dan kemudian pilih Simpan otentikasi.

d. IAM peran —Pilih peran yang sudah ada atau buat IAM IAM peran baru untuk mengakses kredensi repositori dan mengindeks konten Anda.

> **Note**
>
> IAM peran yang digunakan untuk indeks tidak dapat digunakan untuk sumber data. Jika Anda tidak yakin apakah peran yang ada digunakan untuk indeks atau FAQ, pilih Buat peran baru untuk menghindari kesalahan.

e. Pilih Berikutnya.

7. Pada halaman Konfigurasi pengaturan sinkronisasi, masukkan informasi berikut:

a. Pilih antara file Daftar dan daftar Nama berdasarkan kasus penggunaan Anda.

i. Jika Anda memilih Daftar file, masukkan informasi berikut:

- Pilih lokasi —Masukkan jalur ke Amazon S3 bucket Anda.

Tambahkan file daftar pengguna ke Amazon S3 —Pilih untuk menambahkan file daftar pengguna ke Amazon S3 bucket.

Pemetaan grup lokal pengguna —Pilih untuk menggunakan pemetaan grup lokal untuk memfilter konten Anda.

ii. Jika Anda memilih daftar Nama, masukkan informasi berikut:

- Nama pengguna —Masukkan hingga 10 drive pengguna untuk diindeks. Untuk menambahkan lebih dari 10 pengguna, buat file yang berisi nama.

  Tambahkan yang lain —Pilih untuk menambahkan lebih banyak pengguna.

  Pemetaan grup lokal pengguna —Pilih untuk menggunakan pemetaan grup lokal untuk memfilter konten Anda.

b. Untuk konfigurasi tambahan —Tambahkan pola ekspresi reguler untuk menyertakan atau mengecualikan file tertentu. Anda dapat menambahkan hingga 100 pola.

c. Di Jadwal berjalan Sinkronisasi, untuk Frekuensi —Pilih seberapa sering Amazon Kendra akan disinkronkan dengan sumber data Anda.

d. Pilih Berikutnya.

8. Pada halaman Setel pemetaan bidang, masukkan informasi berikut:

   a. Untuk bidang sumber data default dan Pemetaan bidang yang disarankan tambahan — Pilih dari bidang sumber data default Amazon Kendra yang dihasilkan yang ingin Anda petakan ke indeks Anda.

   b. Pilih Berikutnya.

9. Pada halaman Tinjau dan buat, periksa apakah informasi yang Anda masukkan sudah benar dan kemudian pilih Tambahkan sumber data. Anda juga dapat memilih untuk mengedit informasi Anda dari halaman ini. Sumber data Anda akan muncul di halaman Sumber data setelah sumber data berhasil ditambahkan.

API

Untuk terhubung Amazon Kendra ke OneDrive

Anda harus menentukan yang berikut menggunakan OneDriveConfigurationAPI:

- ID Penyewa —Tentukan domain Azure Active Directory organisasi.

- OneDrive Pengguna —Tentukan daftar akun pengguna yang dokumennya harus diindeks.
- Rahasia Nama Sumber Daya Amazon (ARN) —Berikan Nama Sumber Daya Amazon (ARN) Secrets Manager rahasia yang berisi kredensyal otentikasi untuk akun Anda. OneDrive Rahasianya disimpan dalam struktur JSON dengan kunci berikut:

```
{
    "username": "OAuth client ID",
    "password": "client secret"
}
```

> **Note**
>
> Kami menyarankan Anda secara teratur menyegarkan atau memutar kredensyal dan rahasia Anda. Berikan hanya tingkat akses yang diperlukan untuk keamanan Anda sendiri. Kami tidak menyarankan Anda menggunakan kembali kredensyal dan rahasia di seluruh sumber data, dan konektor versi 1.0 dan 2.0 (jika berlaku).

- IAM peran —Tentukan `RoleArn` kapan Anda menelepon `CreateDataSource` untuk memberikan IAM peran dengan izin untuk mengakses Secrets Manager rahasia Anda dan memanggil API publik yang diperlukan untuk OneDrive konektor dan. Amazon Kendra Untuk informasi selengkapnya, lihat IAM peran untuk sumber OneDrive data.

Anda juga dapat menambahkan fitur opsional berikut:

- Filter inklusi dan pengecualian —Tentukan apakah akan menyertakan atau mengecualikan dokumen tertentu.

> **Note**
>
> Sebagian besar sumber data menggunakan pola ekspresi reguler, yang merupakan pola inklusi atau pengecualian yang disebut sebagai filter. Jika Anda menentukan filter inklusi, hanya konten yang cocok dengan filter inklusi yang diindeks. Dokumen apa pun yang tidak cocok dengan filter inklusi tidak diindeks. Jika Anda menentukan filter inklusi dan pengecualian, dokumen yang cocok dengan filter pengecualian tidak akan diindeks, meskipun sesuai dengan filter inklusi.

- Pemetaan bidang —Pilih untuk memetakan bidang sumber OneDrive data Anda ke bidang indeks Anda Amazon Kendra . Untuk informasi lebih lanjut, lihat Memetakan bidang sumber data.

> **Note**
>
> Bidang badan dokumen atau badan dokumen yang setara untuk dokumen Anda diperlukan Amazon Kendra untuk mencari dokumen Anda. Anda harus memetakan nama bidang badan dokumen Anda di sumber data Anda ke nama bidang indeks_`document_body`. Semua kolom lain bersifat opsional.

- Pemfilteran konteks pengguna dan kontrol akses —Amazon Kendra meng-crawl daftar kontrol akses (ACL) untuk dokumen Anda, jika Anda memiliki ACL untuk dokumen Anda. Informasi ACL digunakan untuk memfilter hasil pencarian berdasarkan pengguna atau akses grup mereka ke dokumen. Untuk informasi selengkapnya, lihat Pemfilteran konteks pengguna.

OneDrive Konektor Microsoft V2.0

Microsoft OneDrive adalah layanan penyimpanan berbasis cloud yang dapat Anda gunakan untuk menyimpan, berbagi, dan meng-host konten Anda. Anda dapat menggunakan Amazon Kendra untuk mengindeks sumber OneDrive data Anda.

Anda dapat terhubung Amazon Kendra ke sumber OneDrive data menggunakan Amazon Kendra konsol dan OneDriveConfigurationAPI.

> **Note**
>
> Support untuk OneDrive Connector V1.0/ OneDriveConfiguration API dijadwalkan berakhir pada Juni 2023. Kami merekomendasikan menggunakan OneDrive Connector V2.0/ TemplateConfiguration API. Versi 2.0 menyediakan ACL tambahan dan fungsionalitas crawler identitas.

Untuk memecahkan masalah konektor sumber Amazon Kendra OneDrive data Anda, lihat. Mengatasi masalah sumber data

Topik

Fitur yang didukung

Amazon Kendra OneDrive konektor sumber data mendukung fitur-fitur berikut:

- Pemetaan lapangan
- Pemfilteran konteks pengguna
- Perayap identitas pengguna
- Filter inklusi/pengecualian
- Sinkronisasi konten penuh dan tambahan
- Cloud privat virtual (VPC)

Prasyarat

Sebelum Anda dapat menggunakan Amazon Kendra untuk mengindeks sumber OneDrive data Anda, buat perubahan ini di akun OneDrive dan AWS akun Anda.

Di OneDrive, pastikan Anda memiliki:

- Membuat OneDrive akun di Office 365.
- Mencatat ID penyewa Microsoft 365 Anda. Anda dapat menemukan ID penyewa Anda di Properti Portal Direktori Aktif Azure Anda atau di aplikasi OAuth Anda.
- Membuat aplikasi OAuth di portal Azure dan mencatat ID klien dan rahasia klien atau kredensi klien. Lihat tutorial Microsoft dan contoh aplikasi Terdaftar untuk informasi selengkapnya.

> **Note**
>
> Saat Anda membuat atau mendaftarkan aplikasi di portal Azure, ID rahasia mewakili nilai rahasia yang sebenarnya. Anda harus mencatat atau menyimpan nilai rahasia yang sebenarnya segera saat membuat rahasia dan aplikasi. Anda dapat mengakses rahasia Anda dengan memilih nama aplikasi Anda di portal Azure dan kemudian menavigasi ke opsi menu pada sertifikat dan rahasia.

Anda dapat mengakses ID klien Anda dengan memilih nama aplikasi Anda di portal Azure dan kemudian menavigasi ke halaman ikhtisar. ID Aplikasi (klien) adalah ID klien.

- Menggunakan ID aplikasi AD untuk mendaftarkan kunci rahasia untuk aplikasi di situs AD. Kunci rahasia harus berisi ID aplikasi dan kunci rahasia.
- Menyalin domain AD organisasi.
- Menambahkan izin berikut ke aplikasi AD Anda pada opsi Microsoft Graph:
  - Membaca file di semua koleksi situs (File.Read.All)
  - Baca profil lengkap semua pengguna (User.Read.All)
  - Membaca semua grup (Group.Read.All)
  - Baca semua catatan (Notes.Read.All)
- Menyalin daftar pengguna yang dokumennya harus diindeks. Anda dapat memilih untuk memberikan daftar nama pengguna, atau Anda dapat memberikan nama pengguna dalam file yang disimpan dalam file Amazon S3. Setelah membuat sumber data, Anda dapat:
  - Mengubah daftar pengguna.
  - Ubah dari daftar pengguna ke daftar yang disimpan dalam Amazon S3 bucket.
  - Ubah lokasi Amazon S3 bucket daftar pengguna. Jika Anda mengubah lokasi bucket, Anda juga harus memperbarui IAM peran untuk sumber data agar memiliki akses ke bucket.

> **Note**
>
> Jika Anda menyimpan daftar nama pengguna dalam Amazon S3 bucket, IAM kebijakan untuk sumber data harus menyediakan akses ke bucket dan akses ke kunci yang dienkripsi bucket, jika ada.
> OneDrive Konektor menggunakan Email dari Informasi Kontak yang ada di Properti Pengguna Onedrive. Pastikan pengguna yang datanya ingin dirayapi memiliki bidang email yang dikonfigurasi di halaman Informasi Kontak karena untuk pengguna baru ini mungkin kosong.

Di AWS akun Anda, pastikan Anda memiliki:

- Membuat Amazon Kendra indeks dan, jika menggunakan API, mencatat id indeks.
- Membuat IAM peran untuk sumber data Anda dan, jika menggunakan API, catat ARN peran tersebut IAM .

- Menyimpan kredensyal OneDrive otentikasi Anda AWS Secrets Manager secara rahasia dan, jika menggunakan API, catat ARN rahasia tersebut.

Jika Anda tidak memiliki IAM peran atau rahasia yang ada, Anda dapat menggunakan konsol untuk membuat IAM peran dan Secrets Manager rahasia baru saat Anda menghubungkan sumber OneDrive data Anda Amazon Kendra. Jika Anda menggunakan API, Anda harus memberikan ARN IAM peran dan Secrets Manager rahasia yang ada, dan id indeks.

Instruksi koneksi

Untuk terhubung Amazon Kendra ke sumber OneDrive data Anda, Anda harus memberikan rincian OneDrive kredensyal Anda sehingga Amazon Kendra dapat mengakses data Anda. Jika Anda belum mengkonfigurasi OneDrive untuk Amazon Kendra, lihatPrasyarat.

Console

Untuk terhubung Amazon Kendra ke OneDrive

1. Masuk ke AWS Management Console dan buka Amazon Kendra konsol.
2. Dari panel navigasi kiri, pilih Indeks dan kemudian pilih indeks yang ingin Anda gunakan dari daftar indeks.

> **Note**
>
> Anda dapat memilih untuk mengonfigurasi atau mengedit pengaturan kontrol akses Pengguna Anda di bawah Pengaturan indeks.

3. Pada halaman Memulai, pilih Tambahkan sumber data.
4. Pada halaman Tambahkan sumber data, pilih OneDrive konektor, lalu pilih Tambah konektor.
5. Pada halaman Tentukan detail sumber data, masukkan informasi berikut:

   a. Dalam Nama dan deskripsi, untuk Nama sumber data —Masukkan nama untuk sumber data Anda. Anda dapat memasukkan tanda hubung tetapi bukan spasi.

   b. (Opsional) Deskripsi —Masukkan deskripsi opsional untuk sumber data Anda.

   c. Dalam Bahasa default —Pilih bahasa untuk memfilter dokumen Anda untuk indeks. Kecuali Anda menentukan sebaliknya, bahasa default ke bahasa Inggris. Bahasa yang ditentukan dalam metadata dokumen mengesampingkan bahasa yang dipilih.

d. Di Tag, untuk Tambahkan tag baru —Sertakan tag opsional untuk mencari dan memfilter sumber daya Anda atau melacak AWS biaya Anda.

e. Pilih Berikutnya.

6. Pada halaman Tentukan akses dan keamanan, masukkan informasi berikut:

a. OneDrive ID penyewa —Masukkan ID OneDrive penyewa tanpa protokol.

b. Otorisasi — Aktifkan atau nonaktifkan informasi daftar kontrol akses (ACL) untuk dokumen Anda, jika Anda memiliki ACL dan ingin menggunakannya untuk kontrol akses. ACL menentukan dokumen mana yang dapat diakses pengguna dan grup. Informasi ACL digunakan untuk memfilter hasil pencarian berdasarkan pengguna atau akses grup mereka ke dokumen. Untuk informasi selengkapnya, lihat Pemfilteran konteks pengguna.

c. Dalam Otentikasi —Pilih antara Baru dan yang Ada.

d. i. Jika Anda memilih Existing, pilih rahasia yang ada untuk Select secret.

ii. Jika Anda memilih Baru, masukkan informasi berikut di bagian AWS Secrets Manager Rahasia baru:

A. Nama rahasia —Nama untuk rahasiamu. Awalan 'AmazonKendra- OneDrive -' secara otomatis ditambahkan ke nama rahasia Anda.

B. Untuk ID Klien dan Rahasia Klien —Masukkan ID klien dan rahasia klien dan kemudian pilih Simpan otentikasi.

e. Di Konfigurasi VPC dan grup keamanan - opsional, untuk Virtual Private Cloud (VPC) —Anda dapat memilih untuk menggunakan VPC. Jika demikian, Anda harus menambahkan Subnet dan grup keamanan VPC.

f. Perayap identitas —Tentukan apakah akan mengaktifkan crawler Amazon Kendra identitas. Perayap identitas menggunakan informasi daftar kontrol akses (ACL) untuk dokumen Anda untuk memfilter hasil penelusuran berdasarkan akses pengguna atau grup mereka ke dokumen. Jika Anda memiliki ACL untuk dokumen Anda dan memilih untuk menggunakan ACL Anda, Anda juga dapat memilih untuk mengaktifkan crawler Amazon Kendra identitas untuk mengonfigurasi pemfilteran konteks pengguna dari hasil pencarian. Jika tidak, jika crawler identitas dimatikan, semua dokumen dapat dicari secara publik. Jika Anda ingin menggunakan kontrol akses untuk dokumen dan crawler identitas dimatikan, Anda dapat menggunakan PutPrincipalMappingAPI untuk mengunggah informasi akses pengguna dan grup untuk pemfilteran konteks pengguna.

g. IAM peran —Pilih peran yang sudah ada atau buat IAM IAM peran baru untuk mengakses kredensi repositori dan mengindeks konten Anda.

> **Note**
>
> IAM peran yang digunakan untuk indeks tidak dapat digunakan untuk sumber data. Jika Anda tidak yakin apakah peran yang ada digunakan untuk indeks atau FAQ, pilih Buat peran baru untuk menghindari kesalahan.

h. Pilih Berikutnya.

7. Pada halaman Konfigurasi pengaturan sinkronisasi, masukkan informasi berikut:

8. a. Untuk Sinkronisasi lingkup —Pilih OneDrive data pengguna mana yang akan diindeks. Anda dapat menambahkan maksimal 10 pengguna secara manual.

   b. Untuk Konfigurasi tambahan —Tambahkan pola ekspresi reguler untuk menyertakan atau mengecualikan konten tertentu. Anda dapat menambahkan hingga 100 pola.

   c. Mode sinkronisasi —Pilih cara Anda ingin memperbarui indeks saat konten sumber data Anda berubah. Saat Anda menyinkronkan sumber data Amazon Kendra untuk pertama kalinya, semua konten dirayapi dan diindeks secara default. Anda harus menjalankan sinkronisasi penuh data Anda jika sinkronisasi awal Anda gagal, bahkan jika Anda tidak memilih sinkronisasi penuh sebagai opsi mode sinkronisasi Anda.

      - Sinkronisasi penuh: Indeks baru semua konten, ganti konten yang ada setiap kali sumber data Anda disinkronkan dengan indeks Anda.
      - Sinkronisasi baru yang dimodifikasi: Indeks hanya konten baru dan yang dimodifikasi setiap kali sumber data Anda disinkronkan dengan indeks Anda. Amazon Kendra dapat menggunakan mekanisme sumber data Anda untuk melacak perubahan konten dan mengindeks konten yang berubah sejak sinkronisasi terakhir.
      - Sinkronisasi baru, dimodifikasi, dihapus: Indeks hanya konten baru, dimodifikasi, dan dihapus setiap kali sumber data Anda disinkronkan dengan indeks Anda. Amazon Kendra dapat menggunakan mekanisme sumber data Anda untuk melacak perubahan konten dan mengindeks konten yang berubah sejak sinkronisasi terakhir.

   d. Di Jadwal berjalan Sinkronisasi, untuk Frekuensi —Pilih seberapa sering Amazon Kendra akan disinkronkan dengan sumber data Anda.

   e. Pilih Berikutnya.

9. Pada halaman Setel pemetaan bidang, masukkan informasi berikut:

a. Untuk bidang sumber data default dan Pemetaan bidang yang disarankan tambahan — Pilih dari bidang sumber data default Amazon Kendra yang dihasilkan yang ingin Anda petakan ke indeks Anda.

b. Pilih Berikutnya.

10. Pada halaman Tinjau dan buat, periksa apakah informasi yang Anda masukkan sudah benar dan kemudian pilih Tambahkan sumber data. Anda juga dapat memilih untuk mengedit informasi Anda dari halaman ini. Sumber data Anda akan muncul di halaman Sumber data setelah sumber data berhasil ditambahkan.

API

Untuk terhubung Amazon Kendra ke OneDrive

Anda harus menentukan JSON dari skema sumber data menggunakan API. TemplateConfiguration Anda harus memberikan informasi berikut ini:

- Sumber data —Tentukan tipe sumber data seperti `ONEDRIVEV2` saat Anda menggunakan skema TemplateConfigurationJSON. Tentukan juga sumber data seperti `TEMPLATE` saat Anda memanggil CreateDataSourceAPI.
- ID penyewa —Tentukan ID penyewa Microsoft 365. Anda dapat menemukan ID penyewa Anda di Properti Portal Direktori Aktif Azure Anda atau di aplikasi OAuth Anda.
- Mode sinkronisasi —Tentukan cara Amazon Kendra memperbarui indeks Anda saat konten sumber data Anda berubah. Saat Anda menyinkronkan sumber data Amazon Kendra untuk pertama kalinya, semua konten dirayapi dan diindeks secara default. Anda harus menjalankan sinkronisasi penuh data Anda jika sinkronisasi awal Anda gagal, bahkan jika Anda tidak memilih sinkronisasi penuh sebagai opsi mode sinkronisasi Anda. Anda dapat memilih antara:
  - `FORCED_FULL_CRAWL`untuk mengindeks semua konten baru, mengganti konten yang ada setiap kali sumber data Anda disinkronkan dengan indeks Anda.
  - `FULL_CRAWL`untuk mengindeks hanya konten baru, dimodifikasi, dan dihapus setiap kali sumber data Anda disinkronkan dengan indeks Anda. Amazon Kendra dapat menggunakan mekanisme sumber data Anda untuk melacak perubahan konten dan mengindeks konten yang berubah sejak sinkronisasi terakhir.
  - `CHANGE_LOG`untuk mengindeks hanya konten baru dan yang dimodifikasi setiap kali sumber data Anda disinkronkan dengan indeks Anda. Amazon Kendra dapat menggunakan

mekanisme sumber data Anda untuk melacak perubahan konten dan mengindeks konten yang berubah sejak sinkronisasi terakhir.

- Rahasia Nama Sumber Daya Amazon (ARN) —Berikan Nama Sumber Daya Amazon (ARN) Secrets Manager rahasia yang berisi kredensi otentikasi yang Anda buat di akun Anda. OneDrive

  Jika Anda menggunakan otentikasi OAuth 2.0, rahasia disimpan dalam struktur JSON dengan kunci berikut:

  ```
  {
      "clientId": "client ID",
      "clientSecret": "client secret"
  }
  ```

  > **Note**
  >
  > Kami menyarankan Anda secara teratur menyegarkan atau memutar kredensyal dan rahasia Anda. Berikan hanya tingkat akses yang diperlukan untuk keamanan Anda sendiri. Kami tidak menyarankan Anda menggunakan kembali kredensyal dan rahasia di seluruh sumber data, dan konektor versi 1.0 dan 2.0 (jika berlaku).

- IAM peran —Tentukan `RoleArn` kapan Anda menelepon `CreateDataSource` untuk memberikan IAM peran dengan izin untuk mengakses Secrets Manager rahasia Anda dan memanggil API publik yang diperlukan untuk OneDrive konektor dan. Amazon Kendra Untuk informasi selengkapnya, lihat IAM peran untuk sumber OneDrive data.

Anda juga dapat menambahkan fitur opsional berikut:

- Virtual Private Cloud (VPC) **`VpcConfiguration`** —Tentukan kapan Anda menelepon. `CreateDataSource` Untuk informasi selengkapnya, lihat Mengkonfigurasi Amazon Kendra untuk menggunakan Amazon VPC.
- Filter inklusi dan pengecualian —Anda dapat menentukan apakah akan menyertakan atau mengecualikan file, OneNote bagian, dan OneNote halaman tertentu.

> **Note**
>
> Sebagian besar sumber data menggunakan pola ekspresi reguler, yang merupakan pola inklusi atau pengecualian yang disebut sebagai filter. Jika Anda menentukan filter inklusi, hanya konten yang cocok dengan filter inklusi yang diindeks. Dokumen apa pun yang tidak cocok dengan filter inklusi tidak diindeks. Jika Anda menentukan filter inklusi dan pengecualian, dokumen yang cocok dengan filter pengecualian tidak akan diindeks, meskipun sesuai dengan filter inklusi.

- Perayap identitas —Tentukan apakah akan mengaktifkan crawler Amazon Kendra identitas. Perayap identitas menggunakan informasi daftar kontrol akses (ACL) untuk dokumen Anda untuk memfilter hasil penelusuran berdasarkan akses pengguna atau grup mereka ke dokumen. Jika Anda memiliki ACL untuk dokumen Anda dan memilih untuk menggunakan ACL Anda, Anda juga dapat memilih untuk mengaktifkan crawler Amazon Kendra identitas untuk mengonfigurasi pemfilteran konteks pengguna dari hasil pencarian. Jika tidak, jika crawler identitas dimatikan, semua dokumen dapat dicari secara publik. Jika Anda ingin menggunakan kontrol akses untuk dokumen dan crawler identitas dimatikan, Anda dapat menggunakan PutPrincipalMappingAPI untuk mengunggah informasi akses pengguna dan grup untuk pemfilteran konteks pengguna.
- Pemetaan bidang —Anda hanya dapat memetakan bidang indeks bawaan atau umum untuk konektor. Amazon Kendra OneDrive Pemetaan bidang khusus tidak tersedia untuk OneDrive konektor karena keterbatasan API. Untuk informasi lebih lanjut, lihat Memetakan bidang sumber data.

Untuk daftar kunci JSON penting lainnya untuk dikonfigurasi, lihat OneDrive Skema templat Microsoft.

Pelajari selengkapnya

Untuk mempelajari lebih lanjut tentang mengintegrasikan Amazon Kendra dengan sumber OneDrive data Anda, lihat:

- Mengumumkan OneDrive konektor Microsoft (V2) yang diperbarui untuk Amazon Kendra.

Microsoft SharePoint

SharePoint adalah layanan pembuatan situs web kolaboratif yang dapat Anda gunakan untuk menyesuaikan konten web dan membuat halaman, situs, pustaka dokumen, dan daftar. Anda dapat menggunakan Amazon Kendra untuk mengindeks sumber SharePoint data Anda.

Amazon Kendra saat ini mendukung SharePoint Online dan SharePoint Server (versi 2013, 2016, 2019, dan Edisi Berlangganan).

Anda dapat terhubung Amazon Kendra ke sumber SharePoint data menggunakan Amazon Kendra konsol, TemplateConfigurationAPI, atau SharePointConfigurationAPI.

Amazon Kendra memiliki dua versi SharePoint konektor. Fitur yang didukung dari setiap versi meliputi:

SharePoint Konektor V1.0 /API SharePointConfiguration

- Ubah log
- Pemetaan lapangan
- Pemfilteran konteks pengguna
- Filter inklusi/pengecualian
- Cloud privat virtual (VPC)

SharePoint Konektor V2.0 /API TemplateConfiguration

- Pemetaan lapangan
- Pemfilteran konteks pengguna
- Perayapan identitas pengguna
- Filter inklusi/pengecualian
- Sinkronisasi konten penuh dan tambahan
- Cloud privat virtual (VPC)

> **Note**
>
> Support untuk SharePoint konektor V1.0/ SharePointConfiguration API dijadwalkan berakhir pada tahun 2023. Kami merekomendasikan migrasi ke atau menggunakan SharePoint konektor V2.0/ TemplateConfiguration API.

Untuk memecahkan masalah konektor sumber Amazon Kendra SharePoint data Anda, lihat. Mengatasi masalah sumber data

Topik

- SharePoint konektor V1.0
- SharePoint konektor V2.0

SharePoint konektor V1.0

SharePoint adalah layanan pembuatan situs web kolaboratif yang dapat Anda gunakan untuk menyesuaikan konten web dan membuat halaman, situs, pustaka dokumen, dan daftar. Jika Anda adalah SharePoint pengguna, Anda dapat menggunakan Amazon Kendra untuk mengindeks sumber SharePoint data Anda.

> **Note**
>
> Support untuk SharePoint konektor V1.0/ SharePointConfiguration API dijadwalkan berakhir pada tahun 2023. Kami merekomendasikan migrasi ke atau menggunakan SharePoint konektor V2.0/ TemplateConfiguration API.

Untuk memecahkan masalah konektor sumber Amazon Kendra SharePoint data Anda, lihat. Mengatasi masalah sumber data

Topik

- Fitur yang didukung
- Prasyarat
- Instruksi koneksi
- Pelajari selengkapnya

Fitur yang didukung

- Ubah log
- Pemetaan lapangan
- Pemfilteran konteks pengguna
- Filter inklusi/pengecualian
- Cloud privat virtual (VPC)

Prasyarat

Sebelum dapat digunakan Amazon Kendra untuk mengindeks sumber SharePoint data Anda, buat perubahan ini di akun SharePoint dan AWS akun Anda.

Di SharePoint, pastikan Anda memiliki:

- Mencatat URL SharePoint situs yang ingin Anda indeks.
- Untuk SharePoint Online:
  - Mencatat kredensyal otentikasi dasar Anda yang berisi nama pengguna dan kata sandi dengan izin admin situs.
  - Opsional: Kredensyal OAuth 2.0 yang dihasilkan yang berisi nama pengguna, kata sandi, ID klien, dan rahasia klien.
  - Default Keamanan Dinonaktifkan di portal Azure Anda menggunakan pengguna administratif. Untuk informasi selengkapnya tentang mengelola setelan default keamanan di portal Azure, lihat dokumentasi Microsoft tentang cara mengaktifkan/menonaktifkan default keamanan.
- Untuk SharePoint Server:
  - Mencatat nama domain SharePoint Server Anda (nama NetBIOS di Direktori Aktif Anda). Anda menggunakan ini, bersama dengan nama pengguna dan kata sandi otentikasi SharePoint dasar Anda, untuk menghubungkan SharePoint Server ke Amazon Kendra.

> **Note**
>
> Jika Anda menggunakan SharePoint Server dan perlu mengonversi Daftar Kontrol Akses (ACL) Anda ke format email untuk pemfilteran pada konteks pengguna, berikan URL server LDAP dan basis pencarian LDAP. Atau Anda dapat menggunakan penggantian domain direktori. URL server LDAP adalah nama domain lengkap dan nomor port (misalnya, ldap: //example.com:389). Basis pencarian LDAP adalah pengontrol domain 'example'

dan 'com'. Dengan penggantian domain direktori, Anda dapat menggunakan domain email alih-alih menggunakan URL server LDAP dan basis pencarian LDAP. Misalnya, domain email untuk username@example.com adalah 'example.com'. Anda dapat menggunakan override ini jika Anda tidak khawatir tentang memvalidasi domain Anda dan hanya ingin menggunakan domain email Anda.

- Menambahkan izin berikut ke SharePoint akun Anda:

  Untuk SharePoint daftar

  - Buka Item—Lihat sumber dokumen dengan penangan file sisi server.
  - Lihat Halaman Aplikasi—Lihat formulir, tampilan, dan halaman aplikasi. Hitung daftar.
  - Lihat Item—Lihat item dalam daftar dan dokumen di pustaka dokumen.
  - Lihat Versi—Lihat versi sebelumnya dari item daftar atau dokumen.

  Untuk SharePoint situs web

  - Jelajahi Direktori—Hitung file dan folder di situs web menggunakan antarmuka Designer dan Web DAV. SharePoint
  - Jelajahi Informasi Pengguna—Lihat informasi tentang pengguna situs web.
  - Hitung Izin—Hitung izin di situs web, daftar, folder, dokumen, atau item daftar.
  - Buka — Buka situs web, daftar, atau folder untuk mengakses item di dalam wadah.
  - Gunakan Fitur Integrasi Klien—Gunakan SOAP, WebDAV, model objek klien, atau SharePoint antarmuka Desainer untuk mengakses situs web.
  - Gunakan Antarmuka Jarak Jauh — Gunakan fitur yang meluncurkan aplikasi klien.
  - Lihat Halaman — Lihat halaman di situs web.
- Memeriksa setiap dokumen unik di dalam SharePoint dan di seluruh sumber data lain yang Anda rencanakan untuk digunakan untuk indeks yang sama. Setiap sumber data yang ingin Anda gunakan untuk indeks tidak boleh berisi dokumen yang sama di seluruh sumber data. ID dokumen bersifat global untuk indeks dan harus unik per indeks.

Di dalam Anda Akun AWS, pastikan Anda memiliki:

- Membuat Amazon Kendra indeks dan, jika menggunakan API, mencatat ID indeks.
- Membuat IAM peran untuk sumber data Anda dan, jika menggunakan API, catat ARN peran tersebut IAM .

> **Note**
>
> Jika Anda mengubah jenis otentikasi dan kredensyal, Anda harus memperbarui IAM peran Anda untuk mengakses ID rahasia yang benar AWS Secrets Manager .

- Menyimpan kredensyal SharePoint otentikasi Anda AWS Secrets Manager secara rahasia dan, jika menggunakan API, catat ARN rahasia tersebut.

> **Note**
>
> Kami menyarankan Anda secara teratur menyegarkan atau memutar kredensyal dan rahasia Anda. Berikan hanya tingkat akses yang diperlukan untuk keamanan Anda sendiri. Kami tidak menyarankan Anda menggunakan kembali kredensyal dan rahasia di seluruh sumber data, dan konektor versi 1.0 dan 2.0 (jika berlaku).

Jika Anda tidak memiliki IAM peran atau rahasia yang ada, Anda dapat menggunakan konsol untuk membuat IAM peran dan Secrets Manager rahasia baru saat Anda menghubungkan sumber SharePoint data Anda Amazon Kendra. Jika Anda menggunakan API, Anda harus memberikan ARN IAM peran dan Secrets Manager rahasia yang ada, dan ID indeks.

Instruksi koneksi

Untuk terhubung Amazon Kendra ke sumber SharePoint data Anda, Anda harus memberikan rincian SharePoint kredensyal Anda sehingga Amazon Kendra dapat mengakses data Anda. Jika Anda belum mengkonfigurasi SharePoint untuk Amazon Kendra lihatPrasyarat.

Console

Untuk terhubung Amazon Kendra ke SharePoint

1. Masuk ke Konsol AWS Manajemen dan buka Amazon Kendra konsol.
2. Dari panel navigasi kiri, pilih Indeks dan kemudian pilih indeks yang ingin Anda gunakan dari daftar indeks.

> **Note**
>
> Anda dapat memilih untuk mengonfigurasi atau mengedit pengaturan kontrol akses Pengguna Anda di bawah Pengaturan indeks.

3. Pada halaman Memulai, pilih Tambahkan sumber data.
4. Pada halaman Tambahkan sumber data, pilih SharePoint konektor v1.0, lalu pilih Tambahkan sumber data.
5. Pada halaman Tentukan detail sumber data, masukkan informasi berikut:
   a. Dalam Nama dan deskripsi, untuk Nama sumber data —Masukkan nama untuk sumber data Anda. Anda dapat memasukkan tanda hubung tetapi bukan spasi.
   b. (Opsional) Deskripsi —Masukkan deskripsi opsional untuk sumber data Anda.
   c. Dalam Bahasa default —Pilih bahasa untuk memfilter dokumen Anda untuk indeks. Kecuali Anda menentukan sebaliknya, bahasa default ke bahasa Inggris. Bahasa yang ditentukan dalam metadata dokumen mengesampingkan bahasa yang dipilih.
   d. Di Tag, untuk Tambahkan tag baru —Sertakan tag opsional untuk mencari dan memfilter sumber daya Anda atau melacak AWS biaya Anda.
   e. Pilih Berikutnya.
6. Pada halaman Tentukan akses dan keamanan, masukkan informasi berikut:
   a. Untuk metode Hosting —Pilih antara SharePoint Online dan SharePointServer.
      i. Untuk SharePointOnline —Masukkan URL Situs khusus untuk repositori Anda SharePoint.
      ii. Untuk SharePointServer —Pilih SharePoint versi Anda, masukkan URL Situs khusus untuk SharePoint repositori Anda, dan masukkan Amazon S3 jalur ke lokasi sertifikat SSL Anda.
   b. (Hanya SharePoint server) Untuk proxy Web —Masukkan nama Host dan nomor Port SharePoint instans internal Anda. Nomor port harus berupa nilai numerik antara 0 dan 65535.
   c. Untuk Otentikasi —Pilih di antara opsi berikut berdasarkan kasus penggunaan Anda:
      i. Untuk SharePoint Online—Pilih antara otentikasi Dasar dan otentikasi OAuth 2.0.
      ii. Untuk SharePoint Server—Pilih antara None, LDAP, dan Manual.

d. Untuk AWS Secrets Manager rahasia —Pilih rahasia yang ada atau buat Secrets Manager rahasia baru untuk menyimpan kredensyal SharePoint otentikasi Anda. Jika Anda memilih untuk membuat rahasia baru, jendela AWS Secrets Manager rahasia terbuka. Anda harus memasukkan nama Rahasia. Awalan 'AmazonKendra- SharePoint -' secara otomatis ditambahkan ke nama rahasia Anda.

e. Masukkan informasi lain berikut di jendela Buat AWS Secrets Manager rahasia:

   i. Pilih dari opsi otentikasi SharePoint Cloud berikut, berdasarkan kasus penggunaan Anda:

      A. Otentikasi dasar —Masukkan nama pengguna SharePoint akun Anda sebagai Nama pengguna dan kata sandi SharePoint akun sebagai Kata Sandi.

      B. Otentikasi OAuth 2.0 —Masukkan nama pengguna SharePoint akun Anda sebagai Nama pengguna, kata sandi SharePoint akun sebagai Kata Sandi, SharePoint ID unik yang dibuat secara otomatis sebagai ID Klien, dan string rahasia bersama yang digunakan oleh keduanya SharePoint dan sebagai rahasia Klien. Amazon Kendra

   ii. Pilih dari opsi otentikasi SharePoint Server berikut, berdasarkan kasus penggunaan Anda:

      A. Tidak ada —Masukkan nama pengguna SharePoint akun Anda sebagai Nama pengguna, kata sandi SharePoint akun Anda sebagai Kata Sandi, dan Nama Domain Server Anda.

      B. LDAP ***—Masukkan nama pengguna SharePoint akun Anda sebagai Nama pengguna, kata sandi SharePoint akun sebagai Kata Sandi, Titik Akhir Server LDAP Anda (termasuk protokol dan nomor port, misalnya ldap: //example.com:389), dan Basis Pencarian LDAP Anda (misalnya, dc = contoh, dc = com).***

      C. Manual —Masukkan nama pengguna SharePoint akun Anda sebagai Nama pengguna, kata sandi SharePoint akun Anda sebagai Kata Sandi, dan Penggantian Domain Email Anda (domain email pengguna atau grup direktori).

   iii. Pilih Simpan.

f. Virtual Private Cloud (VPC) — Anda juga harus menambahkan Subnet dan grup keamanan VPC.

> **Note**
>
> Anda harus menggunakan VPC jika Anda menggunakan SharePoint Server. Amazon VPC adalah opsional untuk SharePoint versi lain.

g. IAM peran —Pilih peran yang sudah ada atau buat IAM IAM peran baru untuk mengakses kredensi repositori dan mengindeks konten Anda.

> **Note**
>
> IAM peran yang digunakan untuk indeks tidak dapat digunakan untuk sumber data. Jika Anda tidak yakin apakah peran yang ada digunakan untuk indeks atau FAQ, pilih Buat peran baru untuk menghindari kesalahan.

h. Pilih Berikutnya.

7. Pada halaman Konfigurasi pengaturan sinkronisasi, masukkan informasi berikut:

   a. Gunakan Ubah log —Pilih untuk memperbarui indeks Anda alih-alih menyinkronkan semua file Anda.

   b. Lampiran perayapan —Pilih untuk merayapi lampiran.

   c. Gunakan pemetaan grup lokal —Pilih untuk memastikan bahwa dokumen difilter dengan benar.

   d. Konfigurasi tambahan —Tambahkan pola ekspresi reguler untuk menyertakan atau mengecualikan file tertentu. Anda dapat menambahkan hingga 100 pola.

   e. Di Sync menjalankan jadwal untuk Frekuensi —Seberapa sering Amazon Kendra akan disinkronkan dengan sumber data Anda.

   f. Pilih Berikutnya.

8. Pada halaman Setel pemetaan bidang, masukkan informasi berikut:

   a. Amazon Kendra pemetaan bidang default —Pilih dari bidang sumber data default Amazon Kendra yang dihasilkan yang ingin Anda petakan ke indeks Anda.

   b. Untuk pemetaan bidang Kustom —Tambahkan bidang sumber data khusus untuk membuat nama bidang indeks untuk dipetakan dan tipe data bidang.

   c. Pilih Berikutnya.

9. Pada halaman Tinjau dan buat, periksa apakah informasi yang Anda masukkan sudah benar dan kemudian pilih Tambahkan sumber data. Anda juga dapat memilih untuk mengedit informasi Anda dari halaman ini. Sumber data Anda akan muncul di halaman Sumber data setelah sumber data berhasil ditambahkan.

API

Untuk terhubung Amazon Kendra ke SharePoint

Anda harus menentukan yang berikut menggunakan SharePointConfigurationAPI:

- SharePointVersi —Tentukan SharePoint versi yang Anda gunakan saat mengonfigurasi SharePoint. Ini adalah kasus tidak masalah jika Anda menggunakan SharePoint Server 2013, SharePoint Server 2016, SharePoint Server 2019, atau SharePoint Online.
- Rahasia Nama Sumber Daya Amazon (ARN) —Berikan Nama Sumber Daya Amazon (ARN) Secrets Manager rahasia yang berisi kredensyal otentikasi yang Anda buat di SharePoint akun Anda.Rahasia disimpan dalam struktur JSON.

  Untuk otentikasi dasar SharePoint Online, berikut ini adalah struktur JSON minimum yang harus ada dalam rahasia Anda:

```
{
    "userName": "user name",
    "password": "password"
}
```

  Untuk otentikasi OAuth 2.0 SharePoint Online, berikut ini adalah struktur JSON minimum yang harus ada dalam rahasia Anda:

```
{
    "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"
}
```

  Untuk otentikasi dasar SharePoint Server, berikut ini adalah struktur JSON minimum yang harus ada dalam rahasia Anda:

```
{
    "userName": "user name",
    "password": "password",
    "domain": "server domain name"
}
```

Untuk otentikasi SharePoint Server LDAP (jika Anda perlu mengonversi daftar kontrol akses (ACL) ke format email untuk pemfilteran pada konteks pengguna, Anda dapat menyertakan URL server LDAP dan basis pencarian LDAP dalam rahasia Anda), berikut ini adalah struktur JSON minimum yang harus ada dalam rahasia Anda:

```
{
    "userName": "user name",
    "password": "password",
    "domain": "server domain name"
    "ldapServerUrl": "ldap://example.com:389",
    "ldapSearchBase": "dc=example,dc=com"
}
```

Untuk otentikasi SharePoint Server Manual, berikut ini adalah struktur JSON minimum yang harus ada dalam rahasia Anda:

```
{
    "userName": "user name",
    "password": "password",
    "domain": "server domain name",
    "emailDomainOverride": "example.com"
}
```

> **Note**
>
> Kami menyarankan Anda secara teratur menyegarkan atau memutar kredensyal dan rahasia Anda. Berikan hanya tingkat akses yang diperlukan untuk keamanan Anda sendiri. Kami tidak menyarankan Anda menggunakan kembali kredensyal dan rahasia di seluruh sumber data, dan konektor versi 1.0 dan 2.0 (jika berlaku).

- IAM peran —Tentukan `RoleArn` kapan Anda menelepon `CreateDataSource` untuk memberikan IAM peran dengan izin untuk mengakses Secrets Manager rahasia Anda dan

memanggil API publik yang diperlukan untuk SharePoint konektor dan. Amazon Kendra Untuk informasi selengkapnya, lihat IAM peran untuk sumber SharePoint data.

- Amazon VPC—Jika Anda menggunakan SharePoint Server, tentukan `VpcConfiguration` sebagai bagian dari konfigurasi sumber data. Lihat Mengkonfigurasi Amazon Kendra untuk menggunakan VPC.

Anda juga dapat menambahkan fitur opsional berikut:

- Web proxy —Apakah akan terhubung ke URL SharePoint situs Anda melalui proxy web. Anda dapat menggunakan opsi ini hanya untuk SharePoint Server.
- Daftar pengindeksan —Apakah Amazon Kendra harus mengindeks isi lampiran ke SharePoint daftar item.
- Ubah log —Apakah Amazon Kendra harus menggunakan mekanisme log perubahan sumber SharePoint data untuk menentukan apakah dokumen harus diperbarui dalam indeks.

> **Note**
>
> Gunakan log perubahan jika Anda tidak Amazon Kendra ingin memindai semua dokumen. Jika log perubahan Anda besar, mungkin perlu waktu Amazon Kendra lebih sedikit untuk memindai dokumen di sumber SharePoint data daripada memproses log perubahan. Jika Anda menyinkronkan sumber SharePoint data Anda dengan indeks Anda untuk pertama kalinya, semua dokumen dipindai.

- Filter inklusi dan pengecualian —Anda dapat menentukan apakah akan menyertakan atau mengecualikan konten tertentu.

> **Note**
>
> Sebagian besar sumber data menggunakan pola ekspresi reguler, yang merupakan pola inklusi atau pengecualian yang disebut sebagai filter. Jika Anda menentukan filter inklusi, hanya konten yang cocok dengan filter inklusi yang diindeks. Dokumen apa pun yang tidak cocok dengan filter inklusi tidak diindeks. Jika Anda menentukan filter inklusi dan pengecualian, dokumen yang cocok dengan filter pengecualian tidak akan diindeks, meskipun sesuai dengan filter inklusi.

- Pemetaan bidang —Pilih untuk memetakan bidang sumber SharePoint data Anda ke bidang indeks Anda Amazon Kendra . Untuk informasi lebih lanjut, lihat Memetakan bidang sumber data.

  > **Note**
  >
  > Bidang badan dokumen atau badan dokumen yang setara untuk dokumen Anda diperlukan Amazon Kendra untuk mencari dokumen Anda. Anda harus memetakan nama bidang badan dokumen Anda di sumber data Anda ke nama bidang indeks_`document_body`. Semua kolom lain bersifat opsional.

- Pemfilteran konteks pengguna dan kontrol akses —Amazon Kendra meng-crawl daftar kontrol akses (ACL) untuk dokumen Anda, jika Anda memiliki ACL untuk dokumen Anda. Informasi ACL digunakan untuk memfilter hasil pencarian berdasarkan pengguna atau akses grup mereka ke dokumen. Untuk informasi selengkapnya, lihat Pemfilteran konteks pengguna.

Pelajari selengkapnya

Untuk mempelajari lebih lanjut tentang mengintegrasikan Amazon Kendra dengan sumber SharePoint data Anda, lihat:

- Memulai dengan konektor Amazon Kendra SharePoint Online

SharePoint konektor V2.0

SharePoint adalah layanan pembuatan situs web kolaboratif yang dapat Anda gunakan untuk menyesuaikan konten web dan membuat halaman, situs, pustaka dokumen, dan daftar. Anda dapat menggunakan Amazon Kendra untuk mengindeks sumber SharePoint data Anda.

Amazon Kendra saat ini mendukung SharePoint Online dan SharePoint Server (2013, 2016, 2019, dan Edisi Berlangganan).

> **Note**
>
> Support untuk SharePoint konektor V1.0/ SharePointConfiguration API dijadwalkan berakhir pada tahun 2023. Kami merekomendasikan migrasi ke atau menggunakan SharePoint konektor V2.0/ TemplateConfiguration API.

Untuk memecahkan masalah konektor sumber Amazon Kendra SharePoint data Anda, lihat. Mengatasi masalah sumber data

Topik

Fitur yang didukung

Amazon Kendra SharePoint konektor sumber data mendukung fitur-fitur berikut:

- Pemetaan lapangan
- Pemfilteran konteks pengguna
- Perayapan identitas pengguna
- Pola inklusi/pengecualian
- Sinkronisasi konten penuh dan tambahan
- Cloud privat virtual (VPC)

Prasyarat

Sebelum dapat digunakan Amazon Kendra untuk mengindeks sumber SharePoint data Anda, buat perubahan ini di akun SharePoint dan AWS akun Anda.

Di SharePoint Online, pastikan Anda memiliki:

- Menyalin URL SharePoint instans Anda. Format untuk URL host yang Anda masukkan adalah *`https://yourdomain.sharepoint.com/sites/mysite`*. URL Anda harus dimulai dengan `https` dan berisi`sharepoint.com`.
- Menyalin nama domain URL SharePoint instans Anda.
- Mencatat kredensyal otentikasi dasar Anda yang berisi nama pengguna dan kata sandi dengan izin admin situs untuk terhubung ke Online. SharePoint
- Default Keamanan Dinonaktifkan di portal Azure Anda menggunakan pengguna administratif. Untuk informasi selengkapnya tentang mengelola setelan default keamanan di portal Azure, lihat dokumentasi Microsoft tentang cara mengaktifkan/menonaktifkan default keamanan.

- Otentikasi multi-faktor (MFA) yang dinonaktifkan di SharePoint akun Anda, sehingga tidak diblokir untuk Amazon Kendra merayapi konten Anda. SharePoint
- Jika menggunakan jenis otentikasi selain otentikasi Dasar: Menyalin ID penyewa instans Anda. SharePoint Untuk detail tentang cara menemukan ID penyewa, lihat Menemukan ID penyewa Microsoft 365 Anda.
- Jika Anda perlu bermigrasi ke otentikasi pengguna cloud dengan Microsoft Entra, lihat dokumentasi Microsoft tentang otentikasi cloud.
- Untuk otentikasi OAuth 2.0 dan otentikasi token penyegaran OAuth 2.0: Mencatat kredensi otentikasi Dasar Anda yang berisi nama pengguna dan kata sandi yang Anda gunakan untuk terhubung ke SharePoint Online dan ID klien serta rahasia klien yang dihasilkan setelah mendaftar dengan Azure AD. SharePoint
  - Jika Anda tidak menggunakan ACL, tambahkan izin berikut:

Grafik Microsoft	SharePoint
• Catatan.Read.All (Aplikasi) —Baca semua notebook OneNote • Sites.Read.All (Aplikasi) —Baca item di semua koleksi situs	• AllSites.Baca (Delegasi) —Baca item di semua koleksi situs

> **Note**
>
> Catatan.Read.All dan Sites.Read.All hanya diperlukan jika Anda ingin merayapi Dokumen. OneNote
> Jika Anda ingin merayapi situs tertentu, izin dapat dibatasi untuk situs tertentu daripada semua situs yang tersedia di domain. Anda mengonfigurasi izin Sites.Selected (Aplikasi). Dengan izin API ini, Anda perlu mengatur izin akses di setiap situs secara eksplisit melalui Microsoft Graph API. Untuk informasi selengkapnya, lihat blog Microsoft di Situs. Izin yang dipilih.

  - Jika Anda menggunakan ACL, tambahkan izin berikut:

Grafik Microsoft	SharePoint
• Group.Member.Read.All (Aplikasi) —Baca semua keanggotaan grup • Catatan.Read.All (Aplikasi) —Baca semua notebook OneNote • Situs. FullControl.All (Delegated) — Diperlukan untuk mengambil ACL dokumen • Sites.Read.All (Aplikasi) —Baca item di semua koleksi situs • User.Read.All (Aplikasi) —Baca profil lengkap semua pengguna	• AllSites.Baca (Delegasi) —Baca item di semua koleksi situs

> **Note**
>
> GroupMember.Read.All dan User.Read.All hanya diperlukan jika crawler Identity diaktifkan.
> Jika Anda ingin merayapi situs tertentu, izin dapat dibatasi untuk situs tertentu daripada semua situs yang tersedia di domain. Anda mengonfigurasi izin Sites.Selected (Aplikasi). Dengan izin API ini, Anda perlu mengatur izin akses di setiap situs secara eksplisit melalui Microsoft Graph API. Untuk informasi selengkapnya, lihat blog Microsoft di Situs. Izin yang dipilih.

- Untuk otentikasi Khusus Aplikasi Azure AD: Kunci pribadi dan ID Klien yang Anda buat setelah mendaftar SharePoint dengan Azure AD. Perhatikan juga sertifikat X.509.
  - Jika Anda tidak menggunakan ACL, tambahkan izin berikut:

SharePoint
• Sites.Read.All (Aplikasi) —Diperlukan untuk mengakses item dan daftar di semua koleksi situs

> **Note**
>
> Jika Anda ingin merayapi situs tertentu, izin dapat dibatasi untuk situs tertentu daripada semua situs yang tersedia di domain. Anda mengonfigurasi izin Sites.Selected (Aplikasi). Dengan izin API ini, Anda perlu mengatur izin akses di setiap situs secara eksplisit melalui Microsoft Graph API. Untuk informasi selengkapnya, lihat blog Microsoft di Situs. Izin yang dipilih.

- Jika Anda menggunakan ACL, tambahkan izin berikut:

SharePoint
• Situs. FullControl.All (Application) — Diperlukan untuk mengambil ACL dokumen

> **Note**
>
> Jika Anda ingin merayapi situs tertentu, izin dapat dibatasi untuk situs tertentu daripada semua situs yang tersedia di domain. Anda mengonfigurasi izin Sites.Selected (Aplikasi). Dengan izin API ini, Anda perlu mengatur izin akses di setiap situs secara eksplisit melalui Microsoft Graph API. Untuk informasi selengkapnya, lihat blog Microsoft di Situs. Izin yang dipilih.

- Untuk autentikasi SharePoint App-Only: SharePoint Mencatat ID klien dan rahasia klien yang dihasilkan saat memberikan izin ke SharePoint App Only, dan ID Klien serta rahasia Klien Anda yang dihasilkan saat Anda mendaftarkan SharePoint aplikasi dengan Azure AD.

> **Note**
>
> SharePoint Otentikasi Khusus Aplikasi tidak didukung untuk SharePoint versi 2013.

- (Opsional) Jika Anda merayapi OneNote dokumen dan menggunakan crawler Identity, tambahkan izin berikut:

Grafik Microsoft
• GroupMember.Read.All (Aplikasi) —Baca semua keanggotaan grup • Catatan.Read.All (Aplikasi) —Baca semua notebook OneNote • Sites.Read.All (Aplikasi) —Baca item di semua koleksi situs • User.Read.All (Aplikasi) —Baca profil lengkap semua pengguna

> **Note**
>
> Tidak diperlukan izin API untuk merayapi entitas menggunakan otentikasi Dasar dan SharePoint otentikasi khusus aplikasi.

Di SharePoint Server, pastikan Anda memiliki:

- Menyalin URL SharePoint instans Anda dan nama domain URL Anda SharePoint . Format untuk URL host yang Anda masukkan adalah *`https://yourcompany/sites/mysite`*. URL Anda harus dimulai dengan`https`.

  > **Note**
  >
  > (On-premise/server) Amazon Kendra memeriksa apakah informasi titik akhir yang disertakan sama dengan informasi titik akhir yang AWS Secrets Manager ditentukan dalam detail konfigurasi sumber data Anda. Ini membantu melindungi dari masalah wakil yang membingungkan, yang merupakan masalah keamanan di mana pengguna tidak memiliki izin untuk melakukan tindakan tetapi menggunakan Amazon Kendra sebagai proxy untuk mengakses rahasia yang dikonfigurasi dan melakukan tindakan. Jika nanti Anda mengubah informasi titik akhir Anda, Anda harus membuat rahasia baru untuk menyinkronkan informasi ini.

- Otentikasi multi-faktor (MFA) yang dinonaktifkan di SharePoint akun Anda, sehingga tidak diblokir untuk Amazon Kendra merayapi konten Anda. SharePoint

- Jika menggunakan otentikasi SharePoint App-Only untuk kontrol akses:
  - Menyalin ID SharePoint klien yang dihasilkan saat Anda mendaftarkan App Only di Tingkat Situs. Format ID klien adalah ClientId @TenantId. Misalnya, *ffa956f3-8f89-44e7-b0e4-49670756342c @888d0b57 -69f1-4fb8-957f-e1f0bedf82fe*.
  - Menyalin rahasia SharePoint klien yang dihasilkan saat Anda mendaftarkan App Only di Tingkat Situs.

  Catatan: Karena ID klien dan rahasia klien dibuat untuk satu situs hanya ketika Anda mendaftarkan otentikasi SharePoint Server untuk App Only, hanya satu URL situs yang didukung untuk otentikasi SharePoint App Only.

  > **Note**
  >
  > SharePoint Otentikasi Khusus Aplikasi tidak didukung untuk SharePoint versi 2013.

- Jika menggunakan ID Email dengan Domain Kustom untuk kontrol akses:
  - *Mencatat nilai domain email kustom Anda—misalnya: "amazon.com".*
- Jika menggunakan ID Email dengan Domain dari otorisasi IDP, salin:
  - LDAP Server Endpoint (titik akhir server LDAP termasuk protokol dan nomor port). Misalnya: *ldap: //example.com:389*.
  - Basis Pencarian LDAP (basis pencarian pengguna LDAP). Misalnya: *CN = Users, DC = SharePoint, DC = COM*.
  - Nama pengguna LDAP dan kata sandi LDAP.
- Baik kredensyal otentikasi NTLM yang dikonfigurasi atau kredensyal otentikasi Kerberos yang dikonfigurasi yang berisi nama pengguna (nama pengguna akun) dan kata sandi (SharePoint kata sandi akun). SharePoint

Di dalam Anda Akun AWS, pastikan Anda memiliki:

- Membuat Amazon Kendra indeks dan, jika menggunakan API, mencatat ID indeks.
- Membuat IAM peran untuk sumber data Anda dan, jika menggunakan API, catat ARN peran tersebut IAM .

> **Note**
>
> Jika Anda mengubah jenis otentikasi dan kredensyal, Anda harus memperbarui IAM peran Anda untuk mengakses ID rahasia yang benar AWS Secrets Manager .

- Menyimpan kredensyal SharePoint otentikasi Anda AWS Secrets Manager secara rahasia dan, jika menggunakan API, catat ARN rahasia tersebut.

> **Note**
>
> Kami menyarankan Anda secara teratur menyegarkan atau memutar kredensyal dan rahasia Anda. Berikan hanya tingkat akses yang diperlukan untuk keamanan Anda sendiri. Kami tidak menyarankan Anda menggunakan kembali kredensyal dan rahasia di seluruh sumber data, dan konektor versi 1.0 dan 2.0 (jika berlaku).

Jika Anda tidak memiliki IAM peran atau rahasia yang ada, Anda dapat menggunakan konsol untuk membuat IAM peran dan Secrets Manager rahasia baru saat Anda menghubungkan sumber SharePoint data Anda Amazon Kendra. Jika Anda menggunakan API, Anda harus memberikan ARN IAM peran dan Secrets Manager rahasia yang ada, dan ID indeks.

Instruksi koneksi

Untuk terhubung Amazon Kendra ke sumber SharePoint data Anda, Anda harus memberikan rincian SharePoint kredensyal Anda sehingga Amazon Kendra dapat mengakses data Anda. Jika Anda belum mengkonfigurasi SharePoint untuk Amazon Kendra lihatPrasyarat.

Console: SharePoint Online

Untuk terhubung Amazon Kendra ke SharePoint Online

1. Masuk ke Konsol AWS Manajemen dan buka Amazon Kendra konsol.
2. Dari panel navigasi kiri, pilih Indeks dan kemudian pilih indeks yang ingin Anda gunakan dari daftar indeks.

> **Note**
>
> Anda dapat memilih untuk mengonfigurasi atau mengedit pengaturan kontrol akses Pengguna Anda di bawah Pengaturan indeks.

3. Pada halaman Memulai, pilih Tambahkan sumber data.
4. Pada halaman Tambahkan sumber data, pilih SharePoint konektor V2.0, lalu pilih Tambahkan sumber data.
5. Pada halaman Tentukan detail sumber data, masukkan informasi berikut:
   a. Dalam Nama dan deskripsi, untuk Nama sumber data —Masukkan nama untuk sumber data Anda. Anda dapat memasukkan tanda hubung tetapi bukan spasi.
   b. (Opsional) Deskripsi —Masukkan deskripsi opsional untuk sumber data Anda.
   c. Dalam Bahasa default —Pilih bahasa untuk memfilter dokumen Anda untuk indeks. Kecuali Anda menentukan sebaliknya, bahasa default ke bahasa Inggris. Bahasa yang ditentukan dalam metadata dokumen mengesampingkan bahasa yang dipilih.
   d. Di Tag, untuk Tambahkan tag baru —Sertakan tag opsional untuk mencari dan memfilter sumber daya Anda atau melacak AWS biaya Anda.
   e. Pilih Berikutnya.
6. Pada halaman Tentukan akses dan keamanan, masukkan informasi berikut:
   a. Di Sumber, untuk Metode Hosting —Pilih SharePointOnline.
   b. URL situs khusus untuk SharePoint repositori Anda —Masukkan URL host. SharePoint Format untuk URL host yang Anda masukkan adalah *`https://yourdomain.sharepoint.com/sites/mysite.`* URL harus dimulai dengan `https` protokol. Pisahkan URL dengan baris baru. Anda dapat menambahkan hingga 100 URL.
   c. Domain —Masukkan SharePoint domain. Misalnya, domain di URL *`https://yourdomain.sharepoint.com/sites/mysite`* adalah *`yourdomain`*.
   d. Untuk Otorisasi, Anda dapat memilih dari opsi ACL berikut:
      - Nama utama pengguna — Kontrol akses akan didasarkan pada nama utama Pengguna yang diambil dari Azure Portal.
      - Email - Kontrol akses akan didasarkan pada id email yang diambil dari Azure Portal.

> **Note**
>
> Jika Anda tidak menentukan nilai, Email dianggap sebagai nilai default.

e. Untuk Otentikasi, pilih antara otentikasi Dasar, OAuth 2.0, Azure AD App-Only, otentikasi App-Only, dan otentikasi SharePoint token refresh OAuth 2.0 berdasarkan kasus penggunaan Anda.

   i. Jika menggunakan Basic Authentication, masukkan informasi berikut:

   - Untuk AWS Secrets Manager rahasia —Pilih rahasia yang ada atau buat Secrets Manager rahasia baru untuk menyimpan kredensyal SharePoint otentikasi Anda. Jika Anda memilih untuk membuat rahasia baru, jendela AWS Secrets Manager rahasia terbuka. Masukkan informasi berikut di jendela:
     - Nama rahasia —Nama untuk rahasiamu. Awalan 'AmazonKendra- SharePoint -' secara otomatis ditambahkan ke nama rahasia Anda.
     - Nama pengguna —Nama pengguna untuk SharePoint akun Anda.
     - Kata sandi —Kata sandi untuk SharePoint akun Anda.

   ii. Jika menggunakan otentikasi OAuth 2.0, masukkan informasi berikut:

   - ID Penyewa —ID Penyewa akun Anda. SharePoint
   - Untuk AWS Secrets Manager rahasia —Pilih rahasia yang ada atau buat Secrets Manager rahasia baru untuk menyimpan kredensyal SharePoint otentikasi Anda. Jika Anda memilih untuk membuat rahasia baru, jendela AWS Secrets Manager rahasia terbuka. Masukkan informasi berikut di jendela:
     - Nama rahasia —Nama untuk rahasiamu. Awalan 'AmazonKendra- SharePoint -' secara otomatis ditambahkan ke nama rahasia Anda.
     - Nama pengguna —Nama pengguna untuk SharePoint akun Anda.
     - Kata sandi —Kata sandi untuk SharePoint akun Anda.
     - ID Klien —ID klien Azure AD dihasilkan saat Anda mendaftar SharePoint di Azure AD.
     - Rahasia klien —Rahasia klien Azure AD dihasilkan saat Anda mendaftar SharePoint di Azure AD.

   iii. Jika menggunakan autentikasi Azure AD App-Only, masukkan informasi berikut:

- ID Penyewa —ID Penyewa akun Anda. SharePoint
- Sertifikat X.509 yang ditandatangani sendiri Azure AD —Sertifikat untuk mengautentikasi konektor Azure AD.
- Untuk AWS Secrets Manager rahasia —Pilih rahasia yang ada atau buat Secrets Manager rahasia baru untuk menyimpan kredensyal SharePoint otentikasi Anda. Jika Anda memilih untuk membuat rahasia baru, jendela AWS Secrets Manager rahasia terbuka. Masukkan informasi berikut di jendela:
  - Nama rahasia —Nama untuk rahasiamu. Awalan 'AmazonKendra- SharePoint -' secara otomatis ditambahkan ke nama rahasia Anda.
  - ID Klien —ID klien Azure AD dihasilkan saat Anda mendaftar SharePoint di Azure AD.
  - Kunci pribadi —Kunci pribadi untuk mengautentikasi konektor untuk Azure AD.

iv. Jika menggunakan otentikasi SharePoint App-Only, masukkan informasi berikut:

- ID Penyewa —ID Penyewa akun Anda. SharePoint
- Untuk AWS Secrets Manager rahasia —Pilih rahasia yang ada atau buat Secrets Manager rahasia baru untuk menyimpan kredensyal SharePoint otentikasi Anda. Jika Anda memilih untuk membuat rahasia baru, jendela AWS Secrets Manager rahasia terbuka. Masukkan informasi berikut di jendela:
  - Nama rahasia —Nama untuk rahasiamu. Awalan 'AmazonKendra- SharePoint -' secara otomatis ditambahkan ke nama rahasia Anda.
  - SharePoint ID klien —ID SharePoint klien yang Anda buat saat Anda mendaftarkan App Only di Level Penyewa. *Format clientID adalah clientId@. TenantId* Misalnya, *ffa956f3-8f89-44e7-b0e4-49670756342c @888d0b57 -69f1-4fb8-957f-e1f0bedf82fe*.
  - SharePoint rahasia klien —Rahasia SharePoint klien dihasilkan saat Anda mendaftar untuk App Only di Level Penyewa.
  - ID Klien —ID klien Azure AD dihasilkan saat Anda mendaftar SharePoint di Azure AD.
  - Rahasia klien —Rahasia klien Azure AD dihasilkan saat Anda mendaftar SharePoint ke Azure AD.

v. Jika menggunakan otentikasi token refresh OAuth 2.0, masukkan informasi berikut:

- ID Penyewa —ID Penyewa akun Anda. SharePoint

- Untuk AWS Secrets Manager rahasia —Pilih rahasia yang ada atau buat Secrets Manager rahasia baru untuk menyimpan kredensyal SharePoint otentikasi Anda. Jika Anda memilih untuk membuat rahasia baru, jendela AWS Secrets Manager rahasia terbuka. Masukkan informasi berikut di jendela:
  - Nama rahasia —Nama untuk rahasiamu. Awalan 'AmazonKendra- SharePoint -' secara otomatis ditambahkan ke nama rahasia Anda.
  - ID Klien —ID klien Azure AD unik yang dihasilkan saat Anda mendaftar SharePoint di Azure AD.
  - Rahasia klien —Rahasia klien Azure AD dihasilkan saat Anda mendaftar SharePoint ke Azure AD.
  - Refresh token —Token penyegaran yang dihasilkan Amazon Kendra untuk SharePoint terhubung.

f. Perayap identitas - (Diaktifkan hanya ketika ACL diaktifkan) Pilih untuk mengaktifkan crawler Amazon Kendra identitas untuk menyinkronkan informasi identitas. Jika Anda memilih untuk menonaktifkan crawler identitas, Anda harus mengunggah informasi utama menggunakan PutPrincipalMappingAPI.

   Anda juga dapat memilih untuk:

   i. Crawl Local Group Mapping —Aktifkan untuk merayapi pemetaan grup lokal.

   ii. Crawl AD Group Mapping —Aktifkan untuk merayapi pemetaan grup Azure Active Directory.

   > **Note**
   >
   > Perayapan pemetaan Grup AD hanya tersedia untuk OAuth 2.0, token penyegaran OAuth 2.0, dan otentikasi App Only. SharePoint

g. (Opsional) Konfigurasikan VPC dan grup keamanan —Pilih VPC yang akan digunakan dengan instans Anda. SharePoint Jika demikian, Anda harus menambahkan Subnet dan grup keamanan VPC.

h. IAM peran —Pilih peran yang sudah ada atau buat IAM IAM peran baru untuk mengakses kredensi repositori dan mengindeks konten Anda.

> **Note**
>
> IAM peran yang digunakan untuk indeks tidak dapat digunakan untuk sumber data. Jika Anda tidak yakin apakah peran yang ada digunakan untuk indeks atau FAQ, pilih Buat peran baru untuk menghindari kesalahan.

i. Pilih Berikutnya.

7. Pada halaman Konfigurasi pengaturan sinkronisasi, masukkan informasi berikut:

   a. Dalam lingkup Sinkronisasi, pilih dari opsi berikut:

      i. Pilih entitas —Pilih entitas yang ingin dirayapi. Anda dapat memilih untuk meng-crawl Semua entitas atau kombinasi File, Lampiran, Halaman Tautan, Acara, Komentar, dan Data Daftar.

      ii. Dalam konfigurasi Tambahan, untuk pola regex Entitas —Tambahkan pola ekspresi reguler untuk Tautan, Halaman, dan Acara untuk menyertakan entitas tertentu alih-alih menyinkronkan semua dokumen Anda.

      iii. Pola Regex —Tambahkan pola ekspresi reguler untuk menyertakan atau mengecualikan file berdasarkan jalur File, Nama file, Jenis file, nama OneNote bagian, dan nama OneNote halaman alih-alih menyinkronkan semua dokumen Anda. Anda dapat menambahkan hingga 100.

      > **Note**
      >
      > OneNote crawling hanya tersedia untuk OAuth 2.0, token penyegaran OAuth 2.0, dan otentikasi App Only. SharePoint

   b. Untuk mode Sinkronisasi, pilih cara memperbarui indeks saat konten sumber data berubah. Saat Anda menyinkronkan sumber data Amazon Kendra untuk pertama kalinya, semua konten disinkronkan secara default.

      - Sinkronisasi penuh —Sinkronkan semua konten terlepas dari status sinkronisasi sebelumnya.
      - Sinkronisasi dokumen baru atau yang dimodifikasi —Sinkronkan hanya dokumen baru atau yang dimodifikasi.

- Sinkronisasi dokumen baru, dimodifikasi, atau dihapus —Sinkronkan hanya dokumen baru, dimodifikasi, dan dihapus.

c. Dalam jadwal berjalan Sinkronisasi, untuk Frekuensi —Seberapa sering Amazon Kendra akan disinkronkan dengan sumber data Anda.

d. Pilih Berikutnya.

8. Pada halaman Setel pemetaan bidang, masukkan informasi berikut:

a. Untuk Halaman Acara, File, Tautan, Lampiran, dan Komentar —Pilih dari bidang sumber data default yang Amazon Kendra dihasilkan yang ingin Anda petakan ke indeks Anda.

b. Tambahkan bidang —Untuk menambahkan bidang sumber data kustom untuk membuat nama bidang indeks untuk dipetakan dan tipe data bidang.

c. Pilih Berikutnya.

9. Pada halaman Tinjau dan buat, periksa apakah informasi yang Anda masukkan sudah benar dan kemudian pilih Tambahkan sumber data. Anda juga dapat memilih untuk mengedit informasi Anda dari halaman ini. Sumber data Anda akan muncul di halaman Sumber data setelah sumber data berhasil ditambahkan.

Console: SharePoint Server

Untuk terhubung Amazon Kendra ke SharePoint

1. Masuk ke Konsol AWS Manajemen dan buka Amazon Kendra konsol.
2. Dari panel navigasi kiri, pilih Indeks dan kemudian pilih indeks yang ingin Anda gunakan dari daftar indeks.

> **Note**
>
> Anda dapat memilih untuk mengonfigurasi atau mengedit pengaturan kontrol akses Pengguna Anda di bawah Pengaturan indeks.

3. Pada halaman Memulai, pilih Tambahkan sumber data.
4. Pada halaman Tambahkan sumber data, pilih SharePoint konektor V2.0, lalu pilih Tambahkan sumber data.
5. Pada halaman Tentukan detail sumber data, masukkan informasi berikut:

a. Dalam Nama dan deskripsi, untuk Nama sumber data —Masukkan nama untuk sumber data Anda. Anda dapat memasukkan tanda hubung tetapi bukan spasi.

b. (Opsional) Deskripsi —Masukkan deskripsi opsional untuk sumber data Anda.

c. Dalam Bahasa default —Pilih bahasa untuk memfilter dokumen Anda untuk indeks. Kecuali Anda menentukan sebaliknya, bahasa default ke bahasa Inggris. Bahasa yang ditentukan dalam metadata dokumen mengesampingkan bahasa yang dipilih.

d. Di Tag, untuk Tambahkan tag baru —Sertakan tag opsional untuk mencari dan memfilter sumber daya Anda atau melacak AWS biaya Anda.

e. Pilih Berikutnya.

6. Pada halaman Tentukan akses dan keamanan, masukkan informasi berikut:

a. Di Sumber, untuk Metode Hosting —Pilih SharePointServer.

b. Pilih SharePoint Versi —Pilih antara SharePoint 2013, SharePoint 2016, SharePoint 2019, dan SharePoint (Edisi Berlangganan).

c. URL situs khusus untuk SharePoint repositori Anda —Masukkan URL host. SharePoint Format untuk URL host yang Anda masukkan adalah *https://yourcompany/sites/mysite.* URL harus dimulai dengan `https` protokol. Pisahkan URL dengan baris baru. Anda dapat menambahkan hingga 100 URL.

d. Domain —Masukkan SharePoint domain. Misalnya, domain di URL *https://yourcompany/sites/mysite* adalah *perusahaanmu*

e. Lokasi sertifikat SSL —Masukkan Amazon S3 jalur ke file sertifikat SSL Anda.

f. (Opsional) Untuk proxy Web —Masukkan nama host (tanpa `https://` protokol `http://` atau), dan nomor port yang digunakan oleh protokol transport URL host. Nilai numerik nomor port harus antara 0 dan 65535.

g. Otorisasi — Aktifkan atau nonaktifkan informasi daftar kontrol akses (ACL) untuk dokumen Anda, jika Anda memiliki ACL dan ingin menggunakannya untuk kontrol akses. ACL menentukan dokumen mana yang dapat diakses pengguna dan grup. Informasi ACL digunakan untuk memfilter hasil pencarian berdasarkan pengguna atau akses grup mereka ke dokumen. Untuk informasi selengkapnya, lihat Pemfilteran konteks pengguna.

   Untuk SharePoint Server Anda dapat memilih dari opsi ACL berikut:

   i. ID Email dengan Domain dari IDP —Kontrol akses akan didasarkan pada id email yang diekstrak dari domain email yang diambil dari penyedia identitas dasar (IDP).

Anda memberikan detail koneksi IDP dalam Secrets Manager rahasia Anda selama Otentikasi.

ii. ID Email dengan Domain Kustom —Kontrol akses akan didasarkan pada ID email. Anda ingin memberikan nilai domain email. Misalnya, "*amazon.com*". Domain email akan digunakan untuk membangun ID email untuk kontrol akses. Anda harus memasukkan domain email Anda menggunakan Add Email Domain.

iii. Domain\ User dengan Domain —Kontrol akses akan disusun menggunakan format Domain\ User ID. Anda harus memberikan nama domain yang valid. Misalnya: *"sharepoint2019"* untuk membangun kontrol akses.

h. Untuk Otentikasi, pilih antara otentikasi SharePoint App-Only, otentikasi NTLM, dan otentikasi Kerberos berdasarkan kasus penggunaan Anda.

i. Masukkan informasi berikut untuk otentikasi NTLM dan otentikasi Kerberos:

Untuk AWS Secrets Manager rahasia —Pilih rahasia yang ada atau buat Secrets Manager rahasia baru untuk menyimpan kredensyal SharePoint otentikasi Anda. Jika Anda memilih untuk membuat rahasia baru, jendela AWS Secrets Manager rahasia terbuka. Masukkan informasi berikut di jendela:

- Nama rahasia —Nama untuk rahasiamu. Awalan 'AmazonKendra- SharePoint -' secara otomatis ditambahkan ke nama rahasia Anda.
- Nama pengguna —Nama pengguna untuk SharePoint akun Anda.
- Kata sandi —Kata sandi untuk SharePoint akun Anda.

Jika menggunakan ID Email dengan Domain dari IDP, masukkan juga:

- LDAP Server Endpoint — Endpoint dari server LDAP, termasuk protokol dan nomor port. Misalnya: *ldap: //example.com:389*.
- Basis Pencarian LDAP —Basis pencarian pengguna LDAP. Misalnya: *CN = Users, DC = SharePoint, DC = COM*.
- Nama pengguna LDAP —Nama pengguna LDAP Anda.
- Kata Sandi LDAP —Kata sandi LDAP Anda.

ii. Masukkan informasi berikut untuk otentikasi SharePoint App-Only.

Untuk AWS Secrets Manager rahasia —Pilih rahasia yang ada atau buat Secrets Manager rahasia baru untuk menyimpan kredensyal SharePoint otentikasi Anda.

Jika Anda memilih untuk membuat rahasia baru, jendela AWS Secrets Manager rahasia terbuka. Masukkan informasi berikut di jendela:

- Nama rahasia —Nama untuk rahasiamu. Awalan 'AmazonKendra- SharePoint -' secara otomatis ditambahkan ke nama rahasia Anda.
- ID Klien —ID SharePoint klien yang Anda buat saat Anda mendaftarkan App Only di Tingkat Situs. Format ClientID adalah clientId@. TenantId Misalnya, *ffa956f3-8f89-44e7-b0e4-49670756342c @888d0b57 -69f1-4fb8-957f-e1f0bedf82fe*.
- SharePoint rahasia klien —Rahasia SharePoint klien dihasilkan saat Anda mendaftar untuk Aplikasi Hanya di Tingkat Situs.

  Catatan: Karena ID klien dan rahasia klien dibuat untuk satu situs hanya ketika Anda mendaftarkan otentikasi SharePoint Server untuk App Only, hanya satu URL situs yang didukung untuk otentikasi SharePoint App Only.

Jika menggunakan ID Email dengan Domain dari IDP, masukkan juga:

- LDAP Server Endpoint — Endpoint dari server LDAP, termasuk protokol dan nomor port. Misalnya: *ldap: //example.com:389*.
- Basis Pencarian LDAP —Basis pencarian pengguna LDAP. Misalnya: *CN = Users, DC = SharePoint, DC = COM*.
- Nama pengguna LDAP —Nama pengguna LDAP Anda.
- Kata Sandi LDAP —Kata sandi LDAP Anda.

i. Perayap identitas —Tentukan apakah akan mengaktifkan crawler Amazon Kendra identitas. Perayap identitas menggunakan informasi daftar kontrol akses (ACL) untuk dokumen Anda untuk memfilter hasil penelusuran berdasarkan akses pengguna atau grup mereka ke dokumen. Jika Anda memiliki ACL untuk dokumen Anda dan memilih untuk menggunakan ACL Anda, Anda juga dapat memilih untuk mengaktifkan crawler Amazon Kendra identitas untuk mengonfigurasi pemfilteran konteks pengguna dari hasil pencarian. Jika tidak, jika crawler identitas dimatikan, semua dokumen dapat dicari secara publik. Jika Anda ingin menggunakan kontrol akses untuk dokumen dan crawler identitas dimatikan, Anda dapat menggunakan PutPrincipalMappingAPI untuk mengunggah informasi akses pengguna dan grup untuk pemfilteran konteks pengguna.

   i. Crawl Local Group Mapping —Aktifkan untuk merayapi pemetaan grup lokal.

ii. (Untuk ID Email dengan Domain dari IDP saja) Crawl AD Group Mapping —Aktifkan untuk merayapi pemetaan Direktori Aktif.

> **Note**
>
> Perayapan pemetaan Grup AD hanya tersedia autentikasi SharePoint App Only.

j. (Opsional) Konfigurasikan VPC dan grup keamanan —Pilih VPC yang akan digunakan dengan instans Anda. SharePoint Jika demikian, Anda harus menambahkan Subnet dan grup keamanan VPC.

k. IAM peran —Pilih peran yang sudah ada atau buat IAM IAM peran baru untuk mengakses kredensi repositori dan mengindeks konten Anda.

> **Note**
>
> IAM peran yang digunakan untuk indeks tidak dapat digunakan untuk sumber data. Jika Anda tidak yakin apakah peran yang ada digunakan untuk indeks atau FAQ, pilih Buat peran baru untuk menghindari kesalahan.

l. Pilih Berikutnya.

7. Pada halaman Konfigurasi pengaturan sinkronisasi, masukkan informasi berikut:

a. Dalam lingkup Sinkronisasi, pilih dari opsi berikut:

i. Pilih entitas —Pilih entitas yang ingin dirayapi. Anda dapat memilih untuk merayapi Semua entitas atau kombinasi File, Lampiran, Halaman Tautan, Acara, dan Data Daftar.

ii. Dalam konfigurasi Tambahan, untuk pola regex Entitas —Tambahkan pola ekspresi reguler untuk Tautan, Halaman, dan Acara untuk menyertakan entitas tertentu alih-alih menyinkronkan semua dokumen Anda.

iii. Pola Regex —Tambahkan pola ekspresi reguler untuk menyertakan atau mengecualikan file berdasarkan jalur File Nama file Jenis file, nama OneNote bagian, dan nama OneNote halaman alih-alih menyinkronkan semua dokumen Anda. Anda dapat menambahkan hingga 100.

> **Note**
>
> OneNote crawling hanya tersedia untuk otentikasi SharePoint App Only.

b. Mode sinkronisasi —Pilih cara memperbarui indeks saat konten sumber data berubah. Saat Anda menyinkronkan sumber data Amazon Kendra untuk pertama kalinya, semua konten dirayapi dan diindeks secara default. Anda harus menjalankan sinkronisasi penuh data Anda jika sinkronisasi awal Anda gagal, bahkan jika Anda tidak memilih sinkronisasi penuh sebagai opsi mode sinkronisasi Anda.

   - Sinkronisasi penuh: Indeks baru semua konten, ganti konten yang ada setiap kali sumber data Anda disinkronkan dengan indeks Anda.
   - Sinkronisasi baru yang dimodifikasi: Indeks hanya konten baru dan yang dimodifikasi setiap kali sumber data Anda disinkronkan dengan indeks Anda. Amazon Kendra dapat menggunakan mekanisme sumber data Anda untuk melacak perubahan konten dan mengindeks konten yang berubah sejak sinkronisasi terakhir.
   - Sinkronisasi baru, dimodifikasi, dihapus: Indeks hanya konten baru, dimodifikasi, dan dihapus setiap kali sumber data Anda disinkronkan dengan indeks Anda. Amazon Kendra dapat menggunakan mekanisme sumber data Anda untuk melacak perubahan konten dan mengindeks konten yang berubah sejak sinkronisasi terakhir.

c. Dalam jadwal berjalan Sinkronisasi, untuk Frekuensi —Seberapa sering Amazon Kendra akan disinkronkan dengan sumber data Anda.

d. Pilih Berikutnya.

8. Pada halaman Setel pemetaan bidang, masukkan informasi berikut:

   a. Untuk Halaman Acara, File, Tautan, Lampiran, dan Data Daftar —Pilih dari bidang sumber data default yang Amazon Kendra dihasilkan yang ingin Anda petakan ke indeks Anda.

   b. Tambahkan bidang —Untuk menambahkan bidang sumber data kustom untuk membuat nama bidang indeks untuk dipetakan dan tipe data bidang.

   c. Pilih Berikutnya.

9. Pada halaman Tinjau dan buat, periksa apakah informasi yang Anda masukkan sudah benar dan kemudian pilih Tambahkan sumber data. Anda juga dapat memilih untuk mengedit informasi Anda dari halaman ini. Sumber data Anda akan muncul di halaman Sumber data setelah sumber data berhasil ditambahkan.

API

Untuk terhubung Amazon Kendra ke SharePoint

Anda harus menentukan JSON dari skema sumber data menggunakan API. TemplateConfiguration Anda harus memberikan informasi berikut ini:

- Sumber data —Tentukan tipe sumber data seperti `SHAREPOINTV2` saat Anda menggunakan skema TemplateConfigurationJSON. Tentukan juga sumber data seperti `TEMPLATE` saat Anda memanggil CreateDataSourceAPI.
- Metadata Titik Akhir Repositori —Tentukan dan contoh Anda. `tenantID` `domain` `siteUrls` SharePoint
- Mode sinkronisasi —Tentukan cara Amazon Kendra memperbarui indeks Anda saat konten sumber data Anda berubah. Saat Anda menyinkronkan sumber data Amazon Kendra untuk pertama kalinya, semua konten dirayapi dan diindeks secara default. Anda harus menjalankan sinkronisasi penuh data Anda jika sinkronisasi awal Anda gagal, bahkan jika Anda tidak memilih sinkronisasi penuh sebagai opsi mode sinkronisasi Anda. Anda dapat memilih antara:
  - `FORCED_FULL_CRAWL`untuk mengindeks semua konten baru, mengganti konten yang ada setiap kali sumber data Anda disinkronkan dengan indeks Anda.
  - `FULL_CRAWL`untuk mengindeks hanya konten baru, dimodifikasi, dan dihapus setiap kali sumber data Anda disinkronkan dengan indeks Anda. Amazon Kendra dapat menggunakan mekanisme sumber data Anda untuk melacak perubahan konten dan mengindeks konten yang berubah sejak sinkronisasi terakhir.
  - `CHANGE_LOG`untuk mengindeks hanya konten baru dan yang dimodifikasi setiap kali sumber data Anda disinkronkan dengan indeks Anda. Amazon Kendra dapat menggunakan mekanisme sumber data Anda untuk melacak perubahan konten dan mengindeks konten yang berubah sejak sinkronisasi terakhir.
- Perayap identitas —Tentukan apakah akan mengaktifkan crawler Amazon Kendra identitas. Perayap identitas menggunakan informasi daftar kontrol akses (ACL) untuk dokumen Anda untuk memfilter hasil penelusuran berdasarkan akses pengguna atau grup mereka ke dokumen. Jika Anda memiliki ACL untuk dokumen Anda dan memilih untuk menggunakan ACL Anda, Anda juga dapat memilih untuk mengaktifkan crawler Amazon Kendra identitas untuk mengonfigurasi pemfilteran konteks pengguna dari hasil pencarian. Jika tidak, jika crawler identitas dimatikan, semua dokumen dapat dicari secara publik. Jika Anda ingin menggunakan kontrol akses untuk dokumen dan crawler identitas dimatikan, Anda dapat menggunakan

PutPrincipalMappingAPI untuk mengunggah informasi akses pengguna dan grup untuk pemfilteran konteks pengguna.

> **Note**
>
> Crawler identitas hanya tersedia saat Anda menyetel `crawlAcl` ke`true`.

- Properti Tambahan Repositori —Tentukan:
  - (Untuk Azure AD) `s3bucketName` dan `s3certificateName` Anda gunakan untuk menyimpan sertifikat X.509 yang ditandatangani sendiri Azure AD Anda.
  - Jenis otentikasi (`auth_Type`) yang Anda gunakan, apakah`0Auth2`,`0Auth2App`,`0Auth2Certificate`,`Basic`,, `0Auth2_RefreshTokenNTLM`, dan`Kerberos`.
  - Version (`version`) yang Anda gunakan, apakah `Server` atau`0nline`. Jika Anda menggunakan `Server` Anda dapat lebih lanjut menentukan `onPremVersion` sebagai`2013`,, `20162019`, atau`SubscriptionEdition`.
- Rahasia Nama Sumber Daya Amazon (ARN) —Berikan Nama Sumber Daya Amazon (ARN) Secrets Manager rahasia yang berisi kredensyal otentikasi yang Anda buat di akun Anda. SharePoint

  Jika Anda menggunakan SharePoint Online, Anda dapat memilih antara otentikasi Dasar, OAuth 2.0, Azure AD App-only, dan App Only. SharePoint Berikut ini adalah struktur JSON minimum yang harus ada dalam rahasia Anda untuk setiap opsi otentikasi:

  - Otentikasi dasar

    ```
    {
        "userName": "SharePoint account user name",
        "password": "SharePoint account password"
    }
    ```

  - Otentikasi OAuth 2.0

    ```
    {
        "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"
    ```

```
}
```

- Autentikasi Khusus Aplikasi Azure AD

```
{
    "clientId": "client id generated when registering SharePoint with Azure AD",
    "privateKey": "private key to authorize connection with Azure AD"
}
```

- SharePoint Autentikasi Hanya Aplikasi

```
{
    "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"
}
```

- Otentikasi token refresh OAuth 2.0

```
{
    "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"
}
```

Jika Anda menggunakan SharePoint Server, Anda dapat memilih antara otentikasi SharePoint App-Only, otentikasi NTLM, dan otentikasi Kerberos. Berikut ini adalah struktur JSON minimum yang harus ada dalam rahasia Anda untuk setiap opsi otentikasi:

- SharePoint Autentikasi Hanya Aplikasi

```
{
    "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 Autentikasi App-Only dengan domain dari otorisasi IDP

```
{
    "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"
}
```

- (Hanya server) otentikasi NTLM atau Kerberos

```
{
    "siteUrlsHash": "Hash representation of SharePoint site URLs",
    "userName": "SharePoint account user name",
    "password": "SharePoint account password"
}
```

- (Hanya server) Otentikasi NTLM atau Kerberos dengan domain dari otorisasi IDP

```
{
    "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"
}
```

> **Note**
>
> Kami menyarankan Anda secara teratur menyegarkan atau memutar kredensyal dan rahasia Anda. Berikan hanya tingkat akses yang diperlukan untuk keamanan Anda

sendiri. Kami tidak menyarankan Anda menggunakan kembali kredensyal dan rahasia di seluruh sumber data, dan konektor versi 1.0 dan 2.0 (jika berlaku).

- IAM peran —Tentukan `RoleArn` kapan Anda menelepon `CreateDataSource` untuk memberikan IAM peran dengan izin untuk mengakses Secrets Manager rahasia Anda dan memanggil API publik yang diperlukan untuk SharePoint konektor dan. Amazon Kendra Untuk informasi selengkapnya, lihat IAM peran untuk sumber SharePoint data.

Anda juga dapat menambahkan fitur opsional berikut:

- Virtual Private Cloud (VPC) **`VpcConfiguration`** —Tentukan kapan Anda menelepon. `CreateDataSource` Untuk informasi selengkapnya, lihat Mengkonfigurasi Amazon Kendra untuk menggunakan Amazon VPC.
- Filter inklusi dan pengecualian —Anda dapat menentukan apakah akan menyertakan atau mengecualikan file tertentu, OneNotes, dan konten lainnya.

> **Note**
>
> Sebagian besar sumber data menggunakan pola ekspresi reguler, yang merupakan pola inklusi atau pengecualian yang disebut sebagai filter. Jika Anda menentukan filter inklusi, hanya konten yang cocok dengan filter inklusi yang diindeks. Dokumen apa pun yang tidak cocok dengan filter inklusi tidak diindeks. Jika Anda menentukan filter inklusi dan pengecualian, dokumen yang cocok dengan filter pengecualian tidak akan diindeks, meskipun sesuai dengan filter inklusi.

- Pemetaan bidang —Pilih untuk memetakan bidang sumber SharePoint data Anda ke bidang indeks Anda Amazon Kendra . Untuk informasi lebih lanjut, lihat Memetakan bidang sumber data.

> **Note**
>
> Bidang badan dokumen atau badan dokumen yang setara untuk dokumen Anda diperlukan Amazon Kendra untuk mencari dokumen Anda. Anda harus memetakan nama bidang badan dokumen Anda di sumber data Anda ke nama bidang indeks_`document_body`. Semua kolom lain bersifat opsional.

Untuk daftar kunci JSON penting lainnya untuk dikonfigurasi, lihat SharePoint Skema templat Microsoft.

Catatan

- Konektor mendukung pemetaan bidang khusus hanya untuk entitas File.
- Untuk semua versi SharePoint Server, token ACL harus dalam huruf kecil. *Untuk **Email dengan Domain dari IDP** dan **Email ID dengan Custom Domain** ACL, misalnya: user@sharepoint2019.com.* Untuk Domain\ User dengan Domain ACL, misalnya: *sharepoint2013*\ user.
- Konektor tidak mendukung mode log perubahan/Sinkronisasi konten baru atau yang dimodifikasi untuk SharePoint tahun 2013.
- Jika nama entitas memiliki % karakter dalam namanya, konektor akan melewati file-file ini karena keterbatasan API.
- OneNote hanya dapat dirayapi oleh konektor menggunakan ID Penyewa, dan dengan token penyegaran OAuth 2.0, OAuth 2.0, atau otentikasi SharePoint App Only diaktifkan untuk Online. SharePoint
- Konektor merayapi bagian pertama OneNote dokumen menggunakan nama defaultnya saja, meskipun dokumen tersebut diganti namanya.
- Konektor merayapi tautan di SharePoint 2019, SharePoint Online, dan Edisi Berlangganan, hanya jika Halaman dan File dipilih sebagai entitas yang akan dirayapi selain Tautan.
- Konektor merayapi tautan pada SharePoint tahun 2013 dan SharePoint 2016 jika Tautan dipilih sebagai entitas yang akan dirayapi.
- Konektor merayapi lampiran daftar dan komentar hanya jika Data Daftar juga dipilih sebagai entitas yang akan di-crawl.
- Konektor merayapi lampiran peristiwa hanya jika Peristiwa juga dipilih sebagai entitas yang akan dirayapi.
- Untuk versi SharePoint Online, token ACL akan dalam huruf kecil. *Misalnya, jika **nama utama Pengguna** adalah MaryMajor@domain .com di portal Azure, token ACL di SharePoint Connector adalah marymajor@domain.com.*
- Di Perayap Identitas untuk SharePoint Online dan Server, jika Anda ingin merayapi grup bersarang, Anda harus mengaktifkan Perayapan Lokal dan Grup AD.
- Jika Anda menggunakan SharePoint Online, dan Nama Utama Pengguna di Portal Azure Anda adalah kombinasi dari huruf besar dan huruf kecil, SharePoint API secara internal mengonversinya

menjadi huruf kecil. Karena itu, Amazon Kendra SharePoint konektor menetapkan ACL dalam huruf kecil.

Microsoft SQL Server

Microsoft SQL Serveradalah sistem manajemen basis data relasional (RDBMS) yang dikembangkan oleh Microsoft. Jika Anda adalah Microsoft SQL Server pengguna, Anda dapat menggunakan Amazon Kendra untuk mengindeks sumber Microsoft SQL Server data Anda. Konektor sumber Amazon Kendra Microsoft SQL Server data mendukung MS SQL Server 2019.

Anda dapat terhubung Amazon Kendra ke sumber Microsoft SQL Server data menggunakan Amazon Kendra konsol dan TemplateConfigurationAPI.

Untuk memecahkan masalah konektor sumber Amazon Kendra Microsoft SQL Server data Anda, lihat. Mengatasi masalah sumber data

Topik

- Fitur yang didukung
- Prasyarat
- Instruksi koneksi
- Catatan

Fitur yang didukung

- Pemetaan lapangan
- Pemfilteran konteks pengguna
- Filter inklusi/pengecualian
- Sinkronisasi konten penuh dan tambahan
- Cloud privat virtual (VPC)

Prasyarat

Sebelum Anda dapat menggunakan Amazon Kendra untuk mengindeks sumber Microsoft SQL Server data Anda, buat perubahan ini di akun Microsoft SQL Server dan AWS akun Anda.

DiMicrosoft SQL Server, pastikan Anda memiliki:

- Mencatat nama pengguna dan kata sandi database Anda.

> **Important**
>
> Sebagai praktik terbaik, sediakan Amazon Kendra kredensil basis data hanya-baca.

- Menyalin url, port, dan instance host database Anda.
- Memeriksa setiap dokumen unik di dalam Microsoft SQL Server dan di seluruh sumber data lain yang Anda rencanakan untuk digunakan untuk indeks yang sama. Setiap sumber data yang ingin Anda gunakan untuk indeks tidak boleh berisi dokumen yang sama di seluruh sumber data. ID dokumen bersifat global untuk indeks dan harus unik per indeks.

Di dalam Anda Akun AWS, pastikan Anda memiliki:

- Membuat Amazon Kendra indeks dan, jika menggunakan API, mencatat ID indeks.
- Membuat IAM peran untuk sumber data Anda dan, jika menggunakan API, catat ARN peran tersebut IAM .

> **Note**
>
> Jika Anda mengubah jenis otentikasi dan kredensyal, Anda harus memperbarui IAM peran Anda untuk mengakses ID rahasia yang benar AWS Secrets Manager .

- Menyimpan kredensyal Microsoft SQL Server otentikasi Anda AWS Secrets Manager secara rahasia dan, jika menggunakan API, catat ARN rahasia tersebut.

> **Note**
>
> Kami menyarankan Anda secara teratur menyegarkan atau memutar kredensil dan rahasia Anda. Berikan hanya tingkat akses yang diperlukan untuk keamanan Anda sendiri. Kami tidak menyarankan Anda menggunakan kembali kredensyal dan rahasia di seluruh sumber data, dan konektor versi 1.0 dan 2.0 (jika berlaku).

Jika Anda tidak memiliki IAM peran atau rahasia yang ada, Anda dapat menggunakan konsol untuk membuat IAM peran dan Secrets Manager rahasia baru saat Anda menghubungkan sumber

Microsoft SQL Server data Anda Amazon Kendra. Jika Anda menggunakan API, Anda harus memberikan ARN IAM peran dan Secrets Manager rahasia yang ada, dan ID indeks.

Instruksi koneksi

Untuk terhubung Amazon Kendra ke sumber Microsoft SQL Server data Anda, Anda harus memberikan rincian Microsoft SQL Server kredensyal Anda sehingga Amazon Kendra dapat mengakses data Anda. Jika Anda belum mengkonfigurasi Microsoft SQL Server untuk Amazon Kendra lihatPrasyarat.

Console

Untuk terhubung Amazon Kendra ke Microsoft SQL Server

1. Masuk ke AWS Management Console dan buka Amazon Kendra konsol.
2. Dari panel navigasi kiri, pilih Indeks dan kemudian pilih indeks yang ingin Anda gunakan dari daftar indeks.

   > **Note**
   >
   > Anda dapat memilih untuk mengonfigurasi atau mengedit pengaturan kontrol akses Pengguna Anda di bawah Pengaturan indeks.

3. Pada halaman Memulai, pilih Tambahkan sumber data.
4. Pada halaman Tambahkan sumber data, pilih Microsoft SQL Serverkonektor, lalu pilih Tambah konektor.
5. Pada halaman Tentukan detail sumber data, masukkan informasi berikut:

   a. Di Nama dan deskripsi, untuk Nama sumber data —Masukkan nama untuk sumber data Anda. Anda dapat memasukkan tanda hubung tetapi bukan spasi.

   b. (Opsional) Deskripsi —Masukkan deskripsi opsional untuk sumber data Anda.

   c. Dalam Bahasa default —Pilih bahasa untuk memfilter dokumen Anda untuk indeks. Kecuali Anda menentukan sebaliknya, bahasa default ke bahasa Inggris. Bahasa yang ditentukan dalam metadata dokumen mengesampingkan bahasa yang dipilih.

   d. Di Tag, untuk Tambahkan tag baru —Sertakan tag opsional untuk mencari dan memfilter sumber daya Anda atau melacak AWS biaya Anda.

   e. Pilih Berikutnya.

6. Pada halaman Tentukan akses dan keamanan, masukkan informasi berikut:

a. Di Sumber, masukkan informasi berikut:

b. Host — Masukkan nama host database.

c. Port — Masukkan port database.

d. Instance - Masukkan instance database.

e. Aktifkan lokasi sertifikat SSL —Pilih untuk memasukkan Amazon S3 jalur ke file sertifikat SSL Anda.

f. Dalam Otentikasi —masukkan informasi berikut:

- AWS Secrets Manager rahasia —Pilih rahasia yang ada atau buat Secrets Manager rahasia baru untuk menyimpan kredensyal Microsoft SQL Server otentikasi Anda. Jika Anda memilih untuk membuat rahasia baru, jendela AWS Secrets Manager rahasia terbuka.

  A. Masukkan informasi berikut di jendela Buat AWS Secrets Manager rahasia:

     I. Nama rahasia —Nama untuk rahasiamu. Awalan 'AmazonKendra-Microsoft SQL Server -' secara otomatis ditambahkan ke nama rahasia Anda.

     II. Untuk nama pengguna Database, dan Kata Sandi —Masukkan nilai kredensi otentikasi yang Anda salin dari database Anda.

  B. Pilih Simpan.

g. Virtual Private Cloud (VPC) —Anda dapat memilih untuk menggunakan VPC. Jika demikian, Anda harus menambahkan Subnet dan grup keamanan VPC.

h. IAM peran —Pilih peran yang ada atau buat IAM IAM peran baru untuk mengakses kredensi repositori dan mengindeks konten Anda.

> **Note**
>
> IAM peran yang digunakan untuk indeks tidak dapat digunakan untuk sumber data. Jika Anda tidak yakin apakah peran yang ada digunakan untuk indeks atau FAQ, pilih Buat peran baru untuk menghindari kesalahan.

i. Pilih Berikutnya.

7. Pada halaman Konfigurasi pengaturan sinkronisasi, masukkan informasi berikut:

a. Dalam lingkup Sinkronisasi, pilih dari opsi berikut:

- Kueri SQL —Masukkan pernyataan kueri SQL seperti operasi SELECT dan JOIN. Kueri SQL harus kurang dari 32KB. Amazon Kendra akan merayapi semua konten database yang cocok dengan kueri Anda.

  > **Note**
  >
  > Jika nama tabel menyertakan karakter khusus (non alfanumerik) dalam nama, Anda harus menggunakan tanda kurung siku di sekitar nama tabel. Misalnya, *pilih * dari [my-database-table]*

- Kolom kunci primer —Menyediakan kunci utama untuk tabel database. Ini mengidentifikasi tabel dalam database Anda.
- Judul kolom —Berikan nama kolom judul dokumen dalam tabel database Anda.
- Kolom tubuh —Berikan nama kolom badan dokumen dalam tabel database Anda.

b. Dalam Konfigurasi tambahan — opsional, pilih dari opsi berikut untuk menyinkronkan konten tertentu alih-alih menyinkronkan semua file:

- Kolom pendeteksi perubahan —Masukkan nama kolom yang Amazon Kendra akan digunakan untuk mendeteksi perubahan konten. Amazon Kendra akan mengindeks ulang konten ketika ada perubahan di salah satu kolom ini.
- Kolom ID Pengguna —Masukkan nama kolom yang berisi ID Pengguna agar diizinkan mengakses konten.
- Kolom Grup —Masukkan nama kolom yang berisi grup untuk diizinkan mengakses konten.
- Kolom URL sumber —Masukkan nama kolom yang berisi URL Sumber yang akan diindeks.
- Kolom stempel waktu —Masukkan nama kolom yang berisi stempel waktu. Amazon Kendra menggunakan informasi cap waktu untuk mendeteksi perubahan dalam konten Anda dan hanya menyinkronkan konten yang diubah.
- Kolom zona waktu —Masukkan nama kolom yang berisi zona waktu untuk konten yang akan dirayapi.
- Format stempel waktu —Masukkan nama kolom yang berisi format cap waktu yang akan digunakan untuk mendeteksi perubahan konten dan menyinkronkan ulang konten Anda.

c. Mode sinkronisasi —Pilih cara Anda ingin memperbarui indeks saat konten sumber data Anda berubah. Saat Anda menyinkronkan sumber data Amazon Kendra untuk pertama kalinya, semua konten dirayapi dan diindeks secara default. Anda harus menjalankan sinkronisasi penuh data Anda jika sinkronisasi awal Anda gagal, bahkan jika Anda tidak memilih sinkronisasi penuh sebagai opsi mode sinkronisasi Anda.

   - Sinkronisasi penuh: Indeks baru semua konten, ganti konten yang ada setiap kali sumber data Anda disinkronkan dengan indeks Anda.
   - Sinkronisasi baru yang dimodifikasi: Indeks hanya konten baru dan yang dimodifikasi setiap kali sumber data Anda disinkronkan dengan indeks Anda. Amazon Kendra dapat menggunakan mekanisme sumber data Anda untuk melacak perubahan konten dan mengindeks konten yang berubah sejak sinkronisasi terakhir.
   - Sinkronisasi baru, dimodifikasi, dihapus: Indeks hanya konten baru, dimodifikasi, dan dihapus setiap kali sumber data Anda disinkronkan dengan indeks Anda. Amazon Kendra dapat menggunakan mekanisme sumber data Anda untuk melacak perubahan konten dan mengindeks konten yang berubah sejak sinkronisasi terakhir.

d. Dalam jadwal berjalan Sinkronisasi, untuk Frekuensi —Seberapa sering Amazon Kendra akan disinkronkan dengan sumber data Anda.

e. Pilih Berikutnya.

8. Pada halaman Setel pemetaan bidang, masukkan informasi berikut:

   a. Pilih dari bidang sumber data default yang dihasilkan - ID dokumen, judul dokumen, dan URL Sumber - yang ingin Anda petakan ke Amazon Kendra indeks.

   b. Tambahkan bidang —Untuk menambahkan bidang sumber data kustom untuk membuat nama bidang indeks untuk dipetakan dan tipe data bidang.

   c. Pilih Berikutnya.

9. Pada halaman Tinjau dan buat, periksa apakah informasi yang Anda masukkan sudah benar dan kemudian pilih Tambahkan sumber data. Anda juga dapat memilih untuk mengedit informasi Anda dari halaman ini. Sumber data Anda akan muncul di halaman Sumber data setelah sumber data berhasil ditambahkan.

API

Untuk terhubung Amazon Kendra ke Microsoft SQL Server

Anda harus menentukan yang berikut menggunakan TemplateConfigurationAPI:

- Sumber data —Tentukan tipe sumber data seperti `JDBC` saat Anda menggunakan skema TemplateConfigurationJSON. Tentukan juga sumber data seperti `TEMPLATE` saat Anda memanggil CreateDataSourceAPI.
- Jenis database —Anda harus menentukan jenis database sebagai`sqlserver`.
- Kueri SQL —Tentukan pernyataan kueri SQL seperti operasi SELECT dan JOIN. Kueri SQL harus kurang dari 32KB. Amazon Kendra akan merayapi semua konten database yang cocok dengan kueri Anda.

  > **Note**
  >
  > Jika nama tabel menyertakan karakter khusus (non alfanumerik) dalam nama, Anda harus menggunakan tanda kurung siku di sekitar nama tabel. Misalnya, *`pilih * dari [my-database-table]`*

- Mode sinkronisasi —Tentukan cara Amazon Kendra memperbarui indeks Anda saat konten sumber data Anda berubah. Saat Anda menyinkronkan sumber data Amazon Kendra untuk pertama kalinya, semua konten dirayapi dan diindeks secara default. Anda harus menjalankan sinkronisasi penuh data Anda jika sinkronisasi awal Anda gagal, bahkan jika Anda tidak memilih sinkronisasi penuh sebagai opsi mode sinkronisasi Anda. Anda dapat memilih antara:
  - `FORCED_FULL_CRAWL`untuk mengindeks semua konten baru, mengganti konten yang ada setiap kali sumber data Anda disinkronkan dengan indeks Anda.
  - `FULL_CRAWL`untuk mengindeks hanya konten baru, dimodifikasi, dan dihapus setiap kali sumber data Anda disinkronkan dengan indeks Anda. Amazon Kendra dapat menggunakan mekanisme sumber data Anda untuk melacak perubahan konten dan mengindeks konten yang berubah sejak sinkronisasi terakhir.
  - `CHANGE_LOG`untuk mengindeks hanya konten baru dan yang dimodifikasi setiap kali sumber data Anda disinkronkan dengan indeks Anda. Amazon Kendra dapat menggunakan mekanisme sumber data Anda untuk melacak perubahan konten dan mengindeks konten yang berubah sejak sinkronisasi terakhir.
- Rahasia Nama Sumber Daya Amazon (ARN) —Berikan Nama Sumber Daya Amazon (ARN) Secrets Manager rahasia yang berisi kredensyal otentikasi yang Anda buat di akun Anda. Microsoft SQL Server Rahasianya disimpan dalam struktur JSON dengan kunci berikut:

```
{
    "user name": "database user name",
    "password": "password"
```

```
}
```

> **Note**
>
> Kami menyarankan Anda secara teratur menyegarkan atau memutar kredensil dan rahasia Anda. Berikan hanya tingkat akses yang diperlukan untuk keamanan Anda sendiri. Kami tidak menyarankan Anda menggunakan kembali kredensyal dan rahasia di seluruh sumber data, dan konektor versi 1.0 dan 2.0 (jika berlaku).

- IAM peran —Tentukan `RoleArn` kapan Anda menelepon `CreateDataSource` untuk memberikan IAM peran dengan izin untuk mengakses Secrets Manager rahasia Anda dan memanggil API publik yang diperlukan untuk Microsoft SQL Server konektor dan. Amazon Kendra Untuk informasi selengkapnya, lihat IAM peran untuk sumber Microsoft SQL Server data.

Anda juga dapat menambahkan fitur opsional berikut:

- Virtual Private Cloud (VPC) **`VpcConfiguration`** —Tentukan kapan Anda menelepon. `CreateDataSource` Untuk informasi selengkapnya, lihat Mengkonfigurasi Amazon Kendra untuk menggunakan Amazon VPC.
- Filter penyertaan dan pengecualian —Anda dapat menentukan apakah akan menyertakan konten tertentu menggunakan ID pengguna, grup, URL sumber, stempel waktu, dan zona waktu.
- Pemfilteran konteks pengguna dan kontrol akses —Amazon Kendra meng-crawl daftar kontrol akses (ACL) untuk dokumen Anda, jika Anda memiliki ACL untuk dokumen Anda. Informasi ACL digunakan untuk memfilter hasil pencarian berdasarkan pengguna atau akses grup mereka ke dokumen. Untuk informasi selengkapnya, lihat Pemfilteran konteks pengguna.
- Pemetaan bidang —Pilih untuk memetakan bidang sumber Microsoft SQL Server data Anda ke bidang indeks Anda Amazon Kendra . Untuk informasi lebih lanjut, lihat Memetakan bidang sumber data.

> **Note**
>
> Bidang badan dokumen atau badan dokumen yang setara untuk dokumen Anda diperlukan Amazon Kendra untuk mencari dokumen Anda. Anda harus memetakan

nama bidang badan dokumen Anda di sumber data Anda ke nama bidang indeks_`document_body`. Semua kolom lain bersifat opsional.

Untuk daftar kunci JSON penting lainnya untuk dikonfigurasi, lihatSkema templat Microsoft SQL Server.

Catatan

- Baris database yang dihapus tidak akan dilacak saat Amazon Kendra memeriksa konten yang diperbarui.
- Ukuran nama bidang dan nilai dalam deretan database Anda tidak dapat melebihi 400KB.
- Jika Anda memiliki sejumlah besar data dalam sumber data database Anda, dan tidak Amazon Kendra ingin mengindeks semua konten database Anda setelah sinkronisasi pertama, Anda dapat memilih untuk menyinkronkan hanya dokumen baru, dimodifikasi, atau dihapus.
- Sebagai praktik terbaik, sediakan Amazon Kendra kredensil basis data hanya-baca.
- Sebagai praktik terbaik, hindari menambahkan tabel dengan data sensitif atau informasi identitas pribadi (PII).

Tim Microsoft

Microsoft Teams adalah alat kolaborasi perusahaan untuk pengiriman pesan, rapat, dan berbagi file. Jika Anda adalah pengguna Microsoft Teams, Anda dapat menggunakan Amazon Kendra untuk mengindeks sumber data Microsoft Teams Anda.

Anda dapat terhubung Amazon Kendra ke sumber data Microsoft Teams menggunakan Amazon Kendra konsol dan TemplateConfigurationAPI.

Untuk memecahkan masalah konektor sumber data Amazon Kendra Microsoft Teams, lihat. Mengatasi masalah sumber data

Topik

- Fitur yang didukung
- Prasyarat
- Instruksi koneksi
- Pelajari selengkapnya

Fitur yang didukung

- Pemetaan lapangan
- Pemfilteran konteks pengguna
- Perayapan identitas pengguna
- Filter inklusi/pengecualian
- Sinkronisasi konten penuh dan tambahan
- Cloud privat virtual (VPC)

Prasyarat

Sebelum dapat digunakan Amazon Kendra untuk mengindeks sumber data Microsoft Teams, buat perubahan ini di Tim dan AWS akun Microsoft Anda.

Di Microsoft Teams, pastikan Anda memiliki:

- Membuat akun Microsoft Teams di Office 365.
- Mencatat ID penyewa Microsoft 365 Anda. Anda dapat menemukan ID penyewa Anda di Properti Portal Direktori Aktif Azure Anda atau di aplikasi OAuth Anda.
- Membuat aplikasi OAuth di portal Azure dan mencatat ID klien dan rahasia klien atau kredensi klien. Lihat tutorial Microsoft dan contoh aplikasi Terdaftar untuk informasi selengkapnya.

> **Note**
>
> Saat Anda membuat atau mendaftarkan aplikasi di portal Azure, ID rahasia mewakili nilai rahasia yang sebenarnya. Anda harus mencatat atau menyimpan nilai rahasia yang sebenarnya segera saat membuat rahasia dan aplikasi. Anda dapat mengakses rahasia Anda dengan memilih nama aplikasi Anda di portal Azure dan kemudian menavigasi ke opsi menu pada sertifikat dan rahasia.
> Anda dapat mengakses ID klien Anda dengan memilih nama aplikasi Anda di portal Azure dan kemudian menavigasi ke halaman ikhtisar. ID Aplikasi (klien) adalah ID klien.

- Menambahkan izin yang diperlukan. Anda dapat memilih untuk menambahkan semua izin, atau Anda dapat membatasi cakupan dengan memilih lebih sedikit izin berdasarkan entitas yang ingin dirayapi. Tabel berikut mencantumkan izin tingkat aplikasi oleh entitas yang sesuai:

Entitas	Izin yang Diperlukan untuk Sinkronisasi Data	Izin yang Diperlukan untuk Sinkronisasi Identitas
Posting Saluran	• ChannelMessage.Baca.Semua • Group.Read.All • Pengguna.Baca • User.Read.All	TeamMember.Baca.Semua
Lampiran Saluran	• ChannelMessage.Baca.Semua • Group.Read.All • Pengguna.Baca • User.Read.All	TeamMember.Baca.Semua
Saluran Wiki	• Group.Read.All • Pengguna.Baca • User.Read.All	TeamMember.Baca.Semua
Pesan Obrolan	• Chat.Read.All • ChatMessage.Baca.Semua • ChatMember.Baca.Semua • Pengguna.Baca • User.Read.All • Group.Read.All	TeamMember.Baca.Semua
Obrolan Rapat	• Chat.Read.All • ChatMessage.Baca • ChatMember.Baca.Semua • Pengguna.Baca • User.Read.All • Group.Read.All	TeamMember.Baca.Semua

Entitas	Izin yang Diperlukan untuk Sinkronisasi Data	Izin yang Diperlukan untuk Sinkronisasi Identitas
Lampiran Obrolan	• Chat.Read.All • ChatMessage.Baca • ChatMember.Baca.Semua • Pengguna.Baca • User.Read.All • Group.Read.All	TeamMember.Baca.Semua
Berkas Rapat	• Chat.Read.All • ChatMessage.Baca.Semua • ChatMember.Baca.Semua • Pengguna.Baca • User.Read.All • Group.Read.All • File.Read.All	TeamMember.Baca.Semua
Rapat Kalender	• Chat.Read.All • ChatMessage.Baca.Semua • ChatMember.Baca.Semua • Pengguna.Baca • User.Read.All • Group.Read.All • File.Read.All	TeamMember.Baca.Semua
Catatan Rapat	• Pengguna.Baca • User.Read.All • Group.Read.All • File.Read.All	TeamMember.Baca.Semua

- Memeriksa setiap dokumen unik di Microsoft Teams dan di seluruh sumber data lain yang Anda rencanakan untuk digunakan untuk indeks yang sama. Setiap sumber data yang ingin Anda

gunakan untuk indeks tidak boleh berisi dokumen yang sama di seluruh sumber data. ID dokumen bersifat global untuk indeks dan harus unik per indeks.

Di dalam Anda Akun AWS, pastikan Anda memiliki:

- Membuat Amazon Kendra indeks dan, jika menggunakan API, mencatat ID indeks.
- Membuat IAM peran untuk sumber data Anda dan, jika menggunakan API, catat ARN peran tersebut IAM .

> **Note**
>
> Jika Anda mengubah jenis otentikasi dan kredensialnya, Anda harus memperbarui IAM peran Anda untuk mengakses ID rahasia yang benar AWS Secrets Manager .

- Menyimpan kredensi otentikasi Microsoft Teams Anda AWS Secrets Manager secara rahasia dan, jika menggunakan API, catat ARN rahasianya.

> **Note**
>
> Kami menyarankan Anda secara teratur menyegarkan atau memutar kredensi dan rahasia Anda. Berikan hanya tingkat akses yang diperlukan untuk keamanan Anda sendiri. Kami tidak menyarankan Anda menggunakan kembali kredensil dan rahasia di seluruh sumber data, dan konektor versi 1.0 dan 2.0 (jika berlaku).

Jika Anda tidak memiliki IAM peran atau rahasia yang ada, Anda dapat menggunakan konsol untuk membuat IAM peran dan Secrets Manager rahasia baru saat Anda menghubungkan sumber data Microsoft Teams Amazon Kendra. Jika Anda menggunakan API, Anda harus memberikan ARN IAM peran dan Secrets Manager rahasia yang ada, dan ID indeks.

Instruksi koneksi

Untuk menyambung Amazon Kendra ke sumber data Microsoft Teams, Anda harus memberikan detail yang diperlukan dari sumber data Microsoft Teams agar Amazon Kendra dapat mengakses data Anda. Jika Anda belum mengonfigurasi Microsoft Teams Amazon Kendra, lihatPrasyarat.

Console

Untuk terhubung Amazon Kendra ke Microsoft Teams

1. Masuk ke AWS Management Console dan buka Amazon Kendra konsol.
2. Dari panel navigasi kiri, pilih Indeks dan kemudian pilih indeks yang ingin Anda gunakan dari daftar indeks.

> **Note**
>
> Anda dapat memilih untuk mengonfigurasi atau mengedit pengaturan kontrol akses Pengguna Anda di bawah Pengaturan indeks.

3. Pada halaman Memulai, pilih Tambahkan sumber data.
4. Pada halaman Tambah sumber data, pilih konektor Microsoft Teams, lalu pilih Tambah konektor.
5. Pada halaman Tentukan detail sumber data, masukkan informasi berikut:
    a. Di Nama dan deskripsi, untuk Nama sumber data —Masukkan nama untuk sumber data Anda. Anda dapat memasukkan tanda hubung tetapi bukan spasi.
    b. (Opsional) Deskripsi —Masukkan deskripsi opsional untuk sumber data Anda.
    c. Dalam Bahasa default —Pilih bahasa untuk memfilter dokumen Anda untuk indeks. Kecuali Anda menentukan sebaliknya, bahasa default ke bahasa Inggris. Bahasa yang ditentukan dalam metadata dokumen mengesampingkan bahasa yang dipilih.
    d. Di Tag, untuk Tambahkan tag baru —Sertakan tag opsional untuk mencari dan memfilter sumber daya Anda atau melacak AWS biaya Anda.
    e. Pilih Berikutnya.
6. Pada halaman Tentukan akses dan keamanan, masukkan informasi berikut:
    a. Sumber —Masukkan ID penyewa Microsoft 365 Anda. Anda dapat menemukan ID penyewa Anda di Properti Portal Direktori Aktif Azure Anda atau di aplikasi OAuth Anda.
    b. AWS Secrets Manager rahasia —Pilih rahasia yang ada atau buat Secrets Manager rahasia baru untuk menyimpan kredensi otentikasi Microsoft Teams Anda. Jika Anda memilih untuk membuat rahasia baru, jendela AWS Secrets Manager rahasia terbuka.
        i. Masukkan informasi berikut di jendela Buat AWS Secrets Manager rahasia:
            A. Nama rahasia —Nama untuk rahasiamu. Awalan 'AmazonKendra-Microsoft Teams-' secara otomatis ditambahkan ke nama rahasia Anda.

B. Untuk ID Klien dan rahasia Klien —Masukkan nilai kredensi otentikasi yang Anda buat di akun Microsoft Teams Anda di portal Azure.

ii. Pilih Simpan.

c. Model pembayaran —Anda dapat memilih model lisensi dan pembayaran untuk akun Microsoft Teams Anda. Model pembayaran Model A dibatasi untuk model lisensi dan pembayaran yang memerlukan kepatuhan keamanan. Model pembayaran Model B cocok untuk model lisensi dan pembayaran yang tidak memerlukan kepatuhan keamanan.

d. Virtual Private Cloud (VPC) —Anda dapat memilih untuk menggunakan VPC. Jika demikian, Anda harus menambahkan Subnet dan grup keamanan VPC.

e. Perayap identitas —Tentukan apakah akan mengaktifkan crawler Amazon Kendra identitas. Perayap identitas menggunakan informasi daftar kontrol akses (ACL) untuk dokumen Anda untuk memfilter hasil penelusuran berdasarkan akses pengguna atau grup mereka ke dokumen. Jika Anda memiliki ACL untuk dokumen Anda dan memilih untuk menggunakan ACL Anda, Anda juga dapat memilih untuk mengaktifkan crawler Amazon Kendra identitas untuk mengonfigurasi pemfilteran konteks pengguna dari hasil pencarian. Jika tidak, jika crawler identitas dimatikan, semua dokumen dapat dicari secara publik. Jika Anda ingin menggunakan kontrol akses untuk dokumen dan crawler identitas dimatikan, Anda dapat menggunakan PutPrincipalMappingAPI untuk mengunggah informasi akses pengguna dan grup untuk pemfilteran konteks pengguna.

f. IAM peran —Pilih peran yang ada atau buat IAM IAM peran baru untuk mengakses kredensi repositori dan mengindeks konten.

> **Note**
>
> IAM peran yang digunakan untuk indeks tidak dapat digunakan untuk sumber data. Jika Anda tidak yakin apakah peran yang ada digunakan untuk indeks atau FAQ, pilih Buat peran baru untuk menghindari kesalahan.

g. Pilih Berikutnya.

7. Pada halaman Konfigurasi pengaturan sinkronisasi, masukkan informasi berikut:

a. Sinkronkan konten —Pilih konten untuk disinkronkan.

b. Konfigurasi tambahan — Anda dapat menggunakan pengaturan ini secara opsional untuk mengindeks konten tertentu alih-alih menyinkronkan semua dokumen.

c. Mode sinkronisasi —Pilih cara memperbarui indeks saat konten sumber data berubah. Saat Anda menyinkronkan sumber data Amazon Kendra untuk pertama kalinya, semua konten dirayapi dan diindeks secara default. Anda harus menjalankan sinkronisasi penuh data Anda jika sinkronisasi awal Anda gagal, bahkan jika Anda tidak memilih sinkronisasi penuh sebagai opsi mode sinkronisasi Anda.

- Sinkronisasi penuh: Indeks baru semua konten, ganti konten yang ada setiap kali sumber data Anda disinkronkan dengan indeks Anda.
- Sinkronisasi baru yang dimodifikasi: Indeks hanya konten baru dan yang dimodifikasi setiap kali sumber data Anda disinkronkan dengan indeks Anda. Amazon Kendra dapat menggunakan mekanisme sumber data Anda untuk melacak perubahan konten dan mengindeks konten yang berubah sejak sinkronisasi terakhir.
- Sinkronisasi baru, dimodifikasi, dihapus: Indeks hanya konten baru, dimodifikasi, dan dihapus setiap kali sumber data Anda disinkronkan dengan indeks Anda. Amazon Kendra dapat menggunakan mekanisme sumber data Anda untuk melacak perubahan konten dan mengindeks konten yang berubah sejak sinkronisasi terakhir.

8. Pada halaman Setel pemetaan bidang, masukkan informasi berikut:

   a. Bidang sumber data default —Pilih dari bidang sumber data default yang Amazon Kendra dihasilkan yang ingin Anda petakan ke indeks Anda.

   b. Tambahkan bidang —Untuk menambahkan bidang sumber data kustom untuk membuat nama bidang indeks untuk dipetakan dan tipe data bidang.

   c. Pilih Berikutnya.

9. Pada halaman Tinjau dan buat, periksa apakah informasi yang Anda masukkan sudah benar dan kemudian pilih Tambahkan sumber data. Anda juga dapat memilih untuk mengedit informasi Anda dari halaman ini. Sumber data Anda akan muncul di halaman Sumber data setelah sumber data berhasil ditambahkan.

API

Untuk terhubung Amazon Kendra ke Microsoft Teams

Anda harus menentukan JSON dari skema sumber data menggunakan API. TemplateConfiguration Anda harus memberikan informasi berikut ini:

- Sumber data —Tentukan tipe sumber data seperti `MSTEAMS` saat Anda menggunakan skema TemplateConfigurationJSON. Tentukan juga sumber data seperti `TEMPLATE` saat Anda memanggil CreateDataSourceAPI.
- ID Penyewa —Anda dapat menemukan ID penyewa Anda di Properti Portal Direktori Aktif Azure Anda atau di aplikasi OAuth Anda.
- Mode sinkronisasi —Tentukan cara Amazon Kendra memperbarui indeks Anda saat konten sumber data Anda berubah. Saat Anda menyinkronkan sumber data Amazon Kendra untuk pertama kalinya, semua konten dirayapi dan diindeks secara default. Anda harus menjalankan sinkronisasi penuh data Anda jika sinkronisasi awal Anda gagal, bahkan jika Anda tidak memilih sinkronisasi penuh sebagai opsi mode sinkronisasi Anda. Anda dapat memilih antara:
  - `FORCED_FULL_CRAWL`untuk mengindeks semua konten baru, mengganti konten yang ada setiap kali sumber data Anda disinkronkan dengan indeks Anda.
  - `FULL_CRAWL`untuk mengindeks hanya konten baru, dimodifikasi, dan dihapus setiap kali sumber data Anda disinkronkan dengan indeks Anda. Amazon Kendra dapat menggunakan mekanisme sumber data Anda untuk melacak perubahan konten dan mengindeks konten yang berubah sejak sinkronisasi terakhir.
  - `CHANGE_LOG`untuk mengindeks hanya konten baru dan yang dimodifikasi setiap kali sumber data Anda disinkronkan dengan indeks Anda. Amazon Kendra dapat menggunakan mekanisme sumber data Anda untuk melacak perubahan konten dan mengindeks konten yang berubah sejak sinkronisasi terakhir.
- Rahasia Nama Sumber Daya Amazon (ARN) —Berikan Nama Sumber Daya Amazon (ARN) Secrets Manager rahasia yang berisi kredensi otentikasi untuk akun Microsoft Teams Anda. Rahasianya disimpan dalam struktur JSON dengan kunci berikut:

```
{
    "clientId": "client ID",
    "clientSecret": "client secret"
}
```

> **Note**
>
> Kami menyarankan Anda secara teratur menyegarkan atau memutar kredensi dan rahasia Anda. Berikan hanya tingkat akses yang diperlukan untuk keamanan Anda sendiri. Kami tidak menyarankan Anda menggunakan kembali kredensil dan rahasia di seluruh sumber data, dan konektor versi 1.0 dan 2.0 (jika berlaku).

- IAM peran —Tentukan `RoleArn` kapan Anda menelepon `CreateDataSource` untuk memberikan IAM peran dengan izin untuk mengakses Secrets Manager rahasia Anda dan memanggil API publik yang diperlukan untuk konektor Microsoft Teams dan. Amazon Kendra Untuk informasi selengkapnya, lihat IAM peran untuk sumber data Microsoft Teams.

Anda juga dapat menambahkan fitur opsional berikut:

- Virtual Private Cloud (VPC) **`VpcConfiguration`** —Tentukan kapan Anda menelepon. `CreateDataSource` Untuk informasi selengkapnya, lihat Mengkonfigurasi Amazon Kendra untuk menggunakan Amazon VPC.
- Filter penyertaan dan pengecualian —Tentukan apakah akan menyertakan atau mengecualikan konten tertentu di Microsoft Teams. Anda dapat menyertakan atau mengecualikan nama tim, nama saluran, nama file dan jenis file, email pengguna, OneNote bagian, dan OneNote halaman. Anda juga dapat menentukan apakah akan mengindeks pesan obrolan dan lampiran, posting saluran dan lampiran, wiki saluran, konten kalender, obrolan rapat dan file dan catatan.

  > **Note**
  >
  > Sebagian besar sumber data menggunakan pola ekspresi reguler, yang merupakan pola inklusi atau pengecualian yang disebut sebagai filter. Jika Anda menentukan filter inklusi, hanya konten yang cocok dengan filter inklusi yang diindeks. Dokumen apa pun yang tidak cocok dengan filter inklusi tidak diindeks. Jika Anda menentukan filter inklusi dan pengecualian, dokumen yang cocok dengan filter pengecualian tidak akan diindeks, meskipun sesuai dengan filter inklusi.

- Perayap identitas —Tentukan apakah akan mengaktifkan crawler Amazon Kendra identitas. Perayap identitas menggunakan informasi daftar kontrol akses (ACL) untuk dokumen Anda untuk memfilter hasil penelusuran berdasarkan akses pengguna atau grup mereka ke dokumen. Jika Anda memiliki ACL untuk dokumen Anda dan memilih untuk menggunakan ACL Anda, Anda juga dapat memilih untuk mengaktifkan crawler Amazon Kendra identitas untuk mengonfigurasi pemfilteran konteks pengguna dari hasil pencarian. Jika tidak, jika crawler identitas dimatikan, semua dokumen dapat dicari secara publik. Jika Anda ingin menggunakan kontrol akses untuk dokumen dan crawler identitas dimatikan, Anda dapat menggunakan PutPrincipalMappingAPI untuk mengunggah informasi akses pengguna dan grup untuk pemfilteran konteks pengguna.

- Pemetaan bidang —Pilih untuk memetakan bidang sumber data Microsoft Teams Anda ke bidang indeks Anda Amazon Kendra . Untuk informasi lebih lanjut, lihat Memetakan bidang sumber data.

  > **Note**
  >
  > Bidang badan dokumen atau badan dokumen yang setara untuk dokumen Anda diperlukan Amazon Kendra untuk mencari dokumen Anda. Anda harus memetakan nama bidang badan dokumen Anda di sumber data Anda ke nama bidang indeks_`document_body`. Semua kolom lain bersifat opsional.

Untuk daftar kunci JSON penting lainnya untuk dikonfigurasi, lihatSkema templat Microsoft Teams.

Pelajari selengkapnya

Untuk mempelajari lebih lanjut tentang mengintegrasikan Amazon Kendra dengan sumber data Microsoft Teams, lihat:

- Cari sumber data Microsoft Teams organisasi Anda secara cerdas dengan Amazon Kendra konektor untuk Microsoft Teams

Microsoft Yammer

Microsoft Yammer adalah alat kolaborasi perusahaan untuk pengiriman pesan, rapat, dan berbagi file. Jika Anda adalah pengguna Microsoft Yammer, Anda dapat menggunakan Amazon Kendra untuk mengindeks sumber data Microsoft Yammer Anda.

Anda dapat terhubung Amazon Kendra ke sumber data Microsoft Yammer menggunakan Amazon Kendra konsol dan TemplateConfigurationAPI.

Untuk memecahkan masalah konektor sumber data Amazon Kendra Microsoft Yammer, lihat. Mengatasi masalah sumber data

Fitur yang didukung

- Pemetaan lapangan

- Filter inklusi/pengecualian
- Sinkronisasi konten penuh dan tambahan
- Cloud privat virtual (VPC)

Prasyarat

Sebelum Anda dapat menggunakan Amazon Kendra untuk mengindeks sumber data Microsoft Yammer Anda, buat perubahan ini di Microsoft Yammer dan AWS akun Anda.

Di Microsoft Yammer, pastikan Anda memiliki:

- Membuat akun administratif Microsoft Yammer di Office 365.
- Mencatat nama pengguna dan kata sandi Microsoft Yammer Anda.
- Mencatat ID penyewa Microsoft 365 Anda. Anda dapat menemukan ID penyewa Anda di Properti Portal Direktori Aktif Azure Anda atau di aplikasi OAuth Anda.
- Membuat aplikasi OAuth di portal Azure dan mencatat ID klien dan rahasia klien atau kredensi klien. Lihat tutorial Microsoft dan contoh aplikasi Terdaftar untuk informasi selengkapnya.

> **Note**
>
> Saat Anda membuat atau mendaftarkan aplikasi di portal Azure, ID rahasia mewakili nilai rahasia yang sebenarnya. Anda harus mencatat atau menyimpan nilai rahasia yang sebenarnya segera saat membuat rahasia dan aplikasi. Anda dapat mengakses rahasia Anda dengan memilih nama aplikasi Anda di portal Azure dan kemudian menavigasi ke opsi menu pada sertifikat dan rahasia.
> Anda dapat mengakses ID klien Anda dengan memilih nama aplikasi Anda di portal Azure dan kemudian menavigasi ke halaman ikhtisar. ID Aplikasi (klien) adalah ID klien.

- Memeriksa setiap dokumen unik di Microsoft Yammer dan di seluruh sumber data lain yang Anda rencanakan untuk digunakan untuk indeks yang sama. Setiap sumber data yang ingin Anda gunakan untuk indeks tidak boleh berisi dokumen yang sama di seluruh sumber data. ID dokumen bersifat global untuk indeks dan harus unik per indeks.

Di dalam Anda Akun AWS, pastikan Anda memiliki:

- Membuat Amazon Kendra indeks dan, jika menggunakan API, mencatat ID indeks.

- Membuat IAM peran untuk sumber data Anda dan, jika menggunakan API, catat ARN peran tersebut IAM .

> **Note**
>
> Jika Anda mengubah jenis otentikasi dan kredensialnya, Anda harus memperbarui IAM peran Anda untuk mengakses ID rahasia yang benar AWS Secrets Manager .

- Menyimpan kredensi otentikasi Microsoft Yammer Anda secara AWS Secrets Manager rahasia dan, jika menggunakan API, catat ARN rahasianya.

> **Note**
>
> Kami menyarankan Anda secara teratur menyegarkan atau memutar kredensi dan rahasia Anda. Berikan hanya tingkat akses yang diperlukan untuk keamanan Anda sendiri. Kami tidak menyarankan Anda menggunakan kembali kredensil dan rahasia di seluruh sumber data, dan konektor versi 1.0 dan 2.0 (jika berlaku).

Jika Anda tidak memiliki IAM peran atau rahasia yang ada, Anda dapat menggunakan konsol untuk membuat IAM peran dan Secrets Manager rahasia baru saat Anda menghubungkan sumber data Microsoft Yammer Anda. Amazon Kendra Jika Anda menggunakan API, Anda harus memberikan ARN IAM peran dan Secrets Manager rahasia yang ada, dan ID indeks.

Instruksi koneksi

Untuk terhubung Amazon Kendra ke sumber data Microsoft Yammer Anda, Anda harus memberikan rincian yang diperlukan dari sumber data Microsoft Yammer Anda sehingga Amazon Kendra dapat mengakses data Anda. Jika Anda belum mengonfigurasi Microsoft Yammer untuk Amazon Kendra, lihatPrasyarat.

Console

Untuk terhubung Amazon Kendra ke Microsoft Yammer

1. Masuk ke AWS Management Console dan buka Amazon Kendra konsol.
2. Dari panel navigasi kiri, pilih Indeks dan kemudian pilih indeks yang ingin Anda gunakan dari daftar indeks.

> **Note**
>
> Anda dapat memilih untuk mengonfigurasi atau mengedit pengaturan kontrol akses Pengguna Anda di bawah Pengaturan indeks.

3. Pada halaman Memulai, pilih Tambahkan sumber data.
4. Pada halaman Tambah sumber data, pilih konektor Microsoft Yammer, lalu pilih Tambah konektor.
5. Pada halaman Tentukan detail sumber data, masukkan informasi berikut:
    a. Dalam Nama dan deskripsi, untuk Nama sumber data —Masukkan nama untuk sumber data Anda. Anda dapat memasukkan tanda hubung tetapi bukan spasi.
    b. (Opsional) Deskripsi —Masukkan deskripsi opsional untuk sumber data Anda.
    c. Dalam Bahasa default —Pilih bahasa untuk memfilter dokumen Anda untuk indeks. Kecuali Anda menentukan sebaliknya, bahasa default ke bahasa Inggris. Bahasa yang ditentukan dalam metadata dokumen mengesampingkan bahasa yang dipilih.
    d. Di Tag, untuk Tambahkan tag baru —Sertakan tag opsional untuk mencari dan memfilter sumber daya Anda atau melacak AWS biaya Anda.
    e. Pilih Berikutnya.
6. Pada halaman Tentukan akses dan keamanan, masukkan informasi berikut:
    a. Sumber —Gunakan URL Microsoft Yammer Anda.
    b. AWS Secrets Manager rahasia —Pilih rahasia yang ada atau buat Secrets Manager rahasia baru untuk menyimpan kredensi otentikasi Microsoft Yammer Anda. Jika Anda memilih untuk membuat rahasia baru, jendela AWS Secrets Manager rahasia terbuka.
        i. Masukkan informasi berikut di jendela Buat AWS Secrets Manager rahasia:
            A. Nama rahasia —Nama untuk rahasiamu. Awalan 'AmazonKendra-Microsoft Yammer -' secara otomatis ditambahkan ke nama rahasia Anda.
            B. Untuk Nama Pengguna, Kata Sandi —Masukkan nama pengguna dan kata sandi Microsoft Yammer Anda.
            C. Untuk ID Klien, Rahasia klien —Masukkan nilai kredensi otentikasi yang Anda buat dari akun Microsoft Yammer Anda di portal Azure.
        ii. Pilih Simpan.

c. Virtual Private Cloud (VPC) —Anda dapat memilih untuk menggunakan VPC. Jika demikian, Anda harus menambahkan Subnet dan grup keamanan VPC.

d. Perayap identitas —Tentukan apakah akan mengaktifkan crawler Amazon Kendra identitas. Perayap identitas menggunakan informasi daftar kontrol akses (ACL) untuk dokumen Anda untuk memfilter hasil penelusuran berdasarkan akses pengguna atau grup mereka ke dokumen. Jika Anda memiliki ACL untuk dokumen Anda dan memilih untuk menggunakan ACL Anda, Anda juga dapat memilih untuk mengaktifkan crawler Amazon Kendra identitas untuk mengonfigurasi pemfilteran konteks pengguna dari hasil pencarian. Jika tidak, jika crawler identitas dimatikan, semua dokumen dapat dicari secara publik. Jika Anda ingin menggunakan kontrol akses untuk dokumen dan crawler identitas dimatikan, Anda dapat menggunakan PutPrincipalMappingAPI untuk mengunggah informasi akses pengguna dan grup untuk pemfilteran konteks pengguna.

e. IAM peran —Pilih peran yang sudah ada atau buat IAM IAM peran baru untuk mengakses kredensi repositori dan mengindeks konten Anda.

> **Note**
>
> IAM peran yang digunakan untuk indeks tidak dapat digunakan untuk sumber data. Jika Anda tidak yakin apakah peran yang ada digunakan untuk indeks atau FAQ, pilih Buat peran baru untuk menghindari kesalahan.

f. Pilih Berikutnya.

7. Pada halaman Konfigurasi pengaturan sinkronisasi, masukkan informasi berikut:

a. Sejak tanggal —Tentukan tanggal untuk mulai merayapi data Anda di Microsoft Yammer.

b. Sinkronkan konten —Pilih jenis konten yang ingin Anda indeks. Misalnya, pesan publik, pesan pribadi, dan lampiran.

c. Konfigurasi tambahan —Anda dapat menggunakan opsi ini secara opsional untuk mengindeks konten tertentu alih-alih menyinkronkan semua dokumen. Misalnya, Anda dapat mengindeks nama komunitas tertentu dan menggunakan pola ekspresi reguler untuk menyertakan atau mengecualikan file tertentu.

d. Mode sinkronisasi —Pilih cara Anda ingin memperbarui indeks saat konten sumber data Anda berubah. Saat Anda menyinkronkan sumber data Amazon Kendra untuk pertama kalinya, semua konten dirayapi dan diindeks secara default. Anda harus menjalankan sinkronisasi penuh data Anda jika sinkronisasi awal Anda gagal, bahkan jika Anda tidak memilih sinkronisasi penuh sebagai opsi mode sinkronisasi Anda.

- Sinkronisasi penuh: Indeks baru semua konten, ganti konten yang ada setiap kali sumber data Anda disinkronkan dengan indeks Anda.
- Sinkronisasi baru yang dimodifikasi: Indeks hanya konten baru dan yang dimodifikasi setiap kali sumber data Anda disinkronkan dengan indeks Anda. Amazon Kendra dapat menggunakan mekanisme sumber data Anda untuk melacak perubahan konten dan mengindeks konten yang berubah sejak sinkronisasi terakhir.
- Sinkronisasi baru, dimodifikasi, dihapus: Indeks hanya konten baru, dimodifikasi, dan dihapus setiap kali sumber data Anda disinkronkan dengan indeks Anda. Amazon Kendra dapat menggunakan mekanisme sumber data Anda untuk melacak perubahan konten dan mengindeks konten yang berubah sejak sinkronisasi terakhir.

8. Pada halaman Setel pemetaan bidang, masukkan informasi berikut:

   a. Bidang sumber data default —Pilih dari bidang sumber data default yang Amazon Kendra dihasilkan yang ingin Anda petakan ke indeks Anda.

   b. Tambahkan bidang —Untuk menambahkan bidang sumber data kustom untuk membuat nama bidang indeks untuk dipetakan dan tipe data bidang.

   c. Pilih Berikutnya.

9. Pada halaman Tinjau dan buat, periksa apakah informasi yang Anda masukkan sudah benar dan kemudian pilih Tambahkan sumber data. Anda juga dapat memilih untuk mengedit informasi Anda dari halaman ini. Sumber data Anda akan muncul di halaman Sumber data setelah sumber data berhasil ditambahkan.

API

Untuk terhubung Amazon Kendra ke Microsoft Yammer

Anda harus menentukan JSON dari skema sumber data menggunakan API. TemplateConfiguration Anda harus memberikan informasi berikut ini:

- Sumber data —Tentukan tipe sumber data seperti `YAMMER` saat Anda menggunakan skema TemplateConfigurationJSON. Tentukan juga sumber data seperti `TEMPLATE` saat Anda memanggil CreateDataSourceAPI.
- Mode sinkronisasi —Tentukan cara Amazon Kendra memperbarui indeks Anda saat konten sumber data Anda berubah. Saat Anda menyinkronkan sumber data Amazon Kendra untuk pertama kalinya, semua konten dirayapi dan diindeks secara default. Anda harus menjalankan

sinkronisasi penuh data Anda jika sinkronisasi awal Anda gagal, bahkan jika Anda tidak memilih sinkronisasi penuh sebagai opsi mode sinkronisasi Anda. Anda dapat memilih antara:

- `FORCED_FULL_CRAWL`untuk mengindeks semua konten baru, mengganti konten yang ada setiap kali sumber data Anda disinkronkan dengan indeks Anda.
- `FULL_CRAWL`untuk mengindeks hanya konten baru, dimodifikasi, dan dihapus setiap kali sumber data Anda disinkronkan dengan indeks Anda. Amazon Kendra dapat menggunakan mekanisme sumber data Anda untuk melacak perubahan konten dan mengindeks konten yang berubah sejak sinkronisasi terakhir.
- `CHANGE_LOG`untuk mengindeks hanya konten baru dan yang dimodifikasi setiap kali sumber data Anda disinkronkan dengan indeks Anda. Amazon Kendra dapat menggunakan mekanisme sumber data Anda untuk melacak perubahan konten dan mengindeks konten yang berubah sejak sinkronisasi terakhir.

- Rahasia Nama Sumber Daya Amazon (ARN) —Berikan Nama Sumber Daya Amazon (ARN) Secrets Manager rahasia yang berisi kredensi otentikasi untuk akun Microsoft Yammer Anda. Rahasianya disimpan dalam struktur JSON dengan kunci berikut:

```
{
    "username": "user name",
    "password": "password",
    "clientId": "client ID",
    "clientSecret": "client secret"
}
```

> **Note**
>
> Kami menyarankan Anda secara teratur menyegarkan atau memutar kredensi dan rahasia Anda. Berikan hanya tingkat akses yang diperlukan untuk keamanan Anda sendiri. Kami tidak menyarankan Anda menggunakan kembali kredensil dan rahasia di seluruh sumber data, dan konektor versi 1.0 dan 2.0 (jika berlaku).

- IAM peran —Tentukan `RoleArn` kapan Anda memanggil `CreateDataSource` untuk memberikan IAM peran dengan izin untuk mengakses Secrets Manager rahasia Anda dan memanggil API publik yang diperlukan untuk konektor Microsoft Yammer dan. Amazon Kendra Untuk informasi selengkapnya, lihat IAM peran untuk sumber data Microsoft Yammer.

Anda juga dapat menambahkan fitur opsional berikut:

- Virtual Private Cloud (VPC) **`VpcConfiguration`** —Tentukan kapan Anda menelepon. `CreateDataSource` Untuk informasi selengkapnya, lihat Mengkonfigurasi Amazon Kendra untuk menggunakan Amazon VPC.
- Filter inklusi dan pengecualian —Tentukan apakah akan menyertakan atau mengecualikan konten tertentu.

> **Note**
>
> Sebagian besar sumber data menggunakan pola ekspresi reguler, yang merupakan pola inklusi atau pengecualian yang disebut sebagai filter. Jika Anda menentukan filter inklusi, hanya konten yang cocok dengan filter inklusi yang diindeks. Dokumen apa pun yang tidak cocok dengan filter inklusi tidak diindeks. Jika Anda menentukan filter inklusi dan pengecualian, dokumen yang cocok dengan filter pengecualian tidak akan diindeks, meskipun sesuai dengan filter inklusi.

- Perayap identitas —Tentukan apakah akan mengaktifkan crawler Amazon Kendra identitas. Perayap identitas menggunakan informasi daftar kontrol akses (ACL) untuk dokumen Anda untuk memfilter hasil penelusuran berdasarkan akses pengguna atau grup mereka ke dokumen. Jika Anda memiliki ACL untuk dokumen Anda dan memilih untuk menggunakan ACL Anda, Anda juga dapat memilih untuk mengaktifkan crawler Amazon Kendra identitas untuk mengonfigurasi pemfilteran konteks pengguna dari hasil pencarian. Jika tidak, jika crawler identitas dimatikan, semua dokumen dapat dicari secara publik. Jika Anda ingin menggunakan kontrol akses untuk dokumen dan crawler identitas dimatikan, Anda dapat menggunakan PutPrincipalMappingAPI untuk mengunggah informasi akses pengguna dan grup untuk pemfilteran konteks pengguna.
- Pemetaan bidang —Pilih untuk memetakan bidang sumber data Microsoft Yammer Anda ke bidang indeks Anda. Amazon Kendra Untuk informasi lebih lanjut, lihat Memetakan bidang sumber data.

> **Note**
>
> Bidang badan dokumen atau badan dokumen yang setara untuk dokumen Anda diperlukan Amazon Kendra untuk mencari dokumen Anda. Anda harus memetakan nama bidang badan dokumen Anda di sumber data Anda ke nama bidang indeks_`document_body`. Semua kolom lain bersifat opsional.

Pelajari selengkapnya

Untuk mempelajari lebih lanjut tentang mengintegrasikan Amazon Kendra dengan sumber data Microsoft Yammer, lihat:

- Mengumumkan konektor Yammer untuk Amazon Kendra

MySQL

MySQLadalah sistem manajemen database relasional open source. Jika Anda adalah MySQL pengguna, Anda dapat menggunakan Amazon Kendra untuk mengindeks sumber MySQL data Anda. Konektor sumber Amazon Kendra MySQL data mendukung MySQL 8.0. 21.

Anda dapat terhubung Amazon Kendra ke sumber MySQL data menggunakan Amazon Kendra konsol dan TemplateConfigurationAPI.

Untuk memecahkan masalah konektor sumber Amazon Kendra MySQL data Anda, lihat. Mengatasi masalah sumber data

Topik

- Fitur yang didukung
- Prasyarat
- Instruksi koneksi
- Catatan

Fitur yang didukung

- Pemetaan lapangan
- Pemfilteran konteks pengguna
- Filter inklusi/pengecualian
- Sinkronisasi konten penuh dan tambahan
- Cloud privat virtual (VPC)

Prasyarat

Sebelum Anda dapat menggunakan Amazon Kendra untuk mengindeks sumber MySQL data Anda, buat perubahan ini di akun MySQL dan AWS akun Anda.

DiMySQL, pastikan Anda memiliki:

- Mencatat nama pengguna dan kata sandi database Anda.

> **Important**
>
> Sebagai praktik terbaik, sediakan Amazon Kendra kredensil basis data hanya-baca.

- Menyalin url, port, dan instance host database Anda.
- Memeriksa setiap dokumen unik di dalam MySQL dan di seluruh sumber data lain yang Anda rencanakan untuk digunakan untuk indeks yang sama. Setiap sumber data yang ingin Anda gunakan untuk indeks tidak boleh berisi dokumen yang sama di seluruh sumber data. ID dokumen bersifat global untuk indeks dan harus unik per indeks.

Di dalam Anda Akun AWS, pastikan Anda memiliki:

- Membuat Amazon Kendra indeks dan, jika menggunakan API, mencatat ID indeks.
- Membuat IAM peran untuk sumber data Anda dan, jika menggunakan API, catat ARN peran tersebut IAM .

> **Note**
>
> Jika Anda mengubah jenis otentikasi dan kredensyal, Anda harus memperbarui IAM peran Anda untuk mengakses ID rahasia yang benar AWS Secrets Manager .

- Menyimpan kredensyal MySQL otentikasi Anda AWS Secrets Manager secara rahasia dan, jika menggunakan API, catat ARN rahasia tersebut.

> **Note**
>
> Kami menyarankan Anda secara teratur menyegarkan atau memutar kredensil dan rahasia Anda. Berikan hanya tingkat akses yang diperlukan untuk keamanan Anda sendiri. Kami

tidak menyarankan Anda menggunakan kembali kredensyal dan rahasia di seluruh sumber data, dan konektor versi 1.0 dan 2.0 (jika berlaku).

Jika Anda tidak memiliki IAM peran atau rahasia yang ada, Anda dapat menggunakan konsol untuk membuat IAM peran dan Secrets Manager rahasia baru saat menghubungkan sumber MySQL data Amazon Kendra. Jika Anda menggunakan API, Anda harus memberikan ARN IAM peran dan Secrets Manager rahasia yang ada, dan ID indeks.

Instruksi koneksi

Untuk terhubung Amazon Kendra ke sumber MySQL data Anda, Anda harus memberikan rincian MySQL kredensyal Anda sehingga Amazon Kendra dapat mengakses data Anda. Jika Anda belum mengkonfigurasi MySQL untuk Amazon Kendra lihatPrasyarat.

Console

Untuk terhubung Amazon Kendra ke MySQL

1. Masuk ke AWS Management Console dan buka Amazon Kendra konsol.
2. Dari panel navigasi kiri, pilih Indeks dan kemudian pilih indeks yang ingin Anda gunakan dari daftar indeks.

   > **Note**
   >
   > Anda dapat memilih untuk mengonfigurasi atau mengedit pengaturan kontrol akses Pengguna Anda di bawah Pengaturan indeks.

3. Pada halaman Memulai, pilih Tambahkan sumber data.
4. Pada halaman Tambahkan sumber data, pilih MySQLkonektor, lalu pilih Tambah konektor.
5. Pada halaman Tentukan detail sumber data, masukkan informasi berikut:

   a. Di Nama dan deskripsi, untuk Nama sumber data —Masukkan nama untuk sumber data Anda. Anda dapat memasukkan tanda hubung tetapi bukan spasi.

   b. (Opsional) Deskripsi —Masukkan deskripsi opsional untuk sumber data Anda.

   c. Dalam Bahasa default —Pilih bahasa untuk memfilter dokumen Anda untuk indeks. Kecuali Anda menentukan sebaliknya, bahasa default ke bahasa Inggris. Bahasa yang ditentukan dalam metadata dokumen menggantikan bahasa yang dipilih.

d. Di Tag, untuk Tambahkan tag baru —Sertakan tag opsional untuk mencari dan memfilter sumber daya Anda atau melacak AWS biaya Anda.

e. Pilih Berikutnya.

6. Pada halaman Tentukan akses dan keamanan, masukkan informasi berikut:

a. Di Sumber, masukkan informasi berikut:

b. Host — Masukkan nama host database.

c. Port — Masukkan port database.

d. Instance - Masukkan instance database.

e. Aktifkan lokasi sertifikat SSL —Pilih untuk memasukkan Amazon S3 jalur ke file sertifikat SSL Anda.

f. Dalam Otentikasi —masukkan informasi berikut:

- AWS Secrets Manager rahasia —Pilih rahasia yang ada atau buat Secrets Manager rahasia baru untuk menyimpan kredensyal MySQL otentikasi Anda. Jika Anda memilih untuk membuat rahasia baru, jendela AWS Secrets Manager rahasia terbuka.

  A. Masukkan informasi berikut di jendela Buat AWS Secrets Manager rahasia:

     I. Nama rahasia —Nama untuk rahasiamu. Awalan 'AmazonKendra- MySQL -' secara otomatis ditambahkan ke nama rahasia Anda.

     II. Untuk nama pengguna Database, dan Kata Sandi —Masukkan nilai kredensi otentikasi yang Anda salin dari database Anda.

  B. Pilih Simpan.

g. Virtual Private Cloud (VPC) —Anda dapat memilih untuk menggunakan VPC. Jika demikian, Anda harus menambahkan Subnet dan grup keamanan VPC.

h. IAM peran —Pilih peran yang sudah ada atau buat IAM IAM peran baru untuk mengakses kredensi repositori dan mengindeks konten Anda.

> **Note**
>
> IAM peran yang digunakan untuk indeks tidak dapat digunakan untuk sumber data. Jika Anda tidak yakin apakah peran yang ada digunakan untuk indeks atau FAQ, pilih Buat peran baru untuk menghindari kesalahan.

i. Pilih Berikutnya.

7. Pada halaman Konfigurasi pengaturan sinkronisasi, masukkan informasi berikut:

   a. Dalam lingkup Sinkronisasi, pilih dari opsi berikut:

      - Kueri SQL —Masukkan pernyataan kueri SQL seperti operasi SELECT dan JOIN. Kueri SQL harus kurang dari 32KB. Amazon Kendra akan merayapi semua konten database yang cocok dengan kueri Anda.
      - Kolom kunci primer —Berikan kunci utama untuk tabel database. Ini mengidentifikasi tabel dalam database Anda.
      - Judul kolom —Berikan nama kolom judul dokumen dalam tabel database Anda.
      - Kolom tubuh —Berikan nama kolom badan dokumen dalam tabel database Anda.

   b. Dalam Konfigurasi tambahan — opsional, pilih dari opsi berikut untuk menyinkronkan konten tertentu alih-alih menyinkronkan semua file:

      - Kolom pendeteksi perubahan —Masukkan nama kolom yang Amazon Kendra akan digunakan untuk mendeteksi perubahan konten. Amazon Kendra akan mengindeks ulang konten ketika ada perubahan di salah satu kolom ini.
      - Kolom ID Pengguna —Masukkan nama kolom yang berisi ID Pengguna agar diizinkan mengakses konten.
      - Kolom Grup —Masukkan nama kolom yang berisi grup untuk diizinkan mengakses konten.
      - Kolom URL sumber —Masukkan nama kolom yang berisi URL Sumber yang akan diindeks.
      - Kolom stempel waktu —Masukkan nama kolom yang berisi stempel waktu. Amazon Kendra menggunakan informasi cap waktu untuk mendeteksi perubahan dalam konten Anda dan hanya menyinkronkan konten yang diubah.
      - Kolom zona waktu —Masukkan nama kolom yang berisi zona waktu untuk konten yang akan dirayapi.
      - Format stempel waktu —Masukkan nama kolom yang berisi format cap waktu yang akan digunakan untuk mendeteksi perubahan konten dan menyinkronkan ulang konten Anda.

   c. Mode sinkronisasi —Pilih cara memperbarui indeks saat konten sumber data berubah. Saat Anda menyinkronkan sumber data Amazon Kendra untuk pertama kalinya, semua konten dirayapi dan diindeks secara default. Anda harus menjalankan sinkronisasi penuh

data Anda jika sinkronisasi awal Anda gagal, bahkan jika Anda tidak memilih sinkronisasi penuh sebagai opsi mode sinkronisasi Anda.

- Sinkronisasi penuh: Indeks baru semua konten, ganti konten yang ada setiap kali sumber data Anda disinkronkan dengan indeks Anda.
- Sinkronisasi baru yang dimodifikasi: Indeks hanya konten baru dan yang dimodifikasi setiap kali sumber data Anda disinkronkan dengan indeks Anda. Amazon Kendra dapat menggunakan mekanisme sumber data Anda untuk melacak perubahan konten dan mengindeks konten yang berubah sejak sinkronisasi terakhir.
- Sinkronisasi baru, dimodifikasi, dihapus: Indeks hanya konten baru, dimodifikasi, dan dihapus setiap kali sumber data Anda disinkronkan dengan indeks Anda. Amazon Kendra dapat menggunakan mekanisme sumber data Anda untuk melacak perubahan konten dan mengindeks konten yang berubah sejak sinkronisasi terakhir.

d. Dalam jadwal berjalan Sinkronisasi, untuk Frekuensi —Seberapa sering Amazon Kendra akan disinkronkan dengan sumber data Anda.

e. Pilih Berikutnya.

8. Pada halaman Setel pemetaan bidang, masukkan informasi berikut:

a. Pilih dari bidang sumber data default yang dihasilkan - ID dokumen, judul dokumen, dan URL Sumber - yang ingin Anda petakan ke Amazon Kendra indeks.

b. Tambahkan bidang —Untuk menambahkan bidang sumber data kustom untuk membuat nama bidang indeks untuk dipetakan dan tipe data bidang.

c. Pilih Berikutnya.

9. Pada halaman Tinjau dan buat, periksa apakah informasi yang Anda masukkan sudah benar dan kemudian pilih Tambahkan sumber data. Anda juga dapat memilih untuk mengedit informasi Anda dari halaman ini. Sumber data Anda akan muncul di halaman Sumber data setelah sumber data berhasil ditambahkan.

API

Untuk terhubung Amazon Kendra ke MySQL

Anda harus menentukan yang berikut menggunakan TemplateConfigurationAPI:

- Sumber data —Tentukan tipe sumber data seperti `JDBC` saat Anda menggunakan skema TemplateConfigurationJSON. Tentukan juga sumber data seperti `TEMPLATE` saat Anda memanggil CreateDataSourceAPI.
- Jenis database —Anda harus menentukan jenis database sebagai`mySql`.
- Kueri SQL —Tentukan pernyataan kueri SQL seperti operasi SELECT dan JOIN. Kueri SQL harus kurang dari 32KB. Amazon Kendra akan merayapi semua konten database yang cocok dengan kueri Anda.
- Mode sinkronisasi —Tentukan cara Amazon Kendra memperbarui indeks Anda saat konten sumber data Anda berubah. Saat Anda menyinkronkan sumber data Amazon Kendra untuk pertama kalinya, semua konten dirayapi dan diindeks secara default. Anda harus menjalankan sinkronisasi penuh data Anda jika sinkronisasi awal Anda gagal, bahkan jika Anda tidak memilih sinkronisasi penuh sebagai opsi mode sinkronisasi Anda. Anda dapat memilih antara:
  - `FORCED_FULL_CRAWL`untuk mengindeks semua konten baru, mengganti konten yang ada setiap kali sumber data Anda disinkronkan dengan indeks Anda.
  - `FULL_CRAWL`untuk mengindeks hanya konten baru, dimodifikasi, dan dihapus setiap kali sumber data Anda disinkronkan dengan indeks Anda. Amazon Kendra dapat menggunakan mekanisme sumber data Anda untuk melacak perubahan konten dan mengindeks konten yang berubah sejak sinkronisasi terakhir.
  - `CHANGE_LOG`untuk mengindeks hanya konten baru dan yang dimodifikasi setiap kali sumber data Anda disinkronkan dengan indeks Anda. Amazon Kendra dapat menggunakan mekanisme sumber data Anda untuk melacak perubahan konten dan mengindeks konten yang berubah sejak sinkronisasi terakhir.
- Rahasia Nama Sumber Daya Amazon (ARN) —Berikan Nama Sumber Daya Amazon (ARN) Secrets Manager rahasia yang berisi kredensyal otentikasi yang Anda buat di akun Anda. MySQL Rahasianya disimpan dalam struktur JSON dengan kunci berikut:

```
{
    "user name": "database user name",
    "password": "password"
}
```

> **Note**
>
> Kami menyarankan Anda secara teratur menyegarkan atau memutar kredensil dan rahasia Anda. Berikan hanya tingkat akses yang diperlukan untuk keamanan Anda

sendiri. Kami tidak menyarankan Anda menggunakan kembali kredensyal dan rahasia di seluruh sumber data, dan konektor versi 1.0 dan 2.0 (jika berlaku).

- IAM peran —Tentukan `RoleArn` kapan Anda menelepon `CreateDataSource` untuk memberikan IAM peran dengan izin untuk mengakses Secrets Manager rahasia Anda dan memanggil API publik yang diperlukan untuk MySQL konektor dan. Amazon Kendra Untuk informasi selengkapnya, lihat IAM peran untuk sumber MySQL data.

Anda juga dapat menambahkan fitur opsional berikut:

- Virtual Private Cloud (VPC) **`VpcConfiguration`** —Tentukan kapan Anda menelepon. `CreateDataSource` Untuk informasi selengkapnya, lihat Mengkonfigurasi Amazon Kendra untuk menggunakan Amazon VPC.
- Filter penyertaan dan pengecualian —Anda dapat menentukan apakah akan menyertakan konten tertentu menggunakan ID pengguna, grup, URL sumber, stempel waktu, dan zona waktu.
- Pemfilteran konteks pengguna dan kontrol akses —Amazon Kendra meng-crawl daftar kontrol akses (ACL) untuk dokumen Anda, jika Anda memiliki ACL untuk dokumen Anda. Informasi ACL digunakan untuk memfilter hasil pencarian berdasarkan pengguna atau akses grup mereka ke dokumen. Untuk informasi selengkapnya, lihat Pemfilteran konteks pengguna.
- Pemetaan bidang —Pilih untuk memetakan bidang sumber MySQL data Anda ke bidang indeks Anda Amazon Kendra . Untuk informasi lebih lanjut, lihat Memetakan bidang sumber data.

> **Note**
>
> Bidang badan dokumen atau badan dokumen yang setara untuk dokumen Anda diperlukan Amazon Kendra untuk mencari dokumen Anda. Anda harus memetakan nama bidang badan dokumen Anda di sumber data Anda ke nama bidang indeks_`document_body`. Semua kolom lain bersifat opsional.

Catatan

- Baris database yang dihapus tidak akan dilacak saat Amazon Kendra memeriksa konten yang diperbarui.
- Ukuran nama bidang dan nilai dalam deretan database Anda tidak dapat melebihi 400KB.

- Jika Anda memiliki sejumlah besar data dalam sumber data database Anda, dan tidak Amazon Kendra ingin mengindeks semua konten database Anda setelah sinkronisasi pertama, Anda dapat memilih untuk menyinkronkan hanya dokumen baru, dimodifikasi, atau dihapus.
- Sebagai praktik terbaik, sediakan Amazon Kendra kredensil basis data hanya-baca.
- Sebagai praktik terbaik, hindari menambahkan tabel dengan data sensitif atau informasi identitas pribadi (PII).

Oracle Database

Oracle Databaseadalah sistem manajemen basis data. Jika Anda adalah Oracle Database pengguna, Anda dapat menggunakan Amazon Kendra untuk mengindeks sumber Oracle Database data Anda. Konektor sumber Amazon Kendra Oracle Database data mendukung Oracle Database 18c, 19c, dan 21c.

Anda dapat terhubung Amazon Kendra ke sumber Oracle Database data menggunakan Amazon Kendra konsol dan TemplateConfigurationAPI.

Untuk memecahkan masalah konektor sumber Amazon Kendra Oracle Database data Anda, lihat. Mengatasi masalah sumber data

Topik

- Fitur yang didukung
- Prasyarat
- Instruksi koneksi
- Catatan

Fitur yang didukung

- Pemetaan lapangan
- Pemfilteran konteks pengguna
- Filter inklusi/pengecualian
- Sinkronisasi konten penuh dan tambahan
- Cloud privat virtual (VPC)

Prasyarat

Sebelum dapat digunakan Amazon Kendra untuk mengindeks sumber Oracle Database data Anda, buat perubahan ini di akun Oracle Database dan AWS akun Anda.

DiOracle Database, pastikan Anda memiliki:

- Mencatat nama pengguna dan kata sandi database Anda.

> **Important**
>
> Sebagai praktik terbaik, sediakan Amazon Kendra kredensil basis data hanya-baca.

- Menyalin url, port, dan instance host database Anda.
- Memeriksa setiap dokumen unik di dalam Oracle Database dan di seluruh sumber data lain yang Anda rencanakan untuk digunakan untuk indeks yang sama. Setiap sumber data yang ingin Anda gunakan untuk indeks tidak boleh berisi dokumen yang sama di seluruh sumber data. ID dokumen bersifat global untuk indeks dan harus unik per indeks.

Di dalam Anda Akun AWS, pastikan Anda memiliki:

- Membuat Amazon Kendra indeks dan, jika menggunakan API, mencatat ID indeks.
- Membuat IAM peran untuk sumber data Anda dan, jika menggunakan API, catat ARN peran tersebut IAM .

> **Note**
>
> Jika Anda mengubah jenis otentikasi dan kredensyal, Anda harus memperbarui IAM peran Anda untuk mengakses ID rahasia yang benar AWS Secrets Manager .

- Menyimpan kredensyal Oracle Database otentikasi Anda AWS Secrets Manager secara rahasia dan, jika menggunakan API, catat ARN rahasia tersebut.

> **Note**
>
> Kami menyarankan Anda secara teratur menyegarkan atau memutar kredensil dan rahasia Anda. Berikan hanya tingkat akses yang diperlukan untuk keamanan Anda sendiri. Kami

tidak menyarankan Anda menggunakan kembali kredensyal dan rahasia di seluruh sumber data, dan konektor versi 1.0 dan 2.0 (jika berlaku).

Jika Anda tidak memiliki IAM peran atau rahasia yang ada, Anda dapat menggunakan konsol untuk membuat IAM peran dan Secrets Manager rahasia baru saat menghubungkan sumber Oracle Database data Amazon Kendra. Jika Anda menggunakan API, Anda harus memberikan ARN IAM peran dan Secrets Manager rahasia yang ada, dan ID indeks.

Instruksi koneksi

Untuk terhubung Amazon Kendra ke sumber Oracle Database data Anda, Anda harus memberikan rincian Oracle Database kredensyal Anda sehingga Amazon Kendra dapat mengakses data Anda. Jika Anda belum mengkonfigurasi Oracle Database untuk Amazon Kendra lihatPrasyarat.

Console

Untuk terhubung Amazon Kendra ke Oracle Database

1. Masuk ke AWS Management Console dan buka Amazon Kendra konsol.
2. Dari panel navigasi kiri, pilih Indeks dan kemudian pilih indeks yang ingin Anda gunakan dari daftar indeks.

   > **Note**
   >
   > Anda dapat memilih untuk mengonfigurasi atau mengedit pengaturan kontrol akses Pengguna di bawah Pengaturan indeks.

3. Pada halaman Memulai, pilih Tambahkan sumber data.
4. Pada halaman Tambahkan sumber data, pilih Oracle Databasekonektor, lalu pilih Tambah konektor.
5. Pada halaman Tentukan detail sumber data, masukkan informasi berikut:

   a. Di Nama dan deskripsi, untuk Nama sumber data —Masukkan nama untuk sumber data Anda. Anda dapat memasukkan tanda hubung tetapi bukan spasi.

   b. (Opsional) Deskripsi —Masukkan deskripsi opsional untuk sumber data Anda.

c. Dalam Bahasa default —Pilih bahasa untuk memfilter dokumen Anda untuk indeks. Kecuali Anda menentukan sebaliknya, bahasa default ke bahasa Inggris. Bahasa yang ditentukan dalam metadata dokumen mengesampingkan bahasa yang dipilih.

d. Di Tag, untuk Tambahkan tag baru —Sertakan tag opsional untuk mencari dan memfilter sumber daya Anda atau melacak AWS biaya Anda.

e. Pilih Berikutnya.

6. Pada halaman Tentukan akses dan keamanan, masukkan informasi berikut:

a. Di Sumber, masukkan informasi berikut:

b. Host — Masukkan nama host database.

c. Port — Masukkan port database.

d. Instance - Masukkan instance database.

e. Aktifkan lokasi sertifikat SSL —Pilih untuk memasukkan Amazon S3 jalur ke file sertifikat SSL Anda.

f. Dalam Otentikasi —masukkan informasi berikut:

- AWS Secrets Manager rahasia —Pilih rahasia yang ada atau buat Secrets Manager rahasia baru untuk menyimpan kredensyal Oracle Database otentikasi Anda. Jika Anda memilih untuk membuat rahasia baru, jendela AWS Secrets Manager rahasia terbuka.

  A. Masukkan informasi berikut di jendela Buat AWS Secrets Manager rahasia:

     I. Nama rahasia —Nama untuk rahasiamu. Awalan 'AmazonKendra- Oracle Database -' secara otomatis ditambahkan ke nama rahasia Anda.

     II. Untuk nama pengguna Database, dan Kata Sandi —Masukkan nilai kredensi otentikasi yang Anda salin dari database Anda.

  B. Pilih Simpan.

g. Virtual Private Cloud (VPC) —Anda dapat memilih untuk menggunakan VPC. Jika demikian, Anda harus menambahkan Subnet dan grup keamanan VPC.

h. IAM peran —Pilih peran yang ada atau buat IAM IAM peran baru untuk mengakses kredensyal repositori dan mengindeks konten Anda.

> **Note**
>
> IAM peran yang digunakan untuk indeks tidak dapat digunakan untuk sumber data. Jika Anda tidak yakin apakah peran yang ada digunakan untuk indeks atau FAQ, pilih Buat peran baru untuk menghindari kesalahan.

i. Pilih Berikutnya.

7. Pada halaman Konfigurasi pengaturan sinkronisasi, masukkan informasi berikut:

   a. Dalam lingkup Sinkronisasi, pilih dari opsi berikut:

   - Kueri SQL —Masukkan pernyataan kueri SQL seperti operasi SELECT dan JOIN. Kueri SQL harus kurang dari 32KB. Amazon Kendra akan merayapi semua konten database yang cocok dengan kueri Anda.
   - Kolom kunci primer —Menyediakan kunci utama untuk tabel database. Ini mengidentifikasi tabel dalam database Anda.
   - Judul kolom —Berikan nama kolom judul dokumen dalam tabel database Anda.
   - Kolom tubuh —Berikan nama kolom badan dokumen dalam tabel database Anda.

   b. Dalam Konfigurasi tambahan — opsional, pilih dari opsi berikut untuk menyinkronkan konten tertentu alih-alih menyinkronkan semua file:

   - Kolom pendeteksi perubahan —Masukkan nama kolom yang Amazon Kendra akan digunakan untuk mendeteksi perubahan konten. Amazon Kendra akan mengindeks ulang konten ketika ada perubahan di salah satu kolom ini.
   - Kolom ID Pengguna —Masukkan nama kolom yang berisi ID Pengguna agar diizinkan mengakses konten.
   - Kolom Grup —Masukkan nama kolom yang berisi grup untuk diizinkan mengakses konten.
   - Kolom URL sumber —Masukkan nama kolom yang berisi URL Sumber yang akan diindeks.
   - Kolom stempel waktu —Masukkan nama kolom yang berisi stempel waktu. Amazon Kendra menggunakan informasi cap waktu untuk mendeteksi perubahan dalam konten Anda dan hanya menyinkronkan konten yang diubah.
   - Kolom zona waktu —Masukkan nama kolom yang berisi zona waktu untuk konten yang akan dirayapi.

- Format stempel waktu —Masukkan nama kolom yang berisi format cap waktu yang akan digunakan untuk mendeteksi perubahan konten dan menyinkronkan ulang konten Anda.

c. Mode sinkronisasi —Pilih cara memperbarui indeks saat konten sumber data berubah. Saat Anda menyinkronkan sumber data Amazon Kendra untuk pertama kalinya, semua konten dirayapi dan diindeks secara default. Anda harus menjalankan sinkronisasi penuh data Anda jika sinkronisasi awal Anda gagal, bahkan jika Anda tidak memilih sinkronisasi penuh sebagai opsi mode sinkronisasi Anda.

- Sinkronisasi penuh: Indeks baru semua konten, ganti konten yang ada setiap kali sumber data Anda disinkronkan dengan indeks Anda.
- Sinkronisasi baru yang dimodifikasi: Indeks hanya konten baru dan yang dimodifikasi setiap kali sumber data Anda disinkronkan dengan indeks Anda. Amazon Kendra dapat menggunakan mekanisme sumber data Anda untuk melacak perubahan konten dan mengindeks konten yang berubah sejak sinkronisasi terakhir.
- Sinkronisasi baru, dimodifikasi, dihapus: Indeks hanya konten baru, dimodifikasi, dan dihapus setiap kali sumber data Anda disinkronkan dengan indeks Anda. Amazon Kendra dapat menggunakan mekanisme sumber data Anda untuk melacak perubahan konten dan mengindeks konten yang berubah sejak sinkronisasi terakhir.

d. Dalam jadwal berjalan Sinkronisasi, untuk Frekuensi —Seberapa sering Amazon Kendra akan disinkronkan dengan sumber data Anda.

e. Pilih Berikutnya.

8. Pada halaman Setel pemetaan bidang, masukkan informasi berikut:

a. Pilih dari bidang sumber data default yang dihasilkan - ID dokumen, judul dokumen, dan URL Sumber - yang ingin Anda petakan ke Amazon Kendra indeks.

b. Tambahkan bidang —Untuk menambahkan bidang sumber data kustom untuk membuat nama bidang indeks untuk dipetakan dan tipe data bidang.

c. Pilih Berikutnya.

9. Pada halaman Tinjau dan buat, periksa apakah informasi yang Anda masukkan sudah benar dan kemudian pilih Tambahkan sumber data. Anda juga dapat memilih untuk mengedit informasi Anda dari halaman ini. Sumber data Anda akan muncul di halaman Sumber data setelah sumber data berhasil ditambahkan.

API

Untuk terhubung Amazon Kendra ke Oracle Database

Anda harus menentukan yang berikut menggunakan TemplateConfigurationAPI:

- Sumber data —Tentukan tipe sumber data seperti `JDBC` saat Anda menggunakan skema TemplateConfigurationJSON. Juga tentukan sumber data seperti `TEMPLATE` saat Anda memanggil CreateDataSourceAPI.
- Jenis database —Anda harus menentukan jenis database sebagai`oracle`.
- Kueri SQL —Tentukan pernyataan kueri SQL seperti operasi SELECT dan JOIN. Kueri SQL harus kurang dari 32KB. Amazon Kendra akan merayapi semua konten database yang cocok dengan kueri Anda.
- Mode sinkronisasi —Tentukan cara Amazon Kendra memperbarui indeks Anda saat konten sumber data Anda berubah. Saat Anda menyinkronkan sumber data Amazon Kendra untuk pertama kalinya, semua konten dirayapi dan diindeks secara default. Anda harus menjalankan sinkronisasi penuh data Anda jika sinkronisasi awal Anda gagal, bahkan jika Anda tidak memilih sinkronisasi penuh sebagai opsi mode sinkronisasi Anda. Anda dapat memilih antara:
  - `FORCED_FULL_CRAWL`untuk mengindeks semua konten baru, mengganti konten yang ada setiap kali sumber data Anda disinkronkan dengan indeks Anda.
  - `FULL_CRAWL`untuk mengindeks hanya konten baru, dimodifikasi, dan dihapus setiap kali sumber data Anda disinkronkan dengan indeks Anda. Amazon Kendra dapat menggunakan mekanisme sumber data Anda untuk melacak perubahan konten dan mengindeks konten yang berubah sejak sinkronisasi terakhir.
  - `CHANGE_LOG`untuk mengindeks hanya konten baru dan yang dimodifikasi setiap kali sumber data Anda disinkronkan dengan indeks Anda. Amazon Kendra dapat menggunakan mekanisme sumber data Anda untuk melacak perubahan konten dan mengindeks konten yang berubah sejak sinkronisasi terakhir.
- Rahasia Nama Sumber Daya Amazon (ARN) —Berikan Nama Sumber Daya Amazon (ARN) Secrets Manager rahasia yang berisi kredensyal otentikasi yang Anda buat di akun Anda. Oracle Database Rahasianya disimpan dalam struktur JSON dengan kunci berikut:

```
{
    "user name": "database user name",
    "password": "password"
}
```

> **Note**
>
> Kami menyarankan Anda secara teratur menyegarkan atau memutar kredensil dan rahasia Anda. Berikan hanya tingkat akses yang diperlukan untuk keamanan Anda sendiri. Kami tidak menyarankan Anda menggunakan kembali kredensyal dan rahasia di seluruh sumber data, dan konektor versi 1.0 dan 2.0 (jika berlaku).

- IAM peran —Tentukan `RoleArn` kapan Anda menelepon `CreateDataSource` untuk memberikan IAM peran dengan izin untuk mengakses Secrets Manager rahasia Anda dan memanggil API publik yang diperlukan untuk Oracle Database konektor dan. Amazon Kendra Untuk informasi selengkapnya, lihat IAM peran untuk sumber Oracle Database data.

Anda juga dapat menambahkan fitur opsional berikut:

- Virtual Private Cloud (VPC) **`VpcConfiguration`** —Tentukan kapan Anda menelepon. `CreateDataSource` Untuk informasi selengkapnya, lihat Mengkonfigurasi Amazon Kendra untuk menggunakan Amazon VPC.
- Filter penyertaan dan pengecualian —Anda dapat menentukan apakah akan menyertakan konten tertentu menggunakan ID pengguna, grup, URL sumber, stempel waktu, dan zona waktu.
- Pemfilteran konteks pengguna dan kontrol akses —Amazon Kendra meng-crawl daftar kontrol akses (ACL) untuk dokumen Anda, jika Anda memiliki ACL untuk dokumen Anda. Informasi ACL digunakan untuk memfilter hasil pencarian berdasarkan pengguna atau akses grup mereka ke dokumen. Untuk informasi selengkapnya, lihat Pemfilteran konteks pengguna.
- Pemetaan bidang —Pilih untuk memetakan bidang sumber Oracle Database data Anda ke bidang indeks Anda Amazon Kendra . Untuk informasi lebih lanjut, lihat Memetakan bidang sumber data.

> **Note**
>
> Bidang badan dokumen atau badan dokumen yang setara untuk dokumen Anda diperlukan Amazon Kendra untuk mencari dokumen Anda. Anda harus memetakan nama bidang badan dokumen Anda di sumber data Anda ke nama bidang indeks_`document_body`. Semua kolom lain bersifat opsional.

Untuk daftar kunci JSON penting lainnya untuk dikonfigurasi, lihatSkema templat Oracle Database.

Catatan

- Baris database yang dihapus tidak akan dilacak saat Amazon Kendra memeriksa konten yang diperbarui.
- Ukuran nama bidang dan nilai dalam deretan database Anda tidak dapat melebihi 400KB.
- Jika Anda memiliki sejumlah besar data dalam sumber data database Anda, dan tidak Amazon Kendra ingin mengindeks semua konten database Anda setelah sinkronisasi pertama, Anda dapat memilih untuk menyinkronkan hanya dokumen baru, dimodifikasi, atau dihapus.
- Sebagai praktik terbaik, sediakan Amazon Kendra kredensil basis data hanya-baca.
- Sebagai praktik terbaik, hindari menambahkan tabel dengan data sensitif atau informasi identitas pribadi (PII).

PostgreSQL

PostgreSQLadalah sistem manajemen database open source. Jika Anda adalah PostgreSQL pengguna, Anda dapat menggunakan Amazon Kendra untuk mengindeks sumber PostgreSQL data Anda. Konektor sumber Amazon Kendra PostgreSQL data mendukung PostgreSQL 9.6.

Anda dapat terhubung Amazon Kendra ke sumber PostgreSQL data menggunakan Amazon Kendra konsol dan TemplateConfigurationAPI.

Untuk memecahkan masalah konektor sumber Amazon Kendra PostgreSQL data Anda, lihat. Mengatasi masalah sumber data

Topik

- Fitur yang didukung
- Prasyarat
- Instruksi koneksi
- Catatan

Fitur yang didukung

- Pemetaan lapangan

- Pemfilteran konteks pengguna
- Filter inklusi/pengecualian
- Sinkronisasi konten penuh dan tambahan
- Cloud privat virtual (VPC)

Prasyarat

Sebelum Anda dapat menggunakan Amazon Kendra untuk mengindeks sumber PostgreSQL data Anda, buat perubahan ini di akun PostgreSQL dan AWS akun Anda.

DiPostgreSQL, pastikan Anda memiliki:

- Mencatat nama pengguna dan kata sandi database Anda.

> **Important**
>
> Sebagai praktik terbaik, sediakan Amazon Kendra kredensil basis data hanya-baca.

- Menyalin url, port, dan instance host database Anda.
- Memeriksa setiap dokumen unik di dalam PostgreSQL dan di seluruh sumber data lain yang Anda rencanakan untuk digunakan untuk indeks yang sama. Setiap sumber data yang ingin Anda gunakan untuk indeks tidak boleh berisi dokumen yang sama di seluruh sumber data. ID dokumen bersifat global untuk indeks dan harus unik per indeks.

Di dalam Anda Akun AWS, pastikan Anda memiliki:

- Membuat Amazon Kendra indeks dan, jika menggunakan API, mencatat ID indeks.
- Membuat IAM peran untuk sumber data Anda dan, jika menggunakan API, catat ARN peran tersebut IAM .

> **Note**
>
> Jika Anda mengubah jenis otentikasi dan kredensyal, Anda harus memperbarui IAM peran Anda untuk mengakses ID rahasia yang benar AWS Secrets Manager .

- Menyimpan kredensyal PostgreSQL otentikasi Anda AWS Secrets Manager secara rahasia dan, jika menggunakan API, catat ARN rahasia tersebut.

> **Note**
>
> Kami menyarankan Anda secara teratur menyegarkan atau memutar kredensil dan rahasia Anda. Berikan hanya tingkat akses yang diperlukan untuk keamanan Anda sendiri. Kami tidak menyarankan Anda menggunakan kembali kredensyal dan rahasia di seluruh sumber data, dan konektor versi 1.0 dan 2.0 (jika berlaku).

Jika Anda tidak memiliki IAM peran atau rahasia yang ada, Anda dapat menggunakan konsol untuk membuat IAM peran dan Secrets Manager rahasia baru saat menghubungkan sumber PostgreSQL data Amazon Kendra. Jika Anda menggunakan API, Anda harus memberikan ARN IAM peran dan Secrets Manager rahasia yang ada, dan ID indeks.

Instruksi koneksi

Untuk terhubung Amazon Kendra ke sumber PostgreSQL data Anda, Anda harus memberikan rincian PostgreSQL kredensyal Anda sehingga Amazon Kendra dapat mengakses data Anda. Jika Anda belum mengkonfigurasi PostgreSQL untuk Amazon Kendra lihatPrasyarat.

Console

Untuk terhubung Amazon Kendra ke PostgreSQL

1. Masuk ke AWS Management Console dan buka Amazon Kendra konsol.
2. Dari panel navigasi kiri, pilih Indeks dan kemudian pilih indeks yang ingin Anda gunakan dari daftar indeks.

   > **Note**
   >
   > Anda dapat memilih untuk mengonfigurasi atau mengedit pengaturan kontrol akses Pengguna Anda di bawah Pengaturan indeks.

3. Pada halaman Memulai, pilih Tambahkan sumber data.
4. Pada halaman Tambahkan sumber data, pilih PostgreSQLkonektor, lalu pilih Tambah konektor.
5. Pada halaman Tentukan detail sumber data, masukkan informasi berikut:

a. Di Nama dan deskripsi, untuk Nama sumber data —Masukkan nama untuk sumber data Anda. Anda dapat memasukkan tanda hubung tetapi bukan spasi.

b. (Opsional) Deskripsi —Masukkan deskripsi opsional untuk sumber data Anda.

c. Dalam Bahasa default —Pilih bahasa untuk memfilter dokumen Anda untuk indeks. Kecuali Anda menentukan sebaliknya, bahasa default ke bahasa Inggris. Bahasa yang ditentukan dalam metadata dokumen mengesampingkan bahasa yang dipilih.

d. Di Tag, untuk Tambahkan tag baru —Sertakan tag opsional untuk mencari dan memfilter sumber daya Anda atau melacak AWS biaya Anda.

e. Pilih Berikutnya.

6. Pada halaman Tentukan akses dan keamanan, masukkan informasi berikut:

a. Di Sumber, masukkan informasi berikut:

b. Host — Masukkan nama host database.

c. Port — Masukkan port database.

d. Instance - Masukkan instance database.

e. Aktifkan lokasi sertifikat SSL —Pilih untuk memasukkan Amazon S3 jalur ke file sertifikat SSL Anda.

f. Dalam Otentikasi —masukkan informasi berikut:

- AWS Secrets Manager rahasia —Pilih rahasia yang ada atau buat Secrets Manager rahasia baru untuk menyimpan kredensyal PostgreSQL otentikasi Anda. Jika Anda memilih untuk membuat rahasia baru, jendela AWS Secrets Manager rahasia terbuka.

  A. Masukkan informasi berikut di jendela Buat AWS Secrets Manager rahasia:

     I. Nama rahasia —Nama untuk rahasiamu. Awalan 'AmazonKendra-PostgreSQL -' secara otomatis ditambahkan ke nama rahasia Anda.

     II. Untuk nama pengguna Database, dan Kata Sandi —Masukkan nilai kredensi otentikasi yang Anda salin dari database Anda.

  B. Pilih Simpan.

g. Virtual Private Cloud (VPC) —Anda dapat memilih untuk menggunakan VPC. Jika demikian, Anda harus menambahkan Subnet dan grup keamanan VPC.

h. IAM peran —Pilih peran yang sudah ada atau buat IAM IAM peran baru untuk mengakses kredensi repositori dan mengindeks konten Anda.

> **Note**
>
> IAM peran yang digunakan untuk indeks tidak dapat digunakan untuk sumber data. Jika Anda tidak yakin apakah peran yang ada digunakan untuk indeks atau FAQ, pilih Buat peran baru untuk menghindari kesalahan.

i. Pilih Berikutnya.

7. Pada halaman Konfigurasi pengaturan sinkronisasi, masukkan informasi berikut:

   a. Dalam lingkup Sinkronisasi, pilih dari opsi berikut:

   - Kueri SQL —Masukkan pernyataan kueri SQL seperti operasi SELECT dan JOIN. Kueri SQL harus kurang dari 32KB. Amazon Kendra akan merayapi semua konten database yang cocok dengan kueri Anda.
   - Kolom kunci primer —Berikan kunci utama untuk tabel database. Ini mengidentifikasi tabel dalam database Anda.
   - Judul kolom —Berikan nama kolom judul dokumen dalam tabel database Anda.
   - Kolom tubuh —Berikan nama kolom badan dokumen dalam tabel database Anda.

   b. Dalam Konfigurasi tambahan — opsional, pilih dari opsi berikut untuk menyinkronkan konten tertentu alih-alih menyinkronkan semua file:

   - Kolom pendeteksi perubahan —Masukkan nama kolom yang Amazon Kendra akan digunakan untuk mendeteksi perubahan konten. Amazon Kendra akan mengindeks ulang konten ketika ada perubahan di salah satu kolom ini.
   - Kolom ID Pengguna —Masukkan nama kolom yang berisi ID Pengguna agar diizinkan mengakses konten.
   - Kolom Grup —Masukkan nama kolom yang berisi grup untuk diizinkan mengakses konten.
   - Kolom URL sumber —Masukkan nama kolom yang berisi URL Sumber yang akan diindeks.
   - Kolom stempel waktu —Masukkan nama kolom yang berisi stempel waktu. Amazon Kendra menggunakan informasi cap waktu untuk mendeteksi perubahan dalam konten Anda dan hanya menyinkronkan konten yang diubah.

- Kolom zona waktu —Masukkan nama kolom yang berisi zona waktu untuk konten yang akan dirayapi.
- Format stempel waktu —Masukkan nama kolom yang berisi format cap waktu yang akan digunakan untuk mendeteksi perubahan konten dan menyinkronkan ulang konten Anda.

c. Mode sinkronisasi —Pilih cara memperbarui indeks saat konten sumber data berubah. Saat Anda menyinkronkan sumber data Amazon Kendra untuk pertama kalinya, semua konten dirayapi dan diindeks secara default. Anda harus menjalankan sinkronisasi penuh data Anda jika sinkronisasi awal Anda gagal, bahkan jika Anda tidak memilih sinkronisasi penuh sebagai opsi mode sinkronisasi Anda.

- Sinkronisasi penuh: Indeks baru semua konten, ganti konten yang ada setiap kali sumber data Anda disinkronkan dengan indeks Anda.
- Sinkronisasi baru yang dimodifikasi: Indeks hanya konten baru dan yang dimodifikasi setiap kali sumber data Anda disinkronkan dengan indeks Anda. Amazon Kendra dapat menggunakan mekanisme sumber data Anda untuk melacak perubahan konten dan mengindeks konten yang berubah sejak sinkronisasi terakhir.
- Sinkronisasi baru, dimodifikasi, dihapus: Indeks hanya konten baru, dimodifikasi, dan dihapus setiap kali sumber data Anda disinkronkan dengan indeks Anda. Amazon Kendra dapat menggunakan mekanisme sumber data Anda untuk melacak perubahan konten dan mengindeks konten yang berubah sejak sinkronisasi terakhir.

d. Dalam jadwal berjalan Sinkronisasi, untuk Frekuensi —Seberapa sering Amazon Kendra akan disinkronkan dengan sumber data Anda.

e. Pilih Berikutnya.

8. Pada halaman Setel pemetaan bidang, masukkan informasi berikut:

a. Pilih dari bidang sumber data default yang dihasilkan - ID dokumen, judul dokumen, dan URL Sumber - yang ingin Anda petakan ke Amazon Kendra indeks.

b. Tambahkan bidang —Untuk menambahkan bidang sumber data kustom untuk membuat nama bidang indeks untuk dipetakan dan tipe data bidang.

c. Pilih Berikutnya.

9. Pada halaman Tinjau dan buat, periksa apakah informasi yang Anda masukkan sudah benar dan kemudian pilih Tambahkan sumber data. Anda juga dapat memilih untuk mengedit informasi Anda dari halaman ini. Sumber data Anda akan muncul di halaman Sumber data setelah sumber data berhasil ditambahkan.

API

Untuk terhubung Amazon Kendra ke PostgreSQL

Anda harus menentukan yang berikut menggunakan TemplateConfigurationAPI:

- Sumber data —Tentukan tipe sumber data seperti `JDBC` saat Anda menggunakan skema TemplateConfigurationJSON. Tentukan juga sumber data seperti `TEMPLATE` saat Anda memanggil CreateDataSourceAPI.
- Jenis database —Anda harus menentukan jenis database sebagai`postgresql`.
- Kueri SQL —Tentukan pernyataan kueri SQL seperti operasi SELECT dan JOIN. Kueri SQL harus kurang dari 32KB. Amazon Kendra akan merayapi semua konten database yang cocok dengan kueri Anda.
- Mode sinkronisasi —Tentukan cara Amazon Kendra memperbarui indeks Anda saat konten sumber data Anda berubah. Saat Anda menyinkronkan sumber data Amazon Kendra untuk pertama kalinya, semua konten dirayapi dan diindeks secara default. Anda harus menjalankan sinkronisasi penuh data Anda jika sinkronisasi awal Anda gagal, bahkan jika Anda tidak memilih sinkronisasi penuh sebagai opsi mode sinkronisasi Anda. Anda dapat memilih antara:
  - `FORCED_FULL_CRAWL`untuk mengindeks semua konten baru, mengganti konten yang ada setiap kali sumber data Anda disinkronkan dengan indeks Anda.
  - `FULL_CRAWL`untuk mengindeks hanya konten baru, dimodifikasi, dan dihapus setiap kali sumber data Anda disinkronkan dengan indeks Anda. Amazon Kendra dapat menggunakan mekanisme sumber data Anda untuk melacak perubahan konten dan mengindeks konten yang berubah sejak sinkronisasi terakhir.
  - `CHANGE_LOG`untuk mengindeks hanya konten baru dan yang dimodifikasi setiap kali sumber data Anda disinkronkan dengan indeks Anda. Amazon Kendra dapat menggunakan mekanisme sumber data Anda untuk melacak perubahan konten dan mengindeks konten yang berubah sejak sinkronisasi terakhir.
- Rahasia Nama Sumber Daya Amazon (ARN) —Berikan Nama Sumber Daya Amazon (ARN) Secrets Manager rahasia yang berisi kredensyal otentikasi yang Anda buat di akun Anda. PostgreSQL Rahasianya disimpan dalam struktur JSON dengan kunci berikut:

```
{
    "user name": "database user name",
    "password": "password"
}
```

> **Note**
>
> Kami menyarankan Anda secara teratur menyegarkan atau memutar kredensil dan rahasia Anda. Berikan hanya tingkat akses yang diperlukan untuk keamanan Anda sendiri. Kami tidak menyarankan Anda menggunakan kembali kredensyal dan rahasia di seluruh sumber data, dan konektor versi 1.0 dan 2.0 (jika berlaku).

- IAM peran —Tentukan `RoleArn` kapan Anda menelepon `CreateDataSource` untuk memberikan IAM peran dengan izin untuk mengakses Secrets Manager rahasia Anda dan memanggil API publik yang diperlukan untuk PostgreSQL konektor dan. Amazon Kendra Untuk informasi selengkapnya, lihat IAM peran untuk sumber PostgreSQL data.

Anda juga dapat menambahkan fitur opsional berikut:

- Virtual Private Cloud (VPC) **`VpcConfiguration`** —Tentukan kapan Anda menelepon. `CreateDataSource` Untuk informasi selengkapnya, lihat Mengkonfigurasi Amazon Kendra untuk menggunakan Amazon VPC.
- Filter penyertaan dan pengecualian —Anda dapat menentukan apakah akan menyertakan konten tertentu menggunakan ID pengguna, grup, URL sumber, stempel waktu, dan zona waktu.
- Pemfilteran konteks pengguna dan kontrol akses —Amazon Kendra meng-crawl daftar kontrol akses (ACL) untuk dokumen Anda, jika Anda memiliki ACL untuk dokumen Anda. Informasi ACL digunakan untuk memfilter hasil pencarian berdasarkan pengguna atau akses grup mereka ke dokumen. Untuk informasi selengkapnya, lihat Pemfilteran konteks pengguna.
- Pemetaan bidang —Pilih untuk memetakan bidang sumber PostgreSQL data Anda ke bidang indeks Anda Amazon Kendra . Untuk informasi lebih lanjut, lihat Memetakan bidang sumber data.

> **Note**
>
> Bidang badan dokumen atau badan dokumen yang setara untuk dokumen Anda diperlukan Amazon Kendra untuk mencari dokumen Anda. Anda harus memetakan nama bidang badan dokumen Anda di sumber data Anda ke nama bidang indeks_`document_body`. Semua kolom lain bersifat opsional.

Untuk daftar kunci JSON penting lainnya untuk dikonfigurasi, lihatSkema Templat PostgreSQL.

Catatan

- Baris database yang dihapus tidak akan dilacak saat Amazon Kendra memeriksa konten yang diperbarui.
- Ukuran nama bidang dan nilai dalam deretan database Anda tidak dapat melebihi 400KB.
- Jika Anda memiliki sejumlah besar data dalam sumber data database Anda, dan tidak Amazon Kendra ingin mengindeks semua konten database Anda setelah sinkronisasi pertama, Anda dapat memilih untuk menyinkronkan hanya dokumen baru, dimodifikasi, atau dihapus.
- Sebagai praktik terbaik, sediakan Amazon Kendra kredensil basis data hanya-baca.
- Sebagai praktik terbaik, hindari menambahkan tabel dengan data sensitif atau informasi identitas pribadi (PII).

Menyindir

Quip adalah perangkat lunak produktivitas kolaboratif yang menawarkan kemampuan penulisan dokumen waktu nyata. Anda dapat menggunakan Amazon Kendra untuk mengindeks folder Quip, file, komentar file, ruang obrolan, dan lampiran Quip Anda.

Anda dapat terhubung Amazon Kendra ke sumber data Quip menggunakan Amazon Kendra konsol dan QuipConfigurationAPI.

Untuk memecahkan masalah konektor sumber data Amazon Kendra Quip, lihat. Mengatasi masalah sumber data

Topik

- Fitur yang didukung
- Prasyarat
- Instruksi koneksi
- Pelajari selengkapnya

Fitur yang didukung

Amazon Kendra Konektor sumber data Quip mendukung fitur-fitur berikut:

- Pemetaan lapangan
- Pemfilteran konteks pengguna
- Filter inklusi/pengecualian
- Cloud privat virtual (VPC)

Prasyarat

Sebelum Anda dapat menggunakan Amazon Kendra untuk mengindeks sumber data Quip Anda, buat perubahan ini di Quip dan AWS akun Anda.

Di Quip, pastikan Anda memiliki:

- Akun Quip dengan izin administratif.
- Kredensi otentikasi Quip dibuat yang menyertakan token akses pribadi. Lihat dokumentasi Quip tentang otentikasi untuk informasi selengkapnya.
- Menyalin domain situs Quip Anda. Misalnya, *`https://quip-company.quipdomain.com/browse`* di mana *`quipdomain adalah domain`*.
- Memeriksa setiap dokumen unik di Quip dan di seluruh sumber data lain yang Anda rencanakan untuk digunakan untuk indeks yang sama. Setiap sumber data yang ingin Anda gunakan untuk indeks tidak boleh berisi dokumen yang sama di seluruh sumber data. ID dokumen bersifat global untuk indeks dan harus unik per indeks.

Di dalam Anda Akun AWS, pastikan Anda memiliki:

- Membuat Amazon Kendra indeks dan, jika menggunakan API, mencatat ID indeks.
- Membuat IAM peran untuk sumber data Anda dan, jika menggunakan API, catat ARN peran tersebut IAM .

> **Note**
>
> Jika Anda mengubah jenis otentikasi dan kredensyal, Anda harus memperbarui IAM peran Anda untuk mengakses ID rahasia yang benar AWS Secrets Manager .

- Menyimpan kredensi otentikasi Quip Anda secara AWS Secrets Manager rahasia dan, jika menggunakan API, catat ARN rahasia tersebut.

> **Note**
>
> Kami menyarankan Anda secara teratur menyegarkan atau memutar kredensil dan rahasia Anda. Berikan hanya tingkat akses yang diperlukan untuk keamanan Anda sendiri. Kami tidak menyarankan Anda menggunakan kembali kredensyal dan rahasia di seluruh sumber data, dan konektor versi 1.0 dan 2.0 (jika berlaku).

Jika Anda tidak memiliki IAM peran atau rahasia yang ada, Anda dapat menggunakan konsol untuk membuat IAM peran dan Secrets Manager rahasia baru saat Anda menghubungkan sumber data Quip. Amazon Kendra Jika Anda menggunakan API, Anda harus memberikan ARN IAM peran dan Secrets Manager rahasia yang ada, dan ID indeks.

Instruksi koneksi

Untuk terhubung Amazon Kendra ke sumber data Quip Anda, Anda harus memberikan rincian yang diperlukan dari sumber data Quip Anda sehingga Amazon Kendra dapat mengakses data Anda. Jika Anda belum mengkonfigurasi Quip untuk Amazon Kendra, lihatPrasyarat.

Console

Untuk terhubung Amazon Kendra ke Quip

1. Masuk ke AWS Management Console dan buka Amazon Kendra konsol.
2. Dari panel navigasi kiri, pilih Indeks dan kemudian pilih indeks yang ingin Anda gunakan dari daftar indeks.

   > **Note**
   >
   > Anda dapat memilih untuk mengonfigurasi atau mengedit pengaturan kontrol akses Pengguna Anda di bawah Pengaturan indeks.

3. Pada halaman Memulai, pilih Tambahkan sumber data.
4. Pada halaman Tambah sumber data, pilih konektor Quip, lalu pilih Tambah konektor.
5. Pada halaman Tentukan detail sumber data, masukkan informasi berikut:

   a. Dalam Nama dan deskripsi, untuk Nama sumber data —Masukkan nama untuk sumber data Anda. Anda dapat memasukkan tanda hubung tetapi bukan spasi.

b. (Opsional) Deskripsi —Masukkan deskripsi opsional untuk sumber data Anda.

c. Dalam Bahasa default —Pilih bahasa untuk memfilter dokumen Anda untuk indeks. Kecuali Anda menentukan sebaliknya, bahasa default ke bahasa Inggris. Bahasa yang ditentukan dalam metadata dokumen mengesampingkan bahasa yang dipilih.

d. Di Tag, untuk Tambahkan tag baru —Sertakan tag opsional untuk mencari dan memfilter sumber daya Anda atau melacak AWS biaya Anda.

e. Pilih Berikutnya.

6. Pada halaman Tentukan akses dan keamanan, masukkan informasi berikut:

a. Nama domain Quip —Masukkan Quip yang Anda salin dari akun Quip Anda.

b. AWS Secrets Manager rahasia —Pilih rahasia yang ada atau buat Secrets Manager rahasia baru untuk menyimpan kredensyal otentikasi Quip Anda. Jika Anda memilih untuk membuat rahasia baru, jendela AWS Secrets Manager rahasia terbuka.

i. Masukkan informasi berikut di jendela Buat AWS Secrets Manager rahasia:

A. Nama rahasia —Nama untuk rahasiamu. Awalan 'AmazonKendra-Quip-' secara otomatis ditambahkan ke nama rahasia Anda.

B. Token Quip —Masukkan token akses pribadi Quip yang Anda buat di akun Quip Anda.

ii. Pilih Simpan.

c. Virtual Private Cloud (VPC) —Anda dapat memilih untuk menggunakan VPC. Jika demikian, Anda harus menambahkan Subnet dan grup keamanan VPC.

d. IAM peran —Pilih peran yang sudah ada atau buat IAM IAM peran baru untuk mengakses kredensi repositori dan mengindeks konten Anda.

> **Note**
>
> IAM peran yang digunakan untuk indeks tidak dapat digunakan untuk sumber data. Jika Anda tidak yakin apakah peran yang ada digunakan untuk indeks atau FAQ, pilih Buat peran baru untuk menghindari kesalahan.

e. Pilih Berikutnya.

7. Pada halaman Konfigurasi pengaturan sinkronisasi, masukkan informasi berikut:

a. Tambahkan ID folder Quip ke crawl —ID folder Quip yang ingin Anda jelajahi.

> **Note**
>
> Untuk merayapi folder root, termasuk semua sub-folder dan dokumen di dalamnya, masukkan ID folder root. Untuk merayapi sub-folder tertentu, tambahkan ID sub-folder tertentu.

b. Konfigurasi tambahan (tipe konten) —Masukkan jenis konten yang ingin dirayapi.

c. Pola Regex —Pola ekspresi reguler untuk menyertakan atau mengecualikan file tertentu. Anda dapat menambahkan hingga 100 pola.

d. Dalam jadwal berjalan Sinkronisasi, untuk Frekuensi —Pilih seberapa sering Amazon Kendra akan disinkronkan dengan sumber data Anda.

e. Pilih Berikutnya.

8. Pada halaman Setel pemetaan bidang, masukkan informasi berikut:

a. Pilih dari bidang sumber data default yang dihasilkan yang ingin Anda petakan untuk Amazon Kendra diindeks.

b. Tambahkan bidang —Untuk menambahkan bidang sumber data kustom untuk membuat nama bidang indeks untuk dipetakan dan tipe data bidang.

c. Pilih Berikutnya.

9. Pada halaman Tinjau dan buat, periksa apakah informasi yang Anda masukkan sudah benar dan kemudian pilih Tambahkan sumber data. Anda juga dapat memilih untuk mengedit informasi Anda dari halaman ini. Sumber data Anda akan muncul di halaman Sumber data setelah sumber data berhasil ditambahkan.

API

Untuk terhubung Amazon Kendra ke Quip

Anda harus menentukan yang berikut menggunakan QuipConfiguration API:

- Domain situs Quip —Misalnya, *`https://quip-company.quipdomain.com/browse`* di mana *`quipdomain adalah domain`*.
- Rahasia Nama Sumber Daya Amazon (ARN) —Berikan Nama Sumber Daya Amazon (ARN) Secrets Manager rahasia yang berisi kredensyal otentikasi untuk akun Quip Anda. Rahasianya disimpan dalam struktur JSON dengan kunci berikut:

```
{
    "accessToken": "token"
}
```

> **Note**
>
> Kami menyarankan Anda secara teratur menyegarkan atau memutar kredensil dan rahasia Anda. Berikan hanya tingkat akses yang diperlukan untuk keamanan Anda sendiri. Kami tidak menyarankan Anda menggunakan kembali kredensyal dan rahasia di seluruh sumber data, dan konektor versi 1.0 dan 2.0 (jika berlaku).

- IAM role —Tentukan `RoleArn` kapan Anda menelepon `CreateDataSource` untuk memberikan IAM peran dengan izin untuk mengakses Secrets Manager rahasia Anda dan memanggil API publik yang diperlukan untuk konektor Quip dan. Amazon Kendra Untuk informasi selengkapnya, lihat IAM peran untuk sumber data Quip.

Anda juga dapat menambahkan fitur opsional berikut:

- Virtual Private Cloud (VPC) —Tentukan `VpcConfiguration` sebagai bagian dari konfigurasi sumber data. Lihat Mengkonfigurasi Amazon Kendra untuk menggunakan VPC.
- Filter inklusi dan pengecualian —Tentukan apakah akan menyertakan atau mengecualikan file tertentu.

> **Note**
>
> Sebagian besar sumber data menggunakan pola ekspresi reguler, yang merupakan pola inklusi atau pengecualian yang disebut sebagai filter. Jika Anda menentukan filter inklusi, hanya konten yang cocok dengan filter inklusi yang diindeks. Dokumen apa pun yang tidak cocok dengan filter inklusi tidak diindeks. Jika Anda menentukan filter inklusi dan pengecualian, dokumen yang cocok dengan filter pengecualian tidak akan diindeks, meskipun sesuai dengan filter inklusi.

- Folder —Tentukan folder Quip dan subfolder yang ingin Anda indeks

> **Note**
>
> Untuk merayapi folder root, termasuk semua sub-folder dan dokumen di dalamnya, masukkan ID folder root. Untuk merayapi sub-folder tertentu, tambahkan ID sub-folder tertentu.

- Lampiran, ruang obrolan, komentar file —Pilih apakah akan menyertakan crawling lampiran, konten ruang obrolan, dan komentar file.
- Pemetaan bidang —Pilih untuk memetakan bidang sumber data Quip Anda ke bidang indeks Anda. Amazon Kendra Untuk informasi lebih lanjut, lihat Memetakan bidang sumber data.

> **Note**
>
> Bidang badan dokumen atau badan dokumen yang setara untuk dokumen Anda diperlukan Amazon Kendra untuk mencari dokumen Anda. Anda harus memetakan nama bidang badan dokumen Anda di sumber data Anda ke nama bidang indeks `_document_body`. Semua kolom lain bersifat opsional.

- Pemfilteran konteks pengguna dan kontrol akses —Amazon Kendra meng-crawl daftar kontrol akses (ACL) untuk dokumen Anda, jika Anda memiliki ACL untuk dokumen Anda. Informasi ACL digunakan untuk memfilter hasil pencarian berdasarkan pengguna atau akses grup mereka ke dokumen. Untuk informasi selengkapnya, lihat Pemfilteran konteks pengguna.

Pelajari selengkapnya

Untuk mempelajari lebih lanjut tentang mengintegrasikan Amazon Kendra dengan sumber data Quip, lihat:

- Cari pengetahuan dalam dokumen Quip dengan pencarian cerdas menggunakan konektor Quip untuk Amazon Kendra

Salesforce

Salesforce adalah alat manajemen hubungan pelanggan (CRM) untuk mengelola tim dukungan, penjualan, dan pemasaran. Anda dapat menggunakan Amazon Kendra untuk mengindeks objek standar Salesforce Anda dan bahkan objek kustom.

Anda dapat terhubung Amazon Kendra ke sumber data Salesforce menggunakan Amazon Kendra konsol, TemplateConfigurationAPI, atau API. SalesforceConfiguration

Amazon Kendra memiliki dua versi konektor Salesforce. Fitur yang didukung dari setiap versi meliputi:

Konektor Salesforce V1.0 /API SalesforceConfiguration

- Pemetaan lapangan
- Pemfilteran konteks pengguna
- Filter inklusi/pengecualian

Konektor Salesforce V2.0 /API TemplateConfiguration

- Pemetaan lapangan
- Pemfilteran konteks pengguna
- Perayapan identitas pengguna
- Filter inklusi/pengecualian
- Sinkronisasi konten penuh dan tambahan
- Perayapan lampiran entitas
- Cloud privat virtual (VPC)

> **Note**
>
> Support untuk konektor Salesforce V1.0/ SalesforceConfiguration API dijadwalkan berakhir pada tahun 2023. Kami merekomendasikan untuk bermigrasi ke atau menggunakan konektor Salesforce V2.0/API. TemplateConfiguration

Untuk memecahkan masalah konektor sumber data Amazon Kendra Salesforce Anda, lihat. Mengatasi masalah sumber data

Topik

- Konektor Salesforce V1.0
- Konektor Salesforce V2.0

Konektor Salesforce V1.0

Salesforce adalah alat manajemen hubungan pelanggan (CRM) untuk mengelola tim dukungan, penjualan, dan pemasaran. Anda dapat menggunakan Amazon Kendra untuk mengindeks objek standar Salesforce Anda dan bahkan objek kustom.

> **Important**
>
> Amazon Kendra menggunakan Salesforce API versi 48. Salesforce API membatasi jumlah permintaan yang dapat Anda buat per hari. Jika Salesforce melebihi permintaan tersebut, ia mencoba lagi sampai dapat melanjutkan.

> **Note**
>
> Support untuk konektor Salesforce V1.0/ SalesforceConfiguration API dijadwalkan berakhir pada tahun 2023. Kami merekomendasikan untuk bermigrasi ke atau menggunakan konektor Salesforce V2.0/API. TemplateConfiguration

Untuk memecahkan masalah konektor sumber data Amazon Kendra Salesforce Anda, lihat. Mengatasi masalah sumber data

Topik

Fitur yang didukung

Amazon Kendra Konektor sumber data Salesforce mendukung fitur-fitur berikut:

- Pemetaan lapangan
- Pemfilteran konteks pengguna
- Filter inklusi/pengecualian

Prasyarat

Sebelum Anda dapat menggunakan Amazon Kendra untuk mengindeks sumber data Salesforce Anda, buat perubahan ini di Salesforce dan akun Anda. AWS

Di Salesforce, pastikan Anda memiliki:

- Membuat akun Salesforce dan telah mencatat nama pengguna dan kata sandi yang Anda gunakan untuk terhubung ke Salesforce.
- Membuat akun Salesforce Connected App dengan OAuth diaktifkan dan telah menyalin kunci konsumen (ID klien) dan rahasia konsumen (rahasia klien) yang ditetapkan ke Aplikasi Salesforce Connected Anda. Lihat dokumentasi Salesforce di Aplikasi Terhubung untuk informasi selengkapnya.
- Menyalin token keamanan Salesforce yang terkait dengan akun yang digunakan untuk terhubung ke Salesforce.
- Menyalin URL instance Salesforce yang ingin Anda indeks. Biasanya, ini adalah *https://.salesforce.com/.* <company> Server harus menjalankan aplikasi yang terhubung dengan Salesforce.
- Menambahkan kredensyal ke server Salesforce Anda untuk pengguna dengan akses hanya-baca ke Salesforce dengan mengkloning ReadOnly profil dan kemudian menambahkan izin Lihat Semua Data dan Kelola Artikel. Kredensil ini mengidentifikasi pengguna yang membuat koneksi dan aplikasi terhubung Salesforce yang terhubung ke. Amazon Kendra
- Memeriksa setiap dokumen unik di Salesforce dan di seluruh sumber data lain yang Anda rencanakan untuk digunakan untuk indeks yang sama. Setiap sumber data yang ingin Anda gunakan untuk indeks tidak boleh berisi dokumen yang sama di seluruh sumber data. ID dokumen bersifat global untuk indeks dan harus unik per indeks.

Di dalam Anda Akun AWS, pastikan Anda memiliki:

- Membuat Amazon Kendra indeks dan, jika menggunakan API, mencatat ID indeks.
- Membuat IAM peran untuk sumber data Anda dan, jika menggunakan API, catat ARN peran tersebut IAM .

> **Note**
>
> Jika Anda mengubah jenis otentikasi dan kredensyal, Anda harus memperbarui IAM peran Anda untuk mengakses ID rahasia yang benar AWS Secrets Manager .

- Menyimpan kredensi otentikasi Salesforce Anda secara AWS Secrets Manager rahasia dan, jika menggunakan API, catat ARN rahasia tersebut.

> **Note**
>
> Kami menyarankan Anda secara teratur menyegarkan atau memutar kredensil dan rahasia Anda. Berikan hanya tingkat akses yang diperlukan untuk keamanan Anda sendiri. Kami tidak menyarankan Anda menggunakan kembali kredensyal dan rahasia di seluruh sumber data, dan konektor versi 1.0 dan 2.0 (jika berlaku).

Jika Anda tidak memiliki IAM peran atau rahasia yang ada, Anda dapat menggunakan konsol untuk membuat IAM peran dan Secrets Manager rahasia baru saat Anda menghubungkan sumber data Salesforce. Amazon Kendra Jika Anda menggunakan API, Anda harus memberikan ARN IAM peran dan Secrets Manager rahasia yang ada, dan ID indeks.

Instruksi koneksi

Untuk terhubung Amazon Kendra ke sumber data Salesforce Anda, Anda harus memberikan rincian yang diperlukan dari sumber data Salesforce Anda sehingga Amazon Kendra dapat mengakses data Anda. Jika Anda belum mengkonfigurasi Salesforce untuk Amazon Kendra lihat. Prasyarat

Console

Untuk terhubung Amazon Kendra ke Salesforce

1. Masuk ke Konsol AWS Manajemen dan buka Amazon Kendra konsol.
2. Dari panel navigasi kiri, pilih Indeks dan kemudian pilih indeks yang ingin Anda gunakan dari daftar indeks.

> **Note**
>
> Anda dapat memilih untuk mengonfigurasi atau mengedit pengaturan kontrol akses Pengguna Anda di bawah Pengaturan indeks.

3. Pada halaman Memulai, pilih Tambahkan sumber data.
4. Pada halaman Tambah sumber data, pilih Konektor Salesforce V1.0, lalu pilih Tambah konektor.
5. Pada halaman Tentukan detail sumber data, masukkan informasi berikut:
   a. Nama sumber data —Masukkan nama untuk sumber data Anda. Anda dapat memasukkan tanda hubung tetapi bukan spasi.
   b. (Opsional) Deskripsi —Masukkan deskripsi opsional untuk sumber data Anda.
   c. Bahasa default — Bahasa untuk memfilter dokumen Anda untuk indeks. Kecuali Anda menentukan sebaliknya, bahasa default ke bahasa Inggris. Bahasa yang ditentukan dalam metadata menggantikan bahasa yang dipilih.
   d. Tambahkan tag baru —Tag untuk mencari dan memfilter sumber daya Anda atau melacak biaya bersama Anda.
   e. Pilih Berikutnya.
6. Pada halaman Tentukan akses dan keamanan, masukkan informasi berikut:
   a. URL Salesforce —Masukkan URL instance untuk situs Salesforce yang ingin Anda indeks.
   b. Untuk Jenis otentikasi, pilih antara Existing dan New untuk menyimpan kredensyal otentikasi Salesforce Anda. Jika Anda memilih untuk membuat rahasia baru, jendela AWS Secrets Manager rahasia terbuka.
      - Masukkan informasi berikut di jendela Buat AWS Secrets Manager rahasia:
        A. Nama rahasia —Nama untuk rahasiamu. Awalan 'AmazonKendra-Salesforce-' secara otomatis ditambahkan ke nama rahasia Anda.
        B. Untuk Nama Pengguna, Kata Sandi, Token keamanan, Kunci konsumen, Rahasia konsumen, dan URL Otentikasi —Masukkan nilai kredensi otentikasi yang Anda buat di akun Salesforce Anda.
        C. Pilih Simpan otentikasi.

c. IAM peran —Pilih peran yang sudah ada atau buat IAM IAM peran baru untuk mengakses kredensi repositori dan mengindeks konten Anda.

> **Note**
>
> IAM peran yang digunakan untuk indeks tidak dapat digunakan untuk sumber data. Jika Anda tidak yakin apakah peran yang ada digunakan untuk indeks atau FAQ, pilih Buat peran baru untuk menghindari kesalahan.

d. Pilih Berikutnya.

7. Pada halaman Konfigurasi pengaturan sinkronisasi, masukkan informasi berikut:

a. Untuk lampiran Crawl —Pilih untuk meng-crawl semua objek, artikel, dan feed yang dilampirkan.

b. Untuk objek Standar, artikel Pengetahuan, dan umpan obrolan —Pilih entitas Salesforce atau jenis konten yang ingin dirayapi.

> **Note**
>
> Anda harus memberikan informasi konfigurasi untuk mengindeks setidaknya satu objek standar, artikel pengetahuan, atau umpan obrolan. Jika Anda memilih untuk merayapi artikel Pengetahuan, Anda harus menentukan jenis artikel pengetahuan yang akan diindeks, nama artikel, dan apakah akan mengindeks bidang standar semua artikel pengetahuan atau hanya bidang jenis artikel kustom. Jika Anda memilih untuk mengindeks artikel kustom, Anda harus menentukan nama internal dari jenis artikel. Anda dapat menentukan hingga 10 jenis artikel.

c. Frekuensi —Seberapa sering Amazon Kendra akan disinkronkan dengan sumber data Anda.

d. Pilih Berikutnya.

8. Pada halaman Setel pemetaan bidang, masukkan informasi berikut:

a. Untuk artikel pengetahuan Standar, Lampiran objek standar, dan Pemetaan bidang yang disarankan tambahan —Pilih dari bidang sumber data default Amazon Kendra yang dihasilkan yang ingin Anda petakan ke indeks Anda.

> **Note**
>
> Diperlukan pemetaan `_document_body` indeks. Anda tidak dapat mengubah pemetaan antara `Salesforce ID` bidang dan Amazon Kendra `_document_id` bidang.

b. Tambahkan bidang —Untuk menambahkan bidang sumber data kustom untuk membuat nama bidang indeks untuk dipetakan dan tipe data bidang.

c. Pilih Berikutnya.

9. Pada halaman Tinjau dan buat, periksa apakah informasi yang Anda masukkan sudah benar dan kemudian pilih Tambahkan sumber data. Anda juga dapat memilih untuk mengedit informasi Anda dari halaman ini. Sumber data Anda akan muncul di halaman Sumber data setelah sumber data berhasil ditambahkan.

API

Untuk terhubung Amazon Kendra ke Salesforce

Anda harus menentukan SalesforceConfigurationAPI berikut ini:

- URL Server —URL contoh untuk situs Salesforce yang ingin Anda indeks.
- Rahasia Nama Sumber Daya Amazon (ARN) —Berikan Nama Sumber Daya Amazon (ARN) Secrets Manager rahasia yang berisi kredensyal otentikasi untuk akun Salesforce Anda. Rahasianya disimpan dalam struktur JSON dengan kunci berikut:

```
{
    "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"
}
```

> **Note**
>
> Kami menyarankan Anda secara teratur menyegarkan atau memutar kredensil dan rahasia Anda. Berikan hanya tingkat akses yang diperlukan untuk keamanan Anda sendiri. Kami tidak menyarankan Anda menggunakan kembali kredensyal dan rahasia di seluruh sumber data, dan konektor versi 1.0 dan 2.0 (jika berlaku).

- IAM peran —Tentukan `RoleArn` kapan Anda menelepon `CreateDataSource` untuk memberikan IAM peran dengan izin untuk mengakses Secrets Manager rahasia Anda dan memanggil API publik yang diperlukan untuk konektor Salesforce dan. Amazon Kendra Untuk informasi selengkapnya, lihat IAM peran untuk sumber data Salesforce.
- Anda harus memberikan informasi konfigurasi untuk mengindeks setidaknya satu objek standar, artikel pengetahuan, atau umpan obrolan.
  - Objek standar —Jika Anda memilih untuk merayapi objek Standar, Anda harus menentukan nama objek standar dan nama bidang dalam tabel objek standar yang berisi konten dokumen.
  - Artikel pengetahuan —Jika Anda memilih untuk merayapi artikel Pengetahuan, Anda harus menentukan jenis artikel pengetahuan yang akan diindeks, status artikel pengetahuan yang akan diindeks, dan apakah akan mengindeks bidang standar semua artikel pengetahuan atau hanya bidang jenis artikel khusus.
  - Umpan obrolan —Jika Anda memilih untuk merayapi umpan Chatter, Anda harus menentukan nama kolom dalam tabel Salesforce FeedItem yang berisi konten yang akan diindeks.

Anda juga dapat menambahkan fitur opsional berikut:

- Filter inklusi dan pengecualian —Tentukan apakah akan menyertakan atau mengecualikan lampiran file tertentu.

> **Note**
>
> Sebagian besar sumber data menggunakan pola ekspresi reguler, yang merupakan pola inklusi atau pengecualian yang disebut sebagai filter. Jika Anda menentukan filter inklusi, hanya konten yang cocok dengan filter inklusi yang diindeks. Dokumen apa pun yang tidak cocok dengan filter inklusi tidak diindeks. Jika Anda menentukan filter inklusi

dan pengecualian, dokumen yang cocok dengan filter pengecualian tidak akan diindeks, meskipun sesuai dengan filter inklusi.

- Pemetaan bidang —Pilih untuk memetakan bidang sumber data Salesforce Anda ke bidang indeks Anda. Amazon Kendra Untuk informasi lebih lanjut, lihat Memetakan bidang sumber data.

> **Note**
>
> Bidang badan dokumen atau badan dokumen yang setara untuk dokumen Anda diperlukan Amazon Kendra untuk mencari dokumen Anda. Anda harus memetakan nama bidang badan dokumen Anda di sumber data Anda ke nama bidang indeks_`document_body`. Semua kolom lain bersifat opsional.

- Pemfilteran konteks pengguna dan kontrol akses —Amazon Kendra meng-crawl daftar kontrol akses (ACL) untuk dokumen Anda, jika Anda memiliki ACL untuk dokumen Anda. Informasi ACL digunakan untuk memfilter hasil pencarian berdasarkan pengguna atau akses grup mereka ke dokumen. Untuk informasi selengkapnya, lihat Pemfilteran konteks pengguna.

Konektor Salesforce V2.0

Salesforce adalah alat manajemen hubungan pelanggan (CRM) untuk mengelola tim dukungan, penjualan, dan pemasaran. Anda dapat menggunakan Amazon Kendra untuk mengindeks objek standar Salesforce Anda dan bahkan objek kustom.

Konektor sumber data Amazon Kendra Salesforce mendukung edisi Salesforce berikut: Edisi Pengembang dan Edisi Perusahaan.

> **Note**
>
> Support untuk konektor Salesforce V1.0/ SalesforceConfiguration API dijadwalkan berakhir pada tahun 2023. Kami merekomendasikan untuk bermigrasi ke atau menggunakan konektor Salesforce V2.0/API. TemplateConfiguration

Untuk memecahkan masalah konektor sumber data Amazon Kendra Salesforce Anda, lihat. Mengatasi masalah sumber data

Topik

Fitur yang didukung

Amazon Kendra Konektor sumber data Salesforce mendukung fitur-fitur berikut:

- Pemetaan lapangan
- Pemfilteran konteks pengguna
- Perayapan identitas pengguna
- Filter inklusi/pengecualian
- Sinkronisasi konten penuh dan tambahan
- Perayapan lampiran entitas
- Cloud privat virtual (VPC)

Prasyarat

Sebelum Anda dapat menggunakan Amazon Kendra untuk mengindeks sumber data Salesforce Anda, buat perubahan ini di Salesforce dan akun Anda. AWS

Di Salesforce, pastikan Anda memiliki:

- Membuat akun administratif Salesforce dan telah mencatat nama pengguna dan kata sandi yang Anda gunakan untuk terhubung ke Salesforce.
- Menyalin token keamanan Salesforce yang terkait dengan akun yang digunakan untuk terhubung ke Salesforce.
- Membuat akun Salesforce Connected App dengan OAuth diaktifkan dan telah menyalin kunci konsumen (ID klien) dan rahasia konsumen (rahasia klien) yang ditetapkan ke Aplikasi Salesforce Connected Anda. Lihat dokumentasi Salesforce di Aplikasi Terhubung untuk informasi selengkapnya.

- Menyalin URL instance Salesforce yang ingin Anda indeks. Biasanya, ini adalah *https://.salesforce.com/.* <company> Server harus menjalankan aplikasi yang terhubung dengan Salesforce.
- Menambahkan kredensyal ke server Salesforce Anda untuk pengguna dengan akses hanya-baca ke Salesforce dengan mengkloning ReadOnly profil dan kemudian menambahkan izin Lihat Semua Data dan Kelola Artikel. Kredensil ini mengidentifikasi pengguna yang membuat koneksi dan aplikasi terhubung Salesforce yang terhubung ke. Amazon Kendra
- Memeriksa setiap dokumen unik di Salesforce dan di seluruh sumber data lain yang Anda rencanakan untuk digunakan untuk indeks yang sama. Setiap sumber data yang ingin Anda gunakan untuk indeks tidak boleh berisi dokumen yang sama di seluruh sumber data. ID dokumen bersifat global untuk indeks dan harus unik per indeks.

Di dalam Anda Akun AWS, pastikan Anda memiliki:

- Membuat Amazon Kendra indeks dan, jika menggunakan API, mencatat ID indeks.
- Membuat IAM peran untuk sumber data Anda dan, jika menggunakan API, catat ARN peran tersebut IAM .

> **Note**
>
> Jika Anda mengubah jenis otentikasi dan kredensyal, Anda harus memperbarui IAM peran Anda untuk mengakses ID rahasia yang benar AWS Secrets Manager .

- Menyimpan kredensi otentikasi Salesforce Anda secara AWS Secrets Manager rahasia dan, jika menggunakan API, catat ARN rahasia tersebut.

> **Note**
>
> Kami menyarankan Anda secara teratur menyegarkan atau memutar kredensil dan rahasia Anda. Berikan hanya tingkat akses yang diperlukan untuk keamanan Anda sendiri. Kami tidak menyarankan Anda menggunakan kembali kredensyal dan rahasia di seluruh sumber data, dan konektor versi 1.0 dan 2.0 (jika berlaku).

Jika Anda tidak memiliki IAM peran atau rahasia yang ada, Anda dapat menggunakan konsol untuk membuat IAM peran dan Secrets Manager rahasia baru saat Anda menghubungkan sumber data

Salesforce. Amazon Kendra Jika Anda menggunakan API, Anda harus memberikan ARN IAM peran dan Secrets Manager rahasia yang ada, dan ID indeks.

Instruksi koneksi

Untuk terhubung Amazon Kendra ke sumber data Salesforce Anda, Anda harus memberikan rincian yang diperlukan dari sumber data Salesforce Anda sehingga Amazon Kendra dapat mengakses data Anda. Jika Anda belum mengkonfigurasi Salesforce untuk Amazon Kendra lihat. Prasyarat

Console

Untuk terhubung Amazon Kendra ke Salesforce:

1. Masuk ke Konsol AWS Manajemen dan buka Amazon Kendra konsol.
2. Dari panel navigasi kiri, pilih Indeks dan kemudian pilih indeks yang ingin Anda gunakan dari daftar indeks.

> **Note**
>
> Anda dapat memilih untuk mengonfigurasi atau mengedit pengaturan kontrol akses Pengguna Anda di bawah Pengaturan indeks.

3. Pada halaman Memulai, pilih Tambahkan sumber data.
4. Pada halaman Tambah sumber data, pilih Konektor Salesforce V2.0, lalu pilih Tambah konektor.
5. Pada halaman Tentukan detail sumber data, masukkan informasi berikut:
   a. Nama sumber data —Masukkan nama untuk sumber data Anda. Anda dapat memasukkan tanda hubung tetapi bukan spasi.
   b. (Opsional) Deskripsi —Masukkan deskripsi opsional untuk sumber data Anda.
   c. Bahasa default — Bahasa untuk memfilter dokumen Anda untuk indeks. Kecuali Anda menentukan sebaliknya, bahasa default ke bahasa Inggris. Bahasa yang ditentukan dalam metadata menggantikan bahasa yang dipilih.
   d. Pilih Berikutnya.
6. Pada halaman Tentukan akses dan keamanan, masukkan informasi berikut:
   a. URL Salesforce —Masukkan URL contoh untuk situs Salesforce yang ingin Anda indeks.

b. Otorisasi — Aktifkan atau nonaktifkan informasi daftar kontrol akses (ACL) untuk dokumen Anda, jika Anda memiliki ACL dan ingin menggunakannya untuk kontrol akses. ACL menentukan dokumen mana yang dapat diakses pengguna dan grup. Informasi ACL digunakan untuk memfilter hasil pencarian berdasarkan pengguna atau akses grup mereka ke dokumen. Untuk informasi selengkapnya, lihat Pemfilteran konteks pengguna.

c. Masukkan rahasia yang ada atau jika Anda membuat rahasia baru, jendela AWS Secrets Manager rahasia terbuka.

- Otentikasi —Masukkan informasi berikut di jendela Buat AWS Secrets Manager rahasia:

  A. Nama rahasia —Nama untuk rahasiamu. Awalan 'AmazonKendra-Salesforce-' secara otomatis ditambahkan ke nama rahasia Anda.

  B. Untuk Nama Pengguna, Kata Sandi, Token keamanan, Kunci konsumen, Rahasia konsumen, dan URL Otentikasi —Masukkan nilai kredensi otentikasi yang Anda buat dan unduh dari akun Salesforce Anda.

  C. Pilih Simpan otentikasi.

d. Virtual Private Cloud (VPC) —Anda dapat memilih untuk menggunakan VPC. Jika demikian, Anda harus menambahkan Subnet dan grup keamanan VPC.

e. Perayap identitas —Tentukan apakah akan mengaktifkan crawler Amazon Kendra identitas. Perayap identitas menggunakan informasi daftar kontrol akses (ACL) untuk dokumen Anda untuk memfilter hasil penelusuran berdasarkan akses pengguna atau grup mereka ke dokumen. Jika Anda memiliki ACL untuk dokumen Anda dan memilih untuk menggunakan ACL Anda, Anda juga dapat memilih untuk mengaktifkan crawler Amazon Kendra identitas untuk mengonfigurasi pemfilteran konteks pengguna dari hasil pencarian. Jika tidak, jika crawler identitas dimatikan, semua dokumen dapat dicari secara publik. Jika Anda ingin menggunakan kontrol akses untuk dokumen dan crawler identitas dimatikan, Anda dapat menggunakan PutPrincipalMappingAPI untuk mengunggah informasi akses pengguna dan grup untuk pemfilteran konteks pengguna.

f. IAM peran —Pilih peran yang sudah ada atau buat IAM IAM peran baru untuk mengakses kredensi repositori dan mengindeks konten Anda.

> **Note**
>
> IAM peran yang digunakan untuk indeks tidak dapat digunakan untuk sumber data. Jika Anda tidak yakin apakah peran yang ada digunakan untuk indeks atau FAQ, pilih Buat peran baru untuk menghindari kesalahan.

g. Pilih Berikutnya.

7. Pada halaman Konfigurasi pengaturan sinkronisasi, masukkan informasi berikut:

   a. Untuk lampiran Crawl —Pilih untuk meng-crawl semua objek Salesforce yang terpasang.

   b. Untuk objek Standar, objek Standar dengan lampiran, dan objek Standar tanpa lampiran dan Artikel Pengetahuan —Pilih entitas Salesforce atau jenis konten yang ingin dirayapi.

   c. Anda harus memberikan informasi konfigurasi untuk mengindeks setidaknya satu objek standar, artikel pengetahuan, atau umpan obrolan. Jika Anda memilih untuk merayapi artikel Pengetahuan, Anda harus menentukan jenis artikel pengetahuan yang akan diindeks. Anda dapat memilih diterbitkan, diarsipkan, draf, dan lampiran.

      Filter Regex —Tentukan pola regex untuk menyertakan item katalog tertentu.

8. Untuk konfigurasi tambahan:

   - Informasi ACL Semua daftar kontrol akses disertakan secara default. Menghapus pilihan daftar kontrol akses akan membuat semua file dalam kategori itu publik.
   - Pola Regex —Tambahkan pola ekspresi reguler untuk menyertakan atau mengecualikan file tertentu. Anda dapat menambahkan hingga 100 pola.

   Mode sinkronisasi —Pilih cara memperbarui indeks saat konten sumber data berubah. Saat Anda menyinkronkan sumber data Amazon Kendra untuk pertama kalinya, semua konten dirayapi dan diindeks secara default. Anda harus menjalankan sinkronisasi penuh data Anda jika sinkronisasi awal Anda gagal, bahkan jika Anda tidak memilih sinkronisasi penuh sebagai opsi mode sinkronisasi Anda.

   - Sinkronisasi penuh: Indeks baru semua konten, ganti konten yang ada setiap kali sumber data Anda disinkronkan dengan indeks Anda.
   - Sinkronisasi baru yang dimodifikasi: Indeks hanya konten baru dan yang dimodifikasi setiap kali sumber data Anda disinkronkan dengan indeks Anda. Amazon Kendra dapat

menggunakan mekanisme sumber data Anda untuk melacak perubahan konten dan mengindeks konten yang berubah sejak sinkronisasi terakhir.

- Sinkronisasi baru, dimodifikasi, dihapus: Indeks hanya konten baru, dimodifikasi, dan dihapus setiap kali sumber data Anda disinkronkan dengan indeks Anda. Amazon Kendra dapat menggunakan mekanisme sumber data Anda untuk melacak perubahan konten dan mengindeks konten yang berubah sejak sinkronisasi terakhir.

9. Pilih Berikutnya.
10. Pada halaman Setel pemetaan bidang, masukkan informasi berikut:

    a. Untuk artikel pengetahuan Standar, Lampiran objek standar, dan Pemetaan bidang yang disarankan tambahan —Pilih dari bidang sumber data default Amazon Kendra yang dihasilkan yang ingin Anda petakan ke indeks Anda.

    > **Note**
    >
    > Diperlukan pemetaan `_document_body` indeks. Anda tidak dapat mengubah pemetaan antara `Salesforce ID` bidang dan Amazon Kendra `_document_id` bidang. Anda dapat memetakan bidang Salesforce apa pun ke judul dokumen atau badan dokumen bidang indeks reservasi/default Amazon Kendra.

    b. Tambahkan bidang —Untuk menambahkan bidang sumber data kustom untuk membuat nama bidang indeks untuk dipetakan dan tipe data bidang.

    c. Pilih Berikutnya.
11. Pada halaman Tinjau dan buat, periksa apakah informasi yang Anda masukkan sudah benar dan kemudian pilih Tambahkan sumber data. Anda juga dapat memilih untuk mengedit informasi Anda dari halaman ini. Sumber data Anda akan muncul di halaman Sumber data setelah sumber data berhasil ditambahkan.

API

Untuk terhubung Amazon Kendra ke Salesforce

Anda harus menentukan JSON dari skema sumber data menggunakan API. TemplateConfiguration Anda harus memberikan informasi berikut ini:

- Sumber data —Tentukan tipe sumber data seperti `SALESFORCEV2` saat Anda menggunakan skema TemplateConfigurationJSON. Juga tentukan sumber data seperti `TEMPLATE` saat Anda memanggil CreateDataSourceAPI.
- URL Host —Tentukan URL host instance Salesforce.
- Mode sinkronisasi —Tentukan cara Amazon Kendra memperbarui indeks Anda saat konten sumber data Anda berubah. Saat Anda menyinkronkan sumber data Amazon Kendra untuk pertama kalinya, semua konten dirayapi dan diindeks secara default. Anda harus menjalankan sinkronisasi penuh data Anda jika sinkronisasi awal Anda gagal, bahkan jika Anda tidak memilih sinkronisasi penuh sebagai opsi mode sinkronisasi Anda. Anda dapat memilih antara:
  - `FORCED_FULL_CRAWL`untuk mengindeks semua konten baru, mengganti konten yang ada setiap kali sumber data Anda disinkronkan dengan indeks Anda.
  - `FULL_CRAWL`untuk mengindeks hanya konten baru, dimodifikasi, dan dihapus setiap kali sumber data Anda disinkronkan dengan indeks Anda. Amazon Kendra dapat menggunakan mekanisme sumber data Anda untuk melacak perubahan konten dan mengindeks konten yang berubah sejak sinkronisasi terakhir.
  - `CHANGE_LOG`untuk mengindeks hanya konten baru dan yang dimodifikasi setiap kali sumber data Anda disinkronkan dengan indeks Anda. Amazon Kendra dapat menggunakan mekanisme sumber data Anda untuk melacak perubahan konten dan mengindeks konten yang berubah sejak sinkronisasi terakhir.
- Rahasia Nama Sumber Daya Amazon (ARN) —Berikan Nama Sumber Daya Amazon (ARN) Secrets Manager rahasia yang berisi kredensyal otentikasi untuk akun Salesforce Anda. Rahasianya disimpan dalam struktur JSON dengan kunci berikut:

```
{
    "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"
}
```

> **Note**
>
> Kami menyarankan Anda secara teratur menyegarkan atau memutar kredensil dan rahasia Anda. Berikan hanya tingkat akses yang diperlukan untuk keamanan Anda sendiri. Kami tidak menyarankan Anda menggunakan kembali kredensyal dan rahasia di seluruh sumber data, dan konektor versi 1.0 dan 2.0 (jika berlaku).

- IAM peran —Tentukan `RoleArn` kapan Anda menelepon `CreateDataSource` untuk memberikan IAM peran dengan izin untuk mengakses Secrets Manager rahasia Anda dan memanggil API publik yang diperlukan untuk konektor Salesforce dan. Amazon Kendra Untuk informasi selengkapnya, lihat IAM peran untuk sumber data Salesforce.

Anda juga dapat menambahkan fitur opsional berikut:

- Virtual Private Cloud (VPC) **`VpcConfiguration`** —Tentukan kapan Anda menelepon. `CreateDataSource` Untuk informasi selengkapnya, lihat Mengkonfigurasi Amazon Kendra untuk menggunakan Amazon VPC.
- Filter inklusi dan pengecualian —Anda dapat menentukan apakah akan menyertakan atau mengecualikan dokumen, akun, kampanye, kasus, kontak, prospek, peluang, solusi, tugas, grup, obrolan, dan file entitas kustom tertentu.

> **Note**
>
> Sebagian besar sumber data menggunakan pola ekspresi reguler, yang merupakan pola inklusi atau pengecualian yang disebut sebagai filter. Jika Anda menentukan filter inklusi, hanya konten yang cocok dengan filter inklusi yang diindeks. Dokumen apa pun yang tidak cocok dengan filter inklusi tidak diindeks. Jika Anda menentukan filter inklusi dan pengecualian, dokumen yang cocok dengan filter pengecualian tidak akan diindeks, meskipun sesuai dengan filter inklusi.

- Perayap identitas —Tentukan apakah akan mengaktifkan crawler Amazon Kendra identitas. Perayap identitas menggunakan informasi daftar kontrol akses (ACL) untuk dokumen Anda untuk memfilter hasil penelusuran berdasarkan akses pengguna atau grup mereka ke dokumen. Jika Anda memiliki ACL untuk dokumen Anda dan memilih untuk menggunakan ACL Anda, Anda juga dapat memilih untuk mengaktifkan crawler Amazon Kendra identitas untuk mengonfigurasi pemfilteran konteks pengguna dari hasil pencarian. Jika tidak, jika crawler

identitas dimatikan, semua dokumen dapat dicari secara publik. Jika Anda ingin menggunakan kontrol akses untuk dokumen dan crawler identitas dimatikan, Anda dapat menggunakan PutPrincipalMappingAPI untuk mengunggah informasi akses pengguna dan grup untuk pemfilteran konteks pengguna.

- Pemetaan bidang —Pilih untuk memetakan bidang sumber data Salesforce Anda ke bidang indeks Anda. Amazon Kendra Untuk informasi lebih lanjut, lihat Memetakan bidang sumber data.

> **Note**
>
> Bidang badan dokumen atau badan dokumen yang setara untuk dokumen Anda diperlukan Amazon Kendra untuk mencari dokumen Anda. Anda harus memetakan nama bidang badan dokumen Anda di sumber data Anda ke nama bidang indeks `_document_body`. Semua kolom lain bersifat opsional.

Untuk daftar kunci JSON penting lainnya untuk dikonfigurasi, lihatSkema templat Salesforce.

Pelajari selengkapnya

Untuk mempelajari lebih lanjut tentang mengintegrasikan Amazon Kendra dengan sumber data Salesforce Anda, lihat:

- Mengumumkan konektor Salesforce yang diperbarui (V2) untuk Amazon Kendra

ServiceNow

ServiceNow menyediakan sistem manajemen layanan berbasis cloud untuk membuat dan mengelola alur kerja tingkat organisasi, seperti layanan TI, sistem tiket, dan dukungan. Anda dapat menggunakannya Amazon Kendra untuk mengindeks ServiceNow katalog, artikel pengetahuan, insiden, dan lampirannya.

Anda dapat terhubung Amazon Kendra ke sumber ServiceNow data menggunakan Amazon Kendra konsol, TemplateConfigurationAPI, atau ServiceNowConfigurationAPI.

Amazon Kendra memiliki dua versi ServiceNow konektor. Fitur yang didukung dari setiap versi meliputi:

ServiceNow konektor V1.0 /API ServiceNowConfiguration

- Pemetaan lapangan
- ServiceNow versi contoh: London, Others
- Pola inklusi/pengecualian: Katalog layanan, artikel pengetahuan, lampiran

ServiceNow konektor V2.0 /API TemplateConfiguration

- Pemetaan lapangan
- Pemfilteran konteks pengguna
- Filter inklusi/pengecualian
- Sinkronisasi konten penuh dan inkremental
- ServiceNow versi contoh: Roma, Sandiego, Tokyo, Lainnya
- Cloud privat virtual (VPC)

> **Note**
>
> Support untuk ServiceNow konektor V1.0/ ServiceNowConfiguration API dijadwalkan berakhir pada tahun 2023. Kami merekomendasikan migrasi ke atau menggunakan ServiceNow konektor V2.0/ TemplateConfiguration API.

Untuk memecahkan masalah konektor sumber Amazon Kendra ServiceNow data Anda, lihat. Mengatasi masalah sumber data

Topik

- ServiceNow konektor V1.0
- ServiceNow konektor V2.0
- Menentukan dokumen yang akan diindeks dengan kueri

ServiceNow konektor V1.0

ServiceNow menyediakan sistem manajemen layanan berbasis cloud untuk membuat dan mengelola alur kerja tingkat organisasi, seperti layanan TI, sistem tiket, dan dukungan. Anda dapat

menggunakannya Amazon Kendra untuk mengindeks ServiceNow katalog, artikel pengetahuan, dan lampirannya.

> **Note**
>
> Support untuk ServiceNow konektor V1.0/ ServiceNowConfiguration API dijadwalkan berakhir pada tahun 2023. Kami merekomendasikan migrasi ke atau menggunakan ServiceNow konektor V2.0/ TemplateConfiguration API.

Untuk memecahkan masalah konektor sumber Amazon Kendra ServiceNow data Anda, lihat. Mengatasi masalah sumber data

Topik

- Fitur yang didukung
- Prasyarat
- Instruksi koneksi
- Pelajari selengkapnya

Fitur yang didukung

Amazon Kendra ServiceNow konektor sumber data mendukung fitur-fitur berikut:

- ServiceNow versi contoh: London, Others
- Pola inklusi/pengecualian: Katalog layanan, artikel pengetahuan, dan lampirannya

Prasyarat

Sebelum Anda dapat menggunakan Amazon Kendra untuk mengindeks sumber ServiceNow data Anda, buat perubahan ini di akun ServiceNow dan AWS akun Anda.

Di ServiceNow, pastikan Anda memiliki:

- Membuat akun ServiceNow administrator dan telah membuat sebuah ServiceNow instance.
- Menyalin host URL ServiceNow instans Anda. Misalnya, jika URL instans adalah *`https://your-domain.service-now.com`*, format untuk URL host yang Anda masukkan adalah *`your-domain.service-now.com`*.

- Mencatat kredensi otentikasi dasar Anda yang berisi nama pengguna dan kata sandi untuk memungkinkan Anda terhubung Amazon Kendra ke instans Anda. ServiceNow
- Opsional: Mengonfigurasi token kredenal OAuth 2.0 yang dapat mengidentifikasi Amazon Kendra dan menghasilkan nama pengguna, kata sandi, ID klien, dan rahasia klien. Nama pengguna dan kata sandi harus menyediakan akses ke basis ServiceNow pengetahuan dan katalog layanan. Lihat ServiceNow dokumentasi tentang otentikasi OAuth 2.0 untuk informasi selengkapnya.
- Menambahkan izin berikut:
  - kb_category
  - kb_knowledge
  - kb_knowledge_base
  - kb_uc_cannot_read_mtom
  - kb_uc_can_read_mtom
  - sc_catalog
  - sc_category
  - sc_cat_item
  - sys_attachment
  - sys_attachment_doc
  - sys_user_role
- Memeriksa setiap dokumen unik di dalam ServiceNow dan di seluruh sumber data lain yang Anda rencanakan untuk digunakan untuk indeks yang sama. Setiap sumber data yang ingin Anda gunakan untuk indeks tidak boleh berisi dokumen yang sama di seluruh sumber data. ID dokumen bersifat global untuk indeks dan harus unik per indeks.

Di dalam Anda Akun AWS, pastikan Anda memiliki:

- Membuat Amazon Kendra indeks dan, jika menggunakan API, mencatat ID indeks.
- Membuat IAM peran untuk sumber data Anda dan, jika menggunakan API, catat ARN peran tersebut IAM .

> **Note**
>
> Jika Anda mengubah jenis otentikasi dan kredensialnya, Anda harus memperbarui IAM peran Anda untuk mengakses ID rahasia yang benar AWS Secrets Manager .

- Menyimpan kredensi ServiceNow otentikasi Anda AWS Secrets Manager secara rahasia dan, jika menggunakan API, catat ARN rahasia tersebut.

> **Note**
>
> Kami menyarankan Anda secara teratur menyegarkan atau memutar kredensil dan rahasia Anda. Berikan hanya tingkat akses yang diperlukan untuk keamanan Anda sendiri. Kami tidak menyarankan Anda menggunakan kembali kredensyal dan rahasia di seluruh sumber data, dan konektor versi 1.0 dan 2.0 (jika berlaku).

Jika Anda tidak memiliki IAM peran atau rahasia yang ada, Anda dapat menggunakan konsol untuk membuat IAM peran dan Secrets Manager rahasia baru saat Anda menghubungkan sumber ServiceNow data Anda Amazon Kendra. Jika Anda menggunakan API, Anda harus memberikan ARN IAM peran dan Secrets Manager rahasia yang ada, dan ID indeks.

Instruksi koneksi

Untuk terhubung Amazon Kendra ke sumber ServiceNow data Anda, Anda harus memberikan rincian yang diperlukan dari sumber ServiceNow data Anda sehingga Amazon Kendra dapat mengakses data Anda. Jika Anda belum mengkonfigurasi ServiceNow untuk Amazon Kendra lihatPrasyarat.

Console

Untuk terhubung Amazon Kendra ke ServiceNow

1. Masuk ke Konsol AWS Manajemen dan buka Amazon Kendra konsol.
2. Dari panel navigasi kiri, pilih Indeks dan kemudian pilih indeks yang ingin Anda gunakan dari daftar indeks.

> **Note**
>
> Anda dapat memilih untuk mengonfigurasi atau mengedit pengaturan kontrol akses Pengguna Anda di bawah Pengaturan indeks.

3. Pada halaman Memulai, pilih Tambahkan sumber data.
4. Pada halaman Tambahkan sumber data, pilih ServiceNowkonektor V1.0, lalu pilih Tambahkan sumber data.
5. Pada halaman Tentukan detail sumber data, masukkan informasi berikut:

a. Dalam Nama dan deskripsi, untuk Nama sumber data —Masukkan nama untuk sumber data Anda. Anda dapat memasukkan tanda hubung tetapi bukan spasi.

b. (Opsional) Deskripsi —Masukkan deskripsi opsional untuk sumber data Anda.

c. Dalam Bahasa default —Pilih bahasa untuk memfilter dokumen Anda untuk indeks. Kecuali Anda menentukan sebaliknya, bahasa default ke bahasa Inggris. Bahasa yang ditentukan dalam metadata dokumen menggantikan bahasa yang dipilih.

d. Di Tag, untuk Tambahkan tag baru —Sertakan tag opsional untuk mencari dan memfilter sumber daya Anda atau melacak AWS biaya Anda.

e. Pilih Berikutnya.

6. Pada halaman Tentukan akses dan keamanan, masukkan informasi berikut:

a. ServiceNow host —Masukkan URL ServiceNow host.

b. ServiceNow versi —Pilih ServiceNow versi Anda.

c. Pilih antara otentikasi Dasar dan otentikasi Oauth 2.0 berdasarkan kasus penggunaan Anda.

d. AWS Secrets Manager rahasia —Pilih rahasia yang ada atau buat Secrets Manager rahasia baru untuk menyimpan kredensyal ServiceNow otentikasi Anda. Jika Anda memilih untuk membuat rahasia baru, jendela AWS Secrets Manager rahasia terbuka.

   i. Nama rahasia —Nama untuk rahasiamu. Awalan 'AmazonKendra- ServiceNow -' secara otomatis ditambahkan ke nama rahasia Anda.

   ii. Jika menggunakan Otentikasi Dasar—Masukkan nama Rahasia, Nama Pengguna, dan Kata Sandi untuk akun Anda. ServiceNow

   Jika menggunakan Otentikasi OAuth2—Masukkan nama Rahasia, Nama Pengguna, Kata Sandi, ID Klien, dan Rahasia Klien yang Anda buat di akun Anda. ServiceNow

   iii. Pilih Simpan dan tambahkan rahasia.

e. IAM peran —Pilih peran yang ada atau buat IAM IAM peran baru untuk mengakses kredensyal repositori dan mengindeks konten Anda.

> **Note**
>
> IAM peran yang digunakan untuk indeks tidak dapat digunakan untuk sumber data. Jika Anda tidak yakin apakah peran yang ada digunakan untuk indeks atau FAQ, pilih Buat peran baru untuk menghindari kesalahan.

f. Pilih Berikutnya.

7. Pada halaman Konfigurasi pengaturan sinkronisasi, masukkan informasi berikut:

   a. Sertakan artikel pengetahuan —Pilih untuk mengindeks artikel pengetahuan.

   b. Jenis artikel pengetahuan —Pilih antara Sertakan hanya artikel publik dan Sertakan artikel berdasarkan kueri ServiceNow filter berdasarkan kasus penggunaan Anda. Jika Anda memilih Sertakan artikel berdasarkan kueri ServiceNow filter, Anda harus memasukkan kueri Filter yang disalin dari ServiceNow akun Anda.

   c. Sertakan lampiran artikel pengetahuan —Pilih untuk mengindeks lampiran artikel pengetahuan. Anda juga dapat memilih jenis file tertentu untuk diindeks.

   d. Sertakan item katalog —Pilih untuk mengindeks item katalog.

   e. Sertakan lampiran item katalog —Pilih untuk mengindeks lampiran item katalog. Anda juga dapat memilih jenis file tertentu untuk diindeks.

   f. Frekuensi —Seberapa sering Amazon Kendra akan disinkronkan dengan sumber data Anda.

   g. Pilih Berikutnya.

8. Pada halaman Setel pemetaan bidang, masukkan informasi berikut:

   a. Artikel pengetahuan dan Katalog layanan —Pilih dari bidang sumber data default yang Amazon Kendra dihasilkan dan pemetaan bidang tambahan yang disarankan yang ingin Anda petakan ke indeks Anda.

   b. Tambahkan bidang —Untuk menambahkan bidang sumber data kustom untuk membuat nama bidang indeks untuk dipetakan dan tipe data bidang.

   c. Pilih Berikutnya.

9. Pada halaman Tinjau dan buat, periksa apakah informasi yang Anda masukkan sudah benar dan kemudian pilih Tambahkan sumber data. Anda juga dapat memilih untuk mengedit informasi Anda dari halaman ini. Sumber data Anda akan muncul di halaman Sumber data setelah sumber data berhasil ditambahkan.

API

Untuk terhubung Amazon Kendra ke ServiceNow

Anda harus menentukan yang berikut menggunakan ServiceNowConfiguration API:

- URL sumber data —Tentukan ServiceNow URL. Titik akhir host akan terlihat seperti berikut: *your-domain.service-now.com*.
- Instance host sumber data —Tentukan versi instance ServiceNow host sebagai salah satu `LONDON` atau`OTHERS`.
- Rahasia Nama Sumber Daya Amazon (ARN) —Berikan Nama Sumber Daya Amazon (ARN) Secrets Manager rahasia yang berisi kredensyal otentikasi yang Anda buat di akun Anda. ServiceNow

  Jika Anda menggunakan otentikasi dasar, rahasia disimpan dalam struktur JSON dengan kunci berikut:

```
{
    "username": "user name",
    "password": "password"
}
```

  Jika Anda menggunakan otentikasi OAuth2, rahasia disimpan dalam struktur JSON dengan kunci berikut:

```
{
    "username": "user name",
    "password": "password",
    "clientId": "client id",
    "clientSecret": "client secret"
}
```

  > **Note**
  >
  > Kami menyarankan Anda secara teratur menyegarkan atau memutar kredensil dan rahasia Anda. Berikan hanya tingkat akses yang diperlukan untuk keamanan Anda sendiri. Kami tidak menyarankan Anda menggunakan kembali kredensyal dan rahasia di seluruh sumber data, dan konektor versi 1.0 dan 2.0 (jika berlaku).

- IAM peran —Tentukan `RoleArn` kapan Anda menelepon `CreateDataSource` untuk memberikan IAM peran dengan izin untuk mengakses Secrets Manager rahasia Anda dan memanggil API publik yang diperlukan untuk ServiceNow konektor dan. Amazon Kendra Untuk informasi selengkapnya, lihat IAM peran untuk sumber ServiceNow data.

Anda juga dapat menambahkan fitur opsional berikut:

- Pemetaan bidang —Pilih untuk memetakan bidang sumber ServiceNow data Anda ke bidang indeks Anda Amazon Kendra . Untuk informasi lebih lanjut, lihat Memetakan bidang sumber data.

> **Note**
>
> Bidang badan dokumen atau badan dokumen yang setara untuk dokumen Anda diperlukan Amazon Kendra untuk mencari dokumen Anda. Anda harus memetakan nama bidang badan dokumen Anda di sumber data Anda ke nama bidang indeks_`document_body`. Semua kolom lain bersifat opsional.

- Filter inklusi dan pengecualian —Tentukan apakah akan menyertakan atau mengecualikan lampiran file tertentu dari katalog dan artikel pengetahuan.

> **Note**
>
> Sebagian besar sumber data menggunakan pola ekspresi reguler, yang merupakan pola inklusi atau pengecualian yang disebut sebagai filter. Jika Anda menentukan filter inklusi, hanya konten yang cocok dengan filter inklusi yang diindeks. Dokumen apa pun yang tidak cocok dengan filter inklusi tidak diindeks. Jika Anda menentukan filter inklusi dan pengecualian, dokumen yang cocok dengan filter pengecualian tidak akan diindeks, meskipun sesuai dengan filter inklusi.

- Parameter pengindeksan —Anda juga dapat memilih untuk menentukan apakah akan:
  - Mengindeks artikel pengetahuan dan katalog layanan, atau keduanya. Jika Anda memilih untuk mengindeks artikel pengetahuan dan item katalog layanan, Anda harus memberikan nama ServiceNow bidang yang dipetakan ke kolom isi dokumen indeks dalam Amazon Kendra indeks.
  - Lampiran indeks ke artikel pengetahuan dan item katalog.

- Gunakan ServiceNow kueri yang memilih dokumen dari satu atau lebih basis pengetahuan. Basis pengetahuan boleh bersifat publik atau privat. Untuk informasi selengkapnya, lihat Menentukan dokumen untuk diindeks dengan kueri.

Pelajari selengkapnya

Untuk mempelajari lebih lanjut tentang mengintegrasikan Amazon Kendra dengan sumber ServiceNow data Anda, lihat:

- Memulai dengan konektor Amazon Kendra ServiceNow Online

ServiceNow konektor V2.0

ServiceNow menyediakan sistem manajemen layanan berbasis cloud untuk membuat dan mengelola alur kerja tingkat organisasi, seperti layanan TI, sistem tiket, dan dukungan. Anda dapat menggunakannya Amazon Kendra untuk mengindeks ServiceNow katalog, artikel pengetahuan, insiden, dan lampirannya.

Untuk memecahkan masalah konektor sumber Amazon Kendra ServiceNow data Anda, lihat. Mengatasi masalah sumber data

Topik

- Fitur yang didukung
- Prasyarat
- Instruksi koneksi
- Pelajari selengkapnya

Fitur yang didukung

Amazon Kendra ServiceNow konektor sumber data mendukung fitur-fitur berikut:

- Pemetaan lapangan
- Pemfilteran konteks pengguna
- Filter inklusi/pengecualian
- Sinkronisasi konten penuh dan inkremental
- ServiceNow versi contoh: Roma, Sandiego, Tokyo, Lainnya

- Cloud privat virtual (VPC)

Prasyarat

Sebelum Anda dapat menggunakan Amazon Kendra untuk mengindeks sumber ServiceNow data Anda, buat perubahan ini di akun ServiceNow dan AWS akun Anda.

Di ServiceNow, pastikan Anda memiliki:

- Membuat Instans Pengembang Pribadi atau Perusahaan dan memiliki ServiceNow instance dengan peran administratif.
- Menyalin host URL ServiceNow instans Anda. Format URL host yang Anda masukkan adalah *your-domain.service-now.com*. Anda memerlukan URL ServiceNow instans Anda untuk terhubung Amazon Kendra.
- Mencatat kredensi otentikasi dasar Anda dari nama pengguna dan kata sandi untuk memungkinkan untuk terhubung Amazon Kendra ke instans Anda. ServiceNow
- Opsional: Kredensyal klien OAuth 2.0 yang dikonfigurasi yang dapat mengidentifikasi Amazon Kendra menggunakan nama pengguna, kata sandi, dan ID klien yang dihasilkan, dan rahasia klien. Lihat ServiceNow dokumentasi tentang otentikasi OAuth 2.0 untuk informasi selengkapnya.
- Memeriksa setiap dokumen unik di dalam ServiceNow dan di seluruh sumber data lain yang Anda rencanakan untuk digunakan untuk indeks yang sama. Setiap sumber data yang ingin Anda gunakan untuk indeks tidak boleh berisi dokumen yang sama di seluruh sumber data. ID dokumen bersifat global untuk indeks dan harus unik per indeks.

Di dalam Anda Akun AWS, pastikan Anda memiliki:

- Membuat Amazon Kendra indeks dan, jika menggunakan API, mencatat ID indeks.
- Membuat IAM peran untuk sumber data Anda dan, jika menggunakan API, catat ARN peran tersebut IAM .

> **Note**
>
> Jika Anda mengubah jenis otentikasi dan kredensialnya, Anda harus memperbarui IAM peran Anda untuk mengakses ID rahasia yang benar AWS Secrets Manager .

- Menyimpan kredensi ServiceNow otentikasi Anda AWS Secrets Manager secara rahasia dan, jika menggunakan API, catat ARN rahasia tersebut.

> **Note**
>
> Kami menyarankan Anda secara teratur menyegarkan atau memutar kredensil dan rahasia Anda. Berikan hanya tingkat akses yang diperlukan untuk keamanan Anda sendiri. Kami tidak menyarankan Anda menggunakan kembali kredensyal dan rahasia di seluruh sumber data, dan konektor versi 1.0 dan 2.0 (jika berlaku).

Jika Anda tidak memiliki IAM peran atau rahasia yang ada, Anda dapat menggunakan konsol untuk membuat IAM peran dan Secrets Manager rahasia baru saat Anda menghubungkan sumber ServiceNow data Anda Amazon Kendra. Jika Anda menggunakan API, Anda harus memberikan ARN IAM peran dan Secrets Manager rahasia yang ada, dan ID indeks.

Instruksi koneksi

Untuk terhubung Amazon Kendra ke sumber ServiceNow data Anda, Anda harus memberikan rincian yang diperlukan dari sumber ServiceNow data Anda sehingga Amazon Kendra dapat mengakses data Anda. Jika Anda belum mengkonfigurasi ServiceNow untuk Amazon Kendra lihatPrasyarat.

Console

Untuk terhubung Amazon Kendra ke ServiceNow

1. Masuk ke Konsol AWS Manajemen dan buka Amazon Kendra konsol.
2. Dari panel navigasi kiri, pilih Indeks dan kemudian pilih indeks yang ingin Anda gunakan dari daftar indeks.

   > **Note**
   >
   > Anda dapat memilih untuk mengonfigurasi atau mengedit pengaturan kontrol akses Pengguna Anda di bawah Pengaturan indeks.

3. Pada halaman Memulai, pilih Tambahkan sumber data.
4. Pada halaman Tambahkan sumber data, pilih ServiceNowkonektor V2.0, lalu pilih Tambahkan sumber data.
5. Pada halaman Tentukan detail sumber data, masukkan informasi berikut:

a. Dalam Nama dan deskripsi, untuk Nama sumber data —Masukkan nama untuk sumber data Anda. Anda dapat memasukkan tanda hubung tetapi bukan spasi.

b. (Opsional) Deskripsi —Masukkan deskripsi opsional untuk sumber data Anda.

c. Dalam Bahasa default —Pilih bahasa untuk memfilter dokumen Anda untuk indeks. Kecuali Anda menentukan sebaliknya, bahasa default ke bahasa Inggris. Bahasa yang ditentukan dalam metadata dokumen menggantikan bahasa yang dipilih.

d. Di Tag, untuk Tambahkan tag baru —Sertakan tag opsional untuk mencari dan memfilter sumber daya Anda atau melacak AWS biaya Anda.

e. Pilih Berikutnya.

6. Pada halaman Tentukan akses dan keamanan, masukkan informasi berikut:

a. ServiceNow host —Masukkan URL ServiceNow host. Format URL host yang Anda masukkan adalah *your-domain.service-now.com*.

b. ServiceNow versi —Pilih versi ServiceNow instans Anda. Anda dapat memilih dari Roma, Sandiego, Tokyo, atau Lainnya.

c. Otorisasi — Aktifkan atau nonaktifkan informasi daftar kontrol akses (ACL) untuk dokumen Anda, jika Anda memiliki ACL dan ingin menggunakannya untuk kontrol akses. ACL menentukan dokumen mana yang dapat diakses pengguna dan grup. Informasi ACL digunakan untuk memfilter hasil pencarian berdasarkan pengguna atau akses grup mereka ke dokumen. Untuk informasi selengkapnya, lihat Pemfilteran konteks pengguna.

d. Otentikasi —Pilih antara otentikasi Dasar dan otentikasi Oauth 2.0.

e. AWS Secrets Manager rahasia —Pilih rahasia yang ada atau buat Secrets Manager rahasia baru untuk menyimpan kredensyal ServiceNow otentikasi Anda. Jika Anda memilih untuk membuat rahasia baru, jendela AWS Secrets Manager rahasia terbuka. Masukkan informasi berikut di jendela:

i. Nama rahasia —Nama untuk rahasiamu. Awalan 'AmazonKendra- ServiceNow -' secara otomatis ditambahkan ke nama rahasia Anda.

ii. Jika menggunakan Otentikasi Dasar—Masukkan nama Rahasia, Nama Pengguna, dan Kata Sandi untuk akun Anda. ServiceNow

Jika menggunakan Oautentikasi OAuth2.0 — Masukkan nama Rahasia, Nama Pengguna, Kata Sandi, ID Klien, dan Rahasia Klien yang Anda buat di akun Anda. ServiceNow

iii. Pilih Simpan dan tambahkan rahasia.

f. Virtual Private Cloud (VPC) —Anda dapat memilih untuk menggunakan VPC. Jika demikian, Anda harus menambahkan Subnet dan grup keamanan VPC.

g. Perayap identitas —Tentukan apakah akan mengaktifkan crawler Amazon Kendra identitas. Perayap identitas menggunakan informasi daftar kontrol akses (ACL) untuk dokumen Anda untuk memfilter hasil penelusuran berdasarkan akses pengguna atau grup mereka ke dokumen. Jika Anda memiliki ACL untuk dokumen Anda dan memilih untuk menggunakan ACL Anda, Anda juga dapat memilih untuk mengaktifkan crawler Amazon Kendra identitas untuk mengonfigurasi pemfilteran konteks pengguna dari hasil pencarian. Jika tidak, jika crawler identitas dimatikan, semua dokumen dapat dicari secara publik. Jika Anda ingin menggunakan kontrol akses untuk dokumen dan crawler identitas dimatikan, Anda dapat menggunakan PutPrincipalMappingAPI untuk mengunggah informasi akses pengguna dan grup untuk pemfilteran konteks pengguna.

h. IAM peran —Pilih peran yang ada atau buat IAM IAM peran baru untuk mengakses kredensyal repositori dan mengindeks konten Anda.

> **Note**
>
> IAM peran yang digunakan untuk indeks tidak dapat digunakan untuk sumber data. Jika Anda tidak yakin apakah peran yang ada digunakan untuk indeks atau FAQ, pilih Buat peran baru untuk menghindari kesalahan.

i. Pilih Berikutnya.

7. Pada halaman Konfigurasi pengaturan sinkronisasi, masukkan informasi berikut:

   a. Untuk artikel Pengetahuan, pilih dari opsi berikut:

      - Artikel pengetahuan —Pilih untuk mengindeks artikel pengetahuan.
      - Lampiran artikel pengetahuan —Pilih untuk mengindeks lampiran artikel pengetahuan.
      - Jenis artikel pengetahuan —Pilih antara Hanya artikel publik dan artikel Pengetahuan berdasarkan kueri ServiceNow filter berdasarkan kasus penggunaan Anda.
        Jika Anda memilih Sertakan artikel berdasarkan kueri ServiceNow filter, Anda harus memasukkan kueri Filter yang disalin dari ServiceNow akun Anda.
        Contoh kueri filter meliputi: workflow_state = draft^eq, kb_knowledge_base=dfc19531bf2021003f07e2c1ac0739ab^text ISNOTEMPTY^EQ, article_type=text^active=true^eq.

> **Important**
>
> Jika Anda memilih untuk merayapi Hanya artikel publik, hanya Amazon Kendra merayapi artikel pengetahuan yang diberi peran akses publik. ServiceNow

- Sertakan artikel berdasarkan filter deskripsi singkat —Tentukan pola ekspresi reguler untuk menyertakan atau mengecualikan artikel tertentu.

b. Untuk item katalog Layanan:

- Item katalog layanan —Pilih untuk mengindeks item katalog layanan.
- Lampiran item katalog layanan —Pilih untuk mengindeks lampiran item katalog layanan.
- Item katalog layanan aktif —Pilih untuk mengindeks item katalog layanan aktif.
- Item katalog layanan tidak aktif —Pilih untuk mengindeks item katalog layanan yang tidak aktif.
- Kueri filter —Pilih untuk menyertakan item katalog layanan berdasarkan filter yang ditentukan dalam ServiceNow instance Anda. *Contoh kueri filter meliputi: short_descriptionLikeAccess^category=2809952237b1300054b6a3549dbe5dd4 nameStartsWithService^active=true^eq.*
- Sertakan item katalog layanan berdasarkan filter deskripsi singkat —Tentukan pola regex untuk menyertakan item katalog tertentu.

c. Untuk Insiden:

- Insiden —Pilih untuk mengindeks insiden layanan.
- Lampiran insiden —Pilih untuk mengindeks lampiran insiden.
- Insiden aktif —Pilih untuk mengindeks insiden aktif.
- Insiden tidak aktif —Pilih untuk mengindeks insiden tidak aktif.
- Jenis insiden aktif —Pilih antara Semua insiden, Insiden terbuka, Terbuka - insiden yang tidak ditetapkan, dan Insiden yang diselesaikan tergantung pada kasus penggunaan Anda.
- Kueri filter —Pilih untuk menyertakan insiden berdasarkan filter yang ditentukan dalam instance Anda ServiceNow . *Contoh kueri filter meliputi: short_descriptionliketest^urgency=3^state=1^eq, priority=2^category=software^eq.*

- Sertakan insiden berdasarkan filter deskripsi singkat —Tentukan pola regex untuk menyertakan insiden tertentu.

d. Untuk konfigurasi tambahan:

- Informasi ACL —Daftar kontrol akses untuk entitas yang telah Anda pilih disertakan secara default. Menghapus pilihan daftar kontrol akses akan membuat semua file dalam kategori itu publik. Opsi ACL secara otomatis dinonaktifkan untuk entitas yang tidak dipilih. Untuk artikel publik ACL tidak diterapkan.
- Untuk Ukuran file Maksimum - Tentukan batas ukuran file di MB yang akan dirayapi Amazon Kendra. Amazon Kendra hanya akan merayapi file dalam batas ukuran yang Anda tentukan. Ukuran file default adalah 50MB. Ukuran file maksimum harus lebih besar dari 0MB dan kurang dari atau sama dengan 50MB.
- Pola regex lampiran —Tambahkan pola ekspresi reguler untuk menyertakan atau mengecualikan file katalog, artikel pengetahuan, dan insiden tertentu yang terlampir. Anda dapat menambahkan hingga 100 pola.

e. Mode sinkronisasi —Pilih cara memperbarui indeks saat konten sumber data berubah. Saat Anda menyinkronkan sumber data Amazon Kendra untuk pertama kalinya, semua konten dirayapi dan diindeks secara default. Anda harus menjalankan sinkronisasi penuh data Anda jika sinkronisasi awal Anda gagal, bahkan jika Anda tidak memilih sinkronisasi penuh sebagai opsi mode sinkronisasi Anda.

- Sinkronisasi penuh: Indeks baru semua konten, ganti konten yang ada setiap kali sumber data Anda disinkronkan dengan indeks Anda.
- Sinkronisasi baru, dimodifikasi, dihapus: Indeks hanya konten baru, dimodifikasi, dan dihapus setiap kali sumber data Anda disinkronkan dengan indeks Anda. Amazon Kendra dapat menggunakan mekanisme sumber data Anda untuk melacak perubahan konten dan mengindeks konten yang berubah sejak sinkronisasi terakhir.

f. Dalam jadwal berjalan Sinkronisasi, untuk Frekuensi —Seberapa sering Amazon Kendra akan disinkronkan dengan sumber data Anda.

g. Pilih Berikutnya.

8. Pada halaman Setel pemetaan bidang, masukkan informasi berikut:

a. Artikel pengetahuan, Katalog layanan, Lampiran, dan Insiden —Pilih dari bidang sumber data default yang Amazon Kendra dihasilkan yang ingin dipetakan ke indeks.

b. Tambahkan bidang —Untuk menambahkan bidang sumber data kustom untuk membuat nama bidang indeks untuk dipetakan dan tipe data bidang.

c. Pilih Berikutnya.

9. Pada halaman Tinjau dan buat, periksa apakah informasi yang Anda masukkan sudah benar dan kemudian pilih Tambahkan sumber data. Anda juga dapat memilih untuk mengedit informasi Anda dari halaman ini. Sumber data Anda akan muncul di halaman Sumber data setelah sumber data berhasil ditambahkan.

API

Untuk terhubung Amazon Kendra ke ServiceNow

Anda harus menentukan JSON dari skema sumber data menggunakan API. TemplateConfiguration Anda harus memberikan informasi berikut ini:

- Sumber data —Tentukan tipe sumber data seperti `SERVICENOWV2` saat Anda menggunakan skema TemplateConfigurationJSON. Juga tentukan sumber data seperti `TEMPLATE` saat Anda memanggil CreateDataSourceAPI.
- URL Host —Tentukan versi instance ServiceNow host. Misalnya, *`your-domain.service-now.com`*.
- Jenis otentikasi —Tentukan jenis otentikasi yang Anda gunakan, apakah `basicAuth` atau `OAuth2` untuk instans Anda. ServiceNow
- ServiceNow versi instance —Tentukan ServiceNow instance yang Anda gunakan, apakah`Tokyo`,, `SandiegoRome`, atau`Others`.
- Mode sinkronisasi —Tentukan cara Amazon Kendra memperbarui indeks Anda saat konten sumber data Anda berubah. Saat Anda menyinkronkan sumber data Amazon Kendra untuk pertama kalinya, semua konten dirayapi dan diindeks secara default. Anda harus menjalankan sinkronisasi penuh data Anda jika sinkronisasi awal Anda gagal, bahkan jika Anda tidak memilih sinkronisasi penuh sebagai opsi mode sinkronisasi Anda. Anda dapat memilih antara:
  - `FORCED_FULL_CRAWL`untuk mengindeks semua konten baru, mengganti konten yang ada setiap kali sumber data Anda disinkronkan dengan indeks Anda.
  - `FULL_CRAWL`untuk mengindeks hanya konten baru, dimodifikasi, dan dihapus setiap kali sumber data Anda disinkronkan dengan indeks Anda. Amazon Kendra dapat menggunakan mekanisme sumber data Anda untuk melacak perubahan konten dan mengindeks konten yang berubah sejak sinkronisasi terakhir.

- Rahasia Nama Sumber Daya Amazon (ARN) —Berikan Nama Sumber Daya Amazon (ARN) Secrets Manager rahasia yang berisi kredensyal otentikasi yang Anda buat di akun Anda. ServiceNow

  Jika Anda menggunakan otentikasi dasar, rahasia disimpan dalam struktur JSON dengan kunci berikut:

  ```
  {
      "username": "user name",
      "password": "password"
  }
  ```

  > **Note**
  >
  > Kami menyarankan Anda secara teratur menyegarkan atau memutar kredensil dan rahasia Anda. Berikan hanya tingkat akses yang diperlukan untuk keamanan Anda sendiri. Kami tidak menyarankan Anda menggunakan kembali kredensyal dan rahasia di seluruh sumber data, dan konektor versi 1.0 dan 2.0 (jika berlaku).

- Jika Anda menggunakan kredensil klien OAuth2, rahasia disimpan dalam struktur JSON dengan kunci berikut:

  ```
  {
      "username": "user name",
      "password": "password",
      "clientId": "client id",
      "clientSecret": "client secret"
  }
  ```

- IAM peran —Tentukan `RoleArn` kapan Anda menelepon `CreateDataSource` untuk memberikan IAM peran dengan izin untuk mengakses Secrets Manager rahasia Anda dan memanggil API publik yang diperlukan untuk ServiceNow konektor dan. Amazon Kendra Untuk informasi selengkapnya, lihat IAM peran untuk sumber ServiceNow data.

Anda juga dapat menambahkan fitur opsional berikut:

- Virtual Private Cloud (VPC) **`VpcConfiguration`** —Tentukan kapan Anda menelepon. `CreateDataSource` Untuk informasi selengkapnya, lihat Mengkonfigurasi Amazon Kendra untuk menggunakan Amazon VPC.

- Filter penyertaan dan pengecualian —Anda dapat menentukan apakah akan menyertakan atau mengecualikan file terlampir tertentu menggunakan nama file dan jenis file artikel pengetahuan, katalog layanan, dan insiden.

  > **Note**
  >
  > Sebagian besar sumber data menggunakan pola ekspresi reguler, yang merupakan pola inklusi atau pengecualian yang disebut sebagai filter. Jika Anda menentukan filter inklusi, hanya konten yang cocok dengan filter inklusi yang diindeks. Dokumen apa pun yang tidak cocok dengan filter inklusi tidak diindeks. Jika Anda menentukan filter inklusi dan pengecualian, dokumen yang cocok dengan filter pengecualian tidak akan diindeks, meskipun sesuai dengan filter inklusi.

- Dokumen khusus untuk diindeks —Anda dapat menggunakan ServiceNow kueri untuk menentukan dokumen yang Anda inginkan dari satu atau beberapa basis pengetahuan, termasuk basis pengetahuan pribadi. Akses ke basis pengetahuan ditentukan oleh pengguna yang Anda gunakan untuk terhubung ke ServiceNow instance. Untuk informasi selengkapnya, lihat Menentukan dokumen untuk diindeks dengan kueri.
- Parameter pengindeksan —Anda juga dapat memilih untuk menentukan apakah akan:
  - Mengindeks artikel pengetahuan, katalog layanan, dan insiden atau semua ini. Jika Anda memilih untuk mengindeks artikel pengetahuan, item katalog layanan, dan insiden, Anda harus memberikan nama ServiceNow bidang yang dipetakan ke bidang isi dokumen indeks dalam indeks. Amazon Kendra
  - Lampiran indeks ke artikel pengetahuan, item katalog layanan, dan insiden.
  - Sertakan artikel pengetahuan, item katalog layanan, dan insiden berdasarkan pola `short description` filter.
  - Pilih untuk memfilter item dan insiden katalog layanan aktif dan tidak aktif.
  - Pilih untuk memfilter insiden berdasarkan jenis insiden.
  - Pilih entitas mana yang harus dirayapi ACL mereka.
  - Anda dapat menggunakan ServiceNow kueri untuk menentukan dokumen yang Anda inginkan dari satu atau lebih basis pengetahuan, termasuk basis pengetahuan pribadi. Akses ke basis pengetahuan ditentukan oleh pengguna yang Anda gunakan untuk terhubung ke ServiceNow instance. Untuk informasi selengkapnya, lihat Menentukan dokumen untuk diindeks dengan kueri.

- Perayap identitas —Tentukan apakah akan mengaktifkan crawler Amazon Kendra identitas. Perayap identitas menggunakan informasi daftar kontrol akses (ACL) untuk dokumen Anda untuk memfilter hasil penelusuran berdasarkan akses pengguna atau grup mereka ke dokumen. Jika Anda memiliki ACL untuk dokumen Anda dan memilih untuk menggunakan ACL Anda, Anda juga dapat memilih untuk mengaktifkan crawler Amazon Kendra identitas untuk mengonfigurasi pemfilteran konteks pengguna dari hasil pencarian. Jika tidak, jika crawler identitas dimatikan, semua dokumen dapat dicari secara publik. Jika Anda ingin menggunakan kontrol akses untuk dokumen dan crawler identitas dimatikan, Anda dapat menggunakan PutPrincipalMappingAPI untuk mengunggah informasi akses pengguna dan grup untuk pemfilteran konteks pengguna.
- Pemetaan bidang —Pilih untuk memetakan bidang sumber ServiceNow data Anda ke bidang indeks Anda Amazon Kendra . Untuk informasi lebih lanjut, lihat Memetakan bidang sumber data.

> **Note**
>
> Bidang badan dokumen atau badan dokumen yang setara untuk dokumen Anda diperlukan Amazon Kendra untuk mencari dokumen Anda. Anda harus memetakan nama bidang badan dokumen Anda di sumber data Anda ke nama bidang indeks_`document_body`. Semua kolom lain bersifat opsional.

Untuk daftar kunci JSON penting lainnya untuk dikonfigurasi, lihatServiceNow skema templat.

Pelajari selengkapnya

Untuk mempelajari lebih lanjut tentang mengintegrasikan Amazon Kendra dengan sumber ServiceNow data Anda, lihat:

- Memulai dengan Amazon Kendra Mengumumkan ServiceNow konektor yang diperbarui (V2) untuk Amazon Kendra

Menentukan dokumen yang akan diindeks dengan kueri

Anda dapat menggunakan ServiceNow kueri untuk menentukan dokumen yang ingin Anda sertakan dalam Amazon Kendra indeks. Ketika menggunakan kueri, Anda dapat menentukan beberapa basis

pengetahuan, termasuk basis pengetahuan privat. Akses ke basis pengetahuan ditentukan oleh pengguna yang Anda gunakan untuk terhubung ke ServiceNow instance.

Untuk membuat kueri, Anda menggunakan pembuat ServiceNow kueri. Anda dapat menggunakan pembuat kueri untuk membuat kueri dan menguji apakah kueri mengembalikan daftar dokumen yang benar.

Untuk membuat kueri menggunakan ServiceNow konsol

1. Masuk ke ServiceNow konsol.
2. Dari menu sebelah kiri, pilih Pengetahuan, kemudian Artikel, lalu pilih Semua.
3. Di bagian atas halaman, pilih ikon filter.
4. Gunakan pembuat kueri untuk membuat kueri.
5. Ketika kueri selesai, klik kanan kueri dan pilih Salin kueri untuk menyalin kueri dari pembuat kueri. Simpan kueri ini untuk digunakan Amazon Kendra.

Pastikan Anda tidak mengubah parameter kueri apa pun saat menyalin kueri. Jika salah satu parameter kueri tidak dikenali, ServiceNow memperlakukan parameter sebagai kosong dan tidak menggunakannya untuk memfilter hasil.

Kendur

Slack adalah aplikasi komunikasi perusahaan yang memungkinkan pengguna mengirim pesan dan lampiran melalui berbagai saluran publik dan pribadi. Anda dapat menggunakan Amazon Kendra untuk mengindeks saluran publik dan pribadi Slack Anda, pesan bot dan arsip, file dan lampiran, pesan langsung dan grup. Anda juga dapat memilih konten tertentu untuk difilter.

> **Note**
>
> Amazon Kendra sekarang mendukung konektor Slack yang ditingkatkan.

Konsol telah ditingkatkan secara otomatis untuk Anda. Konektor baru apa pun yang Anda buat di konsol akan menggunakan arsitektur yang ditingkatkan. Jika Anda menggunakan API, Anda sekarang harus menggunakan TemplateConfigurationobjek alih-alih `SlackConfiguration` objek untuk mengonfigurasi konektor Anda.
Konektor yang dikonfigurasi menggunakan konsol lama dan arsitektur API akan terus berfungsi seperti yang dikonfigurasi. Namun, Anda tidak akan dapat mengedit atau memperbaruinya. Jika Anda ingin mengedit atau memperbarui konfigurasi konektor Anda, Anda harus membuat konektor baru.
Kami merekomendasikan untuk memigrasikan alur kerja konektor Anda ke versi yang ditingkatkan. Support untuk konektor yang dikonfigurasi menggunakan arsitektur lama dijadwalkan berakhir pada Juni 2024.

Anda dapat terhubung Amazon Kendra ke sumber data Slack menggunakan Amazon Kendra konsol atau TemplateConfigurationAPI.

Untuk memecahkan masalah konektor sumber data Amazon Kendra Slack, lihat. Mengatasi masalah sumber data

Topik

- Fitur yang didukung
- Prasyarat
- Instruksi koneksi
- Pelajari selengkapnya

Fitur yang didukung

Amazon Kendra Konektor sumber data Slack mendukung fitur-fitur berikut:

- Pemetaan lapangan
- Pemfilteran konteks pengguna
- Perayapan identitas pengguna
- Filter inklusi/pengecualian
- Sinkronisasi konten penuh dan tambahan
- Cloud privat virtual (VPC)

Prasyarat

Sebelum Anda dapat menggunakan Amazon Kendra untuk mengindeks sumber data Slack Anda, buat perubahan ini di Slack dan AWS akun Anda.

Di Slack, pastikan Anda memiliki:

- Membuat token OAuth Pengguna Slack Bot atau token OAuth Pengguna Slack. Anda dapat memilih salah satu token untuk terhubung Amazon Kendra ke sumber data Slack Anda. Lihat dokumentasi Slack pada token akses untuk informasi selengkapnya.

  > **Note**
  >
  > Jika Anda menggunakan token bot sebagai bagian dari kredensyal Slack Anda, Anda tidak dapat mengindeks pesan langsung dan pesan grup dan Anda harus menambahkan token bot ke saluran yang ingin Anda indeks.

- Mencatat ID tim ruang kerja Slack Anda dari URL halaman utama ruang kerja Slack Anda. Misalnya, *https://app.slack.com/client/T0123456789/...* dimana *T0123456789* adalah ID tim.
- Menambahkan cakupan/izin Oauth berikut:

Lingkup token pengguna	Lingkup token bot
• saluran:sejarah • saluran:baca • emoji: baca • file: baca • kelompok:sejarah • kelompok:baca • im:sejarah • im:baca • mpim:sejarah • mpim:baca • tim: baca • users.profile:baca	• saluran:sejarah • saluran:kelola • saluran:baca • percakapan.connect:kelola • percakapan.connect:baca • file: baca • kelompok:sejarah • kelompok:baca • im:sejarah • im:baca • mpim:sejarah • mpim:baca

Lingkup token pengguna	Lingkup token bot
• pengguna:baca • pengguna:read.email	• reaksi:baca • tim: baca • grup pengguna:baca • users.profile:baca • pengguna:baca • pengguna:read.email

- Memeriksa setiap dokumen unik di Slack dan di seluruh sumber data lain yang Anda rencanakan untuk digunakan untuk indeks yang sama. Setiap sumber data yang ingin Anda gunakan untuk indeks tidak boleh berisi dokumen yang sama di seluruh sumber data. ID dokumen bersifat global untuk indeks dan harus unik per indeks.

Di dalam Anda Akun AWS, pastikan Anda memiliki:

- Membuat Amazon Kendra indeks dan, jika menggunakan API, mencatat ID indeks.
- Membuat IAM peran untuk sumber data Anda dan, jika menggunakan API, catat ARN peran tersebut IAM .

> **Note**
>
> Jika Anda mengubah jenis otentikasi dan kredensyal, Anda harus memperbarui IAM peran Anda untuk mengakses ID rahasia yang benar AWS Secrets Manager .

- Menyimpan kredensi otentikasi Slack Anda secara AWS Secrets Manager rahasia dan, jika menggunakan API, catat ARN rahasia tersebut.

> **Note**
>
> Kami menyarankan Anda secara teratur menyegarkan atau memutar kredensil dan rahasia Anda. Berikan hanya tingkat akses yang diperlukan untuk keamanan Anda sendiri. Kami tidak menyarankan Anda menggunakan kembali kredensyal dan rahasia di seluruh sumber data, dan konektor versi 1.0 dan 2.0 (jika berlaku).

Jika Anda tidak memiliki IAM peran atau rahasia yang ada, Anda dapat menggunakan konsol untuk membuat IAM peran dan Secrets Manager rahasia baru saat Anda menghubungkan sumber data Slack. Amazon Kendra Jika Anda menggunakan API, Anda harus memberikan ARN IAM peran dan Secrets Manager rahasia yang ada, dan ID indeks.

Instruksi koneksi

Untuk terhubung Amazon Kendra ke sumber data Slack Anda, Anda harus memberikan rincian yang diperlukan dari sumber data Slack Anda sehingga Amazon Kendra dapat mengakses data Anda. Jika Anda belum mengkonfigurasi Slack untuk Amazon Kendra, lihatPrasyarat.

Console

Untuk terhubung Amazon Kendra ke Slack

1. Masuk ke AWS Management Console dan buka Amazon Kendra konsol.
2. Dari panel navigasi kiri, pilih Indeks dan kemudian pilih indeks yang ingin Anda gunakan dari daftar indeks.

> **Note**
>
> Anda dapat memilih untuk mengonfigurasi atau mengedit pengaturan kontrol akses Pengguna Anda di bawah Pengaturan indeks.

3. Pada halaman Memulai, pilih Tambahkan sumber data.
4. Pada halaman Tambahkan sumber data, pilih konektor Slack, lalu pilih Tambah konektor.
5. Pada halaman Tentukan detail sumber data, masukkan informasi berikut:
   a. Di Nama dan deskripsi, untuk Nama sumber data —Masukkan nama untuk sumber data Anda. Anda dapat memasukkan tanda hubung tetapi bukan spasi.
   b. (Opsional) Deskripsi —Masukkan deskripsi opsional untuk sumber data Anda.
   c. Dalam Bahasa default —Pilih bahasa untuk memfilter dokumen Anda untuk indeks. Kecuali Anda menentukan sebaliknya, bahasa default ke bahasa Inggris. Bahasa yang ditentukan dalam metadata dokumen mengesampingkan bahasa yang dipilih.
   d. Di Tag, untuk Tambahkan tag baru —Sertakan tag opsional untuk mencari dan memfilter sumber daya Anda atau melacak AWS biaya Anda.
   e. Pilih Berikutnya.

6. Pada halaman Tentukan akses dan keamanan, masukkan informasi berikut:

   a. Di Sumber, untuk ID tim ruang kerja Slack —ID tim ruang kerja Slack Anda.

   b. AWS Secrets Manager rahasia —Pilih rahasia yang ada atau buat Secrets Manager rahasia baru untuk menyimpan kredensyal otentikasi Slack Anda. Jika Anda memilih untuk membuat rahasia baru, jendela AWS Secrets Manager rahasia terbuka.

      i. Masukkan informasi berikut di jendela Buat AWS Secrets Manager rahasia:

         A. Nama rahasia —Nama untuk rahasiamu. Awalan 'AmazonKendra-Slack-' secara otomatis ditambahkan ke nama rahasia Anda.

         B. Untuk token Slack —Masukkan nilai kredensi otentikasi yang Anda buat di akun Slack Anda.

      ii. Pilih Simpan.

   c. Virtual Private Cloud (VPC) —Anda dapat memilih untuk menggunakan VPC. Jika demikian, Anda harus menambahkan Subnet dan grup keamanan VPC.

   d. Perayap identitas —Tentukan apakah akan mengaktifkan crawler Amazon Kendra identitas. Perayap identitas menggunakan informasi daftar kontrol akses (ACL) untuk dokumen Anda untuk memfilter hasil penelusuran berdasarkan akses pengguna atau grup mereka ke dokumen. Jika Anda memiliki ACL untuk dokumen Anda dan memilih untuk menggunakan ACL Anda, Anda juga dapat memilih untuk mengaktifkan crawler Amazon Kendra identitas untuk mengonfigurasi pemfilteran konteks pengguna dari hasil pencarian. Jika tidak, jika crawler identitas dimatikan, semua dokumen dapat dicari secara publik. Jika Anda ingin menggunakan kontrol akses untuk dokumen dan crawler identitas dimatikan, Anda dapat menggunakan PutPrincipalMappingAPI untuk mengunggah informasi akses pengguna dan grup untuk pemfilteran konteks pengguna.

   e. IAM peran —Pilih peran yang sudah ada atau buat IAM IAM peran baru untuk mengakses kredensi repositori dan mengindeks konten Anda.

      > **Note**
      >
      > IAM peran yang digunakan untuk indeks tidak dapat digunakan untuk sumber data. Jika Anda tidak yakin apakah peran yang ada digunakan untuk indeks atau FAQ, pilih Buat peran baru untuk menghindari kesalahan.

   f. Pilih Berikutnya.

7. Pada halaman Konfigurasi pengaturan sinkronisasi, masukkan informasi berikut:

a. Pilih jenis konten yang akan di-crawl —Entitas Slack atau tipe konten yang ingin dirayapi. Anda dapat memilih dari Semua saluran, saluran Publik, Saluran pribadi, Pesan grup, dan pesan pribadi.

b. Pilih tanggal mulai crawl —Masukkan tanggal dari mana Amazon Kendra akan meng-crawl konten Slack Anda.

c. Untuk konfigurasi Tambahan — opsional masukkan informasi berikut:

- (Opsional) Id/Nama Saluran —Jika Anda memilih untuk menyinkronkan konten dari saluran, Anda dapat menyertakan konten untuk disinkronkan dari saluran tertentu dengan memberikan ID saluran dan nama saluran.
- Pesan —Pilih apakah akan menyertakan pesan bot, atau pesan yang diarsipkan, atau pesan bot dan pesan yang diarsipkan.

> **Note**
>
> Jika Anda memilih untuk mengonfigurasi filter untuk ID Saluran dan Nama Saluran, konektor Amazon Kendra Slack akan memprioritaskan ID saluran di atas nama saluran.
> Jika Anda memilih untuk mengonfigurasi filter untuk ID Saluran atau Nama Saluran, konektor Amazon Kendra Slack akan mengabaikan pesan Pribadi dan Grup meskipun Anda telah memilih untuk merayapi pesan pribadi dan grup dalam lingkup Sinkronisasi.

- Pola Regex —Pola ekspresi reguler untuk menyertakan atau mengecualikan file tertentu. Anda dapat menambahkan hingga 100 pola. Contoh pola regex meliputi:
  - Jenis file — .pdf, .docx
  - Nama file — Hello*.txt,. TestFile *

d. Mode sinkronisasi —Pilih cara Anda ingin memperbarui indeks saat konten sumber data Anda berubah. Saat Anda menyinkronkan sumber data Amazon Kendra untuk pertama kalinya, semua konten dirayapi dan diindeks secara default. Anda harus menjalankan sinkronisasi penuh data Anda jika sinkronisasi awal Anda gagal, bahkan jika Anda tidak memilih sinkronisasi penuh sebagai opsi mode sinkronisasi Anda.

- Sinkronisasi penuh: Indeks baru semua konten, ganti konten yang ada setiap kali sumber data Anda disinkronkan dengan indeks Anda.

- Sinkronisasi baru, dimodifikasi, dihapus: Indeks hanya konten baru, dimodifikasi, dan dihapus setiap kali sumber data Anda disinkronkan dengan indeks Anda. Amazon Kendra dapat menggunakan mekanisme sumber data Anda untuk melacak perubahan konten dan mengindeks konten yang berubah sejak sinkronisasi terakhir.

e. Dalam jadwal berjalan Sinkronisasi, untuk Frekuensi —Seberapa sering Amazon Kendra akan disinkronkan dengan sumber data Anda.

f. Pilih Berikutnya.

8. Pada halaman Setel pemetaan bidang, masukkan informasi berikut:

a. Untuk pemetaan bidang Slack —Pilih dari bidang sumber data default Amazon Kendra yang dihasilkan yang ingin Anda petakan ke indeks Anda.

b. Tambahkan bidang —Untuk menambahkan bidang sumber data kustom untuk membuat nama bidang indeks untuk dipetakan dan tipe data bidang.

c. Pilih Berikutnya.

9. Pada halaman Tinjau dan buat, periksa apakah informasi yang Anda masukkan sudah benar dan kemudian pilih Tambahkan sumber data. Anda juga dapat memilih untuk mengedit informasi Anda dari halaman ini. Sumber data Anda akan muncul di halaman Sumber data setelah sumber data berhasil ditambahkan.

API

Untuk terhubung Amazon Kendra ke Slack

Anda harus menentukan JSON dari skema sumber data menggunakan API. TemplateConfiguration Anda harus memberikan informasi berikut ini:

- Sumber data —Tentukan tipe sumber data seperti `SLACK` saat Anda menggunakan skema TemplateConfigurationJSON. Tentukan juga sumber data seperti `TEMPLATE` saat Anda memanggil CreateDataSourceAPI.
- ID tim ruang kerja Slack —ID tim Slack yang Anda salin dari URL halaman utama Slack Anda.
- Sejak tanggal —Tanggal untuk mulai merayapi data Anda dari tim ruang kerja Slack Anda. Tanggal harus mengikuti format ini: yyyy-mm-dd.
- Mode sinkronisasi —Tentukan cara Amazon Kendra memperbarui indeks Anda saat konten sumber data Anda berubah. Saat Anda menyinkronkan sumber data Amazon Kendra untuk pertama kalinya, semua konten dirayapi dan diindeks secara default. Anda harus menjalankan

sinkronisasi penuh data Anda jika sinkronisasi awal Anda gagal, bahkan jika Anda tidak memilih sinkronisasi penuh sebagai opsi mode sinkronisasi Anda. Anda dapat memilih antara:

- `FORCED_FULL_CRAWL`untuk mengindeks semua konten baru, mengganti konten yang ada setiap kali sumber data Anda disinkronkan dengan indeks Anda.
- `FULL_CRAWL`untuk mengindeks hanya konten baru, dimodifikasi, dan dihapus setiap kali sumber data Anda disinkronkan dengan indeks Anda. Amazon Kendra dapat menggunakan mekanisme sumber data Anda untuk melacak perubahan konten dan mengindeks konten yang berubah sejak sinkronisasi terakhir.
- `CHANGE_LOG`untuk mengindeks hanya konten baru dan yang dimodifikasi setiap kali sumber data Anda disinkronkan dengan indeks Anda. Amazon Kendra dapat menggunakan mekanisme sumber data Anda untuk melacak perubahan konten dan mengindeks konten yang berubah sejak sinkronisasi terakhir.

- Perayap identitas —Tentukan apakah akan mengaktifkan crawler Amazon Kendra identitas. Perayap identitas menggunakan informasi daftar kontrol akses (ACL) untuk dokumen Anda untuk memfilter hasil penelusuran berdasarkan akses pengguna atau grup mereka ke dokumen. Jika Anda memiliki ACL untuk dokumen Anda dan memilih untuk menggunakan ACL Anda, Anda juga dapat memilih untuk mengaktifkan crawler Amazon Kendra identitas untuk mengonfigurasi pemfilteran konteks pengguna dari hasil pencarian. Jika tidak, jika crawler identitas dimatikan, semua dokumen dapat dicari secara publik. Jika Anda ingin menggunakan kontrol akses untuk dokumen dan crawler identitas dimatikan, Anda dapat menggunakan PutPrincipalMappingAPI untuk mengunggah informasi akses pengguna dan grup untuk pemfilteran konteks pengguna.
- Rahasia Nama Sumber Daya Amazon (ARN) —Berikan Nama Sumber Daya Amazon (ARN) Secrets Manager rahasia yang berisi kredensyal otentikasi untuk akun Slack Anda. Rahasianya disimpan dalam struktur JSON dengan kunci berikut:

```
{
    "slackToken": "token"
}
```

> **Note**
>
> Kami menyarankan Anda secara teratur menyegarkan atau memutar kredensil dan rahasia Anda. Berikan hanya tingkat akses yang diperlukan untuk keamanan Anda

sendiri. Kami tidak menyarankan Anda menggunakan kembali kredensyal dan rahasia di seluruh sumber data, dan konektor versi 1.0 dan 2.0 (jika berlaku).

- IAM peran —Tentukan `RoleArn` kapan Anda menelepon `CreateDataSource` untuk memberikan IAM peran dengan izin untuk mengakses Secrets Manager rahasia Anda dan memanggil API publik yang diperlukan untuk konektor Slack dan. Amazon Kendra Untuk informasi selengkapnya, lihat IAM peran untuk sumber data Slack.

Anda juga dapat menambahkan fitur opsional berikut:

- Virtual Private Cloud (VPC) **`VpcConfiguration`** —Tentukan kapan Anda menelepon. `CreateDataSource` Untuk informasi selengkapnya, lihat Mengkonfigurasi Amazon Kendra untuk menggunakan Amazon VPC.
- Saluran tertentu —Filter berdasarkan saluran publik atau pribadi, dan tentukan saluran tertentu berdasarkan ID mereka.
- Jenis saluran dan pesan —Apakah Amazon Kendra harus mengindeks saluran publik dan pribadi Anda, grup dan pesan langsung Anda, serta bot Anda dan pesan yang diarsipkan. Jika Anda menggunakan token bot sebagai bagian dari kredensyal otentikasi Slack Anda, Anda harus menambahkan token bot ke saluran yang ingin Anda indeks. Anda tidak dapat mengindeks pesan langsung dan pesan grup menggunakan token bot.
- Lihat ke belakang —Anda dapat memilih untuk mengonfigurasi `lookBack` parameter sehingga konektor Slack merayapi konten yang diperbarui atau dihapus hingga jumlah jam tertentu sebelum sinkronisasi konektor terakhir Anda.
- Filter inklusi dan pengecualian —Tentukan apakah akan menyertakan atau mengecualikan konten Slack tertentu. Jika Anda menggunakan token bot sebagai bagian dari kredensyal otentikasi Slack Anda, Anda harus menambahkan token bot ke saluran yang ingin Anda indeks. Anda tidak dapat mengindeks pesan langsung dan pesan grup menggunakan token bot.

> **Note**
>
> Sebagian besar sumber data menggunakan pola ekspresi reguler, yang merupakan pola inklusi atau pengecualian yang disebut sebagai filter. Jika Anda menentukan filter inklusi, hanya konten yang cocok dengan filter inklusi yang diindeks. Dokumen apa pun yang tidak cocok dengan filter inklusi tidak diindeks. Jika Anda menentukan filter inklusi

dan pengecualian, dokumen yang cocok dengan filter pengecualian tidak akan diindeks, meskipun sesuai dengan filter inklusi.

- Pemetaan bidang —Pilih untuk memetakan bidang sumber data Slack Anda ke bidang indeks Anda. Amazon Kendra Untuk informasi lebih lanjut, lihat Memetakan bidang sumber data.

> **Note**
>
> Bidang badan dokumen atau badan dokumen yang setara untuk dokumen Anda diperlukan Amazon Kendra untuk mencari dokumen Anda. Anda harus memetakan nama bidang badan dokumen Anda di sumber data Anda ke nama bidang indeks_`document_body`. Semua kolom lain bersifat opsional.

Untuk daftar kunci JSON penting lainnya untuk dikonfigurasi, lihat skema Slack template.

Pelajari selengkapnya

Untuk mempelajari lebih lanjut tentang mengintegrasikan Amazon Kendra dengan sumber data Slack Anda, lihat:

- Mengungkap pengetahuan di ruang kerja Slack dengan pencarian cerdas menggunakan konektor Slack Amazon Kendra

Zendesk

Zendesk adalah sistem manajemen hubungan pelanggan yang membantu bisnis mengotomatisasi dan meningkatkan interaksi dukungan pelanggan. Anda dapat menggunakan Amazon Kendra untuk mengindeks tiket dukungan Zendesk Anda, komentar tiket, lampiran tiket, artikel pusat bantuan, komentar artikel, lampiran komentar artikel, topik panduan komunitas, posting komunitas, dan komentar posting komunitas.

Anda dapat memfilter berdasarkan nama organisasi jika Anda ingin mengindeks tiket yang hanya ada dalam organisasi tertentu. Anda juga dapat memilih untuk menetapkan tanggal crawl kapan Anda ingin memulai crawling data dari Zendesk.

Anda dapat terhubung Amazon Kendra ke sumber data Zendesk Anda menggunakan Amazon Kendra konsol dan TemplateConfigurationAPI.

Untuk memecahkan masalah konektor sumber data Amazon Kendra Zendesk Anda, lihat. Mengatasi masalah sumber data

Topik

- Fitur yang didukung
- Prasyarat
- Instruksi koneksi
- Pelajari selengkapnya

Fitur yang didukung

Amazon Kendra Konektor sumber data Zendesk mendukung fitur-fitur berikut:

- Ubah log
- Pemetaan lapangan
- Pemfilteran konteks pengguna
- Filter inklusi/pengecualian
- Cloud privat virtual (VPC)

Prasyarat

Sebelum Anda dapat menggunakan Amazon Kendra untuk mengindeks sumber data Zendesk Anda, buat perubahan ini di Zendesk dan AWS akun Anda.

Di Zendesk, pastikan Anda memiliki:

- Membuat akun administratif Zendesk Suite (Professional/Enterprise).
- Mencatat URL host Zendesk Anda. Misalnya, *https://{sub-domain (https://{host/)}.zendesk.com/*.

> **Note**
>
> (On-premise/server) Amazon Kendra memeriksa apakah informasi titik akhir yang disertakan sama dengan informasi titik akhir yang AWS Secrets Manager ditentukan dalam detail konfigurasi sumber data Anda. Ini membantu melindungi dari masalah wakil yang membingungkan, yang merupakan masalah keamanan di mana pengguna tidak

memiliki izin untuk melakukan tindakan tetapi menggunakan Amazon Kendra sebagai proxy untuk mengakses rahasia yang dikonfigurasi dan melakukan tindakan. Jika nanti Anda mengubah informasi titik akhir Anda, Anda harus membuat rahasia baru untuk menyinkronkan informasi ini.

- Menghasilkan token kredensi OAuth 2.0 yang berisi ID klien, rahasia klien, nama pengguna, dan kata sandi. Lihat dokumentasi Zendesk tentang pembuatan token OAuth 2.0 untuk informasi selengkapnya.
- Menambahkan cakupan OAuth 2.0 berikut:
  - baca
- Opsional: Menginstal sertifikat SSL untuk memungkinkan Amazon Kendra untuk terhubung.
- Memeriksa setiap dokumen unik di Zendesk dan di seluruh sumber data lain yang Anda rencanakan untuk digunakan untuk indeks yang sama. Setiap sumber data yang ingin Anda gunakan untuk indeks tidak boleh berisi dokumen yang sama di seluruh sumber data. ID dokumen bersifat global untuk indeks dan harus unik per indeks.

Di dalam Anda Akun AWS, pastikan Anda memiliki:

- Membuat Amazon Kendra indeks dan, jika menggunakan API, mencatat ID indeks.
- Membuat IAM peran untuk sumber data Anda dan, jika menggunakan API, catat ARN peran tersebut IAM .

> **Note**
>
> Jika Anda mengubah jenis otentikasi dan kredensialnya, Anda harus memperbarui IAM peran Anda untuk mengakses ID rahasia yang benar AWS Secrets Manager .

- Menyimpan kredensi otentikasi Zendesk Anda secara AWS Secrets Manager rahasia dan, jika menggunakan API, catat ARN rahasianya.

> **Note**
>
> Kami menyarankan Anda secara teratur menyegarkan atau memutar kredensil dan rahasia Anda. Berikan hanya tingkat akses yang diperlukan untuk keamanan Anda sendiri. Kami tidak menyarankan Anda menggunakan kembali kredensyal dan rahasia di seluruh sumber data, dan konektor versi 1.0 dan 2.0 (jika berlaku).

Jika Anda tidak memiliki IAM peran atau rahasia yang ada, Anda dapat menggunakan konsol untuk membuat IAM peran dan Secrets Manager rahasia baru saat Anda menghubungkan sumber data Zendesk Anda. Amazon Kendra Jika Anda menggunakan API, Anda harus memberikan ARN IAM peran dan Secrets Manager rahasia yang ada, dan ID indeks.

Instruksi koneksi

Untuk terhubung Amazon Kendra ke sumber data Zendesk Anda, Anda harus memberikan rincian yang diperlukan dari sumber data Zendesk Anda sehingga Amazon Kendra dapat mengakses data Anda. Jika Anda belum mengkonfigurasi Zendesk untuk Amazon Kendra, lihatPrasyarat.

Console

Untuk terhubung Amazon Kendra ke Zendesk

1. Masuk ke AWS Management Console dan buka Amazon Kendra konsol.
2. Dari panel navigasi kiri, pilih Indeks dan kemudian pilih indeks yang ingin Anda gunakan dari daftar indeks.

> **Note**
>
> Anda dapat memilih untuk mengonfigurasi atau mengedit pengaturan kontrol akses Pengguna Anda di bawah Pengaturan indeks.

3. Pada halaman Memulai, pilih Tambahkan sumber data.
4. Pada halaman Tambah sumber data, pilih konektor Zendesk, lalu pilih Tambah konektor.
5. Pada halaman Tentukan detail sumber data, masukkan informasi berikut:
   a. Dalam Nama dan deskripsi, untuk Nama sumber data —Masukkan nama untuk sumber data Anda. Anda dapat memasukkan tanda hubung tetapi bukan spasi.
   b. (Opsional) Deskripsi —Masukkan deskripsi opsional untuk sumber data Anda.
   c. Dalam Bahasa default —Pilih bahasa untuk memfilter dokumen Anda untuk indeks. Kecuali Anda menentukan sebaliknya, bahasa default ke bahasa Inggris. Bahasa yang ditentukan dalam metadata dokumen mengesampingkan bahasa yang dipilih.
   d. Di Tag, untuk Tambahkan tag baru —Sertakan tag opsional untuk mencari dan memfilter sumber daya Anda atau melacak AWS biaya Anda.
   e. Pilih Berikutnya.

6. Pada halaman Tentukan akses dan keamanan, masukkan informasi berikut:

   a. URL Zendesk —Masukkan URL Zendesk Anda.

   b. AWS Secrets Manager rahasia —Pilih rahasia yang ada atau buat Secrets Manager rahasia baru untuk menyimpan kredensi otentikasi Zendesk Anda. Jika Anda memilih untuk membuat rahasia baru, jendela AWS Secrets Manager rahasia terbuka.

      i. Masukkan informasi berikut di jendela Buat AWS Secrets Manager rahasia:

         A. Nama rahasia —Nama untuk rahasiamu. Awalan 'AmazonKendra-Zendesk-' secara otomatis ditambahkan ke nama rahasia Anda.

         B. Untuk ID Klien, Rahasia klien, Nama pengguna, Kata Sandi —Masukkan nilai kredensi otentikasi yang Anda buat di akun Zendesk Anda.

      ii. Pilih Simpan.

   c. Virtual Private Cloud (VPC) —Anda dapat memilih untuk menggunakan VPC. Jika demikian, Anda harus menambahkan Subnet dan grup keamanan VPC.

   d. IAM peran —Pilih peran yang sudah ada atau buat IAM IAM peran baru untuk mengakses kredensi repositori dan mengindeks konten Anda.

      > **Note**
      >
      > IAM peran yang digunakan untuk indeks tidak dapat digunakan untuk sumber data. Jika Anda tidak yakin apakah peran yang ada digunakan untuk indeks atau FAQ, pilih Buat peran baru untuk menghindari kesalahan.

   e. Pilih Berikutnya.

7. Pada halaman Konfigurasi pengaturan sinkronisasi, masukkan informasi berikut:

   a. Pilih entitas atau jenis konten —Entitas Zendesk atau tipe konten yang ingin dirayapi.

   b. Ubah log —Pilih untuk memperbarui indeks Anda hanya dengan konten baru dan yang dimodifikasi alih-alih menyinkronkan semua file Anda.

   c. Nama organisasi —Masukkan nama organisasi Zendesk untuk memfilter sinkronisasi Anda.

   d. Sinkronkan tanggal mulai —Tanggal dari mana Anda ingin mengindeks konten Anda.

   e. Pola Regex —Pola ekspresi reguler untuk menyertakan atau mengecualikan file tertentu. Anda dapat menambahkan hingga 100 pola.

f. Di Sinkronkan jadwal lari untuk Frekuensi —Pilih seberapa sering Amazon Kendra akan disinkronkan dengan sumber data Anda.

g. Pilih Berikutnya.

8. Pada halaman Setel pemetaan bidang, masukkan informasi berikut:

   a. Untuk Tiket, Komentar tiket, Lampiran komentar tiket, Artikel, Komentar artikel, Lampiran komentar artikel, Topik komunitas, Posting komunitas, Komentar posting komunitas — Pilih dari bidang sumber data default yang Amazon Kendra dihasilkan yang ingin Anda petakan ke indeks Anda.

   b. Tambahkan bidang —Untuk menambahkan bidang sumber data kustom untuk membuat nama bidang indeks untuk dipetakan dan tipe data bidang.

   c. Pilih Berikutnya.

9. Pada halaman Tinjau dan buat, periksa apakah informasi yang Anda masukkan sudah benar dan kemudian pilih Tambahkan sumber data. Anda juga dapat memilih untuk mengedit informasi Anda dari halaman ini. Sumber data Anda akan muncul di halaman Sumber data setelah sumber data berhasil ditambahkan.

API

Untuk terhubung Amazon Kendra ke Zendesk

Anda harus menentukan JSON dari skema sumber data menggunakan API. TemplateConfiguration Anda harus memberikan informasi berikut ini:

- Sumber data —Tentukan tipe sumber data seperti `ZENDESK` saat Anda menggunakan skema TemplateConfigurationJSON. Tentukan juga sumber data seperti `TEMPLATE` saat Anda memanggil CreateDataSourceAPI.
- URL Host —Berikan URL host Zendesk Anda sebagai bagian dari konfigurasi koneksi atau detail titik akhir repositori. Misalnya, *`https://yoursubdomain.zendesk.com`*.
- Ubah log —Apakah Amazon Kendra harus menggunakan mekanisme log perubahan sumber data Zendesk untuk menentukan apakah dokumen harus diperbarui dalam indeks.

> **Note**
>
> Gunakan log perubahan jika Anda tidak Amazon Kendra ingin memindai semua dokumen. Jika log perubahan Anda besar, mungkin perlu waktu Amazon Kendra lebih

sedikit untuk memindai dokumen di sumber data Zendesk daripada memproses log perubahan. Jika Anda menyinkronkan sumber data Zendesk Anda dengan indeks Anda untuk pertama kalinya, semua dokumen dipindai.

- Rahasia Nama Sumber Daya Amazon (ARN) —Berikan Nama Sumber Daya Amazon (ARN) Secrets Manager rahasia yang berisi kredensi otentikasi untuk akun Zendesk Anda. Rahasianya disimpan dalam struktur JSON dengan kunci berikut:

```
{
    "hostUrl": "https://yoursubdomain.zendesk.com",
    "clientId": "client ID",
    "clientSecret": "Zendesk client secret",
    "userName": "Zendesk user name",
    "password": "Zendesk password"
}
```

> **Note**
>
> Kami menyarankan Anda secara teratur menyegarkan atau memutar kredensil dan rahasia Anda. Berikan hanya tingkat akses yang diperlukan untuk keamanan Anda sendiri. Kami tidak menyarankan Anda menggunakan kembali kredensyal dan rahasia di seluruh sumber data, dan konektor versi 1.0 dan 2.0 (jika berlaku).

- IAM peran —Tentukan `RoleArn` kapan Anda menelepon `CreateDataSource` untuk memberikan IAM peran dengan izin untuk mengakses Secrets Manager rahasia Anda dan memanggil API publik yang diperlukan untuk konektor Zendesk dan. Amazon Kendra Untuk informasi selengkapnya, lihat IAM peran untuk sumber data Zendesk.

Anda juga dapat menambahkan fitur opsional berikut:

- Virtual Private Cloud (VPC) **`VpcConfiguration`** —Tentukan kapan Anda menelepon. `CreateDataSource` Untuk informasi selengkapnya, lihat Mengkonfigurasi Amazon Kendra untuk menggunakan Amazon VPC.
- Filter inklusi dan pengecualian —Tentukan apakah akan menyertakan atau mengecualikan:
  - Tiket Dukungan, komentar tiket, dan/atau lampiran komentar tiket
  - Artikel pusat bantuan, lampiran artikel, dan komentar artikel
  - Memandu topik komunitas, posting, atau posting komentar

> **Note**
>
> Sebagian besar sumber data menggunakan pola ekspresi reguler, yang merupakan pola inklusi atau pengecualian yang disebut sebagai filter. Jika Anda menentukan filter inklusi, hanya konten yang cocok dengan filter inklusi yang diindeks. Dokumen apa pun yang tidak cocok dengan filter inklusi tidak diindeks. Jika Anda menentukan filter inklusi dan pengecualian, dokumen yang cocok dengan filter pengecualian tidak akan diindeks, meskipun sesuai dengan filter inklusi.

- Pemfilteran konteks pengguna dan kontrol akses —Amazon Kendra meng-crawl daftar kontrol akses (ACL) untuk dokumen Anda, jika Anda memiliki ACL untuk dokumen Anda. Informasi ACL digunakan untuk memfilter hasil pencarian berdasarkan pengguna atau akses grup mereka ke dokumen. Untuk informasi selengkapnya, lihat Pemfilteran konteks pengguna.
- Pemetaan bidang —Pilih untuk memetakan bidang sumber data Zendesk Anda ke bidang indeks Anda. Amazon Kendra Untuk informasi lebih lanjut, lihat Memetakan bidang sumber data.

> **Note**
>
> Bidang badan dokumen atau badan dokumen yang setara untuk dokumen Anda diperlukan Amazon Kendra untuk mencari dokumen Anda. Anda harus memetakan nama bidang badan dokumen Anda di sumber data Anda ke nama bidang indeks_`document_body`. Semua kolom lain bersifat opsional.

Untuk daftar kunci JSON penting lainnya untuk dikonfigurasi, lihatSkema template Zendesk.

Pelajari selengkapnya

Untuk mempelajari lebih lanjut tentang mengintegrasikan Amazon Kendra dengan sumber data Zendesk Anda, lihat:

- Temukan wawasan dari Zendesk dengan pencarian cerdas Amazon Kendra

Memetakan bidang sumber data

Amazon Kendra konektor sumber data dapat memetakan bidang dokumen atau konten dari sumber data Anda ke bidang dalam Amazon Kendra indeks Anda. Secara default, setiap konektor dirancang untuk merayapi bidang sumber data tertentu. Bidang sumber data default dan propertinya tidak dapat diubah atau disesuaikan. Di Amazon Kendra konsol, bidang default dan properti bidang default yang tidak dapat diedit berwarna abu-abu.

Amazon Kendra konektor juga memungkinkan Anda untuk memetakan dokumen khusus atau bidang konten dari sumber data Anda ke bidang khusus dalam indeks Anda. Misalnya, jika Anda memiliki bidang di sumber data yang disebut “dept” yang berisi informasi departemen untuk dokumen, Anda dapat memetakannya ke bidang indeks yang disebut “Departemen”. Dengan begitu, Anda dapat menggunakan bidang saat menanyakan dokumen.

Anda juga dapat memetakan bidang yang Amazon Kendra dipesan atau umum seperti`_created_at`. Jika sumber data Anda memiliki bidang yang disebut “creation_date”, Anda dapat memetakannya ke bidang Amazon Kendra cadangan setara yang disebut. `_created_at` Untuk informasi selengkapnya tentang bidang yang Amazon Kendra dicadangkan, lihat Atribut atau bidang dokumen.

Anda dapat memetakan bidang untuk sebagian besar sumber data. Anda dapat membuat pemetaan bidang untuk sumber data berikut:

- Manajer Pengalaman Adobe
- Alfresco
- Aurora (MySQL)
- Aurora (PostgreSQL)
- Amazon FSx (Jendela)
- Amazon FSx (NetApp ONTAP)
- Amazon RDS/Aurora
- Amazon RDS (Microsoft SQL Server)
- Amazon RDS (MySQL)
- Amazon RDS (Oracle)
- Amazon RDS (PostgreSQL)
- Amazon Kendra Perayap Web

- Amazon WorkDocs
- Kotak
- Confluence
- Dropbox
- Drupal
- GitHub
- Google Workspace Drives
- Gmail
- IBM DB2
- Jira
- Microsoft Exchange
- Microsoft OneDrive
- Microsoft SharePoint
- Tim Microsoft
- Microsoft SQL Server
- Microsoft Yammer
- MySQL
- Oracle Database
- PostgreSQL
- Menyindir
- Salesforce
- ServiceNow
- Kendur
- Zendesk

Jika Anda menyimpan dokumen di bucket S3, atau sumber data S3, Anda menentukan bidang menggunakan file metadata JSON. Untuk informasi selengkapnya, lihat konektor sumber data S3.

Memetakan bidang sumber data ke bidang indeks memerlukan tiga langkah:

1. Buat indeks. Untuk informasi lebih lanjut, lihat Membuat indeks.
2. Perbarui indeks untuk menambahkan bidang.

3. Buat sumber data dan sertakan pemetaan bidang untuk memetakan bidang yang dicadangkan dan bidang khusus apa pun untuk Amazon Kendra mengindeks bidang.

Untuk memperbarui indeks untuk menambahkan bidang kustom, gunakan konsol untuk mengedit pemetaan bidang sumber data dan menambahkan bidang kustom atau menggunakan API. UpdateIndex Anda dapat menambahkan total 500 bidang kustom ke indeks Anda.

Untuk sumber data basis data, jika nama kolom basis data cocok dengan nama bidang terpesan, bidang dan kolom akan otomatis dipetakan.

Dengan UpdateIndexAPI, Anda menambahkan bidang cadangan dan kustom menggunakan`DocumentMetadataConfigurationUpdates`.

Contoh JSON berikut digunakan `DocumentMetadataConfigurationUpdates` untuk menambahkan bidang yang disebut “Departemen” ke indeks.

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

Saat Anda membuat bidang, Anda memiliki opsi untuk mengatur bagaimana bidang tersebut digunakan untuk pencarian. Anda dapat memilih dari opsi berikut:

- Displayable —Menentukan apakah bidang dikembalikan dalam respons kueri. Default-nya adalah `true`.
- Facetable —Menunjukkan bahwa bidang dapat digunakan untuk membuat faset. Default-nya adalah `false`.
- Dapat dicari —Menentukan apakah bidang digunakan dalam pencarian. Secara default adalah `true` untuk bidang string dan `false` untuk bidang nomor dan tanggal.
- Sortable —Menunjukkan bahwa bidang dapat digunakan untuk mengurutkan respons dari kueri. Hanya dapat diatur untuk bidang tanggal, angka, dan string. Tidak dapat diatur untuk bidang daftar string.

Contoh JSON berikut digunakan `DocumentMetadataConfigurationUpdates` untuk menambahkan bidang yang disebut “Departemen” ke indeks dan menandainya sebagai facetable.

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

Menggunakan bidang dokumen yang Amazon Kendra dicadangkan atau umum

Dengan UpdateIndex API, Anda dapat membuat kolom cadangan atau umum menggunakan `DocumentMetadataConfigurationUpdates` dan menentukan nama bidang indeks Amazon Kendra cadangan untuk dipetakan ke atribut/nama bidang dokumen yang setara. Anda juga dapat membuat bidang khusus. Jika Anda menggunakan konektor sumber data, sebagian besar menyertakan pemetaan bidang yang memetakan bidang dokumen sumber data Anda ke bidang Amazon Kendra indeks. Jika Anda menggunakan konsol, Anda memperbarui bidang dengan memilih sumber data, memilih tindakan edit, dan kemudian melanjutkan di sebelah bagian pemetaan bidang untuk mengonfigurasi sumber data.

Anda dapat mengonfigurasi `Search` objek untuk menetapkan bidang sebagai dapat ditampilkan, facetable, dapat dicari, dan dapat diurutkan. Anda dapat mengonfigurasi `Relevance` objek untuk mengatur urutan peringkat bidang, durasi peningkatan, atau periode waktu untuk diterapkan pada peningkatan, kesegaran, nilai kepentingan, dan nilai kepentingan yang dipetakan ke nilai bidang tertentu. Jika Anda menggunakan konsol, Anda dapat mengatur pengaturan pencarian untuk bidang dengan memilih opsi facet di menu navigasi. Untuk mengatur penyetelan relevansi, pilih opsi untuk mencari indeks Anda di menu navigasi, masukkan kueri, dan gunakan opsi panel samping untuk menyetel relevansi pencarian. Anda tidak dapat mengubah jenis bidang setelah Anda membuat bidang.

Amazon Kendra memiliki bidang dokumen cadangan atau umum berikut yang dapat Anda gunakan:

- `_authors`Daftar satu atau lebih penulis yang bertanggung jawab atas isi dokumen.
- `_category`Sebuah kategori yang menempatkan dokumen dalam kelompok tertentu.

- `_created_at`—Tanggal dan waktu dalam format ISO 8601 bahwa dokumen itu dibuat. Misalnya, 2012-03-25T 12:30:10 +01:00 adalah format tanggal-waktu ISO 8601 untuk 25 Maret 2012 pukul 12:30 (ditambah 10 detik) di Waktu Eropa Tengah.
- `_data_source_id`—Pengidentifikasi sumber data yang berisi dokumen.
- `_document_body`—Isi dokumen.
- `_document_id`—Pengidentifikasi unik untuk dokumen.
- `_document_title`—Judul dokumen.
- `_excerpt_page_number`—Nomor halaman dalam file PDF tempat kutipan dokumen muncul. Jika indeks Anda dibuat sebelum 8 September 2020, Anda harus mengindeks ulang dokumen sebelum dapat menggunakan atribut ini.
- `_faq_id`—Jika ini adalah dokumen tipe tanya jawab (FAQ), pengenal unik untuk FAQ.
- `_file_type`—Jenis file dokumen, seperti pdf atau doc.
- `_last_updated_at`Tanggal dan waktu dalam format ISO 8601 bahwa dokumen terakhir diperbarui. Misalnya, 2012-03-25T 12:30:10 +01:00 adalah format tanggal-waktu ISO 8601 untuk 25 Maret 2012 pukul 12:30 (ditambah 10 detik) di Waktu Eropa Tengah.
- `_source_uri`—URI tempat dokumen tersedia. Misalnya, URI dokumen di situs web perusahaan.
- `_version`—Pengidentifikasi untuk versi dokumen tertentu.
- `_view_count`—Berapa kali dokumen telah dilihat.
- `_language_code`(String) —Kode untuk bahasa yang berlaku untuk dokumen. Ini default ke bahasa Inggris jika Anda tidak menentukan bahasa. Untuk informasi selengkapnya tentang bahasa yang didukung, termasuk kodenya, lihat Menambahkan dokumen dalam bahasa selain bahasa Inggris.

Untuk bidang kustom, Anda membuat bidang ini menggunakan `DocumentMetadataConfigurationUpdates` `UpdateIndex` API, seperti yang Anda lakukan saat membuat bidang cadangan atau umum. Anda harus mengatur tipe data yang sesuai untuk bidang kustom Anda. Jika Anda menggunakan konsol, Anda memperbarui bidang dengan memilih sumber data, memilih tindakan edit, dan kemudian melanjutkan di sebelah bagian pemetaan bidang untuk mengonfigurasi sumber data. Beberapa sumber data tidak mendukung penambahan bidang baru atau bidang khusus. Anda tidak dapat mengubah jenis bidang setelah Anda membuat bidang.

Berikut ini adalah jenis yang dapat Anda atur untuk bidang khusus:

- Tanggal

- Angka
- String
- Daftar string

Jika Anda menambahkan dokumen ke indeks menggunakan BatchPutDocumentAPI, `Attributes` daftar bidang/atribut dokumen Anda dan Anda membuat bidang menggunakan objek. `DocumentAttribute`

Untuk dokumen yang diindeks dari sumber Amazon S3 data, Anda membuat bidang menggunakan file metadata JSON yang menyertakan informasi bidang.

Jika Anda menggunakan database yang didukung sebagai sumber data, Anda dapat mengonfigurasi bidang menggunakan opsi pemetaan bidang.

Menambahkan dokumen dalam bahasa selain bahasa Inggris

Anda dapat mengindeks dokumen dalam berbagai bahasa. Jika Anda tidak menentukan bahasa, Amazon Kendra indeks dokumen dalam bahasa Inggris secara default. Anda menyertakan kode bahasa untuk dokumen dalam metadata dokumen sebagai bidang. Lihat Pemetaan bidang dan atribut Kustom untuk informasi selengkapnya tentang `_language_code` bidang untuk dokumen.

Anda dapat menentukan kode bahasa untuk semua dokumen Anda di sumber data Anda saat Anda menelepon CreateDataSource. Jika dokumen tidak memiliki kode bahasa yang ditentukan dalam bidang metadata, dokumen diindeks menggunakan kode bahasa yang ditentukan untuk semua dokumen di tingkat sumber data. Di konsol, Anda dapat mengindeks dokumen dalam bahasa yang didukung hanya di tingkat sumber data. Pergi ke Sumber data, lalu Tentukan halaman detail sumber data, dan pilih bahasa dari Bahasa tarik-turun.

Anda juga dapat mencari atau menanyakan dokumen dalam bahasa yang didukung. Untuk informasi selengkapnya, lihat Mencari dalam bahasa.

Bahasa berikut dan kodenya didukung (Bahasa Inggris atau `en` didukung secara default jika Anda tidak menentukan bahasa). Tabel ini mencakup bahasa yang Amazon Kendra mendukung dengan pencarian semantik penuh, serta bahasa yang hanya mendukung pencocokan kata kunci sederhana. Bahasa yang mendukung pencarian semantik penuh ditandai dengan tanda bintang dan dalam teks tebal di tabel berikut. Bahasa Inggris (bahasa default) juga didukung dengan pencarian semantik penuh.

Nama bahasa	Kode bahasa
Arab	`ar`
Orang Armenia	`hy`
Basque	`eu`
Bengali	`bn`
Bulgaria	`bg`
bahasa katala	`ca`
Bahasa Mandarin — disederhanakan dan tradisional*	`zh`
Bahasa Ceko	`cs`
Orang Denmark	`da`
Bahasa Belanda	`nl`
orang Finlandia	`fi`
Prancis - termasuk Prancis (Kanada) *	`fr`
Galicia	`gl`
Jerman*	`de`
Yunani	`el`
bahasa Hindi	`hi`
Bahasa Hungaria	`hu`
orang Indonesia	`id`
orang Irlandia	`ga`

Nama bahasa	Kode bahasa
Bahasa Italia	`it`
Jepang*	`ja`
Korea*	`ko`
Latvia	`lv`
Lituania	`lt`
Norwegia	`no`
Persia	`fa`
Bahasa Portugis	`pt`
Portugis (Brasil) *	`pt-BR`
Rumania	`ro`
Bahasa Rusia	`ru`
Sorani	`ckb`
Spanyol - termasuk Spanyol (Meksiko) *	`es`
Bahasa Swedia	`sv`
Turki	`tr`

* Pencarian semantik didukung untuk bahasa tersebut.

Untuk bahasa yang mendukung pencarian semantik, fitur berikut didukung.

- Relevansi dokumen di luar pencocokan kata kunci sederhana.
- FAQ di luar pencocokan kata kunci sederhana.
- Mengekstrak jawaban dari dokumen berdasarkan Amazon Kendra pemahaman bacaan.
- Ember kepercayaan (sangat tinggi, tinggi, sedang, dan rendah) dari hasil pencarian.

Untuk bahasa yang tidak mendukung pencarian semantik, pencocokan kata kunci sederhana didukung untuk relevansi dokumen dan FAQ.

Sinonim (termasuk sinonim khusus), pembelajaran tambahan dan umpan balik, dan saran kueri hanya didukung untuk bahasa Inggris (bahasa default).

Mengkonfigurasi Amazon Kendra untuk menggunakan Amazon VPC

Amazon Kendra dapat terhubung ke virtual private cloud (VPC) yang Anda buat Amazon Virtual Private Cloud untuk mengindeks konten yang disimpan dalam sumber data yang berjalan di cloud pribadi Anda. Saat membuat konektor sumber data, Anda dapat menyediakan grup keamanan dan pengidentifikasi subnet untuk subnet yang berisi sumber data Anda. Dengan informasi ini, Amazon Kendra buat elastic network interface yang digunakannya untuk berkomunikasi secara aman dengan sumber data Anda dalam VPC Anda.

Untuk menyiapkan konektor sumber Amazon Kendra data Amazon VPC, Anda dapat menggunakan operasi AWS Management Console atau CreateDataSourceAPI. Jika Anda menggunakan konsol, Anda menghubungkan VPC selama proses konfigurasi konektor.

> **Note**
>
> Amazon VPC Fitur ini opsional saat menyiapkan konektor sumber Amazon Kendra data. Jika sumber data Anda dapat diakses dari internet publik, Anda tidak perlu mengaktifkan Amazon VPC fitur tersebut. Tidak semua konektor sumber Amazon Kendra data mendukung Amazon VPC.

Jika sumber data Anda tidak berjalan Amazon VPC dan tidak dapat diakses dari internet publik, pertama-tama Anda menghubungkan sumber data Anda ke VPC menggunakan jaringan pribadi virtual (VPN). Kemudian, Anda dapat menghubungkan sumber data Anda Amazon Kendra dengan menggunakan kombinasi Amazon VPC dan AWS Virtual Private Network. Untuk informasi tentang pengaturan VPN, lihat AWS VPN dokumentasi.

Topik

- Mengkonfigurasi Amazon VPC dukungan untuk konektor Amazon Kendra
- Siapkan sumber Amazon Kendra data untuk terhubung Amazon VPC

- Menghubungkan ke basis data di VPC
- Memecahkan masalah koneksi VPC

Mengkonfigurasi Amazon VPC dukungan untuk konektor Amazon Kendra

Untuk mengonfigurasi Amazon VPC untuk digunakan dengan Amazon Kendra konektor Anda, lakukan langkah-langkah berikut.

Langkah-langkah

- Langkah 1. Buat Amazon VPC subnet untuk Amazon Kendra
- Langkah 2. Buat grup Amazon VPC keamanan untuk Amazon Kendra
- Langkah 3. Konfigurasikan sumber data eksternal Anda dan Amazon VPC

Langkah 1. Buat Amazon VPC subnet untuk Amazon Kendra

Buat atau pilih Amazon VPC subnet yang ada yang Amazon Kendra dapat digunakan untuk mengakses sumber data Anda. Subnet yang disiapkan harus berada di salah satu dari berikut Wilayah AWS dan Availability Zone:

- AS Barat (Oregon) /us-barat-2—usw2-az1, usw2-az2, usw2-az3
- AS Timur (Virginia N.) /us-timur-1—gunakan1-az1, gunakan1-az2, gunakan1-az4
- AS Timur (Ohio) /us-timur-2—gunakan2-az1, gunakan2-az2, gunakan2-az3
- Asia Pasifik (Tokyo) /ap-timur laut-1 — apne1-az1, apne1-az2, apne1-az4
- Asia Pasifik (Mumbai) /ap-selatan-1—aps1-az1, aps1-az2, aps1-az3
- Asia Pasifik (Singapura) /ap-tenggara 1—apse1-az1, apse1-az2, apse1-az3
- Asia Pasifik (Sydney) /ap-tenggara 2—apse2-az1, apse2-az2, apse2-az3
- Kanada (Tengah) /ca-central-1—cac1-az1, cac1-az2, cac1-az4
- Eropa (Irlandia) /eu-barat-1—euw1-az1, uew1-az2, euw1-az3
- Eropa (London) /eu-barat-2—usw2-az1, usw2-az2, usw2-az3

Sumber data Anda harus dapat diakses dari subnet yang Anda berikan ke Amazon Kendra konektor.

Untuk informasi selengkapnya tentang cara mengonfigurasi Amazon VPC subnet, lihat Subnet untuk Anda Amazon VPC di Panduan Pengguna Amazon VPC.

Jika Amazon Kendra harus merutekan koneksi antara dua atau lebih subnet, Anda dapat menyiapkan beberapa subnet. Misalnya, subnet yang berisi sumber data Anda kehabisan alamat IP. Dalam hal ini, Anda dapat Amazon Kendra menyediakan subnet tambahan yang memiliki alamat IP yang cukup dan terhubung ke subnet pertama. Jika Anda mencantumkan lebih dari satu subnet, subnet harus dapat berkomunikasi satu sama lain.

Langkah 2. Buat grup Amazon VPC keamanan untuk Amazon Kendra

Untuk menghubungkan konektor sumber Amazon Kendra data Anda Amazon VPC, Anda harus menyiapkan satu atau beberapa grup keamanan dari VPC Anda untuk ditetapkan. Amazon Kendra Grup keamanan akan dikaitkan dengan elastic network interface yang dibuat oleh Amazon Kendra. Antarmuka jaringan ini mengontrol lalu lintas masuk dan keluar ke dan dari Amazon Kendra saat mengakses subnet. Amazon VPC

Pastikan bahwa aturan keluar grup keamanan Anda memungkinkan lalu lintas dari konektor sumber Amazon Kendra data untuk mengakses subnet dan sumber data yang akan Anda sinkronkan. Misalnya, Anda mungkin menggunakan MySQL konektor untuk menyinkronkan dari MySQL database. Jika Anda menggunakan port default, grup keamanan harus mengizinkan Amazon Kendra untuk mengakses port 3306 pada host yang menjalankan database.

Sebaiknya Anda mengonfigurasi grup keamanan default dengan nilai berikut Amazon Kendra untuk digunakan:

- Aturan masuk - Jika Anda memilih untuk membiarkan ini kosong, semua lalu lintas masuk akan diblokir.
- Aturan keluar — Tambahkan satu aturan untuk mengizinkan semua lalu lintas keluar sehingga Amazon Kendra dapat memulai permintaan untuk disinkronkan dari sumber data Anda.
  - Versi IP - IPv4
  - Jenis — Semua lalu lintas
  - Protokol — Semua lalu lintas
  - Rentang port - Semua
  - Tujuan — 0.0.0.0/0

Untuk informasi selengkapnya tentang cara mengonfigurasi grup Amazon VPC keamanan, lihat Aturan grup keamanan di Panduan Pengguna Amazon VPC.

Langkah 3. Konfigurasikan sumber data eksternal Anda dan Amazon VPC

Pastikan sumber data eksternal Anda memiliki konfigurasi izin dan pengaturan jaringan yang benar Amazon Kendra untuk mengaksesnya. Anda dapat menemukan petunjuk terperinci tentang cara mengonfigurasi sumber data Anda di bagian prasyarat di setiap halaman konektor.

Juga, periksa Amazon VPC pengaturan Anda dan pastikan bahwa sumber data eksternal Anda dapat dijangkau dari subnet yang akan Anda tetapkan. Amazon Kendra Untuk melakukan ini, kami sarankan Anda membuat Amazon EC2 instance di subnet yang sama dengan grup keamanan yang sama dan menguji akses ke sumber data Anda dari Amazon EC2 instance ini. Untuk informasi selengkapnya, lihat Memecahkan masalah koneksi Amazon VPC.

Siapkan sumber Amazon Kendra data untuk terhubung Amazon VPC

Saat Anda menambahkan sumber data baru Amazon Kendra, Anda dapat menggunakan Amazon VPC fitur ini jika konektor sumber data yang dipilih mendukung fitur ini.

Anda dapat mengatur sumber Amazon Kendra data baru dengan Amazon VPC diaktifkan dengan menggunakan AWS Management Console atau Amazon Kendra API. Secara khusus, gunakan operasi CreateDataSourceAPI, lalu gunakan `VpcConfiguration` parameter untuk memberikan informasi berikut:

- `SubnetIds`— Daftar pengidentifikasi subnet Amazon VPC
- `SecurityGroupIds`— Daftar pengidentifikasi kelompok Amazon VPC keamanan

Jika Anda menggunakan konsol, Anda memberikan Amazon VPC informasi yang diperlukan selama konfigurasi konektor. Untuk menggunakan konsol untuk mengaktifkan fitur Amazon VPC untuk konektor, pertama-tama Anda memilih VPC Amazon. Kemudian, Anda memberikan pengidentifikasi subnet VPC Amazon dan pengidentifikasi grup keamanan VPC Amazon apa pun. Anda dapat memilih subnet Amazon VPC dan grup keamanan Amazon VPC yang Anda buat di Mengonfigurasi Amazon VPC, atau menggunakan yang sudah ada.

Topik

- Melihat Amazon VPC pengidentifikasi
- Memeriksa IAM peran sumber data Anda

Melihat Amazon VPC pengidentifikasi

Pengidentifikasi untuk subnet dan grup keamanan dikonfigurasi di konsol. Amazon VPC Untuk melihat pengidentifikasi, gunakan prosedur berikut.

Untuk melihat pengenal subnet

1. Masuk ke AWS Management Console dan buka konsol VPC Amazon di https://console.aws.amazon.com/vpc/.
2. Dari panel navigasi, pilih Subnet.
3. Dari daftar Subnet, pilih subnet yang berisi server database Anda.
4. Dari tab Detail, buat catatan pengenal di bidang Subnet ID.

Untuk melihat pengenal grup keamanan

1. Masuk ke AWS Management Console dan buka konsol VPC Amazon di https://console.aws.amazon.com/vpc/.
2. Dari panel navigasi, pilih Grup keamanan.
3. Dari daftar grup keamanan, pilih grup yang ingin Anda lihat pengenalnya.
4. Dari tab Detail, buat catatan pengenal di bidang ID Grup Keamanan.

Memeriksa IAM peran sumber data Anda

Pastikan bahwa konektor sumber data Anda AWS Identity and Access Management IAM) peran berisi izin untuk mengakses Anda Amazon VPC.

Jika Anda menggunakan konsol untuk membuat peran baru untuk IAM peran Anda, Amazon Kendra secara otomatis menambahkan izin yang benar ke IAM peran Anda atas nama Anda. Jika Anda menggunakan API, atau menggunakan IAM peran yang ada, periksa apakah peran Anda berisi izin untuk mengakses Amazon VPC. Untuk memverifikasi bahwa Anda memiliki izin yang tepat, lihat IAM peran untuk VPC.

Anda dapat memodifikasi sumber data yang ada untuk menggunakan Amazon VPC subnet yang berbeda. Namun, periksa IAM peran sumber data Anda dan, jika perlu, modifikasi untuk mencerminkan perubahan agar konektor sumber Amazon Kendra data berfungsi dengan baik.

Menghubungkan ke basis data di VPC

Contoh berikut menunjukkan bagaimana menghubungkan MySQL database yang berjalan di virtual private cloud (VPC). Contohnya mengasumsikan bahwa Anda memulai dengan VPC default Anda dan Anda perlu membuat MySQL database. Jika Anda sudah memiliki VPC, pastikan itu dikonfigurasi seperti yang ditunjukkan. Jika Anda memiliki MySQL database, Anda dapat menggunakannya alih-alih membuat yang baru.

Langkah-langkah

- Langkah 1: Konfigurasikan VPC
- Langkah 2: Buat dan konfigurasikan grup keamanan
- Langkah 3: Buat basis data
- Langkah 4: Buat konektor sumber data

Langkah 1: Konfigurasikan VPC

Konfigurasikan VPC Anda sehingga Anda memiliki subnet pribadi dan grup keamanan Amazon Kendra untuk mengakses MySQL database yang berjalan di subnet. Subnet yang disediakan dalam konfigurasi VPC harus berada di Wilayah AS Barat (Oregon), Wilayah AS Timur (Virginia N.), atau Wilayah Eropa (Irlandia).

Untuk mengkonfigurasi VPC menggunakan Amazon VPC

1. Masuk ke AWS Management Console dan buka konsol VPC Amazon di https://console.aws.amazon.com/vpc/.
2. Dari panel navigasi, pilih Tabel perutean, lalu pilih Buat tabel perutean.
3. Untuk bidang Nama, masukkan**`Private subnet route table`**. Dari dropdown VPC, pilih VPC Anda, lalu pilih Buat tabel rute. Pilih Tutup untuk kembali ke daftar tabel perutean.
4. Dari panel navigasi, pilih gateway NAT, lalu pilih Buat gateway NAT.
5. Dari dropdown Subnet, pilih subnet yang merupakan subnet publik. Catat subnet ID.
6. Jika Anda tidak memiliki Alamat IP elastis, pilih Buat EIP Baru, pilih Buat Gateway NAT, lalu pilih Tutup.
7. Dari panel navigasi, pilih Tabel rute.
8. Dari daftar tabel perutean, pilih Tabel rute subnet privat yang Anda buat pada langkah 3. Dari Tindakan, pilih Edit rute.

9. Pilih Tambahkan rute. Untuk tujuan, masukkan **`0.0.0.0/0`** untuk memungkinkan semua lalu lintas keluar ke internet. Untuk Target, pilih NAT Gateway, lalu pilih gateway yang Anda buat di langkah 4. Pilih Simpan perubahan, lalu pilih Tutup.
10. Dari Tindakan, pilih Edit pengaitan subnet.
11. Pilih subnet yang ingin dijadikan privat. Jangan memilih subnet dengan gateway NAT yang Anda catat sebelumnya. Pilih Simpan asosiasi setelah selesai.

Langkah 2: Buat dan konfigurasikan grup keamanan

Selanjutnya, konfigurasikan grup keamanan untuk basis data Anda.

Untuk membuat dan mengkonfigurasi grup keamanan

1. Masuk ke AWS Management Console dan buka konsol VPC Amazon di https://console.aws.amazon.com/vpc/.
2. Dari deskripsi VPC Anda, catat CIDR IPv4 yang ada.
3. Dari panel navigasi, pilih Grup keamanan lalu pilih Buat grup keamanan.
4. Untuk Nama grup keamanan, masukkan **`DataSourceInboundSecurityGroup`**. Berikan deskripsi, lalu pilih VPC Anda dari daftar. Pilih Buat grup keamanan dan kemudian pilih Tutup.
5. Pilih tab Aturan masuk.
6. Pilih Edit aturan masuk, lalu pilih Tambah aturan
7. Untuk database, masukkan nomor port untuk rentang Port. Misalnya, untuk MySQL itu**`3306`**, dan, untuk HTTPS, itu**`443`**. Untuk Sumber, ketikkan Perutean Inter-Domain Tanpa Kelas (CIDR) VPC Anda. Pilih Simpan aturan, kemudian pilih Tutup.

Grup keamanan memungkinkan siapa pun dalam VPC untuk terhubung ke basis data, dan memungkinkan koneksi keluar ke internet.

Langkah 3: Buat basis data

Buat database untuk menyimpan dokumen Anda, atau Anda dapat menggunakan database yang ada.

Untuk petunjuk tentang cara membuat MySQL database, lihat MySQL.

Langkah 4: Buat konektor sumber data

Setelah Anda mengkonfigurasi VPC Anda dan membuat database Anda, Anda dapat membuat konektor sumber data untuk database. Untuk informasi tentang konektor database yang Amazon Kendra mendukung, lihat Konektor yang didukung.

Untuk database Anda, pastikan bahwa Anda mengkonfigurasi VPC Anda, subnet pribadi yang Anda buat di VPC Anda, dan grup keamanan yang Anda buat di VPC Anda.

Memecahkan masalah koneksi VPC

Jika Anda mengalami masalah dengan koneksi virtual private cloud (VPC) Anda, periksa apakah IAM izin, pengaturan grup keamanan, dan tabel rute subnet dikonfigurasi dengan benar.

Salah satu penyebab potensial dari sinkronisasi konektor sumber data yang gagal adalah bahwa sumber data mungkin tidak dapat dijangkau dari subnet yang Anda tetapkan. Amazon Kendra Untuk mengatasi masalah ini, sebaiknya Anda membuat Amazon EC2 instance dengan pengaturan yang sama Amazon VPC . Kemudian, coba akses sumber data dari Amazon EC2 instance ini menggunakan panggilan REST API atau metode lain (berdasarkan tipe spesifik sumber data Anda).

Jika Anda berhasil mengakses sumber data dari Amazon EC2 instance yang Anda buat, itu berarti sumber data Anda dapat dijangkau dari subnet ini. Oleh karena itu, masalah sinkronisasi Anda tidak terkait dengan sumber data Anda yang tidak dapat diakses oleh Amazon VPC.

Jika Anda tidak dapat mengakses Amazon EC2 instans dari konfigurasi VPC dan memvalidasinya dengan Amazon EC2 instance yang Anda buat, Anda perlu memecahkan masalah lebih lanjut. Misalnya, jika Anda memiliki Amazon S3 konektor yang sinkronisasi gagal dengan kesalahan terkait masalah koneksi, Anda dapat mengatur Amazon EC2 instance dengan Amazon VPC konfigurasi yang sama dengan yang Anda tetapkan ke Amazon S3 konektor Anda. Kemudian, gunakan instans Amazon EC2 ini untuk menguji apakah Anda Amazon VPC telah diatur dengan benar.

Berikut ini adalah contoh pengaturan Amazon EC2 instance untuk memecahkan masalah Amazon VPC koneksi Anda dengan sumber Amazon S3 data.

Topik

- Langkah 1: Luncurkan sebuah Amazon EC2 instance
- Langkah 2: Connect ke Amazon EC2 instance
- Langkah 3: Uji Amazon S3 akses

Langkah 1: Luncurkan sebuah Amazon EC2 instance

1. Masuk ke AWS Management Console dan buka konsol Amazon EC2 di https://console.aws.amazon.com/ec2/.
2. Pilih Luncurkan instance.
3. Pilih Pengaturan jaringan, lalu pilih Edit, lalu lakukan hal berikut:

   a. Pilih VPC dan Subnet yang sama dengan yang Anda tetapkan. Amazon Kendra

   b. Untuk Firewall (grup keamanan), pilih Pilih grup keamanan yang ada. Kemudian, pilih grup keamanan yang Anda tetapkan Amazon Kendra.

   > **Note**
   >
   > Kelompok keamanan harus mengizinkan lalu lintas keluar ke Amazon S3.

   c. Setel Auto-tetapkan IP publik ke Nonaktifkan.

   d. Dalam Detail lanjutan, lakukan hal berikut:

   - Untuk profil instans IAM, pilih Buat profil IAM baru untuk membuat dan melampirkan profil IAM instance ke instans Anda. Pastikan profil memiliki izin untuk mengakses Amazon S3. Untuk informasi selengkapnya, lihat Bagaimana cara memberikan akses Amazon EC2 instans ke Amazon S3 bucket? di AWS re:Post.
   - Biarkan semua pengaturan lainnya sebagai default.

   e. Tinjau dan luncurkan Amazon EC2 instance.

Langkah 2: Connect ke Amazon EC2 instance

Setelah Amazon EC2 instance Anda berjalan, buka halaman detail instance Anda dan sambungkan ke instance Anda. Untuk melakukannya, gunakan langkah-langkah di Connect ke instans Anda tanpa memerlukan alamat IPv4 publik menggunakan EC2 Instance Connect Endpoint di Panduan Pengguna untuk Instans Amazon EC2 Linux.

Langkah 3: Uji Amazon S3 akses

Setelah Anda terhubung ke terminal Amazon EC2 instans Anda, jalankan AWS CLI perintah untuk menguji koneksi dari subnet pribadi ini ke Amazon S3 bucket Anda.

Untuk menguji Amazon S3 akses, ketik AWS CLI perintah berikut di AWS CLI: `aws s3 ls`

Setelah AWS CLI perintah berjalan, tinjau hal-hal berikut:

- Jika Anda telah mengatur IAM izin yang diperlukan dengan benar dan Amazon S3 penyiapan Anda benar, Anda akan melihat daftar Amazon S3 bucket Anda.
- Jika Anda melihat kesalahan izin seperti`Access Denied`, kemungkinan konfigurasi VPC Anda benar, tetapi ada yang salah dengan IAM izin atau Amazon S3 kebijakan bucket Anda.

Jika perintahnya habis waktu, kemungkinan koneksi Anda habis waktu karena pengaturan VPC Anda salah dan instans Amazon EC2 tidak dapat mengakses Amazon S3 dari subnet Anda. Konfigurasikan ulang VPC Anda, dan coba lagi.

Menghapus indeks, sumber data, atau dokumen yang diunggah secara batch

Bagian ini menunjukkan cara menghapus indeks, respositori sumber data dokumen dalam indeks Anda, atau dokumen dalam indeks yang Anda unggah secara batch.

Topik

Menghapus indeks

Anda dapat menghapus indeks dari Amazon Kendra saat Anda tidak lagi menggunakan indeks. Misalnya, menghapus indeks saat:

- Anda tidak lagi menggunakan indeks dan ingin mengurangi biaya ke akun AWS Anda. Amazon KendraIndeks dikenakan biaya saat sedang berjalan apakah Anda membuat kueri pada indeks atau tidak.
- Anda ingin mengkonfigurasi ulang indeks untuk edisi yang berbeda. Amazon Kendra Menghapus indeks yang ada dan kemudian membuat yang baru dengan edisi yang berbeda.
- Anda telah mencapai jumlah maksimum indeks di akun Anda dan tidak ingin melebihi kuota Anda. Menghapus indeks yang ada dan menambahkan yang baru. Untuk informasi tentang jumlah maksimum indeks yang dapat Anda buat, lihat Kuota.

Untuk menghapus indeks, gunakan konsolAWS Command Line Interface, AWS CloudFormation skrip, atau `DeleteIndex` API. Menghapus indeks akan menghapus indeks dan semua sumber data terkait dan juga data dokumen. Menghapus indeks tidak akan menghapus dokumen asli dari penyimpanan Anda.

Menghapus indeks adalah operasi asinkron. Ketika Anda mulai menghapus indeks, status indeks berubah menjadi `DELETING`. Ini tetap dalam status `DELETING` sampai semua informasi yang terkait dengan indeks dihapus. Setelah indeks dihapus, itu tidak lagi muncul dalam hasil panggilan ke ListIndicesAPI. Jika Anda memanggil DescribeIndexAPI dengan pengidentifikasi indeks dihapus, Anda menerima dan `ResourceNotFound` pengecualian.

Untuk menghapus indeks (konsol)

1. Masuk ke AWS Management Console dan buka Amazon Kendra konsol di https://console.aws.amazon.com/kendra/.
2. Di panel navigasi, pilih indeks, lalu pilih indeks yang akan dihapus.
3. Pilih Hapus untuk menghapus indeks yang dipilih.

Untuk menghapus suatu indeks (CLI)

- Di AWS CLI, gunakan perintah berikut. Perintah ini diformat untuk Linux dan macOS. Jika menggunakan Windows, ganti karakter kelanjutan baris Unix (\) dengan caret (^).

```
aws kendra delete-index \
   --id index-id
```

Menghapus sumber data

Anda menghapus sumber data ketika Anda ingin menghapus informasi yang terkandung dalam sumber data dari Amazon Kendra indeks Anda. Misalnya, hapus sumber data saat:

- Sumber data salah dikonfigurasi. Hapus sumber data, tunggu sampai sumber data selesai dihapus, lalu buat ulang.
- Memigrasikan dokumen dari satu sumber data ke sumber data lainnya. Hapus sumber data asli dan buat ulang di lokasi yang baru.
- Anda telah mencapai batas sumber data untuk indeks. Hapus salah satu sumber data yang ada, lalu tambahkan yang baru. Untuk informasi lebih lanjut tentang jumlah sumber data yang dapat Anda buat, lihat Kuota.

Untuk menghapus sumber data, gunakan konsol, AWS Command Line Interface (AWS CLI), `DeleteDataSource` API, atau AWS CloudFormation skrip. Menghapus sumber data akan menghapus semua informasi tentang sumber data tersebut dari indeks. Jika hanya ingin berhenti menyinkronkan sumber data, ubah jadwal sinkronisasi untuk sumber data menjadi "berjalan sesuai permintaan".

Menghapus sumber data adalah operasi asinkron. Saat Anda mulai menghapus sumber data, status sumber data akan berubah menjadi `DELETING`. Sumber data tetap dalam status `DELETING` sampai

semua informasi yang terkait dengannya dihapus. Setelah sumber data dihapus, itu tidak lagi muncul di hasil panggilan ke ListDataSourcesAPI. Jika Anda memanggil DescribeDataSourceAPI dengan pengidentifikasi sumber data yang dihapus, Anda menerima `ResourceNotFound` pengecualian.

> **Note**
>
> Menghapus seluruh sumber data atau menyinkronkan kembali indeks Anda setelah menghapus dokumen tertentu dari sumber data dapat memakan waktu hingga satu jam atau lebih, tergantung pada jumlah dokumen yang ingin Anda hapus.

Untuk menghapus sumber data (konsol)

1. Masuk ke AWS Management Console dan buka Amazon Kendra konsol di https://console.aws.amazon.com/kendra/.
2. Di panel navigasi, pilih Indeks, lalu pilih indeks berisi sumber data yang akan dihapus.
3. Di panel navigasi, pilih Sumber data.
4. Pilih sumber data yang akan dihapus.
5. Pilih Hapus untuk menghapus sumber data.

Untuk menghapus sumber data (CLI)

- Di AWS Command Line Interface, gunakan perintah berikut. Perintah ini diformat untuk Linux dan macOS. Jika menggunakan Windows, ganti karakter kelanjutan baris Unix (\) dengan caret (^).

```
aws kendra delete-data-source \
   --id data-source-id \
   --index-id index-id
```

Saat Anda menghapus sumber data, Amazon Kendra hapus semua informasi yang tersimpan tentang sumber data. Amazon Kendramenghapus semua data dokumen yang disimpan dalam indeks, dan semua sejarah berjalan dan metrik yang terkait dengan sumber data. Menghapus sumber data tidak akan menghapus dokumen asli dari penyimpanan Anda.

Dokumen dalam sumber data dapat dimasukkan dalam jumlah dokumen yang dikembalikan oleh `DescribeIndex` API saat Amazon Kendra menghapus sumber data. Dokumen dari sumber data dapat muncul di hasil pencarian saat Amazon Kendra menghapus sumber data.

Amazon Kendramelepaskan sumber daya untuk sumber data segera setelah Anda memanggil `DeleteDataSource` API atau memilih untuk menghapus sumber data di konsol. Jika Anda menghapus sumber data untuk mengurangi jumlah sumber data di bawah batas, Anda dapat langsung membuat sumber data baru.

Jika Anda menghapus sumber data lalu membuat sumber data lain untuk data dokumen, tunggu hingga sumber data pertama selesai dihapus sebelum menyinkronkan sumber data yang baru.

Anda dapat menghapus sumber data yang sedang dalam proses sinkronisasi denganAmazon Kendra. Sinkronisasi dihentikan dan sumber data dihapus. Jika mencoba memulai sinkronisasi saat sumber data sedang dihapus, Anda akan mendapatkan pengecualian `ConflictException`.

Anda tidak dapat menghapus sumber data jika indeks yang terkait berada dalam status `DELETING`. Menghapus indeks akan menghapus semua sumber data untuk indeks. Anda dapat mulai menghapus indeks selagi sumber data untuk indeks tersebut dalam status `DELETING`.

Jika Anda memiliki dua sumber data yang menunjuk ke dokumen yang sama, seperti dua sumber data yang menunjuk ke Amazon S3 bucket yang sama, dokumen dalam indeks mungkin tidak konsisten ketika salah satu sumber data dihapus. Ketika dua sumber data mereferensikan dokumen yang sama, hanya satu salinan data dokumen yang akan disimpan dalam indeks. Menghapus satu sumber data akan menghapus data indeks untuk dokumen. Sumber data lainnya tidak menyadari bahwa dokumen telah dihapus, jadi tidak Amazon Kendra akan mengindeks ulang dokumen dengan benar saat berikutnya disinkronkan. Jika memiliki dua sumber data yang mengarah ke lokasi dokumen yang sama, Anda harus menghapus kedua sumber data lalu membuat ulang satu sumber data.

Menghapus dokumen yang diunggah secara batch

Anda dapat menghapus dokumen langsung dari indeks menggunakan BatchDeleteDocumentAPI. Anda tidak dapat menghapus dokumen secara langsung menggunakan konsol. Jika Anda menggunakan konsol, Anda dapat menghapus dokumen tertentu dari repositori sumber data Anda dan menyinkronkan ulang dengan indeks Anda atau menghapus seluruh konektor sumber data.

Menghapus dokumen dari indeks menggunakan `BatchDeleteDocument` adalah operasi asinkron. Setelah Anda memanggil `BatchDeleteDocument` API, Anda menggunakan

BatchGetDocumentStatusAPI untuk memantau kemajuan penghapusan dokumen Anda. Ketika dokumen dihapus dari indeks, Amazon Kendra kembali `NOT_FOUND` sebagai status.

> **Note**
>
> Menghapus dokumen dari indeks menggunakan `BatchDeleteDocument` bisa memakan waktu hingga satu jam atau lebih, tergantung pada jumlah dokumen yang ingin Anda hapus.

Untuk menghapus batch upload dokumen dari indeks (CLI)

- Di AWS Command Line Interface, gunakan perintah berikut. Perintah ini diformat untuk Linux dan macOS. Jika menggunakan Windows, ganti karakter kelanjutan baris Unix (\) dengan caret (^).

```
aws kendra batch-delete-document \
   --index-id index-id \
   --document-id-list 'doc-id-1' 'doc-id-2'
```

Memperkaya dokumen Anda selama konsumsi

Anda dapat mengubah bidang atau atribut metadata konten dan dokumen selama proses konsumsi dokumen. Dengan Amazon Kendra fitur Pengayaan Dokumen Kustom, Anda dapat membuat, memodifikasi, atau menghapus atribut dan konten dokumen saat Anda memasukkan dokumen Anda. Amazon Kendra Ini berarti Anda dapat memanipulasi dan menelan data Anda sesuai kebutuhan.

Fitur ini memberi Anda kendali atas bagaimana dokumen Anda diperlakukan dan dicernaAmazon Kendra. Misalnya, Anda dapat menggosok informasi yang dapat diidentifikasi secara pribadi dalam metadata dokumen sambil menelan dokumen Anda. Amazon Kendra

Cara lain Anda dapat menggunakan fitur ini adalah dengan memanggil fungsi Lambda AWS Lambda untuk menjalankan Optical Character Recognition (OCR) pada gambar, terjemahan pada teks, dan tugas lain untuk menyiapkan data untuk pencarian atau analisis. Misalnya, Anda dapat memanggil fungsi untuk menjalankan OCR pada gambar. Fungsi ini dapat menafsirkan teks dari gambar dan memperlakukan setiap gambar sebagai dokumen tekstual. Sebuah perusahaan yang menerima surat-in survei pelanggan dan menyimpan survei ini sebagai gambar bisa menelan gambar-gambar ini sebagai dokumen tekstual ke dalam. Amazon Kendra Perusahaan kemudian dapat mencari informasi survei pelanggan yang berharga diAmazon Kendra.

Anda dapat menggunakan operasi dasar untuk menerapkan sebagai parse pertama data Anda, dan kemudian menggunakan fungsi Lambda untuk menerapkan operasi yang lebih kompleks pada data Anda. Misalnya, Anda dapat menggunakan operasi dasar untuk menghapus semua nilai di bidang metadata dokumen 'Customer_ID', dan kemudian menerapkan fungsi Lambda untuk mengekstrak teks dari gambar teks dalam dokumen.

Bagaimana Custom Document Enrichment bekerja

Proses keseluruhan Custom Document Enrichment adalah sebagai berikut:

1. Anda mengonfigurasi Pengayaan Dokumen Kustom saat membuat atau memperbarui sumber data, atau mengindeks dokumen Anda secara langsung. Amazon Kendra
2. Amazon Kendramenerapkan konfigurasi inline atau logika dasar untuk mengubah data Anda. Untuk informasi selengkapnya, lihat the section called “Operasi dasar untuk mengubah metadata”.
3. Jika Anda memilih untuk mengkonfigurasi manipulasi data lanjutan, Amazon Kendra dapat menerapkan ini pada dokumen asli, mentah Anda atau pada dokumen terstruktur dan diurai. Untuk

informasi selengkapnya, lihat the section called “Fungsi Lambda: ekstrak dan ubah metadata atau konten”.

4. Dokumen Anda diubah dicerna ke dalam. Amazon Kendra

Pada setiap titik dalam proses ini, jika konfigurasi Anda tidak valid, Amazon Kendra melempar kesalahan.

Saat Anda menelepon CreateDataSourceUpdateDataSource,, atau BatchPutDocumentAPI, Anda menyediakan konfigurasi Pengayaan Dokumen Kustom. Jika Anda meneleponBatchPutDocument, Anda harus mengkonfigurasi Pengayaan Dokumen Kustom dengan setiap permintaan. Jika Anda menggunakan konsol, Anda memilih indeks Anda dan kemudian pilih Dokumen enrichments untuk mengkonfigurasi Custom Document Enrichment.

Jika Anda menggunakan pengayaan Dokumen di konsol, Anda dapat memilih untuk hanya mengonfigurasi operasi dasar atau hanya fungsi Lambda atau keduanya, seperti Anda dapat menggunakan API. Anda dapat memilih Berikutnya dalam langkah-langkah konsol untuk memilih untuk tidak mengonfigurasi operasi dasar dan hanya fungsi Lambda, termasuk apakah akan diterapkan ke data asli (pra-ekstraksi) atau terstruktur (pasca-ekstraksi). Anda hanya dapat menyimpan konfigurasi Anda dengan menyelesaikan semua langkah di konsol. Konfigurasi dokumen Anda tidak disimpan jika Anda tidak menyelesaikan semua langkah.

Operasi dasar untuk mengubah metadata

Anda dapat memanipulasi bidang dokumen dan konten Anda menggunakan logika dasar. Ini termasuk menghapus nilai dalam bidang, memodifikasi nilai dalam bidang menggunakan kondisi, atau membuat bidang. Untuk manipulasi lanjutan yang melampaui apa yang dapat Anda manipulasi menggunakan logika dasar, panggil fungsi Lambda. Untuk informasi selengkapnya, lihat the section called “Fungsi Lambda: ekstrak dan ubah metadata atau konten”.

Untuk menerapkan logika dasar, Anda menentukan bidang target yang ingin Anda manipulasi menggunakan DocumentAttributeTargetobjek. Anda memberikan kunci atribut. Misalnya, kunci 'Departemen' adalah bidang atau atribut yang menyimpan semua nama departemen yang terkait dengan dokumen. Anda juga dapat menentukan nilai yang akan digunakan di bidang target jika kondisi tertentu terpenuhi. Anda mengatur kondisi menggunakan DocumentAttributeConditionobjek. Misalnya, jika kolom 'Source_URI' berisi 'keuangan' dalam nilai URI, maka isi ulang bidang target 'Departemen' dengan nilai target 'Keuangan' untuk dokumen. Anda juga dapat menghapus nilai-nilai atribut dokumen target.

Untuk menerapkan logika dasar menggunakan konsol, pilih indeks Anda dan kemudian pilih Pengayaan dokumen di menu navigasi. Pergi ke Konfigurasi operasi dasar untuk menerapkan manipulasi dasar ke bidang dokumen dan konten Anda.

Berikut ini adalah contoh menggunakan logika dasar untuk menghapus semua nomor identifikasi pelanggan di bidang dokumen yang disebut 'Customer_ID'.

Contoh 1: Menghapus nomor identifikasi pelanggan yang terkait dengan dokumen

Data sebelum manipulasi dasar diterapkan.

Document_ID	Tubuh_Teks	Customer_ID
1	Lorem Ipsum.	CID1234
2	Lorem Ipsum.	CID1235
3	Lorem Ipsum.	CID1236

Data setelah manipulasi dasar diterapkan.

Document_ID	Tubuh_Teks	Customer_ID
1	Lorem Ipsum.	
2	Lorem Ipsum.	
3	Lorem Ipsum.	

Berikut ini adalah contoh menggunakan logika dasar untuk membuat bidang yang disebut 'Departemen' dan mengisi ulang bidang ini dengan nama departemen berdasarkan informasi dari bidang 'Source_uri'. Ini menggunakan kondisi bahwa jika bidang 'Source_URI' berisi 'keuangan' dalam nilai URI, kemudian mengisi ulang bidang target 'Departemen' dengan nilai target 'Keuangan' untuk dokumen.

Contoh 2: Membuat bidang 'Departemen' dan mengisi ulang dengan nama departemen yang terkait dengan dokumen menggunakan kondisi.

Data sebelum manipulasi dasar diterapkan.

Document_ID	Tubuh_Teks	Sumber_URI
1	Lorem Ipsum.	keuangan/1
2	Lorem Ipsum.	keuangan/2
3	Lorem Ipsum.	keuangan/3

Data setelah manipulasi dasar diterapkan.

Document_ID	Tubuh_Teks	Sumber_URI	Departemen
1	Lorem Ipsum.	keuangan/1	Keuangan
2	Lorem Ipsum.	keuangan/2	Keuangan
3	Lorem Ipsum.	keuangan/3	Keuangan

> **Note**
>
> Amazon Kendratidak dapat membuat kolom dokumen target jika belum dibuat sebagai bidang indeks. Setelah Anda membuat bidang indeks Anda, Anda dapat membuat bidang dokumen menggunakan`DocumentAttributeTarget`. Amazon Kendrakemudian memetakan bidang metadata dokumen yang baru dibuat ke bidang indeks Anda.

Kode berikut adalah contoh mengkonfigurasi manipulasi data dasar untuk menghapus nomor identifikasi pelanggan yang terkait dengan dokumen.

Console

Untuk mengkonfigurasi manipulasi data dasar untuk menghapus nomor identifikasi pelanggan

1. Di panel navigasi kiri, di bawah Indeks, pilih Pengayaan dokumen, lalu pilih Tambahkan pengayaan dokumen.
2. Pada halaman Konfigurasi operasi dasar, pilih dari dropdown sumber data Anda yang ingin Anda ubah bidang dokumen dan konten. Kemudian pilih dari dropdown nama bidang

dokumen 'Customer_ID', pilih dari dropdown nama bidang indeks 'Customer_ID', dan pilih dari dropdown tindakan target Hapus. Kemudian pilih Tambahkan operasi dasar.

CLI

Untuk mengkonfigurasi manipulasi data dasar untuk menghapus nomor identifikasi pelanggan

```
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

Untuk mengkonfigurasi manipulasi data dasar untuk menghapus nomor identifikasi pelanggan

```
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

Untuk mengkonfigurasi manipulasi data dasar untuk menghapus nomor identifikasi pelanggan

```
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");
    }
}
```

Fungsi Lambda: ekstrak dan ubah metadata atau konten

Anda dapat memanipulasi bidang dokumen dan konten Anda menggunakan fungsi Lambda. Ini berguna jika Anda ingin melampaui logika dasar dan menerapkan manipulasi data lanjutan. Misalnya, menggunakan Optical Character Recognition (OCR), yang menafsirkan teks dari gambar, dan memperlakukan setiap gambar sebagai dokumen tekstual. Atau, mengambil tanggal-waktu saat ini di zona waktu tertentu dan memasukkan tanggal-waktu di mana ada nilai kosong untuk bidang tanggal.

Anda dapat menerapkan logika dasar terlebih dahulu dan kemudian menggunakan fungsi Lambda untuk memanipulasi data Anda lebih lanjut, atau sebaliknya. Anda juga dapat memilih untuk hanya menerapkan fungsi Lambda.

Amazon Kendradapat memanggil fungsi Lambda untuk menerapkan manipulasi data lanjutan selama proses konsumsi sebagai bagian dari Anda. CustomDocumentEnrichmentConfiguration Anda menentukan peran yang menyertakan izin untuk menjalankan fungsi Lambda dan mengakses Amazon S3 bucket Anda untuk menyimpan output manipulasi IAM data Anda—lihat peran akses.

Amazon Kendradapat menerapkan fungsi Lambda pada dokumen asli, mentah Anda atau pada dokumen terstruktur dan terurai. Anda dapat mengonfigurasi fungsi Lambda yang mengambil data asli atau mentah Anda dan menerapkan manipulasi data Anda menggunakan. PreExtractionHookConfiguration Anda juga dapat mengonfigurasi fungsi Lambda yang mengambil dokumen terstruktur dan menerapkan manipulasi data Anda. PostExtractionHookConfiguration Amazon Kendramengekstrak metadata dokumen dan teks untuk menyusun dokumen Anda. Fungsi Lambda Anda harus mengikuti struktur permintaan dan respons wajib. Untuk informasi selengkapnya, lihat the section called “Kontrak data untuk fungsi Lambda”.

Untuk mengonfigurasi fungsi Lambda di konsol, pilih indeks Anda, lalu pilih Pengayaan dokumen di menu navigasi. Pergi ke fungsi Configure Lambda untuk mengkonfigurasi fungsi Lambda.

Anda dapat mengkonfigurasi hanya satu fungsi Lambda untuk `PreExtractionHookConfiguration` dan dan hanya satu fungsi Lambda untuk. `PostExtractionHookConfiguration` Namun, fungsi Lambda Anda dapat menjalankan fungsi lain yang dibutuhkannya. Anda dapat mengkonfigurasi keduanya `PreExtractionHookConfiguration` dan `PostExtractionHookConfiguration` atau salah satunya. Fungsi Lambda Anda tidak boleh melebihi waktu berjalan 5 menit dan fungsi Lambda Anda tidak boleh melebihi waktu berjalan 1 menit. `PreExtractionHookConfiguration` `PostExtractionHookConfiguration` Mengkonfigurasi Custom Document Enrichment secara alami membutuhkan waktu lebih lama untuk menelan dokumen Anda ke dalam Amazon Kendra daripada jika Anda tidak mengkonfigurasi ini.

Anda dapat mengkonfigurasi Amazon Kendra untuk memanggil fungsi Lambda hanya jika kondisi terpenuhi. Misalnya, Anda dapat menentukan kondisi bahwa jika ada nilai tanggal-waktu kosong, maka Amazon Kendra harus memanggil fungsi yang menyisipkan tanggal-waktu saat ini.

Berikut ini adalah contoh penggunaan fungsi Lambda untuk menjalankan OCR untuk menafsirkan teks dari gambar dan menyimpan teks ini dalam bidang yang disebut 'Document_Image_Text'.

Contoh 1: Mengekstrak teks dari gambar untuk membuat dokumen tekstual

Data sebelum manipulasi lanjutan diterapkan.

Document_ID	Document_Image
1	image_1.png
2	image_2.png
3	image_3.png

Data setelah manipulasi lanjutan diterapkan.

Document_ID	Document_Image	Document_Image_Text
1	image_1.png	Tanggapan survei yang dikirimkan
2	image_2.png	Tanggapan survei yang dikirimkan
3	image_3.png	Tanggapan survei yang dikirimkan

Berikut ini adalah contoh penggunaan fungsi Lambda untuk memasukkan tanggal-waktu saat ini untuk nilai tanggal kosong. Ini menggunakan kondisi bahwa jika nilai bidang tanggal adalah 'null', kemudian ganti ini dengan tanggal-waktu saat ini.

Contoh 2: Mengganti nilai kosong di bidang Last_Updated dengan tanggal-waktu saat ini.

Data sebelum manipulasi lanjutan diterapkan.

Document_ID	Tubuh_Teks	Last_Diperbarui
1	Lorem Ipsum.	Januari 1, 2020
2	Lorem Ipsum.	
3	Lorem Ipsum.	1 Juli 2020

Data setelah manipulasi lanjutan diterapkan.

Document_ID	Tubuh_Teks	Last_Diperbarui
1	Lorem Ipsum.	Januari 1, 2020
2	Lorem Ipsum.	Desember 1, 2021
3	Lorem Ipsum.	1 Juli 2020

Kode berikut adalah contoh konfigurasi fungsi Lambda untuk manipulasi data tingkat lanjut pada data asli mentah.

Console

Untuk mengonfigurasi fungsi Lambda untuk manipulasi data lanjutan pada data asli mentah

1. Di panel navigasi kiri, di bawah Indeks, pilih Pengayaan dokumen, lalu pilih Tambahkan pengayaan dokumen.
2. Pada halaman Konfigurasi fungsi Lambda, di bagian Lambda untuk pra-ekstraksi, pilih dari dropdown fungsi Lambda ARN dan bucket Anda. Amazon S3 Tambahkan peran IAM akses Anda dengan memilih opsi untuk membuat peran baru dari dropdown. Ini menciptakan Amazon Kendra izin yang diperlukan untuk membuat pengayaan dokumen.

CLI

Untuk mengonfigurasi fungsi Lambda untuk manipulasi data lanjutan pada data asli mentah

```
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

Untuk mengonfigurasi fungsi Lambda untuk manipulasi data lanjutan pada data asli mentah

```
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

Untuk mengonfigurasi fungsi Lambda untuk manipulasi data lanjutan pada data asli mentah

```
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");
    }
}
```

Kontrak data untuk fungsi Lambda

Fungsi Lambda Anda untuk manipulasi data tingkat lanjut berinteraksi dengan Amazon Kendra kontrak data. Kontrak adalah struktur permintaan dan respons wajib dari fungsi Lambda Anda. Jika fungsi Lambda Anda tidak mengikuti struktur ini, maka Amazon Kendra lempar kesalahan.

Fungsi Lambda Anda `PreExtractionHookConfiguration` harus mengharapkan struktur permintaan berikut:

```
{
    "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>
}
```

`metadata`Struktur, yang meliputi `CustomDocumentAttribute` struktur, adalah sebagai berikut:

```
{
    "attributes": [<CustomDocumentAttribute<]
}

CustomDocumentAttribute
```

```
{
    "name": <str>,
    "value": <CustomDocumentAttributeValue>
}

CustomDocumentAttributeValue
{
    "stringValue": <str>,
    "integerValue": <int>,
    "longValue": <long>,
    "stringListValue": list<str>,
    "dateValue": <str>
}
```

Fungsi Lambda Anda `PreExtractionHookConfiguration` harus mematuhi struktur respons berikut:

```
{
    "version": <str>,
    "dataBlobStringEncodedInBase64": <str>, //In the case of a data blob
    "s3ObjectKey": <str>, //In the case of an S3 bucket
    "metadataUpdates": [<CustomDocumentAttribute>]
}
```

Fungsi Lambda Anda `PostExtractionHookConfiguration` harus mengharapkan struktur permintaan berikut:

```
{
    "version": <str>,
    "s3Bucket": <str>,
    "s3ObjectKey": <str>,
    "metadata": <Metadata>
}
```

Fungsi Lambda Anda `PostExtractionHookConfiguration` harus mematuhi struktur respons berikut:

```
PostExtractionHookConfiguration Lambda Response
{
    "version": <str>,
    "s3ObjectKey": <str>,
```

```
    "metadataUpdates": [<CustomDocumentAttribute>]
}
```

Dokumen Anda yang diubah diunggah ke Amazon S3 bucket Anda. Dokumen yang diubah harus mengikuti format yang ditunjukkan dithe section called “Format dokumen terstruktur”.

Format dokumen terstruktur

Amazon Kendramengunggah dokumen terstruktur Anda ke Amazon S3 bucket yang diberikan. Dokumen terstruktur mengikuti format ini:

```
Kendra document

{
   "textContent": <TextContent>
}

TextContent
{
  "documentBodyText": <str>
}
```

Contoh fungsi Lambda yang mematuhi kontrak data

Kode Python berikut adalah contoh fungsi Lambda yang menerapkan manipulasi lanjutan dari bidang metadata_authors,_document_title, dan isi isi pada dokumen mentah atau asli.

Dalam kasus konten tubuh berada dalam ember Amazon S3

```
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"]}}
        ]
    }
```

Dalam kasus konten tubuh berada dalam gumpalan data

```
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"]}}
        ]
    }
```

Kode Python berikut adalah contoh dari fungsi Lambda yang menerapkan manipulasi lanjutan dari bidang metadata_authors,_document_title, dan isi isi pada dokumen terstruktur atau diurai.

```
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":{"stringListValue":["author1", "author2"]}}
        ]
    }
```

Mencari indeks

Untuk mencari Amazon Kendra indeks, Anda menggunakan Query API. `Query`API mengembalikan informasi tentang dokumen yang diindeks yang Anda gunakan dalam aplikasi Anda. Bagian ini menunjukkan cara membuat kueri, melakukan filter, dan menafsirkan respons yang Anda dapatkan dari `Query` API.

Untuk mencari dokumen yang telah Anda indeks Amazon Lex, gunakan Amazon Kendra AMAZON. KendraSearchIntent. Untuk contoh mengonfigurasi Amazon Kendra dengan Amazon Lex, lihat Membuat Bot FAQ untuk Indeks. Amazon Kendra

Topik

Mengueri sebuah indeks

Saat Anda mencari indeks Anda, Amazon Kendra gunakan semua informasi yang Anda berikan tentang dokumen Anda untuk menentukan dokumen yang paling relevan dengan istilah pencarian yang dimasukkan. Beberapa item yang Amazon Kendra dipertimbangkan adalah:

- Teks atau badan dokumen.
- Judul dokumen.
- Bidang teks khusus yang telah Anda tandai sebagai dapat dicari.

- Bidang tanggal yang telah Anda tunjukkan harus digunakan untuk menentukan “kesegaran” dokumen.
- Bidang lain yang dapat memberikan informasi yang relevan.

Amazon Kendra juga dapat memfilter respons berdasarkan filter bidang/atribut apa pun yang mungkin telah Anda tetapkan untuk pencarian. Misalnya, jika Anda memiliki bidang khusus yang disebut “departemen”, Anda dapat memfilter respons untuk mengembalikan hanya dokumen dari departemen yang disebut “legal”. Untuk informasi selengkapnya, lihat Bidang atau atribut khusus.

Hasil pencarian yang dikembalikan diurutkan berdasarkan relevansi yang Amazon Kendra menentukan untuk setiap dokumen. Hasilnya dipaginasi sehingga Anda dapat menampilkan halaman pada satu waktu untuk pengguna Anda.

Untuk mencari dokumen yang telah Anda indeks Amazon Lex, gunakan Amazon Kendra AMAZON.KendraSearchIntent. Untuk contoh mengonfigurasi Amazon Kendra dengan Amazon Lex, lihat Membuat Bot FAQ untuk Indeks. Amazon Kendra

Contoh berikut menunjukkan cara mencari indeks. Amazon Kendra menentukan jenis hasil pencarian (jawaban, dokumen, pertanyaan-jawaban) yang paling cocok untuk kueri. Anda tidak dapat mengonfigurasi Amazon Kendra untuk mengembalikan jenis respons penelusuran tertentu (jawaban, dokumen, pertanyaan-jawaban) ke kueri.

Untuk informasi selengkapnya tentang respons kueri, lihat Respons kueri dan jenis respons.

Prasyarat

Sebelum menggunakan Query API untuk menanyakan indeks:

- Siapkan izin yang diperlukan untuk indeks dan sambungkan ke sumber data atau unggah dokumen secara batch. Untuk informasi selengkapnya, lihat IAM peran. Anda menggunakan Nama Sumber Daya Amazon peran saat memanggil API untuk membuat konektor indeks dan sumber data atau unggahan dokumen secara batch.
- Siapkan salah satu AWS Command Line Interface, SDK, atau pergi ke Amazon Kendra konsol. Untuk informasi selengkapnya, lihat Menyiapkan Amazon Kendra.
- Buat indeks dan sambungkan ke sumber data dokumen atau dokumen unggahan batch. Untuk informasi selengkapnya, lihat Membuat indeks dan Membuat konektor sumber data.

Mencari indeks (konsol)

Anda dapat menggunakan Amazon Kendra konsol untuk mencari dan menguji indeks Anda. Anda bisa membuat kueri dan melihat hasilnya.

Untuk mencari indeks dengan konsol

1. Masuk ke AWS Management Console dan buka Amazon Kendra konsol di http://console.aws.amazon.com/kendra/.
2. Di panel navigasi, pilih Indeks.
3. Pilih indeks Anda.
4. Di menu navigasi, pilih opsi untuk mencari indeks Anda.
5. Masukkan kueri di kotak teks dan kemudian tekan enter.
6. Amazon Kendra mengembalikan hasil pencarian.

Anda juga bisa mendapatkan ID kueri untuk pencarian dengan memilih ikon bola lampu di panel samping.

Mencari indeks (SDK)

Untuk mencari indeks dengan Python atau Java

- Contoh berikut mencari indeks. Mengubah nilai `query` ke kueri pencarian Anda dan `index_id` atau `indexId` untuk pengenal indeks dari indeks yang ingin Anda cari.

  Anda juga bisa mendapatkan ID kueri untuk pencarian sebagai bagian dari elemen respons saat Anda memanggil Query API.

  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");
        }
    }
}
```

Mencari indeks (Postman)

Anda dapat menggunakan Postman untuk menanyakan dan menguji Amazon Kendra indeks Anda.

Untuk mencari indeks menggunakan Postman

1. Buat koleksi baru di Postman dan atur jenis permintaan ke POST.
2. Masukkan URL titik akhir. Misalnya, https://kendra. .amazonaws.com. <region>
3. Pilih tab Otorisasi dan masukkan informasi berikut.
   - Ketik —Pilih AWS tanda tangan.
   - AccessKey—Masukkan kunci akses yang dihasilkan saat Anda membuat IAM pengguna.
   - SecretKey—Masukkan kunci rahasia yang dihasilkan saat Anda membuat IAM pengguna.
   - AWS Wilayah —Masukkan wilayah indeks Anda. Misalnya, us-barat-2.
   - Nama Layanan —Masukkan kendra. Ini peka huruf besar/kecil, jadi harus huruf kecil.

   > **Warning**
   >
   > Jika Anda memasukkan nama layanan yang salah atau tidak menggunakan huruf kecil, kesalahan akan muncul setelah Anda memilih Kirim untuk mengirim permintaan: “Kredenal harus dicakup ke layanan 'kendra' yang benar.”
   > Anda juga harus memeriksa apakah Anda memasukkan kunci akses dan kunci rahasia yang benar.

4. Pilih tab Header dan masukkan informasi kunci dan nilai berikut.
   - Kunci: X-Amz-Target

     Nilai: com.amazonaws.kendra. AWSKendraFrontendService.Permintaan
   - Kunci: Pengkodean Konten

     Nilai: amz-1.0
5. Pilih tab Body dan lakukan hal berikut.
   - Pilih tipe JSON mentah untuk isi permintaan.
   - Masukkan JSON yang menyertakan ID indeks dan teks kueri Anda.

```
{
    "IndexId": "index-id",
    "QueryText": "enter a query here"
}
```

> **Warning**
>
> Jika JSON Anda tidak menggunakan indendasi yang benar, kesalahan akan muncul: "". SerializationException Periksa indendasi di JSON Anda.

6. Pilih Kirim (dekat kanan atas).

Mencari dengan sintaks kueri tingkat lanjut

Anda dapat membuat kueri yang lebih spesifik daripada kata kunci sederhana atau kueri bahasa alami dengan menggunakan sintaks kueri lanjutan atau operator. Ini termasuk rentang, Boolean, wildcard, dan banyak lagi. Dengan menggunakan operator, Anda dapat memberikan kueri Anda lebih banyak konteks dan lebih menyempurnakan hasil pencarian.

Amazon Kendra mendukung operator berikut.

- Boolean: Logika untuk membatasi atau memperluas pencarian. Misalnya, `amazon AND sports` batasi pencarian hanya untuk mencari dokumen yang berisi kedua istilah tersebut.
- Tanda kurung: Membaca istilah kueri bersarang dalam urutan prioritas. Misalnya, `(amazon AND sports) NOT rainforest` membaca `(amazon AND sports)` sebelumnya`NOT rainforest`.
- Rentang: Tanggal atau nilai rentang numerik. Rentang bisa inklusif, eksklusif, atau tidak terbatas. Misalnya, Anda dapat mencari dokumen yang terakhir diperbarui antara 1 Januari 2020 dan 31 Desember 2020, termasuk tanggal-tanggal tersebut.
- Bidang: Menggunakan bidang tertentu untuk membatasi pencarian. Misalnya, Anda dapat mencari dokumen yang memiliki 'Amerika Serikat' di bidang 'lokasi'.
- Wildcard: Sebagian cocok dengan string teks. Misalnya, `Cloud*` bisa cocok CloudFormation. Amazon Kendra saat ini hanya mendukung wildcard trailing.
- Kutipan yang tepat: Cocokkan dengan string teks. Misalnya, dokumen yang berisi`"Amazon Kendra" "pricing"`.

Anda dapat menggunakan kombinasi dari salah satu operator di atas.

Perhatikan bahwa penggunaan operator yang berlebihan atau kueri yang sangat kompleks dapat memengaruhi latensi kueri. Wildcard adalah beberapa operator paling mahal dalam hal latensi. Aturan umum adalah semakin banyak istilah dan operator yang Anda gunakan, semakin besar

potensi dampak pada latensi. Faktor lain yang memengaruhi latensi termasuk ukuran rata-rata dokumen yang diindeks, ukuran indeks Anda, pemfilteran apa pun pada hasil pencarian, dan beban keseluruhan pada indeks Anda. Amazon Kendra

Boolean

Anda dapat menggabungkan atau mengecualikan kata-kata menggunakan operator Boolean`AND`,`OR`,`NOT`.

Berikut ini adalah contoh menggunakan operator Boolean.

`amazon AND sports`

Mengembalikan hasil pencarian yang berisi istilah 'amazon' dan 'olahraga' dalam teks, seperti olahraga video Amazon Prime atau konten serupa lainnya.

`sports OR recreation`

Mengembalikan hasil pencarian yang berisi istilah 'olahraga' atau 'rekreasi', atau keduanya, dalam teks.

`amazon NOT rainforest`

Mengembalikan hasil pencarian yang berisi istilah 'amazon' tetapi bukan istilah 'hutan hujan' dalam teks. Ini untuk mencari dokumen tentang perusahaan Amazon, bukan Hutan Hujan Amazon.

Tanda kurung

Anda dapat menanyakan kata-kata bersarang dalam urutan prioritas dengan menggunakan tanda kurung. Tanda kurung menunjukkan Amazon Kendra bagaimana kueri harus dibaca.

Berikut ini adalah contoh penggunaan operator kurung.

`(amazon AND sports) NOT rainforest`

Mengembalikan dokumen yang berisi istilah 'amazon' dan 'olahraga' dalam teks, tetapi bukan istilah 'hutan hujan'. Ini untuk mencari olahraga video Amazon Prime atau konten serupa lainnya, bukan olahraga petualangan di Hutan Hujan Amazon. Tanda kurung membantu menunjukkan bahwa `amazon AND sports` harus dibaca sebelumnya. `NOT rainforest` Kueri tidak boleh dibaca sebagai`amazon AND (sports NOT rainforest)`.

`(amazon AND (sports OR recreation)) NOT rainforest`

Mengembalikan dokumen yang berisi istilah 'olahraga' atau 'rekreasi', atau keduanya, dan istilah 'amazon'. Tapi itu tidak termasuk istilah 'hutan hujan'. Ini untuk mencari olahraga atau rekreasi video Amazon Prime, bukan olahraga petualangan di Hutan Hujan Amazon. Tanda kurung membantu menunjukkan bahwa `sports OR recreation` harus dibaca sebelum menggabungkan dengan 'amazon', yang dibaca sebelumnya. `NOT rainforest` Kueri tidak boleh dibaca sebagai`amazon AND (sports OR (recreation NOT rainforest))`.

Rentang

Anda dapat menggunakan berbagai nilai untuk memfilter hasil pencarian. Anda menentukan atribut dan nilai rentang. Ini bisa berupa tanggal atau tipe numerik.

Rentang tanggal harus dalam format berikut:

- Zaman
- YYYY
- YYYY-mm
- YYYY-MM-DD
- YYYY-MM-DD't'hh

Anda juga dapat menentukan apakah akan menyertakan atau mengecualikan nilai rentang yang lebih rendah dan lebih tinggi.

Berikut ini adalah contoh penggunaan operator jangkauan.

`_processed_date:>2019-12-31 AND _processed_date:<2021-01-01`

Mengembalikan dokumen yang diproses pada 2020 — lebih dari 31 Desember 2019 dan kurang dari 1 Januari 2021.

`_processed_date:>=2020-01-01 AND _processed_date:<=2020-12-31`

Mengembalikan dokumen yang diproses pada 2020 — lebih besar dari atau sama dengan 1 Januari 2020 dan kurang dari atau sama dengan 31 Desember 2020.

`_document_likes:<1`

Mengembalikan dokumen dengan nol suka atau tidak ada umpan balik pengguna—kurang dari 1 suka.

Anda dapat menentukan apakah rentang harus diperlakukan sebagai inklusif atau eksklusif dari nilai rentang yang diberikan.

Inklusif

`_last_updated_at:[2020-01-01 TO 2020-12-31]`

Dokumen pengembalian terakhir diperbarui pada 2020 — termasuk hari-hari 1 Desember 2020 dan 31 Desember 2020.

Eksklusif

`_last_updated_at:{2019-12-31 TO 2021-01-01}`

Mengembalikan dokumen terakhir diperbarui pada tahun 2020—tidak termasuk hari-hari 31 Desember 2019 dan 1 Januari 2021.

< and **>**Untuk rentang tak terbatas yang tidak inklusif atau eksklusif, cukup gunakan operator. Misalnya, `_last_updated_at:>2019-12-31 AND _last_updated_at:<2021-01-01`

Bidang

Anda dapat membatasi pencarian Anda hanya untuk mengembalikan dokumen yang memenuhi nilai di bidang tertentu. Bidang bisa dari jenis apa saja.

Berikut ini adalah contoh penggunaan operator konteks tingkat lapangan.

`status:"Incomplete" AND financial_year:2021`

Mengembalikan dokumen untuk tahun buku 2021 dengan statusnya sebagai tidak lengkap.

`(sports OR recreation) AND country:"United States" AND level:"professional"`

Mengembalikan dokumen yang membahas olahraga profesional atau rekreasi di Amerika Serikat.

Wildcard

Anda dapat memperluas pencarian Anda untuk memperhitungkan varian kata dan frasa menggunakan operator wildcard. Ini berguna saat mencari varian nama. Amazon Kendra saat ini

hanya mendukung wildcard trailing. Jumlah karakter awalan untuk wildcard trailing harus lebih besar dari dua.

Berikut ini adalah contoh penggunaan operator wildcard.

`Cloud*`

Mengembalikan dokumen yang berisi varian seperti CloudFormation dan CloudWatch.

`kendra*aws`

Mengembalikan dokumen yang berisi varian seperti kendra.amazonaws.

`kendra*aws*`

Mengembalikan dokumen yang berisi varian seperti kendra.amazonaws.com

Kutipan yang tepat

Anda dapat menggunakan tanda kutip untuk mencari kecocokan persis dari sepotong teks.

Berikut ini adalah contoh penggunaan tanda kutip.

`"Amazon Kendra" "pricing"`

Mengembalikan dokumen yang berisi frasa 'Amazon Kendra' dan istilah 'harga'. Dokumen harus berisi Amazon Kendra'' dan 'harga' untuk mengembalikan hasil.

`"Amazon Kendra" "pricing" cost`

Mengembalikan dokumen yang berisi frasa 'Amazon Kendra' dan istilah 'harga', dan opsional istilah 'biaya'. Dokumen harus berisi 'Amazon Kendra' dan 'harga' untuk mengembalikan hasil, tetapi mungkin tidak termasuk 'biaya'.

Sintaks kueri tidak valid

Amazon Kendra mengeluarkan peringatan jika ada masalah dengan sintaks kueri Anda atau kueri Anda saat ini tidak didukung oleh Amazon Kendra. Untuk informasi selengkapnya, lihat dokumentasi API untuk peringatan kueri.

Kueri berikut adalah contoh sintaks kueri yang tidak valid.

`_last_updated_at:<2021-12-32`

Tanggal tidak valid. Hari ke-32 tidak ada dalam kalender Gregorian, yang digunakan oleh. Amazon Kendra

`_view_count:ten`

Nilai numerik tidak valid. Digit harus digunakan untuk mewakili nilai numerik.

`nonExistentField:123`

Pencarian bidang tidak valid. Bidang harus ada untuk menggunakan pencarian lapangan.

`Product:[A TO D]`

Rentang tidak valid. Nilai numerik atau tanggal harus digunakan untuk rentang.

`OR Hello`

Boolean tidak valid. Operator harus digunakan dengan persyaratan dan ditempatkan di antara persyaratan.

Mencari dalam bahasa

Anda dapat mencari dokumen dalam bahasa yang didukung. Anda meneruskan kode bahasa AttributeFilteruntuk mengembalikan dokumen yang difilter dalam bahasa pilihan Anda. Anda dapat mengetik kueri dalam bahasa yang didukung.

Jika Anda tidak menentukan bahasa, Amazon Kendra kueri dokumen dalam bahasa Inggris secara default. Untuk informasi selengkapnya tentang bahasa yang didukung, termasuk kodenya, lihat Menambahkan dokumen dalam bahasa selain bahasa Inggris.

Untuk mencari dokumen dalam bahasa yang didukung di konsol, pilih indeks Anda, lalu pilih opsi untuk mencari indeks Anda dari menu navigasi. Pilih bahasa yang ingin Anda kembalikan dokumen dengan memilih pengaturan pencarian dan kemudian memilih bahasa dari Bahasa dropdown.

Contoh berikut menunjukkan cara mencari dokumen dalam bahasa Spanyol.

Untuk mencari indeks dalam bahasa Spanyol di konsol

1. Masuk ke AWS Management Console dan buka Amazon Kendra konsol di http://console.aws.amazon.com/kendra/.
2. Di menu navigasi, pilih Indeks dan pilih indeks Anda.
3. Di menu navigasi, pilih opsi untuk mencari indeks Anda.

4. Di pengaturan pencarian, pilih dropdown Bahasa dan pilih Spanyol.
5. Masukkan kueri ke dalam kotak teks dan kemudian tekan enter.
6. Amazon Kendra mengembalikan hasil pencarian dalam bahasa Spanyol.

Untuk mencari indeks dalam bahasa Spanyol menggunakan CLI, Python atau Java

- Contoh berikut mencari indeks dalam bahasa Spanyol. Ubah nilai `searchString` ke kueri penelusuran Anda dan nilai `indexID` ke pengenal indeks yang ingin Anda cari. Kode bahasa untuk bahasa Spanyol adalah`es`. Anda dapat menggantinya dengan kode bahasa Anda sendiri.

  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");
```

```
        }
    }
}
```

Mengambil bagian

Anda dapat menggunakan RetrieveAPI sebagai retriever untuk sistem retrieval augmented generation (RAG).

Sistem RAG menggunakan kecerdasan buatan generatif untuk membangun aplikasi penjawab pertanyaan. Sistem RAG terdiri dari retriever dan large language models (LLM). Diberikan kueri, retriever mengidentifikasi potongan teks yang paling relevan dari kumpulan dokumen dan memasukkannya ke LLM untuk memberikan jawaban yang paling berguna. Kemudian, LLM menganalisis potongan atau bagian teks yang relevan dan menghasilkan respons komprehensif untuk kueri.

`Retrieve`API melihat potongan teks atau kutipan yang disebut sebagai bagian dan mengembalikan bagian atas yang paling relevan dengan kueri.

Seperti QueryAPI, `Retrieve` API juga mencari informasi yang relevan menggunakan pencarian semantik. Pencarian semantik memperhitungkan konteks permintaan pencarian, ditambah semua informasi yang tersedia dari dokumen yang diindeks. Namun, secara default, `Query` API hanya mengembalikan bagian kutipan hingga 100 kata token. Dengan `Retrieve` API, Anda dapat mengambil bagian yang lebih panjang hingga 200 kata token dan hingga 100 bagian yang relevan secara semantik. Ini tidak termasuk respons tipe tanya jawab atau FAQ dari indeks Anda. Bagian-bagian tersebut adalah kutipan teks yang dapat diekstraksi secara semantik dari beberapa dokumen dan beberapa bagian dari dokumen yang sama. Jika dalam kasus ekstrim dokumen Anda menghasilkan nol bagian menggunakan `Retrieve` API, Anda dapat menggunakan `Query` API dan jenis responsnya.

Anda juga dapat melakukan hal berikut dengan `Retrieve` API:

- Mengesampingkan peningkatan pada tingkat indeks
- Filter berdasarkan bidang atau atribut dokumen
- Filter berdasarkan akses pengguna atau grup mereka ke dokumen
- Lihat ember skor kepercayaan untuk hasil bagian yang diambil. Ember kepercayaan memberikan peringkat relatif yang menunjukkan seberapa yakin Amazon Kendra bahwa respons tersebut relevan dengan kueri.

> **Note**
>
> Bucket skor kepercayaan saat ini hanya tersedia untuk bahasa Inggris.

Anda juga dapat menyertakan bidang tertentu dalam respons yang mungkin memberikan informasi tambahan yang berguna.

`Retrieve`API saat ini tidak mendukung semua fitur yang didukung oleh `Query` API. Fitur berikut tidak didukung: kueri menggunakan sintaks kueri lanjutan, koreksi ejaan yang disarankan untuk kueri, faset, saran kueri untuk melengkapi kueri penelusuran secara otomatis, dan pembelajaran inkremental. Perhatikan bahwa tidak semua fitur berlaku untuk `Retrieve` API. Setiap rilis `Retrieve` API di masa mendatang akan didokumentasikan dalam panduan ini.

`Retrieve`API membagikan jumlah unit kapasitas kueri yang Anda tetapkan untuk indeks Anda. Untuk informasi selengkapnya tentang apa yang disertakan dalam unit kapasitas tunggal dan kapasitas dasar default untuk indeks, lihat Menyesuaikan kapasitas.

> **Note**
>
> Anda tidak dapat menambahkan kapasitas jika Anda menggunakan Edisi Amazon Kendra Pengembang; Anda hanya dapat menambahkan kapasitas saat menggunakan Amazon Kendra Enterprise Edition. Untuk informasi selengkapnya tentang apa yang disertakan dalam Edisi Pengembang dan Perusahaan, lihat Amazon Kendra Edisi.

Berikut ini adalah contoh penggunaan `Retrieve` API untuk mengambil 100 bagian paling relevan dari dokumen dalam indeks untuk kueri "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");
        }
    }
}
```

Menjelajahi indeks

Anda dapat menelusuri dokumen berdasarkan atribut atau aspeknya tanpa harus mengetik kueri penelusuran. Amazon Kendra Index Browse dapat membantu pengguna menemukan dokumen dengan menjelajahi indeks secara bebas tanpa mempertimbangkan kueri tertentu. Ini juga membantu pengguna Anda menelusuri indeks secara luas sebagai titik awal dalam pencarian mereka.

Index Browse hanya dapat digunakan untuk mencari berdasarkan atribut dokumen atau aspek dengan jenis pengurutan. Anda tidak dapat mencari seluruh indeks menggunakan Index Browse. Jika teks kueri hilang, maka Amazon Kendra minta filter atribut dokumen atau faset, dan jenis pengurutan.

Untuk mengizinkan penelusuran indeks menggunakan Query API, Anda harus menyertakan AttributeFilteratau Facet, dan SortingConfiguration. Untuk mengizinkan penjelajahan indeks di konsol, pilih indeks Anda di bawah Indeks di menu navigasi, lalu pilih opsi untuk mencari indeks Anda. Di kotak pencarian, tekan tombol Enter dua kali. Pilih dropdown Filter hasil pencarian untuk memilih filter dan pilih dropdown Urutkan untuk memilih jenis penyortiran.

Berikut ini adalah contoh penelusuran indeks untuk dokumen dalam bahasa Spanyol dalam urutan tanggal pembuatan dokumen yang menurun.

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())
            .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");
        }
    }
}
```

Menampilkan hasil pencarian

Anda dapat menampilkan dokumen tertentu di hasil penelusuran saat pengguna mengeluarkan kueri tertentu. Ini membantu membuat hasil lebih terlihat dan menonjol bagi pengguna Anda. Hasil unggulan dipisahkan dari daftar hasil yang biasa, dan ditampilkan di bagian atas halaman pencarian. Anda dapat bereksperimen dengan menampilkan dokumen yang berbeda untuk pertanyaan yang berbeda, atau memastikan dokumen tertentu mendapatkan visibilitas yang layak mereka dapatkan.

Anda memetakan kueri tertentu ke dokumen tertentu untuk ditampilkan dalam hasil. Jika kueri berisi kecocokan persis, maka satu atau lebih dokumen spesifik ditampilkan dalam hasil pencarian.

Misalnya, Anda dapat menentukan bahwa jika pengguna Anda mengeluarkan kueri 'produk baru 2023', lalu pilih dokumen berjudul 'Apa yang baru' dan 'Segera hadir' untuk ditampilkan di bagian

atas halaman hasil pencarian. Ini membantu memastikan dokumen-dokumen tentang produk baru ini mendapatkan visibilitas yang layak mereka dapatkan.

Amazon Kendra tidak menduplikasi hasil pencarian jika hasil sudah dipilih untuk ditampilkan di bagian atas halaman hasil pencarian. Hasil unggulan tidak lagi diberi peringkat sebagai hasil pertama jika sudah ditampilkan di atas semua hasil lainnya.

Untuk menampilkan hasil tertentu, Anda harus menentukan kecocokan persis dari kueri teks lengkap, bukan kecocokan sebagian kueri menggunakan kata kunci atau frasa yang terkandung dalam kueri. Misalnya, jika Anda hanya menentukan kueri 'Kendra' dalam kumpulan hasil unggulan, kueri seperti 'Bagaimana Kendra memberi peringkat hasil secara semantik? ' tidak akan membuat hasil yang ditampilkan. Hasil unggulan dirancang untuk kueri tertentu, bukan kueri yang cakupannya terlalu luas. Amazon Kendra secara alami menangani kueri jenis kata kunci untuk memberi peringkat dokumen yang paling berguna dalam hasil pencarian, menghindari fitur hasil yang berlebihan berdasarkan kata kunci sederhana.

Jika ada kueri tertentu yang sering digunakan pengguna Anda, maka Anda dapat menentukan kueri ini untuk hasil unggulan. Misalnya, jika Anda melihat kueri teratas Anda menggunakan Amazon Kendra Analytics dan menemukan kueri spesifik itu, seperti 'Bagaimana hasil peringkat kendra secara semantik? ' dan 'pencarian semantik kendra', sering digunakan, maka kueri ini mungkin berguna untuk menentukan untuk menampilkan dokumen berjudul 'pencarian 101'.Amazon Kendra

Amazon Kendra memperlakukan kueri untuk hasil unggulan sebagai tidak peka huruf besar/kecil. Amazon Kendra mengonversi kueri ke huruf kecil, dan menggantikan karakter spasi putih dengan satu spasi. Amazon Kendra mencocokkan semua karakter lain sebagaimana adanya ketika Anda menentukan kueri untuk hasil unggulan.

Anda membuat serangkaian hasil unggulan yang dipetakan ke kueri tertentu menggunakan CreateFeaturedResultsSetAPI. Jika Anda menggunakan konsol, pilih indeks, lalu pilih Hasil unggulan di menu navigasi untuk membuat set hasil unggulan. Anda dapat membuat hingga 50 set hasil unggulan per indeks, hingga empat dokumen yang akan ditampilkan per set, dan hingga 49 teks kueri per set hasil unggulan. Anda dapat meminta untuk meningkatkan batas ini dengan menghubungi Support.

Anda dapat memilih dokumen yang sama di beberapa set hasil unggulan. Namun, Anda tidak boleh menggunakan teks kueri pencocokan persis yang sama di beberapa set. Kueri yang Anda tentukan untuk hasil unggulan harus unik per hasil fitur yang ditetapkan untuk setiap indeks.

Anda dapat mengatur urutan dokumen saat memilih hingga empat dokumen unggulan. Jika Anda menggunakan API, urutan daftar dokumen unggulan sama dengan yang ditampilkan dalam hasil

unggulan. Jika Anda menggunakan konsol, Anda cukup menyeret dan melepas urutan dokumen saat Anda memilih dokumen untuk ditampilkan dalam hasil.

Kontrol akses, di mana pengguna dan grup tertentu memiliki akses ke dokumen tertentu dan yang lainnya tidak, masih dihormati saat mengonfigurasi hasil unggulan. Itu juga berlaku untuk pemfilteran konteks pengguna. Misalnya, pengguna A termasuk dalam grup perusahaan 'Interns', yang seharusnya tidak mengakses dokumen rahasia perusahaan. Jika pengguna A memasukkan kueri yang menampilkan dokumen rahasia perusahaan, pengguna A tidak melihat dokumen ini ditampilkan dalam hasil mereka. Itu juga berlaku untuk hasil lain di halaman hasil pencarian. Anda juga dapat menggunakan tag untuk mengontrol akses ke set hasil unggulan, yang merupakan Amazon Kendra sumber daya yang Anda kendalikan aksesnya.

Berikut ini adalah contoh pembuatan serangkaian hasil unggulan dengan kueri “produk baru 2023", “produk baru tersedia” yang dipetakan ke dokumen berjudul “Apa yang baru” (doc-id-1) dan “Segera hadir” (doc-id-2).

CLI

```
aws kendra create-featured-results-set \
 --featured-results-set-name 'New product docs to feature' \
 --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 decription 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,
        Decription = 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.")
```

Pencarian tabel untuk HTML

Amazon Kendra fitur pencarian tabular dapat mencari dan mengekstrak jawaban dari tabel yang disematkan dalam dokumen HTML. Saat Anda mencari indeks Anda, Amazon Kendra sertakan kutipan dari tabel jika relevan dengan kueri dan berikan informasi yang berguna.

Amazon Kendra melihat semua informasi dalam teks isi dokumen, termasuk informasi yang berguna dalam tabel. Misalnya, indeks berisi laporan bisnis dengan tabel tentang biaya operasi, pendapatan, dan informasi keuangan lainnya. Untuk pertanyaan, “berapa biaya operasi tahunan dari 2020-2022?” , Amazon Kendra dapat mengembalikan kutipan dari tabel yang berisi kolom tabel yang

relevan “Operasi (jutaan USD)” dan “Tahun keuangan”, dan baris tabel yang berisi nilai pendapatan untuk tahun 2020, 2021, dan 2022. Kutipan tabel disertakan dalam hasil, bersama dengan judul dokumen, tautan ke dokumen lengkap, dan bidang dokumen lain yang Anda pilih untuk disertakan.

Kutipan tabel dapat ditampilkan dalam hasil pencarian apakah informasi tersebut ditemukan dalam satu sel tabel atau beberapa sel. Misalnya, Amazon Kendra dapat menampilkan kutipan tabel disesuaikan untuk masing-masing jenis query:

- “kartu kredit suku bunga tertinggi pada tahun 2020"
- “kartu kredit suku bunga tertinggi dari 2020-2022"
- “3 kartu kredit suku bunga tertinggi di 2020-2022"
- “kartu kredit dengan suku bunga kurang dari 10%”
- “Semua kartu kredit bunga rendah yang tersedia”

Amazon Kendra menyoroti sel tabel atau sel yang paling relevan dengan kueri. Sel yang paling relevan dengan baris, kolom, dan nama kolom yang sesuai ditampilkan di hasil pencarian. Kutipan tabel menampilkan hingga lima kolom dan tiga baris, tergantung pada berapa banyak sel tabel yang relevan dengan kueri dan berapa banyak kolom yang tersedia di tabel asli. Sel paling relevan teratas ditampilkan dalam kutipan tabel, bersama dengan sel paling relevan berikutnya.

Responsnya mencakup keranjang kepercayaan (`MEDIUMHIGH,,VERY_HIGH`) untuk menunjukkan seberapa relevan jawaban tabel dengan kueri. Jika nilai sel tabel `VERY_HIGH` dalam kepercayaan diri, maka itu menjadi 'jawaban teratas' dan disorot. Untuk nilai sel tabel yang percaya `HIGH` diri, maka mereka disorot. Untuk nilai sel tabel yang percaya `MEDIUM` diri, maka mereka tidak disorot. Keyakinan keseluruhan untuk jawaban tabel dikembalikan dalam respons. Misalnya, jika tabel berisi sebagian besar sel tabel dengan `HIGH` keyakinan, maka kepercayaan keseluruhan yang dikembalikan dalam respons untuk jawaban tabel adalah `HIGH` kepercayaan diri.

Secara default, tabel tidak diberi tingkat kepentingan yang lebih tinggi atau lebih berat daripada komponen dokumen lainnya. Dalam dokumen, jika tabel hanya sedikit relevan dengan kueri, tetapi ada paragraf yang sangat relevan, Amazon Kendra mengembalikan kutipan paragraf. Hasil pencarian menampilkan bagian konten yang memberikan jawaban terbaik dan informasi yang paling berguna, dalam dokumen yang sama atau dokumen lain. Jika kepercayaan untuk tabel jatuh di bawah `MEDIUM` kepercayaan, maka kutipan tabel tidak dikembalikan dalam respons.

Untuk menggunakan pencarian tabular pada indeks yang ada, Anda harus mengindeks ulang konten Anda.

Amazon Kendra pencarian tabular mendukung sinonim (termasuk sinonim khusus). Amazon Kendra hanya mendukung dokumen dalam bahasa Inggris dengan tabel HTML yang berada dalam tag tabel.

Contoh berikut menunjukkan kutipan tabel termasuk dalam hasil query. Untuk melihat contoh JSON dengan respons kueri, termasuk kutipan tabel, lihat Tanggapan dan jenis kueri.

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");
        }
    }
}
```

Saran kueri

Amazon Kendra Saran kueri dapat membantu pengguna Anda mengetik kueri penelusuran mereka lebih cepat dan memandu pencarian mereka.

Amazon Kendra menyarankan kueri yang relevan dengan pengguna Anda berdasarkan salah satu dari berikut ini:

- Kueri populer dalam riwayat kueri atau log kueri

- Isi bidang dokumen/atribut

Anda dapat mengatur preferensi Anda untuk menggunakan riwayat kueri atau bidang dokumen dengan menetapkan `SuggestionTypes` sebagai salah satu `QUERY` atau `DOCUMENT_ATTRIBUTES` dan panggilan GetQuerySuggestions. Secara default, Amazon Kendra menggunakan riwayat kueri untuk mendasarkan saran. Jika riwayat kueri dan bidang dokumen diaktifkan saat Anda memanggil UpdateQuerySuggestionsConfigdan Anda belum menyetel `SuggestionTypes` preferensi Anda untuk menggunakan bidang dokumen, maka Amazon Kendra gunakan riwayat kueri.

Jika Anda menggunakan konsol, Anda dapat mendasarkan saran kueri pada riwayat kueri atau bidang dokumen. Pertama-tama Anda memilih indeks Anda dan kemudian pilih Saran kueri di bawah Pengayaan di menu navigasi. Kemudian pilih Konfigurasikan saran kueri. Setelah mengonfigurasi saran kueri, Anda akan diarahkan ke konsol pencarian tempat Anda dapat memilih bidang Riwayat kueri atau Dokumen di panel kanan dan memasukkan kueri penelusuran di bilah pencarian.

Secara default, saran kueri menggunakan riwayat kueri dan bidang dokumen keduanya diaktifkan tanpa biaya tambahan. Anda dapat menonaktifkan jenis saran kueri ini kapan saja dengan menggunakan `UpdateQuerySuggestionsConfig` API. Untuk menonaktifkan saran kueri berdasarkan riwayat kueri, setel `Mode` ke `DISABLED` saat memanggil`UpdateQuerySuggestionsConfig`. Untuk menonaktifkan saran kueri berdasarkan bidang dokumen, atur `AttributeSuggestionsMode` ke `INACTIVE` dalam konfigurasi bidang dokumen dan kemudian panggil`UpdateQuerySuggestionsConfig>`. Jika Anda menggunakan konsol, Anda dapat menonaktifkan saran kueri di pengaturan Saran kueri.

Saran kueri tidak peka huruf besar/kecil. Amazon Kendra mengonversi awalan kueri dan kueri yang disarankan menjadi huruf kecil, mengabaikan semua tanda kutip tunggal dan ganda, dan mengganti beberapa karakter spasi putih dengan satu spasi. Amazon Kendra cocok dengan semua karakter khusus lainnya sebagaimana adanya. Amazon Kendra tidak menunjukkan saran jika pengguna mengetik kurang dari dua karakter atau lebih dari 60 karakter.

Topik

- Saran kueri menggunakan riwayat kueri
- Saran kueri menggunakan bidang dokumen
- Blokir kueri tertentu atau konten bidang dokumen dari saran

Saran kueri menggunakan riwayat kueri

Topik

Anda dapat memilih untuk menyarankan kueri yang relevan dengan pengguna Anda berdasarkan kueri populer dalam riwayat kueri atau log kueri. Amazon Kendra menggunakan semua kueri yang dicari dan dipelajari pengguna Anda dari kueri ini untuk memberikan saran kepada pengguna Anda. Amazon Kendra menyarankan kueri populer kepada pengguna saat mereka mulai mengetik kueri mereka. Amazon Kendra menyarankan kueri jika awalan atau beberapa karakter pertama dari kueri cocok dengan apa yang mulai diketik pengguna sebagai kueri mereka.

Misalnya, pengguna mulai mengetik kueri 'acara yang akan datang'. Amazon Kendra telah belajar dari riwayat kueri bahwa banyak pengguna telah mencari 'acara mendatang 2050' berkali-kali. Pengguna melihat 'acara mendatang 2050' muncul tepat di bawah bilah pencarian mereka, melengkapi permintaan pencarian mereka secara otomatis. Pengguna memilih saran kueri ini, dan dokumen 'Peristiwa baru: Apa yang terjadi di 2050' dikembalikan dalam hasil pencarian.

Anda dapat menentukan cara Amazon Kendra memilih kueri yang memenuhi syarat untuk disarankan kepada pengguna Anda. Misalnya, Anda dapat menentukan bahwa saran kueri harus dicari oleh setidaknya 10 pengguna unik (default adalah tiga), telah dicari dalam 30 hari terakhir, dan tidak mengandung kata atau frasa dari daftar blokir Anda. Amazon Kendra mensyaratkan bahwa kueri memiliki setidaknya satu hasil pencarian dan berisi setidaknya satu kata lebih dari empat karakter.

Pengaturan untuk memilih kueri untuk saran

Anda dapat mengonfigurasi pengaturan berikut untuk memilih kueri saran dengan menggunakan UpdateQuerySuggestionsConfigAPI:

- Mode —Saran kueri menggunakan riwayat kueri adalah salah satu `ENABLED` atau`LEARN_ONLY`. Amazon Kendra mengaktifkan saran kueri secara default. `LEARN_ONLY`mematikan saran kueri. Jika dimatikan, Amazon Kendra terus pelajari saran tetapi tidak membuat saran kueri kepada pengguna.

- Jendela waktu log kueri —Seberapa terbaru kueri Anda di jendela waktu log kueri Anda. Rentang waktu adalah jumlah hari dari hari ini hingga hari sebelumnya.
- Kueri tanpa informasi pengguna —Setel `TRUE` untuk menyertakan semua kueri, atau setel `FALSE` ke hanya menyertakan kueri dengan informasi pengguna. Anda dapat menggunakan setelan ini jika aplikasi penelusuran menyertakan informasi pengguna, seperti ID pengguna, saat pengguna mengeluarkan kueri. Secara default, setelan ini tidak memfilter kueri jika tidak ada informasi pengguna tertentu yang terkait dengan kueri. Namun, Anda dapat menggunakan pengaturan ini untuk hanya membuat saran berdasarkan kueri yang menyertakan informasi pengguna.
- Pengguna unik — Jumlah minimum pengguna unik yang harus mencari kueri agar memenuhi syarat untuk menyarankan kepada pengguna Anda. Jumlah ini adalah nilai integer.
- Jumlah kueri —Jumlah minimum kali kueri harus dicari agar kueri memenuhi syarat untuk disarankan kepada pengguna Anda. Jumlah ini adalah nilai integer.

Setelan ini memengaruhi cara kueri dipilih sebagai kueri populer untuk disarankan kepada pengguna Anda. Bagaimana Anda menyetel pengaturan Anda akan bergantung pada kebutuhan spesifik Anda, misalnya:

- Jika pengguna Anda biasanya mencari rata-rata sebulan sekali, maka Anda dapat mengatur jumlah hari di jendela waktu log kueri menjadi 30 hari. Dengan menggunakan pengaturan itu, Anda menangkap sebagian besar kueri terbaru pengguna Anda sebelum menjadi usang di jendela waktu.
- Jika hanya sejumlah kecil kueri Anda yang menyertakan informasi pengguna, dan Anda tidak ingin menyarankan kueri berdasarkan ukuran sampel yang kecil, maka Anda dapat mengatur kueri untuk menyertakan semua pengguna.
- Jika Anda menentukan kueri populer sebagai sedang dicari oleh setidaknya 10 pengguna unik dan mencari setidaknya 100 kali, maka Anda setel pengguna unik menjadi 10 dan jumlah permintaan menjadi 100.

> **Warning**
>
> Perubahan pengaturan Anda mungkin tidak segera berlaku. Anda dapat melacak perubahan pengaturan dengan menggunakan DescribeQuerySuggestionsConfigAPI. Waktu untuk pengaturan yang diperbarui diterapkan tergantung pada pembaruan yang Anda buat dan jumlah kueri penelusuran dalam indeks Anda. Amazon Kendra secara otomatis memperbarui

saran setiap 24 jam, setelah Anda mengubah pengaturan atau setelah Anda menerapkan daftar blokir.

CLI

Untuk mengambil saran kueri

```
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
```

Untuk memperbarui saran kueri

Misalnya, untuk mengubah jendela waktu log kueri dan berapa kali kueri harus dicari:

```
aws kendra update-query-suggestions-config \
 --index-id index-id \
 --query-log-look-back-window-in-days 30 \
 --minimum-query-count 100
```

Python

Untuk mengambil saran kueri

```
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.")
```

Untuk memperbarui saran kueri

Misalnya, untuk mengubah jendela waktu log kueri dan berapa kali kueri harus dicari:

```
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.")
```

Hapus saran sambil mempertahankan riwayat kueri

Anda dapat menghapus saran kueri dengan menggunakan ClearQuerySuggestionsAPI. Menghapus saran hanya menghapus saran kueri yang ada, bukan kueri dalam riwayat kueri. Saat Anda menghapus saran, Amazon Kendra pelajari saran baru berdasarkan kueri baru yang ditambahkan ke log kueri sejak Anda menghapus saran.

CLI

Untuk menghapus saran kueri

```
aws  kendra clear-query-suggestions \
 --index-id index-id
```

Python

Untuk menghapus saran kueri

```
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.")
```

Saran tidak tersedia

Jika Anda tidak melihat saran untuk kueri, itu bisa karena salah satu alasan berikut:

- Tidak ada cukup kueri dalam indeks Anda Amazon Kendra untuk dipelajari.
- Pengaturan saran kueri Anda terlalu ketat, sehingga sebagian besar kueri disaring dari saran.
- Anda baru-baru ini menghapus saran, dan Amazon Kendra masih membutuhkan waktu untuk mengumpulkan kueri baru untuk mempelajari saran baru.

Anda dapat memeriksa pengaturan Anda saat ini menggunakan DescribeQuerySuggestionsConfigAPI.

Saran kueri menggunakan bidang dokumen

Topik

- Pengaturan untuk memilih bidang untuk saran
- Kontrol pengguna di bidang dokumen

Anda dapat memilih untuk menyarankan kueri yang relevan dengan pengguna Anda berdasarkan isi bidang dokumen. Alih-alih menggunakan riwayat kueri untuk menyarankan kueri relevan populer lainnya, Anda dapat menggunakan informasi yang terkandung dalam bidang dokumen yang berguna untuk melengkapi kueri secara otomatis. Amazon Kendra mencari konten yang relevan di bidang yang disetel ke `Suggestable` dan yang selaras dengan kueri pengguna Anda. Kemudian, Amazon Kendra sarankan konten ini kepada pengguna Anda ketika mereka mulai mengetik kueri mereka.

Misalnya, jika Anda menentukan bidang judul untuk mendasarkan saran dan pengguna mulai mengetik kueri 'Bagaimana amazon ken... ', judul yang paling relevan 'Cara Amazon Kendra kerja' dapat disarankan untuk melengkapi pencarian secara otomatis. Pengguna melihat 'Cara Amazon Kendra kerja' muncul langsung di bawah bilah pencarian mereka, melengkapi permintaan pencarian mereka secara otomatis. Pengguna memilih saran kueri ini, dan dokumen 'Cara Amazon Kendra kerja' dikembalikan dalam hasil pencarian.

Anda dapat menggunakan isi bidang `String` dan `StringList` jenis dokumen apa pun untuk menyarankan kueri dengan menyetel bidang `Suggestable` sebagai bagian dari konfigurasi bidang Anda untuk saran kueri. Anda juga dapat menggunakan daftar blokir sehingga bidang dokumen yang disarankan yang berisi kata atau frasa tertentu tidak ditampilkan kepada pengguna Anda. Anda dapat menggunakan satu daftar blok. Daftar blokir berlaku apakah Anda menetapkan saran kueri untuk menggunakan riwayat kueri atau bidang dokumen.

Pengaturan untuk memilih bidang untuk saran

Anda dapat mengonfigurasi pengaturan berikut untuk memilih bidang dokumen untuk saran menggunakan AttributeSuggestionsConfigdan memanggil UpdateQuerySuggestionsConfigAPI untuk memperbarui pengaturan di tingkat indeks:

- Mode saran bidang/atribut —Saran kueri menggunakan bidang dokumen adalah salah satu atau. `ACTIVE` `INACTIVE` Amazon Kendra mengaktifkan saran kueri secara default.

- Bidang/atribut yang dapat disarankan —Nama bidang atau kunci bidang untuk mendasarkan saran. Bidang ini harus diatur TRUE untuk`Suggestable`, sebagai bagian dari konfigurasi bidang. Anda dapat mengganti konfigurasi bidang pada tingkat kueri sambil mempertahankan konfigurasi di tingkat indeks. Gunakan GetQuerySuggestionsAPI untuk mengubah `AttributeSuggestionConfig` pada tingkat kueri. Konfigurasi ini pada tingkat kueri dapat berguna untuk bereksperimen dengan cepat menggunakan bidang dokumen yang berbeda tanpa harus memperbarui konfigurasi di tingkat indeks.
- Bidang/atribut tambahan —Bidang tambahan yang ingin Anda sertakan dalam respons untuk saran kueri. Bidang ini digunakan untuk memberikan informasi tambahan dalam tanggapan; Namun, mereka tidak digunakan untuk mendasarkan saran.

> **Warning**
>
> Perubahan pengaturan Anda mungkin tidak segera berlaku. Anda dapat melacak perubahan pengaturan dengan menggunakan DescribeQuerySuggestionsConfigAPI. Waktu untuk pengaturan yang diperbarui diterapkan tergantung pada pembaruan yang Anda buat. Amazon Kendra secara otomatis memperbarui saran setiap 24 jam, setelah Anda mengubah pengaturan atau setelah Anda menerapkan daftar blokir.

CLI

Untuk mengambil saran kueri dan mengganti konfigurasi bidang dokumen pada tingkat kueri alih-alih harus mengubah konfigurasi di tingkat indeks.

```
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
```

Untuk memperbarui saran kueri

Misalnya, untuk mengubah konfigurasi bidang dokumen di tingkat indeks:

```
aws kendra update-query-suggestions-config \
```

```
 --index-id index-id \
 --attribute-suggestions-config '{"SuggestableConfigList": '[{"SuggestableConfig":
 "_document_title", "Suggestable": true}]', "AttributeSuggestionsMode": "ACTIVE"}'
```

Python

Untuk mengambil saran kueri dan mengganti konfigurasi bidang dokumen pada tingkat kueri alih-alih harus mengubah konfigurasi di tingkat indeks.

```
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.")
```

Untuk memperbarui saran kueri

Misalnya, untuk mengubah konfigurasi bidang dokumen di tingkat indeks:

```
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.")
```

Kontrol pengguna di bidang dokumen

Anda dapat menerapkan pemfilteran konteks pengguna ke bidang dokumen yang ingin menjadi dasar saran kueri. Ini menyaring informasi bidang dokumen berdasarkan akses pengguna atau grup mereka ke dokumen. Misalnya, seorang magang mencari portal perusahaan dan tidak memiliki akses ke dokumen perusahaan rahasia. Oleh karena itu, kueri yang disarankan berdasarkan judul dokumen rahasia, atau bidang lain yang dapat disarankan, tidak ditampilkan kepada magang.

Anda dapat mengindeks dokumen Anda dengan daftar kontrol akses (ACL), menentukan pengguna dan grup mana yang diberi akses ke dokumen mana. Kemudian, Anda dapat menerapkan pemfilteran konteks pengguna ke bidang dokumen Anda untuk saran kueri. Pemfilteran konteks pengguna yang saat ini disetel untuk indeks Anda adalah pemfilteran konteks pengguna yang sama yang diterapkan pada konfigurasi bidang dokumen Anda untuk saran kueri. Pemfilteran konteks pengguna adalah bagian dari konfigurasi bidang dokumen Anda. Anda menggunakan AttributeSuggestionsGetConfigdan menelepon GetQuerySuggestions.

Blokir kueri tertentu atau konten bidang dokumen dari saran

Daftar blokir berhenti Amazon Kendra menyarankan kueri tertentu kepada pengguna Anda. Daftar blok adalah daftar kata atau frasa yang ingin Anda kecualikan dari saran kueri. Amazon Kendra tidak termasuk kueri yang berisi kecocokan persis kata atau frasa dalam daftar blokir.

Anda dapat menggunakan daftar blokir untuk melindungi terhadap kata-kata atau frasa ofensif yang biasanya muncul di riwayat kueri atau bidang dokumen Anda dan yang Amazon Kendra dapat dipilih sebagai saran. Daftar blokir juga dapat Amazon Kendra mencegah menyarankan kueri yang berisi informasi yang tidak siap untuk dirilis atau diumumkan secara publik. Misalnya, pengguna Anda sering menanyakan tentang rilis produk baru potensial yang akan datang. Namun, Anda tidak ingin menyarankan produk karena Anda belum siap untuk merilisnya. Anda dapat memblokir kueri yang berisi nama produk dan informasi produk dari saran.

Anda dapat membuat daftar blokir untuk kueri dengan menggunakan CreateQuerySuggestionsBlockListAPI. Anda meletakkan setiap blok kata atau frasa pada baris terpisah dalam file teks. Kemudian Anda mengunggah file teks ke bucket Amazon S3 Anda dan memberikan jalur atau lokasi ke file tersebut. Amazon S3 Amazon Kendra saat ini mendukung pembuatan hanya satu daftar blok.

Anda dapat mengganti file teks dari kata dan frasa yang diblokir di Amazon S3 ember Anda. Untuk memperbarui daftar blokir Amazon Kendra, gunakan UpdateQuerySuggestionsBlockListAPI.

Gunakan DescribeQuerySuggestionsBlockListAPI untuk mendapatkan status daftar blokir Anda. `DescribeQuerySuggestionsBlockList`juga dapat memberi Anda informasi berguna lainnya, seperti berikut ini:

- Saat daftar blokir Anda terakhir diperbarui
- Berapa banyak kata atau frasa dalam daftar blok Anda saat ini
- Pesan kesalahan yang berguna saat membuat daftar blokir

Anda juga dapat menggunakan ListQuerySuggestionsBlockListsAPI untuk mendapatkan daftar ringkasan daftar blokir untuk indeks.

Untuk menghapus daftar blokir Anda, gunakan DeleteQuerySuggestionsBlockListAPI.

Pembaruan daftar blokir Anda mungkin tidak segera diberlakukan. Anda dapat melacak pembaruan dengan menggunakan `DescribeQuerySuggestionsBlockList` API.

CLI

Untuk membuat daftar blokir

```
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
```

Untuk memperbarui daftar blokir

```
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
```

Untuk menghapus daftar blokir

```
aws kendra delete-query-suggestions-block-list \
 --index-id index-id \
 --id block-list-id
```

Python

Untuk membuat daftar blokir

```
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.")
```

Untuk memperbarui daftar blokir

```
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.")
```

Untuk menghapus daftar blokir

```
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.")
```

Pemeriksa ejaan kueri

Amazon Kendra Pemeriksa Ejaan menyarankan koreksi ejaan untuk kueri. Ini dapat membantu Anda menjaga kemunculan hasil pencarian nol seminimal mungkin dan mengembalikan hasil yang relevan. Pengguna Anda mungkin tidak menerima hasil penelusuran dari kueri yang salah eja tanpa hasil yang cocok atau tidak ada dokumen yang dikembalikan. Atau, pengguna Anda mungkin menerima hasil penelusuran yang tidak relevan dari kueri yang salah eja.

Pemeriksa Ejaan dirancang untuk menyarankan koreksi untuk kata-kata yang salah eja berdasarkan kata-kata yang muncul di dokumen Anda yang diindeks dan seberapa dekat kata yang dikoreksi cocok dengan kata yang salah eja. Misalnya, jika kata 'pernyataan' muncul di dokumen Anda yang diindeks, maka ini bisa sangat cocok dengan kata 'statments' yang salah eja dalam kueri 'laporan keuangan akhir tahun'.

Pemeriksa Ejaan mengembalikan kata-kata yang dimaksudkan atau dikoreksi yang menggantikan kata yang salah eja dalam teks kueri asli. Misalnya, 'depoying kendre search' dapat mengembalikan 'menerapkan pencarian Kendra' Anda juga dapat menggunakan lokasi offset yang disediakan di API untuk menyorot atau memiringkan kata-kata koreksi yang dikembalikan dalam kueri di aplikasi front-end Anda. Di konsol, kata-kata yang dikoreksi disorot atau dicetak miring secara default. Misalnya, 'menyebarkan pencarian Kendra'.

Untuk istilah khusus bisnis atau khusus yang muncul dalam dokumen Anda yang diindeks, Pemeriksa Ejaan tidak salah memahami istilah ini sebagai kesalahan ejaan dalam kueri. Misalnya, 'amazon macie' tidak dikoreksi ke 'amazon mace'.

Untuk kata-kata dengan tanda hubung, seperti 'akhir tahun', Pemeriksa Ejaan memperlakukan ini sebagai kata-kata individual untuk menyarankan koreksi untuk kata-kata ini. Misalnya, koreksi yang disarankan untuk 'yaer-end' bisa jadi 'akhir tahun'.

Untuk `DOCUMENT` dan jenis respons `QUESTION_ANSWER` kueri, Pemeriksa Ejaan menyarankan koreksi terhadap kata-kata yang salah eja berdasarkan kata-kata di badan dokumen. Badan dokumen lebih dapat diandalkan daripada judul untuk menyarankan koreksi yang sangat cocok dengan kata-kata yang salah eja. Untuk jenis respons `ANSWER` kueri, Pemeriksa Ejaan menyarankan koreksi berdasarkan kata-kata dalam dokumen tanya jawab default di indeks Anda.

Anda dapat mengaktifkan Pemeriksa Ejaan menggunakan objek. SpellCorrectionConfiguration Anda mengatur `IncludeQuerySpellCheckSuggestions` ke`TRUE`. Pemeriksa Ejaan diaktifkan secara default di konsol. Itu dibangun ke konsol secara default.

Pemeriksa Ejaan juga dapat menyarankan koreksi ejaan untuk kueri dalam berbagai bahasa, tidak hanya bahasa Inggris. Untuk daftar bahasa yang didukung untuk Pemeriksa Ejaan, lihat bahasa yang Amazon Kendra didukung.

Menggunakan pemeriksa ejaan kueri dengan batas default

Pemeriksa Ejaan dirancang dengan default atau batas tertentu. Berikut ini adalah daftar batas saat ini yang berlaku saat Anda mengaktifkan saran koreksi ejaan.

- Koreksi ejaan yang disarankan tidak dapat dikembalikan untuk kata-kata yang panjangnya kurang dari tiga karakter atau lebih dari 30 karakter. Untuk mengizinkan lebih dari 30 karakter atau kurang dari tiga karakter, hubungi Support.
- Koreksi ejaan yang disarankan tidak dapat membatasi saran berdasarkan kontrol akses pengguna atau daftar kontrol akses Anda untuk pemfilteran konteks pengguna. Koreksi ejaan didasarkan pada semua kata dalam dokumen Anda yang diindeks, apakah kata-kata tersebut dibatasi untuk pengguna tertentu atau tidak. Jika Anda ingin menghindari kata-kata tertentu yang muncul dalam koreksi mantra yang disarankan untuk kueri, maka jangan aktifkan. `SpellCorrectionConfiguration`
- Koreksi ejaan yang disarankan tidak dapat dikembalikan untuk kata-kata yang menyertakan angka. Misalnya, 'bagaimana 2 bukan br8k ubun2'.
- Koreksi ejaan yang disarankan tidak dapat menggunakan kata-kata yang tidak muncul di dokumen yang diindeks.
- Koreksi ejaan yang disarankan tidak dapat menggunakan kata-kata yang sering dikunjungi kurang dari 0,01 persen dalam dokumen Anda yang diindeks. Untuk mengubah ambang 0,01%, hubungi Support.

Penyaringan dan pencarian faset

Anda dapat meningkatkan hasil penelusuran atau respons dari Query API dengan menggunakan filter. Filter membatasi dokumen dalam merespons hal-hal yang langsung berlaku untuk kueri. Untuk membuat saran penelusuran segi, gunakan logika Boolean untuk menyaring atribut dokumen tertentu dari respons atau dokumen yang tidak sesuai dengan kriteria tertentu. Anda dapat menentukan aspek menggunakan `Facets` parameter di `Query` API.

Untuk mencari dokumen yang telah Anda indeks Amazon Lex, gunakan Amazon Kendra AMAZON. KendraSearchIntent. Untuk contoh mengonfigurasi Amazon Kendra dengan Amazon Lex, lihat Membuat Bot FAQ untuk Indeks. Amazon Kendra Anda juga dapat

memberikan filter untuk respons dengan menggunakan AttributeFilter. Ini adalah filter kueri di JSON saat mengkonfigurasi`AMAZON.KendraSearchIntent`. Untuk menyediakan filter atribut saat mengonfigurasi maksud penelusuran di konsol, buka editor maksud dan pilih Amazon Kendra kueri untuk menyediakan filter kueri di JSON. Untuk informasi selengkapnya`AMAZON.KendraSearchIntent`, lihat panduan Amazon Lex dokumentasi.

Faset

Faset adalah tampilan terbatas dari serangkaian hasil pencarian. Misalnya, Anda dapat memberikan hasil pencarian untuk kota-kota di seluruh dunia, di mana dokumen difilter oleh kota tertentu yang terkait dengannya. Atau, Anda dapat membuat aspek untuk menampilkan hasil oleh penulis tertentu.

Anda dapat menggunakan atribut dokumen atau bidang metadata yang terkait dengan dokumen sebagai aspek sehingga pengguna Anda dapat mencari berdasarkan kategori atau nilai dalam aspek tersebut. Anda juga dapat menampilkan aspek bersarang di hasil pencarian sehingga pengguna Anda dapat mencari tidak hanya berdasarkan kategori atau bidang tetapi juga berdasarkan sub kategori atau sub bidang.

Contoh berikut menunjukkan cara mendapatkan informasi facet untuk atribut kustom “Kota”.

```
response=kendra.query(
        QueryText = query,
        IndexId = index,
        Facets = [
            {
                "DocumentAttributeKey" : "City"
            }
        ]
        )
```

Anda dapat menggunakan aspek bersarang untuk lebih mempersempit pencarian. Misalnya, atribut dokumen atau aspek “Kota” menyertakan nilai yang disebut “Seattle”. Selain itu, atribut dokumen atau aspek "CityRegion" termasuk nilai “Utara” dan “Selatan” untuk dokumen yang ditugaskan ke “Seattle”. Anda dapat menampilkan aspek bersarang dengan jumlah mereka di hasil pencarian sehingga dokumen dapat dicari tidak hanya berdasarkan kota tetapi juga oleh wilayah dalam kota.

Perhatikan bahwa aspek bersarang dapat memengaruhi latensi kueri. Aturan umum adalah semakin banyak aspek bersarang yang Anda gunakan, semakin besar potensi dampak pada latensi. Faktor lain yang memengaruhi latensi termasuk ukuran rata-rata dokumen yang diindeks, ukuran indeks Anda, kueri yang sangat kompleks, dan beban keseluruhan pada indeks Anda. Amazon Kendra

Contoh berikut menunjukkan cara mendapatkan informasi facet untuk atribut kustom CityRegion "", sebagai aspek bersarang dalam “Kota”.

```
response=kendra.query(
        QueryText = query,
        IndexId = index,
        Facets = [
            {
                "DocumentAttributeKey" : "City",
                "Facets": [
                    {
                        "DocumentAttributeKey" : "CityRegion"
                    }
                ]
            }
        ]
        )
```

Informasi facet, seperti jumlah dokumen, dikembalikan dalam array `FacetResults` respon. Anda menggunakan isi untuk menampilkan saran pencarian berfaset dalam aplikasi Anda. Misalnya, jika atribut dokumen “Kota” berisi kota tempat pencarian dapat diterapkan, gunakan informasi tersebut untuk menampilkan daftar pencarian kota. Pengguna dapat memilih kota untuk memfilter hasil pencarian mereka. Untuk melakukan pencarian faceted, panggil Query API dan gunakan atribut dokumen yang dipilih untuk memfilter hasil.

Anda dapat menampilkan hingga 10 nilai faset per faset untuk kueri, dan hanya satu aspek bersarang dalam satu segi. Jika Anda ingin meningkatkan batas ini, hubungi Support. Jika Anda ingin membatasi jumlah nilai faset per faset menjadi kurang dari 10, Anda dapat menentukan ini di `Facet` objek.

Contoh respons JSON berikut menunjukkan aspek yang dicakup ke atribut dokumen “Kota”. Tanggapan tersebut mencakup jumlah dokumen untuk nilai faset.

```
{
    'FacetResults': [
        {
            'DocumentAttributeKey': 'City',
            'DocumentAttributeValueCountPairs': [
                {
                    'Count': 3,
                    'DocumentAttributeValue': {
```

```
                        'StringValue': 'Dubai'
                    }
                },
                {
                    'Count': 3,
                    'DocumentAttributeValue': {
                        'StringValue': 'Seattle'
                    }
                },
                {
                    'Count': 1,
                    'DocumentAttributeValue': {
                        'StringValue': 'Paris'
                    }
                }
            ]
        }
    ]
```

Anda juga dapat menampilkan informasi aspek untuk aspek bersarang, seperti wilayah dalam kota, untuk memfilter hasil pencarian lebih lanjut.

Contoh respons JSON berikut menunjukkan aspek yang dicakup ke atribut dokumen "CityRegion", sebagai aspek bersarang dalam “Kota”. Responsnya mencakup jumlah dokumen untuk nilai faset bersarang.

```
{
    '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'
                                    }
                                }
                             ]
                        }
                    ]
                }
        }
    ]
}
```

Bila Anda menggunakan bidang daftar string untuk membuat faset, hasil faset kembali didasarkan pada isi daftar string. Misalnya, jika Anda memiliki bidang daftar string yang berisi dua item, satu dengan daftar “dachshund”, “sausage dog” dan satu dengan nilai “husky”, Anda mendapatkan `FacetResults` dengan tiga aspek.

Untuk informasi selengkapnya, lihat Respons kueri dan jenis respons.

Menggunakan atribut dokumen untuk menyaring hasil pencarian

Secara default, `Query` mengembalikan semua hasil pencarian. Untuk menyaring respons, Anda dapat melakukan operasi logis pada atribut dokumen. Misalnya, jika Anda hanya menginginkan dokumen untuk kota tertentu, Anda dapat memfilter atribut dokumen khusus “Kota” dan “Negara”. Anda gunakan AttributeFilteruntuk membuat operasi Boolean pada filter yang Anda berikan.

Sebagian besar atribut dapat digunakan untuk menyaring respons untuk semuajenis respons. Namun, atribut `_excerpt_page_number` hanya berlaku untuk jenis respons `ANSWER` saat menyaring respons.

Contoh berikut menunjukkan bagaimana melakukan operasi AND logis dengan menyaring pada kota tertentu, Seattle, dan negara bagian, Washington.

```
response=kendra.query(
        QueryText = query,
        IndexId = index,
```

```
        AttributeFilter = {'AndAllFilters':
            [
                {"EqualsTo": {"Key": "City","Value": {"StringValue": "Seattle"}}},
                {"EqualsTo": {"Key": "State","Value": {"StringValue": "Washington"}}}
            ]
            }
        )
```

Contoh berikut menunjukkan cara melakukan operasi OR logis untuk ketika salah satu kunci `Fileformat`, `Author`, atau `SourceURI` sesuai dengan nilai yang ditentukan.

```
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"}}}
            ]
            }
        )
```

Untuk bidang `StringList`, gunakan filter atribut `ContainsAny` atau `ContainsAll` untuk mengembalikan dokumen dengan string yang ditentukan. Contoh berikut menunjukkan cara untuk mengembalikan semua dokumen yang memiliki nilai-nilai “Seattle” atau “Portland” di atribut khusus `Locations` mereka.

```
response=kendra.query(
        QueryText = query,
        IndexId = index,
        AttributeFilter = {
                "ContainsAny": { "Key": "Locations", "Value": { "StringListValue":
 [ "Seattle", "Portland"] }}
            }
        )
```

Memfilter atribut setiap dokumen dalam hasil pencarian

Amazon Kendra mengembalikan atribut dokumen untuk setiap dokumen dalam hasil pencarian. Anda dapat memfilter atribut dokumen tertentu yang ingin Anda sertakan dalam respons sebagai bagian dari hasil pencarian. Secara default, semua atribut dokumen yang ditetapkan ke dokumen dikembalikan dalam respons.

Dalam contoh berikut, hanya atribut dokumen `_source_uri` dan `_author` termasuk dalam respons untuk dokumen.

```
response=kendra.query(
        QueryText = query,
        IndexId = index,
        RequestedDocumentAttributes = ["_source_uri", "_author"]
        )
```

Penyaringan pada konteks pengguna

Anda dapat memfilter hasil pencarian pengguna berdasarkan akses pengguna atau grup mereka ke dokumen. Anda dapat menggunakan token pengguna, ID pengguna, atau atribut pengguna untuk memfilter dokumen. Amazon Kendra juga dapat memetakan pengguna ke grup mereka. Anda dapat memilih untuk digunakan AWS IAM Identity Center sebagai toko/sumber identitas Anda.

Pemfilteran konteks pengguna adalah semacam pencarian yang dipersonalisasi dengan manfaat mengontrol akses ke dokumen. Misalnya, tidak semua tim yang mencari informasi di portal perusahaan harus mengakses dokumen perusahaan yang sangat rahasia, juga dokumen ini tidak relevan untuk semua pengguna. Hanya pengguna atau grup tim tertentu yang diberi akses ke dokumen rahasia yang harus melihat dokumen-dokumen ini di hasil pencarian mereka.

Ketika dokumen diindeks Amazon Kendra, daftar kontrol akses yang sesuai (ACL) dicerna untuk sebagian besar dokumen. ACL menentukan nama pengguna dan nama grup yang diizinkan atau ditolak untuk akses ke dokumen. Dokumen tanpa ACL adalah dokumen publik.

Amazon Kendra dapat mengekstrak informasi pengguna atau grup yang terkait dengan setiap dokumen untuk sebagian besar sumber data. Misalnya, dokumen di Quip dapat menyertakan daftar 'berbagi' pengguna terpilih yang diberi akses ke dokumen. Jika Anda menggunakan bucket S3 sebagai sumber data, Anda menyediakan file JSON untuk ACL Anda dan menyertakan jalur S3 ke file ini sebagai bagian dari konfigurasi sumber data. Jika Anda menambahkan dokumen secara

langsung ke indeks, Anda menentukan ACL di objek Principal sebagai bagian dari objek dokumen di BatchPutDocumentAPI.

Anda dapat menggunakan CreateAccessControlConfigurationAPI untuk mengonfigurasi ulang kontrol akses tingkat dokumen yang ada tanpa mengindeks semua dokumen Anda lagi. Misalnya, indeks Anda berisi dokumen perusahaan rahasia yang hanya dapat diakses oleh karyawan atau pengguna tertentu. Salah satu pengguna ini meninggalkan perusahaan atau beralih ke tim yang harus diblokir untuk mengakses dokumen rahasia. Pengguna masih memiliki akses ke dokumen rahasia karena pengguna memiliki akses ketika dokumen Anda sebelumnya diindeks. Anda dapat membuat konfigurasi kontrol akses khusus untuk pengguna dengan tolak akses. Anda nantinya dapat memperbarui konfigurasi kontrol akses untuk mengizinkan akses jika pengguna kembali ke perusahaan dan bergabung kembali dengan tim 'top-rahasia'. Anda dapat mengonfigurasi ulang kontrol akses untuk dokumen Anda saat keadaan berubah.

Untuk menerapkan konfigurasi kontrol akses ke dokumen tertentu, Anda memanggil BatchPutDocumentAPI yang `AccessControlConfigurationId` disertakan dalam objek Dokumen. Jika Anda menggunakan bucket S3 sebagai sumber data, Anda memperbarui `.metadata.json` dengan `AccessControlConfigurationId` dan menyinkronkan sumber data Anda. Amazon Kendra saat ini hanya mendukung konfigurasi kontrol akses untuk sumber data S3 dan dokumen yang diindeks menggunakan API. `BatchPutDocument`

Penyaringan berdasarkan token pengguna

Saat Anda menanyakan indeks, Anda dapat menggunakan token pengguna untuk memfilter hasil pencarian berdasarkan akses pengguna atau grup mereka ke dokumen. Saat Anda mengeluarkan kueri, Amazon Kendra mengekstrak dan memvalidasi token, menarik dan memeriksa informasi pengguna dan grup, dan menjalankan kueri. Semua dokumen yang dapat diakses pengguna, termasuk dokumen publik, dikembalikan. Untuk informasi selengkapnya, lihat Kontrol akses pengguna berbasis Token.

Anda memberikan token pengguna di UserContextobjek dan meneruskannya di Query API.

Berikut ini menunjukkan cara memasukkan token pengguna.

```
response = kendra.query(
    QueryText = query,
    IndexId = index,
    UserToken = {
        Token = "token"
```

```
    })
```

Anda dapat memetakan pengguna ke grup. Bila Anda menggunakan penyaringan konteks pengguna, tidak perlu untuk menyertakan semua kelompok yang dimiliki pengguna ketika Anda mengeluarkan kueri. Dengan PutPrincipalMappingAPI, Anda dapat memetakan pengguna ke grup mereka. Jika Anda tidak ingin menggunakan `PutPrincipalMapping` API, Anda harus memberikan nama pengguna dan semua grup yang dimiliki pengguna saat Anda mengeluarkan kueri. Anda juga dapat mengambil tingkat akses grup dan pengguna di sumber identitas Pusat Identitas IAM Anda dengan menggunakan objek. UserGroupResolutionConfiguration

Pemfilteran berdasarkan ID pengguna dan grup

Saat Anda menanyakan indeks, Anda dapat menggunakan ID pengguna dan grup untuk memfilter hasil penelusuran berdasarkan akses pengguna atau grup mereka ke dokumen. Saat Anda mengeluarkan kueri, Amazon Kendra memeriksa informasi pengguna dan grup dan menjalankan kueri. Semua dokumen yang relevan dengan kueri yang dapat diakses pengguna, termasuk dokumen publik, dikembalikan.

Anda juga dapat memfilter hasil pencarian berdasarkan sumber data yang dapat diakses pengguna dan grup. Hal ini berguna jika grup terkait dengan beberapa sumber data, tetapi Anda hanya ingin grup tersebut mengakses dokumen dalam sumber data tertentu. Misalnya, grup "Penelitian", "Rekayasa", serta "Penjualan dan Pemasaran" semuanya terkait dengan dokumen perusahaan yang disimpan dalam sumber data Confluence dan Salesforce. Namun, tim "Penjualan dan Pemasaran" hanya membutuhkan akses ke dokumen terkait pelanggan yang disimpan di Salesforce. Jadi ketika pengguna penjualan dan pemasaran mencari dokumen terkait pelanggan, mereka dapat melihat dokumen dari Salesforce dalam hasil mereka. Pengguna yang tidak bekerja di penjualan dan pemasaran tidak melihat dokumen Salesforce dalam hasil pencarian mereka.

Anda memberikan informasi kepada pengguna, grup, dan sumber data dalam UserContextobjek dan meneruskannya di Query API. ID pengguna, dan daftar grup dan sumber data harus sesuai dengan nama yang Anda tentukan di objek Utama untuk mengidentifikasi pengguna, grup, dan sumber data. Dengan `Principal` objek, Anda dapat menambahkan pengguna, grup, atau sumber data ke daftar izinkan atau daftar penolakan untuk mengakses dokumen.

Anda diminta untuk memberikan salah satu hal berikut:

- Pengguna dan kelompok informasi, dan (opsional) sumber data informasi.
- Hanya informasi pengguna jika Anda memetakan pengguna ke grup dan sumber data menggunakan PutPrincipalMappingAPI. Anda juga dapat mengambil tingkat akses grup

dan pengguna di sumber identitas Pusat Identitas IAM Anda dengan menggunakan objek. UserGroupResolutionConfiguration

Jika informasi ini tidak termasuk dalam query, Amazon Kendra mengembalikan semua dokumen. Jika Anda memberikan informasi ini, hanya dokumen dengan ID pengguna, grup, dan sumber data yang cocok yang dikembalikan.

Berikut ini menunjukkan cara menyertakan ID pengguna, grup, dan sumber data.

```
response = kendra.query(
    QueryText = query,
    IndexId = index,
    UserId = {
        UserId = "user1"
    },
    Groups = {
        Groups = ["Sales and Marketing"]
    },
    DataSourceGroups = {
        DataSourceGroups = [{"DataSourceId" : "SalesforceCustomerDocsGroup", "GroupId":
 "Sales and Marketing"}]
    })
```

Pemfilteran berdasarkan atribut

Saat Anda menanyakan indeks, Anda dapat menggunakan atribut bawaan `_user_id` dan `_group_id` memfilter hasil pencarian berdasarkan pengguna dan akses grup mereka ke dokumen. Anda dapat mengatur hingga 100 pengenal grup. Saat Anda mengeluarkan kueri, Amazon Kendra memeriksa informasi pengguna dan grup dan menjalankan kueri. Semua dokumen yang relevan dengan kueri yang dapat diakses pengguna, termasuk dokumen publik, dikembalikan.

Anda memberikan atribut pengguna dan grup dalam AttributeFilterobjek dan meneruskannya di Query API.

Contoh berikut menunjukkan permintaan yang menyaring respon kueri berdasarkan ID pengguna dan kelompok “HR” dan “IT”, yang dimiliki pengguna. Kueri akan mengembalikan dokumen yang memiliki pengguna atau grup “HR” atau “IT” dalam daftar izinkan. Jika pengguna atau salah satu grup ada dalam daftar tolak untuk dokumen, dokumen tidak dikembalikan.

```
response = kendra.query(
```

```
        QueryText = query,
        IndexId = index,
        AttributeFilter = {
            "OrAllFilters": [
                {
                    "EqualsTo": {
                        "Key": "_user_id",
                        "Value": {
                            "StringValue": "user1"
                        }
                     }
                },
                {
                    "EqualsTo": {
                        "Key": "_group_ids",
                        "Value": {
                            "StringListValue": ["HR", "IT"]
                        }
                    }
                }
            ]
        }
        )
```

Anda juga dapat menentukan sumber data mana yang dapat diakses grup di objek `Principal`.

> **Note**
>
> Pemfilteran konteks pengguna bukan kontrol autentikasi atau otorisasi untuk konten Anda. Itu tidak melakukan otentikasi pengguna pada pengguna dan grup yang dikirim ke `Query` API. Terserah aplikasi Anda untuk memastikan bahwa informasi pengguna dan grup yang dikirim ke `Query` API diautentikasi dan diotorisasi.

Ada implementasi dari penyaringan konteks pengguna untuk setiap sumber data. Bagian berikut menjelaskan setiap implementasi.

Topik

- Penyaringan konteks pengguna untuk dokumen yang ditambahkan langsung ke indeks
- Penyaringan konteks pengguna untuk pertanyaan yang sering diajukan
- Pemfilteran konteks pengguna untuk sumber data

Penyaringan konteks pengguna untuk dokumen yang ditambahkan langsung ke indeks

Saat Anda menambahkan dokumen langsung ke indeks menggunakan BatchPutDocumentAPI, Amazon Kendra dapatkan informasi pengguna dan grup dari `AccessControlList` bidang dokumen. Anda menyediakan daftar kontrol akses (ACL) untuk dokumen Anda dan ACL dicerna dengan dokumen Anda.

Anda menentukan ACL di objek Principal sebagai bagian dari objek Document di `BatchPutDocument` API. Anda memberikan informasi berikut:

- Akses yang harus dimiliki pengguna atau grup. Anda dapat mengatakan `ALLOW` atau `DENY`.
- Jenis entitas. Anda dapat mengatakan `USER` atau `GROUP`.
- Nama pengguna atau grup.

Anda dapat menambahkan hingga 200 entri di bidang `AccessControlList`.

Penyaringan konteks pengguna untuk pertanyaan yang sering diajukan

Saat Anda menambahkan FAQ ke indeks, Amazon Kendra dapatkan informasi pengguna dan grup dari `AccessControlList` objek/bidang file FAQ JSON. Anda juga dapat menggunakan file CSV FAQ dengan bidang atau atribut khusus untuk kontrol akses.

Anda memberikan informasi berikut:

- Akses yang harus dimiliki pengguna atau grup. Anda dapat mengatakan `ALLOW` atau `DENY`.
- Jenis entitas. Anda dapat mengatakan `USER` atau `GROUP`.
- Nama pengguna atau grup.

Untuk informasi selengkapnya, lihat file FAQ.

Pemfilteran konteks pengguna untuk sumber data

Amazon Kendra juga merayapi informasi daftar kontrol akses pengguna dan grup (ACL) dari konektor sumber data yang didukung. Ini berguna untuk pemfilteran konteks pengguna, di mana hasil pencarian difilter berdasarkan akses pengguna atau grup mereka ke dokumen.

Topik

- Pemfilteran konteks pengguna untuk sumber data MySQL
- Pemfilteran konteks pengguna untuk sumber data Oracle Database
- Pemfilteran konteks pengguna untuk sumber data PostgreSQL
- Pemfilteran konteks pengguna untuk sumber data Quip
- Penyaringan konteks pengguna untuk sumber data Salesforce
- Pemfilteran konteks pengguna untuk sumber ServiceNow data
- Pemfilteran konteks pengguna untuk sumber data Slack
- Pemfilteran konteks pengguna untuk sumber data Zendesk

Pemfilteran konteks pengguna untuk sumber data Adobe Experience Manager

Saat Anda menggunakan sumber data Adobe Experience Manager, Amazon Kendra dapatkan informasi pengguna dan grup dari instance Adobe Experience Manager.

Grup dan ID pengguna dipetakan sebagai berikut:

- `_group_ids`ID Grup ada di konten Adobe Experience Manager di mana ada izin akses yang ditetapkan. Mereka dipetakan dari nama-nama grup di Adobe Experience Manager.
- `_user_id`ID Pengguna ada di konten Adobe Experience Manager di mana ada izin akses yang ditetapkan. Mereka dipetakan dari email pengguna sebagai ID di Adobe Experience Manager.

Anda dapat menambahkan hingga 200 entri di bidang `AccessControlList`.

Pemfilteran konteks pengguna untuk sumber data Alfresco

Bila Anda menggunakan sumber data Alfresco, Amazon Kendra dapatkan informasi pengguna dan grup dari instance Alfresco.

Grup dan ID pengguna dipetakan sebagai berikut:

- `_group_ids`—ID Grup ada di Alfresco pada file di mana ada izin akses yang ditetapkan. Mereka dipetakan dari nama sistem grup (bukan nama tampilan) di Alfresco.
- `_user_id`—ID Pengguna ada di Alfresco pada file di mana ada izin akses yang ditetapkan. Mereka dipetakan dari email pengguna sebagai ID di Alfresco.

Anda dapat menambahkan hingga 200 entri di bidang `AccessControlList`.

Pemfilteran konteks pengguna untuk sumber Aurora data (MySQL)

Saat Anda menggunakan sumber data Aurora (MySQL) Amazon Kendra , dapatkan informasi pengguna dan grup dari kolom di tabel sumber. Anda menentukan kolom ini di konsol atau menggunakan TemplateConfigurationobjek sebagai bagian dari CreateDataSourceAPI.

Sumber data database Aurora (MySQL) memiliki batasan sebagai berikut:

- Anda hanya dapat menentukan daftar izinkan untuk sumber data basis data. Anda tidak dapat menentukan daftar tolak.
- Anda hanya dapat menentukan grup. Anda tidak dapat menentukan pengguna individu untuk daftar izinkan.
- Kolom database harus berupa string yang berisi daftar grup yang dibatasi titik koma.

Pemfilteran konteks pengguna untuk sumber data Aurora (PostgreSQL)

Saat Anda menggunakan sumber data Aurora (PostgreSQL) Amazon Kendra , dapatkan informasi pengguna dan grup dari kolom di tabel sumber. Anda menentukan kolom ini di konsol atau menggunakan TemplateConfigurationobjek sebagai bagian dari CreateDataSourceAPI.

Sumber data database Aurora (PostgreSQL) memiliki batasan sebagai berikut:

- Anda hanya dapat menentukan daftar izinkan untuk sumber data basis data. Anda tidak dapat menentukan daftar tolak.
- Anda hanya dapat menentukan grup. Anda tidak dapat menentukan pengguna individu untuk daftar izinkan.
- Kolom database harus berupa string yang berisi daftar grup yang dibatasi titik koma.

Pemfilteran konteks pengguna untuk sumber Amazon FSx data

Saat Anda menggunakan sumber Amazon FSx data, Amazon Kendra dapatkan informasi pengguna dan grup dari layanan direktori Amazon FSx instance.

Amazon FSx Grup dan ID pengguna dipetakan sebagai berikut:

- `_group_ids`—ID Grup ada di file Amazon FSx di mana ada izin akses yang ditetapkan. Mereka dipetakan dari nama grup sistem di layanan direktori. Amazon FSx

- `_user_id`—ID Pengguna ada di file Amazon FSx di mana ada izin akses yang ditetapkan. Mereka dipetakan dari nama pengguna sistem di layanan direktori. Amazon FSx

Anda dapat menambahkan hingga 200 entri di bidang `AccessControlList`.

Penyaringan konteks pengguna untuk sumber data basis data

Bila Anda menggunakan sumber data database, seperti Amazon Aurora PostgreSQL, Amazon Kendra mendapatkan informasi pengguna dan grup dari kolom dalam tabel sumber. Anda menentukan kolom ini di AclConfigurationobjek sebagai bagian dari DatabaseConfigurationobjek di CreateDataSourceAPI.

Sumber data basis data memiliki batasan sebagai berikut:

- Anda hanya dapat menentukan daftar izinkan untuk sumber data basis data. Anda tidak dapat menentukan daftar tolak.
- Anda hanya dapat menentukan grup. Anda tidak dapat menentukan pengguna individu untuk daftar izinkan.
- Kolom database harus berupa string yang berisi daftar grup yang dibatasi titik koma.

Pemfilteran konteks pengguna untuk Amazon RDS sumber data (Microsoft SQL Server)

Bila Anda menggunakan sumber data Amazon RDS (Microsoft SQL Server), Amazon Kendra mendapatkan informasi pengguna dan grup dari kolom di tabel sumber. Anda menentukan kolom ini di konsol atau menggunakan TemplateConfigurationobjek sebagai bagian dari CreateDataSourceAPI.

Sumber data database Amazon RDS (Microsoft SQL Server) memiliki batasan sebagai berikut:

- Anda hanya dapat menentukan daftar izinkan untuk sumber data basis data. Anda tidak dapat menentukan daftar tolak.
- Anda hanya dapat menentukan grup. Anda tidak dapat menentukan pengguna individu untuk daftar izinkan.
- Kolom database harus berupa string yang berisi daftar grup yang dibatasi titik koma.

Pemfilteran konteks pengguna untuk sumber Amazon RDS data (MySQL)

Saat Anda menggunakan sumber data Amazon RDS (MySQL) Amazon Kendra , dapatkan informasi pengguna dan grup dari kolom di tabel sumber. Anda menentukan kolom ini di konsol atau menggunakan TemplateConfigurationobjek sebagai bagian dari CreateDataSourceAPI.

Sumber data database Amazon RDS (MySQL) memiliki batasan sebagai berikut:

- Anda hanya dapat menentukan daftar izinkan untuk sumber data basis data. Anda tidak dapat menentukan daftar tolak.
- Anda hanya dapat menentukan grup. Anda tidak dapat menentukan pengguna individu untuk daftar izinkan.
- Kolom database harus berupa string yang berisi daftar grup yang dibatasi titik koma.

Pemfilteran konteks pengguna untuk sumber Amazon RDS data (Oracle)

Saat Anda menggunakan sumber data Amazon RDS (Oracle), Amazon Kendra dapatkan informasi pengguna dan grup dari kolom di tabel sumber. Anda menentukan kolom ini di konsol atau menggunakan TemplateConfigurationobjek sebagai bagian dari CreateDataSourceAPI.

Sumber data database Amazon RDS (Oracle) memiliki batasan sebagai berikut:

- Anda hanya dapat menentukan daftar izinkan untuk sumber data basis data. Anda tidak dapat menentukan daftar tolak.
- Anda hanya dapat menentukan grup. Anda tidak dapat menentukan pengguna individu untuk daftar izinkan.
- Kolom database harus berupa string yang berisi daftar grup yang dibatasi titik koma.

Pemfilteran konteks pengguna untuk sumber data Amazon RDS (PostgreSQL)

Saat Anda menggunakan sumber data Amazon RDS (PostgreSQL) Amazon Kendra , dapatkan informasi pengguna dan grup dari kolom di tabel sumber. Anda menentukan kolom ini di konsol atau menggunakan TemplateConfigurationobjek sebagai bagian dari CreateDataSourceAPI.

Sumber data database Amazon RDS (PostgreSQL) memiliki batasan sebagai berikut:

- Anda hanya dapat menentukan daftar izinkan untuk sumber data basis data. Anda tidak dapat menentukan daftar tolak.

- Anda hanya dapat menentukan grup. Anda tidak dapat menentukan pengguna individu untuk daftar izinkan.
- Kolom database harus berupa string yang berisi daftar grup yang dibatasi titik koma.

Pemfilteran konteks pengguna untuk sumber Amazon S3 data

Anda menambahkan pemfilteran konteks pengguna ke dokumen dalam sumber Amazon S3 data menggunakan file metadata yang terkait dengan dokumen. Anda menambahkan informasi ke bidang `AccessControlList` dalam dokumen JSON. Untuk informasi selengkapnya tentang menambahkan metadata ke dokumen yang diindeks dari sumber Amazon S3 data, lihat metadata dokumen S3.

Anda menyediakan tiga bagian informasi:

- Akses yang harus dimiliki entitas. Anda dapat mengatakan `ALLOW` atau `DENY`.
- Jenis entitas. Anda dapat mengatakan `USER` atau `GROUP`.
- Nama entitas.

Anda dapat menambahkan hingga 200 entri di bidang `AccessControlList`.

Pemfilteran konteks pengguna untuk sumber Amazon WorkDocs data

Saat Anda menggunakan sumber Amazon WorkDocs data, Amazon Kendra dapatkan informasi pengguna dan grup dari Amazon WorkDocs instance.

Amazon WorkDocs Grup dan ID pengguna dipetakan sebagai berikut:

- `_group_ids`—ID Grup ada di file Amazon WorkDocs di mana ada izin akses yang ditetapkan. Mereka dipetakan dari nama-nama grup di Amazon WorkDocs.
- `_user_id`—ID Pengguna ada di file Amazon WorkDocs di mana ada izin akses yang ditetapkan. Mereka dipetakan dari nama pengguna di Amazon WorkDocs.

Anda dapat menambahkan hingga 200 entri di bidang `AccessControlList`.

Pemfilteran konteks pengguna untuk sumber data Kotak

Bila Anda menggunakan sumber data Box, Amazon Kendra dapatkan informasi pengguna dan grup dari instance Box.

Grup Box dan ID pengguna dipetakan sebagai berikut:

- `_group_ids`—ID Grup ada di Kotak pada file di mana ada izin akses yang ditetapkan. Mereka dipetakan dari nama-nama grup di Box.
- `_user_id`—ID Pengguna ada di Kotak pada file di mana ada izin akses yang ditetapkan. Mereka dipetakan dari email pengguna sebagai ID pengguna di Box.

Anda dapat menambahkan hingga 200 entri di bidang `AccessControlList`.

Penyaringan konteks pengguna untuk sumber data basis data

Saat Anda menggunakan sumber data Confluence, Amazon Kendra dapatkan informasi pengguna dan grup dari instance Confluence.

Anda mengonfigurasi pengguna dan grup akses ke ruang menggunakan halaman izin ruang. Untuk halaman dan blog, Anda menggunakan halaman pembatasan. Untuk informasi selengkapnya tentang ruang izin, lihat Gambaran Umum Izin Ruang di situs web Support Confluence. Untuk informasi selengkapnya tentang batasan halaman dan blog, lihat Pembatasan Halaman di situs web Support Confluence.

Grup Confluence dan nama pengguna dipetakan sebagai berikut:

- `_group_ids`Nama grup ada di spasi, halaman, dan blog di mana ada batasan. Mereka dipetakan dari nama grup di Confluence. Nama grup selalu huruf kecil.

- `_user_id`Nama pengguna ada di ruang, halaman, atau blog di mana ada batasan. Mereka dipetakan tergantung pada jenis instance Confluence yang Anda gunakan.

  Untuk konektor Confluence v1.0

  - Server — `_user_id` Ini adalah nama pengguna. Nama pengguna selalu huruf kecil.
  - `_user_id`Cloud—Ini adalah ID akun pengguna.

  Untuk konektor Confluence v2.0

  - Server — `_user_id` Ini adalah nama pengguna. Nama pengguna selalu huruf kecil.
  - `_user_id`Cloud—Ini adalah ID email pengguna.

  > **Important**
  >
  > Agar pemfilteran konteks pengguna berfungsi dengan benar untuk konektor Confluence Anda, Anda perlu memastikan bahwa visibilitas pengguna yang diberikan akses ke

halaman Confluence disetel ke Siapa pun. Untuk informasi selengkapnya, lihat Mengatur visibilitas email Anda di Dokumentasi Pengembang Atlassian.

Anda dapat menambahkan hingga 200 entri di bidang `AccessControlList`.

Pemfilteran konteks pengguna untuk sumber data Dropbox

Saat Anda menggunakan sumber data Dropbox, Amazon Kendra dapatkan informasi pengguna dan grup dari instans Dropbox.

Grup dan ID pengguna dipetakan sebagai berikut:

- `_group_ids`ID Grup ada di Dropbox pada file di mana ada izin akses yang ditetapkan. Mereka dipetakan dari nama-nama grup di Dropbox.
- `_user_id`—ID Pengguna ada di Dropbox pada file di mana ada izin akses yang ditetapkan. Mereka dipetakan dari email pengguna sebagai ID di Dropbox.

Anda dapat menambahkan hingga 200 entri di bidang `AccessControlList`.

Pemfilteran konteks pengguna untuk sumber data Drupal

Bila Anda menggunakan sumber data Drupal, Amazon Kendra dapatkan informasi pengguna dan grup dari Drupalinstance.

Grup dan ID pengguna dipetakan sebagai berikut:

- `_group_ids`— ID Grup ada di Drupal pada file di mana ada izin akses yang ditetapkan. Mereka dipetakan dari nama-nama grup di Drupal.
- `_user_id`— ID Pengguna ada di Drupal pada file di mana ada izin akses yang ditetapkan. Mereka dipetakan dari email pengguna sebagai ID di Drupal.

Anda dapat menambahkan hingga 200 entri di bidang `AccessControlList`.

Pemfilteran konteks pengguna untuk sumber GitHub data

Saat Anda menggunakan sumber GitHub data, Amazon Kendra dapatkan informasi pengguna dari GitHub instance.

ID GitHub pengguna dipetakan sebagai berikut:

- `_user_id`—ID Pengguna ada di file GitHub di mana ada izin akses yang ditetapkan. Mereka dipetakan dari email pengguna sebagai ID di GitHub.

Anda dapat menambahkan hingga 200 entri di bidang `AccessControlList`.

Pemfilteran konteks pengguna untuk sumber data Gmail

Saat Anda menggunakan sumber data Gmail, Amazon Kendra dapatkan informasi pengguna dari instance Gmail.

ID pengguna dipetakan sebagai berikut:

- `_user_id`— ID pengguna ada di Gmail pada file di mana ada izin akses yang ditetapkan. Mereka dipetakan dari email pengguna sebagai ID di Gmail.

Anda dapat menambahkan hingga 200 entri di bidang `AccessControlList`.

Penyaringan konteks pengguna untuk sumber data Google Drive

Sumber data Drive Google Workspace mengembalikan informasi pengguna dan grup untuk pengguna dan grup Google Drive. Keanggotaan grup dan domain dipetakan ke bidang indeks `_group_ids`. Nama pengguna Google Drive dipetakan ke bidang `_user_id`.

Saat Anda memberikan satu atau beberapa alamat email pengguna di `Query` API, hanya dokumen yang telah dibagikan dengan alamat email tersebut yang dikembalikan. Parameter `AttributeFilter` berikut hanya mengembalikan dokumen yang dibagikan dengan "martha@example.com”.

```
"AttributeFilter": {
                "EqualsTo":{
                   "Key": "_user_id",
                   "Value": {
                       "StringValue": "martha@example.com"
                   }
               }
           }
```

Jika Anda memberikan satu atau lebih alamat email grup dalam permintaan, hanya dokumen yang dibagikan dengan grup yang akan dikembalikan. Parameter `AttributeFilter` berikut hanya mengembalikan dokumen yang dibagikan dengan grup "hr@example.com".

```
"AttributeFilter": {
                "EqualsTo":{
                   "Key": "_group_ids",
                   "Value": {
                       "StringListValue": ["hr@example.com"]
                   }
               }
           }
```

Jika Anda menyertakan domain dalam kueri, semua dokumen yang dibagikan dengan domain akan dikembalikan. Parameter `AttributeFilter` berikut hanya mengembalikan dokumen yang dibagikan dengan domain "example.com".

```
"AttributeFilter": {
                "EqualsTo":{
                   "Key": "_group_ids",
                   "Value": {
                       "StringListValue": ["example.com"]
                   }
               }
           }
```

Anda dapat menambahkan hingga 200 entri di bidang `AccessControlList`.

Pemfilteran konteks pengguna untuk sumber data IBM DB2

Saat Anda menggunakan sumber data IBM DB2, Amazon Kendra dapatkan informasi pengguna dan grup dari kolom di tabel sumber. Anda menentukan kolom ini di konsol atau menggunakan TemplateConfigurationobjek sebagai bagian dari CreateDataSourceAPI.

Sumber data database IBM DB2 memiliki keterbatasan sebagai berikut:

- Anda hanya dapat menentukan daftar izinkan untuk sumber data basis data. Anda tidak dapat menentukan daftar tolak.
- Anda hanya dapat menentukan grup. Anda tidak dapat menentukan pengguna individu untuk daftar izinkan.
- Kolom database harus berupa string yang berisi daftar grup yang dibatasi titik koma.

Pemfilteran konteks pengguna untuk sumber data Jira

Saat Anda menggunakan sumber data Jira, Amazon Kendra dapatkan informasi pengguna dan grup dari instance Jira.

ID pengguna Jira dipetakan sebagai berikut:

- `_user_id`—ID Pengguna ada di Jira pada file di mana ada izin akses yang ditetapkan. Mereka dipetakan dari email pengguna sebagai ID pengguna di Jira.

Anda dapat menambahkan hingga 200 entri di bidang `AccessControlList`.

Pemfilteran konteks pengguna untuk sumber data Microsoft Exchange

Saat Anda menggunakan sumber data Microsoft Exchange, Amazon Kendra dapatkan informasi pengguna dari instance Microsoft Exchange.

ID pengguna Microsoft Exchange dipetakan sebagai berikut:

- `_user_id`ID Pengguna ada di izin Microsoft Exchange bagi pengguna untuk mengakses konten tertentu. Mereka dipetakan dari nama pengguna sebagai ID di Microsoft Exchange.

Anda dapat menambahkan hingga 200 entri di bidang `AccessControlList`.

Pemfilteran konteks pengguna untuk sumber OneDrive data Microsoft

Amazon Kendra mengambil informasi pengguna dan grup dari Microsoft OneDrive ketika mengindeks dokumen di situs. Informasi pengguna dan grup diambil dari SharePoint situs Microsoft yang mendasari yang dihosting OneDrive.

Saat Anda menggunakan OneDrive pengguna atau grup untuk memfilter hasil pencarian, hitung ID sebagai berikut:

1. Dapatkan nama situs. Misalnya, `https://host.onmicrosoft.com/sites/siteName.`
2. Ambil MD5 hash dari nama situs. Misalnya, `430a6b90503eef95c89295c8999c7981`.
3. Buat email pengguna atau ID grup dengan menggabungkan hash MD5 dengan bar vertikal (|) dan ID. Misalnya, jika nama grup adalah "localGroupName“, ID grup adalah:

```
"430a6b90503eef95c89295c8999c7981 | localGroupName"
```

> **Note**
>
> Sertakan spasi sebelum dan sesudah bilah vertikal. Bilah vertikal digunakan untuk mengidentifikasi `localGroupName` dengan hash MD5-nya.

Untuk nama pengguna "someone@host.onmicrosoft.com," ID pengguna akan jadi seperti berikut:

`"430a6b90503eef95c89295c8999c7981 | someone@host.onmicrosoft.com"`

Kirim ID pengguna atau grup ke Amazon Kendra sebagai `_group_id` atribut `_user_id` or saat Anda memanggil Query API. Misalnya, AWS CLI perintah yang menggunakan grup untuk memfilter hasil pencarian terlihat seperti ini:

```
aws kendra  query \
                --index-id index ID
                --query-text "query text"
                --attribute-filter '{
                   "EqualsTo":{
                     "Key": "_group_id",
                     "Value": {"StringValue": "430a6b90503eef95c89295c8999c7981 |
 localGroupName"}
                  }}'
```

Anda dapat menambahkan hingga 200 entri di bidang `AccessControlList`.

Pemfilteran konteks pengguna untuk sumber data Microsoft OneDrive v2.0

Sumber data Microsoft OneDrive v2.0 mengembalikan informasi bagian dan halaman dari entitas daftar kontrol OneDrive akses (ACL). Amazon Kendra menggunakan domain OneDrive penyewa untuk terhubung ke OneDrive instance dan kemudian dapat memfilter hasil pencarian berdasarkan akses pengguna atau grup ke bagian dan nama file.

Untuk objek standar, `_user_id` dan `_group_id` digunakan sebagai berikut:

- `_user_id`— ID email OneDrive pengguna Microsoft Anda dipetakan ke `_user_id` bidang.
- `_group_id`— Email OneDrive grup Microsoft Anda dipetakan ke `_group_id` bidang.

Anda dapat menambahkan hingga 200 entri di bidang `AccessControlList`.

Pemfilteran konteks pengguna untuk sumber SharePoint data Microsoft

Amazon Kendra mengambil informasi pengguna dan grup dari Microsoft SharePoint ketika mengindeks dokumen situs. Untuk memfilter hasil penelusuran berdasarkan akses pengguna atau grup, berikan informasi pengguna dan grup saat Anda memanggil `Query` API.

Untuk menyaring menggunakan nama pengguna, gunakan alamat email pengguna. Sebagai contoh, johnstiles@example.com.

Bila Anda menggunakan SharePoint grup untuk memfilter hasil pencarian, hitung ID grup sebagai berikut:

Untuk grup lokal

1. Dapatkan nama situs. Misalnya, `https://host.onmicrosoft.com/sites/siteName.`
2. Ambil hash SHA256 dari nama situs. Misalnya, `430a6b90503eef95c89295c8999c7981`.
3. Buat ID grup dengan menggabungkan hash SHA256 dengan bar vertikal (|) dan nama grup. Misalnya, jika nama grup adalah "localGroupName“, ID grup adalah:

   ```
   "430a6b90503eef95c89295c8999c7981 | localGroupName"
   ```

   > **Note**
   >
   > Sertakan spasi sebelum dan sesudah bilah vertikal. Bilah vertikal digunakan untuk mengidentifikasi `localGroupName` dengan hash SHA256-nya.

Kirim ID grup Amazon Kendra sebagai `_group_id` atribut saat Anda memanggil Query API. Misalnya, AWS CLI perintahnya terlihat seperti ini:

```
aws kendra  query \
                --index-id index ID
                --query-text "query text"
                --attribute-filter '{
                   "EqualsTo":{
                     "Key": "_group_id",
                     "Value": {"StringValue": "430a6b90503eef95c89295c8999c7981 |
 localGroupName"}
```

```
                }}'
```

Untuk grup AD

1. Gunakan ID grup AD untuk mengonfigurasi pemfilteran hasil penelusuran.

Kirim ID grup Amazon Kendra sebagai `_group_id` atribut saat Anda memanggil Query API. Misalnya, AWS CLI perintahnya terlihat seperti ini:

```
aws kendra  query \
               --index-id index ID
               --query-text "query text"
               --attribute-filter '{
                  "EqualsTo":{
                    "Key": "_group_id",
                    "Value": {"StringValue": "AD group"}
                  }}'
```

Anda dapat menambahkan hingga 200 entri di bidang `AccessControlList`.

Pemfilteran konteks pengguna untuk sumber data Microsoft SQL Server

Bila Anda menggunakan sumber data Microsoft SQL Server, Amazon Kendra mendapatkan informasi pengguna dan grup dari kolom di tabel sumber. Anda menentukan kolom ini di konsol atau menggunakan TemplateConfigurationobjek sebagai bagian dari CreateDataSourceAPI.

Sumber data database Microsoft SQL Server memiliki batasan sebagai berikut:

- Anda hanya dapat menentukan daftar izinkan untuk sumber data basis data. Anda tidak dapat menentukan daftar tolak.
- Anda hanya dapat menentukan grup. Anda tidak dapat menentukan pengguna individu untuk daftar izinkan.
- Kolom database harus berupa string yang berisi daftar grup yang dibatasi titik koma.

Pemfilteran konteks pengguna untuk sumber data Microsoft Teams

Amazon Kendra mengambil informasi pengguna dari Microsoft Teams saat mengindeks dokumen. Informasi pengguna diambil dari instans Microsoft Teams yang mendasarinya.

Anda dapat menambahkan hingga 200 entri di bidang `AccessControlList`.

Pemfilteran konteks pengguna untuk sumber data Microsoft Yammer

Amazon Kendra mengambil informasi pengguna dari Microsoft Yammer ketika mengindeks dokumen. Informasi pengguna dan grup diambil dari instans Microsoft Yammer yang mendasarinya.

ID pengguna Microsoft Yammer dipetakan sebagai berikut:

- `_email_id`— ID email Microsoft dipetakan ke `_user_id` bidang.

Anda dapat menambahkan hingga 200 entri di bidang `AccessControlList`.

Pemfilteran konteks pengguna untuk sumber data MySQL

Bila Anda menggunakan sumber data MySQL Amazon Kendra , mendapatkan informasi pengguna dan grup dari kolom di tabel sumber. Anda menentukan kolom ini di konsol atau menggunakan TemplateConfigurationobjek sebagai bagian dari CreateDataSourceAPI.

Sumber data database MySQL memiliki keterbatasan sebagai berikut:

- Anda hanya dapat menentukan daftar izinkan untuk sumber data basis data. Anda tidak dapat menentukan daftar tolak.
- Anda hanya dapat menentukan grup. Anda tidak dapat menentukan pengguna individu untuk daftar izinkan.
- Kolom database harus berupa string yang berisi daftar grup yang dibatasi titik koma.

Pemfilteran konteks pengguna untuk sumber data Oracle Database

Bila Anda menggunakan sumber data Oracle Database, Amazon Kendra mendapatkan informasi pengguna dan grup dari kolom di tabel sumber. Anda menentukan kolom ini di konsol atau menggunakan TemplateConfigurationobjek sebagai bagian dari CreateDataSourceAPI.

Sumber data database Oracle Database memiliki keterbatasan sebagai berikut:

- Anda hanya dapat menentukan daftar izinkan untuk sumber data basis data. Anda tidak dapat menentukan daftar tolak.
- Anda hanya dapat menentukan grup. Anda tidak dapat menentukan pengguna individu untuk daftar izinkan.
- Kolom database harus berupa string yang berisi daftar grup yang dibatasi titik koma.

Pemfilteran konteks pengguna untuk sumber data PostgreSQL

Bila Anda menggunakan sumber data PostgreSQL Amazon Kendra , mendapatkan informasi pengguna dan grup dari kolom dalam tabel sumber. Anda menentukan kolom ini di konsol atau menggunakan TemplateConfigurationobjek sebagai bagian dari CreateDataSourceAPI.

Sumber data database PostgreSQL memiliki keterbatasan sebagai berikut:

- Anda hanya dapat menentukan daftar izinkan untuk sumber data basis data. Anda tidak dapat menentukan daftar tolak.
- Anda hanya dapat menentukan grup. Anda tidak dapat menentukan pengguna individu untuk daftar izinkan.
- Kolom database harus berupa string yang berisi daftar grup yang dibatasi titik koma.

Pemfilteran konteks pengguna untuk sumber data Quip

Saat Anda menggunakan sumber data Quip, Amazon Kendra dapatkan informasi pengguna dari instance Quip.

ID pengguna Quip dipetakan sebagai berikut:

- `_user_id`—ID Pengguna ada di Quip pada file di mana ada izin akses yang ditetapkan. Mereka dipetakan dari email pengguna sebagai ID di Quip.

Anda dapat menambahkan hingga 200 entri di bidang `AccessControlList`.

Penyaringan konteks pengguna untuk sumber data Salesforce

Sumber data Salesforce mengembalikan informasi pengguna dan grup dari entitas daftar kontrol akses Salesforce (ACL). Anda dapat menerapkan penyaringan konteks pengguna untuk objek standar dan feed obrolan Salesforce. Penyaringan konteks pengguna ini tidak tersedia untuk artikel pengetahuan Salesforce.

Untuk objek standar, `_user_id` dan `_group_ids` digunakan sebagai berikut:

- `_user_id`—Nama pengguna pengguna Salesforce.
- `_group_ids`—
  - Nama Salesforce `Profile`

- Nama Salesforce `Group`
- Nama Salesforce `UserRole`
- Nama Salesforce `PermissionSet`

Untuk feed obrolan, `_user_id` dan `_group_ids` digunakan sebagai berikut:

- `_user_id`—Nama pengguna pengguna Salesforce. Hanya tersedia jika item diposting di feed pengguna.
- `_group_ids`—ID Grup digunakan sebagai berikut. Hanya tersedia jika item umpan diposting dalam grup obrolan atau kolaborasi.
  - Nama obrolan atau grup kolaborasi.
  - Jika grup berupa publik, `PUBLIC:ALL`.

Anda dapat menambahkan hingga 200 entri di bidang `AccessControlList`.

Pemfilteran konteks pengguna untuk sumber ServiceNow data

Pemfilteran konteks pengguna hanya ServiceNow didukung untuk TemplateConfiguration API dan ServiceNow Connector v2.0. ServiceNowConfigurationAPI dan ServiceNow Konektor v1.0. tidak mendukung pemfilteran konteks pengguna.

Saat Anda menggunakan sumber ServiceNow data, Amazon Kendra dapatkan informasi pengguna dan grup dari ServiceNow instance.

Grup dan ID pengguna dipetakan sebagai berikut:

- `_group_ids`—ID Grup ada di file ServiceNow di mana ada izin akses yang ditetapkan. Mereka dipetakan dari nama peran `sys_ids` in ServiceNow.
- `_user_id`—ID Pengguna ada di file ServiceNow di mana ada izin akses yang ditetapkan. Mereka dipetakan dari email pengguna sebagai ID di ServiceNow.

Anda dapat menambahkan hingga 200 entri di bidang `AccessControlList`.

Pemfilteran konteks pengguna untuk sumber data Slack

Saat Anda menggunakan sumber data Slack, Amazon Kendra dapatkan informasi pengguna dari instance Slack.

ID pengguna Slack dipetakan sebagai berikut:

- `_user_id`ID Pengguna ada di Slack pada pesan dan saluran di mana ada izin akses yang ditetapkan. Mereka dipetakan dari email pengguna sebagai ID di Slack.

Anda dapat menambahkan hingga 200 entri di bidang `AccessControlList`.

Pemfilteran konteks pengguna untuk sumber data Zendesk

Bila Anda menggunakan sumber data Zendesk, Amazon Kendra dapatkan informasi pengguna dan grup dari instance Zendesk.

Grup dan ID pengguna dipetakan sebagai berikut:

- `_group_ids`ID Grup ada di tiket Zendesk dan artikel di mana ada izin akses yang ditetapkan. Mereka dipetakan dari nama-nama grup di Zendesk.
- `_user_id`ID Grup ada di tiket Zendesk dan artikel di mana ada izin akses yang ditetapkan. Mereka dipetakan dari email pengguna sebagai ID di Zendesk.

Anda dapat menambahkan hingga 200 entri di bidang `AccessControlList`.

Respons kueri dan jenis respons

Amazon Kendra mendukung respons kueri dan jenis respons yang berbeda.

Jawaban kueri

Panggilan ke Query API mengembalikan informasi tentang hasil pencarian. Hasilnya dalam array QueryResultItemobjek (`ResultItems`). Setiap `QueryResultItem` menyertakan ringkasan hasilnya. Atribut dokumen yang terkait dengan hasil kueri juga disertakan.

Informasi ringkasan

Ringkasan informasi bervariasi tergantung pada jenis hasil. Dalam setiap kasus, itu termasuk teks dokumen yang cocok dengan istilah pencarian. Hal ini juga termasuk menyoroti informasi yang dapat Anda gunakan untuk menyoroti teks pencarian dalam output aplikasi Anda. Misalnya, jika istilah pencarian adalah berapa tinggi Space Needle?, informasi ringkasan mencakup lokasi teks untuk

kata-kata tinggi dan space needle. Untuk informasi selengkapnya tentang respons, lihat Respons kueri dan jenis respons.

Atribut dokumen

Setiap hasil berisi atribut dokumen untuk dokumen yang cocok dengan kueri. Beberapa atribut telah ditetapkan, seperti `DocumentId`, `DocumentTitle`, dan `DocumentUri`. Lainnya adalah atribut kustom yang Anda tetapkan. Anda dapat menggunakan atribut dokumen untuk memfilter respons dari `Query` API. Misalnya, Anda mungkin hanya ingin dokumen yang ditulis oleh penulis tertentu atau versi tertentu dari dokumen. Untuk informasi selengkapnya, lihat Penyaringan dan pencarian faset. Anda menentukan atribut dokumen saat Anda menambahkan dokumen ke indeks. Untuk informasi selengkapnya, lihat Bidang atau atribut khusus.

Berikut ini adalah contoh kode JSON untuk hasil kueri. Perhatikan atribut dokumen di `DocumentAttributes` dan `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
}
```

Jenis respons

Amazon Kendra mengembalikan tiga jenis respon query.

- Jawaban (termasuk jawaban tabel)
- Dokumen
- Pertanyaan dan jawaban

Jenis respons dikembalikan di bidang `Type` respons QueryResultItemobjek.

Jawaban

Amazon Kendra mendeteksi satu atau lebih jawaban pertanyaan dalam tanggapan. Factoid adalah respons terhadap pertanyaan siapa, apa, kapan, atau di mana seperti Di mana pusat layanan terdekat dengan saya? Amazon Kendra mengembalikan teks dalam indeks yang paling cocok dengan query. Teks ada dalam bidang `AnswerText` dan berisi informasi sorotan untuk istilah

pencarian dalam teks respons.`AnswerText` termasuk kutipan dokumen lengkap dengan teks yang disorot, sementara `DocumentExcerpt` termasuk kutipan dokumen terpotong (290 karakter) dengan teks yang disorot.

Amazon Kendra hanya mengembalikan satu jawaban per dokumen, dan itu adalah jawaban dengan keyakinan tertinggi. Untuk mengembalikan beberapa jawaban dari dokumen, Anda harus membagi dokumen menjadi beberapa dokumen.

```
{
    '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''AmazonTextractrepresents
\n''documentsasBlockobjects,
        ''seeDocumentsandBlockObjects.
\n''\n''\n''\n''Forinformationaboutdocument''limits,
        seeLimitsinAmazonTextract.
\n''\n''\n''\n''TheAmazonTextractsynchronous''operationscanprocessdocumentsstoredinanAmazon
\n''S3Bucketoryoucanpass''base64encodedimagebytes.\n''Formoreinformation,
```

```
 see''CallingAmazonTextractSynchronousOperations.''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''Textractrepresents\n'''
    },
    'Type': 'ANSWER'
}
```

Dokumen

Amazon Kendra mengembalikan dokumen peringkat untuk mereka yang cocok dengan istilah pencarian. Peringkat didasarkan pada keyakinan yang Amazon Kendra memiliki keakuratan hasil pencarian. Informasi tentang dokumen yang cocok dikembalikan di QueryResultItem. Ini mencakup judul dokumen. Kutipan mencakup informasi sorotan untuk teks pencarian dan bagian teks yang cocok dalam dokumen. URI untuk dokumen yang cocok adalah di atribut dokumen `SourceURI`. Contoh JSON berikut menunjukkan ringkasan dokumen untuk dokumen yang cocok.

```
{
    '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'
}
```

Pertanyaan dan jawaban

Respons pertanyaan dan jawaban dikembalikan ketika Amazon Kendra mencocokkan pertanyaan dengan salah satu pertanyaan yang sering diajukan dalam indeks Anda. Jawabannya mencakup pertanyaan dan jawaban yang cocok di QueryResultItemlapangan. Ini juga mencakup informasi sorotan untuk istilah kueri yang terdeteksi dalam string kueri. JSON berikut menunjukkan respons tanya jawab. Perhatikan bahwa respons mencakup teks pertanyaan.

```
{
    '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?'
    }
}
```

Untuk informasi tentang menambahkan teks tanya jawab ke indeks, lihat Membuat FAQ.

Menyetel dan menyortir tanggapan

Anda dapat memodifikasi efek dari bidang atau atribut pada relevansi pencarian melalui penyetelan relevansi. Anda juga dapat mengurutkan hasil pencarian berdasarkan atribut atau bidang tertentu.

Topik

- Penyetelan respons
- Menyortir respons

Penyetelan respons

Anda dapat memodifikasi efek dari bidang atau atribut pada relevansi pencarian melalui penyetelan relevansi. Untuk menguji penyetelan relevansi dengan cepat, gunakan Query API untuk meneruskan konfigurasi penyetelan dalam kueri. Kemudian Anda dapat melihat hasil pencarian yang berbeda yang Anda dapatkan dari konfigurasi yang berbeda. Relevansi penyetelan pada tingkat permintaan tidak didukung di konsol. Anda juga dapat menyetel bidang atau atribut yang bertipe `StringList` di tingkat indeks saja. Untuk informasi selengkapnya, lihat Menyetel relevansi penelusuran.

Secara default, respons kueri diurutkan berdasarkan skor relevansi yang Amazon Kendra menentukan untuk setiap hasil dalam respons.

Anda dapat menyetel hasil untuk atribut/bidang bawaan atau kustom dari jenis berikut:

- Nilai tanggal
- Nilai panjang
- Nilai string

Anda tidak dapat mengurutkan atribut dari jenis berikut:

- Nilai daftar string

Rank dan tune hasil dokumen (AWS SDK)

Setel parameter `Searchable` ke betul untuk meningkatkan konfigurasi metadata dokumen.

Untuk menyetel atribut dalam kueri, atur `DocumentRelevanceOverrideConfigurations` parameter `Query` API dan tentukan nama atribut yang akan disetel.

Contoh JSON berikut menunjukkan `DocumentRelevanceOverrideConfigurations` objek yang mengesampingkan penyetelan untuk atribut yang disebut “departemen” dalam indeks.

```
"DocumentRelevanceOverrideConfigurations" : [
    "Name": "department",
    "Relevance": {
        "Importance": 1,
        "ValueImportanceMap": {
            "IT": 3,
            "HR": 7
        }
```

```
    }
]
```

Menyortir respons

Amazon Kendra menggunakan atribut atau bidang penyortiran sebagai bagian dari kriteria untuk dokumen yang dikembalikan oleh kueri. Sebagai contoh, hasil yang dikembalikan oleh kueri diurutkan berdasarkan “_created_at” mungkin tidak berisi hasil yang sama seperti kueri yang diurutkan berdasarkan “_version”.

Secara default, respons kueri diurutkan berdasarkan skor relevansi yang Amazon Kendra menentukan untuk setiap hasil dalam respons. Untuk mengubah urutan pengurutan, buat atribut dokumen dapat diurutkan dan kemudian konfigurasikan Amazon Kendra untuk menggunakan atribut tersebut untuk mengurutkan respons.

Anda dapat mengurutkan hasil pada atribut/bidang bawaan atau kustom dari jenis berikut:

- Nilai tanggal
- Nilai panjang
- Nilai string

Anda tidak dapat mengurutkan atribut dari jenis berikut:

- Nilai daftar string

Anda dapat mengurutkan satu atau beberapa atribut dokumen di setiap kueri. Query mengembalikan 100 hasil. Jika ada kurang dari 100 dokumen dengan set atribut penyortiran, dokumen tanpa nilai untuk atribut pengurutan akan dikembalikan pada akhir hasil, diurutkan berdasarkan relevansi dengan kueri.

Untuk mengurutkan hasil dokumen (AWS SDK)

1. Untuk menggunakan UpdateIndexAPI agar atribut dapat diurutkan, setel `Sortable` parameter ke`true`. Contoh JSON berikut menggunakan `DocumentMetadataConfigurationUpdates` untuk menambahkan atribut yang disebut “Departemen” ke indeks dan membuatnya dapat diurutkan.

   ```
   "DocumentMetadataConfigurationUpdates": [
   ```

```
    {
        "Name": "Department",
        "Type": "STRING_VALUE",
        "Search": {
            "Sortable": "true"
        }
    }
]
```

2. Untuk menggunakan satu atribut yang dapat diurutkan dalam kueri, tetapkan `SortingConfiguration` parameter Query API. Tentukan nama atribut yang akan diurutkan dan apakah akan mengurutkan respons dalam urutan naik atau menurun.

   Contoh JSON berikut menunjukkan parameter `SortingConfiguration` yang Anda gunakan untuk mengurutkan hasil kueri dengan atribut “Departemen” dalam urutan naik.

```
   "SortingConfiguration": {
      "DocumentAttributeKey": "Department",
      "SortOrder": "ASC"
   }
```

3. Untuk menggunakan lebih dari satu atribut yang dapat diurutkan dalam kueri, tetapkan `SortingConfigurations` parameter Query API. Anda dapat mengatur hingga 3 bidang yang Amazon Kendra harus mengurutkan hasilnya. Anda juga dapat menentukan apakah hasilnya harus diurutkan dalam urutan naik atau turun. Kuota bidang sortir dapat ditingkatkan.

   Jika Anda tidak menyediakan konfigurasi penyortiran, hasilnya diurutkan berdasarkan relevansi yang Amazon Kendra menentukan hasilnya. Jika ada seri dalam mengurutkan hasil, hasilnya diurutkan berdasarkan relevansi.

   Contoh JSON berikut menunjukkan `SortingConfigurations` parameter yang Anda gunakan untuk mengurutkan hasil kueri berdasarkan atribut “Nama” dan “Harga” dalam urutan menaik.

```
"CollapseConfiguration" : {
    "DocumentAttributeKey": "Name",
    "SortingConfigurations": [
        {
            "DocumentAttributeKey": "Price",
            "SortOrder": "ASC"
        }
    ],
    "MissingAttributeKeyStrategy": "IGNORE"
```

```
}
```

Untuk mengurutkan hasil dokumen (konsol)

> **Note**
>
> Pengurutan multi-atribut saat ini tidak didukung oleh. AWS Management Console

1. Untuk membuat atribut diurutkan di konsol, pilih Dapat disortir dalam definisi atribut. Anda dapat membuat atribut dapat disortir ketika Anda membuat atribut, atau Anda dapat memodifikasinya nanti.
2. Untuk mengurutkan respons kueri di konsol, pilih atribut untuk mengurutkan respons dari menu Sortir. Hanya atribut yang ditandai dapat diurutkan selama konfigurasi sumber data yang muncul dalam daftar.

Meruntuhkan/memperluas hasil kueri

Saat Anda tersambung Amazon Kendra ke data, data akan merayapi atribut metadata dokumen — seperti `_document_title`, `_created_at`, dan `_document_id` —dan menggunakan atribut atau bidang ini untuk menyediakan kemampuan penelusuran lanjutan selama waktu kueri.

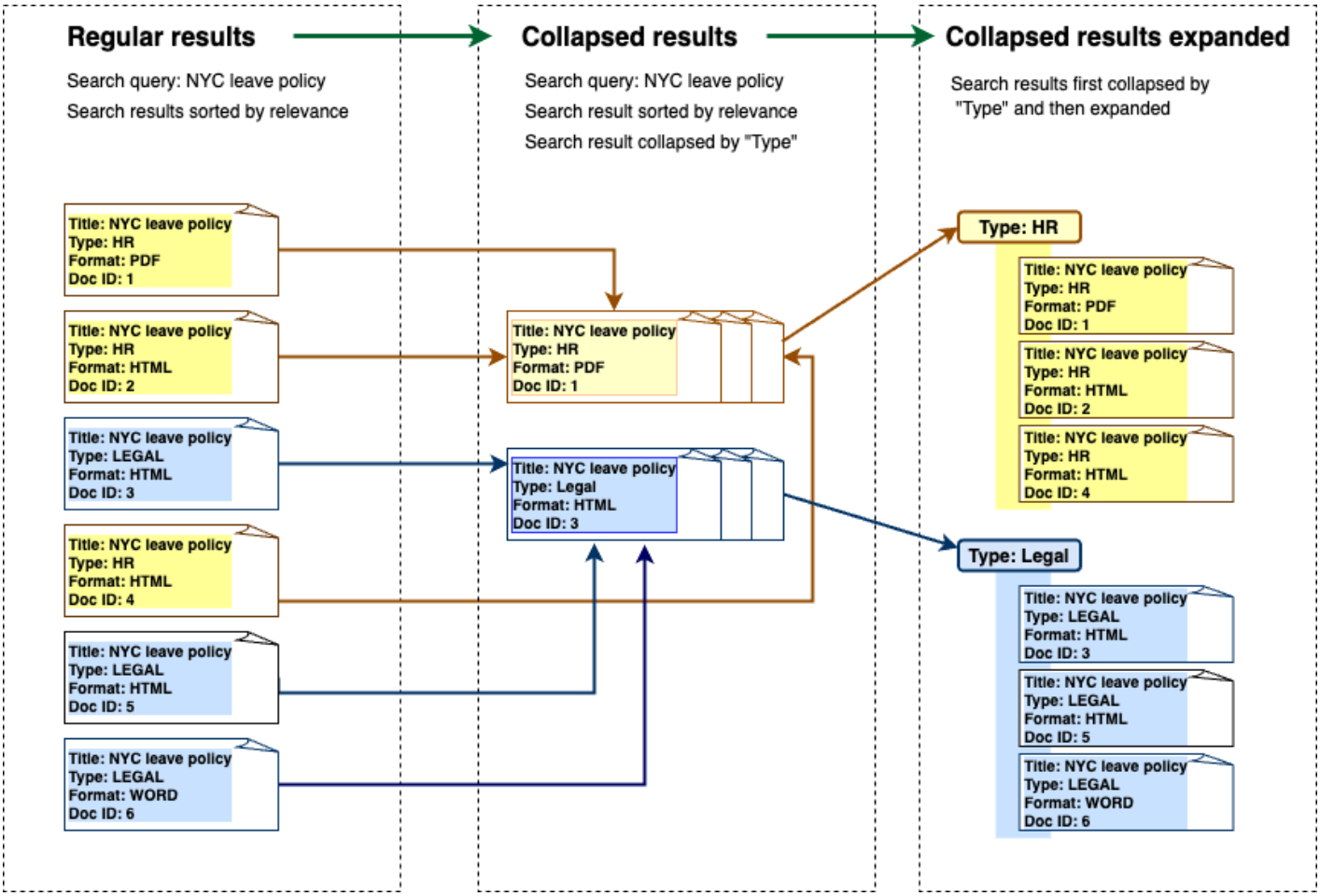
Amazon Kendra Fitur Ciutkan dan perluas hasil kueri memungkinkan Anda mengelompokkan hasil penelusuran menggunakan atribut dokumen umum dan menampilkannya—baik diciutkan atau diperluas sebagian—di bawah dokumen utama yang ditunjuk.

> **Note**
>
> Fitur runtuhkan dan perluas hasil kueri saat ini hanya tersedia melalui Amazon Kendra API.

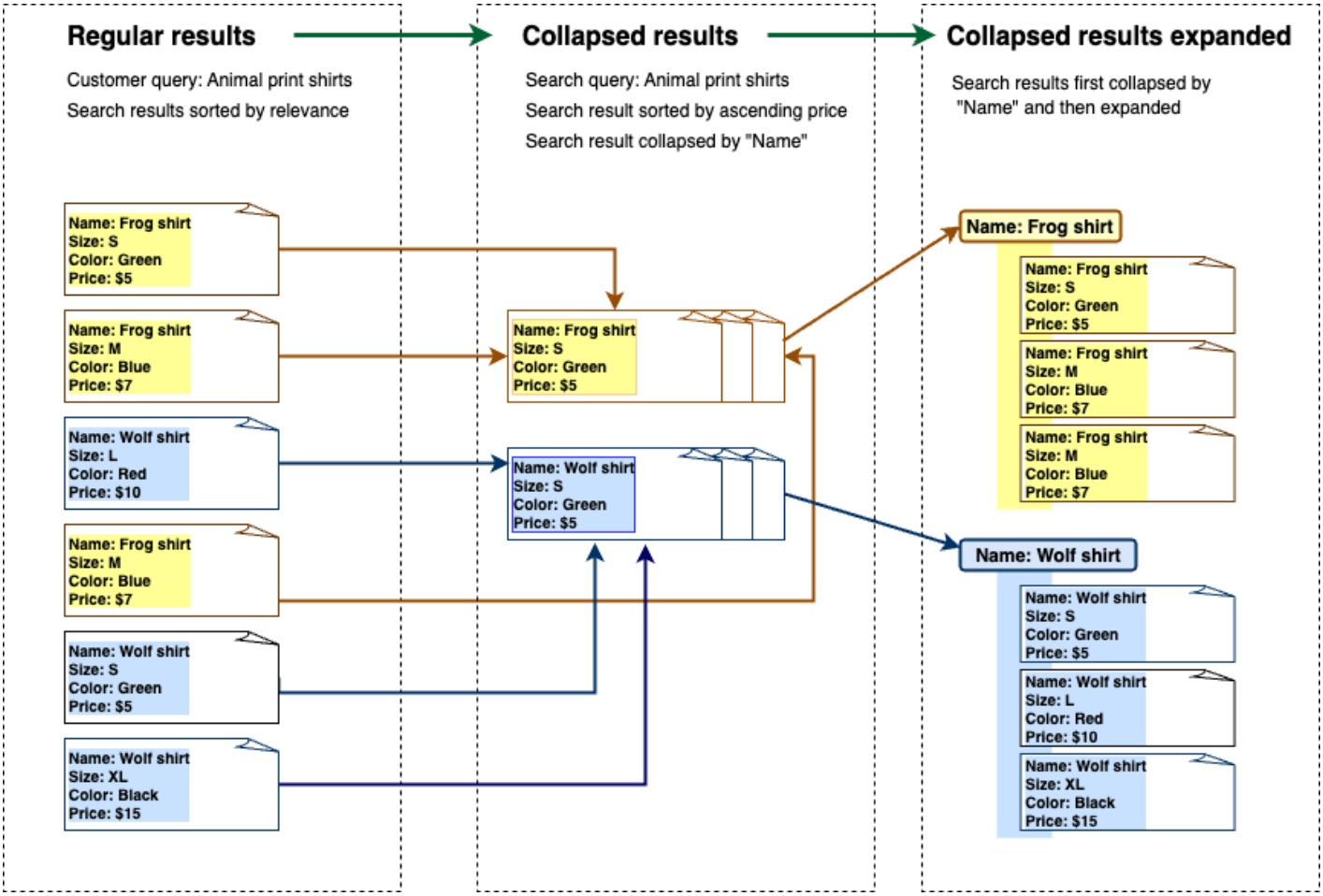
Ini berguna dalam jenis situasi pencarian berikut:

- Beberapa versi konten ada dalam dokumen dalam indeks Anda. Saat pengguna akhir Anda menanyakan indeks, Anda ingin mereka melihat versi dokumen yang paling relevan dengan duplikat tersembunyi/diciutkan. Misalnya, jika indeks Anda berisi beberapa versi dokumen bernama

"Kebijakan cuti NYC", Anda dapat memilih untuk menciutkan dokumen untuk grup tertentu "HR" dan "Legal" menggunakan atribut/bidang "Jenis".



- Indeks Anda berisi beberapa dokumen dengan informasi unik tentang satu jenis item atau objek, seperti inventaris produk, misalnya. Untuk menangkap dan mengurutkan informasi item dengan mudah, Anda ingin pengguna akhir mengakses semua dokumen yang ditautkan oleh item atau objek sebagai satu hasil pencarian. Dalam contoh di bawah ini, pencarian pelanggan pada "kemeja cetak binatang" mengembalikan hasil yang dikelompokkan berdasarkan nama, dan diurutkan berdasarkan urutan harga naik.



Hasil runtuh

Untuk mengelompokkan dokumen serupa atau terkait bersama-sama, Anda harus menentukan atribut yang akan diciutkan (misalnya, Anda dapat menciutkan/mengelompokkan dokumen dengan). `_category` Untuk melakukan ini, panggil Query API dan gunakan CollapseConfigurationobjek untuk menentukan `DocumentAttributeKey` untuk runtuh. `DocumentAttributeKey`Kontrol di mana hasil pencarian bidang akan diciutkan. Bidang kunci atribut yang didukung termasuk `String` dan`Number`. `String list`dan `Date` jenis tidak didukung.

Memilih dokumen utama menggunakan urutan pengurutan

Untuk mengonfigurasi dokumen utama yang akan ditampilkan untuk grup yang diciutkan, Anda menggunakan `SortingConfigurations` parameter di bawah CollapseConfiguration. Misalnya, untuk mendapatkan versi terbaru dari dokumen, Anda akan mengurutkan setiap grup yang diciutkan berdasarkan`_version`. Anda dapat menentukan hingga 3 atribut/bidang untuk diurutkan berdasarkan dan urutan pengurutan untuk setiap atribut/bidang yang digunakan.

`SortingConfigurations` Anda dapat meminta peningkatan kuota untuk jumlah atribut pengurutan.

Secara default, Amazon Kendra urutkan respons kueri berdasarkan skor relevansi yang ditentukan untuk setiap hasil dalam respons. Untuk mengubah urutan pengurutan default, buat atribut dokumen dapat diurutkan dan kemudian konfigurasikan Amazon Kendra untuk menggunakan atribut ini untuk mengurutkan respons. Untuk informasi selengkapnya, lihat Mengurutkan tanggapan.

Strategi kunci dokumen yang hilang

Jika dokumen Anda tidak memiliki nilai atribut ciutkan, Amazon Kendra menawarkan tiga opsi penyesuaian:

- Pilih `COLLAPSE` semua dokumen dengan nilai nol atau hilang dalam satu grup. Ini adalah konfigurasi default.
- Pilih `IGNORE` dokumen dengan nilai nol atau hilang. Dokumen yang diabaikan tidak akan muncul dalam hasil kueri.
- Pilih untuk `EXPAND` setiap dokumen dengan nilai nol atau hilang ke dalam grupnya sendiri.

Memperluas hasil

Anda dapat memilih apakah grup hasil pencarian yang diciutkan diperluas menggunakan `Expand` parameter di CollapseConfigurationobjek. Hasil yang diperluas mempertahankan urutan pengurutan yang sama yang digunakan untuk memilih dokumen utama untuk grup.

Untuk mengonfigurasi jumlah grup hasil pencarian yang diciutkan untuk diperluas, Anda menggunakan `MaxResultItemstoExpand` parameter dalam ExpandConfigurationobjek. Jika Anda menetapkan nilai ini ke 10, misalnya, hanya 10 dari 100 grup hasil pertama yang akan memiliki fungsionalitas yang diperluas.

Untuk mengonfigurasi jumlah hasil yang diperluas untuk ditampilkan per dokumen utama yang diciutkan, gunakan `MaxExpandResultsPerItem` parameter. Misalnya, jika Anda menetapkan nilai ini ke 3, maka paling banyak 3 hasil per grup yang diciutkan akan ditampilkan.

Interaksi dengan Amazon Kendra fitur lain

- Menciutkan dan memperluas hasil tidak mengubah jumlah aspek atau memengaruhi jumlah total hasil yang ditampilkan.

- Amazon Kendra hasil pencarian unggulan tidak akan diciutkan meskipun memiliki nilai bidang yang sama dengan bidang ciutkan yang Anda konfigurasikan.
- Runtuh dan perluasan hasil hanya berlaku untuk hasil tipe`DOCUMENT`.

Penyetelan relevansi pencarian

Amazon Kendra query menghasilkan hasil pencarian yang diberi peringkat berdasarkan relevansinya. Bidang atau atribut yang dapat dicari dalam indeks semua berkontribusi pada peringkat ini.

Anda dapat memodifikasi efek dari bidang atau atribut pada relevansi pencarian melalui penyetelan relevansi. Penyetelan relevansi pencarian dapat dilakukan secara manual pada tingkat indeks, di mana Anda mengatur konfigurasi penyetelan untuk indeks Anda, atau pada tingkat kueri dengan mengesampingkan konfigurasi yang ditetapkan pada tingkat indeks.

Saat Anda menggunakan penyetelan relevansi, hasil diberi peningkatan respons saat kueri menyertakan istilah yang cocok dengan bidang atau atribut. Anda juga menentukan berapa banyak dorongan yang diterima dokumen saat ada kecocokan. Penyetelan relevansi tidak Amazon Kendra menyebabkan menyertakan dokumen dalam respons kueri, itu hanya salah satu faktor yang Amazon Kendra digunakan untuk menentukan relevansi dokumen.

Anda dapat meningkatkan bidang atau atribut tertentu dalam indeks Anda untuk menetapkan lebih penting untuk tanggapan tertentu. Misalnya saat seseorang menelusuri "Kapan re:Invent?" Anda dapat meningkatkan relevansi kesegaran dokumen di lapangan. `_last_update_at` Atau, dalam indeks laporan penelitian, Anda dapat meningkatkan sumber data tertentu di bidang “sumber”.

Anda juga dapat meningkatkan dokumen berdasarkan suara atau jumlah tampilan yang umum di forum dan basis pengetahuan dukungan lainnya. Anda dapat menggabungkan dorongan, misalnya untuk mendorong dokumen yang dilihat lebih lama dan lebih baru.

Anda menetapkan jumlah dorongan yang diterima dokumen dengan menggunakan parameter `Importance`. Semakin tinggi `Importance`, semakin banyak bidang atau atribut yang meningkatkan relevansi dokumen. Saat Anda menyetel indeks atau menyetel pada tingkat kueri, tingkatkan nilai parameter `Importance` sedikit demi sedikit hingga Anda mendapatkan efek yang diinginkan. Untuk menentukan apakah Anda meningkatkan hasil penelusuran, lakukan penelusuran dan bandingkan hasilnya dengan kueri sebelumnya .

Anda dapat menentukan tanggal, nomor, atau atribut string untuk menyetel indeks atau lagu pada tingkat kueri. Anda dapat menyetel bidang atau atribut yang bertipe `StringList` hanya pada tingkat indeks. Setiap bidang atau atribut memiliki kriteria khusus untuk meningkatkan hasil.

- Bidang tanggal atau atribut —Ada tiga kriteria khusus untuk bidang tanggal,`Duration`, `Freshness` dan`RankOrder`.

- `Duration` menentukan jangka waktu berlakunya peningkatan. Misalnya, jika Anda menetapkan jangka waktu 86400 detik (yaitu satu hari), dorongan mulai berkurang setelah satu hari. Semakin tinggi kepentingannya, semakin cepat efek dorongannya berkurang.
- `Freshness` menentukan seberapa baru dokumen saat diterapkan ke bidang atau atribut. Jika Anda menerapkan `Freshness` ke salah satu bidang untuk tanggal dibuat atau tanggal terakhir diperbarui, maka dokumen yang lebih baru dibuat atau yang terakhir diperbarui dianggap "lebih segar" daripada dokumen yang lebih lama. Misalnya, jika dokumen 1 dibuat pada 14 November, dan dokumen 2 dibuat pada 5 November, dokumen 1 "lebih segar" daripada dokumen 2. Dan jika dokumen 1 terakhir diperbarui pada 14 November, dan dokumen 2 terakhir diperbarui pada 20 November, dokumen 2 "lebih segar" daripada dokumen 1. Semakin segar dokumen, semakin banyak dorongan ini diterapkan. Anda hanya dapat memiliki satu `Freshness` di indeks Anda.
- `RankOrder` menerapkan dorongan dalam urutan naik atau turun. Jika Anda menentukan `ASCENDING`, tanggal yang lebih baru akan didahulukan . Jika Anda menentukan `DESCENDING`, tanggal yang lebih awal akan didahulukan.

- Bidang atau atribut angka —Untuk bidang angka atau atribut, Anda dapat menentukan urutan peringkat yang Amazon Kendra harus digunakan saat menentukan relevansi bidang atau atribut. Jika Anda menentukan `ASCENDING`, maka angka yang lebih tinggi akan diutamakan. Jika Anda menentukan `DESCENDING`, maka angka yang lebih rendah didahulukan.
- Bidang atau atribut string —Untuk bidang atau atribut string, Anda dapat membuat kategori bidang untuk memberikan dorongan berbeda pada setiap kategori. Misalnya, jika Anda mendorong bidang atau atribut yang disebut "Departemen", Anda dapat memberikan dorongan yang berbeda untuk dokumen dari "HR" daripada ke dokumen dari "Legal". Anda dapat meningkatkan bidang atau atribut dari jenis tersebut`String`. Anda dapat meningkatkan `StringList` bidang hanya pada tingkat indeks.

penyetelan relevansi pada tingkat indeks

Anda menyetel relevansi bidang atau atribut pada tingkat indeks dengan menggunakan konsol untuk menyetel penyetelan pada detail indeks atau API. UpdateIndex

Contoh berikut menetapkan `_last_updated_at` bidang sebagai `Freshness` bidang untuk dokumen.

```
"DocumentMetadataConfigurationUpdates" : [
    {
        "Name": "_last_updated_at",
```

```
        "Type": "DATE_VALUE",
        "Relevance": {
            "Freshness": TRUE,
            "Importance": 2
        }
    }
]
```

Contoh berikut menerapkan kepentingan yang berbeda untuk kategori yang berbeda di bidang "departemen".

```
"DocumentMetadataConfigurationUpdates" : [
    {
        "Name": "department",
        "Type": "STRING_VALUE",
        "Relevance": {
            "Importance": 2,
            "ValueImportanceMap": {
                "HR": 3,
                "Legal": 1
            }
        }
    }
]
```

penyetelan relevansi pada tingkat kueri

Anda menyetel relevansi bidang atau atribut pada tingkat kueri dengan menggunakan Query API.

Penyetelan relevansi di tingkat kueri tidak didukung di konsol.

Penyetelan pada tingkat kueri dapat mempercepat proses pengujian penyetelan relevansi karena Anda tidak perlu memperbarui konfigurasi penyetelan secara manual dalam indeks untuk setiap pengujian. Anda dapat menyetel relevansi dokumen dengan meneruskan konfigurasi penyetelan dalam kueri. Kemudian Anda dapat melihat hasil yang berbeda yang Anda dapatkan dari konfigurasi yang berbeda. Konfigurasi yang dilewatkan dalam kueri menimpa konfigurasi yang ditetapkan pada tingkat indeks.

Contoh berikut mengesampingkan pentingnya diterapkan pada bidang "departemen" dan setiap kategori departemen ditetapkan pada tingkat indeks, yang ditunjukkan pada contoh di atas.

Saat pengguna memasukkan kueri penelusuran mereka, bidang "departemen" memiliki tingkat kepentingan yang wajar dan departemen Legal lebih penting daripada departemen SDM .

```
"DocumentRelevanceOverrideConfigurations" : [
    {
        "Name": "department",
        "Type": "STRING_VALUE",
        "Relevance": {
            "Importance": 2,
            "ValueImportanceMap": {
                "HR": 2,
                "Legal": 8
            }
        }
    }
]
```

Mendapatkan wawasan dengan analitik penelusuran

Anda dapat menggunakan Analytics Amazon Kendra penelusuran untuk mendapatkan wawasan tentang bagaimana aplikasi penelusuran berhasil atau tidak berhasil membantu pengguna menemukan informasi.

Amazon Kendra Analytics memberikan gambaran tentang bagaimana pengguna Anda berinteraksi dengan aplikasi penelusuran Anda dan seberapa efektif konfigurasi aplikasi penelusuran Anda. Anda dapat melihat data metrik menggunakan GetSnapshotsAPI atau dengan memilih Analytics pada panel navigasi di konsol.

Anda dapat merender data yang dihasilkan `GetSnapshots` di dasbor yang dibuat khusus Anda sendiri. Atau Anda dapat menggunakan dasbor metrik yang disediakan di konsol, yang mencakup grafik visual. Dengan dasbor visual, Anda dapat mencari tren atau pola perilaku pengguna dari waktu ke waktu atau masalah permukaan dengan konfigurasi aplikasi pencarian Anda. Misalnya, grafik garis yang menunjukkan jumlah kueri yang konsisten per hari dan peningkatan yang stabil mungkin menunjukkan peningkatan adopsi dan penggunaan. Di sisi lain, penurunan mendadak mungkin mengindikasikan ada masalah yang harus diselidiki.

Anda dapat menggunakan metrik untuk membuat koneksi antara berbagai titik data untuk memecahkan masalah dengan cara pengguna Anda meminta informasi atau menemukan peluang bisnis. Misalnya, dokumen 'Bagaimana cara kerja AI? ' adalah dokumen yang paling banyak diklik dalam hasil pencarian, dan kueri pencarian teratas adalah 'Bagaimana cara kerja pembelajaran mesin? '. Ini memberi tahu Anda tentang istilah dan bahasa pilihan yang digunakan pengguna Anda. Anda dapat mengintegrasikan istilah-istilah ini dalam dokumen Anda atau menggunakan sinonim khusus untuk istilah ini agar dokumen Anda lebih mudah dicari bagi pengguna Anda.

Metrik untuk pencarian

Ada 10 metrik untuk menganalisis kinerja aplikasi pencarian Anda atau informasi apa yang dicari pengguna Anda. Untuk mengambil data metrik, Anda menentukan nama string dari data metrik yang ingin Anda ambil saat Anda memanggil. `GetSnapshots`

Anda juga harus menyediakan interval waktu atau jendela waktu untuk melihat data metrik. Interval waktu menggunakan zona waktu indeks Anda. Anda dapat melihat data di jendela waktu berikut:

- `THIS_WEEK`: Minggu ini, dimulai pada hari Minggu dan berakhir pada hari sebelum tanggal saat ini.

- `ONE_WEEK_AGO`: Minggu sebelumnya, dimulai pada hari Minggu dan berakhir pada hari Sabtu berikutnya.
- `TWO_WEEKS_AGO`: Minggu sebelum minggu sebelumnya, dimulai pada hari Minggu dan berakhir pada hari Sabtu berikutnya.
- `THIS_MONTH`: Bulan berjalan, dimulai pada hari pertama bulan itu dan berakhir pada hari sebelum tanggal saat ini.
- `ONE_MONTH_AGO`: Bulan sebelumnya, dimulai pada hari pertama bulan itu dan berakhir pada hari terakhir bulan itu.
- `TWO_MONTHS_AGO`: Bulan sebelum bulan sebelumnya, dimulai pada hari pertama bulan itu dan berakhir pada hari terakhir bulan itu.

Di konsol, jendela waktu yang didukung adalah Minggu ini, Minggu sebelumnya, Bulan ini, Bulan sebelumnya.

Rasio klik-tayang

Proporsi kueri yang mengarah ke klik-tayang ke dokumen dalam hasil pencarian. Ini membantu Anda memahami apakah konfigurasi aplikasi penelusuran membantu pengguna menemukan informasi yang relevan dengan kueri mereka. Untuk pertanyaan yang mengembalikan jawaban instan, pengguna mungkin tidak perlu mengklik dokumen untuk informasi lebih lanjut. Untuk informasi selengkapnya, lihat the section called “Tingkat jawaban instan”. Anda harus menelepon SubmitFeedbackuntuk memastikan bahwa umpan balik klik-tayang dikumpulkan.

Untuk mengambil data pada rasio klik-tayang menggunakan `GetSnapshots` API, tentukan sebagai. `metricType` `AGG_QUERY_DOC_METRICS` Anda juga dapat melihat metrik ini di konsol dengan memilih Analytics pada panel navigasi.

Tingkat klik nol

Proporsi kueri yang mengarah ke nol klik dalam hasil pencarian. Ini membantu Anda memahami kesenjangan dalam konten Anda yang memberikan hasil penelusuran yang tidak relevan. Untuk pertanyaan yang mengembalikan jawaban instan, pengguna mungkin tidak perlu mengklik dokumen untuk informasi lebih lanjut. Untuk informasi selengkapnya, lihat the section called “Tingkat jawaban instan”. Selain itu, pengaturan penelusuran Anda, seperti konfigurasi penyetelan, dapat berdampak pada bagaimana dokumen dikembalikan dalam hasil penelusuran.

Untuk mengambil data pada tingkat klik nol menggunakan `GetSnapshots` API, tentukan `metricType` sebagai`AGG_QUERY_DOC_METRICS`. Anda juga dapat melihat metrik ini di konsol dengan memilih Analytics pada panel navigasi.

Tingkat hasil pencarian nol

Proporsi kueri yang mengarah ke nol hasil pencarian. Ini membantu Anda memahami kesenjangan dalam konten Anda tanpa memberikan hasil penelusuran yang relevan.

Untuk mengambil data pada tingkat hasil pencarian nol menggunakan `GetSnapshots` API, tentukan `metricType` sebagai`AGG_QUERY_DOC_METRICS`. Anda juga dapat melihat metrik ini di konsol dengan memilih Analytics pada panel navigasi.

Tingkat jawaban instan

Proporsi pertanyaan dengan jawaban instan atau FAQ dikembalikan. Ini membantu Anda memahami peran jawaban instan dalam memberikan informasi.

Untuk mengambil data pada tingkat jawaban instan menggunakan `GetSnapshots` API, tentukan `metricType` sebagai`AGG_QUERY_DOC_METRICS`. Anda juga dapat melihat metrik ini di konsol dengan memilih Analytics pada panel navigasi.

Kueri teratas

100 kueri teratas yang dicari oleh pengguna Anda. Ini membantu Anda memahami kueri mana yang populer dan jenis informasi yang paling diminati pengguna Anda.

Metrik mencakup berapa kali kueri dicari, proporsi klik-tayang ke dokumen, proporsi tidak ada klik-tayang ke dokumen, kedalaman klik rata-rata dalam hasil pencarian untuk kueri, proporsi jawaban instan untuk kueri, dan kepercayaan rata-rata untuk 10 hasil pencarian pertama untuk kueri.

Untuk mengambil data pada kueri teratas menggunakan `GetSnapshots` API, tentukan sebagai. `metricType` `QUERIES_BY_COUNT` Anda juga dapat melihat metrik ini di konsol dengan memilih Analytics pada panel navigasi di konsol, lalu memilih Kueri teratas di bawah Daftar kueri.

Kueri teratas dengan nol klik

100 kueri teratas yang mengarah ke nol klik di hasil pencarian. Ini membantu Anda memahami kesenjangan dalam konten Anda, di mana ada kekurangan dokumen yang relevan dengan beberapa kueri atau konfigurasi aplikasi pencarian Anda mengembalikan hasil penelusuran yang tidak relevan.

Untuk pertanyaan yang mengembalikan jawaban instan, pengguna mungkin tidak perlu mengklik dokumen untuk informasi lebih lanjut. Untuk informasi selengkapnya, lihat the section called “Tingkat jawaban instan”.

Metrik mencakup berapa kali kueri mengarah ke nol klik, proporsi nol klik untuk kueri, proporsi jawaban instan untuk kueri, dan kepercayaan rata-rata untuk 10 hasil pencarian pertama untuk kueri.

Untuk mengambil data pada kueri teratas dengan nol klik menggunakan `GetSnapshots` API, tentukan sebagai. `metricType` `QUERIES_BY_ZERO_CLICK_RATE` Anda juga dapat melihat metrik ini di konsol dengan memilih Analytics pada panel navigasi di konsol, lalu memilih Kueri klik nol teratas di bawah Daftar kueri.

Kueri teratas dengan hasil pencarian nol

100 kueri teratas yang mengarah ke nol hasil pencarian. Ini membantu Anda memahami kesenjangan dalam konten Anda, di mana tidak ada dokumen yang relevan dengan beberapa pertanyaan. Atau, pengguna Anda mungkin menanyakan dengan istilah khusus yang mungkin menyebabkan tidak ada hasil penelusuran, mendorong Anda untuk membuat sinonim khusus untuk menangani hal ini.

Metrik mencakup berapa kali kueri mengarah ke hasil pencarian nol, proporsi hasil pencarian nol untuk kueri, dan proporsi kali kueri dicari dibandingkan dengan semua kueri.

Untuk mengambil data pada kueri teratas dengan hasil pencarian nol menggunakan `GetSnapshots` API, tentukan sebagai. `metricType` `QUERIES_BY_ZERO_RESULT_RATE` Anda juga dapat melihat metrik ini di konsol dengan memilih Analytics pada panel navigasi di konsol, lalu memilih Kueri hasil nol teratas di bawah Daftar kueri.

Teratas diklik pada dokumen

100 dokumen teratas yang paling banyak diklik dalam hasil pencarian. Ini membantu Anda memahami dokumen atau hasil penelusuran mana yang paling relevan bagi pengguna Anda saat mereka meminta informasi.

Metrik mencakup berapa kali dokumen diklik, jumlah suka yang diterima dokumen dari pengguna Anda (jempol ke atas), jumlah tidak suka yang diterima dokumen dari pengguna Anda (jempol ke bawah).

Untuk mengambil data di atas diklik pada dokumen menggunakan `GetSnapshots` API, tentukan sebagai. `metricType` `DOCS_BY_CLICK_COUNT` Anda juga dapat melihat metrik ini di konsol dengan

memilih Analytics pada panel navigasi di konsol, lalu memilih Dokumen yang diklik teratas di bawah Daftar kueri.

Total kueri

Jumlah total kueri yang dicari oleh pengguna Anda. Ini membantu Anda memahami seberapa terlibat pengguna Anda dengan aplikasi pencarian Anda.

Untuk mengambil data pada total kueri menggunakan `GetSnapshots` API, tentukan sebagai. `metricType` `AGG_QUERY_DOC_METRICS` Anda juga dapat melihat metrik ini di konsol dengan memilih Analytics pada panel navigasi.

Total dokumen

Jumlah total dokumen dalam indeks Anda. Ini membantu Anda membandingkan ukuran indeks Anda dengan jumlah total kueri untuk memeriksa apakah ada jumlah dokumen yang sesuai untuk volume kueri.

Untuk mengambil data pada total dokumen menggunakan `GetSnapshots` API, tentukan `metricType` sebagai`AGG_QUERY_DOC_METRICS`. Anda juga dapat melihat metrik ini di konsol dengan memilih Analytics pada panel navigasi.

Contoh pengambilan data metrik

Kode berikut adalah contoh pengambilan data pada kueri teratas untuk bulan sebelumnya.

Console

Untuk mengambil kueri teratas untuk bulan sebelumnya

1. Di panel navigasi kiri, di bawah Indeks, pilih indeks Anda, lalu pilih Analytics.
2. Pada halaman Analytics, pilih tombol Minggu ini, untuk mengubah jendela waktu untuk mengambil data ke Bulan sebelumnya.
3. Pada halaman Analytics, di bawah Daftar kueri, pilih Kueri teratas.

CLI

Untuk mengambil kueri teratas untuk bulan sebelumnya

```
aws kendra get-snapshots \
```

```
--index-id index-id \
--interval "ONE_MONTH_AGO" \
--metric-type "QUERIES_BY_COUNT"
```

Python

Untuk mengambil kueri teratas untuk bulan sebelumnya

```
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

Untuk mengambil kueri teratas untuk bulan sebelumnya

```
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()))
```

Dari metrik hingga wawasan yang dapat ditindaklanjuti

Wawasan yang dapat ditindaklanjuti adalah potongan informasi bermakna yang diambil dari data mentah dan digunakan untuk memandu tindakan atau keputusan Anda. Untuk mengekstrak makna dari metrik dan menggunakannya untuk mendorong wawasan yang dapat ditindaklanjuti, penting untuk tidak hanya melihat metrik secara terpisah tetapi juga membuat koneksi di antara metrik.

Misalnya, kueri teratas dengan nol klik adalah 'Wilayah mana yang saat ini tersedia? '. Namun, ia juga memiliki tingkat jawaban instan 100 persen. Ini menunjukkan pengguna Anda menerima jawaban atas pertanyaan ini tanpa perlu mengklik hasil pencarian atau dokumen yang memberikan informasi tentang wilayah yang tersedia. Jika Anda melihat nol klik saja, Anda tidak akan mendapatkan cerita lengkap dan mungkin membuat kesimpulan yang salah tentang keberhasilan konfigurasi aplikasi pencarian Anda dalam menangani kueri ini.

Contoh lain dari wawasan yang dapat ditindaklanjuti adalah menemukan peluang bisnis. Bisnis sering mencari peluang untuk menumbuhkan pelanggan mereka dengan menganalisis metrik pencarian. Dokumen yang paling banyak diklik adalah 'Wilayah yang tersedia'. Selain itu, sebagian besar permintaan pencarian teratas terkait dengan pertanyaan tentang ketersediaan produk di wilayah Oseanik, dengan tingkat jawaban instan 100 persen dan rasio klik-tayang tinggi untuk informasi lebih lanjut tentang wilayah yang tersedia sebagai bagian dari jawaban. Ini berarti ada minat dan permintaan untuk produk atau layanan Anda di wilayah ini.

Memvisualisasikan dan melaporkan analitik penelusuran

Ada lima metrik yang mencakup data tren bagi Anda untuk memvisualisasikan dan mencari tren atau pola dari waktu ke waktu. Jika Anda menggunakan konsol, grafik data tren disediakan. Jika Anda menggunakan API, Anda dapat mengambil data tren untuk membuat grafik atau visualisasi Anda

sendiri. Sebagian besar grafik di konsol memplot titik data harian di atas jendela waktu yang Anda pilih.

Konsol menyediakan dasbor metrik tempat Anda dapat memilih grafik dan daftar teratas yang ingin Anda lihat. Anda dapat mengekspor metrik yang ditampilkan di dasbor Anda dalam format CSV dengan memilih Ekspor di halaman beranda Analytics. Anda dapat memasukkan laporan ini dalam dokumen atau presentasi bisnis Anda.

Anda dapat memvisualisasikan metrik berikut:

Grafik total kueri

Grafik garis dari jumlah kueri yang dikeluarkan per hari. Grafik membantu Anda memvisualisasikan pola dalam keterlibatan pengguna harian. Beberapa contoh termasuk peningkatan atau penurunan keterlibatan pengguna yang stabil, atau penurunan drastis ke 0 kueri karena crash aplikasi pencarian Anda atau masalah dengan situs web Anda.

Jika Anda menggunakan API, Anda dapat mengambil data ini dengan menentukan`TREND_QUERY_DOC_METRICS`. Anda dapat menggunakan data untuk membuat grafik Anda sendiri, atau menggunakan grafik yang disediakan di konsol.

Grafik rasio klik-tayang

Grafik garis proporsi klik-tayang per hari. Grafik membantu Anda memvisualisasikan pola dalam rasio klik-tayang harian. Beberapa contoh termasuk peningkatan atau penurunan rasio klik-tayang yang stabil, atau penurunan jawaban instan yang mungkin memengaruhi peningkatan klik-tayang.

Jika Anda menggunakan API, Anda dapat mengambil data ini dengan menentukan`TREND_QUERY_DOC_METRICS`. Anda dapat menggunakan data untuk membuat grafik Anda sendiri, atau menggunakan grafik yang disediakan di konsol.

Grafik tingkat klik nol

Grafik garis proporsi nol klik per hari. Grafik membantu Anda memvisualisasikan pola dalam tingkat klik nol harian. Beberapa contoh termasuk peningkatan atau penurunan tingkat klik nol yang stabil, atau peningkatan jawaban instan yang mungkin memengaruhi peningkatan nol klik.

Jika Anda menggunakan API, Anda dapat mengambil data ini dengan menentukan`TREND_QUERY_DOC_METRICS`. Anda dapat menggunakan data untuk membuat grafik Anda sendiri, atau menggunakan grafik yang disediakan di konsol.

Grafik tingkat hasil pencarian nol

Grafik garis proporsi hasil pencarian nol per hari. Grafik membantu Anda memvisualisasikan pola dalam tingkat hasil pencarian nol harian. Beberapa contoh termasuk peningkatan atau penurunan yang stabil dalam tingkat hasil pencarian nol, atau penurunan tajam dalam jumlah dokumen dalam indeks Anda yang mungkin memengaruhi peningkatan hasil pencarian nol.

Jika Anda menggunakan API, Anda dapat mengambil data ini dengan menentukan`TREND_QUERY_DOC_METRICS`. Anda dapat menggunakan data untuk membuat grafik Anda sendiri, atau menggunakan grafik yang disediakan di konsol.

Grafik tingkat jawaban instan

Grafik garis proporsi kueri dengan jawaban instan atau FAQ dikembalikan. Grafik membantu Anda memvisualisasikan pola dalam tingkat jawaban instan harian. Beberapa contoh termasuk peningkatan atau penurunan yang stabil dalam kueri jenis tanya jawab, atau penurunan klik-tayang yang mungkin mempengaruhi peningkatan jawaban instan.

Jika Anda menggunakan API, Anda dapat mengambil data ini dengan menentukan`TREND_QUERY_DOC_METRICS`. Anda dapat menggunakan data untuk membuat grafik Anda sendiri, atau menggunakan grafik yang disediakan di konsol.

Mengirimkan umpan balik untuk pembelajaran tambahan

Amazon Kendra menggunakan pembelajaran inkremental untuk meningkatkan hasil pencarian. Menggunakan umpan balik dari kueri, pembelajaran tambahan meningkatkan algoritme peringkat dan mengoptimalkan hasil penelusuran untuk akurasi yang lebih tinggi.

Misalnya, anggaplah pengguna Anda mencari frasa “manfaat perawatan kesehatan”. Jika pengguna secara konsisten memilih hasil kedua dari daftar, seiring waktu Amazon Kendra meningkatkan hasil itu ke hasil tempat pertama. Dorongan berkurang dari waktu ke waktu, jadi jika pengguna berhenti memilih hasil, Amazon Kendra akhirnya menghapusnya dan menunjukkan hasil lain yang lebih populer sebagai gantinya. Ini membantu Amazon Kendra memprioritaskan hasil berdasarkan relevansi, usia, dan konten.

Pembelajaran tambahan diaktifkan untuk semua indeks dan untuk semua jenis dokumen yang didukung.

Amazon Kendra mulai belajar segera setelah Anda memberikan umpan balik, meskipun dapat memakan waktu lebih dari 24 jam untuk melihat hasil umpan balik. Amazon Kendra menyediakan tiga metode bagi Anda untuk mengirimkan umpan balik: AWS konsol, JavaScript pustaka yang dapat Anda sertakan di halaman hasil penelusuran, dan API yang dapat Anda gunakan.

Amazon Kendra menerima dua jenis umpan balik pengguna:

- Klik —Informasi tentang hasil kueri yang dipilih pengguna. Umpan balik mencakup ID hasil dan timestamp Unix dari tanggal dan waktu di mana hasil pencarian dipilih.

  Untuk mengirimkan umpan balik klik, aplikasi Anda harus mengumpulkan informasi klik dari aktivitas pengguna Anda, dan kemudian mengirimkan informasi itu ke Amazon Kendra. Anda dapat mengumpulkan informasi klik dengan konsol, JavaScript perpustakaan, dan Amazon Kendra API.
- Relevansi — Informasi tentang relevansi hasil pencarian, yang biasanya disediakan pengguna. Umpan balik berisi ID hasil dan indikator relevansi (`RELEVANT` atau `NOT_RELEVANT`). Pengguna menentukan informasi relevansi.

  Untuk mengirimkan umpan balik relevansi, aplikasi Anda harus menyediakan mekanisme umpan balik yang memungkinkan pengguna untuk memilih relevansi yang sesuai untuk hasil kueri, dan kemudian mengirimkan informasi tersebut ke. Amazon Kendra Anda hanya dapat mengumpulkan informasi relevansi dengan konsol dan Amazon Kendra API.

Umpan balik digunakan saat indeks aktif. Umpan balik hanya mempengaruhi indeks yang dikirimi, tidak dapat digunakan di seluruh indeks atau untuk akun yang berbeda.

Anda harus memberikan konteks pengguna tambahan saat Anda menanyakan Amazon Kendra indeks Anda. Ketika Anda memberikan konteks pengguna, Amazon Kendra dapat mengetahui apakah umpan balik diberikan oleh satu pengguna atau oleh beberapa pengguna dan menyesuaikan hasil pencarian yang sesuai.

Ketika Anda memberikan konteks pengguna, umpan balik untuk kueri dikaitkan dengan pengguna tertentu yang disediakan dalam konteks. Jika Anda tidak menentukan konteks pengguna, Anda dapat memberikan ID pengunjung yang digunakan untuk kueri grup dan agregat.

Jika Anda tidak memberikan konteks pengguna atau ID pengunjung, umpan balik tersebut anonim dan dikumpulkan dengan umpan balik anonim lainnya.

Kode berikut menunjukkan bagaimana untuk memasukkan konteks pengguna sebagai token atau ID pengunjung.

```
response = kendra.query(
    QueryText = query,
    IndexId = index,
    UserToken = {
        Token = "token"
    })

    OR

    response = kendra.query(
    QueryText = query,
    IndexId = index,
    VisitorId = "visitor-id")
```

Untuk aplikasi web, Anda dapat menggunakan cookie, lokasi, atau pengguna browser untuk menghasilkan ID pengunjung untuk setiap pengguna.

Untuk kueri utama, volume kueri terbesar, memberikan umpan balik klik-tayang memberikan informasi yang cukup untuk meningkatkan akurasi secara keseluruhan. Untuk kueri ekor yang jarang, ahli materi pelajaran harus mengirimkan umpan balik yang relevan dan tidak relevan untuk meningkatkan akurasi kueri tersebut.

Selain konsol, Anda dapat menggunakan salah satu dari dua metode: JavaScript perpustakaan atau SubmitFeedbackAPI. Anda hanya harus menggunakan satu metode pengumpulan umpan balik.

Untuk hasil terbaik, Anda harus mengirimkan umpan balik dalam waktu 24 jam setelah membuat kueri.

Topik

- Menggunakan Amazon Kendra JavaScript perpustakaan untuk mengirimkan umpan balik
- Menggunakan Amazon Kendra API untuk mengirimkan umpan balik

Menggunakan Amazon Kendra JavaScript perpustakaan untuk mengirimkan umpan balik

Amazon Kendra menyediakan JavaScript pustaka yang dapat Anda gunakan untuk menambahkan umpan balik klik ke halaman hasil pencarian Anda. Untuk menggunakan pustaka, Anda menyisipkan tanda skrip dalam kode klien Anda yang menampilkan hasil pencarian, lalu menambahkan informasi ke setiap tautan dokumen di daftar hasil Anda. Saat pengguna memilih tautan untuk melihat dokumen, klik informasi dikirim ke Amazon Kendra.

Pustaka bekerja dengan browser yang mendukung JavaScript versi ES6/ES2015.

Langkah 1: Masukkan tag skrip ke dalam aplikasi Amazon Kendra pencarian Anda

Dalam kode klien Anda yang merender hasil Amazon Kendra pencarian, masukkan <script>tag dan tambahkan referensi ke JavaScript pustaka:

```
<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>
```

Skrip secara asinkron mengunduh JavaScript pustaka dari CDN yang Amazon Kendra dihosting dan menginisialisasi variabel global yang disebut `kendraFeedback` yang memungkinkan Anda mengatur parameter opsional.

Ganti *URL unduhan pustaka* dan *titik akhir umpan balik* dengan pengenal dari tabel berikut berdasarkan wilayah yang menghosting indeks Anda Amazon Kendra .

Wilayah	Unduh URL	Titik akhir umpan balik
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://d2iezfpnpcoujy.cloudfront.net/ksf-v1.js	https://wg6nim909c.execute-api.us-west-2.amazonaws.com/prod/submit
ca-central-1	https://d1zbkfomowykaq.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

Wilayah	Unduh URL	Titik akhir umpan balik
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

Misalnya, jika indeks Anda di US East (N. Virginia), *URL unduh pustaka* adalah `https://d2zm0lpns956f8.cloudfront.net/ksf-v1.js` dan *titik akhir umpan balik* adalah `https://ujxwp5s92h.execute-api.us-east-1.amazonaws.com/prod/submit`.

Ada dua pengaturan opsional yang dapat Anda buat untuk Amazon Kendra JavaScript perpustakaan:

- `disableCookies`— Secara default, Amazon Kendra menetapkan cookie yang secara unik mengidentifikasi pengguna. Atur ini ke `true` untuk menonaktifkan cookie.

  ```
  kendraFeedback('disableCookie', 'true | false');
  ```

  `searchDivClassName`— Secara default, Amazon Kendra memantau semua tautan di halaman hasil pencarian Anda untuk klik. Atur ini ke nama kelas `<div>` untuk hanya memantau tautan di kelas tertentu.

  ```
  kendraFeedback('searchDivClassName', 'class name');
  ```

Langkah 2: Tambahkan token umpan balik ke hasil pencarian

Di halaman hasil Anda, tambahkan atribut HTML yang dipanggil `data-kendra-token` ke tanda jangkar atau tanda induk langsung div yang berisi tautan ke dokumen dari respons kueri. Sebagai contoh:

```
<a href="document location" data-kendra-token="feedback token value"></a>
OR
<div data-url="document location" data-kendra-token="feedback token value"></div>
```

Sebuah respons kueri berisi token di bidang `feedbackToken`. Token unik mengidentifikasi respons jika pengguna memilihnya. Menetapkan nilai token ke atribut `data-kendra-token`. Amazon Kendra JavaScript Pustaka mencari token ini ketika pengguna memilih hasil dan mengirimkannya ke Amazon Kendra titik akhir sebagai umpan balik.

Amazon Kendra JavaScript Perpustakaan hanya mengirimkan token umpan balik dan metadata lainnya seperti waktu hasil dipilih dan ID pengunjung unik.

Langkah 3: Menguji umpan balik

Untuk memastikan bahwa JavaScript pustaka dikonfigurasi dengan benar dan mengirimkan umpan balik ke titik akhir yang tepat, lakukan hal berikut. Contoh ini menggunakan peramban Chrome.

1. Buka alat developer Web di peramban. Di Chrome, buka menu Chrome di pojok kanan atas peramban, pilih Alat lainnya, lalu pilih Alat developer.
2. Pastikan tidak ada kesalahan yang terkait dengan Amazon Kendra JavaScript pustaka di tab konsol.
3. Buat pencarian dan pilih hasil apa pun. Di tab Jaringan alat developer. Anda akan melihat permintaan yang dikirim ke titik akhir umpan balik, token untuk hasil, dan status 200 OK.

Menggunakan Amazon Kendra API untuk mengirimkan umpan balik

Untuk menggunakan Amazon Kendra API untuk mengirimkan umpan balik kueri, gunakan SubmitFeedbackAPI. Untuk mengidentifikasi kueri, Anda memberikan ID indeks indeks yang diterapkan kueri, dan ID kueri ditampilkan dalam respons dari Query API.

Contoh berikut menunjukkan cara mengirimkan umpan balik klik dan relevansi menggunakan Amazon Kendra API. Anda dapat mengirimkan beberapa set umpan balik melalui `ClickFeedbackItems` dan jajaran `RelevanceFeedbackItems`. Contoh ini mengirimkan satu klik dan satu item umpan balik relevansi. Pengiriman umpan balik menggunakan waktu saat ini.

Untuk mengirimkan umpan balik untuk pencarian (AWS SDK)

1. Anda dapat menggunakan kode contoh berikut dengan nilai yang diperlukan:

   a. `index id`—ID indeks tempat kueri berlaku.

   b. `query id`—Kueri yang ingin Anda berikan umpan balik.

   c. `result id`—ID dari hasil kueri yang ingin Anda berikan umpan balik. Respon kueri berisi ID hasil.

   d. `relevance value`—Entah `RELEVANT` (hasil kueri relevan) atau `NOT_RELEVANT` (hasil kueri tidak relevan).

   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. Jalankan kode tersebut. Setelah umpan balik dikirimkan, kode menampilkan pesan.

Menambahkan sinonim khusus ke indeks

Untuk menambahkan sinonim khusus ke indeks, Anda menentukannya dalam file tesaurus. Anda dapat memasukkan istilah khusus bisnis atau khusus dalam Amazon Kendra menggunakan sinonim. Sinonim bahasa Inggris generik, seperti`leader, head`, dibangun ke dalam Amazon Kendra dan tidak boleh dimasukkan dalam file tesaurus, termasuk sinonim generik yang menggunakan tanda hubung. Amazon Kendra mendukung sinonim untuk semua jenis respons, yang mencakup jenis `DOCUMENT` respons dan `QUESTION_ANSWER` atau jenis `ANSWER` respons. Amazon Kendra saat ini tidak mendukung penambahan sinonim yang ditandai sebagai stopwords. Ini harus dimasukkan dalam rilis future.

Amazon Kendra membuat korelasi antara sinonim. Misalnya, menggunakan pasangan sinonim`Dynamo, Amazon DynamoDB`, Amazon Kendra berkorelasi Dynamo dengan. Amazon DynamoDB Kuerinya “Apa itu dynamo?” kemudian mengembalikan dokumen seperti “Apa itu Amazon DynamoDB?”. Dengan sinonim, Amazon Kendra dapat lebih mudah mengambil korelasi.

File tesaurus adalah file teks yang disimpan dalam ember. Amazon S3 Lihat Menambahkan tesaurus ke indeks.

File tesaurus menggunakan format sinonim Solr. Amazon Kendra memiliki batas jumlah tesauri per indeks. Lihat Kuota.

Sinonim dapat berguna dalam skenario berikut:

- Istilah khusus yang bukan sinonim bahasa Inggris tradisional seperti `NLP, Natural Language Processing`.
- Kata benda yang tepat dengan asosiasi semantik yang kompleks. Ini adalah kata benda yang jarang dimengerti masyarakat umum, misalnya, dalam machine learning, `cost, loss, model performance`.
- Berbagai bentuk nama produk, misalnya, `Elastic Compute Cloud, EC2`.
- Istilah khusus domain atau bisnis tertentu, seperti nama produk. Misalnya, `Route53, DNS`.

Jangan menggunakan sinonim dalam skenario berikut:

- Sinonim bahasa Inggris generik seperti `leader, head`. Sinonim ini tidak khusus domain, dan menggunakan sinonim dalam skenario ini mungkin memiliki efek yang tidak diinginkan.

- Kesalahan tipografi seperti `teh => the`.
- Varian morfologi seperti jamak dan memiliki kata benda, bentuk kata sifat komparatif dan superlatif, dan bentuk lampau, partisip masa lalu dan bentuk kata kerja progresif. Salah satu contoh kata sifat komparatif dan superlatif adalah `good, better, best`.
- Kata berhenti unigram (satu kata) seperti `WHO`. Kata berhenti unigram tidak diperbolehkan dalam tesaurus dan dikecualikan dari pencarian. Misalnya, `WHO => World Health Organization` ditolak. Anda dapat menggunakan `W.H.O.` hanya sebagai istilah sinonim, dan Anda dapat menggunakan kata henti sebagai bagian dari sinonim multi-kata. Misalnya, `of` diperbolehkan, tapi `United States of America` tidak.

Sinonim khusus memudahkan untuk meningkatkan pemahaman Amazon Kendra tentang terminologi spesifik bisnis Anda dengan memperluas pertanyaan Anda untuk mencakup sinonim khusus bisnis Anda. Meskipun sinonim dapat meningkatkan akurasi pencarian, penting untuk memahami bagaimana sinonim mempengaruhi latensi sehingga Anda dapat mengoptimalkannya untuk ini.

Aturan umum untuk sinonim adalah: semakin banyak istilah dalam kueri Anda yang dicocokkan dan diperluas dengan sinonim, semakin besar potensi dampak pada latensi. Faktor lain yang memengaruhi latensi termasuk ukuran rata-rata dokumen yang diindeks, ukuran indeks Anda, pemfilteran apa pun pada hasil penelusuran, dan beban keseluruhan pada indeks Anda. Amazon Kendra Kueri yang tidak cocok dengan sinonim apa pun tidak akan terpengaruh.

Panduan umum tentang bagaimana sinonim memengaruhi latensi:

Kasus penggunaan	Peningkatan latensi*
Bahasa alami yang khas atau kueri kata kunci masing-masing terdiri dari 3 hingga 5 kata	Kurang dari 15 persen
1 istilah kueri melebar ke 3 sinonim	
Indeks sekitar 500.000 dokumen (rata-rata 10,48 KB teks yang diekstrak per dokumen) atau 30.000 FAQ / pasangan pertanyaan	

*Performa bervariasi berdasarkan penggunaan spesifik Anda atas sinonim dan konfigurasi pada indeks Anda. Sebaiknya uji performa penelusuran untuk mendapatkan tolok ukur yang lebih akurat untuk kasus penggunaan spesifik Anda.

Jika tesaurus Anda besar, memiliki rasio ekspansi jangka tinggi, dan peningkatan latensi Anda tidak dalam batas yang dapat diterima, Anda dapat mencoba salah satu atau kedua hal berikut:

- Potong tesaurus Anda untuk mengurangi rasio ekspansi (jumlah sinonim per istilah).
- Potong cakupan keseluruhan istilah (jumlah baris dalam tesaurus Anda).

Atau, Anda dapat meningkatkan kapasitas penyediaan (unit penyimpanan virtual) untuk mengimbangi peningkatan latensi.

Topik

Membuat file tesaurus

File Amazon Kendra TESAURUS adalah file yang dikodekan UTF-8 yang berisi daftar sinonim dalam format daftar sinonim Solr. File tesaurus harus kurang dari 5 MB.

Ada dua cara untuk menentukan pemetaan sinonim:

- Sinonim dua arah ditetapkan sebagai daftar istilah yang dipisahkan koma. Jika pengguna Anda menanyakan salah satu istilah, maka semua istilah dalam daftar digunakan untuk mencari dokumen, yang mencakup istilah kueri asli.
- Sinonim searah ditentukan sebagai istilah yang dipisahkan oleh simbol “**=>**” di antara mereka untuk memetakan istilah ke sinonimnya. Jika pengguna Anda menanyakan istilah di sebelah kiri simbol “**=>**”, maka itu dipetakan ke istilah di sebelah kanan untuk mencari dokumen menggunakan sinonim. Itu tidak dipetakan sebaliknya, membuat ini searah.

Sinonim itu sendiri peka huruf besar/kecil, tetapi istilah yang mereka petakan tidak peka huruf besar/kecil. Misalnya, `ML => Machine Learning` jika pengguna Anda menanyakan “ML” atau “mL” atau menggunakan beberapa kasus lain, itu akan dipetakan ke “Machine Learning”. Jika Anda memetakan

ini sebaliknya`Machine Learning => ML`, maka “Machine Learning” atau “machine learning” atau kasus lain akan dipetakan ke “ML”.

Sinonim tidak mencari kecocokan persis pada karakter khusus. Misalnya, jika Anda mencari "dead-letter-queue“, Amazon Kendra dapat mengembalikan dokumen yang cocok dengan “antrian surat mati” (tidak ada tanda hubung). Jika dokumen Anda berisi tanda hubung, seperti "dead-letter-queue“, Amazon Kendra proses dokumen selama pencarian untuk menghapus tanda hubung. Untuk istilah sinonim bahasa Inggris generik yang dibangun ke dalam Amazon Kendra dan tidak boleh dimasukkan dalam file tesaurus, Amazon Kendra dapat mencari versi tanda hubung dari istilah dan versi non-tanda hubung dari istilah tersebut. Misalnya, jika Anda mencari “pihak ketiga” dan “pihak ketiga”, Amazon Kendra mengembalikan dokumen yang cocok dengan salah satu versi istilah tersebut.

Untuk sinonim yang berisi stopword atau kata yang umum digunakan, Amazon Kendra mengembalikan dokumen yang cocok dengan istilah termasuk stopword. Misalnya, Anda dapat membuat aturan sinonim untuk memetakan “saat naik pesawat” dan “orientasi”. Anda tidak dapat menggunakan stopwords sendirian untuk sinonim. Misalnya, jika Anda mencari “on”, Amazon Kendra tidak dapat mengembalikan semua dokumen yang berisi “on”.

Beberapa aturan sinonim diabaikan. Misalnya, `a => b` adalah aturan, tetapi `a => a` diabaikan dan tidak dihitung sebagai aturan.

Jumlah istilah adalah jumlah istilah unik dalam file theaurus. Contoh file di bawah ini mencakup istilah`AWS CodeStar`,`ML`,`Machine Learning`,`autoscaling group`,`ASG`, dan banyak lagi.

Ada jumlah maksimum aturan sinonim per tesaurus dan jumlah maksimum sinonim per istilah. Untuk informasi selengkapnya, lihat Kuota untuk Amazon Kendra.

Contoh berikut menunjukkan file tesaurus dengan aturan sinonim. Setiap baris berisi aturan sinonim tunggal. Baris kosong dan komentar diabaikan.

```
# 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.
```

Menambahkan tesaurus ke indeks

Prosedur berikut menunjukkan cara menambahkan file tesaurus yang berisi sinonim indeks. Diperlukan waktu hingga 30 menit untuk melihat efek dari file tesaurus Anda yang diperbarui. Untuk informasi selengkapnya tentang file tesaurus, lihat Membuat file tesaurus.

Console

Untuk menambahkan tesaurus

1. Di panel navigasi kiri, di bawah indeks tempat Anda ingin menambahkan daftar sinonim, tesaurus Anda, pilih Sinonim.
2. Pada halaman Sinonim, pilih Tambahkan Thesaurus.
3. Dalam Tentukan tesaurus, berikan nama tesaurus Anda dan deskripsi opsional.
4. Dalam pengaturan Tesaurus, berikan Amazon S3 jalur ke file tesaurus Anda. File harus lebih kecil dari 5 MB.
5. Untuk Peran IAM, pilih peran atau pilih Buat peran baru dan tentukan nama peran untuk membuat peran baru. Amazon Kendra menggunakan peran ini untuk mengakses Amazon S3 sumber daya atas nama Anda. Peran IAM memiliki awalan "AmazonKendra-".
6. Pilih Simpan untuk menyimpan konfigurasi dan menambahkan tesaurus. Setelah tesaurus diserap, ia aktif dan sinonim disorot dalam hasil. Diperlukan waktu hingga 30 menit untuk melihat efek file tesaurus Anda.

CLI

Untuk menambahkan thesarus ke indeks dengan AWS CLI, panggil: `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
```

Panggil `list-thesauri` untuk melihat daftar tesaurus:

```
aws kendra list-thesauri \
--index-id index-id
```

Untuk melihat detail tesaurus, panggil `describe-thesaurus`:

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

```
--index-id thesaurus-id
```

Diperlukan waktu hingga 30 menit untuk melihat efek file tesaurus Anda.

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.");
  }
}
```

Memperbarui tesaurus

Anda dapat mengubah konfigurasi tesaurus setelah dibuat. Anda dapat mengubah detail seperti nama tesaurus dan informasi IAM. Anda juga dapat mengubah lokasi path file tesaurus Amazon S3. Jika Anda mengubah jalur ke file tesaurus, Amazon Kendra ganti tesaurus yang ada dengan tesaurus yang ditentukan di jalur yang diperbarui.

Diperlukan waktu hingga 30 menit untuk melihat efek dari file tesaurus Anda yang diperbarui.

> **Note**
>
> Jika ada kesalahan validasi atau sintaks dalam file tesaurus, file tesaurus yang diunggah sebelumnya akan dipertahankan.

Prosedur berikut menunjukkan cara mengubah detail tesaurus.

Console

Untuk mengubah detail tesaurus

1. Di panel navigasi kiri, di bawah indeks yang ingin Anda ubah, pilih Sinonim.
2. Pada halaman Sinonim, pilih tesaurus yang ingin Anda ubah dan kemudian pilih Edit.
3. Pada halaman Memperbarui tesaurus, perbarui detail tesaurus.
4. (Opsional) Pilih Ubah jalur file tesaurus dan kemudian tentukan Amazon S3 jalur ke file tesaurus baru. File tesaurus yang ada digantikan oleh file yang Anda tentukan. Jika Anda tidak mengubah jalur, Amazon Kendra muat ulang tesaurus dari jalur yang ada.

   Jika Anda memilih Simpan file tesaurus saat ini, Amazon Kendra tidak memuat ulang file tesaurus.
5. Pilih Simpan untuk menyimpan konfigurasi.

Anda juga dapat memuat ulang tesaurus dari path tesaurus yang ada.

Untuk memuat ulang tesaurus dari path yang ada

1. Di panel navigasi kiri, di bawah indeks yang ingin Anda ubah, pilih Sinonim.
2. Pada halaman Sinonim, pilih tesaurus yang ingin dimuat ulang dan kemudian pilih Refresh.

3. Pada halaman Reload thesaurus file, konfirmasikan bahwa Anda ingin me-refresh file tesaurus.

CLI

Untuk memperbarui tesaurus, panggil `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.");
  }
}
```

Menghapus tesaurus

Prosedur berikut menunjukkan cara menghapus tesaurus.

Console

1. Di panel navigasi kiri, di bawah indeks yang ingin Anda ubah, pilih Sinonim.
2. Pada halaman Sinonim, pilih tesaurus yang ingin Anda hapus.
3. Pada halaman Detail tesaurus, pilih Hapus dan kemudian konfirmasikan untuk menghapus.

CLI

Untuk menghapus thesarus ke indeks dengan AWS CLI, panggil: `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);
  }
}
```

Sorotan dalam hasil pencarian

Penyorotan sinonim aktif secara default. Informasi sorotan disertakan dalam hasil Amazon Kendra kueri SDK dan CLI. Jika Anda berinteraksi dengan Amazon Kendra menggunakan SDK atau CLI, Anda menentukan cara menampilkan hasil.

Sorotan sinonim akan mempunyai jenis sorotan `THESAURUS_SYNONYM`. Untuk informasi selengkapnya tentang sorotan, lihat objek Sorotan.

Tutorial: Membangun solusi pencarian cerdas yang diperkaya metadata dengan Amazon Kendra

Tutorial ini menunjukkan kepada Anda bagaimana membangun solusi pencarian cerdas berbasis bahasa alami yang diperkaya metadata untuk data perusahaan Anda menggunakan Amazon Kendra, Amazon Comprehend, AmazonSimple Storage Service (S3), dan. AWS CloudShell

Amazon Kendra adalah layanan pencarian cerdas yang dapat membangun indeks pencarian untuk repositori data bahasa alami yang tidak terstruktur dan tidak terstruktur. Untuk memudahkan pelanggan Anda menemukan dan memfilter jawaban yang relevan, Anda dapat menggunakan Amazon Comprehend untuk mengekstrak metadata dari data Anda dan memasukkannya ke dalam indeks pencarian Amazon Kendra Anda.

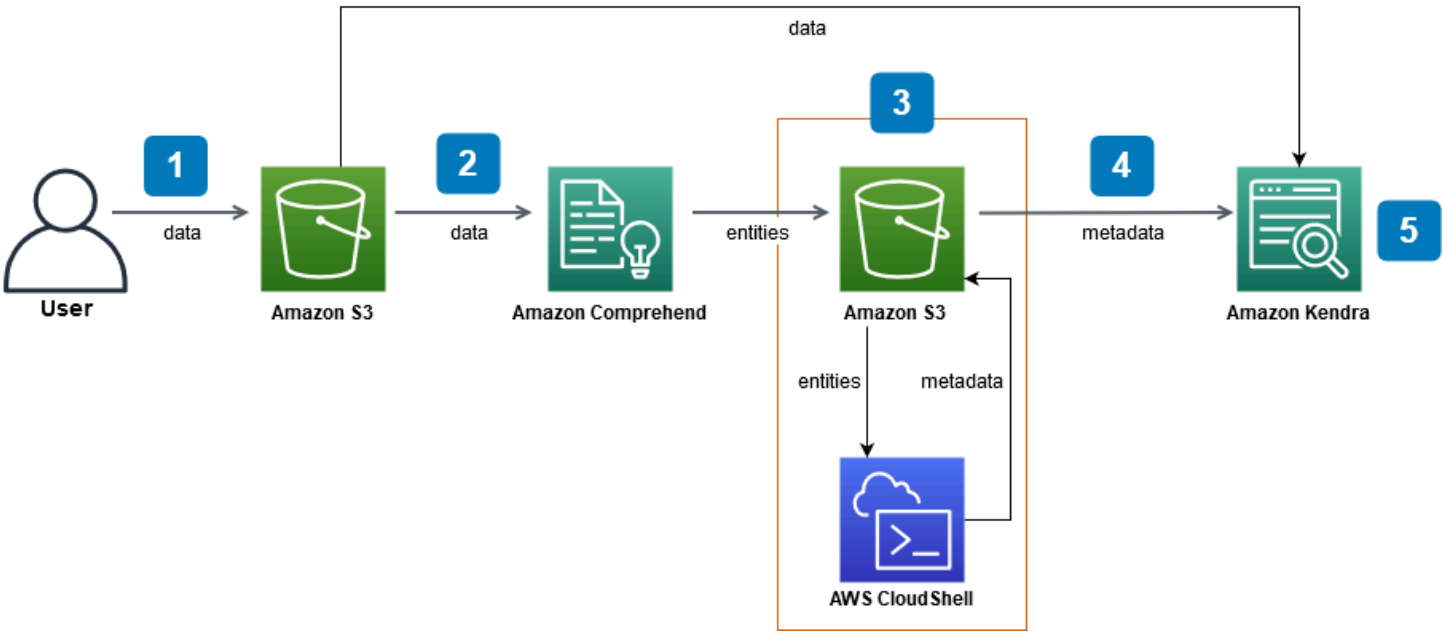
Amazon Comprehend adalah layanan pemrosesan bahasa alami (NLP) yang dapat mengidentifikasi entitas. Entitas adalah referensi ke orang, tempat, lokasi, organisasi, dan objek dalam data Anda.

Tutorial ini menggunakan contoh kumpulan data artikel berita untuk mengekstrak entitas, mengubahnya menjadi metadata, dan memasukkannya ke indeks Amazon Kendra Anda untuk menjalankan pencarian. Metadata yang ditambahkan memungkinkan Anda memfilter hasil pencarian menggunakan subset dari entitas ini, dan meningkatkan akurasi penelusuran. Dengan mengikuti tutorial ini, Anda akan belajar cara membuat solusi pencarian untuk data perusahaan Anda tanpa pengetahuan pembelajaran mesin khusus.

Tutorial ini menunjukkan kepada Anda bagaimana membangun solusi pencarian Anda menggunakan langkah-langkah berikut:

1. Menyimpan kumpulan data sampel artikel berita di Amazon S3.
2. Menggunakan Amazon Comprehend untuk mengekstrak entitas dari data Anda.
3. Menjalankan skrip Python 3 untuk mengubah entitas menjadi format metadata indeks Amazon Kendra dan menyimpan metadata ini di S3.
4. Membuat indeks pencarian Amazon Kendra dan menelan data dan metadata.
5. Query indeks pencarian.

Diagram berikut menunjukkan alur kerja:



Perkiraan waktu untuk menyelesaikan tutorial ini: 1 jam

Perkiraan biaya: Beberapa tindakan dalam tutorial ini dikenakan biaya pada AWS akun Anda. Untuk informasi lebih lanjut tentang biaya setiap layanan, lihat halaman harga untuk Amazon S3, AmazonComprehend,, dan Amazon Kendra AWS CloudShell.

Topik

Prasyarat

Untuk menyelesaikan tutorial ini, Anda memerlukan sumber daya berikut:

- Akun AWS. Jika Anda tidak memiliki AWS akun, ikuti langkah-langkah dalam Menyiapkan Amazon Kendra untuk menyiapkan AWS akun Anda.

- Komputer pengembangan yang menjalankan Windows, macOS, atau Linux, untuk mengakses AWS Management Console. Untuk informasi selengkapnya, lihat Mengonfigurasi Konsol AWS Manajemen.
- Pengguna AWS Identity and Access Management(IAM). Untuk mempelajari cara menyiapkan pengguna dan grup IAM untuk akun Anda, lihat bagian Memulai di Panduan Pengguna IAM.

  Jika Anda menggunakanAWS Command Line Interface, Anda juga perlu melampirkan kebijakan berikut untuk pengguna IAM Anda untuk memberikan izin dasar yang diperlukan untuk menyelesaikan tutorial ini.

  Untuk informasi selengkapnya, lihat Membuat kebijakan IAM dan Menambahkan dan menghapus izin identitas IAM.
- Daftar Layanan AWS Regional. Untuk mengurangi latensi, Anda harus memilih AWS wilayah yang paling dekat dengan lokasi geografis Anda yang didukung oleh Amazon Comprehend dan Amazon Kendra.
- (Opsional) Sebuah AWS Key Management Service. Meskipun tutorial ini tidak menggunakan enkripsi, Anda mungkin ingin menggunakan praktik terbaik enkripsi untuk kasus penggunaan spesifik Anda.
- (Opsional) Amazon Virtual Private Cloud. Meskipun tutorial ini tidak menggunakan VPC, Anda mungkin ingin menggunakan praktik terbaik VPC untuk memastikan keamanan data untuk kasus penggunaan spesifik Anda.

Langkah 1: Menambahkan dokumen ke Amazon S3

Sebelum menjalankan tugas analisis entitas Amazon Comprehend pada kumpulan data Anda, Anda membuat bucket Amazon S3 untuk menghosting data, metadata, dan output analisis entitas Amazon Comprehend.

Topik

- Mengunduh kumpulan data sampel
- Membuat sebuah bucket Amazon S3
- Membuat folder data dan metadata di bucket S3
- Mengunggah data input

Mengunduh kumpulan data sampel

Sebelum Amazon Comprehend dapat menjalankan tugas analisis entitas pada data Anda, Anda harus mengunduh dan mengekstrak set data dan mengunggahnya ke bucket S3.

Untuk mengunduh dan mengekstrak dataset (Console)

1. Unduh folder tutorial-dataset.zip di perangkat Anda.
2. Ekstrak `tutorial-dataset` folder untuk mengakses `data` folder.

Untuk mengunduh dan mengekstrak dataset (Terminal)

1. Untuk men-download`tutorial-dataset`, jalankan perintah berikut pada jendela terminal:

   Linux

   ```
   curl -o path/tutorial-dataset.zip https://docs.aws.amazon.com/kendra/latest/dg/
   samples/tutorial-dataset.zip
   ```

   Dengan:

   - *`path/`* adalah filepath lokal ke lokasi tempat Anda ingin menyimpan folder zip.

   macOS

   ```
   curl -o path/tutorial-dataset.zip https://docs.aws.amazon.com/kendra/latest/dg/
   samples/tutorial-dataset.zip
   ```

   Dengan:

   - *`path/`* adalah filepath lokal ke lokasi tempat Anda ingin menyimpan folder zip.

   Windows

   ```
   curl -o path/tutorial-dataset.zip https://docs.aws.amazon.com/kendra/latest/dg/
   samples/tutorial-dataset.zip
   ```

   Dengan:

- *path/* adalah filepath lokal ke lokasi tempat Anda ingin menyimpan folder zip.

2. Untuk mengekstrak data dari folder zip, jalankan perintah berikut pada jendela terminal:

   Linux

   ```
   unzip path/tutorial-dataset.zip -d path/
   ```

   Dengan:

   - *path/* adalah filepath lokal ke folder zip tersimpan Anda.

   macOS

   ```
   unzip path/tutorial-dataset.zip -d path/
   ```

   Dengan:

   - *path/* adalah filepath lokal ke folder zip tersimpan Anda.

   Windows

   ```
   tar -xf path/tutorial-dataset.zip -C path/
   ```

   Dengan:

   - *path/* adalah filepath lokal ke folder zip tersimpan Anda.

Pada akhir langkah ini, Anda harus memiliki file yang diekstrak dalam folder didekompresi yang disebut. `tutorial-dataset` Folder ini berisi `README` file dengan atribusi open source Apache 2.0 dan folder bernama `data` berisi dataset untuk tutorial ini. Dataset terdiri dari 100 file dengan `.story` ekstensi.

Membuat sebuah bucket Amazon S3

Setelah mengunduh dan mengekstraksi folder data sampel, Anda menyimpannya di bucket Amazon S3.

> **Important**
>
> Nama bucket Amazon S3 harus unik di semua. AWS

Untuk membuat bucket S3 (Console)

1. Masuk ke AWS Management Console dan buka konsol Amazon S3 di https://console.aws.amazon.com/s3/.
2. Di Bucket, pilih Buat bucket.
3. Untuk Nama bucket, masukkan nama yang unik.
4. Untuk Wilayah, pilih AWS wilayah tempat Anda ingin membuat bucket.

   > **Note**
   >
   > Anda harus memilih wilayah yang mendukung Amazon Comprehend dan Amazon Kendra. Anda tidak dapat mengubah wilayah bucket setelah Anda membuatnya.

5. Simpan pengaturan default untuk pengaturan Blokir Akses Publik untuk bucket, Pembuatan Versi Bucket, dan Tag ini.
6. Untuk enkripsi Default, pilih Nonaktifkan.
7. Simpan pengaturan default untuk pengaturan Lanjutan.
8. Tinjau konfigurasi bucket Anda, lalu pilih Buat bucket.

Untuk membuat bucket S3 () AWS CLI

1. Untuk membuat bucket S3, gunakan perintah create-bucket di: AWS CLI

   Linux

   ```
   aws s3api create-bucket \
           --bucket DOC-EXAMPLE-BUCKET \
           --region aws-region \
           --create-bucket-configuration LocationConstraint=aws-region
   ```

   Dengan:

- *DOC-EXAMPLE-BUCKET adalah nama bucket* Anda,
- *aws-region* adalah wilayah tempat Anda ingin membuat bucket Anda.

macOS

```
aws s3api create-bucket \
        --bucket DOC-EXAMPLE-BUCKET \
        --region aws-region \
        --create-bucket-configuration LocationConstraint=aws-region
```

Dengan:

- *DOC-EXAMPLE-BUCKET adalah nama bucket* Anda,
- *aws-region* adalah wilayah tempat Anda ingin membuat bucket Anda.

Windows

```
aws s3api create-bucket ^
        --bucket DOC-EXAMPLE-BUCKET ^
        --region aws-region ^
        --create-bucket-configuration LocationConstraint=aws-region
```

Dengan:

- *DOC-EXAMPLE-BUCKET adalah nama bucket* Anda,
- *aws-region* adalah wilayah tempat Anda ingin membuat bucket Anda.

> **Note**
>
> Anda harus memilih wilayah yang mendukung Amazon Comprehend dan Amazon Kendra. Anda tidak dapat mengubah wilayah bucket setelah Anda membuatnya.

2. Untuk memastikan bahwa bucket Anda berhasil dibuat, gunakan perintah list:

Linux

```
aws s3 ls
```

macOS

```
aws s3 ls
```

Windows

```
aws s3 ls
```

Membuat folder data dan metadata di bucket S3

Setelah membuat bucket S3, Anda membuat folder data dan metadata di dalamnya.

Untuk membuat folder di bucket S3 Anda (Console)

1. Buka konsol Amazon S3 di https://console.aws.amazon.com/s3/.
2. Di Bucket, klik nama bucket Anda dari daftar bucket.
3. Dari tab Objects, pilih Create folder.
4. Untuk nama folder baru, masukkan**`data`**.
5. Untuk pengaturan enkripsi, pilih Nonaktifkan.
6. Pilih Membuat folder.
7. Ulangi langkah 3 hingga 6 untuk membuat folder lain untuk menyimpan metadata Amazon Kendra dan beri nama folder yang dibuat pada langkah 4. **`metadata`**

Untuk membuat folder di bucket S3 Anda () AWS CLI

1. Untuk membuat `data` folder di bucket S3 Anda, gunakan perintah put-object di: AWS CLI

   Linux

```
aws s3api put-object \
        --bucket DOC-EXAMPLE-BUCKET \
```

```
        --key data/
```

Dengan:

- *DOC-EXAMPLE-BUCKET adalah nama bucket* Anda.

macOS

```
aws s3api put-object \
        --bucket DOC-EXAMPLE-BUCKET \
        --key data/
```

Dengan:

- *DOC-EXAMPLE-BUCKET adalah nama bucket* Anda.

Windows

```
aws s3api put-object ^
        --bucket DOC-EXAMPLE-BUCKET ^
        --key data/
```

Dengan:

- *DOC-EXAMPLE-BUCKET adalah nama bucket* Anda.

2. Untuk membuat `metadata` folder di bucket S3 Anda, gunakan perintah put-object di: AWS CLI

Linux

```
aws s3api put-object \
        --bucket DOC-EXAMPLE-BUCKET \
        --key metadata/
```

Dengan:

- *DOC-EXAMPLE-BUCKET adalah nama bucket* Anda.

macOS

```
aws s3api put-object \
        --bucket DOC-EXAMPLE-BUCKET \
        --key metadata/
```

Dengan:

- *DOC-EXAMPLE-BUCKET adalah nama bucket* Anda.

Windows

```
aws s3api put-object ^
        --bucket DOC-EXAMPLE-BUCKET ^
        --key metadata/
```

Dengan:

- *DOC-EXAMPLE-BUCKET adalah nama bucket* Anda.

3. Untuk memastikan bahwa folder Anda berhasil dibuat, periksa isi bucket Anda menggunakan perintah list:

Linux

```
aws s3 ls s3://DOC-EXAMPLE-BUCKET/
```

Dengan:

- *DOC-EXAMPLE-BUCKET adalah nama bucket* Anda.

macOS

```
aws s3 ls s3://DOC-EXAMPLE-BUCKET/
```

Dengan:

- *DOC-EXAMPLE-BUCKET adalah nama bucket* Anda.

Windows

```
aws s3 ls s3://DOC-EXAMPLE-BUCKET/
```

Dengan:

- *DOC-EXAMPLE-BUCKET adalah nama bucket* Anda.

Mengunggah data input

Setelah membuat folder data dan metadata, Anda mengunggah kumpulan data sampel ke dalam folder. `data`

Untuk mengunggah kumpulan data sampel ke dalam folder data (Konsol)

1. Buka konsol Amazon S3 di https://console.aws.amazon.com/s3/.
2. Di Bucket, klik pada nama bucket Anda dari daftar bucket dan kemudian klik. `data`
3. Pilih Unggah, lalu pilih Tambahkan file.
4. Di kotak dialog, navigasikan ke `data` folder di dalam `tutorial-dataset` folder di perangkat lokal Anda, pilih semua file, lalu pilih Buka.
5. Simpan pengaturan default untuk Tujuan, Izin, dan Properti.
6. Pilih Upload (Unggah).

Untuk mengunggah kumpulan data sampel ke dalam folder data () AWS CLI

1. Untuk mengunggah data sampel ke dalam `data` folder, gunakan perintah salin diAWS CLI:

   Linux

   ```
   aws s3 cp path/tutorial-dataset/data s3://DOC-EXAMPLE-BUCKET/data/ --recursive
   ```

   Dengan:

   - *path/* adalah filepath ke `tutorial-dataset` folder pada perangkat Anda,
   - *DOC-EXAMPLE-BUCKET adalah nama bucket* Anda.

macOS

```
aws s3 cp path/tutorial-dataset/data s3://DOC-EXAMPLE-BUCKET/data/ --recursive
```

Dengan:

- *path/* adalah filepath ke `tutorial-dataset` folder pada perangkat Anda,
- *DOC-EXAMPLE-BUCKET adalah nama bucket* Anda.

Windows

```
aws s3 cp path/tutorial-dataset/data s3://DOC-EXAMPLE-BUCKET/data/ --recursive
```

Dengan:

- *path/* adalah filepath ke `tutorial-dataset` folder pada perangkat Anda,
- *DOC-EXAMPLE-BUCKET adalah nama bucket* Anda.

2. Untuk memastikan bahwa file set data Anda berhasil diunggah ke `data` folder Anda, gunakan perintah list diAWS CLI:

Linux

```
aws s3 ls s3://DOC-EXAMPLE-BUCKET/data/
```

Dengan:

- *DOC-EXAMPLE-BUCKET adalah nama bucket* S3 Anda.

macOS

```
aws s3 ls s3://DOC-EXAMPLE-BUCKET/data/
```

Dengan:

- *DOC-EXAMPLE-BUCKET adalah nama bucket* S3 Anda.

Windows

```
aws s3 ls s3://DOC-EXAMPLE-BUCKET/data/
```

Dengan:

- *DOC-EXAMPLE-BUCKET adalah nama bucket* S3 Anda.

Pada akhir langkah ini, Anda memiliki bucket S3 dengan kumpulan data Anda disimpan di dalam `data` folder, dan `metadata` folder kosong, yang akan menyimpan metadata Amazon Kendra Anda.

Langkah 2: Menjalankan pekerjaan analisis entitas di Amazon Comprehend

Setelah menyimpan kumpulan data sampel di bucket S3, Anda menjalankan tugas analisis entitas Amazon Comprehend untuk mengekstrak entitas dari dokumen Anda. Entitas ini akan membentuk atribut khusus Amazon Kendra dan membantu Anda memfilter hasil pencarian pada indeks Anda. Untuk informasi selengkapnya, lihat Mendeteksi Entitas.

Topik

- Menjalankan pekerjaan analisis entitas Amazon Comprehend

Menjalankan pekerjaan analisis entitas Amazon Comprehend

Untuk mengekstrak entitas dari kumpulan data, Anda menjalankan tugas analisis entitas Amazon Comprehend.

Jika Anda menggunakan AWS CLI dalam langkah ini, pertama-tama Anda membuat dan melampirkan peran dan kebijakan AWS IAM untuk Amazon Comprehend dan kemudian menjalankan tugas analisis entitas. Untuk menjalankan tugas analisis entitas pada data sampel Anda, Amazon Comprehend perlu:

- peran AWS Identity and Access Management (IAM) yang mengenalinya sebagai entitas tepercaya
- kebijakan AWS IAM yang dilampirkan ke peran IAM yang memberikan izin untuk mengakses bucket S3 Anda

Untuk informasi selengkapnya, lihat Cara Amazon Comprehend bekerja dengan IAM dan Kebijakan Berbasis Identitas untuk Amazon Comprehend.

Untuk menjalankan tugas analisis entitas Amazon Comprehend (Console)

1. Buka konsol Amazon Comprehend di https://console.aws.amazon.com/comprehend/.

   > **Important**
   >
   > Pastikan Anda berada di wilayah yang sama dengan tempat Anda membuat bucket Amazon S3. Jika Anda berada di wilayah lain, pilih AWS wilayah tempat Anda membuat bucket S3 dari pemilih Wilayah di bilah navigasi atas.

2. Pilih Luncurkan Amazon Comprehend.
3. Di panel navigasi kiri, pilih Pekerjaan analisis.
4. Pilih Buat tugas.
5. Di bagian Pengaturan pekerjaan, lakukan hal berikut:
   a. Untuk Nama, masukkan **`data-entities-analysis`**.
   b. Untuk Jenis analisis, pilih Entitas.
   c. Untuk Bahasa, pilih Bahasa Inggris.
   d. Jauhkan enkripsi Job dimatikan.
6. Di bagian Input data, lakukan hal berikut:
   a. Untuk Sumber data, pilih Dokumen saya.
   b. Untuk lokasi S3, pilih Browse S3.
   c. Untuk Pilih sumber daya, klik nama bucket Anda dari daftar bucket.
   d. Untuk Objects, pilih tombol opsi untuk `data` dan pilih Choose.
   e. Untuk format Input, pilih Satu dokumen per file.
7. Di bagian Data keluaran, lakukan hal berikut:
   a. Untuk lokasi S3, pilih Browse S3 dan kemudian pilih kotak opsi untuk bucket Anda dari daftar bucket dan pilih Pilih.
   b. Jauhkan Enkripsi dimatikan.
8. Di bagian Izin akses, lakukan hal berikut:

a. Untuk peran IAM, pilih Buat peran IAM.

b. Agar Izin dapat mengakses, pilih bucket Input dan Output S3.

c. Untuk akhiran Nama, masukkan**`comprehend-role`**. Peran ini menyediakan akses ke bucket Amazon S3 Anda.

9. Simpan pengaturan VPC default.

10. Pilih Buat tugas.

Untuk menjalankan pekerjaan analisis entitas Amazon Comprehend () AWS CLI

1. Untuk membuat dan melampirkan peran IAM untuk Amazon Comprehend yang mengenalinya sebagai entitas tepercaya, lakukan hal berikut:

   a. Simpan kebijakan kepercayaan berikut sebagai file JSON yang dipanggil `comprehend-trust-policy.json` dalam editor teks di perangkat lokal Anda.

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

   b. Untuk membuat peran IAM yang dipanggil `comprehend-role` dan melampirkan `comprehend-trust-policy.json` file yang disimpan ke dalamnya, gunakan perintah create-role:

      Linux

```
aws iam create-role \
          --role-name comprehend-role \
          --assume-role-policy-document file://path/comprehend-trust-
policy.json
```

Dengan:

- *path/* adalah filepath ke perangkat lokal `comprehend-trust-policy.json` Anda.

macOS

```
aws iam create-role \
          --role-name comprehend-role \
          --assume-role-policy-document file://path/comprehend-trust-
policy.json
```

Dengan:

- *path/* adalah filepath ke perangkat lokal `comprehend-trust-policy.json` Anda.

Windows

```
aws iam create-role ^
          --role-name comprehend-role ^
          --assume-role-policy-document file://path/comprehend-trust-
policy.json
```

Dengan:

- *path/* adalah filepath ke perangkat lokal `comprehend-trust-policy.json` Anda.

c. Salin Amazon Resource Name (ARN) ke editor teks Anda dan simpan secara lokal sebagai. `comprehend-role-arn`

> **Note**
>
> ARN memiliki format yang mirip dengan arn:aws:iam*: :123456789012:role/comprehend-role*. Anda membutuhkan ARN yang Anda simpan `comprehend-role-arn` untuk menjalankan pekerjaan analisis Amazon Comprehend.

2. Untuk membuat dan melampirkan kebijakan IAM ke peran IAM Anda yang memberikan izin untuk mengakses bucket S3 Anda, lakukan hal berikut:

a. Simpan kebijakan kepercayaan berikut sebagai file JSON yang dipanggil `comprehend-S3-access-policy.json` dalam editor teks di perangkat lokal Anda.

```
{
    "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. Untuk membuat kebijakan IAM yang dipanggil `comprehend-S3-access-policy` untuk mengakses bucket S3 Anda, gunakan perintah create-policy:

Linux

```
aws iam create-policy \
```

```
          --policy-name comprehend-S3-access-policy \
          --policy-document file://path/comprehend-S3-access-policy.json
```

Dengan:

- *path/* adalah filepath ke perangkat lokal `comprehend-S3-access-policy.json` Anda.

macOS

```
aws iam create-policy \
          --policy-name comprehend-S3-access-policy \
          --policy-document file://path/comprehend-S3-access-policy.json
```

Dengan:

- *path/* adalah filepath ke perangkat lokal `comprehend-S3-access-policy.json` Anda.

Windows

```
aws iam create-policy ^
          --policy-name comprehend-S3-access-policy ^
          --policy-document file://path/comprehend-S3-access-policy.json
```

Dengan:

- *path/* adalah filepath ke perangkat lokal `comprehend-S3-access-policy.json` Anda.

c. Salin Amazon Resource Name (ARN) ke editor teks Anda dan simpan secara lokal sebagai. `comprehend-S3-access-arn`

> **Note**
>
> ARN memiliki format yang mirip dengan arn:aws:iam*: :123456789012:role/comprehend-s3-access-policy*. Anda memerlukan ARN yang Anda simpan

`comprehend-S3-access-arn` untuk melampirkan peran `comprehend-S3-access-policy` IAM Anda.

d. Untuk melampirkan `comprehend-S3-access-policy` peran IAM Anda, gunakan attach-role-policyperintah:

Linux

```
aws iam attach-role-policy \
          --policy-arn policy-arn \
          --role-name comprehend-role
```

Dengan:

- *policy-arn adalah ARN* yang Anda simpan sebagai. `comprehend-S3-access-arn`

macOS

```
aws iam attach-role-policy \
          --policy-arn policy-arn \
          --role-name comprehend-role
```

Dengan:

- *policy-arn adalah ARN* yang Anda simpan sebagai. `comprehend-S3-access-arn`

Windows

```
aws iam attach-role-policy ^
          --policy-arn policy-arn ^
          --role-name comprehend-role
```

Dengan:

- *policy-arn adalah ARN* yang Anda simpan sebagai. `comprehend-S3-access-arn`

3. Untuk menjalankan tugas analisis entitas Amazon Comprehend, gunakan perintah: start-entities-detection-job

   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
   ```

   Dengan:

   - *DOC-EXAMPLE-BUCKET adalah nama bucket* S3 Anda,
   - *role-arn adalah ARN* yang Anda selamatkan sebagai, `comprehend-role-arn`
   - *aws-region adalah wilayah* AndaAWS.

   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
   ```

   Dengan:

   - *DOC-EXAMPLE-BUCKET adalah nama bucket* S3 Anda,
   - *role-arn adalah ARN* yang Anda selamatkan sebagai, `comprehend-role-arn`
   - *aws-region adalah wilayah* AndaAWS.

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
```

Dengan:

- *DOC-EXAMPLE-BUCKET adalah nama bucket* S3 Anda,
- *role-arn adalah ARN* yang Anda selamatkan sebagai, `comprehend-role-arn`
- *aws-region adalah wilayah* AndaAWS.

4. Salin analisis entitas `JobId` dan simpan dalam editor teks sebagai`comprehend-job-id`. `JobId`Membantu Anda melacak status pekerjaan analisis entitas Anda.
5. Untuk melacak kemajuan pekerjaan analisis entitas Anda, gunakan describe-entities-detection-jobperintah:

   Linux

   ```
   aws comprehend describe-entities-detection-job \
           --job-id entities-job-id \
           --region aws-region
   ```

   Dengan:

   - *entities-job-id*adalah Anda yang diselamatkan`comprehend-job-id`,
   - *aws-region adalah wilayah* AndaAWS.

   macOS

   ```
   aws comprehend describe-entities-detection-job \
           --job-id entities-job-id \
   ```

```
        --region aws-region
```

Dengan:

- *entities-job-id*adalah Anda yang diselamatkan`comprehend-job-id`,
- *aws-region adalah wilayah* AndaAWS.

Windows

```
aws comprehend describe-entities-detection-job ^
        --job-id entities-job-id ^
        --region aws-region
```

Dengan:

- *entities-job-id*adalah Anda yang diselamatkan`comprehend-job-id`,
- *aws-region adalah wilayah* AndaAWS.

Hal ini dapat mengambil beberapa menit `JobStatus` untuk mengubah ke`COMPLETED`.

Pada akhir langkah ini, Amazon Comprehend menyimpan hasil analisis entitas sebagai `output.tar.gz` file zip di dalam `output` folder dalam folder yang dibuat secara otomatis di bucket S3 Anda. Pastikan status pekerjaan analisis Anda selesai sebelum Anda melanjutkan ke langkah berikutnya.

Langkah 3: Memformat keluaran analisis entitas sebagai metadata Amazon Kendra

Untuk mengonversi entitas yang diekstrak oleh Amazon Comprehend ke format metadata yang diperlukan oleh indeks Amazon Kendra, Anda menjalankan skrip Python 3. Hasil konversi disimpan dalam `metadata` folder di bucket Amazon S3 Anda.

Untuk informasi selengkapnya tentang format dan struktur metadata Amazon Kendra, lihat metadata dokumen S3.

Topik

- Mengunduh dan mengekstraksi output Amazon Comprehend

- Mengunggah output ke bucket S3
- Mengonversi output ke format metadata Amazon Kendra
- Membersihkan bucket Amazon S3 Anda

Mengunduh dan mengekstraksi output Amazon Comprehend

Untuk memformat keluaran analisis entitas Amazon Comprehend, Anda harus mengunduh arsip analisis entitas Amazon Comprehend terlebih dahulu dan mengekstrak file analisis `output.tar.gz` entitas.

Untuk mengunduh dan mengekstrak file keluaran (Konsol)

1. Di panel navigasi konsol Amazon Comprehend, navigasikan ke pekerjaan Analisis.
2. Pilih pekerjaan `data-entities-analysis` analisis entitas Anda.
3. Di bawah Keluaran, pilih tautan yang ditampilkan di sebelah Lokasi data keluaran. Ini mengarahkan Anda ke `output.tar.gz` arsip di bucket S3 Anda.
4. Di tab Ikhtisar, pilih Unduh.

> **Tip**
>
> Output dari semua pekerjaan analisis Amazon Comprehend memiliki nama yang sama. Mengganti nama arsip Anda akan membantu Anda melacaknya dengan lebih mudah.

5. Dekompresi dan ekstrak file Amazon Comprehend yang diunduh ke perangkat Anda.

Untuk mengunduh dan mengekstrak file keluaran (AWS CLI)

1. Untuk mengakses nama folder buatan otomatis Amazon Comprehend di bucket S3 Anda yang berisi hasil pekerjaan analisis entitas, gunakan perintah: describe-entities-detection-job

   Linux

   ```
   aws comprehend describe-entities-detection-job \
             --job-id entities-job-id \
             --region aws-region
   ```

   Dengan:

- *entities-job-id*adalah Anda diselamatkan `comprehend-job-id` darithe section called “Langkah 2: Mendeteksi entitas”,
- *aws-region adalah wilayah* AndaAWS.

macOS

```
aws comprehend describe-entities-detection-job \
          --job-id entities-job-id \
          --region aws-region
```

Dengan:

- *entities-job-id*adalah Anda diselamatkan `comprehend-job-id` darithe section called “Langkah 2: Mendeteksi entitas”,
- *aws-region adalah wilayah* AndaAWS.

Windows

```
aws comprehend describe-entities-detection-job ^
          --job-id entities-job-id ^
          --region aws-region
```

Dengan:

- *entities-job-id*adalah Anda diselamatkan `comprehend-job-id` darithe section called “Langkah 2: Mendeteksi entitas”,
- *aws-region adalah wilayah* AndaAWS.

2. Dari `OutputDataConfig` objek dalam deskripsi pekerjaan entitas Anda, salin dan simpan `S3Uri` nilai seperti `comprehend-S3uri` pada editor teks.

> **Note**
>
> `S3Uri`Nilai memiliki format yang mirip dengan *s3://DOC-EXAMPLE-BUCKET /...* / output/output.tar.gz.

3. Untuk mengunduh arsip keluaran entitas, gunakan perintah salin:

Linux

```
aws s3 cp s3://DOC-EXAMPLE-BUCKET/.../output/output.tar.gz path/output.tar.gz
```

Dengan:

- *s3://DOC-CONTOH-BUCKET /...* /output/output.tar.gz adalah `S3Uri` nilai yang Anda simpan sebagai`comprehend-S3uri`,
- *path/* adalah direktori lokal tempat Anda ingin menyimpan output.

macOS

```
aws s3 cp s3://DOC-EXAMPLE-BUCKET/.../output/output.tar.gz path/output.tar.gz
```

Dengan:

- *s3://DOC-CONTOH-BUCKET /...* /output/output.tar.gz adalah `S3Uri` nilai yang Anda simpan sebagai`comprehend-S3uri`,
- *path/* adalah direktori lokal tempat Anda ingin menyimpan output.

Windows

```
aws s3 cp s3://DOC-EXAMPLE-BUCKET/.../output/output.tar.gz path/output.tar.gz
```

Dengan:

- *s3://DOC-CONTOH-BUCKET /...* /output/output.tar.gz adalah `S3Uri` nilai yang Anda simpan sebagai`comprehend-S3uri`,
- *path/* adalah direktori lokal tempat Anda ingin menyimpan output.

4. Untuk mengekstrak output entitas, jalankan perintah berikut pada jendela terminal:

Linux

```
tar -xf path/output.tar.gz -C path/
```

Dengan:

- *path/* adalah filepath ke `output.tar.gz` arsip yang diunduh di perangkat lokal Anda.

macOS

```
tar -xf path/output.tar.gz -C path/
```

Dengan:

- *path/* adalah filepath ke `output.tar.gz` arsip yang diunduh di perangkat lokal Anda.

Windows

```
tar -xf path/output.tar.gz -C path/
```

Dengan:

- *path/* adalah filepath ke `output.tar.gz` arsip yang diunduh di perangkat lokal Anda.

Pada akhir langkah ini, Anda harus memiliki file di perangkat Anda yang dipanggil `output` dengan daftar entitas yang diidentifikasi Amazon Comprehend.

Mengunggah output ke bucket S3

Setelah mengunduh dan mengekstrak file analisis entitas Amazon Comprehend, Anda mengunggah file yang diekstrak `output` ke bucket Amazon S3 Anda.

Untuk mengunggah file keluaran Amazon Comprehend yang diekstrak (Console)

1. Buka konsol Amazon S3 di https://console.aws.amazon.com/s3/.
2. Di Bucket, klik pada nama bucket Anda dan kemudian pilih Upload.
3. Di File dan folder, pilih Tambahkan file.
4. Di kotak dialog, navigasikan ke `output` file yang diekstrak di perangkat Anda, pilih, dan pilih Buka.
5. Simpan pengaturan default untuk Tujuan, Izin, dan Properti.
6. Pilih Upload (Unggah).

Untuk mengunggah file keluaran Amazon Comprehend yang diekstrak () AWS CLI

1. Untuk mengunggah `output` file yang diekstrak ke bucket Anda, gunakan perintah salin:

   Linux

   ```
   aws s3 cp path/output s3://DOC-EXAMPLE-BUCKET/output
   ```

   Dengan:

   - *path/* adalah filepath lokal ke file yang diekstrak, `output`
   - *DOC-EXAMPLE-BUCKET adalah nama bucket* S3 Anda.

   macOS

   ```
   aws s3 cp path/output s3://DOC-EXAMPLE-BUCKET/output
   ```

   Dengan:

   - *path/* adalah filepath lokal ke file yang diekstrak, `output`
   - *DOC-EXAMPLE-BUCKET adalah nama bucket* S3 Anda.

   Windows

   ```
   aws s3 cp path/output s3://DOC-EXAMPLE-BUCKET/output
   ```

   Dengan:

   - *path/* adalah filepath lokal ke file yang diekstrak, `output`
   - *DOC-EXAMPLE-BUCKET adalah nama bucket* S3 Anda.

2. Untuk memastikan bahwa `output` file berhasil diunggah ke bucket S3 Anda, periksa isinya dengan menggunakan perintah list:

   Linux

   ```
   aws s3 ls s3://DOC-EXAMPLE-BUCKET/
   ```

Dengan:

- *DOC-EXAMPLE-BUCKET adalah nama bucket* S3 Anda.

macOS

```
aws s3 ls s3://DOC-EXAMPLE-BUCKET/
```

Dengan:

- *DOC-EXAMPLE-BUCKET adalah nama bucket* S3 Anda.

Windows

```
aws s3 ls s3://DOC-EXAMPLE-BUCKET/
```

Dengan:

- *DOC-EXAMPLE-BUCKET adalah nama bucket* S3 Anda.

Mengonversi output ke format metadata Amazon Kendra

Untuk mengonversi output Amazon Comprehend ke metadata Amazon Kendra, Anda menjalankan skrip Python 3. Jika Anda menggunakan Konsol, Anda gunakan AWS CloudShell untuk langkah ini.

Untuk menjalankan skrip Python 3 (Console)

1. Unduh file zip converter.py.zip di perangkat Anda.
2. Ekstrak file `converter.py` Python 3.
3. Masuk ke AWSManagement Console dan pastikan AWS wilayah Anda diatur ke wilayah yang sama dengan bucket S3 dan pekerjaan analisis Amazon Comprehend Anda.
4. Pilih AWS CloudShellikon atau ketik AWSCloudShelldi kotak Cari di bilah navigasi atas untuk meluncurkan lingkungan.

> **Note**
>
> Saat AWS CloudShell diluncurkan di jendela browser baru untuk pertama kalinya, panel selamat datang menampilkan dan mencantumkan fitur-fitur utama. Shell siap untuk interaksi setelah Anda menutup panel ini dan menampilkan prompt perintah.

5. Setelah terminal disiapkan, pilih Tindakan dari panel navigasi dan kemudian pilih Unggah file dari menu.
6. Di kotak dialog yang terbuka, pilih Pilih file dan kemudian pilih file Python 3 yang diunduh `converter.py` dari perangkat Anda. Pilih Upload (Unggah).
7. Di AWS CloudShell lingkungan, masukkan perintah berikut:

```
python3 converter.py
```

8. Ketika antarmuka shell meminta Anda untuk Masukkan nama bucket S3 Anda, masukkan nama bucket S3 Anda dan tekan enter.
9. Ketika antarmuka shell meminta Anda untuk Masukkan filepath penuh ke file output Comprehend Anda, masukkan dan tekan enter. **`output`**
10. Ketika antarmuka shell meminta Anda untuk Memasukkan filepath penuh ke folder metadata Anda, masukkan dan tekan enter. **`metadata/`**

> **Important**
>
> Agar metadata diformat dengan benar, nilai input dalam langkah 8-10 harus tepat.

Untuk menjalankan script Python 3 () AWS CLI

1. Untuk mengunduh file Python 3`converter.py`, jalankan perintah berikut pada jendela terminal:

   Linux

   ```
   curl -o path/converter.py.zip https://docs.aws.amazon.com/kendra/latest/dg/
   samples/converter.py.zip
   ```

   Dengan:

- *path/* adalah filepath ke lokasi tempat Anda ingin menyimpan file zip.

macOS

```
curl -o path/converter.py.zip https://docs.aws.amazon.com/kendra/latest/dg/
samples/converter.py.zip
```

Dengan:

- *path/* adalah filepath ke lokasi tempat Anda ingin menyimpan file zip.

Windows

```
curl -o path/converter.py.zip https://docs.aws.amazon.com/kendra/latest/dg/
samples/converter.py.zip
```

Dengan:

- *path/* adalah filepath ke lokasi tempat Anda ingin menyimpan file zip.

2. Untuk mengekstrak file Python 3, jalankan perintah berikut pada jendela terminal:

Linux

```
unzip path/converter.py.zip -d path/
```

Dengan:

- *path/adalah* filepath untuk disimpan Anda. `converter.py.zip`

macOS

```
unzip path/converter.py.zip -d path/
```

Dengan:

- *path/adalah* filepath untuk disimpan Anda. `converter.py.zip`

Windows

```
tar -xf path/converter.py.zip -C path/
```

Dengan:

- *path/adalah* filepath untuk disimpan Anda. `converter.py.zip`

3. Pastikan bahwa Boto3 diinstal pada perangkat Anda dengan menjalankan perintah berikut.

Linux

```
pip3 show boto3
```

macOS

```
pip3 show boto3
```

Windows

```
pip3 show boto3
```

> **Note**
>
> Jika Anda tidak menginstal Boto3, jalankan `pip3 install boto3` untuk menginstalnya.

4. Untuk menjalankan script Python 3 untuk mengkonversi `output` file, jalankan perintah berikut.

Linux

```
python path/converter.py
```

Dengan:

- *path/adalah* filepath untuk disimpan Anda. `converter.py.zip`

macOS

```
python path/converter.py
```

Dengan:

- *path/adalah* filepath untuk disimpan Anda. `converter.py.zip`

Windows

```
python path/converter.py
```

Dengan:

- *path/adalah* filepath untuk disimpan Anda. `converter.py.zip`

5. Ketika AWS CLI meminta Anda untuk`Enter the name of your S3 bucket`, masukkan nama bucket S3 Anda dan tekan enter.
6. Ketika AWS CLI meminta Anda untuk`Enter the full filepath to your Comprehend output file`, masukkan **`output`** dan tekan enter.
7. Ketika AWS CLI meminta Anda untuk`Enter the full filepath to your metadata folder`, masukkan **`metadata/`** dan tekan enter.

> **Important**
>
> Agar metadata diformat dengan benar, nilai input dalam langkah 5-7 harus tepat.

Pada akhir langkah ini, metadata yang diformat disimpan di dalam `metadata` folder di bucket S3 Anda.

Membersihkan bucket Amazon S3 Anda

Karena indeks Amazon Kendra menyinkronkan semua file yang disimpan dalam bucket, kami sarankan Anda membersihkan bucket Amazon S3 untuk mencegah hasil pencarian yang berlebihan.

Untuk membersihkan bucket Amazon S3 (Console)

1. Buka konsol Amazon S3 di https://console.aws.amazon.com/s3/.
2. Di Bucket, pilih bucket Anda, lalu pilih folder keluaran analisis entitas Amazon Comprehend, file analisis entitas Amazon Comprehend, dan `.temp` file Amazon Comprehend yang diekstrak. `output`
3. Dari tab Ikhtisar pilih Menghapus.
4. Di Hapus objek, pilih Hapus objek secara permanen? dan masukkan **`permanently delete`** di bidang input teks.
5. Pilih Hapus objek.

Untuk membersihkan bucket Amazon S3 () AWS CLI

1. Untuk menghapus semua file dan folder di bucket S3 Anda kecuali `metadata` folder `data` dan, gunakan perintah remove diAWS CLI:

   Linux

   ```
   aws s3 rm s3://DOC-EXAMPLE-BUCKET/ --recursive --exclude "data/*" --exclude
    "metadata/*"
   ```

   Dengan:

   - *`DOC-EXAMPLE-BUCKET adalah nama bucket`* S3 Anda.

   macOS

   ```
   aws s3 rm s3://DOC-EXAMPLE-BUCKET/ --recursive --exclude "data/*" --exclude
    "metadata/*"
   ```

   Dengan:

   - *`DOC-EXAMPLE-BUCKET adalah nama bucket`* S3 Anda.

Windows

```
aws s3 rm s3://DOC-EXAMPLE-BUCKET/ --recursive --exclude "data/*" --exclude
 "metadata/*"
```

Dengan:

- *DOC-EXAMPLE-BUCKET adalah nama bucket* S3 Anda.

2. Untuk memastikan bahwa objek berhasil dihapus dari bucket S3 Anda, periksa isinya dengan menggunakan perintah list:

Linux

```
aws s3 ls s3://DOC-EXAMPLE-BUCKET/
```

Dengan:

- *DOC-EXAMPLE-BUCKET adalah nama bucket* S3 Anda.

macOS

```
aws s3 ls s3://DOC-EXAMPLE-BUCKET/
```

Dengan:

- *DOC-EXAMPLE-BUCKET adalah nama bucket* S3 Anda.

Windows

```
aws s3 ls s3://DOC-EXAMPLE-BUCKET/
```

Dengan:

- *DOC-EXAMPLE-BUCKET adalah nama bucket* S3 Anda.

Pada akhir langkah ini, Anda telah mengonversi keluaran analisis entitas Amazon Comprehend ke metadata Amazon Kendra. Anda sekarang siap untuk membuat indeks Amazon Kendra.

Langkah 4: Membuat indeks Amazon Kendra dan menelan metadata

Untuk mengimplementasikan solusi pencarian cerdas Anda, Anda membuat indeks Amazon Kendra dan menyerap data S3 dan metadata ke dalamnya.

Sebelum menambahkan metadata ke indeks Amazon Kendra, Anda membuat kolom indeks kustom yang sesuai dengan atribut dokumen kustom, yang pada gilirannya sesuai dengan jenis entitas Amazon Comprehend. Amazon Kendra menggunakan kolom indeks dan atribut dokumen khusus yang Anda buat untuk mencari dan memfilter dokumen Anda.

Untuk informasi selengkapnya, lihat Mengindeks dan Membuat atribut dokumen kustom.

Topik

- Membuat indeks Amazon Kendra
- Memperbarui peran IAM untuk akses Amazon S3
- Membuat kolom indeks pencarian khusus Amazon Kendra
- Menambahkan bucket Amazon S3 sebagai sumber data untuk indeks
- Menyinkronkan indeks Amazon Kendra

Membuat indeks Amazon Kendra

Untuk mengkueri dokumen sumber Anda, Anda membuat indeks Amazon Kendra.

Jika Anda menggunakan langkah ini, Anda membuat dan melampirkan peran dan kebijakan AWS IAM yang memungkinkan Amazon Kendra mengakses CloudWatch log Anda sebelum membuat indeks. AWS CLI Untuk informasi selengkapnya, lihat Prasyarat.

Untuk membuat indeks Amazon Kendra (Konsol)

1. Buka konsol Amazon Kendra di https://console.aws.amazon.com/kendra/.

> **Important**
>
> Pastikan Anda berada di wilayah yang sama tempat Anda membuat pekerjaan analisis entitas Amazon Comprehend dan bucket Amazon S3 Anda. Jika Anda berada di wilayah lain, pilih AWS wilayah tempat Anda membuat bucket Amazon S3 dari pemilih Wilayah di bilah navigasi atas.

2. Pilih Buat indeks.
3. Untuk detail Indeks pada halaman Tentukan detail indeks, lakukan hal berikut:
   a. Untuk nama Indeks, masukkan**`kendra-index`**.
   b. Jaga agar bidang Deskripsi kosong.
   c. Untuk peran IAM, pilih Buat peran baru. Peran ini menyediakan akses ke bucket Amazon S3 Anda.
   d. Untuk Nama peran, masukkan **`kendra-role`**. Peran IAM akan memiliki awalan`AmazonKendra-`.
   e. Simpan pengaturan default untuk Enkripsi dan Tag dan pilih Berikutnya.
4. Untuk Pengaturan kontrol akses pada halaman Konfigurasi kontrol akses pengguna, pilih Tidak, lalu pilih Berikutnya.
5. Untuk Menyediakan edisi pada halaman Rincian penyediaan, pilih Edisi pengembang dan pilih Buat.

Untuk membuat indeks Amazon Kendra () AWS CLI

1. Untuk membuat dan melampirkan peran IAM untuk Amazon Kendra yang mengenalinya sebagai entitas tepercaya, lakukan hal berikut:
   a. Simpan kebijakan kepercayaan berikut sebagai file JSON yang dipanggil `kendra-trust-policy.json` dalam editor teks di perangkat lokal Anda.

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

```
        },
        "Action": "sts:AssumeRole"
    }
}
```

b. Untuk membuat peran IAM yang dipanggil `kendra-role` dan melampirkan `kendra-trust-policy.json` file yang disimpan ke dalamnya, gunakan perintah create-role:

Linux

```
aws iam create-role \
          --role-name kendra-role \
          --assume-role-policy-document file://path/kendra-trust-policy.json
```

Dengan:

- *path/* adalah filepath ke perangkat lokal `kendra-trust-policy.json` Anda.

macOS

```
aws iam create-role \
          --role-name kendra-role \
          --assume-role-policy-document file://path/kendra-trust-policy.json
```

Dengan:

- *path/* adalah filepath ke perangkat lokal `kendra-trust-policy.json` Anda.

Windows

```
aws iam create-role ^
          --role-name kendra-role ^
          --assume-role-policy-document file://path/kendra-trust-policy.json
```

Dengan:

- *path/* adalah filepath ke perangkat lokal `kendra-trust-policy.json` Anda.

c. Salin Amazon Resource Name (ARN) ke editor teks Anda dan simpan secara lokal sebagai. `kendra-role-arn`

> **Note**
>
> ARN memiliki format yang mirip dengan arn:aws:iam*: :123456789012:role/kendra-role*. Anda membutuhkan ARN yang Anda simpan `kendra-role-arn` untuk menjalankan pekerjaan Amazon Kendra.

2. Sebelum membuat indeks, Anda harus memberikan izin untuk menulis ke CloudWatch Log. `kendra-role` Caranya, lakukan langkah-langkah berikut:

   a. Simpan kebijakan kepercayaan berikut sebagai file JSON yang dipanggil `kendra-cloudwatch-policy.json` dalam editor teks di perangkat lokal Anda.

```
{
   "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:*"
      }
   ]
}
```

Ganti *aws-region dengan AWS wilayah* Anda, dan *aws-account-id*dengan 12 digit AWS ID akun Anda.

b. Untuk membuat kebijakan IAM untuk mengakses CloudWatch Log, gunakan perintah create-policy:

Linux

```
aws iam create-policy \
          --policy-name kendra-cloudwatch-policy \
          --policy-document file://path/kendra-cloudwatch-policy.json
```

Dengan:

- *path/* adalah filepath ke perangkat lokal `kendra-cloudwatch-policy.json` Anda.

macOS

```
aws iam create-policy \
          --policy-name kendra-cloudwatch-policy \
          --policy-document file://path/kendra-cloudwatch-policy.json
```

Dengan:

- *path/* adalah filepath ke perangkat lokal `kendra-cloudwatch-policy.json` Anda.

Windows

```
aws iam create-policy ^
          --policy-name kendra-cloudwatch-policy ^
```

```
        --policy-document file://path/kendra-cloudwatch-policy.json
```

Dengan:

- *path/* adalah filepath ke perangkat lokal `kendra-cloudwatch-policy.json` Anda.

c. Salin Amazon Resource Name (ARN) ke editor teks Anda dan simpan secara lokal sebagai. `kendra-cloudwatch-arn`

> **Note**
>
> ARN memiliki format yang mirip dengan *arn:aws:iam: :123456789012:role/*. kendra-cloudwatch-policy Anda memerlukan ARN yang Anda simpan `kendra-cloudwatch-arn` untuk melampirkan peran `kendra-cloudwatch-policy` IAM Anda.

d. Untuk melampirkan `kendra-cloudwatch-policy` peran IAM Anda, gunakan attach-role-policyperintah:

Linux

```
aws iam attach-role-policy \
        --policy-arn policy-arn \
        --role-name kendra-role
```

Dengan:

- *policy-arn* adalah Anda diselamatkan. `kendra-cloudwatch-arn`

macOS

```
aws iam attach-role-policy \
        --policy-arn policy-arn \
        --role-name kendra-role
```

Dengan:

- *policy-arn* adalah Anda diselamatkan. `kendra-cloudwatch-arn`

Windows

```
aws iam attach-role-policy ^
          --policy-arn policy-arn ^
          --role-name kendra-role
```

Dengan:

- *policy-arn* adalah Anda diselamatkan. `kendra-cloudwatch-arn`

3. Untuk membuat indeks, gunakan perintah create-index:

Linux

```
aws kendra create-index \
        --name kendra-index \
        --edition DEVELOPER_EDITION \
        --role-arn role-arn \
        --region aws-region
```

Dengan:

- *peran-arn adalah Anda diselamatkan*, `kendra-role-arn`
- *aws-region adalah wilayah* AndaAWS.

macOS

```
aws kendra create-index \
        --name kendra-index \
        --edition DEVELOPER_EDITION \
        --role-arn role-arn \
        --region aws-region
```

Dengan:

- *peran-arn adalah Anda diselamatkan*, `kendra-role-arn`
- *aws-region adalah wilayah* AndaAWS.

Windows

```
aws kendra create-index ^
        --name kendra-index ^
        --edition DEVELOPER_EDITION ^
        --role-arn role-arn ^
        --region aws-region
```

Dengan:

- *peran-arn adalah Anda diselamatkan*, `kendra-role-arn`
- *aws-region adalah wilayah* AndaAWS.

4. Salin indeks `Id` dan simpan dalam editor teks sebagai`kendra-index-id`. `Id`Membantu Anda melacak status pembuatan indeks Anda.
5. Untuk melacak kemajuan pekerjaan pembuatan indeks Anda, gunakan perintah describe-index:

Linux

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

Dengan:

- *kendra-index-id*adalah Anda yang diselamatkan`kendra-index-id`,
- *aws-region adalah wilayah* AndaAWS.

macOS

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

Dengan:

- *kendra-index-id*adalah Anda yang diselamatkan`kendra-index-id`,

- *aws-region adalah wilayah* AndaAWS.

Windows

```
aws kendra describe-index ^
        --id kendra-index-id ^
        --region aws-region
```

Dengan:

- *kendra-index-id*adalah Anda yang diselamatkan`kendra-index-id`,
- *aws-region adalah wilayah* AndaAWS.

Proses pembuatan indeks rata-rata memakan waktu 15 menit, tetapi bisa memakan waktu lebih lama. Ketika status indeks aktif, indeks Anda siap digunakan. Sementara indeks Anda sedang dibuat, Anda dapat memulai langkah berikutnya.

Jika Anda menggunakan langkah ini, Anda membuat dan melampirkan kebijakan IAM ke peran IAM Amazon Kendra Anda yang memberikan izin indeks Anda untuk mengakses bucket S3 Anda. AWS CLI

Memperbarui peran IAM untuk akses Amazon S3

Saat indeks dibuat, Anda memperbarui peran IAM Amazon Kendra Anda untuk memungkinkan indeks yang Anda buat untuk membaca data dari bucket Amazon S3 Anda. Untuk informasi lebih lanjut, lihat Peran akses IAM untuk Amazon Kendra.

Untuk memperbarui peran IAM Anda (Console)

1. Buka konsol IAM di https://console.aws.amazon.com/iam/.
2. Di panel navigasi kiri, pilih Peran dan masukkan **`kendra-role`** di kotak Cari di atas Nama peran.
3. Dari opsi yang disarankan, klik`kendra-role`.
4. Di Ringkasan, pilih Lampirkan kebijakan.
5. Di Lampirkan izin, di kotak Pencarian, masukkan **`S3`** dan pilih kotak centang di samping ReadOnlyAccess kebijakan AmazonS3 dari opsi yang disarankan.

6. Pilih Lampirkan kebijakan. Pada halaman Ringkasan, Anda sekarang akan melihat dua kebijakan yang dilampirkan pada peran IAM.
7. Kembali ke konsol Amazon Kendra di https://console.aws.amazon.com/kendra/ dan tunggu status indeks Anda berubah dari Creating to Active sebelum melanjutkan ke langkah berikutnya.

Untuk memperbarui peran IAM Anda () AWS CLI

1. Simpan teks berikut dalam file JSON yang dipanggil `kendra-S3-access-policy.json` dalam editor teks pada perangkat lokal Anda.

```
{
   "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"
         ]
      }
```

```
    ]
}
```

Ganti *DOC-EXAMPLE-BUCKET* dengan nama bucket S3 Anda, *aws-region dengan wilayah* Anda, dengan ID akun AWS 12 digit Anda, dan *aws-account-id*dengan yang Anda simpanAWS. *kendra-index-id*kendra-index-id

2. Untuk membuat kebijakan IAM untuk mengakses bucket S3 Anda, gunakan perintah create-policy:

   Linux

   ```
   aws iam create-policy \
             --policy-name kendra-S3-access-policy \
             --policy-document file://path/kendra-S3-access-policy.json
   ```

   Dengan:

   - *path/* adalah filepath ke perangkat lokal kendra-S3-access-policy.json Anda.

   macOS

   ```
   aws iam create-policy \
             --policy-name kendra-S3-access-policy \
             --policy-document file://path/kendra-S3-access-policy.json
   ```

   Dengan:

   - *path/* adalah filepath ke perangkat lokal kendra-S3-access-policy.json Anda.

   Windows

   ```
   aws iam create-policy ^
             --policy-name kendra-S3-access-policy ^
             --policy-document file://path/kendra-S3-access-policy.json
   ```

   Dengan:

   - *path/* adalah filepath ke perangkat lokal kendra-S3-access-policy.json Anda.

3. Salin Amazon Resource Name (ARN) ke editor teks Anda dan simpan secara lokal sebagai. `kendra-S3-access-arn`

> **Note**
>
> ARN memiliki format yang mirip dengan arn:aws:iam*: :123456789012:role/Kendra-S3-access-policy*. Anda memerlukan ARN yang Anda simpan `kendra-S3-access-arn` untuk melampirkan peran `kendra-S3-access-policy` IAM Anda.

4. Untuk melampirkan `kendra-S3-access-policy` peran IAM Amazon Kendra Anda, gunakan perintah attach-role-policy:

   Linux

   ```
   aws iam attach-role-policy \
            --policy-arn policy-arn \
            --role-name kendra-role
   ```

   Dengan:

   - *policy-arn* adalah Anda diselamatkan. `kendra-S3-access-arn`

   macOS

   ```
   aws iam attach-role-policy \
            --policy-arn policy-arn \
            --role-name kendra-role
   ```

   Dengan:

   - *policy-arn* adalah Anda diselamatkan. `kendra-S3-access-arn`

   Windows

   ```
   aws iam attach-role-policy ^
            --policy-arn policy-arn ^
            --role-name kendra-role
   ```

Dengan:

- *policy-arn* adalah Anda diselamatkan. `kendra-S3-access-arn`

Membuat kolom indeks pencarian khusus Amazon Kendra

Untuk mempersiapkan Amazon Kendra untuk mengenali metadata Anda sebagai atribut dokumen kustom, Anda membuat bidang kustom yang sesuai dengan jenis entitas Amazon Comprehend. Anda memasukkan sembilan jenis entitas Amazon Comprehend berikut sebagai bidang kustom:

- COMMERCIAL_ITEM
- TANGGAL
- ACARA
- LOKASI
- ORGANISASI
- LAINNYA
- PRIBADI
- KUANTITAS
- JUDUL

> **Important**
>
> Jenis entitas yang salah eja tidak akan dikenali oleh indeks.

Untuk membuat bidang khusus untuk indeks Amazon Kendra (Konsol)

1. Buka konsol Amazon Kendra di https://console.aws.amazon.com/kendra/.
2. Dari daftar Indeks, klik`kendra-index`.
3. Dari panel navigasi kiri, di bawah Manajemen data, pilih Definisi Facet.
4. Dari menu Index fields, pilih Add field.
5. Dalam Tambahkan indeks bidang kotak dialog, lakukan hal berikut:

   a. Di Nama bidang, masukkan**`COMMERCIAL_ITEM`**.

b. Di Tipe data, pilih String daftar.

c. Di Jenis penggunaan, pilih Facetable, Searchable, dan Displayable, lalu pilih Tambah.

d. Ulangi langkah a ke c untuk setiap jenis entitas Amazon Comprehend: COMMERCIAL_ITEM, DATE, EVENT, LOCATION, ORGANIZATION, OTHER, PERSON, QUANTITY, TITLE.

Konsol menampilkan pesan penambahan lapangan yang berhasil. Anda dapat memilih untuk menutupnya sebelum melanjutkan dengan langkah berikutnya.

Untuk membuat bidang khusus untuk indeks Amazon Kendra () AWS CLI

1. Simpan teks berikut sebagai file JSON yang dipanggil `custom-attributes.json` dalam editor teks di perangkat lokal Anda.

```
[
   {
       "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. Untuk membuat bidang kustom dalam indeks Anda, gunakan perintah update-index:

   Linux

   ```
   aws kendra update-index \
           --id kendra-index-id \
           --document-metadata-configuration-updates file://path/custom-
   attributes.json \
           --region aws-region
   ```

   Dengan:

   - *kendra-index-id*adalah Anda yang diselamatkan`kendra-index-id`,
   - *path/* adalah filepath ke perangkat lokal `custom-attributes.json` Anda,
   - *aws-region adalah wilayah* AndaAWS.

   macOS

   ```
   aws kendra update-index \
           --id kendra-index-id \
           --document-metadata-configuration-updates file://path/custom-
   attributes.json \
           --region aws-region
   ```

   Dengan:

   - *kendra-index-id*adalah Anda yang diselamatkan`kendra-index-id`,

- *path/* adalah filepath ke perangkat lokal `custom-attributes.json` Anda,
- *aws-region adalah wilayah* AndaAWS.

Windows

```
aws kendra update-index ^
        --id kendra-index-id ^
        --document-metadata-configuration-updates file://path/custom-
attributes.json ^
        --region aws-region
```

Dengan:

- *kendra-index-id*adalah Anda yang diselamatkan`kendra-index-id`,
- *path/* adalah filepath ke perangkat lokal `custom-attributes.json` Anda,
- *aws-region adalah wilayah* AndaAWS.

3. Untuk memverifikasi bahwa atribut kustom telah ditambahkan ke indeks Anda, gunakan perintah describe-index:

Linux

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

Dengan:

- *kendra-index-id*adalah Anda diselamatkan`kendra-index-id`,
- *aws-region adalah wilayah* AndaAWS.

macOS

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

Dengan:

- *kendra-index-id*adalah Anda diselamatkan`kendra-index-id`,
- *aws-region adalah wilayah* AndaAWS.

Windows

```
aws kendra describe-index ^
        --id kendra-index-id ^
        --region aws-region
```

Dengan:

- *kendra-index-id*adalah Anda diselamatkan`kendra-index-id`,
- *aws-region adalah wilayah* AndaAWS.

Menambahkan bucket Amazon S3 sebagai sumber data untuk indeks

Sebelum dapat menyinkronkan indeks, Anda harus menghubungkan sumber data S3 Anda ke indeks tersebut.

Untuk menghubungkan bucket S3 ke indeks Amazon Kendra (Konsol)

1. Buka konsol Amazon Kendra di https://console.aws.amazon.com/kendra/.
2. Dari daftar Indeks, klik`kendra-index`.
3. Dari menu navigasi kiri, di bawah Manajemen data, pilih Sumber data.
4. Di bawah bagian Pilih jenis konektor sumber data, navigasikan ke Amazon S3, dan pilih Tambah konektor.
5. Di halaman Tentukan detail sumber data, lakukan hal berikut:
   a. Di bawah Nama dan deskripsi, untuk Nama sumber data, masukkan**`S3-data-source`**.
   b. Jauhkan bagian Deskripsi kosong.
   c. Simpan pengaturan default untuk Tag.
   d. Pilih Selanjutnya.
6. Pada halaman Konfigurasi pengaturan sinkronisasi, di bagian Lingkup sinkronisasi, lakukan hal berikut:

a. Di Masukkan lokasi sumber data, pilih Jelajahi S3.

b. Di Pilih sumber daya, pilih bucket S3 Anda, lalu pilih Pilih.

c. Di Lokasi folder awalan file metadata, pilih Jelajahi S3.

d. Di Pilih sumber daya, klik nama bucket Anda dari daftar bucket.

e. Untuk Objects, pilih kotak opsi untuk `metadata` dan pilih Choose. Bidang lokasi sekarang harus mengatakan`metadata/`.

f. Simpan pengaturan default untuk lokasi file konfigurasi daftar kontrol akses, Pilih kunci dekripsi, dan Konfigurasi tambahan.

7. Untuk peran IAM, pada halaman Konfigurasi pengaturan sinkronisasi, pilih`kendra-role`.
8. Pada halaman Konfigurasi pengaturan sinkronisasi, di bawah Sinkronisasi jadwal jalankan, untuk Frekuensi, pilih Jalankan sesuai permintaan, lalu pilih Berikutnya.
9. Pada halaman Tinjau dan buat, tinjau pilihan Anda untuk detail sumber data dan pilih Tambahkan sumber data.

Untuk menghubungkan bucket S3 ke indeks Amazon Kendra () AWS CLI

1. Simpan teks berikut sebagai file JSON yang dipanggil `S3-data-connector.json` dalam editor teks di perangkat lokal Anda.

```
{
   "S3Configuration":{
      "BucketName":"DOC-EXAMPLE-BUCKET",
      "DocumentsMetadataConfiguration":{
         "S3Prefix":"metadata"
      }
   }
}
```

   Ganti *DOC-EXAMPLE-BUCKET dengan nama bucket* S3 Anda.

2. Untuk menghubungkan bucket S3 Anda ke indeks Anda, gunakan create-data-sourceperintah:

   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
```

Dengan:

- *kendra-index-id*adalah Anda diselamatkan`kendra-index-id`,
- *path/* adalah filepath ke perangkat lokal `S3-data-connector.json` Anda,
- *peran-arn adalah Anda diselamatkan*, `kendra-role-arn`
- *aws-region adalah wilayah* AndaAWS.

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
```

Dengan:

- *kendra-index-id*adalah Anda diselamatkan`kendra-index-id`,
- *path/* adalah filepath ke perangkat lokal `S3-data-connector.json` Anda,
- *peran-arn adalah Anda diselamatkan*, `kendra-role-arn`
- *aws-region adalah wilayah* AndaAWS.

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
```

Dengan:

- *kendra-index-id*adalah Anda diselamatkan`kendra-index-id`,
- *path/* adalah filepath ke perangkat lokal `S3-data-connector.json` Anda,
- *peran-arn adalah Anda diselamatkan*, `kendra-role-arn`
- *aws-region adalah wilayah* AndaAWS.

3. Salin konektor `Id` dan simpan dalam editor teks sebagai`S3-connector-id`. The `Id` membantu Anda melacak status proses data-koneksi.
4. Untuk memastikan bahwa sumber data S3 Anda berhasil terhubung, gunakan describe-data-sourceperintah:

   Linux

   ```
   aws kendra describe-data-source \
           --id S3-connector-id \
           --index-id kendra-index-id \
           --region aws-region
   ```

   Dengan:

   - *S3-connector-ID* adalah yang Anda simpan, `S3-connector-id`
   - *kendra-index-id*adalah Anda diselamatkan`kendra-index-id`,
   - *aws-region adalah wilayah* AndaAWS.

   macOS

   ```
   aws kendra describe-data-source \
           --id S3-connector-id \
           --index-id kendra-index-id \
           --region aws-region
   ```

   Dengan:

   - *S3-connector-ID* adalah yang Anda simpan, `S3-connector-id`
   - *kendra-index-id*adalah Anda diselamatkan`kendra-index-id`,

- *aws-region adalah wilayah* AndaAWS.

Windows

```
aws kendra describe-data-source ^
        --id S3-connector-id ^
        --index-id kendra-index-id ^
        --region aws-region
```

Dengan:

- *S3-connector-ID* adalah yang Anda simpan, `S3-connector-id`
- *kendra-index-id*adalah Anda diselamatkan`kendra-index-id`,
- *aws-region adalah wilayah* AndaAWS.

Pada akhir langkah ini, sumber data Amazon S3 Anda terhubung ke indeks.

Menyinkronkan indeks Amazon Kendra

Dengan sumber data Amazon S3 ditambahkan, Anda sekarang menyinkronkan indeks Amazon Kendra Anda ke sana.

Untuk menyinkronkan indeks Amazon Kendra (Konsol)

1. Buka konsol Amazon Kendra di https://console.aws.amazon.com/kendra/.
2. Dari daftar Indeks, klik`kendra-index`.
3. Dari menu navigasi kiri, pilih Sumber data.
4. Dari Sumber data, pilih`S3-data-source`.
5. Dari bilah navigasi atas, pilih Sinkronkan sekarang.

Untuk menyinkronkan indeks Amazon Kendra () AWS CLI

1. Untuk menyinkronkan indeks Anda, gunakan perintah start-data-source-sync-job:

   Linux

```
aws kendra start-data-source-sync-job \
```

```
        --id S3-connector-id \
        --index-id kendra-index-id \
        --region aws-region
```

Dengan:

- *S3-connector-ID* adalah yang Anda simpan, `S3-connector-id`
- *kendra-index-id*adalah Anda diselamatkan`kendra-index-id`,
- *aws-region adalah wilayah* AndaAWS.

macOS

```
aws kendra start-data-source-sync-job \
        --id S3-connector-id \
        --index-id kendra-index-id \
        --region aws-region
```

Dengan:

- *S3-connector-ID* adalah yang Anda simpan, `S3-connector-id`
- *kendra-index-id*adalah Anda diselamatkan`kendra-index-id`,
- *aws-region adalah wilayah* AndaAWS.

Windows

```
aws kendra start-data-source-sync-job ^
        --id S3-connector-id ^
        --index-id kendra-index-id ^
        --region aws-region
```

Dengan:

- *S3-connector-ID* adalah yang Anda simpan, `S3-connector-id`
- *kendra-index-id*adalah Anda diselamatkan`kendra-index-id`,
- *aws-region adalah wilayah* AndaAWS.

2. Untuk memeriksa status sinkronisasi indeks, gunakan perintah list-data-source-sync-jobs:

Linux

```
aws kendra list-data-source-sync-jobs \
        --id S3-connector-id \
        --index-id kendra-index-id \
        --region aws-region
```

Dengan:

- *S3-connector-ID* adalah yang Anda simpan, `S3-connector-id`
- *kendra-index-id*adalah Anda diselamatkan`kendra-index-id`,
- *aws-region adalah wilayah* AndaAWS.

macOS

```
aws kendra list-data-source-sync-jobs \
        --id S3-connector-id \
        --index-id kendra-index-id \
        --region aws-region
```

Dengan:

- *S3-connector-ID* adalah yang Anda simpan, `S3-connector-id`
- *kendra-index-id*adalah Anda diselamatkan`kendra-index-id`,
- *aws-region adalah wilayah* AndaAWS.

Windows

```
aws kendra list-data-source-sync-jobs ^
        --id S3-connector-id ^
        --index-id kendra-index-id ^
        --region aws-region
```

Dengan:

- *S3-connector-ID* adalah yang Anda simpan, `S3-connector-id`
- *kendra-index-id*adalah Anda diselamatkan`kendra-index-id`,

- *aws-region adalah wilayah* AndaAWS.

Pada akhir langkah ini, Anda telah membuat indeks Amazon Kendra yang dapat dicari dan dapat disaring untuk kumpulan data Anda.

Langkah 5: Menanyakan indeks Amazon Kendra

Indeks Amazon Kendra Anda sekarang siap untuk kueri bahasa alami. Saat Anda mencari indeks, Amazon Kendra menggunakan semua data dan metadata yang Anda berikan untuk mengembalikan jawaban paling akurat ke kueri penelusuran Anda.

Ada tiga jenis kueri yang dapat dijawab Amazon Kendra:

- Pertanyaan factoid (pertanyaan “siapa”, “apa”, “kapan”, atau “di mana”)
- Pertanyaan deskriptif (pertanyaan “bagaimana”)
- Pencarian kata kunci (pertanyaan yang maksud dan cakupannya tidak jelas)

Topik

- Menanyakan indeks Amazon Kendra Anda
- Memfilter hasil pencarian

Menanyakan indeks Amazon Kendra Anda

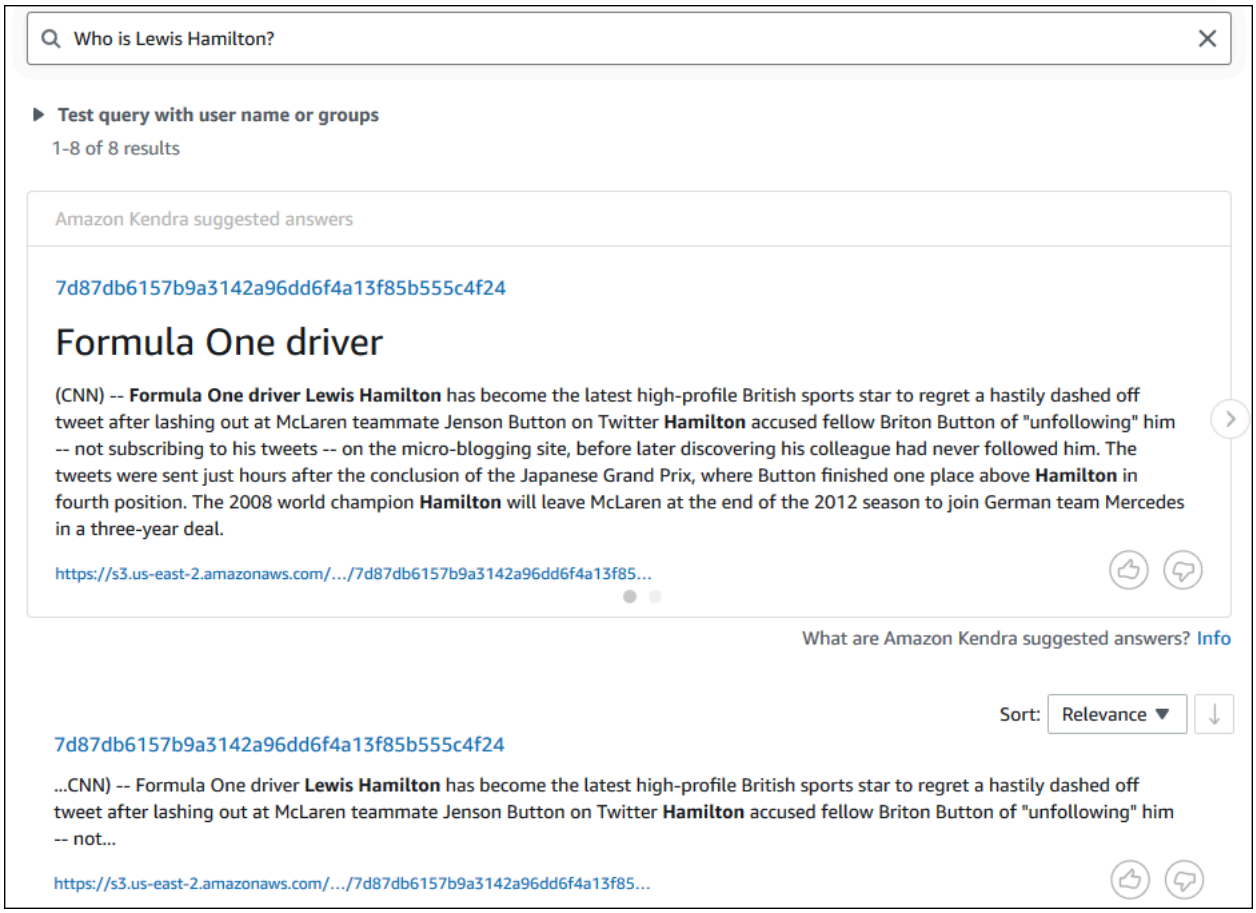
Anda dapat membuat kueri indeks Amazon Kendra menggunakan pertanyaan yang sesuai dengan tiga jenis kueri yang didukung Amazon Kendra. Untuk informasi selengkapnya, lihat Kueri.

Contoh pertanyaan di bagian ini telah dipilih berdasarkan kumpulan data sampel.

Untuk mengkueri indeks Amazon Kendra (Konsol)

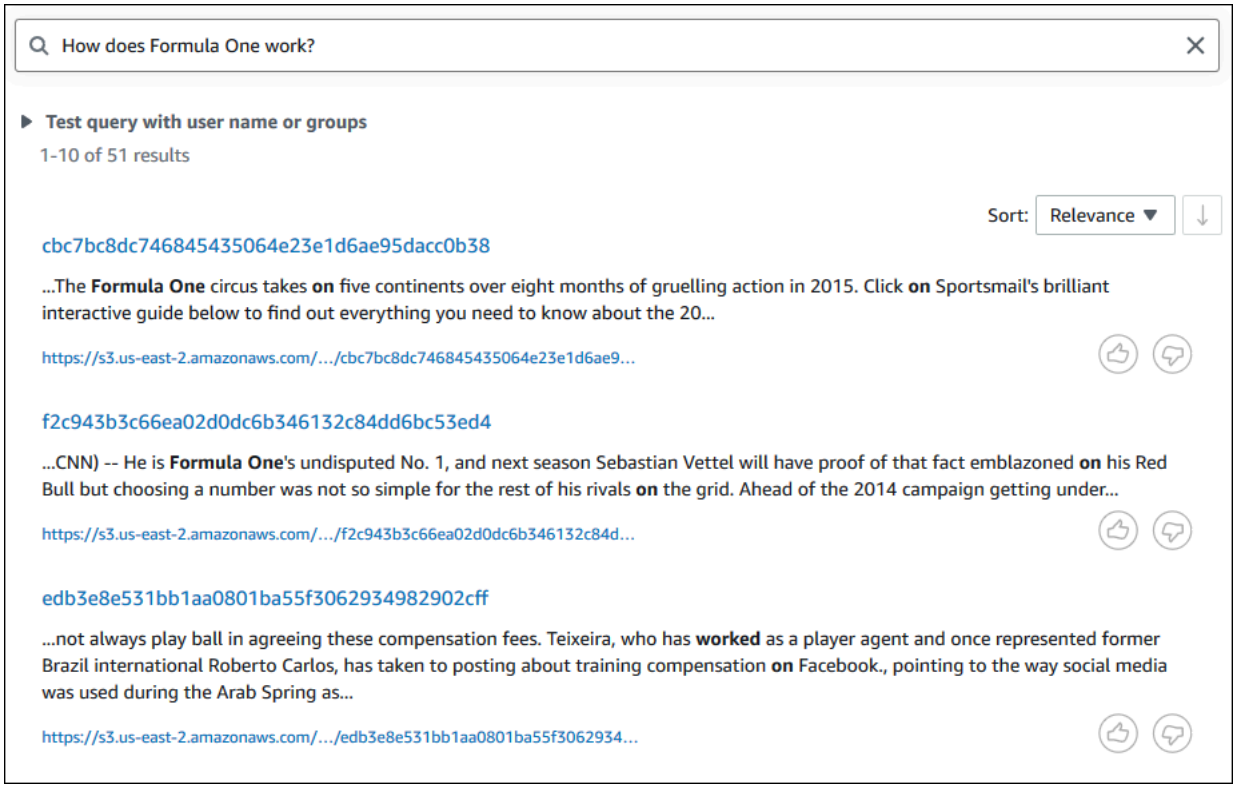
1. Buka konsol Amazon Kendra di https://console.aws.amazon.com/kendra/.
2. Dari daftar Indeks, klik`kendra-index`.
3. Dari menu navigasi kiri, pilih opsi untuk mencari indeks Anda.
4. Untuk menjalankan query factoid sampel, masukkan **`Who is Lewis Hamilton?`** di kotak pencarian dan tekan enter.

Hasil yang dikembalikan pertama adalah jawaban yang disarankan Amazon Kendra, bersama dengan file data yang berisi jawabannya. Hasil lainnya membentuk kumpulan dokumen yang direkomendasikan.



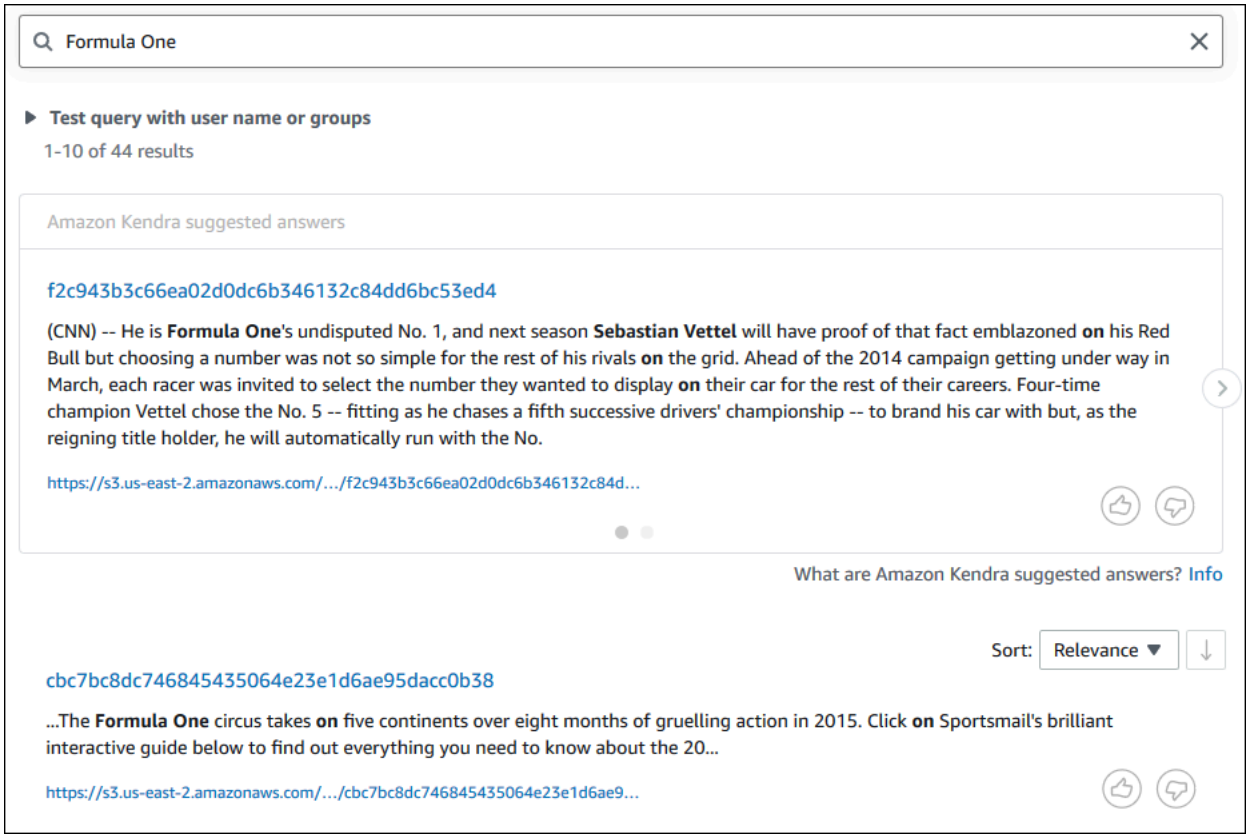
5. Untuk menjalankan kueri deskriptif, masukkan **`How does Formula One work?`** di kotak pencarian dan tekan enter.

   Anda akan melihat hasil lain yang dikembalikan oleh konsol Amazon Kendra, kali ini dengan frasa yang relevan disorot.



6. Untuk menjalankan pencarian kata kunci, masukkan **`Formula One`** di kotak pencarian dan tekan enter.

   Anda akan melihat hasil lain yang dikembalikan oleh konsol Amazon Kendra, diikuti oleh hasil untuk semua sebutan frasa lainnya dalam kumpulan data.



Untuk mengkueri indeks Amazon Kendra () AWS CLI

1. Untuk menjalankan query factoid sampel, gunakan perintah query:

   Linux

   ```
   aws kendra query \
           --index-id kendra-index-id \
           --query-text "Who is Lewis Hamilton?" \
           --region aws-region
   ```

   Dengan:

   - *kendra-index-id*adalah Anda diselamatkan`kendra-index-id`,
   - *aws-region adalah wilayah* AndaAWS.

macOS

```
aws kendra query \
        --index-id kendra-index-id \
        --query-text "Who is Lewis Hamilton?" \
        --region aws-region
```

Dengan:

- *kendra-index-id*adalah Anda diselamatkan`kendra-index-id`,
- *aws-region adalah wilayah* AndaAWS.

Windows

```
aws kendra query ^
        --index-id kendra-index-id ^
        --query-text "Who is Lewis Hamilton?" ^
        --region aws-region
```

Dengan:

- *kendra-index-id*adalah Anda diselamatkan`kendra-index-id`,
- *aws-region adalah wilayah* AndaAWS.

AWS CLIMenampilkan hasil kueri Anda.

2. Untuk menjalankan contoh kueri deskriptif, gunakan perintah query:

Linux

```
aws kendra query \
        --index-id kendra-index-id \
        --query-text "How does Formula One work?" \
        --region aws-region
```

Dengan:

- *kendra-index-id*adalah Anda diselamatkan`kendra-index-id`,

- *aws-region adalah wilayah* AndaAWS.

macOS

```
aws kendra query \
        --index-id kendra-index-id \
        --query-text "How does Formula One work?" \
        --region aws-region
```

Dengan:

- *kendra-index-id*adalah Anda diselamatkan`kendra-index-id`,
- *aws-region adalah wilayah* AndaAWS.

Windows

```
aws kendra query ^
        --index-id kendra-index-id ^
        --query-text "How does Formula One work?" ^
        --region aws-region
```

Dengan:

- *kendra-index-id*adalah Anda diselamatkan`kendra-index-id`,
- *aws-region adalah wilayah* AndaAWS.

AWS CLIMenampilkan hasil untuk kueri Anda.

3. Untuk menjalankan pencarian kata kunci sampel, gunakan perintah query:

Linux

```
aws kendra query \
        --index-id kendra-index-id \
        --query-text "Formula One" \
        --region aws-region
```

Dengan:

- *kendra-index-id*adalah Anda diselamatkan`kendra-index-id`,
- *aws-region adalah wilayah* AndaAWS.

macOS

```
aws kendra query \
        --index-id kendra-index-id \
        --query-text "Formula One" \
        --region aws-region
```

Dengan:

- *kendra-index-id*adalah Anda diselamatkan`kendra-index-id`,
- *aws-region adalah wilayah* AndaAWS.

Windows

```
aws kendra query ^
        --index-id kendra-index-id ^
        --query-text "Formula One" ^
        --region aws-region
```

Dengan:

- *kendra-index-id*adalah Anda diselamatkan`kendra-index-id`,
- *aws-region adalah wilayah* AndaAWS.

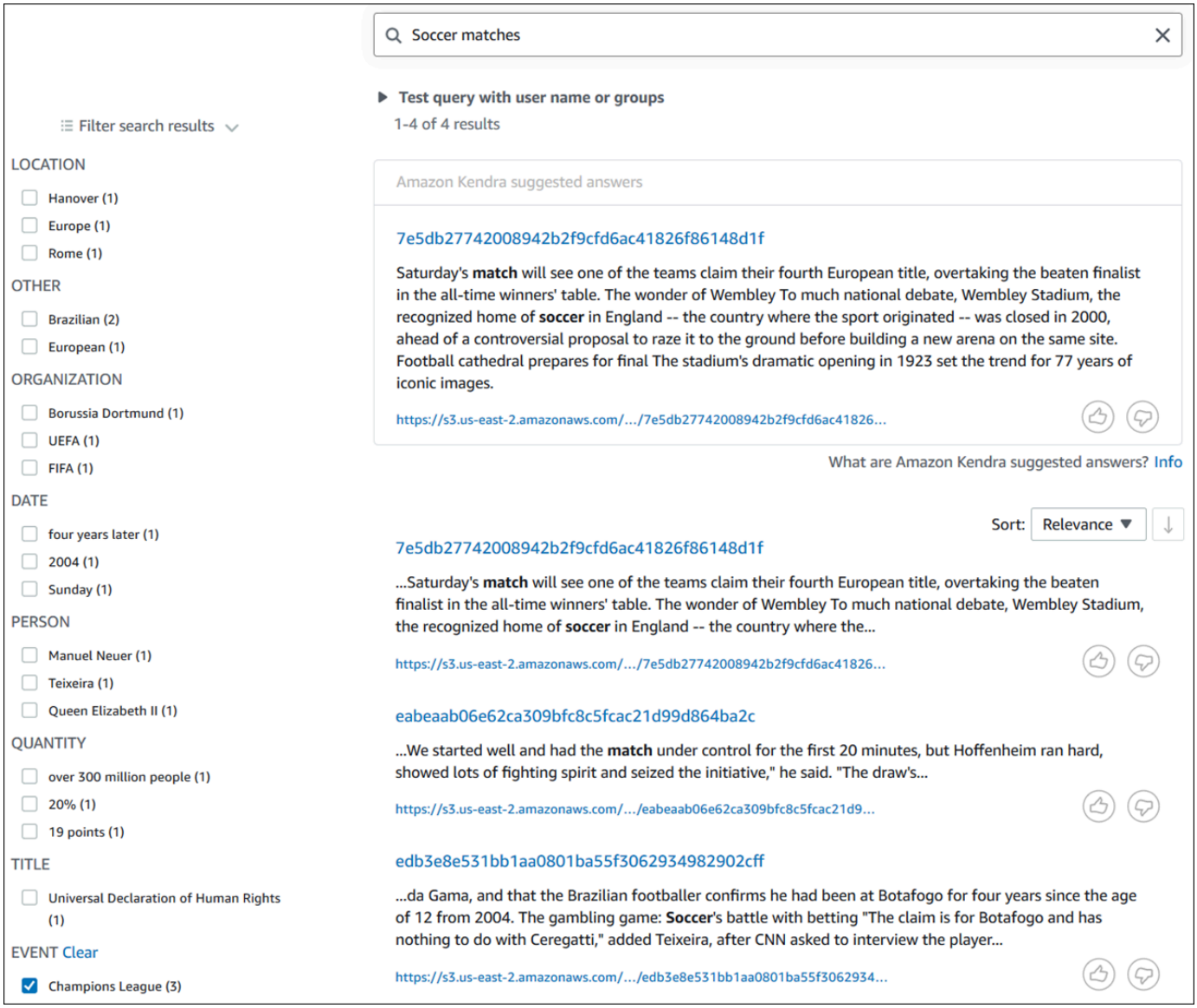
AWS CLIMenampilkan jawaban yang dikembalikan untuk kueri Anda.

Memfilter hasil pencarian

Anda dapat memfilter dan mengurutkan hasil pencarian menggunakan atribut dokumen khusus di konsol Amazon Kendra. Untuk informasi selengkapnya tentang cara Amazon Kendra memproses kueri, lihat Memfilter kueri.

Untuk memfilter hasil pencarian Anda (Konsol)

1. Buka konsol Amazon Kendra di https://console.aws.amazon.com/kendra/.
2. Dari daftar Indeks, klik`kendra-index`.
3. Dari menu navigasi kiri, pilih opsi untuk mencari indeks Anda.
4. Di kotak pencarian, masukkan **`Soccer matches`** sebagai kueri dan tekan enter.
5. Dari menu navigasi kiri, pilih Filter hasil pencarian untuk melihat daftar aspek yang dapat Anda gunakan untuk memfilter pencarian Anda.
6. Pilih kotak centang untuk “Liga Champions” di bawah subjudul EVENT, untuk melihat hasil pencarian Anda hanya disaring oleh hasil yang berisi “Liga Champions”.



Untuk memfilter hasil pencarian Anda (AWS CLI)

1. Untuk melihat entitas dari jenis tertentu (sepertiEVENT) yang tersedia untuk pencarian, gunakan perintah query:

   Linux

   ```
   aws kendra query \
           --index-id kendra-index-id \
           --query-text "Soccer matches" \
           --facets '[{"DocumentAttributeKey":"EVENT"}]' \
           --region aws-region
   ```

   Dengan:

   - *kendra-index-id*adalah Anda diselamatkan`kendra-index-id`,
   - *aws-region adalah wilayah* AndaAWS.

   macOS

   ```
   aws kendra query \
           --index-id kendra-index-id \
           --query-text "Soccer matches" \
           --facets '[{"DocumentAttributeKey":"EVENT"}]' \
           --region aws-region
   ```

   Dengan:

   - *kendra-index-id*adalah Anda diselamatkan`kendra-index-id`,
   - *aws-region adalah wilayah* AndaAWS.

   Windows

   ```
   aws kendra query ^
           --index-id kendra-index-id ^
           --query-text "Soccer matches" ^
           --facets '[{"DocumentAttributeKey":"EVENT"}]' ^
           --region aws-region
   ```

Dengan:

- *kendra-index-id*adalah Anda diselamatkan`kendra-index-id`,
- *aws-region adalah wilayah* AndaAWS.

AWS CLIMenampilkan hasil pencarian. Untuk mendapatkan daftar aspek jenis`EVENT`, arahkan ke bagian "FacetResults" dari AWS CLI output untuk melihat daftar aspek yang dapat disaring dengan jumlah mereka. Misalnya, salah satu aspeknya adalah “Liga Champions”.

> **Note**
>
> Alih-alih`EVENT`, Anda dapat memilih salah satu bidang indeks yang Anda buat the section called “Membuat indeks Amazon Kendra” untuk `DocumentAttributeKey` nilainya.

2. Untuk menjalankan pencarian yang sama tetapi hanya memfilter berdasarkan hasil yang berisi “Liga Champions”, gunakan perintah kueri:

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
```

Dengan:

- *kendra-index-id*adalah Anda diselamatkan`kendra-index-id`,
- *aws-region adalah wilayah* AndaAWS.

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
```

Dengan:

- *kendra-index-id*adalah Anda diselamatkan`kendra-index-id`,
- *aws-region adalah wilayah* AndaAWS.

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
```

Dengan:

- *kendra-index-id*adalah Anda diselamatkan`kendra-index-id`,
- *aws-region adalah wilayah* AndaAWS.

AWS CLIMenampilkan hasil pencarian yang disaring.

Langkah 6: Membersihkan

Membersihkan file Anda

Untuk menghentikan biaya di AWS akun Anda setelah Anda menyelesaikan tutorial ini, Anda dapat mengambil langkah-langkah berikut:

1. Menghapus bucket Amazon S3

   Untuk informasi tentang menghapus bucket, lihat Menghapus bucket.
2. Menghapus indeks Amazon Kendra

   Untuk informasi tentang menghapus indeks Amazon Kendra, lihat Menghapus indeks.

3. Menghapus **converter.py**

- Untuk Konsol: Buka AWS CloudShell, dan pastikan wilayah diatur ke AWS wilayah Anda. Setelah shell bash dimuat, ketik perintah berikut ke lingkungan dan tekan enter.

```
rm converter.py
```

- UntukAWS CLI: Jalankan perintah berikut pada jendela terminal.

  Linux

  ```
  rm file/converter.py
  ```

  Dengan:

  - *file/* adalah filepath ke `converter.py` perangkat lokal Anda.

  macOS

  ```
  rm file/converter.py
  ```

  Dengan:

  - *file/* adalah filepath ke `converter.py` perangkat lokal Anda.

  Windows

  ```
  rm file/converter.py
  ```

  Dengan:

  - *file/* adalah filepath ke `converter.py` perangkat lokal Anda.

Pelajari selengkapnya

Untuk mempelajari lebih lanjut tentang mengintegrasikan Amazon Kendra ke dalam alur kerja Anda, Anda dapat melihat blogpost berikut:

- Penandaan metadata konten untuk penelusuran yang disempurnakan
- Bangun solusi pencarian cerdas dengan pengayaan konten otomatis

Untuk mempelajari lebih lanjut tentang Amazon Comprehend, Anda dapat melihat Panduan Pengembang Amazon Comprehend.

Pemantauan dan pencatatan untuk Amazon Kendra

Topik

Memantau indeks Anda (konsol)

Gunakan konsol Amazon Kendra untuk memantau status indeks dan sumber data. Anda dapat menggunakan informasi ini untuk melacak ukuran dan persyaratan penyimpanan indeks Anda dan untuk memantau kemajuan dan keberhasilan sinkronisasi antara indeks dan sumber data Anda.

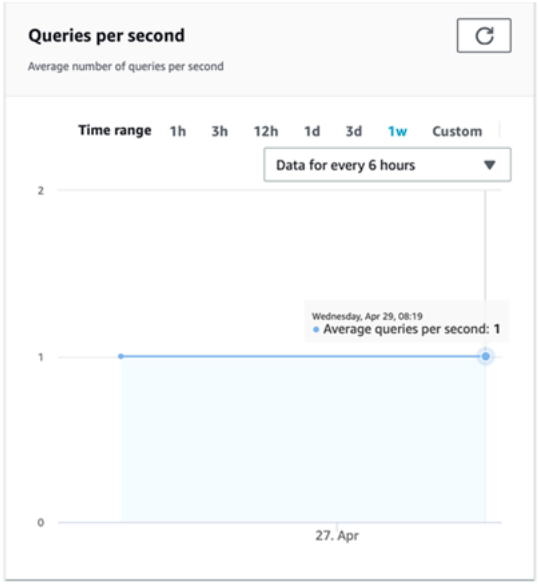
Untuk melihat metrik indeks (konsol)

1. Masuk ke AWS Management Console dan buka konsol Amazon Kendra di https://console.aws.amazon.com/kendra/home.
2. Dari daftar indeks, pilih indeks untuk dilihat.
3. Gulir layar untuk melihat metrik indeks.

Anda dapat melihat metrik berikut tentang indeks Anda.

- Jumlah dokumen —Jumlah total dokumen yang diindeks. Ini mencakup semua dokumen dari semua sumber data. Gunakan metrik ini untuk menentukan apakah Anda perlu membeli lebih banyak atau lebih sedikit unit penyimpanan untuk indeks Anda.

- Kueri per detik —Jumlah kueri indeks yang diminta setiap detik. Gunakan metrik ini untuk menentukan apakah Anda perlu membeli lebih banyak atau lebih sedikit unit kueri untuk indeks Anda.



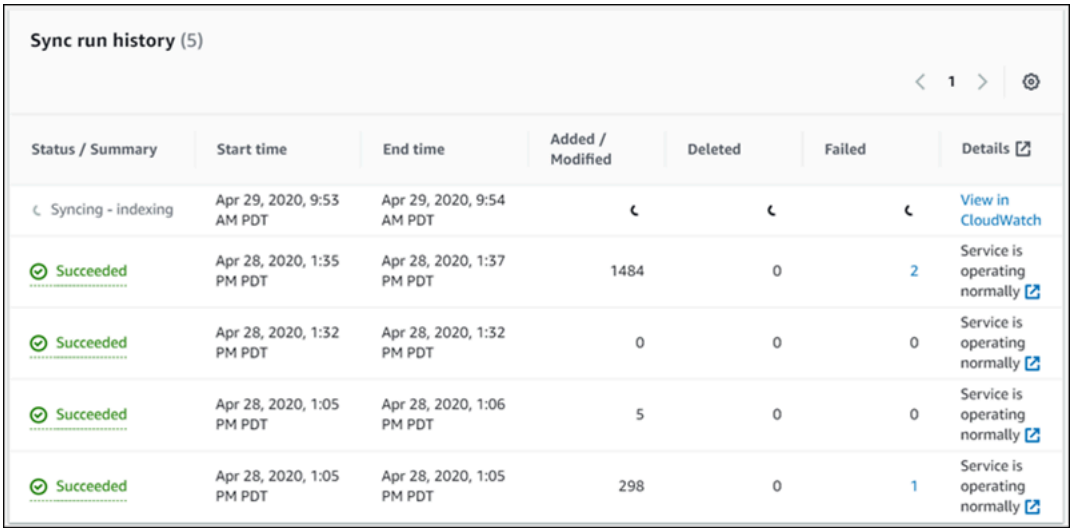
Untuk memantau kemajuan dan keberhasilan sinkronisasi antara indeks Anda dan sumber data, gunakan konsol Amazon Kendra. Gunakan informasi ini untuk membantu menentukan kesehatan sumber data Anda.

Untuk melihat metrik sinkronisasi (konsol)

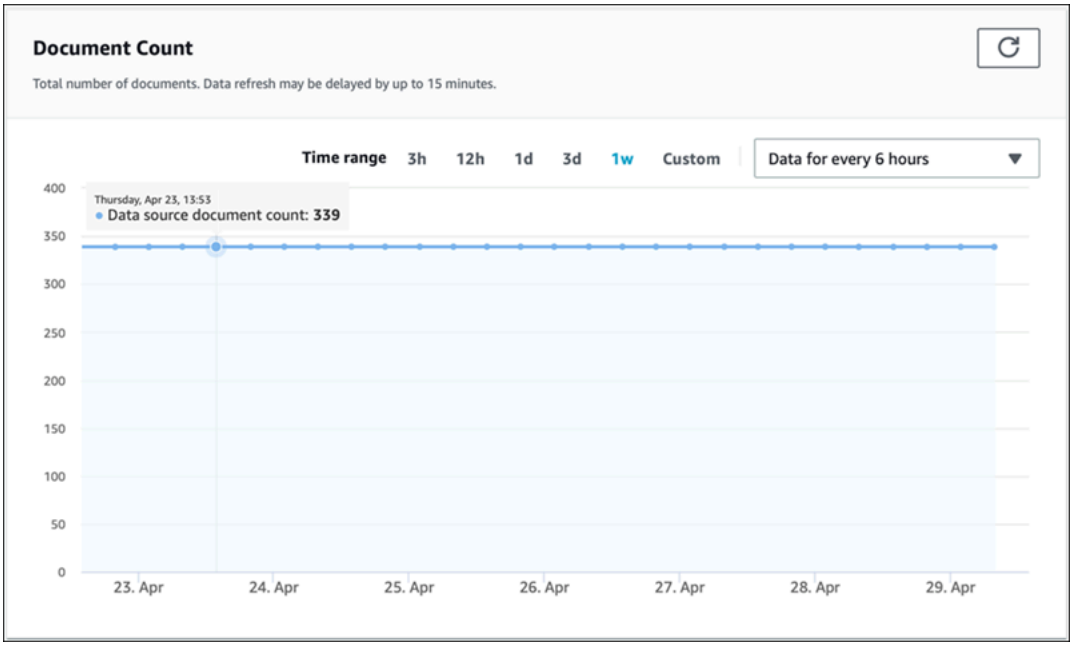
1. Masuk ke AWS Management Console dan buka konsol Amazon Kendra di https://console.aws.amazon.com/kendra/home.
2. Dari daftar indeks, pilih indeks untuk melihat metrik sinkronisasi.
3. Dari menu sebelah kiri, pilih Sumber data.
4. Dari daftar sumber data, pilih sumber data yang akan dilihat.
5. Gulir layar untuk melihat metrik menjalankan sinkronisasi.

Anda dapat melihat informasi berikut.

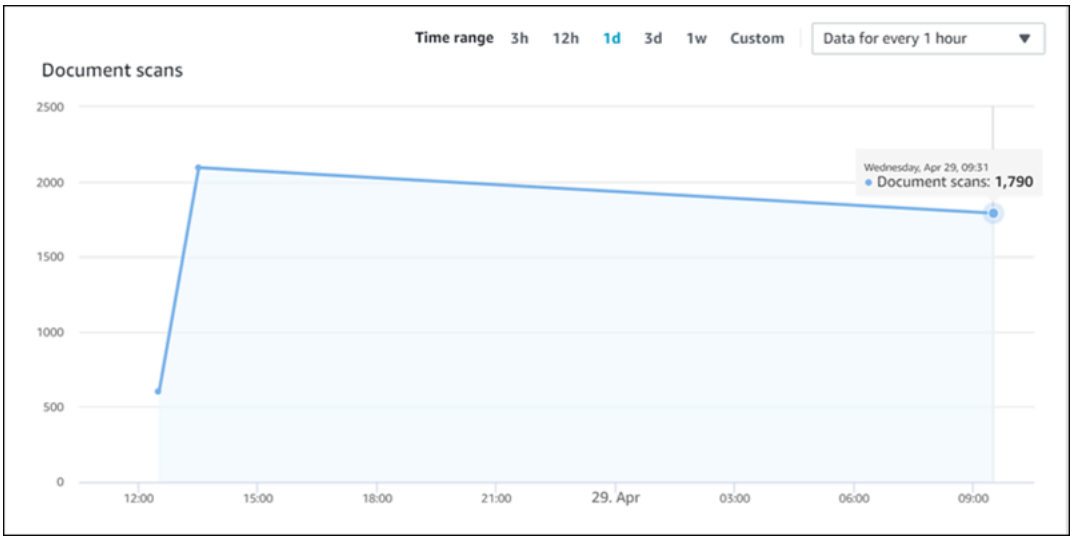
- Riwayat lari sinkronisasi —Statistik tentang sinkronisasi berjalan, termasuk waktu mulai dan akhir, jumlah dokumen yang ditambahkan, dihapus, dan gagal. Jika sinkronisasi berjalan gagal, ada link ke CloudWatch Log dengan informasi lebih lanjut. Pilih ikon pengaturan di kiri atas untuk mengubah kolom yang ditampilkan dalam riwayat. Gunakan informasi ini untuk menentukan kesehatan umum sumber data Anda.



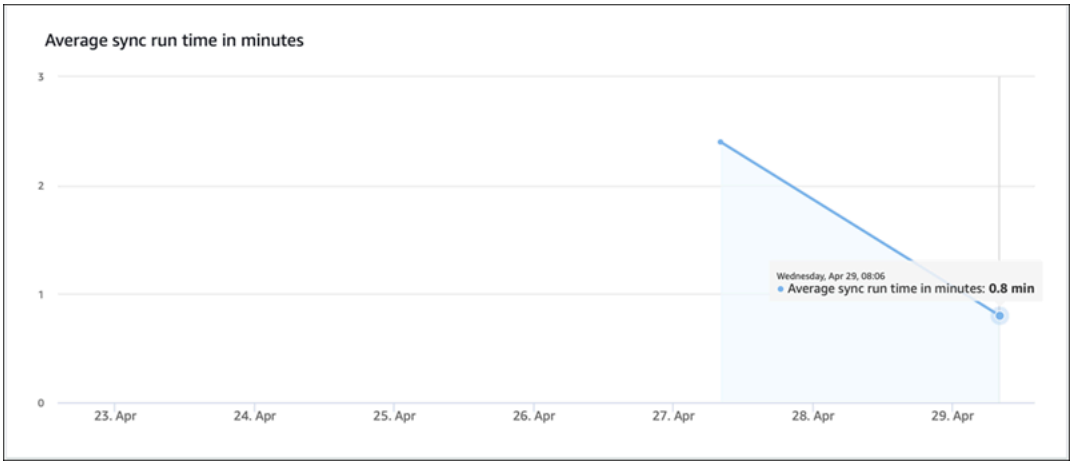
- Jumlah dokumen —Jumlah total dokumen yang diindeks dari sumber data ini. Ini adalah total semua dokumen yang ditambahkan ke sumber data dikurangi total semua dokumen yang dihapus dari sumber data. Gunakan informasi ini untuk menentukan berapa banyak dokumen dari sumber data ini termasuk dalam indeks.



- Pemindaian dokumen —Jumlah total dokumen yang dipindai selama sinkronisasi dijalankan. Ini mencakup semua dokumen dalam sumber data, termasuk yang ditambahkan, diperbarui, dihapus, atau tidak diubah. Gunakan informasi ini untuk menentukan apakah Amazon Kendra memindai semua dokumen di sumber data. Jumlah dokumen yang dipindai mempengaruhi jumlah yang dikenakan untuk layanan tersebut.



- Waktu berjalan sinkronisasi rata-rata dalam hitungan menit —Rata-rata lamanya waktu yang dibutuhkan agar sinkronisasi selesai. Waktu yang diperlukan untuk menyinkronkan sumber data akan memengaruhi jumlah yang dibebankan untuk layanan.



Mencatat panggilan API Amazon Kendra dengan log AWS CloudTrail

Amazon Kendra terintegrasi denganAWS CloudTrailLayanan yang menyediakan catatan tindakan yang dilakukan oleh pengguna, peran, atauAWSlayanan di Amazon Kendra. CloudTrail menangkap semua panggilan API dari Amazon Kendra sebagai peristiwa, termasuk panggilan dari konsol Amazon Kendra dan dari panggilan kode ke Amazon Kendra Apis. Jika Anda membuat jejak, Anda dapat mengaktifkan pengiriman CloudTrail event ke dan Amazon S3 bucket, termasuk acara untuk Amazon Kendra. Jika Anda tidak mengonfigurasi jejak, Anda masih dapat melihat peristiwa terbaru di CloudTrail konsol diRiwayat acara. Menggunakan informasi yang dikumpulkan oleh CloudTrail, Anda dapat menentukan permintaan yang dibuat ke Amazon Kendra, alamat IP dari mana permintaan itu dibuat, siapa yang membuat permintaan, kapan permintaan itu dibuat, dan detail tambahan.

Untuk mempelajari lebih lanjut tentang CloudTrail, termasuk cara mengkonfigurasi dan mengaktifkannya, lihatAWS CloudTrailPanduan Pengguna.

Informasi Amazon Kendra di CloudTrail

CloudTrail diaktifkan padaAWSakun saat Anda membuat akun. Ketika aktivitas terjadi di Amazon Kendra, aktivitas itu dicatat dalam a CloudTrail Event bersama dengan lainnyaAWSacara layanan di CloudTrail Riwayat acara. Anda dapat melihat, mencari, dan mengunduh peristiwa terbaru di akun AWS Anda. Untuk informasi lain, lihat Melihat Peristiwa dengan Riwayat Peristiwa CloudTrail.

Untuk catatan peristiwa yang sedang berlangsung di akun AWS Anda, termasuk peristiwa untuk Amazon Kendra, buatlah jejak. SEBUAHjejakadalah konfigurasi yang memungkinkan CloudTrail untuk mengirim event sebagai file log ke bucket S3 tertentu. Secara default, ketika Anda membuat

jejak di konsol tersebut, jejak diterapkan ke semua Wilayah AWS. Jejak mencatat peristiwa dari semua Wilayah di partisi AWS dan mengirimkan berkas log ke bucket S3 yang Anda tentukan. Selain itu, Anda dapat mengonfigurasiAWSLayanan untuk menganalisis dan menindaklanjuti data peristiwa yang dikumpulkan CloudTrail log. Untuk informasi selengkapnya, lihat :

- Ikhtisar untuk Membuat Jejak
- CloudTrail Layanan dan Integrasi yang Didukung
- Mengonfigurasi Notifikasi Amazon SNS untuk CloudTrail
- Menerima CloudTrail Mencatat File dari Beberapa WilayahdanMenerima CloudTrail Mencatat File dari Beberapa Akun

CloudTrail mencatat semua tindakan Amazon Kendra, yang didokumentasikan diAPI Referensi. Misalnya, panggilan ke`CreateIndex`,`CreateDataSource`, dan`Query`operasi menghasilkan entri di CloudTrail file log.

Setiap entri peristiwa atau log berisi informasi tentang siapa yang membuat permintaan tersebut. Untuk informasi lain, lihat Elemen userIdentity CloudTrail.

Contoh: Entri file log Amazon Kendra

SEBUAHjejakadalah konfigurasi yang memungkinkan pengiriman peristiwa sebagai file log ke bucket S3 tertentu. CloudTrail file log berisi satu atau beberapa entri log. Sebuahperistiwamewakili satu permintaan dari sumber mana pun dan mencakup informasi tentang tindakan yang diminta, tanggal dan waktu tindakan, parameter permintaan, dan sebagainya. CloudTrail File log bukan merupakan jejak tumpukan yang diurutkan dari panggilan API publik, sehingga file tersebut tidak muncul dalam urutan tertentu.

Panggilan ke operasi `Query` menciptakan entri berikut.

```
       {
           "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"
    },
```

Penskalaan Amazon Kendra Intelligent Ranking Amazon KendraAWS CloudTraillog

Amazon Kendra Intelligent Ranking terintegrasi denganAWS CloudTrailLayanan yang menyediakan catatan tindakan yang dilakukan oleh pengguna, peran, atauAWSlayanan di Amazon Kendra Intelligent Ranking. CloudTrail menangkap semua panggilan API dari Amazon Kendra Intelligent Ranking sebagai peristiwa, termasuk panggilan kode ke Amazon Kendra Intelligent Ranking API. Jika Anda membuat jejak, Anda dapat mengaktifkan pengiriman CloudTrail event ke dan Amazon S3 bucket, termasuk acara Amazon Kendra Intelligent Ranking. Jika Anda tidak mengonfigurasi jejak,

Anda masih dapat melihat peristiwa terbaru di CloudTrail konsol diRiwayat acara. Menggunakan informasi yang dikumpulkan oleh CloudTrail, Anda dapat menentukan permintaan yang dibuat ke Amazon Kendra Intelligent Ranking, alamat IP dari mana permintaan dibuat, siapa yang membuat permintaan, kapan permintaan dibuat, dan detail tambahan.

Untuk mempelajari lebih lanjut tentang CloudTrail, termasuk cara mengkonfigurasi dan mengaktifkannya, lihatAWS CloudTrailPanduan Pengguna.

Informasi Peringkat Cerdas Amazon Kendra di CloudTrail

CloudTrail diaktifkan padaAWSakun saat Anda membuat akun. Ketika aktivitas terjadi di Amazon Kendra Intelligent Ranking, aktivitas tersebut dicatat dalam Amazon Kendra Intelligent Ranking, aktivitas tersebut dicatat dalam Amazon Kendra Intelligent Ranking CloudTrailEvent bersama dengan lainnyaAWSacara layanan di CloudTrail Riwayat acara. Anda dapat melihat, mencari, dan mengunduh peristiwa terbaru di akun AWS Anda. Untuk informasi selengkapnya, lihatPemantauan Acara dengan CloudTrail Riwayat Acara.

Untuk catatan peristiwa yang sedang berlangsung diAWSakun, termasuk acara untuk Amazon Kendra Intelligent Ranking, buat jejak. SEBUAHjejakadalah konfigurasi yang memungkinkan CloudTrail untuk mengirim event sebagai file log ke bucket S3 tertentu. Secara default, ketika Anda membuat jejak di konsol tersebut, jejak diterapkan ke semua Wilayah AWS. Jejak mencatat peristiwa dari semua Wilayah di partisi AWS dan mengirimkan berkas log ke bucket S3 yang Anda tentukan. Selain itu, Anda dapat mengonfigurasiAWSLayanan untuk menganalisis dan menindaklanjuti data peristiwa yang dikumpulkan CloudTrail log. Untuk informasi selengkapnya, lihat :

- Ikhtisar untuk Membuat Jejak
- CloudTrail Layanan dan Integrasi yang Didukung
- Mengonfigurasi Notifikasi Amazon SNS untuk CloudTrail
- Menerima CloudTrail Mencatat File dari Beberapa WilayahdanMenerima CloudTrail Mencatat File dari Beberapa Akun

CloudTrail mencatat semua tindakan Amazon Kendra Intelligent Ranking, yang didokumentasikan di Amazon Kendra Intelligent Ranking, yang didokumentasikan diAPI Referensi. Misalnya, panggilan ke`CreateRescoreExecutionPlan`menghasilkan entri di CloudTrail file log.

Setiap entri peristiwa atau log berisi informasi tentang siapa yang membuat permintaan tersebut. Untuk informasi lain, lihat Elemen userIdentity CloudTrail.

Contoh: Entri file log Amazon Kendra Intelligent Ranking

SEBUAHjejakadalah konfigurasi yang memungkinkan pengiriman peristiwa sebagai file log ke bucket S3 tertentu. CloudTrail file log berisi satu atau beberapa entri log. Sebuahperistiwamewakili satu permintaan dari sumber mana pun dan mencakup informasi tentang tindakan yang diminta, tanggal dan waktu tindakan, parameter permintaan, dan sebagainya. CloudTrail File log bukan merupakan jejak tumpukan yang diurutkan dari panggilan API publik, sehingga file tersebut tidak muncul dalam urutan tertentu.

Panggilan ke operasi `CreateRescoreExecutionPlan` menciptakan entri berikut.

```
{
            "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"
        }
    }
```

Pemantauan Amazon Kendra dengan Amazon Kendra dengan Amazon Kendra dengan Amazon Kendra dengan Amazon Kendra CloudWatch

Untuk melacak kesehatan indeks Anda, gunakan Amazon CloudWatch. dengan CloudWatch, Anda bisa mendapatkan metrik untuk sinkronisasi dokumen untuk indeks. Anda juga dapat mengatur CloudWatch Alarm harus diberi notifikasi ketika satu atau beberapa metrik melebihi ambang batas waktu tertentu. Misalnya, Anda dapat memantau jumlah dokumen yang dikirim untuk diindeks atau jumlah dokumen yang gagal diindeks.

Anda harus memiliki CloudWatch izin untuk memantau Amazon Kendra CloudWatch. Untuk informasi selengkapnya, lihatOtentikasi dan Kontrol Akses untuk Amazon CloudWatchdiAmazon CloudWatchPanduan Pengguna.

Melihat metrik Amazon Kendra

Mencatat metrik Amazon Kendra dengan CloudWatch konsol

Untuk melihat metrik (CloudWatch konsol)

1. MencatatAWS Management Consoledan buka CloudWatch konsol dihttps://console.aws.amazon.com/cloudwatch/.
2. Pilih Metrik, pilih Semua Metrik, dan kemudian pilih Kendra.
3. Pilih dimensi, pilih nama metrik, lalu pilih Tambahkan ke grafik.
4. Pilih nilai untuk rentang tanggal. Hitungan metrik untuk rentang tanggal yang dipilih akan ditampilkan dalam grafik.

Membuat alarm

SEBUAH CloudWatch Alarm mengawasi satu metrik selama periode waktu tertentu dan melakukan satu atau beberapa tindakan: mengirim notifikasi ke bagian atas Amazon Simple Notification Service (Amazon SNS) atau kebijakan Penskalaan Otomatis. Tindakan atau tindakan didasarkan pada nilai metrik yang relatif terhadap ambang batas tertentu selama beberapa periode waktu yang Anda tentukan. CloudWatch juga dapat mengirim pesan Amazon SNS saat alarm berubah status.

CloudWatch Alarm memanggil tindakan hanya ketika status berubah dan selama periode waktu tertentu.

Untuk mengatur alarm

1. MencatatAWS Management Consoledan buka CloudWatch konsol dihttps://console.aws.amazon.com/cloudwatch/.
2. PilihAlarmdan kemudian memilihBuat alarm.
3. Pilih metrik. PilihKendrametrik untuk indeks dan sumber data Anda. Juga atur waktu sebagai jumlah jam, hari, minggu, atau kebiasaan yang ditetapkan.
4. Pilih statistik Anda. Sebagai contohRata-rata. Juga pilih periode waktu pemicu alarm Anda sebagai jumlah menit, jam, per hari, atau kustom yang ditetapkan.
5. Pilih ambang batas Anda untuk memicu alarm, apakah akan menggunakan nilai statis atau pita dan kondisi untuk memenuhi ambang batas.
6. Pilih status alarm untuk pemicu, apakah metrik harus berada di luar ambang batas yang Anda tetapkan, atau status lain. Pilih email siapa/mana untuk mengirim pemberitahuan alarm.
7. Jika Anda puas dengan alarm, pilihBuat alarm.

> **Note**
>
> Anda harus memberikan nama untuk CloudWatch alarm

CloudWatch Metrik untuk Pekerjaan sinkronisasi indeks

Tabel berikut menjelaskan metrik Amazon Kendra untuk tugas sinkronisasi sumber data.

Jika Anda menggunakan API atau CLI, Anda harus menentukan`Namespace`sebagai 'AWS/Kendra' selain`MetricName`pilihan Anda saat menggunakanGetMetricStatisticsAPI.

Metrik	Deskripsi
`DocumentsCrawled`	Jumlah dokumen yang dipindai atau ditemukan oleh tugas sinkronisasi selama proses berjalan. Dimensi: • IndexId • DataSourceId Unit: Jumlah
`DocumentsSubmittedForIndexing`	Jumlah dokumen yang dikirimkan tugas sinkronisasi ke indeks. Dimensi: • IndexId • DataSourceId Unit: Jumlah
`DocumentsSubmittedForIndexingFailed`	Jumlah dokumen yang gagal diindeks. Catat isi CloudWatch log untuk pekerjaan sinkronisasi untuk detailnya. Dimensi:

Metrik	Deskripsi
	• IndexId • DataSourceId Unit: Jumlah
DocumentsSubmittedForDeletion	Jumlah dokumen yang diminta oleh tugas sinkronisasi untuk dihapus dari indeks. Dimensi: • IndexId • DataSourceId Unit: Jumlah
DocumentsSubmittedForDeletionFailed	Jumlah dokumen yang gagal dihapus. Catat isi CloudWatch log untuk pekerjaan sinkronisasi untuk detailnya. Dimensi: • IndexId • DataSourceId Unit: Jumlah

Metrik untuk sumber data Amazon Kendra

Tabel berikut menjelaskan metrik Amazon Kendra untuk tugas sinkronisasi sumber data. Metrik yang ditandai dengan tanda bintang (*) hanya digunakan untuk sumber data Amazon S3.

Jika Anda menggunakan API atau CLI, Anda harus menentukan`Namespace`sebagai 'AWS/Kendra' selain`MetricName`pilihan Anda saat menggunakanGetMetricStatisticsAPI.

Metrik	Deskripsi
DocumentsSkippedNoChange *	Jumlah dokumen yang diperiksa dan ditemukan tidak berubah sehingga tidak dikirimkan untuk pengindeksan. Dimensi: • IndexId • DataSourceId Unit: Jumlah
DocumentsSkippedInvalidMetadata *	Jumlah dokumen yang dilewati karena ada masalah dengan file metadata terkait. Catat isi CloudWatch log untuk menjalankan sinkronis asi untuk detailnya. Dimensi: • IndexId • DataSourceId Unit: Jumlah
DocumentsCrawled	Jumlah file dokumen yang diperiksa. Dimensi: • IndexId • DataSourceId Unit: Jumlah
DocumentsSubmittedForDeletion	Jumlah dokumen yang diperiksa yang dihapus dari sumber data dan diajukan untuk dihapus. Dimensi:

Metrik	Deskripsi
	• IndexId • DataSourceId Unit: Jumlah
DocumentsSubmittedForDeletionFailed	Jumlah dokumen yang gagal dihapus dari sumber data. Dimensi: • IndexId • DataSourceId Unit: Jumlah
DocumentsSubmittedForIndexing	Jumlah dokumen yang diperiksa dan diserahkan untuk pengindeksan. Dimensi: • IndexId • DataSourceId Unit: Jumlah
DocumentsSubmittedForIndexingFailed	Jumlah dokumen yang diserahkan untuk idexing yang tidak dapat diindeks. Dimensi: • IndexId • DataSourceId Unit: Jumlah

Metrik untuk dokumen yang diindeks

Tabel berikut menjelaskan metrik Amazon Kendra untuk dokumen yang diindeks. Untuk dokumen yang diindeks menggunakan operasi BatchPutDocument, hanya dimensi `IndexId` yang didukung.

Jika Anda menggunakan API atau CLI, Anda harus menentukan`Namespace`sebagai 'AWS/Kendra' selain`MetricName`pilihan Anda saat menggunakanGetMetricStatisticsAPI.

Metrik	Deskripsi
`DocumentsIndexed`	Jumlah dokumen yang diindeks. Dimensi: • IndexId • DataSourceId Unit: Jumlah
`DocumentsFailedToIndex`	Jumlah dokumen yang tidak dapat diindeks. Catat isi CloudWatch Mencatat detailnya. Dimensi: • IndexId • DataSourceId Unit: Jumlah
`IndexQueryCount`	Jumlah kueri indeks per menit. Dimensi: • IndexId Unit: Jumlah

Pemantauan Amazon Kendra dengan Amazon Kendra dengan Amazon Kendra dengan Amazon Kendra dengan Amazon Kendra CloudWatch Log

Amazon Kendra menggunakan Amazon Kendra CloudWatch Log untuk memberi Anda wawasan tentang pengoperasian sumber data. Amazon Kendra mencatat detail proses untuk dokumen saat diindeks. Ini mencatat kesalahan dari sumber data Anda yang terjadi saat dokumen Anda sedang diindeks. Anda menggunakan CloudWatch Log untuk memantau, menyimpan dan mengakses file log.

CloudWatch Log menyimpan peristiwa log di aliran log yang merupakan bagian dari grup log. Amazon Kendra menggunakan fitur ini sebagai berikut:

- Grup Log — Amazon Kendra menyimpan semua aliran log Anda dalam satu grup log untuk setiap indeks. Amazon Kendra membuat grup log saat indeks dibuat. Pengidentifikasi grup log selalu dimulai dengan "aws/kendra/".
- Aliran Log — Amazon Kendra membuat aliran log sumber data di grup log untuk setiap pekerjaan sinkronisasi indeks yang Anda jalankan. Ini juga membuat pengaliran log dokumen baru ketika pengaliran mencapai sekitar 500 entri.
- Entri log—Amazon Kendra membuat entri log di aliran log saat mengindeks dokumen. Setiap entri memberikan informasi tentang pemrosesan dokumen atau kesalahan apa pun yang ditemui.

Untuk informasi lebih lanjut tentang penggunaan CloudWatch Log, lihatApa Itu Mencatat atat atat atat atat atat atat atat atat atat atatdiPanduan Pengguna Mencatat atat atat atat atat atat catatan Amazon Cloud Watch.

Amazon Kendra menciptakan dua jenis pengaliran log:

- Pengaliran log sumber data
- Pengaliran log dokumen

Pengaliran log sumber data

Pengaliran log sumber data mempublikasikan entri tentang tugas sinkronisasi indeks Anda. Setiap tugas sinkronisasi membuat pengaliran log baru yang digunakan untuk mempublikasikan entri. Nama pengaliran log adalah:

```
data source id/YYYY-MM-DD-HH/data source sync job ID
```

Pengaliran log baru dibuat untuk setiap tugas sinkronisasi yang dijalankan.

Ada tiga jenis pesan log diterbitkan ke pengaliran log sumber data:

- Pesan log untuk dokumen yang gagal dikirim untuk pengindeksan. Berikut ini adalah contoh pesan ini untuk dokumen di sumber data S3:

```
{
    "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."
}
```

- Pesan log untuk dokumen yang gagal dikirim untuk penghapusan. Berikut adalah contoh dari jenis peristiwa ini:

```
{
    "DocumentId": "document ID",
    "Message": "Failed to delete document via BatchDeleteDocument.",
    "ErrorCode": "InvalidRequest",
    "ErrorMessage": "Document can't be deleted because it doesn't exist."
}
```

- Pesan log ketika file metadata tidak valid untuk dokumen di bucket Amazon S3 ditemukan. Berikut adalah contoh dari jenis peristiwa ini.

```
{
    "Message": "Found invalid metadata
 file bucket/prefix/filename.extension.metadata.json."
}
```

- Untuk SharePoint dan konektor basis data, Amazon Kendra hanya menulis pesan ke aliran log jika dokumen tidak dapat diindeks. Berikut ini adalah contoh dari pesan galat yang dicatat Amazon Kendra.

```
{
```

```
    "DocumentID": "document ID",
    "IndexID": "index ID",
    "SourceURI": "",
    "CrawlStatus": "FAILED",
    "ErrorCode": "403",
    "ErrorMessage": "Access Denied",
    "DataSourceErrorCode": "403"
}
```

Pengaliran log dokumen

Amazon Kendra mencatat informasi tentang pemrosesan dokumen saat diindeks. Amazon Kendra mencatat sekumpulan pesan untuk dokumen yang disimpan di sumber data Amazon S3. Ini mencatat kesalahan hanya untuk dokumen yang disimpan di Microsoft SharePoint atau sumber data database

Jika dokumen ditambahkan ke indeks menggunakan operasi BatchPutDocument, pengaliran log dinamai sebagai berikut:

```
YYYY-MM-DD-HH/UUID
```

Jika dokumen ditambahkan ke indeks menggunakan sumber data, pengaliran log dinamai sebagai berikut:

```
dataSourceId/YYYY-MM-DD-HH/UUID
```

Setiap pengaliran log berisi hingga 500 pesan.

Jika pengindeksan dokumen gagal, pesan ini akan ditampilkan ke pengaliran log:

```
{
    "DocumentId": "document ID",
    "IndexName": "index name",
    "IndexId": "index ID"
    "SourceURI": "source URI"
    "IndexingStatus": "DocumentFailedToIndex",
    "ErrorCode": "400 | 500",
    "ErrorMessage": "message"
}
```

Keamanan di Amazon Kendra

Keamanan cloud di AWS adalah prioritas tertinggi. Sebagai AWS pelanggan, Anda mendapat manfaat dari pusat data dan arsitektur jaringan yang dibangun untuk memenuhi persyaratan organisasi yang paling sensitif terhadap keamanan.

Keamanan adalah tanggung jawab bersama antara Anda AWS dan Anda. Model tanggung jawab bersama menjelaskan hal ini sebagai keamanan dari cloud dan keamanan dalam cloud:

- Keamanan cloud —AWS bertanggung jawab untuk melindungi infrastruktur yang menjalankan AWS layanan di AWS Cloud. AWS juga memberi Anda layanan yang dapat Anda gunakan dengan aman. Auditor pihak ketiga secara teratur menguji dan memverifikasi efektivitas keamanan kami sebagai bagian dari Program AWS Kepatuhan Program AWS Kepatuhan . Untuk mempelajari tentang program kepatuhan yang berlaku untuk Amazon Kendra, lihat AWS Layanan dalam Lingkup berdasarkan AWS Layanan Program Kepatuhan dalam Lingkup oleh Program .
- Keamanan di cloud — Tanggung jawab Anda ditentukan oleh AWS layanan yang Anda gunakan. Anda juga bertanggung jawab atas faktor lain, yang mencakup sensitivitas data Anda, persyaratan perusahaan Anda, serta undang-undang dan peraturan yang berlaku.

Dokumentasi ini membantu Anda memahami cara menerapkan model tanggung jawab bersama saat menggunakan Amazon Kendra. Topik berikut menunjukkan cara mengonfigurasi Amazon Kendra untuk memenuhi tujuan keamanan dan kepatuhan Anda. Anda juga mempelajari cara menggunakan AWS layanan lain yang membantu Anda memantau dan mengamankan sumber daya Amazon Kendra Anda.

Topik

- Analisis konfigurasi dan kerentanan di AWS Identity and Access Management

Perlindungan Data di Amazon Kendra

Model tanggung jawab AWS bersama model berlaku untuk perlindungan data di Amazon Kendra. Seperti yang dijelaskan dalam model AWS ini, bertanggung jawab untuk melindungi infrastruktur global yang menjalankan semua AWS Cloud. Anda bertanggung jawab untuk mempertahankan kendali atas konten yang di-host pada infrastruktur ini. Anda juga bertanggung jawab atas tugas-tugas konfigurasi dan manajemen keamanan untuk Layanan AWS yang Anda gunakan. Lihat informasi yang lebih lengkap tentang privasi data dalam Pertanyaan Umum Privasi Data. Lihat informasi tentang perlindungan data di Eropa di pos blog Model Tanggung Jawab Bersama dan GDPR AWS di Blog Keamanan AWS .

Untuk tujuan perlindungan data, kami menyarankan Anda melindungi Akun AWS kredensil dan mengatur pengguna individu dengan AWS IAM Identity Center atau AWS Identity and Access Management (IAM). Dengan cara itu, setiap pengguna hanya diberi izin yang diperlukan untuk memenuhi tanggung jawab tugasnya. Kami juga menyarankan supaya Anda mengamankan data dengan cara-cara berikut:

- Gunakan autentikasi multi-faktor (MFA) pada setiap akun.
- Gunakan SSL/TLS untuk berkomunikasi dengan sumber daya. AWS Kami mensyaratkan TLS 1.2 dan menganjurkan TLS 1.3.
- Siapkan API dan pencatatan aktivitas pengguna dengan AWS CloudTrail.
- Gunakan solusi AWS enkripsi, bersama dengan semua kontrol keamanan default di dalamnya Layanan AWS.
- Gunakan layanan keamanan terkelola lanjut seperti Amazon Macie, yang membantu menemukan dan mengamankan data sensitif yang disimpan di Amazon S3.
- Jika Anda memerlukan modul kriptografi tervalidasi FIPS 140-2 saat mengakses AWS melalui antarmuka baris perintah atau API, gunakan titik akhir FIPS. Lihat informasi yang lebih lengkap tentang titik akhir FIPS yang tersedia di Standar Pemrosesan Informasi Federal (FIPS) 140-2.

Kami sangat merekomendasikan agar Anda tidak pernah memasukkan informasi identifikasi yang sensitif, seperti nomor rekening pelanggan Anda, ke dalam tanda atau bidang isian bebas seperti bidang Nama. Ini termasuk saat Anda bekerja dengan Amazon Kendra atau lainnya Layanan AWS menggunakan konsol, API AWS CLI, atau AWS SDK. Data apa pun yang Anda masukkan ke dalam tanda atau bidang isian bebas yang digunakan untuk nama dapat digunakan untuk log penagihan

atau log diagnostik. Saat Anda memberikan URL ke server eksternal, kami sangat menganjurkan supaya Anda tidak menyertakan informasi kredensial di dalam URL untuk memvalidasi permintaan Anda ke server itu.

Enkripsi saat diam

Amazon Kendra mengenkripsi data at rest Anda dengan kunci enkripsi pilihan Anda. Anda dapat memilih salah satu dari yang berikut ini:

- Kunci AWS KMS AWS yang dimiliki. Jika Anda tidak menentukan kunci enkripsi, data Anda akan dienkripsi dengan kunci ini secara default.
- Kunci KMS yang AWS dikelola di akun Anda. Kunci ini dibuat, dikelola, dan digunakan atas nama Anda oleh Amazon Kendra. Nama kunci tersebut adalah `aws/kendra`.
- Kunci yang dikelola pelanggan. Anda dapat memberikan ARN kunci enkripsi yang Anda buat di akun Anda. Saat Anda menggunakan kunci KMS yang dikelola pelanggan, Anda harus memberikan kunci kebijakan kunci yang memungkinkan Amazon Kendra menggunakan kunci tersebut. Pilih kunci KMS enkripsi simetris yang dikelola pelanggan, Amazon Kendra tidak mendukung kunci KMS asimetris. Untuk informasi selengkapnya, lihat Manajemen kunci.

Enkripsi dalam bergerak

Amazon Kendra menggunakan protokol HTTPS untuk berkomunikasi dengan aplikasi klien Anda. Menggunakan HTTPS dan AWS tanda tangan untuk berkomunikasi dengan layanan lain atas nama aplikasi Anda. Jika Anda menggunakan VPC, Anda dapat menggunakan AWS PrivateLink untuk membuat koneksi pribadi antara VPC Anda dan Amazon Kendra.

Manajemen kunci

Amazon Kendra mengenkripsi konten indeks Anda menggunakan salah satu dari tiga jenis kunci. Anda dapat memilih salah satu dari yang berikut ini:

- AWS KMS yang dimiliki AWS . Ini adalah opsi default.
- Kunci KMS yang AWS dikelola. Kunci ini dibuat di akun Anda serta dikelola dan digunakan atas nama Anda oleh Amazon Kendra.
- Kunci KMS yang dikelola pelanggan. Anda dapat membuat kunci tersebut ketika membuat indeks Amazon Kendra atau sumber data, atau membuatnya menggunakan konsol AWS KMS . Pilih kunci KMS enkripsi simetris yang dikelola pelanggan. Amazon Kendra tidak mendukung kunci

KMS asimetris. Untuk informasi selengkapnya, lihat Penggunaan Kunci Simetris dan Asimetris di Panduan Developer AWS Key Management Service.

Amazon Kendra Amazon Kendra Peringkat Cerdas dan antarmuka titik akhir VPC ()AWS PrivateLink

Anda dapat membuat koneksi privat antara VPC Anda dan Amazon Kendra dengan membuat VPC endpoint antarmuka. Endpoint antarmuka didukung oleh AWS PrivateLink, teknologi yang memungkinkan Anda mengakses API Amazon Kendra secara pribadi tanpa gateway internet, perangkat NAT, koneksi VPN, atau AWS koneksi Direct Connect. Instans dalam VPC Anda tidak memerlukan alamat IP publik untuk berkomunikasi dengan API Amazon Kendra. Lalu lintas antara VPC Anda dan Amazon Kendra tidak meninggalkan jaringan Amazon.

Setiap titik akhir antarmuka diwakili oleh satu atau beberapa Antarmuka Jaringan Elastis di subnet Anda.

Pertimbangan untuk Amazon Kendra dan Amazon Kendra Intelligent Ranking VPC endpoint

Sebelum Anda menyiapkan titik akhir VPC antarmuka untuk Amazon Kendra atau Amazon Kendra Intelligent Ranking, pastikan Anda meninjau prasyarat di Panduan Pengguna Amazon VPC.

Amazon Kendra dan Amazon Kendra Intelligent Ranking mendukung panggilan ke semua tindakan API-nya dari VPC Anda.

Membuat titik akhir VPC antarmuka untuk Amazon Kendra dan Amazon Kendra Intelligent Ranking

Anda dapat membuat titik akhir VPC untuk layanan Amazon Kendra atau Amazon Kendra Intelligent Ranking menggunakan konsol VPC Amazon atau (). AWS Command Line Interface AWS CLI

Buat VPC endpoint untuk Amazon Kendra menggunakan nama layanan berikut:

- com.amazonaws.*region*.kendra

Buat titik akhir VPC untuk Amazon Kendra Intelligent Ranking menggunakan nama layanan berikut:

- aws.api. *wilayah .kendra-ranking*

Setelah membuat titik akhir VPC, Anda dapat menggunakan AWS CLI perintah contoh berikut yang menggunakan `endpoint-url` parameter untuk menentukan titik akhir antarmuka ke Amazon Kendra API:

```
aws kendra list-indices --endpoint-url https://VPC endpoint
```

`Titik akhir VPC` adalah nama DNS yang dihasilkan saat titik akhir antarmuka dibuat. Nama ini mencakup ID titik akhir VPC, dan nama layanan Amazon Kendra, yang mencakup wilayah tersebut. Misalnya, `vpce-1234-abcdef.kendra.us-west-2.vpce.amazonaws.com`.

Jika Anda mengaktifkan DNS pribadi untuk titik akhir, Anda dapat membuat permintaan API ke Amazon Kendra menggunakan nama DNS default untuk wilayah tersebut. Misalnya, `kendra.us-east-1.amazonaws.com`.

Untuk informasi selengkapnya, lihat Membuat titik akhir antarmuka dalam Panduan Pengguna Amazon VPC.

Membuat kebijakan titik akhir VPC untuk Amazon Kendra dan Amazon Kendra Intelligent Ranking

Anda dapat melampirkan kebijakan titik akhir ke titik akhir VPC Anda yang mengontrol akses ke Amazon Kendra atau Amazon Kendra Intelligent Ranking.

Kebijakan untuk Amazon Kendra atau Amazon Kendra Intelligent Ranking menentukan informasi berikut:

- Pengguna prinsip/resmi yang dapat melakukan tindakan.
- Tindakan yang dapat dilakukan.
- Sumber daya yang menjadi target tindakan.

Contoh: Kebijakan VPC endpoint untuk tindakan Amazon Kendra

Berikut adalah contoh kebijakan titik akhir untuk Amazon Kendra. Saat dilampirkan ke titik akhir, kebijakan ini memberikan akses ke semua tindakan Amazon Kendra yang tersedia untuk semua prinsipal/pengguna resmi di semua sumber daya.

```
{
   "Statement":[
      {
```

```
         "Principal":"*",
         "Effect":"Allow",
         "Action":[
            "kendra:*"
         ],
         "Resource":"*"
      }
   ]
}
```

Contoh: Kebijakan titik akhir VPC untuk tindakan Amazon Kendra Intelligent Ranking

Berikut ini adalah contoh kebijakan endpoint untuk Amazon Kendra Intelligent Ranking. Saat dilampirkan ke titik akhir, kebijakan ini memberikan akses ke semua tindakan Peringkat Cerdas Amazon Kendra yang tersedia untuk semua prinsipal/pengguna resmi di semua sumber daya.

```
{
   "Statement":[
      {
         "Principal":"*",
         "Effect":"Allow",
         "Action":[
            "kendra-ranking:*"
         ],
         "Resource":"*"
      }
   ]
}
```

Untuk informasi selengkapnya, lihat Mengontrol akses ke titik akhir VPC menggunakan kebijakan titik akhir di Panduan Pengguna Amazon VPC.

Identity and access management untuk Amazon Kendra

AWS Identity and Access Management (IAM) adalah Layanan AWS yang membantu administrator mengontrol akses ke AWS sumber daya dengan aman. Administrator IAM mengendalikan siapa yang dapat diautentikasi (masuk) dan diotorisasi (memiliki izin) untuk menggunakan sumber daya Amazon Kendra. IAM adalah Layanan AWS yang dapat Anda gunakan tanpa biaya tambahan.

Topik

- Audiens

- Mengautentikasi dengan identitas
- Mengelola akses menggunakan kebijakan
- Cara kerja Amazon Kendra dengan IAM
- Contoh kebijakan berbasis Identitas Amazon Kendra
- AWS kebijakan terkelola untuk Amazon Kendra
- Pemecahan masalah Identitas dan Akses Amazon Kendra

Audiens

Cara Anda menggunakan AWS Identity and Access Management (IAM) berbeda, tergantung pada pekerjaan yang Anda lakukan di Amazon Kendra.

Pengguna layanan – Jika Anda menggunakan layanan Amazon Kendra untuk melakukan tugas, administrator Anda akan memberikan kredensial dan izin yang dibutuhkan. Saat Anda menggunakan lebih banyak fitur di Amazon Kendra untuk melakukan pekerjaan, Anda mungkin memerlukan izin tambahan. Memahami cara akses dikelola dapat membantu Anda meminta izin yang tepat dari administrator Anda. Jika Anda tidak dapat mengakses fitur di Amazon Kendra, lihat Pemecahan masalah Identitas dan Akses Amazon Kendra.

Administrator layanan – Jika Anda bertanggung jawab atas sumber daya Amazon Kendra di perusahaan, Anda mungkin memiliki akses penuh ke Amazon Kendra. Tugas Anda adalah menentukan fitur dan sumber daya Amazon Kendra mana yang harus diakses pengguna layanan Anda. Kemudian, Anda harus mengirimkan permintaan kepada administrator IAM Anda untuk mengubah izin pengguna layanan Anda. Tinjau informasi di halaman ini untuk memahami konsep Basic IAM. Untuk mempelajari selengkapnya tentang bagaimana perusahaan Anda dapat menggunakan IAM dengan Amazon Kendra, lihat Cara kerja Amazon Kendra dengan IAM.

Administrator IAM – Jika Anda seorang administrator IAM, Anda mungkin ingin mempelajari detail tentang bagaimana Anda dapat menulis kebijakan untuk mengelola akses ke Amazon Kendra. Untuk melihat contoh kebijakan berbasis identitas Amazon Kendra yang dapat Anda gunakan di IAM, lihat Contoh kebijakan berbasis Identitas Amazon Kendra.

Mengautentikasi dengan identitas

Otentikasi adalah cara Anda masuk AWS menggunakan kredensyal identitas Anda. Anda harus diautentikasi (masuk ke AWS) sebagai Pengguna root akun AWS, sebagai pengguna IAM, atau dengan mengasumsikan peran IAM.

Anda dapat masuk AWS sebagai identitas federasi dengan menggunakan kredensil yang disediakan melalui sumber identitas. AWS IAM Identity Center Pengguna (IAM Identity Center), autentikasi masuk tunggal perusahaan Anda, dan kredensi Google atau Facebook Anda adalah contoh identitas federasi. Saat Anda masuk sebagai identitas gabungan, administrator Anda sebelumnya menyiapkan federasi identitas menggunakan peran IAM. Ketika Anda mengakses AWS dengan menggunakan federasi, Anda secara tidak langsung mengambil peran.

Bergantung pada jenis pengguna Anda, Anda dapat masuk ke AWS Management Console atau portal AWS akses. Untuk informasi selengkapnya tentang masuk AWS, lihat Cara masuk ke Panduan AWS Sign-In Pengguna Anda Akun AWS.

Jika Anda mengakses AWS secara terprogram, AWS sediakan kit pengembangan perangkat lunak (SDK) dan antarmuka baris perintah (CLI) untuk menandatangani permintaan Anda secara kriptografis dengan menggunakan kredensil Anda. Jika Anda tidak menggunakan AWS alat, Anda harus menandatangani permintaan sendiri. Untuk informasi selengkapnya tentang penggunaan metode yang disarankan untuk menandatangani permintaan sendiri, lihat Menandatangani permintaan AWS API di Panduan Pengguna IAM.

Apa pun metode autentikasi yang digunakan, Anda mungkin diminta untuk menyediakan informasi keamanan tambahan. Misalnya, AWS merekomendasikan agar Anda menggunakan otentikasi multi-faktor (MFA) untuk meningkatkan keamanan akun Anda. Untuk mempelajari selengkapnya, silakan lihat Autentikasi multi-faktor dalam Panduan Pengguna AWS IAM Identity Center dan Menggunakan autentikasi multi-faktor (MFA) di AWS dalam Panduan Pengguna IAM.

Akun AWS pengguna root

Saat Anda membuat Akun AWS, Anda mulai dengan satu identitas masuk yang memiliki akses lengkap ke semua Layanan AWS dan sumber daya di akun. Identitas ini disebut pengguna Akun AWS root dan diakses dengan masuk dengan alamat email dan kata sandi yang Anda gunakan untuk membuat akun. Kami sangat menyarankan agar Anda tidak menggunakan pengguna root untuk tugas sehari-hari. Lindungi kredensial pengguna root Anda dan gunakan kredensial tersebut untuk melakukan tugas yang hanya dapat dilakukan pengguna root. Untuk daftar lengkap tugas yang mengharuskan Anda masuk sebagai pengguna root, lihat bagian Tugas yang memerlukan kredensial pengguna root dalam Panduan Pengguna IAM.

Pengguna dan grup IAM

Pengguna IAM adalah identitas dalam diri Anda Akun AWS yang memiliki izin khusus untuk satu orang atau aplikasi. Apabila memungkinkan, kami merekomendasikan untuk mengandalkan pada

kredensial sementara alih-alih membuat pengguna IAM yang memiliki kredensial jangka panjang seperti kata sandi dan kunci akses. Namun, jika Anda memiliki kasus penggunaan tertentu yang memerlukan kredensial jangka panjang dengan pengguna IAM, kami merekomendasikan Anda merotasi kunci akses. Untuk informasi selengkapnya, silakan lihat Merotasi kunci akses secara teratur untuk kasus penggunaan yang memerlukan kredensial jangka panjang dalam Panduan Pengguna IAM.

Grup IAM adalah identitas yang menentukan sekumpulan pengguna IAM. Anda tidak dapat masuk sebagai grup. Anda dapat menggunakan grup untuk menentukan izin bagi beberapa pengguna sekaligus. Grup mempermudah pengelolaan izin untuk sejumlah besar pengguna sekaligus. Sebagai contoh, Anda dapat memiliki grup yang diberi nama IAMAdmins dan memberikan izin kepada grup tersebut untuk mengelola sumber daya IAM.

Pengguna berbeda dari peran. Pengguna secara unik terkait dengan satu orang atau aplikasi, tetapi peran dimaksudkan untuk dapat digunakan oleh siapa pun yang membutuhkannya. Pengguna memiliki kredensial jangka panjang permanen, tetapi peran memberikan kredensial sementara. Untuk mempelajari selengkapnya, silakan lihat Kapan harus membuat pengguna IAM (bukan peran) dalam Panduan Pengguna IAM.

Peran IAM

Peran IAM adalah identitas dalam diri Anda Akun AWS yang memiliki izin khusus. Peran ini mirip dengan pengguna IAM, tetapi tidak terkait dengan orang tertentu. Anda dapat mengambil peran IAM untuk sementara AWS Management Console dengan beralih peran. Anda dapat mengambil peran dengan memanggil operasi AWS CLI atau AWS API atau dengan menggunakan URL kustom. Untuk informasi selengkapnya tentang cara menggunakan peran, lihat Menggunakan peran IAM dalam Panduan Pengguna IAM.

Peran IAM dengan kredensial sementara berguna dalam situasi berikut:

- Akses pengguna gabungan – Untuk menetapkan izin ke sebuah identitas gabungan, Anda dapat membuat peran dan menentukan izin untuk peran tersebut. Ketika identitas gabungan mengautentikasi, identitas tersebut terhubung dengan peran dan memperoleh izin yang ditentukan oleh peran. Untuk informasi tentang peran-peran untuk federasi, lihat Membuat peran untuk Penyedia Identitas pihak ketiga dalam Panduan Pengguna IAM. Jika menggunakan Pusat Identitas IAM, Anda harus mengonfigurasi serangkain izin. Untuk mengontrol apa yang dapat diakses oleh identitas Anda setelah diautentikasi, Pusat Identitas IAM menghubungkan izin yang ditetapkan dengan peran di IAM. Untuk informasi tentang rangkaian izin, lihat Rangkaian izin dalam Panduan Pengguna AWS IAM Identity Center .

- Izin pengguna IAM sementara – Pengguna atau peran IAM dapat mengambil peran IAM guna mendapatkan berbagai izin secara sementara untuk tugas tertentu.
- Akses lintas akun – Anda dapat menggunakan peran IAM untuk mengizinkan seseorang (pengguna utama tepercaya) dengan akun berbeda untuk mengakses sumber daya yang ada di akun Anda. Peran adalah cara utama untuk memberikan akses lintas akun. Namun, dengan beberapa Layanan AWS, Anda dapat melampirkan kebijakan secara langsung ke sumber daya (alih-alih menggunakan peran sebagai proxy). Untuk mempelajari perbedaan antara kebijakan peran dan kebijakan berbasis sumber daya untuk akses lintas akun, lihat Bagaimana peran IAM berbeda dari kebijakan berbasis sumber daya dalam Panduan Pengguna IAM.
- Akses lintas layanan — Beberapa Layanan AWS menggunakan fitur lain Layanan AWS. Sebagai contoh, ketika Anda memanggil suatu layanan, biasanya layanan tersebut menjalankan aplikasi di Amazon EC2 atau menyimpan objek di Amazon S3. Layanan dapat melakukan hal tersebut menggunakan izin pengguna utama, menggunakan peran layanan, atau menggunakan peran terkait layanan.
  - Sesi akses teruskan (FAS) — Saat Anda menggunakan pengguna atau peran IAM untuk melakukan tindakan AWS, Anda dianggap sebagai prinsipal. Saat menggunakan beberapa layanan, Anda mungkin melakukan tindakan yang kemudian dilanjutkan oleh tindakan lain pada layanan yang berbeda. FAS menggunakan izin dari pemanggilan utama Layanan AWS, dikombinasikan dengan permintaan Layanan AWS untuk membuat permintaan ke layanan hilir. Permintaan FAS hanya dibuat ketika layanan menerima permintaan yang memerlukan interaksi dengan orang lain Layanan AWS atau sumber daya untuk menyelesaikannya. Dalam hal ini, Anda harus memiliki izin untuk melakukan kedua tindakan tersebut. Untuk detail kebijakan ketika mengajukan permintaan FAS, lihat Sesi akses maju.
  - Peran layanan – Peran layanan adalah peran IAM yang dijalankan oleh layanan untuk melakukan tindakan atas nama Anda. Administrator IAM dapat membuat, memodifikasi, dan menghapus peran layanan dari dalam IAM. Untuk informasi selengkapnya, lihat Membuat peran untuk mendelegasikan izin ke Layanan AWS dalam Panduan Pengguna IAM.
  - Peran terkait layanan — Peran terkait layanan adalah jenis peran layanan yang ditautkan ke peran layanan. Layanan AWS Layanan tersebut dapat menjalankan peran untuk melakukan tindakan atas nama Anda. Peran terkait layanan muncul di Anda Akun AWS dan dimiliki oleh layanan. Administrator IAM dapat melihat, tetapi tidak dapat mengedit izin untuk peran terkait layanan.
- Aplikasi yang berjalan di Amazon EC2 — Anda dapat menggunakan peran IAM untuk mengelola kredensi sementara untuk aplikasi yang berjalan pada instans EC2 dan membuat atau permintaan API. AWS CLI AWS Cara ini lebih dianjurkan daripada menyimpan kunci akses dalam instans

EC2. Untuk menetapkan AWS peran ke instans EC2 dan membuatnya tersedia untuk semua aplikasinya, Anda membuat profil instance yang dilampirkan ke instance. Profil instans berisi peran dan memungkinkan program yang berjalan pada instans EC2 untuk mendapatkan kredensial sementara. Untuk informasi selengkapnya, lihat Menggunakan peran IAM untuk memberikan izin ke aplikasi yang berjalan di instans Amazon EC2 dalam Panduan Pengguna IAM.

Untuk mempelajari apakah kita harus menggunakan peran IAM atau pengguna IAM, lihat Kapan harus membuat peran IAM (bukan pengguna) dalam Panduan Pengguna IAM.

Mengelola akses menggunakan kebijakan

Anda mengontrol akses AWS dengan membuat kebijakan dan melampirkannya ke AWS identitas atau sumber daya. Kebijakan adalah objek AWS yang, ketika dikaitkan dengan identitas atau sumber daya, menentukan izinnya. AWS mengevaluasi kebijakan ini ketika prinsipal (pengguna, pengguna root, atau sesi peran) membuat permintaan. Izin dalam kebijakan dapat menentukan permintaan yang diizinkan atau ditolak. Sebagian besar kebijakan disimpan AWS sebagai dokumen JSON. Untuk informasi selengkapnya tentang struktur dan isi dokumen kebijakan JSON, silakan lihat Gambaran Umum kebijakan JSON dalam Panduan Pengguna IAM.

Administrator dapat menggunakan kebijakan AWS JSON untuk menentukan siapa yang memiliki akses ke apa. Artinya, pengguna utama manakah yang dapat melakukan tindakan pada sumber daya apa, dan dalam kondisi apa.

Secara default, pengguna dan peran tidak memiliki izin. Untuk memberikan izin kepada pengguna untuk melakukan tindakan pada sumber daya yang mereka perlukan, administrator IAM dapat membuat kebijakan IAM. Administrator kemudian dapat menambahkan kebijakan IAM ke peran, dan pengguna dapat menjalankan peran.

Kebijakan IAM mendefinisikan izin untuk suatu tindakan terlepas dari metode yang Anda gunakan untuk operasi. Sebagai contoh, anggap saja Anda memiliki kebijakan yang mengizinkan tindakan `iam:GetRole`. Pengguna dengan kebijakan tersebut bisa mendapatkan informasi peran dari AWS Management Console, API AWS CLI, atau AWS API.

Kebijakan berbasis identitas

Kebijakan berbasis identitas adalah dokumen kebijakan izin JSON yang dapat Anda lampirkan ke sebuah identitas, seperti pengguna IAM, grup pengguna IAM, atau peran IAM. Kebijakan ini mengontrol tindakan apa yang dapat dilakukan oleh pengguna dan peran, pada sumber daya

mana, dan dalam keadaan apa. Untuk mempelajari cara membuat kebijakan berbasis identitas, lihat Membuat kebijakan IAM dalam Panduan Pengguna IAM.

Kebijakan berbasis identitas dapat dikategorikan lebih lanjut sebagai kebijakan inline atau kebijakan terkelola. Kebijakan inline disematkan langsung ke satu pengguna, grup, atau peran. Kebijakan terkelola adalah kebijakan mandiri yang dapat Anda lampirkan ke beberapa pengguna, grup, dan peran dalam. Akun AWS Kebijakan AWS terkelola mencakup kebijakan terkelola dan kebijakan yang dikelola pelanggan. Untuk mempelajari cara memilih antara kebijakan terkelola atau kebijakan inline, lihat Memilih antara kebijakan terkelola dan kebijakan inline dalam Panduan Pengguna IAM.

Kebijakan berbasis sumber daya

Kebijakan berbasis sumber daya adalah dokumen kebijakan JSON yang Anda lampirkan ke sumber daya. Contoh kebijakan berbasis sumber daya adalah kebijakan tepercaya peran IAM dan kebijakan bucket Amazon S3. Dalam layanan yang mendukung kebijakan berbasis sumber daya, administrator layanan dapat menggunakannya untuk mengontrol akses ke sumber daya tertentu. Untuk sumber daya tempat kebijakan dilampirkan, kebijakan menentukan tindakan apa yang dapat dilakukan oleh pengguna utama tertentu pada sumber daya tersebut dan dalam kondisi apa. Anda harus menentukan pengguna utama dalam kebijakan berbasis sumber daya. Prinsipal dapat mencakup akun, pengguna, peran, pengguna federasi, atau. Layanan AWS

Kebijakan berbasis sumber daya merupakan kebijakan inline yang terletak di layanan tersebut. Anda tidak dapat menggunakan kebijakan AWS terkelola dari IAM dalam kebijakan berbasis sumber daya.

Daftar kontrol akses (ACL)

Daftar kontrol akses (ACL) mengendalikan pengguna utama mana (anggota akun, pengguna, atau peran) yang memiliki izin untuk mengakses sumber daya. ACL serupa dengan kebijakan berbasis sumber daya, meskipun tidak menggunakan format dokumen kebijakan JSON.

Amazon S3, AWS WAF, dan Amazon VPC adalah contoh layanan yang mendukung ACL. Untuk mempelajari ACL selengkapnya, lihat Gambaran umum daftar kontrol akses (ACL) dalam Panduan Pengembang Amazon Simple Storage Service.

Jenis kebijakan lain

AWS mendukung jenis kebijakan tambahan yang kurang umum. Jenis-jenis kebijakan ini dapat mengatur izin maksimum yang diberikan kepada Anda berdasarkan jenis kebijakan yang lebih umum.

- Batasan izin – Batasan izin adalah fitur lanjutan di mana Anda menetapkan izin maksimum yang dapat diberikan oleh kebijakan berbasis identitas kepada entitas IAM (pengguna atau peran IAM).

Anda dapat menetapkan batasan izin untuk suatu entitas. Izin yang dihasilkan adalah perpotongan antara kebijakan berbasis identitas milik entitas dan batasan izinnya. Kebijakan berbasis sumber daya yang menentukan pengguna atau peran dalam bidang `Principal` tidak dibatasi oleh batasan izin. Penolakan secara eksplisit terhadap salah satu kebijakan ini akan mengesampingkan izin tersebut. Untuk informasi selengkapnya tentang batasan izin, lihat Batasan izin untuk entitas IAM dalam Panduan Pengguna IAM.

- Kebijakan kontrol layanan (SCP) — SCP adalah kebijakan JSON yang menentukan izin maksimum untuk organisasi atau unit organisasi (OU) di. AWS Organizations AWS Organizations adalah layanan untuk mengelompokkan dan mengelola secara terpusat beberapa Akun AWS yang dimiliki bisnis Anda. Jika Anda mengaktifkan semua fitur di organisasi, Anda dapat menerapkan kebijakan kontrol layanan (SCP) ke salah satu atau semua akun Anda. SCP membatasi izin untuk entitas di akun anggota, termasuk masing-masing. Pengguna root akun AWS Untuk informasi selengkapnya tentang Organisasi dan SCP, lihat Cara kerja SCP dalam Panduan Pengguna AWS Organizations .
- Kebijakan sesi – Kebijakan sesi adalah kebijakan lanjutan yang Anda teruskan sebagai parameter saat Anda membuat sesi sementara secara terprogram untuk peran atau pengguna gabungan. Izin sesi yang dihasilkan adalah perpotongan antara kebijakan berbasis identitas pengguna atau peran dan kebijakan sesi. Izin juga bisa datang dari kebijakan berbasis sumber daya. Penolakan secara eksplisit terhadap salah satu kebijakan ini akan mengesampingkan izin tersebut. Untuk informasi selengkapnya, lihat Kebijakan sesi dalam Panduan Pengguna IAM.

Berbagai jenis kebijakan

Jika beberapa jenis kebijakan diterapkan pada suatu permintaan, izin yang dihasilkan akan lebih rumit untuk dipahami. Untuk mempelajari cara AWS menentukan apakah akan mengizinkan permintaan saat beberapa jenis kebijakan terlibat, lihat Logika evaluasi kebijakan di Panduan Pengguna IAM.

Cara kerja Amazon Kendra dengan IAM

Sebelum menggunakan IAM untuk mengelola akses ke Amazon Kendra, Anda harus memahami fitur IAM apa saja yang tersedia untuk digunakan dengan Amazon Kendra. Untuk mendapatkan tampilan tingkat tinggi tentang cara Amazon Kendra dan layanan AWS lainnya bekerja dengan IAM, AWS lihat Layanan yang Bekerja dengan IAM di Panduan Pengguna IAM.

Topik

- Kebijakan berbasis identitas Amazon Kendra
- Kebijakan berbasis Sumber Daya Amazon Kendra

- Daftar kontrol akses (ACL)
- Otorisasi berdasarkan tanda Amazon Kendra
- IAM Role Amazon Kendra

Kebijakan berbasis identitas Amazon Kendra

Dengan kebijakan berbasis identitas IAM, Anda dapat menentukan tindakan dan sumber daya yang diperbolehkan atau ditolak serta kondisi di mana tindakan diperbolehkan atau ditolak. Amazon Kendra mendukung tindakan, sumber daya, dan kunci syarat tertentu. Untuk mempelajari semua elemen yang Anda gunakan dalam kebijakan JSON, lihat Referensi Elemen Kebijakan JSON IAM dalam Panduan Pengguna IAM.

Tindakan

Administrator dapat menggunakan kebijakan AWS JSON untuk menentukan siapa yang memiliki akses ke apa. Artinya, pengguna utama manakah yang dapat melakukan tindakan pada sumber daya apa, dan dalam kondisi apa.

Elemen `Action` dari kebijakan JSON menjelaskan tindakan-tindakan yang dapat Anda gunakan untuk mengizinkan atau menolak akses dalam sebuah kebijakan. Tindakan kebijakan biasanya memiliki nama yang sama dengan operasi AWS API terkait. Ada beberapa pengecualian, misalnya tindakan hanya izin yang tidak memiliki operasi API yang cocok. Ada juga beberapa operasi yang memerlukan beberapa tindakan dalam suatu kebijakan. Tindakan tambahan ini disebut tindakan dependen.

Menyertakan tindakan dalam kebijakan untuk memberikan izin untuk melakukan operasi terkait.

Tindakan kebijakan di Amazon Kendra menggunakan prefiks berikut sebelum tindakan: `kendra:`. Misalnya, untuk memberikan izin kepada seseorang untuk mencantumkan indeks Amazon Kendra dengan operasi ListIndicesAPI, Anda menyertakan `kendra:ListIndices` tindakan tersebut dalam kebijakan mereka. Pernyataan kebijakan harus memuat elemen `Action` atau `NotAction`. Amazon Kendra menentukan serangkaian tindakannya sendiri yang menjelaskan tugas yang dapat Anda lakukan dengan layanan ini.

Untuk menetapkan beberapa tindakan dalam satu pernyataan, pisahkan dengan koma seperti berikut:

```
"Action": [
```

```
      "kendra:action1",
      "kendra:action2"
```

Anda dapat menentukan beberapa tindakan menggunakan wildcard (*). Sebagai contoh, untuk menentukan semua tindakan yang dimulai dengan kata `Describe`, sertakan tindakan berikut:

```
"Action": "kendra:Describe*"
```

Untuk melihat daftar tindakan Amazon Kendra, lihat Tindakan yang Ditetapkan oleh Amazon Kendra di Panduan Pengguna IAM.

Sumber daya

Administrator dapat menggunakan kebijakan AWS JSON untuk menentukan siapa yang memiliki akses ke apa. Artinya, pengguna utama manakah yang dapat melakukan tindakan pada sumber daya apa, dan dalam kondisi apa.

Elemen kebijakan JSON `Resource` menentukan objek yang menjadi target penerapan tindakan. Pernyataan harus menyertakan entah elemen `Resource` atau `NotResource`. Praktik terbaiknya, tentukan sumber daya menggunakan Amazon Resource Name (ARN). Anda dapat melakukan ini untuk tindakan yang mendukung jenis sumber daya tertentu, yang dikenal sebagai izin tingkat sumber daya.

Untuk tindakan yang tidak mendukung izin di tingkat sumber daya, misalnya operasi pencantuman, gunakan wildcard (*) untuk menunjukkan bahwa pernyataan tersebut berlaku untuk semua sumber daya.

```
"Resource": "*"
```

Sumber daya indeks Amazon Kendra memiliki ARN berikut:

```
arn:${Partition}:kendra:${Region}:${Account}:index/${IndexId}
```

Untuk informasi selengkapnya tentang format ARN, lihat Nama Sumber Daya Amazon (ARN) dan Ruang Nama AWS Layanan.

Misalnya, untuk menetapkan indeks dalam pernyataan Anda, gunakan GUID indeks ARN berikut:

```
"Resource": "arn:aws:kendra:${Region}:${Account}:index/${GUID}"
```

Untuk menetapkan semua indeks milik akun tertentu, gunakan wildcard (*):

```
"Resource": "arn:aws:${Region}:${Account}:index/*"
```

Beberapa tindakan Amazon Kendra, seperti membuat sumber daya, tidak dapat dilakukan pada sumber daya tertentu. Dalam kasus tersebut, Anda harus menggunakan wildcard (*).

```
"Resource": "*"
```

Untuk melihat daftar jenis sumber daya Amazon Kendra dan ARN miliknya, lihat Sumber Daya yang Ditetapkan oleh Amazon Kendra dalam Panduan Pengguna IAM. Untuk mempelajari tindakan yang ARN setiap sumber dayanya dapat Anda tentukan, lihat Tindakan yang Ditentukan oleh Amazon Kendra.

Kunci syarat

Administrator dapat menggunakan kebijakan AWS JSON untuk menentukan siapa yang memiliki akses ke apa. Artinya, pengguna utama manakah yang dapat melakukan tindakan pada sumber daya apa, dan dalam kondisi apa.

Elemen `Condition` (atau blok `Condition`) memungkinkan Anda menentukan kondisi di mana suatu pernyataan akan diterapkan. Elemen `Condition` bersifat opsional. Anda dapat membuat ekspresi kondisional yang menggunakan operator kondisi, misalnya sama dengan atau kurang dari, untuk mencocokkan kondisi dalam kebijakan dengan nilai-nilai yang diminta.

Jika Anda menentukan beberapa elemen `Condition` dalam sebuah pernyataan, atau beberapa kunci dalam elemen `Condition` tunggal, AWS akan mengevaluasinya dengan menggunakan operasi `AND` yang logis. Jika Anda menentukan beberapa nilai untuk satu kunci kondisi, AWS mengevaluasi kondisi menggunakan `OR` operasi logis. Semua kondisi harus dipenuhi sebelum izin pernyataan diberikan.

Anda juga dapat menggunakan variabel placeholder saat menentukan kondisi. Sebagai contoh, Anda dapat memberikan izin kepada pengguna IAM untuk mengakses sumber daya hanya jika izin tersebut mempunyai tanda yang sesuai dengan nama pengguna IAM mereka. Untuk informasi selengkapnya, silakan lihat Elemen kebijakan IAM: variabel dan tanda dalam Panduan Pengguna IAM.

AWS mendukung kunci kondisi global dan kunci kondisi khusus layanan. Untuk melihat semua kunci kondisi AWS global, lihat kunci konteks kondisi AWS global di Panduan Pengguna IAM.

Amazon Kendra tidak menyediakan kunci syarat khusus layanan, tetapi mendukung penggunaan beberapa kunci syarat global. Untuk melihat semua kunci kondisi AWS global, lihat Kunci Konteks Kondisi AWS Global di Panduan Pengguna IAM.

Contoh-contoh

Untuk melihat contoh kebijakan berbasis identitas Amazon Kendra, lihat Contoh kebijakan berbasis Identitas Amazon Kendra.

Kebijakan berbasis Sumber Daya Amazon Kendra

Amazon Kendra tidak mendukung kebijakan berbasis sumber daya.

Daftar kontrol akses (ACL)

Amazon Kendra tidak mendukung daftar kontrol akses (ACL) untuk akses ke layanan dan sumber daya AWS .

Otorisasi berdasarkan tanda Amazon Kendra

Anda dapat mengaitkan tanda dengan jenis sumber daya Amazon Kendra tertentu untuk mengotorisasi akses ke sumber daya tersebut. Untuk mengontrol akses berdasarkan tanda, berikan informasi tanda dalam elemen syarat kebijakan menggunakan `aws:RequestTag/key-name`, atau kunci syarat `aws:TagKeys`.

Tabel berikut mencantumkan tindakan, jenis sumber daya yang sesuai, dan kunci syarat untuk kontrol akses berbasis tanda. Setiap tindakan diotorisasi berdasarkan tanda yang terkait dengan jenis sumber daya yang sesuai.

Tindakan	Jenis sumber daya	Kunci syarat
CreateDataSource		`aws:RequestTag` , `aws:TagKeys`
CreateFaq		`aws:RequestTag` , `aws:TagKeys`

Tindakan	Jenis sumber daya	Kunci syarat
CreateIndex		`aws:RequestTag` , `aws:TagKeys`
API_ ListTagsForResource	sumber data, Pertanyaan yang Sering Diajukan, indeks	
TagResource	sumber data, Pertanyaan yang Sering Diajukan, indeks	`aws:RequestTag` , `aws:TagKeys`
UntagResource	sumber data, Pertanyaan yang Sering Diajukan, indeks	`aws:TagKeys`

Untuk informasi selengkapnya tentang penandaan sumber daya Amazon Kendra, lihat Tag. Untuk melihat contoh kebijakan berbasis identitas yang membatasi akses ke sumber daya berdasarkan tanda sumber daya, lihat Contoh kebijakan berbasis tanda. Untuk informasi tentang penggunaan tanda untuk membatasi akses ke sumber daya, lihat Mengontrol akses menggunakan tanda di Panduan Pengguna IAM.

IAM Role Amazon Kendra

Peran IAM adalah entitas dalam AWS akun Anda yang memiliki izin tertentu.

Menggunakan kredensial sementara dengan Amazon Kendra

Anda dapat menggunakan kredensial sementara untuk masuk dengan gabungan, menjalankan IAM role, atau menjalankan peran lintas akun. Anda memperoleh kredensil keamanan sementara dengan memanggil operasi AWS STS API seperti AssumeRoleatau. GetFederationToken

Amazon Kendra mendukung penggunaan kredensial sementara.

Peran layanan

Fitur ini memungkinkan layanan untuk menerima peran layanan atas nama Anda. Peran ini mengizinkan layanan untuk mengakses sumber daya di layanan lain untuk menyelesaikan tindakan atas nama Anda. Peran layanan muncul di akun IAM Anda dan dimiliki oleh akun tersebut. Ini berarti administrator IAM dapat mengubah izin untuk peran ini. Namun, melakukan hal itu dapat merusak fungsionalitas layanan.

Amazon Kendra mendukung peran layanan.

Memilih IAM role di Amazon Kendra

Ketika membuat indeks, memanggil operasi `BatchPutDocument`, membuat sumber data, atau membuat Pertanyaan yang Sering Diajukan, Anda harus memberikan Amazon Resource Name (ARN) peran akses yang digunakan Amazon Kendra untuk mengakses sumber daya yang diperlukan atas nama Anda. Jika sudah membuat peran, konsol Amazon Kendra akan memberi Anda daftar peran untuk dipilih. Penting untuk memilih peran yang mengizinkan akses ke sumber daya yang Anda butuhkan. Untuk informasi selengkapnya, lihat IAM peran akses untuk Amazon Kendra.

Contoh kebijakan berbasis Identitas Amazon Kendra

Secara default, pengguna dan peran tidak memiliki izin untuk membuat atau memodifikasi sumber daya Amazon Kendra. Mereka juga tidak dapat melakukan tugas menggunakan AWS Management Console, AWS CLI, atau AWS API. Administrator IAM harus membuat kebijakan IAM yang memberikan izin kepada pengguna dan peran untuk melakukan operasi API tertentu pada sumber daya yang diperlukan. Administrator kemudian harus melampirkan kebijakan tersebut ke pengguna atau grup yang memerlukan izin tersebut.

Untuk mempelajari cara membuat kebijakan berbasis identitas IAM menggunakan contoh dokumen kebijakan JSON ini, lihat Membuat Kebijakan pada Tab JSON dalam Panduan Pengguna IAM.

Topik

- Praktik terbaik kebijakan
- AWS Kebijakan Terkelola (Standar) untuk Amazon Kendra
- Izinkan pengguna melihat izin mereka sendiri
- Mengakses satu indeks Amazon Kendra
- Contoh kebijakan berbasis tanda

Praktik terbaik kebijakan

Kebijakan berbasis identitas menentukan apakah seseorang dapat membuat, mengakses, atau menghapus sumber daya Amazon Kendra di akun Anda. Tindakan ini mengenakan biaya kepada Akun AWS Anda. Ketika Anda membuat atau mengedit kebijakan berbasis identitas, ikuti panduan dan rekomendasi ini:

- Mulailah dengan kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit — Untuk mulai memberikan izin kepada pengguna dan beban kerja Anda, gunakan kebijakan AWS terkelola yang memberikan izin untuk banyak kasus penggunaan umum. Mereka tersedia di Anda Akun AWS. Kami menyarankan Anda mengurangi izin lebih lanjut dengan menentukan kebijakan yang dikelola AWS pelanggan yang khusus untuk kasus penggunaan Anda. Untuk informasi selengkapnya, lihat kebijakan terkelola AWS atau kebijakan terkelola AWS untuk fungsi tugas dalam Panduan Pengguna IAM.
- Menerapkan izin dengan hak akses paling rendah – Ketika Anda menetapkan izin dengan kebijakan IAM, hanya berikan izin yang diperlukan untuk melakukan tugas. Anda melakukan ini dengan menentukan tindakan yang dapat diambil pada sumber daya tertentu dalam kondisi tertentu, juga dikenal sebagai izin dengan hak akses paling rendah. Untuk informasi selengkapnya tentang cara menggunakan pengguna IAM untuk mengajukan izin, lihat Kebijakan dan izin di IAM dalam Panduan Pengguna IAM.
- Menggunakan syarat dalam kebijakan IAM untuk membatasi akses lebih lanjut – Anda dapat menambahkan suatu syarat ke kebijakan Anda untuk membatasi akses ke tindakan dan sumber daya. Sebagai contoh, Anda dapat menulis kondisi kebijakan untuk menentukan bahwa semua permintaan harus dikirim menggunakan SSL. Anda juga dapat menggunakan ketentuan untuk memberikan akses ke tindakan layanan jika digunakan melalui yang spesifik Layanan AWS, seperti AWS CloudFormation. Untuk informasi selengkapnya, lihat Elemen kebijakan JSON IAM: Syarat dalam Panduan Pengguna IAM.
- Menggunakan IAM Access Analyzer untuk memvalidasi kebijakan IAM Anda guna memastikan izin yang aman dan berfungsi – IAM Access Analyzer memvalidasi kebijakan baru dan yang sudah ada sehingga kebijakan tersebut mematuhi bahasa kebijakan IAM (JSON) dan praktik terbaik IAM. IAM Access Analyzer menyediakan lebih dari 100 pemeriksaan kebijakan dan rekomendasi yang dapat ditindaklanjuti untuk membantu Anda membuat kebijakan yang aman dan fungsional. Untuk informasi selengkapnya, lihat Validasi kebijakan IAM Access Analyzer dalam Panduan Pengguna IAM.
- Memerlukan otentikasi multi-faktor (MFA) - Jika Anda memiliki skenario yang mengharuskan pengguna IAM atau pengguna root di Anda, Akun AWS aktifkan MFA untuk keamanan tambahan. Untuk mewajibkan MFA saat operasi API dipanggil, tambahkan kondisi MFA pada kebijakan Anda. Untuk informasi selengkapnya, lihat Mengonfigurasi akses API yang diproteksi MFA dalam Panduan Pengguna IAM.

Untuk informasi selengkapnya tentang praktik terbaik dalam IAM, lihat Praktik terbaik keamanan di IAM dalam Panduan Pengguna IAM.

AWS Kebijakan Terkelola (Standar) untuk Amazon Kendra

AWS mengatasi banyak kasus penggunaan umum dengan menyediakan kebijakan IAM mandiri yang dibuat dan dikelola oleh. AWS Kebijakan ini disebut kebijakan AWS terkelola. AWS Kebijakan terkelola memudahkan Anda untuk menetapkan izin kepada pengguna, grup, dan peran daripada jika Anda harus menulis kebijakan sendiri. Untuk informasi selengkapnya, lihat Menambahkan Izin ke Pengguna dalam Panduan Pengguna IAM.

Kebijakan AWS terkelola berikut, yang dapat Anda lampirkan ke grup dan peran di akun Anda, khusus untuk Amazon Kendra:

- AmazonKendraReadOnly— Memberikan akses hanya-baca ke sumber daya Amazon Kendra.
- AmazonKendraFullAccess— Memberikan akses penuh untuk membuat, membaca, memperbarui, menghapus, menandai, dan menjalankan semua sumber daya Amazon Kendra.

Untuk konsol tersebut, peran Anda juga harus memiliki izin `iam:CreateRole`, `iam:CreatePolicy`, `iam:AttachRolePolicy`, dan `s3:ListBucket`.

> **Note**
>
> Anda dapat meninjau izin ini dengan masuk ke konsol IAM dan mencari kebijakan tertentu.

Anda juga dapat membuat kebijakan kustom sendiri untuk memberikan izin bagi tindakan API Amazon Kendra. Anda dapat melampirkan kebijakan kustom ini ke IAM role atau grup yang memerlukan izin tersebut. Untuk contoh kebijakan IAM bagi Amazon Kendra, lihat Contoh kebijakan berbasis Identitas Amazon Kendra.

Izinkan pengguna melihat izin mereka sendiri

Contoh ini menunjukkan cara membuat kebijakan yang mengizinkan para pengguna IAM melihat kebijakan inline dan terkelola yang dilampirkan ke identitas pengguna mereka. Kebijakan ini mencakup izin untuk menyelesaikan tindakan ini di konsol atau menggunakan API atau secara terprogram. AWS CLI AWS

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

```
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "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": "*"
        }
    ]
}
```

Mengakses satu indeks Amazon Kendra

Dalam contoh ini, Anda ingin memberi pengguna di AWS akun Anda akses untuk menanyakan indeks.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "QueryIndex",
            "Effect": "Allow",
            "Action": [
                "kendra:Query"
            ],
```

```
            "Resource": "arn:aws:kendra:${Region}:${Account}:index/${Index ID}"
        }
    ]
}
```

Contoh kebijakan berbasis tanda

Kebijakan berbasis tanda adalah dokumen kebijakan JSON yang menentukan tindakan yang dapat dilakukan oleh prinsip pada sumber daya yang ditandai.

Contoh: Menggunakan tanda untuk mengakses sumber daya

Kebijakan contoh ini memberikan izin kepada pengguna atau peran di AWS akun Anda untuk menggunakan `Query` operasi dengan sumber daya apa pun yang ditandai dengan kunci **`department`** dan nilainya. **`finance`**

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "kendra:Query"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/department": "finance"
                }
            }
        }
   ]
}
```

Contoh: Gunakan tag untuk mengaktifkan operasi Amazon Kendra

Kebijakan contoh ini memberikan izin kepada pengguna atau peran di AWS akun Anda untuk menggunakan operasi Amazon Kendra apa pun `TagResource` kecuali operasi dengan sumber daya apa pun yang ditandai dengan **`department`** kunci dan nilainya. **`finance`**

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

```
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "kendra:*",
            "Resource": "*"
        },
        {
            "Effect": "Deny",
            "Action": [
                "kendra:TagResource"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/department": "finance"
                }
            }
        }
    ]
}
```

Contoh: Menggunakan tanda untuk membatasi akses ke operasi

Contoh kebijakan ini membatasi akses untuk pengguna atau peran di AWS akun Anda untuk menggunakan `CreateIndex` operasi kecuali pengguna memberikan **`department`** tag dan memiliki nilai yang diizinkan **`finance`** dan**`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 kebijakan terkelola untuk Amazon Kendra

Untuk menambahkan izin ke pengguna, grup, dan peran, lebih mudah menggunakan kebijakan AWS terkelola daripada menulis kebijakan sendiri. Dibutuhkan waktu dan keahlian untuk membuat kebijakan yang dikelola pelanggan IAM yang hanya memberi tim Anda izin yang mereka butuhkan. Untuk memulai dengan cepat, Anda dapat menggunakan kebijakan AWS terkelola kami. Kebijakan ini mencakup kasus penggunaan umum dan tersedia di AWS akun Anda. Untuk informasi selengkapnya tentang kebijakan AWS AWS terkelola, lihat kebijakan terkelola di Panduan Pengguna IAM.

AWS layanan memelihara dan memperbarui kebijakan AWS terkelola. Anda tidak dapat mengubah izin dalam kebijakan AWS terkelola. Layanan terkadang menambahkan izin tambahan ke kebijakan yang dikelola AWS untuk mendukung fitur-fitur baru. Jenis pembaruan ini akan memengaruhi semua identitas (pengguna, grup, dan peran) di mana kebijakan tersebut dilampirkan. Layanan kemungkinan besar akan memperbarui kebijakan yang dikelola AWS saat ada fitur baru yang diluncurkan atau saat ada operasi baru yang tersedia. Layanan tidak menghapus izin dari kebijakan AWS terkelola, sehingga pembaruan kebijakan tidak akan merusak izin yang ada.

Selain itu, AWS mendukung kebijakan terkelola untuk fungsi pekerjaan yang mencakup beberapa layanan. Misalnya, kebijakan ReadOnlyAccess AWS terkelola menyediakan akses hanya-baca ke semua AWS layanan dan sumber daya. Saat layanan meluncurkan fitur baru, AWS tambahkan izin

hanya-baca untuk operasi dan sumber daya baru. Untuk melihat daftar dan deskripsi dari kebijakan fungsi tugas, lihat kebijakan yang dikelola AWS untuk fungsi tugas di Panduan Pengguna IAM.

AWS kebijakan terkelola: AmazonKendraReadOnly

Memberikan akses baca saja ke sumber daya Amazon Kendra. Kebijakan ini mencakup izin berikut.

- `kendra` – Mengizinkan pengguna melakukan tindakan yang mengembalikan daftar item atau detail tentang item. Ini termasuk operasi API yang dimulai dengan`Describe`,`List`,`Query`,`BatchGetDocumentStatus`,`GetQuerySuggestions`, atau`GetSnapshots`.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "kendra:Describe*",
                "kendra:List*",
                "kendra:Query",
                "kendra:BatchGetDocumentStatus",
                "kendra:GetQuerySuggestions",
                "kendra:GetSnapshots"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

AWS kebijakan terkelola: AmazonKendraFullAccess

Memberikan akses penuh untuk membuat, membaca, memperbarui, menghapus, menandai, dan menjalankan semua sumber daya Amazon Kendra. Kebijakan ini mencakup izin berikut.

- `kendra`—Memungkinkan kepala sekolah membaca dan menulis akses ke semua tindakan di Amazon Kendra.

- `s3`—Memungkinkan kepala sekolah mendapatkan lokasi bucket Amazon S3 dan daftar bucket.
- `iam`—Memungkinkan kepala sekolah untuk lulus dan daftar peran.
- `kms`—Memungkinkan kepala sekolah untuk mendeskripsikan dan daftar AWS KMS kunci dan alias.
- `secretsmanager`—Memungkinkan kepala sekolah untuk membuat, mendeskripsikan, dan membuat daftar rahasia.
- `ec2`Memungkinkan prinsipal untuk mendeskripsikan grup keamanan, VCP (Virtual Private Cloud), dan subnet.
- `cloudwatch`—Memungkinkan kepala sekolah untuk melihat metrik Cloud Watch.

```
{
    "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 memperbarui kebijakan terkelola AWS

Lihat detail tentang pembaruan kebijakan AWS terkelola untuk Amazon Kendra sejak layanan ini mulai melacak perubahan ini. Untuk mendapatkan pemberitahuan otomatis tentang perubahan pada halaman ini, mulai langganan umpan RSS di halaman riwayat Dokumen Amazon Kendra.

Perubahan	Deskripsi	Tanggal
AmazonKendraReadOnly—Tambahkan izin untuk mendukung GetSnapshots, API BatchGetDocumentStatus	Amazon Kendra menambahkan API `GetSnapshots` baru dan. `BatchGetDocumentStatus` `GetSnapshots` menyediakan data yang menunjukkan bagaimana pengguna Anda berinteraksi dengan aplikasi penelusuran Anda. `BatchGetDocumentStatus` memantau kemajuan pengindeksan dokumen Anda.	Januari 3, 2022
AmazonKendraReadOnly—Tambahkan izin untuk mendukung operasi GetQuerySuggestions	Amazon Kendra menambahkan API baru `GetQuerySuggestions` yang memungkinkan akses untuk mendapatkan saran kueri untuk kueri penelusuran populer, membantu memandu pencarian pengguna Anda. Saat pengguna mengetik kueri pencarian mereka, kueri yang disarankan membantu	27 Mei 2021

Perubahan	Deskripsi	Tanggal
	melengkapi pencarian mereka secara otomatis.	
Amazon Kendra mulai melacak perubahan	Amazon Kendra mulai melacak perubahan untuk kebijakan yang AWS dikelola.	27 Mei 2021

Pemecahan masalah Identitas dan Akses Amazon Kendra

Gunakan informasi berikut untuk membantu Anda mendiagnosis dan mengatasi masalah umum yang mungkin Anda temui saat bekerja menggunakan Amazon Kendra dan IAM.

Topik

- Saya tidak diotorisasi untuk melakukan tindakan di Amazon Kendra
- Saya tidak berwenang untuk melakukan iam: PassRole
- Saya adalah administrator dan ingin mengizinkan orang lain mengakses Amazon Kendra
- Saya ingin mengizinkan orang di luar AWS akun saya untuk mengakses sumber daya Amazon Kendra saya

Saya tidak diotorisasi untuk melakukan tindakan di Amazon Kendra

Jika AWS Management Console memberitahu Anda bahwa Anda tidak berwenang untuk melakukan tindakan, maka Anda harus menghubungi administrator Anda untuk bantuan. Administrator Anda adalah orang yang memberi Anda kredensial masuk.

Contoh kesalahan berikut terjadi ketika `mateojackson` pengguna mencoba menggunakan konsol untuk melihat detail tentang indeks tetapi tidak memiliki `kendra:DescribeIndex` izin.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 kendra:DescribeIndex on resource: index ARN
```

Dalam hal ini, Mateo meminta administratornya untuk memperbarui kebijakan miliknya agar dia dapat mengakses sumber daya `index` dengan menggunakan tindakan `kendra:DescribeIndex`.

Saya tidak berwenang untuk melakukan iam: PassRole

Jika Anda menerima kesalahan bahwa Anda tidak berwenang untuk melakukan `iam:PassRole` tindakan, kebijakan Anda harus diperbarui agar Anda dapat meneruskan peran ke Amazon Kendra.

Beberapa Layanan AWS memungkinkan Anda untuk meneruskan peran yang ada ke layanan tersebut alih-alih membuat peran layanan baru atau peran terkait layanan. Untuk melakukannya, Anda harus memiliki izin untuk meneruskan peran ke layanan.

Contoh kesalahan berikut terjadi saat pengguna IAM bernama `marymajor` mencoba menggunakan konsol tersebut untuk melakukan tindakan di Amazon Kendra. Namun, tindakan tersebut memerlukan layanan untuk mendapatkan izin yang diberikan oleh peran layanan. Mary tidak memiliki izin untuk meneruskan peran tersebut pada layanan.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

Dalam kasus ini, kebijakan Mary harus diperbarui agar dia mendapatkan izin untuk melakukan tindakan `iam:PassRole` tersebut.

Jika Anda memerlukan bantuan, hubungi AWS administrator Anda. Administrator Anda adalah orang yang memberi Anda kredensial masuk.

Saya adalah administrator dan ingin mengizinkan orang lain mengakses Amazon Kendra

Untuk mengizinkan orang lain mengakses Amazon Kendra, Anda harus membuat entitas IAM (pengguna atau peran) bagi orang atau aplikasi yang memerlukan akses. Mereka akan menggunakan kredensial untuk entitas tersebut untuk mengakses AWS. Anda kemudian harus melampirkan kebijakan pada entitas yang memberi mereka izin yang benar di Amazon Kendra.

Untuk segera mulai, lihat Membuat pengguna dan grup khusus IAM pertama Anda di Panduan Pengguna IAM.

Saya ingin mengizinkan orang di luar AWS akun saya untuk mengakses sumber daya Amazon Kendra saya

Anda dapat membuat peran yang dapat digunakan pengguna di akun lain atau pengguna di luar organisasi Anda untuk mengakses sumber daya Anda. Anda dapat menentukan siapa saja yang

dipercaya untuk mengambil peran tersebut. Untuk layanan yang mendukung kebijakan berbasis sumber daya atau daftar kontrol akses (ACL), Anda dapat menggunakan kebijakan tersebut untuk memberi pengguna akses ke sumber daya Anda.

Untuk mempelajari selengkapnya, periksa hal berikut:

- Untuk mempelajari apakah Amazon Kendra mendukung fitur ini, lihat Cara kerja Amazon Kendra dengan IAM.
- Untuk mempelajari cara menyediakan akses ke sumber daya Anda di seluruh sumber daya Akun AWS yang Anda miliki, lihat Menyediakan akses ke pengguna IAM di pengguna lain Akun AWS yang Anda miliki di Panduan Pengguna IAM.
- Untuk mempelajari cara menyediakan akses ke sumber daya Anda kepada pihak ketiga Akun AWS, lihat Menyediakan akses yang Akun AWS dimiliki oleh pihak ketiga dalam Panduan Pengguna IAM.
- Untuk mempelajari cara memberikan akses melalui federasi identitas, lihat Menyediakan akses ke pengguna terautentikasi eksternal (gabungan identitas) dalam Panduan Pengguna IAM.
- Untuk mempelajari perbedaan antara penggunaan peran dan kebijakan berbasis sumber daya untuk akses lintas akun, lihat Perbedaan antara peran IAM dan kebijakan berbasis sumber daya di Panduan Pengguna IAM.

Praktik terbaik keamanan

Amazon Kendra menyediakan sejumlah fitur keamanan untuk dipertimbangkan saat Anda mengembangkan dan menerapkan kebijakan keamanan Anda sendiri. Praktik terbaik berikut adalah pedoman umum dan tidak mewakili solusi keamanan yang lengkap. Karena praktik terbaik ini mungkin tidak sesuai atau cukup untuk lingkungan Anda, anggap sebagai pertimbangan yang membantu dan bukan sebagai resep.

Terapkan prinsip hak istimewa paling rendah

Amazon Kendra menyediakan kebijakan akses terperinci untuk aplikasi yang menggunakan peran. IAM Kami menyarankan agar peran diberikan hanya set minimum hak istimewa yang diperlukan oleh pekerjaan, seperti mencakup aplikasi Anda dan akses ke tujuan log. Kami juga merekomendasikan untuk mengaudit pekerjaan untuk izin secara teratur dan setiap perubahan pada aplikasi Anda.

Izin kontrol akses berbasis peran (RBAC)

Administrator harus secara ketat mengontrol izin kontrol akses berbasis peran (RBAC) untuk aplikasi Amazon Kendra.

Pencatatan log dan pemantauan di Amazon Kendra

Pemantauan adalah bagian penting dalam mempertahankan keandalan, ketersediaan, dan performa aplikasi Amazon Kendra Anda. Untuk memantau panggilan API Amazon Kendra, Anda dapat menggunakannya. AWS CloudTrail Untuk memantau status pekerjaan Anda, gunakan Amazon CloudWatch Logs.

- CloudWatch Alarm Amazon —Menggunakan CloudWatch alarm, Anda menonton satu metrik selama periode waktu yang Anda tentukan. Jika metrik melebihi kebijakan. CloudWatch alarm tidak memanggil tindakan ketika metrik berada dalam keadaan tertentu. Sebaliknya, kondisi tersebut harus diubah dan dipertahankan selama periode tertentu. Untuk informasi selengkapnya, lihat Pemantauan Amazon Kendra dengan Amazon Kendra dengan Amazon Kendra dengan Amazon Kendra dengan Amazon Kendra CloudWatch.
- AWS CloudTrail Log — CloudTrail menyediakan catatan tindakan yang diambil oleh pengguna, peran, atau AWS layanan di Amazon Kendra atau Amazon Kendra Intelligent Ranking. Dengan menggunakan informasi yang dikumpulkan oleh CloudTrail, Anda dapat menentukan permintaan yang dibuat ke Amazon Kendra, alamat IP dari mana permintaan itu dibuat, siapa yang membuat permintaan, kapan dibuat, dan detail tambahan. Lihat informasi yang lebih lengkap di Mencatat panggilan API Amazon Kendra dengan log AWS CloudTrail dan Penskalaan Amazon Kendra Intelligent Ranking Amazon KendraAWS CloudTraillog.

Validasi kepatuhan untuk Amazon Kendra

Auditor pihak ketiga menilai keamanan dan kepatuhan Amazon Kendra sebagai bagian dari beberapa program kepatuhan Amazon Kendra. Amazon Kendra mematuhi hal-hal berikut:

- Undang-Undang Akuntabilitas dan Portabilitas Asuransi Kesehatan (HIPAA)
- Sistem dan Kontrol Organisasi (SOC) 2
- Program Asesor Terdaftar Keamanan Informasi (IRAP)
- Program Manajemen Risiko dan Otorisasi Federal (FedRAMP) Moderat di wilayah Timur/Barat AS

- Program Manajemen Risiko dan Otorisasi Federal (FedRAMP) Tinggi di wilayah AWS GovCloud (AS-Barat)

Untuk daftar AWS layanan dalam lingkup program kepatuhan tertentu, lihat AWS Layanan dalam Lingkup oleh AWS Layanan Program Kepatuhan . Untuk informasi umum, lihat Program AWS Kepatuhan Program AWS .

Anda dapat mengunduh laporan audit pihak ketiga menggunakan AWS Artifact. Untuk informasi selengkapnya, lihat Mengunduh Laporan di Laporan AWS Pengunduhan Artefak .

Tanggung jawab kepatuhan Anda saat menggunakan Amazon Kendra ditentukan oleh sensitivitas data Anda, tujuan kepatuhan perusahaan Anda, serta hukum dan peraturan yang berlaku. AWS menyediakan sumber daya berikut untuk membantu kepatuhan:

- Panduan Mulai Cepat Keamanan dan Kepatuhan Panduan Mulai penerapan ini membahas pertimbangan arsitektur dan memberikan langkah-langkah untuk menerapkan keamanan- dan lingkungan dasar yang berfokus pada kepatuhan. AWS
- Arsitektur untuk Whitepaper Keamanan dan Kepatuhan HIPAA —Whitepaper ini menjelaskan bagaimana perusahaan dapat menggunakan untuk membuat aplikasi yang sesuai dengan HIPAA. AWS
- AWS Sumber Daya AWS —Kumpulan buku kerja dan panduan ini mungkin berlaku untuk industri dan lokasi Anda.
- Mengevaluasi Sumber Daya dengan Aturan dalam Panduan AWS Config Pengembang AWS Config —Layanan menilai seberapa baik konfigurasi sumber daya Anda mematuhi praktik internal, pedoman industri, dan peraturan.
- AWS Security Hub AWS Layanan ini memberikan pandangan komprehensif tentang keadaan keamanan Anda di dalamnya AWS yang membantu Anda memeriksa kepatuhan Anda terhadap standar industri keamanan dan praktik terbaik.

Ketahanan dalam Amazon Kendra

Infrastruktur AWS global dibangun di sekitar AWS Wilayah dan Zona Ketersediaan. AWS Wilayah menyediakan beberapa Availability Zone yang terpisah secara fisik dan terisolasi, yang terhubung dengan latensi rendah, throughput tinggi, dan jaringan yang sangat redundan. Dengan Availability Zone, Anda dapat mendesain dan mengoperasikan aplikasi dan basis data yang secara otomatis mengalami kegagalan di antara zona tanpa gangguan. Zona Ketersediaan memiliki ketersediaan

dan toleransi kesalahan yang lebih baik, dan dapat diskalakan dibandingkan infrastruktur pusat data tunggal atau multi tradisional.

Untuk informasi selengkapnya tentang AWS Wilayah dan Availability Zone, lihat Infrastruktur AWS Global.

Dengan infrastruktur AWS global, Amazon Kendra Enterprise Edition toleran terhadap kesalahan, skalabel, dan sangat tersedia. Mengembalikan indeks ke versi sebelumnya saat ini tidak didukung, tetapi Anda dapat merefresh atau membuat ulang bagian indeks dengan menghapus dan menambahkan kembali sumber data yang ada ke indeks Anda.

Keamanan Infrastruktur di Amazon Kendra

Sebagai layanan terkelola, Amazon Kendra dilindungi oleh keamanan jaringan AWS global. Untuk informasi tentang layanan AWS keamanan dan cara AWS melindungi infrastruktur, lihat Keamanan AWS Cloud. Untuk mendesain AWS lingkungan Anda menggunakan praktik terbaik untuk keamanan infrastruktur, lihat Perlindungan Infrastruktur dalam Kerangka Kerja yang AWS Diarsiteksikan dengan Baik Pilar Keamanan.

Anda menggunakan panggilan API yang AWS dipublikasikan untuk mengakses Amazon Kendra melalui jaringan. Klien harus mendukung hal-hal berikut:

- Keamanan Lapisan Pengangkutan (TLS). Kami mensyaratkan TLS 1.2 dan menganjurkan TLS 1.3.
- Sandi cocok dengan sistem kerahasiaan maju sempurna (perfect forward secrecy, PFS) seperti DHE (Ephemeral Diffie-Hellman) atau ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). Sebagian besar sistem modern seperti Java 7 dan versi lebih baru mendukung mode-mode ini.

Selain itu, permintaan harus ditandatangani dengan menggunakan ID kunci akses dan kunci akses rahasia yang terkait dengan pengguna utama IAM. Atau Anda dapat menggunakan AWS Security Token Service (AWS STS) untuk menghasilkan kredensial keamanan sementara untuk menandatangani permintaan.

Analisis konfigurasi dan kerentanan di AWS Identity and Access Management

AWS menangani tugas-tugas keamanan dasar seperti sistem operasi tamu (OS) dan patching database, konfigurasi firewall, dan pemulihan bencana. Prosedur ini telah ditinjau dan disertifikasi oleh pihak ketiga yang sesuai. Untuk detail selengkapnya, lihat sumber daya berikut:

- Model Tanggung Jawab Bersama
- AWS: Ikhtisar Proses Keamanan (whitepaper)

Sumber daya berikut juga membahas konfigurasi dan analisis kerentanan di AWS Identity and Access Management (IAM):

- Validasi kepatuhan untuk AWS Identity and Access Management
- Praktik terbaik keamanan dan kasus penggunaan di AWS Identity and Access Management.

Kuota untuk Amazon Kendra

Wilayah yang didukung

Untuk daftar AWS wilayah yang Amazon Kendra tersedia, lihat Amazon Kendra wilayah dan titik akhir di Referensi Umum Amazon Web Services.

Kuota

Kuota layanan, juga disebut sebagai batas, adalah jumlah maksimum sumber daya layanan untuk AWS akun Anda. Untuk informasi selengkapnya, lihat Service Quotas Amazon Kendra di Referensi Umum AWS .

Kuota indeks

Deskripsi	Default	Edisi	Dapat disesuaikan
Jumlah maksimum indeks per akun	10	Pengembang, Perusahaan	Ya
Jumlah teks yang diekstraksi untuk indeks dalam satu unit (Pengembang). Anda tidak dapat menambahkan unit tambahan untuk mengekstrak teks untuk Edisi Pengembang.	3 GB	Developer	Tidak
Jumlah teks yang diekstraksi untuk indeks dalam satu unit (Enterprise). Anda dapat menambahk	30 GB	Perusahaan	Ya

Deskripsi	Default	Edisi	Dapat disesuaikan
an hingga 100 unit tambahan untuk mengekstraksi teks untuk Enterprise Edition, atau cukup hubungi Support.			

Kuota konektor sumber data

Deskripsi	Default	Edisi	Dapat disesuaikan
Jumlah maksimum konektor sumber data per indeks (Pengembang)	5	Developer	Tidak
Jumlah maksimum konektor sumber data per indeks (Perusahaan)	50	Perusahaan	Ya
Ukuran maksimum dari satu dokumen atau file mentah saat menggunakan konektor sumber data	50 MB	Pengembang, Perusahaan	Ya
Jumlah maksimum awalan S3 dalam file konfigurasi daftar kontrol akses yang disertakan dalam konektor sumber data Amazon S3	100	Pengembang, Perusahaan	Tidak

Deskripsi	Default	Edisi	Dapat disesuaikan
Ukuran maksimum file konfigurasi daftar kontrol akses yang disertakan dalam konektor sumber Amazon S3 data	50 MB	Pengembang, Perusahaan	Ya

Kuota FAQ

Deskripsi	Default	Edisi	Dapat disesuaikan
Jumlah maksimum FAQ per indeks	30	Pengembang, Perusahaan	Ya
Ukuran maksimal 1 FAQ	5 MB	Pengembang, Perusahaan	Ya
Jumlah maksimum hasil yang dikembali kan untuk FAQ	4	Pengembang, Perusahaan	Ya
Jumlah maksimum karakter yang diizinkan untuk pertanyaan FAQ	300	Pengembang, Perusahaan	Tidak
Jumlah maksimum karakter dalam jawaban FAQ	2000	Pengembang, Perusahaan	Tidak

Kuota tesaurus

Deskripsi	Default	Edisi	Dapat disesuaikan
Jumlah maksimum tesaurus per indeks	1	Pengembang, Perusahaan	Tidak
Ukuran maksimum file tesaurus	5 MB	Pengembang, Perusahaan	Ya
Jumlah maksimum aturan sinonim per tesaurus	10.000	Pengembang, Perusahaan	Ya
Jumlah maksimum sinonim per istilah di semua tesauri dalam indeks	10	Pengembang, Perusahaan	Tidak

Amazon Kendra kuota pengalaman

Deskripsi	Default	Edisi	Dapat disesuaikan
Jumlah maksimum Amazon Kendra pengalaman per indeks	50	Pengembang, Perusahaan	Ya

Kuota kueri dan hasil pencarian

Deskripsi	Default	Edisi	Dapat disesuaikan
Jumlah kueri per detik untuk indeks dalam satu unit (Pengemba	0,05	Developer	Tidak

Deskripsi	Default	Edisi	Dapat disesuaikan
ng). Anda tidak dapat menambahkan unit tambahan untuk kueri untuk Edisi Pengembang.			
Jumlah kueri per detik untuk indeks dalam satu unit (Enterpri se). Anda dapat menambahkan hingga 100 unit tambahan untuk kueri untuk Enterprise Edition, atau cukup hubungi Support.	0.1	Perusahaan	Ya
Jumlah maksimum karakter per teks kueri	1000	Pengembang, Perusahaan	Ya
Jumlah maksimum hasil pencarian per kueri. Default adalah 100. Untuk memungkinkan lebih dari 100 hasil, cukup hubungi Support.	100	Pengembang, Perusahaan	Ya
Jumlah maksimum hasil pencarian per halaman	100	Pengembang, Perusahaan	Ya

Deskripsi	Default	Edisi	Dapat disesuaikan
Jumlah maksimum kata token per teks kueri sebelum pemotongan. Defaultnya adalah 30. Untuk mengizinkan lebih dari 30 kata, cukup hubungi Support.	30	Pengembang, Perusahaan	Ya
Ukuran daftar grup pengguna maksimum per atribut kueri	10	Pengembang, Perusahaan	Ya
Ukuran daftar string maksimum per atribut kueri	10	Pengembang, Perusahaan	Ya

Kuota saran kueri

Deskripsi	Default	Edisi	Dapat disesuaikan
Jumlah maksimum saran kueri yang dikembalikan per GetQuerySuggestions panggilan	10	Pengembang, Perusahaan	Ya
Jumlah bidang/atribut maksimum untuk saran kueri per panggilan GetQuerySuggestions	10	Pengembang, Perusahaan	Ya

Deskripsi	Default	Edisi	Dapat disesuaikan
Jumlah maksimum bidang/atribut tambahan untuk saran kueri per panggilan GetQuerySuggestions	5	Pengembang, Perusahaan	Ya
Jumlah maksimum daftar blok per indeks	1	Pengembang, Perusahaan	Tidak
Ukuran maksimum file teks daftar blok	2 MB	Pengembang, Perusahaan	Ya
Jumlah maksimum item (kata atau frasa) dalam daftar blok	20.000	Pengembang, Perusahaan	Ya
Jumlah maksimum saran kueri yang dikoreksi ejaan untuk ditampilkan dalam panggilan API. `Query`	1	Pengembang, Perusahaan	Ya

Kuota dokumen

Deskripsi	Default	Edisi	Dapat disesuaikan
Jumlah teks yang diekstraksi untuk indeks dalam satu unit (Pengembang). Anda tidak dapat menambahkan unit tambahan untuk mengekstr	3 GB	Developer	Tidak

Deskripsi	Default	Edisi	Dapat disesuaikan
ak teks untuk Edisi Pengembang.			
Jumlah teks yang diekstraksi untuk indeks dalam satu unit (Enterprise). Anda dapat menambahk an hingga 100 unit tambahan untuk mengekstraksi teks untuk Enterprise Edition, atau cukup hubungi Support.	30 GB	Perusahaan	Ya
Ukuran maksimum dari satu dokumen atau file mentah saat menggunakan konektor sumber data	50 MB	Pengembang, Perusahaan	Ya
Ukuran maksimum satu dokumen atau file mentah saat menggunak an `BatchPutD ocument` API	5 MB	Pengembang, Perusahaan	Ya
Jumlah maksimum teks yang diekstraksi dari satu dokumen	5 MB	Pengembang, Perusahaan	Tidak
Jumlah maksimum bidang/atribut khusus per indeks	500	Pengembang, Perusahaan	Tidak

Kuota hasil pencarian unggulan

Deskripsi	Default	Edisi	Dapat disesuaikan
Jumlah maksimum dokumen unggulan per set hasil unggulan	4	Perusahaan	Ya
Jumlah maksimum teks kueri per set hasil unggulan	49	Perusahaan	Tidak
Jumlah maksimum karakter per teks kueri dalam set hasil unggulan	1000	Perusahaan	Ya
Jumlah maksimum set hasil unggulan per indeks	50	Perusahaan	Ya

Rescore/rerank kuota hasil pencarian

Deskripsi	Default	Edisi	Dapat disesuaikan
Jumlah maksimum `Rescore` permintaan per detik untuk rencana eksekusi skor ulang atau satu unit kapasitas. Anda dapat menambahkan hingga 1000 unit tambahan.	0,01	Perusahaan	Tidak

Deskripsi	Default	Edisi	Dapat disesuaikan
Jumlah maksimum rencana eksekusi skor ulang per akun.	50	Perusahaan	Ya
Jumlah maksimum token `Title` untuk dokumen dalam `Rescore` permintaan.	100	Perusahaan	Tidak
Jumlah maksimum token `Body` untuk dokumen dalam `Rescore` permintaan.	200	Perusahaan	Tidak
Jumlah maksimum dokumen dalam `Rescore` permintaan.	25	Perusahaan	Tidak
Jumlah maksimum dokumen per grup dalam `Rescore` permintaan.	3	Perusahaan	Tidak

Untuk informasi selengkapnya tentang kuota Amazon Kendra layanan dan untuk meminta peningkatan kuota, lihat Service Quotas.

Pemecahan Masalah

Bagian ini dapat membantu Anda memecahkan masalah umum yang mungkin Anda temukan saat bekerja dengannya Amazon Kendra.

Topik

Mengatasi masalah sumber data

Bagian ini dapat membantu Anda memecahkan masalah umum saat mengonfigurasi dan menggunakan konektor sumber Amazon Kendra data.

Dokumen saya tidak diindeks

Ketika Anda menyinkronkan Amazon Kendra indeks Anda dengan sumber data, Anda mungkin mengalami masalah yang mencegah dokumen diindeks. Pengindeksan adalah proses dua langkah. Pertama, sumber data diperiksa untuk dokumen baru dan diperbarui untuk diindeks, dan untuk menemukan dokumen untuk dihapus dari indeks. Kedua, pada tingkat dokumen, setiap dokumen diakses dan diindeks.

Kesalahan dapat terjadi di salah satu langkah berikut. Kesalahan tingkat sumber data dilaporkan di konsol dalam bagian riwayat jalan sinkronisasi dari halaman detail sumber data. Status tugas sinkronisasi dapat Berhasil, Tidak lengkap, atau Gagal. Anda juga dapat melihat jumlah dokumen yang diindeks dan dihapus selama tugas berlangsung. Jika statusnya adalah Gagal, pesan akan ditampilkan dalam kolom Detail.

Kesalahan tingkat dokumen dilaporkan dalam Amazon CloudWatch Logs. Anda dapat melihat kesalahan menggunakan CloudWatch konsol.

Untuk membuat laporan status sinkronisasi dokumen, lihat Saya ingin membuat laporan status sinkronisasi untuk dokumen saya.

Tugas sinkronisasi saya gagal

Tugas sinkronisasi biasanya gagal ketika ada kesalahan konfigurasi dalam indeks atau sumber data. Di konsol, Anda dapat menemukan pesan kesalahan di bagian Sync run history pada halaman detail sumber data, di bawah kolom Detail. Kesalahan tingkat dokumen dilaporkan dalam Amazon CloudWatch Logs. Pesan kesalahan memberikan informasi tentang apa yang salah. Masalahnya biasanya indeks atau sumber data tidak memiliki IAM izin yang tepat. Pesan kesalahan menjelaskan izin yang hilang. Berikut beberapa pesan kesalahan yang dapat Anda terima:

`Failed to create log group for job. Please make sure that the IAM role provided has sufficient permissions.`

Jika peran indeks Anda tidak memiliki izin untuk digunakan CloudWatch, sumber data tidak akan dapat membuat CloudWatch log. Jika Anda mendapatkan kesalahan ini, Anda harus menambahkan CloudWatch izin ke peran indeks.

`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.`

Bila Anda menggunakan sumber Amazon S3 data, Amazon Kendra harus memiliki izin untuk mengakses bucket yang berisi dokumen. Anda perlu menambahkan izin Amazon Kendra untuk membaca bucket ke IAM peran sumber data.

`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 membutuhkan izin untuk mengasumsikan IAM peran indeks dan sumber data. Anda perlu menambahkan kebijakan kepercayaan ke peran dengan izin untuk tindakan `sts:AssumeRole`.

Untuk IAM kebijakan yang Amazon Kendra perlu mengindeks sumber data, lihat IAM peran.

Untuk membuat laporan status sinkronisasi dokumen, lihat Saya ingin membuat laporan status sinkronisasi untuk dokumen saya.

Tugas sinkronisasi saya tidak lengkap

Pekerjaan umumnya tidak lengkap ketika mereka telah menyelesaikan proses tingkat sumber data tetapi memiliki beberapa kesalahan selama proses tingkat dokumen. Ketika pekerjaan tidak lengkap, beberapa dokumen mungkin tidak berhasil diindeks. Untuk sumber Amazon S3 data, pekerjaan yang tidak lengkap biasanya disebabkan oleh:

- Metadata yang tidak valid untuk satu atau lebih dokumen.
- Ketika dokumen diserahkan untuk pengindeksan tetapi setidaknya satu dokumen tidak diserahkan.
- Ketika dokumen diserahkan untuk dihapus dari indeks tetapi setidaknya satu dokumen tidak diserahkan.

Untuk memecahkan masalah pekerjaan sinkronisasi yang tidak lengkap, lihat dulu log Anda. CloudWatch

1. Dari kolom detail, pilih Lihat detail di CloudWatch.
2. Meninjau pesan kesalahan untuk melihat apa yang menyebabkan dokumen gagal.

Untuk membuat laporan status sinkronisasi dokumen, lihat Saya ingin membuat laporan status sinkronisasi untuk dokumen saya.

Tugas sinkronisasi saya berhasil tetapi tidak ada dokumen yang diindeks

Kadang-kadang, pekerjaan sinkronisasi indeks akan ditandai sebagai Berhasil tetapi tidak ada dokumen baru atau diperbarui yang diindeks saat Anda mengharapkannya. Alasan yang mungkin termasuk:

- Periksa CloudWatch `DocumentsSubmittedForIndexingFailed` metrik untuk melihat apakah ada dokumen yang gagal disinkronkan. Periksa CloudWatch log Anda untuk detailnya.
- Untuk sumber Amazon S3 data, Anda mungkin telah memberikan Amazon Kendra nama bucket atau awalan yang salah. Pastikan bucket yang digunakan Amazon Kendra adalah yang berisi dokumen untuk diindeks.
- Saat mengindeks ulang dokumen yang gagal diindeks di pekerjaan sebelumnya, tidak Amazon Kendra akan mengindeksnya kecuali Anda telah mengubah dokumen atau file metadata terkait.

Untuk membuat laporan status sinkronisasi dokumen, lihat Saya ingin membuat laporan status sinkronisasi untuk dokumen saya.

Saya mengalami masalah format file saat menyinkronkan sumber data saya

Jika Anda mengalami masalah format file saat menambahkan file ke sumber data Anda atau menyinkronkan sumber data Anda, pastikan bahwa jenis dokumen Anda Amazon Kendra didukung. Untuk daftar jenis dokumen yang didukung oleh Amazon Kendra lihat Jenis atau format dokumen.

Jika Anda menggunakan `BatchPutDocument` API dengan file teks biasa, tentukan `PLAIN_TEXT` sebagai tipe konten.

Saya ingin membuat laporan riwayat sinkronisasi untuk dokumen saya

Saat Anda menyinkronkan konektor sumber Amazon Kendra data, Amazon Kendra dapat menghasilkan laporan status sinkronisasi untuk setiap dokumen di sumber data Anda dan menyalinnya ke Amazon S3 bucket. Selama proses ini, data Anda dienkripsi menggunakan AWS KMS kunci dan hanya dapat dilihat oleh Anda. Status dokumen yang dilaporkan dapat berupa salah satu dari berikut: Gagal, Selesai, atau Berhasil dengan kesalahan.

Sebelum Anda dapat membuat laporan status sinkronisasi, Anda harus melakukan hal berikut:

- Tambahkan prinsip Amazon Kendra layanan berikut ke kebijakan Amazon S3 akses Anda

```
{
    “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/*”
        }
    ]
}
```

- Buat Amazon S3 bucket dengan izin akses ke Amazon Kendra

Jika Anda menggunakan konsol, untuk membuat laporan status sinkronisasi, pilih untuk mengaktifkan opsi Pembuatan riwayat sinkronisasi dari halaman Detail sumber data. Kemudian, masukkan lokasi Amazon S3 bucket dan pilih dari opsi konfigurasi yang tersedia. Laporan akan dihasilkan dari sinkronisasi berikutnya setelah Anda mengaktifkan laporan generate.

Jika Anda menghapus Amazon S3 bucket, Anda akan kehilangan data log dan harus menyiapkan bucket baru untuk menyimpan laporan sinkronisasi baru.

Menghasilkan status laporan sinkronisasi saat ini hanya didukung untuk Amazon S3 konektor.

Berapa lama waktu yang dibutuhkan untuk menyinkronkan sumber data?

Jika tidak ada pembaruan dokumen, waktu sinkronisasi untuk Amazon Kendra indeks meningkat dalam proporsi linier dengan jumlah dokumen. Misalnya, 1.000 dokumen tanpa pembaruan akan memakan waktu sekitar lima menit untuk disinkronkan dan 2.000 dokumen tanpa pembaruan akan memakan waktu sekitar 10 menit. Jika ada pembaruan pada dokumen, maka waktu sinkronisasi akan meningkat berdasarkan jumlah dokumen yang diperbarui.

Berapa biaya untuk menyinkronkan sumber data?

Saat Anda menyinkronkan indeks Anda, dibutuhkan dua menit untuk melakukan pemanasan dan mengaktifkan Amazon EC2 untuk membuat koneksi yang diperlukan. Anda tidak dikenakan biaya selama proses ini. Pengukur penggunaan Anda dimulai hanya setelah pekerjaan sinkronisasi dimulai. Untuk informasi lebih lanjut tentang Amazon Kendra harga, lihat Amazon Kendra harga.

Saya mendapatkan kesalahan Amazon EC2 otorisasi

Jika terjadi kesalahan operasi yang Amazon EC2 tidak sah selama sinkronisasi untuk sumber data virtual private cloud (VPC), kemungkinan peran IAM VPC Anda tidak memiliki izin yang diperlukan. Harap periksa apakah IAM peran yang Anda gunakan untuk sumber data Anda memiliki izin terlampir. Untuk informasi selengkapnya, lihat IAM Peran cloud pribadi virtual.

Saya tidak dapat menggunakan tautan indeks pencarian untuk membuka Amazon S3 objek saya

Amazon Kendra Indeks Anda hanya dapat mengakses file yang sumber Amazon S3 data memberikan izin untuk mengaksesnya. Misalnya, Amazon Kendra tidak dapat mengubah Amazon S3 izin yang menentukan apakah suatu objek dimaksudkan untuk publik atau dienkripsi. Amazon Kendra juga tidak memiliki izin default untuk membuat atau mengembalikan tautan yang ditandatangani untuk Amazon S3 objek. Jika Anda ingin mengaktifkan penautan yang ditandatangani untuk Amazon S3 objek dalam Amazon Kendra indeks, Anda memiliki dua opsi:

- Anda dapat menggunakan tanda tangani hasil kueri indeks Anda dengan objek uri sumber sebelum mengembalikan hasilnya ke halaman pencarian. Untuk step-by-step panduan proses ini, lihat Berbagi objek menggunakan URL yang telah ditetapkan sebelumnya.
- Anda dapat mengganti uri sumber metadata Amazon S3 objek dan membuat layanan Anda tersedia melalui jaringan pengiriman CloudFront konten (CDN) yang terhubung ke bucket. Amazon

S3 Atau, Anda dapat menggunakan titik akhir API Gateway proxy yang mengembalikan URL yang telah ditetapkan sebelumnya dan mengarahkan ulang ke URL tersebut.

Saya mendapatkan pesan kesalahan AccessDenied Saat Menggunakan File Sertifikat SSL

Jika Anda mendapatkan kesalahan akses ditolak saat menggunakan sertifikat SSL dengan sumber data Anda, pastikan IAM peran Anda memiliki izin untuk mengakses file sertifikat SSL di lokasi yang ditentukan. Jika sertifikat dienkripsi dengan AWS KMS kunci, IAM peran Anda juga harus memiliki izin untuk mendekripsi menggunakan kunci. AWS KMS Untuk informasi selengkapnya, lihat Otentikasi dan kontrol akses untuk AWS KMS.

Saya mendapatkan kesalahan otorisasi saat menggunakan sumber SharePoint data

Jika Anda mendapatkan kesalahan otorisasi saat menyinkronkan indeks Anda dengan sumber SharePoint data, konfirmasikan bahwa Anda memiliki peran Admin Situs yang ditetapkan untuk Anda. SharePoint

Indeks saya tidak merayapi dokumen dari sumber data Confluence saya

Jika Amazon Kendra indeks Anda tidak merayapi dokumen dari sumber data Confluence selama proses sinkronisasi, konfirmasikan bahwa Anda adalah bagian dari Grup Administrator di Confluence.

Memecahkan masalah hasil pencarian dokumen

Bagian ini dapat membantu Anda memperbaiki masalah dalam hasil Amazon Kendra pencarian Anda.

Hasil pencarian saya tidak relevan dengan permintaan pencarian saya

Jika hasil pencarian Anda tampak tidak relevan, mungkin karena alasan berikut:

- Hasil dengan `LOW` percaya diri termasuk dalam hasil. Anda dapat memfilter hasil dengan `LOW` percaya diri dengan menggunakan `ScoreAttributes` kolom untuk mengecualikan hasil apa pun dengan nilai`LOW`. QueryResultItem Amazon Kendra memberikan setiap hasil nilai bucket kepercayaan dari salah satu`VERY_HIGH`,`HIGH`, `MEDIUM` dan`LOW`. Nilai-nilai ini menunjukkan tingkat kepercayaan bahwa suatu hasil relevan dengan kueri. Juga, terlepas dari ember kepercayaan,

Amazon Kendra mengembalikan tiga jenis hasil dalam urutan berikut: ANSWER (kutipan jawaban yang disarankan), (FAQ) dan QUESTION_ANSWER DOCUMENT (kutipan dokumen). Oleh karena itu, adalah mungkin untuk QUESTION_ANSWER hasil LOW kepercayaan untuk diposisikan di atas DOCUMENT hasil VERY_HIGH kepercayaan. Namun, tidak selalu benar bahwa LOW kepercayaan diri QUESTION_ANSWER adalah hasil yang lebih baik daripada VERY_HIGH kepercayaan diriDOCUMENT.

- Bidang atau atribut metadata tertentu didorong ke nilai yang sangat tinggi, memengaruhi peringkat hasil. Amazon Kendra mencari indeks Anda menggunakan beberapa parameter seperti judul dokumen, teks, tanggal, dan bidang atau atribut teks khusus. Anda dapat bereksperimen dengan nilai peningkatan yang berbeda untuk mendapatkan hasil terbaik di semua kueri. Anda juga dapat menggunakan penyetelan relevansi dinamis pada tingkat kueri untuk menggunakan nilai peningkatan yang berbeda untuk setiap kueri.
- Pengguna Anda menggunakan istilah khusus saat mereka meminta informasi dan tidak ada sinonim khusus yang disiapkan untuk indeks Anda untuk menangani istilah khusus ini. Untuk detail selengkapnya tentang cara dan kapan menggunakan sinonim, lihat Menambahkan sinonim kustom ke indeks.

Mengapa saya hanya melihat 100 hasil?

Amazon Kendra mengembalikan jumlah total dokumen yang relevan. 100 teratas dikembalikan per kueri secara default. Hasilnya dipaginasi. Anda dapat menggunakan PageNumber untuk mengakses halaman yang berbeda.

Anda dapat mengonfigurasi Amazon Kendra untuk mengembalikan hingga 1.000 dokumen atau hasil pencarian per kueri, dengan hingga 100 hasil per halaman. Untuk mengembalikan lebih dari 100 hasil, Anda dapat meminta ini dengan menghubungi Quotas Support. Meningkatkan jumlah hasil pencarian dapat memengaruhi latensi.

Mengapa dokumen yang saya harapkan hilang?

Amazon Kendra mendukung daftar kontrol akses (ACL) berdasarkan pengguna dan grup. Amazon Kendra mencerna kebijakan ACL melalui konektor. Jika indeks tidak mengkonfigurasi ACL, hanya dokumen yang cocok dengan filter atribut untuk pengguna dan kelompok yang akan ditampilkan. Jika filter atribut pengguna atau grup disediakan, dokumen tanpa ACL tidak akan ditampilkan.

Jika Anda menggunakan kontrol akses berbasis token, dokumen tanpa kebijakan ACL dan dokumen yang cocok dengan pengguna dan grup akan ditampilkan.

Mengapa saya melihat dokumen yang memiliki kebijakan ACL?

Jika indeks tidak mengonfigurasi kebijakan kontrol akses, maka pengguna dan grup dapat disediakan oleh filter. Jika tidak ada filter pengguna dan grup yang diterapkan, maka semua dokumen terkait akan dikembalikan. Setiap kebijakan ACL akan diabaikan.

Memecahkan masalah umum

Amazon Kendra menggunakan CloudWatch metrik dan log untuk memberikan wawasan tentang sinkronisasi sumber data Anda. Anda dapat menggunakan metrik dan log untuk menentukan apa yang salah dengan menjalankan sinkronisasi dan cara memperbaikinya.

Untuk pemecahan masalah umum, mulailah dengan metrik Anda CloudWatch .

- Periksa metrik `DocumentsCrawled` untuk melihat berapa banyak dokumen yang diperiksa sumber data Anda. Untuk Amazon S3 bucket, jika jumlahnya kurang dari yang Anda harapkan, periksa apakah sumber data Anda mengarah ke bucket yang tepat.
- Periksa metrik `DocumentsSkippedNoChange` untuk melihat berapa banyak dokumen yang dilewati karena tidak berubah sejak sinkronisasi terakhir. Jika nomor tersebut tidak sesuai dengan yang Anda harapkan, periksa apakah repositori Anda telah diperbarui dengan benar.
- Periksa metrik `DocumentsSkippedInvalidMetadata` untuk melihat berapa banyak dokumen yang memiliki metadata yang tidak valid. Periksa CloudWatch log Anda untuk melihat kesalahan spesifik yang terjadi.
- Periksa `DocumentsSubmittedForIndexingFailed` metrik untuk melihat berapa banyak dokumen yang dikirim dari sumber data ke indeks tetapi gagal diindeks. Misalnya, jika Anda menggunakan atribut metadata dalam sumber Amazon S3 data yang belum didefinisikan sebagai bidang indeks kustom, dokumen tidak akan diindeks. Periksa CloudWatch log Anda untuk melihat kesalahan spesifik yang terjadi.
- Periksa metrik `DocumentsSubmittedForDeletionFailed` untuk melihat berapa banyak dokumen yang coba dihapus oleh sumber data dari indeks, tetapi gagal dihapus dari indeks. Periksa CloudWatch log Anda untuk melihat kesalahan spesifik yang terjadi.

Anda dapat melihat CloudWatch log untuk menjalankan sinkronisasi tertentu untuk mendapatkan detail kesalahan yang terjadi selama proses. Untuk informasi selengkapnya tentang CloudWatch log dengan Amazon Kendra, lihat CloudWatch Logs.

Amazon KendraPeringkat Cerdas

Amazon KendraIntelligent Ranking menggunakan kemampuan pencarian Amazon Kendra semantik untuk secara cerdas memberi peringkat ulang hasil layanan pencarian.

Topik

Amazon Kendra Peringkat Cerdas untuk dikelola sendiri OpenSearch

Anda dapat memanfaatkan Amazon Kendra kemampuan pencarian semantik untuk meningkatkan hasil pencarian dari OpenSearch, layanan pencarian sumber terbuka yang dikelola sendiri berdasarkan Lisensi Apache 2.0. Plugin Amazon Kendra Intelligent Ranking secara semantik memberi peringkat ulang hasil menggunakan OpenSearch. Amazon Kendra Ini dilakukan dengan memahami arti dan konteks kueri penelusuran menggunakan bidang tertentu, seperti badan dokumen atau judul, dari hasil OpenSearch pencarian default.

Ambil, misalnya, kueri ini: “alamat utama utama”. Karena 'alamat' memiliki beberapa arti, Amazon Kendra dapat menyimpulkan makna di balik kueri untuk mengembalikan informasi yang relevan selaras dengan makna yang dimaksudkan. Dalam konteks ini, ini adalah pidato utama konferensi. Layanan pencarian yang lebih sederhana mungkin tidak memperhitungkan maksud dan mungkin dapat mengembalikan hasil untuk alamat jalan di Main Street, misalnya.

Plugin Intelligent Ranking untuk OpenSearch tersedia untuk OpenSearch (dikelola sendiri) versi 2.4.0 dan yang lebih baru. Anda dapat menginstal plugin menggunakan skrip Bash start cepat untuk membangun gambar Docker baru OpenSearch dengan plugin Intelligent Ranking disertakan. Lihat Menyiapkan plugin pencarian cerdas —ini adalah contoh pengaturan untuk membuat Anda bangun dan berjalan dengan cepat.

Cara kerja plugin pencarian cerdas

Proses keseluruhan plugin Intelligent Ranking untuk OpenSearch (dikelola sendiri) adalah sebagai berikut:

1. OpenSearch Pengguna mengeluarkan kueri, dan OpenSearch memberikan respons kueri atau daftar dokumen yang relevan dengan kueri.
2. Plugin Intelligent Ranking mengambil respons kueri dan mengekstrak informasi dari dokumen.
3. Plugin Intelligent Ranking membuat panggilan ke API Rescore Amazon Kendra Intelligent Ranking.
4. `Rescore`API mengambil informasi yang diekstraksi dari dokumen dan secara semantik memberi peringkat ulang hasil pencarian.
5. `Rescore`API mengirimkan hasil pencarian peringkat ulang kembali ke plugin. Plugin mengatur ulang hasil pencarian dalam respons OpenSearch pencarian untuk mencerminkan peringkat semantik baru.

Plugin Intelligent Ranking memberi peringkat ulang hasil menggunakan bidang “body” dan “title”. Bidang plugin ini dapat dipetakan ke bidang dalam OpenSearch indeks Anda yang paling sesuai dengan definisi badan dan judul dokumen. Misalnya, jika indeks Anda berisi bab-ab buku dengan bidang seperti “chapter_heading” dan “chapter_contents”, Anda dapat memetakan yang pertama ke “judul” dan yang terakhir ke “badan” untuk mendapatkan hasil terbaik.

Menyiapkan plugin pencarian cerdas

Berikut ini menguraikan cara mengatur dengan cepat OpenSearch (dikelola sendiri) dengan plugin Intelligent Ranking.

Menyiapkan OpenSearch (dikelola sendiri) dengan plugin Intelligent Ranking (pengaturan cepat)

Jika Anda sudah menggunakan gambar Docker`opensearch:2.4.0`, Anda dapat menggunakan Dockerfile ini untuk membangun gambar baru OpenSearch 2.4.0 dengan plugin Intelligent Ranking. Anda menyertakan wadah untuk gambar baru di file docker-compose.ymlmu atau file opensearch.ymlmu. Anda juga menyertakan ID rencana eksekusi skor ulang yang dihasilkan dari pembuatan rencana eksekusi skor ulang, bersama dengan informasi wilayah dan titik akhir Anda—lihat langkah 2 untuk membuat rencana eksekusi skor ulang.

Jika sebelumnya Anda telah mengunduh versi gambar `opensearch` Docker yang lebih tua dari 2.4.0, Anda harus menggunakan gambar Docker `opensearch:2.4.0` atau yang lebih baru dan membuat gambar baru dengan plugin Intelligent Ranking disertakan.

1. Unduh dan instal Docker Desktop untuk sistem operasi Anda. Docker Desktop mencakup Docker Compose dan Docker Engine. Disarankan agar Anda memeriksa apakah komputer Anda memenuhi persyaratan sistem yang disebutkan dalam detail instalasi Docker.

Anda juga dapat meningkatkan persyaratan penggunaan memori Anda dalam pengaturan Desktop Docker Anda. Anda bertanggung jawab atas persyaratan penggunaan Docker di luar batas penggunaan yang tersedia secara gratis untuk layanan Docker. Lihat langganan Docker.

Periksa status Docker Desktop “berjalan”.

2. Ketentuan Peringkat Amazon Kendra Cerdas dan persyaratan kapasitas Anda. Setelah Anda memberikan Amazon Kendra Intelligent Ranking, Anda akan dikenakan biaya per jam berdasarkan unit kapasitas yang Anda tetapkan. Lihat informasi tingkat dan harga gratis.

   Anda menggunakan CreateRescoreExecutionPlanAPI untuk menyediakan`Rescore API`. Jika Anda tidak memerlukan unit kapasitas lebih dari satu unit default, jangan tambahkan lebih banyak unit dan berikan hanya nama untuk rencana eksekusi skor ulang Anda. Anda juga dapat memperbarui persyaratan kapasitas Anda dengan menggunakan UpdateRescoreExecutionPlanAPI. Untuk informasi selengkapnya, lihat secara semantik memberi peringkat hasil layanan penelusuran.

   Secara opsional, Anda dapat pergi ke langkah 3 untuk membuat rencana eksekusi skor ulang default ketika Anda menjalankan skrip Bash mulai cepat.

   Catatan untuk langkah 4, skor ulang ID rencana eksekusi yang disertakan dalam respons.

   CLI

   ```
   aws kendra-ranking create-rescore-execution-plan \
     --name MyRescoreExecutionPlan \
     --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. Unduh skrip Bash mulai cepat dari GitHub untuk versi Anda OpenSearch dengan memilih cabang versi dari dropdown cabang utama.

   Skrip ini menggunakan gambar Docker untuk OpenSearch dan OpenSearch Dasbor menggunakan versi yang Anda pilih di GitHub repositori skrip. Ini mengunduh file zip untuk plugin Intelligent Ranking, dan menghasilkan `Dockerfile` untuk membangun gambar Docker baru OpenSearch yang menyertakan plugin. Ini juga membuat file docker-compose.yl yang menyertakan wadah untuk OpenSearch plugin Intelligent Ranking dan Dasbor. OpenSearch Skrip menambahkan ID rencana eksekusi skor ulang Anda, informasi wilayah, dan titik akhir (menggunakan wilayah) ke file docker-compose.yl. Skrip kemudian berjalan `docker-compose up` untuk memulai wadah OpenSearch dengan Intelligent Ranking disertakan dan OpenSearch Dashboards. Untuk menghentikan wadah tanpa melepasnya, jalankan`docker-compose stop`. Untuk menghapus wadah, jalankan`docker-compose down`.

4. Buka terminal Anda dan di direktori skrip Bash, jalankan perintah berikut.

   ```
   bash search_processing_kendra_quickstart.sh -p <execution-plan-id> -r <region>
   ```

   Saat menjalankan perintah ini, Anda memberikan ID rencana eksekusi skor ulang yang Anda catat di langkah 2 saat Anda menyediakan Amazon Kendra Intelligent Ranking, bersama dengan informasi wilayah Anda. Secara opsional, Anda dapat menyediakan Amazon Kendra Intelligent Ranking dengan menggunakan `--create-execution-plan` opsi. Ini membuat rencana eksekusi skor ulang dengan nama default dan kapasitas default.

   Untuk tidak kehilangan indeks Anda saat wadah sementara default dihapus, indeks Anda dapat bertahan di seluruh eksekusi dengan memberikan nama volume data menggunakan opsi. `--volume-name` Jika sebelumnya Anda membuat indeks, Anda dapat menentukan volume di file docker-compose.yl atau opensearch.yml. Anda. Agar volume Anda tetap utuh, jangan lari`docker-compose down -v`.

   Skrip Bash start cepat mengonfigurasi AWS kredensyal Anda di OpenSearch keystore untuk terhubung ke Intelligent Ranking. Amazon Kendra Untuk memberikan AWS kredensyal Anda ke skrip, gunakan `--profile` opsi untuk menentukan profil. AWS Jika `--profile` opsi tidak ditentukan, maka skrip Bash start cepat mencoba membaca AWS kredensyal (kunci akses/rahasia, token sesi opsional) dari variabel lingkungan, dan kemudian dari profil default. AWS Jika `--profile` opsi tidak ditentukan dan tidak ada kredensyal yang ditemukan, skrip tidak akan meneruskan kredensyal ke keystore. OpenSearch Jika tidak ada kredensyal yang ditentukan

di OpenSearch keystore, plugin masih memeriksa kredensyal di Rantai Penyedia Kredensyal Default, termasuk kredensyal Amazon ECS kontainer atau kredensyal profil instance yang dikirimkan melalui layanan metadata. Amazon EC2

Pastikan Anda telah membuat IAM peran dengan izin yang diperlukan untuk memanggil Amazon Kendra Intelligent Ranking. Berikut ini adalah contoh IAM kebijakan untuk memberikan izin untuk menggunakan `Rescore` API untuk rencana eksekusi skor ulang tertentu:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "kendra-ranking:Rescore",
            "Resource": "arn:aws:kendra-ranking:${Region}:${Account}:rescore-
execution-plan/${RescoreExecutionPlanId}"
        }
    ]
}
```

Contoh docker-compose.yl

Contoh file docker-compose.yl menggunakan OpenSearch 2.4.0 atau yang lebih baru dengan plugin Intelligent Ranking dan Dashboards 2.4.0 atau yang lebih baru. 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
```

Contoh Dockerfile dan membangun gambar

Contoh `Dockerfile` untuk menggunakan OpenSearch 2.4.0 atau yang lebih baru dengan plugin Intelligent Ranking.

```
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
```

Membangun gambar Docker OpenSearch dengan plugin Intelligent Ranking.

```
docker build --tag=<Docker image tag name of OpenSearch with Intelligent Ranking
 plugin>
```

Berinteraksi dengan plugin pencarian cerdas

Setelah Anda mengatur OpenSearch (dikelola sendiri) dengan plugin Intelligent Ranking, Anda dapat berinteraksi dengan plugin menggunakan perintah curl atau pustaka OpenSearch klien. Kredensyal default untuk mengakses OpenSearch dengan plugin Intelligent Ranking adalah nama pengguna 'admin' dan kata sandi 'admin'.

Untuk menerapkan pengaturan plugin Intelligent Ranking ke OpenSearch indeks:

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)
```

Anda harus menyertakan nama bidang teks utama yang ingin Anda gunakan untuk menentukan peringkat ulang, seperti badan dokumen atau bidang isi dokumen. Anda juga dapat menyertakan bidang teks lainnya, seperti judul dokumen atau ringkasan dokumen.

Sekarang Anda dapat mengeluarkan kueri apa pun dan hasilnya diberi peringkat menggunakan plugin Intelligent Ranking.

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)
```

Untuk menghapus setelan plugin Intelligent Ranking untuk OpenSearch indeks:

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)
```

Untuk menguji plugin Intelligent Ranking pada kueri tertentu atau untuk menguji pada kolom tubuh dan judul tertentu:

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)
```

Membandingkan OpenSearch hasil dengan Amazon Kendra hasil

Anda dapat membandingkan hasil peringkat side-by-side OpenSearch (dikelola sendiri) dengan Amazon Kendra hasil peringkat ulang. OpenSearch Dasbor versi 2.4.0 dan yang lebih baru menawarkan side-by-side hasil sehingga Anda dapat membandingkan bagaimana OpenSearch peringkat dokumen dengan bagaimana Amazon Kendra atau plugin memberi peringkat dokumen untuk kueri penelusuran.

Sebelum Anda dapat membandingkan hasil OpenSearch peringkat dengan hasil Amazon Kendra peringkat ulang, pastikan OpenSearch Dasbor Anda didukung oleh OpenSearch server dengan plugin Intelligent Ranking. Anda dapat mengatur ini menggunakan Docker dan skrip Bash mulai cepat. Lihat Menyiapkan plugin pencarian cerdas.

Berikut ini menguraikan cara membandingkan OpenSearch dan Amazon Kendra mencari hasil di OpenSearch Dasbor. Untuk informasi selengkapnya, lihat OpenSearchDokumentasi.

Membandingkan hasil pencarian di OpenSearch Dasbor

1. Buka http://localhost:5601 dan masuk ke OpenSearch Dasbor. Kredensyal default adalah nama pengguna 'admin' dan kata sandi 'admin'.
2. Pilih Cari Relevansi dari OpenSearch plugin di menu navigasi.
3. Masukkan teks pencarian di bilah pencarian.
4. Pilih indeks Anda untuk Query 1 dan masukkan kueri di OpenSearch Query DSL. Anda dapat menggunakan `%SearchText%` variabel untuk merujuk ke teks pencarian yang Anda masukkan di bilah pencarian. Untuk contoh kueri ini, lihat OpenSearch Dokumentasi. Hasil yang

dikembalikan untuk kueri ini adalah OpenSearch hasil tanpa menggunakan plugin Intelligent Ranking.

5. Pilih indeks yang sama untuk Query 2 dan masukkan kueri yang sama di OpenSearch Query DSL. Selain itu, sertakan ekstensi dengan `kendra_intelligent_ranking` dan tentukan wajib `body_field` untuk diberi peringkat. Anda juga dapat menentukan bidang judul, tetapi bidang tubuh adalah wajib. Untuk contoh kueri ini, lihat OpenSearch Dokumentasi. Hasil yang dikembalikan untuk kueri ini adalah hasil yang Amazon Kendra diberi peringkat ulang menggunakan plugin Intelligent Ranking. Plugin peringkat hingga 25 hasil.
6. Pilih Cari untuk mengembalikan dan membandingkan hasil.

Secara semantik memberi peringkat hasil layanan pencarian

Amazon Kendra Intelligent Ranking menggunakan Amazon Kendra kemampuan pencarian semantik untuk menentukan peringkat ulang hasil layanan pencarian. Ini dilakukan dengan mempertimbangkan konteks permintaan pencarian, ditambah semua informasi yang tersedia dari dokumen layanan pencarian. Amazon Kendra Intelligent Ranking dapat meningkatkan pencocokan kata kunci sederhana.

CreateRescoreExecutionPlanAPI membuat resource Amazon Kendra Intelligent Ranking yang digunakan untuk menyediakan Rescore API. `Rescore`API memberi peringkat ulang hasil penelusuran dari layanan penelusuran seperti OpenSearch (dikelola sendiri).

Saat meneleponCreateRescoreExecutionPlan, Anda menetapkan unit kapasitas yang diperlukan untuk menentukan peringkat ulang hasil layanan pencarian. Jika Anda tidak membutuhkan lebih banyak unit kapasitas di luar default unit tunggal, jangan ubah default. Berikan hanya nama untuk rencana eksekusi skor ulang Anda. Anda dapat mengatur hingga 1000 unit tambahan. Untuk informasi tentang apa yang termasuk dalam satu unit kapasitas, lihat Menyesuaikan kapasitas. Setelah Anda memberikan Amazon Kendra Intelligent Ranking, Anda akan dikenakan biaya per jam berdasarkan unit kapasitas yang Anda tetapkan. Lihat informasi tingkat dan harga gratis.

ID rencana eksekusi skor ulang dihasilkan dan dikembalikan dalam respons saat Anda meneleponCreateRescoreExecutionPlan. `Rescore`API menggunakan ID rencana eksekusi skor ulang untuk menentukan peringkat ulang hasil layanan penelusuran menggunakan kapasitas yang Anda tetapkan. Anda menyertakan ID rencana eksekusi skor ulang dalam file konfigurasi layanan pencarian Anda. Misalnya, jika Anda menggunakan OpenSearch (dikelola sendiri), Anda menyertakan ID rencana eksekusi skor ulang di file docker-compose.yl atau opensearch.yml—lihat Hasil peringkat (layanan mandiri) secara cerdas. OpenSearch

Nama Sumber Daya Amazon (ARN) juga dihasilkan dalam respons saat Anda menelepon. `CreateRescoreExecutionPlan` Anda dapat menggunakan ARN ini untuk membuat kebijakan izin di AWS Identity and Access Management (IAM) untuk membatasi akses pengguna ke ARN tertentu untuk rencana eksekusi skor ulang tertentu. Untuk contoh IAM kebijakan yang memberikan izin untuk menggunakan `Rescore` API untuk rencana eksekusi skor ulang tertentu, lihat Peringkat Amazon Kendra Cerdas untuk dikelola sendiri OpenSearch.

Berikut ini adalah contoh pembuatan rencana eksekusi rescore dengan unit kapasitas diatur ke 1.

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.");
  }
}
```

Berikut ini adalah contoh memperbarui rencana eksekusi rescore untuk mengatur unit kapasitas ke 2.

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.");
  }
}
```

Berikut ini adalah contoh penggunaan `Rescore` API.

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());
```

```
    }
}
```

Riwayat dokumen untuk Amazon Kendra

- Pembaruan dokumentasi terbaru: 27 Februari 2024

Tabel berikut menjelaskan perubahan penting dalam setiap rilis Amazon Kendra. Untuk notifikasi tentang pembaruan dokumentasi ini, Anda dapat berlangganan ke umpan RSS.

Perubahan	Deskripsi	Tanggal
Fitur baru	Amazon Kendra sekarang mendukung versi terbaru dari konektor sumber GitHub data. Untuk informasi lebih lanjut, lihat GitHub.	Februari 27, 2024
Fitur baru	Amazon Kendra sekarang mendukung versi terbaru dari konektor sumber Amazon FSx data. Untuk informasi selengkapnya, lihat Amazon FSx (Windows) dan Amazon FSx (NetAppONTAP).	Februari 8, 2024
Fitur baru	Amazon Kendra sekarang mendukung versi terbaru dari konektor sumber data Slack. Untuk informasi lebih lanjut, lihat Slack.	Januari 11, 2024
Fitur baru	Amazon Kendra sekarang mendukung penciutan dan perluasan hasil pencarian Anda. Untuk informasi selengkapnya, lihat Menciutkan/memperluas hasil penelusuran.	19 Oktober 2023

Fitur baru	Amazon Kendra sekarang mendukung konektor sumber data Aurora (MySQL). Untuk informasi selengkapnya, lihat Aurora (MySQL).	28 September 2023
Fitur baru	Amazon Kendra sekarang mendukung konektor sumber Aurora data (PostgreSQL). Untuk informasi lebih lanjut, lihat Aurora (PostgreSQL).	28 September 2023
Fitur baru	Amazon Kendra sekarang mendukung konektor sumber data Amazon RDS (MySQL). Untuk informasi selengkapnya, lihat Amazon RDS (MySQL).	28 September 2023
Fitur baru	Amazon Kendra sekarang mendukung konektor sumber data Amazon RDS (Microsoft SQL Server). Untuk informasi selengkapnya, lihat Amazon RDS (Microsoft SQL Server).	28 September 2023
Fitur baru	Amazon Kendra sekarang mendukung konektor sumber data Amazon RDS (Oracle). Untuk informasi lebih lanjut, lihat Amazon RDS (Oracle).	28 September 2023
Fitur baru	Amazon Kendra sekarang mendukung konektor sumber Amazon RDS data (PostgreSQL). Untuk informasi lebih lanjut, lihat Amazon RDS (PostgreSQL).	28 September 2023

Fitur baru	Amazon Kendra sekarang mendukung konektor sumber data IBM DB2. Untuk informasi lebih lanjut, lihat IBM DB2.	28 September 2023
Fitur baru	Amazon Kendra sekarang mendukung konektor sumber data Microsoft SQL Server. Untuk informasi selengkapnya, lihat Microsoft SQL Server.	28 September 2023
Fitur baru	Amazon Kendra sekarang mendukung konektor sumber data MySQL. Untuk informasi selengkapnya, lihat MySQL.	28 September 2023
Fitur baru	Amazon Kendra sekarang mendukung konektor sumber data Oracle Database. Untuk informasi selengkapnya, lihat Oracle Database.	28 September 2023
Fitur baru	Amazon Kendra sekarang mendukung konektor sumber data PostgreSQL. Untuk informasi lebih lanjut, lihat PostgreSQL.	28 September 2023
Fitur baru	Amazon Kendra sekarang menyediakan konektor sumber data untuk Drupal. Untuk informasi lebih lanjut, lihat Drupal.	September 6, 2023

Fitur baru	Ambil bagian yang relevan secara semantik menggunakan Amazon Kendra Retrieve API untuk sistem retrieval augmented generation (RAG).	22 Juni 2023
Fitur baru	Amazon Kendra sekarang mendukung versi terbaru dari konektor sumber data Amazon Kendra Web Crawler. Untuk informasi selengkapnya, lihat Amazon Kendra Web Crawler v2.0.	Juni 21, 2023
Perluasan wilayah	Amazon Kendra sekarang tersedia di Eropa (London) (eu-barat-2).	Juni 5, 2023
Fitur baru	Amazon Kendra sekarang mendukung versi terbaru dari konektor sumber data Alfresco. Untuk informasi lebih lanjut, lihat Alfresco.	16 Mei 2023
Fitur baru	Amazon Kendra sekarang menyediakan konektor sumber data untuk Adobe Experience Manager. Untuk informasi selengkapnya, lihat Adobe Experience Manager.	11 Mei 2023

Fitur baru	Amazon Kendra sekarang mendukung konfigurasi bidang/atribut dokumen saat Anda menelepon. GetQuerySuggestions Anda sekarang dapat mendasarkan saran kueri pada isi bidang dokumen. Untuk informasi selengkapnya, lihat Saran kueri.	2 Mei 2023
Fitur baru	Amazon Kendra sekarang menyediakan konektor sumber data untuk Gmail. Untuk informasi selengkapnya, lihat Gmail.	13 April 2023
Fitur baru	Amazon Kendra sekarang mendukung versi terbaru dari konektor sumber OneDrive data Microsoft. Untuk informasi selengkapnya, lihat Microsoft OneDrive v2.0.	3 April 2023
Fitur baru	Tingkatkan visibilitas dokumen baru atau promosikan dokumen tertentu saat pengguna Anda mengetik kueri tertentu menggunakan hasil Unggulan.	30 Maret 2023
Fitur baru	Amazon Kendra sekarang mendukung konektor sumber data yang diperbarui untuk Microsoft SharePoint. Untuk informasi selengkapnya, lihat Microsoft SharePoint.	2 Maret 2023

Fitur baru	Amazon Kendra sekarang mendukung versi terbaru dari konektor sumber data Confluence. Untuk informasi lebih lanjut, lihat Confluence.	1 Maret 2023
Perluasan wilayah	Amazon Kendra sekarang tersedia di Asia Pasifik (Tokyo) (ap-timur laut-1).	7 Februari 2023
Fitur baru	Amazon Kendra sekarang menyediakan konektor sumber data untuk Microsoft Exchange. Untuk informasi selengkapnya, lihat Microsoft Exchange.	Januari 12, 2023
Fitur baru	Amazon Kendra sekarang menyediakan konektor sumber data untuk Microsoft Yammer. Untuk informasi selengkapnya, lihat Microsoft Yammer.	Januari 12, 2023
Fitur baru	Amazon Kendra sekarang mendukung pengindek san jenis dokumen RTF, XML, XSLT, MS_EXCEL, CSV, JSON, dan MD. Untuk informasi selengkapnya, lihat Jenis dokumen.	11 Januari 2023
Fitur baru	Amazon Kendra sekarang mendukung versi terbaru dari konektor sumber Amazon S3 data. Untuk informasi selengkapnya, lihat Amazon S3.	10 Januari 2023

Fitur baru	OpenSearchHasil pencarian (dikelola sendiri) dapat diberi peringkat semantik menggunakan Amazon Kendra Intelligent Ranking.	Januari 9, 2023
Fitur baru	Amazon Kendra sekarang menyediakan konektor sumber data untuk Microsoft Teams. Untuk informasi selengkapnya, lihat Microsoft Teams.	5 Januari 2023
Fitur baru	Amazon Kendra memiliki konektor sumber data yang diperbarui untuk Google Drive. Untuk informasi selengkapnya, lihat Google Drive.	5 Januari 2023
Fitur baru	Amazon Kendra memiliki konektor sumber data yang diperbarui untuk ServiceNow. Untuk informasi lebih lanjut, lihat ServiceNow.	21 Desember 2022
Fitur baru	Amazon Kendra memiliki konektor sumber data yang diperbarui untuk Salesforce. Untuk informasi lebih lanjut, lihat Salesforce.	21 Desember 2022
Perluasan wilayah	Amazon Kendra sekarang tersedia di Asia Pasifik (Mumbai) (ap-selatan-1).	14 Desember 2022

Fitur baru	Amazon Kendrafitur pencarian tabular dapat mencari dan mengekstrak jawaban dari tabel yang disematkan dalam dokumen HTML.	27 November 2022
Fitur baru	Amazon Kendra mendukung pencarian semantik untuk satu set bahasa tertentu.	27 November 2022
Fitur baru	Amazon Kendra sekarang menyediakan konektor sumber data untuk Dropbox. Untuk informasi selengkapnya, lihat Dropbox.	September 27, 2022
Fitur baru	Amazon Kendra sekarang menyediakan konektor sumber data untuk Zendesk. Untuk informasi lebih lanjut, lihat Zendesk.	17 Agustus 2022
Fitur baru	Kontrol akses tingkat dokumen sekarang dapat dikonfigurasi ulang setelah Anda mengindeks dokumen Anda. Untuk informasi selengkapnya, lihat Konfigurasi kontrol akses.	14 Juli 2022
Fitur baru	Amazon Kendra sekarang menyediakan konektor sumber data untuk Alfresco. Untuk informasi lebih lanjut, lihat Alfresco.	30 Juni 2022

Fitur baru	Amazon Kendra sekarang menyediakan konektor sumber data untuk GitHub. Untuk informasi lebih lanjut, lihat GitHub.	2 Juni 2022
Fitur baru	Amazon Kendra sekarang menyediakan konektor sumber data untuk Jira. Untuk informasi lebih lanjut, lihat Jira.	12 Mei 2022
Fitur baru	Aspek bersarang dalam suatu segi dapat ditampilkan dalam hasil pencarian. Untuk informasi lebih lanjut, lihat Aspek.	Mei 5, 2022
Fitur baru	Amazon Kendra sekarang menyediakan konektor sumber data untuk Quip. Untuk informasi lebih lanjut, lihat Quip.	19 April 2022
Fitur baru	Amazon Kendra sekarang menyediakan konektor sumber data untuk Box. Untuk informasi selengkapnya, lihat Kotak.	April 6, 2022
Fitur baru	Amazon Kendra sekarang menyediakan konektor sumber data untuk Slack. Untuk informasi lebih lanjut, lihat Slack.	Maret 14, 2022

Fitur baru	Amazon Kendra sekarang menyediakan konektor sumber data untuk Amazon FSx. Untuk informasi selengkapnya, lihat Amazon FSx.	8 Februari 2022
AWS pembaruan kebijakan terkelola - Kebijakan baru	Amazon Kendra menambahkan kebijakan AWS terkelola baru. Untuk informasi selengkapnya, lihat Kebijakan AWS terkelola untuk Amazon Kendra.	Januari 3, 2022
Fitur baru	Amazon Kendra aplikasi pencarian dapat digunakan dalam beberapa klik tanpa perlu kode front-end apa pun. Untuk informasi selengkapnya, lihat Menerapkan aplikasi penelusuran tanpa kode.	1 Desember 2021
Fitur baru	Metadata dan konten dokumen dapat diperkaya selama proses konsumsi dokumen. Untuk informasi selengkapnya, lihat Menyesuaikan metadata dokumen selama proses konsumsi.	1 Desember 2021
Fitur baru	Amazon Kendra menawarkan analisis pencarian untuk mendapatkan wawasan yang berguna ke dalam aplikasi pencarian Anda. Untuk informasi selengkapnya, lihat Mendapatkan wawasan dengan analitik penelusuran.	1 Desember 2021

Perluasan wilayah	Amazon Kendra sekarang tersedia di AWS GovCloud (AS-Barat) (us-gov-west-1).	13 Oktober 2021
Fitur baru	Amazon Kendra sekarang dapat mengindeks dokumen dalam berbagai bahasa dan memfilter hasil pencarian berdasarkan bahasa. Lihat Menambahkan dokumen dalam bahasa selain bahasa Inggris dan Mencari dalam bahasa.	7 Oktober 2021
Fitur baru	Amazon Kendra sekarang terintegrasi dengan direktori Pusat Identitas untuk mengambil tingkat akses grup dan pengguna untuk pemfilter an konteks pengguna. Lihat Konfigurasi grup pengguna untuk Pusat Identitas IAM.	Oktober 6, 2021
Tutorial baru	Amazon Kendra sekarang menyediakan tutorial yang memandu Anda melalui cara membangun solusi pencarian yang diperkaya metadata. Lihat Membangun solusi pencarian cerdas.	13 Agustus 2021
Fitur baru	Amazon Kendra sekarang menyediakan konektor sumber data untuk Amazon WorkDocs. Untuk informasi selengkapnya, lihat Amazon WorkDocs.	20 Juli 2021

Fitur baru	Amazon Kendra sekarang menyediakan perayap web untuk merayapi dan mengindeks halaman web. Untuk informasi selengkapnya, lihat Web crawler.	17 Juni 2021
Perluasan wilayah	Amazon Kendra sekarang tersedia di Kanada (Tengah) (ca-central-1).	16 Juni 2021
Perluasan wilayah	Amazon Kendra sekarang tersedia di AS Timur (Ohio) (us-timur-2).	7 Juni 2021
Fitur baru	Amazon Kendra sekarang mendukung saran kueri, di mana pengguna disarankan kueri populer yang relevan dengan pencarian mereka. Untuk informasi selengkapnya, lihat Menyarankan kueri penelusuran populer.	27 Mei 2021
AWS pembaruan kebijakan terkelola - Kebijakan baru	Amazon Kendra menambahkan kebijakan AWS terkelola baru. Untuk informasi selengkapnya, lihat Kebijakan AWS terkelola untuk Amazon Kendra.	27 Mei 2021
Perluasan wilayah	Amazon Kendra sekarang tersedia di Asia Pasifik (Singapura) (ap-tenggara 1).	5 Mei 2021

Fitur baru	Amazon Kendra sekarang mendukung penyetelan relevansi pencarian dalam kueri dengan mengganti konfigurasi penyetelan yang ditetapkan pada tingkat indeks. Untuk informasi selengkapnya, lihat Penyetelan relevansi pencarian dan Respon penyetelan.	20 April 2021
Fitur baru	Amazon Kendra sekarang mendukung otentikasi OAuth 2.0 dan menggunakan ServiceNow kueri untuk memilih dokumen untuk pengindeksan. Untuk informasi lebih lanjut, lihat ServiceNow.	1 April 2021
Fitur baru	Amazon Kendra sekarang mendukung pembelajaran inkremental untuk dokumen FAQ. Untuk informasi selengkapnya, lihat Mengirimkan umpan balik untuk pembelajaran tambahan.	17 Februari 2021
Fitur baru	Amazon Kendra sekarang mendukung sinonim indeks. Untuk informasi selengkapnya, lihat Menambahkan sinonim ke indeks.	10 Desember 2020

Fitur baru	Amazon Kendra sekarang menyediakan konektor basis data untuk Google Workspace Drive. Untuk informasi selengkapnya, lihat Menggunakan sumber data Google Workspace Drive.	8 Desember 2020
Fitur baru	Amazon Kendra sekarang menyediakan JavaScrip t perpustakaan yang memudahkan Anda untuk memberikan umpan balik kueri Amazon Kendra. Untuk informasi selengkapnya, lihat Mengirimkan umpan balik.	8 Desember 2020
Fitur baru	Amazon Kendra sekarang mendukung kontrol akses pengguna berbasis token. Untuk informasi selengkap nya, lihat Mengontrol akses ke dokumen dalam indeks.	5 November 2020
Fitur baru	Konektor sumber data Amazon Kendra Confluenc e sekarang bekerja dengan cloud Confluence. Untuk informasi selengkapnya, lihat Menggunakan sumber data Confluence.	5 November 2020
Perluasan wilayah	Amazon Kendra sekarang tersedia di Asia Pasifik (Sydney) (ap-tenggara 2).	2 November 2020

Fitur baru	Amazon Kendra sekarang menyediakan konektor sumber data untuk server Confluence. Untuk informasi selengkapnya, lihat Menggunakan sumber data Confluence.	26 Oktober 2020
Fitur baru	Amazon Kendra sekarang menyediakan sumber data yang dapat Anda gunakan untuk menghasilkan statistik untuk konektor kustom Anda. Untuk informasi selengkapnya, lihat Menggunakan sumber data kustom.	21 Oktober 2020
Fitur baru	Amazon Kendra sekarang mendukung atribut khusus untuk pertanyaan yang sering diajukan. Untuk informasi selengkapnya, lihat Menambahkan pertanyaan dan jawaban.	17 September 2020
Fitur baru	Amazon Kendra sekarang mengembalikan skor kepercayaan untuk hasil kueri. Untuk informasi lebih lanjut, lihat QueryResultItem.	15 September 2020
Fitur baru	AWS CloudFormation sekarang mendukung Amazon Kendra. Untuk informasi selengkapnya, lihat referensi jenis Amazon Kendra sumber daya - AWS CloudFormation.	10 September 2020

Fitur baru	Amazon Kendra menambahkan dukungan untuk AWS PrivateLink. Untuk informasi selengkapnya, lihat Amazon Kendra dan antarmuka titik akhir VPC (). AWS PrivateLink	7 Juli 2020
Panduan baru	Panduan ini adalah perilisan pertama dari Panduan Developer Amazon Kendra .	11 Mei 2020

Referensi API

Dokumentasi referensi API sekarang menjadi panduan terpisah.

AWSGlosarium

Untuk AWS terminologi terbaru, lihat AWSglosarium di Referensi. Glosarium AWS

Terjemahan disediakan oleh mesin penerjemah. Jika konten terjemahan yang diberikan bertentangan dengan versi bahasa Inggris aslinya, utamakan versi bahasa Inggris.