aws

Guida per gli sviluppatori

Amazon Kendra

Amazon Kendra: Guida per gli sviluppatori

Table of Contents

Cos'è Amazon Kendra?

Amazon Kendraè un servizio di ricerca intelligente che utilizza l'elaborazione del linguaggio naturale e algoritmi avanzati di apprendimento automatico per restituire risposte specifiche alle domande di ricerca dai tuoi dati.

A differenza della tradizionale ricerca basata su parole chiave, Amazon Kendra utilizza le sue capacità di comprensione semantica e contestuale per decidere se un documento è pertinente a una query di ricerca. Fornisce risposte specifiche alle domande, offrendo agli utenti un'esperienza simile all'interazione con un esperto umano.

> **Note**
>
> Puoi anche utilizzare le funzionalità Amazon Kendra di ricerca semantica per riclassificare i risultati di un altro servizio di ricerca. Vedi Amazon KendraIntelligent Ranking per maggiori dettagli.

ConAmazon Kendra, puoi creare un'esperienza di ricerca unificata collegando più archivi di dati a un indice e inserendo e scansionando documenti. Puoi utilizzare i metadati dei tuoi documenti per creare un'esperienza di ricerca personalizzata e ricca di funzionalità per i tuoi utenti, aiutandoli a trovare in modo efficiente le risposte giuste alle loro domande.

Che cos'è Amazon Kendra?

Esecuzione di query Amazon Kendra

Puoi porre Amazon Kendra i seguenti tipi di domande:

Domande pratiche: semplici domande su chi, cosa, quando o dove, ad esempio dov'è il centro di assistenza più vicino a Seattle? Le domande sui fatti contengono risposte basate sui fatti che possono essere restituite come una singola parola o frase. La risposta viene recuperata da una FAQ o dai documenti indicizzati.

Domande descrittive: domande in cui la risposta può essere una frase, un passaggio o un intero documento. Ad esempio, come posso connettere il mio Echo Plus alla mia rete? Oppure, come posso ottenere agevolazioni fiscali per le famiglie a basso reddito?

Domande con parole chiave e linguaggio naturale: domande che includono contenuti complessi e colloquiali il cui significato potrebbe non essere chiaro. Ad esempio, discorso principale. Quando Amazon Kendra incontra una parola come «indirizzo», che ha più significati contestuali, deduce correttamente il significato alla base della query di ricerca e restituisce informazioni pertinenti.

Vantaggi di Amazon Kendra

Amazon Kendraè altamente scalabile, in grado di soddisfare le esigenze di prestazioni, è strettamente integrato con altri AWS servizi come Amazon S3e e offre una Amazon Lexsicurezza di livello aziendale. Alcuni dei vantaggi derivanti dall'utilizzo di Amazon Kendra sono:

Semplicità: Amazon Kendra fornisce una console e un'API per la gestione dei documenti da cercare. Puoi utilizzare una semplice API di ricerca per Amazon Kendra integrarla nelle tue applicazioni client, come siti Web o applicazioni mobili.

Connettività: Amazon Kendra può connettersi a archivi di dati o fonti di dati di terze parti come Microsoft. SharePoint Puoi indicizzare e cercare facilmente i tuoi documenti utilizzando la tua fonte di dati.

Precisione: a differenza dei servizi di ricerca tradizionali che utilizzano la ricerca per parole chiave, Amazon Kendra tenta di comprendere il contesto della domanda e restituisce la parola, il frammento o il documento più pertinente per la ricerca. Amazon Kendrautilizza l'apprendimento automatico per migliorare i risultati della ricerca nel tempo.

Sicurezza: Amazon Kendra offre un'esperienza di ricerca aziendale altamente sicura. I risultati della ricerca riflettono il modello di sicurezza della tua organizzazione e possono essere filtrati in base all'accesso di utenti o gruppi ai documenti. I clienti sono responsabili dell'autenticazione e dell'autorizzazione dell'accesso degli utenti.

Amazon KendraEdizioni

Amazon Kendraha due versioni: Developer Edition ed Enterprise Edition. La tabella seguente descrive le loro caratteristiche e le differenze tra i due.

Amazon KendraEdizione per sviluppatori	Amazon KendraEdizione Enterprise
Amazon KendraLa Developer Edition offre tutte le funzionalità di Amazon Kendra a un costo inferiore.	Amazon KendraEnterprise Edition offre tutte le funzionalità Amazon Kendra ed è progettata per i contesti di produzione.

Amazon KendraEdizione per sviluppatori	Amazon KendraEdizione Enterprise
Caso d'uso ideale • Scopri come Amazon Kendra indicizza i tuoi documenti • Prova delle funzionalità • Sviluppo di applicazioni che utilizzano Amazon Kendra Caratteristiche • Un piano gratuito con 750 ore di utilizzo incluse • Fino a 5 indici con un massimo di 5 fonti di dati ciascuno • 10.000 documenti o 3 GB di testo estratto • Circa 4.000 interrogazioni al giorno o 0,05 interrogazioni al secondo • Funziona in 1 zona di disponibilità (AZ): vedi Zone di disponibilità (data center nelle AWS regioni) Limitazioni • Non per applicazioni di produzione • Nessuna garanzia di latenza o disponibilità	Caso d'uso ideale • Indicizzazione dell'intera libreria di documenti aziendali • Implementazione dell'applicazione in un ambiente di produzione Caratteristiche • Fino a 5 indici con un massimo di 50 fonti di dati ciascuno • 100.000 documenti o 30 GB di testo estratto • Circa 8.000 interrogazioni al giorno o 0,1 query al secondo • Funziona in 3 zone di disponibilità (AZ): vedi Zone di disponibilità (data center nelle AWS regioni) **Note** Puoi aumentare questa quota utilizzan do la console Service Quotas. Limitazioni • Nessuno

Note

Per un elenco delle regioni, degli endpoint e delle quote di servizio supportate daAmazon Kendra, vedi Amazon Kendraendpoint e quote.

Prezzi di Amazon Kendra

Puoi iniziare gratuitamente con la Amazon Kendra Developer Edition che prevede un utilizzo fino a 750 ore per i primi 30 giorni.

Dopo la scadenza del periodo di prova, ti verranno addebitati tutti gli Amazon Kendra indici forniti, anche se sono vuoti e non viene eseguita alcuna query. Dopo la scadenza del periodo di prova, sono previsti costi aggiuntivi per la scansione e la sincronizzazione di documenti utilizzando le Amazon Kendra fonti di dati.

Per un elenco completo di costi e prezzi, consulta la sezione Amazon Kendraprezzi.

È il primo utilizzo di Amazon Kendra?

Se è la prima volta che utilizzi Amazon Kendra, ti consigliamo di leggere le seguenti sezioni in ordine:

1	2	3	4	5	6
Funzionamento di Amazon Kendra	Nozioni di base	Creazione di un indice	Aggiungere documenti direttamente a un indice con caricamento in batch	Creazione di un connettore di origine dati	Ricerca in un indice
Presenta i Amazon Kendra componenti e descrive come utilizzarli per creare una soluzione di ricerca.	Spiega come configurare il tuo account e testare l'API Amazon Kendra di ricerca.	Spiega come utilizzarlo Amazon Kendra per creare un indice di ricerca e aggiungere fonti di dati per sincronizzare i documenti.	Spiega come aggiungere documenti direttamente a un Amazon Kendra indice.	Spiega come aggiungere documenti dall'archivio dati a un Amazon Kendra indice.	Spiega come utilizzare l'API Amazon Kendra di ricerca per cercare in un indice.

Funzionamento di Amazon Kendra

Amazon Kendra fornisce funzionalità di ricerca all'applicazione. Indicizza i documenti direttamente o dal tuo archivio di documenti di terze parti e fornisce in modo intelligente le informazioni pertinenti agli utenti. È possibile utilizzarlo Amazon Kendra per creare un indice aggiornabile di documenti di vari tipi. Per un elenco dei tipi di documenti supportati da, Amazon Kendra vedere Tipi di documenti.

Amazon Kendra si integra con altri servizi. Ad esempio, puoi potenziare i Amazon Lex chat bot con la funzione di Amazon Kendra ricerca per fornire risposte utili alle domande degli utenti. Puoi usare un Amazon Simple Storage Service bucket come fonte di dati per Amazon Kendra connetterti e indicizzare i tuoi documenti. Inoltre, puoi configurare politiche di accesso o autorizzazioni per le risorse che utilizzano. AWS Identity and Access Management

Amazon Kendra ha i seguenti componenti:

- Un indice che contiene i documenti e li rende ricercabili.
- Una fonte di dati che archivia i tuoi documenti e a cui Amazon Kendra si connette. Puoi sincronizzare automaticamente un'origine dati con un Amazon Kendra indice in modo che l'indice rimanga aggiornato con l'archivio di origine.
- Un'API per l'aggiunta di documenti che aggiunge documenti direttamente a un indice.

È possibile Amazon Kendra utilizzarla tramite la console o l'API. Puoi creare, aggiornare ed eliminare gli indici. L'eliminazione di un indice comporta l'eliminazione di tutti i relativi connettori di origine dati e l'eliminazione definitiva di tutte le informazioni relative al documento. Amazon Kendra

Argomenti

- Indice
- Documenti
- Origini dati
- Query
- Tag

Indice

Un indice contiene il contenuto dei documenti ed è strutturato in modo da renderli ricercabili. Il modo in cui si aggiungono documenti all'indice dipende da come vengono archiviati i documenti.

- Se si archiviano i documenti in un tipo di archivio, ad esempio un Amazon S3 bucket o un SharePoint sito Microsoft, si utilizza un connettore di origine dati per indicizzare i documenti dal repository.
- Se non archivi i documenti in un repository, utilizzi l'BatchPutDocumentAPI per indicizzarli direttamente.
- Per le domande e le risposte alle FAQ, che devono essere archiviate in un bucket Amazon Kendra (Amazon S3), le carichi dal bucket

Puoi creare indici con la Amazon Kendra console, il AWS CLI o un SDK. AWS Per informazioni sui tipi di documenti che possono essere indicizzati, consulta Tipi di documento.

Utilizzo di campi di Amazon Kendra documento riservati o comuni

Con l'UpdateIndex API, è possibile creare campi riservati o comuni utilizzando `DocumentMetadataConfigurationUpdates` e specificando il nome del campo indice Amazon Kendra riservato da mappare all'attributo/nome di campo equivalente del documento. Puoi anche creare campi personalizzati. Se utilizzi un connettore di origine dati, la maggior parte include mappature di campi che mappano i campi del documento di origine dati ai campi Amazon Kendra indice. Se utilizzi la console, aggiorni i campi selezionando l'origine dati, selezionando l'azione di modifica e quindi procedendo accanto alla sezione delle mappature dei campi per configurare l'origine dati.

Puoi configurare l'`Search`oggetto per impostare un campo come visualizzabile, personalizzabile, ricercabile e ordinabile. È possibile configurare l'`Relevance`oggetto per impostare l'ordine di classificazione, la durata dell'aumento o il periodo di tempo di un campo da applicare a boosting, freshness, value di importanza e valori di importanza mappati a valori di campo specifici. Se utilizzi la console, puoi configurare le impostazioni di ricerca per un campo selezionando l'opzione facet nel menu di navigazione. Per impostare l'ottimizzazione della pertinenza, seleziona l'opzione di ricerca nell'indice nel menu di navigazione, inserisci una query e utilizza le opzioni del pannello laterale per ottimizzare la pertinenza della ricerca. Non è possibile modificare il tipo di campo dopo averlo creato.

Amazon Kendra contiene i seguenti campi di documento riservati o comuni che è possibile utilizzare:

- `_authors`—Un elenco di uno o più autori responsabili del contenuto del documento.
- `_category`—Una categoria che colloca un documento in un gruppo specifico.
- `_created_at`—La data e l'ora in formato ISO 8601 in cui è stato creato il documento. Ad esempio, 2012-03-25T12:30:10+01:00 è il formato data/ora ISO 8601 per il 25 marzo 2012 alle 12:30 (più 10 secondi) nel fuso orario dell'Europa centrale (CET).
- `_data_source_id`—L'identificatore della fonte di dati che contiene il documento.
- `_document_body`—Il contenuto del documento.
- `_document_id`—Un identificatore univoco per il documento.
- `_document_title`—Il titolo del documento.
- `_excerpt_page_number`—Il numero di pagina in un file PDF in cui viene visualizzato l'estratto del documento. Se l'indice è stato creato prima dell'8 settembre 2020, è necessario reindicizzare i documenti prima di poter utilizzare questo attributo.
- `_faq_id`—Se si tratta di un documento di tipo domanda-risposta (FAQ), un identificatore univoco per le domande frequenti.
- `_file_type`—Il tipo di file del documento, ad esempio pdf o doc.
- `_last_updated_at`—La data e l'ora in formato ISO 8601 dell'ultimo aggiornamento del documento. Ad esempio, 2012-03-25T12:30:10+01:00 è il formato data/ora ISO 8601 per il 25 marzo 2012 alle 12:30 (più 10 secondi) nel fuso orario dell'Europa centrale (CET).
- `_source_uri`—L'URI in cui è disponibile il documento. Ad esempio, l'URI del documento sul sito Web di un'azienda.
- `_version`—Un identificatore per la versione specifica di un documento.
- `_view_count`—Il numero di volte in cui il documento è stato visualizzato.
- `_language_code`(String) —Il codice per una lingua che si applica al documento. Il valore predefinito è l'inglese se non si specifica una lingua. Per ulteriori informazioni sulle lingue supportate, compresi i relativi codici, consulta Aggiungere documenti in lingue diverse dall'inglese.

Per i campi personalizzati, puoi creare questi campi utilizzando `DocumentMetadataConfigurationUpdates` l'`UpdateIndex`API, proprio come quando crei un campo riservato o comune. È necessario impostare il tipo di dati appropriato per il campo personalizzato. Se utilizzi la console, aggiorni i campi selezionando l'origine dati, selezionando l'azione di modifica e quindi procedendo accanto alla sezione delle mappature dei campi per configurare l'origine dati. Alcune fonti di dati non supportano l'aggiunta di nuovi campi o campi personalizzati. Non è possibile modificare il tipo di campo dopo averlo creato.

Di seguito sono riportati i tipi che è possibile impostare per i campi personalizzati:

- Data
- Numero
- Stringa
- Elenco stringhe

Se hai aggiunto documenti all'indice utilizzando l'BatchPutDocumentAPI, `Attributes` elenca i campi/gli attributi dei tuoi documenti e crei campi utilizzando l'oggetto. `DocumentAttribute`

Per i documenti indicizzati da un'origine Amazon S3 dati, crei campi utilizzando un file di metadati JSON che include le informazioni sui campi.

Se utilizzi un database supportato come fonte di dati, puoi configurare i campi utilizzando l'opzione di mappatura dei campi.

Ricerca negli indici

Dopo aver creato un indice, puoi iniziare a cercare i tuoi documenti. Per ulteriori informazioni, vedere Ricerca negli indici.

Documenti

Questa sezione spiega come Amazon Kendra indicizza i numerosi formati di documenti supportati e i diversi campi/attributi dei documenti.

Argomenti

- Tipi o formati di documenti
- Attributi o campi del documento

Tipi o formati di documenti

Amazon Kendra supporta i tipi o i formati di documenti più diffusi come PDF, HTML PowerPoint, Word e altri. Un indice può contenere più formati di documenti.

Amazon Kendra estrae il contenuto all'interno dei documenti per renderli ricercabili. I documenti vengono analizzati in modo da ottimizzare la ricerca sul testo estratto e su qualsiasi contenuto

tabulare (tabelle HTML) all'interno dei documenti. Ciò significa strutturare i documenti in campi o attributi utilizzati per la ricerca. I metadati del documento, come la data dell'ultima modifica, possono essere campi utili per la ricerca.

I documenti possono essere organizzati in righe e colonne. Ad esempio, ogni documento è una riga e ogni campo/attributo del documento, come il titolo e il contenuto del corpo, è una colonna. Ad esempio, se si utilizza un database come fonte di dati, i dati devono essere strutturati o organizzati in righe e colonne.

Puoi aggiungere documenti all'indice nei seguenti modi:

- API BatchPutDocument
- Connettore di origine dati

Se desideri aggiungere un file di domande frequenti, utilizzi l'CreateFaqAPI per aggiungere il file archiviato in un Amazon S3 bucket. Puoi scegliere tra un formato CSV di base, un formato CSV che include campi/attributi personalizzati in un'intestazione e un formato JSON che include campi personalizzati. Il formato predefinito è CSV di base.

Di seguito vengono fornite informazioni su ogni formato di documento supportato e su come viene Amazon Kendra trattato ogni formato durante l'indicizzazione dei documenti.

Formato del documento	Trattata come	Come viene trattato il documento	Struttura originale
Formato di documento portatile (PDF)	HTML	Convertito in HTML, quindi il contenuto viene estratto.	Non strutturato
HyperText Linguaggio di markup (HTML)	HTML	I tag HTML vengono filtrati per estrarre il contenuto. Il contenuto deve essere compreso tra i tag di `HTML` inizio e di chiusura principali (`<HTML>content</HTML>`).	Semistrutturato

Formato del documento	Trattata come	Come viene trattato il documento	Struttura originale
Extensible Markup Language (XML)	XML	I tag XML vengono filtrati per estrarre il contenuto.	Semistrutturato
Trasformazione del linguaggio XSLT (Extensible Stylesheet Language Transformation)	XSLT	I tag vengono filtrati per estrarre il contenuto.	Semistrutturato
MarkDown (MD)	Testo semplice	Il contenuto viene estratto con la MarkDown sintassi inclusa.	Semistrutturato
Comma Separated Values (CSV)	CSV	Contenuto estratto da ogni cella, con un singolo file trattato come risultato di un unico documento.	Strutturato per i file delle domande frequenti, altrimenti semistrutturato
Microsoft Excel (XLS e XLSX)	XLS e XLSX	Contenuto estratto da ogni cella, con un singolo file trattato come risultato di un unico documento.	Semi-strutturato
JavaScript Notazione di oggetti (JSON)	Testo semplice	Il contenuto viene estratto con la sintassi JSON inclusa.	Semistrutturato
Formato RTF (RTF)	RTF	La sintassi RTF viene filtrata per estrarre il contenuto.	Semistrutturato

Formato del documento	Trattata come	Come viene trattato il documento	Struttura originale
Microsoft PowerPoint (PPT)	PPT	Solo il contenuto testuale viene estratto dalle PowerPoint diapositive per la ricerca. Le immagini e gli altri contenuti non vengono estratti.	Non strutturato
Microsoft Word (DOCX)	DOCX	Solo il contenuto testuale viene estratto dalle pagine di Word per la ricerca. Le immagini e gli altri contenuti non vengono estratti.	Non strutturato
Testo semplice (TXT)	TXT	Tutto il testo del documento di testo viene estratto.	Non strutturato

Attributi o campi del documento

A un documento sono associati attributi o campi. I campi di un documento sono le proprietà di un documento o ciò che è contenuto nella struttura di un documento. Ad esempio, ogni documento potrebbe contenere titolo, corpo del testo e autore. Puoi anche aggiungere campi personalizzati per documenti specifici. Ad esempio, se nell'indice vengono ricercate documenti fiscali, è possibile specificare un campo personalizzato per il tipo di documento fiscale, ad esempio W-2, 1099 e così via.

Prima di poter utilizzare un campo di documento in una query, è necessario mapparlo a un campo indice. Ad esempio, il campo del titolo può essere mappato al campo. `_document_title` Per ulteriori informazioni, vedere Mappatura dei campi. Per aggiungere un nuovo campo, devi creare un campo indice a cui mappare il campo. I campi indice vengono creati utilizzando la console o l'UpdateIndexAPI.

Puoi utilizzare i campi del documento per filtrare le risposte e creare risultati di ricerca sfaccettati. Ad esempio, puoi filtrare una risposta per restituire solo una versione specifica di un documento oppure puoi filtrare le ricerche per restituire solo 1099 tipi di documenti fiscali che corrispondono al termine di ricerca. Per ulteriori informazioni, consulta Filtraggio e ricerca sfaccettata.

È inoltre possibile utilizzare i campi del documento per ottimizzare manualmente la risposta alla query. Ad esempio, puoi scegliere di aumentare l'importanza del campo del titolo per aumentare il peso che viene Amazon Kendra assegnato al campo nel determinare quali documenti restituire nella risposta. Per ulteriori informazioni, consulta Ottimizzazione della pertinenza della ricerca.

Se aggiungete un documento direttamente a un indice, specificate i campi nel parametro di input del documento all'BatchPutDocumentAPI. Si specificano i valori dei campi personalizzati in una matrice di DocumentAttributeoggetti. Se si utilizza un'origine dati, il metodo utilizzato per aggiungere i campi del documento dipende dall'origine dati. Per ulteriori informazioni, consulta la sezione Mappatura dei campi di origine dei dati.

Utilizzo di campi di documento Amazon Kendra riservati o comuni

Con l'UpdateIndex API, è possibile creare campi riservati o comuni utilizzando `DocumentMetadataConfigurationUpdates` e specificando il nome del campo indice Amazon Kendra riservato da mappare all'attributo/nome di campo equivalente del documento. Puoi anche creare campi personalizzati. Se utilizzi un connettore di origine dati, la maggior parte include mappature di campi che mappano i campi del documento di origine dati ai campi Amazon Kendra indice. Se utilizzi la console, aggiorni i campi selezionando l'origine dati, selezionando l'azione di modifica e quindi procedendo accanto alla sezione delle mappature dei campi per configurare l'origine dati.

Puoi configurare l'`Search`oggetto per impostare un campo come visualizzabile, personalizzabile, ricercabile e ordinabile. È possibile configurare l'`Relevance`oggetto per impostare l'ordine di classificazione, la durata dell'aumento o il periodo di tempo di un campo da applicare a boosting, freshness, value di importanza e valori di importanza mappati a valori di campo specifici. Se utilizzi la console, puoi configurare le impostazioni di ricerca per un campo selezionando l'opzione facet nel menu di navigazione. Per impostare l'ottimizzazione della pertinenza, seleziona l'opzione di ricerca nell'indice nel menu di navigazione, inserisci una query e utilizza le opzioni del pannello laterale per ottimizzare la pertinenza della ricerca. Non è possibile modificare il tipo di campo dopo averlo creato.

Amazon Kendra contiene i seguenti campi di documento riservati o comuni che è possibile utilizzare:

- `_authors`—Un elenco di uno o più autori responsabili del contenuto del documento.

- `_category`—Una categoria che colloca un documento in un gruppo specifico.
- `_created_at`—La data e l'ora in formato ISO 8601 in cui è stato creato il documento. Ad esempio, 2012-03-25T12:30:10+01:00 è il formato data/ora ISO 8601 per il 25 marzo 2012 alle 12:30 (più 10 secondi) nel fuso orario dell'Europa centrale (CET).
- `_data_source_id`—L'identificatore della fonte di dati che contiene il documento.
- `_document_body`—Il contenuto del documento.
- `_document_id`—Un identificatore univoco per il documento.
- `_document_title`—Il titolo del documento.
- `_excerpt_page_number`—Il numero di pagina in un file PDF in cui viene visualizzato l'estratto del documento. Se l'indice è stato creato prima dell'8 settembre 2020, è necessario reindicizzare i documenti prima di poter utilizzare questo attributo.
- `_faq_id`—Se si tratta di un documento di tipo domanda-risposta (FAQ), un identificatore univoco per le domande frequenti.
- `_file_type`—Il tipo di file del documento, ad esempio pdf o doc.
- `_last_updated_at`—La data e l'ora in formato ISO 8601 dell'ultimo aggiornamento del documento. Ad esempio, 2012-03-25T12:30:10+01:00 è il formato data/ora ISO 8601 per il 25 marzo 2012 alle 12:30 (più 10 secondi) nel fuso orario dell'Europa centrale (CET).
- `_source_uri`—L'URI in cui è disponibile il documento. Ad esempio, l'URI del documento sul sito Web di un'azienda.
- `_version`—Un identificatore per la versione specifica di un documento.
- `_view_count`—Il numero di volte in cui il documento è stato visualizzato.
- `_language_code`(String) —Il codice per una lingua che si applica al documento. Il valore predefinito è l'inglese se non si specifica una lingua. Per ulteriori informazioni sulle lingue supportate, compresi i relativi codici, consulta Aggiungere documenti in lingue diverse dall'inglese.

Per i campi personalizzati, puoi creare questi campi utilizzando `DocumentMetadataConfigurationUpdates` l'`UpdateIndex`API, proprio come quando crei un campo riservato o comune. È necessario impostare il tipo di dati appropriato per il campo personalizzato. Se utilizzi la console, aggiorni i campi selezionando l'origine dati, selezionando l'azione di modifica e quindi procedendo accanto alla sezione delle mappature dei campi per configurare l'origine dati. Alcune fonti di dati non supportano l'aggiunta di nuovi campi o campi personalizzati. Non è possibile modificare il tipo di campo dopo averlo creato.

Di seguito sono riportati i tipi che è possibile impostare per i campi personalizzati:

- Data
- Numero
- Stringa
- Elenco stringhe

Se hai aggiunto documenti all'indice utilizzando l'BatchPutDocumentAPI, `Attributes` elenca i campi/gli attributi dei tuoi documenti e crei campi utilizzando l'oggetto. `DocumentAttribute`

Per i documenti indicizzati da un'origine Amazon S3 dati, crei campi utilizzando un file di metadati JSON che include le informazioni sui campi.

Se utilizzi un database supportato come fonte di dati, puoi configurare i campi utilizzando l'opzione di mappatura dei campi.

Origini dati

Un'origine dati è un archivio o una posizione di dati che Amazon Kendra si connette ai documenti o ai contenuti e li indicizza. Ad esempio, è possibile configurare la connessione Amazon Kendra a Microsoft per SharePoint eseguire la scansione e l'indicizzazione dei documenti archiviati in questa fonte. Puoi anche indicizzare le pagine Web fornendo gli URL Amazon Kendra per la scansione. È possibile sincronizzare automaticamente un'origine dati con un Amazon Kendra indice in modo che i documenti aggiunti, aggiornati o eliminati nell'origine dati vengano aggiunti, aggiornati o eliminati anche nell'indice.

Le fonti di dati supportate sono:

- Adobe Experience Manager
- Alfresco
- Aurora (MySQL)
- Aurora (PostgreSQL)
- Amazon FSx (Windows)
- Amazon FSx (NetApp SU TAP)
- Fonti di dati del database
- Amazon RDS (Microsoft SQL Server)
- Amazon RDS (MySQL)

- Amazon RDS (Oracle)
- Amazon RDS (PostgreSQL)
- Amazon S3 secchi
- Amazon Kendra Web crawler
- Amazon WorkDocs
- Box (Cubo)
- Confluenza
- Fonti di dati personalizzate
- Dropbox
- Drupal
- GitHub
- Gmail
- Unità Google Workspace
- IBM DB2
- Jira
- Microsoft Exchange
- Microsoft OneDrive
- Microsoft SharePoint
- Microsoft Teams
- Microsoft SQL Server
- Microsoft Yammer
- MySQL
- Banca dati Oracle
- PostgreSQL
- battuta
- Salesforce
- ServiceNow
- Slack
- Zendesk

Per un elenco dei tipi o dei formati di documento supportati da, Amazon Kendra vedi Tipi di documento. È necessario creare un indice prima di creare un connettore di origine dati per indicizzare i documenti dalla fonte dati.

> **Note**
>
> Per creare un indice di documenti, non è necessario utilizzare una fonte di dati. Puoi aggiungere documenti direttamente a un indice con il caricamento in batch. Per ulteriori informazioni, consulta Aggiungere documenti direttamente a un indice.

Per una procedura dettagliata sull'uso della Amazon Kendra console, della AWS CLI o degli SDK, consulta Guida introduttiva.

Query

Per ottenere risposte, gli utenti eseguono una query su un indice. Gli utenti possono utilizzare il linguaggio naturale nelle loro interrogazioni. La risposta contiene informazioni, come il titolo, un estratto di testo e la posizione dei documenti nell'indice che forniscono la risposta migliore.

Amazon Kendra utilizza tutte le informazioni fornite sui documenti, non solo il contenuto dei documenti, per determinare se un documento è pertinente alla query. Ad esempio, se l'indice contiene informazioni su quando i documenti sono stati aggiornati l'ultima volta, è possibile Amazon Kendra assegnare una maggiore rilevanza ai documenti che sono stati aggiornati più di recente.

Una query può anche contenere criteri su come filtrare la risposta in modo da Amazon Kendra restituire solo i documenti che soddisfano i criteri di filtro. Ad esempio, se è stato creato un campo indice denominato dipartimento, è possibile filtrare la risposta in modo che vengano restituiti solo i documenti con il campo reparto impostato su legale. Per ulteriori informazioni, vedere Filtraggio della ricerca.

È possibile influenzare i risultati di una query regolando la pertinenza dei singoli campi dell'indice. L'ottimizzazione modifica l'importanza di un campo nei risultati. Ad esempio, se si aumenta l'importanza dei documenti inserendo la nuova categoria, è più probabile che i documenti con questa categoria vengano inclusi nella risposta. Per ulteriori informazioni, consulta Ottimizzazione della pertinenza della ricerca.

Per ulteriori informazioni sull'utilizzo delle query, vedere Ricerca in un indice.

Tag

Gestisci gli indici, le fonti di dati e le domande frequenti assegnando tag o etichette. Puoi utilizzare i tag per classificare le tue Amazon Kendra risorse in vari modi. Ad esempio, per scopo, proprietario, applicazione o qualsiasi combinazione. Ogni tag consiste di una chiave e di un valore, entrambi personalizzabili.

I tag ti aiutano a:

- Identifica e organizza AWS le tue risorse. Molti AWS servizi supportano l'etichettatura, quindi puoi assegnare lo stesso tag a risorse di servizi diversi per indicare che le risorse sono correlate. Ad esempio, puoi etichettare un indice e il Amazon Lex bot che utilizza l'indice con lo stesso tag.
- Assegnare i costi. Puoi attivare i tag nella AWS Billing and Cost Management dashboard. AWS utilizza i tag per classificare i costi e fornirti un rapporto mensile sull'allocazione dei costi. Per ulteriori informazioni, consulta Allocazione dei costi e etichettatura in Informazioni su AWS Billing and Cost Management.
- Controllare l'accesso alle risorse. Puoi utilizzare i tag nelle politiche AWS Identity and Access Management (IAM) che controllano l'accesso alle risorse. Amazon Kendra Puoi associare queste politiche a un IAM ruolo o a un utente per attivare il controllo degli accessi basato su tag. Per ulteriori informazioni, consulta Autorizzazione basata sui tag.

Puoi creare e gestire i tag utilizzando AWS Management Console, the AWS Command Line Interface (AWS CLI) o l' Amazon Kendra API.

Assegnazione di tag alle risorse

Se utilizzi la Amazon Kendra console, puoi taggare le risorse quando le crei o aggiungerle in un secondo momento. Puoi anche utilizzare la console per aggiornare o rimuovere i tag.

Se utilizzi AWS Command Line Interface (AWS CLI) o l' Amazon Kendra API, utilizza le seguenti operazioni per gestire i tag per le tue risorse:

- CreateDataSource—Applica i tag quando crei un'origine dati.
- CreateFaq—Applica i tag quando crei una FAQ.
- CreateIndex—Applica tag quando crei un indice.
- ListTagsForResource—Visualizza i tag associati a una risorsa.
- TagResource—Aggiunge e modifica i tag per una risorsa.

- UntagResource—Rimuove i tag da una risorsa.

Limitazioni applicate ai tag

Le seguenti restrizioni si applicano ai tag sulle Amazon Kendra risorse:

- Numero massimo di tag: 50
- Lunghezza massima della chiave: 128 caratteri
- Lunghezza massima del valore: 256 caratteri
- Caratteri validi per chiave e valore—a—z, A—Z, spazio e i seguenti caratteri: _.:/= + - e @
- Per chiavi e valori viene fatta distinzione tra maiuscole e minuscole
- Non utilizzare `aws:` come prefisso per le chiavi; l'utilizzo di questo prefisso è esclusivo di AWS

Configurazione di Amazon Kendra

Prima di utilizzare Amazon Kendra, devi disporre di un account Amazon Web Services AWS (). Dopo aver creato un AWS account, puoi accedere ad Amazon Kendra tramite la console Amazon Kendra, AWS Command Line Interface il () o gli SDK. AWS CLI AWS

Questa guida include esempi per AWS CLI Java e Python.

Argomenti

Iscriviti per AWS

Quando ti registri ad Amazon Web Services (AWS), il tuo account viene automaticamente registrato per tutti i servizi in AWS, incluso Amazon Kendra. Ti vengono addebitati solo i servizi che utilizzi.

Se hai già un AWS account, passa all'attività successiva. Se non disponi di un account AWS , utilizza la seguente procedura per crearne uno.

Per iscriverti a AWS

1. Apri https://aws.amazon.com, quindi scegli Crea un AWS account.
2. Seguire le istruzioni visualizzate sullo schermo per completare la creazione dell'account. Annota il tuo numero di AWS conto a 12 cifre. Come parte della procedura di registrazione si riceverà una telefonata, durante la quale si dovrà inserire un PIN usando la tastiera del telefono.
3. Crea un utente amministratore AWS Identity and Access Management (IAM). Per le istruzioni, consultare l'articolo Creazione del primo utente e del primo gruppo di IAM nella Guida per l'utente di AWS Identity and Access Management .

Regioni ed endpoint

Un endpoint è un URL che rappresenta il punto di partenza per un servizio Web. Ogni endpoint è associato a una AWS regione specifica. Se utilizzi una combinazione della console Amazon Kendra,

AWS CLI degli SDK Amazon Kendra e di Amazon Kendra, presta attenzione alle relative regioni predefinite poiché tutti i componenti Amazon Kendra di una determinata campagna (indice, query, ecc.) devono essere creati nella stessa regione. Per le regioni e gli endpoint supportati da Amazon Kendra, consulta Regioni ed endpoint.

Configurazione del AWS CLI

La AWS Command Line Interface (AWS CLI) è uno strumento di sviluppo unificato per la gestione di AWS servizi, tra cui Amazon Kendra. Consigliamo di installarla.

1. Per installare AWS CLI, segui le istruzioni riportate in Installazione dell'interfaccia a riga di AWS comando nella Guida per l'utente dell'interfaccia a riga di AWS comando.
2. Per configurare AWS CLI e impostare un profilo a cui richiamare AWS CLI, segui le istruzioni riportate nella Guida per l'utente della Configurazione dell'interfaccia AWS CLI a riga di AWS comando.
3. Per confermare che il AWS CLI profilo è configurato correttamente, esegui il seguente comando:

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

   Se il profilo è stato configurato correttamente, viene visualizzato un output simile al seguente:

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

4. Per verificare che AWS CLI sia configurato per l'uso con Amazon Kendra, esegui i seguenti comandi:

   ```
   aws kendra help
   ```

   Se AWS CLI è configurato correttamente, verrà visualizzato un elenco dei AWS CLI comandi supportati per Amazon Kendra, Amazon Kendra runtime e Amazon Kendra events.

AWS Configurazione degli SDK

Scarica e installa gli AWS SDK che desideri utilizzare. Questa guida fornisce esempi per Python. Per informazioni su altri AWS SDK, consulta Tools for Amazon Web Services.

Il pacchetto per Python SDK si chiama Boto3.

Prima di eseguire i seguenti comandi Python, devi prima scaricare e installare Python 3.6 o versione successiva per il tuo sistema operativo. Il supporto per Python 3.5 e versioni precedenti è obsoleto. Se non hai pip incluso nella tua directory Python Scripts, puoi scaricare get-pip.py e memorizzarlo nella tua directory Scripts. Puoi anche impostare la tua directory Python come Path o variabile di ambiente usando un programma terminale.

```
# 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
```

Per utilizzare Boto3, devi configurare le credenziali di autenticazione per il tuo AWS account utilizzando la console IAM.

IAM ruoli di accesso per Amazon Kendra

Quando si crea un indice, una fonte di dati o una FAQ, è Amazon Kendra necessario accedere alle AWS risorse necessarie per creare la Amazon Kendra risorsa. È necessario creare una politica AWS Identity and Access Management (IAM) prima di creare la Amazon Kendra risorsa. Quando chiami l'operazione, fornisci l'Amazon Resource Name (ARN) del ruolo con la policy allegata. Ad esempio, se stai chiamando l'BatchPutDocumentAPI per aggiungere documenti da un Amazon S3 bucket, fornisci un ruolo Amazon Kendra con una policy che ha accesso al bucket.

Puoi creare un nuovo IAM ruolo nella Amazon Kendra console o scegliere un ruolo IAM esistente da utilizzare. La console mostra i ruoli che hanno la stringa «kendra» o «Kendra» nel nome del ruolo.

I seguenti argomenti forniscono dettagli sulle politiche richieste. Se IAM crei ruoli utilizzando la Amazon Kendra console, queste politiche vengono create automaticamente.

Argomenti

IAM ruoli per gli indici

Quando si crea un indice, è necessario fornire a un IAM ruolo il permesso di scrivere a un. Amazon CloudWatch È inoltre necessario fornire una politica di fiducia che Amazon Kendra consenta di assumere il ruolo. Di seguito sono riportate le politiche che devono essere fornite.

IAM ruoli per gli indici

Una politica di ruolo per consentire l'accesso Amazon Kendra a un CloudWatch registro.

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

Una politica di ruolo per consentire l' Amazon Kendra accesso AWS Secrets Manager. Se si utilizza il contesto utente con Secrets Manager come posizione chiave, è possibile utilizzare la seguente politica.

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

Una politica di fiducia Amazon Kendra per consentire di assumere un ruolo.

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

IAM ruoli per l' BatchPutDocumentAPI

> **Warning**
>
> Amazon Kendra non utilizza una policy bucket che concede le autorizzazioni a un Amazon Kendra principale per interagire con un bucket S3. Utilizza invece i ruoli. IAM Assicurati che Amazon Kendra non sia incluso come membro fidato nella tua bucket policy per evitare problemi di sicurezza dei dati derivanti dalla concessione accidentale di autorizzazioni a responsabili arbitrari. Tuttavia, puoi aggiungere una policy sui bucket per utilizzare un bucket su account diversi. Amazon S3 Per ulteriori informazioni, consulta Politiche da utilizzare Amazon S3 su più account. Per informazioni sui IAM ruoli per le fonti di dati S3, consulta IAM ruoli.

Quando utilizzi l'BatchPutDocumentAPI per indicizzare i documenti in un Amazon S3 bucket, devi fornire un IAM ruolo Amazon Kendra con accesso al bucket. È inoltre necessario fornire una politica di fiducia che Amazon Kendra consenta di assumere il ruolo. Se i documenti nel bucket sono crittografati, è necessario fornire l'autorizzazione a utilizzare la chiave master del AWS KMS cliente (CMK) per decrittografare i documenti.

IAM ruoli per l'API BatchPutDocument

Una politica di ruolo richiesta per consentire l'accesso Amazon Kendra a un Amazon S3 bucket.

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

Una politica di fiducia per consentire Amazon Kendra di assumere un ruolo.

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

Si consiglia di includere `aws:sourceAccount` e `aws:sourceArn` nella politica di fiducia. Ciò limita le autorizzazioni e verifica in modo sicuro se `aws:sourceAccount` e `aws:sourceArn` sono le stesse fornite nella politica di IAM ruolo per l'azione`sts:AssumeRole`. Ciò impedisce alle entità non autorizzate di accedere ai tuoi IAM ruoli e alle loro autorizzazioni. Per ulteriori informazioni, consulta la AWS Identity and Access Management guida sul problema del vice confuso.

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

```
    ]
}
```

Una politica di ruolo opzionale che consente di Amazon Kendra utilizzare una chiave master AWS KMS del cliente (CMK) per decrittografare i documenti in un 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 ruoli per le fonti di dati

Quando utilizzi l'CreateDataSourceAPI, devi assegnare a Amazon Kendra un IAM ruolo che disponga dell'autorizzazione ad accedere alle risorse. Le autorizzazioni specifiche richieste dipendono dall'origine dei dati.

IAM ruoli per le fonti di dati di Adobe Experience Manager

Quando utilizzi Adobe Experience Manager, fornisci un ruolo con le seguenti politiche.

- Autorizzazione ad accedere al tuo AWS Secrets Manager segreto per autenticare Adobe Experience Manager.
- Autorizzazione a chiamare le API pubbliche richieste per il connettore Adobe Experience Manager.
- Autorizzazione a chiamare le `BatchPutDocument`,`BatchDeleteDocument`,`PutPrincipalMapping`, `DeletePrincipalMapping`,`DescribePrincipalMapping`, e le `ListGroupsOlderThanOrderingId` API.

> **Note**
>
> Puoi connettere un'origine dati di Adobe Experience Manager a Amazon Kendra through Amazon VPC. Se utilizzi un Amazon VPC, devi aggiungere autorizzazioni aggiuntive.

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

Una politica di fiducia per consentire Amazon Kendra di assumere un ruolo.

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

IAM ruoli per le fonti di dati Alfresco

Quando utilizzi Alfresco, fornisci un ruolo con le seguenti politiche.

- Autorizzazione ad accedere al tuo AWS Secrets Manager segreto per autenticare Alfresco.
- Autorizzazione a chiamare le API pubbliche richieste per il connettore Alfresco.
- Autorizzazione a chiamare le`BatchPutDocument`,`BatchDeleteDocument`,`PutPrincipalMapping`, `DeletePrincipalMappingDescribePrincipalMapping`, e `ListGroupsOlderThanOrderingId` API.

> **Note**
>
> È possibile connettere un'origine dati Alfresco a Amazon Kendra Amazon VPC Se si utilizza un Amazon VPC, è necessario aggiungere autorizzazioni aggiuntive.

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

Una politica di fiducia per consentire Amazon Kendra di assumere un ruolo.

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

IAM ruoli per sorgenti dati Aurora (MySQL)

Quando si utilizza Aurora (MySQL), si fornisce un ruolo con le seguenti politiche.

- Autorizzazione ad accedere al tuo AWS Secrets Manager segreto per autenticare il tuo Aurora (MySQL).
- Autorizzazione a chiamare le API pubbliche richieste per il connettore Aurora (MySQL).
- Autorizzazione a chiamare le`BatchPutDocument`,`BatchDeleteDocument`, `PutPrincipalMapping` `DeletePrincipalMappingDescribePrincipalMapping`, e API. `ListGroupsOlderThanOrderingId`

> **Note**
>
> È possibile connettere un' Aurora origine dati (MySQL) a through. Amazon Kendra Amazon VPC Se si utilizza un Amazon VPC, è necessario aggiungere autorizzazioni aggiuntive.

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

Una politica di fiducia per consentire Amazon Kendra di assumere un ruolo.

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

IAM ruoli per sorgenti dati Aurora (PostgreSQL)

Quando si utilizza Aurora (PostgreSQL), si assegna un ruolo con le seguenti politiche.

- Autorizzazione ad accedere al tuo AWS Secrets Manager segreto per autenticare il tuo Aurora (PostgreSQL).
- Autorizzazione a chiamare le API pubbliche richieste per il connettore Aurora (PostgreSQL).
- Autorizzazione a chiamare le`BatchPutDocument`,, `BatchDeleteDocument` `PutPrincipalMapping``DeletePrincipalMapping`, `DescribePrincipalMapping` e API. `ListGroupsOlderThanOrderingId`

> **Note**
>
> È possibile connettere un' Aurora origine dati (PostgreSQL) a through. Amazon Kendra Amazon VPC Se si utilizza un Amazon VPC, è necessario aggiungere autorizzazioni aggiuntive.

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

Una politica di fiducia per consentire Amazon Kendra di assumere un ruolo.

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

IAM ruoli per le fonti di Amazon FSx dati

Quando si utilizza Amazon FSx, si fornisce un ruolo con le seguenti politiche.

- Autorizzazione ad accedere al AWS Secrets Manager segreto per autenticare il Amazon FSx file system.
- Autorizzazione di accesso Amazon Virtual Private Cloud (VPC) dove risiede il Amazon FSx file system.
- Autorizzazione a ottenere il nome di dominio di Active Directory per il Amazon FSx file system.
- Autorizzazione a chiamare le API pubbliche richieste per il Amazon FSx connettore.

- Autorizzazione a chiamare `BatchPutDocument` e alle `BatchDeleteDocument` API per aggiornare l'indice.

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

Una politica di fiducia per consentire Amazon Kendra di assumere un ruolo.

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

IAM ruoli per le fonti di dati del database

Quando si utilizza un database come origine dati, si fornisce un ruolo Amazon Kendra con le autorizzazioni necessarie per connettersi a. Ciò include:

- Autorizzazione ad accedere al AWS Secrets Manager segreto che contiene il nome utente e la password per il sito. Per ulteriori informazioni sul contenuto del segreto, consulta le fonti di dati.
- Autorizzazione a utilizzare la chiave master AWS KMS del cliente (CMK) per decrittografare il nome utente e la password segreti memorizzati da. Secrets Manager
- Autorizzazione all'uso `BatchPutDocument` e alle `BatchDeleteDocument` operazioni di aggiornamento dell'indice.
- Autorizzazione ad accedere al Amazon S3 bucket che contiene il certificato SSL utilizzato per comunicare con il sito.

> **Note**
>
> È possibile connettere le sorgenti di dati del database a Through. Amazon Kendra Amazon VPC Se si utilizza un Amazon VPC, è necessario aggiungere autorizzazioni aggiuntive.

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

Esistono due politiche opzionali che è possibile utilizzare con un'origine dati.

Se hai crittografato il Amazon S3 bucket che contiene il certificato SSL utilizzato per comunicare con, fornisci una politica per consentire Amazon Kendra l'accesso alla chiave.

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

```
}
```

Se utilizzi un VPC, fornisci una policy che dia Amazon Kendra accesso alle risorse richieste. Consulta IAM i ruoli per le fonti di dati, VPC per la policy richiesta.

Una politica di fiducia per consentire Amazon Kendra di assumere un ruolo.

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

IAM ruoli per le origini dati Amazon RDS (Microsoft SQL Server)

Quando si utilizza un connettore di origine dati Amazon RDS (Microsoft SQL Server), si fornisce un ruolo con le seguenti politiche.

- Autorizzazione ad accedere al AWS Secrets Manager segreto per autenticare l'istanza di origine dati Amazon RDS (Microsoft SQL Server).
- Autorizzazione a chiamare le API pubbliche richieste per il connettore di origine dati Amazon RDS (Microsoft SQL Server).
- Autorizzazione a chiamare le `BatchPutDocument`,`BatchDeleteDocument`, `PutPrincipalMapping`, `DeletePrincipalMapping`,`DescribePrincipalMapping`, e `ListGroupsOlderThanOrderingId` API.

> **Note**
>
> È possibile connettere un'origine dati Amazon RDS (Microsoft SQL Server) a Amazon Kendra through Amazon VPC. Se si utilizza un Amazon VPC, è necessario aggiungere autorizzazioni aggiuntive.

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

Una politica di fiducia per consentire Amazon Kendra di assumere un ruolo.

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

IAM ruoli per sorgenti dati Amazon RDS (MySQL)

Quando si utilizza un connettore di origine dati Amazon RDS (MySQL), si fornisce un ruolo con le seguenti politiche.

- Autorizzazione ad accedere al tuo AWS Secrets Manager segreto per autenticare la tua Amazon RDS istanza di origine dati (MySQL).
- Autorizzazione a chiamare le API pubbliche richieste per il connettore di Amazon RDS origine dati (MySQL).
- Autorizzazione a chiamare le`BatchPutDocument`,`BatchDeleteDocument`, `PutPrincipalMapping` `DeletePrincipalMappingDescribePrincipalMapping`, e le API. `ListGroupsOlderThanOrderingId`

> **Note**
>
> È possibile connettere un' Amazon RDS origine dati (MySQL) a through. Amazon Kendra Amazon VPC Se si utilizza un Amazon VPC, è necessario aggiungere autorizzazioni aggiuntive.

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

Una politica di fiducia per consentire Amazon Kendra di assumere un ruolo.

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

IAM ruoli per le fonti di dati Amazon RDS (Oracle)

Quando si utilizza un connettore di origine dati Amazon RDS Oracle, si fornisce un ruolo con le seguenti politiche.

- Autorizzazione ad accedere al AWS Secrets Manager segreto per autenticare l'istanza dell'origine dati Amazon RDS (Oracle).
- Autorizzazione a chiamare le API pubbliche richieste per il connettore di origine dati Amazon RDS (Oracle).
- Autorizzazione a chiamare le `BatchPutDocument`,`BatchDeleteDocument`,`PutPrincipalMapping`,

`DeletePrincipalMapping`, `DescribePrincipalMapping`, e `ListGroupsOlderThanOrderingId` API.

> **Note**
>
> È possibile connettere un'origine dati Amazon RDS Amazon Kendra Oracle Amazon VPC a. Se si utilizza un Amazon VPC, è necessario aggiungere autorizzazioni aggiuntive.

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

Una politica di fiducia per consentire Amazon Kendra di assumere un ruolo.

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

IAM ruoli per sorgenti dati Amazon RDS (PostgreSQL)

Quando utilizzi un connettore di origine dati Amazon RDS (PostgreSQL), fornisci un ruolo con le seguenti politiche.

- Autorizzazione ad accedere al AWS Secrets Manager segreto per autenticare l'istanza di Amazon RDS origine dati (PostgreSQL).
- Autorizzazione a chiamare le API pubbliche richieste per il connettore di Amazon RDS origine dati (PostgreSQL).

- Autorizzazione a chiamare le`BatchPutDocument`,, `BatchDeleteDocument` `PutPrincipalMapping`,`DeletePrincipalMapping`, `DescribePrincipalMapping` e le API. `ListGroupsOlderThanOrderingId`

> **Note**
>
> È possibile connettere un' Amazon RDS origine dati (PostgreSQL) a through. Amazon Kendra Amazon VPC Se si utilizza un Amazon VPC, è necessario aggiungere autorizzazioni aggiuntive.

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

Una politica di fiducia per consentire Amazon Kendra di assumere un ruolo.

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

IAM ruoli per le fonti di Amazon S3 dati

> **Warning**
>
> Amazon Kendra non utilizza una policy bucket che concede le autorizzazioni a un Amazon Kendra principale per interagire con un bucket S3. Utilizza invece i ruoli. IAM Assicurati che Amazon Kendra non sia incluso come membro fidato nella tua bucket policy per evitare

problemi di sicurezza dei dati derivanti dalla concessione accidentale di autorizzazioni a responsabili arbitrari. Tuttavia, puoi aggiungere una policy sui bucket per utilizzare un bucket su account diversi. Amazon S3 Per ulteriori informazioni, consulta Politiche da utilizzare Amazon S3 su più account (scorri verso il basso).

Quando si utilizza un Amazon S3 bucket come fonte di dati, si fornisce un ruolo autorizzato ad accedere al bucket e a utilizzare le operazioni `BatchPutDocument` and`BatchDeleteDocument`. Se i documenti nel Amazon S3 bucket sono crittografati, è necessario fornire l'autorizzazione a utilizzare la chiave master del AWS KMS cliente (CMK) per decrittografare i documenti.

Le seguenti politiche relative ai ruoli devono consentire l'assunzione di un ruolo Amazon Kendra . Scorri più in basso per visualizzare una politica di fiducia per assumere un ruolo.

Una politica di ruolo obbligatoria Amazon Kendra per consentire l'utilizzo di un Amazon S3 bucket come fonte di dati.

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

Una politica di ruolo opzionale che consente di Amazon Kendra utilizzare una chiave master AWS KMS del cliente (CMK) per decrittografare i documenti in un 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"
            ]
        }
    ]
}
```

Una politica di ruolo opzionale per consentire l'accesso Amazon Kendra a un Amazon S3 bucket, utilizzando un e senza attivare o condividere Amazon VPC le autorizzazioni. AWS KMS AWS KMS

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

Una politica di ruolo opzionale per consentire l'accesso Amazon Kendra a un Amazon S3 bucket mentre si utilizza un e con le autorizzazioni Amazon VPC attivate. AWS KMS

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

Una politica di fiducia per consentire di Amazon Kendra assumere un ruolo.

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

Politiche da utilizzare Amazon S3 su più account

Se il Amazon S3 bucket si trova in un account diverso da quello utilizzato per l' Amazon Kendra indice, puoi creare politiche per utilizzarlo su più account.

Una politica di ruolo per utilizzare il Amazon S3 bucket come fonte di dati quando il bucket si trova in un account diverso da quello dell'indice. Amazon Kendra Nota che `s3:PutObjectAcl` i `s3:PutObject` e sono facoltativi e li usi se desideri includere un file di configurazione per la tua lista di controllo degli accessi.

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

Una policy relativa ai bucket per consentire al ruolo della fonte di Amazon S3 dati di accedere al Amazon S3 bucket su più account. Tieni presente che `s3:PutObjectAcl` i `s3:PutObject` e sono facoltativi e li usi se desideri includere un file di configurazione per la tua lista di controllo degli accessi.

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

Una politica di fiducia Amazon Kendra per consentire di assumere un ruolo.

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

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

IAM ruoli per le fonti di dati Amazon Kendra Web Crawler

Quando utilizzi Amazon Kendra Web Crawler, fornisci un ruolo con le seguenti politiche:

- Autorizzazione ad accedere al AWS Secrets Manager segreto che contiene le credenziali per connettersi ai siti Web o a un server proxy Web supportato dall'autenticazione di base. Per ulteriori informazioni sul contenuto del segreto, consulta Utilizzo di un'origine dati del web crawler.
- Autorizzazione a utilizzare la chiave master AWS KMS del cliente (CMK) per decrittografare il nome utente e la password segreti memorizzati da. Secrets Manager
- Autorizzazione all'uso `BatchPutDocument` e alle `BatchDeleteDocument` operazioni di aggiornamento dell'indice.
- Se utilizzi un Amazon S3 bucket per archiviare l'elenco di URL iniziali o sitemap, includi l'autorizzazione ad accedere al bucket. Amazon S3

> **Note**
>
> Puoi connettere un'origine dati del Amazon Kendra Web Crawler a. Amazon Kendra Amazon VPC Se si utilizza un Amazon VPC, è necessario aggiungere autorizzazioni aggiuntive.

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

Se memorizzi gli URL iniziali o le sitemap in un Amazon S3 bucket, devi aggiungere questa autorizzazione al ruolo.

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

Una politica di fiducia per consentire di assumere un ruolo Amazon Kendra .

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

IAM ruoli per le fonti di Amazon WorkDocs dati

Quando si utilizza Amazon WorkDocs, si fornisce un ruolo con le seguenti politiche

- Autorizzazione a verificare l'ID della directory (ID dell'organizzazione) che corrisponde all'archivio Amazon WorkDocs del sito.
- Autorizzazione a ottenere il nome di dominio di Active Directory che contiene la directory Amazon WorkDocs del sito.
- Autorizzazione a chiamare le API pubbliche richieste per il Amazon WorkDocs connettore.
- Autorizzazione a chiamare `BatchPutDocument` e alle `BatchDeleteDocument` API per aggiornare l'indice.

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

Una politica di fiducia per consentire Amazon Kendra di assumere un ruolo.

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

IAM ruoli per le fonti di dati Box

Quando usi Box, fornisci un ruolo con le seguenti politiche.

- Autorizzazione ad accedere al tuo AWS Secrets Manager segreto per autenticare Slack.
- Autorizzazione a chiamare le API pubbliche richieste per il connettore Box.
- Autorizzazione a chiamare le `BatchPutDocument`,`BatchDeleteDocument`, `PutPrincipalMapping`, `DeletePrincipalMapping`, `DescribePrincipalMapping` e `ListGroupsOlderThanOrderingId` API.

> **Note**
>
> Puoi connettere un'origine dati Box a Amazon Kendra . Amazon VPC Se utilizzi un Amazon VPC, devi aggiungere autorizzazioni aggiuntive.

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

Una politica di fiducia per consentire Amazon Kendra di assumere un ruolo.

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

IAM ruoli per le fonti di dati Confluence

IAM ruoli per Confluence Connector v1.0

Quando utilizzi un server Confluence come origine dati, fornisci un ruolo con le seguenti politiche:

- Autorizzazione ad accedere al AWS Secrets Manager segreto che contiene le credenziali necessarie per connettersi a Confluence. Per ulteriori informazioni sul contenuto del segreto, consulta Fonti di dati Confluence.
- Autorizzazione a utilizzare la chiave master AWS KMS del cliente (CMK) per decrittografare il nome utente e la password segreti memorizzati da. Secrets Manager
- Autorizzazione all'uso `BatchPutDocument` e alle `BatchDeleteDocument` operazioni di aggiornamento dell'indice.

> **Note**
>
> Puoi connettere un'origine dati Confluence a Amazon Kendra through. Amazon VPC Se utilizzi un Amazon VPC, devi aggiungere autorizzazioni aggiuntive.

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

Se utilizzi un VPC, fornisci una policy che dia Amazon Kendra accesso alle risorse richieste. Consulta IAM i ruoli per le fonti di dati, VPC per la policy richiesta.

Una politica di fiducia per consentire Amazon Kendra di assumere un ruolo.

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

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

IAM ruoli per Confluence Connector v2.0

Per un'origine dati Confluence Connector v2.0, fornisci un ruolo con le seguenti politiche.

- Autorizzazione ad accedere al AWS Secrets Manager segreto che contiene le credenziali di autenticazione per Confluence. Per ulteriori informazioni sul contenuto del segreto, consulta Fonti di dati Confluence.
- Autorizzazione a utilizzare la chiave master AWS KMS del cliente (CMK) per decrittografare il nome utente e la password segreti memorizzati da. AWS Secrets Manager
- Autorizzazione all'uso `BatchPutDocument` e alle `BatchDeleteDocument` operazioni di aggiornamento dell'indice.

È inoltre necessario allegare una politica di fiducia che Amazon Kendra consenta di assumere il ruolo.

> **Note**
>
> Puoi connettere un'origine dati Confluence a Amazon Kendra through. Amazon VPC Se utilizzi un Amazon VPC, devi aggiungere autorizzazioni aggiuntive.

Una politica di ruolo per consentire la connessione Amazon Kendra a 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"
    }
  ]
}
```

Una politica di fiducia per consentire di Amazon Kendra assumere un ruolo.

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

IAM ruoli per le fonti di dati di Dropbox

Quando utilizzi Dropbox, fornisci un ruolo con le seguenti norme.

- Autorizzazione ad accedere al tuo AWS Secrets Manager segreto per autenticare il tuo Dropbox.
- Autorizzazione a chiamare le API pubbliche richieste per il connettore Dropbox.
- Autorizzazione a chiamare le`BatchPutDocument`,`BatchDeleteDocument`, `PutPrincipalMapping` `DeletePrincipalMappingDescribePrincipalMapping`, e `ListGroupsOlderThanOrderingId` le API.

> **Note**
>
> Puoi connettere una fonte di dati Dropbox a Amazon Kendra . Amazon VPC Se utilizzi un Amazon VPC, devi aggiungere ulteriori autorizzazioni.

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

Una politica di fiducia per consentire Amazon Kendra di assumere un ruolo.

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

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

IAM ruoli per le fonti di dati Drupal

Quando usi Drupal, fornisci un ruolo con le seguenti politiche.

- Autorizzazione ad accedere al tuo AWS Secrets Manager segreto per autenticare il tuo Drupal.
- Autorizzazione a chiamare le API pubbliche richieste per il connettore Drupal.
- Autorizzazione a chiamare le`BatchPutDocument`,`BatchDeleteDocument`,, `PutPrincipalMapping` `DeletePrincipalMappingDescribePrincipalMapping`, e API. `ListGroupsOlderThanOrderingId`

> **Note**
>
> Puoi connettere una fonte di dati Drupal a tramite. Amazon Kendra Amazon VPC Se si utilizza un Amazon VPC, è necessario aggiungere autorizzazioni aggiuntive.

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

Una politica di fiducia per consentire Amazon Kendra di assumere un ruolo.

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

```
    ]
}
```

IAM ruoli per le fonti di GitHub dati

Quando si utilizza GitHub, si fornisce un ruolo con le seguenti politiche.

- Autorizzazione ad accedere al tuo AWS Secrets Manager segreto per autenticare il tuo GitHub.
- Autorizzazione a chiamare le API pubbliche richieste per il GitHub connettore.
- Autorizzazione a chiamare le `BatchPutDocument`,`BatchDeleteDocument`, `PutPrincipalMapping`, `DeletePrincipalMapping`,`DescribePrincipalMapping`, e `ListGroupsOlderThanOrderingId` API.

> **Note**
>
> È possibile connettere un'origine GitHub dati a Amazon Kendra through Amazon VPC. Se si utilizza un Amazon VPC, è necessario aggiungere autorizzazioni aggiuntive.

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

Una politica di fiducia per consentire Amazon Kendra di assumere un ruolo.

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

```
    ]
}
```

IAM ruoli per le fonti di dati di Gmail

Quando utilizzi Gmail, fornisci un ruolo con le seguenti politiche.

- Autorizzazione ad accedere al tuo AWS Secrets Manager segreto per autenticare Gmail.
- Autorizzazione a chiamare le API pubbliche richieste per Gmailconnector.
- Autorizzazione a chiamare le`BatchPutDocument`,`BatchDeleteDocument`,, `PutPrincipalMapping` `DeletePrincipalMappingDescribePrincipalMapping`, e API. `ListGroupsOlderThanOrderingId`

> **Note**
>
> Puoi connettere un'origine dati Gmail a Amazon Kendra . Amazon VPC Se si utilizza un Amazon VPC, è necessario aggiungere autorizzazioni aggiuntive.

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

Una politica di fiducia per consentire Amazon Kendra di assumere un ruolo.

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

IAM ruoli per le fonti di dati di Google Drive

Quando utilizzi un'origine dati Google Workspace Drive, fornisci un ruolo Amazon Kendra con le autorizzazioni necessarie per la connessione al sito. Ciò include:

- Autorizzazione a ottenere e decrittografare il codice AWS Secrets Manager segreto contenente l'e-mail dell'account cliente, l'e-mail dell'account amministratore e la chiave privata necessari per connettersi al sito di Google Drive. Per ulteriori informazioni sul contenuto del segreto, consulta Fonti di dati di Google Drive.
- Autorizzazione all'uso delle BatchDeleteDocumentAPI BatchPutDocumente.

> **Note**
>
> Puoi connettere una fonte di dati di Google Drive a Amazon Kendra tramite Amazon VPC. Se utilizzi un Amazon VPC, devi aggiungere ulteriori autorizzazioni.

La seguente IAM politica fornisce le autorizzazioni necessarie:

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

Una politica di fiducia per consentire Amazon Kendra di assumere un ruolo.

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

IAM ruoli per le fonti di dati IBM DB2

Quando utilizzi un connettore di origine dati IBM DB2, fornisci un ruolo con le seguenti politiche.

- Autorizzazione ad accedere al AWS Secrets Manager segreto per autenticare l'istanza di origine dati IBM DB2.
- Autorizzazione a chiamare le API pubbliche richieste per il connettore di origine dati IBM DB2.
- Autorizzazione a chiamare le`BatchPutDocument`,`BatchDeleteDocument`, `PutPrincipalMapping` `DeletePrincipalMappingDescribePrincipalMapping`, e API. `ListGroupsOlderThanOrderingId`

> **Note**
>
> È possibile connettere un'origine dati IBM DB2 a through. Amazon Kendra Amazon VPC Se si utilizza un Amazon VPC, è necessario aggiungere autorizzazioni aggiuntive.

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

Una politica di fiducia per consentire Amazon Kendra di assumere un ruolo.

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

IAM ruoli per le fonti di dati Jira

Quando usi Jira, fornisci un ruolo con le seguenti politiche.

- Autorizzazione ad accedere al tuo AWS Secrets Manager segreto per autenticare Jira.
- Autorizzazione a chiamare le API pubbliche richieste per il connettore Jira.
- Autorizzazione a chiamare le`BatchPutDocument`,`BatchDeleteDocument`,`PutPrincipalMapping`, `DeletePrincipalMappingDescribePrincipalMapping`, e `ListGroupsOlderThanOrderingId` API.

> **Note**
>
> Puoi connettere un'origine dati Jira a Amazon Kendra . Amazon VPC Se si utilizza un Amazon VPC, è necessario aggiungere autorizzazioni aggiuntive.

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

Una politica di fiducia per consentire Amazon Kendra di assumere un ruolo.

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

IAM ruoli per le origini dati di Microsoft Exchange

Quando si utilizza un'origine dati di Microsoft Exchange, si fornisce un ruolo Amazon Kendra con le autorizzazioni necessarie per la connessione al sito. Ciò include:

- Autorizzazione a ottenere e decrittografare il AWS Secrets Manager segreto che contiene l'ID dell'applicazione e la chiave segreta necessari per connettersi al sito di Microsoft Exchange. Per ulteriori informazioni sul contenuto del segreto, vedere Origini dati di Microsoft Exchange.
- Autorizzazione all'uso delle BatchDeleteDocumentAPI BatchPutDocumente.

> **Note**
>
> È possibile connettere un'origine dati Microsoft Exchange a Amazon Kendra tramite Amazon VPC. Se si utilizza un Amazon VPC, è necessario aggiungere ulteriori autorizzazioni.

La seguente IAM politica fornisce le autorizzazioni necessarie:

```
{
  "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"
```

```
  }]
}
```

Se stai archiviando l'elenco di utenti da indicizzare in un Amazon S3 bucket, devi anche fornire l'autorizzazione per utilizzare l'operazione `GetObject` S3. La seguente IAM politica fornisce le autorizzazioni necessarie:

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

Una politica di fiducia per consentire Amazon Kendra di assumere un ruolo.

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

IAM ruoli per le origini OneDrive dati Microsoft

Quando si utilizza un'origine OneDrive dati Microsoft, si fornisce un ruolo Amazon Kendra con le autorizzazioni necessarie per la connessione al sito. Ciò include:

- Autorizzazione a ottenere e decrittografare il AWS Secrets Manager segreto che contiene l'ID dell'applicazione e la chiave segreta necessari per connettersi al sito. OneDrive Per ulteriori informazioni sul contenuto del segreto, vedi Origini OneDrive dati Microsoft.
- Autorizzazione all'uso delle BatchDeleteDocumentAPI BatchPutDocumente.

> **Note**
>
> È possibile connettere un'origine OneDrive dati Microsoft a Amazon Kendra tramite Amazon VPC. Se si utilizza un Amazon VPC, è necessario aggiungere autorizzazioni aggiuntive.

La seguente IAM politica fornisce le autorizzazioni necessarie:

```
{
  "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"
```

```
  }]
}
```

Se stai archiviando l'elenco di utenti da indicizzare in un Amazon S3 bucket, devi anche fornire l'autorizzazione per utilizzare l'operazione `GetObject` S3. La seguente IAM politica fornisce le autorizzazioni necessarie:

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

Una politica di fiducia per consentire Amazon Kendra di assumere un ruolo.

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

IAM ruoli per le origini SharePoint dati Microsoft

IAM ruoli per SharePoint Connector v1.0

Per un'origine dati Microsoft SharePoint Connector v1.0, fornisci un ruolo con le seguenti politiche.

- Autorizzazione ad accedere al AWS Secrets Manager segreto che contiene il nome utente e la password per il SharePoint sito. Per ulteriori informazioni sul contenuto del segreto, vedi Origini SharePoint dati Microsoft.
- Autorizzazione a utilizzare la chiave master AWS KMS del cliente (CMK) per decrittografare il nome utente e la password segreti memorizzati da. AWS Secrets Manager
- Autorizzazione all'uso `BatchPutDocument` e alle `BatchDeleteDocument` operazioni di aggiornamento dell'indice.

- Autorizzazione ad accedere al Amazon S3 bucket che contiene il certificato SSL utilizzato per comunicare con il SharePoint sito.

È inoltre necessario allegare una politica di fiducia che Amazon Kendra consenta di assumere il ruolo.

> **Note**
>
> È possibile connettere un'origine SharePoint dati Microsoft a Amazon Kendra tramite Amazon VPC. Se si utilizza un Amazon VPC, è necessario aggiungere autorizzazioni aggiuntive.

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

Se hai crittografato il Amazon S3 bucket che contiene il certificato SSL utilizzato per comunicare con il SharePoint sito, fornisci una politica per consentire Amazon Kendra l'accesso alla chiave.

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

Una politica di fiducia per consentire di Amazon Kendra assumere un ruolo.

```
{
```

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

IAM ruoli per SharePoint Connector v2.0

Per un'origine dati Microsoft SharePoint Connector v2.0, fornisci un ruolo con le seguenti politiche.

- Autorizzazione ad accedere al AWS Secrets Manager segreto che contiene le credenziali di autenticazione per il SharePoint sito. Per ulteriori informazioni sul contenuto del segreto, vedi Origini SharePoint dati Microsoft.
- Autorizzazione a utilizzare la chiave master AWS KMS del cliente (CMK) per decrittografare il nome utente e la password segreti memorizzati da. AWS Secrets Manager
- Autorizzazione all'uso `BatchPutDocument` e alle `BatchDeleteDocument` operazioni di aggiornamento dell'indice.
- Autorizzazione ad accedere al Amazon S3 bucket che contiene il certificato SSL utilizzato per comunicare con il SharePoint sito.

È inoltre necessario allegare una politica di fiducia che Amazon Kendra consenta di assumere il ruolo.

> **Note**
>
> È possibile connettere un'origine SharePoint dati Microsoft a Amazon Kendra tramite Amazon VPC. Se si utilizza un Amazon VPC, è necessario aggiungere autorizzazioni aggiuntive.

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

Se hai crittografato il Amazon S3 bucket che contiene il certificato SSL utilizzato per comunicare con il SharePoint sito, fornisci una politica per consentire Amazon Kendra l'accesso alla chiave.

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

```
        }
    ]
}
```

Una politica di fiducia per consentire di Amazon Kendra assumere un ruolo.

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

IAM ruoli per le origini dati Microsoft SQL Server

Quando si utilizza Microsoft SQL Server, si fornisce un ruolo con le seguenti politiche.

- Autorizzazione ad accedere al AWS Secrets Manager segreto per autenticare l'istanza di Microsoft SQL Server.
- Autorizzazione a chiamare le API pubbliche richieste per il connettore Microsoft SQL Server.
- Autorizzazione a chiamare le `BatchPutDocument`,`BatchDeleteDocument`, `PutPrincipalMapping`, `DeletePrincipalMapping`,`DescribePrincipalMapping`, e `ListGroupsOlderThanOrderingId` API.

> **Note**
>
> È possibile connettere un'origine dati Microsoft SQL Server a Amazon Kendra through Amazon VPC. Se si utilizza un Amazon VPC, è necessario aggiungere autorizzazioni aggiuntive.

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

Una politica di fiducia per consentire Amazon Kendra di assumere un ruolo.

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

IAM ruoli per le origini dati Microsoft Teams

Quando utilizzi un'origine dati Microsoft Teams, fornisci un ruolo Amazon Kendra con le autorizzazioni necessarie per la connessione al sito. Ciò include:

- Autorizzazione a ottenere e decrittografare il AWS Secrets Manager segreto che contiene l'ID client e il segreto del client necessari per connettersi a Microsoft Teams. Per ulteriori informazioni sul contenuto del segreto, consulta Origini dati di Microsoft Teams.

> **Note**
>
> Puoi connettere un'origine dati Microsoft Teams a Amazon Kendra Amazon VPC. Se si utilizza un Amazon VPC, è necessario aggiungere autorizzazioni aggiuntive.

La seguente IAM politica fornisce le autorizzazioni necessarie:

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

Una politica di fiducia per consentire Amazon Kendra di assumere un ruolo.

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

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

IAM ruoli per le origini dati Microsoft Yammer

Quando si utilizza un'origine dati Microsoft Yammer, si fornisce un ruolo Amazon Kendra con le autorizzazioni necessarie per la connessione al sito. Ciò include:

- Autorizzazione a ottenere e decrittografare il AWS Secrets Manager segreto che contiene l'ID dell'applicazione e la chiave segreta necessari per connettersi al sito Microsoft Yammer. Per ulteriori informazioni sul contenuto del segreto, vedere Origini dati di Microsoft Yammer.
- Autorizzazione all'uso delle API BatchPutDocumente BatchDeleteDocument.

> **Note**
>
> È possibile connettere un'origine dati Microsoft Yammer a Amazon Kendra through. Amazon VPC Se si utilizza un Amazon VPC, è necessario aggiungere autorizzazioni aggiuntive.

La seguente IAM politica fornisce le autorizzazioni necessarie:

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

Se stai archiviando l'elenco di utenti da indicizzare in un Amazon S3 bucket, devi anche fornire l'autorizzazione per utilizzare l'operazione `GetObject` S3. La seguente IAM politica fornisce le autorizzazioni necessarie:

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

Una politica di fiducia per consentire Amazon Kendra di assumere un ruolo.

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

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

IAM ruoli per sorgenti dati MySQL

Quando si utilizza un connettore di origine dati My SQL, si fornisce un ruolo con le seguenti politiche.

- Autorizzazione ad accedere al AWS Secrets Manager segreto per autenticare l'istanza di origine dati My SQL.
- Autorizzazione a chiamare le API pubbliche richieste per il connettore di origine dati My SQL.
- Autorizzazione a chiamare le `BatchPutDocument`,`BatchDeleteDocument`, `PutPrincipalMapping`, `DeletePrincipalMapping`,`DescribePrincipalMapping`, e `ListGroupsOlderThanOrderingId` API.

> **Note**
>
> È possibile connettere un'origine dati MySQL a through. Amazon Kendra Amazon VPC Se si utilizza un Amazon VPC, è necessario aggiungere autorizzazioni aggiuntive.

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

Una politica di fiducia per consentire Amazon Kendra di assumere un ruolo.

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

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

IAM ruoli per le fonti di dati Oracle

Quando si utilizza un connettore di origine dati Oracle, si fornisce un ruolo con le seguenti politiche.

- Autorizzazione ad accedere al AWS Secrets Manager segreto per autenticare l'istanza dell'origine dati Oracle.
- Autorizzazione a chiamare le API pubbliche richieste per il connettore di origine dati Oracle.
- Autorizzazione a chiamare le `BatchPutDocument`,`BatchDeleteDocument`, `PutPrincipalMapping`, `DeletePrincipalMapping`,`DescribePrincipalMapping`, e `ListGroupsOlderThanOrderingId` API.

> **Note**
>
> È possibile connettere un'origine dati Amazon Kendra Oracle Amazon VPC a. Se si utilizza un Amazon VPC, è necessario aggiungere autorizzazioni aggiuntive.

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

Una politica di fiducia per consentire Amazon Kendra di assumere un ruolo.

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

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

IAM ruoli per le sorgenti dati PostgreSQL

Quando utilizzi un connettore di origine dati PostgreSQL, fornisci un ruolo con le seguenti politiche.

- Autorizzazione ad accedere al AWS Secrets Manager segreto per autenticare l'istanza di origine dati PostgreSQL.
- Autorizzazione a chiamare le API pubbliche richieste per il connettore di origine dati PostgreSQL.
- Autorizzazione a chiamare le`BatchPutDocument`,, `BatchDeleteDocument` `PutPrincipalMapping`, `DeletePrincipalMapping` `DescribePrincipalMapping` e API. `ListGroupsOlderThanOrderingId`

> **Note**
>
> È possibile connettere un'origine dati PostgreSQL a through. Amazon Kendra Amazon VPC Se si utilizza un Amazon VPC, è necessario aggiungere autorizzazioni aggiuntive.

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

Una politica di fiducia per consentire Amazon Kendra di assumere un ruolo.

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

```
      }
   ]
}
```

IAM ruoli per le fonti di dati Quip

Quando usi Quip, fornisci un ruolo con le seguenti politiche.

- Autorizzazione ad accedere al tuo AWS Secrets Manager segreto per autenticare Quip.
- Autorizzazione a chiamare le API pubbliche richieste per il connettore Quip.
- Autorizzazione a chiamare le`BatchPutDocument`,`BatchDeleteDocument`,`PutPrincipalMapping`, `DeletePrincipalMappingDescribePrincipalMapping`, e `ListGroupsOlderThanOrderingId` API.

> **Note**
>
> Puoi connettere una fonte di dati Quip a Amazon Kendra . Amazon VPC Se si utilizza un Amazon VPC, è necessario aggiungere autorizzazioni aggiuntive.

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

Una politica di fiducia per consentire Amazon Kendra di assumere un ruolo.

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

```
    ]
}
```

IAM ruoli per le fonti di dati Salesforce

Quando utilizzi Salesforce come fonte di dati, fornisci un ruolo con le seguenti politiche:

- Autorizzazione ad accedere al AWS Secrets Manager segreto che contiene il nome utente e la password per il sito Salesforce. Per ulteriori informazioni sul contenuto del segreto, consulta le fonti di dati di Salesforce.
- Autorizzazione a utilizzare la chiave master AWS KMS del cliente (CMK) per decrittografare il nome utente e la password segreti memorizzati da. Secrets Manager
- Autorizzazione all'uso `BatchPutDocument` e alle `BatchDeleteDocument` operazioni di aggiornamento dell'indice.

> **Note**
>
> È possibile connettere un'origine dati Salesforce a Amazon Kendra through. Amazon VPC Se si utilizza un Amazon VPC, è necessario aggiungere autorizzazioni aggiuntive.

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

Una politica di fiducia per consentire Amazon Kendra di assumere un ruolo.

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

IAM ruoli per le fonti di ServiceNow dati

Quando utilizzi un ServiceNow come fonte di dati, fornisci un ruolo con le seguenti politiche:

- Autorizzazione ad accedere al Secrets Manager segreto che contiene il nome utente e la password per il ServiceNow sito. Per ulteriori informazioni sul contenuto del segreto, consulta le fonti di ServiceNow dati.

- Autorizzazione a utilizzare la chiave master AWS KMS del cliente (CMK) per decrittografare il nome utente e la password segreti memorizzati da. Secrets Manager
- Autorizzazione all'uso `BatchPutDocument` e alle `BatchDeleteDocument` operazioni di aggiornamento dell'indice.

> **Note**
>
> È possibile connettere un'origine ServiceNow dati a Amazon Kendra through Amazon VPC. Se si utilizza un Amazon VPC, è necessario aggiungere autorizzazioni aggiuntive.

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

Una politica di fiducia per consentire Amazon Kendra di assumere un ruolo.

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

IAM ruoli per le fonti di dati Slack

Quando usi Slack, fornisci un ruolo con le seguenti politiche.

- Autorizzazione ad accedere al tuo AWS Secrets Manager segreto per autenticare Slack.
- Autorizzazione a chiamare le API pubbliche richieste per il connettore Slack.
- Autorizzazione a chiamare leBatchPutDocument,BatchDeleteDocument,PutPrincipalMapping, DeletePrincipalMappingDescribePrincipalMapping, e ListGroupsOlderThanOrderingId API.

> **Note**
>
> Puoi connettere una fonte di dati Slack a Amazon Kendra . Amazon VPC Se utilizzi un Amazon VPC, devi aggiungere autorizzazioni aggiuntive.

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

Una politica di fiducia per consentire Amazon Kendra di assumere un ruolo.

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

IAM ruoli per le fonti di dati Zendesk

Quando utilizzi Zendesk, fornisci un ruolo con le seguenti politiche.

- Autorizzazione ad accedere al tuo AWS Secrets Manager segreto per autenticare la tua Zendesk Suite.
- Autorizzazione a chiamare le API pubbliche richieste per il connettore Zendesk.
- Autorizzazione a chiamare le`BatchPutDocument`,`BatchDeleteDocument`,`PutPrincipalMapping`, `DeletePrincipalMappingDescribePrincipalMapping`, e `ListGroupsOlderThanOrderingId` API.

> **Note**
>
> È possibile connettere un'origine dati Zendesk a Amazon Kendra . Amazon VPC Se si utilizza un Amazon VPC, è necessario aggiungere autorizzazioni aggiuntive.

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

Una politica di fiducia per consentire Amazon Kendra di assumere un ruolo.

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

Ruolo del cloud privato virtuale (VPC) IAM

Se utilizzi un cloud privato virtuale (VPC) per connetterti alla tua origine dati, devi fornire le seguenti autorizzazioni aggiuntive.

Ruolo 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": "*"
    }
}
```

Una politica di fiducia per consentire Amazon Kendra di assumere un ruolo.

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

IAM ruoli per le domande frequenti (FAQ)

Quando utilizzi l'CreateFaqAPI per caricare domande e risposte in un indice, devi fornire un IAM ruolo Amazon Kendra con accesso al Amazon S3 bucket che contiene i file sorgente. Se i file di origine sono crittografati, è necessario fornire l'autorizzazione a utilizzare la chiave master AWS KMS del cliente (CMK) per decrittografare i file.

IAM ruoli per le domande frequenti

Una politica di ruolo obbligatoria per consentire l'accesso Amazon Kendra a un Amazon S3 bucket.

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

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

Una politica di ruolo opzionale che consente di Amazon Kendra utilizzare una chiave master AWS KMS del cliente (CMK) per decrittografare i file in un 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"
                    ]
                }
            }
        }
    ]
}
```

Una politica di fiducia per consentire di assumere un ruolo Amazon Kendra .

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

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

IAM ruoli per i suggerimenti di interrogazione

Quando si utilizza un Amazon S3 file come elenco di blocchi di suggerimenti per le interrogazioni, si fornisce un ruolo autorizzato ad accedere al Amazon S3 file e al Amazon S3 bucket. Se il file di testo della lista di blocco (il Amazon S3 file) nel Amazon S3 bucket è crittografato, è necessario fornire l'autorizzazione a utilizzare la chiave master del AWS KMS cliente (CMK) per decrittografare i documenti.

IAM ruoli per i suggerimenti di interrogazione

Una politica di ruolo obbligatoria che consente di Amazon Kendra utilizzare il Amazon S3 file come elenco di blocchi per i suggerimenti di interrogazione.

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

Una politica di ruolo opzionale che consente di Amazon Kendra utilizzare una chiave master AWS KMS del cliente (CMK) per decrittografare i documenti in un 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"
            ]
        }
    ]
}
```

Una politica di fiducia per consentire di assumere un ruolo Amazon Kendra .

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

IAM ruoli per la mappatura principale di utenti e gruppi

Quando utilizzi l'PutPrincipalMappingAPI per mappare gli utenti ai rispettivi gruppi per filtrare i risultati della ricerca in base al contesto dell'utente, devi fornire un elenco di utenti o sottogruppi che appartengono a un gruppo. Se l'elenco include più di 1000 utenti o sottogruppi per gruppo, devi fornire un ruolo con l'autorizzazione ad accedere al Amazon S3 file dell'elenco e al bucket. Amazon S3 Se il file di testo (il Amazon S3 file) dell'elenco nel Amazon S3 bucket è crittografato, è necessario fornire l'autorizzazione a utilizzare la chiave master del AWS KMS cliente (CMK) per decrittografare i documenti.

IAM ruoli per la mappatura principale

Una politica di ruolo obbligatoria Amazon Kendra per consentire l'utilizzo del Amazon S3 file come elenco di utenti e sottogruppi che appartengono a un gruppo.

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

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

Una politica di ruolo opzionale che consente di Amazon Kendra utilizzare una chiave master AWS KMS del cliente (CMK) per decrittografare i documenti in un 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"
            ]
        }
    ]
}
```

Una politica di fiducia per consentire di assumere un ruolo Amazon Kendra .

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

```
}
```

Si consiglia di includere `aws:sourceAccount` e `aws:sourceArn` nella politica di fiducia. Ciò limita le autorizzazioni e verifica in modo sicuro se `aws:sourceAccount` e `aws:sourceArn` sono le stesse fornite nella politica di IAM ruolo per l'azione`sts:AssumeRole`. Ciò impedisce alle entità non autorizzate di accedere ai tuoi IAM ruoli e alle loro autorizzazioni. Per ulteriori informazioni, consulta la AWS Identity and Access Management guida sul problema del vice confuso.

```
{
    "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 ruoli per AWS IAM Identity Center

Quando si utilizza l'UserGroupResolutionConfigurationoggetto per recuperare i livelli di accesso di gruppi e utenti da una fonte di AWS IAM Identity Center identità, è necessario fornire un ruolo con autorizzazione di accesso IAM Identity Center.

IAM ruoli per AWS IAM Identity Center

Una politica di ruolo obbligatoria per consentire l' Amazon Kendra accesso 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"
              ]
            }
          }
        }
    ]
}
```

Una politica di fiducia Amazon Kendra per consentire di assumere un ruolo.

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

```
      }
   ]
}
```

IAM ruoli per Amazon Kendra le esperienze

Quando utilizzi le CreateExperienceo UpdateExperienceAPI per creare o aggiornare un'applicazione di ricerca, devi fornire un ruolo con l'autorizzazione ad accedere alle operazioni necessarie e a IAM Identity Center.

IAM ruoli per l'esperienza Amazon Kendra di ricerca

Una politica di ruolo obbligatoria per consentire l'accesso Amazon Kendra a `Query` operazioni, `QuerySuggestions` `SubmitFeedback` operazioni e a IAM Identity Center che archivia le informazioni su utenti e gruppi.

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

Una politica di fiducia Amazon Kendra per consentire di assumere un ruolo.

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

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

Si consiglia di includere `aws:sourceAccount` e `aws:sourceArn` nella politica di fiducia. Ciò limita le autorizzazioni e verifica in modo sicuro se `aws:sourceAccount` e `aws:sourceArn` sono le stesse fornite nella politica di IAM ruolo per l'azione`sts:AssumeRole`. Ciò impedisce alle entità non autorizzate di accedere ai tuoi IAM ruoli e alle loro autorizzazioni. Per ulteriori informazioni, consulta la AWS Identity and Access Management guida sul problema del vice confuso.

```
{
    "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 ruoli per Custom Document Enrichment

Quando si utilizza l'CustomDocumentEnrichmentConfigurationoggetto per applicare modifiche avanzate ai metadati e al contenuto del documento, è necessario fornire un ruolo con le autorizzazioni necessarie per l'esecuzione e/o. `PreExtractionHookConfiguration`

`PostExtractionHookConfiguration` È possibile configurare una funzione Lambda per `PreExtractionHookConfiguration` e/o applicare modifiche avanzate `PostExtractionHookConfiguration` ai metadati e ai contenuti del documento durante il processo di inserimento. Se scegli di attivare Server Side Encryption per il tuo Amazon S3 bucket, devi fornire l'autorizzazione a utilizzare la chiave master del AWS KMS cliente (CMK) per crittografare e decrittografare gli oggetti memorizzati nel bucket. Amazon S3

IAM ruoli per Custom Document Enrichment

Una politica dei ruoli obbligatoria Amazon Kendra per consentire l'esecuzione `PreExtractionHookConfiguration` e `PostExtractionHookConfiguration` con crittografia per il Amazon S3 bucket.

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

Una politica di ruolo opzionale per Amazon Kendra consentirne l'esecuzione `PreExtractionHookConfiguration` e `PostExtractionHookConfiguration` senza crittografia per il Amazon S3 bucket.

```
{
  "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"
  }]
```

```
}
```

Una politica di fiducia per consentire Amazon Kendra di assumere un ruolo.

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

Si consiglia di includere `aws:sourceAccount` e `aws:sourceArn` nella politica di fiducia. Ciò limita le autorizzazioni e verifica in modo sicuro se `aws:sourceAccount` e `aws:sourceArn` sono le stesse fornite nella politica di IAM ruolo per l'azione`sts:AssumeRole`. Ciò impedisce alle entità non autorizzate di accedere ai tuoi IAM ruoli e alle loro autorizzazioni. Per ulteriori informazioni, consulta la AWS Identity and Access Management guida sul problema del vice confuso.

```
{
    "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/*"
```

```
                }
            }
        }
    ]
}
```

Distribuzione di Amazon Kendra

Quando arriva il momento di implementareAmazon Kendrase effettui una ricerca sul tuo sito web, forniamo il codice sorgente che puoi usare con React per iniziare a usare la tua applicazione con un vantaggio. Il codice sorgente viene fornito gratuitamente con una licenza MIT modificata. Puoi usarlo così com'è o modificarlo per le tue esigenze. L'app React fornita è un esempio per aiutarti a iniziare. Non è un'app pronta per la produzione.

Per implementare un'applicazione di ricerca senza codice e generare un URL endpoint per la pagina di ricerca con controllo dell'accesso, consultaAmazon KendraGeneratore di esperienze.

Il codice di esempio seguente aggiungeAmazon Kendracerca in un'applicazione web React esistente:

- https://kendrasamples.s3.amazonaws.com/kendrasamples-react-app.zip—File di esempio che gli sviluppatori possono utilizzare per creare un'esperienza di ricerca funzionale nella loro applicazione web React esistente.

Gli esempi sono modellati sulla pagina di ricerca diAmazon Kendraconsolle. Hanno le stesse funzionalità per la ricerca e la visualizzazione dei risultati di ricerca. È possibile utilizzare l'intero esempio oppure scegliere solo una delle funzionalità per uso personale.

Per visualizzare i tre componenti della pagina di ricerca nellaAmazon Kendraconsole, scegli l'icona del codice (</>) dal menu a destra. Passa il puntatore su ogni sezione per visualizzare una breve descrizione del componente e per ottenere l'URL della fonte del componente.

Argomenti

Panoramica

Aggiungi il codice di esempio a un'applicazione web React esistente per attivare la ricerca. Il codice di esempio include un file Readme con i passaggi per configurare un nuovo ambiente di sviluppo React. I dati di esempio contenuti nell'esempio di codice possono essere utilizzati per dimostrare una ricerca. I file di ricerca e i componenti nel codice di esempio sono strutturati come segue:

- Pagina di ricerca principale (`Search.tsx`): questa è la pagina principale che contiene tutti i componenti. Qui è possibile integrare l'applicazione conAmazon KendraAPI.
- Barra di ricerca: questo è il componente in cui un utente inserisce un termine di ricerca e richiama la funzione di ricerca.
- Risultati: questo è il componente che visualizza i risultati diAmazon Kendra. Ha tre componenti: risposte suggerite, risultati delle domande frequenti e documenti consigliati.
- Sfaccettature: questo è il componente che mostra le sfaccettature nei risultati della ricerca e consente di scegliere una sfaccettatura per restringere la ricerca.
- Impaginazione: questo è il componente da cui viene impaginata la rispostaAmazon Kendra.

Prerequisiti

Prima di iniziare, avrai bisogno di:

- Node.js e npminstallato. È richiesta la versione 19 o precedente di Node.js.
- Python 3 o Python 2scaricato e installato.
- SDK for JavaoAWS SDK for JavaScriptper l'invio di chiamate API aAmazon Kendra.
- Un'applicazione web React esistente. Il codice di esempio include un file Readme con i passaggi su come configurare un nuovo ambiente di sviluppo React, incluso l'utilizzo di framework/librerie richiesti. Puoi anche seguire le istruzioni per l'utente.Documentazione di React sulla creazione di un'app web React.
- Le librerie e le dipendenze richieste configurate nell'ambiente di sviluppo. Il codice di esempio include un file Readme che elenca le librerie e le dipendenze dei pacchetti richieste. Si noti che`sass`è obbligatorio, come`node-sass`è obsoleto. Se l'hai installato in precedenza`node-sass`, disinstallalo e installa`sass`.

Configurazione dell'esempio

Una procedura completa per l'aggiuntaAmazon Kendrala ricerca in un'applicazione React si trova nel file Readme incluso nell'esempio di codice.

Per iniziare a utilizzare kendrasamples-react-app.zip

1. Assicurati di aver completato laPrerequisiti, incluso il download e l'installazione di Node.js e npm.
2. Scarica kendrasamples-react-app.zip e unzip.
3. Apri il tuo terminale e vai a`aws-kendra-example-react-app/src/services/`. Apertalocal-dev-credentials.jsone fornisci le tue credenziali. Non aggiungete questo file a nessun archivio pubblico.
4. Vai a`aws-kendra-example-react-app`e installa le dipendenze in`package.json`. Esegui `npm install`.
5. Avvia una versione demo della tua app sul tuo server. Esegui `npm start`. Puoi fermare il server locale accedendo alla tastieraCmd/`Ctrl + C`.
6. Puoi cambiare la porta o l'host (ad esempio, l'indirizzo IP) accedendo a`package.json`e aggiorna l'host e la porta:`"start": "HOST=[host] PORT=[port] react-scripts start"`. Se usi Windows:`"start": "set HOST=[host] && set PORT=[port] && react-scripts start"`.
7. Se disponi di un dominio web registrato, puoi specificarlo in`package.json`dopo il nome della tua app. Ad esempio, `"homepage": "https://mywebsite.com"`. Devi correrenpm `install`di nuovo per aggiornare le nuove dipendenze, quindi eseguirenpm `start`.
8. Per creare l'app, eseguinpm `build`. Carica il contenuto della directory di compilazione sul tuo provider di hosting.

> **Warning**
>
> L'app React ènonpronto per la produzione. È un esempio di implementazione di un'app perAmazon Kendraricerca.

Pagina di ricerca principale

La pagina di ricerca principale (`Search.tsx`) contiene tutti i componenti di ricerca di esempio. Include il componente della barra di ricerca per l'output, i componenti dei risultati per visualizzare la risposta diQueryAPI e un componente di impaginazione per sfogliare la risposta.

Componente per la ricerca

Il componente di ricerca fornisce una casella di testo per inserire il testo della query. IlonSearchla funzione è un hook che richiama la funzione principale in`Search.tsx`per laAmazon Kendra interrogazioneChiamata per l'utente.

Componente per i risultati

Il componente dei risultati mostra la risposta del`Query`API. I risultati sono mostrati in tre aree separate.

- Risposte suggerite: questi sono i migliori risultati restituiti da`Query`API. Contiene fino a tre risposte suggerite. Nella risposta, hanno il tipo di risultato`ANSWER`.
- Risposte alle domande frequenti: questi sono i risultati delle domande frequenti restituiti dalla risposta. Le domande frequenti vengono aggiunte all'indice separatamente. Nella risposta, hanno il tipo`QUESTION_ANSWER`. Per ulteriori informazioni, consulta la paginaDomande e risposte.
- Documenti consigliati: si tratta di documenti aggiuntivi cheAmazon Kendraritorna nella risposta. Nella risposta del`Query`API, hanno il tipo`DOCUMENT`.

I componenti dei risultati condividono un set di componenti per funzionalità come evidenziazione, titoli, link e altro. I componenti condivisi devono essere presenti affinché i componenti dei risultati funzionino.

Componente Facets

Il componente sfaccettature elenca le sfaccettature disponibili nei risultati della ricerca. Ogni sfaccettatura classifica la risposta in base a una dimensione specifica, ad esempio l'autore. Puoi affinare la ricerca a un aspetto specifico scegliendone uno dall'elenco.

Dopo aver selezionato un facet, il componente chiama`Query`con un filtro di attributi che limita la ricerca ai documenti che corrispondono al facet.

componente di impaginazione

Il componente di impaginazione consente di visualizzare i risultati della ricerca dal`Query`API in più pagine. Chiama il`Query`API con`PageSize`e`PageNumber`parametri per ottenere una pagina specifica di risultati.

Creazione di un'esperienza di ricerca senza codice

Puoi creare e distribuire unAmazon Kendraapplicazione di ricerca senza la necessità di alcun codice front-end.Amazon Kendra Generatore di esperienzeti aiuta a creare e distribuire un'applicazione di ricerca completamente funzionale in pochi clic, in modo da poter iniziare subito a cercare. Puoi personalizzare la tua pagina di ricerca e ottimizzare la ricerca per adattare l'esperienza alle esigenze degli utenti.Amazon Kendragenera un URL endpoint unico e completamente ospitato della pagina di ricerca per iniziare a cercare documenti e domande frequenti. Puoi creare rapidamente una bozza della tua esperienza di ricerca e condividerla con altri.

Per personalizzare la ricerca, utilizzi il modello di esperienza di ricerca disponibile nel generatore. Puoi invitare altre persone a collaborare alla creazione della tua esperienza di ricerca o valutare i risultati della ricerca per ottimizzarli. Una volta che l'esperienza di ricerca è pronta per consentire agli utenti di iniziare la ricerca, è sufficiente condividere l'URL sicuro dell'endpoint.

Come funziona il motore di ricerca Experience Builder

Il processo complessivo di creazione di un'esperienza di ricerca è il seguente:

1. Puoi creare la tua esperienza di ricerca assegnandole un nome, una descrizione e scegliendo le fonti di dati che desideri utilizzare per la tua esperienza di ricerca.
2. Puoi configurare l'elenco di utenti e gruppi inAWS IAM Identity Centere poi assegna loro i diritti di accesso alla tua esperienza di ricerca. Includi te stesso come proprietario dell'esperienza. Per ulteriori informazioni, consulta the section called “Fornire l'accesso alla pagina di ricerca”.
3. Si apre laAmazon KendraExperience Builder per progettare e ottimizzare la tua pagina di ricerca. Puoi condividere l'URL dell'endpoint della tua esperienza di ricerca con altri a cui assegnare diritti di accesso propri per la modifica o per la visualizzazione della ricerca.

Chiamate il`CreateExperience`API per creare e configurare la tua esperienza di ricerca. Se usi la console, seleziona il tuo indice e poi selezionaEsperienzenel menu di navigazione per configurare la tua esperienza.

Progetta e ottimizza la tua esperienza di ricerca

Dopo aver creato e configurato l'esperienza di ricerca, apri l'esperienza di ricerca utilizzando un URL dell'endpoint per iniziare a personalizzare la ricerca in qualità di proprietario con diritti di accesso editoriali. Digiti la query nella casella di ricerca, quindi personalizza la ricerca utilizzando le opzioni di modifica sul pannello laterale per vedere come si applicano alla tua pagina. Quando sei pronto per la pubblicazione, consultaPubblica. Puoi anche passare daPassa alla visualizzazione in diretta, per visualizzare l'ultima versione pubblicata della pagina di ricerca, ePassa alla modalità di costruzione, per modificare o personalizzare la pagina di ricerca.

Di seguito sono riportati i modi in cui è possibile personalizzare l'esperienza di ricerca.

Filtro

Aggiungi una ricerca sfaccettata o filtra in base agli attributi del documento. Ciò include gli attributi personalizzati. Puoi aggiungere un filtro utilizzando i tuoi campi di metadati configurati. Ad esempio, per eseguire una ricerca sfaccettata per ogni categoria di città, utilizza un`_category`attributo di documento personalizzato che contiene tutte le categorie di città.

Risposta suggerita

Aggiungi risposte generate dall'apprendimento automatico alle domande degli utenti. Per esempio«Quanto è difficile questo corso?».Amazon Kendrasa recuperare il testo più pertinente in tutti i documenti che si riferiscono alla difficoltà di un corso e suggerire la risposta più pertinente.

Domande frequenti

Aggiungi un documento di domande frequenti per fornire risposte alle domande frequenti. Per esempio«Quante ore occorrono per completare questo corso?».Amazon Kendrapuò utilizzare il documento FAQ contenente la risposta a questa domanda e fornire la risposta corretta.

Ordina

Aggiungi l'ordinamento dei risultati di ricerca in modo che gli utenti possano organizzare i risultati per pertinenza, ora di creazione, ora dell'ultimo aggiornamento e altri criteri di ordinamento.

Documenti di

Configura la modalità di visualizzazione dei documenti o dei risultati della ricerca nella pagina di ricerca. È possibile configurare il numero di risultati da visualizzare sulla pagina, includere

l'impaginazione come i numeri di pagina, attivare un pulsante di feedback degli utenti e disporre la modalità di visualizzazione dei campi dei metadati dei documenti nei risultati di ricerca.

Linguaggio

Seleziona una lingua per filtrare i risultati della ricerca o i documenti nella lingua selezionata.

Casella di ricerca

Configura la dimensione e il testo segnaposto della casella di ricerca, oltre a consentire suggerimenti di query.

Ottimizzazione della rilevanza

Aggiungete il potenziamento dei campi di metadati dei documenti per attribuire maggiore importanza a questi campi quando gli utenti cercano documenti. Puoi aggiungere un peso che inizia da 1 e aumenta gradualmente fino a 10. Puoi potenziare i tipi di campo di testo, data e numerici. Ad esempio, per dare`_last_updated_ate_created_at`più peso o importanza rispetto agli altri campi, attribuisci a questi campi un peso compreso tra 1 e 10, a seconda della loro importanza. Puoi applicare diverse configurazioni di ottimizzazione della pertinenza per ogni applicazione o esperienza di ricerca.

Fornire l'accesso alla pagina di ricerca

L'accesso alla tua esperienza di ricerca avviene tramite IAM Identity Center. Quando configuri la tua esperienza di ricerca, concedi ad altre persone elencate nella directory del tuo Identity Center l'accesso al tuoAmazon Kendrapagina di ricerca. Ricevono un'e-mail che li invita ad accedere utilizzando le proprie credenziali in IAM Identity Center per accedere alla pagina di ricerca. È necessario configurare IAM Identity Center a livello di organizzazione o titolare dell'account inAWS Organizations. Per ulteriori informazioni su la configurazione di IAM Identity Center, consultaGuida per l'utente.

Attivi le identità utente in IAM Identity Center con la tua esperienza di ricerca e assegnaleVisualizzatoreoProprietarioautorizzazioni di accesso tramite l'API o la console.

- Visualizzatore: È autorizzato a inviare domande, ricevere risposte suggerite pertinenti alla ricerca e contribuire con il proprio feedback aAmazon Kendrain modo da continuare a migliorare la ricerca.
- Proprietario: È autorizzato a personalizzare il design della pagina di ricerca, ottimizzare la ricerca e utilizzare l'applicazione di ricerca comeVisualizzatore. La disabilitazione dell'accesso ai visualizzatori nella console non è attualmente supportata.

Per assegnare ad altre persone l'accesso alla tua esperienza di ricerca, devi prima attivare le identità utente in IAM Identity Center conAmazon Kendraesperienza utilizzando ilExperienceConfigurationoggetto. Specificate il nome del campo che contiene gli identificatori degli utenti, come il nome utente o l'indirizzo e-mail. Quindi concedi al tuo elenco di utenti l'accesso alla tua esperienza di ricerca utilizzando ilAssociateEntitiesToExperienceAPI e definisci le relative autorizzazioni comeVisualizzatoreoProprietarioutilizzando ilAssociatePersonasToEntitiesAPI. Si specifica ogni utente o gruppo utilizzando ilEntityConfigurationoggetto e se tale utente o gruppo è unVisualizzatoreoProprietarioutilizzando ilEntityPersonaConfiguratonoggetto.

Per assegnare ad altre persone l'accesso alla tua esperienza di ricerca utilizzando la console, devi prima creare un'esperienza e confermare la tua identità e il fatto di esserne il proprietario. Quindi puoi assegnare altri utenti o gruppi come visualizzatori o proprietari. Nella console, seleziona l'indice, quindiEsperienzenel menu di navigazione. Dopo aver creato la tua esperienza, puoi selezionarla dall'elenco. Vai aGestione degli accessiper assegnare utenti o gruppi come visualizzatori o proprietari.

Configurazione di un'esperienza di ricerca

Di seguito è riportato un esempio di configurazione o creazione di un'esperienza di ricerca.

Console

Per la creazione diAmazon Kendraesperienza di ricerca

1. Nel riquadro di navigazione a sinistra, sottoIndici, selezionaEsperienzee quindi selezionaCrea un'esperienza.
2. SulConfigura l'esperienzapagina, inserisci un nome e una descrizione per la esperienza, scegli le fonti di contenuti e scegli il ruolo IAM per la tua esperienza. Per ulteriori informazioni sui ruoli IAM, consultaRuoli IAM perAmazon Kendraesperienze.
3. SulConferma la tua identità da un elenco dell'Identity Centerpagina, seleziona il tuo ID utente, ad esempio la tua email. Se non disponi di una directory Identity Center, inserisci semplicemente il tuo nome completo e l'email per creare una directory Identity Center. Ciò include te come utente dell'esperienza e ti assegna automaticamente i diritti di accesso del proprietario.
4. SulScrivi una recensione per aprire Experience Builderpagina, consulta i dettagli di configurazioneCrea esperienza e apri Experience Builderper iniziare a modificare la pagina di ricerca.

CLI

Per la creazione diAmazon Kendraesperienza

```
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

Per la creazione diAmazon Kendraesperienza

```
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

Per creare un Amazon Kendra

```
package com.amazonaws.kendra;

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

```
import software.amazon.awssdk.services.kendra.model.DescribeExperienceResponse;
import software.amazon.awssdk.services.kendra.model.ExperienceStatus;


public class CreateExperienceExample {

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

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

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

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

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

```
        String experienceEndpoints = createExperienceResponse.endpoints();

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

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

Regolazione della capacità

Amazon Kendra fornisce risorse per l'indice in unità di capacità. Ogni unità di capacità fornisce risorse aggiuntive per l'indice. Esistono unità di capacità separate per l'archiviazione dei documenti e per le interrogazioni. È possibile aggiungere unità di capacità solo agli indici Amazon Kendra Enterprise Edition. Non è possibile aggiungere capacità a un indice Developer Edition.

Un'unità di capacità di archiviazione dei documenti fornisce il seguente spazio di archiviazione aggiuntivo per l'indice.

- 100.000 documenti o 30 GB di spazio di archiviazione.

Un'unità di capacità di interrogazione fornisce le seguenti interrogazioni aggiuntive per l'indice.

- 0,1 query al secondo o circa 8.000 query al giorno.

Ogni indice ha una capacità di base pari a 1 unità di capacità (30 GB di storage e 0,1 query al secondo). È previsto un costo aggiuntivo per ogni unità di capacità aggiuntiva. Per informazioni dettagliate, consulta Prezzi di Amazon Kendra.

È possibile aggiungere fino a 100 unità di capacità extra alle risorse di storage e interrogare un indice. Se hai bisogno di più unità, contatta semplicemente l'assistenza.

È possibile regolare la capacità delle unità fino a 5 volte al giorno in base alle proprie esigenze di utilizzo. Non è possibile ridurre la capacità di archiviazione dei documenti al di sotto del numero di documenti archiviati nell'indice. Ad esempio, se stai archiviando 150.000 documenti, non puoi ridurre la capacità di archiviazione al di sotto di 1 unità aggiuntiva.

Puoi visualizzare le risorse utilizzate da un indice nella console selezionando il nome dell'indice per aprire le impostazioni dell'indice e altre informazioni oppure puoi utilizzare l'DescribeIndexAPI.

Amazon Kendra restituisce eccezioni anche quando si supera la capacità di un indice. Si ottiene un `ServiceQuotaExceededException` quando la dimensione totale estratta di tutti i documenti supera il limite di un indice. Si ottiene un valore `InvalidRequest` per ogni documento quando il numero di documenti supera il limite di un indice. Si ottiene un `ThrottlingException` quando il numero di interrogazioni al secondo supera il limite. Per ulteriori informazioni sui limiti, consulta Quotas for. Amazon Kendra

Le interrogazioni accumulate dureranno fino a 24 ore.

Capacità di visualizzazione

Visualizza le risorse utilizzate dall'indice con la Amazon Kendra console selezionando il nome dell'indice per accedere ai dettagli. La console fornisce anche grafici di utilizzo che consentono di determinare la capacità di storage e di interrogazione utilizzata dall'indice. È possibile utilizzare queste informazioni per pianificare quando aggiungere capacità aggiuntiva.

Per visualizzare l'archiviazione dei documenti e le query, usa (console)

1. Accedere AWS Management Console e aprire la Amazon Kendra console all'indirizzo https://console.aws.amazon.com/kendra/home.
2. Dall'elenco degli indici, scegli l'indice a cui desideri accedere.
3. Scorri fino alla sezione delle impostazioni per visualizzare l'attuale capacità totale di archiviazione dei documenti e la capacità di interrogazione.

Per visualizzare la capacità utilizzando l' Amazon Kendra API, utilizza il `CapacityUnits` parametro nell'DescribeIndexAPI.

Aggiungere e rimuovere capacità

Se hai bisogno di capacità aggiuntiva per l'indice, puoi aggiungerla utilizzando la console o l' Amazon Kendra API.

Per aggiungere o rimuovere la capacità di archiviazione o di interrogazione (console)

1. Accedi AWS Management Console e apri la Amazon Kendra console all'indirizzo https://console.aws.amazon.com/kendra/home.
2. Dall'elenco degli indici, scegli l'indice a cui desideri accedere.
3. Seleziona Modifica o seleziona Modifica dal menu a discesa Azioni.
4. Seleziona Avanti per accedere alla pagina dei dettagli del provisioning.
5. Aggiungi o rimuovi unità di capacità di archiviazione dei documenti e/o di interrogazione.
6. Continua a selezionare Avanti per andare alla pagina di revisione, quindi seleziona Aggiorna per salvare le modifiche.

Dopo aver aggiornato la capacità dell'indice, possono essere necessari alcuni minuti prima che le modifiche abbiano effetto.

Per aggiungere o rimuovere capacità utilizzando l' Amazon Kendra API, utilizza il `CapacityUnits` parametro nell'UpdateIndexAPI.

Amazon Kendra Capacità di classificazione intelligente

Un'unità di capacità fornisce le seguenti richieste di rescore aggiuntive al secondo per un piano di esecuzione di rescore. Un piano di esecuzione di rescore è una risorsa utilizzata per fornire l'API Rescore.

- 0,01 richieste al secondo.

Ogni piano di esecuzione di rescore ha una capacità di base pari a 1 unità di capacità (0,01 richieste al secondo). È previsto un costo aggiuntivo per ogni unità di capacità aggiuntiva. Per informazioni dettagliate, consulta Prezzi di Amazon Kendra.

È possibile aggiungere fino a 1000 unità di capacità extra per un piano di esecuzione di rescore. Se hai bisogno di più unità, contatta semplicemente l'assistenza.

Capacità di interrogazione e suggerimenti

Quando si utilizzano i suggerimenti di query, esiste una capacità di query di base di 2,5 GetQuerySuggestionschiamate al secondo. La `GetQuerySuggestions` capacità è cinque volte la capacità di interrogazione fornita per un indice o la capacità di base di 2,5 chiamate al secondo, a seconda di quale sia il valore maggiore. Ad esempio, la capacità di base per un indice è di 0,1 query al secondo e la capacità di `GetQuerySuggestions` ha una base di 2,5 chiamate al secondo. Se aggiungi altre 0,1 query al secondo a un totale di 0,2 query al secondo per un indice, la capacità di `GetQuerySuggestions` è di 2,5 chiamate al secondo (superiore a cinque volte 0,2 query al secondo).

Amazon Kendra capacità di esperienza

Capacità di esperienza di ricerca

Amazon Kendra inizia a rallentare, `QueryQuerySuggestions`, `SubmitFeedback` la tua Amazon Kendra esperienza a 15 richieste al secondo e 40 richieste al secondo in caso di query bursting. Per un indice con più di 150 unità di capacità di interrogazione, questi limiti sono ancora validi.

Ad esempio, le unità di capacità di query per l'indice sono 150, quindi la tua applicazione di esperienza di ricerca può gestire 15 richieste al secondo. Tuttavia, se passassi a 200 unità di capacità di query, la tua app per l'esperienza di ricerca continuerebbe a gestire solo 15 richieste al secondo. Se limiti l'indice a 100 unità di capacità di query, la tua app per l'esperienza di ricerca gestirà solo 10 richieste al secondo.

Scoppio di query adattive

Amazon Kendra ha una capacità di base prevista di 1 unità di capacità di interrogazione. È possibile utilizzare fino a 8.000 query al giorno con un throughput minimo di 0,1 query al secondo (per unità di capacità di query). Le query accumulate dureranno fino a 24 ore e possono gestire picchi di traffico. La quantità di burst consentita varia perché dipende dal carico del cluster in un dato momento. Fornisci un numero sufficiente di unità di capacità di interrogazione per gestire i livelli di carico di picco.

Un approccio adattivo alla gestione di picchi di traffico imprevisti oltre il throughput assegnato è l'adaptive query Amazon Kendra bursting integrato. L'Adaptive Query Bursting è disponibile nell'Enterprise Edition di. Amazon Kendra

L'Adaptive Query Bursting è una funzionalità integrata che consente di applicare la capacità di interrogazione inutilizzata per gestire il traffico imprevisto. Amazon Kendra accumula le query inutilizzate alla frequenza di query preimpostate al secondo, ogni secondo, fino al numero massimo di query che hai fornito per l'indice. Amazon Kendra Queste query accumulate vengono utilizzate per traffico imprevisto superiore alla capacità allocata. Le prestazioni ottimali dell'adaptive query bursting possono variare in base a diversi fattori, quali la dimensione totale dell'indice, la complessità delle query, l'accumulo di query non utilizzate e il carico complessivo dell'indice. Si consiglia di eseguire test di carico personalizzati per misurare con precisione la capacità di bursting.

Nozioni di base

Questa sezione mostra come creare un'origine dati e aggiungere i documenti a un Amazon Kendra indice. Vengono fornite istruzioni per la AWS consoleAWS CLI, un programma Python che utilizza e un programma Java che utilizza il. AWS SDK for Python (Boto3) AWS SDK for Java

Argomenti

Prerequisiti

I passaggi seguenti sono i prerequisiti per gli esercizi iniziali. I passaggi mostrano come configurare il tuo account, creare un IAM ruolo che Amazon Kendra autorizzi a effettuare chiamate per tuo conto e indicizzare i documenti da un Amazon S3 bucket. Un bucket S3 viene utilizzato come esempio, ma puoi utilizzare altre fonti di dati che lo supportano. Amazon Kendra Vedi Fonti di dati.

Registrarsi per creare un Account AWS

Se non disponi di un Account AWS, completa la procedura seguente per crearne uno.

Per registrarsi a un Account AWS

1. Apri la pagina all'indirizzo https://portal.aws.amazon.com/billing/signup.
2. Segui le istruzioni online.

   Nel corso della procedura di registrazione riceverai una telefonata, durante la quale sarà necessario inserire un codice di verifica attraverso la tastiera del telefono.

Durante la registrazione di un Account AWS, viene creato un Utente root dell'account AWS. L'utente root dispone dell'accesso a tutte le risorse e tutti i Servizi AWSnell'account. Come best practice di sicurezza, assegna l'accesso amministrativo a un utente amministrativo e utilizza solo l'utente root per eseguire attività che richiedono l'accesso di un utente root.

Al termine del processo di registrazione, riceverai un'e-mail di conferma da AWS. È possibile visualizzare l'attività corrente dell'account e gestire l'account in qualsiasi momento accedendo all'indirizzo https://aws.amazon.com/ e selezionando Il mio account.

Creazione di un utente amministratore

Dopo esserti registratoAccount AWS, proteggi Utente root dell'account AWSAWS IAM Identity Center, abilita e crea un utente amministrativo in modo da non utilizzare l'utente root per le attività quotidiane.

Protezione dell'Utente root dell'account AWS

1. Accedi alla AWS Management Console come proprietario dell'account scegliendo Utente root e immettendo l'indirizzo email del Account AWS. Nella pagina successiva, inserisci la password.

   Per informazioni sull'accesso utilizzando un utente root, consulta la pagina Accesso come utente root della Guida per l'utente di Accedi ad AWS.
2. Abilita l'autenticazione a più fattori (MFA) per l'utente root.

   Per ricevere istruzioni, consulta Abilitazione di un dispositivo MFA virtuale per l'utente root dell'Account AWS (console) nella Guida per l'utente IAM.

Creazione di un utente amministratore

1. Abilita IAM Identity Center.

   Per istruzioni, consulta Enabling AWS IAM Identity Center nella Guida AWS IAM Identity Center per l'utente.
2. In IAM Identity Center, concedi l'accesso amministrativo a un utente amministrativo.

   Per un tutorial sull'utilizzo di IAM Identity Center directory come fonte di identità, consulta Configurare l'accesso utente con le impostazioni predefinite IAM Identity Center directory nella Guida per l'AWS IAM Identity Centerutente.

Accesso come utente amministratore

- Per accedere con l'utente IAM Identity Center, utilizza l'URL di accesso che è stato inviato al tuo indirizzo e-mail quando hai creato l'utente IAM Identity Center.

  Per informazioni sull'accesso utilizzando un utente IAM Identity Center, consulta Accedere al portale di accesso AWS nella Guida per l'utente Accedi ad AWS.

- Se utilizzi un bucket S3 contenente documenti da testareAmazon Kendra, crea un bucket S3 nella stessa regione che stai utilizzando. Amazon Kendra Per istruzioni, consulta Creazione e configurazione di un bucket S3 nella Guida per l'utente di Amazon Simple Storage Service.

  Carica i tuoi documenti nel tuo bucket S3. Per istruzioni, consulta Caricamento, download e gestione di oggetti nella Guida per l'utente di Amazon Simple Storage Service.

  Se utilizzi un'altra fonte di dati, devi disporre di un sito attivo e delle credenziali per connetterti all'origine dati.

Se utilizzi la console per iniziare, inizia conGuida introduttiva alla Amazon Kendra console.

Amazon Kendrarisorse:AWS CLI, SDK, console

Sono necessarie alcune autorizzazioni se utilizzi la CLI, l'SDK o la console.

Per utilizzarlo Amazon Kendra per la CLI, l'SDK o la console, devi disporre delle autorizzazioni necessarie per creare e gestire risorse Amazon Kendra per tuo conto. A seconda del caso d'uso, queste autorizzazioni includono l'accesso all'Amazon KendraAPI stessa, AWS KMS keys se desideri crittografare i dati tramite una directory CMK personalizzata, Identity Center se desideri integrare o creare un'esperienza di AWS IAM Identity Center ricerca. Per un elenco completo delle autorizzazioni per diversi casi d'uso, consulta i ruoli. IAM

Innanzitutto, devi assegnare le seguenti autorizzazioni al tuo utente IAM.

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

In secondo luogo, se utilizzi la CLI o l'SDK, devi anche creare un IAM ruolo e una policy per l'accesso. Amazon CloudWatch Logs Se si utilizza la console, non è necessario creare un IAM ruolo e una politica a tale scopo. Lo crei come parte della procedura della console.

Per creare un IAM ruolo e una politica per l'AWS CLISDK che consentano di accedere Amazon KendraAmazon CloudWatch Logs a.

1. Accedi a AWS Management Console e apri la console IAM all'indirizzo https://console.aws.amazon.com/iam/.
2. Dal menu a sinistra, scegli Politiche, quindi scegli Crea politica.
3. Scegli JSON e sostituisci la politica predefinita con la seguente:

```
{
    "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. Scegli Esamina la policy.
5. Assegna un nome alla politica "KendraPolicyForGettingStartedIndex" e quindi scegli Crea politica.
6. Dal menu a sinistra, scegli Ruoli, quindi scegli Crea ruolo.
7. Scegli Un altro AWS account, quindi digita l'ID del tuo account in ID account. Scegli Successivo: Autorizzazioni.
8. Scegli la politica che hai creato sopra, quindi scegli Avanti: Tag
9. Non aggiungere alcun tag. Seleziona Successivo: Revisione.
10. Assegna un nome al ruolo "KendraRoleForGettingStartedIndex" e quindi scegli Crea ruolo.
11. Trova il ruolo che hai appena creato. Scegli il nome del ruolo per aprire il riepilogo. Scegli Relazioni di fiducia, quindi scegli Modifica relazione di fiducia.
12. Sostituisci la relazione di fiducia esistente con la seguente:

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

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

13. Scegliere Update trust Policy (Aggiorna policy di attendibilità).

In terzo luogo, se utilizzi an Amazon S3 per archiviare i tuoi documenti o utilizzi S3 per eseguire dei testAmazon Kendra, devi anche creare un IAM ruolo e una policy per accedere al tuo bucket. Se utilizzi un'altra fonte di dati, consulta i IAMruoli per le fonti di dati.

Per creare un IAM ruolo e una politica che consentano di Amazon Kendra accedere e indicizzare il tuo Amazon S3 bucket.

1. Accedi a AWS Management Console e apri la console IAM all'indirizzo https://console.aws.amazon.com/iam/.
2. Dal menu a sinistra, scegli Politiche, quindi scegli Crea politica.
3. Scegli JSON e sostituisci la politica predefinita con la seguente:

```
{
    "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. Scegli Esamina la policy.
5. Assegna un nome alla politica KendraPolicyForGettingStartedDataSource "" e quindi scegli Crea politica.
6. Dal menu a sinistra, scegli Ruoli, quindi scegli Crea ruolo.
7. Scegli Un altro AWS account, quindi digita l'ID del tuo account in ID account. Scegli Successivo: Autorizzazioni.
8. Scegli la politica che hai creato sopra, quindi scegli Avanti: Tag
9. Non aggiungere alcun tag. Seleziona Successivo: Revisione.
10. Assegna un nome al ruolo KendraRoleForGettingStartedDataSource "", quindi scegli Crea ruolo.
11. Trova il ruolo che hai appena creato. Scegli il nome del ruolo per aprire il riepilogo. Scegli Relazioni di fiducia, quindi scegli Modifica relazione di fiducia.
12. Sostituisci la relazione di fiducia esistente con la seguente:

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

```
}
```

13. Scegliere Update trust Policy (Aggiorna policy di attendibilità).

A seconda di come desideri utilizzare l'Amazon KendraAPI, esegui una delle seguenti operazioni.

- Nozioni di base (AWS CLI)
- Nozioni di base (AWS SDK for Java)
- Nozioni di base (AWS SDK for Python (Boto3))

Guida introduttiva alla Amazon Kendra console

Le procedure seguenti mostrano come creare e testare un Amazon Kendra indice utilizzando la AWS console. Nelle procedure si creano un indice e un'origine dati per un indice. Infine, testate il vostro indice effettuando una richiesta di ricerca.

Fase 1: Creare un indice (console)

1. Accedi alla console di AWS gestione e apri la Amazon Kendra console all'indirizzo https://console.aws.amazon.com/kendra/.
2. Seleziona Crea indice nella sezione Indici.
3. Nella pagina Specificare i dettagli dell'indice, assegna un nome e una descrizione all'indice.
4. In IAMRuolo, scegli Crea un nuovo ruolo, quindi assegna un nome al ruolo. Il IAM ruolo avrà il prefisso "AmazonKendra-».
5. Lascia tutti gli altri campi ai valori predefiniti. Seleziona Avanti.
6. Nella pagina Configura il controllo dell'accesso utente, scegli Avanti.
7. Nella pagina dei dettagli del provisioning, scegli Developer edition.
8. Scegli Crea per creare il tuo indice.
9. Attendi la creazione dell'indice. Amazon Kendrafornisce l'hardware per l'indice. Questa operazione può richiedere del tempo.

Passaggio 2: aggiungere un'origine dati a un indice (console)

1. Visualizza le fonti di dati disponibili a cui Amazon Kendra connetterti e indicizzare i tuoi documenti.

2. Nel riquadro di navigazione, seleziona Origini dati, quindi seleziona Aggiungi origine dati per l'origine dati scelta.
3. Segui i passaggi per configurare l'origine dati.

Passaggio 3: Per cercare un indice (console)

1. Nel riquadro di navigazione, scegli l'opzione per cercare nell'indice.
2. Inserisci un termine di ricerca appropriato per il tuo indice. Vengono visualizzati i risultati principali e i risultati principali del documento.

Nozioni di base (AWS CLI)

La procedura seguente mostra come creare un Amazon Kendra indice utilizzandoAWS CLI. La procedura crea un'origine dati, un indice, ed esegue una query sull'indice.

Per creare un Amazon Kendra indice (CLI)

1. Esegui il. Prerequisiti
2. Immettete il seguente comando per creare un indice.

```
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. Amazon KendraAttendi la creazione dell'indice. Controlla lo stato di avanzamento usando il seguente comando. Quando il campo dello stato è`ACTIVE`, vai al passaggio successivo.

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

4. Al prompt dei comandi, inserisci il seguente comando per creare un'origine dati.

```
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"}}'
```

Se ti connetti alla tua fonte di dati utilizzando uno schema modello, configura lo schema del modello.

```
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. La creazione dell'origine dati richiederà Amazon Kendra un po' di tempo. Inserisci il seguente comando per verificare lo stato di avanzamento. Quando lo stato è`ACTIVE`, vai al passaggio successivo.

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

6. Immettere il seguente comando per sincronizzare la fonte di dati.

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

7. Amazon Kendraindicizzerà la tua fonte di dati. La quantità di tempo necessaria dipende dal numero di documenti. È possibile controllare lo stato del processo di sincronizzazione utilizzando il comando seguente. Quando lo stato è`ACTIVE`, vai al passaggio successivo.

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

8. Immettete il seguente comando per creare una query.

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

I risultati della ricerca vengono visualizzati in formato JSON.

Nozioni di base (AWS SDK for Python (Boto3))

Il seguente programma è un esempio di utilizzo Amazon Kendra in un programma Python. Il programma esegue le seguenti azioni:

1. Crea un nuovo indice utilizzando l'CreateIndexoperazione.
2. Attende il completamento della creazione dell'indice. Utilizza l'DescribeIndexoperazione per monitorare lo stato dell'indice.
3. Una volta che l'indice è attivo, crea una fonte di dati utilizzando l'CreateDataSourceoperazione.
4. Attende il completamento della creazione dell'origine dati. Utilizza l'DescribeDataSourceoperazione per monitorare lo stato della fonte di dati.
5. Quando l'origine dati è attiva, sincronizza l'indice con il contenuto dell'origine dati utilizzando l'StartDataSourceSyncJoboperazione.

```
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.")
```

Nozioni di base (AWS SDK for Java)

Il seguente programma è un esempio di utilizzo Amazon Kendra in un programma Java. Il programma esegue le seguenti azioni:

1. Crea un nuovo indice utilizzando l'CreateIndexoperazione.
2. Attende il completamento della creazione dell'indice. Utilizza l'DescribeIndexoperazione per monitorare lo stato dell'indice.
3. Una volta che l'indice è attivo, crea una fonte di dati utilizzando l'CreateDataSourceoperazione.
4. Attende il completamento della creazione dell'origine dati. Utilizza l'DescribeDataSourceoperazione per monitorare lo stato della fonte di dati.
5. Quando l'origine dati è attiva, sincronizza l'indice con il contenuto dell'origine dati utilizzando l'StartDataSourceSyncJoboperazione.

```
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");
    }
}
```

Guida introduttiva a un'origine Amazon S3 dati (console)

Puoi utilizzare la Amazon Kendra console per iniziare a utilizzare un Amazon S3 bucket come archivio dati. Quando si utilizza la console, si specificano tutte le informazioni di connessione necessarie per indicizzare il contenuto del bucket. Per ulteriori informazioni, consulta Amazon S3.

Utilizza la procedura seguente per creare un'origine dati bucket S3 di base utilizzando la configurazione predefinita. La procedura presuppone che sia stato creato un indice seguendo i passaggi del passaggio 1 diGuida introduttiva alla Amazon Kendra console.

Per creare un'origine dati del bucket S3 utilizzando la console Amazon Kendra

1. Accedi AWS Management Console e apri la Amazon Kendra console all'indirizzo https://console.aws.amazon.com/kendra/home.
2. Dall'elenco degli indici, scegli l'indice a cui desideri aggiungere l'origine dati.
3. Scegli Aggiungi fonti di dati.
4. Dall'elenco dei connettori delle sorgenti dati, scegli Amazon S3.
5. Nella pagina Definisci attributi, assegna un nome alla fonte di dati e, facoltativamente, una descrizione. Lascia vuoto il campo Tag. Seleziona Next (Successivo) per continuare.

6. Nel campo Inserisci la posizione della sorgente dati, inserisci il nome del bucket S3 che contiene i tuoi documenti. Puoi inserire il nome direttamente oppure puoi cercarlo scegliendo Sfoglia. Il bucket deve trovarsi nella stessa regione dell'indice.
7. Nel IAMruolo scegli Crea un nuovo ruolo e quindi digita un nome di ruolo. Per ulteriori informazioni, consulta IAMi ruoli per le fonti di Amazon S3 dati.
8. Nella sezione Imposta la pianificazione delle esecuzioni di sincronizzazione, scegli Esegui su richiesta.
9. Seleziona Next (Successivo) per continuare.
10. Nella pagina Rivedi e crea, controlla i dettagli della tua fonte di dati S3. Se desideri apportare modifiche, scegli il pulsante Modifica accanto all'elemento che desideri modificare. Quando sei soddisfatto delle tue scelte, scegli Crea per creare la tua fonte dati S3.

Dopo aver scelto Crea, Amazon Kendra inizia a creare l'origine dati. La creazione dell'origine dati può richiedere diversi minuti. Al termine, lo stato dell'origine dati cambia da Creazione a Attiva.

Dopo aver creato l'origine dati, è necessario sincronizzare l'Amazon Kendraindice con l'origine dati. Scegli Sincronizza ora per avviare il processo di sincronizzazione. La sincronizzazione dell'origine dati può richiedere da alcuni minuti a diverse ore, a seconda del numero e delle dimensioni dei documenti.

Guida introduttiva a un'origine dati del database MySQL (console)

Puoi usare la Amazon Kendra console per iniziare a utilizzare un database MySQL come fonte di dati. Quando usi la console, specifichi le informazioni di connessione necessarie per indicizzare il contenuto di un database MySQL. Per ulteriori informazioni, consulta Using a database data source (Utilizzo di un'origine dati del database).

Devi prima creare un database MySQL, quindi puoi creare una fonte di dati per il database.

Utilizzare la procedura seguente per creare un database MySQL di base. La procedura presuppone che sia già stato creato un indice dopo il passaggio 1 diGuida introduttiva alla Amazon Kendra console.

Per creare un database MySQL

1. Accedere alla AWS Management Console e aprire la console Amazon RDS all'indirizzo https://console.aws.amazon.com/rds/.

2. Dal riquadro di navigazione, scegli Gruppi di sottoreti, quindi scegli Crea gruppo di sottorete DB.
3. Assegna un nome al gruppo e scegli il tuo Virtual Private Cloud (VPC). Per ulteriori informazioni sulla configurazione di un VPC, vedere Configurazione Amazon Kendra per l'utilizzo di un VPC.
4. Aggiungi le sottoreti private del tuo VPC. Le tue sottoreti private sono quelle che non sono connesse al tuo NAT. Seleziona Create (Crea).
5. Dal riquadro di navigazione, scegli Database e quindi scegli Crea database.
6. Utilizzate i seguenti parametri per creare il database. Lascia tutti gli altri parametri ai valori predefiniti.
   - Opzioni del motore —MySQL
   - Modelli: livello gratuito
   - Impostazioni credenziali: inserisci e conferma una password
   - In Connettività, scegli Configurazione di connettività aggiuntiva. Effettua le seguenti scelte.
     - Gruppo di sottoreti: scegli il gruppo di sottoreti creato nel passaggio 4.
     - Gruppo di sicurezza VPC: scegli il gruppo che contiene le regole in entrata e in uscita che hai creato nel tuo VPC. Ad esempio, **`DataSourceSecurityGroup`**. Per ulteriori informazioni sulla configurazione di un VPC, vedere Configurazione Amazon Kendra per l'utilizzo di un VPC.
   - In Configurazione aggiuntiva, imposta il nome del database iniziale su**`content`**.
7. Scegliere Crea database.
8. Dall'elenco dei database, scegli il tuo nuovo database. Prendi nota dell'endpoint del database.
9. Dopo aver creato il database, è necessario creare una tabella per contenere i documenti. La creazione di una tabella non rientra nell'ambito di queste istruzioni. Quando crei la tua tabella, tieni presente quanto segue:
   - Nome del database— **`content`**
   - Nome della tabella— **`documents`**
   - Colonne: **`IDTitle`**,**`Body`**, e**`LastUpdate`**. Se lo desideri, puoi includere colonne aggiuntive.

Ora che hai creato il tuo database MySQL, puoi creare una fonte di dati per il database.

Per creare un'origine dati MySQL

1. Accedi AWS Management Console e apri la Amazon Kendra console all'indirizzo https://console.aws.amazon.com/kendra/home.
2. Nel riquadro di navigazione, scegli Indici, quindi scegli il tuo indice.
3. Scegli Aggiungi fonti di dati, quindi scegli Amazon RDS.
4. Digita un nome e una descrizione per l'origine dati, quindi scegli Avanti.
5. Scegli MySQL.
6. In Accesso alla connessione, inserisci le seguenti informazioni:
   - Endpoint: l'endpoint del database creato in precedenza.
   - Porta: il numero di porta per il database. Per MySQL, l'impostazione predefinita è 3306.
   - Tipo di autenticazione: scegli Nuovo.
   - Nuovo nome contenitore segreto: un nome per il Secrets Manager contenitore per le credenziali del database.
   - Nome utente: il nome di un utente con accesso amministrativo al database.
   - Password: la password per l'utente, quindi scegli Salva autenticazione.
   - Nome del database —**`content`**.
   - Nome della tabella —**`documents`**.
   - Ruolo IAM: scegli Crea un nuovo ruolo, quindi digita un nome per il ruolo.
7. Nella configurazione della colonna, inserisci quanto segue:
   - Nome della colonna ID del documento — **`ID`**
   - Nome della colonna del titolo del documento: **`Title`**
   - Nome della colonna di dati del documento — **`Body`**
8. In Rilevamento delle modifiche alla colonna, inserisci quanto segue:
   - Cambia le colonne di rilevamento — **`LastUpdate`**
9. In Configura VPC e gruppo di sicurezza, fornisci quanto segue:
   - In Virtual Private Cloud (VPC), scegli il tuo VPC.
   - In Subnet, scegli le sottoreti private che hai creato nel tuo VPC.

- Nei gruppi di sicurezza VPC, scegli il gruppo di sicurezza che contiene le regole in entrata e in uscita che hai creato nel tuo VPC per i database MySQL. Ad esempio, **`DataSourceSecurityGroup`**.

10. In Imposta la pianificazione dell'esecuzione sincronizzata, scegli Esegui su richiesta, quindi scegli Avanti.
11. In Mappatura dei campi della sorgente dati, scegli Avanti.
12. Controlla la configurazione della tua fonte di dati per assicurarti che sia corretta. Quando sei sicuro che tutto sia corretto, scegli Crea.

Guida introduttiva a un'origine di AWS IAM Identity Center identità (console)

Una fonte di AWS IAM Identity Center identità contiene informazioni sui tuoi utenti e gruppi. Ciò è utile per configurare il filtro contestuale degli utenti, in cui Amazon Kendra filtra i risultati di ricerca per diversi utenti in base all'accesso dell'utente o del relativo gruppo ai documenti.

Per creare una fonte di identità IAM Identity Center, devi attivare IAM Identity Center e creare un'organizzazione in AWS Organizations. Quando attivi IAM Identity Center e crei un'organizzazione per la prima volta, per impostazione predefinita viene utilizzata automaticamente la directory Identity Center come origine dell'identità. Puoi passare ad Active Directory (gestito o autogestito da Amazon) o a un provider di identità esterno come fonte di identità. A tal fine, devi seguire le linee guida corrette: consulta Modifica della fonte di identità di IAM Identity Center. Puoi avere una sola fonte di identità per organizzazione.

Affinché agli utenti e ai gruppi vengano assegnati diversi livelli di accesso ai documenti, è necessario includere gli utenti e i gruppi nell'elenco di controllo degli accessi quando si inseriscono documenti nell'indice. Ciò consente agli utenti e ai gruppi di cercare documenti Amazon Kendra in base al loro livello di accesso. Quando si effettua una query, l'ID utente deve corrispondere esattamente al nome utente in IAM Identity Center.

È inoltre necessario concedere le autorizzazioni necessarie per utilizzare IAM Identity Center con Amazon Kendra. Per ulteriori informazioni, consulta IAM i ruoli per IAM Identity Center.

Per configurare una fonte di identità IAM Identity Center

1. Apri la console IAM Identity Center.
2. Scegli Abilita IAM Identity Center, quindi scegli Crea AWS organizzazione.

La directory Identity Center viene creata per impostazione predefinita e ti viene inviata un'e-mail per verificare l'indirizzo e-mail associato all'organizzazione.

3. Per aggiungere un gruppo all' AWS organizzazione, nel riquadro di navigazione, scegli Gruppi.
4. Nella pagina Gruppi, scegli Crea gruppo e inserisci un nome e una descrizione del gruppo nella finestra di dialogo. Scegli Crea.
5. Per aggiungere un utente alle tue Organizzazioni, nel riquadro di navigazione, scegli Utenti.
6. Nella pagina Users (Utenti), scegliere Add user (Aggiungi utente). In User details (Dettagli utente) specificare tutti i campi obbligatori. In Password scegliere Send an email to the user (Invia un messaggio e-mail all'utente). Seleziona Avanti.
7. Per aggiungere un utente a un gruppo, scegli Gruppi e seleziona un gruppo.
8. Nella pagina Dettagli, in Membri del gruppo, scegli Aggiungi utente.
9. Nella pagina Aggiungi utenti al gruppo, seleziona l'utente che desideri aggiungere come membro del gruppo. Puoi selezionare più utenti da aggiungere a un gruppo.
10. Per sincronizzare l'elenco di utenti e gruppi con IAM Identity Center, modifica la fonte di identità in Active Directory o provider di identità esterno.

    La directory Identity Center è la fonte di identità predefinita e richiede l'aggiunta manuale di utenti e gruppi utilizzando questa fonte se non disponi di un elenco personale gestito da un provider. Per modificare la fonte di identità, devi seguire le linee guida corrette in merito: consulta Modifica della fonte di identità di IAM Identity Center.

> **Note**
>
> Se utilizzi Active Directory o un provider di identità esterno come fonte di identità, devi mappare gli indirizzi e-mail degli utenti ai nomi utente di IAM Identity Center quando specifichi il protocollo System for Cross-domain Identity Management (SCIM). Per ulteriori informazioni, consulta la guida IAM Identity Center su SCIM per abilitare IAM Identity Center.

Dopo aver configurato la fonte di identità IAM Identity Center, puoi attivarla nella console quando crei o modifichi l'indice. Vai a Controllo dell'accesso degli utenti nelle impostazioni dell'indice e modifica le impostazioni per consentire il recupero delle informazioni sui gruppi di utenti da IAM Identity Center.

Puoi anche attivare IAM Identity Center utilizzando l'UserGroupResolutionConfigurationoggetto. Fornisci l'`UserGroupResolutionMode`annuncio `AWS_SSO` e crei un IAM ruolo che autorizza

a chiamare`sso:ListDirectoryAssociations`,`sso-directory:SearchUsers`,`sso-directory:ListGroupsForUser`,`sso-directory:DescribeGroups`.

> **Warning**
>
> Amazon Kendra attualmente non supporta l'utilizzo `UserGroupResolutionConfiguration` con un account di membro AWS dell'organizzazione per la fonte di identità IAM Identity Center. È necessario creare l'indice nell'account di gestione dell'organizzazione per poterlo utilizzare`UserGroupResolutionConfiguration`.

Di seguito è riportata una panoramica su come configurare un'origine dati con `UserGroupResolutionConfiguration` un controllo dell'accesso degli utenti per filtrare i risultati della ricerca in base al contesto dell'utente. Ciò presuppone che tu abbia già creato un indice e un IAM ruolo per gli indici. Crei un indice e fornisci il IAM ruolo utilizzando l'API. CreateIndex

Configurazione di un'origine dati con **`UserGroupResolutionConfiguration`** filtro del contesto utente

1. Crea un IAM ruolo che dia il permesso di accedere alla tua fonte di identità IAM Identity Center.
2. Configura `UserGroupResolutionConfiguration`impostando la modalità su `AWS_SSO` e chiama UpdateIndexper aggiornare l'indice per utilizzare IAM Identity Center.
3. Se desideri utilizzare il controllo dell'accesso utente basato su token per filtrare i risultati della ricerca in base al contesto dell'utente, imposta su `USER_TOKEN` Quando UserContextPolicychiami. `UpdateIndex` Altrimenti, Amazon Kendra esegue la scansione dell'elenco di controllo degli accessi per ciascuno dei tuoi documenti per la maggior parte dei connettori di origini dati. Puoi anche filtrare i risultati della ricerca in base al contesto dell'utente nell'API Query fornendo informazioni su utenti e gruppi in. `UserContext` È inoltre possibile mappare gli utenti ai rispettivi gruppi PutPrincipalMappingin modo da fornire l'ID utente solo quando si invia la query.
4. Crea un IAM ruolo che autorizzi l'accesso alla tua fonte di dati.
5. Configura la tua fonte di dati. È necessario fornire le informazioni di connessione richieste per connettersi alla fonte dati.
6. Crea una fonte di dati utilizzando l'CreateDataSourceAPI. Fornisci l'`DataSourceConfiguration`oggetto, che include `TemplateConfiguration` l'ID dell'indice,

il IAM ruolo dell'origine dati, il tipo di origine dati, e assegna un nome all'origine dati. Puoi anche aggiornare la tua fonte di dati.

Modifica della fonte di identità di IAM Identity Center

> **Warning**
>
> La modifica della fonte di identità nelle impostazioni di IAM Identity Center potrebbe influire sulla conservazione delle informazioni su utenti e gruppi. Per eseguire questa operazione in sicurezza, si consiglia di consultare la sezione Considerazioni per la modifica della fonte di identità. Quando si modifica la fonte di identità, viene generato un nuovo ID di origine dell'identità. Verifica di utilizzare l'ID corretto prima di attivare la `AWS_SSO` modalità UserGroupResolutionConfiguration.

Per modificare la fonte di identità di IAM Identity Center

1. Apri la console IAM Identity Center>.
2. Seleziona Impostazioni.
3. Nella pagina Impostazioni, in Identity source, scegli Cambia.
4. Nella pagina Cambia origine identità, seleziona la tua fonte di identità preferita, quindi scegli Avanti.

Creazione di un indice

Puoi creare un indice utilizzando la console o chiamando l'CreateIndexAPI. Puoi usare AWS Command Line Interface (AWS CLI) o SDK con l'API. Dopo aver creato l'indice, puoi aggiungere documenti direttamente all'indice o da una fonte di dati.

Per creare un indice, devi fornire l'Amazon Resource Name (ARN) di un ruolo AWS Identity and Access Management (IAM) a cui gli indici possano accedere. CloudWatch Per ulteriori informazioni, consulta i IAM ruoli per gli indici.

Le schede seguenti forniscono una procedura per creare un indice utilizzando gli ed esempi di codice per l' AWS Management Consoleutilizzo degli SDK AWS CLI Python e Java.

Console

Per creare un indice

1. Accedere alla console AWS di gestione e aprirla Amazon Kendra all'indirizzo https://console.aws.amazon.com/kendra/.
2. Seleziona Crea indice nella sezione Indici.
3. In Specificare i dettagli dell'indice, assegna un nome e una descrizione all'indice.
4. Nel IAM ruolo fornisci un IAM ruolo. Per trovare un ruolo, scegli tra i ruoli del tuo account che contengono la parola «kendra» o inserisci il nome di un altro ruolo. Per ulteriori informazioni sulle autorizzazioni richieste dal ruolo, consulta IAM ruoli per gli indici.
5. Seleziona Avanti.
6. Nella pagina Configura il controllo dell'accesso utente, scegli Avanti. Puoi aggiornare l'indice per utilizzare i token per il controllo degli accessi dopo aver creato un indice. Per ulteriori informazioni, vedere Controllo dell'accesso ai documenti.
7. Nella pagina dei dettagli del provisioning, scegli Crea.
8. La creazione dell'indice potrebbe richiedere del tempo. Controlla l'elenco degli indici per controllare lo stato di avanzamento della creazione dell'indice. Quando lo stato dell'indice è impostato su`ACTIVE`, l'indice è pronto per l'uso.

AWS CLI

Per creare un indice

1. Utilizzate il seguente comando per creare un indice. `role-arn`Deve essere l'Amazon Resource Name (ARN) di un IAM ruolo in grado di eseguire Amazon Kendra azioni. Per ulteriori informazioni, consulta IAM i ruoli.

   Il comando è formattato per Linux e macOS. Se utilizzate Windows, sostituite il carattere di continuazione della riga Unix (\) con un accento circonflesso (^).

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

2. La creazione dell'indice potrebbe richiedere del tempo. Per verificare lo stato dell'indice, utilizzate l'ID dell'indice restituito da `create-index` con il comando seguente. Quando lo stato dell'indice è`ACTIVE`, l'indice è pronto per l'uso.

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

Python

Per creare un indice

- Fornite i valori per le seguenti variabili nell'esempio di codice che segue:
  - `description`—Una descrizione dell'indice che stai creando. Si tratta di un'opzione facoltativa.
  - `index_name`—Il nome dell'indice che stai creando.
  - `role_arn`—Amazon Resource Name (ARN) di un ruolo che può Amazon Kendra eseguire API. Per ulteriori informazioni, consulta i ruoli. IAM

  ```
  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

Per creare un indice

- Fornite i valori per le seguenti variabili nell'esempio di codice che segue:
  - `description`—Una descrizione dell'indice che stai creando. Si tratta di un'opzione facoltativa.
  - `index_name`—Il nome dell'indice che stai creando.
  - `role_arn`—Amazon Resource Name (ARN) di un ruolo che può Amazon Kendra eseguire API. Per ulteriori informazioni, consulta i ruoli. IAM

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

Dopo aver creato l'indice, puoi aggiungervi dei documenti. Puoi aggiungerli direttamente o creare una fonte di dati che aggiorni l'indice a intervalli regolari.

Argomenti

- Aggiungere documenti direttamente a un indice con caricamento in batch
- Aggiungere domande frequenti (FAQ) a un indice
- Creazione di campi di documento personalizzati
- Controllo dell'accesso degli utenti ai documenti con token

Aggiungere documenti direttamente a un indice con caricamento in batch

Puoi aggiungere documenti direttamente a un indice utilizzando l'BatchPutDocumentAPI. Non puoi aggiungere documenti direttamente utilizzando la console. Se usi la console, ti connetti a una fonte di dati per aggiungere documenti all'indice. I documenti possono essere aggiunti da un bucket S3 o forniti come dati binari. Per un elenco dei tipi di documenti supportati da, Amazon Kendra vedi Tipi di documenti.

L'aggiunta di documenti a un indice utilizzando `BatchPutDocument` è un'operazione asincrona. Dopo aver chiamato l'`BatchPutDocument`API, la usi per monitorare lo BatchGetDocumentStatusstato di avanzamento dell'indicizzazione dei documenti. Quando chiami l'`BatchGetDocumentStatus`API con un elenco di ID di documento, restituisce lo stato del documento. Quando lo stato del documento è `INDEXED` o`FAILED`, l'elaborazione del documento è completa. Quando lo stato è`FAILED`, l'`BatchGetDocumentStatus`API restituisce il motivo per cui il documento non può essere indicizzato.

Se desideri modificare i campi o gli attributi dei metadati del contenuto e del documento durante il processo di inserimento del documento, consulta Custom Document Enrichment. Amazon Kendra Se desideri utilizzare un'origine dati personalizzata, ogni documento inviato tramite l'`BatchPutDocument`API richiede un ID dell'origine dati e un ID di esecuzione come attributi o campi. Per ulteriori informazioni, consulta Attributi obbligatori per le origini dati personalizzate.

> **Note**
>
> L'ID di ogni documento deve essere univoco per indice. Non puoi creare un'origine dati per indicizzare i tuoi documenti con i relativi ID univoci e quindi utilizzare l'`BatchPutDocument`API per indicizzare gli stessi documenti o viceversa. Puoi eliminare un'origine dati e quindi utilizzare l'`BatchPutDocument`API per indicizzare gli stessi documenti o viceversa. L'utilizzo delle `BatchDeleteDocument` API `BatchPutDocument` and in combinazione con un connettore di origine Amazon Kendra dati per lo stesso set di documenti potrebbe causare incongruenze con i dati. Consigliamo invece di utilizzare il connettore di origine dati Amazon Kendra personalizzato.

I seguenti documenti della guida per sviluppatori mostrano come aggiungere documenti direttamente a un indice.

Argomenti

Aggiungere documenti con l' BatchPutDocumentAPI

L'esempio seguente aggiunge un blob di testo a un indice BatchPutDocumentchiamando. Puoi utilizzare l'`BatchPutDocument`API per aggiungere documenti direttamente all'indice. Per un elenco dei tipi di documenti supportati da, Amazon Kendra vedi Tipi di documenti.

Per un esempio di creazione di un indice utilizzando gli AWS CLI e SDK, consulta Creazione di un indice. Per configurare la CLI e gli SDK, consulta Configurazione. Amazon Kendra

> **Note**
>
> I file aggiunti all'indice devono essere in un flusso di byte con codifica UTF-8.

Negli esempi seguenti, il testo con codifica UTF-8 viene aggiunto all'indice.

CLI

Nel AWS Command Line Interface, utilizzare il comando seguente. Il comando è formattato per Linux e macOS. Se utilizzate Windows, sostituite il carattere di continuazione della riga Unix (\) con un accento circonflesso (^).

```
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));
    }
}
```

Aggiungere documenti da un bucket S3

Puoi aggiungere documenti direttamente all'indice da un Amazon S3 bucket utilizzando l'API. BatchPutDocument Puoi aggiungere fino a 10 documenti nella stessa chiamata. Quando utilizzi un bucket S3, devi fornire un IAM ruolo con l'autorizzazione ad accedere al bucket che contiene i tuoi documenti. Specificate il ruolo nel parametro. `RoleArn`

L'utilizzo dell'BatchPutDocumentAPI per aggiungere documenti da un Amazon S3 bucket è un'operazione una tantum. Per mantenere un indice sincronizzato con il contenuto di un bucket, crea una fonte di dati. Amazon S3 Per ulteriori informazioni, consulta la fonte Amazon S3 dei dati.

Per un esempio di creazione di un indice utilizzando gli AWS CLI e gli SDK, consulta Creazione di un indice. Per configurare la CLI e gli SDK, consulta Configurazione. Amazon Kendra Per informazioni sulla creazione di un bucket S3, consulta la documentazione. Amazon Simple Storage Service

Nell'esempio seguente, due documenti di Microsoft Word vengono aggiunti all'indice utilizzando l'`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));
    }
}
```

Aggiungere domande frequenti (FAQ) a un indice

Puoi aggiungere domande frequenti (FAQ) direttamente all'indice utilizzando la console o l'CreateFaqAPI. L'aggiunta di domande frequenti a un indice è un'operazione asincrona. I dati delle domande frequenti vengono inseriti in un file archiviato in un bucket. Amazon Simple Storage Service Puoi usare file CSV o JSON come input per le tue FAQ:

- CSV di base: un file CSV in cui ogni riga contiene una domanda, una risposta e un URI di origine opzionale.
- CSV personalizzato: un file CSV che contiene domande, risposte e intestazioni per campi/attributi personalizzati che puoi utilizzare per suddividere, visualizzare o ordinare le risposte alle domande frequenti. Puoi anche definire campi di controllo dell'accesso per limitare la risposta alle domande frequenti a determinati utenti e gruppi a cui è consentito visualizzare la risposta alle domande frequenti.
- JSON: un file JSON che contiene domande, risposte e campi/attributi personalizzati che puoi utilizzare per suddividere, visualizzare o ordinare le risposte alle domande frequenti. Puoi anche definire campi di controllo dell'accesso per limitare la risposta alle domande frequenti a determinati utenti e gruppi a cui è consentito visualizzare la risposta alle domande frequenti.

Ad esempio, quello che segue è un file CSV di base che fornisce risposte a domande sulle cliniche gratuite a Spokane, Washington USA e Mountain View, Missouri, USA.

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

> **Note**
>
> Il file FAQ deve essere un file con codifica UTF-8.

Argomenti

Creazione di campi indice per un file di domande frequenti

Quando utilizzi un file CSV o JSON personalizzato come input, puoi dichiarare campi personalizzati per le tue domande frequenti. Ad esempio, puoi creare un campo personalizzato che assegna a ogni domanda FAQ un reparto aziendale. Quando le domande frequenti vengono restituite in una risposta, puoi utilizzare il reparto come sfaccettatura per restringere la ricerca solo a «Risorse Umane» o «Finanze», ad esempio.

Un campo personalizzato deve essere mappato a un campo indice. Nella console, si utilizza la pagina di definizione di Facet per creare un campo indice. Quando si utilizza l'API, è necessario innanzitutto creare un campo indice utilizzando l'UpdateIndexAPI.

Il tipo di campo/attributo nel file FAQ deve corrispondere al tipo del campo indice associato. Ad esempio, il campo «Dipartimento» è un campo `STRING_LIST` di tipo. Pertanto, è necessario fornire i valori per il campo department come elenco di stringhe nel file delle domande frequenti. Puoi controllare il tipo di campi indice utilizzando la pagina di definizione di Facet nella console o utilizzando l'DescribeIndexAPI.

Quando crei un campo indice mappato a un attributo personalizzato, puoi contrassegnarlo come visualizzabile, sfaccettato o ordinabile. Non puoi rendere ricercabile un attributo personalizzato.

Oltre agli attributi personalizzati, puoi anche utilizzare i campi Amazon Kendra riservati o comuni in un file CSV o JSON personalizzato. Per ulteriori informazioni, consulta Attributi o campi del documento.

File CSV di base

Usa un file CSV di base quando desideri utilizzare una struttura semplice per le domande frequenti. In un file CSV di base, ogni riga contiene due o tre campi: una domanda, una risposta e un URI di origine opzionale che rimanda a un documento con ulteriori informazioni.

Il contenuto del file deve essere conforme al formato comune RFC 4180 e al tipo MIME per i file CSV (Comma-Separated Values).

Di seguito è riportato un file di domande frequenti nel formato CSV di base.

```
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 personalizzato

Utilizza un file CSV personalizzato per aggiungere campi/attributi personalizzati alle domande frequenti. Per un file CSV personalizzato, usi una riga di intestazione nel file CSV per definire gli attributi aggiuntivi.

Il file CSV deve contenere i seguenti due campi obbligatori:

- `_question`—La domanda più frequente
- `_answer`—La risposta alla domanda più frequente

Il file può contenere sia campi Amazon Kendra riservati che campi personalizzati. Di seguito è riportato un esempio di file CSV personalizzato.

```
_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
```

Il contenuto del file personalizzato deve essere conforme al formato comune RFC 4180 e al tipo MIME per i file CSV (Comma-Separated Values).

Di seguito sono elencati i tipi di campi personalizzati:

- Data: valori di data e ora con codifica ISO 8601.

  Ad esempio, 2012-03-25T 12:30:10 + 01:00 è il formato data-ora ISO 8601 per il 25 marzo 2012 alle 12:30 (più 10 secondi) nel fuso orario dell'Europa centrale.
- `1234`Lunghi: numeri, ad esempio.
- String—Valori di tipo String. Se la stringa contiene virgole, racchiudi l'intero valore tra virgolette doppie («) (ad esempio,). `"custom attribute, and more"`
- Elenco stringhe: un elenco di valori di stringa. Elenca i valori in un elenco separato da virgole racchiuso tra virgolette («) (ad esempio,). `"item1, item2, item3"` Se l'elenco contiene solo una voce, è possibile omettere le virgolette (ad esempio,). `item1`

Un file CSV personalizzato può contenere campi di controllo dell'accesso degli utenti. Puoi utilizzare questi campi per limitare l'accesso alle domande frequenti a determinati utenti e gruppi. Per filtrare in base al contesto dell'utente, l'utente deve fornire informazioni sull'utente e sul gruppo nella query. In caso contrario, vengono restituite tutte le domande frequenti pertinenti. Per ulteriori informazioni, consulta Filtraggio del contesto utente.

Di seguito sono elencati i filtri contestuali utente per le domande frequenti:

- `_acl_user_allow`—Gli utenti inclusi nell'elenco consentito possono visualizzare le domande frequenti nella risposta alla query. Le domande frequenti non vengono restituite agli altri utenti.
- `_acl_user_deny`—Gli utenti nell'elenco degli utenti non autorizzati non possono visualizzare le domande frequenti nella risposta alla query. Le domande frequenti vengono restituite a tutti gli altri utenti quando sono pertinenti alla domanda.
- `_acl_group_allow`—Gli utenti che sono membri di un gruppo consentito possono visualizzare le domande frequenti nella risposta alla query. Le domande frequenti non vengono restituite agli utenti che sono membri di un altro gruppo.
- `_acl_group_deny`—Gli utenti che sono membri di un gruppo negato non possono visualizzare le domande frequenti nella risposta alla query. Le domande frequenti vengono restituite agli altri gruppi quando sono pertinenti alla query.

Fornisci i valori per gli elenchi di autorizzazione e rifiuto in elenchi separati da virgole racchiusi tra virgolette (ad esempio,). `"user1,user2,user3"` È possibile includere un utente o un gruppo in un elenco di utenti consentiti o in un elenco di utenti non autorizzati, ma non entrambi quando lo stesso

utente è autorizzato individualmente ma anche in un gruppo negato. Se includi un utente o un gruppo in entrambi, riceverai un errore.

Di seguito è riportato un esempio di file CSV personalizzato con informazioni sul contesto dell'utente.

```
_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

Puoi utilizzare un file JSON per fornire domande, risposte e campi per il tuo indice. Puoi aggiungere qualsiasi campo Amazon Kendra riservato o campo personalizzato alle domande frequenti.

Di seguito è riportato lo schema per il 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
    ]
}
```

Il seguente file JSON di esempio mostra due documenti di domande frequenti. Uno dei documenti contiene solo la domanda e la risposta richieste. L'altro documento include anche informazioni aggiuntive sul campo e sul contesto utente o sul controllo degli accessi.

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

Di seguito sono elencati i tipi di campi personalizzati:

- Data: un valore di stringa JSON con valori di data e ora codificati ISO 8601. Ad esempio, 2012-03-25T 12:30:10 + 01:00 è il formato data-ora ISO 8601 per il 25 marzo 2012 alle 12:30 (più 10 secondi) nel fuso orario dell'Europa centrale.
- Long: `1234` un valore numerico JSON, ad esempio.
- Stringa: un valore di stringa JSON (ad esempio,). `"custom attribute"`
- Elenco di stringhe: una matrice JSON di valori di stringa (ad esempio,). `["item1,item2,item3"]`

Un file JSON può contenere campi di controllo dell'accesso degli utenti. Puoi utilizzare questi campi per limitare l'accesso alle domande frequenti a determinati utenti e gruppi. Per filtrare in base al contesto dell'utente, l'utente deve fornire informazioni sull'utente e sul gruppo nella query. In caso contrario, vengono restituite tutte le domande frequenti pertinenti. Per ulteriori informazioni, consulta Filtraggio del contesto utente.

È possibile includere un utente o un gruppo in un elenco consentito o in un elenco negato, ma non entrambi se lo stesso utente è autorizzato individualmente, ma anche se lo stesso utente è negato al gruppo. Se includi un utente o un gruppo in entrambi, riceverai un errore.

Di seguito è riportato un esempio di inclusione del controllo dell'accesso degli utenti in una domanda frequente su JSON.

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

Utilizzo del file FAQ

Dopo aver archiviato il file di input delle FAQ in un bucket S3, usi la console o l'`CreateFaq`API per inserire le domande e le risposte nel tuo indice. Se desideri aggiornare una FAQ, elimina la FAQ e creala di nuovo. Utilizzi l'`DeleteFaq`API per eliminare una FAQ.

Devi fornire un IAM ruolo che abbia accesso al bucket S3 che contiene i tuoi file sorgente. Specificate il ruolo nella console o nel `RoleArn` parametro. Di seguito è riportato un esempio di aggiunta di un file di domande frequenti a un indice.

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 di domande frequenti in lingue diverse dall'inglese

Puoi indicizzare una FAQ in una lingua supportata. Amazon Kendra indicizza le domande frequenti in inglese per impostazione predefinita se non si specifica una lingua. È possibile specificare il codice della lingua quando si richiama l'CreateFaqoperazione oppure è possibile includere il codice della lingua per una FAQ nei metadati delle domande frequenti come campo. Se una FAQ non ha un codice di lingua nei metadati specificati in un campo di metadati, le domande frequenti vengono indicizzate utilizzando il codice della lingua specificato al momento della chiamata dell'operazione. `CreateFAQ` Per indicizzare un documento di domande frequenti in una lingua supportata nella console, vai su Domande frequenti e seleziona Aggiungi domande frequenti. Scegli una lingua dal menu a discesa Lingua.

Creazione di campi di documento personalizzati

Puoi creare attributi o campi personalizzati per i tuoi documenti nel tuo indice Amazon Kendra. Ad esempio, puoi creare un campo o un attributo personalizzato chiamato «Dipartimento» con i valori di «HR», «Sales» e «Manufacturing». Se mappi questi campi o attributi personalizzati al tuo indice Amazon Kendra, puoi utilizzarli per filtrare i risultati della ricerca e includere documenti in base all'attributo del dipartimento «HR», ad esempio.

Prima di poter utilizzare un campo o un attributo personalizzato, devi prima creare il campo nell'indice. Usa la console per modificare le mappature dei campi dell'origine dati per aggiungere un campo personalizzato o usa l'UpdateIndexAPI per creare il campo indice. Non è possibile modificare il tipo di dati del campo dopo averlo creato.

Per la maggior parte delle fonti di dati, i campi dell'origine dati esterna vengono mappati ai campi corrispondenti in Amazon Kendra. Per ulteriori informazioni, consulta la sezione Mappatura dei campi

di origine dei dati. Per le sorgenti dati S3, puoi creare campi o attributi personalizzati utilizzando un file di metadati JSON.

Puoi creare fino a 500 campi o attributi personalizzati.

Puoi anche utilizzare campi Amazon Kendra riservati o comuni. Per ulteriori informazioni, consulta Attributi o campi del documento.

Argomenti

Aggiornamento dei campi personalizzati del documento

Con l'`UpdateIndex`API, aggiungi campi o attributi personalizzati utilizzando il `DocumentMetadataConfigurationUpdates` parametro.

Il seguente esempio JSON utilizza `DocumentMetadataConfigurationUpdates` l'aggiunta di un campo chiamato «Dipartimento» all'indice.

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

Le seguenti sezioni includono esempi per aggiungere attributi o campi personalizzati utilizzando BatchPutDocumente per un'origine dati Amazon S3.

Argomenti

Aggiungere attributi o campi personalizzati con l'API BatchPutDocument

Quando utilizzi l'BatchPutDocumentAPI per aggiungere un documento all'indice, specifichi campi o attributi personalizzati come parte di`Attributes`. Puoi aggiungere più campi o attributi quando chiami l'API. Puoi creare fino a 500 campi o attributi personalizzati. L'esempio seguente è un campo o un attributo personalizzato che aggiunge «Dipartimento» a un documento.

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

Aggiungere attributi o campi personalizzati a un'origine Amazon S3 dati

Quando usi un bucket S3 come fonte di dati per il tuo indice, aggiungi metadati ai documenti con file di metadati complementari. I file JSON di metadati vengono inseriti in una struttura di directory parallela ai documenti. Per ulteriori informazioni, consulta Metadati dei documenti S3.

È possibile specificare campi o attributi personalizzati nella struttura `Attributes` JSON. È possibile creare fino a 500 campi o attributi personalizzati. Ad esempio, l'esempio seguente utilizza `Attributes` per definire tre campi o attributi personalizzati e un campo riservato.

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

I passaggi seguenti illustrano come aggiungere attributi personalizzati a un'origine dati Amazon S3.

Argomenti

- Passaggio 1: creare un indice Amazon Kendra
- Passaggio 2: aggiorna l'indice per aggiungere campi di documento personalizzati
- Fase 3: creare un'origine dati Amazon S3 e mappare i campi dell'origine dati su attributi personalizzati

Passaggio 1: creare un indice Amazon Kendra

Segui i passaggi indicati Creazione di un indice per creare il tuo indice Amazon Kendra.

Passaggio 2: aggiorna l'indice per aggiungere campi di documento personalizzati

Dopo aver creato un indice, aggiungete dei campi ad esso. La procedura seguente mostra come aggiungere campi a un indice utilizzando la console e la CLI.

Console

Per creare campi indice

1. Assicurati di aver creato un indice.
2. Quindi, dal menu di navigazione a sinistra, da Gestione dati, scegli Definizione delle sfaccettature.
3. Nella guida alle impostazioni dei campi Indice, da Campi indice, scegli Aggiungi campo per aggiungere campi personalizzati.
4. Nella finestra di dialogo Aggiungi campo indice, procedi come segue:
   - Nome campo: aggiungi un nome di campo.
   - Tipo di dati: seleziona il tipo di dati, che si tratti di stringa, elenco di stringhe o data.
   - Tipi di utilizzo: seleziona i tipi di utilizzo, che siano Facetable, Ricercabili, Visualizzabili e Ordinabili.

     Quindi, seleziona Aggiungi.

   Ripeti l'ultimo passaggio per tutti gli altri campi che desideri mappare.

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
        }
    }
...
]"
```

Fase 3: creare un'origine dati Amazon S3 e mappare i campi dell'origine dati su attributi personalizzati

Per creare un'origine dati Amazon S3 e mappare i campi su di essa, segui le istruzioni riportate in. Amazon S3

Se utilizzi l'API, usa l'`fieldMappings`attributo sotto `configuration` quando usi l'CreateDataSourceAPI.

Per una panoramica di come vengono mappati i campi delle sorgenti dati, consultaMappatura dei campi delle fonti di dati.

Controllo dell'accesso degli utenti ai documenti con token

Puoi controllare quali utenti o gruppi possono accedere a determinati documenti nel tuo indice o visualizzare determinati documenti nei loro risultati di ricerca. Questo si chiama filtraggio del contesto utente. È una sorta di ricerca personalizzata con il vantaggio di controllare l'accesso ai documenti. Ad esempio, non tutti i team che cercano informazioni nel portale aziendale devono accedere ai documenti aziendali top secret, né questi documenti sono pertinenti per tutti gli utenti. Solo utenti o gruppi di team specifici a cui è consentito l'accesso a documenti top secret dovrebbero visualizzare questi documenti nei risultati di ricerca.

Amazon Kendrasupporta il controllo degli accessi degli utenti basato su token utilizzando i seguenti tipi di token:

- ID aperto
- JWT con un segreto condiviso
- JWT con una chiave pubblica

- JSON

Amazon Kendraoffre una ricerca aziendale altamente sicura per le tue applicazioni di ricerca. I risultati della ricerca riflettono il modello di sicurezza della tua organizzazione. I clienti sono responsabili dell'autenticazione e dell'autorizzazione degli utenti ad accedere alla loro applicazione di ricerca. Al momento della ricerca,Amazon Kendrail servizio filtra i risultati della ricerca in base all'ID utente fornito dall'applicazione di ricerca del cliente e agli elenchi di controllo dell'accesso ai documenti (ACL) raccolti dalAmazon Kendraconnettori durante il periodo di indicizzazione/indicizzazione. I risultati della ricerca restituiscono URL che rimandano agli archivi dei documenti originali più brevi estratti. L'accesso al documento completo è ancora imposto dall'archivio originale.

Argomenti

Usare OpenID

Per configurare un Amazon Kendra indice per utilizzare un token OpenID per il controllo degli accessi, è necessario l'URL JWKS (JSON Web Key Set) del provider OpenID. Nella maggior parte dei casi l'URL JWKS ha il seguente formato (se segue OpenID Discovery). `https://domain-name/.well_known/jwks.json`

Gli esempi seguenti mostrano come utilizzare un token OpenID per il controllo dell'accesso degli utenti quando si crea un indice.

Console

1. Scegli Crea indice per iniziare a creare un nuovo indice.
2. Nella pagina Specificare i dettagli dell'indice, assegna un nome e una descrizione all'indice.
3. Per IAM il ruolo, seleziona un ruolo o seleziona Crea un nuovo ruolo e specifica un nome di ruolo per creare un nuovo ruolo. Il ruolo IAM avrà il prefisso "AmazonKendra-».
4. Lascia tutti gli altri campi ai valori predefiniti. Seleziona Successivo.
5. Nella pagina Configura il controllo dell'accesso utente, in Impostazioni di controllo degli accessi, scegli Sì per utilizzare i token per il controllo degli accessi.

6. In Configurazione token, selezionate OpenID come tipo di token.
7. Specificate l'URL di una chiave di firma. L'URL deve puntare a un set di chiavi Web JSON.
8. Facoltativo In Configurazione avanzata:
    a. Specificare un nome utente da utilizzare nel controllo ACL.
    b. Specificare uno o più gruppi da utilizzare nel controllo ACL.
    c. Specificare l'emittente che convaliderà l'emittente del token.
    d. Specificare gli ID client. È necessario specificare un'espressione regolare che corrisponda al pubblico nel JWT.
9. Nella pagina dei dettagli del provisioning, scegli Developer edition.
10. Scegli Crea per creare il tuo indice.
11. Attendi la creazione dell'indice. Amazon Kendra fornisce l'hardware per l'indice. Questa operazione può richiedere del tempo.

CLI

Per creare un indice AWS CLI utilizzando un file di input JSON, create innanzitutto un file JSON con i parametri desiderati:

```
{
    "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"
}
```

È possibile sovrascrivere i nomi dei campi utente e gruppo predefiniti. Il valore predefinito per `UserNameAttributeField` è «user». Il valore predefinito per `GroupAttributeField` è «groups».

Quindi, chiama `create-index` utilizzando il file di input. Ad esempio, se il nome del file JSON è`create-index-openid.json`, puoi utilizzare quanto segue:

```
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'
)
```

Utilizzo di un token Web JSON (JWT) con un segreto condiviso

Gli esempi seguenti mostrano come utilizzare JSON Web Token (JWT) con un token segreto condiviso per il controllo dell'accesso degli utenti quando si crea un indice.

Console

1. Scegli Crea indice per iniziare a creare un nuovo indice.
2. Nella pagina Specificare i dettagli dell'indice, assegna un nome e una descrizione all'indice.

3. Per il ruolo IAM, seleziona un ruolo o seleziona Crea un nuovo ruolo e specifica un nome di ruolo per creare un nuovo ruolo. Il IAM ruolo avrà il prefisso "AmazonKendra-».
4. Lascia tutti gli altri campi ai valori predefiniti. Seleziona Successivo.
5. Nella pagina Configura il controllo dell'accesso utente, in Impostazioni di controllo degli accessi, scegli Sì per utilizzare i token per il controllo degli accessi.
6. In Configurazione del token, seleziona JWT con segreto condiviso come tipo di token.
7. In Parametri per la firma del segreto condiviso, scegli il Tipo di segreto. Puoi utilizzare un segreto AWS Secrets Manager condiviso esistente o crearne uno nuovo.

   Per creare un nuovo segreto condiviso, scegli Nuovo e segui questi passaggi:

   a. In Nuovo AWS Secrets Manager segreto, specifica un nome segreto. Il prefisso `AmazonKendra-` verrà aggiunto quando si salva la chiave pubblica.
   b. Specificate un ID chiave. L'ID della chiave è un suggerimento che indica quale chiave è stata utilizzata per proteggere la firma web JSON del token.
   c. Scegli l'algoritmo di firma per il token. Questo è l'algoritmo crittografico utilizzato per proteggere il token ID. Per ulteriori informazioni su RSA, consulta Crittografia RSA.
   d. Specificare un segreto condiviso inserendo un segreto con codifica URL base64. Puoi anche selezionare Genera segreto per generare un segreto per te. Devi assicurarti che il segreto sia un segreto con codifica URL base64.
   e. (Facoltativo) Specificate quando il segreto condiviso è valido. È possibile specificare la data e l'ora in cui un segreto è valido, valido fino a o entrambi. Il segreto sarà valido nell'intervallo specificato.
   f. Seleziona Salva segreto per salvare il nuovo segreto.
8. (Facoltativo) In Configurazione avanzata:

   a. Specificate un nome utente da utilizzare nel controllo ACL.
   b. Specificare uno o più gruppi da utilizzare nel controllo ACL.
   c. Specificare l'emittente che convaliderà l'emittente del token.
   d. Specificare gli ID del reclamo. È necessario specificare un'espressione regolare che corrisponda al pubblico nel JWT.
9. Nella pagina dei dettagli del provisioning, scegli Developer edition.
10. Scegli Crea per creare il tuo indice.

11. Attendi la creazione dell'indice. Amazon Kendra fornisce l'hardware per l'indice. Questa operazione può richiedere del tempo.

CLI

Puoi usare il token JWT con un segreto condiviso all'interno di AWS Secrets Manager. Il segreto deve essere un segreto con codifica URL base64. È necessario l' Secrets Manager ARN e il Amazon Kendra ruolo deve avere accesso alla `GetSecretValue` Secrets Manager risorsa. Se stai crittografando la Secrets Manager risorsa con AWS KMS, il ruolo deve avere accesso anche all'azione di decrittografia.

Per creare un indice AWS CLI utilizzando un file di input JSON, create innanzitutto un file JSON con i parametri desiderati:

```
{
    "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"
}
```

È possibile sovrascrivere i nomi dei campi utente e gruppo predefiniti. Il valore predefinito per `UserNameAttributeField` è «user». Il valore predefinito per `GroupAttributeField` è «groups».

Quindi, chiama `create-index` utilizzando il file di input. Ad esempio, se il nome del file JSON è`create-index-openid.json`, puoi utilizzare quanto segue:

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

Il segreto deve avere il seguente formato in 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"
    }
  ]
}
```

Per ulteriori informazioni su JWT, vedere jwt.io.

Python

Puoi usare il token JWT con un segreto condiviso all'interno di. AWS Secrets Manager Il segreto deve essere un segreto con codifica URL base64. È necessario l' Secrets Manager ARN e il Amazon Kendra ruolo deve avere accesso alla `GetSecretValue` Secrets Manager risorsa. Se stai crittografando la Secrets Manager risorsa con AWS KMS, il ruolo deve avere accesso anche all'azione di decrittografia.

```
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'
)
```

Utilizzo di un token Web JSON (JWT) con una chiave pubblica

Gli esempi seguenti mostrano come utilizzare JSON Web Token (JWT) con una chiave pubblica per il controllo dell'accesso degli utenti quando si crea un indice. Per ulteriori informazioni su JWT, consulta jwt.io.

Console

1. Scegli Crea indice per iniziare a creare un nuovo indice.
2. Nella pagina Specificare i dettagli dell'indice, assegna un nome e una descrizione all'indice.
3. Per il ruolo IAM, seleziona un ruolo o seleziona Crea un nuovo ruolo e specifica un nome di ruolo per creare un nuovo ruolo. Il IAM ruolo avrà il prefisso "AmazonKendra-».
4. Lascia tutti gli altri campi ai valori predefiniti. Seleziona Successivo.
5. Nella pagina Configura il controllo dell'accesso utente, in Impostazioni di controllo degli accessi, scegli Sì per utilizzare i token per il controllo degli accessi.
6. In Configurazione del token, seleziona JWT con chiave pubblica come tipo di token.
7. In Parametri per la firma della chiave pubblica, scegli il tipo di segreto. Puoi usare un AWS Secrets Manager segreto esistente o crearne uno nuovo.

   Per creare un nuovo segreto, scegli Nuovo e segui questi passaggi:

   a. In Nuovo AWS Secrets Manager segreto, specifica un nome segreto. Il prefisso `AmazonKendra-` verrà aggiunto quando si salva la chiave pubblica.
   b. Specificate un ID chiave. L'ID della chiave è un suggerimento che indica quale chiave è stata utilizzata per proteggere la firma web JSON del token.
   c. Scegli l'algoritmo di firma per il token. Questo è l'algoritmo crittografico utilizzato per proteggere il token ID. Per ulteriori informazioni su RSA, consulta Crittografia RSA.
   d. In Attributi del certificato, specifica una catena di certificati opzionale. La catena di certificati è composta da un elenco di certificati. Inizia con il certificato di un server e termina con il certificato radice.

e. Facoltativo Specificare l'impronta digitale o l'impronta digitale. Dovrebbe essere l'hash di un certificato, calcolato su tutti i dati del certificato e sulla sua firma.

f. Specificare l'esponente. Questo è il valore esponenziale per la chiave pubblica RSA. È rappresentato come valore con codifica Base64urlUInt.

g. Specificare il modulo. Questo è il valore esponenziale per la chiave pubblica RSA. È rappresentato come valore con codifica Base64urlUInt.

h. Seleziona Salva chiave per salvare la nuova chiave.

8. Facoltativo In configurazione avanzata:

a. Specificare un nome utente da utilizzare nel controllo ACL.

b. Specificare uno o più gruppi da utilizzare nel controllo ACL.

c. Specificare l'emittente che convaliderà l'emittente del token.

d. Specificare gli ID client. È necessario specificare un'espressione regolare che corrisponda al pubblico nel JWT.

9. Nella pagina dei dettagli del provisioning, scegli Developer edition.

10. Scegli Crea per creare il tuo indice.

11. Attendi la creazione dell'indice. Amazon Kendra fornisce l'hardware per l'indice. Questa operazione può richiedere del tempo.

CLI

Puoi usare JWT con una chiave pubblica all'interno di un AWS Secrets Manager. È necessario l' Secrets Manager ARN e il Amazon Kendra ruolo deve avere accesso alla `GetSecretValue` Secrets Manager risorsa. Se stai crittografando la Secrets Manager risorsa con AWS KMS, il ruolo deve avere accesso anche all'azione di decrittografia.

Per creare un indice AWS CLI utilizzando un file di input JSON, create innanzitutto un file JSON con i parametri desiderati:

```
{
    "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"
}
```

È possibile sovrascrivere i nomi dei campi utente e gruppo predefiniti. Il valore predefinito per `UserNameAttributeField` è «user». Il valore predefinito per `GroupAttributeField` è «groups».

Quindi, chiama `create-index` utilizzando il file di input. Ad esempio, se il nome del file JSON è`create-index-openid.json`, puoi utilizzare quanto segue:

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

Il segreto deve avere il seguente formato in 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"
      ]
    }
  ]
}
```

Per ulteriori informazioni su JWT, vedere 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'
)
```

Utilizzo di JSON

Gli esempi seguenti mostrano come utilizzare JSON per il controllo degli accessi degli utenti quando si crea un indice.

> **Warning**
>
> Il token JSON è un payload non convalidato. Questo dovrebbe essere usato solo quando le richieste Amazon Kendra provengono da un server affidabile e mai da un browser.

Console

1. Scegli Crea indice per iniziare a creare un nuovo indice.
2. Nella pagina Specificare i dettagli dell'indice, assegna un nome e una descrizione all'indice.
3. Per IAM il ruolo, seleziona un ruolo o seleziona Crea un nuovo ruolo e specifica un nome di ruolo per creare un nuovo ruolo. Il IAM ruolo avrà il prefisso "AmazonKendra-».

4. Lascia tutti gli altri campi ai valori predefiniti. Seleziona Successivo.
5. Nella pagina Configura il controllo dell'accesso utente, in Impostazioni di controllo degli accessi, scegli Sì per utilizzare i token per il controllo degli accessi.
6. In Configurazione token, seleziona JSON come tipo di token.
7. Specificate un nome utente da utilizzare nel controllo ACL.
8. Specificare uno o più gruppi da utilizzare nel controllo ACL.
9. Seleziona Successivo.
10. Nella pagina dei dettagli del provisioning, scegli Developer edition.
11. Scegli Crea per creare il tuo indice.
12. Attendi la creazione dell'indice. Amazon Kendra fornisce l'hardware per l'indice. Questa operazione può richiedere del tempo.

CLI

Per creare un indice AWS CLI utilizzando un file di input JSON, create innanzitutto un file JSON con i parametri desiderati:

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

Quindi, chiama `create-index` utilizzando il file di input. Ad esempio, se il nome del file JSON è`create-index-openid.json`, puoi utilizzare quanto segue:

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

Se non utilizzi Open ID per AWS IAM Identity Center, puoi inviarci il token in formato JSON. In tal caso, è necessario specificare quale campo del token JSON contiene il nome utente e quale campo contiene i gruppi. I valori dei campi del gruppo devono essere un array di stringhe JSON. Ad esempio, se utilizzi SAML, il tuo token sarebbe simile al seguente:

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

`TokenConfiguration`Specificherebbe il nome utente e i nomi dei campi del gruppo:

```
{
    "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'
)
```

Creazione di un connettore di origine dati

Puoi creare un connettore di origine dati per Amazon Kendra connetterti e indicizzare i tuoi documenti. Amazon Kendra può connettersi a Microsoft SharePoint, Google Drive e molti altri provider. Quando crei un connettore di origine dati, fornisci Amazon Kendra le informazioni di configurazione necessarie per connetterti al tuo repository di origine. A differenza dell'aggiunta di documenti direttamente a un indice, puoi scansionare periodicamente la fonte di dati per aggiornare l'indice.

Ad esempio, supponiamo di avere un archivio di documenti fiscali archiviati in un Amazon S3 bucket. Di tanto in tanto, i documenti esistenti vengono modificati e nuovi documenti vengono aggiunti all'archivio. Se aggiungi il repository Amazon Kendra come origine dati, puoi mantenere aggiornato l'indice impostando sincronizzazioni periodiche tra l'origine dati e l'indice.

Puoi scegliere di aggiornare un indice manualmente utilizzando la console o l'API. StartDataSourceSyncJob Altrimenti, imposti una pianificazione per aggiornare un indice e sincronizzarlo con la tua fonte di dati.

Un indice può avere più di un'origine dati. Ogni fonte di dati può avere una propria pianificazione degli aggiornamenti. Ad esempio, è possibile aggiornare l'indice dei documenti di lavoro quotidianamente o anche ogni ora, aggiornando manualmente i documenti archiviati ogni volta che l'archivio cambia.

Se desiderate modificare i metadati o gli attributi e il contenuto del documento durante il processo di inserimento del documento, consultate Custom Document Enrichment. Amazon Kendra

> **Note**
>
> Ogni ID del documento deve essere unico per indice. Non puoi creare un'origine dati per indicizzare i tuoi documenti con i relativi ID univoci e quindi utilizzare l'`BatchPutDocument`API per indicizzare gli stessi documenti o viceversa. Puoi eliminare un'origine dati e quindi utilizzare l'`BatchPutDocument`API per indicizzare gli stessi documenti o viceversa. L'utilizzo delle `BatchDeleteDocument` API `BatchPutDocument` and in combinazione con un connettore di origine Amazon Kendra dati per lo stesso set di documenti potrebbe causare incongruenze con i dati. Consigliamo invece di utilizzare il connettore di origine dati Amazon Kendra personalizzato.

> **Note**
>
> I file aggiunti all'indice devono essere in un flusso di byte con codifica UTF-8. Per ulteriori informazioni sui documenti in, consultate Documenti. Amazon Kendra

Impostazione di una pianificazione degli aggiornamenti

Configura l'origine dati in modo che si aggiorni periodicamente con la console o utilizzando il `Schedule` parametro quando crei o aggiorni un'origine dati. Il contenuto del parametro è una stringa che contiene una stringa di pianificazione in `cron` formato o una stringa vuota per indicare che l'indice viene aggiornato su richiesta. Per il formato di un'espressione cron, consulta Schedule Expressions for Rules nella Guida per l'Amazon CloudWatch Events utente. Amazon Kendra supporta solo espressioni cron. Non supporta le espressioni di frequenza.

Impostazione di una lingua

Puoi indicizzare tutti i tuoi documenti in una fonte di dati in una lingua supportata. Quando chiami, specifichi il codice della lingua per tutti i tuoi documenti nella tua fonte di dati CreateDataSource. Se un documento non ha un codice di lingua specificato in un campo di metadati, il documento viene indicizzato utilizzando il codice della lingua specificato per tutti i documenti a livello di origine dati. Se non specifichi una lingua, Amazon Kendra indicizza i documenti in una fonte di dati in inglese per impostazione predefinita. Per ulteriori informazioni sulle lingue supportate, compresi i relativi codici, consulta Aggiungere documenti in lingue diverse dall'inglese.

Puoi indicizzare tutti i tuoi documenti in una fonte di dati in una lingua supportata utilizzando la console. Vai a Fonti dati e modifica la tua fonte di dati o Aggiungi origine dati se stai aggiungendo una nuova fonte di dati. Nella pagina Specificare i dettagli dell'origine dati, scegli una lingua dal menu a discesa Lingua. Seleziona Aggiorna o continua a inserire le informazioni di configurazione per connetterti alla tua fonte di dati.

Connettori per sorgenti dati

Questa sezione mostra come connettersi ai database e Amazon Kendra agli archivi di sorgenti dati supportati utilizzando Amazon Kendra in AWS Management Console e le Amazon Kendra API.

Argomenti

- Schemi di modelli di origini dati
- Adobe Experience Manager
- Alfresco
- Aurora (MySQL)
- Aurora (PostgreSQL)
- Amazon FSx (Finestre)
- Amazon FSx (NetApp SU TAP)
- Amazon RDS/Aurora
- Amazon RDS (Microsoft SQL Server)
- Amazon RDS (MySQL)
- Amazon RDS (Oracle)
- Amazon RDS (PostgreSQL)
- Amazon S3
- Amazon Kendra Web crawler
- Amazon WorkDocs
- Box (Cubo)
- Confluence
- Connettore sorgente dati personalizzato
- Dropbox
- Drupal
- GitHub
- Gmail
- Google Drive
- IBM DB2
- Jira
- Microsoft Exchange
- Microsoft OneDrive
- Microsoft SharePoint
- Microsoft SQL Server

- Microsoft Teams
- Microsoft Yammer
- MySQL
- Oracle Database
- PostgreSQL
- battuta
- Salesforce
- ServiceNow
- Slack
- Zendesk

Schemi di modelli di origini dati

Di seguito sono riportati gli schemi di modelli per le fonti di dati in cui sono supportati i modelli.

Argomenti

- Adobe Experience Managerschema del modello
- Amazon FSx schema del modello (Windows)
- Amazon FSx schema del modello (NetApp ONTAP)
- Alfrescoschema modello
- Aurora Schema del modello (MySQL)
- Aurora Schema del modello (PostgreSQL)
- Amazon RDS Schema del modello (Microsoft SQL Server)
- Amazon RDS Schema del modello (MySQL)
- Amazon RDS schema modello (Oracle)
- Amazon RDS Schema del modello (PostgreSQL)
- Amazon S3 schema modello
- Amazon Kendra Schema del modello Web Crawler
- Schema del modello Confluence
- Schema del modello Dropbox

- Schema del modello Drupal
- GitHub schema modello
- Schema del modello Gmail
- Schema del modello di Google Drive
- Schema del modello IBM DB2
- Schema del modello di Microsoft Exchange
- Schema OneDrive modello Microsoft
- Schema SharePoint modello Microsoft
- Schema del modello di Microsoft SQL Server
- Schema del modello Microsoft Teams
- Schema del modello di Microsoft Yammer
- Schema del modello MySQL
- Schema del modello di database Oracle
- Schema del modello PostgreSQL
- Schema del modello Salesforce
- ServiceNow schema modello
- Schema del modello Slack
- Schema del modello Zendesk

Adobe Experience Managerschema del modello

Includi un JSON che contiene lo schema dell'origine dati come parte dell'TemplateConfigurationoggetto. Fornisci l'URL dell'Adobe Experience Managerhost, il tipo di autenticazione e se utilizzi Adobe Experience Manager (AEM) come servizio cloud o AEM On-Premise come parte della configurazione della connessione o dei dettagli dell'endpoint del repository. Inoltre, specifica il tipo di origine dati`AEM`, un segreto per le credenziali di autenticazione e altre configurazioni necessarie. È quindi necessario specificare `TEMPLATE` come `Type` quando si chiama. CreateDataSource

Puoi utilizzare il modello fornito in questa guida per sviluppatori. Per ulteriori informazioni, consulta Adobe Experience ManagerSchema JSON.

La tabella seguente descrive i parametri dello schema AEM JSON.

Configurazione	Descrizione
Configurazione della connessione	Informazioni di configurazione per l'endpoint per l'origine dati.
repositoryEndpointMetadata	Le informazioni sull'endpoint per l'origine dati.
AEMUrl	L'URL dell'Adobe Experience Managerhost. Ad esempio, se utilizzi AEM On-Premise, includi il nome host e la porta:. https://hostname:port Oppure, se utilizzi AEM come servizio cloud, puoi utilizzare l'URL dell'autore:. https://author-xxxxxx-xxxxxxx.adobeaemcloud.com
authType	Il tipo di autenticazione che usi, se `Basic` o`OAuth2`.
deploymentType	Il tipo di Adobe Experience Manager quello che usi, o. `CLOUD` `ON_PREMISE`
Configurazioni del repository	Informazioni di configurazione per il contenuto dell'origine dati. Ad esempio, la configurazione di tipi specifici di contenuti e mappature dei campi.
• page • asset	Un elenco di oggetti che mappano gli attributi o i nomi dei campi delle Adobe Experience Manager pagine e delle risorse per Amazon Kendra indicizzare i nomi dei campi. Per ulteriori informazioni, consulta la sezione Mappatura dei campi di origine dei dati.
Proprietà aggiuntive	Opzioni di configurazione aggiuntive per i contenuti della fonte di dati.
timeZoneId	Se utilizzi AEM On-Premise e il fuso orario del server è diverso dal fuso orario del connettor e o dell'indice Amazon Kendra AEM, puoi

Configurazione	Descrizione
	specificare il fuso orario del server da allineare al connettore o all'indice AEM. Il fuso orario predefinito per AEM On-Premis e è il fuso orario del connettore o dell'indice AEM. Amazon Kendra Il fuso orario predefinito per AEM come servizio cloud è l'ora media di Greenwich.
• pageRootPaths • assetRootPaths	Un elenco di percorsi principali per pagine e risorse. Ad esempio, il percorso principale di una pagina potrebbe essere /content/sub e il percorso principale per una risorsa potrebbe essere /content/sub/asset1.
CrawlAssets	`true`per eseguire la scansione delle risorse.
Scansiona le pagine	`true`per eseguire la scansione delle pagine.
• pagePathInclusionSchemi • pageNameInclusionSchemi • assetPathInclusionSchemi • assetTypeInclusionSchemi • assetNameInclusionSchemi	Un elenco di modelli di espressioni regolari per includere determinate pagine e risorse nella fonte di Adobe Experience Manager dati. Le pagine e le risorse che corrispondono ai modelli sono incluse nell'indice. Le pagine e le risorse che non corrispondono ai modelli sono escluse dall'indice. Se una pagina o una risorsa corrisponde sia a un modello di inclusione che a uno di esclusione, il modello di esclusione ha la precedenza e il contenuto non è incluso nell'indice.

Configurazione	Descrizione
• pagePathExclusionSchemi • pageNameExclusionSchemi • assetPathExclusionSchemi • assetTypeInclusionSchemi • assetNameInclusionSchemi	Un elenco di modelli di espressioni regolari per escludere determinate pagine e risorse dalla fonte di Adobe Experience Manager dati. Le pagine e le risorse che corrispondono ai modelli sono escluse dall'indice. Le pagine e le risorse che non corrispondono ai modelli sono incluse nell'indice. Se una pagina o una risorsa corrisponde sia a un modello di inclusione che a uno di esclusione, il modello di esclusione ha la precedenza e il contenuto non è incluso nell'indice.
Componenti della pagina	Un elenco di nomi per i componenti specifici della pagina che desideri indicizzare.
contentFragmentVariations	Un elenco di nomi per le varianti specifiche salvate di Adobe Experience Manager Content Fragments che desiderate indicizzare.
tipo	Il tipo di origine dati. Specificare `AEM` come tipo di origine dati.
enableIdentityCrawler	`true`utilizzare il crawler Amazon Kendra di identità per sincronizzare le informazioni sull'identità/principali su utenti e gruppi con accesso a determinati documenti. Se il crawler di identità è disattivato, tutti i documenti possono essere ricercati pubblicamente. Se desideri utilizzare il controllo degli accessi per i tuoi documenti e il crawler di identità è disattivato, in alternativa puoi utilizzare l'PutPrincipalMappingAPI per caricare le informazioni di accesso di utenti e gruppi.

Configurazione	Descrizione
SyncMode	Specificate come Amazon Kendra aggiornar e l'indice quando il contenuto dell'origine dati cambia. Puoi scegliere tra: • `FORCED_FULL_CRAWL` per indicizzare nuovamente tutti i contenuti, sostituendo i contenuti esistenti ogni volta che l'origine dati si sincronizza con l'indice. • `FULL_CRAWL` per indicizzare solo i contenuti nuovi, modificati ed eliminati ogni volta che l'origine dati si sincronizza con l'indice. Amazon Kendra può utilizzare il meccanism o dell'origine dati per tenere traccia delle modifiche ai contenuti e indicizzare i contenuti modificati dall'ultima sincroniz zazione. • `CHANGE_LOG` per indicizzare solo contenuti nuovi e modificati ogni volta che l'origine dati si sincronizza con l'indice. Amazon Kendra può utilizzare il meccanismo dell'origine dati per tenere traccia delle modifiche ai contenuti e indicizzare i contenuti modificati dall'ultima sincronizzazione.
Segretario ARN	L'Amazon Resource Name (ARN) di un AWS Secrets Manager segreto che contiene le coppie chiave-valore necessarie per connettersi ad Adobe Experience Manager. Per informazi oni su queste coppie chiave-valore, consulta le istruzioni di connessione per Adobe Experience Manager.
version	La versione di questo modello attualmente supportata.

Adobe Experience ManagerSchema 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 schema del modello (Windows)

Includi un JSON che contiene lo schema dell'origine dati come parte dell'TemplateConfigurationoggetto. L'ID del file system viene fornito come parte della configurazione della connessione o dei dettagli dell'endpoint del repository. È inoltre necessario specificare il tipo di

origine datiFSX, un segreto per le credenziali di autenticazione e altre configurazioni necessarie. È quindi necessario specificare `TEMPLATE` come `Type` quando si chiama. CreateDataSource

Puoi utilizzare il modello fornito in questa guida per sviluppatori. Per informazioni, consulta Amazon FSx (Windows) Schema JSON.

La tabella seguente descrive i parametri dello schema JSON Amazon FSx (Windows).

Configurazione	Descrizione
Configurazione della connessione	Informazioni di configurazione per l'endpoint per l'origine dati.
repositoryEndpointMetadata	Le informazioni sull'endpoint per l'origine dati.
fileSystemId	L'identificatore del Amazon FSx file system. È possibile trovare l'ID del file system nella dashboard dei file system della Amazon FSx console.
fileSystemType	Il tipo di Amazon FSx file system. Da utilizzare Windows File Server come tipo di file system, specificare`WINDOWS`.
Configurazioni del repository	Informazioni di configurazione per il contenuto dell'origine dati. Ad esempio, la configurazione di tipi specifici di contenuti e mappature dei campi.
Tutti	Un elenco di oggetti che mappano gli attributi o i nomi dei campi dei file nell'origine Amazon FSx dati per Amazon Kendra indicizzare i nomi dei campi. Per ulteriori informazioni, consulta la sezione Mappatura dei campi di origine dei dati.
Proprietà aggiuntive	Opzioni di configurazione aggiuntive per i contenuti della fonte di dati.
isCrawlAcl	`true`per eseguire la scansione delle informazioni dell'elenco di controllo degli accessi (ACL)

Configurazione	Descrizione
	per i documenti, se disponi di un ACL e desideri utilizzarlo per il controllo degli accessi. L'ACL specifica a quali documenti possono accedere utenti e gruppi. Le informazioni ACL vengono utilizzate per filtrare i risultati della ricerca in base all'accesso dell'utente o del relativo gruppo ai documenti. Per ulteriori informazioni, consulta Filtraggio del contesto utente.
Modelli di inclusione	Un elenco di modelli di espressioni regolari per includere determinati file nella fonte di dati Amazon FSx . I file che corrispondono ai modelli sono inclusi nell'indice. I file che non corrispondono ai modelli sono esclusi dall'indi ce. Se un file corrisponde sia a un modello di esclusione sia a un modello di inclusione, il modello di esclusione ha la precedenza e il file non viene incluso nell'indice.
Modelli di esclusione	Un elenco di modelli di espressioni regolari per escludere determinati file nella fonte di Amazon FSx dati. I file che corrispondono ai modelli sono esclusi dall'indice. I file che non corrispon dono ai modelli sono inclusi nell'indice. Se un file corrisponde sia a un modello di esclusione che a uno di inclusione, il modello di esclusion e ha la precedenza e il file non viene incluso nell'indice.

Configurazione	Descrizione
enableIdentityCrawler	`true`utilizzare il crawler Amazon Kendra di identità per sincronizzare le informazi oni sull'identità/principali su utenti e gruppi con accesso a determinati documenti. Se il crawler di identità è disattivato, tutti i documenti possono essere ricercati pubblicamente. Se desideri utilizzare il controllo degli accessi per i tuoi documenti e il crawler di identità è disattiva to, in alternativa puoi utilizzare l'PutPrinci palMappingAPI per caricare le informazioni di accesso di utenti e gruppi.
SyncMode	Specificate come Amazon Kendra aggiornar e l'indice quando il contenuto dell'origine dati cambia. Puoi scegliere tra: • `FORCED_FULL_CRAWL` per indicizzare nuovamente tutti i contenuti, sostituendo i contenuti esistenti ogni volta che l'origine dati si sincronizza con l'indice. • `FULL_CRAWL` per indicizzare solo i contenuti nuovi, modificati ed eliminati ogni volta che l'origine dati si sincronizza con l'indice. Amazon Kendra può utilizzare il meccanism o dell'origine dati per tenere traccia delle modifiche ai contenuti e indicizzare i contenuti modificati dall'ultima sincroniz zazione.
tipo	Il tipo di fonte di dati. Per le origini dati del file system Windows, specificare`FSX`.

Amazon FSx (Windows) Schema 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 schema del modello (NetApp ONTAP)

Includi un JSON che contiene lo schema dell'origine dati come parte dell'TemplateConfigurationoggetto. L'ID del file system e la macchina virtuale di archiviazione (SVM) vengono forniti come parte della configurazione della connessione o dei dettagli dell'endpoint del repository. È inoltre necessario specificare il tipo di origine dati`FSXONTAP`, un segreto per le credenziali di autenticazione e altre configurazioni necessarie. È quindi necessario specificare `TEMPLATE` come `Type` quando si chiama. CreateDataSource

Puoi utilizzare il modello fornito in questa guida per sviluppatori. Per informazioni, consulta Amazon FSx (NetApp ONTAP) Schema JSON.

La tabella seguente descrive i parametri dello schema JSON Amazon FSx (NetApp ONTAP).

Configurazione	Descrizione
Configurazione della connessione	Informazioni di configurazione per l'endpoint per l'origine dati.
repositoryEndpointMetadata	Le informazioni sull'endpoint per l'origine dati.
fileSystemId	L'identificatore del Amazon FSx file system. È possibile trovare l'ID del file system nella dashboard dei file system della Amazon FSx console. Per informazioni su come creare un file system nella Amazon FSx console per NetApp ONTAP, consulta la Guida introduttiva di NetApp ONTAP nella Guida per l'FSx for ONTAP utente.
fileSystemType	Il tipo di Amazon FSx file system. Da utilizzare NetApp ONTAP come tipo di file system, specificare`ONTAP`.
SVMid	L'identificatore della macchina virtuale di archiviazione (SVM) utilizzata con il Amazon FSx file system per. NetApp ONTAP È possibile trovare l'ID SVM accedendo alla dashboard dei file system nella Amazon FSx console, selezionando l'ID del file system e quindi selezionando Macchine virtuali di archiviazione. Per informazioni su come creare un file system nella Amazon FSx console perNetApp ONTAP, consulta la Guida introduttiva di NetApp ONTAP nella Guida per l'FSx for ONTAP utente.
Tipo di protocollo	Sia che si utilizzi il protocollo Common Internet File System (CIFS) per Windows o il protocollo Network File System (NFS) per Linux.

Configurazione	Descrizione
Configurazioni del repository	Informazioni di configurazione per il contenuto dell'origine dati. Ad esempio, la configurazione di tipi specifici di contenuti e mappature dei campi.
file	Un elenco di oggetti che mappano gli attributi o i nomi dei campi dei file nell'origine Amazon FSx dati per Amazon Kendra indicizzare i nomi dei campi. Per ulteriori informazioni, consulta la sezione Mappatura dei campi di origine dei dati. I nomi dei campi dell'origine dati devono esistere nei metadati personalizzati dei file.
Proprietà aggiuntive	Opzioni di configurazione aggiuntive per i contenuti della fonte di dati.
Scansiona LACL	`true`per eseguire la scansione delle informazioni dell'elenco di controllo degli accessi (ACL) per i documenti, se si dispone di un ACL e si desidera utilizzarlo per il controllo degli accessi. L'ACL specifica a quali documenti possono accedere utenti e gruppi. Le informazioni ACL vengono utilizzate per filtrare i risultati della ricerca in base all'accesso dell'utente o del relativo gruppo ai documenti. Per ulteriori informazioni, consulta Filtraggio del contesto utente.

Configurazione	Descrizione
Modelli di inclusione	Un elenco di modelli di espressioni regolari per includere determinati file nella fonte di dati Amazon FSx . I file che corrispondono ai modelli sono inclusi nell'indice. I file che non corrispondono ai modelli sono esclusi dall'indi ce. Se un file corrisponde sia a un modello di esclusione sia a un modello di inclusione, il modello di esclusione ha la precedenza e il file non viene incluso nell'indice.
Modelli di esclusione	Un elenco di modelli di espressioni regolari per escludere determinati file nella fonte di Amazon FSx dati. I file che corrispondono ai modelli sono esclusi dall'indice. I file che non corrispon dono ai modelli sono inclusi nell'indice. Se un file corrisponde sia a un modello di esclusione che a uno di inclusione, il modello di esclusion e ha la precedenza e il file non viene incluso nell'indice.
tipo	Il tipo di origine dati. Per le fonti di dati del NetApp ONTAP file system, specifica re`FSX0NTAP`.

Configurazione	Descrizione
SyncMode	Specificate come Amazon Kendra aggiornar e l'indice quando il contenuto dell'origine dati cambia. Puoi scegliere tra: • `FORCED_FULL_CRAWL` per indicizzare nuovamente tutti i contenuti, sostituendo i contenuti esistenti ogni volta che l'origine dati si sincronizza con l'indice. • `FULL_CRAWL` per indicizzare solo i contenuti nuovi, modificati ed eliminati ogni volta che l'origine dati si sincronizza con l'indice. Amazon Kendra può utilizzare il meccanism o dell'origine dati per tenere traccia delle modifiche ai contenuti e indicizzare i contenuti modificati dall'ultima sincroniz zazione.

Configurazione	Descrizione

Segretario ARN	L'Amazon Resource Name (ARN) di un AWS Secrets Manager segreto che contiene le coppie chiave-valore necessarie per connetter si al file system. Amazon FSx Il segreto deve contenere una struttura JSON con le seguenti chiavi:
	
	`{ "username": " user@corp.example.com ", "password": " password" }`
	
	Se utilizzi il protocollo NFS per il tuo Amazon FSx file system, il segreto viene archiviato in una struttura JSON con le seguenti chiavi:
	
	`{ "leftId": "left ID", "rightId": " right ID", "preSharedKey": " pre-shared key " }`

Amazon FSx (NetApp ONTAP) Schema 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"
  ]
}
```

Alfrescoschema modello

Includi un JSON che contiene lo schema dell'origine dati come parte dell'TemplateConfigurationoggetto. Fornisci l'ID del Alfresco sito, l'URL del repository, l'URL dell'interfaccia utente, il tipo di autenticazione, se utilizzi il cloud o in locale e il tipo di contenuto che desideri sottoporre a scansione. Lo fornisci come parte della configurazione della connessione o dei dettagli dell'endpoint del repository. Specificate inoltre il tipo di origine dati`ALFRESCO`, come segreto per le credenziali di autenticazione e altre configurazioni necessarie. È quindi necessario specificare `TEMPLATE` come `Type` quando si chiama. CreateDataSource

Puoi utilizzare il modello fornito in questa guida per sviluppatori. Per informazioni, consulta AlfrescoSchema JSON.

La tabella seguente descrive i parametri dello schema JSON di Alfresco.

Configurazione	Descrizione
Configurazione della connessione	Informazioni di configurazione per l'endpoint per l'origine dati.
repositoryEndpointMetadata	Le informazioni sull'endpoint per l'origine dati.
SiteID	L'identificatore del sito Alfresco.
RepoUrl	L'URL del tuo repository. Alfresco Puoi ottenere l'URL del repository dal tuo Alfresco amministr atore. Ad esempio, se utilizzi Alfresco Cloud (PaaS), l'URL del repository potrebbe essere. https://company.alfrescocloud.com Oppure, se utilizzi Alfresco On-Premises, l'URL del repository potrebbe essere. https://company-al fresco-instance.company-domain.suffix:port
webAppUrl	L'URL della tua interfaccia Alfresco utente. Puoi ottenere l'URL Alfresco dell'interfaccia utente dal tuo Alfresco amministratore. Ad esempio, l'URL dell'interfaccia utente potrebbe essere https://example.com.

Configurazione	Descrizione
repositoryAdditionalProperties	Proprietà aggiuntive per la connessione all'endpoint del repository/origine dati.
authType	Il tipo di autenticazione che usi, se `OAuth2` o`Basic`.
tipo (distribuzione)	Il tipo di Alfresco quello che usi, se `PAAS` o`ON-PREM`.
Tipo di scansione	Il tipo di contenuto che desideri sottoporre a scansione, che si tratti di `ASPECT` (contenut i contrassegnati con «Aspetti» inAlfresco), `SITE_ID` (contenuti all'interno di un Alfresco sito specifico) o `ALL_SITES` (contenuti presenti in tutti i Alfresco siti).
Configurazioni del repository	Informazioni di configurazione per il contenuto dell'origine dati. Ad esempio, la configurazione di tipi specifici di contenuti e mappature dei campi.
• documento • comment	Un elenco di oggetti che mappano gli attributi o i nomi dei campi dei documenti e dei commenti Alfresco ai Amazon Kendra nomi dei campi indicizzati. Per ulteriori informazioni, consulta la sezione Mappatura dei campi di origine dei dati.
Proprietà aggiuntive	Opzioni di configurazione aggiuntive per i contenuti della fonte di dati.
Nome dell'aspetto	Il nome di un 'Aspect' specifico che desideri indicizzare.
Proprietà dell'aspetto	Un elenco di proprietà di contenuto specifiche di «Aspect» che desideri indicizzare.
enableFineGrainedControllo	`true`per eseguire la scansione di «Aspetti».

Configurazione	Descrizione
isCrawlComment	`true`per eseguire la scansione dei commenti.
• inclusionFileNameSchemi • inclusionFileTypeSchemi • inclusionFilePathSchemi	Un elenco di modelli di espressioni regolari per includere determinati file nella fonte di Alfresco dati. I file che corrispondono ai modelli sono inclusi nell'indice. I file che non corrispondono ai modelli sono esclusi dall'indice. Se un file corrisponde sia a un modello di inclusione che di esclusione, il modello di esclusione ha la precedenza e il file non viene incluso nell'indi ce.
• exclusionFileNamePattern • exclusionFileTypeSchemi • exclusionFilePathSchemi	Un elenco di modelli di espressioni regolari per escludere determinati file nella fonte di Alfresco dati. I file che corrispondono ai modelli sono esclusi dall'indice. I file che non corrispondono ai modelli sono inclusi nell'indice. Se un file corrisponde sia a un modello di inclusione che a uno di esclusione, il modello di esclusione ha la precedenza e il file non viene incluso nell'indi ce.
tipo	Il tipo di origine dati. Specificare `ALFRESCO` come tipo di origine dati.

Configurazione	Descrizione

Segretario ARN	L'Amazon Resource Name (ARN) di un AWS Secrets Manager segreto che contiene le coppie chiave-valore necessarie per connetter si al tuo. Alfresco Il segreto deve contenere una struttura JSON con le seguenti chiavi:
	
	Se utilizzi l'autenticazione di base:
	
	`{ "username": " user name", "password": " password" }`
	
	Se si utilizza l'autenticazione OAuth 2.0:
	
	`{ "clientId": " client ID", "clientSecret": " client secret", "tokenUrl": " token URL" }`

Configurazione	Descrizione
SyncMode	Specificate come Amazon Kendra aggiornar e l'indice quando il contenuto dell'origine dati cambia. Puoi scegliere tra: • `FORCED_FULL_CRAWL` per indicizzare nuovamente tutti i contenuti, sostituendo i contenuti esistenti ogni volta che l'origine dati si sincronizza con l'indice. • `FULL_CRAWL` per indicizzare solo i contenuti nuovi, modificati ed eliminati ogni volta che l'origine dati si sincronizza con l'indice. Amazon Kendra può utilizzare il meccanism o dell'origine dati per tenere traccia delle modifiche ai contenuti e indicizzare i contenuti modificati dall'ultima sincroniz zazione.
enableIdentityCrawler	`true`utilizzare il crawler Amazon Kendra di identità per sincronizzare le informazi oni sull'identità/principali su utenti e gruppi con accesso a determinati documenti. Se il crawler di identità è disattivato, tutti i documenti possono essere ricercati pubblicamente. Se desideri utilizzare il controllo degli accessi per i tuoi documenti e il crawler di identità è disattiva to, in alternativa puoi utilizzare l'PutPrinci palMappingAPI per caricare le informazioni di accesso di utenti e gruppi.
version	La versione di questo modello attualmente supportata.

AlfrescoSchema 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 Schema del modello (MySQL)

Includi un JSON che contiene lo schema dell'origine dati come parte dell'oggetto. TemplateConfiguration Specificate il tipo di origine dati come`JDBC`, il tipo di database come`mysql`, un segreto per le credenziali di autenticazione e altre configurazioni necessarie. È quindi necessario specificare `TEMPLATE` come `Type` quando si chiama. CreateDataSource

Puoi utilizzare il modello fornito in questa guida per sviluppatori. Per informazioni, consulta Aurora Schema JSON (MySQL).

La tabella seguente descrive i parametri dello schema JSON Aurora (MySQL).

Configurazione	Descrizione
Configurazione della connessione	Informazioni di configurazione per l'endpoint per l'origine dati.
repositoryEndpointMetadata	Informazioni di configurazione necessarie per connettere la fonte di dati. • dbType: il tipo di database Java utilizzato, indipendentemente dal fatto che si tratti di`mysql`,, `db2postgresql` , `oracle` o. `sqlserver` • dbHost: il nome host del database. • dbPort: la porta del database. • dbInstance: l'istanza del database.
Configurazioni del repository	Informazioni di configurazione per il contenuto dell'origine dati. Ad esempio, la configurazione di tipi specifici di contenuti e mappature dei campi. Specificare il tipo di origine dati e l'ARN segreto.
documento	Un elenco di oggetti che mappano gli attributi o i nomi di campo del contenuto del database per Amazon Kendra indicizzare i nomi dei campi.

Configurazione	Descrizione
	Per ulteriori informazioni, consulta la sezione Mappatura dei campi di origine dei dati.
Proprietà aggiuntive	Opzioni di configurazione aggiuntive per i contenuti della fonte di dati. Utilizzatelo per includere o escludere contenuti specifici nella fonte di dati del database.
Chiave primaria	Fornisci la chiave primaria per la tabella del database. Questo identifica una tabella all'inter no del database.
Colonna del titolo	Fornisci il nome della colonna del titolo del documento all'interno della tabella del database.
Corpo/colonna	Fornisci il nome della colonna del titolo del documento all'interno della tabella del database.
sqlQuery	Inserisci istruzioni di query SQL come le operazioni SELECT e JOIN. Le query SQL devono pesare meno di 32 KB. Amazon Kendra eseguirà la scansione di tutto il contenuto del database che corrisponde alla tua query.
colonna Timestamp	Inserisci il nome della colonna che contiene i timestamp. Amazon Kendra utilizza le informazi oni relative alla marca temporale per rilevare le modifiche ai contenuti e sincronizzare solo i contenuti modificati.
formato Timestamp	Inserisci il nome della colonna che contiene i formati di timestamp da utilizzare per rilevare le modifiche ai contenuti e risincronizzare i contenuti.

Configurazione	Descrizione
timezone	Inserisci il nome della colonna che contiene i fusi orari per il contenuto da sottoporre a scansione.
changeDetectingColumns	Inserisci i nomi delle colonne che Amazon Kendra verranno utilizzate per rilevare le modifiche al contenuto. Amazon Kendra reindicizzerà il contenuto in caso di modifica in una di queste colonne
allowedUsersColumns	Inserisci il nome della colonna che contiene gli ID utente a cui consentire l'accesso ai contenuti .
allowedGroupsColumn	Inserisci il nome della colonna che contiene gli ID utente a cui consentire l'accesso ai contenuti .
SourceURIColumn	Inserisci il nome della colonna che contiene gli URL di origine da indicizzare.
isSslEnabled	Inserisci istruzioni di query SQL come le operazioni SELECT e JOIN. Le query SQL devono pesare meno di 32 KB. Amazon Kendra eseguirà la scansione di tutto il contenuto del database che corrisponde alla tua query.
tipo	Il tipo di fonte di dati. Specificare `JDBC` come tipo di origine dati.

Configurazione	Descrizione
SyncMode	Specificate come Amazon Kendra aggiornar e l'indice quando il contenuto dell'origine dati cambia. Puoi scegliere tra: • `FORCED_FULL_CRAWL` per indicizzare nuovamente tutti i contenuti, sostituendo i contenuti esistenti ogni volta che l'origine dati si sincronizza con l'indice. • `FULL_CRAWL` per indicizzare solo i contenuti nuovi, modificati ed eliminati ogni volta che l'origine dati si sincronizza con l'indice. Amazon Kendra può utilizzare il meccanism o dell'origine dati per tenere traccia delle modifiche ai contenuti e indicizzare i contenuti modificati dall'ultima sincroniz zazione. • `CHANGE_LOG` per indicizzare solo contenuti nuovi e modificati ogni volta che l'origine dati si sincronizza con l'indice. Amazon Kendra può utilizzare il meccanismo dell'origine dati per tenere traccia delle modifiche ai contenuti e indicizzare i contenuti modificati dall'ultima sincronizzazione.
Segretario ARN	L'Amazon Resource Name (ARN) di un segreto di Secrets Manager che contiene il nome utente e la password necessari per connetter si al database. Il segreto deve contenere una struttura JSON con le seguenti chiavi: `{ "user name": "database user name", "password": " password" }`

Configurazione	Descrizione
version	La versione del modello attualmente supportata.

Aurora Schema JSON (MySQL)

```
{
  "$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 Schema del modello (PostgreSQL)

Includi un JSON che contiene lo schema dell'origine dati come parte dell'oggetto. TemplateConfiguration Specificate il tipo di origine dati come`JDBC`, il tipo di database come`postgresql`, un segreto per le credenziali di autenticazione e altre configurazioni necessarie. È quindi necessario specificare `TEMPLATE` come `Type` quando si chiama. CreateDataSource

Puoi utilizzare il modello fornito in questa guida per sviluppatori. Per informazioni, consulta Aurora Schema JSON (PostgreSQL).

La tabella seguente descrive i parametri dello schema Aurora JSON (PostgreSQL).

Configurazione	Descrizione
Configurazione della connessione	Informazioni di configurazione per l'endpoint per l'origine dati.
repositoryEndpointMetadata	Informazioni di configurazione necessarie per connettere la fonte di dati. • dbType: il tipo di database Java utilizzato, indipendentemente dal fatto che si tratti di`mysql`,, `db2postgresql` , `oracle` o. `sqlserver` • dbHost: il nome host del database. • dbPort: la porta del database. • dbInstance: l'istanza del database.
Configurazioni del repository	Informazioni di configurazione per il contenuto dell'origine dati. Ad esempio, la configurazione di tipi specifici di contenuti e mappature dei campi. Specificare il tipo di origine dati e l'ARN segreto.
documento	Un elenco di oggetti che mappano gli attributi o i nomi di campo del contenuto del database per Amazon Kendra indicizzare i nomi dei campi.

Configurazione	Descrizione
	Per ulteriori informazioni, consulta la sezione Mappatura dei campi di origine dei dati.
Proprietà aggiuntive	Opzioni di configurazione aggiuntive per i contenuti della fonte di dati. Utilizzatelo per includere o escludere contenuti specifici nella fonte di dati del database.
Chiave primaria	Fornisci la chiave primaria per la tabella del database. Questo identifica una tabella all'inter no del database.
Colonna del titolo	Fornisci il nome della colonna del titolo del documento all'interno della tabella del database.
Corpo/colonna	Fornisci il nome della colonna del titolo del documento all'interno della tabella del database.
sqlQuery	Inserisci istruzioni di query SQL come le operazioni SELECT e JOIN. Le query SQL devono pesare meno di 32 KB. Amazon Kendra eseguirà la scansione di tutto il contenuto del database che corrisponde alla tua query.
colonna Timestamp	Inserisci il nome della colonna che contiene i timestamp. Amazon Kendra utilizza le informazi oni relative alla marca temporale per rilevare le modifiche ai contenuti e sincronizzare solo i contenuti modificati.
formato Timestamp	Inserisci il nome della colonna che contiene i formati di timestamp da utilizzare per rilevare le modifiche ai contenuti e risincronizzare i contenuti.

Configurazione	Descrizione
timezone	Inserisci il nome della colonna che contiene i fusi orari per il contenuto da sottoporre a scansione.
changeDetectingColumns	Inserisci i nomi delle colonne che Amazon Kendra verranno utilizzate per rilevare le modifiche al contenuto. Amazon Kendra reindicizzerà il contenuto in caso di modifica in una di queste colonne
allowedUsersColumns	Inserisci il nome della colonna che contiene gli ID utente a cui consentire l'accesso ai contenuti .
allowedGroupsColumn	Inserisci il nome della colonna che contiene gli ID utente a cui consentire l'accesso ai contenuti .
SourceURIColumn	Inserisci il nome della colonna che contiene gli URL di origine da indicizzare.
isSslEnabled	Inserisci istruzioni di query SQL come le operazioni SELECT e JOIN. Le query SQL devono pesare meno di 32 KB. Amazon Kendra eseguirà la scansione di tutto il contenuto del database che corrisponde alla tua query.
tipo	Il tipo di fonte di dati. Specificare `JDBC` come tipo di origine dati.

Configurazione	Descrizione
SyncMode	Specificate come Amazon Kendra aggiornar e l'indice quando il contenuto dell'origine dati cambia. Puoi scegliere tra: • `FORCED_FULL_CRAWL` per indicizzare nuovamente tutti i contenuti, sostituendo i contenuti esistenti ogni volta che l'origine dati si sincronizza con l'indice. • `FULL_CRAWL` per indicizzare solo i contenuti nuovi, modificati ed eliminati ogni volta che l'origine dati si sincronizza con l'indice. Amazon Kendra può utilizzare il meccanism o dell'origine dati per tenere traccia delle modifiche ai contenuti e indicizzare i contenuti modificati dall'ultima sincroniz zazione. • `CHANGE_LOG` per indicizzare solo contenuti nuovi e modificati ogni volta che l'origine dati si sincronizza con l'indice. Amazon Kendra può utilizzare il meccanismo dell'origine dati per tenere traccia delle modifiche ai contenuti e indicizzare i contenuti modificati dall'ultima sincronizzazione.
Segretario ARN	L'Amazon Resource Name (ARN) di un segreto di Secrets Manager che contiene il nome utente e la password necessari per connetter si al database. Il segreto deve contenere una struttura JSON con le seguenti chiavi: `{ "user name": "database user name", "password": " password" }`

Configurazione	Descrizione
version	La versione del modello attualmente supportata.

Aurora Schema JSON (PostgreSQL)

```
{
  "$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 Schema del modello (Microsoft SQL Server)

Includi un JSON che contiene lo schema dell'origine dati come parte dell'TemplateConfigurationoggetto. Specificate il tipo di origine dati come`JDBC`, il tipo di database come`sqlserver`, un segreto per le credenziali di autenticazione e altre configurazioni necessarie. È quindi necessario specificare `TEMPLATE` come `Type` quando si chiama. CreateDataSource

Puoi utilizzare il modello fornito in questa guida per sviluppatori. Per informazioni, consulta Amazon RDS Schema JSON (Microsoft SQL Server).

La tabella seguente descrive i parametri dello schema JSON Amazon RDS (Microsoft SQL Server).

Configurazione	Descrizione
Configurazione della connessione	Informazioni di configurazione per l'endpoint per l'origine dati.
repositoryEndpointMetadata	Informazioni di configurazione necessarie per connettere la fonte di dati. • dbType: il tipo di database Java utilizzato, indipendentemente dal fatto che si tratti di`mysql`,, `db2postgresql` , `oracle` o. `sqlserver` • dbHost: il nome host del database. • dbPort: la porta del database. • dbInstance: l'istanza del database.
Configurazioni del repository	Informazioni di configurazione per il contenuto dell'origine dati. Ad esempio, la configurazione di tipi specifici di contenuti e mappature dei campi. Specificare il tipo di origine dati e l'ARN segreto.
documento	Un elenco di oggetti che mappano gli attributi o i nomi di campo del contenuto del database per Amazon Kendra indicizzare i nomi dei campi.

Configurazione	Descrizione
	Per ulteriori informazioni, consulta la sezione Mappatura dei campi di origine dei dati.
Proprietà aggiuntive	Opzioni di configurazione aggiuntive per i contenuti della fonte di dati. Utilizzatelo per includere o escludere contenuti specifici nella fonte di dati del database.
Chiave primaria	Fornisci la chiave primaria per la tabella del database. Questo identifica una tabella all'inter no del database.
Colonna del titolo	Fornisci il nome della colonna del titolo del documento all'interno della tabella del database.
Corpo/colonna	Fornisci il nome della colonna del titolo del documento all'interno della tabella del database.
sqlQuery	Inserisci istruzioni di query SQL come le operazioni SELECT e JOIN. Le query SQL devono pesare meno di 32 KB. Amazon Kendra eseguirà la scansione di tutto il contenuto del database che corrisponde alla tua query.
colonna Timestamp	Inserisci il nome della colonna che contiene i timestamp. Amazon Kendra utilizza le informazi oni relative alla marca temporale per rilevare le modifiche ai contenuti e sincronizzare solo i contenuti modificati.
formato Timestamp	Inserisci il nome della colonna che contiene i formati di timestamp da utilizzare per rilevare le modifiche ai contenuti e risincronizzare i contenuti.

Configurazione	Descrizione
timezone	Inserisci il nome della colonna che contiene i fusi orari per il contenuto da sottoporre a scansione.
changeDetectingColumns	Inserisci i nomi delle colonne che Amazon Kendra verranno utilizzate per rilevare le modifiche al contenuto. Amazon Kendra reindicizzerà il contenuto in caso di modifica in una di queste colonne
allowedUsersColumns	Inserisci il nome della colonna che contiene gli ID utente a cui consentire l'accesso ai contenuti .
allowedGroupsColumn	Inserisci il nome della colonna che contiene gli ID utente a cui consentire l'accesso ai contenuti .
SourceURIColumn	Inserisci il nome della colonna che contiene gli URL di origine da indicizzare.
isSslEnabled	Inserisci istruzioni di query SQL come le operazioni SELECT e JOIN. Le query SQL devono pesare meno di 32 KB. Amazon Kendra eseguirà la scansione di tutto il contenuto del database che corrisponde alla tua query.
tipo	Il tipo di fonte di dati. Specificare `JDBC` come tipo di origine dati.

Configurazione	Descrizione
SyncMode	Specificate come Amazon Kendra aggiornar e l'indice quando il contenuto dell'origine dati cambia. Puoi scegliere tra: • `FORCED_FULL_CRAWL` per indicizzare nuovamente tutti i contenuti, sostituendo i contenuti esistenti ogni volta che l'origine dati si sincronizza con l'indice. • `FULL_CRAWL` per indicizzare solo i contenuti nuovi, modificati ed eliminati ogni volta che l'origine dati si sincronizza con l'indice. Amazon Kendra può utilizzare il meccanism o dell'origine dati per tenere traccia delle modifiche ai contenuti e indicizzare i contenuti modificati dall'ultima sincroniz zazione. • `CHANGE_LOG` per indicizzare solo contenuti nuovi e modificati ogni volta che l'origine dati si sincronizza con l'indice. Amazon Kendra può utilizzare il meccanismo dell'origine dati per tenere traccia delle modifiche ai contenuti e indicizzare i contenuti modificati dall'ultima sincronizzazione.
Segretario ARN	L'Amazon Resource Name (ARN) di un segreto di Secrets Manager che contiene il nome utente e la password necessari per connetter si al database. Il segreto deve contenere una struttura JSON con le seguenti chiavi: `{ "user name": "database user name", "password": " password" }`

Configurazione	Descrizione
version	La versione del modello attualmente supportata.

Amazon RDS Schema JSON (Microsoft SQL Server)

```
{
  "$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 Schema del modello (MySQL)

Includi un JSON che contiene lo schema dell'origine dati come parte dell'oggetto. TemplateConfiguration Specificate il tipo di origine dati come`JDBC`, il tipo di database come`mysql`, un segreto per le credenziali di autenticazione e altre configurazioni necessarie. È quindi necessario specificare `TEMPLATE` come `Type` quando si chiama. CreateDataSource

Puoi utilizzare il modello fornito in questa guida per sviluppatori. Per informazioni, consulta Amazon RDS Schema JSON (MySQL).

La tabella seguente descrive i parametri dello schema JSON Amazon RDS (MySQL).

Configurazione	Descrizione
Configurazione della connessione	Informazioni di configurazione per l'endpoint per l'origine dati.
repositoryEndpointMetadata	Informazioni di configurazione necessarie per connettere la fonte di dati. • dbType: il tipo di database Java utilizzato, indipendentemente dal fatto che si tratti di`mysql`,, `db2postgresql` , `oracle` o. `sqlserver` • dbHost: il nome host del database. • dbPort: la porta del database. • dbInstance: l'istanza del database.
Configurazioni del repository	Informazioni di configurazione per il contenuto dell'origine dati. Ad esempio, la configurazione di tipi specifici di contenuti e mappature dei campi. Specificare il tipo di origine dati e l'ARN segreto.
documento	Un elenco di oggetti che mappano gli attributi o i nomi di campo del contenuto del database per Amazon Kendra indicizzare i nomi dei campi.

Configurazione	Descrizione
	Per ulteriori informazioni, consulta la sezione Mappatura dei campi di origine dei dati.
Proprietà aggiuntive	Opzioni di configurazione aggiuntive per i contenuti della fonte di dati. Utilizzatelo per includere o escludere contenuti specifici nella fonte di dati del database.
Chiave primaria	Fornisci la chiave primaria per la tabella del database. Questo identifica una tabella all'inter no del database.
Colonna del titolo	Fornisci il nome della colonna del titolo del documento all'interno della tabella del database.
Corpo/colonna	Fornisci il nome della colonna del titolo del documento all'interno della tabella del database.
sqlQuery	Inserisci istruzioni di query SQL come le operazioni SELECT e JOIN. Le query SQL devono pesare meno di 32 KB. Amazon Kendra eseguirà la scansione di tutto il contenuto del database che corrisponde alla tua query.
colonna Timestamp	Inserisci il nome della colonna che contiene i timestamp. Amazon Kendra utilizza le informazi oni relative alla marca temporale per rilevare le modifiche ai contenuti e sincronizzare solo i contenuti modificati.
formato Timestamp	Inserisci il nome della colonna che contiene i formati di timestamp da utilizzare per rilevare le modifiche ai contenuti e risincronizzare i contenuti.

Configurazione	Descrizione
timezone	Inserisci il nome della colonna che contiene i fusi orari per il contenuto da sottoporre a scansione.
changeDetectingColumns	Inserisci i nomi delle colonne che Amazon Kendra verranno utilizzate per rilevare le modifiche al contenuto. Amazon Kendra reindicizzerà il contenuto in caso di modifica in una di queste colonne
allowedUsersColumns	Inserisci il nome della colonna che contiene gli ID utente a cui consentire l'accesso ai contenuti .
allowedGroupsColumn	Inserisci il nome della colonna che contiene gli ID utente a cui consentire l'accesso ai contenuti .
SourceURIColumn	Inserisci il nome della colonna che contiene gli URL di origine da indicizzare.
isSslEnabled	Inserisci istruzioni di query SQL come le operazioni SELECT e JOIN. Le query SQL devono pesare meno di 32 KB. Amazon Kendra eseguirà la scansione di tutto il contenuto del database che corrisponde alla tua query.
tipo	Il tipo di fonte di dati. Specificare `JDBC` come tipo di origine dati.

Configurazione	Descrizione
SyncMode	Specificate come Amazon Kendra aggiornar e l'indice quando il contenuto dell'origine dati cambia. Puoi scegliere tra: • `FORCED_FULL_CRAWL` per indicizzare nuovamente tutti i contenuti, sostituendo i contenuti esistenti ogni volta che l'origine dati si sincronizza con l'indice. • `FULL_CRAWL` per indicizzare solo i contenuti nuovi, modificati ed eliminati ogni volta che l'origine dati si sincronizza con l'indice. Amazon Kendra può utilizzare il meccanism o dell'origine dati per tenere traccia delle modifiche ai contenuti e indicizzare i contenuti modificati dall'ultima sincroniz zazione. • `CHANGE_LOG` per indicizzare solo contenuti nuovi e modificati ogni volta che l'origine dati si sincronizza con l'indice. Amazon Kendra può utilizzare il meccanismo dell'origine dati per tenere traccia delle modifiche ai contenuti e indicizzare i contenuti modificati dall'ultima sincronizzazione.
Segretario ARN	L'Amazon Resource Name (ARN) di un segreto di Secrets Manager che contiene il nome utente e la password necessari per connetter si al database. Il segreto deve contenere una struttura JSON con le seguenti chiavi: `{ "user name": "database user name", "password": " password" }`

Configurazione	Descrizione
version	La versione del modello attualmente supportata.

Amazon RDS Schema JSON (MySQL)

```
{
  "$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 schema modello (Oracle)

Includi un JSON che contiene lo schema dell'origine dati come parte dell'TemplateConfigurationoggetto. Specificate il tipo di origine dati come`JDBC`, il tipo di database come`oracle`, un segreto per le credenziali di autenticazione e altre configurazioni necessarie. È quindi necessario specificare `TEMPLATE` come `Type` quando si chiama. CreateDataSource

Puoi utilizzare il modello fornito in questa guida per sviluppatori. Per informazioni, consulta Amazon RDS Schema JSON (Oracle).

La tabella seguente descrive i parametri dello schema JSON Amazon RDS (Oracle).

Configurazione	Descrizione
Configurazione della connessione	Informazioni di configurazione per l'endpoint per l'origine dati.
repositoryEndpointMetadata	Informazioni di configurazione necessarie per connettere la fonte di dati. • dbType: il tipo di database Java utilizzato, indipendentemente dal fatto che si tratti di`mysql`,, `db2postgresql` , `oracle` o. `sqlserver` • dbHost: il nome host del database. • dbPort: la porta del database. • dbInstance: l'istanza del database.
Configurazioni del repository	Informazioni di configurazione per il contenuto dell'origine dati. Ad esempio, la configurazione di tipi specifici di contenuti e mappature dei campi. Specificare il tipo di origine dati e l'ARN segreto.
documento	Un elenco di oggetti che mappano gli attributi o i nomi di campo del contenuto del database per Amazon Kendra indicizzare i nomi dei campi.

Configurazione	Descrizione
	Per ulteriori informazioni, consulta la sezione Mappatura dei campi di origine dei dati.
Proprietà aggiuntive	Opzioni di configurazione aggiuntive per i contenuti della fonte di dati. Utilizzatelo per includere o escludere contenuti specifici nella fonte di dati del database.
Chiave primaria	Fornisci la chiave primaria per la tabella del database. Questo identifica una tabella all'inter no del database.
Colonna del titolo	Fornisci il nome della colonna del titolo del documento all'interno della tabella del database.
Corpo/colonna	Fornisci il nome della colonna del titolo del documento all'interno della tabella del database.
sqlQuery	Inserisci istruzioni di query SQL come le operazioni SELECT e JOIN. Le query SQL devono pesare meno di 32 KB. Amazon Kendra eseguirà la scansione di tutto il contenuto del database che corrisponde alla tua query.
colonna Timestamp	Inserisci il nome della colonna che contiene i timestamp. Amazon Kendra utilizza le informazi oni relative alla marca temporale per rilevare le modifiche ai contenuti e sincronizzare solo i contenuti modificati.
formato Timestamp	Inserisci il nome della colonna che contiene i formati di timestamp da utilizzare per rilevare le modifiche ai contenuti e risincronizzare i contenuti.

Configurazione	Descrizione
timezone	Inserisci il nome della colonna che contiene i fusi orari per il contenuto da sottoporre a scansione.
changeDetectingColumns	Inserisci i nomi delle colonne che Amazon Kendra verranno utilizzate per rilevare le modifiche al contenuto. Amazon Kendra reindicizzerà il contenuto in caso di modifica in una di queste colonne
allowedUsersColumns	Inserisci il nome della colonna che contiene gli ID utente a cui consentire l'accesso ai contenuti .
allowedGroupsColumn	Inserisci il nome della colonna che contiene gli ID utente a cui consentire l'accesso ai contenuti .
SourceURIColumn	Inserisci il nome della colonna che contiene gli URL di origine da indicizzare.
isSslEnabled	Inserisci istruzioni di query SQL come le operazioni SELECT e JOIN. Le query SQL devono pesare meno di 32 KB. Amazon Kendra eseguirà la scansione di tutto il contenuto del database che corrisponde alla tua query.
tipo	Il tipo di fonte di dati. Specificare `JDBC` come tipo di origine dati.

Configurazione	Descrizione
SyncMode	Specificate come Amazon Kendra aggiornar e l'indice quando il contenuto dell'origine dati cambia. Puoi scegliere tra: • `FORCED_FULL_CRAWL` per indicizzare nuovamente tutti i contenuti, sostituendo i contenuti esistenti ogni volta che l'origine dati si sincronizza con l'indice. • `FULL_CRAWL` per indicizzare solo i contenuti nuovi, modificati ed eliminati ogni volta che l'origine dati si sincronizza con l'indice. Amazon Kendra può utilizzare il meccanism o dell'origine dati per tenere traccia delle modifiche ai contenuti e indicizzare i contenuti modificati dall'ultima sincroniz zazione. • `CHANGE_LOG` per indicizzare solo contenuti nuovi e modificati ogni volta che l'origine dati si sincronizza con l'indice. Amazon Kendra può utilizzare il meccanismo dell'origine dati per tenere traccia delle modifiche ai contenuti e indicizzare i contenuti modificati dall'ultima sincronizzazione.
Secretary ARN	L'Amazon Resource Name (ARN) di un segreto di Secrets Manager che contiene il nome utente e la password necessari per connetter si al database. Il segreto deve contenere una struttura JSON con le seguenti chiavi: `{ "user name": "database user name", "password": " password" }`

Configurazione	Descrizione
version	La versione del modello attualmente supportata.

Amazon RDS Schema JSON (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"
  ]
}
```

Amazon RDS Schema del modello (PostgreSQL)

Includi un JSON che contiene lo schema dell'origine dati come parte dell'oggetto. TemplateConfiguration Specificate il tipo di origine dati come`JDBC`, il tipo di database come`postgresql`, un segreto per le credenziali di autenticazione e altre configurazioni necessarie. È quindi necessario specificare `TEMPLATE` come `Type` quando si chiama. CreateDataSource

Puoi utilizzare il modello fornito in questa guida per sviluppatori. Per informazioni, consulta Amazon RDS Schema JSON (PostgreSQL).

La tabella seguente descrive i parametri dello schema Amazon RDS JSON (PostgreSQL).

Configurazione	Descrizione
Configurazione della connessione	Informazioni di configurazione per l'endpoint per l'origine dati.
repositoryEndpointMetadata	Informazioni di configurazione necessarie per connettere la fonte di dati. • dbType: il tipo di database Java utilizzato, indipendentemente dal fatto che si tratti di`mysql`,, `db2postgresql` , `oracle` o. `sqlserver` • dbHost: il nome host del database. • dbPort: la porta del database. • dbInstance: l'istanza del database.
Configurazioni del repository	Informazioni di configurazione per il contenuto dell'origine dati. Ad esempio, la configurazione di tipi specifici di contenuti e mappature dei campi. Specificare il tipo di origine dati e l'ARN segreto.
documento	Un elenco di oggetti che mappano gli attributi o i nomi di campo del contenuto del database per Amazon Kendra indicizzare i nomi dei campi.

Configurazione	Descrizione
	Per ulteriori informazioni, consulta la sezione Mappatura dei campi di origine dei dati.
Proprietà aggiuntive	Opzioni di configurazione aggiuntive per i contenuti della fonte di dati. Utilizzatelo per includere o escludere contenuti specifici nella fonte di dati del database.
Chiave primaria	Fornisci la chiave primaria per la tabella del database. Questo identifica una tabella all'inter no del database.
Colonna del titolo	Fornisci il nome della colonna del titolo del documento all'interno della tabella del database.
Corpo/colonna	Fornisci il nome della colonna del titolo del documento all'interno della tabella del database.
sqlQuery	Inserisci istruzioni di query SQL come le operazioni SELECT e JOIN. Le query SQL devono pesare meno di 32 KB. Amazon Kendra eseguirà la scansione di tutto il contenuto del database che corrisponde alla tua query.
colonna Timestamp	Inserisci il nome della colonna che contiene i timestamp. Amazon Kendra utilizza le informazi oni relative alla marca temporale per rilevare le modifiche ai contenuti e sincronizzare solo i contenuti modificati.
formato Timestamp	Inserisci il nome della colonna che contiene i formati di timestamp da utilizzare per rilevare le modifiche ai contenuti e risincronizzare i contenuti.

Configurazione	Descrizione
timezone	Inserisci il nome della colonna che contiene i fusi orari per il contenuto da sottoporre a scansione.
changeDetectingColumns	Inserisci i nomi delle colonne che Amazon Kendra verranno utilizzate per rilevare le modifiche al contenuto. Amazon Kendra reindicizzerà il contenuto in caso di modifica in una di queste colonne
allowedUsersColumns	Inserisci il nome della colonna che contiene gli ID utente a cui consentire l'accesso ai contenuti .
allowedGroupsColumn	Inserisci il nome della colonna che contiene gli ID utente a cui consentire l'accesso ai contenuti .
SourceURIColumn	Inserisci il nome della colonna che contiene gli URL di origine da indicizzare.
isSslEnabled	Inserisci istruzioni di query SQL come le operazioni SELECT e JOIN. Le query SQL devono pesare meno di 32 KB. Amazon Kendra eseguirà la scansione di tutto il contenuto del database che corrisponde alla tua query.
tipo	Il tipo di fonte di dati. Specificare `JDBC` come tipo di origine dati.

Configurazione	Descrizione
SyncMode	Specificate come Amazon Kendra aggiornar e l'indice quando il contenuto dell'origine dati cambia. Puoi scegliere tra: • `FORCED_FULL_CRAWL` per indicizzare nuovamente tutti i contenuti, sostituendo i contenuti esistenti ogni volta che l'origine dati si sincronizza con l'indice. • `FULL_CRAWL` per indicizzare solo i contenuti nuovi, modificati ed eliminati ogni volta che l'origine dati si sincronizza con l'indice. Amazon Kendra può utilizzare il meccanism o dell'origine dati per tenere traccia delle modifiche ai contenuti e indicizzare i contenuti modificati dall'ultima sincroniz zazione. • `CHANGE_LOG` per indicizzare solo contenuti nuovi e modificati ogni volta che l'origine dati si sincronizza con l'indice. Amazon Kendra può utilizzare il meccanismo dell'origine dati per tenere traccia delle modifiche ai contenuti e indicizzare i contenuti modificati dall'ultima sincronizzazione.
Secretary ARN	L'Amazon Resource Name (ARN) di un segreto di Secrets Manager che contiene il nome utente e la password necessari per connetter si al database. Il segreto deve contenere una struttura JSON con le seguenti chiavi: `{ "user name": "database user name", "password": " password" }`

Configurazione	Descrizione
version	La versione del modello attualmente supportata.

Amazon RDS Schema JSON (PostgreSQL)

```
{
  "$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 schema modello

Includi un JSON che contiene lo schema dell'origine dati come parte della configurazione del modello. Fornisci il nome del bucket S3 come parte della configurazione della connessione o dei dettagli dell'endpoint del repository. Specificate anche il tipo di origine dati e le altre configurazioni `S3` necessarie. È quindi necessario specificare `TEMPLATE` come `Type` quando si chiama CreateDataSource.

Puoi utilizzare il modello fornito in questa guida per sviluppatori. Per informazioni, consulta Schema JSON S3.

La tabella seguente descrive i parametri dello schema Amazon S3 JSON.

Configurazione	Descrizione
Configurazione della connessione	Informazioni di configurazione per l'endpoint per l'origine dati.
repositoryEndpointMetadata	Le informazioni sull'endpoint per l'origine dati.
BucketName	Il nome del tuo Amazon S3 bucket.
Configurazioni del repository	Informazioni di configurazione per il contenuto dell'origine dati. Ad esempio, la configurazione di tipi specifici di contenuti e mappature dei campi.
Proprietà aggiuntive	Opzioni di configurazione aggiuntive per i contenuti della fonte di dati
• Modelli di inclusione • Modelli di esclusione • Prefissi di inclusione • Prefissi di esclusione	Un elenco di modelli di espressioni regolari per includere o escludere file specifici nella fonte di dati. Amazon S3 I file che corrispondono ai modelli sono inclusi nell'indice. I file che non corrispondono ai modelli sono esclusi dall'indi ce. Se un file corrisponde sia a un modello di esclusione sia a un modello di inclusione, il modello di esclusione ha la precedenza e il file non viene incluso nell'indice.

Configurazione	Descrizione
aclConfigurationFilePercorso	Il percorso del file che controlla l'accesso ai documenti in un Amazon Kendra indice.
metadataFilesPrefix	La posizione all'interno del bucket per i file di metadati.
SyncMode	Specificate come Amazon Kendra aggiornar e l'indice quando il contenuto dell'origine dati cambia. Puoi scegliere tra: • `FORCED_FULL_CRAWL` per indicizzare nuovamente tutti i contenuti, sostituendo i contenuti esistenti ogni volta che l'origine dati si sincronizza con l'indice. • `FULL_CRAWL` per indicizzare solo i contenuti nuovi, modificati ed eliminati ogni volta che l'origine dati si sincronizza con l'indice. Amazon Kendra può utilizzare il meccanism o dell'origine dati per tenere traccia delle modifiche ai contenuti e indicizzare i contenuti modificati dall'ultima sincroniz zazione.
tipo	Il tipo di fonte di dati. Specificare `S3` come tipo di origine dati.
version	La versione del modello supportata.

Schema JSON S3

```
{
  "$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 Schema del modello Web Crawler

Includi un JSON che contiene lo schema dell'origine dati come parte dell'oggetto. TemplateConfiguration

Fornisci gli URL iniziali o del punto di partenza oppure puoi fornire gli URL della mappa del sito, come parte della configurazione della connessione o dei dettagli dell'endpoint del repository. Invece di elencare manualmente tutti gli URL, puoi fornire il percorso del Amazon S3 bucket che memorizza un file di testo per l'elenco di URL iniziali o file XML della mappa del sito, che puoi raggruppare in un file ZIP in S3.

Specificate anche il tipo di origine dati`WEBCRAWLERV2`, come le credenziali di autenticazione del sito Web e il tipo di autenticazione se i siti Web richiedono l'autenticazione e altre configurazioni necessarie.

È quindi necessario specificare `TEMPLATE` come `Type` quando si chiama. CreateDataSource

> **Important**
>
> La creazione di connettori Web Crawler v2.0 non è supportata da. AWS CloudFormation Utilizza il connettore Web Crawler v1.0 se hai bisogno di assistenza. AWS CloudFormation

Quando selezioni i siti Web da indicizzare, devi rispettare la Policy di uso accettabile di Amazon e tutti gli altri termini di Amazon. Ricorda che devi utilizzare Amazon Kendra Web Crawler solo per indicizzare le tue pagine Web o le pagine Web che hai l'autorizzazione a indicizzare. Per informazioni su come impedire a Amazon Kendra Web Crawler di indicizzare i siti Web, consulta. Configurazione del file per Web Crawler *robots.txt*Amazon Kendra

Puoi utilizzare il modello fornito in questa guida per sviluppatori. Per informazioni, consulta Amazon Kendra Schema JSON di Web Crawler.

La tabella seguente descrive i parametri dello schema JSON di Amazon Kendra Web Crawler.

Configurazione	Descrizione
Configurazione della connessione	Informazioni di configurazione per l'endpoint per l'origine dati.
repositoryEndpointMetadata	Le informazioni sull'endpoint per l'origine dati.
siteMapUrls	L'elenco degli URL della mappa del sito per i siti Web di cui desideri eseguire la scansione. Puoi elencare fino a tre URL di mappa del sito.
s3 SeedUrl	Il percorso S3 del file di testo che memorizza l'elenco degli URL iniziali o dei punti di partenza. Ad esempio, s3://bucket-name/directory/. Ogni URL nel file di testo deve essere formattato su una riga separata. Puoi elencare fino a 100 URL iniziali in un file.
s3 SiteMapUrl	Il percorso S3 dei file XML della mappa del sito. Ad esempio, s3://bucket-name/directory/. Puoi elencare fino a tre file XML della mappa del sito. Puoi raggruppare più file Sitemap in un file

Configurazione	Descrizione
	ZIP e archiviare il file ZIP nel tuo Amazon S3 bucket.
seedUrlConnections	L'elenco degli URL iniziali o dei punti di partenza per i siti Web che desideri scansiona re. Puoi elencare fino a 100 URL iniziali.
Vedi URL	L'URL del seme o del punto di partenza.
autenticazione	Il tipo di autenticazione se i tuoi siti web richiedono la stessa autenticazione, altrimenti specifica`NoAuthentication` .
Configurazioni del repository	Informazioni di configurazione per il contenuto dell'origine dati. Ad esempio, la configurazione di tipi specifici di contenuti e mappature dei campi.
• Pagina Web • attachment	Un elenco di oggetti che mappano gli attributi o i nomi dei campi delle pagine Web e dei file di pagine Web per Amazon Kendra indicizzare i nomi dei campi. Ad esempio, il tag del titolo della pagina Web HTML può essere mappato al campo dell'`_document_title` indice. Per ulteriori informazioni, consulta la sezione Mappatura dei campi di origine dei dati.

Configurazione	Descrizione
SyncMode	Specificate come Amazon Kendra aggiornar e l'indice quando il contenuto dell'origine dati cambia. Puoi scegliere tra: • `FORCED_FULL_CRAWL` per indicizzare nuovamente tutti i contenuti, sostituendo i contenuti esistenti ogni volta che l'origine dati si sincronizza con l'indice. • `FULL_CRAWL` per indicizzare solo i contenuti nuovi, modificati ed eliminati ogni volta che l'origine dati si sincronizza con l'indice. Amazon Kendra può utilizzare il meccanism o dell'origine dati per tenere traccia delle modifiche ai contenuti e indicizzare i contenuti modificati dall'ultima sincroniz zazione.
Proprietà aggiuntive	Opzioni di configurazione aggiuntive per i contenuti della fonte di dati.
Limite di velocità	Il numero massimo di URL di cui viene eseguita la ricerca per indicizzazione per host di sito Web al minuto.
maxFileSize	La dimensione massima (in MB) di una pagina Web o di un allegato da sottoporre a scansione.
Profondità di scansione	Il numero di livelli dall'URL iniziale a cui sottoporre a scansione. Ad esempio, la pagina URL iniziale ha la profondità 1 e tutti i collegamenti ipertestuali di questa pagina che vengono sottoposti a scansione hanno la profondità 2.

Configurazione	Descrizione
maxLinksPerUrl	Il numero massimo di URL su una pagina Web da includere durante la scansione di un sito Web. Questo numero è per pagina Web. Quando si esegue la scansione delle pagine Web di un sito Web, vengono sottoposti a scansione anche tutti gli URL a cui le pagine Web rimandano. Gli URL di una pagina Web vengono sottoposti a scansione in ordine di visualizzazione.
crawlSubDomain	`true`per eseguire la scansione dei domini del sito Web con sottodomini. Ad esempio, se l'URL iniziale è "abc.example.com«, vengono sottoposti a scansione anche" a.abc.exa mple.com "e" b.abc.example.com ". Se non lo imposti `crawlSubDomain` o `crawlAllD omain` non lo fai`true`, esegue la scansione Amazon Kendra solo dei domini dei siti web che desideri sottoporre a scansione.
crawlAllDomain	`true`per eseguire la scansione dei domini dei siti Web con sottodomini e altri domini a cui si collegano le pagine Web. Se non lo imposti `crawlSubDomain` o non lo fai`true`, esegue `crawlAllDomain` la scansione Amazon Kendra solo dei domini dei siti Web di cui desideri eseguire la scansione.
HonorRobots	`true`per rispettare le direttive robots.txt dei siti Web di cui si desidera eseguire la scansione . Queste direttive controllano il modo in cui Amazon Kendra Web Crawler esegue la scansione dei siti Web, se Amazon Kendra può eseguire la scansione solo di contenuti specifici o non eseguire la scansione di alcun contenuto.

Configurazione	Descrizione
Crawlat/Allegati	`true`per eseguire la scansione dei file a cui si collegano le pagine Web.
• URL di inclusione CrawlPatterns • URL di inclusione IndexPatterns	Un elenco di modelli di espressioni regolari che includono la scansione di determinati URL e l'indicizzazione di eventuali collegamenti ipertestuali su queste pagine Web con URL. Gli URL che corrispondono ai modelli sono inclusi nell'indice. Gli URL che non corrispondono ai modelli sono esclusi dall'indice. Se un URL corrisponde sia a un modello di inclusione che a uno di esclusione, il modello di esclusione ha la precedenza e le pagine Web dell'URL/sito Web non sono incluse nell'indice.
• URL di esclusione CrawlPatterns • URL di esclusione IndexPatterns	Un elenco di modelli di espressioni regolari per escludere la scansione di determinati URL e l'indicizzazione di eventuali collegamenti ipertestuali su queste pagine Web con URL. Gli URL che corrispondono ai modelli sono esclusi dall'indice. Gli URL che non corrispon dono ai modelli sono inclusi nell'indice. Se un URL corrisponde sia a un modello di inclusione che a uno di esclusione, il modello di esclusion e ha la precedenza e le pagine Web dell'URL/ sito Web non sono incluse nell'indice.

Configurazione	Descrizione
inclusionFileIndexSchemi	Un elenco di modelli di espressioni regolari per includere determinati file di pagine Web. I file che corrispondono ai modelli sono inclusi nell'indice. I file che non corrispondono ai modelli sono esclusi dall'indice. Se un file corrisponde sia a un modello di inclusione che di esclusione, il modello di esclusione ha la precedenza e il file non viene incluso nell'indi ce.
exclusionFileIndexPattern	Un elenco di modelli di espressioni regolari per escludere determinati file di pagine Web. I file che corrispondono ai modelli sono esclusi dall'indice. I file che non corrispondono ai modelli sono inclusi nell'indice. Se un file corrisponde sia a un modello di inclusione che a uno di esclusione, il modello di esclusione ha la precedenza e il file non viene incluso nell'indi ce.
proxy	Informazioni sulla configurazione richiesta per effettuare la connessione ai siti Web interni tramite un proxy Web.
host	Il nome host del server proxy che desideri utilizzare per connetterti ai siti Web interni. Ad esempio, il nome host di https://a.example.com/ page1.htmlè "a.example.com».
port	Il numero di porta del server proxy che desideri utilizzare per connetterti ai siti Web interni. Ad esempio, 443 è la porta standard per HTTPS.

Configurazione	Descrizione
SecretArn (proxy)	Se sono necessarie le credenziali del proxy Web per connettersi all'host di un sito Web, è possibile creare un AWS Secrets Manager segreto che memorizza le credenziali. Fornisci l'Amazon Resource Name (ARN) del segreto.
tipo	Il tipo di origine dati. Specificare `WEBCRAWLER V2` come tipo di origine dati.

Configurazione	Descrizione
Segretario ARN	L'Amazon Resource Name (ARN) di un AWS Secrets Manager segreto utilizzato se i tuoi siti Web richiedono l'autenticazione per accedere ai siti Web. Memorizzi le credenzia li di autenticazione per il sito Web nel segreto che contiene coppie chiave-valore JSON. Se utilizzi basic o NTML/Kerberos, inserisci il nome utente e la password. Le chiavi JSON nel segreto devono essere e. `userName` `password` Il protocollo di autenticazione NTLM include l'hashing delle password e il protocollo di autenticazione Kerberos include la crittogra fia delle password. Se utilizzi SAML o l'autenticazione tramite modulo, inserisci il nome utente e la password, XPath per il campo del nome utente (e il pulsante del nome utente se usi SAML), XPaths per il campo e il pulsante della password e l'URL della pagina di accesso. Le chiavi JSON nel segreto devono essere`userName`,,, `password``userNameF ieldXpath` , `userNameButtonXpath` e. `passwordFieldXpath` `passwordB uttonXpath` `loginPageUrl` Puoi trovare gli XPaths (XML Path Language) degli elementi utilizzando gli strumenti di sviluppo del tuo browser web. Gli XPaths di solito seguono questo formato:. `//tagname[@Attribu te='Value']` Amazon Kendra verifica inoltre se le informazi oni sull'endpoint (URL iniziali) incluse nel segreto sono le stesse informazioni sull'endp

Configurazione	Descrizione
	oint specificate nei dettagli di configurazione dell'endpoint dell'origine dati.
version	La versione di questo modello attualmente supportata.

Amazon Kendra Schema JSON di 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"
  ]
}
```

Schema del modello Confluence

Includi un JSON che contiene lo schema dell'origine dati come parte dell'oggetto. TemplateConfiguration Fornisci l'URL dell'host Confluence, il metodo di hosting e il tipo di autenticazione come parte della configurazione della connessione o dei dettagli dell'endpoint del repository. Specificate anche il tipo di origine dati`CONFLUENCEV2`, un segreto per le credenziali di autenticazione e altre configurazioni necessarie. È quindi necessario specificare `TEMPLATE` come `Type` quando si chiama. CreateDataSource

Puoi utilizzare il modello fornito in questa guida per sviluppatori. Per informazioni, consulta Schema JSON di Confluence.

La tabella seguente descrive i parametri dello schema JSON di Confluence.

Configurazione	Descrizione
Configurazione della connessione	Informazioni di configurazione per l'endpoint per l'origine dati.
repositoryEndpointMetadata	Le informazioni sull'endpoint per l'origine dati.
HostUrl	L'URL per la tua istanza Confluence. *Ad esempio, https://example.confluence.com.*
tipo	Il metodo di hosting per l'istanza Confluence, se `SAAS` e. `ON_PREM`
authType	Il metodo di autenticazione per l'istanza di Confluence, if`Basic`, `OAuth2` or. `Personal-token`
Configurazioni del repository	Informazioni di configurazione per il contenuto dell'origine dati. Ad esempio, la configurazione di tipi specifici di contenuti e mappature dei campi.
• spazio • page • blog • comment • attachment	Un elenco di oggetti che mappano gli attributi o i nomi dei campi degli spazi, delle pagine, dei blog, dei commenti e degli allegati di Confluence ai Amazon Kendra nomi dei campi indice. Per ulteriori informazioni, consulta la sezione Mappatura dei campi di origine dei dati. I nomi dei campi dell'origine dei dati Confluence devono essere presenti nei metadati personalizzati di Confluence.
Proprietà aggiuntive	Opzioni di configurazione aggiuntive per i contenuti della fonte di dati.
isCrawlAcl	`true`per eseguire la scansione delle informazioni dell'elenco di controllo degli accessi (ACL) per i documenti, se disponi di un ACL e desideri

Configurazione	Descrizione
	utilizzarlo per il controllo degli accessi. L'ACL specifica a quali documenti possono accedere utenti e gruppi. Le informazioni ACL vengono utilizzate per filtrare i risultati della ricerca in base all'accesso dell'utente o del relativo gruppo ai documenti. Per ulteriori informazioni, consulta Filtraggio del contesto utente.
fieldForUserId	Specificare `email` se si desidera utilizzare l'e-mail dell'utente come ID utente. `email`viene utilizzato per impostazione predefinita ed è attualmente l'unico tipo di ID utente supportato.
• inclusionSpaceKeyFiltro • exclusionSpaceKeyFiltro • pageTitleRegEX • blogTitleRegEX • commentTitleRegEX • attachmentTitleRegEX • inclusionFileTypeSchemi • exclusionFileTypeSchemi • inclusionUrlPatterns • exclusionUrlPatterns	Un elenco di modelli di espressioni regolari per includere e/o escludere determinati file nella fonte dati Confluence. I file che corrispondono ai modelli sono inclusi nell'indice. I file che non corrispondono ai modelli sono esclusi dall'indi ce. Se un file corrisponde sia a un modello di esclusione sia a un modello di inclusione, il modello di esclusione ha la precedenza e il file non viene incluso nell'indice.
ProxyHost	Il nome host del proxy web che utilizzi, senza il protocollo `http://` or`https://`.
ProxyPort	Il numero di porta utilizzato dal protocollo di trasporto dell'URL dell'host. Deve essere un valore numerico compreso tra 0 e 65535.

Configurazione	Descrizione
• isCrawlPersonalSpazio • isCrawlArchivedSpazio • isCrawlArchivedPagina • isCrawlPage • isCrawlBlog • isCrawlPageCommento • isCrawlPageAllegato • isCrawlBlogCommento • isCrawlBlogAllegato	`true`per eseguire la scansione dei file negli spazi personali, nelle pagine, nei blog, nei commenti alle pagine, negli allegati delle pagine, nei commenti e negli allegati del blog di Confluence.
maxFileSizeInMegaBytes	Specificate il limite di dimensione del file in MB che può essere sottoposto a scansione . Amazon Kendra Amazon Kendra esegue la scansione solo dei file entro il limite di dimensione definito. La dimensione predefinita del file è 50 MB. La dimensione massima del file deve essere superiore a 0 MB e inferiore o uguale a 50 MB.
tipo	Il tipo di origine dati. Specificare `CONFLUENCEV2` come tipo di origine dati.
enableIdentityCrawler	`true`utilizzare il crawler Amazon Kendra di identità per sincronizzare le informazioni sull'identità/principali su utenti e gruppi con accesso a determinati documenti. Se il crawler di identità è disattivato, tutti i documenti possono essere ricercati pubblicamente. Se desideri utilizzare il controllo degli accessi per i tuoi documenti e il crawler di identità è disattivato, in alternativa puoi utilizzare l'PutPrincipalMappingAPI per caricare le informazioni di accesso di utenti e gruppi.

Configurazione	Descrizione
SyncMode	Specificate come Amazon Kendra aggiornar e l'indice quando il contenuto dell'origine dati cambia. Puoi scegliere tra: • `FORCED_FULL_CRAWL` per indicizzare nuovamente tutti i contenuti, sostituendo i contenuti esistenti ogni volta che l'origine dati si sincronizza con l'indice. • `FULL_CRAWL` per indicizzare solo i contenuti nuovi, modificati ed eliminati ogni volta che l'origine dati si sincronizza con l'indice. Amazon Kendra può utilizzare il meccanism o dell'origine dati per tenere traccia delle modifiche ai contenuti e indicizzare i contenuti modificati dall'ultima sincroniz zazione.
Secretary ARN	L'Amazon Resource Name (ARN) di un AWS Secrets Manager segreto che contiene le coppie chiave-valore necessarie per connetter si a Confluence. Per informazioni su queste coppie chiave-valore, consulta le istruzioni di connessione per Confluence.
version	La versione di questo modello attualmente supportata.

Schema JSON di Confluence

```
{
  "$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"
  ]
```

```
}
```

Schema del modello Dropbox

Includi un JSON che contiene lo schema dell'origine dati come parte dell'TemplateConfigurationoggetto. Fornisci la chiave dell'app Dropbox, il segreto dell'app e il token di accesso come parte del segreto che memorizza le tue credenziali di autenticazione. Specificate inoltre il tipo di origine dati`DROPBOX`, il tipo di token di accesso che desiderate utilizzare (temporaneo o permanente) e altre configurazioni necessarie. È quindi necessario specificare `TEMPLATE` come `Type` quando si chiama CreateDataSource.

Puoi utilizzare il modello fornito in questa guida per sviluppatori. Per informazioni, consulta Schema JSON di Dropbox.

La tabella seguente descrive i parametri dello schema JSON di Dropbox.

Configurazione	Descrizione
Configurazione della connessione	Informazioni di configurazione per l'endpoint per l'origine dati.
repositoryEndpointMetadata	Le informazioni sull'endpoint per l'origine dati. Questa fonte di dati non specifica un endpoint in. `repositoryEndpointMetadata` Piuttosto, le informazioni di connessione sono incluse in un AWS Secrets Manager segreto fornito dall'`secretArn` utente.
Configurazioni del repository	Informazioni di configurazione per il contenuto dell'origine dati. Ad esempio, la configurazione di tipi specifici di contenuti e mappature dei campi.
• file • paper • carta • scorciatoia	Un elenco di oggetti che mappano gli attributi o i nomi dei campi dei tuoi file Dropbox, Dropbox Paper e scorciatoie per Amazon Kendra indicizzare i nomi dei campi. Per ulteriori informazioni, consulta la sezione Mappatura dei campi di origine dei dati.

Configurazione	Descrizione
Secretarn	L'Amazon Resource Name (ARN) di un AWS Secrets Manager segreto che contiene le coppie chiave-valore necessarie per connettersi al tuo Dropbox. Il segreto deve contenere una struttura JSON con le seguenti chiavi: `{ "appKey": "Dropbox app key", "appSecret": " Dropbox app secret", "accesstoken": " temporary access token or refresh access token" }`
Proprietà aggiuntive	Opzioni di configurazione aggiuntive per i contenuti della fonte di dati.
• inclusionFileNameSchemi • inclusionFileTypeSchemi	Un elenco di modelli di espressioni regolari per includere determinati nomi e tipi di file nella tua fonte di dati Dropbox. I file che corrispondono ai modelli sono inclusi nell'indice. I file che non corrispondono ai modelli sono esclusi dall'indi ce. Se un file corrisponde sia a un modello di esclusione sia a un modello di inclusione, il modello di esclusione ha la precedenza e il file non viene incluso nell'indice.
• exclusionFileNamePattern • exclusionFileTypeSchemi	Un elenco di modelli di espressioni regolari per escludere determinati nomi e tipi di file dalla tua fonte di dati Dropbox. I file che corrispondono ai modelli sono esclusi dall'indice. I file che non corrispondono ai modelli sono inclusi nell'indi ce. Se un file corrisponde sia a un modello di esclusione che a uno di inclusione, il modello di esclusione ha la precedenza e il file non viene incluso nell'indice.

Configurazione	Descrizione
• Scansiona il file • Carta strisciata • Carta strisciata T • Scorciatoia Crawl	`true`per scansionare i file nei tuoi documenti Dropbox, Dropbox Paper, modelli di Dropbox Paper e collegamenti alle pagine web archiviati nel tuo Dropbox.
tipo	Il tipo di fonte di dati. Specificare `DROPBOX` come tipo di origine dati.
useChangeLog	`true`per utilizzare il registro delle modifiche di Dropbox per determinare quali documenti devono essere aggiunti, aggiornati o eliminati nell'indice. A seconda delle dimensioni del registro delle modifiche, l'utilizzo del registro delle modifiche potrebbe richiedere Amazon Kendra più tempo rispetto alla scansione di tutti i documenti nel tuo Dropbox.
TokenType	Specificate il tipo di token di accesso: token di accesso permanente o temporaneo. Ti consigliamo di creare un token di accesso di aggiornamento che non scada mai in Dropbox anziché affidarti a un token di accesso monouso che scade dopo 4 ore. Crei un'app e un token di accesso per l'aggiornamento nella console per sviluppatori Dropbox e fornisci il token di accesso come segreto.
version	La versione di questo modello attualmente supportata.

Schema JSON di Dropbox

```
{
  "$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"
  ]
```

```
}
```

Schema del modello Drupal

Includi un JSON che contiene lo schema dell'origine dati come parte dell'oggetto. TemplateConfiguration Fornisci l'URL dell'host Drupal e il tipo di autenticazione come parte della configurazione della connessione o dei dettagli dell'endpoint del repository. Specificate anche il tipo di fonte di dati come DRUPAL, un segreto per le vostre credenziali di autenticazione e altre configurazioni necessarie. Quindi specifichi `TEMPLATE` come quando chiami. `Type` CreateDataSource

Puoi utilizzare il modello fornito in questa guida per sviluppatori. Per informazioni, consulta Schema JSON di Drupal.

La tabella seguente descrive i parametri dello schema JSON di Drupal.

Configurazione	Descrizione
Configurazione della connessione	Informazioni di configurazione per l'endpoint per l'origine dati.
repositoryEndpointMetadata	Le informazioni sull'endpoint per l'origine dati.
HostUrl	L'URL host del tuo sito web Drupal. <hostname ><drupalsitename>Ad esempio, *`https:///`* .
Configurazioni del repository	Informazioni di configurazione per il contenuto dell'origine dati.
• contenuto • comment • attachment	Un elenco di oggetti che mappano gli attributi o i nomi dei campi dei file Drupal. Per ulteriori informazioni, consulta la sezione Mappatura dei campi di origine dei dati. I nomi dei campi delle sorgenti dati Drupal devono esistere nei metadati personalizzati di Drupal.
Proprietà aggiuntive	Opzioni di configurazione aggiuntive per i contenuti della fonte di dati.

Configurazione	Descrizione
• inclusionFileNameSchemi • articleTitleInclusionSchemi • pageTitleInclusionSchemi • customContentTitleInclusionPatterns • basicBlockTitleInclusionPatterns • customBlockTitleInclusionPatterns	Un elenco di modelli di espressioni regolari per includere determinati file nella fonte di dati Drupal. I file che corrispondono ai modelli sono inclusi nell'indice. I file che non corrispondono ai modelli sono esclusi dall'indice. Se un file corrisponde sia a un modello di esclusione sia a un modello di inclusione, il modello di esclusione ha la precedenza e il file non viene incluso nell'indice.
• exclusionFileNamePattern • articleTitleExclusionSchemi • pageTitleExclusionSchemi • customContentTitleExclusionPatterns • basicBlockTitleExclusionPatterns • customBlockTitleExclusionPatterns	Un elenco di modelli di espressioni regolari per escludere determinati file nella fonte di dati Drupal. I file che corrispondono ai modelli sono esclusi dall'indice. I file che non corrispondono ai modelli sono inclusi nell'indice. Se un file corrisponde sia a un modello di esclusione che a uno di inclusione, il modello di esclusione ha la precedenza e il file non viene incluso nell'indi ce.
Definizioni dei contenuti • contentType • Definizione del campo • isCrawlComments • isCrawlFiles • isCrawlArticle • isCrawlBasicPagina • isCrawlBasicBlocca • isCrawlCustomContentTypesList	Specificate i tipi di contenuto da sottoporr e a scansione e se eseguire la scansione di commenti e allegati per i tipi di contenuto selezionati.
tipo	Il tipo di origine dati. Specificare `DRUPAL` come tipo di origine dati.

Configurazione	Descrizione
authType	Il tipo di autenticazione che usi, se `BASIC-AUTH` o `OAUTH2`.
SyncMode	Specificate come Amazon Kendra aggiornare l'indice quando il contenuto dell'origine dati cambia. Puoi scegliere tra: • `FORCED_FULL_CRAWL` per indicizzare nuovamente tutti i contenuti, sostituendo i contenuti esistenti ogni volta che l'origine dati si sincronizza con l'indice. • `FULL_CRAWL` per indicizzare solo i contenuti nuovi, modificati ed eliminati ogni volta che l'origine dati si sincronizza con l'indice. Amazon Kendra può utilizzare il meccanismo dell'origine dati per tenere traccia delle modifiche ai contenuti e indicizzare i contenuti modificati dall'ultima sincronizzazione. • `CHANGE_LOG` per indicizzare solo contenuti nuovi e modificati ogni volta che l'origine dati si sincronizza con l'indice. Amazon Kendra può utilizzare il meccanismo dell'origine dati per tenere traccia delle modifiche ai contenuti e indicizzare i contenuti modificati dall'ultima sincronizzazione.

Configurazione	Descrizione
enableIdentityCrawler	`true`utilizzare il crawler Amazon Kendra di identità per sincronizzare le informazioni sull'identità/principali su utenti e gruppi con accesso a determinati documenti. Se il crawler di identità è disattivato, tutti i documenti possono essere ricercati pubblicamente. Se desideri utilizzare il controllo degli accessi per i tuoi documenti e il crawler di identità è disattivato, in alternativa puoi utilizzare l'PutPrincipalMappingAPI per caricare le informazioni di accesso di utenti e gruppi.

Secretarn	L'Amazon Resource Name (ARN) di un AWS Secrets Manager segreto che contiene le coppie chiave-valore necessarie per connettersi a Drupal. Il segreto deve contenere una struttura JSON con le seguenti chiavi:
	
	Se utilizzi l'autenticazione di base:
	
	`{ "username": "user name", "passwords": "password" }`
	
	Se si utilizza l'autenticazione OAuth 2.0:
	
	`{ "username": "user name", "password": "password" , "clientId": "client id", "clientSecret": "client secret" }`

version	La versione di questo modello attualmente supportata.

Schema JSON di 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 schema modello

Includi un JSON che contiene lo schema dell'origine dati come parte dell'TemplateConfigurationoggetto. Fornisci l'URL dell' GitHub host, il nome dell'organizzazione e se utilizzi il GitHub cloud o in GitHub locale come parte della configurazione della connessione o dei dettagli dell'endpoint del repository. Specificate anche il tipo di origine dati`GITHUB`, un segreto per le credenziali di autenticazione e altre configurazioni necessarie. È quindi necessario specificare `TEMPLATE` come `Type` quando si chiama. CreateDataSource

Puoi utilizzare il modello fornito in questa guida per sviluppatori. Per informazioni, consulta GitHub Schema JSON.

La tabella seguente descrive i parametri dello schema GitHub JSON.

Configurazione	Descrizione
Configurazione della connessione	Informazioni di configurazione per l'endpoint per l'origine dati.
repositoryEndpointMetadata	Le informazioni sull'endpoint per l'origine dati.
tipo	Specificate il tipo come `SAAS` o`ON_PREMISE` .
HostUrl	L'URL dell' GitHub host. Ad esempio, se utilizzi GitHub SaaS/Enterprise Cloud:. https://api.github.com Oppure, se utilizzi GitHub On-premise/Enterprise Server:. https://on-prem-host-url/api/v3/
Nome dell'organizzazione	Puoi trovare il nome della tua organizzazione quando accedi al GitHub desktop e vai alla sezione Le mie organizzazioni nel menu a discesa dell'immagine del profilo.
Configurazioni del repository	Informazioni di configurazione per il contenuto dell'origine dati. Ad esempio, la configurazione di tipi specifici di contenuti e mappature dei campi.

Configurazione	Descrizione
• GHRepository • GH Commit • ghIssueDocument • ghIssueComment • ghIssueAttachment • Documento GHPR • Commento GHPR • Allegato GHPR	Un elenco di oggetti che mappano gli attributi o i nomi di campo dei tuoi GitHub contenuti per Amazon Kendra indicizzare i nomi dei campi. Per ulteriori informazioni, consulta la sezione Mappatura dei campi di origine dei dati.
Proprietà aggiuntive	Opzioni di configurazione aggiuntive per i contenuti della fonte di dati.
isCrawlAcl	`true`per eseguire la scansione delle informazioni dell'elenco di controllo degli accessi (ACL) per i documenti, se disponi di un ACL e desideri utilizzarlo per il controllo degli accessi. L'ACL specifica a quali documenti possono accedere e cercare utenti e gruppi. Le informazioni ACL vengono utilizzate per filtrare i risultati della ricerca in base all'accesso dell'utente o del relativo gruppo ai documenti. Per ulteriori informazioni, consulta Filtraggio del contesto utente.
fieldForUserId	Specificate il tipo di ID utente che desiderate utilizzare per la scansione ACL. Specificate `email` se desiderate utilizzare l'e-mail dell'utente per l'ID utente o `username` se desiderate utilizzare il nome utente per l'ID utente. Se non si specifica un'opzione, `email` viene utilizzata per impostazione predefinita.
RepositoryFilter	Un elenco di nomi dei repository e dei nomi dei rami specifici che desideri indicizzare.

Configurazione	Descrizione
CrawlRepository	`true`per eseguire la scansione dei repository.
crawlRepositoryDocuments	`true`per eseguire la scansione dei documenti del repository.
problema di scansione	`true`problemi di scansione.
crawlIssueComment	`true`per scansionare i commenti dei problemi.
crawlIssueCommentAllegato	`true`per eseguire la scansione degli allegati dei commenti.
crawlPullRequest	`true`per eseguire la scansione delle richieste pull.
crawlPullRequestCommento	`true`per scansionare i commenti della richiesta .
crawlPullRequestCommentAttachment	`true`per eseguire la scansione degli allegati dei commenti della richiesta.
• inclusionFolderNameSchemi • inclusionFileTypeSchemi • inclusionFileNameSchemi	Un elenco di modelli di espressioni regolari per includere determinati contenuti nella fonte di GitHub dati. I contenuti che corrispondono ai modelli sono inclusi nell'indice. I contenuti che non corrispondono ai modelli sono esclusi dall'indice. Se un contenuto corrisponde sia a un modello di inclusione che a uno di esclusion e, il modello di esclusione ha la precedenza e il contenuto non viene incluso nell'indice.

Configurazione	Descrizione
• exclusionFolderNameSchemi • exclusionFileTypeSchemi • exclusionFileNameSchemi	Un elenco di modelli di espressioni regolari per escludere determinati contenuti nella fonte di GitHub dati. I contenuti che corrispondono ai modelli sono esclusi dall'indice. I contenuti che non corrispondono ai modelli sono inclusi nell'indice. Se un contenuto corrisponde sia a un modello di inclusione che a uno di esclusion e, il modello di esclusione ha la precedenza e il contenuto non viene incluso nell'indice.
tipo	Il tipo di origine dati. Specificare `GITHUB` come tipo di origine dati.
enableIdentityCrawler	`true`utilizzare il crawler Amazon Kendra di identità per sincronizzare le informazi oni sull'identità/principali su utenti e gruppi con accesso a determinati documenti. Se il crawler di identità è disattivato, tutti i documenti possono essere ricercati pubblicamente. Se desideri utilizzare il controllo degli accessi per i tuoi documenti e il crawler di identità è disattiva to, in alternativa puoi utilizzare l'PutPrinci palMappingAPI per caricare le informazioni di accesso di utenti e gruppi.

Configurazione	Descrizione
SyncMode	Specificate come Amazon Kendra aggiornar e l'indice quando il contenuto dell'origine dati cambia. Puoi scegliere tra: • `FORCED_FULL_CRAWL` per indicizzare nuovamente tutti i contenuti, sostituendo i contenuti esistenti ogni volta che l'origine dati si sincronizza con l'indice. • `FULL_CRAWL` per indicizzare solo i contenuti nuovi, modificati ed eliminati ogni volta che l'origine dati si sincronizza con l'indice. Amazon Kendra può utilizzare il meccanism o dell'origine dati per tenere traccia delle modifiche ai contenuti e indicizzare i contenuti modificati dall'ultima sincroniz zazione. • `CHANGE_LOG` per indicizzare solo contenuti nuovi e modificati ogni volta che l'origine dati si sincronizza con l'indice. Amazon Kendra può utilizzare il meccanismo dell'origine dati per tenere traccia delle modifiche ai contenuti e indicizzare i contenuti modificati dall'ultima sincronizzazione.
Secretary ARN	L'Amazon Resource Name (ARN) di un AWS Secrets Manager segreto che contiene le coppie chiave-valore necessarie per connetter si al tuo. GitHub Il segreto deve contenere una struttura JSON con le seguenti chiavi: `{ "personalToken": " token" }`

Configurazione	Descrizione
version	La versione di questo modello attualmente supportata.

GitHub Schema JSON

Di seguito è riportato lo schema 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"
    ]
}
```

Schema del modello Gmail

Includi un JSON che contiene lo schema dell'origine dati come parte dell'TemplateConfigurationoggetto. Specificate il tipo di origine dati`GMAIL`, un segreto per le credenziali di autenticazione e altre configurazioni necessarie. È quindi necessario specificare `TEMPLATE` come `Type` quando si chiama. CreateDataSource

Puoi utilizzare il modello fornito in questa guida per sviluppatori. Per informazioni, consulta Schema JSON di Gmail.

La tabella seguente descrive i parametri dello schema JSON di Gmail.

Configurazione	Descrizione
Configurazione della connessione	Informazioni di configurazione per l'endpoint per l'origine dati.
Configurazioni del repository	Informazioni di configurazione per il contenuto dell'origine dati. Ad esempio, la configurazione di tipi specifici di contenuti e mappature dei

Configurazione	Descrizione
	campi. Specificare il tipo di origine dati e l'ARN segreto.
• message • allegati	Un elenco di oggetti che mappano gli attributi o i nomi dei campi dei messaggi e degli allegati di Gmail ai nomi dei campi Amazon Kendra indicizzati. Per ulteriori informazioni, consulta la sezione Mappatura dei campi di origine dei dati.
Proprietà aggiuntive	Opzioni di configurazione aggiuntive per i contenuti della fonte di dati.
• inclusionLabelNameSchemi • exclusionLabelNameSchemi • inclusionAttachmentTypeSchemi • exclusionAttachmentTypeSchemi • inclusionAttachmentNameSchemi • exclusionAttachmentNameSchemi • inclusionSubjectFilter • exclusionSubjectFilter • isSubjectAnd • inclusionFromFilter • exclusionFromFilter • inclusionToFilter • exclusionToFilter • inclusionCcFilter • exclusionCcFilter • inclusionBccFilter • exclusionBccFilter	Un elenco di modelli di espressioni regolari per includere o escludere messaggi con nomi di oggetto specifici nell'origine dati di Gmail. I file che corrispondono ai modelli sono inclusi nell'indice. Se un file corrisponde sia a un modello di inclusione che a uno di esclusione, il modello di esclusione ha la precedenza e il file non viene incluso nell'indice.
beforeDateFilter	Specificate i messaggi e gli allegati da includere prima di una certa data.

Configurazione	Descrizione
afterDateFilter	Specificate i messaggi e gli allegati da includere dopo una certa data.
isCrawlAttachment	Un valore booleano per scegliere se scansiona re gli allegati. I messaggi vengono sottoposti a scansione automatica.
tipo	Il tipo di origine dati. Specificare `GMAIL` come tipo di origine dati.
shouldCrawlDraftMessaggi	Un valore booleano per scegliere se scansiona re le bozze dei messaggi.

Configurazione	Descrizione
SyncMode	Specificate come Amazon Kendra aggiornar e l'indice quando il contenuto dell'origine dati cambia. Puoi scegliere tra: • `FORCED_FULL_CRAWL` per indicizzare nuovamente tutti i contenuti, sostituendo i contenuti esistenti ogni volta che l'origine dati si sincronizza con l'indice. • `FULL_CRAWL` per indicizzare solo i contenuti nuovi, modificati ed eliminati ogni volta che l'origine dati si sincronizza con l'indice. Amazon Kendra può utilizzare il meccanism o dell'origine dati per tenere traccia delle modifiche ai contenuti e indicizzare i contenuti modificati dall'ultima sincroniz zazione. **Important** Poiché non esiste un'API per aggiornar e i messaggi Gmail eliminati definitiv amente, qualsiasi contenuto nuovo, modificato o eliminato viene sincroniz zato: • Non rimuoverà dal tuo indice i messaggi eliminati definitivamente da Gmail Amazon Kendra • Non sincronizzerà le modifiche nelle etichette delle email di Gmail Per sincronizzare le modifiche alle etichette delle sorgenti dati di Gmail e i messaggi email eliminati definitiv

Configurazione	Descrizione
	amente con il tuo Amazon Kendra indice, devi eseguire periodicamente ricerche per indicizzazione complete.
Segretario ARN	L'Amazon Resource Name (ARN) di un segreto di Secrets Manager che contiene le coppie chiave-valore necessarie per connettersi a Gmail. Il segreto deve contenere una struttura JSON con le seguenti chiavi: `{ "adminAccountEmailId": " service account email", "clientEmailId": " user account email", "privateKey": " private key" }`
version	La versione del modello attualmente supportat a.

Schema JSON di 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"
  ]
}
```

Schema del modello di Google Drive

Includi un JSON che contiene lo schema dell'origine dati come parte dell'TemplateConfigurationoggetto. Specificate il tipo di origine datiGOOGLEDRIVE2, un segreto per le credenziali di autenticazione e altre configurazioni necessarie. È quindi necessario specificare `TEMPLATE` come `Type` quando si chiama. CreateDataSource

Puoi utilizzare il modello fornito in questa guida per sviluppatori. Per informazioni, consulta Schema JSON di Google Drive.

La tabella seguente descrive i parametri dello schema JSON di Google Drive.

Configurazione	Descrizione
Configurazione della connessione	Informazioni di configurazione per l'origine dati.
repositoryEndpointMetadata	Le informazioni sull'endpoint per l'origine dati. Questa fonte di dati non specifica un endpoint. Scegli il tipo di autenticazione: `serviceAccount` e `OAuth2`. Le informazioni di connessione sono incluse in un AWS Secrets Manager segreto fornito dall'utente`secretArn` .
authType	Scegli tra `serviceAccount` e `OAuth2` in base al tuo caso d'uso.

Configurazione	Descrizione
Configurazioni del repository	Informazioni di configurazione per il contenuto dell'origine dati. Ad esempio, la configurazione di tipi specifici di contenuti e mappature dei campi.
• file • comment	Un elenco di oggetti che mappano gli attributi o i nomi dei campi di Google Drive per Amazon Kendra indicizzare i nomi dei campi. Per ulteriori informazioni, consulta la sezione Mappatura dei campi di origine dei dati.
Proprietà aggiuntive	Opzioni di configurazione aggiuntive per i contenuti della fonte di dati
• maxFileSizeInMegaBytes	Specificate un limite di dimensione del file in MB che Amazon Kendra deve essere sottopost o a scansione.
• isCrawlComment	`true`per eseguire la scansione dei commenti nella tua fonte di dati Google Drive.
• isCrawlMyDriveAndSharedWithMe	`true`per scansionare MyDrive e condividere le unità con me nella tua fonte di dati Google Drive.
• isCrawlSharedUnità	`true`per eseguire la scansione dei Drive condivisi nella tua fonte di dati Google Drive.

Configurazione	Descrizione
isCrawlAcl	`true`per eseguire la scansione delle informazioni dell'elenco di controllo degli accessi (ACL) per i tuoi documenti, se disponi di un ACL e desideri utilizzarlo per il controllo degli accessi. L'ACL specifica a quali documenti possono accedere e cercare utenti e gruppi. Le informazioni ACL vengono utilizzate per filtrare i risultati della ricerca in base all'accesso dell'utente o del relativo gruppo ai documenti. Per ulteriori informazioni, consulta Filtraggio del contesto utente.
• excludeUserAccounts • excludeSharedDrives • excludeMimeTypes • exclusionFileTypeSchemi • exclusionFileNameSchemi • exclusionFilePathFiltro	Un elenco di modelli di espressioni regolari per escludere determinati file nella fonte di dati di Google Drive. I file che corrispondono ai modelli sono esclusi dall'indice. I file che non corrispondono ai modelli sono inclusi nell'indice. Se un file corrisponde sia a un modello di esclusione che a uno di inclusione, il modello di esclusione ha la precedenza e il file non viene incluso nell'indice.
• includeUserAccounts • includeSharedDrives • includeMimeTypes • inclusionFileTypePattern • inclusionFileNameSchemi • inclusionFilePathFiltro	Un elenco di modelli di espressioni regolari per includere determinati file nella fonte di dati di Google Drive. I file che corrispondono ai modelli sono inclusi nell'indice. I file che non corrispondono ai modelli sono esclusi dall'indice. Se un file corrisponde sia a un modello di inclusione che di esclusione, il modello di esclusione ha la precedenza e il file non viene incluso nell'indice.
tipo	Il tipo di origine dati. Specificare `GOOGLEDRIVEV2` come tipo di origine dati.

Configurazione	Descrizione
enableIdentityCrawler	`true`utilizzare il crawler Amazon Kendra di identità per sincronizzare le informazioni sull'identità/principali su utenti e gruppi con accesso a determinati documenti. Se il crawler di identità è disattivato, tutti i documenti possono essere ricercati pubblicamente. Se desideri utilizzare il controllo degli accessi per i tuoi documenti e il crawler di identità è disattivato, in alternativa puoi utilizzare l'PutPrincipalMappingAPI per caricare le informazioni di accesso di utenti e gruppi.

Configurazione	Descrizione
SyncMode	Specificate come Amazon Kendra aggiornar e l'indice quando il contenuto dell'origine dati cambia. Puoi scegliere tra: • `FORCED_FULL_CRAWL` per indicizzare nuovamente tutti i contenuti, sostituendo i contenuti esistenti ogni volta che l'origine dati si sincronizza con l'indice. • `FULL_CRAWL` per indicizzare solo i contenuti nuovi, modificati ed eliminati ogni volta che l'origine dati si sincronizza con l'indice. Amazon Kendra può utilizzare il meccanism o dell'origine dati per tenere traccia delle modifiche ai contenuti e indicizzare i contenuti modificati dall'ultima sincroniz zazione. • `CHANGE_LOG` per indicizzare solo contenuti nuovi e modificati ogni volta che l'origine dati si sincronizza con l'indice. Amazon Kendra può utilizzare il meccanismo dell'origine dati per tenere traccia delle modifiche ai contenuti e indicizzare i contenuti modificati dall'ultima sincronizzazione.

Configurazione	Descrizione

Secretary ARN	L'Amazon Resource Name (ARN) di un AWS Secrets Manager segreto che contiene le coppie chiave-valore necessarie per connettersi a Google Drive. Il segreto deve contenere una struttura JSON con le seguenti chiavi:
	
	Se utilizzi l'autenticazione dell'account di servizio Google:
	
	`{ "clientEmail": " user account email", "adminAccountEmail": " service account email", "privateKey": " private key" }`
	
	Se si utilizza l'autenticazione OAuth 2.0:
	
	`{ "clientID": " OAuth client ID", "clientSecret": " client secret", "refreshToken": " refresh token" }`

version	La versione di questo modello attualmente supportata.

Schema JSON di Google Drive

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

Schema del modello IBM DB2

Includi un JSON che contiene lo schema dell'origine dati come parte dell'oggetto. TemplateConfiguration Specificate il tipo di origine dati come`JDBC`, il tipo di database come`db2`, un segreto per le credenziali di autenticazione e altre configurazioni necessarie. È quindi necessario specificare `TEMPLATE` come `Type` quando si chiama. CreateDataSource

Puoi utilizzare il modello fornito in questa guida per sviluppatori. Per informazioni, consulta Schema JSON IBM DB2.

La tabella seguente descrive i parametri dello schema JSON IBM DB2.

Configurazione	Descrizione
Configurazione della connessione	Informazioni di configurazione per l'endpoint per l'origine dati.

Configurazione	Descrizione
repositoryEndpointMetadata	Informazioni di configurazione necessarie per connettere la fonte di dati. • dbType: il tipo di database Java utilizzat o, indipendentemente dal fatto che si tratti di `mysql`, `db2` `postgresql` , `oracle` o. `sqlserver` • dbHost: il nome host del database. • dbPort: la porta del database. • dbInstance: l'istanza del database.
Configurazioni del repository	Informazioni di configurazione per il contenuto dell'origine dati. Ad esempio, la configurazione di tipi specifici di contenuti e mappature dei campi. Specificare il tipo di origine dati e l'ARN segreto.
documento	Un elenco di oggetti che mappano gli attributi o i nomi di campo del contenuto del database per Amazon Kendra indicizzare i nomi dei campi. Per ulteriori informazioni, consulta la sezione Mappatura dei campi di origine dei dati.
Proprietà aggiuntive	Opzioni di configurazione aggiuntive per i contenuti della fonte di dati. Utilizzatelo per includere o escludere contenuti specifici nella fonte di dati del database.
Chiave primaria	Fornisci la chiave primaria per la tabella del database. Questo identifica una tabella all'inter no del database.
Colonna del titolo	Fornisci il nome della colonna del titolo del documento all'interno della tabella del database.

Configurazione	Descrizione
Corpo/colonna	Fornisci il nome della colonna del titolo del documento all'interno della tabella del database.
sqlQuery	Inserisci istruzioni di query SQL come le operazioni SELECT e JOIN. Le query SQL devono pesare meno di 32 KB. Amazon Kendra eseguirà la scansione di tutto il contenuto del database che corrisponde alla tua query.
colonna Timestamp	Inserisci il nome della colonna che contiene i timestamp. Amazon Kendra utilizza le informazioni relative alla marca temporale per rilevare le modifiche ai contenuti e sincronizzare solo i contenuti modificati.
formato Timestamp	Inserisci il nome della colonna che contiene i formati di timestamp da utilizzare per rilevare le modifiche ai contenuti e risincronizzare i contenuti.
timezone	Inserisci il nome della colonna che contiene i fusi orari per il contenuto da sottoporre a scansione.
changeDetectingColumns	Inserisci i nomi delle colonne che Amazon Kendra verranno utilizzate per rilevare le modifiche al contenuto. Amazon Kendra reindicizzerà il contenuto in caso di modifica in una di queste colonne
allowedUsersColumns	Inserisci il nome della colonna che contiene gli ID utente a cui consentire l'accesso ai contenuti .

Configurazione	Descrizione
allowedGroupsColumn	Inserisci il nome della colonna che contiene gli ID utente a cui consentire l'accesso ai contenuti .
SourceURIColumn	Inserisci il nome della colonna che contiene gli URL di origine da indicizzare.
isSslEnabled	Inserisci istruzioni di query SQL come le operazioni SELECT e JOIN. Le query SQL devono pesare meno di 32 KB. Amazon Kendra eseguirà la scansione di tutto il contenuto del database che corrisponde alla tua query.
tipo	Il tipo di fonte di dati. Specificare `JDBC` come tipo di origine dati.

Configurazione	Descrizione
SyncMode	Specificate come Amazon Kendra aggiornar e l'indice quando il contenuto dell'origine dati cambia. Puoi scegliere tra: • `FORCED_FULL_CRAWL` per indicizzare nuovamente tutti i contenuti, sostituendo i contenuti esistenti ogni volta che l'origine dati si sincronizza con l'indice. • `FULL_CRAWL` per indicizzare solo i contenuti nuovi, modificati ed eliminati ogni volta che l'origine dati si sincronizza con l'indice. Amazon Kendra può utilizzare il meccanism o dell'origine dati per tenere traccia delle modifiche ai contenuti e indicizzare i contenuti modificati dall'ultima sincroniz zazione. • `CHANGE_LOG` per indicizzare solo contenuti nuovi e modificati ogni volta che l'origine dati si sincronizza con l'indice. Amazon Kendra può utilizzare il meccanismo dell'origine dati per tenere traccia delle modifiche ai contenuti e indicizzare i contenuti modificati dall'ultima sincronizzazione.
Secretary ARN	L'Amazon Resource Name (ARN) di un segreto di Secrets Manager che contiene il nome utente e la password necessari per connetter si al database. Il segreto deve contenere una struttura JSON con le seguenti chiavi: `{ "user name": "database user name", "password": " password" }`

Configurazione	Descrizione
version	La versione del modello attualmente supportata.

Schema JSON IBM DB2

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

Schema del modello di Microsoft Exchange

Includi un JSON che contiene lo schema dell'origine dati come parte dell'TemplateConfigurationoggetto. L'ID del tenant viene fornito come parte della configurazione della connessione o dei dettagli dell'endpoint del repository. Specificate anche il tipo di origine dati`MSEXCHANGE`, un segreto per le credenziali di autenticazione e altre configurazioni necessarie. È quindi necessario specificare `TEMPLATE` come `Type` quando si chiama. CreateDataSource

Puoi utilizzare il modello fornito in questa guida per sviluppatori. Per informazioni, consulta Schema JSON di Microsoft Exchange.

La tabella seguente descrive i parametri dello schema JSON di Microsoft Exchange.

Configurazione	Descrizione
Configurazione della connessione	Informazioni di configurazione per l'endpoint per l'origine dati.
repositoryEndpointMetadata	Le informazioni sull'endpoint per l'origine dati.
TenantID	L'ID tenant di Microsoft 365. Puoi trovare il tuo ID tenant nelle proprietà del tuo portale di Azure Active Directory o nell'applicazione OAuth.
Configurazioni del repository	Informazioni di configurazione per il contenuto dell'origine dati. Ad esempio, la configurazione di tipi specifici di contenuti e mappature dei campi.
• e-mail • attachment • calendario • contatta • notes	Un elenco di oggetti che mappano gli attributi o i nomi di campo dell'origine dati di Microsoft Exchange ai campi Amazon Kendra indicizza ti. Per ulteriori informazioni, consulta la sezione Mappatura dei campi di origine dei dati.
Proprietà aggiuntive	Opzioni di configurazione aggiuntive per il contenuto dell'origine dati

Configurazione	Descrizione
Modelli di inclusione	Un elenco di modelli di espressioni regolari per includere determinati file nell'origine dati di Microsoft Exchange. I file che corrispondono ai modelli sono inclusi nell'indice. I file che non corrispondono ai modelli sono esclusi dall'indi ce. Se un file corrisponde sia a un modello di esclusione sia a un modello di inclusione, il modello di esclusione ha la precedenza e il file non viene incluso nell'indice.
Modelli di esclusione	Un elenco di modelli di espressioni regolari per escludere determinati file nell'origine dati Microsoft Exchange. I file che corrispondono ai modelli sono esclusi dall'indice. I file che non corrispondono ai modelli sono inclusi nell'indi ce. Se un file corrisponde sia a un modello di esclusione che a uno di inclusione, il modello di esclusione ha la precedenza e il file non viene incluso nell'indice.
• inclusionUsersList • inclusionUsersFileNome • inclusionDomainUsers	Un elenco di modelli di espressioni regolari per includere determinati utenti e file utente nell'origine dati di Microsoft Exchange. Gli utenti che corrispondono ai modelli sono inclusi nell'indice. Gli utenti che non corrispondono ai modelli sono esclusi dall'indice. Se un utente soddisfa sia un modello di inclusione che uno di esclusione, il modello di esclusione ha la precedenza e l'utente non viene incluso nell'indi ce.

Configurazione	Descrizione
• exclusionUsersList • exclusionUsersFileNome • exclusionDomainUsers	Un elenco di modelli di espressioni regolari per escludere determinati utenti e file utente nell'origine dati Microsoft Exchange. Gli utenti che corrispondono ai modelli vengono esclusi dall'indice. Gli utenti che non corrispondono ai modelli vengono inclusi nell'indice. Se un utente corrisponde sia a un modello di esclusione che a uno di inclusione, il modello di esclusione ha la precedenza e l'utente non viene incluso nell'indice.
Nome del bucket S3	Il nome del tuo bucket S3, se lo desideri utilizzare.
• CrawlCalendar • Esplora le note • Esplora i contatti • crawlFolderAcl	`true`per eseguire la scansione di questi tipi di contenuti e accedere alle informazioni di controllo dell'origine dati di Microsoft Exchange.
startCalendarDateOra	Puoi configurare una data e un'ora di inizio specifiche per il contenuto del calendario.
endCalendarDateOra	Puoi configurare una data-ora di fine specifica per il contenuto del calendario.
subject	È possibile configurare una riga dell'oggetto specifica per il contenuto della posta.
Email da	Puoi configurare un'e-mail specifica per il contenuto del messaggio «Da» o del mittente.
Invia un'email a	Puoi configurare un'e-mail specifica per il contenuto della posta «A» o del destinatario.

Configurazione	Descrizione
SyncMode	Specificate come Amazon Kendra aggiornar e l'indice quando il contenuto dell'origine dati cambia. Puoi scegliere tra: • `FORCED_FULL_CRAWL` per indicizzare nuovamente tutti i contenuti, sostituendo i contenuti esistenti ogni volta che l'origine dati si sincronizza con l'indice. • `FULL_CRAWL` per indicizzare solo i contenuti nuovi, modificati ed eliminati ogni volta che l'origine dati si sincronizza con l'indice. Amazon Kendra può utilizzare il meccanism o dell'origine dati per tenere traccia delle modifiche ai contenuti e indicizzare i contenuti modificati dall'ultima sincroniz zazione. • `CHANGE_LOG` per indicizzare solo contenuti nuovi e modificati ogni volta che l'origine dati si sincronizza con l'indice. Amazon Kendra può utilizzare il meccanismo dell'origine dati per tenere traccia delle modifiche ai contenuti e indicizzare i contenuti modificati dall'ultima sincronizzazione.
tipo	Il tipo di fonte di dati. Specificare `MSEXCHANG E` come tipo di origine dati.
Segretario ARN	L'Amazon Resource Name (ARN) di un AWS Secrets Manager segreto che contiene le coppie chiave-valore necessarie per connetter si a Microsoft Exchange. Ciò include l'ID cliente e il segreto del cliente generati quando crei un'applicazione OAuth nel portale di Azure.

Configurazione	Descrizione
version	La versione di questo modello attualmente supportata.

Schema JSON di Microsoft Exchange

```
{
  "$schema": "http://json-schema.org/draft-04/schema#",
  "type": "object",
  "properties": {
    "connectionConfiguration": {
      "type": "object",
      "properties": {
        "repositoryEndpointMetadata": {
          "type": "object",
          "properties": {
            "tenantId": {
              "type": "string",
              "pattern": "^[0-9a-f]{8}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]
{12}$",
              "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"
  ]
}
```

Schema OneDrive modello Microsoft

Includi un JSON che contiene lo schema dell'origine dati come parte dell'TemplateConfigurationoggetto. L'ID del tenant viene fornito come parte della configurazione della connessione o dei dettagli dell'endpoint del repository. Specificate inoltre il tipo di origine dati`ONEDRIVEV2`, un segreto per le credenziali di autenticazione e altre configurazioni necessarie. È quindi necessario specificare `TEMPLATE` come `Type` quando si chiama. CreateDataSource

Puoi utilizzare il modello fornito in questa guida per sviluppatori. Per informazioni, consulta Schema Microsoft OneDrive JSON.

La tabella seguente descrive i parametri dello schema Microsoft OneDrive JSON.

Configurazione	Descrizione
Configurazione della connessione	Informazioni di configurazione per l'endpoint per l'origine dati.
repositoryEndpointMetadata	Le informazioni sull'endpoint per l'origine dati.
TenantID	L'ID tenant di Microsoft 365. Puoi trovare il tuo ID tenant nelle proprietà del tuo portale di Azure Active Directory o nell'applicazione OAuth.

Configurazione	Descrizione
Configurazioni del repository	Informazioni di configurazione per il contenuto dell'origine dati. Ad esempio, la configurazione di tipi specifici di contenuti e mappature dei campi.
file	Un elenco di oggetti che mappano gli attributi o i nomi di campo dei OneDrive file Microsoft per Amazon Kendra indicizzare i nomi dei campi. Per ulteriori informazioni, consulta la sezione Mappatura dei campi di origine dei dati.
Proprietà aggiuntive	Opzioni di configurazione aggiuntive per i contenuti della fonte di dati
• userNameFilter • userFilterPath • inclusionFileTypeSchemi • exclusionFileTypeSchemi • inclusionFileNameSchemi • exclusionFileNameSchemi • inclusionFilePathSchemi • exclusionFilePathSchemi • inclusionOneNoteSectionNamePatterns • exclusionOneNoteSectionNamePatterns • inclusionOneNotePageNamePatterns • exclusionOneNotepageNamePatterns	Puoi scegliere di indicizzare file, OneNote sezioni, OneNote pagine specifici e filtrarli in base al nome utente.
isUserNameSu S3	`true`per fornire un elenco di nomi utente in un file archiviato in un file. Amazon S3
tipo	Il tipo di origine dati. Specificare `ONEDRIVEV2` come tipo di origine dati.

Configurazione	Descrizione
enableIdentityCrawler	`true`utilizzare il crawler Amazon Kendra di identità per sincronizzare le informazioni sull'identità/principali su utenti e gruppi con accesso a determinati documenti. Se il crawler di identità è disattivato, tutti i documenti possono essere ricercati pubblicamente. Se desideri utilizzare il controllo degli accessi per i tuoi documenti e il crawler di identità è disattivato, in alternativa puoi utilizzare l'PutPrincipalMappingAPI per caricare le informazioni di accesso di utenti e gruppi.
tipo	Il tipo di fonte di dati. Specificare `ONEDRIVEV2` come tipo di origine dati.

Configurazione	Descrizione
SyncMode	Specificate come Amazon Kendra aggiornar e l'indice quando il contenuto dell'origine dati cambia. Puoi scegliere tra: • `FORCED_FULL_CRAWL` per indicizzare nuovamente tutti i contenuti, sostituendo i contenuti esistenti ogni volta che l'origine dati si sincronizza con l'indice. • `FULL_CRAWL` per indicizzare solo i contenuti nuovi, modificati ed eliminati ogni volta che l'origine dati si sincronizza con l'indice. Amazon Kendra può utilizzare il meccanism o dell'origine dati per tenere traccia delle modifiche ai contenuti e indicizzare i contenuti modificati dall'ultima sincroniz zazione. • `CHANGE_LOG` per indicizzare solo contenuti nuovi e modificati ogni volta che l'origine dati si sincronizza con l'indice. Amazon Kendra può utilizzare il meccanismo dell'origine dati per tenere traccia delle modifiche ai contenuti e indicizzare i contenuti modificati dall'ultima sincronizzazione.

Configurazione	Descrizione
Secretary ARN	L'Amazon Resource Name (ARN) di un AWS Secrets Manager segreto che contiene le coppie chiave-valore necessarie per connettersi a Microsoft. OneDrive Il segreto deve contenere una struttura JSON con le seguenti chiavi: `{ "clientId": " client ID", "clientSecret": " client secret" }`
version	La versione di questo modello attualmente supportata.

Schema Microsoft OneDrive 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"
     ]
    }
```

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

Schema SharePoint modello Microsoft

Includi un JSON che contiene lo schema dell'origine dati come parte dell'TemplateConfigurationoggetto. Fornisci l'URL/URL del SharePoint sito, il dominio e anche un ID tenant, se necessario, come parte della configurazione della connessione o dei dettagli dell'endpoint

del repository. Specificate anche il tipo di origine dati`SHAREPOINTV2`, un segreto per le credenziali di autenticazione e altre configurazioni necessarie. È quindi necessario specificare `TEMPLATE` come Tipo quando si chiama. CreateDataSource

Puoi utilizzare il modello fornito in questa guida per sviluppatori. Per informazioni, consulta SharePoint Schema JSON.

La tabella seguente descrive i parametri dello schema Microsoft SharePoint JSON.

Configurazione	Descrizione
Configurazione della connessione	Informazioni di configurazione per l'endpoint per l'origine dati
repositoryEndpointMetadata	Le informazioni sull'endpoint per l'origine dati
TenantID	L'ID inquilino del tuo account. SharePoint
domain	Il dominio del tuo SharePoint account.
URL del sito	Gli URL host del tuo account. SharePoint
repositoryAdditionalProperties	Proprietà aggiuntive per la connessione all'endpoint del repository/origine dati.
S3bucketName	Il nome del Amazon S3 bucket in cui è archiviato il certificato X.509 autofirmato di Azure AD.
Nome del certificato S3	Il nome del certificato X.509 autofirmato di Azure AD archiviato nel bucket. Amazon S3
authType	Il tipo di autenticazione che utilizzi, se`OAuth2`,`OAuth2Certificate` ,`OAuth2App` ,`Basic`, `OAuth2_RefreshToken` `NTLM`, o`Kerberos`.
version	La SharePoint versione che usi, se `Server` o`Online`.

Configurazione	Descrizione
onPremVersion	La versione del SharePoint server che usi, se `2013` `20162019`, o`SubscriptionEditio n` .
Configurazioni del repository	Informazioni di configurazione per il contenuto dell'origine dati. Ad esempio, la configurazione di tipi specifici di contenuti e mappature dei campi.
• evento • page • file • collegamento • attachment • comment	Un elenco di oggetti che mappano gli attributi o i nomi dei campi dei SharePoint contenuti per Amazon Kendra indicizzare i nomi dei campi. Per ulteriori informazioni, consulta la sezione Mappatura dei campi di origine dei dati.
Proprietà aggiuntive	Opzioni di configurazione aggiuntive per i contenuti della fonte di dati.
• eventTitleFilterRegEx • pageTitleFilterRegEx • linkTitleFilterRegEx • inclusionFilePath • exclusionFilePath • inclusionFileTypeSchemi • exclusionFileTypeSchemi • inclusionFileNameSchemi • exclusionFileNameSchemi • inclusionOneNoteSectionNamePatterns • exclusionOneNoteSectionNamePatterns • inclusionOneNotePageNamePatterns • exclusionOneNotePageNamePatterns	Un elenco di modelli di espressioni regolari per includere/escludere determinati contenuti nella fonte di dati SharePoint . Gli elementi di contenuto che corrispondono ai modelli di inclusione sono inclusi nell'indice. Gli elementi di contenuto che non corrispondono ai modelli di inclusione sono esclusi dall'indice. Se un file corrisponde sia a un modello di inclusione che di esclusione, il modello di esclusione ha la precedenza e il file non viene incluso nell'indi ce.

Configurazione	Descrizione
• Scansiona i file • Esplora le pagine • CrawleEvents • Crawl Comments • Esplora i link • CrawlAtt Allegati	`true`per eseguire la scansione di questi tipi di contenuti.
Scansiona LACL	`true`per eseguire la scansione delle informazioni dell'elenco di controllo degli accessi (ACL) per i documenti, se si dispone di un ACL e si desidera utilizzarlo per il controllo degli accessi. L'ACL specifica a quali documenti possono accedere e cercare utenti e gruppi. Le informazioni ACL vengono utilizzate per filtrare i risultati della ricerca in base all'accesso dell'utente o del relativo gruppo ai documenti. Per ulteriori informazioni, consulta Filtraggio del contesto utente.
fieldForUserId	Specificare `email` se si desidera utilizzare l'e-mail dell'utente per l'ID utente o `userPrincipalName` se si desidera utilizzare un nome utente per l'ID utente. Se non si specifica un'opzione, `email` viene utilizzata per impostazione predefinita.
Configurazione ACL	Specificare `ACLWithLDAPEmailFmt` `ACLWithManualEmailFmt` , o. `ACLWithUsernameFmtM`
Dominio di posta elettronica	Il dominio dell'email. Ad esempio, "*amazon.com* ».

Configurazione	Descrizione
• isCrawlLocalGroupMapping • isCrawlAdGroupMapping	`true`per eseguire la scansione delle informazioni di mappatura dei gruppi.
ProxyHost	Il nome host del proxy Web utilizzato, senza il protocollo http://o https://.
ProxyPort	Il numero di porta utilizzato dal protocollo di trasporto dell'URL dell'host. Deve essere un valore numerico compreso tra 0 e 65535.
tipo	Specificare `SHAREPOINTV2` come tipo di origine dati
enableIdentityCrawler	`true`utilizzare il crawler Amazon Kendra di identità per sincronizzare le informazioni sull'identità/principali su utenti e gruppi con accesso a determinati documenti. Se il crawler di identità è disattivato, tutti i documenti possono essere ricercati pubblicamente. Se desideri utilizzare il controllo degli accessi per i tuoi documenti e il crawler di identità è disattivato, in alternativa puoi utilizzare l'PutPrincipalMappingAPI per caricare le informazioni di accesso di utenti e gruppi.

Configurazione	Descrizione
SyncMode	Specificate come Amazon Kendra aggiornar e l'indice quando il contenuto dell'origine dati cambia. Puoi scegliere tra: • `FORCED_FULL_CRAWL` per indicizzare nuovamente tutti i contenuti, sostituendo i contenuti esistenti ogni volta che l'origine dati si sincronizza con l'indice. • `FULL_CRAWL` per indicizzare solo i contenuti nuovi, modificati ed eliminati ogni volta che l'origine dati si sincronizza con l'indice. Amazon Kendra può utilizzare il meccanism o dell'origine dati per tenere traccia delle modifiche ai contenuti e indicizzare i contenuti modificati dall'ultima sincroniz zazione. • `CHANGE_LOG` per indicizzare solo contenuti nuovi e modificati ogni volta che l'origine dati si sincronizza con l'indice. Amazon Kendra può utilizzare il meccanismo dell'origine dati per tenere traccia delle modifiche ai contenuti e indicizzare i contenuti modificati dall'ultima sincronizzazione.
Secretary ARN	L'Amazon Resource Name (ARN) di un AWS Secrets Manager segreto che contiene le coppie chiave-valore necessarie per connetter si al tuo. SharePoint Per informazioni su queste coppie chiave-valore, consulta le istruzioni di connessione per Online e Server. SharePoint SharePoint
version	La versione di questo modello attualmente supportata.

SharePoint Schema 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"
 ]
}
```

Schema del modello di Microsoft SQL Server

Includi un JSON che contiene lo schema dell'origine dati come parte dell'TemplateConfigurationoggetto. Specificate il tipo di origine dati come`JDBC`, il tipo di database come`sqlserver`, un segreto per le credenziali di autenticazione e altre configurazioni necessarie. È quindi necessario specificare `TEMPLATE` come `Type` quando si chiama. CreateDataSource

Puoi utilizzare il modello fornito in questa guida per sviluppatori. Per informazioni, consulta Schema JSON di Microsoft SQL Server.

La tabella seguente descrive i parametri dello schema JSON di Micorosft SQL Server.

Configurazione	Descrizione
Configurazione della connessione	Informazioni di configurazione per l'endpoint per l'origine dati.

Configurazione	Descrizione
repositoryEndpointMetadata	Informazioni di configurazione necessarie per connettere la fonte di dati. • dbType: il tipo di database Java utilizzato, indipendentemente dal fatto che si tratti di `mysql`, `db2` `postgresql`, `oracle` o `sqlserver` • dbHost: il nome host del database. • dbPort: la porta del database. • dbInstance: l'istanza del database.
Configurazioni del repository	Informazioni di configurazione per il contenuto dell'origine dati. Ad esempio, la configurazione di tipi specifici di contenuti e mappature dei campi. Specificare il tipo di origine dati e l'ARN segreto.
documento	Un elenco di oggetti che mappano gli attributi o i nomi di campo del contenuto del database per Amazon Kendra indicizzare i nomi dei campi. Per ulteriori informazioni, consulta la sezione Mappatura dei campi di origine dei dati.
Proprietà aggiuntive	Opzioni di configurazione aggiuntive per i contenuti della fonte di dati. Utilizzatelo per includere o escludere contenuti specifici nella fonte di dati del database.
Chiave primaria	Fornisci la chiave primaria per la tabella del database. Questo identifica una tabella all'interno del database.
Colonna del titolo	Fornisci il nome della colonna del titolo del documento all'interno della tabella del database.

Configurazione	Descrizione
Corpo/colonna	Fornisci il nome della colonna del titolo del documento all'interno della tabella del database.
sqlQuery	Inserisci istruzioni di query SQL come le operazioni SELECT e JOIN. Le query SQL devono pesare meno di 32 KB. Amazon Kendra eseguirà la scansione di tutto il contenuto del database che corrisponde alla tua query.
colonna Timestamp	Inserisci il nome della colonna che contiene i timestamp. Amazon Kendra utilizza le informazioni relative alla marca temporale per rilevare le modifiche ai contenuti e sincronizzare solo i contenuti modificati.
formato Timestamp	Inserisci il nome della colonna che contiene i formati di timestamp da utilizzare per rilevare le modifiche ai contenuti e risincronizzare i contenuti.
timezone	Inserisci il nome della colonna che contiene i fusi orari per il contenuto da sottoporre a scansione.
changeDetectingColumns	Inserisci i nomi delle colonne che Amazon Kendra verranno utilizzate per rilevare le modifiche al contenuto. Amazon Kendra reindicizzerà il contenuto in caso di modifica in una di queste colonne
allowedUsersColumns	Inserisci il nome della colonna che contiene gli ID utente a cui consentire l'accesso ai contenuti .

Configurazione	Descrizione
allowedGroupsColumn	Inserisci il nome della colonna che contiene gli ID utente a cui consentire l'accesso ai contenuti .
SourceURIColumn	Inserisci il nome della colonna che contiene gli URL di origine da indicizzare.
isSslEnabled	Inserisci istruzioni di query SQL come le operazioni SELECT e JOIN. Le query SQL devono pesare meno di 32 KB. Amazon Kendra eseguirà la scansione di tutto il contenuto del database che corrisponde alla tua query.
tipo	Il tipo di fonte di dati. Specificare `JDBC` come tipo di origine dati.

Configurazione	Descrizione
SyncMode	Specificate come Amazon Kendra aggiornar e l'indice quando il contenuto dell'origine dati cambia. Puoi scegliere tra: • `FORCED_FULL_CRAWL` per indicizzare nuovamente tutti i contenuti, sostituendo i contenuti esistenti ogni volta che l'origine dati si sincronizza con l'indice. • `FULL_CRAWL` per indicizzare solo i contenuti nuovi, modificati ed eliminati ogni volta che l'origine dati si sincronizza con l'indice. Amazon Kendra può utilizzare il meccanism o dell'origine dati per tenere traccia delle modifiche ai contenuti e indicizzare i contenuti modificati dall'ultima sincroniz zazione. • `CHANGE_LOG` per indicizzare solo contenuti nuovi e modificati ogni volta che l'origine dati si sincronizza con l'indice. Amazon Kendra può utilizzare il meccanismo dell'origine dati per tenere traccia delle modifiche ai contenuti e indicizzare i contenuti modificati dall'ultima sincronizzazione.
Secretary ARN	L'Amazon Resource Name (ARN) di un segreto di Secrets Manager che contiene il nome utente e la password necessari per connetter si al database. Il segreto deve contenere una struttura JSON con le seguenti chiavi: `{ "user name": "database user name", "password": " password" }`

Configurazione	Descrizione
version	La versione del modello attualmente supportata.

Schema JSON di Microsoft SQL Server

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

Schema del modello Microsoft Teams

Includi un JSON che contiene lo schema dell'origine dati come parte dell'TemplateConfigurationoggetto. L'ID del tenant viene fornito come parte della configurazione della connessione o dei dettagli dell'endpoint del repository. Specificate anche il tipo di origine datiMSTEAMS, un segreto per le credenziali di autenticazione e altre configurazioni necessarie. È quindi necessario specificare TEMPLATE come Type quando si chiama. CreateDataSource

Puoi utilizzare il modello fornito in questa guida per sviluppatori. Per informazioni, consulta Schema JSON di Microsoft Teams.

La tabella seguente descrive i parametri dello schema JSON di Microsoft Teams.

Configurazione	Descrizione
Configurazione della connessione	Informazioni di configurazione per l'endpoint per l'origine dati.
repositoryEndpointMetadata	Le informazioni sull'endpoint per l'origine dati.
TenantID	L'ID tenant di Microsoft 365. Puoi trovare il tuo ID tenant nelle proprietà del tuo portale di Azure Active Directory o nell'applicazione OAuth.
Configurazioni del repository	Informazioni di configurazione per il contenuto dell'origine dati. Ad esempio, la configurazione di tipi specifici di contenuti e mappature dei campi.
• Messaggio di chat • Allegato alla chat • Channel Post • Canale Wiki • Allegato al canale • Chat di riunione • File della riunione • Nota sulla riunione	Un elenco di oggetti che mappano gli attributi o i nomi di campo del contenuto di Microsoft Teams per Amazon Kendra indicizzare i nomi dei campi. Per ulteriori informazioni, consulta la sezione Mappatura dei campi di origine dei dati.

Configurazione	Descrizione
• Riunione del calendario	
Proprietà aggiuntive	Opzioni di configurazione aggiuntive per i contenuti della fonte di dati.
Modello di pagamento	Speciifica il tipo di modello di pagamento da utilizzare con l'origine dati Microsoft Teams. I modelli di pagamento modello A sono limitati alle licenze e ai modelli di pagamento che richiedono la conformità in materia di sicurezza . I modelli di pagamento modello B sono adatti per licenze e modelli di pagamento che non richiedono la conformità in materia di sicurezza.
• inclusionTeamNameFiltro • inclusionChannelNameFiltro • inclusionFileNameMotivi • inclusionFileTypeSchemi • inclusionUserEmailFiltro • inclusionOneNoteSectionNamePatterns • inclusionOneNotePageNamePatterns	Un elenco di modelli di espressioni regolari per includere determinati contenuti nell'orig ine dati di Microsoft Teams. I contenuti che corrispondono ai modelli sono inclusi nell'indi ce. I contenuti che non corrispondono ai modelli sono esclusi dall'indice. Se il contenuto corrisponde sia a un modello di inclusione che a uno di esclusione, il modello di esclusione ha la precedenza e il contenuto non viene incluso nell'indice.
• exclusionTeamNameFiltro • exclusionChannelNameFiltro • exclusionFileNameMotivi • exclusionFileTypeSchemi • exclusionUserEmailFiltro • exclusionOneNoteSectionNamePatterns • exclusionOneNotePageNamePatterns	Un elenco di modelli di espressioni regolari per escludere determinati contenuti nell'orig ine dati di Microsoft Teams. I contenuti che corrispondono ai modelli sono esclusi dall'indi ce. I contenuti che non corrispondono ai modelli sono inclusi nell'indice. Se il contenuto corrisponde sia a un modello di inclusione che a uno di esclusione, il modello di esclusione ha la precedenza e il contenuto non è incluso nell'indice.

Configurazione	Descrizione
• isCrawlChatMessaggio • isCrawlChatAllegato • isCrawlChannelPosta • isCrawlChannelAllegato • isCrawlChannelWiki • isCrawlCalendarIncontro • isCrawlMeetingChat • isCrawlMeetingFile • isCrawlMeetingNota	`true`per eseguire la scansione di questi tipi di contenuti nell'origine dati Microsoft Teams.
startCalendarDateOra	Puoi configurare una data e un'ora di inizio specifiche per il contenuto del calendario.
endCalendarDateOra	Puoi configurare una data-ora di fine specifica per il contenuto del calendario.
tipo	Il tipo di origine dati. Specificare `MSTEAMS` come tipo di origine dati.
enableIdentityCrawler	`true`utilizzare il crawler Amazon Kendra di identità per sincronizzare le informazi oni sull'identità/principali su utenti e gruppi con accesso a determinati documenti. Se il crawler di identità è disattivato, tutti i documenti possono essere ricercati pubblicamente. Se desideri utilizzare il controllo degli accessi per i tuoi documenti e il crawler di identità è disattiva to, in alternativa puoi utilizzare l'PutPrinci palMappingAPI per caricare le informazioni di accesso di utenti e gruppi.

Configurazione	Descrizione
SyncMode	Specificate come Amazon Kendra aggiornar e l'indice quando il contenuto dell'origine dati cambia. Puoi scegliere tra: • `FORCED_FULL_CRAWL` per indicizzare nuovamente tutti i contenuti, sostituendo i contenuti esistenti ogni volta che l'origine dati si sincronizza con l'indice. • `FULL_CRAWL` per indicizzare solo i contenuti nuovi, modificati ed eliminati ogni volta che l'origine dati si sincronizza con l'indice. Amazon Kendra può utilizzare il meccanism o dell'origine dati per tenere traccia delle modifiche ai contenuti e indicizzare i contenuti modificati dall'ultima sincroniz zazione. • `CHANGE_LOG` per indicizzare solo contenuti nuovi e modificati ogni volta che l'origine dati si sincronizza con l'indice. Amazon Kendra può utilizzare il meccanismo dell'origine dati per tenere traccia delle modifiche ai contenuti e indicizzare i contenuti modificati dall'ultima sincronizzazione.
Secretary ARN	L'Amazon Resource Name (ARN) di un AWS Secrets Manager segreto che contiene le coppie chiave-valore necessarie per connetter si ai tuoi Microsoft Teams. Ciò include l'ID cliente e il segreto del client generati quando crei un'applicazione OAuth nel portale di Azure.
version	La versione di questo modello attualmente supportata.

Schema JSON di Microsoft Teams

```
{
  "$schema": "http://json-schema.org/draft-04/schema#",
  "type": "object",
  "properties": {
    "connectionConfiguration": {
      "type": "object",
      "properties": {
        "repositoryEndpointMetadata": {
          "type": "object",
          "properties": {
            "tenantId": {
              "type": "string",
              "pattern": "^[0-9a-f]{8}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]
{12}$",
              "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"
  ]
}
```

Schema del modello di Microsoft Yammer

Includi un JSON che contiene lo schema dell'origine dati come parte dell'oggetto. TemplateConfiguration Specificate il tipo di origine datiYAMMER, un segreto per le credenziali di autenticazione e altre configurazioni necessarie. È quindi necessario specificare TEMPLATE come Tipo quando si chiama. CreateDataSource

Puoi utilizzare il modello fornito in questa guida per sviluppatori.

Nella tabella seguente vengono descritti i parametri dello schema JSON di Microsoft Yammer.

Configurazione	Descrizione
Configurazione della connessione	Informazioni di configurazione per l'origine dati.
repositoryEndpointMetadata	Le informazioni sull'endpoint per l'origine dati. Questa fonte di dati non specifica un endpoint in. `repositoryEndpointMetadata` Piuttosto, le informazioni di connessione sono incluse in un AWS Secrets Manager segreto fornito dall'`secretArn` utente.
Configurazioni del repository	Informazioni di configurazione per il contenuto dell'origine dati. Ad esempio, la configurazione di tipi specifici di contenuti e mappature dei campi.
• comunità • Utente	Un elenco di oggetti che mappano gli attributi o i nomi di campo dei contenuti di Microsoft

Configurazione	Descrizione
• message • attachment	Yammer ai nomi dei campi indice di Amazon Kendra. Per ulteriori informazioni, consulta la sezione Mappatura dei campi di origine dei dati.
Proprietà aggiuntive	Opzioni di configurazione aggiuntive per i contenuti della fonte di dati
Modelli di inclusione	Un elenco di modelli di espressioni regolari per includere determinati file nell'origine dati Microsoft Yammer. I file che corrispondono ai modelli sono inclusi nell'indice. I file che non corrispondono ai modelli vengono esclusi dall'indice. Se un file corrisponde sia a un modello di esclusione sia a un modello di inclusione, il modello di esclusione ha la precedenza e il file non viene incluso nell'indice.
Modelli di esclusione	Un elenco di modelli di espressioni regolari per escludere determinati file nell'origine dati Microsoft Yammer. I file che corrispondono ai modelli sono esclusi dall'indice. I file che non corrispondono ai modelli sono inclusi nell'indice. Se un file corrisponde sia a un modello di esclusione che a uno di inclusione, il modello di esclusione ha la precedenza e il file non viene incluso nell'indice.
Dal momento della data	È possibile scegliere di configurare un `sinceDate` parametro in modo che il connettore Microsoft Yammer esegua la scansione del contenuto in base a uno specifico. `sinceDate`
communityNameFilter	Puoi scegliere di indicizzare contenuti specifici della community.

Configurazione	Descrizione
• isCrawlMessage • isCrawlAttachment • isCrawlPrivateMessaggio	`true`per eseguire la scansione di messaggi, allegati e messaggi privati.
tipo	Specificare `YAMMER` come tipo di origine dati.
Segretario ARN	L'Amazon Resource Name (ARN) di un AWS Secrets Manager segreto che contiene le coppie chiave-valore necessarie per connetter si a Microsoft Yammer. Ciò include il nome utente e la password di Microsoft Yammer, l'ID client e il segreto client generati quando si crea un'applicazione OAuth nel portale di Azure.
useChangeLog	`true`per utilizzare il registro delle modifiche di Microsoft Yammer per determinare quali documenti devono essere aggiornati nell'indice.

Configurazione	Descrizione
modalità di sincronizzazione	Specificate come Amazon Kendra aggiornar e l'indice quando il contenuto dell'origine dati cambia. Puoi scegliere tra: • `FORCED_FULL_CRAWL` per indicizzare nuovamente tutti i contenuti, sostituendo i contenuti esistenti ogni volta che l'origine dati si sincronizza con l'indice. • `FULL_CRAWL` per indicizzare solo i contenuti nuovi, modificati ed eliminati ogni volta che l'origine dati si sincronizza con l'indice. Amazon Kendra può utilizzare il meccanism o dell'origine dati per tenere traccia delle modifiche ai contenuti e indicizzare i contenuti modificati dall'ultima sincroniz zazione. • `CHANGE_LOG` per indicizzare solo contenuti nuovi e modificati ogni volta che l'origine dati si sincronizza con l'indice. Amazon Kendra può utilizzare il meccanismo dell'origine dati per tenere traccia delle modifiche ai contenuti e indicizzare i contenuti modificati dall'ultima sincronizzazione.

Configurazione	Descrizione
enableIdentityCrawler	`true`utilizzare il crawler Amazon Kendra di identità per sincronizzare le informazioni sull'identità/principali su utenti e gruppi con accesso a determinati documenti. Se il crawler di identità è disattivato, tutti i documenti possono essere ricercati pubblicamente. Se desideri utilizzare il controllo degli accessi per i tuoi documenti e il crawler di identità è disattivato, in alternativa puoi utilizzare l'PutPrincipalMappingAPI per caricare le informazioni di accesso di utenti e gruppi.

Schema JSON di Microsoft Yammer

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

Schema del modello MySQL

Includi un JSON che contiene lo schema dell'origine dati come parte dell'oggetto. TemplateConfiguration Specificate il tipo di origine dati come`JDBC`, il tipo di database come`mysql`, un segreto per le credenziali di autenticazione e altre configurazioni necessarie. È quindi necessario specificare `TEMPLATE` come `Type` quando si chiama. CreateDataSource

Puoi utilizzare il modello fornito in questa guida per sviluppatori. Per informazioni, consulta Schema JSON MySQL.

La tabella seguente descrive i parametri dello schema JSON MySQL.

Configurazione	Descrizione
Configurazione della connessione	Informazioni di configurazione per l'endpoint per l'origine dati.
repositoryEndpointMetadata	Informazioni di configurazione necessarie per connettere la fonte di dati. • dbType: il tipo di database Java utilizzat o, indipendentemente dal fatto che si tratti di `mysql`,, `db2` `postgresql` , `oracle` o. `sqlserver` • dbHost: il nome host del database. • dbPort: la porta del database. • dbInstance: l'istanza del database.
Configurazioni del repository	Informazioni di configurazione per il contenuto dell'origine dati. Ad esempio, la configurazione di tipi specifici di contenuti e mappature dei campi. Specificare il tipo di origine dati e l'ARN segreto.
documento	Un elenco di oggetti che mappano gli attributi o i nomi di campo del contenuto del database per Amazon Kendra indicizzare i nomi dei campi. Per ulteriori informazioni, consulta la sezione Mappatura dei campi di origine dei dati.
Proprietà aggiuntive	Opzioni di configurazione aggiuntive per i contenuti della fonte di dati. Utilizzatelo per includere o escludere contenuti specifici nella fonte di dati del database.
Chiave primaria	Fornisci la chiave primaria per la tabella del database. Questo identifica una tabella all'inter no del database.

Configurazione	Descrizione
Colonna del titolo	Fornisci il nome della colonna del titolo del documento all'interno della tabella del database.
Corpo/colonna	Fornisci il nome della colonna del titolo del documento all'interno della tabella del database.
sqlQuery	Inserisci istruzioni di query SQL come le operazioni SELECT e JOIN. Le query SQL devono pesare meno di 32 KB. Amazon Kendra eseguirà la scansione di tutto il contenuto del database che corrisponde alla tua query.
colonna Timestamp	Inserisci il nome della colonna che contiene i timestamp. Amazon Kendra utilizza le informazioni relative alla marca temporale per rilevare le modifiche ai contenuti e sincronizzare solo i contenuti modificati.
formato Timestamp	Inserisci il nome della colonna che contiene i formati di timestamp da utilizzare per rilevare le modifiche ai contenuti e risincronizzare i contenuti.
timezone	Inserisci il nome della colonna che contiene i fusi orari per il contenuto da sottoporre a scansione.
changeDetectingColumns	Inserisci i nomi delle colonne che Amazon Kendra verranno utilizzate per rilevare le modifiche al contenuto. Amazon Kendra reindicizzerà il contenuto in caso di modifica in una di queste colonne

Configurazione	Descrizione
allowedUsersColumns	Inserisci il nome della colonna che contiene gli ID utente a cui consentire l'accesso ai contenuti .
allowedGroupsColumn	Inserisci il nome della colonna che contiene gli ID utente a cui consentire l'accesso ai contenuti .
SourceURIColumn	Inserisci il nome della colonna che contiene gli URL di origine da indicizzare.
isSslEnabled	Inserisci istruzioni di query SQL come le operazioni SELECT e JOIN. Le query SQL devono pesare meno di 32 KB. Amazon Kendra eseguirà la scansione di tutto il contenuto del database che corrisponde alla tua query.
tipo	Il tipo di fonte di dati. Specificare `JDBC` come tipo di origine dati.

Configurazione	Descrizione
SyncMode	Specificate come Amazon Kendra aggiornar e l'indice quando il contenuto dell'origine dati cambia. Puoi scegliere tra: • `FORCED_FULL_CRAWL` per indicizzare nuovamente tutti i contenuti, sostituendo i contenuti esistenti ogni volta che l'origine dati si sincronizza con l'indice. • `FULL_CRAWL` per indicizzare solo i contenuti nuovi, modificati ed eliminati ogni volta che l'origine dati si sincronizza con l'indice. Amazon Kendra può utilizzare il meccanism o dell'origine dati per tenere traccia delle modifiche ai contenuti e indicizzare i contenuti modificati dall'ultima sincroniz zazione. • `CHANGE_LOG` per indicizzare solo contenuti nuovi e modificati ogni volta che l'origine dati si sincronizza con l'indice. Amazon Kendra può utilizzare il meccanismo dell'origine dati per tenere traccia delle modifiche ai contenuti e indicizzare i contenuti modificati dall'ultima sincronizzazione.
Secretary ARN	L'Amazon Resource Name (ARN) di un segreto di Secrets Manager che contiene il nome utente e la password necessari per connetter si al database. Il segreto deve contenere una struttura JSON con le seguenti chiavi: `{ "user name": "database user name", "password": " password" }`

Configurazione	Descrizione
version	La versione del modello attualmente supportata.

Schema JSON MySQL

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

Schema del modello di database Oracle

Includi un JSON che contiene lo schema dell'origine dati come parte dell'TemplateConfigurationoggetto. Specificate il tipo di origine dati come`JDBC`, il tipo di database come`oracle`, un segreto per le credenziali di autenticazione e altre configurazioni necessarie. È quindi necessario specificare `TEMPLATE` come `Type` quando si chiama. CreateDataSource

Puoi utilizzare il modello fornito in questa guida per sviluppatori. Per informazioni, consulta Schema JSON del database Oracle.

La tabella seguente descrive i parametri dello schema JSON di Oracle Database.

Configurazione	Descrizione
Configurazione della connessione	Informazioni di configurazione per l'endpoint per l'origine dati.
repositoryEndpointMetadata	Informazioni di configurazione necessarie per connettere la fonte di dati. • dbType: il tipo di database Java utilizzato, indipendentemente dal fatto che si tratti di`mysql`,, `db2` `postgresql` , `oracle` o. `sqlserver` • dbHost: il nome host del database. • dbPort: la porta del database. • dbInstance: l'istanza del database.
Configurazioni del repository	Informazioni di configurazione per il contenuto dell'origine dati. Ad esempio, la configurazione di tipi specifici di contenuti e mappature dei campi. Specificare il tipo di origine dati e l'ARN segreto.
documento	Un elenco di oggetti che mappano gli attributi o i nomi di campo del contenuto del database per Amazon Kendra indicizzare i nomi dei campi.

Configurazione	Descrizione
	Per ulteriori informazioni, consulta la sezione Mappatura dei campi di origine dei dati.
Proprietà aggiuntive	Opzioni di configurazione aggiuntive per i contenuti della fonte di dati. Utilizzatelo per includere o escludere contenuti specifici nella fonte di dati del database.
Chiave primaria	Fornisci la chiave primaria per la tabella del database. Questo identifica una tabella all'inter no del database.
Colonna del titolo	Fornisci il nome della colonna del titolo del documento all'interno della tabella del database.
Corpo/colonna	Fornisci il nome della colonna del titolo del documento all'interno della tabella del database.
sqlQuery	Inserisci istruzioni di query SQL come le operazioni SELECT e JOIN. Le query SQL devono pesare meno di 32 KB. Amazon Kendra eseguirà la scansione di tutto il contenuto del database che corrisponde alla tua query.
colonna Timestamp	Inserisci il nome della colonna che contiene i timestamp. Amazon Kendra utilizza le informazi oni relative alla marca temporale per rilevare le modifiche ai contenuti e sincronizzare solo i contenuti modificati.
formato Timestamp	Inserisci il nome della colonna che contiene i formati di timestamp da utilizzare per rilevare le modifiche ai contenuti e risincronizzare i contenuti.

Configurazione	Descrizione
timezone	Inserisci il nome della colonna che contiene i fusi orari per il contenuto da sottoporre a scansione.
changeDetectingColumns	Inserisci i nomi delle colonne che Amazon Kendra verranno utilizzate per rilevare le modifiche al contenuto. Amazon Kendra reindicizzerà il contenuto in caso di modifica in una di queste colonne
allowedUsersColumns	Inserisci il nome della colonna che contiene gli ID utente a cui consentire l'accesso ai contenuti .
allowedGroupsColumn	Inserisci il nome della colonna che contiene gli ID utente a cui consentire l'accesso ai contenuti .
SourceURIColumn	Inserisci il nome della colonna che contiene gli URL di origine da indicizzare.
isSslEnabled	Inserisci istruzioni di query SQL come le operazioni SELECT e JOIN. Le query SQL devono pesare meno di 32 KB. Amazon Kendra eseguirà la scansione di tutto il contenuto del database che corrisponde alla tua query.
tipo	Il tipo di fonte di dati. Specificare `JDBC` come tipo di origine dati.

Configurazione	Descrizione
SyncMode	Specificate come Amazon Kendra aggiornar e l'indice quando il contenuto dell'origine dati cambia. Puoi scegliere tra: • `FORCED_FULL_CRAWL` per indicizzare nuovamente tutti i contenuti, sostituendo i contenuti esistenti ogni volta che l'origine dati si sincronizza con l'indice. • `FULL_CRAWL` per indicizzare solo i contenuti nuovi, modificati ed eliminati ogni volta che l'origine dati si sincronizza con l'indice. Amazon Kendra può utilizzare il meccanism o dell'origine dati per tenere traccia delle modifiche ai contenuti e indicizzare i contenuti modificati dall'ultima sincroniz zazione. • `CHANGE_LOG` per indicizzare solo contenuti nuovi e modificati ogni volta che l'origine dati si sincronizza con l'indice. Amazon Kendra può utilizzare il meccanismo dell'origine dati per tenere traccia delle modifiche ai contenuti e indicizzare i contenuti modificati dall'ultima sincronizzazione.
Secretary ARN	L'Amazon Resource Name (ARN) di un segreto di Secrets Manager che contiene il nome utente e la password necessari per connetter si al database. Il segreto deve contenere una struttura JSON con le seguenti chiavi: `{ "user name": "database user name", "password": " password" }`

Configurazione	Descrizione
version	La versione del modello attualmente supportata.

Schema JSON del 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"
  ]
}
```

Schema del modello PostgreSQL

Includi un JSON che contiene lo schema dell'origine dati come parte dell'oggetto. TemplateConfiguration Specificate il tipo di origine dati come`JDBC`, il tipo di database come`postgresql`, un segreto per le credenziali di autenticazione e altre configurazioni necessarie. È quindi necessario specificare `TEMPLATE` come `Type` quando si chiama. CreateDataSource

Puoi utilizzare il modello fornito in questa guida per sviluppatori. Per informazioni, consulta Schema JSON PostgreSQL.

La tabella seguente descrive i parametri dello schema JSON di PostgreSQL.

Configurazione	Descrizione
Configurazione della connessione	Informazioni di configurazione per l'endpoint per l'origine dati.
repositoryEndpointMetadata	Informazioni di configurazione necessarie per connettere la fonte di dati. • dbType: il tipo di database Java utilizzato, indipendentemente dal fatto che si tratti di`mysql`,, `db2` `postgresql` , `oracle` o. `sqlserver` • dbHost: il nome host del database. • dbPort: la porta del database. • dbInstance: l'istanza del database.
Configurazioni del repository	Informazioni di configurazione per il contenuto dell'origine dati. Ad esempio, la configurazione di tipi specifici di contenuti e mappature dei campi. Specificare il tipo di origine dati e l'ARN segreto.
documento	Un elenco di oggetti che mappano gli attributi o i nomi di campo del contenuto del database per Amazon Kendra indicizzare i nomi dei campi.

Configurazione	Descrizione
	Per ulteriori informazioni, consulta la sezione Mappatura dei campi di origine dei dati.
Proprietà aggiuntive	Opzioni di configurazione aggiuntive per i contenuti della fonte di dati. Utilizzatelo per includere o escludere contenuti specifici nella fonte di dati del database.
Chiave primaria	Fornisci la chiave primaria per la tabella del database. Questo identifica una tabella all'inter no del database.
Colonna del titolo	Fornisci il nome della colonna del titolo del documento all'interno della tabella del database.
Corpo/colonna	Fornisci il nome della colonna del titolo del documento all'interno della tabella del database.
sqlQuery	Inserisci istruzioni di query SQL come le operazioni SELECT e JOIN. Le query SQL devono pesare meno di 32 KB. Amazon Kendra eseguirà la scansione di tutto il contenuto del database che corrisponde alla tua query.
colonna Timestamp	Inserisci il nome della colonna che contiene i timestamp. Amazon Kendra utilizza le informazi oni relative alla marca temporale per rilevare le modifiche ai contenuti e sincronizzare solo i contenuti modificati.
formato Timestamp	Inserisci il nome della colonna che contiene i formati di timestamp da utilizzare per rilevare le modifiche ai contenuti e risincronizzare i contenuti.

Configurazione	Descrizione
timezone	Inserisci il nome della colonna che contiene i fusi orari per il contenuto da sottoporre a scansione.
changeDetectingColumns	Inserisci i nomi delle colonne che Amazon Kendra verranno utilizzate per rilevare le modifiche al contenuto. Amazon Kendra reindicizzerà il contenuto in caso di modifica in una di queste colonne
allowedUsersColumns	Inserisci il nome della colonna che contiene gli ID utente a cui consentire l'accesso ai contenuti .
allowedGroupsColumn	Inserisci il nome della colonna che contiene gli ID utente a cui consentire l'accesso ai contenuti .
SourceURIColumn	Inserisci il nome della colonna che contiene gli URL di origine da indicizzare.
isSslEnabled	Inserisci istruzioni di query SQL come le operazioni SELECT e JOIN. Le query SQL devono pesare meno di 32 KB. Amazon Kendra eseguirà la scansione di tutto il contenuto del database che corrisponde alla tua query.
tipo	Il tipo di fonte di dati. Specificare `JDBC` come tipo di origine dati.

Configurazione	Descrizione
SyncMode	Specificate come Amazon Kendra aggiornar e l'indice quando il contenuto dell'origine dati cambia. Puoi scegliere tra: • `FORCED_FULL_CRAWL` per indicizzare nuovamente tutti i contenuti, sostituendo i contenuti esistenti ogni volta che l'origine dati si sincronizza con l'indice. • `FULL_CRAWL` per indicizzare solo i contenuti nuovi, modificati ed eliminati ogni volta che l'origine dati si sincronizza con l'indice. Amazon Kendra può utilizzare il meccanism o dell'origine dati per tenere traccia delle modifiche ai contenuti e indicizzare i contenuti modificati dall'ultima sincroniz zazione. • `CHANGE_LOG` per indicizzare solo contenuti nuovi e modificati ogni volta che l'origine dati si sincronizza con l'indice. Amazon Kendra può utilizzare il meccanismo dell'origine dati per tenere traccia delle modifiche ai contenuti e indicizzare i contenuti modificati dall'ultima sincronizzazione.
Secretary ARN	L'Amazon Resource Name (ARN) di un segreto di Secrets Manager che contiene il nome utente e la password necessari per connetter si al database. Il segreto deve contenere una struttura JSON con le seguenti chiavi: `{ "user name": "database user name", "password": " password" }`

Configurazione	Descrizione
version	La versione del modello attualmente supportata.

Schema JSON PostgreSQL

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

Schema del modello Salesforce

Includi un JSON che contiene lo schema dell'origine dati come parte dell'oggetto. TemplateConfiguration Fornisci l'URL dell'host Salesforce come parte della configurazione della connessione o dei dettagli dell'endpoint del repository. Specificate inoltre il tipo di origine datiSALESFORCEV2, come segreto per le credenziali di autenticazione e altre configurazioni necessarie. È quindi necessario specificare TEMPLATE come Type quando si chiama. CreateDataSource

Puoi utilizzare il modello fornito in questa guida per sviluppatori. Per informazioni, consulta Schema JSON di Salesforce.

La tabella seguente descrive i parametri dello schema JSON di Salesforce.

Configurazione	Descrizione
Configurazione della connessione	Informazioni di configurazione per l'endpoint per l'origine dati.
repositoryEndpointMetadata	Le informazioni sull'endpoint per l'origine dati.
HostUrl	L'URL dell'istanza Salesforce da indicizzare.
Configurazioni del repository	Informazioni di configurazione per il contenuto dell'origine dati. Ad esempio, la configurazione di tipi specifici di contenuti e mappature dei campi.
• account • contact • campaign • caso • prodotto • piombo • contract • compagno • profilo	Un elenco di oggetti che mappano gli attributi o i nomi di campo delle entità Salesforce per Amazon Kendra indicizzare i nomi dei campi. Per ulteriori informazioni, consulta la sezione Mappatura dei campi di origine dei dati.

Configurazione	Descrizione
• idea • listino prezzi • task • soluzione • attachment • Utente • documento • Articoli di conoscenza • gruppo • opportunità • cicaleccio • entità personalizzata	

Configurazione	Descrizione
Secretarn	L'Amazon Resource Name (ARN) di un AWS Secrets Manager segreto che contiene le coppie chiave-valore necessarie per connetter si a Salesforce. Il segreto deve contenere una struttura JSON con le seguenti chiavi: `{ "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 associate d with the user logging in to the Salesforce instance ", "securityToken": " Token associate d with the user account logging in to the Salesforce instance ", "username": " User name of the user logging in to the Salesforce instance" }`
Proprietà aggiuntive	Opzioni di configurazione aggiuntive per i contenuti della fonte di dati

Configurazione	Descrizione
• AccountFilter • Filtro contatti • Filtro Case • Filtro della campagna • Filtro contrattuale • Filtro di gruppo • Filtro Lead • Filtro del prodotto • Filtro di opportunità • Filtro per i partner • Filtro PriceBook • Filtro Idea • Filtro del profilo • Filtro attività • Filtro della soluzione • Filtro utente • Filtro chiacchierone • Filtro per documenti • knowledgeArticleFilter • Entità personalizzate	Una raccolta di stringhe che specifica quali entità filtrare.

Configurazione	Descrizione
Modelli di inclusione • inclusionDocumentFileTypePatterns • inclusionDocumentFileNamePatterns • inclusionAccountFileTypePatterns • inclusionCampaignFileTypePatterns • inclusionDocumentFileNamePatterns • inclusionCampaignFileNamePatterns • inclusionCaseFileTypePatterns • inclusionCaseFileNamePatterns • inclusionContactFileTypePatterns • inclusionContractFileNamePatterns • inclusionLeadFileTypePatterns • inclusionLeadFileNamePatterns • inclusionOpportunityFileTypePatterns • inclusionOpportunityFileNamePatterns • inclusionSolutionFileTypePatterns • inclusionSolutionFileNamePatterns • inclusionTaskFileTypePatterns • inclusionTaskFileNamePatterns • inclusionGroupFileTypePatterns • inclusionGroupFileNamePatterns • inclusionChatterFileTypePatterns • inclusionChatterFileNamePatterns • inclusionCustomEntityFileTypePatterns • inclusionCustomEntityFileNamePatterns	Un elenco di modelli di espressioni regolari per includere determinati file nella fonte di dati Salesforce. I file che corrispondono ai modelli sono inclusi nell'indice. I file che non corrispon dono ai modelli sono esclusi dall'indice. Se un file corrisponde sia a un modello di esclusion e sia a un modello di inclusione, il modello di esclusione ha la precedenza e il file non viene incluso nell'indice.

Configurazione	Descrizione
Modelli di esclusione • exclusionDocumentFileTypePatterns • exclusionDocumentFileNamePatterns • exclusionAccountFileTypePatterns • exclusionCampaignFileTypePatterns • exclusionCampaignFileNamePatterns • exclusionCaseFileTypePatterns • exclusionCaseFileNamePatterns • exclusionContactFileTypePatterns • exclusionContractFileNamePatterns • exclusionLeadFileTypePatterns • exclusionLeadFileNamePatterns • exclusionOpportunityFileTypePatterns • exclusionOpportunityFileNamePatterns • exclusionSolutionFileTypePatterns • exclusionSolutionFileNamePatterns • exclusionTaskFileTypePatterns • exclusionTaskFileNamePatterns • exclusionGroupFileTypePatterns • exclusionGroupFileNamePatterns • exclusionChatterFileTypePatterns • exclusionChatterFileNamePatterns • exclusionCustomEntityFileTypePatterns • exclusionCustomEntityFileNamePatterns	Un elenco di modelli di espressioni regolari per escludere determinati file nella fonte dati Salesforce. I file che corrispondono ai modelli sono esclusi dall'indice. I file che non corrispon dono ai modelli sono inclusi nell'indice. Se un file corrisponde sia a un modello di esclusione che a uno di inclusione, il modello di esclusion e ha la precedenza e il file non viene incluso nell'indice.

Configurazione	Descrizione
• isCrawlAccount • isCrawlContact • isCrawlCase • isCrawlCampaign • isCrawlProduct • isCrawlLead • isCrawlContract • isCrawlPartner • isCrawlProfile • isCrawlIdea • isCrawlPricebook • isCrawlDocument • crawlSharedDocument • isCrawlGroup • isCrawlOpportunity • isCrawlChatter • isCrawlUser • isCrawlSolution • isCrawlTask • isCrawlAccountAllegati • isCrawlContactAllegati • isCrawlCaseAllegati • isCrawlCampaignAllegati • isCrawlLeadAllegati • isCrawlContractAllegati • isCrawlGroupAllegati • isCrawlOpportunityAllegati • isCrawlChatterAllegati • isCrawlSolutionAllegati	`true`per eseguire la scansione di questi tipi di file nel tuo account Salesforce.

Configurazione	Descrizione

• isCrawlTaskAllegati
• isCrawlCustomEntityAttachments
• isCrawlKnowledgeArticoli
  • isCrawlDraft
  • isCrawlPublish
  • isCrawlArchived	

tipo	Il tipo di origine dati. Specificare `SALESFORCEV2` come tipo di origine dati.
enableIdentityCrawler	`true`utilizzare il crawler Amazon Kendra di identità per sincronizzare le informazioni sull'identità/principali su utenti e gruppi con accesso a determinati documenti. Se il crawler di identità è disattivato, tutti i documenti possono essere ricercati pubblicamente. Se desideri utilizzare il controllo degli accessi per i tuoi documenti e il crawler di identità è disattivato, in alternativa puoi utilizzare l'PutPrincipalMappingAPI per caricare le informazioni di accesso di utenti e gruppi.

Configurazione	Descrizione
SyncMode	Specificate come Amazon Kendra aggiornar e l'indice quando il contenuto dell'origine dati cambia. Puoi scegliere tra: • `FORCED_FULL_CRAWL` per indicizzare nuovamente tutti i contenuti, sostituendo i contenuti esistenti ogni volta che l'origine dati si sincronizza con l'indice. • `FULL_CRAWL` per indicizzare solo i contenuti nuovi, modificati ed eliminati ogni volta che l'origine dati si sincronizza con l'indice. Amazon Kendra può utilizzare il meccanism o dell'origine dati per tenere traccia delle modifiche ai contenuti e indicizzare i contenuti modificati dall'ultima sincroniz zazione. • `CHANGE_LOG` per indicizzare solo contenuti nuovi e modificati ogni volta che l'origine dati si sincronizza con l'indice. Amazon Kendra può utilizzare il meccanismo dell'origine dati per tenere traccia delle modifiche ai contenuti e indicizzare i contenuti modificati dall'ultima sincronizzazione.
version	La versione di questo modello attualmente supportata.

Schema JSON di 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 schema modello

Includi un JSON che contiene lo schema dell'origine dati come parte dell'TemplateConfigurationoggetto. Fornisci l'URL dell' ServiceNow host, il tipo di autenticazione e la versione dell'istanza come parte della configurazione della connessione o dei dettagli dell'endpoint del repository. Specificate anche il tipo di origine dati`SERVICENOWV2`, un segreto per le credenziali di autenticazione e altre configurazioni necessarie. È quindi necessario specificare `TEMPLATE` come `Type` quando si chiama. CreateDataSource

Puoi utilizzare il modello fornito in questa guida per sviluppatori. Per informazioni, consulta ServiceNow Schema JSON.

La tabella seguente descrive i parametri dello schema ServiceNow JSON.

Configurazione	Descrizione
Configurazione della connessione	Informazioni di configurazione per l'endpoint per l'origine dati.
repositoryEndpointMetadata	Le informazioni sull'endpoint per l'origine dati.
HostUrl	L'URL dell' ServiceNow host. Ad esempio, *`your-domain.service-now.com`* .
authType	Il tipo di autenticazione che usi, se `basicAuth` o`0Auth2`.
servicenowInstanceVersion	La ServiceNow versione che usi. Puoi scegliere tra`Tokyo`, `SandiegoRome`, e`0thers`.
Configurazioni del repository	Informazioni di configurazione per il contenuto dell'origine dati. Ad esempio, la configurazione di tipi specifici di contenuti e mappature dei campi.

Configurazione	Descrizione
• Articolo di conoscenza • attachment • Catalogo dei servizi • incidente	Un elenco di oggetti che mappano gli attributi o i nomi dei campi degli articoli della ServiceNow Knowledge Base, degli allegati, del catalogo dei servizi e degli incidenti per Amazon Kendra indicizzare i nomi dei campi. Per ulteriori informazioni, consulta la sezione Mappatura dei campi di origine dei dati. I nomi dei campi dell'origine ServiceNow dati devono esistere nei metadati ServiceNow personalizzati.
proprietà aggiuntive	Opzioni di configurazione aggiuntive per i contenuti della fonte di dati.
maxFileSizeInMegaBytes	Specificare il limite di dimensione del file in MB che Amazon Kendra eseguirà la scansione. Amazon Kendra eseguirà la scansione solo dei file entro il limite di dimensione definito. La dimensione predefinita del file è 50 MB. La dimensione massima del file deve essere superiore a 0 MB e inferiore o uguale a 50 MB.
• knowledgeArticleFilter • incidentQueryFilter • serviceCatalogQueryFiltro • knowledgeArticleTitleRegExp • serviceCatalogTitleRegExp • incidentTitleRegExp • inclusionFileTypeSchemi • exclusionFileTypeSchemi • inclusionFileNameSchemi • exclusionFileNameSchemi • incidentStateType	Un elenco di modelli di espressioni regolari per includere e/o escludere determinati file nella fonte di ServiceNo w dati. I file che corrispondono ai modelli sono inclusi nell'indice. I file che non corrispondono ai modelli sono esclusi dall'indice. Se un file corrisponde sia a un modello di esclusione sia a un modello di inclusione, il modello di esclusione ha la precedenza e il file non viene incluso nell'indice.

Configurazione	Descrizione
• isCrawlKnowledgeArticolo • isCrawlKnowledgeArticleAttachment • includePublicArticlesSolo • isCrawlServiceCatalogo • isCrawlServiceCatalogAttachment • isCrawlActiveServiceCatalog • isCrawlInactiveServiceCatalog • isCrawlIncident • isCrawlIncidentAllegato • isCrawlActiveIncidente • isCrawlInactiveIncidente • Applica ACL ForKnowledgeArticle • Applica ACL ForServiceCatalog • Applica ACL ForIncident	`true`per eseguire la scansione di articoli ServiceNow informativi, cataloghi di servizi, incidenti e allegati.
tipo	Il tipo di origine dati. Specificare `SERVICENOWV2` come tipo di origine dati.
enableIdentityCrawler	`true`utilizzare il crawler Amazon Kendra di identità per sincronizzare le informazioni sull'identità/principali su utenti e gruppi con accesso a determinati documenti . Se il crawler di identità è disattivato, tutti i documenti possono essere ricercati pubblicamente. Se desideri utilizzare il controllo degli accessi per i tuoi documenti e il crawler di identità è disattivato, in alternativa puoi utilizzare l'PutPrincipalMappingAPI per caricare le informazioni di accesso di utenti e gruppi.

Configurazione	Descrizione
SyncMode	Specificate come Amazon Kendra aggiornare l'indice quando il contenuto dell'origine dati cambia. Puoi scegliere tra: • `FORCED_FULL_CRAWL` per indicizzare nuovamente tutti i contenuti, sostituendo i contenuti esistenti ogni volta che l'origine dati si sincronizza con l'indice. • `FULL_CRAWL` per indicizzare solo i contenuti nuovi, modificati ed eliminati ogni volta che l'origine dati si sincronizza con l'indice. Amazon Kendra può utilizzar e il meccanismo dell'origine dati per tenere traccia delle modifiche ai contenuti e indicizzare i contenuti modificati dall'ultima sincronizzazione.

Secretary ARN	L'Amazon Resource Name (ARN) di un AWS Secrets Manager segreto che contiene le coppie chiave-valore necessarie per connettersi al tuo. ServiceNow Il segreto deve contenere una struttura JSON con le seguenti chiavi:
	`{ "username": " user name", "password": " password" }`
	Se utilizzi l'autenticazione OAuth2, il tuo segreto deve contenere una struttura JSON con le seguenti chiavi:
	`{ "username": " user name", "password": " password", "clientId": " client id", "clientSecret": " client secret" }`

version	La versione del modello attualmente supportata.

ServiceNow Schema 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"
  ]
}
```

Schema del modello Slack

Includi un JSON che contiene lo schema dell'origine dati come parte dell'TemplateConfigurationoggetto. L'URL dell'host viene fornito come parte della configurazione della connessione o dei dettagli dell'endpoint del repository. Specificate anche il tipo di origine datiSLACK, un segreto per le credenziali di autenticazione e altre configurazioni necessarie. È quindi necessario specificare TEMPLATE come Type quando si chiama. CreateDataSource

Puoi utilizzare il modello fornito in questa guida per sviluppatori. Per informazioni, consulta Schema JSON di Slack.

La tabella seguente descrive i parametri dello schema JSON di Slack.

Configurazione	Descrizione
Configurazione della connessione	Informazioni di configurazione per l'endpoint per l'origine dati.
repositoryEndpointMetadata	Le informazioni sull'endpoint per l'origine dati.
TeamID	L'ID del team Slack che hai copiato dall'URL della pagina principale di Slack.
Configurazioni del repository	Informazioni di configurazione per il contenuto dell'origine dati. Ad esempio, la configurazione di tipi specifici di contenuti e mappature dei campi.
Tutti	Un elenco di oggetti che mappano gli attributi o i nomi di campo dei Slack contenuti per Amazon Kendra indicizzare i nomi dei campi.

Configurazione	Descrizione
Proprietà aggiuntive	Opzioni di configurazione aggiuntive per i contenuti della fonte di dati.
Modelli di inclusione	Un elenco di modelli di espressioni regolari per includere contenuti specifici nella fonte di datiSlack. I contenuti che corrispondono ai modelli sono inclusi nell'indice. I contenuti che non corrispondono ai modelli sono esclusi dall'indice. Se un contenuto corrisponde sia a un modello di inclusione che a uno di esclusion e, il modello di esclusione ha la precedenza e il contenuto non viene incluso nell'indice.
Modelli di esclusione	Un elenco di modelli di espressioni regolari per escludere contenuti specifici nella fonte di Slack dati. I contenuti che corrispondono ai modelli sono esclusi dall'indice. I contenuti che non corrispondono ai modelli sono inclusi nell'indice. Se un contenuto corrisponde sia a un modello di inclusione che a uno di esclusion e, il modello di esclusione ha la precedenza e il contenuto non viene incluso nell'indice.
crawlBotMessages	`true`per scansionare i messaggi dei bot.
Escludi archiviati	`true`per escludere la scansione dei messaggi archiviati.
Tipo di conversazione	Il tipo di conversazione che desideri indicizzare se`PUBLIC_CHANNEL` , `PRIVATE_CHANNEL` e. `GROUP_MESSAGE` `DIRECT_MESSAGE`
Filtro del canale	Il tipo di canale che desideri indicizzare se o`private_channel` . `public_channel`

Configurazione	Descrizione
Dal momento della data	È possibile scegliere di configurare un `sinceDate` parametro in modo che il Slack connettore esegua la scansione del contenuto in base a uno specifico. `sinceDate`
Guarda indietro	Puoi scegliere di configurare un `lookBack` parametro in modo che il Slack connettore esegua la scansione dei contenuti aggiornati o eliminati fino a un determinato numero di ore prima dell'ultima sincronizzazione del connettor e.
Modalità di sincronizzazione	Specificate come Amazon Kendra aggiornar e l'indice quando il contenuto dell'origine dati cambia. Puoi scegliere tra: • `FORCED_FULL_CRAWL` per indicizzare nuovamente tutti i contenuti, sostituendo i contenuti esistenti ogni volta che l'origine dati si sincronizza con l'indice. • `FULL_CRAWL` per indicizzare solo i contenuti nuovi, modificati ed eliminati ogni volta che l'origine dati si sincronizza con l'indice. Amazon Kendra può utilizzare il meccanism o dell'origine dati per tenere traccia delle modifiche ai contenuti e indicizzare i contenuti modificati dall'ultima sincroniz zazione. • `CHANGE_LOG` per indicizzare solo contenuti nuovi e modificati ogni volta che l'origine dati si sincronizza con l'indice. Amazon Kendra può utilizzare il meccanismo dell'origine dati per tenere traccia delle modifiche ai contenuti e indicizzare i contenuti modificati dall'ultima sincronizzazione.

Configurazione	Descrizione
tipo	Il tipo di fonte di dati. Specificare `SLACK` come tipo di origine dati.
enableIdentityCrawler	`true`utilizzare il crawler Amazon Kendra di identità per sincronizzare le informazioni sull'identità/principali su utenti e gruppi con accesso a determinati documenti. Se il crawler di identità è disattivato, tutti i documenti possono essere ricercati pubblicamente. Se desideri utilizzare il controllo degli accessi per i tuoi documenti e il crawler di identità è disattivato, in alternativa puoi utilizzare l'PutPrincipalMappingAPI per caricare le informazioni di accesso di utenti e gruppi.
Secretarn	L'Amazon Resource Name (ARN) di un AWS Secrets Manager segreto che contiene le coppie chiave-valore necessarie per connettersi al tuo. Slack Il segreto deve contenere una struttura JSON con le seguenti chiavi: `{ "slackToken": " token" }`
version	La versione di questo modello attualmente supportata.

Schema JSON di Slack

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

Schema del modello Zendesk

Includi un JSON che contiene lo schema dell'origine dati come parte dell'TemplateConfigurationoggetto. L'URL dell'host viene fornito come parte della configurazione della connessione o dei dettagli dell'endpoint del repository. Specificate anche il tipo di origine

datiZENDESK, un segreto per le credenziali di autenticazione e altre configurazioni necessarie. È quindi necessario specificare TEMPLATE come Type quando si chiama. CreateDataSource

Puoi utilizzare il modello fornito in questa guida per sviluppatori. Per informazioni, consulta Schema JSON di Zendesk.

La tabella seguente descrive i parametri dello schema JSON di Zendesk.

Configurazione	Descrizione
Configurazione della connessione	Informazioni di configurazione per l'endpoint per l'origine dati.
repositoryEndpointMetadata	Le informazioni sull'endpoint per l'origine dati.
HostUrl	L'URL dell'host Zendesk. Ad esempio, https://yoursubdomain.zendesk.com.
Configurazioni del repository	Informazioni di configurazione per il contenuto dell'origine dati. Ad esempio, la configurazione di tipi specifici di contenuti e mappature dei campi.
• ticket • TicketComment • ticketCommentAttachment • articolo • Commento all'articolo • Allegato all'articolo • Argomento della community • communityPostComment	Un elenco di oggetti che mappano gli attributi o i nomi di campo dei ticket Zendesk ai nomi dei campi indice di Amazon Kendra. Per ulteriori informazioni, consulta la sezione Mappatura dei campi di origine dei dati.
Secretarn	L'Amazon Resource Name (ARN) di un AWS Secrets Manager segreto che contiene le coppie chiave-valore necessarie per connettersi a Zendesk. Il segreto deve contenere una struttura JSON con le seguenti chiavi: URL

Configurazione	Descrizione
	host, ID client, client secret, nome utente e password.
Proprietà aggiuntive	Opzioni di configurazione aggiuntive per i contenuti della fonte di dati
organizationNameFilter	Puoi scegliere di indicizzare i ticket esistenti all'interno di una specifica organizzazione.
Dal momento della data	Puoi scegliere di configurare un `sinceDate` parametro in modo che il connettore Zendesk esegua la scansione dei contenuti in base a uno specifico. `sinceDate`
Modelli di inclusione	Un elenco di modelli di espressioni regolari per includere determinati file nella fonte dati Zendesk. I file che corrispondono ai modelli sono inclusi nell'indice. I file che non corrispon dono ai modelli sono esclusi dall'indice. Se un file corrisponde sia a un modello di inclusione che di esclusione, il modello di esclusione ha la precedenza e il file non viene incluso nell'indi ce.
Modelli di esclusione	Un elenco di modelli di espressioni regolari per escludere determinati file nella fonte dati Zendesk. I file che corrispondono ai modelli sono esclusi dall'indice. I file che non corrispon dono ai modelli sono inclusi nell'indice. Se un file corrisponde sia a un modello di esclusione che a uno di inclusione, il modello di esclusion e ha la precedenza e il file non viene incluso nell'indice.

Configurazione	Descrizione
• isCrawlTicket • isCrawlTicketCommento • isCrawlTicketCommentAttachment • isCrawlArticle • isCrawlArticleCommento • isCrawlArticleAllegato • isCrawlCommunityArgomento • isCrawlCommunityPosta • isCrawlCommunityPostComment	Inserisci "`true`" per eseguire la scansione di questi tipi di contenuti.
tipo	Specificare `ZENDESK` come tipo di origine dati.
useChangeLog	Inserisci "`true`" per utilizzare il log delle modifiche di Zendesk per determinare quali documenti devono essere aggiornati nell'indi ce. A seconda delle dimensioni del registro delle modifiche, potrebbe essere più veloce scansionare i documenti in Zendesk. Se sincronizzi la fonte di dati Zendesk con l'indice per la prima volta, tutti i documenti vengono scansionati.

Schema JSON di Zendesk

```
{
  "$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 Managerè un sistema di gestione dei contenuti utilizzato per creare contenuti per siti Web o app mobili. Puoi utilizzarlo Amazon Kendra per connetterti Adobe Experience Manager e indicizzare le tue pagine e i tuoi contenuti.

Amazon Kendra supporta Adobe Experience Manager (AEM) come istanza di autore di Cloud Service e istanza di autore Adobe Experience Manager e pubblicazione in locale.

Puoi connetterti Amazon Kendra alla tua fonte di Adobe Experience Manager dati utilizzando la Amazon Kendra console o l'API. TemplateConfiguration

Per la risoluzione dei problemi relativi al connettore di origine dati di Amazon Kendra Adobe Experience Manager, consultaRisoluzione dei problemi relativi alle origini dati.

Argomenti

- Funzionalità supportate
- Prerequisiti
- Istruzioni di connessione

Funzionalità supportate

Adobe Experience Manageril connettore di origine dati supporta le seguenti funzionalità:

- mappature dei campi
- Filtraggio del contesto utente

- Filtri di inclusione/esclusione
- Sincronizzazione completa e incrementale dei contenuti
- OAuth 2.0 e autenticazione di base
- Virtual Private Cloud (VPC) (Cloud privato virtuale (VPC)

Prerequisiti

Prima di utilizzarla Amazon Kendra per indicizzare la tua fonte di Adobe Experience Manager dati, apporta queste modifiche ai tuoi account Adobe Experience Manager e AWS .

NelAdobe Experience Manager, assicurati di avere:

- Accesso a un account con privilegi amministrativi o a un utente amministratore.
- Hai copiato l'URL dell'Adobe Experience Managerhost.

> **Note**
>
> (On-premise/server) Amazon Kendra verifica se le informazioni sull'endpoint incluse sono le stesse informazioni sull'endpoint specificate nei AWS Secrets Manager dettagli di configurazione dell'origine dati. In questo modo si evita il problema del confuso vicario, ossia un problema di sicurezza in cui un utente non è autorizzato a eseguire un'azione ma lo utilizza Amazon Kendra come proxy per accedere al segreto configurato ed eseguire l'azione. Se successivamente modifichi le informazioni sull'endpoint, devi creare un nuovo segreto per sincronizzare queste informazioni.

- Hai annotato le credenziali di autenticazione di base del nome utente e della password dell'amministratore.
- Facoltativo: credenziali OAuth 2.0 generate in Adobe Experience Manager (AEM) come servizio cloud o AEM On-Premise. Se utilizzi AEM On-Premise, le credenziali includono l'ID client, il segreto del client e la chiave privata. Se utilizzi AEM come servizio cloud, le credenziali includono l'ID client, il segreto del cliente, la chiave privata, l'ID dell'organizzazione, l'ID tecnico dell'account e l'host (IMS). Adobe Identity Management System Per ulteriori informazioni su come generare queste credenziali per AEM as a Cloud Service, consulta la documentazione. Adobe Experience Manager Per AEM On-Premise, l'implementazione del server Adobe Granite OAuth 2.0 (com.adobe.granite.oauth.server) fornisce il supporto per le funzionalità del server OAuth 2.0 in AEM.

- Controllato, ogni documento è unico in Adobe Experience Manager e tra le altre fonti di dati che intendi utilizzare per lo stesso indice. Ogni fonte di dati che desideri utilizzare per un indice non deve contenere lo stesso documento in tutte le fonti di dati. Gli ID dei documenti sono globali rispetto a un indice e devono essere univoci per indice.

Nel tuo Account AWS, assicurati di avere:

- Ha creato un Amazon Kendra indice e, se si utilizza l'API, ha annotato l'ID dell'indice.
- Hai creato un IAM ruolo per la tua origine dati e, se utilizzi l'API, hai annotato l'ARN del IAM ruolo.

> **Note**
>
> Se modifichi il tipo di autenticazione e le credenziali, devi aggiornare il IAM ruolo per accedere all'ID AWS Secrets Manager segreto corretto.

- Ha archiviato le credenziali di autenticazione di Adobe Experience Manager in un luogo AWS Secrets Manager segreto e, se si utilizza l'API, ha annotato l'ARN del segreto.

> **Note**
>
> Ti consigliamo di aggiornare o ruotare regolarmente le credenziali e il segreto. Fornisci solo il livello di accesso necessario per la tua sicurezza. Non è consigliabile riutilizzare credenziali e segreti tra diverse fonti di dati e versioni dei connettori 1.0 e 2.0 (ove applicabile).

Se non disponi di un IAM ruolo o di un segreto esistente, puoi utilizzare la console per creare un nuovo IAM ruolo e un Secrets Manager segreto quando connetti l'origine dati di Adobe Experience Manager a. Amazon Kendra Se utilizzi l'API, devi fornire l'ARN di un IAM ruolo e di un Secrets Manager segreto esistenti e un ID di indice.

Istruzioni di connessione

Per connetterti Amazon Kendra alla tua fonte di Adobe Experience Manager dati, devi fornire i dettagli necessari della tua origine Adobe Experience Manager dati in modo che Amazon Kendra possa accedere ai tuoi dati. Se non hai ancora configurato Adobe Experience Manager per Amazon Kendra, consultaPrerequisiti.

Console

Per connettersi Amazon Kendra a Adobe Experience Manager

1. Accedi a AWS Management Console e apri la Amazon Kendra console.
2. Dal riquadro di navigazione a sinistra, scegli Indici, quindi scegli l'indice che desideri utilizzare dall'elenco degli indici.

> **Note**
>
> Puoi scegliere di configurare o modificare le impostazioni del controllo dell'accesso degli utenti in Impostazioni dell'indice.

3. Nella pagina Guida introduttiva, scegli Aggiungi origine dati.
4. Nella pagina Aggiungi origine dati, scegli Adobe Experience Manager connector, quindi scegli Aggiungi connettore.
5. Nella pagina Specificare i dettagli dell'origine dati, inserisci le seguenti informazioni:
   a. In Nome e descrizione, per Nome dell'origine dati, inserisci un nome per l'origine dati. Puoi includere trattini ma non spazi.
   b. (Facoltativo) Descrizione: immetti una descrizione facoltativa per l'origine dati.
   c. In Lingua predefinita: scegli una lingua per filtrare i documenti per l'indice. Se non diversamente specificato, la lingua predefinita è l'inglese. La lingua specificata nei metadati del documento ha la precedenza sulla lingua selezionata.
   d. In Tag, per Aggiungi nuovo tag, includi tag opzionali per cercare e filtrare le risorse o tenere traccia dei costi. AWS
   e. Seleziona Successivo.
6. Nella pagina Definisci accesso e sicurezza, inserisci le seguenti informazioni:
   a. Fonte: scegli AEM On-Premise o AEM as a Cloud Service.

      Inserisci l'URL dell'host. Adobe Experience Manager Ad esempio, se utilizzi AEM On-Premise, includi il nome host e la porta:. https://hostname:port Oppure, se utilizzi AEM come servizio cloud, puoi utilizzare l'URL dell'autore:. https://author-xxxxxx-xxxxxxx.adobeaemcloud.com

b. Posizione del certificato SSL: inserite il percorso del certificato SSL archiviato in un bucket. Amazon S3 Lo usi per connetterti ad AEM On-Premise con una connessione SSL sicura.

c. Autorizzazione: attiva o disattiva le informazioni dell'elenco di controllo degli accessi (ACL) per i tuoi documenti, se disponi di un ACL e desideri utilizzarlo per il controllo degli accessi. L'ACL specifica a quali documenti possono accedere utenti e gruppi. Le informazioni ACL vengono utilizzate per filtrare i risultati della ricerca in base all'accesso dell'utente o del relativo gruppo ai documenti. Per ulteriori informazioni, consulta Filtraggio del contesto utente.

d. Autenticazione: scegli l'autenticazione di base o l'autenticazione OAuth 2.0. Quindi scegli un AWS Secrets Manager segreto esistente o crea un nuovo segreto per archiviare le tue credenziali. Adobe Experience Manager Se scegli di creare un nuovo segreto, si apre una finestra AWS Secrets Manager segreta.

   Se hai scelto Autenticazione di base, inserisci un nome per il segreto, il nome utente e la password del Adobe Experience Manager sito. L'utente deve disporre dell'autorizzazione di amministratore o essere un utente amministratore.

   Se hai scelto l'autenticazione OAuth 2.0 e utilizzi AEM On-Premise, inserisci un nome per il segreto, l'ID client, il segreto del client e la chiave privata. Se utilizzi AEM come servizio cloud, inserisci un nome per il segreto, l'ID client, il segreto del cliente, la chiave privata, l'ID dell'organizzazione, l'ID tecnico dell'account e l'host (IMS). Adobe Identity Management System

   Selezionare Salva.

e. Virtual Private Cloud (VPC): puoi scegliere di utilizzare un VPC. In tal caso, è necessario aggiungere sottoreti e gruppi di sicurezza VPC.

f. Identity crawler: specifica se attivare il crawler di identità. Amazon Kendra Il crawler di identità utilizza le informazioni dell'elenco di controllo degli accessi (ACL) per i documenti per filtrare i risultati della ricerca in base all'accesso dell'utente o del relativo gruppo ai documenti. Se disponi di un ACL per i tuoi documenti e scegli di utilizzarlo, puoi anche scegliere di attivare il crawler di identità per configurare il filtraggio Amazon Kendra del contesto utente dei risultati di ricerca. Altrimenti, se il crawler di identità è disattivato, tutti i documenti possono essere ricercati pubblicamente. Se desideri utilizzare il controllo degli accessi per i tuoi documenti e il crawler di identità è disattivato, in alternativa puoi

utilizzare l'PutPrincipalMappingAPI per caricare le informazioni di accesso di utenti e gruppi per il filtraggio del contesto degli utenti.

g. IAM ruolo: scegli un IAM ruolo esistente o creane uno nuovo IAM per accedere alle credenziali del repository e indicizzare il contenuto.

> **Note**
>
> IAM i ruoli utilizzati per gli indici non possono essere utilizzati per le fonti di dati. Se non sei sicuro che un ruolo esistente venga utilizzato per un indice o una FAQ, scegli Crea un nuovo ruolo per evitare errori.

h. Seleziona Successivo.

7. Nella pagina Configura le impostazioni di sincronizzazione, inserisci le seguenti informazioni:

   a. Ambito di sincronizzazione: imposta i limiti per la scansione di determinati tipi di contenuto, componenti della pagina e percorsi root e filtra i contenuti utilizzando modelli di espressioni regex.

      i. Tipi di contenuto: scegliete se eseguire la scansione solo delle pagine o delle risorse o di entrambe.

      ii. (Facoltativo) Configurazione aggiuntiva: configura le seguenti impostazioni:

      - Componenti della pagina: i nomi specifici dei componenti della pagina. Il componente Page è un componente di pagina estensibile progettato per funzionare con l'editor di Adobe Experience Manager modelli e consente di assemblare i componenti dell'intestazione, del piè di pagina e della struttura con l'editor di modelli.
      - Varianti dei frammenti di contenuto: i nomi specifici delle varianti dei frammenti di contenuto. I frammenti di contenuto consentono di progettare, creare, curare e pubblicare contenuti indipendenti dalla pagina in. Adobe Experience Manager Consentono di preparare contenuti pronti per l'uso in più posizioni/su più canali.
      - Percorsi principali: i percorsi principali verso contenuti specifici.
      - Modelli Regex: i modelli di espressioni regolari per includere o escludere determinate pagine e risorse.

   b. Modalità di sincronizzazione: scegli come aggiornare l'indice quando il contenuto della fonte di dati cambia. Quando sincronizzi l'origine dati con Amazon Kendra per la prima volta, tutto il contenuto viene sottoposto a scansione e indicizzato per

impostazione predefinita. Se la sincronizzazione iniziale non è riuscita, devi eseguire una sincronizzazione completa dei dati, anche se non scegli la sincronizzazione completa come opzione della modalità di sincronizzazione.

- Sincronizzazione completa: indicizza di nuovo tutti i contenuti, sostituendo i contenuti esistenti ogni volta che l'origine dati si sincronizza con l'indice.
- Nuova sincronizzazione modificata: indicizza solo i contenuti nuovi e modificati ogni volta che l'origine dati si sincronizza con l'indice. Amazon Kendra può utilizzare il meccanismo dell'origine dati per tenere traccia delle modifiche ai contenuti e indicizzare i contenuti modificati dall'ultima sincronizzazione.
- Sincronizzazione nuova, modificata ed eliminata: indicizza solo i contenuti nuovi, modificati ed eliminati ogni volta che l'origine dati si sincronizza con l'indice. Amazon Kendra può utilizzare il meccanismo dell'origine dati per tenere traccia delle modifiche ai contenuti e indicizzare i contenuti modificati dall'ultima sincronizzazione.

c. ID del fuso orario: se utilizzate AEM On-Premise e il fuso orario del server è diverso dal fuso orario del connettore o dell'indice Amazon Kendra AEM, potete specificare il fuso orario del server da allineare al connettore o all'indice AEM. Il fuso orario predefinito per AEM On-Premise è il fuso orario del connettore o dell'indice AEM. Amazon Kendra Il fuso orario predefinito per AEM come servizio cloud è l'ora media di Greenwich.

d. Pianificazione dell'esecuzione della sincronizzazione: per Frequenza, scegliete la frequenza di sincronizzazione con la fonte di dati. Amazon Kendra

e. Seleziona Successivo.

8. Nella pagina Imposta mappature dei campi, inserisci le seguenti informazioni:

   a. Seleziona uno dei campi di origine dati predefiniti Amazon Kendra generati che desideri mappare all'indice. Per aggiungere campi di origine dati personalizzati, crea un nome di campo indice a cui mappare e il tipo di dati del campo.

   b. Seleziona Successivo.

9. Nella pagina Rivedi e crea, verifica che le informazioni inserite siano corrette, quindi seleziona Aggiungi origine dati. Puoi anche scegliere di modificare le tue informazioni da questa pagina. L'origine dati verrà visualizzata nella pagina Origini dati dopo che l'origine dati sarà stata aggiunta correttamente.

API

Per connettersi Amazon Kendra a Adobe Experience Manager

È necessario specificare un codice JSON dello schema dell'origine dati utilizzando l'TemplateConfigurationAPI. È necessario fornire le seguenti informazioni:

- Origine dati: specifica il tipo di origine dati come `AEM` quando usi lo schema TemplateConfigurationJSON. Specificate anche l'origine dati come `TEMPLATE` quando chiamate l'CreateDataSourceAPI.
- URL host AEM: specifica l'URL dell'Adobe Experience Managerhost. Ad esempio, se utilizzi AEM On-Premise, includi il nome host e la porta:. https://hostname:port Oppure, se utilizzi AEM come servizio cloud, puoi utilizzare l'URL dell'autore:. https://author-xxxxxx-xxxxxxx.adobeaemcloud.com
- Modalità di sincronizzazione: specifica come Amazon Kendra aggiornare l'indice quando il contenuto dell'origine dati cambia. Quando sincronizzi l'origine dati con Amazon Kendra per la prima volta, tutto il contenuto viene sottoposto a scansione e indicizzato per impostazione predefinita. Se la sincronizzazione iniziale non è riuscita, devi eseguire una sincronizzazione completa dei dati, anche se non scegli la sincronizzazione completa come opzione della modalità di sincronizzazione. Puoi scegliere tra:
  - `FORCED_FULL_CRAWL`per indicizzare nuovamente tutti i contenuti, sostituendo i contenuti esistenti ogni volta che l'origine dati si sincronizza con l'indice.
  - `FULL_CRAWL`per indicizzare solo i contenuti nuovi, modificati ed eliminati ogni volta che l'origine dati si sincronizza con l'indice. Amazon Kendra può utilizzare il meccanismo dell'origine dati per tenere traccia delle modifiche ai contenuti e indicizzare i contenuti modificati dall'ultima sincronizzazione.
  - `CHANGE_LOG`per indicizzare solo contenuti nuovi e modificati ogni volta che l'origine dati si sincronizza con l'indice. Amazon Kendra può utilizzare il meccanismo dell'origine dati per tenere traccia delle modifiche ai contenuti e indicizzare i contenuti modificati dall'ultima sincronizzazione.
- Tipo di autenticazione: specifica il tipo di autenticazione che desideri utilizzare, `Basic` oppure`OAuth2`.
- Tipo AEM: specifica il tipo da Adobe Experience Manager utilizzare, oppure. `CLOUD` `ON_PREMISE`
- Secret Amazon Resource Name (ARN): se desideri utilizzare l'autenticazione di base per AEM On-Premise o Cloud, fornisci un codice segreto che memorizza le credenziali di autenticazione del nome utente e della password. Fornisci l'Amazon Resource Name (ARN) di un AWS Secrets Manager segreto. Il segreto viene archiviato in una struttura JSON con le seguenti chiavi:

```
{
    "aemUrl": "Adobe Experience Manager On-Premise host URL",
    "username": "user name with admin permissions",
    "password": "password with admin permissions"
}
```

Se desideri utilizzare l'autenticazione OAuth 2.0 per AEM On-Premise, il segreto viene archiviato in una struttura JSON con le seguenti chiavi:

```
{
    "aemUrl": "Adobe Experience Manager host URL",
    "clientId": "client ID",
    "clientSecret": "client secret",
    "privateKey": "private key"
}
```

Se desideri utilizzare l'autenticazione OAuth 2.0 per AEM come servizio cloud, il segreto viene archiviato in una struttura JSON con le seguenti chiavi:

```
{
    "clientId": "client ID",
    "clientSecret": "client secret",
    "privateKey": "private key",
    "orgId": "organization ID",
    "technicalAccountId": "technical account ID",
    "imsHost": "Adobe Identity Management System (IMS) host"
}
```

- IAM ruolo: specifica `RoleArn` quando chiami `CreateDataSource` per fornire a un IAM ruolo le autorizzazioni per accedere al tuo Secrets Manager segreto e per chiamare le API pubbliche richieste per il connettore Adobe Experience Manager e. Amazon Kendra Per ulteriori informazioni, consulta IAM i ruoli per le fonti di dati di Adobe Experience Manager.

Puoi anche aggiungere le seguenti funzionalità opzionali:

- Virtual Private Cloud (VPC): `VpcConfiguration` specifica quando si chiama. `CreateDataSource` Per ulteriori informazioni, consulta Configurazione Amazon Kendra per l'utilizzo di un Amazon VPC.

- ID del fuso orario: se utilizzate AEM On-Premise e il fuso orario del server è diverso dal fuso orario del connettore o dell'indice Amazon Kendra AEM, potete specificare il fuso orario del server da allineare al connettore o all'indice AEM.

  Il fuso orario predefinito per AEM On-Premise è il fuso orario del connettore o dell'indice AEM. Amazon Kendra Il fuso orario predefinito per AEM come servizio cloud è l'ora media di Greenwich.

  Per informazioni sugli ID dei fusi orari supportati, consultate Schema Adobe Experience ManagerJSON.

- Filtri di inclusione ed esclusione: specificate se includere o escludere determinate pagine e risorse.

  > **Note**
  >
  > La maggior parte delle fonti di dati utilizza modelli di espressioni regolari, che sono modelli di inclusione o esclusione denominati filtri. Se si specifica un filtro di inclusione, viene indicizzato solo il contenuto che corrisponde al filtro di inclusione. Qualsiasi documento che non corrisponde al filtro di inclusione non viene indicizzato. Se si specifica un filtro di inclusione ed esclusione, i documenti che corrispondono al filtro di esclusione non vengono indicizzati, anche se corrispondono al filtro di inclusione.

- Identity crawler: specifica se attivare il crawler di identità. Amazon Kendra Il crawler di identità utilizza le informazioni dell'elenco di controllo degli accessi (ACL) per i documenti per filtrare i risultati della ricerca in base all'accesso dell'utente o del relativo gruppo ai documenti. Se disponi di un ACL per i tuoi documenti e scegli di utilizzarlo, puoi anche scegliere di attivare il crawler di identità per configurare il filtraggio Amazon Kendra del contesto utente dei risultati di ricerca. Altrimenti, se il crawler di identità è disattivato, tutti i documenti possono essere ricercati pubblicamente. Se desideri utilizzare il controllo degli accessi per i tuoi documenti e il crawler di identità è disattivato, in alternativa puoi utilizzare l'PutPrincipalMappingAPI per caricare le informazioni di accesso di utenti e gruppi per il filtraggio del contesto degli utenti.
- Mappature dei campi: scegli di mappare i campi delle sorgenti dati di Adobe Experience Manager ai campi indice. Amazon Kendra Per ulteriori informazioni, consulta la sezione Mappatura dei campi di origine dei dati.

> **Note**
>
> Il campo del corpo del documento o l'equivalente del corpo del documento per i documenti è necessario per Amazon Kendra eseguire la ricerca nei documenti. È necessario mappare il nome del campo del corpo del documento nella fonte dati al nome del campo indice `_document_body`. Tutti gli altri campi sono facoltativi.

Per un elenco di altre importanti chiavi JSON da configurare, consulta lo schema Adobe Experience Manager del modello.

Alfresco

Alfrescoè un servizio di gestione dei contenuti che aiuta i clienti a archiviare e gestire i propri contenuti. Puoi usarlo Amazon Kendra per indicizzare la tua libreria di Alfresco documenti, il wiki e il blog.

Amazon Kendra supporta Alfresco On-Premises e Alfresco Cloud (Platform as a Service).

Puoi connetterti Amazon Kendra alla tua fonte di Alfresco dati utilizzando la Amazon Kendra console o l'TemplateConfigurationAPI.

Per la risoluzione dei problemi relativi al connettore di origine dati Amazon Kendra Alfresco, consultaRisoluzione dei problemi relativi alle origini dati.

Argomenti

- Funzionalità supportate
- Prerequisiti
- Istruzioni di connessione
- Ulteriori informazioni

Funzionalità supportate

Amazon Kendra Alfrescoil connettore di origine dati supporta le seguenti funzionalità:

- mappature dei campi
- Filtri di inclusione/esclusione

- Sincronizzazione completa e incrementale dei contenuti
- Virtual Private Cloud (VPC) (Cloud privato virtuale (VPC)
- Filtraggio del contesto utente
- OAuth 2.0 e autenticazione di base

Prerequisiti

Prima di poterla utilizzare Amazon Kendra per indicizzare la fonte di dati Alfresco, apporta queste modifiche nel tuo and. Alfresco Account AWS

NelAlfresco, assicurati di avere:

- Hai copiato l'URL del Alfresco repository e l'URL dell'applicazione web. Se desideri indicizzare solo un Alfresco sito specifico, copia anche l'ID del sito.
- Hai annotato le tue credenziali di Alfresco autenticazione, che includono un nome utente e una password con almeno autorizzazioni di lettura. Se desideri utilizzare l'autenticazione OAuth 2.0, devi aggiungere l'utente al gruppo degli amministratori. Alfresco
- Facoltativo: credenziali OAuth 2.0 generate in. Alfresco Le credenziali includono l'ID client, il segreto del client e l'URL del token. Per ulteriori informazioni su come configurare i client per Alfresco On-Premises, consulta la documentazione di Alfresco. Se utilizzi Alfresco Cloud (PaaS), devi contattare l'assistenza Hyland per Alfresco l'autenticazione OAuth 2.0.
- È stato verificato che ogni documento sia unico in Alfresco e tra le altre fonti di dati che intendi utilizzare per lo stesso indice. Ogni fonte di dati che si desidera utilizzare per un indice non deve contenere lo stesso documento in tutte le fonti di dati. Gli ID dei documenti sono globali rispetto a un indice e devono essere univoci per indice.

Nel tuo Account AWS, assicurati di avere:

- Ha creato un Amazon Kendra indice e, se si utilizza l'API, ha annotato l'ID dell'indice.
- Hai creato un IAM ruolo per la tua origine dati e, se utilizzi l'API, hai annotato l'ARN del IAM ruolo.

> **Note**
>
> Se modifichi il tipo di autenticazione e le credenziali, devi aggiornare il IAM ruolo per accedere all'ID AWS Secrets Manager segreto corretto.

- Ha archiviato le credenziali di autenticazione Alfresco in un AWS Secrets Manager segreto e, se si utilizza l'API, ha annotato l'ARN del segreto.

> **Note**
>
> Ti consigliamo di aggiornare o ruotare regolarmente le credenziali e il segreto. Fornisci solo il livello di accesso necessario per la tua sicurezza. Non è consigliabile riutilizzare credenziali e segreti tra diverse fonti di dati e versioni dei connettori 1.0 e 2.0 (ove applicabile).

Se non disponi di un IAM ruolo o di un segreto esistente, puoi utilizzare la console per creare un nuovo IAM ruolo e un Secrets Manager segreto quando connetti la tua fonte di dati Alfresco a. Amazon Kendra Se utilizzi l'API, devi fornire l'ARN di un IAM ruolo e di un Secrets Manager segreto esistenti e un ID di indice.

Istruzioni di connessione

Per connetterti Amazon Kendra alla tua fonte di dati Alfresco, devi fornire i dettagli necessari della tua origine dati Alfresco in modo che Amazon Kendra possa accedere ai tuoi dati. Se non hai ancora configurato Alfresco per Amazon Kendra, consulta. Prerequisiti

Console

Per connettersi Amazon Kendra a Alfresco

1. Accedi a AWS Management Console e apri la Amazon Kendra console.
2. Dal riquadro di navigazione a sinistra, scegli Indici, quindi scegli l'indice che desideri utilizzare dall'elenco degli indici.

> **Note**
>
> Puoi scegliere di configurare o modificare le impostazioni del controllo dell'accesso degli utenti in Impostazioni dell'indice.

3. Nella pagina Guida introduttiva, scegli Aggiungi origine dati.
4. Nella pagina Aggiungi origine dati, scegli Alfresco connector, quindi scegli Aggiungi connettore.
5. Nella pagina Specificare i dettagli dell'origine dati, inserisci le seguenti informazioni:

a. In Nome e descrizione, per Nome dell'origine dati, inserisci un nome per l'origine dati. Puoi includere trattini ma non spazi.

b. (Facoltativo) Descrizione: immetti una descrizione facoltativa per l'origine dati.

c. In Lingua predefinita: scegli una lingua per filtrare i documenti per l'indice. Se non diversamente specificato, la lingua predefinita è l'inglese. La lingua specificata nei metadati del documento ha la precedenza sulla lingua selezionata.

d. In Tag, per Aggiungi nuovo tag, includi tag opzionali per cercare e filtrare le risorse o tenere traccia dei costi. AWS

e. Seleziona Successivo.

6. Nella pagina Definisci accesso e sicurezza, inserisci le seguenti informazioni:

a. Alfrescotipo: scegli se utilizzare Alfresco On-Premises o Alfresco Cloud (Platform as a Service).

b. URL del repository Alfresco: immettete l'URL del repository Alfresco. Ad esempio, se si utilizza Alfresco Cloud (PaaS), l'URL del repository potrebbe essere. https://company.alfrescocloud.com Oppure, se utilizzi Alfresco On-Premises, l'URL del repository potrebbe essere. https://company-alfresco-instance.company-domain.suffix:port

c. Applicazione utente Alfresco. URL: inserisci l'URL Alfresco dell'interfaccia utente. Puoi ottenere l'URL del repository dal tuo Alfresco amministratore. Ad esempio, l'URL dell'interfaccia utente potrebbe essere https://example.com.

d. Posizione del certificato SSL: immetti il percorso del certificato SSL archiviato in un bucket. Amazon S3 La usi per connetterti a Alfresco On-Premises con una connessione SSL sicura.

e. Autorizzazione: attiva o disattiva le informazioni dell'elenco di controllo degli accessi (ACL) per i tuoi documenti, se disponi di un ACL e desideri utilizzarlo per il controllo degli accessi. L'ACL specifica a quali documenti possono accedere utenti e gruppi. Le informazioni ACL vengono utilizzate per filtrare i risultati della ricerca in base all'accesso dell'utente o del relativo gruppo ai documenti. Per ulteriori informazioni, consulta Filtraggio del contesto utente.

f. Autenticazione: scegli l'autenticazione di base o l'autenticazione OAuth 2.0. Quindi scegli un Secrets Manager segreto esistente o crea un nuovo segreto per archiviare le tue credenziali. Alfresco Se scegli di creare un nuovo segreto, si apre una finestra AWS Secrets Manager segreta.

Se hai scelto Autenticazione di base, inserisci un nome per il segreto, il nome Alfresco utente e la password.

Se hai scelto l'autenticazione OAuth 2.0, inserisci un nome per il segreto, l'ID client, il segreto del client e l'URL del token.

g. Virtual Private Cloud (VPC): puoi scegliere di utilizzare un VPC. In tal caso, è necessario aggiungere sottoreti e gruppi di sicurezza VPC.

h. Identity crawler: specifica se attivare il crawler di identità. Amazon Kendra Il crawler di identità utilizza le informazioni dell'elenco di controllo degli accessi (ACL) per i documenti per filtrare i risultati della ricerca in base all'accesso dell'utente o del relativo gruppo ai documenti. Se disponi di un ACL per i tuoi documenti e scegli di utilizzarlo, puoi anche scegliere di attivare il crawler di identità per configurare il filtraggio Amazon Kendra del contesto utente dei risultati di ricerca. Altrimenti, se il crawler di identità è disattivato, tutti i documenti possono essere ricercati pubblicamente. Se desideri utilizzare il controllo degli accessi per i tuoi documenti e il crawler di identità è disattivato, in alternativa puoi utilizzare l'PutPrincipalMappingAPI per caricare le informazioni di accesso di utenti e gruppi per il filtraggio del contesto degli utenti.

i. IAM ruolo: scegli un IAM ruolo esistente o creane uno nuovo IAM per accedere alle credenziali del repository e indicizzare il contenuto.

> **Note**
>
> IAM i ruoli utilizzati per gli indici non possono essere utilizzati per le fonti di dati. Se non sei sicuro che un ruolo esistente venga utilizzato per un indice o una FAQ, scegli Crea un nuovo ruolo per evitare errori.

j. Seleziona Successivo.

7. Nella pagina Configura le impostazioni di sincronizzazione, inserisci le seguenti informazioni:

a. Ambito di sincronizzazione: imposta i limiti per la scansione di determinati contenuti e filtra i contenuti utilizzando modelli di espressioni regex.

b. i. Contenuto: scegli se eseguire la scansione dei contenuti contrassegnati con «Aspetti» inAlfresco, dei contenuti all'interno di un Alfresco sito specifico o dei contenuti in tutti i siti. Alfresco

ii. (Facoltativo) Configurazione aggiuntiva: imposta le seguenti impostazioni:

- Includi commenti: scegli di includere commenti nella libreria di Alfresco documenti e nel blog.
- Modelli Regex: modelli di espressioni regolari per includere o escludere determinati file.

c. Modalità di sincronizzazione: scegli come aggiornare l'indice quando il contenuto dell'origine dati cambia. Quando sincronizzi l'origine dati con Amazon Kendra per la prima volta, tutto il contenuto viene sottoposto a scansione e indicizzato per impostazione predefinita. Se la sincronizzazione iniziale non è riuscita, devi eseguire una sincronizzazione completa dei dati, anche se non scegli la sincronizzazione completa come opzione della modalità di sincronizzazione.

- Sincronizzazione completa: indicizza di nuovo tutti i contenuti, sostituendo i contenuti esistenti ogni volta che l'origine dati si sincronizza con l'indice.
- Sincronizzazione nuova, modificata ed eliminata: indicizza solo i contenuti nuovi, modificati ed eliminati ogni volta che l'origine dati si sincronizza con l'indice. Amazon Kendra può utilizzare il meccanismo dell'origine dati per tenere traccia delle modifiche ai contenuti e indicizzare i contenuti modificati dall'ultima sincronizzazione.

d. Nella pianificazione di esecuzione della sincronizzazione, per Frequenza: scegli la frequenza di sincronizzazione con la tua fonte di dati. Amazon Kendra

e. Seleziona Successivo.

8. Nella pagina Imposta le mappature dei campi, inserisci le seguenti informazioni:

a. Seleziona tra i campi di origine dati predefiniti Amazon Kendra generati che desideri mappare al tuo indice.

b. Per aggiungere campi di origine dati personalizzati, crea un nome di campo indice a cui mappare e il tipo di dati del campo.

c. Seleziona Successivo.

9. Nella pagina Rivedi e crea, verifica che le informazioni che hai inserito siano corrette, quindi seleziona Aggiungi origine dati. Puoi anche scegliere di modificare le tue informazioni da questa pagina. L'origine dati verrà visualizzata nella pagina Origini dati dopo che l'origine dati sarà stata aggiunta correttamente.

API

Per connettersi Amazon Kendra a Alfresco

È necessario specificare un codice JSON dello schema dell'origine dati utilizzando l'TemplateConfigurationAPI. È necessario fornire le seguenti informazioni:

- Origine dati: specifica il tipo di origine dati come `ALFRESCO` quando usi lo schema TemplateConfigurationJSON. Specificate anche l'origine dati come `TEMPLATE` quando chiamate l'CreateDataSourceAPI.
- AlfrescoID del sito: specifica l'ID del sito Alfresco.
- AlfrescoURL del repository: specifica l'URL del repository. Alfresco È possibile ottenere l'URL del repository dal proprio amministratore. Alfresco Ad esempio, se utilizzi Alfresco Cloud (PaaS), l'URL del repository potrebbe essere. https://company.alfrescocloud.com Oppure, se utilizzi Alfresco On-Premises, l'URL del repository potrebbe essere. https://company-alfresco-instance.company-domain.suffix:port
- AlfrescoURL dell'applicazione web: specifica l'URL dell'Alfrescointerfaccia utente. È possibile ottenere l'URL del repository dal proprio Alfresco amministratore. Ad esempio, l'URL dell'interfaccia utente potrebbe essere https://example.com.
- Tipo di autenticazione: specifica il tipo di autenticazione che desideri utilizzare, se `OAuth2` o`Basic`.
- Alfrescotipo: specifica il tipo di Alfresco servizio utilizzato, se `PAAS` (Cloud/Platform as a Service) o `ON_PREM` (On-Premises).
- Amazon Resource Name (ARN) segreto: se desideri utilizzare l'autenticazione di base, fornisci un codice segreto che memorizza le credenziali di autenticazione del nome utente e della password. Fornisci l'Amazon Resource Name (ARN) di un AWS Secrets Manager segreto. Il segreto viene archiviato in una struttura JSON con le seguenti chiavi:

```
{
    "username": "user name",
    "password": "password"
}
```

Se desideri utilizzare l'autenticazione OAuth 2.0, il segreto viene archiviato in una struttura JSON con le seguenti chiavi:

```
{
    "clientId": "client ID",
    "clientSecret": "client secret",
    "tokenUrl": "token URL"
```

```
}
```

- IAM role —Specificate `RoleArn` quando chiamate `CreateDataSource` per fornire a un IAM ruolo le autorizzazioni per accedere al vostro Secrets Manager segreto e per chiamare le API pubbliche richieste per il connettore Alfresco e. Amazon Kendra Per ulteriori informazioni, consulta i IAM ruoli per le fonti di dati Alfresco.

Puoi anche aggiungere le seguenti funzionalità opzionali:

- Virtual Private Cloud (VPC): `VpcConfiguration` specifica quando si chiama. `CreateDataSource` Per ulteriori informazioni, consulta Configurazione Amazon Kendra per l'utilizzo di un Amazon VPC.
- Tipo di contenuto: il tipo di contenuto che desideri sottoporre a scansione, che si tratti di contenuti contrassegnati con «Aspetti» inAlfresco, contenuti all'interno di un Alfresco sito specifico o contenuti in tutti i tuoi siti. Alfresco Puoi anche elencare contenuti «Aspetti» specifici.
- Filtri di inclusione ed esclusione: specifica se includere o escludere determinati file.

> **Note**
>
> La maggior parte delle fonti di dati utilizza modelli di espressioni regolari, che sono modelli di inclusione o esclusione denominati filtri. Se si specifica un filtro di inclusione, viene indicizzato solo il contenuto che corrisponde al filtro di inclusione. Qualsiasi documento che non corrisponde al filtro di inclusione non viene indicizzato. Se si specifica un filtro di inclusione ed esclusione, i documenti che corrispondono al filtro di esclusione non vengono indicizzati, anche se corrispondono al filtro di inclusione.

- Modalità di sincronizzazione: specifica come Amazon Kendra aggiornare l'indice quando il contenuto dell'origine dati cambia. Quando sincronizzi l'origine dati con Amazon Kendra per la prima volta, tutto il contenuto viene sottoposto a scansione e indicizzato per impostazione predefinita. Se la sincronizzazione iniziale non è riuscita, devi eseguire una sincronizzazione completa dei dati, anche se non scegli la sincronizzazione completa come opzione della modalità di sincronizzazione. Puoi scegliere tra:
  - `FORCED_FULL_CRAWL`per indicizzare nuovamente tutti i contenuti, sostituendo i contenuti esistenti ogni volta che l'origine dati si sincronizza con l'indice.
  - `FULL_CRAWL`per indicizzare solo i contenuti nuovi, modificati ed eliminati ogni volta che l'origine dati si sincronizza con l'indice. Amazon Kendra può utilizzare il meccanismo

dell'origine dati per tenere traccia delle modifiche ai contenuti e indicizzare i contenuti modificati dall'ultima sincronizzazione.

- Identity crawler: specifica se attivare il crawler Amazon Kendra di identità. Il crawler di identità utilizza le informazioni dell'elenco di controllo degli accessi (ACL) per i documenti per filtrare i risultati della ricerca in base all'accesso dell'utente o del relativo gruppo ai documenti. Se disponi di un ACL per i tuoi documenti e scegli di utilizzarlo, puoi anche scegliere di attivare il crawler di identità per configurare il filtraggio Amazon Kendra del contesto utente dei risultati di ricerca. Altrimenti, se il crawler di identità è disattivato, tutti i documenti possono essere ricercati pubblicamente. Se desideri utilizzare il controllo degli accessi per i tuoi documenti e il crawler di identità è disattivato, in alternativa puoi utilizzare l'PutPrincipalMappingAPI per caricare le informazioni di accesso di utenti e gruppi per il filtraggio del contesto degli utenti.
- Mappature dei campi: scegliete di mappare i campi delle sorgenti dati di Alfresco ai campi indice. Amazon Kendra Per ulteriori informazioni, consulta la sezione Mappatura dei campi di origine dei dati.

> **Note**
>
> Il campo del corpo del documento o l'equivalente del corpo del documento per i documenti è necessario per Amazon Kendra effettuare la ricerca nei documenti. È necessario mappare il nome del campo del corpo del documento nella fonte dati al nome del campo indice`_document_body`. Tutti gli altri campi sono facoltativi.

Per un elenco di altre importanti chiavi JSON da configurare, consulta lo schema Alfresco del modello.

Ulteriori informazioni

Per saperne di più sull'integrazione Amazon Kendra con la tua fonte di dati Alfresco, consulta:

- Cerca in modo intelligente i contenuti utilizzando AlfrescoAmazon Kendra

Aurora (MySQL)

Aurora è un sistema di gestione di database relazionali (RDBMS) creato per il cloud. Se sei un Aurora utente, puoi utilizzarlo Amazon Kendra per indicizzare la tua Aurora (MySQL) fonte di dati.

Il connettore di origine Amazon Kendra Aurora (MySQL) dati supporta Aurora MySQL 3 e Aurora Serverless MySQL 8.0.

Puoi connetterti Amazon Kendra alla tua fonte di Aurora (MySQL) dati utilizzando la console e l'API.Amazon KendraTemplateConfiguration

Per la risoluzione dei problemi relativi al connettore della sorgente Amazon Kendra Aurora (MySQL) dati, consultaRisoluzione dei problemi relativi alle origini dati.

Argomenti

- Funzionalità supportate
- Prerequisiti
- Istruzioni di connessione
- Note

Funzionalità supportate

- Mappature dei campi
- Filtraggio del contesto utente
- Filtri di inclusione/esclusione
- Sincronizzazione completa e incrementale dei contenuti
- Virtual Private Cloud (VPC) (Cloud privato virtuale (VPC)

Prerequisiti

Prima di poterla utilizzare Amazon Kendra per indicizzare la tua fonte di Aurora (MySQL) dati, apporta queste modifiche al tuo account Aurora (MySQL) e AWS ai tuoi account.

NelAurora (MySQL), assicurati di avere:

- Hai annotato il nome utente e la password del tuo database.

> **Important**
>
> È consigliabile fornire credenziali Amazon Kendra di database di sola lettura.

- Hai copiato l'URL, la porta e l'istanza dell'host del database. Puoi trovare queste informazioni sulla Amazon RDS console.
- È stato verificato che ogni documento sia unico all'interno Aurora (MySQL) e tra le altre fonti di dati che intendi utilizzare per lo stesso indice. Ogni fonte di dati che desideri utilizzare per un indice non deve contenere lo stesso documento in tutte le fonti di dati. Gli ID dei documenti sono globali rispetto a un indice e devono essere univoci per indice.

Nel tuo Account AWS, assicurati di avere:

- Ha creato un Amazon Kendra indice e, se si utilizza l'API, ha annotato l'ID dell'indice.
- Hai creato un IAM ruolo per la tua origine dati e, se utilizzi l'API, hai annotato l'ARN del IAM ruolo.

> **Note**
>
> Se modifichi il tipo di autenticazione e le credenziali, devi aggiornare il IAM ruolo per accedere all'ID AWS Secrets Manager segreto corretto.

- Ha archiviato le credenziali di Aurora (MySQL) autenticazione in un AWS Secrets Manager luogo segreto e, se si utilizza l'API, ha annotato l'ARN del segreto.

> **Note**
>
> Ti consigliamo di aggiornare o ruotare regolarmente le credenziali e il segreto. Fornisci solo il livello di accesso necessario per la tua sicurezza. Non è consigliabile riutilizzare credenziali e segreti tra diverse fonti di dati e versioni dei connettori 1.0 e 2.0 (ove applicabile).

Se non disponi di un IAM ruolo o di un segreto esistente, puoi utilizzare la console per creare un nuovo IAM ruolo e un Secrets Manager segreto quando connetti la tua origine Aurora (MySQL) dati a. Amazon Kendra Se utilizzi l'API, devi fornire l'ARN di un IAM ruolo e di un Secrets Manager segreto esistenti e un ID di indice.

Istruzioni di connessione

Per connetterti Amazon Kendra alla tua fonte di Aurora (MySQL) dati devi fornire i dettagli delle tue Aurora (MySQL) credenziali in modo da Amazon Kendra poter accedere ai tuoi dati. Se non lo hai ancora configuratoAurora (MySQL), Amazon Kendra vediPrerequisiti.

Console

Per connettersi Amazon Kendra a Aurora (MySQL)

1. Accedi a AWS Management Console e apri la Amazon Kendra console.
2. Dal riquadro di navigazione a sinistra, scegli Indici, quindi scegli l'indice che desideri utilizzare dall'elenco degli indici.

   > **Note**
   >
   > Puoi scegliere di configurare o modificare le impostazioni del controllo dell'accesso degli utenti in Impostazioni dell'indice.

3. Nella pagina Guida introduttiva, scegli Aggiungi origine dati.
4. Nella pagina Aggiungi origine dati, scegli Aurora (MySQL)connettore, quindi scegli Aggiungi connettore.
5. Nella pagina Specificare i dettagli dell'origine dati, inserisci le seguenti informazioni:
   a. In Nome e descrizione, per Nome dell'origine dati, inserisci un nome per l'origine dati. Puoi includere trattini ma non spazi.
   b. (Facoltativo) Descrizione: immetti una descrizione facoltativa per la tua fonte di dati.
   c. In Lingua predefinita: scegli una lingua per filtrare i documenti per l'indice. Se non diversamente specificato, la lingua predefinita è l'inglese. La lingua specificata nei metadati del documento ha la precedenza sulla lingua selezionata.
   d. In Tag, per Aggiungi nuovo tag, includi tag opzionali per cercare e filtrare le risorse o tenere traccia dei costi. AWS
   e. Seleziona Successivo.
6. Nella pagina Definisci accesso e sicurezza, inserisci le seguenti informazioni:
   a. In Source, inserisci le seguenti informazioni:
   b. Host: inserisci l'URL dell'host del database, per esempio:`http://`*`instance URL`*`.`*`region`*`.rds.amazonaws.com`.
   c. Porta: inserisci la porta del database, ad esempio,`5432`.
   d. Istanza: immettere l'istanza del database.
   e. In Autenticazione, inserisci le seguenti informazioni:

- AWS Secrets Manager segreto: scegli un segreto esistente o creane uno nuovo Secrets Manager per memorizzare le credenziali di Aurora (MySQL) autenticazione. Se scegli di creare un nuovo segreto, si apre una finestra AWS Secrets Manager segreta.

  A. Inserisci le seguenti informazioni nella finestra Crea un AWS Secrets Manager segreto:

     I. Nome segreto: un nome per il tuo segreto. Il prefisso 'AmazonKendra-Aurora (MySQL) -' viene aggiunto automaticamente al nome segreto.

     II. Per nome utente e password del database, immettete i valori delle credenziali di autenticazione copiati dal database.

  B. Selezionare Salva.

f. Virtual Private Cloud (VPC): puoi scegliere di utilizzare un VPC. In tal caso, è necessario aggiungere sottoreti e gruppi di sicurezza VPC.

g. IAM ruolo: scegli un IAM ruolo esistente o creane uno nuovo IAM per accedere alle credenziali del repository e indicizzare il contenuto.

> **Note**
>
> IAM i ruoli utilizzati per gli indici non possono essere utilizzati per le fonti di dati. Se non sei sicuro che un ruolo esistente venga utilizzato per un indice o una FAQ, scegli Crea un nuovo ruolo per evitare errori.

h. Seleziona Successivo.

7. Nella pagina Configura le impostazioni di sincronizzazione, inserisci le seguenti informazioni:

   a. Nell'ambito della sincronizzazione, scegli tra le seguenti opzioni:

   - Query SQL: immetti istruzioni di query SQL come le operazioni SELECT e JOIN. Le query SQL devono pesare meno di 32 KB Le query SQL devono pesare meno di 32 KB e non contenere punto e virgola (;). Amazon Kendra eseguirà la scansione di tutto il contenuto del database che corrisponde alla tua query.
   - Colonna chiave primaria: fornisce la chiave primaria per la tabella del database. Identifica una tabella all'interno del database.

- Colonna del titolo: fornisce il nome della colonna del titolo del documento all'interno della tabella del database.
- Colonna del corpo: fornisce il nome della colonna del corpo del documento all'interno della tabella del database.

b. In Configurazione aggiuntiva, facoltativa, scegli una delle seguenti opzioni per sincronizzare contenuti specifici anziché sincronizzare tutti i file:

- Colonne di rilevamento delle modifiche: immetti i nomi delle colonne che Amazon Kendra verranno utilizzate per rilevare le modifiche al contenuto. Amazon Kendra reindicizzerà il contenuto in caso di modifica in una di queste colonne.
- Colonna ID utenti: immetti il nome della colonna che contiene gli ID utente a cui consentire l'accesso ai contenuti.
- Colonna Gruppi: immetti il nome della colonna che contiene i gruppi a cui consentire l'accesso ai contenuti.
- Colonna URL di origine: inserisci il nome della colonna che contiene gli URL di origine da indicizzare.
- Colonna timestamp: immetti il nome della colonna che contiene i timestamp. Amazon Kendra utilizza le informazioni relative alla marca temporale per rilevare le modifiche ai contenuti e sincronizzare solo i contenuti modificati.
- Colonna dei fusi orari: inserisci il nome della colonna che contiene i fusi orari per il contenuto da sottoporre a scansione.
- Formato timestamp: immetti il nome della colonna che contiene i formati di timestamp da utilizzare per rilevare le modifiche ai contenuti e risincronizzare i contenuti.

c. Modalità di sincronizzazione: scegli come aggiornare l'indice quando il contenuto della fonte dati cambia. Quando sincronizzi l'origine dati con Amazon Kendra per la prima volta, tutto il contenuto viene sottoposto a scansione e indicizzato per impostazione predefinita. Se la sincronizzazione iniziale non è riuscita, devi eseguire una sincronizzazione completa dei dati, anche se non scegli la sincronizzazione completa come opzione della modalità di sincronizzazione.

- Sincronizzazione completa: indicizza di nuovo tutti i contenuti, sostituendo i contenuti esistenti ogni volta che l'origine dati si sincronizza con l'indice.
- Nuova sincronizzazione modificata: indicizza solo i contenuti nuovi e modificati ogni volta che l'origine dati si sincronizza con l'indice. Amazon Kendra può utilizzare

il meccanismo dell'origine dati per tenere traccia delle modifiche ai contenuti e indicizzare i contenuti modificati dall'ultima sincronizzazione.

- Sincronizzazione nuova, modificata ed eliminata: indicizza solo i contenuti nuovi, modificati ed eliminati ogni volta che l'origine dati si sincronizza con l'indice. Amazon Kendra può utilizzare il meccanismo dell'origine dati per tenere traccia delle modifiche ai contenuti e indicizzare i contenuti modificati dall'ultima sincronizzazione.

d. Pianificazione di esecuzione di In Sync, per Frequenza: con quale frequenza Amazon Kendra verrà eseguita la sincronizzazione con la fonte di dati.

e. Seleziona Successivo.

8. Nella pagina Imposta mappature dei campi, inserisci le seguenti informazioni:

a. Seleziona uno dei campi di origine dati predefiniti generati (ID documento, titoli dei documenti e URL di origine) che desideri mappare per indicizzare. Amazon Kendra

b. Aggiungi campo: consente di aggiungere campi di origine dati personalizzati per creare un nome di campo indice a cui mappare e il tipo di dati del campo.

c. Seleziona Successivo.

9. Nella pagina Rivedi e crea, verifica che le informazioni inserite siano corrette, quindi seleziona Aggiungi origine dati. Puoi anche scegliere di modificare le tue informazioni da questa pagina. L'origine dati verrà visualizzata nella pagina Origini dati dopo che l'origine dati sarà stata aggiunta correttamente.

API

Per connettersi Amazon Kendra a Aurora (MySQL)

È necessario specificare quanto segue utilizzando l'TemplateConfigurationAPI:

- Origine dati: specifica il tipo di origine dati come `JDBC` quando usi lo schema TemplateConfigurationJSON. Specificate anche l'origine dati come `TEMPLATE` quando chiamate l'CreateDataSourceAPI.
- Tipo di database: è necessario specificare il tipo di database come`mySql`.
- Query SQL: specifica le istruzioni di query SQL come le operazioni SELECT e JOIN. Le query SQL devono pesare meno di 32 KB. Amazon Kendra eseguirà la scansione di tutto il contenuto del database che corrisponde alla tua query.
- Modalità di sincronizzazione: specifica come Amazon Kendra aggiornare l'indice quando il contenuto dell'origine dati cambia. Quando sincronizzi l'origine dati con Amazon Kendra per

la prima volta, tutto il contenuto viene sottoposto a scansione e indicizzato per impostazione predefinita. Se la sincronizzazione iniziale non è riuscita, devi eseguire una sincronizzazione completa dei dati, anche se non scegli la sincronizzazione completa come opzione della modalità di sincronizzazione. Puoi scegliere tra:

- `FORCED_FULL_CRAWL`per indicizzare nuovamente tutti i contenuti, sostituendo i contenuti esistenti ogni volta che l'origine dati si sincronizza con l'indice.
- `FULL_CRAWL`per indicizzare solo i contenuti nuovi, modificati ed eliminati ogni volta che l'origine dati si sincronizza con l'indice. Amazon Kendra può utilizzare il meccanismo dell'origine dati per tenere traccia delle modifiche ai contenuti e indicizzare i contenuti modificati dall'ultima sincronizzazione.
- `CHANGE_LOG`per indicizzare solo contenuti nuovi e modificati ogni volta che l'origine dati si sincronizza con l'indice. Amazon Kendra può utilizzare il meccanismo dell'origine dati per tenere traccia delle modifiche ai contenuti e indicizzare i contenuti modificati dall'ultima sincronizzazione.

- Amazon Resource Name (ARN) segreto: fornisci l'Amazon Resource Name (ARN) di un Secrets Manager segreto che contiene le credenziali di autenticazione che hai creato nel tuo account. Aurora (MySQL) Il segreto è archiviato in una struttura JSON con le seguenti chiavi:

```
{
    "user name": "database user name",
    "password": "password"
}
```

> **Note**
>
> Ti consigliamo di aggiornare o ruotare regolarmente le credenziali e il segreto. Fornisci solo il livello di accesso necessario per la tua sicurezza. Non è consigliabile riutilizzare credenziali e segreti tra diverse fonti di dati e versioni dei connettori 1.0 e 2.0 (ove applicabile).

- IAM ruolo: specifica `RoleArn` quando chiami `CreateDataSource` per fornire a un IAM ruolo le autorizzazioni per accedere al tuo Secrets Manager segreto e per chiamare le API pubbliche richieste per il connettore e. Aurora (MySQL) Amazon Kendra Per ulteriori informazioni, consulta i IAM ruoli per Aurora (MySQL) le fonti di dati.

Puoi anche aggiungere le seguenti funzionalità opzionali:

- Virtual Private Cloud (VPC): `VpcConfiguration` specifica quando si chiama. `CreateDataSource` Per ulteriori informazioni, consulta Configurazione Amazon Kendra per l'utilizzo di un Amazon VPC.
- Filtri di inclusione ed esclusione: puoi specificare se includere contenuti specifici utilizzando ID utente, gruppi, URL di origine, timestamp e fusi orari.
- Filtraggio del contesto utente e controllo degli accessi:Amazon Kendra esegue la ricerca per indicizzazione dell'elenco di controllo degli accessi (ACL) dei documenti, se disponi di un ACL per i documenti. Le informazioni ACL vengono utilizzate per filtrare i risultati della ricerca in base all'accesso dell'utente o del relativo gruppo ai documenti. Per ulteriori informazioni, consulta Filtraggio del contesto utente.
- Mappature dei campi: scegli di mappare i campi delle sorgenti Aurora (MySQL) dati ai campi indice. Amazon Kendra Per ulteriori informazioni, consulta la sezione Mappatura dei campi di origine dei dati.

> **Note**
>
> Il campo del corpo del documento o l'equivalente del corpo del documento per i documenti è necessario per Amazon Kendra eseguire la ricerca nei documenti. È necessario mappare il nome del campo del corpo del documento nella fonte dati al nome del campo indice`_document_body`. Tutti gli altri campi sono facoltativi.

Per un elenco di altre importanti chiavi JSON da configurare, consultaAurora Schema del modello (MySQL).

Note

- Le righe del database eliminate non verranno registrate durante la Amazon Kendra verifica della presenza di contenuti aggiornati.
- La dimensione dei nomi e dei valori dei campi in una riga del database non può superare i 400 KB.
- Se l'origine dati del database contiene una grande quantità di dati e non desideri Amazon Kendra indicizzare tutto il contenuto del database dopo la prima sincronizzazione, puoi scegliere di sincronizzare solo i documenti nuovi, modificati o eliminati.
- È consigliabile fornire credenziali Amazon Kendra di database di sola lettura.

- È consigliabile evitare di aggiungere tabelle con dati sensibili o informazioni personali identificabili (PII).

Aurora (PostgreSQL)

Aurora è un sistema di gestione di database relazionali (RDBMS) creato per il cloud. Se sei un Aurora utente, puoi utilizzarlo Amazon Kendra per indicizzare la tua Aurora (PostgreSQL) fonte di dati. Il connettore di origine Amazon Kendra Aurora (PostgreSQL) dati supporta Aurora PostgreSQL 1.

Puoi connetterti Amazon Kendra alla tua fonte di Aurora (PostgreSQL) dati utilizzando la Amazon Kendra console e l'API. TemplateConfiguration

Per la risoluzione dei problemi relativi al connettore della sorgente Amazon Kendra Aurora (PostgreSQL) dati, consultaRisoluzione dei problemi relativi alle origini dati.

Argomenti

- Funzionalità supportate
- Prerequisiti
- Istruzioni di connessione
- Note

Funzionalità supportate

- Mappature dei campi
- Filtraggio del contesto utente
- Filtri di inclusione/esclusione
- Sincronizzazione completa e incrementale dei contenuti
- Virtual Private Cloud (VPC) (Cloud privato virtuale (VPC)

Prerequisiti

Prima di poterla utilizzare Amazon Kendra per indicizzare la tua fonte di Aurora (PostgreSQL) dati, apporta queste modifiche al tuo account Aurora (PostgreSQL) e AWS ai tuoi account.

NelAurora (PostgreSQL), assicurati di avere:

- Hai annotato il nome utente e la password del database.

> **Important**
>
> È consigliabile fornire credenziali Amazon Kendra di database di sola lettura.

- Hai copiato l'URL, la porta e l'istanza dell'host del database.
- È stato verificato che ogni documento sia unico all'interno Aurora (PostgreSQL) e tra le altre fonti di dati che intendi utilizzare per lo stesso indice. Ogni fonte di dati che desideri utilizzare per un indice non deve contenere lo stesso documento in tutte le fonti di dati. Gli ID dei documenti sono globali rispetto a un indice e devono essere univoci per indice.

Nel tuo Account AWS, assicurati di avere:

- Ha creato un Amazon Kendra indice e, se si utilizza l'API, ha annotato l'ID dell'indice.
- Hai creato un IAM ruolo per la tua origine dati e, se utilizzi l'API, hai annotato l'ARN del IAM ruolo.

> **Note**
>
> Se modifichi il tipo di autenticazione e le credenziali, devi aggiornare il IAM ruolo per accedere all'ID AWS Secrets Manager segreto corretto.

- Ha archiviato le credenziali di Aurora (PostgreSQL) autenticazione in un AWS Secrets Manager segreto e, se si utilizza l'API, ha annotato l'ARN del segreto.

> **Note**
>
> Ti consigliamo di aggiornare o ruotare regolarmente le credenziali e il segreto. Fornisci solo il livello di accesso necessario per la tua sicurezza. Non è consigliabile riutilizzare credenziali e segreti tra diverse fonti di dati e versioni dei connettori 1.0 e 2.0 (ove applicabile).

Se non disponi di un IAM ruolo o di un segreto esistente, puoi utilizzare la console per creare un nuovo IAM ruolo e un Secrets Manager segreto quando connetti la tua origine Aurora (PostgreSQL) dati a. Amazon Kendra Se utilizzi l'API, devi fornire l'ARN di un IAM ruolo e di un Secrets Manager segreto esistenti e un ID di indice.

Istruzioni di connessione

Per connetterti Amazon Kendra alla tua fonte di Aurora (PostgreSQL) dati devi fornire i dettagli delle tue Aurora (PostgreSQL) credenziali in modo da Amazon Kendra poter accedere ai tuoi dati. Se non lo hai ancora configurato, Aurora (PostgreSQL) Amazon Kendra Prerequisiti consulta.

Console

Per connettersi Amazon Kendra a Aurora (PostgreSQL)

1. Accedi a AWS Management Console e apri la Amazon Kendra console.
2. Dal riquadro di navigazione a sinistra, scegli Indici, quindi scegli l'indice che desideri utilizzare dall'elenco degli indici.

> **Note**
>
> Puoi scegliere di configurare o modificare le impostazioni del controllo dell'accesso degli utenti in Impostazioni dell'indice.

3. Nella pagina Guida introduttiva, scegli Aggiungi origine dati.
4. Nella pagina Aggiungi origine dati, scegli Aurora (PostgreSQL)connettore, quindi scegli Aggiungi connettore.
5. Nella pagina Specificare i dettagli dell'origine dati, inserisci le seguenti informazioni:
   a. In Nome e descrizione, per Nome dell'origine dati, inserisci un nome per l'origine dati. Puoi includere trattini ma non spazi.
   b. (Facoltativo) Descrizione: immetti una descrizione facoltativa per l'origine dati.
   c. In Lingua predefinita: scegli una lingua per filtrare i documenti per l'indice. Se non diversamente specificato, la lingua predefinita è l'inglese. La lingua specificata nei metadati del documento ha la precedenza sulla lingua selezionata.
   d. In Tag, per Aggiungi nuovo tag, includi tag opzionali per cercare e filtrare le risorse o tenere traccia dei costi. AWS
   e. Seleziona Successivo.
6. Nella pagina Definisci accesso e sicurezza, inserisci le seguenti informazioni:
   a. In Source, inserisci le seguenti informazioni:

b. Host: inserisci l'URL dell'host del database, per esempio:`http://instance URL.region.rds.amazonaws.com`.

c. Porta: inserisci la porta del database, ad esempio,`5432`.

d. Istanza: immettere, ad esempio, l'istanza del database`postgres`.

e. Abilita la posizione del certificato SSL: scegli di inserire il Amazon S3 percorso del file del certificato SSL.

f. In Autenticazione, inserisci le seguenti informazioni:

- AWS Secrets Manager segreto: scegli un segreto esistente o creane uno nuovo Secrets Manager per memorizzare le credenziali di Aurora (PostgreSQL) autenticazione. Se scegli di creare un nuovo segreto, si apre una finestra AWS Secrets Manager segreta.

  A. Inserisci le seguenti informazioni nella finestra Crea un AWS Secrets Manager segreto:

     I. Nome segreto: un nome per il tuo segreto. Il prefisso 'AmazonKendra-Aurora (PostgreSQL) -' viene aggiunto automaticamente al nome segreto.

     II. Per nome utente e password del database, immettete i valori delle credenziali di autenticazione copiati dal database.

  B. Selezionare Salva.

g. Virtual Private Cloud (VPC): puoi scegliere di utilizzare un VPC. In tal caso, è necessario aggiungere sottoreti e gruppi di sicurezza VPC.

h. IAM ruolo: scegli un IAM ruolo esistente o creane uno nuovo IAM per accedere alle credenziali del repository e indicizzare il contenuto.

> **Note**
>
> IAM i ruoli utilizzati per gli indici non possono essere utilizzati per le fonti di dati. Se non sei sicuro che un ruolo esistente venga utilizzato per un indice o una FAQ, scegli Crea un nuovo ruolo per evitare errori.

i. Seleziona Successivo.

7. Nella pagina Configura le impostazioni di sincronizzazione, inserisci le seguenti informazioni:

a. Nell'ambito della sincronizzazione, scegli tra le seguenti opzioni:

- Query SQL: immetti istruzioni di query SQL come le operazioni SELECT e JOIN. Le query SQL devono pesare meno di 32 KB Le query SQL devono pesare meno di 32 KB e non contenere punto e virgola (;). Amazon Kendra eseguirà la scansione di tutto il contenuto del database che corrisponde alla tua query.
- Colonna chiave primaria: fornisce la chiave primaria per la tabella del database. Identifica una tabella all'interno del database.
- Colonna del titolo: fornisce il nome della colonna del titolo del documento all'interno della tabella del database.
- Colonna del corpo: fornisce il nome della colonna del corpo del documento all'interno della tabella del database.

b. In Configurazione aggiuntiva, facoltativa, scegli una delle seguenti opzioni per sincronizzare contenuti specifici anziché sincronizzare tutti i file:

- Colonne di rilevamento delle modifiche: immetti i nomi delle colonne che Amazon Kendra verranno utilizzate per rilevare le modifiche al contenuto. Amazon Kendra reindicizzerà il contenuto quando viene apportata una modifica in una di queste colonne.
- Colonna ID utenti: immetti il nome della colonna che contiene gli ID utente a cui consentire l'accesso ai contenuti.
- Colonna Gruppi: immetti il nome della colonna che contiene i gruppi a cui consentire l'accesso ai contenuti.
- Colonna URL di origine: inserisci il nome della colonna che contiene gli URL di origine da indicizzare.
- Colonna timestamp: immetti il nome della colonna che contiene i timestamp. Amazon Kendra utilizza le informazioni relative alla marca temporale per rilevare le modifiche ai contenuti e sincronizzare solo i contenuti modificati.
- Colonna dei fusi orari: inserisci il nome della colonna che contiene i fusi orari per il contenuto da sottoporre a scansione.
- Formato timestamp: immetti il nome della colonna che contiene i formati di timestamp da utilizzare per rilevare le modifiche ai contenuti e risincronizzare i contenuti.

c. Modalità di sincronizzazione: scegli come aggiornare l'indice quando il contenuto della fonte dati cambia. Quando sincronizzi l'origine dati con Amazon Kendra per la prima volta, tutto il contenuto viene sottoposto a scansione e indicizzato per impostazione predefinita. Se la sincronizzazione iniziale non è riuscita, devi eseguire una

sincronizzazione completa dei dati, anche se non scegli la sincronizzazione completa come opzione della modalità di sincronizzazione.

- Sincronizzazione completa: indicizza di nuovo tutti i contenuti, sostituendo i contenuti esistenti ogni volta che l'origine dati si sincronizza con l'indice.
- Nuova sincronizzazione modificata: indicizza solo i contenuti nuovi e modificati ogni volta che l'origine dati si sincronizza con l'indice. Amazon Kendra può utilizzare il meccanismo dell'origine dati per tenere traccia delle modifiche ai contenuti e indicizzare i contenuti modificati dall'ultima sincronizzazione.
- Sincronizzazione nuova, modificata ed eliminata: indicizza solo i contenuti nuovi, modificati ed eliminati ogni volta che l'origine dati si sincronizza con l'indice. Amazon Kendra può utilizzare il meccanismo dell'origine dati per tenere traccia delle modifiche ai contenuti e indicizzare i contenuti modificati dall'ultima sincronizzazione.

d. Pianificazione di esecuzione di In Sync, per Frequenza: con quale frequenza Amazon Kendra verrà eseguita la sincronizzazione con la fonte di dati.

e. Seleziona Successivo.

8. Nella pagina Imposta le mappature dei campi, inserisci le seguenti informazioni:

a. Seleziona uno dei campi di origine dati predefiniti generati (ID documento, titoli dei documenti e URL di origine) che desideri mappare per indicizzare. Amazon Kendra

b. Aggiungi campo: consente di aggiungere campi di origine dati personalizzati per creare un nome di campo indice a cui mappare e il tipo di dati del campo.

c. Seleziona Successivo.

9. Nella pagina Rivedi e crea, verifica che le informazioni inserite siano corrette, quindi seleziona Aggiungi origine dati. Puoi anche scegliere di modificare le tue informazioni da questa pagina. L'origine dati verrà visualizzata nella pagina Origini dati dopo che l'origine dati sarà stata aggiunta correttamente.

API

Per connettersi Amazon Kendra a Aurora (PostgreSQL)

È necessario specificare quanto segue utilizzando l'TemplateConfigurationAPI:

- Origine dati: specifica il tipo di origine dati come `JDBC` quando usi lo schema TemplateConfigurationJSON. Specificate anche l'origine dati come `TEMPLATE` quando chiamate l'CreateDataSourceAPI.
- Tipo di database: è necessario specificare il tipo di database come`postgresql`.
- Query SQL: specifica le istruzioni di query SQL come le operazioni SELECT e JOIN. Le query SQL devono pesare meno di 32 KB. Amazon Kendra eseguirà la scansione di tutto il contenuto del database che corrisponde alla tua query.
- Modalità di sincronizzazione: specifica come Amazon Kendra aggiornare l'indice quando il contenuto dell'origine dati cambia. Quando sincronizzi l'origine dati con Amazon Kendra per la prima volta, tutto il contenuto viene sottoposto a scansione e indicizzato per impostazione predefinita. Se la sincronizzazione iniziale non è riuscita, devi eseguire una sincronizzazione completa dei dati, anche se non scegli la sincronizzazione completa come opzione della modalità di sincronizzazione. Puoi scegliere tra:
  - `FORCED_FULL_CRAWL`per indicizzare nuovamente tutti i contenuti, sostituendo i contenuti esistenti ogni volta che l'origine dati si sincronizza con l'indice.
  - `FULL_CRAWL`per indicizzare solo i contenuti nuovi, modificati ed eliminati ogni volta che l'origine dati si sincronizza con l'indice. Amazon Kendra può utilizzare il meccanismo dell'origine dati per tenere traccia delle modifiche ai contenuti e indicizzare i contenuti modificati dall'ultima sincronizzazione.
  - `CHANGE_LOG`per indicizzare solo contenuti nuovi e modificati ogni volta che l'origine dati si sincronizza con l'indice. Amazon Kendra può utilizzare il meccanismo dell'origine dati per tenere traccia delle modifiche ai contenuti e indicizzare i contenuti modificati dall'ultima sincronizzazione.
- Amazon Resource Name (ARN) segreto: fornisci l'Amazon Resource Name (ARN) di un Secrets Manager segreto che contiene le credenziali di autenticazione che hai creato nel tuo account. Aurora (PostgreSQL) Il segreto è archiviato in una struttura JSON con le seguenti chiavi:

```
{
    "user name": "database user name",
    "password": "password"
}
```

> **Note**
>
> Ti consigliamo di aggiornare o ruotare regolarmente le credenziali e il segreto. Fornisci solo il livello di accesso necessario per la tua sicurezza. Non è consigliabile riutilizzare credenziali e segreti tra diverse fonti di dati e versioni dei connettori 1.0 e 2.0 (ove applicabile).

- IAM ruolo: specifica `RoleArn` quando chiami `CreateDataSource` per fornire a un IAM ruolo le autorizzazioni per accedere al tuo Secrets Manager segreto e per chiamare le API pubbliche richieste per il connettore e. Aurora (PostgreSQL) Amazon Kendra Per ulteriori informazioni, consulta i IAM ruoli per Aurora (PostgreSQL) le fonti di dati.

Puoi anche aggiungere le seguenti funzionalità opzionali:

- Virtual Private Cloud (VPC): `VpcConfiguration` specifica quando si chiama. `CreateDataSource` Per ulteriori informazioni, consulta Configurazione Amazon Kendra per l'utilizzo di un Amazon VPC.
- Filtri di inclusione ed esclusione: puoi specificare se includere contenuti specifici utilizzando ID utente, gruppi, URL di origine, timestamp e fusi orari.
- Filtraggio del contesto utente e controllo degli accessi:Amazon Kendra esegue la ricerca per indicizzazione dell'elenco di controllo degli accessi (ACL) dei documenti, se disponi di un ACL per i documenti. Le informazioni ACL vengono utilizzate per filtrare i risultati della ricerca in base all'accesso dell'utente o del relativo gruppo ai documenti. Per ulteriori informazioni, consulta Filtraggio del contesto utente.
- Mappature dei campi: scegli di mappare i campi delle sorgenti Aurora (PostgreSQL) dati ai campi indice. Amazon Kendra Per ulteriori informazioni, consulta la sezione Mappatura dei campi di origine dei dati.

> **Note**
>
> Il campo del corpo del documento o l'equivalente del corpo del documento per i documenti è necessario per Amazon Kendra eseguire la ricerca nei documenti. È necessario mappare il nome del campo del corpo del documento nella fonte dati al nome del campo indice`_document_body`. Tutti gli altri campi sono facoltativi.

Per un elenco di altre importanti chiavi JSON da configurare, consultaAurora Schema del modello (PostgreSQL).

Note

- Le righe del database eliminate non verranno registrate durante la Amazon Kendra verifica della presenza di contenuti aggiornati.
- La dimensione dei nomi e dei valori dei campi in una riga del database non può superare i 400 KB.
- Se l'origine dati del database contiene una grande quantità di dati e non desideri Amazon Kendra indicizzare tutto il contenuto del database dopo la prima sincronizzazione, puoi scegliere di sincronizzare solo i documenti nuovi, modificati o eliminati.
- È consigliabile fornire credenziali Amazon Kendra di database di sola lettura.
- È consigliabile evitare di aggiungere tabelle con dati sensibili o informazioni personali identificabili (PII).

Amazon FSx (Finestre)

Amazon FSx (Windows) è un sistema di file server completamente gestito e basato sul cloud che offre funzionalità di archiviazione condivise. Se sei un utente Amazon FSx (Windows), puoi utilizzarlo Amazon Kendra per indicizzare la tua fonte di dati Amazon FSx (Windows).

> **Note**
>
> Amazon Kendra ora supporta un connettore aggiornato Amazon FSx (Windows). La console è stata aggiornata automaticamente per te. Tutti i nuovi connettori creati sulla console utilizzeranno l'architettura aggiornata. Se utilizzi l'API, ora devi utilizzare l'TemplateConfigurationoggetto anziché l'`FSxConfiguration`oggetto per configurare il connettore.
> I connettori configurati utilizzando la console e l'architettura API precedenti continueranno a funzionare come configurato. Tuttavia, non potrai modificarli o aggiornarli. Se desideri modificare o aggiornare la configurazione del connettore, devi creare un nuovo connettore. Ti consigliamo di migrare il flusso di lavoro del connettore alla versione aggiornata. La fine del supporto per i connettori configurati utilizzando l'architettura precedente è prevista entro giugno 2024.

Puoi connetterti Amazon Kendra alla tua fonte di dati Amazon FSx (Windows) utilizzando la Amazon Kendra console o l'TemplateConfigurationAPI.

Per la risoluzione dei problemi relativi al connettore di origine dati Amazon Kendra Amazon FSx (Windows), consultaRisoluzione dei problemi relativi alle origini dati.

Argomenti

- Funzionalità supportate
- Prerequisiti
- Istruzioni di connessione
- Ulteriori informazioni

Funzionalità supportate

Amazon Kendra Amazon FSx Il connettore di origine dati (Windows) supporta le seguenti funzionalità:

- Mappature dei campi
- Controllo degli accessi degli utenti
- Scansione delle identità degli utenti
- Filtri di inclusione ed esclusione
- Sincronizzazione completa e incrementale dei contenuti
- Virtual Private Cloud (VPC) (Cloud privato virtuale (VPC)

Prerequisiti

Prima di poterla utilizzare Amazon Kendra per indicizzare la tua fonte di dati Amazon FSx (Windows), controlla i dettagli della tua fonte di dati Amazon FSx (Windows) e. Account AWS

Per Amazon FSx (Windows), assicurati di avere:

- Configurazione Amazon FSx (Windows) con autorizzazioni di lettura e montaggio.
- Ha annotato l'ID del file system. È possibile trovare l'ID del file system nella dashboard dei file system della console Amazon FSx (Windows).
- Hai configurato un cloud privato virtuale utilizzando il Amazon VPC luogo in cui risiede il tuo file system Amazon FSx (Windows).

- Ha annotato le credenziali di autenticazione Amazon FSx (Windows) per un account Active Directory utente. Ciò include il nome utente di Active Directory con il nome di dominio DNS (ad esempio, user@corp.example.com) e la password.

> **Note**
>
> Utilizza solo le credenziali necessarie per il funzionamento del connettore. Non utilizzare credenziali privilegiate come l'amministratore di dominio.

- Selezionato, ogni documento è unico in Amazon FSx (Windows) e tra le altre fonti di dati che intendi utilizzare per lo stesso indice. Ogni fonte di dati che desideri utilizzare per un indice non deve contenere lo stesso documento in tutte le fonti di dati. Gli ID dei documenti sono globali rispetto a un indice e devono essere univoci per indice.

Nel tuo Account AWS, assicurati di avere:

- Ha creato un Amazon Kendra indice e, se si utilizza l'API, ha annotato l'ID dell'indice.
- Hai creato un IAM ruolo per la tua origine dati e, se utilizzi l'API, hai annotato l'ARN del IAM ruolo.

> **Note**
>
> Se modifichi il tipo di autenticazione e le credenziali, devi aggiornare il IAM ruolo per accedere all'ID AWS Secrets Manager segreto corretto.

- Ha archiviato le credenziali di autenticazione Amazon FSx (Windows) in un AWS Secrets Manager segreto e, se si utilizza l'API, ha annotato l'ARN del segreto.

> **Note**
>
> Ti consigliamo di aggiornare o ruotare regolarmente le credenziali e il segreto. Fornisci solo il livello di accesso necessario per la tua sicurezza. Non è consigliabile riutilizzare credenziali e segreti tra diverse fonti di dati e versioni dei connettori 1.0 e 2.0 (ove applicabile).

Se non disponi di un IAM ruolo o di un segreto esistente, puoi utilizzare la console per creare un nuovo IAM ruolo e un Secrets Manager segreto quando connetti la tua origine dati Amazon FSx

(Windows) a. Amazon Kendra Se utilizzi l'API, devi fornire l'ARN di un IAM ruolo e di un Secrets Manager segreto esistenti e un ID di indice.

Istruzioni di connessione

Per connettersi Amazon Kendra all'origine dati Amazon FSx (Windows), è necessario fornire i dettagli necessari dell'origine dati Amazon FSx (Windows) in modo che sia Amazon Kendra possibile accedere ai dati. Se non hai ancora configurato Amazon FSx (Windows) per Amazon Kendra, vediPrerequisiti.

Console

Per connettersi Amazon Kendra al file system Amazon FSx (Windows)

1. Accedi a AWS Management Console e apri la Amazon Kendra console.
2. Dal riquadro di navigazione a sinistra, scegli Indici, quindi scegli l'indice che desideri utilizzare dall'elenco degli indici.

   > **Note**
   >
   > Puoi scegliere di configurare o modificare le impostazioni del controllo dell'accesso degli utenti in Impostazioni dell'indice.

3. Nella pagina Guida introduttiva, scegli Aggiungi origine dati.
4. Nella pagina Aggiungi origine dati, scegli Connettore Amazon FSx (Windows), quindi scegli Aggiungi connettore.
5. Nella pagina Specificare i dettagli dell'origine dati, inserisci le seguenti informazioni:

   a. In Nome e descrizione, per Nome dell'origine dati, inserisci un nome per l'origine dati. Puoi includere trattini ma non spazi.
   b. (Facoltativo) Descrizione: immetti una descrizione facoltativa per la tua fonte di dati.
   c. In Lingua predefinita: scegli una lingua per filtrare i documenti per l'indice. Se non diversamente specificato, la lingua predefinita è l'inglese. La lingua specificata nei metadati del documento ha la precedenza sulla lingua selezionata.
   d. In Tag, per Aggiungi nuovo tag, includi tag opzionali per cercare e filtrare le risorse o tenere traccia dei costi. AWS
   e. Seleziona Successivo.

6. Nella pagina Definisci accesso e sicurezza, inserisci le seguenti informazioni:

a. Amazon FSx (Windows) ID del file system: seleziona dal menu a discesa l'ID del file system esistente, recuperato da Amazon FSx (Windows). In alternativa, crea un file system Amazon FSx (Windows). Puoi trovare l'ID del tuo file system nella dashboard dei file system della console Amazon FSx (Windows).

b. Autorizzazione: attiva o disattiva le informazioni dell'elenco di controllo degli accessi (ACL) per i documenti, se disponi di un ACL e desideri utilizzarlo per il controllo degli accessi. L'ACL specifica a quali documenti possono accedere utenti e gruppi. Le informazioni ACL vengono utilizzate per filtrare i risultati della ricerca in base all'accesso dell'utente o del relativo gruppo ai documenti. Per ulteriori informazioni, consulta Filtraggio del contesto utente.

c. Autenticazione: scegli un AWS Secrets Manager segreto esistente o crea un nuovo segreto per archiviare le credenziali del file system. Se scegli di creare un nuovo segreto, si apre una finestra AWS Secrets Manager segreta.

   Fornisci un segreto che memorizzi le credenziali di autenticazione del nome utente e della password. Il nome utente deve includere il nome di dominio DNS. Ad esempio, user@corp.example.com.

   Salva e aggiungi il tuo segreto.

d. Virtual Private Cloud (VPC): è necessario selezionare un Amazon VPC luogo in cui risiede (Windows). Amazon FSx Includi la sottorete VPC e i gruppi di sicurezza. Vedi Configurazione di un. Amazon VPC

e. IAM ruolo: scegli un ruolo esistente o crea un nuovo IAM IAM ruolo per accedere alle credenziali del repository e indicizzare il contenuto.

   > **Note**
   >
   > IAM i ruoli utilizzati per gli indici non possono essere utilizzati per le fonti di dati. Se non sei sicuro che un ruolo esistente venga utilizzato per un indice o una FAQ, scegli Crea un nuovo ruolo per evitare errori.

f. Seleziona Successivo.

7. Nella pagina Configura le impostazioni di sincronizzazione, inserisci le seguenti informazioni:

   a. Ambito di sincronizzazione, modelli Regex: aggiungi modelli di espressioni regolari per includere o escludere determinati file.

b. Modalità di sincronizzazione: scegli come aggiornare l'indice quando il contenuto della fonte di dati cambia. Quando sincronizzi l'origine dati con Amazon Kendra per la prima volta, tutto il contenuto viene sottoposto a scansione e indicizzato per impostazione predefinita. Se la sincronizzazione iniziale non è riuscita, devi eseguire una sincronizzazione completa dei dati, anche se non scegli la sincronizzazione completa come opzione della modalità di sincronizzazione.

   - Sincronizzazione completa: indicizza di nuovo tutti i contenuti, sostituendo i contenuti esistenti ogni volta che l'origine dati si sincronizza con l'indice.
   - Sincronizzazione nuova, modificata ed eliminata: indicizza solo i contenuti nuovi, modificati ed eliminati ogni volta che l'origine dati si sincronizza con l'indice. Amazon Kendra può utilizzare il meccanismo dell'origine dati per tenere traccia delle modifiche ai contenuti e indicizzare i contenuti modificati dall'ultima sincronizzazione.

c. Pianificazione dell'esecuzione della sincronizzazione: per Frequenza, scegli la frequenza con cui sincronizzare il contenuto della fonte di dati e aggiornare l'indice.

d. Seleziona Successivo.

8. Nella pagina Imposta mappature dei campi, inserisci le seguenti informazioni:

   a. Seleziona tra i campi predefiniti Amazon Kendra generati dei tuoi file che desideri mappare al tuo indice. Per aggiungere campi di origine dati personalizzati, crea un nome di campo indice a cui mappare e il tipo di dati del campo.

   b. Seleziona Successivo.

9. Nella pagina Rivedi e crea, verifica che le informazioni inserite siano corrette, quindi seleziona Aggiungi origine dati. Puoi anche scegliere di modificare le tue informazioni da questa pagina. L'origine dati verrà visualizzata nella pagina Origini dati dopo che l'origine dati sarà stata aggiunta correttamente.

API

Per connettersi Amazon Kendra al file system Amazon FSx (Windows)

È necessario specificare un codice JSON dello schema dell'origine dati utilizzando l'TemplateConfigurationAPI. È necessario fornire le seguenti informazioni:

- Origine dati: specifica il tipo di origine dati come `FSX` quando usi lo schema TemplateConfigurationJSON. Specificate anche l'origine dati come `TEMPLATE` quando chiamate l'CreateDataSourceAPI.

- ID del file system: l'identificatore del file system Amazon FSx (Windows). È possibile trovare l'ID del file system nella dashboard dei file system della console Amazon FSx (Windows).
- Tipo di file system: specifica il tipo di file system. `WINDOWS`
- Virtual Private Cloud (VPC): `VpcConfiguration` specifica quando si chiama. `CreateDataSource` Per ulteriori informazioni, consulta Configurazione Amazon Kendra per l'utilizzo di un Amazon VPC.

  > **Note**
  >
  > È necessario selezionare un Amazon VPC luogo in cui risiede Amazon FSx (Windows). Includi la sottorete VPC e i gruppi di sicurezza.

- Modalità di sincronizzazione: specifica come Amazon Kendra aggiornare l'indice quando il contenuto dell'origine dati cambia. Quando sincronizzi l'origine dati con Amazon Kendra per la prima volta, tutto il contenuto viene sottoposto a scansione e indicizzato per impostazione predefinita. Se la sincronizzazione iniziale non è riuscita, devi eseguire una sincronizzazione completa dei dati, anche se non scegli la sincronizzazione completa come opzione della modalità di sincronizzazione. Puoi scegliere tra:
  - `FORCED_FULL_CRAWL`per indicizzare nuovamente tutti i contenuti, sostituendo i contenuti esistenti ogni volta che l'origine dati si sincronizza con l'indice.
  - `FULL_CRAWL`per indicizzare solo i contenuti nuovi, modificati ed eliminati ogni volta che l'origine dati si sincronizza con l'indice. Amazon Kendra può utilizzare il meccanismo dell'origine dati per tenere traccia delle modifiche ai contenuti e indicizzare i contenuti modificati dall'ultima sincronizzazione.
- Identity crawler: specifica se attivare il crawler Amazon Kendra di identità. Il crawler di identità utilizza le informazioni dell'elenco di controllo degli accessi (ACL) per i documenti per filtrare i risultati della ricerca in base all'accesso dell'utente o del gruppo di appartenenza ai documenti. Se disponi di un ACL per i tuoi documenti e scegli di utilizzarlo, puoi anche scegliere di attivare il crawler di identità per configurare il filtraggio Amazon Kendra del contesto utente dei risultati di ricerca. Altrimenti, se il crawler di identità è disattivato, tutti i documenti possono essere ricercati pubblicamente. Se desideri utilizzare il controllo degli accessi per i tuoi documenti e il crawler di identità è disattivato, in alternativa puoi utilizzare l'PutPrincipalMappingAPI per caricare le informazioni di accesso di utenti e gruppi per il filtraggio del contesto degli utenti.
- Secret Amazon Resource Name (ARN): fornisci l'Amazon Resource Name (ARN) di un Secrets Manager segreto che contiene le credenziali di autenticazione per il tuo account (Windows). Amazon FSx Il segreto è archiviato in una struttura JSON con le seguenti chiavi:

```
{
    "username": "user@corp.example.com",
    "password": "password"
}
```

- IAM ruolo: specifica `RoleArn` quando chiami `CreateDataSource` per fornire a un IAM ruolo le autorizzazioni per accedere al tuo Secrets Manager segreto e per chiamare le API pubbliche richieste per il connettore Amazon FSx (Windows) e. Amazon Kendra Per ulteriori informazioni, consulta IAM i ruoli per le origini dati Amazon FSx (Windows).

Puoi anche aggiungere le seguenti funzionalità opzionali:

- Filtri di inclusione ed esclusione: specificano se includere o escludere determinati file.

> **Note**
>
> La maggior parte delle fonti di dati utilizza modelli di espressioni regolari, che sono modelli di inclusione o esclusione denominati filtri. Se si specifica un filtro di inclusione, viene indicizzato solo il contenuto che corrisponde al filtro di inclusione. Qualsiasi documento che non corrisponde al filtro di inclusione non viene indicizzato. Se si specifica un filtro di inclusione ed esclusione, i documenti che corrispondono al filtro di esclusione non vengono indicizzati, anche se corrispondono al filtro di inclusione.

- Elenco di controllo degli accessi (ACL): specifica se eseguire la scansione delle informazioni ACL per i documenti, se disponi di un ACL e desideri utilizzarlo per il controllo degli accessi. L'ACL specifica a quali documenti possono accedere utenti e gruppi. Le informazioni ACL vengono utilizzate per filtrare i risultati della ricerca in base all'accesso dell'utente o del relativo gruppo ai documenti. Per ulteriori informazioni, consulta Filtraggio del contesto utente.

> **Note**
>
> Per testare il filtraggio del contesto utente su un utente, è necessario includere il nome di dominio DNS come parte del nome utente quando si esegue la query. È necessario disporre delle autorizzazioni amministrative del dominio Active Directory. È inoltre possibile testare il filtraggio del contesto utente in base al nome di un gruppo.

- Mappature dei campi: scegli di mappare i campi dell'origine dati Amazon FSx (Windows) ai campi indice. Amazon Kendra Per ulteriori informazioni, consulta la sezione Mappatura dei campi di origine dei dati.

  > **Note**
  >
  > Il campo del corpo del documento o l'equivalente del corpo del documento per i documenti è necessario per Amazon Kendra eseguire la ricerca nei documenti. È necessario mappare il nome del campo del corpo del documento nella fonte dati al nome del campo indice_`document_body`. Tutti gli altri campi sono facoltativi.

Per un elenco di altre importanti chiavi JSON da configurare, consulta lo schema del modello Amazon FSx (Windows).

Ulteriori informazioni

Per ulteriori informazioni sull'integrazione Amazon Kendra con la tua fonte di dati Amazon FSx (Windows), consulta:

- Cerca in modo sicuro dati non strutturati nei file system Windows con il Amazon Kendra connettore per Amazon FSx (Windows) per. Windows File Server

Amazon FSx (NetApp SU TAP)

Amazon FSx (NetApp ONTAP) è un sistema di file server completamente gestito e basato sul cloud che offre funzionalità di archiviazione condivise. Se sei un utente Amazon FSx (NetApp ONTAP), puoi utilizzarlo Amazon Kendra per indicizzare la tua fonte di dati Amazon FSx (NetApp ONTAP).

Puoi connetterti Amazon Kendra alla tua fonte di dati Amazon FSx (NetApp ONTAP) utilizzando la Amazon Kendra console o l'API. TemplateConfiguration

Per la risoluzione dei problemi relativi al connettore di origine dati Amazon Kendra Amazon FSx (NetApp ONTAP), consulta. Risoluzione dei problemi relativi alle origini dati

Argomenti

- Funzionalità supportate
- Prerequisiti

- Istruzioni di connessione

Funzionalità supportate

Amazon Kendra Amazon FSx Il connettore di origine dati (NetApp ONTAP) supporta le seguenti funzionalità:

- Mappature dei campi
- Controllo degli accessi degli utenti
- Filtri di inclusione ed esclusione
- Sincronizzazione completa e incrementale dei contenuti
- Virtual Private Cloud (VPC) (Cloud privato virtuale (VPC)

Prerequisiti

Prima di poterla utilizzare Amazon Kendra per indicizzare la tua fonte di dati Amazon FSx (NetApp ONTAP), controlla i dettagli della tua fonte di dati Amazon FSx (NetApp ONTAP) e. Account AWS

Per Amazon FSx (NetApp ONTAP), assicurati di avere:

- Configurazione Amazon FSx (NetApp ONTAP) con autorizzazioni di lettura e montaggio.
- Ha annotato l'ID del file system. Puoi trovare l'ID del tuo file system nella dashboard dei file system della console Amazon FSx (NetApp ONTAP).
- Ha annotato l'ID della macchina virtuale di archiviazione (SVM) utilizzato con il file system. È possibile trovare l'ID SVM accedendo alla dashboard File Systems nella console Amazon FSx (NetApp ONTAP), selezionando l'ID del file system e quindi selezionando Storage virtual machines.
- Hai configurato un cloud privato virtuale utilizzando il Amazon VPC luogo in cui risiede il tuo file system Amazon FSx (NetApp ONTAP).
- Hai annotato le tue credenziali di autenticazione Amazon FSx (NetApp ONTAP) per un account utente. Active Directory Ciò include il nome utente di Active Directory con il nome di dominio DNS (ad esempio, user@corp.example.com) e la password. Se utilizzi il protocollo Network File System (NFS) per il tuo file system Amazon FSx (NetApp ONTAP), le credenziali di autenticazione includono un ID sinistro, un ID destro e una chiave precondivisa.

> **Note**
>
> Utilizzate solo le credenziali necessarie per il funzionamento del connettore. Non utilizzare credenziali privilegiate come l'amministratore di dominio.

- È stato selezionato che ogni documento sia unico in Amazon FSx (NetApp ONTAP) e tra le altre fonti di dati che intendi utilizzare per lo stesso indice. Ogni fonte di dati che desideri utilizzare per un indice non deve contenere lo stesso documento in tutte le fonti di dati. Gli ID dei documenti sono globali rispetto a un indice e devono essere univoci per indice.

Nel tuo Account AWS, assicurati di avere:

- Ha creato un Amazon Kendra indice e, se si utilizza l'API, ha annotato l'ID dell'indice.
- Hai creato un IAM ruolo per la tua origine dati e, se utilizzi l'API, hai annotato l'ARN del IAM ruolo.

> **Note**
>
> Se modifichi il tipo di autenticazione e le credenziali, devi aggiornare il IAM ruolo per accedere all'ID AWS Secrets Manager segreto corretto.

- Ha archiviato le credenziali di autenticazione Amazon FSx (NetApp ONTAP) in un AWS Secrets Manager segreto e, se si utilizza l'API, ha annotato l'ARN del segreto.

> **Note**
>
> Ti consigliamo di aggiornare o ruotare regolarmente le credenziali e il segreto. Fornisci solo il livello di accesso necessario per la tua sicurezza. Non è consigliabile riutilizzare credenziali e segreti tra diverse fonti di dati e nelle versioni 1.0 e 2.0 dei connettori (ove applicabile).

Se non disponi di un IAM ruolo o di un segreto esistente, puoi utilizzare la console per creare un nuovo IAM ruolo e un Secrets Manager segreto quando connetti la tua origine dati Amazon FSx (NetApp ONTAP) a. Amazon Kendra Se utilizzi l'API, devi fornire l'ARN di un IAM ruolo e di un Secrets Manager segreto esistenti e un ID di indice.

Istruzioni di connessione

Per connetterti Amazon Kendra alla tua fonte di dati Amazon FSx (NetApp ONTAP), devi fornire i dettagli necessari della tua fonte di dati Amazon FSx (NetApp ONTAP) in modo che Amazon Kendra possa accedere ai tuoi dati. Se non hai ancora configurato Amazon FSx (NetApp ONTAP) per Amazon Kendra, consulta. Prerequisiti

Console

Per connetterti Amazon Kendra al tuo file Amazon FSx system (NetApp ONTAP)

1. Accedi a AWS Management Console e apri la Amazon Kendra console.
2. Dal riquadro di navigazione a sinistra, scegli Indici, quindi scegli l'indice che desideri utilizzare dall'elenco degli indici.

> **Note**
>
> Puoi scegliere di configurare o modificare le impostazioni del controllo dell'accesso degli utenti in Impostazioni dell'indice.

3. Nella pagina Guida introduttiva, scegli Aggiungi origine dati.
4. Nella pagina Aggiungi origine dati, scegli il connettore Amazon FSx (NetApp ONTAP), quindi scegli Aggiungi connettore.
5. Nella pagina Specificare i dettagli dell'origine dati, inserisci le seguenti informazioni:
   a. In Nome e descrizione, per Nome dell'origine dati, inserisci un nome per l'origine dati. Puoi includere trattini ma non spazi.
   b. (Facoltativo) Descrizione: immetti una descrizione facoltativa per l'origine dati.
   c. In Lingua predefinita: scegli una lingua per filtrare i documenti per l'indice. Se non diversamente specificato, la lingua predefinita è l'inglese. La lingua specificata nei metadati del documento ha la precedenza sulla lingua selezionata.
   d. In Tag, per Aggiungi nuovo tag, includi tag opzionali per cercare e filtrare le risorse o tenere traccia dei costi. AWS
   e. Seleziona Successivo.
6. Nella pagina Definisci accesso e sicurezza, inserisci le seguenti informazioni:
   a. Fonte: fornisce le informazioni sul file system.

- Protocollo del file system: scegli il protocollo del tuo file system Amazon FSx (NetApp ONTAP). È possibile scegliere il protocollo Common Internet File System (CIFS) o il protocollo Network File System (NFS) per Linux.
- Amazon FSx ID del file system (NetApp ONTAP): seleziona dal menu a discesa l'ID del file system esistente, recuperato da (ONTAP). Amazon FSx NetApp Oppure, crea un file system (ONTAP Amazon FSx) NetApp . Puoi trovare l'ID del tuo file system nella dashboard dei file system della console Amazon FSx (NetApp ONTAP).
- ID SVM (Amazon FSx (NetApp ONTAPsolo NetApp ONTAP)): fornisci l'ID della macchina virtuale di archiviazione (SVM) del tuo (ONTAP). Amazon FSx NetApp NetApp ONTAP Puoi trovare il tuo ID SVM accedendo alla dashboard File Systems nella console Amazon FSx (NetApp ONTAP), selezionando l'ID del file system e selezionando Storage virtual machines.

b. Autorizzazione: attiva o disattiva le informazioni dell'elenco di controllo degli accessi (ACL) per i tuoi documenti, se disponi di un ACL e desideri utilizzarlo per il controllo degli accessi. L'ACL specifica a quali documenti possono accedere utenti e gruppi. Le informazioni ACL vengono utilizzate per filtrare i risultati della ricerca in base all'accesso dell'utente o del relativo gruppo ai documenti. Per ulteriori informazioni, consulta Filtraggio del contesto utente.

c. Autenticazione: scegli un AWS Secrets Manager segreto esistente o crea un nuovo segreto per archiviare le credenziali del file system. Se scegli di creare un nuovo segreto, si apre una finestra AWS Secrets Manager segreta.

   Fornisci un segreto che memorizzi le credenziali di autenticazione del nome utente e della password. Il nome utente deve includere il nome di dominio DNS. Ad esempio, user@corp.example.com.

   Se utilizzi il protocollo NFS per il tuo file system Amazon FSx (NetApp ONTAP), fornisci un segreto che memorizzi le credenziali di autenticazione dell'ID sinistro, dell'ID destro e della chiave precondivisa.

   Salva e aggiungi il tuo segreto.

d. Virtual Private Cloud (VPC): devi selezionare un Amazon VPC luogo in cui risiede il tuo Amazon FSx (ONTAP). NetApp Includi la sottorete VPC e i gruppi di sicurezza. Vedi Configurazione di un. Amazon VPC

e. IAM ruolo: scegli un ruolo esistente o crea un nuovo IAM IAM ruolo per accedere alle credenziali del repository e indicizzare il contenuto.

> **Note**
>
> IAM i ruoli utilizzati per gli indici non possono essere utilizzati per le fonti di dati. Se non sei sicuro che un ruolo esistente venga utilizzato per un indice o una FAQ, scegli Crea un nuovo ruolo per evitare errori.

f. Seleziona Successivo.

7. Nella pagina Configura le impostazioni di sincronizzazione, inserisci le seguenti informazioni:

   a. Ambito di sincronizzazione, modelli Regex: aggiungi modelli di espressioni regolari per includere o escludere determinati file.

   b. Modalità di sincronizzazione: scegli come aggiornare l'indice quando il contenuto della fonte di dati cambia. Quando sincronizzi l'origine dati con Amazon Kendra per la prima volta, tutto il contenuto viene sottoposto a scansione e indicizzato per impostazione predefinita. Se la sincronizzazione iniziale non è riuscita, devi eseguire una sincronizzazione completa dei dati, anche se non scegli la sincronizzazione completa come opzione della modalità di sincronizzazione.

      - Sincronizzazione completa: indicizza di nuovo tutti i contenuti, sostituendo i contenuti esistenti ogni volta che l'origine dati si sincronizza con l'indice.
      - Sincronizzazione nuova, modificata ed eliminata: indicizza solo i contenuti nuovi, modificati ed eliminati ogni volta che l'origine dati si sincronizza con l'indice. Amazon Kendra può utilizzare il meccanismo dell'origine dati per tenere traccia delle modifiche ai contenuti e indicizzare i contenuti modificati dall'ultima sincronizzazione.

   c. Pianificazione dell'esecuzione della sincronizzazione: per Frequenza, scegli la frequenza con cui sincronizzare il contenuto della fonte di dati e aggiornare l'indice.

   d. Seleziona Successivo.

8. Nella pagina Imposta mappature dei campi, inserisci le seguenti informazioni:

   a. Seleziona tra i campi predefiniti Amazon Kendra generati dei tuoi file che desideri mappare al tuo indice. Per aggiungere campi di origine dati personalizzati, crea un nome di campo indice a cui mappare e il tipo di dati del campo.

   b. Seleziona Successivo.

9. Nella pagina Rivedi e crea, verifica che le informazioni che hai inserito siano corrette, quindi seleziona Aggiungi origine dati. Puoi anche scegliere di modificare le tue informazioni da

questa pagina. L'origine dati verrà visualizzata nella pagina Origini dati dopo che l'origine dati sarà stata aggiunta correttamente.

API

Per connetterti Amazon Kendra al tuo file system Amazon FSx (NetApp ONTAP)

È necessario specificare un codice JSON dello schema di origine dati utilizzando l'TemplateConfigurationAPI. È necessario fornire le seguenti informazioni:

- Origine dati: specifica il tipo di origine dati come `FSXONTAP` quando usi lo schema TemplateConfigurationJSON. Specificate anche l'origine dati come `TEMPLATE` quando chiamate l'CreateDataSourceAPI.
- ID del file system: l'identificatore del file system Amazon FSx (NetApp ONTAP). È possibile trovare l'ID del file system nella dashboard dei file system della console Amazon FSx (NetApp ONTAP).
- ID SVM: l'ID della macchina virtuale di archiviazione (SVM) utilizzato con il file system. Puoi trovare il tuo ID SVM accedendo alla dashboard dei File Systems nella console Amazon FSx (NetApp ONTAP), selezionando l'ID del file system e quindi selezionando Storage virtual machines.
- Tipo di protocollo: specificare se si utilizza il protocollo Common Internet File System (CIFS) o il protocollo Network File System (NFS) per Linux.
- Tipo di file system: specifica il tipo di file system in uno dei due modi. `FSXONTAP`
- Virtual Private Cloud (VPC): `VpcConfiguration` specifica quando si chiama. `CreateDataSource` Per ulteriori informazioni, consulta Configurazione Amazon Kendra per l'utilizzo di un Amazon VPC.

  > **Note**
  >
  > È necessario selezionare un Amazon VPC luogo in cui risiede il proprio Amazon FSx (NetApp ONTAP). Includi la sottorete VPC e i gruppi di sicurezza.

- Secret Amazon Resource Name (ARN): fornisci l'Amazon Resource Name (ARN) di un Secrets Manager segreto che contiene le credenziali di autenticazione per il tuo account (ONTAP). Amazon FSx NetApp Il segreto è archiviato in una struttura JSON con le seguenti chiavi:

```
{
```

```
    "username": "user@corp.example.com",
    "password": "password"
}
```

Se utilizzi il protocollo NFS per il tuo file system Amazon FSx (NetApp ONTAP), il segreto viene archiviato in una struttura JSON con le seguenti chiavi:

```
{
    "leftId": "left ID",
    "rightId": "right ID",
    "preSharedKey": "pre-shared key"
}
```

- IAM ruolo: specifica `RoleArn` quando chiami `CreateDataSource` per fornire a un IAM ruolo le autorizzazioni per accedere al tuo Secrets Manager segreto e per chiamare le API pubbliche richieste per il Amazon FSx connettore (ONTAP) e. NetApp Amazon Kendra Per ulteriori informazioni, consulta IAM i ruoli per le fonti di dati Amazon FSx (NetApp ONTAP).

Puoi anche aggiungere le seguenti funzionalità opzionali:

- Modalità di sincronizzazione: specifica come Amazon Kendra aggiornare l'indice quando il contenuto dell'origine dati cambia. Quando sincronizzi l'origine dati con Amazon Kendra per la prima volta, tutto il contenuto viene sottoposto a scansione e indicizzato per impostazione predefinita. Se la sincronizzazione iniziale non è riuscita, devi eseguire una sincronizzazione completa dei dati, anche se non scegli la sincronizzazione completa come opzione della modalità di sincronizzazione. Puoi scegliere tra:
  - `FORCED_FULL_CRAWL`per indicizzare nuovamente tutti i contenuti, sostituendo i contenuti esistenti ogni volta che l'origine dati si sincronizza con l'indice.
  - `FULL_CRAWL`per indicizzare solo i contenuti nuovi, modificati ed eliminati ogni volta che l'origine dati si sincronizza con l'indice. Amazon Kendra può utilizzare il meccanismo dell'origine dati per tenere traccia delle modifiche ai contenuti e indicizzare i contenuti modificati dall'ultima sincronizzazione.
- Filtri di inclusione ed esclusione: specifica se includere o escludere determinati file.

> **Note**
>
> La maggior parte delle fonti di dati utilizza modelli di espressioni regolari, che sono modelli di inclusione o esclusione denominati filtri. Se si specifica un filtro di inclusione,

viene indicizzato solo il contenuto che corrisponde al filtro di inclusione. Qualsiasi documento che non corrisponde al filtro di inclusione non viene indicizzato. Se si specifica un filtro di inclusione ed esclusione, i documenti che corrispondono al filtro di esclusione non vengono indicizzati, anche se corrispondono al filtro di inclusione.

- Elenco di controllo degli accessi (ACL): specifica se eseguire la scansione delle informazioni ACL per i documenti, se disponi di un ACL e desideri utilizzarlo per il controllo degli accessi. L'ACL specifica a quali documenti possono accedere utenti e gruppi. Le informazioni ACL vengono utilizzate per filtrare i risultati della ricerca in base all'accesso dell'utente o del relativo gruppo ai documenti. Per ulteriori informazioni, consulta Filtraggio del contesto utente.

  > **Note**
  >
  > Per testare il filtraggio del contesto utente su un utente, è necessario includere il nome di dominio DNS come parte del nome utente quando si esegue la query. È necessario disporre delle autorizzazioni amministrative del dominio Active Directory. È inoltre possibile testare il filtraggio del contesto utente in base al nome di un gruppo.

- Mappature dei campi: scegli di mappare i campi delle sorgenti dati Amazon FSx (NetApp ONTAP) ai campi indice. Amazon Kendra Per ulteriori informazioni, consulta la sezione Mappatura dei campi di origine dei dati.

  > **Note**
  >
  > Il campo del corpo del documento o l'equivalente del corpo del documento per i documenti è necessario per Amazon Kendra eseguire la ricerca nei documenti. È necessario mappare il nome del campo del corpo del documento nella fonte dati al nome del campo indice `_document_body`. Tutti gli altri campi sono facoltativi.

Per un elenco di altre importanti chiavi JSON da configurare, consulta lo schema del modello Amazon FSx (NetApp ONTAP).

Amazon RDS/Aurora

È possibile indicizzare i documenti archiviati in un database utilizzando un'origine dati del database. Dopo aver fornito le informazioni di connessione per il database, Amazon Kendra collega e indicizza i documenti.

Amazon Kendra supporta i seguenti database:

- Amazon Aurora MySQL
- Amazon Aurora PostgreSQL
- Amazon RDS per MySQL
- Amazon RDS per PostgreSQL

> **Note**
>
> I database Aurora serverless non sono supportati.

> **Important**
>
> L'obsolescenza di questo connettore Amazon RDS/Aurora è prevista entro la fine del 2023. Amazon Kendra ora supporta nuovi connettori per sorgenti dati del database. Per una migliore esperienza, ti consigliamo di scegliere tra i seguenti nuovi connettori per il tuo caso d'uso:
>
> - Aurora (MySQL)
> - Aurora (PostgreSQL)
> - Amazon RDS (MySQL)
> - Amazon RDS (Microsoft SQL Server)
> - Amazon RDS (Oracle)
> - Amazon RDS (PostgreSQL)
> - IBM DB2
> - Microsoft SQL Server
> - MySQL
> - Banca dati Oracle

- PostgreSQL

Puoi connetterti Amazon Kendra alla fonte di dati del tuo database utilizzando la Amazon Kendra console e l'DatabaseConfigurationAPI.

Per la risoluzione dei problemi relativi al connettore di origine dati del Amazon Kendra database, consultaRisoluzione dei problemi relativi alle origini dati.

Argomenti

- Funzionalità supportate
- Prerequisiti
- Istruzioni di connessione

Funzionalità supportate

Amazon Kendra il connettore di origine dati del database supporta le seguenti funzionalità:

- mappature dei campi
- Filtraggio del contesto utente
- Virtual Private Cloud (VPC) (Cloud privato virtuale (VPC)

Prerequisiti

Prima di poterla utilizzare Amazon Kendra per indicizzare l'origine dati del database, apporta queste modifiche al database e AWS agli account.

Nel tuo database, assicurati di avere:

- Hai annotato le credenziali di autenticazione di base relative al nome utente e alla password per il database.
- Ha copiato il nome host, il numero di porta, l'indirizzo host, il nome del database e il nome della tabella di dati che contiene i dati del documento. Per PostgreSQL, la tabella dati deve essere una tabella pubblica o uno schema pubblico.

> **Note**
>
> L'host e la porta indicano Amazon Kendra dove trovare il server del database su Internet. Il nome del database e il nome della tabella indicano Amazon Kendra dove trovare i dati del documento sul server del database.

- Ha copiato i nomi delle colonne nella tabella di dati che contengono i dati del documento. È necessario includere l'ID del documento, il corpo del documento, le colonne per rilevare se un documento è stato modificato (ad esempio, l'ultima colonna aggiornata) e le colonne facoltative della tabella di dati mappate a campi indice personalizzati. È inoltre possibile mappare qualsiasi nome di campo Amazon Kendra riservato a una colonna della tabella.
- Ha copiato le informazioni sul tipo di motore di database, ad esempio se si utilizza Amazon RDS per MySQL o un altro tipo.
- Selezionato, ogni documento è unico nel database e tra le altre fonti di dati che intendi utilizzare per lo stesso indice. Ogni fonte di dati che desideri utilizzare per un indice non deve contenere lo stesso documento in tutte le fonti di dati. Gli ID dei documenti sono globali rispetto a un indice e devono essere univoci per indice.

Nel tuo Account AWS, assicurati di avere:

- Ha creato un Amazon Kendra indice e, se si utilizza l'API, ha annotato l'ID dell'indice.
- Hai creato un IAM ruolo per la tua origine dati e, se utilizzi l'API, hai annotato l'ARN del IAM ruolo.

> **Note**
>
> Se modifichi il tipo di autenticazione e le credenziali, devi aggiornare il IAM ruolo per accedere all'ID AWS Secrets Manager segreto corretto.

- Ha archiviato le credenziali di autenticazione del database in un AWS Secrets Manager segreto e, se si utilizza l'API, ha annotato l'ARN del segreto.

> **Note**
>
> Ti consigliamo di aggiornare o ruotare regolarmente le credenziali e il segreto. Fornisci solo il livello di accesso necessario per la tua sicurezza. Non è consigliabile riutilizzare

credenziali e segreti tra diverse fonti di dati e versioni dei connettori 1.0 e 2.0 (ove applicabile).

Se non disponi di un IAM ruolo o di un segreto esistente, puoi utilizzare la console per creare un nuovo IAM ruolo e un Secrets Manager segreto quando connetti l'origine dati del database a. Amazon Kendra Se utilizzi l'API, devi fornire l'ARN di un IAM ruolo e di un Secrets Manager segreto esistenti e un ID di indice.

Istruzioni di connessione

Per connettersi Amazon Kendra all'origine dati del database, è necessario fornire i dettagli necessari sull'origine dati del database in modo che sia Amazon Kendra possibile accedere ai dati. Se non hai ancora configurato il database per Amazon Kendra, vediPrerequisiti.

Console

Per connettersi Amazon Kendra a un database

1. Accedere a AWS Management Console e aprire la Amazon Kendra console.
2. Dal riquadro di navigazione a sinistra, scegli Indici, quindi scegli l'indice che desideri utilizzare dall'elenco degli indici.

   > **Note**
   >
   > Puoi scegliere di configurare o modificare le impostazioni del controllo dell'accesso degli utenti in Impostazioni dell'indice.

3. Nella pagina Guida introduttiva, scegli Aggiungi origine dati.
4. Nella pagina Aggiungi origine dati, scegli connettore di database, quindi scegli Aggiungi connettore.
5. Nella pagina Specificare i dettagli dell'origine dati, inserisci le seguenti informazioni:

   a. In Nome e descrizione, per Nome dell'origine dati, inserisci un nome per l'origine dati. Puoi includere trattini ma non spazi.

   b. (Facoltativo) Descrizione: immetti una descrizione facoltativa per la tua fonte di dati.

c. In Lingua predefinita: scegli una lingua per filtrare i documenti per l'indice. Se non diversamente specificato, la lingua predefinita è l'inglese. La lingua specificata nei metadati del documento ha la precedenza sulla lingua selezionata.

d. In Tag, per Aggiungi nuovo tag, includi tag opzionali per cercare e filtrare le risorse o tenere traccia dei costi. AWS

e. Seleziona Successivo.

6. Nella pagina Definisci accesso e sicurezza, inserisci le seguenti informazioni:

a. Endpoint: un nome host DNS, un indirizzo IPv4 o un indirizzo IPv6.

b. Porta: un numero di porta.

c. Database: nome del database.

d. Nome della tabella: nome della tabella.

e. Per Tipo di autenticazione, scegli tra Esistente e Nuovo per memorizzare le credenziali di autenticazione del database. Se scegli di creare un nuovo segreto, si apre una finestra AWS Secrets Manager segreta.

- Inserisci le seguenti informazioni nella finestra Crea un AWS Secrets Manager segreto:

A. Nome segreto: un nome per il tuo segreto. Il prefisso 'AmazonKendra-database-' viene aggiunto automaticamente al nome segreto.

B. Per nome utente e password: inserisci i valori delle credenziali di autenticazione dal tuo account di database.

C. Scegli Salva autenticazione.

f. Virtual Private Cloud (VPC): puoi scegliere di utilizzare un VPC. In tal caso, è necessario aggiungere sottoreti e gruppi di sicurezza VPC.

> **Note**
>
> È necessario utilizzare una sottorete privata. Se l'istanza RDS si trova in una sottorete pubblica del VPC, è possibile creare una sottorete privata con accesso in uscita a un gateway NAT nella sottorete pubblica. Le sottoreti fornite nella configurazione VPC devono trovarsi negli Stati Uniti occidentali (Oregon), negli Stati Uniti orientali (Virginia settentrionale) e nell'UE (Irlanda).

g. IAM ruolo: scegli un IAM ruolo esistente o creane uno nuovo per accedere alle credenziali del IAM repository e indicizzare il contenuto.

> **Note**
>
> IAM i ruoli utilizzati per gli indici non possono essere utilizzati per le fonti di dati. Se non sei sicuro che un ruolo esistente venga utilizzato per un indice o una FAQ, scegli Crea un nuovo ruolo per evitare errori.

h. Seleziona Successivo.

7. Nella pagina Configura le impostazioni di sincronizzazione, inserisci le seguenti informazioni:

   a. Scegli tra Aurora MySQL, MySQL, Aurora PostgreSQL e PostgreSQL in base al tuo caso d'uso.

   b. Racchiudi gli identificatori SQL tra virgolette: seleziona per racchiudere gli identificatori SQL tra virgolette doppie. Ad esempio, «columnName».

   c. Colonna ACL e colonne di rilevamento delle modifiche: configura le colonne Amazon Kendra utilizzate per il rilevamento delle modifiche (ad esempio, l'ultima colonna aggiornata) e l'elenco di controllo degli accessi.

   d. In Sync run schedulation, per Frequenza: scegli la frequenza con cui eseguire la sincronizzazione con la Amazon Kendra tua fonte di dati.

   e. Seleziona Successivo.

8. Nella pagina Imposta le mappature dei campi, inserisci le seguenti informazioni:

   a. Amazon Kendra mappature di campo predefinite: seleziona uno dei campi di origine dati predefiniti Amazon Kendra generati che desideri mappare all'indice. È necessario aggiungere i valori delle colonne del database per e `document_id` `document_body`

   b. Mappature personalizzate dei campi: per aggiungere campi di origine dati personalizzati per creare un nome di campo indice a cui mappare e il tipo di dati del campo.

   c. Seleziona Successivo.

9. Nella pagina Rivedi e crea, verifica che le informazioni inserite siano corrette, quindi seleziona Aggiungi origine dati. Puoi anche scegliere di modificare le tue informazioni da questa pagina. L'origine dati verrà visualizzata nella pagina Origini dati dopo che l'origine dati sarà stata aggiunta correttamente.

API

Per connettersi Amazon Kendra a un database

È necessario specificare quanto segue l'DatabaseConfigurationAPI:

- ColumnConfiguration—Informazioni su dove l'indice deve ottenere le informazioni sul documento dal database. Per ulteriori dettagli, consulta ColumnConfiguration. È necessario specificare i campi `DocumentDataColumnName` (corpo del documento o testo principale) e`DocumentIdColumnName`, e `ChangeDetectingColumn` (ad esempio, ultima colonna aggiornata). La colonna mappata al `DocumentIdColumnName` campo deve essere una colonna intera. L'esempio seguente mostra una semplice configurazione di colonne per un'origine dati del database:

```
"ColumnConfiguration": {
    "ChangeDetectingColumns": [
        "LastUpdateDate",
        "LastUpdateTime"
    ],
    "DocumentDataColumnName": "TextColumn",
    "DocumentIdColumnName": "IdentifierColumn",
    "DocoumentTitleColumnName": "TitleColumn",
    "FieldMappings": [
        {
            "DataSourceFieldName": "AbstractColumn",
            "IndexFieldName": "Abstract"
        }
    ]
}
```

- ConnectionConfiguration—Informazioni di configurazione necessarie per connettersi a un database. Per ulteriori dettagli, consulta ConnectionConfiguration.
- DatabaseEngineType—Il tipo di motore di database che esegue il database. Il `DatabaseHost` campo per `ConnectionConfiguration` deve essere l'endpoint dell'istanza Amazon Relational Database Service (Amazon RDS) per il database. Non utilizzare l'endpoint del cluster.
- Secret Amazon Resource Name (ARN): fornisci l'Amazon Resource Name (ARN) di un Secrets Manager segreto che contiene le credenziali di autenticazione per il tuo account di database. Il segreto è archiviato in una struttura JSON con le seguenti chiavi:

```
{
    "username": "user name",
    "password": "password"
}
```

L'esempio seguente mostra una configurazione del database, incluso l'ARN segreto.

```
"DatabaseConfiguration": {
"ConnectionConfiguration": {
"DatabaseHost": "host.subdomain.domain.tld",
        "DatabaseName": "DocumentDatabase",
        "DatabasePort": 3306,
        "SecretArn": "arn:aws:secretmanager:region:account ID:secret/secret name",
        "TableName": "DocumentTable"
    }
}
```

> **Note**
>
> Ti consigliamo di aggiornare o ruotare regolarmente le credenziali e il segreto. Fornisci solo il livello di accesso necessario per la tua sicurezza. Non è consigliabile riutilizzare credenziali e segreti tra diverse fonti di dati e versioni dei connettori 1.0 e 2.0 (ove applicabile).

- IAM ruolo: specifica `RoleArn` quando chiami `CreateDataSource` per fornire a un IAM ruolo le autorizzazioni per accedere al tuo Secrets Manager segreto e per chiamare le API pubbliche richieste per il connettore del database e. Amazon Kendra Per ulteriori informazioni, consulta IAM i ruoli per le fonti di dati del database.

Puoi anche aggiungere le seguenti funzionalità opzionali:

- Virtual Private Cloud (VPC): specifica `VpcConfiguration` come parte della configurazione dell'origine dati. Vedi Configurazione Amazon Kendra per l'uso di un VPC.

> **Note**
>
> È necessario utilizzare solo una sottorete privata. Se l'istanza RDS si trova in una sottorete pubblica del VPC, è possibile creare una sottorete privata con accesso in uscita a un gateway NAT nella sottorete pubblica. Le sottoreti fornite nella configurazione VPC devono trovarsi negli Stati Uniti occidentali (Oregon), negli Stati Uniti orientali (Virginia settentrionale) e nell'UE (Irlanda).

- Mappature dei campi: scegli di mappare i campi delle sorgenti dati del database ai campi indice. Amazon Kendra Per ulteriori informazioni, consulta la sezione Mappatura dei campi di origine dei dati.

> **Note**
>
> Il campo del corpo del documento o l'equivalente del corpo del documento per i documenti è necessario per Amazon Kendra eseguire la ricerca nei documenti. È necessario mappare il nome del campo del corpo del documento nella fonte dati al nome del campo indice`_document_body`. Tutti gli altri campi sono facoltativi.

- Filtraggio del contesto utente e controllo degli accessi:Amazon Kendra esegue la scansione dell'elenco di controllo degli accessi (ACL) dei documenti, se disponi di un ACL per i documenti. Le informazioni ACL vengono utilizzate per filtrare i risultati della ricerca in base all'accesso dell'utente o del relativo gruppo ai documenti. Per ulteriori informazioni, consulta Filtraggio del contesto utente.

Amazon RDS (Microsoft SQL Server)

SQL Server è un sistema di gestione di database sviluppato da Microsoft. Amazon RDS per SQL Server semplifica la configurazione, il funzionamento e la scalabilità delle distribuzioni di SQL Server nel cloud. Se sei un utente Amazon RDS (Microsoft SQL Server), puoi utilizzarlo Amazon Kendra per indicizzare la tua origine dati Amazon RDS (Microsoft SQL Server). Il connettore di origine dati Amazon Kendra JDBC supporta Microsoft SQL Server 2019.

Puoi connetterti Amazon Kendra alla tua origine dati Amazon RDS (Microsoft SQL Server) utilizzando la Amazon Kendra console e l'TemplateConfigurationAPI.

Per la risoluzione dei problemi relativi al connettore di origine dati Amazon Kendra Amazon RDS (Microsoft SQL Server), vedereRisoluzione dei problemi relativi alle origini dati.

Argomenti

Funzionalità supportate

- Mappature dei campi
- Filtraggio del contesto utente
- Filtri di inclusione/esclusione
- Sincronizzazione completa e incrementale dei contenuti
- Virtual Private Cloud (VPC) (Cloud privato virtuale (VPC)

Prerequisiti

Prima di poterla utilizzare Amazon Kendra per indicizzare l'origine dati Amazon RDS (Microsoft SQL Server), apporta queste modifiche al tuo Amazon RDS (Microsoft SQL Server) e AWS agli account.

In Amazon RDS (Microsoft SQL Server), assicurati di avere:

- Hai annotato il nome utente e la password del database.

> **Important**
>
> È consigliabile fornire credenziali Amazon Kendra di database di sola lettura.

- Hai copiato l'URL, la porta e l'istanza dell'host del database.
- Selezionato, ogni documento è unico in Amazon RDS (Microsoft SQL Server) e tra le altre fonti di dati che intendi utilizzare per lo stesso indice. Ogni origine dati che desideri utilizzare per un indice non deve contenere lo stesso documento in tutte le fonti di dati. Gli ID dei documenti sono globali rispetto a un indice e devono essere univoci per indice.

Nel tuo Account AWS, assicurati di avere:

- Ha creato un Amazon Kendra indice e, se si utilizza l'API, ha annotato l'ID dell'indice.
- Hai creato un IAM ruolo per la tua origine dati e, se utilizzi l'API, hai annotato l'ARN del IAM ruolo.

> **Note**
>
> Se modifichi il tipo di autenticazione e le credenziali, devi aggiornare il IAM ruolo per accedere all'ID AWS Secrets Manager segreto corretto.

- Ha archiviato le credenziali di autenticazione Amazon RDS (Microsoft SQL Server) in un AWS Secrets Manager segreto e, se si utilizza l'API, ha annotato l'ARN del segreto.

> **Note**
>
> Ti consigliamo di aggiornare o ruotare regolarmente le credenziali e il segreto. Fornisci solo il livello di accesso necessario per la tua sicurezza. Non è consigliabile riutilizzare credenziali e segreti tra diverse fonti di dati e versioni dei connettori 1.0 e 2.0 (ove applicabile).

Se non disponi di un IAM ruolo o di un segreto esistente, puoi utilizzare la console per creare un nuovo IAM ruolo e Secrets Manager segreto quando connetti la tua origine dati Amazon RDS (Microsoft SQL Server) a Amazon Kendra. Se utilizzi l'API, devi fornire l'ARN di un IAM ruolo e di un Secrets Manager segreto esistenti e un ID di indice.

Istruzioni di connessione

Per connetterti Amazon Kendra alla tua origine dati Amazon RDS (Microsoft SQL Server) devi fornire i dettagli delle tue credenziali Amazon RDS (Microsoft SQL Server) in modo da Amazon Kendra poter accedere ai tuoi dati. Se non hai ancora configurato Amazon RDS (Microsoft SQL Server), Amazon Kendra consultaPrerequisiti.

Console

Per connettersi Amazon Kendra a Amazon RDS (Microsoft SQL Server)

1. Accedere a AWS Management Console e aprire la Amazon Kendra console.

2. Dal riquadro di navigazione a sinistra, scegli Indici, quindi scegli l'indice che desideri utilizzare dall'elenco degli indici.

> **Note**
>
> Puoi scegliere di configurare o modificare le impostazioni del controllo dell'accesso degli utenti in Impostazioni dell'indice.

3. Nella pagina Guida introduttiva, scegli Aggiungi origine dati.
4. Nella pagina Aggiungi origine dati, scegli Connettore Amazon RDS (Microsoft SQL Server), quindi scegli Aggiungi connettore.
5. Nella pagina Specificare i dettagli dell'origine dati, inserisci le seguenti informazioni:

   a. In Nome e descrizione, per Nome dell'origine dati, inserisci un nome per l'origine dati. Puoi includere trattini ma non spazi.
   b. (Facoltativo) Descrizione: immetti una descrizione facoltativa per l'origine dati.
   c. In Lingua predefinita: scegli una lingua per filtrare i documenti per l'indice. Se non diversamente specificato, la lingua predefinita è l'inglese. La lingua specificata nei metadati del documento ha la precedenza sulla lingua selezionata.
   d. In Tag, per Aggiungi nuovo tag, includi tag opzionali per cercare e filtrare le risorse o tenere traccia dei costi. AWS
   e. Seleziona Successivo.
6. Nella pagina Definisci accesso e sicurezza, inserisci le seguenti informazioni:

   a. In Source, inserisci le seguenti informazioni:
   b. Host: immettere il nome host del database.
   c. Porta: immettere la porta del database.
   d. Istanza: immettere l'istanza del database.
   e. Abilita la posizione del certificato SSL: scegli di inserire il Amazon S3 percorso del file del certificato SSL.
   f. In Autenticazione, inserisci le seguenti informazioni:

      - AWS Secrets Manager segreto: scegli un segreto esistente o crea un nuovo Secrets Manager segreto per archiviare le credenziali di autenticazione Amazon RDS (Microsoft SQL Server). Se scegli di creare un nuovo segreto, si apre una finestra AWS Secrets Manager segreta.

A. Inserisci le seguenti informazioni nella finestra Crea un AWS Secrets Manager segreto:

I. Nome segreto: un nome per il tuo segreto. Il prefisso 'AmazonKendra-Amazon RDS (Microsoft SQL Server) -' viene aggiunto automaticamente al nome segreto.

II. Per nome utente e password del database: immettere i valori delle credenziali di autenticazione copiati dal database.

B. Selezionare Salva.

g. Virtual Private Cloud (VPC): puoi scegliere di utilizzare un VPC. In tal caso, è necessario aggiungere sottoreti e gruppi di sicurezza VPC.

h. IAM ruolo: scegli un IAM ruolo esistente o creane uno nuovo IAM per accedere alle credenziali del repository e indicizzare il contenuto.

> **Note**
>
> IAM i ruoli utilizzati per gli indici non possono essere utilizzati per le fonti di dati. Se non sei sicuro che un ruolo esistente venga utilizzato per un indice o una FAQ, scegli Crea un nuovo ruolo per evitare errori.

i. Seleziona Successivo.

7. Nella pagina Configura le impostazioni di sincronizzazione, inserisci le seguenti informazioni:

a. Nell'ambito della sincronizzazione, scegli tra le seguenti opzioni:

- Query SQL: immetti istruzioni di query SQL come le operazioni SELECT e JOIN. Le query SQL devono pesare meno di 32 KB. Amazon Kendra eseguirà la scansione di tutto il contenuto del database che corrisponde alla tua query.

> **Note**
>
> Se il nome di una tabella include caratteri speciali (non alfanumerici) nel nome, è necessario utilizzare parentesi quadre attorno al nome della tabella. Ad esempio, `seleziona*` da [] my-database-table

- Colonna chiave primaria: fornisce la chiave primaria per la tabella del database. Identifica una tabella all'interno del database.

- Colonna del titolo: fornisce il nome della colonna del titolo del documento all'interno della tabella del database.
- Colonna del corpo: fornisce il nome della colonna del corpo del documento all'interno della tabella del database.

b. In Configurazione aggiuntiva, facoltativa, scegli una delle seguenti opzioni per sincronizzare contenuti specifici anziché sincronizzare tutti i file:

- Colonne di rilevamento delle modifiche: immetti i nomi delle colonne che Amazon Kendra verranno utilizzate per rilevare le modifiche al contenuto. Amazon Kendra reindicizzerà il contenuto quando viene apportata una modifica in una di queste colonne.
- Colonna ID utente: immetti il nome della colonna che contiene gli ID utente a cui consentire l'accesso ai contenuti.
- Colonna Gruppi: immetti il nome della colonna che contiene i gruppi a cui consentire l'accesso ai contenuti.
- Colonna URL di origine: inserisci il nome della colonna che contiene gli URL di origine da indicizzare.
- Colonna timestamp: immetti il nome della colonna che contiene i timestamp. Amazon Kendra utilizza le informazioni relative alla marca temporale per rilevare le modifiche ai contenuti e sincronizzare solo i contenuti modificati.
- Colonna dei fusi orari: inserisci il nome della colonna che contiene i fusi orari per il contenuto da sottoporre a scansione.
- Formato timestamp: immetti il nome della colonna che contiene i formati di timestamp da utilizzare per rilevare le modifiche ai contenuti e risincronizzare i contenuti.

c. Modalità di sincronizzazione: scegli come aggiornare l'indice quando il contenuto della fonte dati cambia. Quando sincronizzi l'origine dati con Amazon Kendra per la prima volta, tutto il contenuto viene sottoposto a scansione e indicizzato per impostazione predefinita. Se la sincronizzazione iniziale non è riuscita, devi eseguire una sincronizzazione completa dei dati, anche se non scegli la sincronizzazione completa come opzione della modalità di sincronizzazione.

- Sincronizzazione completa: indicizza di nuovo tutti i contenuti, sostituendo i contenuti esistenti ogni volta che l'origine dati si sincronizza con l'indice.
- Sincronizzazione nuova e modificata: indicizza solo i contenuti nuovi e modificati ogni volta che l'origine dati si sincronizza con l'indice. Amazon Kendra può utilizzare

il meccanismo dell'origine dati per tenere traccia delle modifiche ai contenuti e indicizzare i contenuti modificati dall'ultima sincronizzazione.

- Sincronizzazione nuova, modificata ed eliminata: indicizza solo i contenuti nuovi, modificati ed eliminati ogni volta che l'origine dati si sincronizza con l'indice. Amazon Kendra può utilizzare il meccanismo dell'origine dati per tenere traccia delle modifiche ai contenuti e indicizzare i contenuti modificati dall'ultima sincronizzazione.

d. Pianificazione di esecuzione di In Sync, per Frequenza: con quale frequenza Amazon Kendra verrà eseguita la sincronizzazione con la fonte di dati.

e. Seleziona Successivo.

8. Nella pagina Imposta le mappature dei campi, inserisci le seguenti informazioni:

a. Seleziona uno dei campi di origine dati predefiniti generati (ID documento, titoli dei documenti e URL di origine) che desideri mappare per indicizzare. Amazon Kendra

b. Aggiungi campo: consente di aggiungere campi di origine dati personalizzati per creare un nome di campo indice a cui mappare e il tipo di dati del campo.

c. Seleziona Successivo.

9. Nella pagina Rivedi e crea, verifica che le informazioni inserite siano corrette, quindi seleziona Aggiungi origine dati. Puoi anche scegliere di modificare le tue informazioni da questa pagina. L'origine dati verrà visualizzata nella pagina Origini dati dopo che l'origine dati sarà stata aggiunta correttamente.

API

Per connettersi Amazon Kendra a Amazon RDS (Microsoft SQL Server)

È necessario specificare quanto segue utilizzando l'TemplateConfigurationAPI:

- Origine dati: specifica il tipo di origine dati come `JDBC` quando usi lo schema TemplateConfigurationJSON. Specificate anche l'origine dati come `TEMPLATE` quando chiamate l'CreateDataSourceAPI.
- Tipo di database: è necessario specificare il tipo di database come`sqlserver`.
- Query SQL: specifica le istruzioni di query SQL come le operazioni SELECT e JOIN. Le query SQL devono pesare meno di 32 KB. Amazon Kendra eseguirà la scansione di tutto il contenuto del database che corrisponde alla tua query.

> **Note**
>
> Se il nome di una tabella include caratteri speciali (non alfanumerici) nel nome, è necessario utilizzare parentesi quadre attorno al nome della tabella. Ad esempio, *seleziona** da [] my-database-table

- Modalità di sincronizzazione: specifica come Amazon Kendra aggiornare l'indice quando il contenuto dell'origine dati cambia. Quando sincronizzi l'origine dati con Amazon Kendra per la prima volta, tutto il contenuto viene sottoposto a scansione e indicizzato per impostazione predefinita. Se la sincronizzazione iniziale non è riuscita, devi eseguire una sincronizzazione completa dei dati, anche se non scegli la sincronizzazione completa come opzione della modalità di sincronizzazione. Puoi scegliere tra:
  - `FORCED_FULL_CRAWL`per indicizzare nuovamente tutti i contenuti, sostituendo i contenuti esistenti ogni volta che l'origine dati si sincronizza con l'indice.
  - `FULL_CRAWL`per indicizzare solo i contenuti nuovi, modificati ed eliminati ogni volta che l'origine dati si sincronizza con l'indice. Amazon Kendra può utilizzare il meccanismo dell'origine dati per tenere traccia delle modifiche ai contenuti e indicizzare i contenuti modificati dall'ultima sincronizzazione.
  - `CHANGE_LOG`per indicizzare solo contenuti nuovi e modificati ogni volta che l'origine dati si sincronizza con l'indice. Amazon Kendra può utilizzare il meccanismo dell'origine dati per tenere traccia delle modifiche ai contenuti e indicizzare i contenuti modificati dall'ultima sincronizzazione.
- Secret Amazon Resource Name (ARN): fornisci l'Amazon Resource Name (ARN) di un Secrets Manager segreto che contiene le credenziali di autenticazione che hai creato nel tuo account (Amazon RDS Microsoft SQL Server). Il segreto è memorizzato in una struttura JSON con le seguenti chiavi:

```
{
    "user name": "database user name",
    "password": "password"
}
```

> **Note**
>
> Ti consigliamo di aggiornare o ruotare regolarmente le credenziali e il segreto. Fornisci solo il livello di accesso necessario per la tua sicurezza. Non è consigliabile riutilizzare

credenziali e segreti tra diverse fonti di dati e versioni dei connettori 1.0 e 2.0 (ove applicabile).

- IAM ruolo: specifica `RoleArn` quando chiami `CreateDataSource` per fornire a un IAM ruolo le autorizzazioni per accedere al tuo Secrets Manager segreto e per chiamare le API pubbliche richieste per il connettore (Amazon RDS Microsoft SQL Server) e. Amazon Kendra Per ulteriori informazioni, consulta IAM ruoli per le origini dati Amazon RDS (Microsoft SQL Server).

Puoi anche aggiungere le seguenti funzionalità opzionali:

- Virtual Private Cloud (VPC): `VpcConfiguration` specifica quando si chiama. `CreateDataSource` Per ulteriori informazioni, consulta Configurazione Amazon Kendra per l'utilizzo di un Amazon VPC.
- Filtri di inclusione ed esclusione: puoi specificare se includere contenuti specifici utilizzando ID utente, gruppi, URL di origine, timestamp e fusi orari.
- Filtraggio del contesto utente e controllo degli accessi:Amazon Kendra esegue la ricerca per indicizzazione dell'elenco di controllo degli accessi (ACL) dei documenti, se disponi di un ACL per i documenti. Le informazioni ACL vengono utilizzate per filtrare i risultati della ricerca in base all'accesso dell'utente o del relativo gruppo ai documenti. Per ulteriori informazioni, consulta Filtraggio del contesto utente.
- Mappature dei campi: scegliere di mappare i campi dell'origine dati (Amazon RDS Microsoft SQL Server) ai Amazon Kendra campi indice. Per ulteriori informazioni, consulta la sezione Mappatura dei campi di origine dei dati.

> **Note**
>
> Il campo del corpo del documento o l'equivalente del corpo del documento per i documenti è necessario per Amazon Kendra eseguire la ricerca nei documenti. È necessario mappare il nome del campo del corpo del documento nella fonte dati al nome del campo indice_`document_body`. Tutti gli altri campi sono facoltativi.

Per un elenco di altre importanti chiavi JSON da configurare, consultaAmazon RDS Schema del modello (Microsoft SQL Server).

Note

- Le righe del database eliminate non verranno registrate durante la Amazon Kendra verifica della presenza di contenuti aggiornati.
- La dimensione dei nomi e dei valori dei campi in una riga del database non può superare i 400 KB.
- Se l'origine dati del database contiene una grande quantità di dati e non desideri Amazon Kendra indicizzare tutto il contenuto del database dopo la prima sincronizzazione, puoi scegliere di sincronizzare solo i documenti nuovi, modificati o eliminati.
- È consigliabile fornire credenziali Amazon Kendra di database di sola lettura.
- È consigliabile evitare di aggiungere tabelle con dati sensibili o informazioni personali identificabili (PII).

Amazon RDS (MySQL)

Amazon RDS (Amazon Relational Database Service) è un servizio Web che semplifica la configurazione, il funzionamento e la scalabilità di un database relazionale nel AWS cloud. Se sei un Amazon RDS utente, puoi utilizzarlo Amazon Kendra per indicizzare la tua fonte di Amazon RDS (MySQL) dati. Il connettore di origine Amazon Kendra dati supporta Amazon RDS MySql 5.6, 5.7 e 8.0.

Puoi connetterti Amazon Kendra alla tua fonte di Amazon RDS (MySQL) dati utilizzando la Amazon Kendra console e l'API. TemplateConfiguration

Per la risoluzione dei problemi relativi al connettore della sorgente Amazon Kendra Amazon RDS (MySQL) dati, consultaRisoluzione dei problemi relativi alle origini dati.

Argomenti

- Funzionalità supportate
- Prerequisiti
- Istruzioni di connessione
- Note

Funzionalità supportate

- Mappature dei campi

- Filtraggio del contesto utente
- Filtri di inclusione/esclusione
- Sincronizzazione completa e incrementale dei contenuti
- Virtual Private Cloud (VPC) (Cloud privato virtuale (VPC)

Prerequisiti

Prima di poterla utilizzare Amazon Kendra per indicizzare la tua fonte di Amazon RDS (MySQL) dati, apporta queste modifiche al tuo account Amazon RDS (MySQL) e AWS ai tuoi account.

NelAmazon RDS (MySQL), assicurati di avere:

- Hai annotato il nome utente e la password del database.

> **Important**
>
> È consigliabile fornire credenziali Amazon Kendra di database di sola lettura.

- Hai copiato l'URL, la porta e l'istanza dell'host del database. Puoi trovare queste informazioni sulla Amazon RDS console.
- È stato verificato che ogni documento sia unico nelle Amazon RDS (MySQL) altre fonti di dati che intendi utilizzare per lo stesso indice. Ogni fonte di dati che desideri utilizzare per un indice non deve contenere lo stesso documento in tutte le fonti di dati. Gli ID dei documenti sono globali rispetto a un indice e devono essere univoci per indice.

Nel tuo Account AWS, assicurati di avere:

- Ha creato un Amazon Kendra indice e, se si utilizza l'API, ha annotato l'ID dell'indice.
- Hai creato un IAM ruolo per la tua origine dati e, se utilizzi l'API, hai annotato l'ARN del IAM ruolo.

> **Note**
>
> Se modifichi il tipo di autenticazione e le credenziali, devi aggiornare il IAM ruolo per accedere all'ID AWS Secrets Manager segreto corretto.

- Ha archiviato le credenziali di Amazon RDS (MySQL) autenticazione in un AWS Secrets Manager segreto e, se si utilizza l'API, ha annotato l'ARN del segreto.

> **Note**
>
> Ti consigliamo di aggiornare o ruotare regolarmente le credenziali e il segreto. Fornisci solo il livello di accesso necessario per la tua sicurezza. Non è consigliabile riutilizzare credenziali e segreti tra diverse fonti di dati e versioni dei connettori 1.0 e 2.0 (ove applicabile).

Se non disponi di un IAM ruolo o di un segreto esistente, puoi utilizzare la console per creare un nuovo IAM ruolo e un Secrets Manager segreto quando connetti la tua origine Amazon RDS (MySQL) dati a. Amazon Kendra Se utilizzi l'API, devi fornire l'ARN di un IAM ruolo e di un Secrets Manager segreto esistenti e un ID di indice.

Istruzioni di connessione

Per connetterti Amazon Kendra alla tua fonte di Amazon RDS (MySQL) dati devi fornire i dettagli delle tue Amazon RDS (MySQL) credenziali in modo da Amazon Kendra poter accedere ai tuoi dati. Se non lo hai ancora configuratoAmazon RDS (MySQL), Amazon Kendra vediPrerequisiti.

Console

Per connettersi Amazon Kendra a Amazon RDS (MySQL)

1. Accedi a AWS Management Console e apri la Amazon Kendra console.
2. Dal riquadro di navigazione a sinistra, scegli Indici, quindi scegli l'indice che desideri utilizzare dall'elenco degli indici.

   > **Note**
   >
   > Puoi scegliere di configurare o modificare le impostazioni del controllo dell'accesso degli utenti in Impostazioni dell'indice.

3. Nella pagina Guida introduttiva, scegli Aggiungi origine dati.
4. Nella pagina Aggiungi origine dati, scegli Amazon RDS (MySQL)connettore, quindi scegli Aggiungi connettore.
5. Nella pagina Specificare i dettagli dell'origine dati, inserisci le seguenti informazioni:

a. In Nome e descrizione, per Nome dell'origine dati, inserisci un nome per l'origine dati. Puoi includere trattini ma non spazi.

b. (Facoltativo) Descrizione: immetti una descrizione facoltativa per l'origine dati.

c. In Lingua predefinita: scegli una lingua per filtrare i documenti per l'indice. Se non diversamente specificato, la lingua predefinita è l'inglese. La lingua specificata nei metadati del documento ha la precedenza sulla lingua selezionata.

d. In Tag, per Aggiungi nuovo tag, includi tag opzionali per cercare e filtrare le risorse o tenere traccia dei costi. AWS

e. Seleziona Successivo.

6. Nella pagina Definisci accesso e sicurezza, inserisci le seguenti informazioni:

a. In Source, inserisci le seguenti informazioni:

b. Host: inserisci l'URL dell'host del database, per esempio:`http://`*`instance URL`*`.`*`region`*`.rds.amazonaws.com`.

c. Porta: inserisci la porta del database, ad esempio,`5432`.

d. Istanza: immettere, ad esempio, l'istanza del database`postgres`.

e. Abilita la posizione del certificato SSL: scegli di inserire il Amazon S3 percorso del file del certificato SSL.

f. In Autenticazione, inserisci le seguenti informazioni:

- AWS Secrets Manager segreto: scegli un segreto esistente o creane uno nuovo Secrets Manager per memorizzare le credenziali di Amazon RDS (MySQL) autenticazione. Se scegli di creare un nuovo segreto, si apre una finestra AWS Secrets Manager segreta.

  A. Inserisci le seguenti informazioni nella finestra Crea un AWS Secrets Manager segreto:

     I. Nome segreto: un nome per il tuo segreto. Il prefisso 'AmazonKendra-Amazon RDS (MySQL) -' viene aggiunto automaticamente al nome segreto.

     II. Per nome utente e password del database, immettete i valori delle credenziali di autenticazione copiati dal database.

  B. Selezionare Salva.

g. Virtual Private Cloud (VPC): puoi scegliere di utilizzare un VPC. In tal caso, è necessario aggiungere sottoreti e gruppi di sicurezza VPC.

h. IAM ruolo: scegli un IAM ruolo esistente o creane uno nuovo IAM per accedere alle credenziali del repository e indicizzare il contenuto.

> **Note**
>
> IAM i ruoli utilizzati per gli indici non possono essere utilizzati per le fonti di dati. Se non sei sicuro che un ruolo esistente venga utilizzato per un indice o una FAQ, scegli Crea un nuovo ruolo per evitare errori.

i. Seleziona Successivo.

7. Nella pagina Configura le impostazioni di sincronizzazione, inserisci le seguenti informazioni:

a. Nell'ambito della sincronizzazione, scegli tra le seguenti opzioni:

- Query SQL: immetti istruzioni di query SQL come le operazioni SELECT e JOIN. Le query SQL devono pesare meno di 32 KB Le query SQL devono pesare meno di 32 KB e non contenere punto e virgola (;). Amazon Kendra eseguirà la scansione di tutto il contenuto del database che corrisponde alla tua query.
- Colonna chiave primaria: fornisce la chiave primaria per la tabella del database. Identifica una tabella all'interno del database.
- Colonna del titolo: fornisce il nome della colonna del titolo del documento all'interno della tabella del database.
- Colonna del corpo: fornisce il nome della colonna del corpo del documento all'interno della tabella del database.

b. In Configurazione aggiuntiva, facoltativa, scegli una delle seguenti opzioni per sincronizzare contenuti specifici anziché sincronizzare tutti i file:

- Colonne di rilevamento delle modifiche: inserisci i nomi delle colonne che Amazon Kendra verranno utilizzate per rilevare le modifiche al contenuto. Amazon Kendra reindicizzerà il contenuto in caso di modifica in una di queste colonne.
- Colonna ID utenti: immetti il nome della colonna che contiene gli ID utente a cui consentire l'accesso ai contenuti.
- Colonna Gruppi: immetti il nome della colonna che contiene i gruppi a cui consentire l'accesso ai contenuti.

- Colonna URL di origine: inserisci il nome della colonna che contiene gli URL di origine da indicizzare.
- Colonna timestamp: immetti il nome della colonna che contiene i timestamp. Amazon Kendra utilizza le informazioni relative alla marca temporale per rilevare le modifiche ai contenuti e sincronizzare solo i contenuti modificati.
- Colonna dei fusi orari: inserisci il nome della colonna che contiene i fusi orari per il contenuto da sottoporre a scansione.
- Formato timestamp: immetti il nome della colonna che contiene i formati di timestamp da utilizzare per rilevare le modifiche ai contenuti e risincronizzare i contenuti.

c. Modalità di sincronizzazione: scegli come aggiornare l'indice quando il contenuto della fonte dati cambia. Quando sincronizzi l'origine dati con Amazon Kendra per la prima volta, tutto il contenuto viene sottoposto a scansione e indicizzato per impostazione predefinita. Se la sincronizzazione iniziale non è riuscita, devi eseguire una sincronizzazione completa dei dati, anche se non scegli la sincronizzazione completa come opzione della modalità di sincronizzazione.

- Sincronizzazione completa: indicizza di nuovo tutti i contenuti, sostituendo i contenuti esistenti ogni volta che l'origine dati si sincronizza con l'indice.
- Nuova sincronizzazione modificata: indicizza solo i contenuti nuovi e modificati ogni volta che l'origine dati si sincronizza con l'indice. Amazon Kendra può utilizzare il meccanismo dell'origine dati per tenere traccia delle modifiche ai contenuti e indicizzare i contenuti modificati dall'ultima sincronizzazione.
- Sincronizzazione nuova, modificata ed eliminata: indicizza solo i contenuti nuovi, modificati ed eliminati ogni volta che l'origine dati si sincronizza con l'indice. Amazon Kendra può utilizzare il meccanismo dell'origine dati per tenere traccia delle modifiche ai contenuti e indicizzare i contenuti modificati dall'ultima sincronizzazione.

d. Pianificazione di esecuzione di In Sync, per Frequenza: con quale frequenza Amazon Kendra verrà eseguita la sincronizzazione con la fonte di dati.

e. Seleziona Successivo.

8. Nella pagina Imposta mappature dei campi, inserisci le seguenti informazioni:

a. Seleziona uno dei campi di origine dati predefiniti generati (ID documento, titoli dei documenti e URL di origine) che desideri mappare per indicizzare. Amazon Kendra

b. Aggiungi campo: consente di aggiungere campi di origine dati personalizzati per creare un nome di campo indice a cui mappare e il tipo di dati del campo.

c. Seleziona Successivo.

9. Nella pagina Rivedi e crea, verifica che le informazioni inserite siano corrette, quindi seleziona Aggiungi origine dati. Puoi anche scegliere di modificare le tue informazioni da questa pagina. L'origine dati verrà visualizzata nella pagina Origini dati dopo che l'origine dati sarà stata aggiunta correttamente.

API

Per connettersi Amazon Kendra a Amazon RDS (MySQL)

È necessario specificare quanto segue utilizzando l'TemplateConfigurationAPI:

- Origine dati: specifica il tipo di origine dati come `JDBC` quando usi lo schema TemplateConfigurationJSON. Specificate anche l'origine dati come `TEMPLATE` quando chiamate l'CreateDataSourceAPI.
- Tipo di database: è necessario specificare il tipo di database come`mySql`.
- Query SQL: specifica le istruzioni di query SQL come le operazioni SELECT e JOIN. Le query SQL devono pesare meno di 32 KB. Amazon Kendra eseguirà la scansione di tutto il contenuto del database che corrisponde alla tua query.
- Modalità di sincronizzazione: specifica come Amazon Kendra aggiornare l'indice quando il contenuto dell'origine dati cambia. Quando sincronizzi l'origine dati con Amazon Kendra per la prima volta, tutto il contenuto viene sottoposto a scansione e indicizzato per impostazione predefinita. Se la sincronizzazione iniziale non è riuscita, devi eseguire una sincronizzazione completa dei dati, anche se non scegli la sincronizzazione completa come opzione della modalità di sincronizzazione. Puoi scegliere tra:
  - `FORCED_FULL_CRAWL`per indicizzare nuovamente tutti i contenuti, sostituendo i contenuti esistenti ogni volta che l'origine dati si sincronizza con l'indice.
  - `FULL_CRAWL`per indicizzare solo i contenuti nuovi, modificati ed eliminati ogni volta che l'origine dati si sincronizza con l'indice. Amazon Kendra può utilizzare il meccanismo dell'origine dati per tenere traccia delle modifiche ai contenuti e indicizzare i contenuti modificati dall'ultima sincronizzazione.
  - `CHANGE_LOG`per indicizzare solo contenuti nuovi e modificati ogni volta che l'origine dati si sincronizza con l'indice. Amazon Kendra può utilizzare il meccanismo dell'origine dati per tenere traccia delle modifiche ai contenuti e indicizzare i contenuti modificati dall'ultima sincronizzazione.

- Amazon Resource Name (ARN) segreto: fornisci l'Amazon Resource Name (ARN) di un Secrets Manager segreto che contiene le credenziali di autenticazione che hai creato nel tuo account. Amazon RDS (MySQL) Il segreto è archiviato in una struttura JSON con le seguenti chiavi:

```
{
    "user name": "database user name",
    "password": "password"
}
```

> **Note**
>
> Ti consigliamo di aggiornare o ruotare regolarmente le credenziali e il segreto. Fornisci solo il livello di accesso necessario per la tua sicurezza. Non è consigliabile riutilizzare credenziali e segreti tra diverse fonti di dati e versioni dei connettori 1.0 e 2.0 (ove applicabile).

- IAM ruolo: specifica `RoleArn` quando chiami `CreateDataSource` per fornire a un IAM ruolo le autorizzazioni per accedere al tuo Secrets Manager segreto e per chiamare le API pubbliche richieste per il connettore e. Amazon RDS (MySQL) Amazon Kendra Per ulteriori informazioni, consulta i IAM ruoli per Amazon RDS (MySQL) le fonti di dati.

Puoi anche aggiungere le seguenti funzionalità opzionali:

- Virtual Private Cloud (VPC): `VpcConfiguration` specifica quando si chiama. `CreateDataSource` Per ulteriori informazioni, consulta Configurazione Amazon Kendra per l'utilizzo di un Amazon VPC.
- Filtri di inclusione ed esclusione: puoi specificare se includere contenuti specifici utilizzando ID utente, gruppi, URL di origine, timestamp e fusi orari.
- Mappature dei campi: scegli di mappare i campi delle sorgenti Amazon RDS (MySQL) dati ai campi indice. Amazon Kendra Per ulteriori informazioni, consulta la sezione Mappatura dei campi di origine dei dati.

> **Note**
>
> Il campo del corpo del documento o l'equivalente del corpo del documento per i documenti è necessario per Amazon Kendra eseguire la ricerca nei documenti. È

necessario mappare il nome del campo del corpo del documento nella fonte dati al nome del campo indice_`document_body`. Tutti gli altri campi sono facoltativi.

- Filtraggio del contesto utente e controllo degli accessi:Amazon Kendra esegue la scansione dell'elenco di controllo degli accessi (ACL) dei documenti, se disponi di un ACL per i documenti. Le informazioni ACL vengono utilizzate per filtrare i risultati della ricerca in base all'accesso dell'utente o del relativo gruppo ai documenti. Per ulteriori informazioni, consulta Filtraggio del contesto utente.

Per un elenco di altre importanti chiavi JSON da configurare, consulta. Amazon RDS Schema del modello (MySQL)

Note

- Le righe del database eliminate non verranno registrate durante la Amazon Kendra verifica della presenza di contenuti aggiornati.
- La dimensione dei nomi e dei valori dei campi in una riga del database non può superare i 400 KB.
- Se l'origine dati del database contiene una grande quantità di dati e non desideri Amazon Kendra indicizzare tutto il contenuto del database dopo la prima sincronizzazione, puoi scegliere di sincronizzare solo i documenti nuovi, modificati o eliminati.
- È consigliabile fornire credenziali Amazon Kendra di database di sola lettura.
- È consigliabile evitare di aggiungere tabelle con dati sensibili o informazioni personali identificabili (PII).

Amazon RDS (Oracle)

Amazon RDS (Amazon Relational Database Service) è un servizio Web che semplifica la configurazione, il funzionamento e la scalabilità di un database relazionale nel AWS cloud. Se sei un Amazon RDS (Oracle) utente, puoi utilizzarlo Amazon Kendra per indicizzare la tua fonte di Amazon RDS (Oracle) dati. Il connettore di origine Amazon Kendra Amazon RDS (Oracle) dati supporta Amazon RDS Oracle Database 21c, Oracle Database 19c, Oracle Database 12c.

Puoi connetterti Amazon Kendra alla tua fonte di Amazon RDS (Oracle) dati utilizzando la Amazon Kendra console e l'API. TemplateConfiguration

Per la risoluzione dei problemi relativi al connettore della sorgente Amazon Kendra Amazon RDS (Oracle) dati, consultaRisoluzione dei problemi relativi alle origini dati.

Argomenti

Funzionalità supportate

- Mappature dei campi
- Filtraggio del contesto utente
- Filtri di inclusione/esclusione
- Sincronizzazione completa e incrementale dei contenuti
- Virtual Private Cloud (VPC) (Cloud privato virtuale (VPC)

Prerequisiti

Prima di poterla utilizzare Amazon Kendra per indicizzare la tua fonte di Amazon RDS (Oracle) dati, apporta queste modifiche al tuo account Amazon RDS (Oracle) e AWS ai tuoi account.

NelAmazon RDS (Oracle), assicurati di avere:

- Hai annotato il nome utente e la password del tuo database.

> **Important**
>
> È consigliabile fornire credenziali Amazon Kendra di database di sola lettura.

- Hai copiato l'URL, la porta e l'istanza dell'host del database.
- È stato verificato che ogni documento sia unico all'interno Amazon RDS (Oracle) e tra le altre fonti di dati che intendi utilizzare per lo stesso indice. Ogni fonte di dati che desideri utilizzare per un indice non deve contenere lo stesso documento in tutte le fonti di dati. Gli ID dei documenti sono globali rispetto a un indice e devono essere univoci per indice.

Nel tuo Account AWS, assicurati di avere:

- Ha creato un Amazon Kendra indice e, se si utilizza l'API, ha annotato l'ID dell'indice.
- Hai creato un IAM ruolo per la tua origine dati e, se utilizzi l'API, hai annotato l'ARN del IAM ruolo.

> **Note**
>
> Se modifichi il tipo di autenticazione e le credenziali, devi aggiornare il IAM ruolo per accedere all'ID AWS Secrets Manager segreto corretto.

- Ha archiviato le credenziali di Amazon RDS (Oracle) autenticazione in un AWS Secrets Manager segreto e, se si utilizza l'API, ha annotato l'ARN del segreto.

> **Note**
>
> Ti consigliamo di aggiornare o ruotare regolarmente le credenziali e il segreto. Fornisci solo il livello di accesso necessario per la tua sicurezza. Non è consigliabile riutilizzare credenziali e segreti tra diverse fonti di dati e versioni dei connettori 1.0 e 2.0 (ove applicabile).

Se non disponi di un IAM ruolo o di un segreto esistente, puoi utilizzare la console per creare un nuovo IAM ruolo e un Secrets Manager segreto quando connetti la tua origine Amazon RDS (Oracle) dati a. Amazon Kendra Se utilizzi l'API, devi fornire l'ARN di un IAM ruolo e di un Secrets Manager segreto esistenti e un ID di indice.

Istruzioni di connessione

Per connetterti Amazon Kendra alla tua fonte di Amazon RDS (Oracle) dati devi fornire i dettagli delle tue Amazon RDS (Oracle) credenziali in modo da Amazon Kendra poter accedere ai tuoi dati. Se non lo hai ancora configurato, Amazon RDS (Oracle) Amazon Kendra Prerequisiti consulta.

Console

Per connettersi Amazon Kendra a Amazon RDS (Oracle)

1. Accedi a AWS Management Console e apri la Amazon Kendra console.
2. Dal riquadro di navigazione a sinistra, scegli Indici, quindi scegli l'indice che desideri utilizzare dall'elenco degli indici.

> **Note**
>
> Puoi scegliere di configurare o modificare le impostazioni del controllo dell'accesso degli utenti in Impostazioni dell'indice.

3. Nella pagina Guida introduttiva, scegli Aggiungi origine dati.
4. Nella pagina Aggiungi origine dati, scegli Amazon RDS (Oracle)connettore, quindi scegli Aggiungi connettore.
5. Nella pagina Specificare i dettagli dell'origine dati, inserisci le seguenti informazioni:
   a. In Nome e descrizione, per Nome dell'origine dati, inserisci un nome per l'origine dati. Puoi includere trattini ma non spazi.
   b. (Facoltativo) Descrizione: immetti una descrizione facoltativa per la tua fonte di dati.
   c. In Lingua predefinita: scegli una lingua per filtrare i documenti per l'indice. Se non diversamente specificato, la lingua predefinita è l'inglese. La lingua specificata nei metadati del documento ha la precedenza sulla lingua selezionata.
   d. In Tag, per Aggiungi nuovo tag, includi tag opzionali per cercare e filtrare le risorse o tenere traccia dei costi. AWS
   e. Seleziona Successivo.
6. Nella pagina Definisci accesso e sicurezza, inserisci le seguenti informazioni:
   a. In Source, inserisci le seguenti informazioni:
   b. Host: immettere il nome host del database.
   c. Porta: immettere la porta del database.
   d. Istanza: immettere l'istanza del database.
   e. Abilita la posizione del certificato SSL: scegli di inserire il Amazon S3 percorso del file del certificato SSL.
   f. In Autenticazione, inserisci le seguenti informazioni:
      - AWS Secrets Manager segreto: scegli un segreto esistente o creane uno nuovo Secrets Manager per memorizzare le credenziali di Amazon RDS (Oracle) autenticazione. Se scegli di creare un nuovo segreto, si apre una finestra AWS Secrets Manager segreta.

A. Inserisci le seguenti informazioni nella finestra Crea un AWS Secrets Manager segreto:

I. Nome segreto: un nome per il tuo segreto. Il prefisso 'AmazonKendra-Amazon RDS (Oracle) -' viene aggiunto automaticamente al nome segreto.

II. Per nome utente e password del database, immettete i valori delle credenziali di autenticazione copiati dal database.

B. Selezionare Salva.

g. Virtual Private Cloud (VPC): puoi scegliere di utilizzare un VPC. In tal caso, è necessario aggiungere sottoreti e gruppi di sicurezza VPC.

h. IAM ruolo: scegli un IAM ruolo esistente o creane uno nuovo IAM per accedere alle credenziali del repository e indicizzare il contenuto.

> **Note**
>
> IAM i ruoli utilizzati per gli indici non possono essere utilizzati per le fonti di dati. Se non sei sicuro che un ruolo esistente venga utilizzato per un indice o una FAQ, scegli Crea un nuovo ruolo per evitare errori.

i. Seleziona Successivo.

7. Nella pagina Configura le impostazioni di sincronizzazione, inserisci le seguenti informazioni:

a. Nell'ambito della sincronizzazione, scegli tra le seguenti opzioni:

- Query SQL: immetti istruzioni di query SQL come le operazioni SELECT e JOIN. Le query SQL devono pesare meno di 32 KB. Amazon Kendra eseguirà la scansione di tutto il contenuto del database che corrisponde alla tua query.
- Colonna chiave primaria: fornisce la chiave primaria per la tabella del database. Identifica una tabella all'interno del database.
- Colonna del titolo: fornisce il nome della colonna del titolo del documento all'interno della tabella del database.
- Colonna del corpo: fornisce il nome della colonna del corpo del documento all'interno della tabella del database.

b. In Configurazione aggiuntiva, facoltativa, scegli una delle seguenti opzioni per sincronizzare contenuti specifici anziché sincronizzare tutti i file:

- Colonne di rilevamento delle modifiche: immetti i nomi delle colonne che Amazon Kendra verranno utilizzate per rilevare le modifiche al contenuto. Amazon Kendra reindicizzerà il contenuto quando viene apportata una modifica in una di queste colonne.
- Colonna ID utenti: immetti il nome della colonna che contiene gli ID utente a cui consentire l'accesso ai contenuti.
- Colonna Gruppi: immetti il nome della colonna che contiene i gruppi a cui consentire l'accesso ai contenuti.
- Colonna URL di origine: inserisci il nome della colonna che contiene gli URL di origine da indicizzare.
- Colonna timestamp: immetti il nome della colonna che contiene i timestamp. Amazon Kendra utilizza le informazioni relative alla marca temporale per rilevare le modifiche ai contenuti e sincronizzare solo i contenuti modificati.
- Colonna dei fusi orari: inserisci il nome della colonna che contiene i fusi orari per il contenuto da sottoporre a scansione.
- Formato timestamp: immetti il nome della colonna che contiene i formati di timestamp da utilizzare per rilevare le modifiche ai contenuti e risincronizzare i contenuti.

c. Modalità di sincronizzazione: scegli come aggiornare l'indice quando il contenuto della fonte dati cambia. Quando sincronizzi l'origine dati con Amazon Kendra per la prima volta, tutto il contenuto viene sottoposto a scansione e indicizzato per impostazione predefinita. Se la sincronizzazione iniziale non è riuscita, devi eseguire una sincronizzazione completa dei dati, anche se non scegli la sincronizzazione completa come opzione della modalità di sincronizzazione.

   - Sincronizzazione completa: indicizza di nuovo tutti i contenuti, sostituendo i contenuti esistenti ogni volta che l'origine dati si sincronizza con l'indice.
   - Nuova sincronizzazione modificata: indicizza solo i contenuti nuovi e modificati ogni volta che l'origine dati si sincronizza con l'indice. Amazon Kendra può utilizzare il meccanismo dell'origine dati per tenere traccia delle modifiche ai contenuti e indicizzare i contenuti modificati dall'ultima sincronizzazione.
   - Sincronizzazione nuova, modificata ed eliminata: indicizza solo i contenuti nuovi, modificati ed eliminati ogni volta che l'origine dati si sincronizza con l'indice. Amazon Kendra può utilizzare il meccanismo dell'origine dati per tenere traccia delle modifiche ai contenuti e indicizzare i contenuti modificati dall'ultima sincronizzazione.

d. Pianificazione di esecuzione di In Sync, per Frequenza: con quale frequenza Amazon Kendra verrà eseguita la sincronizzazione con la fonte di dati.

e. Seleziona Successivo.

8. Nella pagina Imposta le mappature dei campi, inserisci le seguenti informazioni:

a. Seleziona uno dei campi di origine dati predefiniti generati (ID documento, titoli dei documenti e URL di origine) che desideri mappare per indicizzare. Amazon Kendra

b. Aggiungi campo: consente di aggiungere campi di origine dati personalizzati per creare un nome di campo indice a cui mappare e il tipo di dati del campo.

c. Seleziona Successivo.

9. Nella pagina Rivedi e crea, verifica che le informazioni inserite siano corrette, quindi seleziona Aggiungi origine dati. Puoi anche scegliere di modificare le tue informazioni da questa pagina. L'origine dati verrà visualizzata nella pagina Origini dati dopo che l'origine dati sarà stata aggiunta correttamente.

API

Per connettersi Amazon Kendra a Amazon RDS (Oracle)

È necessario specificare quanto segue utilizzando l'TemplateConfigurationAPI:

- Origine dati: specifica il tipo di origine dati come `JDBC` quando usi lo schema TemplateConfigurationJSON. Specificate anche l'origine dati come `TEMPLATE` quando chiamate l'CreateDataSourceAPI.
- Tipo di database: è necessario specificare il tipo di database come`oracle`.
- Query SQL: specifica le istruzioni di query SQL come le operazioni SELECT e JOIN. Le query SQL devono pesare meno di 32 KB. Amazon Kendra eseguirà la scansione di tutto il contenuto del database che corrisponde alla tua query.
- Modalità di sincronizzazione: specifica come Amazon Kendra aggiornare l'indice quando il contenuto dell'origine dati cambia. Quando sincronizzi l'origine dati con Amazon Kendra per la prima volta, tutto il contenuto viene sottoposto a scansione e indicizzato per impostazione predefinita. Se la sincronizzazione iniziale non è riuscita, devi eseguire una sincronizzazione completa dei dati, anche se non scegli la sincronizzazione completa come opzione della modalità di sincronizzazione. Puoi scegliere tra:
  - `FORCED_FULL_CRAWL`per indicizzare nuovamente tutti i contenuti, sostituendo i contenuti esistenti ogni volta che l'origine dati si sincronizza con l'indice.

  - `FULL_CRAWL`per indicizzare solo i contenuti nuovi, modificati ed eliminati ogni volta che l'origine dati si sincronizza con l'indice. Amazon Kendra può utilizzare il meccanismo dell'origine dati per tenere traccia delle modifiche ai contenuti e indicizzare i contenuti modificati dall'ultima sincronizzazione.
  - `CHANGE_LOG`per indicizzare solo contenuti nuovi e modificati ogni volta che l'origine dati si sincronizza con l'indice. Amazon Kendra può utilizzare il meccanismo dell'origine dati per tenere traccia delle modifiche ai contenuti e indicizzare i contenuti modificati dall'ultima sincronizzazione.
- Amazon Resource Name (ARN) segreto: fornisci l'Amazon Resource Name (ARN) di un Secrets Manager segreto che contiene le credenziali di autenticazione che hai creato nel tuo account. Amazon RDS (Oracle) Il segreto è archiviato in una struttura JSON con le seguenti chiavi:

```
{
    "user name": "database user name",
    "password": "password"
}
```

> **Note**
>
> Ti consigliamo di aggiornare o ruotare regolarmente le credenziali e il segreto. Fornisci solo il livello di accesso necessario per la tua sicurezza. Non è consigliabile riutilizzare credenziali e segreti tra diverse fonti di dati e versioni dei connettori 1.0 e 2.0 (ove applicabile).

- IAM ruolo: specifica `RoleArn` quando chiami `CreateDataSource` per fornire a un IAM ruolo le autorizzazioni per accedere al tuo Secrets Manager segreto e per chiamare le API pubbliche richieste per il connettore e. Amazon RDS (Oracle) Amazon Kendra Per ulteriori informazioni, consulta i IAM ruoli per Amazon RDS (Oracle) le fonti di dati.

Puoi anche aggiungere le seguenti funzionalità opzionali:

- Virtual Private Cloud (VPC): `VpcConfiguration` specifica quando si chiama. `CreateDataSource` Per ulteriori informazioni, consulta Configurazione Amazon Kendra per l'utilizzo di un Amazon VPC.

- Filtri di inclusione ed esclusione: puoi specificare se includere contenuti specifici utilizzando ID utente, gruppi, URL di origine, timestamp e fusi orari.
- Filtraggio del contesto utente e controllo degli accessi:Amazon Kendra esegue la ricerca per indicizzazione dell'elenco di controllo degli accessi (ACL) dei documenti, se disponi di un ACL per i documenti. Le informazioni ACL vengono utilizzate per filtrare i risultati della ricerca in base all'accesso dell'utente o del relativo gruppo ai documenti. Per ulteriori informazioni, consulta Filtraggio del contesto utente.
- Mappature dei campi: scegli di mappare i campi delle sorgenti Amazon RDS (Oracle) dati ai campi indice. Amazon Kendra Per ulteriori informazioni, consulta la sezione Mappatura dei campi di origine dei dati.

> **Note**
>
> Il campo del corpo del documento o l'equivalente del corpo del documento per i documenti è necessario per Amazon Kendra eseguire la ricerca nei documenti. È necessario mappare il nome del campo del corpo del documento nella fonte dati al nome del campo indice`_document_body`. Tutti gli altri campi sono facoltativi.

Per un elenco di altre importanti chiavi JSON da configurare, consultaAmazon RDS schema modello (Oracle).

Note

- Le righe del database eliminate non verranno registrate durante la Amazon Kendra verifica della presenza di contenuti aggiornati.
- La dimensione dei nomi e dei valori dei campi in una riga del database non può superare i 400 KB.
- Se l'origine dati del database contiene una grande quantità di dati e non desideri Amazon Kendra indicizzare tutto il contenuto del database dopo la prima sincronizzazione, puoi scegliere di sincronizzare solo i documenti nuovi, modificati o eliminati.
- È consigliabile fornire credenziali Amazon Kendra di database di sola lettura.
- È consigliabile evitare di aggiungere tabelle con dati sensibili o informazioni personali identificabili (PII).

Amazon RDS (PostgreSQL)

Amazon RDS è un servizio web che semplifica la configurazione, il funzionamento e la scalabilità di un database relazionale nel AWS cloud. Se sei un Amazon RDS utente, puoi utilizzarlo Amazon Kendra per indicizzare la tua fonte di Amazon RDS (PostgreSQL) dati. Il connettore di origine Amazon Kendra Amazon RDS (PostgreSQL) dati supporta PostgreSQL 9.6.

Puoi connetterti Amazon Kendra alla tua fonte di Amazon RDS (PostgreSQL) dati utilizzando la Amazon Kendra console e l'API. TemplateConfiguration

Per la risoluzione dei problemi relativi al connettore della sorgente Amazon Kendra Amazon RDS (PostgreSQL) dati, consultaRisoluzione dei problemi relativi alle origini dati.

Argomenti

- Funzionalità supportate
- Prerequisiti
- Istruzioni di connessione
- Note

Funzionalità supportate

- Mappature dei campi
- Filtraggio del contesto utente
- Filtri di inclusione/esclusione
- Sincronizzazione completa e incrementale dei contenuti
- Virtual Private Cloud (VPC) (Cloud privato virtuale (VPC)

Prerequisiti

Prima di poterla utilizzare Amazon Kendra per indicizzare la tua fonte di Amazon RDS (PostgreSQL) dati, apporta queste modifiche al tuo account Amazon RDS (PostgreSQL) e AWS ai tuoi account.

NelAmazon RDS (PostgreSQL), assicurati di avere:

- Hai annotato il nome utente e la password del database.

> **Important**
>
> È consigliabile fornire credenziali Amazon Kendra di database di sola lettura.

- Hai copiato l'URL, la porta e l'istanza dell'host del database. Puoi trovare queste informazioni sulla Amazon RDS console.
- È stato verificato che ogni documento sia unico nelle Amazon RDS (PostgreSQL) altre fonti di dati che intendi utilizzare per lo stesso indice. Ogni fonte di dati che desideri utilizzare per un indice non deve contenere lo stesso documento in tutte le fonti di dati. Gli ID dei documenti sono globali rispetto a un indice e devono essere univoci per indice.

Nel tuo Account AWS, assicurati di avere:

- Ha creato un Amazon Kendra indice e, se si utilizza l'API, ha annotato l'ID dell'indice.
- Hai creato un IAM ruolo per la tua origine dati e, se utilizzi l'API, hai annotato l'ARN del IAM ruolo.

> **Note**
>
> Se modifichi il tipo di autenticazione e le credenziali, devi aggiornare il IAM ruolo per accedere all'ID AWS Secrets Manager segreto corretto.

- Ha archiviato le credenziali di Amazon RDS (PostgreSQL) autenticazione in un AWS Secrets Manager segreto e, se si utilizza l'API, ha annotato l'ARN del segreto.

> **Note**
>
> Ti consigliamo di aggiornare o ruotare regolarmente le credenziali e il segreto. Fornisci solo il livello di accesso necessario per la tua sicurezza. Non è consigliabile riutilizzare credenziali e segreti tra diverse fonti di dati e nelle versioni 1.0 e 2.0 dei connettori (ove applicabile).

Se non disponi di un IAM ruolo o di un segreto esistente, puoi utilizzare la console per creare un nuovo IAM ruolo e un Secrets Manager segreto quando connetti la tua origine Amazon RDS (PostgreSQL) dati a. Amazon Kendra Se utilizzi l'API, devi fornire l'ARN di un IAM ruolo e di un Secrets Manager segreto esistenti e un ID di indice.

Istruzioni di connessione

Per connetterti Amazon Kendra alla tua fonte di Amazon RDS (PostgreSQL) dati devi fornire i dettagli delle tue Amazon RDS (PostgreSQL) credenziali in modo da Amazon Kendra poter accedere ai tuoi dati. Se non lo hai ancora configurato, Amazon RDS (PostgreSQL) Amazon Kendra Prerequisiti consulta.

Console

Per connettersi Amazon Kendra a Amazon RDS (PostgreSQL)

1. Accedi a AWS Management Console e apri la Amazon Kendra console.
2. Dal riquadro di navigazione a sinistra, scegli Indici, quindi scegli l'indice che desideri utilizzare dall'elenco degli indici.

> **Note**
>
> Puoi scegliere di configurare o modificare le impostazioni del controllo dell'accesso degli utenti in Impostazioni dell'indice.

3. Nella pagina Guida introduttiva, scegli Aggiungi origine dati.
4. Nella pagina Aggiungi origine dati, scegli Amazon RDS (PostgreSQL)connettore, quindi scegli Aggiungi connettore.
5. Nella pagina Specificare i dettagli dell'origine dati, inserisci le seguenti informazioni:
   a. In Nome e descrizione, per Nome dell'origine dati, inserisci un nome per l'origine dati. Puoi includere trattini ma non spazi.
   b. (Facoltativo) Descrizione: immetti una descrizione facoltativa per l'origine dati.
   c. In Lingua predefinita: scegli una lingua per filtrare i documenti per l'indice. Se non diversamente specificato, la lingua predefinita è l'inglese. La lingua specificata nei metadati del documento ha la precedenza sulla lingua selezionata.
   d. In Tag, per Aggiungi nuovo tag, includi tag opzionali per cercare e filtrare le risorse o tenere traccia dei costi. AWS
   e. Seleziona Successivo.
6. Nella pagina Definisci accesso e sicurezza, inserisci le seguenti informazioni:
   a. In Source, inserisci le seguenti informazioni:

b. Host: inserisci l'URL dell'host del database, per esempio:`http://instance URL.region.rds.amazonaws.com`.

c. Porta: inserisci la porta del database, ad esempio,`5432`.

d. Istanza: immettere, ad esempio, l'istanza del database`postgres`.

e. Abilita la posizione del certificato SSL: scegli di inserire il Amazon S3 percorso del file del certificato SSL.

f. In Autenticazione, inserisci le seguenti informazioni:

- AWS Secrets Manager segreto: scegli un segreto esistente o creane uno nuovo Secrets Manager per memorizzare le credenziali di Amazon RDS (PostgreSQL) autenticazione. Se scegli di creare un nuovo segreto, si apre una finestra AWS Secrets Manager segreta.

  A. Inserisci le seguenti informazioni nella finestra Crea un AWS Secrets Manager segreto:

     I. Nome segreto: un nome per il tuo segreto. Il prefisso 'AmazonKendra-Amazon RDS (PostgreSQL) -' viene aggiunto automaticamente al nome segreto.

     II. Per nome utente e password del database, immettete i valori delle credenziali di autenticazione copiati dal database.

  B. Selezionare Salva.

g. Virtual Private Cloud (VPC): puoi scegliere di utilizzare un VPC. In tal caso, è necessario aggiungere sottoreti e gruppi di sicurezza VPC.

h. IAM ruolo: scegli un IAM ruolo esistente o creane uno nuovo IAM per accedere alle credenziali del repository e indicizzare il contenuto.

> **Note**
>
> IAM i ruoli utilizzati per gli indici non possono essere utilizzati per le fonti di dati. Se non sei sicuro che un ruolo esistente venga utilizzato per un indice o una FAQ, scegli Crea un nuovo ruolo per evitare errori.

i. Seleziona Successivo.

7. Nella pagina Configura le impostazioni di sincronizzazione, inserisci le seguenti informazioni:

a. Nell'ambito della sincronizzazione, scegli tra le seguenti opzioni:

   - Query SQL: immetti istruzioni di query SQL come le operazioni SELECT e JOIN. Le query SQL devono pesare meno di 32 KB Le query SQL devono pesare meno di 32 KB e non contenere punto e virgola (;). Amazon Kendra eseguirà la scansione di tutto il contenuto del database che corrisponde alla tua query.
   - Colonna chiave primaria: fornisce la chiave primaria per la tabella del database. Identifica una tabella all'interno del database.
   - Colonna del titolo: fornisce il nome della colonna del titolo del documento all'interno della tabella del database.
   - Colonna del corpo: fornisce il nome della colonna del corpo del documento all'interno della tabella del database.

b. In Configurazione aggiuntiva, facoltativa, scegli una delle seguenti opzioni per sincronizzare contenuti specifici anziché sincronizzare tutti i file:

   - Colonne di rilevamento delle modifiche: inserisci i nomi delle colonne che Amazon Kendra verranno utilizzate per rilevare le modifiche al contenuto. Amazon Kendra reindicizzerà il contenuto quando viene apportata una modifica in una di queste colonne.
   - Colonna ID utenti: immetti il nome della colonna che contiene gli ID utente a cui consentire l'accesso ai contenuti.
   - Colonna Gruppi: immetti il nome della colonna che contiene i gruppi a cui consentire l'accesso ai contenuti.
   - Colonna URL di origine: inserisci il nome della colonna che contiene gli URL di origine da indicizzare.
   - Colonna timestamp: immetti il nome della colonna che contiene i timestamp. Amazon Kendra utilizza le informazioni relative alla marca temporale per rilevare le modifiche ai contenuti e sincronizzare solo i contenuti modificati.
   - Colonna dei fusi orari: inserisci il nome della colonna che contiene i fusi orari per il contenuto da sottoporre a scansione.
   - Formato timestamp: immetti il nome della colonna che contiene i formati di timestamp da utilizzare per rilevare le modifiche ai contenuti e risincronizzare i contenuti.

c. Modalità di sincronizzazione: scegli come aggiornare l'indice quando il contenuto della fonte dati cambia. Quando sincronizzi l'origine dati con Amazon Kendra per

la prima volta, tutto il contenuto viene sottoposto a scansione e indicizzato per impostazione predefinita. Se la sincronizzazione iniziale non è riuscita, devi eseguire una sincronizzazione completa dei dati, anche se non scegli la sincronizzazione completa come opzione della modalità di sincronizzazione.

- Sincronizzazione completa: indicizza di nuovo tutti i contenuti, sostituendo i contenuti esistenti ogni volta che l'origine dati si sincronizza con l'indice.
- Sincronizzazione nuova e modificata: indicizza solo i contenuti nuovi e modificati ogni volta che l'origine dati si sincronizza con l'indice. Amazon Kendra può utilizzare il meccanismo dell'origine dati per tenere traccia delle modifiche ai contenuti e indicizzare i contenuti modificati dall'ultima sincronizzazione.
- Sincronizzazione nuova, modificata ed eliminata: indicizza solo i contenuti nuovi, modificati ed eliminati ogni volta che l'origine dati si sincronizza con l'indice. Amazon Kendra può utilizzare il meccanismo dell'origine dati per tenere traccia delle modifiche ai contenuti e indicizzare i contenuti modificati dall'ultima sincronizzazione.

d. Pianificazione di esecuzione di In Sync, per Frequenza: con quale frequenza Amazon Kendra verrà eseguita la sincronizzazione con la fonte di dati.

e. Seleziona Successivo.

8. Nella pagina Imposta le mappature dei campi, inserisci le seguenti informazioni:

a. Seleziona uno dei campi di origine dati predefiniti generati (ID documento, titoli dei documenti e URL di origine) che desideri mappare per indicizzare. Amazon Kendra

b. Aggiungi campo: consente di aggiungere campi di origine dati personalizzati per creare un nome di campo indice a cui mappare e il tipo di dati del campo.

c. Seleziona Successivo.

9. Nella pagina Rivedi e crea, verifica che le informazioni inserite siano corrette, quindi seleziona Aggiungi origine dati. Puoi anche scegliere di modificare le tue informazioni da questa pagina. L'origine dati verrà visualizzata nella pagina Origini dati dopo che l'origine dati sarà stata aggiunta correttamente.

API

Per connettersi Amazon Kendra a Amazon RDS (PostgreSQL)

È necessario specificare quanto segue utilizzando l'TemplateConfigurationAPI:

- Origine dati: specifica il tipo di origine dati come `JDBC` quando usi lo schema TemplateConfigurationJSON. Specificate anche l'origine dati come `TEMPLATE` quando chiamate l'CreateDataSourceAPI.
- Tipo di database: è necessario specificare il tipo di database come`postgresql`.
- Query SQL: specifica le istruzioni di query SQL come le operazioni SELECT e JOIN. Le query SQL devono pesare meno di 32 KB. Amazon Kendra eseguirà la scansione di tutto il contenuto del database che corrisponde alla tua query.
- Modalità di sincronizzazione: specifica come Amazon Kendra aggiornare l'indice quando il contenuto dell'origine dati cambia. Quando sincronizzi l'origine dati con Amazon Kendra per la prima volta, tutto il contenuto viene sottoposto a scansione e indicizzato per impostazione predefinita. Se la sincronizzazione iniziale non è riuscita, devi eseguire una sincronizzazione completa dei dati, anche se non scegli la sincronizzazione completa come opzione della modalità di sincronizzazione. Puoi scegliere tra:
  - `FORCED_FULL_CRAWL`per indicizzare nuovamente tutti i contenuti, sostituendo i contenuti esistenti ogni volta che l'origine dati si sincronizza con l'indice.
  - `FULL_CRAWL`per indicizzare solo i contenuti nuovi, modificati ed eliminati ogni volta che l'origine dati si sincronizza con l'indice. Amazon Kendra può utilizzare il meccanismo dell'origine dati per tenere traccia delle modifiche ai contenuti e indicizzare i contenuti modificati dall'ultima sincronizzazione.
  - `CHANGE_LOG`per indicizzare solo contenuti nuovi e modificati ogni volta che l'origine dati si sincronizza con l'indice. Amazon Kendra può utilizzare il meccanismo dell'origine dati per tenere traccia delle modifiche ai contenuti e indicizzare i contenuti modificati dall'ultima sincronizzazione.
- Amazon Resource Name (ARN) segreto: fornisci l'Amazon Resource Name (ARN) di un Secrets Manager segreto che contiene le credenziali di autenticazione che hai creato nel tuo account. Amazon RDS (PostgreSQL) Il segreto è archiviato in una struttura JSON con le seguenti chiavi:

```
{
    "user name": "database user name",
    "password": "password"
}
```

> **Note**
>
> Ti consigliamo di aggiornare o ruotare regolarmente le credenziali e il segreto. Fornisci solo il livello di accesso necessario per la tua sicurezza. Non è consigliabile riutilizzare credenziali e segreti tra diverse fonti di dati e nelle versioni 1.0 e 2.0 dei connettori (ove applicabile).

- IAM ruolo: specifica `RoleArn` quando chiami `CreateDataSource` per fornire a un IAM ruolo le autorizzazioni per accedere al tuo Secrets Manager segreto e per chiamare le API pubbliche richieste per il connettore e. Amazon RDS (PostgreSQL) Amazon Kendra Per ulteriori informazioni, consulta i IAM ruoli per Amazon RDS (PostgreSQL) le fonti di dati.

Puoi anche aggiungere le seguenti funzionalità opzionali:

- Virtual Private Cloud (VPC): `VpcConfiguration` specifica quando si chiama. `CreateDataSource` Per ulteriori informazioni, consulta Configurazione Amazon Kendra per l'utilizzo di un Amazon VPC.
- Filtri di inclusione ed esclusione: puoi specificare se includere contenuti specifici utilizzando ID utente, gruppi, URL di origine, timestamp e fusi orari.
- Filtraggio del contesto utente e controllo degli accessi:Amazon Kendra esegue la ricerca per indicizzazione dell'elenco di controllo degli accessi (ACL) dei documenti, se disponi di un ACL per i documenti. Le informazioni ACL vengono utilizzate per filtrare i risultati della ricerca in base all'accesso dell'utente o del relativo gruppo ai documenti. Per ulteriori informazioni, consulta Filtraggio del contesto utente.
- Mappature dei campi: scegli di mappare i campi delle sorgenti Amazon RDS (PostgreSQL) dati ai campi indice. Amazon Kendra Per ulteriori informazioni, consulta la sezione Mappatura dei campi di origine dei dati.

> **Note**
>
> Il campo del corpo del documento o l'equivalente del corpo del documento per i documenti è necessario per Amazon Kendra eseguire la ricerca nei documenti. È necessario mappare il nome del campo del corpo del documento nella fonte dati al nome del campo indice_`document_body`. Tutti gli altri campi sono facoltativi.

Per un elenco di altre importanti chiavi JSON da configurare, consultaAmazon RDS Schema del modello (PostgreSQL).

Note

- Le righe del database eliminate non verranno registrate durante la Amazon Kendra verifica della presenza di contenuti aggiornati.
- La dimensione dei nomi e dei valori dei campi in una riga del database non può superare i 400 KB.
- Se l'origine dati del database contiene una grande quantità di dati e non desideri Amazon Kendra indicizzare tutto il contenuto del database dopo la prima sincronizzazione, puoi scegliere di sincronizzare solo i documenti nuovi, modificati o eliminati.
- È consigliabile fornire credenziali Amazon Kendra di database di sola lettura.
- È consigliabile evitare di aggiungere tabelle con dati sensibili o informazioni personali identificabili (PII).

Amazon S3

Amazon S3 è un servizio di archiviazione di oggetti che archivia i dati come oggetti all'interno di bucket. Puoi usarlo Amazon Kendra per indicizzare il tuo archivio di documenti Amazon S3 bucket.

Warning

Amazon Kendra non utilizza una policy bucket che concede le autorizzazioni a un Amazon Kendra principale per interagire con un bucket S3. Utilizza invece i ruoli. IAM Assicurati che Amazon Kendra non sia incluso come membro fidato nella tua bucket policy per evitare problemi di sicurezza dei dati derivanti dalla concessione accidentale di autorizzazioni a responsabili arbitrari. Tuttavia, puoi aggiungere una policy sui bucket per utilizzare un bucket su account diversi. Amazon S3 Per ulteriori informazioni, consulta Politiche da utilizzare Amazon S3 tra gli account (nella scheda IAM Ruoli di S3, sotto IAM Ruoli per le fonti di dati). Per informazioni sui IAM ruoli per le fonti di dati S3, consulta IAM ruoli.

Note

Amazon Kendra ora supporta un connettore aggiornato Amazon S3 .

La console è stata aggiornata automaticamente per te. Tutti i nuovi connettori creati nella console utilizzeranno l'architettura aggiornata. Se utilizzi l'API, ora devi utilizzare l'TemplateConfigurationoggetto anziché l'`S3DataSourceConfiguration`oggetto per configurare il connettore.
I connettori configurati utilizzando la console e l'architettura API precedenti continueranno a funzionare come configurato. Tuttavia, non potrai modificarli o aggiornarli. Se desideri modificare o aggiornare la configurazione del connettore, devi creare un nuovo connettore. Ti consigliamo di migrare il flusso di lavoro del connettore alla versione aggiornata. La fine del supporto per i connettori configurati utilizzando l'architettura precedente è prevista entro giugno 2024.

Puoi connetterti alla tua fonte di Amazon S3 dati utilizzando la Amazon Kendra console o l'TemplateConfigurationAPI.

> **Note**
>
> Per generare un rapporto sullo stato della sincronizzazione per l'origine Amazon S3 dati, consulta Risoluzione dei problemi relativi alle origini dati.

Per la risoluzione dei problemi del connettore di origine dati Amazon Kendra S3, consultaRisoluzione dei problemi relativi alle origini dati.

Argomenti

- Funzionalità supportate
- Prerequisiti
- Istruzioni di connessione
- Creazione di una fonte di dati Amazon S3
- Amazon S3 metadati del documento
- Controllo degli accessi per le fonti di Amazon S3 dati
- Utilizzo Amazon VPC con una fonte di Amazon S3 dati

Funzionalità supportate

- Mappature dei campi

- Filtraggio del contesto utente
- Filtri di inclusione/esclusione
- Sincronizzazione completa e incrementale dei contenuti
- Virtual Private Cloud (VPC) (Cloud privato virtuale (VPC)

Prerequisiti

Prima di poterla utilizzare Amazon Kendra per indicizzare la tua fonte di dati S3, apporta queste modifiche a S3 e agli account. AWS

In S3, assicurati di avere:

- Hai copiato il nome del tuo Amazon S3 bucket.

> **Note**
>
> Il bucket deve trovarsi nella stessa area dell' Amazon Kendra indice e l'indice deve disporre dell'autorizzazione ad accedere al bucket che contiene i documenti.

- Selezionato, ogni documento è unico in S3 e tra le altre fonti di dati che intendi utilizzare per lo stesso indice. Ogni fonte di dati che desideri utilizzare per un indice non deve contenere lo stesso documento in tutte le fonti di dati. Gli ID dei documenti sono globali rispetto a un indice e devono essere univoci per indice.

Nel tuo AWS account, assicurati di avere:

- Hai creato un Amazon Kendra indice e, se utilizzi l'API, hai annotato l'ID dell'indice.
- Hai creato un IAM ruolo per la tua origine dati e, se utilizzi l'API, hai annotato l'ARN del IAM ruolo.

Se non disponi di un IAM ruolo esistente, puoi utilizzare la console per creare un nuovo IAM ruolo quando connetti l'origine dati S3 a. Amazon Kendra Se utilizzi l'API, devi fornire l'ARN di un IAM ruolo esistente e un ID di indice.

Istruzioni di connessione

Per connetterti Amazon Kendra alla tua fonte dati S3, devi fornire i dettagli necessari della tua origine dati S3 in modo che Amazon Kendra possa accedere ai tuoi dati. Se non hai ancora configurato S3 per Amazon Kendra, consulta. Prerequisiti

Console

Per connettersi Amazon Kendra a Amazon S3

1. Accedi a AWS Management Console e apri la Amazon Kendra console.
2. Dal riquadro di navigazione a sinistra, scegli Indici, quindi scegli l'indice che desideri utilizzare dall'elenco degli indici.

> **Note**
>
> Puoi scegliere di configurare o modificare le impostazioni del controllo dell'accesso degli utenti in Impostazioni dell'indice.

3. Nella pagina Guida introduttiva, scegli Aggiungi origine dati.
4. Nella pagina Aggiungi origine dati, scegli Connettore S3, quindi scegli Aggiungi connettore.
5. Nella pagina Specificare i dettagli dell'origine dati, inserisci le seguenti informazioni:
   a. In Nome e descrizione, per Nome dell'origine dati, inserisci un nome per l'origine dati. Puoi includere trattini ma non spazi.
   b. (Facoltativo) Descrizione: immetti una descrizione facoltativa per la tua fonte di dati.
   c. In Lingua predefinita: scegli una lingua per filtrare i documenti per l'indice. Se non diversamente specificato, la lingua predefinita è l'inglese. La lingua specificata nei metadati del documento ha la precedenza sulla lingua selezionata.
   d. In Tag, per Aggiungi nuovo tag, includi tag opzionali per cercare e filtrare le risorse o tenere traccia dei costi. AWS
   e. Seleziona Successivo.
6. Nella pagina Definisci accesso e sicurezza, inserisci le seguenti informazioni opzionali:
   a. IAM ruolo: scegli un IAM ruolo esistente o creane uno nuovo IAM per accedere alle credenziali del repository e indicizzare il contenuto.

> **Note**
>
> IAM i ruoli utilizzati per gli indici non possono essere utilizzati per le fonti di dati. Se non sei sicuro che un ruolo esistente venga utilizzato per un indice o una FAQ, scegli Crea un nuovo ruolo per evitare errori.

b. Virtual Private Cloud (VPC): puoi scegliere di utilizzare un Amazon VPC nel tuo Amazon S3 bucket se non è accessibile dalla rete Internet pubblica. In tal caso, è necessario aggiungere sottoreti e gruppi di sicurezza. Amazon VPC

> **Important**
>
> Assicurati di avere:
>
> - Hai aggiunto un Amazon S3 endpoint al tuo Amazon VPC secondo la procedura descritta in Gateway endpoints for. Amazon S3
> - Hai scelto una sottorete privata in una zona di disponibilità Amazon Kendra supportata. Per maggiori dettagli, consulta Configurazione Amazon KendraAmazon VPC per l'uso di an.
> - Hai configurato il tuo gruppo di sicurezza per consentire l'accesso Amazon Kendra all' Amazon S3 endpoint. Vedi Configurazione Amazon Kendra per l'uso Amazon VPC per maggiori dettagli.

c. Seleziona Successivo.

7. Nella pagina Configura le impostazioni di sincronizzazione, inserisci le seguenti informazioni:

   a. Nell'ambito di sincronizzazione, per Posizione dell'origine dei dati: il percorso del Amazon S3 bucket in cui sono archiviati i dati. Seleziona Browse S3 per scegliere il tuo bucket.

   b. (Facoltativo) Posizione della cartella del prefisso dei file di metadati: il percorso della cartella in cui sono archiviati i metadati. Seleziona Browse S3 per individuare la cartella dei metadati.

   c. (Facoltativo) Posizione del file di configurazione dell'elenco di controllo degli accessi: il percorso della posizione di un file contenente una struttura JSON che specifica le impostazioni di accesso per i file archiviati nell'origine dati S3. Seleziona Browse S3 per individuare il tuo file ACL.

d. (Facoltativo) Seleziona la chiave di decrittografia: seleziona per utilizzare una chiave di decrittografia. È possibile scegliere di utilizzare una chiave esistente. AWS KMS

e. (Facoltativo) In Configurazione aggiuntiva, per Patterns: aggiungi modelli per includere o escludere documenti dall'indice. Tutti i percorsi sono relativi alla posizione dell'origine dati nel bucket S3. Puoi aggiungere fino a 100 pattern.

f. Modalità di sincronizzazione: scegli come aggiornare l'indice quando il contenuto dell'origine dati cambia. Quando sincronizzi l'origine dati con Amazon Kendra per la prima volta, tutto il contenuto viene sottoposto a scansione e indicizzato per impostazione predefinita. Se la sincronizzazione iniziale non è riuscita, devi eseguire una sincronizzazione completa dei dati, anche se non scegli la sincronizzazione completa come opzione della modalità di sincronizzazione.

   - Sincronizzazione completa: indicizza di nuovo tutti i contenuti, sostituendo i contenuti esistenti ogni volta che l'origine dati si sincronizza con l'indice.
   - Sincronizzazione nuova, modificata ed eliminata: indicizza solo i contenuti nuovi, modificati ed eliminati ogni volta che l'origine dati si sincronizza con l'indice. Amazon Kendra può utilizzare il meccanismo dell'origine dati per tenere traccia delle modifiche ai contenuti e indicizzare i contenuti modificati dall'ultima sincronizzazione.

g. Nella pianificazione di esecuzione della sincronizzazione, per Frequenza: scegli la frequenza con cui eseguire Amazon Kendra la sincronizzazione con la tua fonte di dati.

h. Seleziona Successivo.

8. Nella pagina Imposta mappature dei campi, inserisci le seguenti informazioni opzionali:

   a. Mappatura dei campi S3: seleziona tra i campi di origine dati predefiniti Amazon Kendra generati che desideri mappare all'indice.

   b. Aggiungi campo: scegli di aggiungere campi di origine dati personalizzati per creare un nome di campo indice a cui mappare e il tipo di dati del campo.

   c. Seleziona Successivo.

9. Nella pagina Rivedi e crea, verifica che le informazioni inserite siano corrette, quindi seleziona Aggiungi origine dati. Puoi anche scegliere di modificare le tue informazioni da questa pagina. L'origine dati verrà visualizzata nella pagina Origini dati dopo che l'origine dati sarà stata aggiunta correttamente.

API

Per connettersi Amazon Kendra a Amazon S3

È necessario specificare un codice JSON dello schema dell'origine dati utilizzando l'TemplateConfigurationAPI. È necessario fornire le seguenti informazioni:

- BucketName—Il nome del bucket che contiene i documenti.
- Modalità di sincronizzazione: specifica come Amazon Kendra aggiornare l'indice quando il contenuto dell'origine dati cambia. Quando sincronizzi l'origine dati con Amazon Kendra per la prima volta, tutto il contenuto viene sottoposto a scansione e indicizzato per impostazione predefinita. Se la sincronizzazione iniziale non è riuscita, devi eseguire una sincronizzazione completa dei dati, anche se non scegli la sincronizzazione completa come opzione della modalità di sincronizzazione. Puoi scegliere tra:
  - `FORCED_FULL_CRAWL`per indicizzare nuovamente tutti i contenuti, sostituendo i contenuti esistenti ogni volta che l'origine dati si sincronizza con l'indice.
  - `FULL_CRAWL`per indicizzare solo i contenuti nuovi, modificati ed eliminati ogni volta che l'origine dati si sincronizza con l'indice. Amazon Kendra può utilizzare il meccanismo dell'origine dati per tenere traccia delle modifiche ai contenuti e indicizzare i contenuti modificati dall'ultima sincronizzazione.
- IAM ruolo: specifica `RoleArn` quando chiami `CreateDataSource` per fornire a un IAM ruolo le autorizzazioni per accedere al tuo account Secrets Manager segreto e per chiamare le API pubbliche richieste per il connettore S3 e. Amazon Kendra Per ulteriori informazioni, consulta i IAM ruoli per le fonti di dati S3.

Puoi anche aggiungere le seguenti funzionalità opzionali:

- Virtual Private Cloud (VPC): `VpcConfiguration` specifica quando si chiama. `CreateDataSource` Per ulteriori informazioni, consulta Configurazione Amazon Kendra per l'utilizzo di un Amazon VPC.
- Filtri di inclusione ed esclusione: specificano se includere o escludere determinati nomi di file, tipi di file e percorsi di file. Si utilizzano modelli a globo (modelli che possono espandere un pattern di caratteri jolly in un elenco di nomi di percorso che corrispondono al modello specificato). Per esempi, consulta Use of Exclude and Include Filters nel riferimento ai comandi AWS CLI.

- Configurazione dei metadati del documento: aggiunge file di metadati del documento che contengono informazioni come le informazioni sul controllo dell'accesso al documento, l'URI di origine, l'autore del documento e gli attributi personalizzati. Ogni file di metadati contiene metadati relativi a un singolo documento.
- Mappature dei campi: scegli di mappare i campi delle sorgenti dati S3 ai campi indice. Amazon Kendra Per ulteriori informazioni, consulta la sezione Mappatura dei campi di origine dei dati.

> **Note**
>
> Il campo del corpo del documento o l'equivalente del corpo del documento per i documenti è necessario per Amazon Kendra eseguire la ricerca nei documenti. È necessario mappare il nome del campo del corpo del documento nella fonte dati al nome del campo indice_`document_body`. Tutti gli altri campi sono facoltativi.

Per un elenco di altre importanti chiavi JSON da configurare, consultaAmazon S3 schema modello.

Ulteriori informazioni

Per saperne di più sull'integrazione Amazon Kendra con la tua fonte di dati S3, consulta:

- Cerca risposte accurate utilizzando Amazon Kendra S3 Connector con supporto VPC

Creazione di una fonte di dati Amazon S3

Gli esempi seguenti illustrano la creazione di un'origine Amazon S3 dati. Gli esempi presuppongono che siano già stati creati un indice e un IAM ruolo con l'autorizzazione a leggere i dati dall'indice. Per ulteriori informazioni sul IAM ruolo, vedi ruoli di IAM accesso. Per ulteriori informazioni sulla creazione di un indice, vedere Creazione di un indice.

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

Il seguente frammento di codice Python crea una fonte di dati. Amazon S3 Per l'esempio completo, vedi. Nozioni di base (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
    )
```

La creazione dell'origine dati può richiedere del tempo. Puoi monitorare i progressi utilizzando l'DescribeDataSourceAPI. Quando lo stato dell'origine dati è impostatoACTIVE, l'origine dati è pronta per l'uso.

Gli esempi seguenti mostrano come ottenere lo stato di un'origine dati.

CLI

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

Python

Il seguente frammento di codice Python ottiene informazioni su una fonte di dati S3. Per l'esempio completo, vedi. Nozioni di base (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
```

Questa fonte di dati non ha una pianificazione, quindi non viene eseguita automaticamente. Per indicizzare l'origine dati, si chiama StartDataSourceSyncJobper sincronizzare l'indice con l'origine dati.

Gli esempi seguenti mostrano la sincronizzazione di un'origine dati.

CLI

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

Python

Il seguente frammento di codice Python sincronizza un'origine dati. Amazon S3 Per l'esempio completo, vedi. Nozioni di base (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 metadati del documento

È possibile aggiungere metadati, informazioni aggiuntive su un documento, ai documenti contenuti in un Amazon S3 bucket utilizzando un file di metadati. Ogni file di metadati è associato a un documento indicizzato.

I file di metadati devono essere archiviati nello stesso bucket dei file indicizzati. Puoi specificare una posizione all'interno del bucket per i tuoi file di metadati utilizzando la console o il `S3Prefix` campo del `DocumentsMetadataConfiguration` parametro quando crei un'origine dati. Amazon S3 Se non specificate un Amazon S3 prefisso, i file di metadati devono essere archiviati nella stessa posizione dei documenti indicizzati.

Se specificate un Amazon S3 prefisso per i file di metadati, questi si trovano in una struttura di directory parallela ai documenti indicizzati. Amazon Kendra cerca i tuoi metadati solo nella directory specificata. Se i metadati non vengono letti, verifica che la posizione della directory corrisponda alla posizione dei metadati.

Gli esempi seguenti mostrano come la posizione del documento indicizzato sia mappata alla posizione del file di metadati. Nota che la Amazon S3 chiave del documento viene aggiunta al Amazon S3 prefisso dei metadati e quindi dotata del suffisso per formare il percorso del file di metadati `.metadata.json`. Amazon S3 La Amazon S3 chiave combinata, con il Amazon S3 prefisso e il `.metadata.json` suffisso dei metadati, non deve superare un totale di 1024 caratteri. Si consiglia di mantenere la Amazon S3 chiave al di sotto dei 1000 caratteri per tenere conto dei caratteri aggiuntivi quando si combina la chiave con il prefisso e il suffisso.

```
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
```

I metadati del documento sono definiti in un file JSON. Il file deve essere un file di testo UTF-8 senza un marcatore BOM. Il nome del file JSON deve essere. `<document>.<extension>.metadata.json` In questo esempio, «documento» è il nome del documento a cui si applicano i metadati e «estensione» è l'estensione del file del documento. L'ID del documento deve essere univoco in`<document>.<extension>.metadata.json`.

Il contenuto del file JSON segue questo modello. Tutti gli attributi/campi sono opzionali, quindi non è necessario includere tutti gli attributi. È necessario fornire un valore per ogni attributo che si desidera includere; il valore non può essere vuoto. Se non specifichi il`_source_uri`, i link restituiti da Amazon Kendra nei risultati della ricerca rimandano al Amazon S3 bucket che contiene il documento. `DocumentId`è mappato sul campo `s3_document_id` ed è il percorso assoluto del documento in 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."
}
```

I campi `_created_at` e `_last_updated_at` i metadati sono date codificate ISO 8601. Ad esempio, 2012-03-25T 12:30:10 + 01:00 è il formato data-ora ISO 8601 per il 25 marzo 2012 alle 12:30 (più 10 secondi) nel fuso orario dell'Europa centrale.

È possibile aggiungere informazioni aggiuntive al `Attributes` campo relativo a un documento utilizzato per filtrare le interrogazioni o raggruppare le risposte alle interrogazioni. Per ulteriori informazioni, consulta Creazione di campi di documento personalizzati.

È possibile utilizzare il `AccessControlList` campo per filtrare la risposta di una query. In questo modo, solo determinati utenti e gruppi hanno accesso ai documenti. Per ulteriori informazioni, consulta Filtraggio in base al contesto dell'utente.

Controllo degli accessi per le fonti di Amazon S3 dati

È possibile controllare l'accesso ai documenti in un'origine Amazon S3 dati utilizzando un file di configurazione. Il file viene specificato nella console o come `AccessControlListConfiguration` parametro quando si chiama l'UpdateDataSourceAPI CreateDataSourceo.

Il file di configurazione contiene una struttura JSON che identifica un prefisso S3 ed elenca le impostazioni di accesso per il prefisso. Il prefisso può essere un percorso o un singolo file. Se il prefisso è un percorso, le impostazioni di accesso si applicano a tutti i file in quel percorso. Esiste un numero massimo di prefissi S3 nel file di configurazione JSON e una dimensione massima predefinita del file. Per ulteriori informazioni, consulta Quote per Amazon Kendra

È possibile specificare sia utenti che gruppi nelle impostazioni di accesso. Quando si esegue una query sull'indice, si specificano le informazioni sull'utente e sul gruppo. Per ulteriori informazioni, consulta Filtraggio per attributo utente.

La struttura JSON per il file di configurazione deve avere il seguente formato:

```
[
```

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

Utilizzo Amazon VPC con una fonte di Amazon S3 dati

Questo argomento fornisce un step-by-step esempio che mostra come connettersi a un bucket Amazon S3 utilizzando un connettore Amazon S3 tramite Amazon VPC. L'esempio presuppone che tu stia iniziando con un bucket S3 esistente. Ti consigliamo di caricare solo alcuni documenti nel tuo bucket S3 per testare l'esempio.

Puoi connetterti Amazon Kendra al tuo Amazon S3 bucket tramite. Amazon VPC A tale scopo, è necessario specificare la Amazon VPC sottorete e i gruppi Amazon VPC di sicurezza durante la creazione del connettore di origine Amazon S3 dati.

> **Important**
>
> Affinché un Amazon Kendra Amazon S3 connettore possa accedere al tuo Amazon S3 bucket, assicurati di aver assegnato un Amazon S3 endpoint al tuo cloud privato virtuale (VPC).

Per Amazon Kendra sincronizzare i documenti dal tuo Amazon S3 bucket Amazon VPC, devi completare i seguenti passaggi:

- Configura un Amazon S3 endpoint per. Amazon VPCPer ulteriori informazioni su come configurare un Amazon S3 endpoint, consulta la sezione dedicata agli endpoint Gateway Amazon S3 nella Guida.AWS PrivateLink
- (Facoltativo) Hai verificato le policy del Amazon S3 bucket per assicurarti che il Amazon S3 bucket sia accessibile dal cloud privato virtuale (VPC) a cui lo hai assegnato. Amazon KendraPer ulteriori informazioni, consulta Controllare l'accesso dagli endpoint VPC con le policy dei bucket nella Guida per l'utente di Amazon S3

Fasi

- Fase 1: configurare un Amazon VPC
- (Facoltativo) Fase 2: Configurazione della policy sui bucket Amazon S3
- Passaggio 3: creare un connettore per l'origine dei dati di test Amazon S3

Fase 1: configurare un Amazon VPC

Crea una rete VPC che include una sottorete privata con un endpoint Amazon S3 gateway e un gruppo di sicurezza da utilizzare in seguito. Amazon Kendra

Per configurare un VPC con una sottorete privata, un endpoint S3 e un gruppo di sicurezza

1. Accedi a AWS Management Console e apri la console all'indirizzo. Amazon VPC https://console.aws.amazon.com/vpc/
2. Crea un VPC con una sottorete privata e un endpoint S3 da utilizzare: Amazon Kendra

Dal pannello di navigazione, scegli I tuoi VPC, quindi scegli Crea VPC.

a. Per Risorse da creare, scegli VPC e altro.
b. Per il tag Nome, abilita la generazione automatica, quindi inserisci. **`kendra-s3-example`**
c. Per il blocco CIDR IPv4/IPv6, mantieni i valori predefiniti.
d. Per Numero di zone di disponibilità (AZ), scegli il numero 1.
e. Seleziona Personalizza AZ, quindi seleziona una zona di disponibilità dall'elenco delle prime zone di disponibilità.

   Amazon Kendra supporta solo un set specifico di zone di disponibilità.
f. Per Numero di sottoreti pubbliche, scegli il numero 0.
g. Per Numero di sottoreti private, scegli il numero 1.
h. Per NAT gateways (Gateway NAT), scegli None (Nessuno).
i. Per gli endpoint VPC, scegli gateway.Amazon S3 .
j. Lascia il resto dei valori con le impostazioni predefinite.
k. Seleziona Create VPC (Crea VPC).

   Attendi il completamento del flusso di lavoro Create VPC. Quindi, scegli Visualizza VPC per controllare il VPC che hai appena creato.

Ora hai creato una rete VPC con una sottorete privata, che non ha accesso alla rete Internet pubblica.

3. Copia l'ID dell'endpoint VPC del tuo endpoint Amazon S3:

   a. Nel riquadro di navigazione scegli Endpoint.
   b. Nell'elenco degli endpoint, trova l'`kendra-s3-example-vpce-s3`endpoint Amazon S3 che hai appena creato insieme al tuo VPC.
   c. Prendi nota dell'ID dell'endpoint VPC.

   Ora hai creato un endpoint gateway Amazon S3 per accedere al tuo bucket Amazon S3 tramite una sottorete.

4. Crea un gruppo di sicurezza da utilizzare: Amazon Kendra

a. Dal riquadro di navigazione, scegli Gruppi di sicurezza, quindi seleziona Crea gruppo di sicurezza.
b. In Security group name (Nome gruppo di sicurezza) immettere **`s3-data-source-security-group`**.
c. Scegli il tuo VPC dall'Amazon VPCelenco.
d. Lascia le regole in entrata e le regole in uscita come impostazioni predefinite.
e. Scegliere Create Security Group (Crea gruppo di sicurezza).

Ora hai creato un gruppo di sicurezza VPC.

Assegni la sottorete e il gruppo di sicurezza che hai creato al connettore di origine dati Amazon S3 durante il processo di configurazione del connettore. Amazon Kendra

(Facoltativo) Fase 2: Configurazione della policy sui bucket Amazon S3

In questo passaggio facoltativo, scopri come configurare una policy per i bucket Amazon S3 in modo che il tuo bucket Amazon S3 sia accessibile solo dal VPC a cui lo assegni. Amazon Kendra

Amazon Kendra utilizza i ruoli IAM per accedere al tuo bucket Amazon S3 e non richiede la configurazione di una policy per i bucket Amazon S3. Tuttavia, potresti trovare utile creare una policy sui bucket se desideri configurare un Amazon S3 connettore utilizzando un bucket Amazon S3 con politiche esistenti che limitano l'accesso ad esso dalla rete Internet pubblica.

Per configurare la tua policy sui bucket Amazon S3

1. Apri la console Amazon S3 all'indirizzo. https://console.aws.amazon.com/s3/
2. Dal pannello di navigazione, scegli Bucket.
3. Scegli il nome del bucket Amazon S3 con cui desideri effettuare la sincronizzazione. Amazon Kendra
4. Scegli la scheda Autorizzazioni, scorri verso il basso fino alla policy Bucket, quindi fai clic su Modifica.
5. Aggiungi o modifica la tua policy sui bucket per consentire l'accesso solo dall'endpoint VPC che hai creato.

   Di seguito è riportato un esempio di policy di bucket. Sostituisci *`bucket-name`*e *`vpce-id`*con il nome del bucket Amazon S3 e l'ID endpoint Amazon S3 che hai annotato in precedenza.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Principal": "*",
      "Action": "s3:*",
      "Resource": "arn:aws:s3:::bucket-name/*",
      "Condition": {
        "StringNotEquals": {
          "aws:SourceVpce": "vpce-id"
        }
      }
    }
  ]
}
```

6. Seleziona Salva modifiche.

Il tuo bucket S3 è ora accessibile solo dal VPC specifico che hai creato.

Passaggio 3: creare un connettore per l'origine dei dati di test Amazon S3

Per testare la tua Amazon VPC configurazione, crea un Amazon S3 connettore. Quindi, configuralo con il VPC che hai creato seguendo i passaggi descritti in. Amazon S3

Per i valori di Amazon VPC configurazione, scegli i valori che hai creato durante questo esempio:

- Amazon VPC(VPC) — `kendra-s3-example-vpc`
- Sottoreti — `kendra-s3-example-subnet-private1-[availability zone]`
- Gruppi di sicurezza: `s3-data-source-security-group`

Attendi che il connettore finisca di creare. Dopo aver creato il Amazon S3 connettore, scegli Sincronizza ora per avviare una sincronizzazione.

Il completamento della sincronizzazione potrebbe richiedere da alcuni minuti a diverse ore, a seconda del numero di documenti presenti nel Amazon S3 bucket. Per testare l'esempio, ti consigliamo di caricare solo alcuni documenti nel tuo bucket S3. Se la configurazione è corretta, alla fine dovresti vedere lo stato di sincronizzazione impostato su Completato.

In caso di errori, consulta Risoluzione dei problemi di Amazon VPC connessione.

Amazon Kendra Web crawler

È possibile utilizzare Amazon Kendra Web Crawler per eseguire la scansione e indicizzare le pagine Web.

È possibile eseguire la scansione solo di siti Web pubblici o siti Web interni all'azienda che utilizzano il protocollo di comunicazione sicuro Hypertext Transfer Protocol Secure (HTTPS). Se ricevi un errore durante la ricerca per indicizzazione di un sito Web, è possibile che il sito Web non sia in grado di eseguire la ricerca per indicizzazione. Per eseguire la scansione dei siti Web interni, è possibile configurare un proxy Web. Il proxy web deve essere rivolto al pubblico. Puoi anche utilizzare l'autenticazione per accedere e scansionare i siti Web.

Quando selezioni i siti Web da indicizzare, devi rispettare la Policy di uso accettabile di Amazon e tutti gli altri termini di Amazon. Ricorda che devi utilizzare Amazon Kendra Web Crawler solo per indicizzare le tue pagine Web o le pagine Web che hai l'autorizzazione a indicizzare. Per informazioni su come impedire a Amazon Kendra Web Crawler di indicizzare i tuoi siti Web, consulta. Configurazione del file per Web Crawler *robots.txt*Amazon Kendra

> **Note**
>
> L'uso improprio di Amazon Kendra Web Crawler per eseguire una scansione aggressiva di siti Web o pagine Web di cui non sei proprietario non è considerato un uso accettabile.

Amazon Kendra dispone di due versioni del connettore. web crawler Le funzionalità supportate di ogni versione includono:

Amazon Kendra Connettore Web Crawler v1.0/API WebCrawlerConfiguration

- Proxy Web
- Filtri di inclusione/esclusione

Amazon Kendra Connettore Web Crawler v2.0 /API TemplateConfiguration

- Mappature dei campi
- Filtri di inclusione/esclusione

- Sincronizzazione completa e incrementale dei contenuti
- Proxy Web
- Autenticazione di base, NTLM/Kerberos, SAML e basata su moduli per i tuoi siti Web
- Virtual Private Cloud (VPC) (Cloud privato virtuale (VPC)

> **Important**
>
> La creazione di connettori Web Crawler v2.0 non è supportata da. AWS CloudFormation Utilizza il connettore Web Crawler v1.0 se hai bisogno di assistenza. AWS CloudFormation

Per la risoluzione dei problemi relativi al connettore di origine dati del crawler Amazon Kendra Web, consulta. Risoluzione dei problemi relativi alle origini dati

Argomenti

- Amazon Kendra Connettore Web Crawler v1.0
- Amazon Kendra Connettore Web Crawler v2.0
- Configurazione del file per Web Crawler robots.txtAmazon Kendra

Amazon Kendra Connettore Web Crawler v1.0

È possibile utilizzare Amazon Kendra Web Crawler per eseguire la scansione e indicizzare le pagine Web.

È possibile eseguire la scansione solo di siti Web pubblici e siti Web che utilizzano il protocollo di comunicazione sicuro Hypertext Transfer Protocol Secure (HTTPS). Se ricevi un errore durante la ricerca per indicizzazione di un sito Web, è possibile che il sito Web non sia in grado di eseguire la ricerca per indicizzazione. Per eseguire la scansione dei siti Web interni, è possibile configurare un proxy Web. Il proxy web deve essere rivolto al pubblico.

Quando selezioni i siti Web da indicizzare, devi rispettare la Policy di uso accettabile di Amazon e tutti gli altri termini di Amazon. Ricorda che devi utilizzare Amazon Kendra Web Crawler solo per indicizzare le tue pagine Web o le pagine Web che hai l'autorizzazione a indicizzare. Per informazioni su come impedire a Amazon Kendra Web Crawler di indicizzare i tuoi siti Web, consulta. Configurazione del file per Web Crawler *robots.txt*Amazon Kendra

> **Note**
>
> L'uso improprio di Amazon Kendra Web Crawler per eseguire una scansione aggressiva di siti Web o pagine Web di cui non sei proprietario non è considerato un uso accettabile.

Per la risoluzione dei problemi relativi al connettore di origine dati del crawler Amazon Kendra Web, consulta. Risoluzione dei problemi relativi alle origini dati

Argomenti

Funzionalità supportate

- Proxy Web
- Filtri di inclusione/esclusione

Prerequisiti

Prima di utilizzarli Amazon Kendra per indicizzare i tuoi siti web, controlla i dettagli dei tuoi siti web e dei tuoi account. AWS

Per i tuoi siti Web, assicurati di disporre di:

- Hai copiato gli URL iniziali o della mappa del sito web che desideri indicizzare.
- Per i siti Web che richiedono l'autenticazione di base: annota il nome utente e la password e copia il nome host del sito Web e il numero di porta.
- Facoltativo: ha copiato il nome host del sito Web e il numero di porta se si desidera utilizzare un proxy Web per connettersi ai siti Web interni di cui si desidera eseguire la scansione. Il proxy web deve essere rivolto al pubblico. Amazon Kendra supporta la connessione a server proxy Web supportati da un'autenticazione di base oppure è possibile connettersi senza autenticazione.
- Selezionato, ogni documento di pagina Web che desideri indicizzare è unico e tra le altre fonti di dati che intendi utilizzare per lo stesso indice. Ogni fonte di dati che desideri utilizzare per un indice

non deve contenere lo stesso documento in tutte le fonti di dati. Gli ID dei documenti sono globali rispetto a un indice e devono essere univoci per indice.

Nel tuo AWS account, assicurati di avere:

- Hai creato un Amazon Kendra indice e, se utilizzi l'API, hai annotato l'ID dell'indice.
- Hai creato un IAM ruolo per la tua origine dati e, se utilizzi l'API, hai annotato l'ARN del IAM ruolo.

> **Note**
>
> Se modifichi il tipo di autenticazione e le credenziali, devi aggiornare il IAM ruolo per accedere all'ID AWS Secrets Manager segreto corretto.

- Per i siti Web che richiedono l'autenticazione o se utilizzano un proxy Web con autenticazione, memorizzate le credenziali di autenticazione in un AWS Secrets Manager luogo segreto e, se utilizzate l'API, annotate l'ARN del segreto.

> **Note**
>
> Ti consigliamo di aggiornare o ruotare regolarmente le credenziali e il segreto. Fornisci solo il livello di accesso necessario per la tua sicurezza. Non è consigliabile riutilizzare credenziali e segreti tra diverse fonti di dati e nelle versioni 1.0 e 2.0 dei connettori (ove applicabile).

Se non disponi di un IAM ruolo o di un segreto esistente, puoi utilizzare la console per creare un nuovo IAM ruolo e un Secrets Manager segreto quando connetti la tua origine web crawler dati a. Amazon Kendra Se utilizzi l'API, devi fornire l'ARN di un IAM ruolo e di un Secrets Manager segreto esistenti e un ID di indice.

Istruzioni di connessione

Per connetterti Amazon Kendra alla tua fonte di web crawler dati, devi fornire i dettagli necessari della tua origine web crawler dati in modo che Amazon Kendra possa accedere ai tuoi dati. Se non hai ancora configurato web crawler Amazon Kendra SeePrerequisiti.

Console

Per connettersi Amazon Kendra a web crawler

1. Accedi a AWS Management Console e apri la Amazon Kendra console.
2. Dal riquadro di navigazione a sinistra, scegli Indici, quindi scegli l'indice che desideri utilizzare dall'elenco degli indici.

   > **Note**
   >
   > Puoi scegliere di configurare o modificare le impostazioni del controllo dell'accesso degli utenti in Impostazioni dell'indice.

3. Nella pagina Guida introduttiva, scegli Aggiungi origine dati.
4. Nella pagina Aggiungi origine dati, scegli connettore web crawler, quindi scegli Aggiungi connettore.
5. Nella pagina Specificare i dettagli dell'origine dati, inserisci le seguenti informazioni:

   a. In Nome e descrizione, per Nome dell'origine dati, inserisci un nome per l'origine dati. Puoi includere trattini ma non spazi.

   b. (Facoltativo) Descrizione: immetti una descrizione facoltativa per la tua fonte di dati.

   c. In Lingua predefinita: scegli una lingua per filtrare i documenti per l'indice. Se non diversamente specificato, la lingua predefinita è l'inglese. La lingua specificata nei metadati del documento ha la precedenza sulla lingua selezionata.

   d. In Tag, per Aggiungi nuovo tag, includi tag opzionali per cercare e filtrare le risorse o tenere traccia dei costi. AWS

   e. Seleziona Successivo.

6. Nella pagina Definisci accesso e sicurezza, inserisci le seguenti informazioni:

   a. Per Source, scegli tra URL di origine e Sitemap di origine a seconda del caso d'uso e inserisci i valori per ciascuna di esse.

      Puoi aggiungere fino a 10 URL di origine e tre Sitemap.

      > **Note**
      >
      > Se desideri eseguire la scansione di una Sitemap, verifica che l'URL di base o principale sia lo stesso degli URL elencati nella pagina della Sitemap. Ad esempio, se l'URL della mappa del sito è https://example.com/sitemap-

page.html, anche gli URL elencati in questa pagina della mappa del sito devono utilizzare l'URL di base "». https://example.com/

b. (Facoltativo) Per il proxy Web, inserisci le seguenti informazioni:

   i. Nome host: il nome host in cui è richiesto il proxy Web.

   ii. Numero di porta: la porta utilizzata dal protocollo di trasporto degli URL dell'host. Il numero di porta deve essere un valore numerico compreso tra 0 e 65535.

   iii. Per le credenziali del proxy Web: se la connessione al proxy Web richiede l'autenticazione, scegli un segreto esistente o crea un nuovo segreto per archiviare le credenziali di autenticazione. Se scegli di creare un nuovo segreto, si apre una finestra AWS Secrets Manager segreta.

   iv. Inserisci le seguenti informazioni nella finestra Crea un AWS Secrets Manager Secrets Manager segreto:

      A. Nome segreto: un nome per il tuo segreto. Il prefisso 'AmazonKendra-WebCrawler-' viene aggiunto automaticamente al nome segreto.

      B. Per nome utente e password: inserisci queste credenziali di autenticazione di base per i tuoi siti Web.

      C. Selezionare Salva.

c. (Facoltativo) Host con autenticazione: selezionare questa opzione per aggiungere altri host con autenticazione.

d. IAM ruolo: scegli un IAM ruolo esistente o creane uno nuovo IAM per accedere alle credenziali del repository e indicizzare il contenuto.

> **Note**
>
> IAM i ruoli utilizzati per gli indici non possono essere utilizzati per le fonti di dati. Se non sei sicuro che un ruolo esistente venga utilizzato per un indice o una FAQ, scegli Crea un nuovo ruolo per evitare errori.

e. Seleziona Successivo.

7. Nella pagina Configura le impostazioni di sincronizzazione, inserisci le seguenti informazioni:

   a. Intervallo di scansione: scegli il tipo di pagine Web che desideri sottoporre a scansione.

b. Profondità di scansione: seleziona il numero di livelli dall'URL iniziale da sottoporre a scansione. Amazon Kendra

c. Le impostazioni di scansione avanzate e la configurazione aggiuntiva immettono le seguenti informazioni:

   i. Dimensione massima del file: la dimensione massima della pagina Web o degli allegati da sottoporre a scansione. Minimo 0,000001 MB (1 byte). Massimo 50 MB.

   ii. Numero massimo di link per pagina: il numero massimo di link sottoposti a scansione per pagina. I link vengono sottoposti a scansione in ordine di apparizione. Minimo 1 link/pagina. Massimo 1000 collegamenti/pagina.

   iii. Limitazione massima: il numero massimo di URL sottoposti a scansione per nome host al minuto. Minimo 1 URL/nome host/minuto. Massimo 300 URL/nome host/minuto.

   iv. Modelli Regex: aggiungono modelli di espressioni regolari per includere o escludere determinati URL. È possibile aggiungere fino a 100 pattern.

d. In Pianificazione di esecuzione della sincronizzazione, per Frequenza: scegli la frequenza di sincronizzazione con la tua fonte di dati. Amazon Kendra

e. Seleziona Successivo.

8. Nella pagina Rivedi e crea, verifica che le informazioni inserite siano corrette, quindi seleziona Aggiungi origine dati. Puoi anche scegliere di modificare le tue informazioni da questa pagina. L'origine dati verrà visualizzata nella pagina Origini dati dopo che l'origine dati sarà stata aggiunta correttamente.

API

Per connettersi Amazon Kendra a web crawler

È necessario specificare quanto segue utilizzando l'WebCrawlerConfigurationAPI:

- URL: specifica gli URL iniziali o del punto di partenza dei siti Web o gli URL della mappa del sito dei siti Web di cui desideri eseguire la scansione utilizzando and. SeedUrlConfigurationSiteMapsConfiguration

> **Note**
>
> Se desideri eseguire la scansione di una Sitemap, verifica che l'URL di base o principale sia lo stesso degli URL elencati nella pagina della mappa del sito. Ad

esempio, se l'URL della mappa del sito è https://example.com/sitemap-page.html, anche gli URL elencati in questa pagina della mappa del sito devono utilizzare l'URL di base "». https://example.com/

- Secret Amazon Resource Name (ARN): se un sito Web richiede l'autenticazione di base, fornisci il nome host, il numero di porta e un codice segreto che memorizza le credenziali di autenticazione di base del nome utente e della password. L'ARN segreto viene fornito utilizzando l'AuthenticationConfigurationAPI. Il segreto viene archiviato in una struttura JSON con le seguenti chiavi:

```
{
    "username": "user name",
    "password": "password"
}
```

  È inoltre possibile fornire le credenziali del proxy Web utilizzando un AWS Secrets Manager segreto. L'ProxyConfigurationAPI viene utilizzata per fornire il nome host e il numero di porta del sito Web e, facoltativamente, il codice segreto che memorizza le credenziali del proxy Web.
- IAM ruolo: specifica `RoleArn` quando chiami `CreateDataSource` per fornire a un IAM ruolo le autorizzazioni per accedere al tuo Secrets Manager segreto e per chiamare le API pubbliche richieste per il connettore del crawler Web e. Amazon Kendra Per ulteriori informazioni, consulta IAM Ruoli per le fonti di dati del web crawler.

Puoi anche aggiungere le seguenti funzionalità opzionali:

- Modalità di scansione: scegli se eseguire la scansione solo dei nomi host dei siti Web, dei nomi host con sottodomini o anche di altri domini a cui si collegano le pagine Web.
- La «profondità» o il numero di livelli dal livello iniziale alla scansione. Ad esempio, la pagina URL iniziale ha la profondità 1 e tutti i collegamenti ipertestuali di questa pagina che sono anch'essi sottoposti a scansione hanno la profondità 2.
- Il numero massimo di URL su una singola pagina Web da sottoporre a scansione.
- La dimensione massima in MB di una pagina Web da sottoporre a scansione.
- Il numero massimo di URL di cui viene eseguita la ricerca per indicizzazione per host di sito Web al minuto.
- L'host del proxy Web e il numero di porta a cui connettersi e sottoporre a scansione i siti Web interni. Ad esempio, il nome host di https://a.example.com/page1.htmlè "a.example.com" e

il numero di porta è 443, la porta standard per HTTPS. Se sono necessarie le credenziali del proxy Web per connettersi all'host di un sito Web, è possibile crearne una AWS Secrets Manager che memorizzi le credenziali.

- Le informazioni di autenticazione per accedere e scansionare i siti Web che richiedono l'autenticazione dell'utente.
- È possibile estrarre i meta tag HTML come campi utilizzando lo strumento Custom Document Enrichment. Per ulteriori informazioni, consulta la sezione Personalizzazione dei metadati del documento durante il processo di importazione. Per un esempio di estrazione dei meta tag HTML, consulta Esempi CDE.
- Filtri di inclusione ed esclusione: specificate se includere o escludere determinati URL.

> **Note**
>
> La maggior parte delle fonti di dati utilizza modelli di espressioni regolari, che sono modelli di inclusione o esclusione denominati filtri. Se si specifica un filtro di inclusione, viene indicizzato solo il contenuto che corrisponde al filtro di inclusione. Qualsiasi documento che non corrisponde al filtro di inclusione non viene indicizzato. Se si specifica un filtro di inclusione ed esclusione, i documenti che corrispondono al filtro di esclusione non vengono indicizzati, anche se corrispondono al filtro di inclusione.

Ulteriori informazioni

Per ulteriori informazioni sull'integrazione Amazon Kendra con la tua web crawler fonte di dati, consulta:

- Reimmagina la scoperta delle conoscenze utilizzando Web Amazon Kendra Crawler

Amazon Kendra Connettore Web Crawler v2.0

È possibile utilizzare Amazon Kendra Web Crawler per eseguire la scansione e indicizzare le pagine Web.

È possibile eseguire la scansione solo di siti Web pubblici o siti Web interni all'azienda che utilizzano il protocollo di comunicazione sicuro Hypertext Transfer Protocol Secure (HTTPS). Se ricevi un errore durante la ricerca per indicizzazione di un sito Web, è possibile che il sito Web non sia in grado di eseguire la ricerca per indicizzazione. Per eseguire la scansione dei siti Web interni, è

possibile configurare un proxy Web. Il proxy web deve essere rivolto al pubblico. Puoi anche utilizzare l'autenticazione per accedere e scansionare i siti Web.

Amazon Kendra Web Crawler v2.0 utilizza il pacchetto web crawler Selenium e un driver Chromium. Amazon Kendra aggiorna automaticamente la versione di Selenium e il driver Chromium utilizzando Continuous Integration (CI).

Quando selezioni i siti Web da indicizzare, devi rispettare la Policy di uso accettabile di Amazon e tutti gli altri termini di Amazon. Ricorda che devi utilizzare Amazon Kendra Web Crawler solo per indicizzare le tue pagine Web o le pagine Web che hai l'autorizzazione a indicizzare. Per informazioni su come impedire a Amazon Kendra Web Crawler di indicizzare i tuoi siti Web, consulta. Configurazione del file per Web Crawler *robots.txt*Amazon Kendra . L'uso improprio di Amazon Kendra Web Crawler per eseguire una scansione aggressiva di siti Web o pagine Web di cui non si è proprietari non è considerato un uso accettabile.

Per la risoluzione dei problemi relativi al connettore di origine dati del crawler Amazon Kendra Web, consulta. Risoluzione dei problemi relativi alle origini dati

> **Note**
>
> Il connettore Web Crawler v2.0 non supporta la scansione di elenchi di siti Web da bucket crittografati. AWS KMS Amazon S3 Supporta solo la crittografia lato server con chiavi gestite. Amazon S3

> **Important**
>
> La creazione di connettori Web Crawler v2.0 non è supportata da. AWS CloudFormation Utilizza il connettore Web Crawler v1.0 se hai bisogno di assistenza. AWS CloudFormation

Argomenti

- Funzionalità supportate
- Prerequisiti
- Istruzioni di connessione

Funzionalità supportate

- Mappature dei campi
- Filtri di inclusione/esclusione
- Sincronizzazione completa e incrementale dei contenuti
- Proxy Web
- Autenticazione di base, NTLM/Kerberos, SAML e basata su moduli per i tuoi siti Web
- Virtual Private Cloud (VPC) (Cloud privato virtuale (VPC)

Prerequisiti

Prima di utilizzarla Amazon Kendra per indicizzare i siti Web, verifica i dettagli dei siti Web e degli account. AWS

Per i tuoi siti Web, assicurati di disporre di:

- Hai copiato gli URL iniziali o della mappa del sito web che desideri indicizzare. Puoi memorizzare gli URL in un file di testo e caricarlo in un bucket. Amazon S3 Ogni URL nel file di testo deve essere formattato su una riga separata. Se desideri archiviare le tue Sitemap in un Amazon S3 bucket, assicurati di aver copiato il codice XML della Sitemap e di averlo salvato in un file XML. Puoi anche raggruppare più file XML della Sitemap in un file ZIP.

  > **Note**
  >
  > (On-premise/server) Amazon Kendra verifica se le informazioni sull'endpoint incluse sono le stesse informazioni sull'endpoint specificate nei AWS Secrets Manager dettagli di configurazione dell'origine dati. Questo aiuta a proteggersi dal confuso problema del vice, ossia un problema di sicurezza in cui un utente non è autorizzato a eseguire un'azione ma lo utilizza Amazon Kendra come proxy per accedere al segreto configurato ed eseguire l'azione. Se successivamente modifichi le informazioni sull'endpoint, devi creare un nuovo segreto per sincronizzare queste informazioni.

- Per i siti Web che richiedono l'autenticazione di base, NTLM o Kerberos:
  - Ha annotato le credenziali di autenticazione del sito Web, che includono un nome utente e una password.

> **Note**
>
> Amazon Kendra Web Crawler v2.0 supporta il protocollo di autenticazione NTLM che include l'hashing delle password e il protocollo di autenticazione Kerberos che include la crittografia delle password.

- Per i siti Web che richiedono l'autenticazione SAML o tramite modulo di accesso:
  - Hai annotato le credenziali di autenticazione del tuo sito Web, che includono un nome utente e una password.
  - Ha copiato gli XPaths (XML Path Language) del campo del nome utente (e del pulsante del nome utente se si utilizza SAML), del campo della password e del pulsante e ha copiato l'URL della pagina di accesso. Puoi trovare gli XPath degli elementi utilizzando gli strumenti di sviluppo del tuo browser web. Gli XPaths di solito seguono questo formato:. `//tagname[@Attribute='Value']`

> **Note**
>
> Amazon Kendra Web Crawler v2.0 utilizza un browser Chrome headless e le informazioni contenute nel modulo per autenticare e autorizzare l'accesso con un URL protetto da OAuth 2.0.

- Facoltativo: hai copiato il nome host e il numero di porta del server proxy Web se desideri utilizzare un proxy Web per connetterti ai siti Web interni di cui desideri eseguire la scansione. Il proxy web deve essere rivolto al pubblico. Amazon Kendra supporta la connessione a server proxy Web supportati da un'autenticazione di base oppure è possibile connettersi senza autenticazione.
- Facoltativo: hai copiato l'ID di sottorete del cloud privato virtuale (VPC) se desideri utilizzare un VPC per connetterti ai siti Web interni da sottoporre a scansione. Per ulteriori informazioni, consulta Configurazione di un. Amazon VPC
- Selezionato, ogni documento della pagina Web che desideri indicizzare è unico e tra le altre fonti di dati che intendi utilizzare per lo stesso indice. Ogni fonte di dati che desideri utilizzare per un indice non deve contenere lo stesso documento in tutte le fonti di dati. Gli ID dei documenti sono globali rispetto a un indice e devono essere univoci per indice.

Nel tuo AWS account, assicurati di avere:

- Hai creato un Amazon Kendra indice e, se utilizzi l'API, hai annotato l'ID dell'indice.

- Hai creato un IAM ruolo per la tua origine dati e, se utilizzi l'API, hai annotato l'ARN del IAM ruolo.

> **Note**
>
> Se modifichi il tipo di autenticazione e le credenziali, devi aggiornare il IAM ruolo per accedere all'ID AWS Secrets Manager segreto corretto.

- Per i siti Web che richiedono l'autenticazione o se utilizzano un proxy Web con autenticazione, memorizzate le credenziali di autenticazione in un AWS Secrets Manager luogo segreto e, se utilizzate l'API, annotate l'ARN del segreto.

> **Note**
>
> Ti consigliamo di aggiornare o ruotare regolarmente le credenziali e il segreto. Fornisci solo il livello di accesso necessario per la tua sicurezza. Non è consigliabile riutilizzare credenziali e segreti tra diverse fonti di dati e nelle versioni 1.0 e 2.0 dei connettori (ove applicabile).

Se non disponi di un IAM ruolo o di un segreto esistente, puoi utilizzare la console per creare un nuovo IAM ruolo e un Secrets Manager segreto quando connetti la tua origine web crawler dati a. Amazon Kendra Se utilizzi l'API, devi fornire l'ARN di un IAM ruolo e di un Secrets Manager segreto esistenti e un ID di indice.

Istruzioni di connessione

Per connetterti Amazon Kendra alla tua fonte di web crawler dati, devi fornire i dettagli necessari della tua origine web crawler dati in modo che Amazon Kendra possa accedere ai tuoi dati. Se non hai ancora configurato web crawler Amazon Kendra SeePrerequisiti.

Console

Per connettersi Amazon Kendra a web crawler

1. Accedi a AWS Management Console e apri la Amazon Kendra console.
2. Dal riquadro di navigazione a sinistra, scegli Indici, quindi scegli l'indice che desideri utilizzare dall'elenco degli indici.

> **Note**
>
> Puoi scegliere di configurare o modificare le impostazioni del controllo dell'accesso degli utenti in Impostazioni dell'indice.

3. Nella pagina Guida introduttiva, scegli Aggiungi origine dati.
4. Nella pagina Aggiungi origine dati, scegli connettore web crawler, quindi scegli Aggiungi connettore.
5. Nella pagina Specificare i dettagli dell'origine dati, inserisci le seguenti informazioni:
   a. In Nome e descrizione, per Nome dell'origine dati, inserisci un nome per l'origine dati. Puoi includere trattini ma non spazi.
   b. (Facoltativo) Descrizione: immetti una descrizione facoltativa per la tua fonte di dati.
   c. In Lingua predefinita: scegli una lingua per filtrare i documenti per l'indice. Se non diversamente specificato, la lingua predefinita è l'inglese. La lingua specificata nei metadati del documento ha la precedenza sulla lingua selezionata.
   d. In Tag, per Aggiungi nuovo tag, includi tag opzionali per cercare e filtrare le risorse o tenere traccia dei costi. AWS
   e. Seleziona Successivo.
6. Nella pagina Definisci accesso e sicurezza, inserisci le seguenti informazioni:
   a. Sorgente: scegli tra URL di origine, Sitemap di origine, file URL di origine, file Sitemap di origine. Se scegli di utilizzare un file di testo che include un elenco di un massimo di 100 URL iniziali, specifica il percorso del bucket in cui è archiviato il file. Amazon S3 Se scegli di utilizzare un file XML Sitemap, specifichi il percorso del Amazon S3 bucket in cui è archiviato il file. Puoi anche raggruppare più file XML della mappa del sito in un file ZIP. Altrimenti, puoi inserire manualmente fino a 10 URL iniziali o di punto di partenza e fino a tre URL della mappa del sito.

> **Note**
>
> Se desideri eseguire la scansione di una Sitemap, verifica che l'URL di base o principale sia lo stesso degli URL elencati nella pagina della Sitemap. Ad esempio, se l'URL della mappa del sito è https://example.com/sitemap-

page.html, anche gli URL elencati in questa pagina della mappa del sito devono utilizzare l'URL di base "». https://example.com/

Se i tuoi siti Web richiedono l'autenticazione per accedere ai siti Web, puoi scegliere ether basic, NTLM/Kerberos, SAML o l'autenticazione tramite modulo. Altrimenti, scegli l'opzione senza autenticazione.

> **Note**
>
> Se desideri modificare in un secondo momento la tua fonte di dati per cambiare gli URL iniziali con autenticazione alle sitemap, devi creare una nuova fonte di dati. Amazon Kendra configura l'origine dati utilizzando le informazioni sull'endpoint degli URL iniziali nel Secrets Manager segreto per l'autenticazione e pertanto non può riconfigurare l'origine dati quando si passa alle sitemap.

- AWS Secrets Manager segreto: se i tuoi siti Web richiedono la stessa autenticazione per accedere ai siti Web, scegli un segreto esistente o creane uno nuovo Secrets Manager per memorizzare le credenziali del sito Web. Se scegli di creare un nuovo segreto, si apre una finestra AWS Secrets Manager segreta.

  Se hai scelto l'autenticazione di base o NTML/Kerberos, inserisci un nome per il segreto, oltre al nome utente e alla password. Il protocollo di autenticazione NTLM include l'hashing delle password e il protocollo di autenticazione Kerberos include la crittografia delle password.

  Se hai scelto l'autenticazione SAML o Form, inserisci un nome per il segreto, oltre al nome utente e alla password. Usa XPath per il campo del nome utente (e XPath per il pulsante del nome utente se usi SAML). Usa XPaths per il campo e il pulsante della password e l'URL della pagina di accesso. Puoi trovare gli XPaths (XML Path Language) degli elementi utilizzando gli strumenti di sviluppo del tuo browser web. Gli XPaths di solito seguono questo formato:. `//tagname[@Attribute='Value']`

b. (Facoltativo) Proxy Web: immettere il nome host e il numero di porta del server proxy che si desidera utilizzare per connettersi a siti Web interni. Ad esempio, il nome host di https://a.example.com/page1.htmlè "a.example.com" e il numero di porta è 443, la porta

standard per HTTPS. Se sono necessarie le credenziali del proxy Web per connettersi all'host di un sito Web, è possibile crearne una AWS Secrets Manager che memorizzi le credenziali.

c. Virtual Private Cloud (VPC): puoi scegliere di utilizzare un VPC. In tal caso, è necessario aggiungere sottoreti e gruppi di sicurezza VPC.

d. IAM ruolo: scegli un IAM ruolo esistente o creane uno nuovo IAM per accedere alle credenziali del repository e indicizzare il contenuto.

> **Note**
>
> IAM i ruoli utilizzati per gli indici non possono essere utilizzati per le fonti di dati. Se non sei sicuro che un ruolo esistente venga utilizzato per un indice o una FAQ, scegli Crea un nuovo ruolo per evitare errori.

e. Seleziona Successivo.

7. Nella pagina Configura le impostazioni di sincronizzazione, inserisci le seguenti informazioni:

a. Ambito di sincronizzazione: imposta i limiti per la scansione delle pagine Web, compresi i domini, le dimensioni dei file e i collegamenti, e filtra gli URL utilizzando modelli regex.

i. (Facoltativo) Intervallo di domini: scegli se eseguire la scansione solo dei domini dei siti Web, dei domini con sottodomini o anche di altri domini a cui le pagine Web rimandano. Per impostazione predefinita, esegue la scansione Amazon Kendra solo dei domini dei siti Web da sottoporre a scansione.

ii. (Facoltativo) Configurazione aggiuntiva: imposta le seguenti impostazioni:

- Profondità di scansione: la «profondità» o il numero di livelli dal livello iniziale alla scansione. Ad esempio, la pagina URL iniziale ha la profondità 1 e tutti i collegamenti ipertestuali di questa pagina che sono anch'essi sottoposti a scansione hanno la profondità 2.
- Dimensione massima del file: la dimensione massima in MB di una pagina Web o di un allegato da sottoporre a scansione.
- Numero massimo di link per pagina: il numero massimo di URL su una singola pagina Web da sottoporre a scansione.
- Limitazione massima della velocità di scansione: il numero massimo di URL sottoposti a scansione per host del sito Web al minuto.

- File: consente di eseguire la scansione dei file a cui si collegano le pagine Web.
- Scansiona e indicizza gli URL: aggiungi modelli di espressioni regolari per includere o escludere la scansione di determinati URL e l'indicizzazione di eventuali collegamenti ipertestuali su queste pagine Web con URL.

b. Modalità di sincronizzazione: scegli come aggiornare l'indice quando il contenuto dell'origine dati cambia. Quando sincronizzi l'origine dati con Amazon Kendra per la prima volta, tutto il contenuto viene sottoposto a scansione e indicizzato per impostazione predefinita. Se la sincronizzazione iniziale non è riuscita, devi eseguire una sincronizzazione completa dei dati, anche se non scegli la sincronizzazione completa come opzione della modalità di sincronizzazione.

- Sincronizzazione completa: indicizza di nuovo tutti i contenuti, sostituendo i contenuti esistenti ogni volta che l'origine dati si sincronizza con l'indice.
- Sincronizzazione nuova, modificata ed eliminata: indicizza solo i contenuti nuovi, modificati ed eliminati ogni volta che l'origine dati si sincronizza con l'indice. Amazon Kendra può utilizzare il meccanismo dell'origine dati per tenere traccia delle modifiche ai contenuti e indicizzare i contenuti modificati dall'ultima sincronizzazione.

c. Pianificazione dell'esecuzione della sincronizzazione: per Frequenza, scegli la frequenza di sincronizzazione con la tua fonte di dati. Amazon Kendra

d. Seleziona Successivo.

8. Nella pagina Imposta mappature dei campi, inserisci le seguenti informazioni:

   a. Seleziona uno dei campi predefiniti Amazon Kendra generati delle pagine Web e dei file che desideri mappare all'indice.

   b. Seleziona Successivo.

9. Nella pagina Rivedi e crea, verifica che le informazioni inserite siano corrette, quindi seleziona Aggiungi origine dati. Puoi anche scegliere di modificare le tue informazioni da questa pagina. L'origine dati verrà visualizzata nella pagina Origini dati dopo che l'origine dati sarà stata aggiunta correttamente.

API

Per connettersi Amazon Kendra a web crawler

È necessario specificare un codice JSON dello schema dell'origine dati utilizzando l'TemplateConfigurationAPI. È necessario fornire le seguenti informazioni:

- Origine dati: specifica il tipo di origine dati come `WEBCRAWLERV2` quando usi lo schema TemplateConfigurationJSON. Specificate anche l'origine dati come `TEMPLATE` quando chiamate l'CreateDataSourceAPI.
- URL: specifica gli URL iniziali o del punto di partenza dei siti Web o gli URL della mappa del sito dei siti Web di cui desideri eseguire la scansione. Puoi specificare il percorso di un Amazon S3 bucket che memorizza il tuo elenco di URL iniziali. Ogni URL nel file di testo per gli URL iniziali deve essere formattato su una riga separata. Puoi anche specificare il percorso di un Amazon S3 bucket che memorizza i file XML della mappa del sito. Puoi raggruppare più file Sitemap in un file ZIP e archiviare il file ZIP nel tuo bucket. Amazon S3

  > **Note**
  >
  > Se vuoi eseguire la scansione di una Sitemap, verifica che l'URL di base o principale sia lo stesso degli URL elencati nella pagina della Sitemap. Ad esempio, se l'URL della mappa del sito è https://example.com/sitemap-page.html, anche gli URL elencati in questa pagina della mappa del sito devono utilizzare l'URL di base "». https://example.com/

- Modalità di sincronizzazione: specifica come Amazon Kendra aggiornare l'indice quando il contenuto della fonte di dati cambia. Quando sincronizzi l'origine dati con Amazon Kendra per la prima volta, tutto il contenuto viene sottoposto a scansione e indicizzato per impostazione predefinita. Se la sincronizzazione iniziale non è riuscita, devi eseguire una sincronizzazione completa dei dati, anche se non scegli la sincronizzazione completa come opzione della modalità di sincronizzazione. Puoi scegliere tra:
  - `FORCED_FULL_CRAWL`per indicizzare nuovamente tutti i contenuti, sostituendo i contenuti esistenti ogni volta che l'origine dati si sincronizza con l'indice.
  - `FULL_CRAWL`per indicizzare solo i contenuti nuovi, modificati ed eliminati ogni volta che l'origine dati si sincronizza con l'indice. Amazon Kendra può utilizzare il meccanismo dell'origine dati per tenere traccia delle modifiche ai contenuti e indicizzare i contenuti modificati dall'ultima sincronizzazione.
- Autenticazione: se i tuoi siti Web richiedono la stessa autenticazione`BasicAuth`, `NTLM_KerberosSAML`, o `Form` autenticazione. Se i tuoi siti Web non richiedono l'autenticazione, specifica`NoAuthentication`.
- Amazon Resource Name (ARN) segreto: se i tuoi siti Web richiedono l'autenticazione di base, NTLM o Kerberos, fornisci un codice segreto che memorizza le credenziali di autenticazione del

nome utente e della password. Fornisci l'Amazon Resource Name (ARN) di un AWS Secrets Manager segreto. Il segreto viene archiviato in una struttura JSON con le seguenti chiavi:

```
{
    "seedUrlsHash": "Hash representation of all seed URLs",
    "userName": "user name",
    "password": "password"
}
```

Se i tuoi siti Web richiedono l'autenticazione SAML, il segreto viene archiviato in una struttura JSON con le seguenti chiavi:

```
{
    "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"
}
```

Se i tuoi siti Web richiedono l'autenticazione tramite modulo, il segreto viene archiviato in una struttura JSON con le seguenti chiavi:

```
{
    "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"
}
```

Puoi trovare gli XPaths (XML Path Language) degli elementi utilizzando gli strumenti di sviluppo del tuo browser web. Gli XPaths di solito seguono questo formato:. `//tagname[@Attribute='Value']`

Puoi anche fornire le credenziali del proxy web utilizzando and AWS Secrets Manager secret.

- IAM ruolo: specifica `RoleArn` quando chiami `CreateDataSource` per fornire a un IAM ruolo le autorizzazioni per accedere al Secrets Manager segreto e per chiamare le API pubbliche richieste per il connettore del crawler Web e. Amazon Kendra Per ulteriori informazioni, consulta IAM Ruoli per le fonti di dati del web crawler.

Puoi anche aggiungere le seguenti funzionalità opzionali:

- Virtual Private Cloud (VPC): `VpcConfiguration` specifica quando si chiama. `CreateDataSource` Per ulteriori informazioni, consulta Configurazione Amazon Kendra per l'utilizzo di un Amazon VPC.
- Intervallo di domini: scegli se eseguire la scansione dei domini dei siti Web con solo sottodomini o anche di altri domini a cui si collegano le pagine Web. Per impostazione predefinita, esegue la scansione Amazon Kendra solo dei domini dei siti Web che desideri sottoporre a scansione.
- La «profondità» o il numero di livelli dal livello iniziale al crawl. Ad esempio, la pagina URL iniziale ha la profondità 1 e tutti i collegamenti ipertestuali di questa pagina che sono anch'essi sottoposti a scansione hanno la profondità 2.
- Il numero massimo di URL su una singola pagina Web da sottoporre a scansione.
- La dimensione massima in MB di una pagina Web o di un allegato da sottoporre a scansione.
- Il numero massimo di URL di cui viene eseguita la ricerca per indicizzazione per host di sito Web al minuto.
- L'host del proxy Web e il numero di porta per la connessione e la scansione dei siti Web interni. Ad esempio, il nome host di https://a.example.com/page1.htmlè "a.example.com" e il numero di porta è 443, la porta standard per HTTPS. Se sono necessarie le credenziali del proxy Web per connettersi all'host di un sito Web, è possibile crearne una AWS Secrets Manager che memorizzi le credenziali.
- Filtri di inclusione ed esclusione: specificate se includere o escludere la scansione di determinati URL e l'indicizzazione di eventuali collegamenti ipertestuali su queste pagine Web con URL.

> **Note**
>
> La maggior parte delle fonti di dati utilizza modelli di espressioni regolari, che sono modelli di inclusione o esclusione denominati filtri. Se si specifica un filtro di inclusione, viene indicizzato solo il contenuto che corrisponde al filtro di inclusione. Qualsiasi

documento che non corrisponde al filtro di inclusione non viene indicizzato. Se si specifica un filtro di inclusione ed esclusione, i documenti che corrispondono al filtro di esclusione non vengono indicizzati, anche se corrispondono al filtro di inclusione.

- Mappature dei campi: scegli di mappare i campi delle pagine Web e dei file di pagine Web ai campi dell'indice. Amazon Kendra Per ulteriori informazioni, consulta la sezione Mappatura dei campi di origine dei dati.

Per un elenco di altre importanti chiavi JSON da configurare, consulta lo schema del modello Amazon Kendra Web Crawler.

Configurazione del file per Web Crawler **`robots.txt`**Amazon Kendra

Amazon Kendra è un servizio di ricerca intelligente che AWS i clienti utilizzano per indicizzare e cercare documenti di loro scelta. Per indicizzare i documenti sul Web, i clienti possono utilizzare Amazon Kendra Web Crawler, che indica quali URL devono essere indicizzati e altri parametri operativi. Amazon Kendra i clienti devono ottenere l'autorizzazione prima di indicizzare un determinato sito Web.

Amazon Kendra Web Crawler rispetta le direttive robots.txt standard come e. `Allow` `Disallow` Puoi modificare il `robots.txt` file del tuo sito Web per controllare il modo in cui Web Crawler esegue la scansione del tuo sito Amazon Kendra Web.

Configurazione del modo in cui Web Crawler accede al sito Amazon Kendra Web

Puoi controllare il modo in cui il Amazon Kendra Web Crawler indicizza il tuo sito Web utilizzando le direttive e. `Allow` `Disallow` È inoltre possibile controllare quali pagine Web vengono indicizzate e quali pagine Web non vengono sottoposte a scansione.

Per consentire a Amazon Kendra Web Crawler di eseguire la scansione di tutte le pagine Web ad eccezione delle pagine Web non consentite, utilizzate la seguente direttiva:

```
User-agent: amazon-kendra    # Amazon Kendra Web Crawler
Disallow: /credential-pages/ # disallow access to specific pages
```

Per consentire a Amazon Kendra Web Crawler di eseguire la scansione solo di pagine Web specifiche, utilizzate la seguente direttiva:

```
User-agent: amazon-kendra    # Amazon Kendra Web Crawler
```

```
Allow: /pages/ # allow access to specific pages
```

Per consentire a Amazon Kendra Web Crawler di eseguire la scansione di tutto il contenuto del sito Web e impedire la scansione per altri robot, utilizzate la seguente direttiva:

```
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
```

Impedire a Web Crawler di eseguire la scansione del sito Web Amazon Kendra

Puoi impedire a Amazon Kendra Web Crawler di indicizzare il tuo sito Web utilizzando la direttiva. `Disallow` Puoi anche controllare quali pagine web vengono sottoposte a scansione e quali no.

Per impedire a Amazon Kendra Web Crawler di eseguire la scansione del sito Web, utilizzate la seguente direttiva:

```
User-agent: amazon-kendra # Amazon Kendra Web Crawler
Disallow: / # disallow access to any pages
```

Amazon Kendra Web Crawler supporta anche i robot `noindex` e le `nofollow` direttive nei meta tag nelle pagine HTML. Queste direttive impediscono al web crawler di indicizzare una pagina Web e di non seguire più i collegamenti presenti nella pagina Web. Inserisci i meta tag nella sezione del documento per specificare le regole delle regole dei robot.

Ad esempio, la pagina web seguente include le direttive robot `noindex` e: `nofollow`

```
<html>
<head>
    <meta name="robots" content="noindex, nofollow"/>
    ...
</head>
<body>...</body>
</html>
```

Se hai domande o dubbi su Amazon Kendra Web Crawler, puoi contattare il team di supporto.AWS

Amazon WorkDocs

Amazon WorkDocs è un servizio sicuro di collaborazione sui contenuti per la creazione, la modifica, l'archiviazione e la condivisione di contenuti. Puoi usarlo Amazon Kendra per indicizzare la tua fonte di Amazon WorkDocs dati.

Puoi connetterti Amazon Kendra alla tua fonte di Amazon WorkDocs dati utilizzando la Amazon Kendra console e l'WorkDocsConfigurationAPI.

Amazon WorkDocs è disponibile nelle regioni di Oregon, Virginia del Nord, Sydney, Singapore e Irlanda.

Per la risoluzione dei problemi relativi al connettore della sorgente Amazon Kendra WorkDocs dati, consultaRisoluzione dei problemi relativi alle origini dati.

Argomenti

- Funzionalità supportate
- Prerequisiti
- Istruzioni di connessione
- Ulteriori informazioni

Funzionalità supportate

Amazon Kendra WorkDocs il connettore di origine dati supporta le seguenti funzionalità:

- Log delle modifiche
- mappature dei campi
- Filtraggio del contesto utente
- Filtri di inclusione/esclusione

Prerequisiti

Prima di utilizzarla Amazon Kendra per indicizzare la tua fonte di WorkDocs dati, apporta queste modifiche al tuo account e ai tuoi account. WorkDocs AWS

Nel WorkDocs, assicurati di avere:

- Hai annotato l'ID della Amazon WorkDocs directory (ID dell'organizzazione) del tuo Amazon WorkDocs repository.
- È stato selezionato che ogni documento sia unico all'interno WorkDocs e tra le altre fonti di dati che intendi utilizzare per lo stesso indice. Ogni fonte di dati che desideri utilizzare per un indice non deve contenere lo stesso documento in tutte le fonti di dati. Gli ID dei documenti sono globali rispetto a un indice e devono essere univoci per indice.

Nel tuo AWS account, assicurati di avere:

- Hai creato un Amazon Kendra indice e, se utilizzi l'API, hai annotato l'ID dell'indice.
- Hai creato un IAM ruolo per la tua origine dati e, se utilizzi l'API, hai annotato l'ARN del IAM ruolo.

Se non disponi di un IAM ruolo esistente, puoi utilizzare la console per creare un nuovo IAM ruolo quando connetti la tua fonte di WorkDocs dati a Amazon Kendra. Se utilizzi l'API, devi fornire l'ARN di un IAM ruolo esistente e un ID di indice.

Istruzioni di connessione

Per connetterti Amazon Kendra alla tua fonte di WorkDocs dati, devi fornire i dettagli necessari della tua origine WorkDocs dati in modo che Amazon Kendra possa accedere ai tuoi dati. Se non hai ancora configurato WorkDocs per Amazon Kendra, consultaPrerequisiti.

Console

Per connettersi Amazon Kendra a Amazon WorkDocs

1. Accedi a AWS Management Console e apri la Amazon Kendra console.
2. Dal riquadro di navigazione a sinistra, scegli Indici, quindi scegli l'indice che desideri utilizzare dall'elenco degli indici.

   > **Note**
   >
   > Puoi scegliere di configurare o modificare le impostazioni del controllo dell'accesso degli utenti in Impostazioni dell'indice.

3. Nella pagina Guida introduttiva, scegli Aggiungi origine dati.
4. Nella pagina Aggiungi origine dati, scegli WorkDocs connettore, quindi scegli Aggiungi connettore.

5. Nella pagina Specificare i dettagli dell'origine dati, inserisci le seguenti informazioni:

   a. In Nome e descrizione, per Nome dell'origine dati, inserisci un nome per l'origine dati. Puoi includere trattini ma non spazi.

   b. (Facoltativo) Descrizione: immetti una descrizione facoltativa per l'origine dati.

   c. In Lingua predefinita: scegli una lingua per filtrare i documenti per l'indice. Se non diversamente specificato, la lingua predefinita è l'inglese. La lingua specificata nei metadati del documento ha la precedenza sulla lingua selezionata.

   d. In Tag, per Aggiungi nuovo tag, includi tag opzionali per cercare e filtrare le risorse o tenere traccia dei costi. AWS

   e. Seleziona Successivo.

6. Nella pagina Definisci accesso e sicurezza, inserisci le seguenti informazioni:

   a. ID dell'organizzazione specifico Amazon WorkDocs del sito: seleziona l'ID del Amazon WorkDocs sito che desideri indicizzare. Devi aver già creato un sito.

   b. IAM ruolo: scegli un IAM ruolo esistente o crea un nuovo IAM ruolo per accedere alle credenziali del repository e indicizzare il contenuto.

      > **Note**
      >
      > IAM i ruoli utilizzati per gli indici non possono essere utilizzati per le fonti di dati. Se non sei sicuro che un ruolo esistente venga utilizzato per un indice o una FAQ, scegli Crea un nuovo ruolo per evitare errori.

   c. Seleziona Successivo.

7. Nella pagina Configura le impostazioni di sincronizzazione, inserisci le seguenti informazioni:

   a. Esplora i commenti dei documenti: le Amazon WorkDocs entità o i tipi di contenuto che desideri sottoporre a scansione.

   b. Utilizza i registri delle modifiche: seleziona questa opzione per aggiornare l'indice solo con contenuti nuovi o modificati anziché sincronizzare tutti i file.

   c. Modelli Regex: modelli di espressioni regolari per includere o escludere determinati file. È possibile aggiungere fino a 100 pattern.

   d. Pianificazione di esecuzione di In Sync per Frequency: scegli la frequenza di sincronizzazione con la tua fonte di dati. Amazon Kendra

   e. Seleziona Successivo.

8. Nella pagina Imposta le mappature dei campi, inserisci le seguenti informazioni:

   a. Campi di origine dati predefiniti: seleziona uno dei campi di origine dati predefiniti Amazon Kendra generati che desideri mappare all'indice.

   b. Aggiungi campo: consente di aggiungere campi di origine dati personalizzati per creare un nome di campo indice a cui mappare e il tipo di dati del campo.

   c. Seleziona Successivo.

9. Nella pagina Rivedi e crea, verifica che le informazioni inserite siano corrette, quindi seleziona Aggiungi origine dati. Puoi anche scegliere di modificare le tue informazioni da questa pagina. L'origine dati verrà visualizzata nella pagina Origini dati dopo che l'origine dati sarà stata aggiunta correttamente.

API

Per connettersi Amazon Kendra a Amazon WorkDocs

È necessario specificare quanto segue utilizzando l'WorkDocsConfigurationAPI:

- Amazon WorkDocs ID directory: specifica l'ID dell'organizzazione della Amazon WorkDocs directory. Puoi trovare l'ID dell'organizzazione in AWS Directory Service accedendo ad Active Directory e quindi a Directories.
- Ruolo IAM: specifica `RoleArn` quando chiami `CreateDataSource` per fornire a un IAM ruolo le autorizzazioni per accedere alla WorkDocs directory e per chiamare le API pubbliche richieste per il connettore e. WorkDocs Amazon KendraPer ulteriori informazioni, consulta Ruoli IAM per le fonti di dati. WorkDocs

Puoi anche aggiungere le seguenti funzionalità opzionali:

- Registro delle modifiche: Amazon Kendra indica se utilizzare il meccanismo del registro delle modifiche dell'origine WorkDocs dati per determinare se un documento deve essere aggiornato nell'indice.

> **Note**
>
> Utilizza il registro delle modifiche se non desideri Amazon Kendra scansionare tutti i documenti. Se il registro delle modifiche è di grandi dimensioni, la scansione dei documenti nella fonte WorkDocs dati potrebbe richiedere Amazon Kendra meno tempo

rispetto all'elaborazione del registro delle modifiche. Se sincronizzi la fonte di WorkDocs dati con l'indice per la prima volta, tutti i documenti vengono scansionati.

- Filtri di inclusione ed esclusione: specificate se includere o escludere determinati documenti e commenti ai documenti. Ogni commento viene indicizzato come documento separato.

> **Note**
>
> La maggior parte delle fonti di dati utilizza modelli di espressioni regolari, che sono modelli di inclusione o esclusione denominati filtri. Se si specifica un filtro di inclusione, viene indicizzato solo il contenuto che corrisponde al filtro di inclusione. Qualsiasi documento che non corrisponde al filtro di inclusione non viene indicizzato. Se si specifica un filtro di inclusione ed esclusione, i documenti che corrispondono al filtro di esclusione non vengono indicizzati, anche se corrispondono al filtro di inclusione.

- Filtro del contesto utente e controllo degli accessi:Amazon Kendra esegue la ricerca per indicizzazione dell'elenco di controllo degli accessi (ACL) dei documenti, se disponi di un ACL per i documenti. Le informazioni ACL vengono utilizzate per filtrare i risultati della ricerca in base all'accesso dell'utente o del relativo gruppo ai documenti. Per ulteriori informazioni, consulta Filtraggio del contesto utente.
- Mappature dei campi: scegli di mappare i campi delle sorgenti WorkDocs dati ai campi indice. Amazon Kendra Per ulteriori informazioni, consulta la sezione Mappatura dei campi di origine dei dati.

> **Note**
>
> Il campo del corpo del documento o l'equivalente del corpo del documento per i documenti è necessario per Amazon Kendra eseguire la ricerca nei documenti. È necessario mappare il nome del campo del corpo del documento nella fonte dati al nome del campo indice `_document_body`. Tutti gli altri campi sono facoltativi.

Ulteriori informazioni

Per ulteriori informazioni sull'integrazione Amazon Kendra con la tua fonte di WorkDocs dati, consulta:

- Inizia a usare il WorkDocs connettore Amazon Kendra Amazon

Box (Cubo)

Box è un servizio di archiviazione cloud che offre funzionalità di hosting di file. Puoi utilizzarlo Amazon Kendra per indicizzare i contenuti del tuo Box, inclusi commenti, attività e link web.

Puoi connetterti Amazon Kendra alla fonte dati Box utilizzando la Amazon Kendra console e l'BoxConfigurationAPI.

Per la risoluzione dei problemi relativi al connettore di origine dati Amazon Kendra Box, consultaRisoluzione dei problemi relativi alle origini dati.

Argomenti

- Funzionalità supportate
- Prerequisiti
- Istruzioni di connessione
- Ulteriori informazioni

Funzionalità supportate

Amazon Kendra Il connettore di origine dati Box supporta le seguenti funzionalità:

- Log delle modifiche
- Mappature dei campi
- Filtraggio del contesto utente
- Filtri di inclusione/esclusione
- Virtual Private Cloud (VPC) (Cloud privato virtuale (VPC)

Prerequisiti

Prima di utilizzarla Amazon Kendra per indicizzare la fonte di dati Box, apporta queste modifiche a Box e agli account. AWS

In Box, assicurati di avere:

- Un account Box Enterprise o Box Enterprise Plus.
- Ha creato un'app Box personalizzata nella Box Developer Console e l'ha configurata per utilizzare l'autenticazione del server (con JWT).

- Imposta il livello di accesso all'app su App + Enterprise Access e consenti all'app di effettuare chiamate API utilizzando l'intestazione as-user.
- Hai usato l'utente amministratore per aggiungere i seguenti Application Scopes nell'app Box:
  - Scrivi tutti i file e le cartelle archiviati in un Box
  - Gestisci gli utenti
  - Gestisci i gruppi
  - Gestisci le proprietà aziendali
- Coppia di chiavi pubbliche/private generata e scaricata che include un ID client, un client secret, un ID chiave pubblica, un ID chiave privata, una passphrase e un ID aziendale da utilizzare come credenziali di autenticazione. Vedi Coppia di chiavi pubblica e privata per maggiori dettagli.
- Hai copiato il tuo Box Enterprise ID dalle impostazioni della Box Developer Console o dall'app Box. Ad esempio, `801234567`.
- Selezionato, ogni documento è unico in Box e tra le altre fonti di dati che intendi utilizzare per lo stesso indice. Ogni fonte di dati che desideri utilizzare per un indice non deve contenere lo stesso documento in tutte le fonti di dati. Gli ID dei documenti sono globali rispetto a un indice e devono essere univoci per indice.

Nel tuo Account AWS, assicurati di avere:

- Ha creato un Amazon Kendra indice e, se si utilizza l'API, ha annotato l'ID dell'indice.
- Hai creato un IAM ruolo per la tua origine dati e, se utilizzi l'API, hai annotato l'ARN del IAM ruolo.

> **Note**
>
> Se modifichi il tipo di autenticazione e le credenziali, devi aggiornare il IAM ruolo per accedere all'ID AWS Secrets Manager segreto corretto.

- Ha archiviato le credenziali di autenticazione Box in un AWS Secrets Manager luogo segreto e, se si utilizza l'API, ha annotato l'ARN del segreto.

> **Note**
>
> Ti consigliamo di aggiornare o ruotare regolarmente le credenziali e il segreto. Fornisci solo il livello di accesso necessario per la tua sicurezza. Non è consigliabile riutilizzare

credenziali e segreti tra diverse fonti di dati e versioni dei connettori 1.0 e 2.0 (ove applicabile).

Se non disponi di un IAM ruolo o di un segreto esistente, puoi utilizzare la console per creare un nuovo IAM ruolo e un Secrets Manager segreto quando connetti l'origine dati Box a. Amazon Kendra Se utilizzi l'API, devi fornire l'ARN di un IAM ruolo e di un Secrets Manager segreto esistenti e un ID di indice.

Istruzioni di connessione

Per connetterti Amazon Kendra alla fonte dati Box, devi fornire i dettagli necessari sulla fonte dati Box in modo che Amazon Kendra possa accedere ai tuoi dati. Se non hai ancora configurato Box for Amazon Kendra, consultaPrerequisiti.

Console

Per connettersi Amazon Kendra a Box

1. Accedi a AWS Management Console e apri la Amazon Kendra console.
2. Dal riquadro di navigazione a sinistra, scegli Indici, quindi scegli l'indice che desideri utilizzare dall'elenco degli indici.

   > **Note**
   >
   > Puoi scegliere di configurare o modificare le impostazioni del controllo dell'accesso degli utenti in Impostazioni dell'indice.

3. Nella pagina Guida introduttiva, scegli Aggiungi origine dati.
4. Nella pagina Aggiungi origine dati, scegli Box connector, quindi scegli Aggiungi connettore.
5. Nella pagina Specificare i dettagli dell'origine dati, inserisci le seguenti informazioni:

   a. In Nome e descrizione, per Nome dell'origine dati, inserisci un nome per l'origine dati. Puoi includere trattini ma non spazi.

   b. (Facoltativo) Descrizione: immetti una descrizione facoltativa per l'origine dati.

   c. In Lingua predefinita: scegli una lingua per filtrare i documenti per l'indice. Se non diversamente specificato, la lingua predefinita è l'inglese. La lingua specificata nei metadati del documento ha la precedenza sulla lingua selezionata.

d. In Tag, per Aggiungi nuovo tag, includi tag opzionali per cercare e filtrare le risorse o tenere traccia dei costi. AWS

e. Seleziona Successivo.

6. Nella pagina Definisci accesso e sicurezza, inserisci le seguenti informazioni:

a. Box enterprise ID: inserisci il tuo Box Enterprise ID.

b. AWS Secrets Manager segreto: scegli un segreto esistente o creane uno nuovo Secrets Manager per memorizzare le credenziali di autenticazione Box. Se scegli di creare un nuovo segreto, si apre una finestra AWS Secrets Manager segreta.

i. Nome segreto: un nome per il tuo segreto. Il prefisso 'AmazonKendra-Box-' viene aggiunto automaticamente al nome segreto.

ii. Per Client ID, Client Secret, Public Key ID, Private Key ID e Pass Phrase, inserisci i valori della chiave pubblica/privata che hai generato nel tuo account Box e scaricata dal tuo account Box.

iii. Selezionare Salva.

c. Virtual Private Cloud (VPC): puoi scegliere di utilizzare un VPC. In tal caso, è necessario aggiungere sottoreti e gruppi di sicurezza VPC.

d. IAM ruolo: scegli un IAM ruolo esistente o creane uno nuovo IAM per accedere alle credenziali del repository e indicizzare il contenuto.

> **Note**
>
> IAM i ruoli utilizzati per gli indici non possono essere utilizzati per le fonti di dati. Se non sei sicuro che un ruolo esistente venga utilizzato per un indice o una FAQ, scegli Crea un nuovo ruolo per evitare errori.

e. Seleziona Successivo.

7. Nella pagina Configura le impostazioni di sincronizzazione, inserisci le seguenti informazioni:

a. Seleziona entità o tipi di contenuto: le entità Box o i tipi di contenuto che desideri sottoporre a scansione. Ogni commento viene indicizzato come documento separato.

b. Registro delle modifiche: seleziona questa opzione per aggiornare l'indice solo per i contenuti nuovi o modificati anziché sincronizzare tutti i file.

c. Modelli Regex: modelli di espressioni regolari per includere o escludere determinati file. È possibile aggiungere fino a 100 pattern.

d. In Pianificazione di esecuzione della sincronizzazione, per Frequenza: scegli la frequenza di sincronizzazione con la tua fonte di dati. Amazon Kendra

e. Seleziona Successivo.

8. Nella pagina Imposta mappature dei campi, inserisci le seguenti informazioni:

a. Per file e cartelle, commenti, attività e collegamenti Web: seleziona uno dei campi di origine dati predefiniti Amazon Kendra generati che desideri mappare all'indice.

b. Aggiungi campo: consente di aggiungere campi di origine dati personalizzati per creare un nome di campo indice a cui mappare e il tipo di dati del campo.

c. Seleziona Successivo.

9. Nella pagina Rivedi e crea, verifica che le informazioni inserite siano corrette, quindi seleziona Aggiungi origine dati. Puoi anche scegliere di modificare le tue informazioni da questa pagina. L'origine dati verrà visualizzata nella pagina Origini dati dopo che l'origine dati sarà stata aggiunta correttamente.

API

Per connettersi Amazon Kendra a Box

È necessario specificare quanto segue utilizzando l'BoxConfigurationAPI:

Box enterprise ID: fornisci il tuo Box Enterprise ID. Puoi trovare l'ID aziendale nelle impostazioni della Box Developer Console o quando crei un'app in Box.

- Secret Amazon Resource Name (ARN): fornisci l'Amazon Resource Name (ARN) di un Secrets Manager segreto che contiene le credenziali di autenticazione per il tuo account Box. Il segreto è archiviato in una struttura JSON con le seguenti chiavi:

```
{
    "clientID": "client-id",
    "clientSecret": "client-secret",
    "publicKeyID": "public-key-id",
    "privateKey": "private-key",
    "passphrase": "pass-phrase"
}
```

> **Note**
>
> Ti consigliamo di aggiornare o ruotare regolarmente le credenziali e il segreto. Fornisci solo il livello di accesso necessario per la tua sicurezza. Non è consigliabile riutilizzare credenziali e segreti tra diverse fonti di dati e versioni dei connettori 1.0 e 2.0 (ove applicabile).

- IAM ruolo: specifica `RoleArn` quando chiami `CreateDataSource` per fornire a un IAM ruolo le autorizzazioni per accedere al tuo Secrets Manager segreto e per chiamare le API pubbliche richieste per il connettore Box e. Amazon Kendra Per ulteriori informazioni, consulta IAM i ruoli per le sorgenti dati Box.

Puoi anche aggiungere le seguenti funzionalità opzionali:

- Virtual Private Cloud (VPC): specifica `VpcConfiguration` come parte della configurazione dell'origine dati. Vedi Configurazione Amazon Kendra per l'uso di un VPC.
- Registro delle modifiche: Amazon Kendra indica se utilizzare il meccanismo del registro delle modifiche all'origine dati Box per determinare se un documento deve essere aggiornato nell'indice.

> **Note**
>
> Utilizza il registro delle modifiche se non desideri Amazon Kendra scansionare tutti i documenti. Se il registro delle modifiche è di grandi dimensioni, la scansione dei documenti nella fonte dati Box potrebbe richiedere Amazon Kendra meno tempo rispetto all'elaborazione del registro delle modifiche. Se sincronizzi l'origine dati Box con l'indice per la prima volta, tutti i documenti vengono scansionati.

- Commenti, attività, collegamenti Web: specifica se eseguire la scansione di questi tipi di contenuti.

> **Note**
>
> La maggior parte delle fonti di dati utilizza modelli di espressioni regolari, che sono modelli di inclusione o esclusione denominati filtri. Se si specifica un filtro di inclusione, viene indicizzato solo il contenuto che corrisponde al filtro di inclusione. Qualsiasi documento che non corrisponde al filtro di inclusione non viene indicizzato. Se si

specifica un filtro di inclusione ed esclusione, i documenti che corrispondono al filtro di esclusione non vengono indicizzati, anche se corrispondono al filtro di inclusione.

- Filtri di inclusione ed esclusione: specifica se includere o escludere determinati file e cartelle Box.

> **Note**
>
> La maggior parte delle fonti di dati utilizza modelli di espressioni regolari, che sono modelli di inclusione o esclusione denominati filtri. Se si specifica un filtro di inclusione, viene indicizzato solo il contenuto che corrisponde al filtro di inclusione. Qualsiasi documento che non corrisponde al filtro di inclusione non viene indicizzato. Se si specifica un filtro di inclusione ed esclusione, i documenti che corrispondono al filtro di esclusione non vengono indicizzati, anche se corrispondono al filtro di inclusione.

- Filtro del contesto utente e controllo degli accessi:Amazon Kendra esegue la ricerca per indicizzazione dell'elenco di controllo degli accessi (ACL) dei documenti, se disponi di un ACL per i documenti. Le informazioni ACL vengono utilizzate per filtrare i risultati della ricerca in base all'accesso dell'utente o del relativo gruppo ai documenti. Per ulteriori informazioni, consulta Filtraggio del contesto utente.
- Mappature dei campi: scegli di mappare i campi dell'origine dati Box ai campi indice. Amazon Kendra Per ulteriori informazioni, consulta la sezione Mappatura dei campi di origine dei dati.

> **Note**
>
> Il campo relativo al corpo del documento o l'equivalente del corpo del documento è necessario per Amazon Kendra eseguire la ricerca nei documenti. È necessario mappare il nome del campo del corpo del documento nella fonte dati al nome del campo indice`_document_body`. Tutti gli altri campi sono facoltativi.

Ulteriori informazioni

Per ulteriori informazioni sull'integrazione Amazon Kendra con la fonte dati Box, consulta:

- Guida introduttiva al connettore Amazon Kendra Box

Confluence

Confluence è uno strumento collaborativo di gestione del lavoro progettato per condividere, archiviare e lavorare sulla pianificazione di progetti, lo sviluppo di software e la gestione dei prodotti. Puoi utilizzarlo Amazon Kendra per indicizzare gli spazi, le pagine (incluse le pagine annidate), i blog e i commenti e gli allegati di Confluence a pagine e blog indicizzati.

Amazon Kendra supporta sia Confluence Server che Confluence Cloud.

> **Note**
>
> Per impostazione predefinita, Amazon Kendra non indicizza gli archivi e gli spazi personali di Confluence. Puoi scegliere di indicizzarli quando crei l'origine dati. Se non vuoi Amazon Kendra indicizzare uno spazio, contrassegnalo come privato in Confluence.

Puoi connetterti Amazon Kendra alla tua fonte di dati Confluence utilizzando la Amazon Kendra console, l'API o l'TemplateConfigurationAPI. ConfluenceConfiguration

Amazon Kendra dispone di due versioni del connettore Confluence. Le funzionalità supportate di ogni versione includono:

Connettore Confluence V1.0/API ConfluenceConfiguration

- Mappature dei campi
- Filtraggio del contesto utente
- Filtri di inclusione/esclusione
- (Solo per Confluence Server) Cloud privato virtuale (VPC)

Connettore Confluence V2.0/API TemplateConfiguration

- Mappature dei campi
- Filtraggio del contesto utente
- Virtual Private Cloud (VPC) (Cloud privato virtuale (VPC)
- Sincronizza tutti i documenti/Sincronizza solo documenti nuovi, modificati o eliminati
- Modelli di inclusione/esclusione

> **Note**
>
> La fine del supporto per Confluence connector ConfluenceConfiguration V1.0/API è prevista per il 2023. Ti consigliamo di eseguire la migrazione o l'utilizzo di Confluence connector V2.0/API. TemplateConfiguration

Per la risoluzione dei problemi relativi al connettore di origine dati Amazon Kendra Confluence, consulta. Risoluzione dei problemi relativi alle origini dati

Argomenti

Connettore Confluence V1.0

Confluence è uno strumento collaborativo di gestione del lavoro progettato per condividere, archiviare e lavorare sulla pianificazione di progetti, lo sviluppo di software e la gestione dei prodotti. Puoi utilizzarlo Amazon Kendra per indicizzare gli spazi, le pagine (incluse le pagine annidate), i blog e i commenti e gli allegati di Confluence a pagine e blog indicizzati.

> **Note**
>
> La fine del supporto per Confluence connector ConfluenceConfiguration V1.0/API è prevista per il 2023. Ti consigliamo di eseguire la migrazione o l'utilizzo di Confluence connector V2.0/API. TemplateConfiguration

Per la risoluzione dei problemi relativi al connettore di origine dati Amazon Kendra Confluence, consulta. Risoluzione dei problemi relativi alle origini dati

Argomenti

Funzionalità supportate

Amazon Kendra Il connettore di origine dati Confluence supporta le seguenti funzionalità:

- Mappature dei campi
- Filtraggio del contesto utente
- Filtri di inclusione/esclusione
- (Solo per Confluence Server) Cloud privato virtuale (VPC)

Prerequisiti

Prima di poterla utilizzare Amazon Kendra per indicizzare la tua fonte di dati Confluence, apporta queste modifiche a Confluence e agli account. AWS

In Confluence, assicurati di avere:

- Amazon Kendra Autorizzazioni concesse per visualizzare tutti i contenuti all'interno dell'istanza Confluence tramite:
  - Creazione di Amazon Kendra un membro del gruppo. `confluence-administrators`
  - Concessione delle autorizzazioni di amministratore del sito per tutti gli spazi, i blog e le pagine esistenti.
- Hai copiato l'URL dell'istanza di Confluence.
- Per gli utenti SSO (Single Sign-On): attiva la pagina di accesso Show on per il nome utente e la password quando configuri i metodi di autenticazione Confluence in Confluence Data Center.
- Per Confluence Server
  - Hai preso nota delle tue credenziali di autenticazione di base contenenti il nome utente e la password dell'account amministrativo di Confluence a cui connetterti. Amazon Kendra
  - Facoltativo: hai generato un token di accesso personale nel tuo account Confluence a cui connetterti. Amazon Kendra Per ulteriori informazioni, consulta la documentazione di Confluence sulla generazione di token di accesso personali.
- Per Confluence Cloud
  - Hai annotato le tue credenziali di autenticazione di base contenenti il nome utente e la password dell'account amministrativo di Confluence a cui connetterti. Amazon Kendra
- È stato verificato che ogni documento sia unico in Confluence e tra le altre fonti di dati che intendi utilizzare per lo stesso indice. Ogni fonte di dati che desideri utilizzare per un indice non deve

contenere lo stesso documento in tutte le fonti di dati. Gli ID dei documenti sono globali rispetto a un indice e devono essere univoci per indice.

Nel tuo Account AWS, assicurati di avere:

- Ha creato un Amazon Kendra indice e, se si utilizza l'API, ha annotato l'ID dell'indice.
- Hai creato un IAM ruolo per la tua origine dati e, se utilizzi l'API, hai annotato l'ARN del IAM ruolo.

> **Note**
>
> Se modifichi il tipo di autenticazione e le credenziali, devi aggiornare il IAM ruolo per accedere all'ID AWS Secrets Manager segreto corretto.

- Ha archiviato le credenziali di autenticazione Confluence in un AWS Secrets Manager segreto e, se si utilizza l'API, ha annotato l'ARN del segreto.

> **Note**
>
> Ti consigliamo di aggiornare o ruotare regolarmente le credenziali e il segreto. Fornisci solo il livello di accesso necessario per la tua sicurezza. Non è consigliabile riutilizzare credenziali e segreti tra diverse fonti di dati e versioni dei connettori 1.0 e 2.0 (ove applicabile).

Se non disponi di un IAM ruolo o di un segreto esistente, puoi utilizzare la console per creare un nuovo IAM ruolo e un Secrets Manager segreto quando connetti l'origine dati Confluence a. Amazon Kendra Se utilizzi l'API, devi fornire l'ARN di un IAM ruolo e di un Secrets Manager segreto esistenti e un ID di indice.

Istruzioni di connessione

Per connetterti Amazon Kendra alla tua fonte di dati Confluence, devi fornire i dettagli delle tue credenziali Confluence in modo da poter Amazon Kendra accedere ai tuoi dati. Se non hai ancora configurato Confluence for see. Amazon Kendra Prerequisiti

Console

Per connettersi a Confluence Amazon Kendra

1. Accedi alla console di AWS gestione e apri la Amazon Kendra console.
2. Dal riquadro di navigazione a sinistra, scegli Indici, quindi scegli l'indice che desideri utilizzare dall'elenco degli indici.

> **Note**
>
> Puoi scegliere di configurare o modificare le impostazioni del controllo dell'accesso degli utenti in Impostazioni dell'indice.

3. Nella pagina Guida introduttiva, scegli Aggiungi origine dati.
4. Nella pagina Aggiungi origine dati, scegli Confluence connector V1.0, quindi scegli Aggiungi origine dati.
5. Nella pagina Specificare i dettagli dell'origine dati, inserisci le seguenti informazioni:
   a. In Nome e descrizione, per Nome dell'origine dati, inserisci un nome per l'origine dati. Puoi includere trattini ma non spazi.
   b. (Facoltativo) Descrizione: immetti una descrizione facoltativa per la tua fonte di dati.
   c. In Lingua predefinita: scegli una lingua per filtrare i documenti per l'indice. Se non diversamente specificato, la lingua predefinita è l'inglese. La lingua specificata nei metadati del documento ha la precedenza sulla lingua selezionata.
   d. In Tag, per Aggiungi nuovo tag, includi tag opzionali per cercare e filtrare le risorse o tenere traccia dei costi. AWS
   e. Seleziona Successivo.
6. Nella pagina Definisci accesso e sicurezza, inserisci le seguenti informazioni:
   a. Scegli tra il cloud Confluence e il server Confluence in base al tuo caso d'uso.
   b. Se scegli Confluence cloud, inserisci le seguenti informazioni:
      i. Confluence URL: il tuo URL di Confluence.
      ii. AWS Secrets Manager segreto: scegli un segreto esistente o creane uno nuovo per archiviare le credenziali di autenticazione Secrets Manager Confluence. Se scegli di creare un nuovo segreto, si apre una finestra segreta. AWS Secrets Manager
         - Inserisci le seguenti informazioni nella finestra Crea un AWS Secrets Manager segreto:

I. Nome segreto: un nome per il tuo segreto. Il prefisso 'AmazonKendra-Confluence-' viene aggiunto automaticamente al tuo nome segreto.

II. Per nome utente e password: inserisci il tuo nome utente Confluence e il token API Confluence come password.

III. Scegli Salva autenticazione.

c. Se scegli il server Confluence, inserisci le seguenti informazioni:

i. URL Confluence: nome utente e password di Confluence.

ii. (Facoltativo) Per il proxy Web, inserisci le seguenti informazioni:

A. Nome host: nome host per il tuo account Confluence.

B. Numero di porta: porta utilizzata dal protocollo di trasporto degli URL dell'host.

iii. Scegli tra l'autenticazione di base e il token di accesso personale.

iv. AWS Secrets Manager segreto: scegli un segreto esistente o creane uno nuovo Secrets Manager per archiviare le credenziali di autenticazione Confluence. Se scegli di creare un nuovo segreto, si apre una finestra segreta. AWS Secrets Manager

- Inserisci le seguenti informazioni nella finestra Crea un AWS Secrets Manager segreto:

I. Nome segreto: un nome per il tuo segreto. Il prefisso 'AmazonKendra-Confluence-' viene aggiunto automaticamente al tuo nome segreto.

II. Per nome utente e password: inserisci i valori delle credenziali di autenticazione che hai generato e scaricato dal tuo account Confluence. Se utilizzi l'autenticazione di base, usa il nome utente e la password di Confluence come credenziale di autenticazione. Se utilizzi un token di accesso personale, inserisci i dettagli del token di accesso personale che hai creato nel tuo account Confluence.

III. Scegli Salva autenticazione.

d. IAM ruolo: scegli un IAM ruolo esistente o crea un nuovo IAM ruolo per accedere alle credenziali del repository e indicizzare il contenuto.

> **Note**
>
> IAM i ruoli utilizzati per gli indici non possono essere utilizzati per le fonti di dati. Se non sei sicuro che un ruolo esistente venga utilizzato per un indice o una FAQ, scegli Crea un nuovo ruolo per evitare errori.

e. Seleziona Successivo.

7. Nella pagina Configura le impostazioni di sincronizzazione, inserisci le seguenti informazioni:

   a. Per Includi spazi personali e Includi spazi archiviati, scegli i tipi di spazio opzionali da includere in questa fonte di dati.

   b. Per una configurazione aggiuntiva: specifica i modelli di espressioni regolari per includere o escludere determinati contenuti. È possibile aggiungere fino a 100 pattern.

   c. Puoi anche scegliere di eseguire la scansione degli allegati all'interno degli spazi scelti.

   d. In Sincronizza la pianificazione dell'esecuzione, per Frequenza: scegli la frequenza con cui eseguire la sincronizzazione con la tua fonte di dati. Amazon Kendra

   e. Seleziona Successivo.

8. Nella pagina Imposta le mappature dei campi, inserisci le seguenti informazioni:

   a. Per Space, Page, Blog: seleziona tra i campi delle origini dati predefiniti Amazon Kendra generati o le mappature di campo aggiuntive suggerite per aggiungere campi indice.

   b. Aggiungi campo: consente di aggiungere campi di origine dati personalizzati per creare un nome di campo indice a cui mappare e il tipo di dati del campo.

   c. Seleziona Successivo.

9. Nella pagina Rivedi e crea, verifica che le informazioni inserite siano corrette, quindi seleziona Aggiungi origine dati. Puoi anche scegliere di modificare le tue informazioni da questa pagina. L'origine dati verrà visualizzata nella pagina Origini dati dopo che l'origine dati sarà stata aggiunta correttamente.

API

Per connettersi Amazon Kendra a Confluence

È necessario specificare quanto segue utilizzando ConfluenceConfigurationl'API:

- Versione Confluence: specifica la versione dell'istanza di Confluence che stai utilizzando come o. CLOUD SERVER
- Secret Amazon Resource Name (ARN): fornisci l'Amazon Resource Name (ARN) di un Secrets Manager segreto che contiene le credenziali di autenticazione che hai creato nel tuo account Confluence.

  Se utilizzi Confluence Server, puoi utilizzare il nome utente e la password di Confluence o il token di accesso personale come credenziali.

  Quando usi il nome utente e la password di Confluence come credenziali di autenticazione, memorizzi le seguenti credenziali come struttura JSON nel tuo segreto: Secrets Manager

```
{
    "username": "user name",
    "password": "password"
}
```

  Se utilizzi un token di accesso personale per connettere Confluence Server Amazon Kendra, memorizzi le seguenti credenziali come struttura JSON nel tuo segreto: Secrets Manager

```
{
    "patToken": "personal access token"
}
```

  Se utilizzi Confluence Cloud come fonte di Amazon Kendra dati, come password utilizzi il tuo nome utente Confluence e un token API generato nel tuo account Confluence. Memorizzi le seguenti credenziali come struttura JSON nel tuo segreto: Secrets Manager

```
{
    "username": "user name",
    "password": "API token"
}
```

  > **Note**
  >
  > Ti consigliamo di aggiornare o ruotare regolarmente le credenziali e il segreto. Fornisci solo il livello di accesso necessario per la tua sicurezza. Non è consigliabile riutilizzare

credenziali e segreti tra diverse fonti di dati e versioni dei connettori 1.0 e 2.0 (ove applicabile).

- IAM ruolo: specifica `RoleArn` quando chiami `CreateDataSource` per fornire a un IAM ruolo le autorizzazioni per accedere al tuo Secrets Manager segreto e per chiamare le API pubbliche richieste per il connettore Confluence e. Amazon Kendra Per ulteriori informazioni, consulta i IAM ruoli per le fonti di dati Confluence.

Puoi anche aggiungere le seguenti funzionalità opzionali:

- Proxy Web: indica se connettersi all'istanza URL di Confluence tramite un proxy Web. Puoi utilizzare questa opzione per Confluence Server.
- (Solo per Confluence Server) Virtual Private Cloud (VPC)`VpcConfiguration`: specifica come parte della configurazione dell'origine dati. Vedi Configurazione Amazon Kendra per l'uso di un VPC.
- Filtri di inclusione ed esclusione: specificate i modelli di espressioni regolari per includere o escludere determinati spazi, post del blog, pagine, spazi e allegati. Se scegli di indicizzare gli allegati, vengono indicizzati solo gli allegati alle pagine e ai blog indicizzati.

> **Note**
>
> La maggior parte delle fonti di dati utilizza modelli di espressioni regolari, che sono modelli di inclusione o esclusione denominati filtri. Se si specifica un filtro di inclusione, viene indicizzato solo il contenuto che corrisponde al filtro di inclusione. Qualsiasi documento che non corrisponde al filtro di inclusione non viene indicizzato. Se si specifica un filtro di inclusione ed esclusione, i documenti che corrispondono al filtro di esclusione non vengono indicizzati, anche se corrispondono al filtro di inclusione.

- Mappature dei campi: scegli di mappare i campi delle sorgenti dati di Confluence ai campi indice. Amazon Kendra Per ulteriori informazioni, consulta la sezione Mappatura dei campi di origine dei dati.

> **Note**
>
> Il campo del corpo del documento o l'equivalente del corpo del documento per i documenti è necessario per eseguire la ricerca nei documenti. Amazon Kendra È

necessario mappare il nome del campo del corpo del documento nella fonte dati al nome del campo indice_`document_body`. Tutti gli altri campi sono facoltativi.

- Filtraggio del contesto utente e controllo degli accessi:Amazon Kendra esegue la scansione dell'elenco di controllo degli accessi (ACL) dei documenti, se disponi di un ACL per i documenti. Le informazioni ACL vengono utilizzate per filtrare i risultati della ricerca in base all'accesso dell'utente o del relativo gruppo ai documenti. Per ulteriori informazioni, consulta Filtraggio del contesto utente.

Ulteriori informazioni

Per saperne di più sull'integrazione Amazon Kendra con la tua fonte di dati Confluence, consulta:

- Configurazione del connettore Confluence Server Amazon Kendra

Connettore Confluence V2.0

Confluence è uno strumento collaborativo di gestione del lavoro progettato per condividere, archiviare e lavorare sulla pianificazione di progetti, lo sviluppo di software e la gestione dei prodotti. Puoi utilizzarlo Amazon Kendra per indicizzare gli spazi, le pagine (incluse le pagine annidate), i blog e i commenti e gli allegati di Confluence a pagine e blog indicizzati.

Per la risoluzione dei problemi relativi al connettore di origine dati Confluence, consulta. Amazon Kendra Risoluzione dei problemi relativi alle origini dati

Argomenti

- Funzionalità supportate
- Prerequisiti
- Istruzioni di connessione

Funzionalità supportate

Amazon Kendra Il connettore di origine dati Confluence supporta le seguenti funzionalità:

- Mappature dei campi
- Filtraggio del contesto utente
- Modelli di inclusione/esclusione

- Sincronizzazione completa e incrementale dei contenuti
- Virtual Private Cloud (VPC) (Cloud privato virtuale (VPC)

Prerequisiti

Prima di poterla utilizzare Amazon Kendra per indicizzare la tua fonte di dati Confluence, apporta queste modifiche a Confluence e agli account. AWS

In Confluence, assicurati di avere:

- Hai copiato l'URL dell'istanza Confluence. Ad esempio: *https://example.confluence.com*, *https://www.example.confluence.com/* o *https:*//atlassian.net/. È necessario l'URL dell'istanza Confluence a cui connetterti. Amazon Kendra

  Se utilizzi Confluence Cloud, l'URL dell'host deve terminare con atlassian.net/.

  > **Note**
  >
  > I seguenti formati di URL non sono supportati:
  >
  > - *https://example.confluence.com/xyz*
  > - *https://www.example.confluence.com//wiki/spacekey/xxx*
  > - *https://atlassian.net/xyz*

  > **Note**
  >
  > (On-premise/server) Amazon Kendra verifica se le informazioni sull'endpoint incluse sono le stesse informazioni sull'endpoint specificate nei dettagli di configurazione dell' AWS Secrets Manager origine dati. In questo modo si evita il problema del confuso vicario, ossia un problema di sicurezza in cui un utente non è autorizzato a eseguire un'azione ma lo utilizza Amazon Kendra come proxy per accedere al segreto configurato ed eseguire l'azione. Se successivamente modifichi le informazioni sull'endpoint, devi creare un nuovo segreto per sincronizzare queste informazioni.

- Credenziali di autenticazione di base configurate contenenti un nome utente (ID e-mail utilizzato per accedere a Confluence) e una password (password del server Confluence) per consentire

Amazon Kendra la connessione all'istanza Confluence. Per informazioni su come creare un token API Confluence, consulta Gestire i token API per il tuo account Atlassian.

- Facoltativo: credenziali OAuth 2.0 configurate contenenti una chiave dell'app Confluence, un segreto dell'app Confluence, un token di accesso Confluence e un token di aggiornamento Confluence per consentire la connessione all'istanza Confluence. Amazon Kendra Se il token di accesso scade, puoi utilizzare il token di aggiornamento per rigenerare il token di accesso e la coppia di token di aggiornamento. In alternativa, puoi ripetere la procedura di autorizzazione. Per ulteriori informazioni sui token di accesso, consulta Gestire i token di accesso OAuth.
- (Solo per Confluence Server) Facoltativo: hai configurato un token di accesso personale (PAT) contenente un token Confluence per consentire la connessione all'istanza Confluence. Amazon Kendra Per informazioni su come creare un token PAT, consulta Utilizzo dei token di accesso personali.

Nel tuo Account AWS, assicurati di avere:

- Ha creato un Amazon Kendra indice e, se si utilizza l'API, ha annotato l'ID dell'indice.
- Hai creato un IAM ruolo per la tua origine dati e, se utilizzi l'API, hai annotato l'ARN del IAM ruolo.

> **Note**
>
> Se modifichi il tipo di autenticazione e le credenziali, devi aggiornare il IAM ruolo per accedere all'ID AWS Secrets Manager segreto corretto.

- Ha archiviato le credenziali di autenticazione Confluence in un AWS Secrets Manager segreto e, se si utilizza l'API, ha annotato l'ARN del segreto.

> **Note**
>
> Ti consigliamo di aggiornare o ruotare regolarmente le credenziali e il segreto. Fornisci solo il livello di accesso necessario per la tua sicurezza. Non è consigliabile riutilizzare credenziali e segreti tra diverse fonti di dati e versioni dei connettori 1.0 e 2.0 (ove applicabile).

Se non disponi di un IAM ruolo o di un segreto esistente, puoi utilizzare la console per creare un nuovo IAM ruolo e un Secrets Manager segreto quando connetti l'origine dati Confluence a. Amazon

Kendra Se utilizzi l'API, devi fornire l'ARN di un IAM ruolo e di un Secrets Manager segreto esistenti e un ID di indice.

Istruzioni di connessione

Per connetterti Amazon Kendra alla tua fonte di dati Confluence, devi fornire i dettagli delle tue credenziali Confluence in modo da poter Amazon Kendra accedere ai tuoi dati. Se non hai ancora configurato Confluence for see. Amazon Kendra Prerequisiti

Console

Per connettersi a Confluence Amazon Kendra

1. Accedi alla console di AWS gestione e apri la Amazon Kendra console.
2. Dal riquadro di navigazione a sinistra, scegli Indici, quindi scegli l'indice che desideri utilizzare dall'elenco degli indici.

> **Note**
>
> Puoi scegliere di configurare o modificare le impostazioni del controllo dell'accesso degli utenti in Impostazioni dell'indice.

3. Nella pagina Guida introduttiva, scegli Aggiungi origine dati.
4. Nella pagina Aggiungi origine dati, scegli Confluence connector V2.0, quindi scegli Aggiungi connettore.
5. Nella pagina Specificare i dettagli dell'origine dati, inserisci le seguenti informazioni:
   a. In Nome e descrizione, per Nome dell'origine dati, inserisci un nome per l'origine dati. Puoi includere trattini ma non spazi.
   b. (Facoltativo) Descrizione: immetti una descrizione facoltativa per la tua fonte di dati.
   c. In Lingua predefinita: scegli una lingua per filtrare i documenti per l'indice. Se non diversamente specificato, la lingua predefinita è l'inglese. La lingua specificata nei metadati del documento ha la precedenza sulla lingua selezionata.
   d. In Tag, per Aggiungi nuovo tag, includi tag opzionali per cercare e filtrare le risorse o tenere traccia dei costi. AWS
   e. Seleziona Successivo.
6. Nella pagina Definisci accesso e sicurezza, inserisci le seguenti informazioni:

a. In Source, scegli tra Confluence Cloud e Confluence Server in base al metodo di hosting delle sorgenti dati Confluence.

b. URL Confluence: inserisci l'URL dell'host Confluence. *Il formato per l'URL host che inserisci è https://example.confluence.com.*

c. (Solo per Confluence Server) Posizione del certificato SSL: opzionale: inserisci il Amazon S3 percorso del file del certificato SSL per Confluence Server.

d. (Solo per Confluence Server) Proxy Web: opzionale: immettere il nome host del proxy Web (senza il `https://` protocollo `http://` o) e il numero di porta (porta utilizzata dal protocollo di trasporto degli URL dell'host). Il numero di porta deve essere un valore numerico compreso tra 0 e 65535.

e. (Solo per Confluence Server) Autorizzazione: scegli di abilitare l'Access Control List (ACL). Quindi, scegli tra Nome utente ed Email per selezionare il campo che desideri utilizzare per il controllo degli accessi.

f. Scegli tra l'autenticazione di base, l'autenticazione Oauth 2.0 e (solo per il server Confluence) l'autenticazione con token di accesso personale in base al tuo caso d'uso.

g. AWS Secrets Manager segreto: scegli un segreto esistente o crea un nuovo Secrets Manager segreto per archiviare le credenziali di autenticazione Confluence. Se scegli di creare un nuovo segreto, si apre una finestra segreta. AWS Secrets Manager Inserisci le seguenti informazioni nella finestra:

   i. Nome segreto: un nome per il tuo segreto. Il prefisso 'AmazonKendra-Confluence-' viene aggiunto automaticamente al tuo nome segreto.

   ii. Se utilizzi l'autenticazione di base, inserisci il nome segreto, il nome utente e la password (password del server Confluence) che hai generato e scaricato dal tuo account Confluence.

   Se utilizzi l'autenticazione OAuth2.0, inserisci il nome segreto, la chiave dell'app, il segreto dell'app, il token di accesso e il token di aggiornamento che hai creato nel tuo account Confluence.

   (Solo server Confluence) Se utilizzi l'autenticazione con token di accesso personale, inserisci il nome segreto e il token Confluence che hai creato nel tuo account Confluence.

   iii. Scegli Salva e aggiungi segreto.

h. In Configura VPC e gruppo di sicurezza, opzionale, per Virtual Private Cloud (VPC), puoi scegliere di utilizzare un VPC. In tal caso, è necessario aggiungere sottoreti e gruppi di sicurezza VPC.

i. Identity crawler: specifica se attivare il crawler di identità. Amazon Kendra Il crawler di identità utilizza le informazioni dell'elenco di controllo degli accessi (ACL) per i documenti per filtrare i risultati della ricerca in base all'accesso dell'utente o del gruppo di appartenenza ai documenti. Se disponi di un ACL per i tuoi documenti e scegli di utilizzarlo, puoi anche scegliere di attivare il crawler di identità per configurare il filtraggio Amazon Kendra del contesto utente dei risultati di ricerca. Altrimenti, se il crawler di identità è disattivato, tutti i documenti possono essere ricercati pubblicamente. Se desideri utilizzare il controllo degli accessi per i tuoi documenti e il crawler di identità è disattivato, in alternativa puoi utilizzare l'PutPrincipalMappingAPI per caricare le informazioni di accesso di utenti e gruppi per il filtraggio del contesto degli utenti.

j. IAM ruolo: scegli un IAM ruolo esistente o creane uno nuovo IAM per accedere alle credenziali del repository e indicizzare il contenuto.

> **Note**
>
> IAM i ruoli utilizzati per gli indici non possono essere utilizzati per le fonti di dati. Se non sei sicuro che un ruolo esistente venga utilizzato per un indice o una FAQ, scegli Crea un nuovo ruolo per evitare errori.

k. Seleziona Successivo.

7. Nella pagina Configura le impostazioni di sincronizzazione, inserisci le seguenti informazioni:

a. Nell'ambito di sincronizzazione, per sincronizzare i contenuti, scegli di sincronizzare i seguenti tipi di entità: Pagine, Commenti alla pagina, Allegati di pagina, Blog, commenti del blog, Allegati del blog, Spazi personali e Spazi archiviati.

> **Note**
>
> I commenti alla pagina e gli allegati della pagina possono essere selezionati solo se scegli di sincronizzare le pagine. I commenti e gli allegati del blog possono essere selezionati solo se scegli di sincronizzare i blog.

> **Important**
>
> Se non specifichi un pattern regex della chiave Space nella configurazione aggiuntiva, per impostazione predefinita, tutte le pagine e i blog verranno sottoposti a scansione.

b. Nella configurazione aggiuntiva per i modelli regex di Spaces, specifica se includere o escludere spazi specifici nell'indice utilizzando:

- Tasto spaziatore*: ad esempio, my-space-123.*

> **Note**
>
> Se non specifichi un pattern regex della chiave Space nella configurazione aggiuntiva, per impostazione predefinita, tutte le pagine e i blog verranno sottoposti a scansione.

- URL*: ad esempio,. *//MySite/MyDocuments*.
- Tipo di file: ad esempio, *.*\ .pdf, .*\ .txt*.

- Per la dimensione massima del file: specifica il limite di dimensione del file in MB che Amazon Kendra scansionerà. Amazon Kendra eseguirà la scansione solo dei file entro il limite di dimensione definito. La dimensione predefinita del file è 50 MB. La dimensione massima del file deve essere superiore a 0 MB e inferiore o uguale a 50 MB.

- Per i modelli di espressione regolare dei titoli delle entità: specifica i modelli di espressione regolare per includere o escludere determinati blog, pagine, commenti e allegati in base ai titoli.

> **Note**
>
> Se desideri eseguire la scansione di una pagina o sottopagina specifica, puoi utilizzare i modelli di espressione regolare del titolo della pagina per includere o escludere questa pagina.

c. Modalità di sincronizzazione: scegli come aggiornare l'indice quando il contenuto dell'origine dati cambia. Quando sincronizzi l'origine dati con Amazon Kendra per la prima volta, tutto il contenuto viene sottoposto a scansione e indicizzato per impostazione predefinita. Se la sincronizzazione iniziale non è riuscita, devi eseguire una sincronizzazione completa dei dati, anche se non scegli la sincronizzazione completa come opzione della modalità di sincronizzazione.

   - Sincronizzazione completa: indicizza di nuovo tutti i contenuti, sostituendo i contenuti esistenti ogni volta che l'origine dati si sincronizza con l'indice.
   - Sincronizzazione nuova, modificata ed eliminata: indicizza solo i contenuti nuovi, modificati ed eliminati ogni volta che l'origine dati si sincronizza con l'indice. Amazon Kendra può utilizzare il meccanismo dell'origine dati per tenere traccia delle modifiche ai contenuti e indicizzare i contenuti modificati dall'ultima sincronizzazione.

d. Pianificazione di esecuzione di In Sync, per Frequenza: con quale frequenza Amazon Kendra verrà eseguita la sincronizzazione con la fonte di dati.

e. Seleziona Successivo.

8. Nella pagina Imposta le mappature dei campi, inserisci le seguenti informazioni:

   a. Per Spazio, Pagina, Blog, Commento e Allegato: seleziona uno dei campi di origine dati predefiniti Amazon Kendra generati che desideri mappare all'indice.

   b. Aggiungi campo: consente di aggiungere campi di origine dati personalizzati per creare un nome di campo indice a cui mappare e il tipo di dati del campo.

   c. Seleziona Successivo.

9. Nella pagina Rivedi e crea, verifica che le informazioni inserite siano corrette, quindi seleziona Aggiungi origine dati. Puoi anche scegliere di modificare le tue informazioni da questa pagina. L'origine dati verrà visualizzata nella pagina Origini dati dopo che l'origine dati sarà stata aggiunta correttamente.

API

Per connettersi Amazon Kendra a Confluence

È necessario specificare un codice JSON dello schema dell'origine dati utilizzando l'API. TemplateConfiguration È necessario fornire le seguenti informazioni:

- Origine dati: specifica il tipo di origine dati come `CONFLUENCEV2` quando usi lo schema TemplateConfigurationJSON. Specificate anche l'origine dati come `TEMPLATE` quando chiamate l'CreateDataSourceAPI.
- URL host: specifica la versione dell'istanza host Confluence. *Ad esempio, https://example.confluence.com.*
- Modalità di sincronizzazione: specifica come Amazon Kendra aggiornare l'indice quando il contenuto dell'origine dati cambia. Quando sincronizzi l'origine dati con Amazon Kendra per la prima volta, tutto il contenuto viene sottoposto a scansione e indicizzato per impostazione predefinita. Se la sincronizzazione iniziale non è riuscita, devi eseguire una sincronizzazione completa dei dati, anche se non scegli la sincronizzazione completa come opzione della modalità di sincronizzazione. Puoi scegliere tra:
  - `FORCED_FULL_CRAWL`per indicizzare nuovamente tutti i contenuti, sostituendo i contenuti esistenti ogni volta che l'origine dati si sincronizza con l'indice.
  - `FULL_CRAWL`per indicizzare solo i contenuti nuovi, modificati ed eliminati ogni volta che l'origine dati si sincronizza con l'indice. Amazon Kendra può utilizzare il meccanismo dell'origine dati per tenere traccia delle modifiche ai contenuti e indicizzare i contenuti modificati dall'ultima sincronizzazione.
- Tipo di autenticazione: specifica il tipo di autenticazione, se `BasicOAuth2`, `Personal-token` per l'istanza di Confluence.
- (Facoltativo, solo per Confluence Server) Posizione del certificato SSL: specifica l'e che hai utilizzato per archiviare il certificato SSL. `S3bucketName` `s3certificateName`
- Secret Amazon Resource Name (ARN): fornisci l'Amazon Resource Name (ARN) di un Secrets Manager segreto che contiene le credenziali di autenticazione che hai creato nel tuo account Confluence. Se utilizzi l'autenticazione di base dell'account, il segreto viene archiviato in una struttura JSON con le seguenti chiavi:

```
{
    "username": "Confluence account user name",
    "password": "Confluence API token"
```

```
}
```

Se utilizzi l'autenticazione OAuth 2.0, il segreto viene archiviato in una struttura JSON con le seguenti chiavi:

```
{
    "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"
}
```

(Solo per Confluence Server) Se utilizzi l'autenticazione di base, il segreto viene archiviato in una struttura JSON con le seguenti chiavi:

```
{
    "hostUrl": "Confluence Server host URL",
    "username": "Confluence Server user name",
    "password": "Confluence Server password"
}
```

(Solo per Confluence Server) Se utilizzi l'autenticazione con token di accesso personale, il segreto viene archiviato in una struttura JSON con le seguenti chiavi:

```
{
    "hostUrl": "Confluence Server host URL",
    "patToken": "Confluence token"
}
```

> **Note**
>
> Ti consigliamo di aggiornare o ruotare regolarmente le credenziali e il segreto. Fornisci solo il livello di accesso necessario per la tua sicurezza. Non è consigliabile riutilizzare credenziali e segreti tra diverse fonti di dati e versioni dei connettori 1.0 e 2.0 (ove applicabile).

- IAM ruolo: specifica `RoleArn` quando chiami `CreateDataSource` per fornire a un IAM ruolo le autorizzazioni per accedere al tuo Secrets Manager segreto e per chiamare le API pubbliche

richieste per il connettore Confluence e. Amazon Kendra Per ulteriori informazioni, consulta i IAM ruoli per le fonti di dati Confluence.

Puoi anche aggiungere le seguenti funzionalità opzionali:

- Virtual Private Cloud (VPC): `VpcConfiguration` specifica quando si chiama. `CreateDataSource` Per ulteriori informazioni, consulta Configurazione Amazon Kendra per l'utilizzo di un Amazon VPC.
- Filtri di inclusione ed esclusione: puoi specificare se includere o escludere determinati spazi, pagine, blog e relativi commenti e allegati.

  > **Note**
  >
  > La maggior parte delle fonti di dati utilizza modelli di espressioni regolari, che sono modelli di inclusione o esclusione denominati filtri. Se si specifica un filtro di inclusione, viene indicizzato solo il contenuto che corrisponde al filtro di inclusione. Qualsiasi documento che non corrisponde al filtro di inclusione non viene indicizzato. Se si specifica un filtro di inclusione ed esclusione, i documenti che corrispondono al filtro di esclusione non vengono indicizzati, anche se corrispondono al filtro di inclusione.

- Identity crawler: specifica se attivare il crawler di identità. Amazon Kendra Il crawler di identità utilizza le informazioni dell'elenco di controllo degli accessi (ACL) per i documenti per filtrare i risultati della ricerca in base all'accesso dell'utente o del gruppo di appartenenza ai documenti. Se disponi di un ACL per i tuoi documenti e scegli di utilizzarlo, puoi anche scegliere di attivare il crawler di identità per configurare il filtraggio Amazon Kendra del contesto utente dei risultati di ricerca. Altrimenti, se il crawler di identità è disattivato, tutti i documenti possono essere ricercati pubblicamente. Se desideri utilizzare il controllo degli accessi per i tuoi documenti e il crawler di identità è disattivato, in alternativa puoi utilizzare l'PutPrincipalMappingAPI per caricare le informazioni di accesso di utenti e gruppi per il filtraggio del contesto degli utenti.
- Mappature dei campi: scegli di mappare i campi delle sorgenti dati di Confluence ai campi indice. Amazon Kendra Per ulteriori informazioni, consulta la sezione Mappatura dei campi di origine dei dati.

  > **Note**
  >
  > Il campo del corpo del documento o l'equivalente del corpo del documento per i documenti è necessario per eseguire la ricerca nei documenti. Amazon Kendra È

necessario mappare il nome del campo del corpo del documento nella fonte dati al nome del campo indice `_document_body`. Tutti gli altri campi sono facoltativi.

Per un elenco di altre importanti chiavi JSON da configurare, consultaSchema del modello Confluence.

Note

- Il Personal Access Token (PAT) non è disponibile per Confluence Cloud.

Connettore sorgente dati personalizzato

Utilizza un'origine dati personalizzata quando disponi di un repository che Amazon Kendra non fornisce ancora un connettore per l'origine dati per. Puoi usarlo per visualizzare le stesse metriche della cronologia delle esecuzioni fornite dalle fonti di Amazon Kendra dati anche quando non puoi utilizzare le sorgenti dati Amazon Kendra di origine per sincronizzare i tuoi repository. Utilizzalo per creare un'esperienza di monitoraggio della sincronizzazione coerente tra le fonti di Amazon Kendra dati e quelle personalizzate. In particolare, utilizza un'origine dati personalizzata per visualizzare le metriche di sincronizzazione per un connettore di origine dati creato utilizzando le BatchDeleteDocumentAPI BatchPutDocumente.

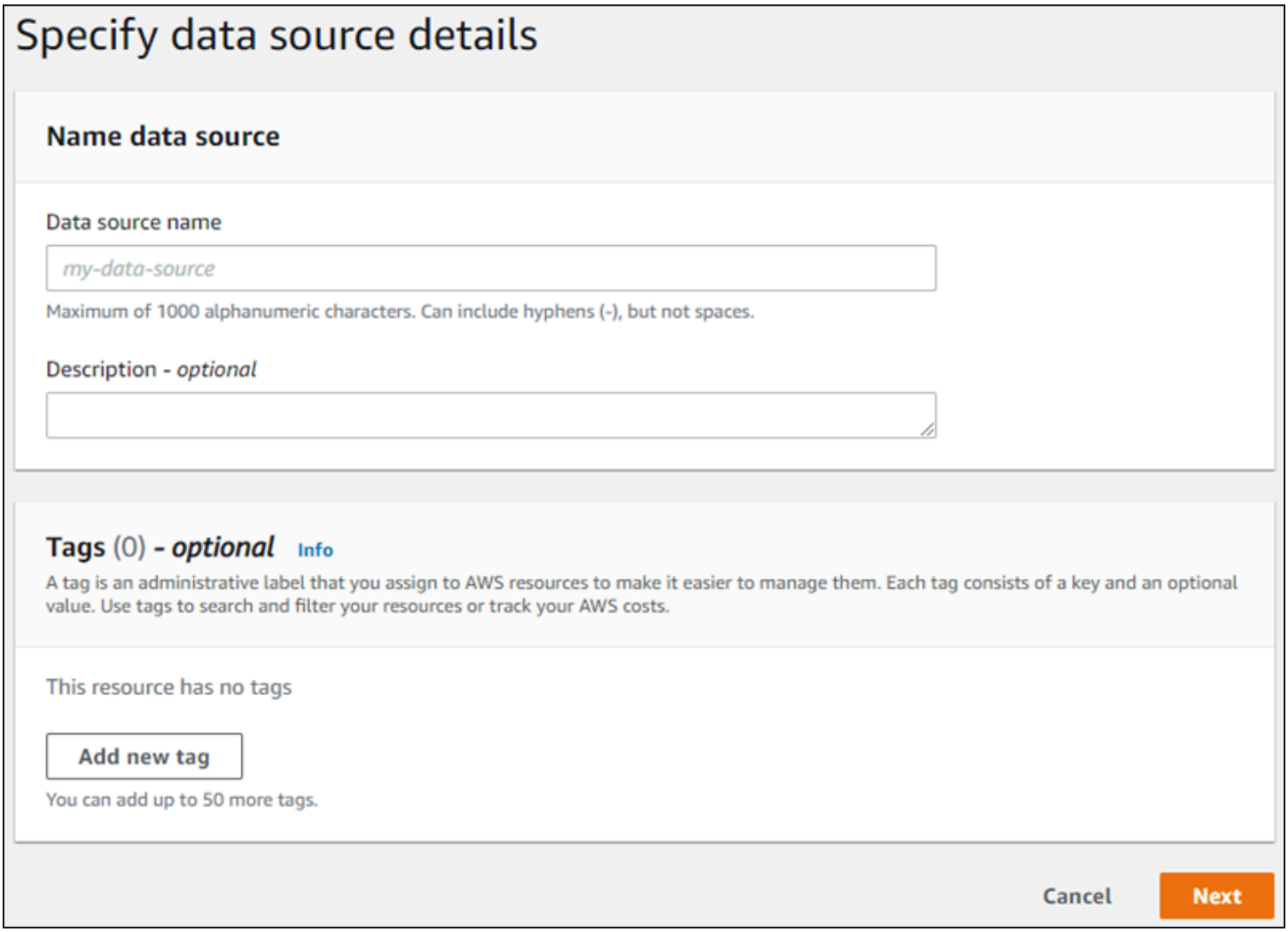
Per la risoluzione dei problemi relativi al connettore di origine dati personalizzato Amazon Kendra, consulta. Risoluzione dei problemi relativi alle origini dati

Quando crei un'origine dati personalizzata, hai il controllo completo su come vengono selezionati i documenti da indicizzare. Amazon Kendrafornisce solo informazioni metriche che è possibile utilizzare per monitorare i processi di sincronizzazione delle sorgenti dati. È necessario creare ed eseguire il crawler che determina i documenti indicizzati dalla fonte di dati.

È necessario specificare il titolo principale dei documenti utilizzando l'oggetto Document e `_source_uri` per `DocumentURI` includerlo nella risposta del risultato. DocumentAttribute`DocumentTitleQuery`

È possibile creare un identificatore per l'origine dati personalizzata utilizzando la console o l'CreateDataSourceAPI. Per utilizzare la console, assegna un nome alla fonte di dati e, facoltativamente, una descrizione e dei tag delle risorse. Dopo aver creato l'origine dati, viene

visualizzato un ID dell'origine dati. Copia questo ID per utilizzarlo quando sincronizzi l'origine dati con l'indice.



Puoi anche creare un'origine dati personalizzata utilizzando l'`CreateDataSource`API. L'API restituisce un ID da utilizzare quando sincronizzi l'origine dati. Quando utilizzi l'`CreateDataSource`API per creare un'origine dati personalizzata, non puoi impostare i `Configuration` `Schedule` parametri `RoleArn` o. Se imposti questi parametri, Amazon Kendra restituisce un'`ValidationException`eccezione.

Per utilizzare un'origine dati personalizzata, create un'applicazione responsabile dell'aggiornamento dell'Amazon Kendraindice. L'applicazione dipende dal crawler creato dall'utente. Il crawler legge i documenti presenti nel repository e determina a quali devono essere inviati. Amazon Kendra L'applicazione deve eseguire le seguenti operazioni:

1. Scansiona il tuo repository e crea un elenco dei documenti in esso contenuti che sono stati aggiunti, aggiornati o eliminati.

2. Chiama l'StartDataSourceSyncJobAPI per segnalare che è in corso un processo di sincronizzazione. Fornisci un ID di origine dati per identificare l'origine dati da sincronizzare. Amazon Kendrarestituisce un ID di esecuzione per identificare un particolare processo di sincronizzazione.
3. Chiama l'BatchDeleteDocumentAPI per rimuovere i documenti dall'indice. Fornisci l'ID dell'origine dati e l'ID di esecuzione per identificare l'origine dati da sincronizzare e il processo a cui è associato questo aggiornamento.
4. Chiama l'StopDataSourceSyncJobAPI per segnalare la fine del processo di sincronizzazione. Dopo aver chiamato l'`StopDataSourceSyncJob`API, l'ID di esecuzione associato non è più valido.
5. Chiama l'ListDataSourceSyncJobsAPI con gli identificatori dell'indice e dell'origine dati per elencare i processi di sincronizzazione per l'origine dati e per visualizzare le metriche per i processi di sincronizzazione.

Dopo aver terminato un processo di sincronizzazione, puoi iniziare un nuovo processo di sincronizzazione. Può trascorrere un periodo di tempo prima che tutti i documenti inviati vengano aggiunti all'indice. Utilizza l'`ListDataSourceSyncJobs`API per visualizzare lo stato del processo di sincronizzazione. Se il risultato `Status` del processo di sincronizzazione è`SYNCING_INDEXING`, alcuni documenti sono ancora in fase di indicizzazione. È possibile avviare un nuovo processo di sincronizzazione quando lo stato del lavoro precedente è `FAILED` o. `SUCCEEDED`

Dopo aver chiamato l'`StopDataSourceSyncJob`API, non puoi utilizzare un identificatore del processo di sincronizzazione in una chiamata alle `BatchDeleteDocument` API `BatchPutDocument` o. In tal caso, tutti i documenti inviati vengono restituiti nel messaggio di `FailedDocuments` risposta dell'API.

Attributi obbligatori

Quando invii un documento all'Amazon Kendrautilizzo dell'`BatchPutDocument`API, ogni documento richiede due attributi per identificare la fonte di dati e l'esecuzione di sincronizzazione a cui appartiene. È necessario fornire i seguenti due attributi per mappare correttamente i documenti dall'origine dati personalizzata a un Amazon Kendra indice:

- `_data_source_id`—L'identificatore della fonte di dati. Viene restituito quando si crea l'origine dati con la console o l'`CreateDataSource`API.

- `_data_source_sync_job_execution_id`—L'identificatore dell'esecuzione di sincronizzazione. Viene restituito quando si avvia la sincronizzazione dell'indice con l'API. `StartDataSourceSyncJob`

Di seguito è riportato il codice JSON necessario per indicizzare un documento utilizzando un'origine dati personalizzata.

```
{
    "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"
}
```

Quando rimuovi un documento dall'indice utilizzando l'`BatchDeleteDocument`API, devi specificare i due campi seguenti nel `DataSourceSyncJobMetricTarget` parametro:

- `DataSourceId`—L'identificatore della fonte di dati. Viene restituito quando si crea l'origine dati con la console o l'`CreateDataSource`API.
- `DataSourceSyncJobId`—L'identificatore dell'esecuzione di sincronizzazione. Viene restituito quando si avvia la sincronizzazione dell'indice con l'API. `StartDataSourceSyncJob`

Di seguito è riportato il codice JSON necessario per eliminare un documento dall'indice utilizzando l'`BatchDeleteDocument`API.

```
{
    "DataSourceSyncJobMetricTarget": {
        "DataSourceId": "data source identifier",
        "DataSourceSyncJobId": "sync job identifier"
    },
    "DocumentIdList": [
        "document identifier"
    ],
    "IndexId": "index identifier"
}
```

Visualizzazione dei parametri

Al termine di un processo di sincronizzazione, puoi utilizzare l'DataSourceSyncJobMetricsAPI per ottenere le metriche associate al processo di sincronizzazione. Usala per monitorare le sincronizzazioni delle sorgenti dati personalizzate.

Se invii lo stesso documento più volte, come parte dell'`BatchPutDocument`API, dell'API o se il `BatchDeleteDocument` documento viene inviato sia per l'aggiunta che per l'eliminazione, il documento viene conteggiato una sola volta nelle metriche.

- `DocumentsAdded`—Il numero di documenti inviati utilizzando l'`BatchPutDocument`API associata a questo processo di sincronizzazione aggiunti all'indice per la prima volta. Se un documento viene inviato per l'aggiunta più di una volta in una sincronizzazione, il documento viene conteggiato solo una volta nelle metriche.
- `DocumentsDeleted`—Il numero di documenti inviati utilizzando l'`BatchDeleteDocument`API associata a questo processo di sincronizzazione è stato eliminato dall'indice. Se un documento viene inviato per l'eliminazione più di una volta in una sincronizzazione, il documento viene conteggiato solo una volta nelle metriche.
- `DocumentsFailed`—Il numero di documenti associati a questo processo di sincronizzazione la cui indicizzazione non è riuscita. Si tratta di documenti che sono stati accettati Amazon Kendra per l'indicizzazione ma che non è stato possibile indicizzare o eliminare. Se un documento non viene accettato daAmazon Kendra, l'identificatore del documento viene restituito nella proprietà di `FailedDocuments` risposta delle API and. `BatchPutDocument` `BatchDeleteDocument`

- `DocumentsModified`—Il numero di documenti modificati inviati utilizzando l'`BatchPutDocument`API associata a questo processo di sincronizzazione che sono stati modificati nell'indice. Amazon Kendra

Amazon Kendraemette Amazon CloudWatch metriche anche durante l'indicizzazione dei documenti. Per ulteriori informazioni, consulta Monitoraggio con. Amazon KendraAmazon CloudWatch

Amazon Kendranon restituisce la `DocumentsScanned` metrica per le fonti di dati personalizzate. Emette anche le CloudWatch metriche elencate nel documento Metriche per le fonti di dati. Amazon Kendra

Ulteriori informazioni

Per ulteriori informazioni sull'integrazione Amazon Kendra con la tua fonte di dati personalizzata, consulta:

- Aggiungere fonti di dati personalizzate a Amazon Kendra

Fonte dati personalizzata (Java)

Il codice seguente fornisce un esempio di implementazione di un'origine dati personalizzata utilizzando Java. Il programma crea innanzitutto un'origine dati personalizzata e quindi sincronizza i nuovi documenti aggiunti all'indice con l'origine dati personalizzata.

Il codice seguente illustra la creazione e l'utilizzo di un'origine dati personalizzata. Quando si utilizza un'origine dati personalizzata nell'applicazione, non è necessario creare una nuova origine dati (processo una tantum) ogni volta che si sincronizza l'indice con l'origine dati. L'ID dell'indice e l'ID dell'origine dati vengono utilizzati per sincronizzare i dati.

```
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 è un servizio di file hosting che offre servizi di archiviazione su cloud, organizzazione dei documenti e creazione di modelli di documenti. Se sei un utente Dropbox, puoi utilizzarlo Amazon Kendra per indicizzare i tuoi file Dropbox, Dropbox Paper, i modelli di Dropbox Paper e i collegamenti memorizzati alle pagine web. Puoi anche configurare l'indicizzazione Amazon Kendra di file Dropbox specifici, modelli di Dropbox Paper, Dropbox Paper e collegamenti a pagine web memorizzati.

Amazon Kendra supporta sia Dropbox che Dropbox Advanced for Dropbox Business.

Puoi connetterti Amazon Kendra alla tua fonte di dati Dropbox utilizzando la Amazon Kendra console e l'API. TemplateConfiguration

Per la risoluzione dei problemi relativi al connettore di origine dati Amazon Kendra di Dropbox, consulta. Risoluzione dei problemi relativi alle origini dati

Argomenti

- Funzionalità supportate
- Prerequisiti
- Istruzioni di connessione
- Ulteriori informazioni

Funzionalità supportate

Amazon Kendra Il connettore di origine dati di Dropbox supporta le seguenti funzionalità:

- Log delle modifiche

- Mappature dei campi
- Filtraggio del contesto utente
- Filtri di inclusione/esclusione
- Virtual Private Cloud (VPC) (Cloud privato virtuale (VPC)

Prerequisiti

Prima di poterla utilizzare Amazon Kendra per indicizzare la tua fonte di dati Dropbox, apporta queste modifiche al tuo Dropbox e ai tuoi account. AWS

In Dropbox, assicurati di avere:

- Hai creato un account Dropbox Advanced e configurato un utente amministratore.
- Hai creato un'app Dropbox con un nome di app univoco, hai attivato Scoped Access. Consulta la documentazione di Dropbox sulla creazione di un'app.
- Ha attivato le autorizzazioni complete di Dropbox sulla console Dropbox e ha aggiunto le seguenti autorizzazioni:
  - files.content.read
  - file.metadata.read
  - condivisione.read
  - file_requests.read
  - gruppi.leggi
  - team_info.leggi
  - team_data.content.leggi
- Hai annotato la chiave dell'app Dropbox, il segreto dell'app Dropbox e il token di accesso Dropbox per le credenziali di autenticazione di base.
- Hai generato e copiato un token di accesso Oauth 2.0 temporaneo per la tua app Dropbox. Questo token è temporaneo e scade dopo 4 ore. Consulta la documentazione di Dropbox sull'autenticazione OAuth.

> **Note**
>
> Ti consigliamo di creare un token di accesso di aggiornamento di Dropbox che non scada mai, anziché affidarti a un token di accesso monouso che scada dopo 4 ore. Un token

di accesso di aggiornamento è permanente e non scade mai, quindi puoi continuare a sincronizzare la tua fonte di dati in futuro.

- Consigliato: hai configurato un token di aggiornamento permanente di Dropbox che non scade mai per consentire di continuare Amazon Kendra a sincronizzare la fonte di dati senza interruzioni. Consulta la documentazione di Dropbox sui token di aggiornamento.
- Checked: ogni documento è unico in Dropbox e tra le altre fonti di dati che intendi utilizzare per lo stesso indice. Ogni fonte di dati che desideri utilizzare per un indice non deve contenere lo stesso documento in tutte le fonti di dati. Gli ID dei documenti sono globali rispetto a un indice e devono essere univoci per indice.

Nel tuo Account AWS, assicurati di avere:

- Ha creato un Amazon Kendra indice e, se si utilizza l'API, ha annotato l'ID dell'indice.
- Hai creato un IAM ruolo per la tua origine dati e, se utilizzi l'API, hai annotato l'ARN del IAM ruolo.

> **Note**
>
> Se modifichi il tipo di autenticazione e le credenziali, devi aggiornare il IAM ruolo per accedere all'ID AWS Secrets Manager segreto corretto.

- Hai archiviato le credenziali di autenticazione Dropbox in un AWS Secrets Manager luogo segreto e, se utilizzi l'API, hai annotato l'ARN del segreto.

> **Note**
>
> Ti consigliamo di aggiornare o ruotare regolarmente le credenziali e il segreto. Fornisci solo il livello di accesso necessario per la tua sicurezza. Non è consigliabile riutilizzare credenziali e segreti tra diverse fonti di dati e versioni dei connettori 1.0 e 2.0 (ove applicabile).

Se non disponi di un IAM ruolo o di un segreto esistente, puoi utilizzare la console per creare un nuovo IAM ruolo e un Secrets Manager segreto quando colleghi la tua fonte di dati Dropbox a. Amazon Kendra Se utilizzi l'API, devi fornire l'ARN di un IAM ruolo e di un Secrets Manager segreto esistenti e un ID di indice.

Istruzioni di connessione

Per connetterti Amazon Kendra alla tua fonte di dati Dropbox, devi fornire i dettagli necessari della tua fonte di dati Dropbox in modo che Amazon Kendra possa accedere ai tuoi dati. Se non hai ancora configurato Dropbox per Amazon Kendra, consulta. Prerequisiti

Console

Per connetterti a Amazon Kendra Dropbox

1. Accedi a AWS Management Console e apri la Amazon Kendra console.
2. Dal riquadro di navigazione a sinistra, scegli Indici, quindi scegli l'indice che desideri utilizzare dall'elenco degli indici.

> **Note**
>
> Puoi scegliere di configurare o modificare le impostazioni del controllo dell'accesso degli utenti in Impostazioni dell'indice.

3. Nella pagina Guida introduttiva, scegli Aggiungi origine dati.
4. Nella pagina Aggiungi sorgente dati, scegli Connettore Dropbox, quindi scegli Aggiungi connettore.
5. Nella pagina Specificare i dettagli dell'origine dati, inserisci le seguenti informazioni:
   a. In Nome e descrizione, per Nome dell'origine dati, inserisci un nome per l'origine dati. Puoi includere trattini ma non spazi.
   b. (Facoltativo) Descrizione: immetti una descrizione facoltativa per l'origine dati.
   c. In Lingua predefinita: scegli una lingua per filtrare i documenti per l'indice. Se non diversamente specificato, la lingua predefinita è l'inglese. La lingua specificata nei metadati del documento ha la precedenza sulla lingua selezionata.
   d. In Tag, per Aggiungi nuovo tag, includi tag opzionali per cercare e filtrare le risorse o tenere traccia dei costi. AWS
   e. Seleziona Successivo.
6. Nella pagina Definisci accesso e sicurezza, inserisci le seguenti informazioni:
   a. Tipo di token di autenticazione: scegli tra token permanente (consigliato) e token di accesso (uso temporaneo) in base al tuo caso d'uso.

b. AWS Secrets Manager segreto: scegli un segreto esistente o creane uno nuovo per archiviare le Secrets Manager credenziali di autenticazione di Dropbox. Se scegli di creare un nuovo segreto, si apre una finestra AWS Secrets Manager segreta.

   i. Inserisci le seguenti informazioni nella finestra Crea un AWS Secrets Manager segreto:

      A. Nome segreto: un nome per il tuo segreto. Il prefisso 'AmazonKendra-Dropbox-' viene aggiunto automaticamente al tuo nome segreto.

      B. Per le informazioni sulla chiave dell'app, sul segreto dell'app e sul token (permanenti o temporanee), inserisci i valori delle credenziali di autenticazione che hai generato dal tuo account Dropbox.

   ii. Selezionare Salva.

c. Virtual Private Cloud (VPC): puoi scegliere di utilizzare un VPC. In tal caso, è necessario aggiungere sottoreti e gruppi di sicurezza VPC.

d. IAM ruolo: scegli un IAM ruolo esistente o creane uno nuovo IAM per accedere alle credenziali del repository e indicizzare il contenuto.

> **Note**
>
> IAM i ruoli utilizzati per gli indici non possono essere utilizzati per le fonti di dati. Se non sei sicuro che un ruolo esistente venga utilizzato per un indice o una FAQ, scegli Crea un nuovo ruolo per evitare errori.

e. Seleziona Successivo.

7. Nella pagina Configura le impostazioni di sincronizzazione, inserisci le seguenti informazioni:

   a. Per selezionare entità o tipi di contenuto: scegli le entità o i tipi di contenuto che desideri sottoporre a scansione.

   b. Cambia modalità di registro: scegli di aggiornare l'indice solo con contenuti nuovi e modificati anziché sincronizzare tutti i file.

   c. Nella configurazione aggiuntiva per i modelli Regex: aggiungi modelli di espressioni regolari per includere o escludere determinati file.

   d. In Sincronizza la pianificazione dell'esecuzione, per la frequenza: scegli la frequenza con cui eseguire la sincronizzazione con la tua fonte di dati. Amazon Kendra

   e. Seleziona Successivo.

8. Nella pagina Imposta mappature dei campi, inserisci le seguenti informazioni:

   a. File, modelli di Dropbox Paper e Dropbox Paper: seleziona tra i campi di origine dati predefiniti Amazon Kendra generati che desideri mappare al tuo indice.

   b. Aggiungi campo: per aggiungere campi di origine dati personalizzati per creare un nome di campo indice a cui mappare e il tipo di dati del campo.

   c. Seleziona Successivo.

9. Nella pagina Rivedi e crea, verifica che le informazioni inserite siano corrette, quindi seleziona Aggiungi origine dati. Puoi anche scegliere di modificare le tue informazioni da questa pagina. L'origine dati verrà visualizzata nella pagina Origini dati dopo che l'origine dati sarà stata aggiunta correttamente.

API

Per connetterti Amazon Kendra a Dropbox

Devi specificare un codice JSON dello schema dell'origine dati utilizzando l'TemplateConfigurationAPI. È necessario fornire le seguenti informazioni:

- Origine dati: specifica il tipo di origine dati come `DROPBOX` quando usi lo schema TemplateConfigurationJSON. Specificate anche l'origine dati come `TEMPLATE` quando chiamate l'CreateDataSourceAPI.
- Registro delle modifiche: se Amazon Kendra utilizzare il meccanismo del registro delle modifiche all'origine dati di Dropbox per determinare se un documento deve essere aggiornato nell'indice.

  > **Note**
  >
  > Utilizza il registro delle modifiche se non desideri Amazon Kendra scansionare tutti i documenti. Se il registro delle modifiche è di grandi dimensioni, potrebbe essere necessario Amazon Kendra meno tempo per scansionare i documenti nella fonte dati Dropbox che per elaborare il registro delle modifiche. Se sincronizzi la fonte di dati di Dropbox con il tuo indice per la prima volta, tutti i documenti vengono scansionati.

- Secret Amazon Resource Name (ARN): fornisci l'Amazon Resource Name (ARN) di un Secrets Manager segreto che contiene le credenziali di autenticazione per il tuo account Dropbox. Il segreto è archiviato in una struttura JSON con le seguenti chiavi:

```
{
    "appKey": "Dropbox app key",
    "appSecret": "Dropbox app secret",
    "accesstoken": "temporary access token or refresh access token"
}
```

> **Note**
>
> Ti consigliamo di aggiornare o ruotare regolarmente le credenziali e il segreto. Fornisci solo il livello di accesso necessario per la tua sicurezza. Non è consigliabile riutilizzare credenziali e segreti tra diverse fonti di dati e versioni dei connettori 1.0 e 2.0 (ove applicabile).

- IAM ruolo: specifica `RoleArn` quando chiami `CreateDataSource` per fornire a un IAM ruolo le autorizzazioni per accedere al tuo Secrets Manager segreto e per chiamare le API pubbliche richieste per il connettore Dropbox e. Amazon Kendra Per ulteriori informazioni, consulta i IAM ruoli per le fonti di dati Dropbox.

Puoi anche aggiungere le seguenti funzionalità opzionali:

- Virtual Private Cloud (VPC): `VpcConfiguration` specifica quando si chiama. `CreateDataSource` Per ulteriori informazioni, consulta Configurazione Amazon Kendra per l'utilizzo di un Amazon VPC.
- Filtri di inclusione ed esclusione: specificano se includere o escludere determinati file.

> **Note**
>
> La maggior parte delle fonti di dati utilizza modelli di espressioni regolari, che sono modelli di inclusione o esclusione denominati filtri. Se si specifica un filtro di inclusione, viene indicizzato solo il contenuto che corrisponde al filtro di inclusione. Qualsiasi documento che non corrisponde al filtro di inclusione non viene indicizzato. Se si specifica un filtro di inclusione ed esclusione, i documenti che corrispondono al filtro di esclusione non vengono indicizzati, anche se corrispondono al filtro di inclusione.

- Filtro del contesto utente e controllo degli accessi:Amazon Kendra esegue la ricerca per indicizzazione dell'elenco di controllo degli accessi (ACL) dei documenti, se disponi di un ACL per i documenti. Le informazioni ACL vengono utilizzate per filtrare i risultati della ricerca

in base all'accesso dell'utente o del relativo gruppo ai documenti. Per ulteriori informazioni, consulta Filtraggio del contesto utente.

- Mappature dei campi: scegli di mappare i campi delle sorgenti dati di Dropbox ai campi dell'indice. Amazon Kendra Per ulteriori informazioni, consulta la sezione Mappatura dei campi di origine dei dati.

> **Note**
>
> Il campo del corpo del documento o l'equivalente del corpo del documento per i tuoi documenti è obbligatorio per Amazon Kendra poter cercare i tuoi documenti. È necessario mappare il nome del campo del corpo del documento nella fonte dati al nome del campo indice `_document_body`. Tutti gli altri campi sono facoltativi.

Per un elenco di altre importanti chiavi JSON da configurare, consultaSchema del modello Dropbox.

Ulteriori informazioni

Per ulteriori informazioni sull'integrazione di Amazon Kendra con la tua fonte di dati Dropbox, consulta:

- Indicizza i tuoi contenuti Dropbox utilizzando il connettore Dropbox per Amazon Kendra

Drupal

Drupal è un sistema di gestione dei contenuti (CMS) open source che puoi utilizzare per creare siti Web e applicazioni Web. È possibile utilizzare Amazon Kendra per indicizzare quanto segue in Drupal:

- Contenuto: articoli, pagine di base, blocchi di base, tipi di contenuto definiti dall'utente, tipi di blocchi definiti dall'utente, tipi di contenuto personalizzati, tipi di blocchi personalizzati
- Commento: per qualsiasi tipo di contenuto e tipo di blocco
- Allegati: per qualsiasi tipo di contenuto e tipo di blocco

Puoi connetterti Amazon Kendra alla tua fonte di dati Drupal utilizzando la console o l'Amazon Kendra API. TemplateConfiguration

Per la risoluzione dei problemi relativi al Amazon Kendra connettore di origine dati Drupal, consulta. Risoluzione dei problemi relativi alle origini dati

Argomenti

- Funzionalità supportate
- Prerequisiti
- Istruzioni di connessione
- Note

Funzionalità supportate

Amazon Kendra Il connettore di origine dati Drupal supporta le seguenti funzionalità:

- Mappature dei campi
- Filtraggio del contesto utente
- Filtri di inclusione/esclusione
- Sincronizzazione completa e incrementale dei contenuti
- Virtual Private Cloud (VPC) (Cloud privato virtuale (VPC)

Prerequisiti

Prima di poterla utilizzare Amazon Kendra per indicizzare la tua fonte di dati Drupal, apporta queste modifiche a Drupal e agli account. AWS

In Drupal, assicurati di avere:

- Hai creato un account Drupal (Standard) Suite e un utente con ruolo di amministratore.
- Ho copiato il nome del sito Drupal e configurato un URL host. <hostname><drupalsitename>Ad esempio, *https:///*.
- Credenziali di autenticazione di base configurate contenenti un nome utente (nome utente di accesso al sito Web Drupal) e una password (password del sito Web Drupal).
- Consigliato: ha configurato un token di credenziali OAuth 2.0. Usa questo token insieme alla concessione della password di Drupal, all'ID cliente, al segreto del client, al nome utente (nome

utente di accesso al sito Web Drupal) e alla password (password del sito Web Drupal) a cui connetterti. Amazon Kendra

- Aggiunte le seguenti autorizzazioni nel tuo account Drupal utilizzando un ruolo di amministratore:
  - amministrare i blocchi
  - amministra la visualizzazione di block_content
  - amministra i campi block_content
  - amministra la visualizzazione del modulo block_content
  - amministra le visualizzazioni
  - visualizzare gli indirizzi e-mail degli utenti
  - visualizza i propri contenuti inediti
  - visualizza le revisioni delle pagine
  - visualizza le revisioni degli articoli
  - visualizza tutte le revisioni
  - visualizza il tema di amministrazione
  - accedere ai contenuti
  - accedere alla panoramica dei contenuti
  - accedere ai commenti
  - contenuti di ricerca
  - panoramica dei file di accesso
  - accedere ai collegamenti contestuali

> **Note**
>
> Se esistono tipi di contenuto definiti dall'utente o tipi di blocchi definiti dall'utente, o se vengono aggiunti visualizzazioni e blocchi al sito Web di Drupal, è necessario fornire loro l'accesso come amministratore.

Nel tuo Account AWS, assicurati di avere:

- Ha creato un Amazon Kendra indice e, se si utilizza l'API, ha annotato l'ID dell'indice.
- Hai creato un IAM ruolo per la tua origine dati e, se utilizzi l'API, hai annotato l'ARN del IAM ruolo.

> **Note**
>
> Se modifichi il tipo di autenticazione e le credenziali, devi aggiornare il IAM ruolo per accedere all'ID AWS Secrets Manager segreto corretto.

- Ha archiviato le credenziali di autenticazione Drupal in un luogo AWS Secrets Manager segreto e, se si utilizza l'API, ha annotato l'ARN del segreto.

> **Note**
>
> Ti consigliamo di aggiornare o ruotare regolarmente le credenziali e il segreto. Fornisci solo il livello di accesso necessario per la tua sicurezza. Non è consigliabile riutilizzare credenziali e segreti tra diverse fonti di dati e versioni dei connettori 1.0 e 2.0 (ove applicabile).

Se non disponi di un IAM ruolo o di un segreto esistente, puoi utilizzare la console per creare un nuovo IAM ruolo e un Secrets Manager segreto quando connetti la tua fonte di dati Drupal a. Amazon Kendra Se utilizzi l'API, devi fornire l'ARN di un IAM ruolo e di un Secrets Manager segreto esistenti e un ID di indice.

Istruzioni di connessione

Per connetterti Amazon Kendra alla tua fonte di dati Drupal devi fornire i dettagli delle tue credenziali Drupal in modo da poter Amazon Kendra accedere ai tuoi dati. Se non hai ancora configurato Drupal, vedi. Amazon Kendra Prerequisiti

Console

Per connettersi Amazon Kendra a Drupal

1. Accedi a AWS Management Console e apri la Amazon Kendra console.
2. Dal riquadro di navigazione a sinistra, scegli Indici, quindi scegli l'indice che desideri utilizzare dall'elenco degli indici.

> **Note**
>
> Puoi scegliere di configurare o modificare le impostazioni del controllo dell'accesso degli utenti in Impostazioni dell'indice.

3. Nella pagina Guida introduttiva, scegli Aggiungi origine dati.
4. Nella pagina Aggiungi origine dati, scegli Connettore Drupal, quindi scegli Aggiungi connettore.
5. Nella pagina Specificare i dettagli dell'origine dati, inserisci le seguenti informazioni:
   a. In Nome e descrizione, per Nome dell'origine dati, inserisci un nome per l'origine dati. Puoi includere trattini ma non spazi.
   b. (Facoltativo) Descrizione: immetti una descrizione facoltativa per la tua fonte di dati.
   c. In Lingua predefinita: scegli una lingua per filtrare i documenti per l'indice. Se non diversamente specificato, la lingua predefinita è l'inglese. La lingua specificata nei metadati del documento ha la precedenza sulla lingua selezionata.
   d. In Tag, per Aggiungi nuovo tag, includi tag opzionali per cercare e filtrare le risorse o tenere traccia dei costi. AWS
   e. Seleziona Successivo.
6. Nella pagina Definisci accesso e sicurezza, inserisci le seguenti informazioni:
   a. In Source, for Host URL: l'URL host del tuo sito Drupal. <hostname><drupalsitename>Ad esempio, *https:///*.
   b. Per la posizione del certificato SSL: inserisci il percorso del certificato SSL memorizzato nel bucket. Amazon S3
   c. Autorizzazione: attiva o disattiva le informazioni dell'elenco di controllo degli accessi (ACL) per i tuoi documenti, se disponi di un ACL e desideri utilizzarlo per il controllo degli accessi. L'ACL specifica a quali documenti possono accedere utenti e gruppi. Le informazioni ACL vengono utilizzate per filtrare i risultati della ricerca in base all'accesso dell'utente o del relativo gruppo ai documenti. Per ulteriori informazioni, consulta Filtraggio del contesto utente.
   d. Per l'autenticazione: scegli tra l'autenticazione di base e l'autenticazione OAuth 2.0 in base al tuo caso d'uso.

e. AWS Secrets Manager segreto: scegli un segreto esistente o crea un nuovo Secrets Manager segreto per archiviare le credenziali di autenticazione Drupal. Se scegli di creare un nuovo segreto, si apre una finestra segreta. AWS Secrets Manager

   i. Inserisci le seguenti informazioni nella finestra Crea un AWS Secrets Manager segreto:

      A. Se hai scelto l'autenticazione di base, inserisci un nome segreto, il nome utente (nome utente del sito Drupal) e la password (password del sito Drupal) che hai copiato e scegli Salva e aggiungi segreto.

      B. Se hai scelto l'autenticazione OAuth 2.0, inserisci un nome segreto, un nome utente (nome utente del sito Drupal), una password (password del sito Drupal), un ID client e un segreto client generati nel tuo account Drupal e scegli Salva e aggiungi segreto.

   ii. Selezionare Salva.

f. Virtual Private Cloud (VPC): puoi scegliere di utilizzare un VPC. In tal caso, è necessario aggiungere sottoreti e gruppi di sicurezza VPC.

g. Identity crawler: specifica se attivare il crawler di identità. Amazon Kendra Il crawler di identità utilizza le informazioni dell'elenco di controllo degli accessi (ACL) per i documenti per filtrare i risultati della ricerca in base all'accesso dell'utente o del relativo gruppo ai documenti. Se disponi di un ACL per i tuoi documenti e scegli di utilizzarlo, puoi anche scegliere di attivare il crawler di identità per configurare il filtraggio Amazon Kendra del contesto utente dei risultati di ricerca. Altrimenti, se il crawler di identità è disattivato, tutti i documenti possono essere ricercati pubblicamente. Se desideri utilizzare il controllo degli accessi per i tuoi documenti e il crawler di identità è disattivato, in alternativa puoi utilizzare l'PutPrincipalMappingAPI per caricare le informazioni di accesso di utenti e gruppi per il filtraggio del contesto degli utenti.

h. IAM ruolo: scegli un IAM ruolo esistente o creane uno nuovo IAM per accedere alle credenziali del repository e indicizzare il contenuto.

> **Note**
>
> IAM i ruoli utilizzati per gli indici non possono essere utilizzati per le fonti di dati. Se non sei sicuro che un ruolo esistente venga utilizzato per un indice o una FAQ, scegli Crea un nuovo ruolo per evitare errori.

i. Seleziona Successivo.

7. Nella pagina Configura le impostazioni di sincronizzazione, inserisci le seguenti informazioni:

a. Per l'ambito di sincronizzazione, scegli una delle seguenti opzioni:

> **Note**
>
> Quando scegli di eseguire la scansione degli articoli, delle pagine di base e dei blocchi di base, i relativi campi predefiniti verranno sincronizzati automaticamente. Puoi anche scegliere di sincronizzare i loro commenti, allegati, campi personalizzati e altre entità personalizzate.

- Per le entità selezionate:
  - Articoli: scegli se eseguire la scansione degli articoli, dei relativi commenti, commenti e allegati.
  - Pagine di base: scegli se eseguire la scansione delle pagine di base, dei relativi commenti e dei relativi allegati.
  - Blocchi base: scegli se eseguire la scansione dei blocchi di base, dei relativi commenti e dei relativi allegati.
  - Puoi anche scegliere di aggiungere tipi di contenuto personalizzati e blocchi personalizzati.

b. Per una configurazione aggiuntiva, facoltativa:

- Per il pattern Regex: aggiungi modelli di espressioni regolari per includere o escludere titoli di entità e nomi di file specifici. È possibile aggiungere fino a 100 pattern.

c. Modalità di sincronizzazione: scegli come aggiornare l'indice quando il contenuto dell'origine dati cambia. Quando sincronizzi l'origine dati con Amazon Kendra per la prima volta, tutto il contenuto viene sottoposto a scansione e indicizzato per impostazione predefinita. Se la sincronizzazione iniziale non è riuscita, devi eseguire una sincronizzazione completa dei dati, anche se non scegli la sincronizzazione completa come opzione della modalità di sincronizzazione.

- Sincronizzazione completa: indicizza di nuovo tutti i contenuti, sostituendo i contenuti esistenti ogni volta che l'origine dati si sincronizza con l'indice.

- Sincronizzazione nuova, modificata ed eliminata: indicizza solo i contenuti nuovi, modificati ed eliminati ogni volta che l'origine dati si sincronizza con l'indice. Amazon Kendra può utilizzare il meccanismo dell'origine dati per tenere traccia delle modifiche ai contenuti e indicizzare i contenuti modificati dall'ultima sincronizzazione.

d. In Sync run schedulation, Frequenza: con quale frequenza Amazon Kendra verrà effettuata la sincronizzazione con la fonte di dati.

e. Seleziona Successivo.

8. Nella pagina Imposta le mappature dei campi, inserisci le seguenti informazioni:

a. Per Contenuto, Commenti e Allegati: seleziona uno dei campi di origine dati predefiniti Amazon Kendra generati che desideri mappare all'indice.

b. Aggiungi campo: consente di aggiungere campi di origine dati personalizzati per creare un nome di campo indice a cui mappare e il tipo di dati del campo.

c. Seleziona Successivo.

9. Nella pagina Rivedi e crea, verifica che le informazioni inserite siano corrette, quindi seleziona Aggiungi origine dati. Puoi anche scegliere di modificare le tue informazioni da questa pagina. L'origine dati verrà visualizzata nella pagina Origini dati dopo che l'origine dati sarà stata aggiunta correttamente.

API

Per connettersi Amazon Kendra a Drupal

È necessario specificare un JSON dello schema dell'origine dati utilizzando l'API. TemplateConfiguration È necessario fornire le seguenti informazioni:

- Origine dati: specifica il tipo di origine dati come `DRUPAL` quando usi lo schema TemplateConfigurationJSON. Specificate anche l'origine dati come `TEMPLATE` quando chiamate l'CreateDataSourceAPI.
- Modalità di sincronizzazione: specifica come Amazon Kendra aggiornare l'indice quando il contenuto dell'origine dati cambia. Quando sincronizzi l'origine dati con Amazon Kendra per la prima volta, tutto il contenuto viene sottoposto a scansione e indicizzato per impostazione predefinita. Se la sincronizzazione iniziale non è riuscita, devi eseguire una sincronizzazione completa dei dati, anche se non scegli la sincronizzazione completa come opzione della modalità di sincronizzazione. Puoi scegliere tra:

  - `FORCED_FULL_CRAWL`per indicizzare nuovamente tutti i contenuti, sostituendo i contenuti esistenti ogni volta che l'origine dati si sincronizza con l'indice.
  - `FULL_CRAWL`per indicizzare solo i contenuti nuovi, modificati ed eliminati ogni volta che l'origine dati si sincronizza con l'indice. Amazon Kendra può utilizzare il meccanismo dell'origine dati per tenere traccia delle modifiche ai contenuti e indicizzare i contenuti modificati dall'ultima sincronizzazione.
  - `CHANGE_LOG`per indicizzare solo contenuti nuovi e modificati ogni volta che l'origine dati si sincronizza con l'indice. Amazon Kendra può utilizzare il meccanismo dell'origine dati per tenere traccia delle modifiche ai contenuti e indicizzare i contenuti modificati dall'ultima sincronizzazione.
- Secret Amazon Resource Name (ARN): fornisci l'Amazon Resource Name (ARN) di un Secrets Manager segreto che contiene le credenziali di autenticazione che hai creato nel tuo account Drupal.

  Se utilizzi l'autenticazione di base, il segreto viene archiviato in una struttura JSON con le seguenti chiavi:

  ```
  {
      "username": "user name",
      "password": "password"
  }
  ```

  Se utilizzi l'autenticazione OAuth 2.0, il segreto viene archiviato in una struttura JSON con le seguenti chiavi:

  ```
  {
      "username": "user name",
      "password": "password",
      "clientId": "client id",
      "clientSecret": "client secret"
  }
  ```

> **Note**
>
> > **Note**
> >
> > Ti consigliamo di aggiornare o ruotare regolarmente le credenziali e il segreto. Fornisci solo il livello di accesso necessario per la tua sicurezza. Non è consigliabile riutilizzare credenziali e segreti tra diverse fonti di dati e versioni dei connettori 1.0 e 2.0 (ove applicabile).

- IAM ruolo: specifica `RoleArn` quando chiami `CreateDataSource` per fornire a un IAM ruolo le autorizzazioni per accedere al tuo Secrets Manager segreto e per chiamare le API pubbliche richieste per il connettore Drupal e. Amazon Kendra Per ulteriori informazioni, consulta i IAM ruoli per le fonti di dati Drupal.

Puoi anche aggiungere le seguenti funzionalità opzionali:

- Virtual Private Cloud (VPC): `VpcConfiguration` specifica quando si chiama. `CreateDataSource` Per ulteriori informazioni, consulta Configurazione Amazon Kendra per l'utilizzo di un Amazon VPC.
- Filtri di inclusione ed esclusione: è possibile specificare se includere contenuti, commenti e allegati. È inoltre possibile specificare modelli di espressioni regolari per includere o escludere contenuti, commenti e allegati.

> **Note**
>
> La maggior parte delle fonti di dati utilizza modelli di espressioni regolari, che sono modelli di inclusione o esclusione denominati filtri. Se si specifica un filtro di inclusione, viene indicizzato solo il contenuto che corrisponde al filtro di inclusione. Qualsiasi documento che non corrisponde al filtro di inclusione non viene indicizzato. Se si specifica un filtro di inclusione ed esclusione, i documenti che corrispondono al filtro di esclusione non vengono indicizzati, anche se corrispondono al filtro di inclusione.

- Identity crawler: specifica se attivare il crawler di identità. Amazon Kendra Il crawler di identità utilizza le informazioni dell'elenco di controllo degli accessi (ACL) per i documenti per filtrare i risultati della ricerca in base all'accesso dell'utente o del relativo gruppo ai documenti. Se

disponi di un ACL per i tuoi documenti e scegli di utilizzarlo, puoi anche scegliere di attivare il crawler di identità per configurare il filtraggio Amazon Kendra del contesto utente dei risultati di ricerca. Altrimenti, se il crawler di identità è disattivato, tutti i documenti possono essere ricercati pubblicamente. Se desideri utilizzare il controllo degli accessi per i tuoi documenti e il crawler di identità è disattivato, in alternativa puoi utilizzare l'PutPrincipalMappingAPI per caricare le informazioni di accesso di utenti e gruppi per il filtraggio del contesto degli utenti.

- Mappature dei campi: scegli di mappare i campi delle sorgenti dati di Drupal ai campi indice. Amazon Kendra Per ulteriori informazioni, consulta la sezione Mappatura dei campi di origine dei dati.

> **Note**
>
> Il campo del corpo del documento o l'equivalente del corpo del documento per i documenti è necessario per Amazon Kendra poter cercare i documenti. È necessario mappare il nome del campo del corpo del documento nella fonte dati al nome del campo indice`_document_body`. Tutti gli altri campi sono facoltativi.

Per un elenco di altre importanti chiavi JSON da configurare, consultaSchema del modello Drupal.

Note

- Le API di Drupal non hanno limiti di limitazione ufficiali.
- Gli SDK Java non sono disponibili per Drupal.
- I dati di Drupal possono essere recuperati solo utilizzando le API JSON native.
- I tipi di contenuto non associati ad alcuna visualizzazione Drupal non possono essere sottoposti a scansione.
- È necessario l'accesso da amministratore per eseguire la scansione dei dati da Drupal Blocks.
- Non è disponibile alcuna API JSON per creare il tipo di contenuto definito dall'utente utilizzando i verbi HTTP.
- Il corpo del documento e i commenti per gli articoli, le pagine di base, i blocchi di base, il tipo di contenuto definito dall'utente e il tipo di blocco definito dall'utente vengono visualizzati in formato HTML. Se il contenuto HTML non è ben formato, i tag correlati all'HTML verranno visualizzati nel corpo del documento e nei commenti e saranno visibili nei risultati Amazon Kendra di ricerca.

- I tipi di contenuto e i tipi di blocco senza descrizione o corpo non verranno inseriti. Amazon Kendra Nell'indice verranno inseriti solo commenti e allegati di tali tipi di contenuto o blocco. Amazon Kendra

GitHub

GitHub è un servizio di hosting basato sul web per lo sviluppo di software che fornisce servizi di archiviazione e gestione del codice con controllo della versione. È possibile utilizzarli Amazon Kendra per indicizzare i file del repository GitHub Enterprise Cloud (SaaS) ed GitHub Enterprise Server (On Prem), inviare e ritirare richieste, emettere e pull request e allegare commenti di richieste di emissione e pull. Puoi anche scegliere di includere o escludere determinati file.

> **Note**
>
> Amazon Kendra ora supporta un GitHub connettore aggiornato.
> La console è stata aggiornata automaticamente per te. Tutti i nuovi connettori creati nella console utilizzeranno l'architettura aggiornata. Se utilizzi l'API, ora devi utilizzare l'TemplateConfigurationoggetto anziché l'`GitHubConfiguration`oggetto per configurare il connettore.
> I connettori configurati utilizzando la console e l'architettura API precedenti continueranno a funzionare come configurato. Tuttavia, non potrai modificarli o aggiornarli. Se desideri modificare o aggiornare la configurazione del connettore, devi creare un nuovo connettore. Ti consigliamo di migrare il flusso di lavoro del connettore alla versione aggiornata. La fine del supporto per i connettori configurati utilizzando l'architettura precedente è prevista entro giugno 2024.

Puoi connetterti Amazon Kendra alla tua fonte di GitHub dati utilizzando la Amazon Kendra console e l'TemplateConfigurationAPI.

Per la risoluzione dei problemi relativi al connettore della sorgente Amazon Kendra GitHub dati, consultaRisoluzione dei problemi relativi alle origini dati.

Argomenti

- Funzionalità supportate
- Prerequisiti
- Istruzioni di connessione

- Ulteriori informazioni

Funzionalità supportate

Amazon Kendra GitHub il connettore di origine dati supporta le seguenti funzionalità:

- mappature dei campi
- Filtraggio del contesto utente
- Scansione delle identità degli utenti
- Filtri di inclusione/esclusione
- Sincronizzazione completa e incrementale dei contenuti
- Virtual Private Cloud (VPC) (Cloud privato virtuale (VPC)

Prerequisiti

Prima di poterla utilizzare Amazon Kendra per indicizzare la tua fonte di GitHub dati, apporta queste modifiche al tuo account GitHub e AWS ai tuoi account.

Nel GitHub, assicurati di avere:

- Hai creato un GitHub utente con autorizzazioni amministrative per l' GitHub organizzazione.
- Creato un classico token di accesso personale per le credenziali di autenticazione. Consulta GitHub la documentazione sulla creazione di un token di accesso personale.
- Consigliato: creato un token OAuth per le credenziali di autenticazione. Utilizza il token OAuth per migliorare i limiti di limitazione delle API e le prestazioni dei connettori. Consulta la GitHub documentazione sull'autorizzazione OAuth.
- Ha indicato l'URL dell' GitHub host per il tipo di GitHub servizio che utilizzi. Ad esempio, l'URL dell'host per il GitHub cloud potrebbe essere *`https://api.github.com`* e l'URL dell'host per il GitHub server potrebbe essere *`https://on-prem-host-url/api/v3/`*.
- Ha annotato il nome dell'organizzazione per GitHub l'account GitHub Enterprise Cloud (SaaS) o l'account GitHub Enterprise Server (locale) a cui desideri connetterti. Puoi trovare il nome della tua organizzazione accedendo al GitHub desktop e selezionando Le tue organizzazioni nel menu a discesa dell'immagine del profilo.
- Facoltativo (solo server): ha generato un certificato SSL e copiato il percorso del certificato memorizzato in un bucket. Amazon S3 Lo usi per connetterti GitHub se hai bisogno di una connessione SSL sicura. Puoi semplicemente generare un certificato X509 autofirmato su qualsiasi

computer utilizzando OpenSSL. Per un esempio di utilizzo di OpenSSL per creare un certificato X509, consulta Creare e firmare un certificato X509.

- Sono state aggiunte le seguenti autorizzazioni:

  Per il cloud GitHub aziendale (SaaS)

  - repository: status
  - public_repo
  - repo: invita
  - leggi: org
  - utente: email
  - leggi: utente

  Per GitHub Enterprise Server (in locale)

  - repo:status
  - public_repo
  - repo: invita
  - leggi: org
  - utente: email
  - leggi: utente
  - amministratore del sito
- È stato selezionato che ogni documento sia unico all'interno GitHub e tra le altre fonti di dati che intendi utilizzare per lo stesso indice. Ogni fonte di dati che desideri utilizzare per un indice non deve contenere lo stesso documento in tutte le fonti di dati. Gli ID dei documenti sono globali rispetto a un indice e devono essere univoci per indice.

Nel tuo Account AWS, assicurati di avere:

- Ha creato un Amazon Kendra indice e, se si utilizza l'API, ha annotato l'ID dell'indice.
- Hai creato un IAM ruolo per la tua origine dati e, se utilizzi l'API, hai annotato l'ARN del IAM ruolo.

> **Note**
>
> Se modifichi il tipo di autenticazione e le credenziali, devi aggiornare il IAM ruolo per accedere all'ID AWS Secrets Manager segreto corretto.

- Ha archiviato le credenziali di GitHub autenticazione in un AWS Secrets Manager luogo segreto e, se si utilizza l'API, ha annotato l'ARN del segreto.

> **Note**
>
> Ti consigliamo di aggiornare o ruotare regolarmente le credenziali e il segreto. Fornisci solo il livello di accesso necessario per la tua sicurezza. Non è consigliabile riutilizzare credenziali e segreti tra diverse fonti di dati e versioni dei connettori 1.0 e 2.0 (ove applicabile).

Se non disponi di un IAM ruolo o di un segreto esistente, puoi utilizzare la console per creare un nuovo IAM ruolo e un Secrets Manager segreto quando connetti la tua origine GitHub dati a. Amazon Kendra Se utilizzi l'API, devi fornire l'ARN di un IAM ruolo e di un Secrets Manager segreto esistenti e un ID di indice.

Istruzioni di connessione

Per connetterti Amazon Kendra alla tua fonte di GitHub dati, devi fornire i dettagli necessari della tua origine GitHub dati in modo che Amazon Kendra possa accedere ai tuoi dati. Se non hai ancora configurato GitHub per Amazon Kendra, consultaPrerequisiti.

Console

Per connettersi Amazon Kendra a GitHub

1. Accedi a AWS Management Console e apri la Amazon Kendra console.
2. Dal riquadro di navigazione a sinistra, scegli Indici, quindi scegli l'indice che desideri utilizzare dall'elenco degli indici.

> **Note**
>
> Puoi scegliere di configurare o modificare le impostazioni del controllo dell'accesso degli utenti in Impostazioni dell'indice.

3. Nella pagina Guida introduttiva, scegli Aggiungi origine dati.
4. Nella pagina Aggiungi origine dati, scegli GitHub connettore, quindi scegli Aggiungi connettore.
5. Nella pagina Specificare i dettagli dell'origine dati, inserisci le seguenti informazioni:

a. In Nome e descrizione, per Nome dell'origine dati, inserisci un nome per l'origine dati. Puoi includere trattini ma non spazi.

b. (Facoltativo) Descrizione: immetti una descrizione facoltativa per la tua fonte di dati.

c. In Lingua predefinita: scegli una lingua per filtrare i documenti per l'indice. Se non diversamente specificato, la lingua predefinita è l'inglese. La lingua specificata nei metadati del documento ha la precedenza sulla lingua selezionata.

d. In Tag, per Aggiungi nuovo tag, includi tag opzionali per cercare e filtrare le risorse o tenere traccia dei costi. AWS

e. Seleziona Successivo.

6. Nella pagina Definisci accesso e sicurezza, inserisci le seguenti informazioni:

a. GitHubsource: scegli tra GitHub Enterprise Cloud ed GitHubEnterprise Server.

b. GitHub URL dell'host: immetti il nome dell' GitHub host.

c. GitHub nome dell'organizzazione: inserisci il nome GitHub dell'organizzazione. Puoi trovare le informazioni sulla tua organizzazione nel tuo GitHub account.

d. Autorizzazione: attiva o disattiva le informazioni dell'elenco di controllo degli accessi (ACL) per i tuoi documenti, se disponi di un ACL e desideri utilizzarlo per il controllo degli accessi. L'ACL specifica a quali documenti possono accedere utenti e gruppi. Le informazioni ACL vengono utilizzate per filtrare i risultati della ricerca in base all'accesso dell'utente o del relativo gruppo ai documenti. Per ulteriori informazioni, consulta Filtraggio del contesto utente.

e. AWS Secrets Manager segreto: scegli un segreto esistente o crea un nuovo Secrets Manager segreto per memorizzare le credenziali di GitHub autenticazione. Se scegli di creare un nuovo segreto, si apre una finestra AWS Secrets Manager segreta.

   i. Inserisci le seguenti informazioni nella finestra Crea un AWS Secrets Manager segreto:

      A. Nome segreto: un nome per il tuo segreto. Il prefisso 'AmazonKendra- GitHub -' viene aggiunto automaticamente al nome segreto.

      B. Per GitHubtoken: inserisci i valori delle credenziali di autenticazione che hai creato nel tuo account. GitHub

   ii. Selezionare Salva.

f. Virtual Private Cloud (VPC): puoi scegliere di utilizzare un VPC. In tal caso, è necessario aggiungere sottoreti e gruppi di sicurezza VPC.

g. Identity crawler: specifica se attivare il crawler di identità. Amazon Kendra Il crawler di identità utilizza le informazioni dell'elenco di controllo degli accessi (ACL) per i documenti per filtrare i risultati della ricerca in base all'accesso dell'utente o del gruppo di appartenenza ai documenti. Se disponi di un ACL per i tuoi documenti e scegli di utilizzarlo, puoi anche scegliere di attivare il crawler di identità per configurare il filtraggio Amazon Kendra contestuale dell'utente dei risultati di ricerca. Altrimenti, se il crawler di identità è disattivato, tutti i documenti possono essere ricercati pubblicamente. Se desideri utilizzare il controllo degli accessi per i tuoi documenti e il crawler di identità è disattivato, in alternativa puoi utilizzare l'PutPrincipalMappingAPI per caricare le informazioni di accesso di utenti e gruppi per il filtraggio del contesto degli utenti.

h. IAM ruolo: scegli un IAM ruolo esistente o creane uno nuovo IAM per accedere alle credenziali del repository e indicizzare il contenuto.

> **Note**
>
> IAM i ruoli utilizzati per gli indici non possono essere utilizzati per le fonti di dati. Se non sei sicuro che un ruolo esistente venga utilizzato per un indice o una FAQ, scegli Crea un nuovo ruolo per evitare errori.

i. Seleziona Successivo.

7. Nella pagina Configura le impostazioni di sincronizzazione, inserisci le seguenti informazioni:

a. Seleziona i repository da sottoporre a scansione: seleziona tra la scansione di Tutti gli archivi o Seleziona i repository.

   Se scegli Seleziona i repository, aggiungi i nomi per i repository in Nome del repository e, facoltativamente, il nome di qualsiasi ramo specifico in Nome del ramo.

b. Tipi di contenuto: seleziona i tipi di contenuto che desideri includere.

c. Modelli Regex: modelli di espressioni regolari per includere o escludere determinati file. È possibile aggiungere fino a 100 pattern.

d. Pianificazione di esecuzione in Sync, per Frequenza: con quale frequenza Amazon Kendra verrà eseguita la sincronizzazione con la fonte di dati.

e. Seleziona Successivo.

8. Modalità di sincronizzazione: scegli come aggiornare l'indice quando il contenuto della fonte di dati cambia. Quando sincronizzi l'origine dati con Amazon Kendra per la prima volta, tutto il contenuto viene sottoposto a scansione e indicizzato per impostazione predefinita. Se la sincronizzazione iniziale non è riuscita, devi eseguire una sincronizzazione completa dei dati, anche se non scegli la sincronizzazione completa come opzione della modalità di sincronizzazione.

   - Sincronizzazione completa: indicizza di nuovo tutti i contenuti, sostituendo i contenuti esistenti ogni volta che l'origine dati si sincronizza con l'indice.
   - Nuova sincronizzazione modificata: indicizza solo i contenuti nuovi e modificati ogni volta che l'origine dati si sincronizza con l'indice. Amazon Kendra può utilizzare il meccanismo dell'origine dati per tenere traccia delle modifiche ai contenuti e indicizzare i contenuti modificati dall'ultima sincronizzazione.
   - Sincronizzazione nuova, modificata ed eliminata: indicizza solo i contenuti nuovi, modificati ed eliminati ogni volta che l'origine dati si sincronizza con l'indice. Amazon Kendra può utilizzare il meccanismo dell'origine dati per tenere traccia delle modifiche ai contenuti e indicizzare i contenuti modificati dall'ultima sincronizzazione.

9. Pianificazione di esecuzione in Sync, per Frequenza: con quale frequenza Amazon Kendra si sincronizza con la tua fonte di dati.
10. Seleziona Successivo.
11. Nella pagina Imposta mappature dei campi, inserisci le seguenti informazioni:

    a. Per Repository, Respository Commit, Issue Document, Issue Comment, Issue Attachment, Pull Request Comment, Pull Request Document, Pull Request Attachment: seleziona uno dei campi Amazon Kendra generati dell'origine dati predefiniti che desideri mappare all'indice.

    b. Aggiungi campo: consente di aggiungere campi di origine dati personalizzati a cui creare un nome di campo indice a cui mappare e il tipo di dati del campo.

    c. Seleziona Successivo.

12. Nella pagina Rivedi e crea, verifica che le informazioni inserite siano corrette, quindi seleziona Aggiungi origine dati. Puoi anche scegliere di modificare le tue informazioni da questa pagina. L'origine dati verrà visualizzata nella pagina Origini dati dopo che l'origine dati sarà stata aggiunta correttamente.

API

Per connettersi Amazon Kendra a GitHub

È necessario specificare un codice JSON dello schema dell'origine dati utilizzando l'TemplateConfigurationAPI. È necessario fornire le seguenti informazioni:

- Origine dati: specifica il tipo di origine dati come `GITHUB` quando usi lo schema TemplateConfigurationJSON. Specificate anche l'origine dati come `TEMPLATE` quando chiamate l'CreateDataSourceAPI.
- GitHubtype: specifica il tipo come `SAAS` o`ON_PREMISE`.
- URL host: specifica l'URL dell' GitHub host o l'URL dell'endpoint dell'API. Ad esempio, se si utilizza GitHub SaaS/Enterprise Cloud, l'URL dell'host potrebbe essere`https://api.github.com`, mentre per GitHub On-Premises/Enterprise Server l'URL dell'host potrebbe essere. `https://on-prem-host-url/api/v3/`
- Nome dell'organizzazione: specificare il nome dell'organizzazione dell'account. GitHub Puoi trovare il nome della tua organizzazione accedendo al GitHub desktop e selezionando Le tue organizzazioni nel menu a discesa dell'immagine del profilo.
- Modalità di sincronizzazione: specifica come Amazon Kendra aggiornare l'indice quando il contenuto della fonte dati cambia. Quando sincronizzi l'origine dati con Amazon Kendra per la prima volta, tutto il contenuto viene sottoposto a scansione e indicizzato per impostazione predefinita. Se la sincronizzazione iniziale non è riuscita, devi eseguire una sincronizzazione completa dei dati, anche se non scegli la sincronizzazione completa come opzione della modalità di sincronizzazione. Puoi scegliere tra:
  - `FORCED_FULL_CRAWL`per indicizzare nuovamente tutti i contenuti, sostituendo i contenuti esistenti ogni volta che l'origine dati si sincronizza con l'indice.
  - `FULL_CRAWL`per indicizzare solo i contenuti nuovi, modificati ed eliminati ogni volta che l'origine dati si sincronizza con l'indice. Amazon Kendra può utilizzare il meccanismo dell'origine dati per tenere traccia delle modifiche ai contenuti e indicizzare i contenuti modificati dall'ultima sincronizzazione.
  - `CHANGE_LOG`per indicizzare solo contenuti nuovi e modificati ogni volta che l'origine dati si sincronizza con l'indice. Amazon Kendra può utilizzare il meccanismo dell'origine dati per tenere traccia delle modifiche ai contenuti e indicizzare i contenuti modificati dall'ultima sincronizzazione.
- Identity crawler: specifica se attivare il crawler Amazon Kendra di identità. Il crawler di identità utilizza le informazioni dell'elenco di controllo degli accessi (ACL) per i documenti

per filtrare i risultati della ricerca in base all'accesso dell'utente o del gruppo di appartenenza ai documenti. Se disponi di un ACL per i tuoi documenti e scegli di utilizzarlo, puoi anche scegliere di attivare il crawler di identità per configurare il filtraggio Amazon Kendra contestuale dell'utente dei risultati di ricerca. Altrimenti, se il crawler di identità è disattivato, tutti i documenti possono essere ricercati pubblicamente. Se desideri utilizzare il controllo degli accessi per i tuoi documenti e il crawler di identità è disattivato, in alternativa puoi utilizzare l'PutPrincipalMappingAPI per caricare le informazioni di accesso di utenti e gruppi per il filtraggio del contesto degli utenti.

- Secret Amazon Resource Name (ARN): fornisci l'Amazon Resource Name (ARN) di un Secrets Manager segreto che contiene le credenziali di autenticazione per il tuo account. GitHub Il segreto è archiviato in una struttura JSON con le seguenti chiavi:

```
{
    "personalToken": "token"
}
```

> **Note**
>
> Ti consigliamo di aggiornare o ruotare regolarmente le credenziali e il segreto. Fornisci solo il livello di accesso necessario per la tua sicurezza. Non è consigliabile riutilizzare credenziali e segreti tra diverse fonti di dati e versioni dei connettori 1.0 e 2.0 (ove applicabile).

- IAM ruolo: specifica `RoleArn` quando chiami `CreateDataSource` per fornire a un IAM ruolo le autorizzazioni per accedere al tuo Secrets Manager segreto e per chiamare le API pubbliche richieste per il connettore e. GitHub Amazon Kendra Per ulteriori informazioni, consulta i IAM ruoli per GitHub le fonti di dati.

Puoi anche aggiungere le seguenti funzionalità opzionali:

- Virtual Private Cloud (VPC): `VpcConfiguration` specifica quando si chiama. `CreateDataSource` Per ulteriori informazioni, consulta Configurazione Amazon Kendra per l'utilizzo di un Amazon VPC.

> **Note**
>
> Se si utilizza un GitHub server, è necessario utilizzare un Amazon VPC per connettersi al server GitHub.

- Filtro repository: filtra i repository in base al nome e ai nomi dei rami.
- Tipi di documenti/contenuti: specificate se eseguire la scansione dei documenti del repository, dei problemi, dei commenti, degli allegati dei commenti, delle richieste pull, dei commenti delle pull request, degli allegati dei commenti delle pull request.
- Filtri di inclusione ed esclusione: specifica se includere o escludere determinati file e cartelle.

> **Note**
>
> La maggior parte delle fonti di dati utilizza modelli di espressioni regolari, che sono modelli di inclusione o esclusione denominati filtri. Se si specifica un filtro di inclusione, viene indicizzato solo il contenuto che corrisponde al filtro di inclusione. Qualsiasi documento che non corrisponde al filtro di inclusione non viene indicizzato. Se si specifica un filtro di inclusione ed esclusione, i documenti che corrispondono al filtro di esclusione non vengono indicizzati, anche se corrispondono al filtro di inclusione.

- Elenco di controllo degli accessi (ACL): specifica se eseguire la scansione delle informazioni ACL per i documenti, se disponi di un ACL e desideri utilizzarlo per il controllo degli accessi. L'ACL specifica a quali documenti possono accedere utenti e gruppi. Le informazioni ACL vengono utilizzate per filtrare i risultati della ricerca in base all'accesso dell'utente o del relativo gruppo ai documenti. Per ulteriori informazioni, consulta Filtraggio del contesto utente.
- Mappature dei campi: scegli di mappare i campi delle sorgenti GitHub dati ai campi indice. Amazon Kendra Puoi includere campi di documenti, commit, problemi, allegati di emissione, commenti, richieste pull, allegati di richieste pull, commenti di pull request, commenti di pull request. Per ulteriori informazioni, consulta la sezione Mappatura dei campi di origine dei dati.

> **Note**
>
> Il campo del corpo del documento o l'equivalente del corpo del documento è obbligatorio per consentire ad Amazon Kendra di effettuare ricerche nei documenti.

È necessario mappare il nome del campo del corpo del documento nella fonte dati al nome del campo indice _document_body. Tutti gli altri campi sono facoltativi.

Per un elenco di altre importanti chiavi JSON da configurare, consulta lo schema del modello. GitHub

Ulteriori informazioni

Per ulteriori informazioni sull'integrazione Amazon Kendra con la tua fonte di GitHub dati, consulta:

- Reimmagina la ricerca nei GitHub repository con la potenza del connettore Amazon Kendra GitHub

Gmail

Gmail è un client di posta elettronica sviluppato da Google attraverso il quale è possibile inviare messaggi di posta elettronica con file allegati. I messaggi di Gmail possono essere ordinati e archiviati all'interno della casella di posta elettronica utilizzando cartelle ed etichette. Puoi utilizzarli Amazon Kendra per indicizzare i messaggi di posta elettronica e gli allegati dei messaggi. È inoltre possibile Amazon Kendra configurare l'inclusione o l'esclusione di messaggi di posta elettronica, allegati di messaggi ed etichette specifici per l'indicizzazione.

Puoi connetterti Amazon Kendra alla tua fonte di dati Gmail utilizzando la Amazon Kendra console e l'API. TemplateConfiguration

Per la risoluzione dei problemi relativi al connettore di origine dati di Amazon Kendra Gmail, consulta. Risoluzione dei problemi relativi alle origini dati

Argomenti

- Funzionalità supportate
- Prerequisiti
- Istruzioni di connessione
- Ulteriori informazioni
- Note

Funzionalità supportate

- Mappature dei campi
- Filtraggio del contesto utente
- Filtri di inclusione/esclusione
- Sincronizzazione completa e incrementale dei contenuti
- Virtual Private Cloud (VPC) (Cloud privato virtuale (VPC)

Prerequisiti

Prima di poterla utilizzare Amazon Kendra per indicizzare la tua fonte di dati Gmail, apporta queste modifiche a Gmail e agli account. AWS

In Gmail, assicurati di avere:

- Hai creato un account amministratore di Google Cloud Platform e hai creato un progetto Google Cloud.
- Hai attivato l'API Gmail e l'API Admin SDK nel tuo account amministratore.
- Hai creato un account di servizio e scaricato una chiave privata JSON per Gmail. Per informazioni su come creare e accedere alla tua chiave privata, consulta la documentazione di Google Cloud su come creare una chiave di account di servizio e le credenziali dell'account di servizio.
- Ho copiato l'email del tuo account di amministratore, l'email del tuo account di servizio e la chiave privata da utilizzare per l'autenticazione.
- Sono stati aggiunti i seguenti ambiti Oauth (utilizzando un ruolo di amministratore) per l'utente e le directory condivise che desideri indicizzare:
  - https://www.googleapis.com/auth/admin.directory.user.readonly
  - https://www.googleapis.com/auth/gmail.readonly
- È stato verificato che ogni documento sia unico in Gmail e tra le altre fonti di dati che intendi utilizzare per lo stesso indice. Ogni fonte di dati che desideri utilizzare per un indice non deve contenere lo stesso documento in tutte le fonti di dati. Gli ID dei documenti sono globali rispetto a un indice e devono essere univoci per indice.

Nel tuo Account AWS, assicurati di avere:

- Ha creato un Amazon Kendra indice e, se si utilizza l'API, ha annotato l'ID dell'indice.

- Hai creato un IAM ruolo per la tua origine dati e, se utilizzi l'API, hai annotato l'ARN del IAM ruolo.

> **Note**
>
> Se modifichi il tipo di autenticazione e le credenziali, devi aggiornare il IAM ruolo per accedere all'ID AWS Secrets Manager segreto corretto.

- Ha archiviato le credenziali di autenticazione di Gmail in un AWS Secrets Manager luogo segreto e, se si utilizza l'API, ha annotato l'ARN del segreto.

> **Note**
>
> Ti consigliamo di aggiornare o ruotare regolarmente le credenziali e il segreto. Fornisci solo il livello di accesso necessario per la tua sicurezza. Non è consigliabile riutilizzare credenziali e segreti tra diverse fonti di dati e versioni dei connettori 1.0 e 2.0 (ove applicabile).

Se non disponi di un IAM ruolo o di un segreto esistente, puoi utilizzare la console per creare un nuovo IAM ruolo e un Secrets Manager segreto quando connetti l'origine dati di Gmail a. Amazon Kendra Se utilizzi l'API, devi fornire l'ARN di un IAM ruolo e di un Secrets Manager segreto esistenti e un ID di indice.

Istruzioni di connessione

Per connetterti Amazon Kendra alla tua fonte di dati Gmail devi fornire i dettagli delle tue credenziali di Gmail in modo da Amazon Kendra poter accedere ai tuoi dati. Se non hai ancora configurato Gmail per, consulta. Amazon KendraPrerequisiti

Console

Per connettersi Amazon Kendra a Gmail

1. Accedi a AWS Management Console e apri la Amazon Kendra console.
2. Dal riquadro di navigazione a sinistra, scegli Indici, quindi scegli l'indice che desideri utilizzare dall'elenco degli indici.

> **Note**
>
> Puoi scegliere di configurare o modificare le impostazioni del controllo dell'accesso degli utenti in Impostazioni dell'indice.

3. Nella pagina Guida introduttiva, scegli Aggiungi origine dati.
4. Nella pagina Aggiungi origine dati, scegli Connettore Gmail, quindi scegli Aggiungi connettore.
5. Nella pagina Specificare i dettagli dell'origine dati, inserisci le seguenti informazioni:
   a. In Nome e descrizione, per Nome dell'origine dati, inserisci un nome per l'origine dati. Puoi includere trattini ma non spazi.
   b. (Facoltativo) Descrizione: immetti una descrizione facoltativa per l'origine dati.
   c. In Lingua predefinita: scegli una lingua per filtrare i documenti per l'indice. Se non diversamente specificato, la lingua predefinita è l'inglese. La lingua specificata nei metadati del documento ha la precedenza sulla lingua selezionata.
   d. In Tag, per Aggiungi nuovo tag, includi tag opzionali per cercare e filtrare le risorse o tenere traccia dei costi. AWS
   e. Seleziona Successivo.
6. Nella pagina Definisci accesso e sicurezza, inserisci le seguenti informazioni:
   a. In Autenticazione AWS Secrets Manager segreta: scegli un segreto esistente o crea un nuovo Secrets Manager segreto per archiviare le credenziali di autenticazione di Gmail. Se scegli di creare un nuovo segreto, si apre una finestra AWS Secrets Manager segreta.
      - Inserisci le seguenti informazioni nella finestra Crea un AWS Secrets Manager segreto:
        A. Nome segreto: un nome per il tuo segreto.
        B. Email del client: l'email del client che hai copiato dal tuo account di servizio Google.
        C. Email dell'account amministratore: l'email dell'account amministratore che desideri utilizzare.

D. Chiave privata: la chiave privata che hai copiato dal tuo account di servizio Google.

E. Selezionare Salva.

b. Virtual Private Cloud (VPC): puoi scegliere di utilizzare un VPC. In tal caso, è necessario aggiungere sottoreti e gruppi di sicurezza VPC.

c. IAM ruolo: scegli un IAM ruolo esistente o creane uno nuovo IAM per accedere alle credenziali del repository e indicizzare il contenuto.

> **Note**
>
> IAM i ruoli utilizzati per gli indici non possono essere utilizzati per le fonti di dati. Se non sei sicuro che un ruolo esistente venga utilizzato per un indice o una FAQ, scegli Crea un nuovo ruolo per evitare errori.

d. Seleziona Successivo.

7. Nella pagina Configura le impostazioni di sincronizzazione, inserisci le seguenti informazioni:

a. Nell'ambito della sincronizzazione, per i tipi di entità: seleziona Allegati dei messaggi per sincronizzare gli allegati dei messaggi. I messaggi verranno sincronizzati per impostazione predefinita.

b. (Facoltativo) Per una configurazione aggiuntiva, inserisci le seguenti informazioni:

i. Intervallo di date: inserisci un intervallo di date per specificare la data di inizio e di fine delle e-mail da sottoporre a scansione.

ii. Domini e-mail: include o esclude i messaggi di posta elettronica in base ai domini.

iii. Parole chiave nell'oggetto: include o esclude i messaggi di posta elettronica in base alle parole chiave presenti nell'oggetto.

> **Note**
>
> Puoi anche scegliere di includere tutti i documenti che corrispondono a tutte le parole chiave dell'oggetto che hai inserito.

iv. Etichette: aggiungi modelli di espressioni regolari per includere o escludere etichette specifiche. È possibile aggiungere fino a 100 motivi.

v. Allegati: aggiungi modelli di espressioni regolari per includere o escludere allegati specifici. È possibile aggiungere fino a 100 motivi.

c. Modalità di sincronizzazione: scegli come aggiornare l'indice quando il contenuto dell'origine dati cambia. Quando sincronizzi l'origine dati con Amazon Kendra per la prima volta, tutto il contenuto viene sottoposto a scansione e indicizzato per impostazione predefinita. Se la sincronizzazione iniziale non è riuscita, devi eseguire una sincronizzazione completa dei dati, anche se non scegli la sincronizzazione completa come opzione della modalità di sincronizzazione.

- Sincronizzazione completa: indicizza di nuovo tutti i contenuti, sostituendo i contenuti esistenti ogni volta che l'origine dati si sincronizza con l'indice.
- Sincronizzazione nuova, modificata ed eliminata: indicizza solo i contenuti nuovi, modificati ed eliminati ogni volta che l'origine dati si sincronizza con l'indice. Amazon Kendra può utilizzare il meccanismo dell'origine dati per tenere traccia delle modifiche ai contenuti e indicizzare i contenuti modificati dall'ultima sincronizzazione.

> **Important**
>
> Poiché non esiste un'API per aggiornare i messaggi Gmail eliminati definitivamente, né per la sincronizzazione dei contenuti nuovi, modificati o eliminati:
>
> - Non rimuoverà dal tuo indice i messaggi eliminati definitivamente da Gmail Amazon Kendra
> - Non sincronizzerà le modifiche nelle etichette delle email di Gmail
>
> Per sincronizzare le modifiche alle etichette delle sorgenti dati di Gmail e i messaggi email eliminati definitivamente con il tuo Amazon Kendra indice, devi eseguire periodicamente ricerche per indicizzazione complete.

d. Pianificazione di esecuzione in Sync, per Frequenza: con quale frequenza Amazon Kendra verrà eseguita la sincronizzazione con la fonte di dati.

e. Seleziona Successivo.

8. Nella pagina Imposta mappature dei campi, inserisci le seguenti informazioni:

a. Per i messaggi e gli allegati dei messaggi: seleziona uno dei campi di origine dati predefiniti Amazon Kendra generati che desideri mappare all'indice.

> **Note**
>
> Amazon Kendra Il connettore di origine dati di Gmail non supporta la creazione di campi indice personalizzati a causa delle limitazioni dell'API.

b. Seleziona Successivo.

9. Nella pagina Rivedi e crea, verifica che le informazioni inserite siano corrette, quindi seleziona Aggiungi origine dati. Puoi anche scegliere di modificare le tue informazioni da questa pagina. L'origine dati verrà visualizzata nella pagina Origini dati dopo che l'origine dati sarà stata aggiunta correttamente.

API

Per connettersi Amazon Kendra a Gmail

È necessario specificare un codice JSON dello schema dell'origine dati utilizzando l'TemplateConfigurationAPI. È necessario fornire le seguenti informazioni:

- Origine dati: specifica il tipo di origine dati come `GMAIL` quando usi lo schema TemplateConfigurationJSON. Specificate anche l'origine dati come `TEMPLATE` quando chiamate l'CreateDataSourceAPI.
- Modalità di sincronizzazione: specifica come Amazon Kendra aggiornare l'indice quando il contenuto dell'origine dati cambia. Quando sincronizzi l'origine dati con Amazon Kendra per la prima volta, tutto il contenuto viene sottoposto a scansione e indicizzato per impostazione predefinita. Se la sincronizzazione iniziale non è riuscita, devi eseguire una sincronizzazione completa dei dati, anche se non scegli la sincronizzazione completa come opzione della modalità di sincronizzazione. Puoi scegliere tra:
  - `FORCED_FULL_CRAWL`per indicizzare nuovamente tutti i contenuti, sostituendo i contenuti esistenti ogni volta che l'origine dati si sincronizza con l'indice.
  - `FULL_CRAWL`per indicizzare solo i contenuti nuovi, modificati ed eliminati ogni volta che l'origine dati si sincronizza con l'indice. Amazon Kendra può utilizzare il meccanismo dell'origine dati per tenere traccia delle modifiche ai contenuti e indicizzare i contenuti modificati dall'ultima sincronizzazione.

> **Important**
>
> Poiché non esiste un'API per aggiornare i messaggi Gmail eliminati definitivamente, né per la sincronizzazione dei contenuti nuovi, modificati o eliminati:
>
> - Non rimuoverà dal tuo indice i messaggi eliminati definitivamente da Gmail Amazon Kendra
> - Non sincronizzerà le modifiche nelle etichette delle email di Gmail
>
> Per sincronizzare le modifiche alle etichette delle sorgenti dati di Gmail e i messaggi email eliminati definitivamente con il tuo Amazon Kendra indice, devi eseguire periodicamente ricerche per indicizzazione complete.

- Secret Amazon Resource Name (ARN): fornisci l'Amazon Resource Name (ARN) di un Secrets Manager segreto che contiene le credenziali di autenticazione per il tuo account Gmail. Il segreto è archiviato in una struttura JSON con le seguenti chiavi:

```
{
    "adminAccountEmailId": "service account email",
    "clientEmailId": "user account email",
    "privateKey": "private key"
}
```

> **Note**
>
> Ti consigliamo di aggiornare o ruotare regolarmente le credenziali e il segreto. Fornisci solo il livello di accesso necessario per la tua sicurezza. Non è consigliabile riutilizzare credenziali e segreti tra diverse fonti di dati e versioni dei connettori 1.0 e 2.0 (ove applicabile).

- IAM ruolo: specifica `RoleArn` quando chiami `CreateDataSource` per fornire a un IAM ruolo le autorizzazioni per accedere al tuo Secrets Manager segreto e per chiamare le API pubbliche richieste per il connettore Gmail e. Amazon Kendra Per ulteriori informazioni, consulta i IAM ruoli per le fonti di dati di Gmail.

Puoi anche aggiungere le seguenti funzionalità opzionali:

- Virtual Private Cloud (VPC): `VpcConfiguration` specifica quando si chiama. `CreateDataSource` Per ulteriori informazioni, consulta Configurazione Amazon Kendra per l'utilizzo di un Amazon VPC.
- Filtri di inclusione ed esclusione: è possibile specificare se includere o escludere messaggi e allegati.

> **Note**
>
> La maggior parte delle fonti di dati utilizza modelli di espressioni regolari, che sono modelli di inclusione o esclusione denominati filtri. Se si specifica un filtro di inclusione, viene indicizzato solo il contenuto che corrisponde al filtro di inclusione. Qualsiasi documento che non corrisponde al filtro di inclusione non viene indicizzato. Se si specifica un filtro di inclusione ed esclusione, i documenti che corrispondono al filtro di esclusione non vengono indicizzati, anche se corrispondono al filtro di inclusione.

- Filtro del contesto utente e controllo degli accessi:Amazon Kendra esegue la ricerca per indicizzazione dell'elenco di controllo degli accessi (ACL) dei documenti, se disponi di un ACL per i documenti. Le informazioni ACL vengono utilizzate per filtrare i risultati della ricerca in base all'accesso dell'utente o del relativo gruppo ai documenti. Per ulteriori informazioni, consulta Filtraggio del contesto utente.
- Mappature dei campi: scegli di mappare i campi dell'origine dati di Gmail ai campi dell'indice. Amazon Kendra Per ulteriori informazioni, consulta la sezione Mappatura dei campi di origine dei dati.

> **Note**
>
> Il campo del corpo del documento o l'equivalente del corpo del documento per i documenti è necessario per Amazon Kendra eseguire la ricerca nei documenti. È necessario mappare il nome del campo del corpo del documento nella fonte dati al nome del campo indice_`document_body`. Tutti gli altri campi sono facoltativi.

> **Note**
>
> Amazon Kendra Il connettore di origine dati di Gmail non supporta la creazione di campi indice personalizzati a causa delle limitazioni dell'API.

Ulteriori informazioni

Per ulteriori informazioni sull'integrazione Amazon Kendra con la tua fonte di dati Gmail, consulta:

- Esegui una ricerca intelligente tra le email nella tua area di lavoro Google utilizzando il connettore Gmail per. Amazon Kendra

Note

- Poiché non esiste un'API per aggiornare i messaggi Gmail eliminati definitivamente, una sincronizzazione dei `FULL_CRAWL` contenuti nuovi, modificati o eliminati:
  - Non rimuoverà dal tuo indice i messaggi che sono stati eliminati definitivamente da Gmail Amazon Kendra
  - Non sincronizzerà le modifiche nelle etichette delle email di Gmail

  Per sincronizzare le modifiche alle etichette delle sorgenti dati di Gmail e i messaggi email eliminati definitivamente con il tuo Amazon Kendra indice, devi eseguire periodicamente ricerche per indicizzazione complete.
- Amazon Kendra Il connettore di origine dati di Gmail non supporta la creazione di campi indice personalizzati a causa delle limitazioni dell'API.

Google Drive

Google Drive è un servizio di archiviazione di file basato sul cloud. Puoi utilizzarlo Amazon Kendra per indicizzare i documenti archiviati nelle cartelle Drive condivise, I miei Drive e Condivisi con me nella tua fonte di dati Google Drive. Puoi indicizzare sia i documenti di Google Workspace sia i documenti elencati in Tipi di documentazione. Puoi anche utilizzare filtri di inclusione ed esclusione per indicizzare i contenuti in base al nome, al tipo di file e al percorso del file.

Puoi connetterti Amazon Kendra alla tua fonte di dati di Google Drive utilizzando la Amazon Kendra console, l'TemplateConfigurationAPI o l'GoogleDriveConfigurationAPI.

Amazon Kendra dispone di due versioni del connettore Google Drive. Le funzionalità supportate di ogni versione includono:

Connettore Google Drive V1.0/API GoogleDriveConfiguration

- Mappature dei campi

- Controllo degli accessi degli utenti
- Filtri di inclusione/esclusione

Connettore Google Drive V2.0/API TemplateConfiguration

- Mappature dei campi
- Controllo degli accessi degli utenti
- Filtri di inclusione/esclusione
- Sincronizzazione completa e incrementale dei contenuti
- Virtual Private Cloud (VPC) (Cloud privato virtuale (VPC)

> **Note**
>
> La fine del supporto per il connettore Google Drive V1.0/Google DriveConfiguration API è prevista per il 2023. Ti consigliamo di eseguire la migrazione o l'utilizzo del connettore Google Drive V2.0/API. TemplateConfiguration

Per la risoluzione dei problemi relativi al connettore di origine dati di Amazon Kendra Google Drive, consulta. Risoluzione dei problemi relativi alle origini dati

Argomenti

- Connettore Google Drive V1.0
- Connettore Google Drive V2.0

Connettore Google Drive V1.0

Google Drive è un servizio di archiviazione di file basato su cloud. Puoi utilizzarlo Amazon Kendra per indicizzare documenti e commenti archiviati nelle cartelle Drive condivise, I miei Drive e Condivisi con me nella tua fonte di dati Google Drive. Puoi indicizzare i documenti di Google Workspace, oltre ai documenti elencati in Tipi di documentazione. Puoi anche utilizzare filtri di inclusione ed esclusione per indicizzare i contenuti in base al nome, al tipo di file e al percorso del file.

> **Note**
>
> La fine del supporto per il connettore Google Drive V1.0/Google DriveConfiguration API è prevista per il 2023. Ti consigliamo di eseguire la migrazione o l'utilizzo del connettore Google Drive V2.0/API. TemplateConfiguration

Per la risoluzione dei problemi relativi al connettore di origine dati di Amazon Kendra Google Drive, consulta. Risoluzione dei problemi relativi alle origini dati

Argomenti

Funzionalità supportate

- Mappature dei campi
- Controllo degli accessi degli utenti
- Filtri di inclusione/esclusione

Prerequisiti

Prima di poterla utilizzare Amazon Kendra per indicizzare la tua fonte di dati Google Drive, apporta queste modifiche su Google Drive e sui tuoi account. AWS

In Google Drive, assicurati di avere:

- O hai ottenuto l'accesso da un ruolo di super amministratore o sei un utente con privilegi amministrativi. Non hai bisogno di un ruolo di super amministratore se ti è stato concesso l'accesso da un ruolo di super amministratore.
- Hai creato un account di servizio con Enable G Suite Domain-wide Delegation attivato e una chiave JSON come chiave privata utilizzando l'account.
- Ho copiato l'email del tuo account utente e l'email del tuo account di servizio. Quando ti connetti, inserisci l'e-mail del tuo account utente come indirizzo e-mail dell'account amministratore e l'e-mail

del tuo account di servizio come e-mail del cliente nel campo Secrets Manager segreto. Amazon Kendra

- Hai aggiunto l'API Admin SDK e l'API Google Drive nel tuo account.
- Hai aggiunto (o richiesto a un utente con un ruolo di super amministratore di aggiungere) le seguenti autorizzazioni al tuo account di servizio utilizzando un ruolo di super amministratore:
  - 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
- È stato verificato che ogni documento sia unico in Google Drive e tra le altre fonti di dati che intendi utilizzare per lo stesso indice. Ogni fonte di dati che desideri utilizzare per un indice non deve contenere lo stesso documento in tutte le fonti di dati. Gli ID dei documenti sono globali rispetto a un indice e devono essere univoci per indice.

Nel tuo Account AWS, assicurati di avere:

- Ha creato un Amazon Kendra indice e, se si utilizza l'API, ha annotato l'ID dell'indice.
- Hai creato un IAM ruolo per la tua origine dati e, se utilizzi l'API, hai annotato l'ARN del IAM ruolo.

> **Note**
>
> Se modifichi il tipo di autenticazione e le credenziali, devi aggiornare il IAM ruolo per accedere all'ID AWS Secrets Manager segreto corretto.

- Ha archiviato le credenziali di autenticazione di Google Drive in un AWS Secrets Manager luogo segreto e, se si utilizza l'API, ha annotato l'ARN del segreto.

> **Note**
>
> Ti consigliamo di aggiornare o ruotare regolarmente le credenziali e il segreto. Fornisci solo il livello di accesso necessario per la tua sicurezza. Non è consigliabile riutilizzare credenziali e segreti tra diverse fonti di dati e versioni dei connettori 1.0 e 2.0 (ove applicabile).

Se non disponi di un IAM ruolo o di un segreto esistente, puoi utilizzare la console per creare un nuovo IAM ruolo e un Secrets Manager segreto quando connetti la tua fonte di dati Google Drive a. Amazon Kendra Se utilizzi l'API, devi fornire l'ARN di un IAM ruolo e di un Secrets Manager segreto esistenti e un ID di indice.

Istruzioni di connessione

Per connetterti Amazon Kendra alla tua fonte di dati Google Drive, devi fornire i dettagli necessari sulla tua fonte di dati Google Drive in modo che Amazon Kendra possa accedere ai tuoi dati. Se non hai ancora configurato Google Drive per Amazon Kendra vederePrerequisiti.

Console

Per connetterti Amazon Kendra a Google Drive

1. Accedi alla console di AWS gestione e apri la Amazon Kendra console.
2. Dal riquadro di navigazione a sinistra, scegli Indici, quindi scegli l'indice che desideri utilizzare dall'elenco degli indici.

   > **Note**
   >
   > Puoi scegliere di configurare o modificare le impostazioni del controllo dell'accesso degli utenti in Impostazioni dell'indice.

3. Nella pagina Guida introduttiva, scegli Aggiungi origine dati.
4. Nella pagina Aggiungi origine dati, scegli il connettore Google Drive V1.0, quindi scegli Aggiungi connettore.
5. Nella pagina Specificare i dettagli dell'origine dati, inserisci le seguenti informazioni:

   a. In Nome e descrizione, per Nome dell'origine dati, inserisci un nome per l'origine dati. Puoi includere trattini ma non spazi.
   b. (Facoltativo) Descrizione: immetti una descrizione facoltativa per la tua fonte di dati.
   c. In Lingua predefinita: scegli una lingua per filtrare i documenti per l'indice. Se non diversamente specificato, la lingua predefinita è l'inglese. La lingua specificata nei metadati del documento ha la precedenza sulla lingua selezionata.
   d. In Tag, per Aggiungi nuovo tag, includi tag opzionali per cercare e filtrare le risorse o tenere traccia dei costi. AWS
   e. Seleziona Successivo.

6. Nella pagina Definisci accesso e sicurezza, inserisci le seguenti informazioni:

   a. Per il tipo di autenticazione: scegli tra esistente e nuovo. Se scegli di utilizzare un segreto esistente, usa Seleziona segreto per scegliere il tuo segreto.

   b. Se scegli di creare un nuovo segreto, si apre un'opzione AWS Secrets Manager segreta.

      - Inserisci le seguenti informazioni nella finestra Crea un AWS Secrets Manager segreto:

        A. Nome segreto: un nome per il tuo segreto. Il prefisso 'AmazonKendra-Google Drive-' viene aggiunto automaticamente al tuo nome segreto.

        B. Per email dell'account amministratore, email del client e chiave privata, inserisci i valori delle credenziali di autenticazione che hai generato e scaricato dal tuo account Google Drive.

        C. Scegli Salva autenticazione.

   c. IAM ruolo: scegli un IAM ruolo esistente o crea un nuovo IAM ruolo per accedere alle credenziali del repository e indicizzare il contenuto.

      > **Note**
      >
      > IAM i ruoli utilizzati per gli indici non possono essere utilizzati per le fonti di dati. Se non sei sicuro che un ruolo esistente venga utilizzato per un indice o una FAQ, scegli Crea un nuovo ruolo per evitare errori.

   d. Seleziona Successivo.

7. Nella pagina Configura le impostazioni di sincronizzazione, inserisci le seguenti informazioni:

   a. Escludi gli account utente: gli utenti di Google Drive che desideri escludere dall'indice. Puoi aggiungere fino a 100 account utente.

   b. Escludi unità condivise: i dischi condivisi di Google Drive che desideri escludere dal tuo indice. Puoi aggiungere fino a 100 unità condivise.

   c. Escludi tipi di file (unità): i tipi di file di Google Drive che desideri escludere dal tuo indice. Puoi anche scegliere di modificare le selezioni dei tipi MIME.

   d. Configurazioni aggiuntive: modelli di espressioni regolari per includere o escludere determinati contenuti. È possibile aggiungere fino a 100 modelli.

e. Frequenza: con quale frequenza Amazon Kendra verrà eseguita la sincronizzazione con la fonte di dati.

f. Seleziona Successivo.

8. Nella pagina Imposta le mappature dei campi, inserisci le seguenti informazioni:

a. Per il nome del GoogleDrive campo e le mappature di campo aggiuntive suggerite, seleziona tra i campi delle origini dati predefiniti Amazon Kendra generati che desideri mappare all'indice.

b. Aggiungi campo: consente di aggiungere campi di origine dati personalizzati per creare un nome di campo indice a cui mappare e il tipo di dati del campo.

c. Seleziona Successivo.

9. Nella pagina Rivedi e crea, verifica che le informazioni inserite siano corrette, quindi seleziona Aggiungi origine dati. Puoi anche scegliere di modificare le tue informazioni da questa pagina. L'origine dati verrà visualizzata nella pagina Origini dati dopo che l'origine dati sarà stata aggiunta correttamente.

API

Per connetterti Amazon Kendra a Google Drive

È necessario specificare quanto segue utilizzando l'GoogleDriveConfigurationAPI:

- Secret Amazon Resource Name (ARN): fornisci l'Amazon Resource Name (ARN) di un Secrets Manager segreto che contiene le credenziali di autenticazione per il tuo account Google Drive. Il segreto è archiviato in una struttura JSON con le seguenti chiavi:

```
{
    "clientAccount": "service account email",
    "adminAccount": "user account email"",
    "privateKey": "private key"
}
```

> **Note**
>
> Ti consigliamo di aggiornare o ruotare regolarmente le credenziali e il segreto. Fornisci solo il livello di accesso necessario per la tua sicurezza. Non è consigliabile riutilizzare

credenziali e segreti tra diverse fonti di dati e versioni dei connettori 1.0 e 2.0 (ove applicabile).

- IAM ruolo: specifica `RoleArn` quando chiami `CreateDataSource` per fornire a un IAM ruolo le autorizzazioni per accedere al tuo Secrets Manager segreto e per chiamare le API pubbliche richieste per il connettore Google Drive e. Amazon Kendra Per ulteriori informazioni, consulta IAM i ruoli per le fonti di dati di Google Drive.

Puoi anche aggiungere le seguenti funzionalità opzionali:

- Filtri di inclusione ed esclusione: per impostazione predefinita Amazon Kendra indicizza tutti i documenti in Google Drive. Puoi specificare se includere o escludere determinati contenuti in unità condivise, account utente, tipi di documenti MIME e file. Se scegli di escludere gli account utente, nessuno dei file in My Drive di proprietà dell'account viene indicizzato. I file condivisi con l'utente vengono indicizzati a meno che non venga escluso anche il proprietario del file.

  > **Note**
  >
  > La maggior parte delle fonti di dati utilizza modelli di espressioni regolari, che sono modelli di inclusione o esclusione denominati filtri. Se si specifica un filtro di inclusione, viene indicizzato solo il contenuto che corrisponde al filtro di inclusione. Qualsiasi documento che non corrisponde al filtro di inclusione non viene indicizzato. Se si specifica un filtro di inclusione ed esclusione, i documenti che corrispondono al filtro di esclusione non vengono indicizzati, anche se corrispondono al filtro di inclusione.

- Mappature dei campi: scegli di mappare i campi delle sorgenti dati di Google Drive ai campi dell'indice. Amazon Kendra Per ulteriori informazioni, consulta la sezione Mappatura dei campi di origine dei dati.

  > **Note**
  >
  > Il campo del corpo del documento o l'equivalente del corpo del documento per i documenti è necessario per Amazon Kendra eseguire la ricerca nei documenti. È necessario mappare il nome del campo del corpo del documento nella fonte dati al nome del campo indice `_document_body`. Tutti gli altri campi sono facoltativi.

- Filtraggio del contesto utente e controllo degli accessi:Amazon Kendra esegue la scansione dell'elenco di controllo degli accessi (ACL) dei documenti, se disponi di un ACL per i documenti. Le informazioni ACL vengono utilizzate per filtrare i risultati della ricerca in base all'accesso dell'utente o del relativo gruppo ai documenti. Per ulteriori informazioni, consulta Filtraggio del contesto utente.

Ulteriori informazioni

Per ulteriori informazioni sull'integrazione Amazon Kendra con la tua fonte di dati Google Drive, consulta:

- Guida introduttiva al connettore Amazon Kendra Google Drive

Connettore Google Drive V2.0

Google Drive è un servizio di archiviazione di file basato su cloud. Puoi utilizzarlo Amazon Kendra per indicizzare documenti e commenti archiviati nelle cartelle Drive condivise, I miei Drive e Condivisi con me nella tua fonte di dati Google Drive. Puoi indicizzare i documenti di Google Workspace, oltre ai documenti elencati in Tipi di documentazione. Puoi anche utilizzare filtri di inclusione ed esclusione per indicizzare i contenuti in base al nome, al tipo di file e al percorso del file.

> **Note**
>
> La fine del supporto per il connettore Google Drive V1.0/Google DriveConfiguration API è prevista per il 2023. Ti consigliamo di eseguire la migrazione o l'utilizzo del connettore Google Drive V2.0/API. TemplateConfiguration

Per la risoluzione dei problemi relativi al connettore di origine dati di Amazon Kendra Google Drive, consulta. Risoluzione dei problemi relativi alle origini dati

Argomenti

- Funzionalità supportate
- Prerequisiti
- Istruzioni di connessione
- Note

Funzionalità supportate

- Mappature dei campi
- Controllo degli accessi degli utenti
- Filtri di inclusione/esclusione
- Sincronizzazione completa e incrementale dei contenuti
- Virtual Private Cloud (VPC) (Cloud privato virtuale (VPC)

Prerequisiti

Prima di poterla utilizzare Amazon Kendra per indicizzare la tua fonte di dati Google Drive, apporta queste modifiche su Google Drive e AWS sui tuoi account.

In Google Drive, assicurati di avere:

- O hai ottenuto l'accesso da un ruolo di super amministratore o sei un utente con privilegi amministrativi. Non hai bisogno di un ruolo di super amministratore se ti è stato concesso l'accesso da un ruolo di super amministratore.
- Credenziali di connessione all'account di servizio Google Drive configurate contenenti l'e-mail dell'account amministratore, l'e-mail del client (e-mail dell'account di servizio) e la chiave privata. Consulta la documentazione di Google Cloud sulla creazione e l'eliminazione delle chiavi dell'account di servizio.
- Hai creato un account Google Cloud Service (un account con l'autorità delegata ad assumere un'identità utente) con Enable G Suite Domain-wide Delegation attivato per server-to-server l'autenticazione, quindi ha generato una chiave privata JSON utilizzando l'account.

  > **Note**
  >
  > La chiave privata deve essere generata dopo la creazione dell'account di servizio.

- Hai aggiunto l'API Admin SDK e l'API Google Drive nel tuo account utente.
- Facoltativo: credenziali di connessione OAuth 2.0 di Google Drive configurate contenenti l'ID client, il segreto del client e il token di aggiornamento come credenziali di connessione per un utente specifico. Ne hai bisogno per eseguire la scansione dei dati dei singoli account. Consulta la documentazione di Google sull'utilizzo di OAuth 2.0 per accedere alle API.
- Hai aggiunto (o richiesto a un utente con un ruolo di super amministratore di aggiungere) i seguenti ambiti OAuth al tuo account di servizio utilizzando un ruolo di super amministratore. Questi ambiti

API sono necessari per eseguire la scansione di tutti i documenti e le informazioni sul controllo degli accessi (ACL) per tutti gli utenti di un dominio Google Workspace:

- https://www.googleapis.com/auth/drive.readonly—View e scarica tutti i tuoi file di Google Drive
- https://www.googleapis.com/auth/drive.metadata.readonly—View metadati per i file nel tuo Google Drive
- https://www.googleapis.com/auth/admin.directory.group.readonly—Scope per recuperare solo informazioni su gruppi, alias di gruppo e membri. È necessario per l'Identity Crawler. Amazon Kendra
- https://www.googleapis.com/auth/admin.directory.user.readonly—Scope per recuperare solo gli utenti o gli alias degli utenti. È necessario per elencare gli utenti nell' Amazon Kendra Identity Crawler e per impostare gli ACL.
- https://www.googleapis.com/auth/cloud-platform—Scope per generare un token di accesso per il recupero di contenuti di file Google Drive di grandi dimensioni.
- https://www.googleapis.com/auth/forms.body.readonly—Scope per recuperare dati da Google Forms.

Per supportare l'API Forms, aggiungi il seguente ambito aggiuntivo:

- https://www.googleapis.com/auth/forms.body.readonly

- È stato verificato che ogni documento sia unico in Google Drive e tra le altre fonti di dati che intendi utilizzare per lo stesso indice. Ogni fonte di dati che desideri utilizzare per un indice non deve contenere lo stesso documento in tutte le fonti di dati. Gli ID dei documenti sono globali rispetto a un indice e devono essere univoci per indice.

Nel tuo Account AWS, assicurati di avere:

- Ha creato un Amazon Kendra indice e, se si utilizza l'API, ha annotato l'ID dell'indice.
- Hai creato un IAM ruolo per la tua origine dati e, se utilizzi l'API, hai annotato l'ARN del IAM ruolo.

> **Note**
>
> Se modifichi il tipo di autenticazione e le credenziali, devi aggiornare il IAM ruolo per accedere all'ID AWS Secrets Manager segreto corretto.

- Ha archiviato le credenziali di autenticazione di Google Drive in un AWS Secrets Manager luogo segreto e, se si utilizza l'API, ha annotato l'ARN del segreto.

> **Note**
>
> Ti consigliamo di aggiornare o ruotare regolarmente le credenziali e il segreto. Fornisci solo il livello di accesso necessario per la tua sicurezza. Non è consigliabile riutilizzare credenziali e segreti tra diverse fonti di dati e versioni dei connettori 1.0 e 2.0 (ove applicabile).

Se non disponi di un IAM ruolo o di un segreto esistente, puoi utilizzare la console per creare un nuovo IAM ruolo e un Secrets Manager segreto quando connetti la tua fonte di dati Google Drive a. Amazon Kendra Se utilizzi l'API, devi fornire l'ARN di un IAM ruolo e di un Secrets Manager segreto esistenti e un ID di indice.

Istruzioni di connessione

Per connetterti Amazon Kendra alla tua fonte di dati Google Drive, devi fornire i dettagli necessari sulla tua fonte di dati Google Drive in modo che Amazon Kendra possa accedere ai tuoi dati. Se non hai ancora configurato Google Drive per Amazon Kendra vederePrerequisiti.

Console

Per connetterti Amazon Kendra a Google Drive

1. Accedi a AWS Management Console e apri la Amazon Kendra console.
2. Dal riquadro di navigazione a sinistra, scegli Indici, quindi scegli l'indice che desideri utilizzare dall'elenco degli indici.

   > **Note**
   >
   > Puoi scegliere di configurare o modificare le impostazioni del controllo dell'accesso degli utenti in Impostazioni dell'indice.

3. Nella pagina Guida introduttiva, scegli Aggiungi origine dati.
4. Nella pagina Aggiungi origine dati, scegli Connettore Google Drive, quindi scegli Aggiungi connettore.
5. Nella pagina Specificare i dettagli dell'origine dati, inserisci le seguenti informazioni:

a. In Nome e descrizione, per Nome dell'origine dati, inserisci un nome per l'origine dati. Puoi includere trattini ma non spazi.

b. (Facoltativo) Descrizione: immetti una descrizione facoltativa per la tua fonte di dati.

c. In Lingua predefinita: scegli una lingua per filtrare i documenti per l'indice. Se non diversamente specificato, la lingua predefinita è l'inglese. La lingua specificata nei metadati del documento ha la precedenza sulla lingua selezionata.

d. In Tag, per Aggiungi nuovo tag, includi tag opzionali per cercare e filtrare le risorse o tenere traccia dei costi. AWS

e. Seleziona Successivo.

6. Nella pagina Definisci accesso e sicurezza, inserisci le seguenti informazioni:

a. Autorizzazione: attiva o disattiva le informazioni dell'elenco di controllo degli accessi (ACL) per i tuoi documenti, se disponi di un ACL e desideri utilizzarlo per il controllo degli accessi. L'ACL specifica a quali documenti possono accedere utenti e gruppi. Le informazioni ACL vengono utilizzate per filtrare i risultati della ricerca in base all'accesso dell'utente o del relativo gruppo ai documenti. Per ulteriori informazioni, consulta Filtraggio del contesto utente.

b. Per l'autenticazione: scegli tra l'account di servizio Google e l'autenticazione OAuth 2.0 in base al tuo caso d'uso.

c. AWS Secrets Manager segreto: scegli un segreto esistente o creane uno nuovo per archiviare le Secrets Manager credenziali di autenticazione di Google Drive. Se scegli di creare un nuovo segreto, si apre una finestra AWS Secrets Manager segreta.

i. Se hai scelto un account di servizio Google, inserisci un nome per il tuo account segreto, l'ID email dell'utente amministratore o «Utente dell'account di servizio» nella configurazione dell'account di servizio (email dell'amministratore), l'ID e-mail dell'account di servizio (email del client) e la chiave privata che hai creato nel tuo account di servizio.

Salva e aggiungi il tuo segreto

ii. Se hai scelto l'autenticazione OAuth 2.0, inserisci un nome per il segreto, l'ID cliente, il segreto client e il token di aggiornamento che hai creato nel tuo account OAuth.

Salva e aggiungi il tuo segreto.

d. Virtual Private Cloud (VPC): puoi scegliere di utilizzare un VPC. In tal caso, è necessario aggiungere sottoreti e gruppi di sicurezza VPC.

e. (Solo per gli utenti dell'autenticazione dell'account del servizio Google)

Identity crawler: specifica se attivare il crawler Amazon Kendra di identità. Il crawler di identità utilizza le informazioni dell'elenco di controllo degli accessi (ACL) per i documenti per filtrare i risultati della ricerca in base all'accesso dell'utente o del relativo gruppo ai documenti. Se disponi di un ACL per i tuoi documenti e scegli di utilizzarlo, puoi anche scegliere di attivare il crawler di identità per configurare il filtraggio Amazon Kendra del contesto utente dei risultati di ricerca. Altrimenti, se il crawler di identità è disattivato, tutti i documenti possono essere ricercati pubblicamente. Se desideri utilizzare il controllo degli accessi per i tuoi documenti e il crawler di identità è disattivato, in alternativa puoi utilizzare l'PutPrincipalMappingAPI per caricare le informazioni di accesso di utenti e gruppi per il filtraggio del contesto degli utenti.

f. IAM ruolo: scegli un IAM ruolo esistente o creane uno nuovo IAM per accedere alle credenziali del repository e indicizzare il contenuto.

> **Note**
>
> IAM i ruoli utilizzati per gli indici non possono essere utilizzati per le fonti di dati. Se non sei sicuro che un ruolo esistente venga utilizzato per un indice o una FAQ, scegli Crea un nuovo ruolo per evitare errori.

g. Seleziona Successivo.

7. Nella pagina Configura le impostazioni di sincronizzazione, inserisci le seguenti informazioni:

a. Sincronizza contenuti: seleziona le opzioni o il contenuto che desideri sottoporre a scansione. Puoi scegliere di eseguire la scansione di My Drive (cartelle personali), Shared Drive (cartelle condivise con te) o entrambi. Puoi anche includere commenti sui file.

b. In Configurazione aggiuntiva - opzionale È inoltre possibile inserire le seguenti informazioni opzionali:

i. Destinatari: aggiungi destinatari specifici per i documenti che desideri sottoporre a scansione.

ii. Dimensione massima del file: imposta il limite di dimensione massima in MB di file da sottoporre a scansione.

iii. Email utente: consente di aggiungere le e-mail degli utenti che si desidera includere o escludere.

iv. Unità condivise: aggiungi i nomi delle unità condivise che desideri includere o escludere.

v. Tipi MIME: aggiungi i tipi MIME che desideri includere o escludere.

vi. Modelli di espressioni regolari delle entità: aggiungono modelli di espressioni regolari per includere o escludere determinati allegati per tutte le entità supportate. È possibile aggiungere fino a 100 pattern.

c. Modalità di sincronizzazione: scegli come aggiornare l'indice quando il contenuto dell'origine dati cambia. Quando sincronizzi l'origine dati con Amazon Kendra per la prima volta, tutto il contenuto viene sottoposto a scansione e indicizzato per impostazione predefinita. Se la sincronizzazione iniziale non è riuscita, devi eseguire una sincronizzazione completa dei dati, anche se non scegli la sincronizzazione completa come opzione della modalità di sincronizzazione.

- Sincronizzazione completa: indicizza di nuovo tutti i contenuti, sostituendo i contenuti esistenti ogni volta che l'origine dati si sincronizza con l'indice.
- Nuova sincronizzazione modificata: indicizza solo i contenuti nuovi e modificati ogni volta che l'origine dati si sincronizza con l'indice. Amazon Kendra può utilizzare il meccanismo dell'origine dati per tenere traccia delle modifiche ai contenuti e indicizzare i contenuti modificati dall'ultima sincronizzazione.
- Sincronizzazione nuova, modificata ed eliminata: indicizza solo i contenuti nuovi, modificati ed eliminati ogni volta che l'origine dati si sincronizza con l'indice. Amazon Kendra può utilizzare il meccanismo dell'origine dati per tenere traccia delle modifiche ai contenuti e indicizzare i contenuti modificati dall'ultima sincronizzazione.

> **Important**
>
> L'API di Google Drive non supporta il recupero dei commenti da un file eliminato definitivamente. I commenti dai file cestinati sono recuperabili. Quando un file viene cestinato, il connettore elimina i commenti dall'indice. Amazon Kendra

d. In Pianificazione di esecuzione della sincronizzazione, per Frequenza, scegli la frequenza con cui sincronizzare il contenuto della fonte di dati e aggiornare l'indice.

e. Nella cronologia di esecuzione di Sync, scegli di archiviare i report generati automaticamente in un attimo Amazon S3 durante la sincronizzazione della tua fonte di dati. Ciò è utile per tenere traccia dei problemi durante la sincronizzazione della fonte di dati.

f. Seleziona Successivo.

8. Nella pagina Imposta mappature dei campi, inserisci le seguenti informazioni:

   a. Per i file: seleziona uno dei campi di origine dati predefiniti Amazon Kendra generati che desideri mappare all'indice.

   > **Note**
   >
   > L'API di Google Drive non supporta la creazione di campi personalizzati. La mappatura personalizzata dei campi non è disponibile per il connettore Google Drive.

   b. Seleziona Successivo.

9. Nella pagina Rivedi e crea, verifica che le informazioni inserite siano corrette, quindi seleziona Aggiungi origine dati. Puoi anche scegliere di modificare le tue informazioni da questa pagina. L'origine dati verrà visualizzata nella pagina Origini dati dopo che l'origine dati sarà stata aggiunta correttamente.

API

Per connetterti Amazon Kendra a Google Drive

È necessario specificare un codice JSON dello schema dell'origine dati utilizzando l'TemplateConfigurationAPI. È necessario fornire le seguenti informazioni:

- Origine dati: specifica il tipo di origine dati come `GOOGLEDRIVEV2` quando usi lo schema TemplateConfigurationJSON. Specificate anche l'origine dati come `TEMPLATE` quando chiamate l'CreateDataSourceAPI.
- Tipo di autenticazione: specifica se utilizzare l'autenticazione dell'account di servizio o l'autenticazione OAuth 2.0.
- Modalità di sincronizzazione: specifica come Amazon Kendra aggiornare l'indice quando il contenuto dell'origine dati cambia. Quando sincronizzi l'origine dati con Amazon Kendra per la prima volta, tutto il contenuto viene sottoposto a scansione e indicizzato per impostazione

predefinita. Se la sincronizzazione iniziale non è riuscita, devi eseguire una sincronizzazione completa dei dati, anche se non scegli la sincronizzazione completa come opzione della modalità di sincronizzazione. Puoi scegliere tra:

- `FORCED_FULL_CRAWL`per indicizzare nuovamente tutti i contenuti, sostituendo i contenuti esistenti ogni volta che l'origine dati si sincronizza con l'indice.
- `FULL_CRAWL`per indicizzare solo i contenuti nuovi, modificati ed eliminati ogni volta che l'origine dati si sincronizza con l'indice. Amazon Kendra può utilizzare il meccanismo dell'origine dati per tenere traccia delle modifiche ai contenuti e indicizzare i contenuti modificati dall'ultima sincronizzazione.
- `CHANGE_LOG`per indicizzare solo contenuti nuovi e modificati ogni volta che l'origine dati si sincronizza con l'indice. Amazon Kendra può utilizzare il meccanismo dell'origine dati per tenere traccia delle modifiche ai contenuti e indicizzare i contenuti modificati dall'ultima sincronizzazione.

> **Important**
>
> L'API di Google Drive non supporta il recupero dei commenti da un file eliminato definitivamente. I commenti dai file cestinati sono recuperabili. Quando un file viene cestinato, il connettore elimina i commenti dall'indice. Amazon Kendra

- Secret Amazon Resource Name (ARN): fornisci l'Amazon Resource Name (ARN) di un Secrets Manager segreto che contiene le credenziali di autenticazione che hai creato nel tuo account Google Drive. Se utilizzi l'autenticazione dell'account del servizio Google, il segreto viene archiviato in una struttura JSON con le seguenti chiavi:

```
{
    "clientEmail": "user account email",
    "adminAccountEmail": "service account email",
    "privateKey": "private key"
}
```

Se utilizzi l'autenticazione OAuth 2.0, il segreto viene archiviato in una struttura JSON con le seguenti chiavi:

```
{
    "clientID": "OAuth client ID",
    "clientSecret": "client secret",
    "refreshToken": "refresh token"
```

```
}
```

> **Note**
>
> Ti consigliamo di aggiornare o ruotare regolarmente le credenziali e il segreto. Fornisci solo il livello di accesso necessario per la tua sicurezza. Non è consigliabile riutilizzare credenziali e segreti tra diverse fonti di dati e versioni dei connettori 1.0 e 2.0 (ove applicabile).

- IAM ruolo: specifica `RoleArn` quando chiami `CreateDataSource` per fornire a un IAM ruolo le autorizzazioni per accedere al tuo Secrets Manager segreto e per chiamare le API pubbliche richieste per il connettore Google Drive e. Amazon Kendra Per ulteriori informazioni, consulta IAM i ruoli per le fonti di dati di Google Drive.

Puoi anche aggiungere le seguenti funzionalità opzionali:

- Virtual Private Cloud (VPC): `VpcConfiguration` specifica quando si chiama. `CreateDataSource` Per ulteriori informazioni, consulta Configurazione Amazon Kendra per l'utilizzo di un Amazon VPC.
- I miei drive, Shared Drives, Comments: puoi specificare se eseguire la scansione di questi tipi di contenuti.
- Filtri di inclusione ed esclusione: puoi specificare se includere o escludere determinati account utente, unità condivise e tipi MIME.

> **Note**
>
> La maggior parte delle fonti di dati utilizza modelli di espressioni regolari, che sono modelli di inclusione o esclusione denominati filtri. Se si specifica un filtro di inclusione, viene indicizzato solo il contenuto che corrisponde al filtro di inclusione. Qualsiasi documento che non corrisponde al filtro di inclusione non viene indicizzato. Se si specifica un filtro di inclusione ed esclusione, i documenti che corrispondono al filtro di esclusione non vengono indicizzati, anche se corrispondono al filtro di inclusione.

- Elenco di controllo degli accessi (ACL): specifica se eseguire la scansione delle informazioni ACL per i documenti, se disponi di un ACL e desideri utilizzarlo per il controllo degli accessi. L'ACL specifica a quali documenti possono accedere utenti e gruppi. Le informazioni ACL

vengono utilizzate per filtrare i risultati della ricerca in base all'accesso dell'utente o del relativo gruppo ai documenti. Per ulteriori informazioni, consulta Filtraggio del contesto utente.

- Identity crawler: specifica se attivare il crawler di identità. Amazon Kendra Il crawler di identità utilizza le informazioni dell'elenco di controllo degli accessi (ACL) per i documenti per filtrare i risultati della ricerca in base all'accesso dell'utente o del relativo gruppo ai documenti. Se disponi di un ACL per i tuoi documenti e scegli di utilizzarlo, puoi anche scegliere di attivare il crawler di identità per configurare il filtraggio Amazon Kendra del contesto utente dei risultati di ricerca. Altrimenti, se il crawler di identità è disattivato, tutti i documenti possono essere ricercati pubblicamente. Se desideri utilizzare il controllo degli accessi per i tuoi documenti e il crawler di identità è disattivato, in alternativa puoi utilizzare l'PutPrincipalMappingAPI per caricare le informazioni di accesso di utenti e gruppi per il filtraggio del contesto degli utenti.
- Mappature dei campi: scegli di mappare i campi delle sorgenti dati di Google Drive ai campi dell'indice. Amazon Kendra Per ulteriori informazioni, consulta la sezione Mappatura dei campi di origine dei dati.

> **Note**
>
> Il campo del corpo del documento o l'equivalente del corpo del documento per i documenti è necessario per Amazon Kendra eseguire la ricerca nei documenti. È necessario mappare il nome del campo del corpo del documento nella fonte dati al nome del campo indice`_document_body`. Tutti gli altri campi sono facoltativi.

Per un elenco di altre importanti chiavi JSON da configurare, consulta lo schema del modello di Google Drive.

Note

- La mappatura personalizzata dei campi non è disponibile per il connettore Google Drive poiché l'interfaccia utente di Google Drive non supporta la creazione di campi personalizzati.
- L'API di Google Drive non supporta il recupero dei commenti da un file eliminato definitivamente. I commenti sono recuperabili, tuttavia, per i file cestinati. Quando un file viene cestinato, il Amazon Kendra connettore eliminerà i commenti dall'indice. Amazon Kendra
- L'API di Google Drive non restituisce i commenti presenti in un file.docx.

IBM DB2

IBM DB2è un sistema di gestione di database relazionali sviluppato daIBM. Se sei un IBM DB2 utente, puoi utilizzarlo Amazon Kendra per indicizzare la tua fonte di IBM DB2 dati. Il connettore di origine Amazon Kendra IBM DB2 dati supporta DB2 11.5.7.

Puoi connetterti Amazon Kendra alla tua fonte di IBM DB2 dati utilizzando la Amazon Kendra console e l'API. TemplateConfiguration

Per la risoluzione dei problemi relativi al connettore della sorgente Amazon Kendra IBM DB2 dati, consultaRisoluzione dei problemi relativi alle origini dati.

Argomenti

- Funzionalità supportate
- Prerequisiti
- Istruzioni di connessione
- Note

Funzionalità supportate

- Mappature dei campi
- Filtraggio del contesto utente
- Filtri di inclusione/esclusione
- Sincronizzazione completa e incrementale dei contenuti
- Virtual Private Cloud (VPC) (Cloud privato virtuale (VPC)

Prerequisiti

Prima di poterla utilizzare Amazon Kendra per indicizzare la tua fonte di IBM DB2 dati, apporta queste modifiche al tuo account IBM DB2 e AWS ai tuoi account.

NelIBM DB2, assicurati di avere:

- Hai annotato il nome utente e la password del database.

> **Important**
>
> È consigliabile fornire credenziali Amazon Kendra di database di sola lettura.

- Hai copiato l'URL, la porta e l'istanza dell'host del database.
- È stato verificato che ogni documento sia unico all'interno IBM DB2 e tra le altre fonti di dati che intendi utilizzare per lo stesso indice. Ogni fonte di dati che desideri utilizzare per un indice non deve contenere lo stesso documento in tutte le fonti di dati. Gli ID dei documenti sono globali rispetto a un indice e devono essere univoci per indice.

Nel tuo Account AWS, assicurati di avere:

- Ha creato un Amazon Kendra indice e, se si utilizza l'API, ha annotato l'ID dell'indice.
- Hai creato un IAM ruolo per la tua origine dati e, se utilizzi l'API, hai annotato l'ARN del IAM ruolo.

> **Note**
>
> Se modifichi il tipo di autenticazione e le credenziali, devi aggiornare il IAM ruolo per accedere all'ID AWS Secrets Manager segreto corretto.

- Ha archiviato le credenziali di IBM DB2 autenticazione in un AWS Secrets Manager segreto e, se si utilizza l'API, ha annotato l'ARN del segreto.

> **Note**
>
> Ti consigliamo di aggiornare o ruotare regolarmente le credenziali e il segreto. Fornisci solo il livello di accesso necessario per la tua sicurezza. Non è consigliabile riutilizzare credenziali e segreti tra diverse fonti di dati e versioni dei connettori 1.0 e 2.0 (ove applicabile).

Se non disponi di un IAM ruolo o di un segreto esistente, puoi utilizzare la console per creare un nuovo IAM ruolo e un Secrets Manager segreto quando connetti la tua origine IBM DB2 dati a. Amazon Kendra Se utilizzi l'API, devi fornire l'ARN di un IAM ruolo e di un Secrets Manager segreto esistenti e un ID di indice.

Istruzioni di connessione

Per connetterti Amazon Kendra alla tua fonte di IBM DB2 dati devi fornire i dettagli delle tue IBM DB2 credenziali in modo da Amazon Kendra poter accedere ai tuoi dati. Se non lo hai ancora configurato, IBM DB2 Amazon Kendra Prerequisiti consulta.

Console

Per connettersi Amazon Kendra a IBM DB2

1. Accedi a AWS Management Console e apri la Amazon Kendra console.
2. Dal riquadro di navigazione a sinistra, scegli Indici, quindi scegli l'indice che desideri utilizzare dall'elenco degli indici.

> **Note**
>
> Puoi scegliere di configurare o modificare le impostazioni del controllo dell'accesso degli utenti in Impostazioni dell'indice.

3. Nella pagina Guida introduttiva, scegli Aggiungi origine dati.
4. Nella pagina Aggiungi origine dati, scegli IBM DB2connettore, quindi scegli Aggiungi connettore.
5. Nella pagina Specificare i dettagli dell'origine dati, inserisci le seguenti informazioni:
   a. In Nome e descrizione, per Nome dell'origine dati, inserisci un nome per l'origine dati. Puoi includere trattini ma non spazi.
   b. (Facoltativo) Descrizione: immetti una descrizione facoltativa per l'origine dati.
   c. In Lingua predefinita: scegli una lingua per filtrare i documenti per l'indice. Se non diversamente specificato, la lingua predefinita è l'inglese. La lingua specificata nei metadati del documento ha la precedenza sulla lingua selezionata.
   d. In Tag, per Aggiungi nuovo tag, includi tag opzionali per cercare e filtrare le risorse o tenere traccia dei costi. AWS
   e. Seleziona Successivo.
6. Nella pagina Definisci accesso e sicurezza, inserisci le seguenti informazioni:
   a. In Source, inserisci le seguenti informazioni:
   b. Host: immettere il nome host del database.

c. Porta: immettere la porta del database.

d. Istanza: immettere l'istanza del database.

e. Abilita la posizione del certificato SSL: scegli di inserire il Amazon S3 percorso del file del certificato SSL.

f. In Autenticazione, inserisci le seguenti informazioni:

- AWS Secrets Manager segreto: scegli un segreto esistente o creane uno nuovo Secrets Manager per memorizzare le credenziali di IBM DB2 autenticazione. Se scegli di creare un nuovo segreto, si apre una finestra AWS Secrets Manager segreta.

  A. Inserisci le seguenti informazioni nella finestra Crea un AWS Secrets Manager segreto:

     I. Nome segreto: un nome per il tuo segreto. Il prefisso 'AmazonKendra- IBM DB2 -' viene aggiunto automaticamente al nome segreto.

     II. Per nome utente e password del database, immettete i valori delle credenziali di autenticazione copiati dal database.

  B. Selezionare Salva.

g. Virtual Private Cloud (VPC): puoi scegliere di utilizzare un VPC. In tal caso, è necessario aggiungere sottoreti e gruppi di sicurezza VPC.

h. IAM ruolo: scegli un IAM ruolo esistente o creane uno nuovo IAM per accedere alle credenziali del repository e indicizzare il contenuto.

> **Note**
>
> IAM i ruoli utilizzati per gli indici non possono essere utilizzati per le fonti di dati. Se non sei sicuro che un ruolo esistente venga utilizzato per un indice o una FAQ, scegli Crea un nuovo ruolo per evitare errori.

i. Seleziona Successivo.

7. Nella pagina Configura le impostazioni di sincronizzazione, inserisci le seguenti informazioni:

a. Nell'ambito della sincronizzazione, scegli tra le seguenti opzioni:

- Query SQL: immetti istruzioni di query SQL come le operazioni SELECT e JOIN. Le query SQL devono pesare meno di 32 KB. Amazon Kendra eseguirà la scansione di tutto il contenuto del database che corrisponde alla tua query.
- Colonna chiave primaria: fornisce la chiave primaria per la tabella del database. Identifica una tabella all'interno del database.
- Colonna del titolo: fornisce il nome della colonna del titolo del documento all'interno della tabella del database.
- Colonna del corpo: fornisce il nome della colonna del corpo del documento all'interno della tabella del database.

b. In Configurazione aggiuntiva, facoltativa, scegli una delle seguenti opzioni per sincronizzare contenuti specifici anziché sincronizzare tutti i file:

- Colonne di rilevamento delle modifiche: immetti i nomi delle colonne che Amazon Kendra verranno utilizzate per rilevare le modifiche al contenuto. Amazon Kendra reindicizzerà il contenuto in caso di modifica in una di queste colonne.
- Colonna ID utente: immetti il nome della colonna che contiene gli ID utente a cui consentire l'accesso ai contenuti.
- Colonna Gruppi: immetti il nome della colonna che contiene i gruppi a cui consentire l'accesso ai contenuti.
- Colonna URL di origine: inserisci il nome della colonna che contiene gli URL di origine da indicizzare.
- Colonna timestamp: immetti il nome della colonna che contiene i timestamp. Amazon Kendra utilizza le informazioni relative alla marca temporale per rilevare le modifiche ai contenuti e sincronizzare solo i contenuti modificati.
- Colonna dei fusi orari: inserisci il nome della colonna che contiene i fusi orari per il contenuto da sottoporre a scansione.
- Formato timestamp: immetti il nome della colonna che contiene i formati di timestamp da utilizzare per rilevare le modifiche ai contenuti e risincronizzare i contenuti.

c. Modalità di sincronizzazione: scegli come aggiornare l'indice quando il contenuto della fonte dati cambia. Quando sincronizzi l'origine dati con Amazon Kendra per la prima volta, tutto il contenuto viene sottoposto a scansione e indicizzato per impostazione predefinita. Se la sincronizzazione iniziale non è riuscita, devi eseguire una sincronizzazione completa dei dati, anche se non scegli la sincronizzazione completa come opzione della modalità di sincronizzazione.

- Sincronizzazione completa: indicizza di nuovo tutti i contenuti, sostituendo i contenuti esistenti ogni volta che l'origine dati si sincronizza con l'indice.
- Nuova sincronizzazione modificata: indicizza solo i contenuti nuovi e modificati ogni volta che l'origine dati si sincronizza con l'indice. Amazon Kendra può utilizzare il meccanismo dell'origine dati per tenere traccia delle modifiche ai contenuti e indicizzare i contenuti modificati dall'ultima sincronizzazione.
- Sincronizzazione nuova, modificata ed eliminata: indicizza solo i contenuti nuovi, modificati ed eliminati ogni volta che l'origine dati si sincronizza con l'indice. Amazon Kendra può utilizzare il meccanismo dell'origine dati per tenere traccia delle modifiche ai contenuti e indicizzare i contenuti modificati dall'ultima sincronizzazione.

d. Pianificazione di esecuzione di In Sync, per Frequenza: con quale frequenza Amazon Kendra verrà eseguita la sincronizzazione con la fonte di dati.

e. Seleziona Successivo.

8. Nella pagina Imposta mappature dei campi, inserisci le seguenti informazioni:

a. Seleziona uno dei campi di origine dati predefiniti generati (ID documento, titoli dei documenti e URL di origine) che desideri mappare per indicizzare. Amazon Kendra

b. Aggiungi campo: consente di aggiungere campi di origine dati personalizzati per creare un nome di campo indice a cui mappare e il tipo di dati del campo.

c. Seleziona Successivo.

9. Nella pagina Rivedi e crea, verifica che le informazioni inserite siano corrette, quindi seleziona Aggiungi origine dati. Puoi anche scegliere di modificare le tue informazioni da questa pagina. L'origine dati verrà visualizzata nella pagina Origini dati dopo che l'origine dati sarà stata aggiunta correttamente.

API

Per connettersi Amazon Kendra a IBM DB2

È necessario specificare quanto segue utilizzando l'TemplateConfigurationAPI:

- Origine dati: specifica il tipo di origine dati come `JDBC` quando usi lo schema TemplateConfigurationJSON. Specificate anche l'origine dati come `TEMPLATE` quando chiamate l'CreateDataSourceAPI.
- Tipo di database: è necessario specificare il tipo di database come`db2`.

- Query SQL: specifica le istruzioni di query SQL come le operazioni SELECT e JOIN. Le query SQL devono pesare meno di 32 KB. Amazon Kendra eseguirà la scansione di tutto il contenuto del database che corrisponde alla tua query.
- Modalità di sincronizzazione: specifica come Amazon Kendra aggiornare l'indice quando il contenuto dell'origine dati cambia. Quando sincronizzi l'origine dati con Amazon Kendra per la prima volta, tutto il contenuto viene sottoposto a scansione e indicizzato per impostazione predefinita. Se la sincronizzazione iniziale non è riuscita, devi eseguire una sincronizzazione completa dei dati, anche se non scegli la sincronizzazione completa come opzione della modalità di sincronizzazione. Puoi scegliere tra:
  - `FORCED_FULL_CRAWL`per indicizzare nuovamente tutti i contenuti, sostituendo i contenuti esistenti ogni volta che l'origine dati si sincronizza con l'indice.
  - `FULL_CRAWL`per indicizzare solo i contenuti nuovi, modificati ed eliminati ogni volta che l'origine dati si sincronizza con l'indice. Amazon Kendra può utilizzare il meccanismo dell'origine dati per tenere traccia delle modifiche ai contenuti e indicizzare i contenuti modificati dall'ultima sincronizzazione.
  - `CHANGE_LOG`per indicizzare solo contenuti nuovi e modificati ogni volta che l'origine dati si sincronizza con l'indice. Amazon Kendra può utilizzare il meccanismo dell'origine dati per tenere traccia delle modifiche ai contenuti e indicizzare i contenuti modificati dall'ultima sincronizzazione.
- Amazon Resource Name (ARN) segreto: fornisci l'Amazon Resource Name (ARN) di un Secrets Manager segreto che contiene le credenziali di autenticazione che hai creato nel tuo account. IBM DB2 Il segreto è archiviato in una struttura JSON con le seguenti chiavi:

```
{
    "user name": "database user name",
    "password": "password"
}
```

> **Note**
>
> Ti consigliamo di aggiornare o ruotare regolarmente le credenziali e il segreto. Fornisci solo il livello di accesso necessario per la tua sicurezza. Non è consigliabile riutilizzare credenziali e segreti tra diverse fonti di dati e versioni dei connettori 1.0 e 2.0 (ove applicabile).

- IAM ruolo: specifica `RoleArn` quando chiami `CreateDataSource` per fornire a un IAM ruolo le autorizzazioni per accedere al tuo Secrets Manager segreto e per chiamare le API pubbliche richieste per il connettore e. IBM DB2 Amazon Kendra Per ulteriori informazioni, consulta i IAM ruoli per IBM DB2 le fonti di dati.

Puoi anche aggiungere le seguenti funzionalità opzionali:

- Virtual Private Cloud (VPC): `VpcConfiguration` specifica quando si chiama. `CreateDataSource` Per ulteriori informazioni, consulta Configurazione Amazon Kendra per l'utilizzo di un Amazon VPC.
- Filtri di inclusione ed esclusione: puoi specificare se includere contenuti specifici utilizzando ID utente, gruppi, URL di origine, timestamp e fusi orari.
- Filtraggio del contesto utente e controllo degli accessi:Amazon Kendra esegue la ricerca per indicizzazione dell'elenco di controllo degli accessi (ACL) dei documenti, se disponi di un ACL per i documenti. Le informazioni ACL vengono utilizzate per filtrare i risultati della ricerca in base all'accesso dell'utente o del relativo gruppo ai documenti. Per ulteriori informazioni, consulta Filtraggio del contesto utente.
- Mappature dei campi: scegli di mappare i campi delle sorgenti IBM DB2 dati ai campi indice. Amazon Kendra Per ulteriori informazioni, consulta la sezione Mappatura dei campi di origine dei dati.

> **Note**
>
> Il campo del corpo del documento o l'equivalente del corpo del documento per i documenti è necessario per Amazon Kendra eseguire la ricerca nei documenti. È necessario mappare il nome del campo del corpo del documento nella fonte dati al nome del campo indice`_document_body`. Tutti gli altri campi sono facoltativi.

Per un elenco di altre importanti chiavi JSON da configurare, consultaSchema del modello IBM DB2.

Note

- Le righe del database eliminate non verranno registrate durante la Amazon Kendra verifica della presenza di contenuti aggiornati.

- La dimensione dei nomi e dei valori dei campi in una riga del database non può superare i 400 KB.
- Se l'origine dati del database contiene una grande quantità di dati e non desideri Amazon Kendra indicizzare tutto il contenuto del database dopo la prima sincronizzazione, puoi scegliere di sincronizzare solo i documenti nuovi, modificati o eliminati.
- È consigliabile fornire credenziali Amazon Kendra di database di sola lettura.
- È consigliabile evitare di aggiungere tabelle con dati sensibili o informazioni personali identificabili (PII).

Jira

Jira è uno strumento di gestione dei progetti per lo sviluppo di software, la gestione dei prodotti e il monitoraggio dei bug. Puoi utilizzarlo Amazon Kendra per indicizzare i progetti, i problemi, i commenti, gli allegati, i registri di lavoro e gli stati di Jira.

Amazon Kendra attualmente supporta solo Jira Cloud.

Puoi connetterti Amazon Kendra alla tua fonte di dati Jira utilizzando la Amazon Kendra console o l'JiraConfiguration API. Per un elenco delle funzionalità supportate da ciascuna di esse, consultaFunzionalità supportate.

Per la risoluzione dei problemi relativi al connettore di origine dati Amazon Kendra Jira, consultaRisoluzione dei problemi relativi alle origini dati.

Argomenti

- Funzionalità supportate
- Prerequisiti
- Istruzioni di connessione
- Ulteriori informazioni

Funzionalità supportate

Amazon Kendra Il connettore di origine dati Jira supporta le seguenti funzionalità:

- Log delle modifiche
- Mappature dei campi
- Filtraggio del contesto utente

- Filtri di inclusione/esclusione
- Virtual Private Cloud (VPC) (Cloud privato virtuale (VPC)

Prerequisiti

Prima di poterla utilizzare Amazon Kendra per indicizzare la tua fonte di dati Jira, apporta queste modifiche a Jira e agli account. AWS

In Jira, assicurati di avere:

- Credenziali di autenticazione del token Jira API create che includono un ID Jira (nome utente o email) e una credenziale Jira (token API Jira). Consulta la documentazione di Atlassian sulla gestione dei token API.
- Hai preso nota dell'URL dell'account Jira nelle impostazioni del tuo account Jira. *Ad esempio, https://company.atlassian.net/.*
- È stato verificato che ogni documento sia unico in Jira e tra le altre fonti di dati che intendi utilizzare per lo stesso indice. Ogni fonte di dati che desideri utilizzare per un indice non deve contenere lo stesso documento in tutte le fonti di dati. Gli ID dei documenti sono globali rispetto a un indice e devono essere univoci per indice.

Nel tuo Account AWS, assicurati di avere:

- Ha creato un Amazon Kendra indice e, se si utilizza l'API, ha annotato l'ID dell'indice.
- Hai creato un IAM ruolo per la tua origine dati e, se utilizzi l'API, hai annotato l'ARN del IAM ruolo.

> **Note**
>
> Se modifichi il tipo di autenticazione e le credenziali, devi aggiornare il IAM ruolo per accedere all'ID AWS Secrets Manager segreto corretto.

- Ha archiviato le credenziali di autenticazione Jira in un AWS Secrets Manager segreto e, se si utilizza l'API, ha annotato l'ARN del segreto.

> **Note**
>
> Ti consigliamo di aggiornare o ruotare regolarmente le credenziali e il segreto. Fornisci solo il livello di accesso necessario per la tua sicurezza. Non è consigliabile riutilizzare

credenziali e segreti tra diverse fonti di dati e nelle versioni 1.0 e 2.0 dei connettori (ove applicabile).

Se non disponi di un IAM ruolo o di un segreto esistente, puoi utilizzare la console per creare un nuovo IAM ruolo e un Secrets Manager segreto quando connetti la tua fonte di dati Jira a. Amazon Kendra Se utilizzi l'API, devi fornire l'ARN di un IAM ruolo e di un Secrets Manager segreto esistenti e un ID di indice.

Istruzioni di connessione

Per connetterti Amazon Kendra alla tua fonte dati Jira, devi fornire i dettagli necessari della tua origine dati Jira in modo che Amazon Kendra possa accedere ai tuoi dati. Se non hai ancora configurato Jira per Amazon Kendra, consulta. Prerequisiti

Console

Per connettersi Amazon Kendra a Jira

1. Accedi a AWS Management Console e apri la Amazon Kendra console.
2. Dal riquadro di navigazione a sinistra, scegli Indici, quindi scegli l'indice che desideri utilizzare dall'elenco degli indici.

   > **Note**
   >
   > Puoi scegliere di configurare o modificare le impostazioni del controllo dell'accesso degli utenti in Impostazioni dell'indice.

3. Nella pagina Guida introduttiva, scegli Aggiungi origine dati.
4. Nella pagina Aggiungi origine dati, scegli Connettore Jira, quindi scegli Aggiungi connettore.
5. Nella pagina Specificare i dettagli dell'origine dati, inserisci le seguenti informazioni:

   a. In Nome e descrizione, per Nome dell'origine dati, inserisci un nome per l'origine dati. Puoi includere trattini ma non spazi.

   b. (Facoltativo) Descrizione: immetti una descrizione facoltativa per l'origine dati.

   c. In Lingua predefinita: scegli una lingua per filtrare i documenti per l'indice. Se non diversamente specificato, la lingua predefinita è l'inglese. La lingua specificata nei metadati del documento ha la precedenza sulla lingua selezionata.

d. In Tag, per Aggiungi nuovo tag, includi tag opzionali per cercare e filtrare le risorse o tenere traccia dei costi. AWS

e. Seleziona Successivo.

6. Nella pagina Definisci accesso e sicurezza, inserisci le seguenti informazioni:

a. URL dell'account Jira: inserisci l'URL del tuo account Jira. *Ad esempio: https://company.atlassian.net/.*

b. AWS Secrets Manager segreto: scegli un segreto esistente o creane uno nuovo Secrets Manager per archiviare le credenziali di autenticazione Jira. Se scegli di creare un nuovo segreto, si apre una finestra AWS Secrets Manager segreta.

i. Inserisci le seguenti informazioni nella finestra Crea un AWS Secrets Manager segreto:

A. Nome segreto: un nome per il tuo segreto. Il prefisso 'AmazonKendra-Jira-' viene aggiunto automaticamente al tuo nome segreto.

B. Per Jira ID: inserisci il nome utente o l'email di Jira.

C. Per Password/Token: inserisci il token API Jira che hai creato dal tuo account Jira.

ii. Selezionare Salva.

c. Virtual Private Cloud (VPC): puoi scegliere di utilizzare un VPC. In tal caso, è necessario aggiungere sottoreti e gruppi di sicurezza VPC.

d. IAM ruolo: scegli un IAM ruolo esistente o creane uno nuovo IAM per accedere alle credenziali del repository e indicizzare il contenuto.

> **Note**
>
> IAM i ruoli utilizzati per gli indici non possono essere utilizzati per le fonti di dati. Se non sei sicuro che un ruolo esistente venga utilizzato per un indice o una FAQ, scegli Crea un nuovo ruolo per evitare errori.

e. Seleziona Successivo.

7. Nella pagina Configura le impostazioni di sincronizzazione, inserisci le seguenti informazioni:

a. Seleziona i progetti Jira da indicizzare: le entità o i tipi di contenuto Jira che desideri sottoporre a scansione.

b. Stati, elementi aggiuntivi e tipi di problema: seleziona il contenuto per rifinire l'ambito dell'indice.

c. Registro delle modifiche: seleziona questa opzione per aggiornare l'indice solo con contenuti nuovi o modificati anziché sincronizzare tutti i file.

d. Modelli Regex: modelli di espressioni regolari per includere o escludere determinati file. È possibile aggiungere fino a 100 pattern.

e. In Pianificazione di esecuzione della sincronizzazione, per Frequenza: scegli la frequenza di sincronizzazione di Amazon Kendra con la tua fonte di dati.

f. Seleziona Successivo.

8. Nella pagina Imposta mappature dei campi, inserisci le seguenti informazioni:

a. Per Project, Issue, Comment, Attachment, Worklog: seleziona uno dei campi di origine dati predefiniti Amazon Kendra generati che desideri mappare all'indice.

b. Aggiungi campo: consente di aggiungere campi di origine dati personalizzati per creare un nome di campo indice a cui mappare e il tipo di dati del campo.

c. Seleziona Successivo.

9. Nella pagina Rivedi e crea, verifica che le informazioni inserite siano corrette, quindi seleziona Aggiungi origine dati. Puoi anche scegliere di modificare le tue informazioni da questa pagina. L'origine dati verrà visualizzata nella pagina Origini dati dopo che l'origine dati sarà stata aggiunta correttamente.

API

Per connettersi Amazon Kendra a Jira

È necessario specificare quanto segue utilizzando l'JiraConfiguration API:

- URL dell'origine dati: specifica l'URL del tuo account Jira. *Ad esempio, company.atlassian.net.*
- Secret Amazon Resource Name (ARN): fornisci l'Amazon Resource Name (ARN) di un Secrets Manager segreto che contiene le credenziali di autenticazione per il tuo account Jira. Il segreto è archiviato in una struttura JSON con le seguenti chiavi:

```
{
    "jiraId": "Jira user name or email",
    "jiraCredential": "Jira API token"
```

```
}
```

> **Note**
>
> Ti consigliamo di aggiornare o ruotare regolarmente le credenziali e il segreto. Fornisci solo il livello di accesso necessario per la tua sicurezza. Non è consigliabile riutilizzare credenziali e segreti tra diverse fonti di dati e nelle versioni 1.0 e 2.0 dei connettori (ove applicabile).

- IAM ruolo: specifica `RoleArn` quando chiami `CreateDataSource` per fornire a un IAM ruolo le autorizzazioni per accedere al tuo Secrets Manager segreto e per chiamare le API pubbliche richieste per il connettore Jira e. Amazon Kendra Per ulteriori informazioni, consulta i IAM ruoli per le sorgenti dati Jira.

Puoi anche aggiungere le seguenti funzionalità opzionali:

- Virtual Private Cloud (VPC): specifica `VpcConfiguration` come parte della configurazione dell'origine dati. Vedi Configurazione Amazon Kendra per l'uso di un VPC.
- Registro delle modifiche: indica se Amazon Kendra utilizzare il meccanismo del registro delle modifiche all'origine dati di Jira per determinare se un documento deve essere aggiornato nell'indice.

> **Note**
>
> Usa il registro delle modifiche se non desideri Amazon Kendra scansionare tutti i documenti. Se il registro delle modifiche è di grandi dimensioni, potrebbe essere necessario Amazon Kendra meno tempo per scansionare i documenti nell'origine dati Jira che per elaborare il registro delle modifiche. Se sincronizzi la fonte di dati Jira con l'indice per la prima volta, tutti i documenti vengono scansionati.

- Filtri di inclusione ed esclusione: puoi specificare se includere o escludere determinati file.

> **Note**
>
> La maggior parte delle fonti di dati utilizza modelli di espressioni regolari, che sono modelli di inclusione o esclusione denominati filtri. Se si specifica un filtro di inclusione, viene indicizzato solo il contenuto che corrisponde al filtro di inclusione. Qualsiasi

documento che non corrisponde al filtro di inclusione non viene indicizzato. Se si specifica un filtro di inclusione ed esclusione, i documenti che corrispondono al filtro di esclusione non vengono indicizzati, anche se corrispondono al filtro di inclusione.

- Commenti, allegati e registri di lavoro: è possibile specificare se eseguire la scansione di determinati commenti, allegati e registri di lavoro relativi a problemi.
- Progetti, problemi, stati: è possibile specificare se eseguire la scansione per indicizzazione di determinati ID di progetto, tipi di problemi e stati.
- Filtraggio del contesto utente e controllo degli accessi:Amazon Kendra esegue la scansione dell'elenco di controllo degli accessi (ACL) dei documenti, se disponi di un ACL per i documenti. Le informazioni ACL vengono utilizzate per filtrare i risultati della ricerca in base all'accesso dell'utente o del relativo gruppo ai documenti. Per ulteriori informazioni, consulta Filtraggio del contesto utente.
- Mappature dei campi: scegli di mappare i campi delle sorgenti dati di Jira ai campi indice. Amazon Kendra Per ulteriori informazioni, consulta la sezione Mappatura dei campi di origine dei dati.

> **Note**
>
> Il campo del corpo del documento o l'equivalente del corpo del documento per i documenti è necessario per Amazon Kendra eseguire la ricerca nei documenti. È necessario mappare il nome del campo del corpo del documento nella fonte dati al nome del campo indice_`document_body`. Tutti gli altri campi sono facoltativi.

Ulteriori informazioni

Per saperne di più sull'integrazione Amazon Kendra con la tua fonte di dati Jira, consulta:

- Cerca in modo intelligente i tuoi progetti Jira con Jira Cloud connector Amazon Kendra

Microsoft Exchange

Microsoft Exchange è uno strumento di collaborazione aziendale per la messaggistica, le riunioni e la condivisione di file. Se sei un utente di Microsoft Exchange, puoi utilizzarlo Amazon Kendra per indicizzare l'origine dati di Microsoft Exchange.

Puoi connetterti Amazon Kendra alla tua origine dati Microsoft Exchange utilizzando la Amazon Kendra console e l'TemplateConfigurationAPI.

Per la risoluzione dei problemi relativi al connettore di origine dati Amazon Kendra Microsoft Exchange, vedereRisoluzione dei problemi relativi alle origini dati.

Funzionalità supportate

- Mappature dei campi
- Filtraggio del contesto utente
- Filtri di inclusione/esclusione
- Sincronizzazione completa e incrementale dei contenuti
- Virtual Private Cloud (VPC) (Cloud privato virtuale (VPC)

Prerequisiti

Prima di poterla utilizzare Amazon Kendra per indicizzare l'origine dati di Microsoft Exchange, apporta queste modifiche a Microsoft Exchange e AWS agli account.

In Microsoft Exchange, assicurati di avere:

- Ha creato un account Microsoft Exchange in Office 365.
- Ha preso nota del tuo ID tenant di Microsoft 365. Puoi trovare il tuo ID tenant nelle proprietà del tuo portale di Azure Active Directory o nell'applicazione OAuth.
- Ha creato un'applicazione OAuth nel portale di Azure e ha annotato l'ID client e il segreto del client o le credenziali del client. Per ulteriori informazioni, consulta il tutorial Microsoft e l'esempio di app registrata.

> **Note**
>
> Quando crei o registri un'app nel portale di Azure, l'ID segreto rappresenta il valore segreto effettivo. È necessario prendere nota o salvare il valore segreto effettivo immediatamente durante la creazione del segreto e dell'app. Puoi accedere al tuo segreto selezionando il nome dell'applicazione nel portale di Azure e quindi accedendo all'opzione di menu relativa a certificati e segreti.

Puoi accedere al tuo ID cliente selezionando il nome dell'applicazione nel portale di Azure e quindi accedendo alla pagina di panoramica. L'ID dell'applicazione (client) è l'ID del client.

- Sono state aggiunte le seguenti autorizzazioni per l'applicazione del connettore:

Microsoft Graph	Office 365 Exchange Online
• Mail.Read (Applicazione) • Posta. ReadBasic (Applicazione) • Posta. ReadBasic.All (Applicazione) • Calendars.Read (Applicazione) • User.Read.All (Applicazione) • Contacts.Read (Applicazione) • Notes.Read.All (Applicazione) • Directory.Read.All (Applicazione) • NOTIZIE. AccessAsUser.Tutto (delegato)	full_access_as_app (Applicazione)

- Selezionato, ogni documento è unico in Microsoft Exchange e tra le altre fonti di dati che intendi utilizzare per lo stesso indice. Ogni fonte di dati che desideri utilizzare per un indice non deve contenere lo stesso documento in tutte le fonti di dati. Gli ID dei documenti sono globali rispetto a un indice e devono essere univoci per indice.

Nel tuo Account AWS, assicurati di avere:

- Ha creato un Amazon Kendra indice e, se si utilizza l'API, ha annotato l'ID dell'indice.
- Hai creato un IAM ruolo per la tua origine dati e, se utilizzi l'API, hai annotato l'ARN del IAM ruolo.

> **Note**
>
> Se modifichi il tipo di autenticazione e le credenziali, devi aggiornare il IAM ruolo per accedere all'ID AWS Secrets Manager segreto corretto.

- Ha archiviato le credenziali di autenticazione di Microsoft Exchange in un AWS Secrets Manager segreto e, se si utilizza l'API, ha annotato l'ARN del segreto.

> **Note**
>
> Ti consigliamo di aggiornare o ruotare regolarmente le credenziali e il segreto. Fornisci solo il livello di accesso necessario per la tua sicurezza. Non è consigliabile riutilizzare credenziali e segreti tra diverse fonti di dati e versioni dei connettori 1.0 e 2.0 (ove applicabile).

Se non disponi di un IAM ruolo o di un segreto esistente, puoi utilizzare la console per creare un nuovo IAM ruolo e Secrets Manager segreto quando connetti l'origine dati di Microsoft Exchange a Amazon Kendra. Se utilizzi l'API, devi fornire l'ARN di un IAM ruolo e di un Secrets Manager segreto esistenti e un ID di indice.

Istruzioni di connessione

Per connettersi Amazon Kendra all'origine dati Microsoft Exchange, è necessario fornire i dettagli necessari dell'origine dati Microsoft Exchange in modo che sia Amazon Kendra possibile accedere ai dati. Se non hai ancora configurato Microsoft Exchange per Amazon Kendra, vediPrerequisiti.

Console

Per connettersi Amazon Kendra a Microsoft Exchange

1. Accedi a AWS Management Console e apri la Amazon Kendra console.
2. Dal riquadro di navigazione a sinistra, scegli Indici, quindi scegli l'indice che desideri utilizzare dall'elenco degli indici.

   > **Note**
   >
   > Puoi scegliere di configurare o modificare le impostazioni del controllo dell'accesso degli utenti in Impostazioni dell'indice.

3. Nella pagina Guida introduttiva, scegli Aggiungi origine dati.
4. Nella pagina Aggiungi origine dati, scegli Connettore Microsoft Exchange, quindi scegli Aggiungi connettore.
5. Nella pagina Specificare i dettagli dell'origine dati, inserisci le seguenti informazioni:

a. In Nome e descrizione, per Nome dell'origine dati, inserisci un nome per l'origine dati. Puoi includere trattini ma non spazi.

b. (Facoltativo) Descrizione: immetti una descrizione facoltativa per l'origine dati.

c. In Lingua predefinita: scegli una lingua per filtrare i documenti per l'indice. Se non diversamente specificato, la lingua predefinita è l'inglese. La lingua specificata nei metadati del documento ha la precedenza sulla lingua selezionata.

d. In Tag, per Aggiungi nuovo tag, includi tag opzionali per cercare e filtrare le risorse o tenere traccia dei costi. AWS

e. Seleziona Successivo.

6. Nella pagina Definisci accesso e sicurezza, inserisci le seguenti informazioni:

a. Fonte: inserisci il tuo ID tenant di Microsoft 365. Puoi trovare il tuo ID tenant nelle proprietà del tuo portale di Azure Active Directory o nell'applicazione OAuth.

b. Autorizzazione: attiva o disattiva le informazioni dell'elenco di controllo degli accessi (ACL) per i tuoi documenti, se disponi di un ACL e desideri utilizzarlo per il controllo degli accessi. L'ACL specifica a quali documenti possono accedere utenti e gruppi. Le informazioni ACL vengono utilizzate per filtrare i risultati della ricerca in base all'accesso dell'utente o del relativo gruppo ai documenti. Per ulteriori informazioni, consulta Filtraggio del contesto utente.

c. AWS Secrets Manager segreto: scegli un segreto esistente o creane uno nuovo Secrets Manager per archiviare le credenziali di autenticazione di Microsoft Exchange. Se scegli di creare un nuovo segreto, si apre una finestra AWS Secrets Manager segreta.

   i. Inserisci le seguenti informazioni nella finestra Crea un AWS Secrets Manager segreto:

      A. Nome segreto: un nome per il tuo segreto. Il prefisso 'AmazonKendra-Microsoft Exchange

      B. Per ID cliente: immettere l'ID client.

      C. Per Client Secret: immetti i valori delle credenziali di autenticazione che hai creato nel tuo account Microsoft Exchange nel portale di Azure.

   ii. Selezionare Salva.

d. Virtual Private Cloud (VPC): puoi scegliere di utilizzare un VPC. In tal caso, è necessario aggiungere sottoreti e gruppi di sicurezza VPC.

e. IAM ruolo: scegli un IAM ruolo esistente o creane uno nuovo IAM per accedere alle credenziali del repository e indicizzare il contenuto.

> **Note**
>
> IAM i ruoli utilizzati per gli indici non possono essere utilizzati per le fonti di dati. Se non sei sicuro che un ruolo esistente venga utilizzato per un indice o una FAQ, scegli Crea un nuovo ruolo per evitare errori.

f. Seleziona Successivo.

7. Nella pagina Configura le impostazioni di sincronizzazione, inserisci le seguenti informazioni:

a. Sincronizza contenuti: seleziona i contenuti da sincronizzare.

b. Configurazione aggiuntiva: puoi facoltativamente indicizzare il seguente contenuto invece di sincronizzare tutti i documenti.

- Tipi di entità: scegli le entità che desideri sincronizzare. Puoi scegliere tra Calendario OneNotese Contatti.
- Scansione del calendario: inserisci la data di inizio e di fine per la sincronizzazione del calendario.
- Includi e-mail: inserisci l'e-mail da e l'e-mail ai domini e le eventuali righe dell'oggetto che desideri includere o escludere nell'indice.
- Regex per domini: aggiungi modelli per includere ed escludere determinati domini di posta elettronica dal tuo indice.
- Modelli Regex: aggiungi modelli di espressioni regolari per includere o escludere determinati file. Puoi aggiungere fino a 100 pattern.

c. Modalità di sincronizzazione: scegli come aggiornare l'indice quando il contenuto dell'origine dati cambia. Quando sincronizzi l'origine dati con Amazon Kendra per la prima volta, tutto il contenuto viene sottoposto a scansione e indicizzato per impostazione predefinita. Se la sincronizzazione iniziale non è riuscita, devi eseguire una sincronizzazione completa dei dati, anche se non scegli la sincronizzazione completa come opzione della modalità di sincronizzazione.

- Sincronizzazione completa: indicizza di nuovo tutti i contenuti, sostituendo i contenuti esistenti ogni volta che l'origine dati si sincronizza con l'indice.

- Nuova sincronizzazione modificata: indicizza solo i contenuti nuovi e modificati ogni volta che l'origine dati si sincronizza con l'indice. Amazon Kendra può utilizzare il meccanismo dell'origine dati per tenere traccia delle modifiche ai contenuti e indicizzare i contenuti modificati dall'ultima sincronizzazione.
- Sincronizzazione nuova, modificata ed eliminata: indicizza solo i contenuti nuovi, modificati ed eliminati ogni volta che l'origine dati si sincronizza con l'indice. Amazon Kendra può utilizzare il meccanismo dell'origine dati per tenere traccia delle modifiche ai contenuti e indicizzare i contenuti modificati dall'ultima sincronizzazione.

8. Nella pagina Imposta mappature dei campi, inserisci le seguenti informazioni:

   a. Campi di origine dati predefiniti: seleziona uno dei campi di origine dati predefiniti Amazon Kendra generati che desideri mappare all'indice.

   > **Note**
   >
   > Il connettore di origine dati di Amazon Kendra Microsoft Exchange non supporta mappature di campi personalizzate.

   b. Seleziona Successivo.

9. Nella pagina Rivedi e crea, verifica che le informazioni inserite siano corrette, quindi seleziona Aggiungi origine dati. Puoi anche scegliere di modificare le tue informazioni da questa pagina. L'origine dati verrà visualizzata nella pagina Origini dati dopo che l'origine dati sarà stata aggiunta correttamente.

API

Per connettersi Amazon Kendra a Microsoft Exchange

È necessario specificare un codice JSON dello schema dell'origine dati utilizzando l'TemplateConfigurationAPI. È necessario fornire le seguenti informazioni:

- Origine dati: specifica il tipo di origine dati come `MSEXCHANGE` quando usi lo schema TemplateConfigurationJSON. Specificate anche l'origine dati come `TEMPLATE` quando chiamate l'CreateDataSourceAPI.
- ID tenant: puoi trovare il tuo ID tenant nelle proprietà del tuo portale di Azure Active Directory o nell'applicazione OAuth.

- Modalità di sincronizzazione: specifica come Amazon Kendra aggiornare l'indice quando il contenuto dell'origine dati cambia. Quando sincronizzi l'origine dati con Amazon Kendra per la prima volta, tutto il contenuto viene sottoposto a scansione e indicizzato per impostazione predefinita. Se la sincronizzazione iniziale non è riuscita, devi eseguire una sincronizzazione completa dei dati, anche se non scegli la sincronizzazione completa come opzione della modalità di sincronizzazione. Puoi scegliere tra:
  - `FORCED_FULL_CRAWL`per indicizzare nuovamente tutti i contenuti, sostituendo i contenuti esistenti ogni volta che l'origine dati si sincronizza con l'indice.
  - `FULL_CRAWL`per indicizzare solo i contenuti nuovi, modificati ed eliminati ogni volta che l'origine dati si sincronizza con l'indice. Amazon Kendra può utilizzare il meccanismo dell'origine dati per tenere traccia delle modifiche ai contenuti e indicizzare i contenuti modificati dall'ultima sincronizzazione.
  - `CHANGE_LOG`per indicizzare solo contenuti nuovi e modificati ogni volta che l'origine dati si sincronizza con l'indice. Amazon Kendra può utilizzare il meccanismo dell'origine dati per tenere traccia delle modifiche ai contenuti e indicizzare i contenuti modificati dall'ultima sincronizzazione.
- Secret Amazon Resource Name (ARN): fornisci l'Amazon Resource Name (ARN) di un Secrets Manager segreto che contiene le credenziali di autenticazione per il tuo account Microsoft Exchange. Il segreto è archiviato in una struttura JSON con le seguenti chiavi:

```
{
    "clientId": "client ID",
    "clientSecret": "client secret"
}
```

> **Note**
>
> Ti consigliamo di aggiornare o ruotare regolarmente le credenziali e il segreto. Fornisci solo il livello di accesso necessario per la tua sicurezza. Non è consigliabile riutilizzare credenziali e segreti tra diverse fonti di dati e versioni dei connettori 1.0 e 2.0 (ove applicabile).

- IAM ruolo: specifica `RoleArn` quando chiami `CreateDataSource` per fornire a un IAM ruolo le autorizzazioni per accedere al tuo Secrets Manager segreto e per chiamare le API pubbliche richieste per il connettore Microsoft Exchange e. Amazon Kendra Per ulteriori informazioni, consulta IAM i ruoli per le origini dati di Microsoft Exchange.

Puoi anche aggiungere le seguenti funzionalità opzionali:

- Virtual Private Cloud (VPC): `VpcConfiguration` specifica quando si chiama. `CreateDataSource` Per ulteriori informazioni, consulta Configurazione Amazon Kendra per l'utilizzo di un Amazon VPC.
- Filtri di inclusione ed esclusione: specificate se includere o escludere determinate pagine e risorse.

> **Note**
>
> La maggior parte delle fonti di dati utilizza modelli di espressioni regolari, che sono modelli di inclusione o esclusione denominati filtri. Se si specifica un filtro di inclusione, viene indicizzato solo il contenuto che corrisponde al filtro di inclusione. Qualsiasi documento che non corrisponde al filtro di inclusione non viene indicizzato. Se si specifica un filtro di inclusione ed esclusione, i documenti che corrispondono al filtro di esclusione non vengono indicizzati, anche se corrispondono al filtro di inclusione.

- Filtro del contesto utente e controllo degli accessi:Amazon Kendra esegue la ricerca per indicizzazione dell'elenco di controllo degli accessi (ACL) dei documenti, se disponi di un ACL per i documenti. Le informazioni ACL vengono utilizzate per filtrare i risultati della ricerca in base all'accesso dell'utente o del relativo gruppo ai documenti. Per ulteriori informazioni, consulta Filtraggio del contesto utente.
- Mappature dei campi: scegliere di mappare i campi dell'origine dati di Microsoft Exchange ai Amazon Kendra campi indice. Per ulteriori informazioni, consulta la sezione Mappatura dei campi di origine dei dati.

> **Note**
>
> Il campo del corpo del documento o l'equivalente del corpo del documento per i documenti è necessario per Amazon Kendra eseguire la ricerca nei documenti. È necessario mappare il nome del campo del corpo del documento nella fonte dati al nome del campo indice`_document_body`. Tutti gli altri campi sono facoltativi.

Ulteriori informazioni

Per ulteriori informazioni sull'integrazione Amazon Kendra con l'origine dati Microsoft Exchange, consulta:

- Indicizza i tuoi contenuti di Microsoft Exchange utilizzando il connettore Exchange per Amazon Kendra

Microsoft OneDrive

Microsoft OneDrive è un servizio di archiviazione basato sul cloud che puoi utilizzare per archiviare, condividere e ospitare i tuoi contenuti. Puoi usarlo Amazon Kendra per indicizzare la tua fonte di OneDrive dati.

Puoi connetterti Amazon Kendra alla tua fonte di OneDrive dati utilizzando la Amazon Kendra console e l'OneDriveConfigurationAPI.

Amazon Kendra dispone di due versioni del OneDrive connettore. Le funzionalità supportate di ogni versione includono:

OneDrive Connettore Microsoft V1.0/API OneDriveConfiguration

- Mappature dei campi
- Filtri di inclusione/esclusione

OneDrive Connettore Microsoft V2.0/API TemplateConfiguration

- Filtraggio del contesto utente
- Crawler di identità utente
- Filtri di inclusione/esclusione
- Sincronizzazione completa e incrementale dei contenuti
- Virtual Private Cloud (VPC) (Cloud privato virtuale (VPC)

> **Note**
>
> Il supporto per il OneDrive connettore OneDriveConfiguration V1.0/API dovrebbe terminare entro giugno 2023. Si consiglia di utilizzare il OneDrive connettore TemplateConfiguration V2.0/API.

Per la risoluzione dei problemi relativi al connettore di origine Amazon Kendra OneDrive dati, consultaRisoluzione dei problemi relativi alle origini dati.

Argomenti

- OneDrive Connettore Microsoft V1.0
- OneDrive Connettore Microsoft V2.0
- Ulteriori informazioni

OneDrive Connettore Microsoft V1.0

Microsoft OneDrive è un servizio di archiviazione basato sul cloud che puoi utilizzare per archiviare, condividere e ospitare i tuoi contenuti. È possibile utilizzare Amazon Kendra per indicizzare l'origine OneDrive dati Microsoft.

> **Note**
>
> Il supporto per il OneDrive connettore V1.0/Microsft OneDrive API dovrebbe terminare entro giugno 2023. Si consiglia di utilizzare il OneDrive connettore V2.0/API. TemplateConfiguration

Per la risoluzione dei problemi relativi al connettore di origine Amazon Kendra OneDrive dati, consultaRisoluzione dei problemi relativi alle origini dati.

Argomenti

- Funzionalità supportate
- Prerequisiti
- Istruzioni di connessione

Funzionalità supportate

- Mappature dei campi
- Filtri di inclusione/esclusione

Prerequisiti

Prima di utilizzarla Amazon Kendra per indicizzare la tua fonte di OneDrive dati, apporta queste modifiche al tuo account e ai tuoi account. OneDrive AWS

In Azure Active Directory (AD), assicurati di avere:

- Hai creato un'applicazione Azure Active Directory (AD).
- Ha usato l'ID dell'applicazione AD per registrare una chiave segreta per l'applicazione sul sito AD. La chiave segreta deve contenere l'ID dell'applicazione e una chiave segreta.
- Ha copiato il dominio AD dell'organizzazione.
- Sono state aggiunte le seguenti autorizzazioni all'applicazione AD nell'opzione Microsoft Graph:
  - Leggi i file in tutte le raccolte di siti (File.Read.All)
  - Leggi il profilo completo di tutti gli utenti (User.Read.All)
  - Leggi i dati della directory (Directory.Read.All)
  - Leggi tutti i gruppi (Group.Read.All)
  - Leggi gli elementi in tutte le raccolte del sito (Site.Read.All)
- È stato copiato l'elenco degli utenti i cui documenti devono essere indicizzati. È possibile scegliere di fornire un elenco di nomi utente oppure fornire i nomi utente in un file archiviato in un file. Amazon S3 Dopo aver creato l'origine dati, puoi:
  - Modificare l'elenco degli utenti.
  - Passa da un elenco di utenti a un elenco memorizzato in un Amazon S3 bucket.
  - Modifica la posizione del Amazon S3 bucket di un elenco di utenti. Se modifichi la posizione del bucket, devi anche aggiornare il IAM ruolo dell'origine dati in modo che abbia accesso al bucket.

> **Note**
>
> Se memorizzi l'elenco dei nomi utente in un Amazon S3 bucket, la IAM politica per l'origine dati deve fornire l'accesso al bucket e l'accesso alla chiave con cui il bucket è stato crittografato, se presente.

- Selezionato, ogni documento è unico nelle OneDrive altre fonti di dati che intendi utilizzare per lo stesso indice. Ogni fonte di dati che desideri utilizzare per un indice non deve contenere lo stesso documento in tutte le fonti di dati. Gli ID dei documenti sono globali rispetto a un indice e devono essere univoci per indice.

Nel tuo Account AWS, assicurati di avere:

- Ha creato un Amazon Kendra indice e, se si utilizza l'API, ha annotato l'ID dell'indice.
- Hai creato un IAM ruolo per la tua origine dati e, se utilizzi l'API, hai annotato l'ARN del IAM ruolo.

> **Note**
>
> Se modifichi il tipo di autenticazione e le credenziali, devi aggiornare il IAM ruolo per accedere all'ID AWS Secrets Manager segreto corretto.

- Ha archiviato le credenziali di OneDrive autenticazione in un AWS Secrets Manager segreto e, se si utilizza l'API, ha annotato l'ARN del segreto.

> **Note**
>
> Ti consigliamo di aggiornare o ruotare regolarmente le credenziali e il segreto. Fornisci solo il livello di accesso necessario per la tua sicurezza. Non è consigliabile riutilizzare credenziali e segreti tra diverse fonti di dati e nelle versioni 1.0 e 2.0 dei connettori (ove applicabile).

Se non disponi di un IAM ruolo o di un segreto esistente, puoi utilizzare la console per creare un nuovo IAM ruolo e un Secrets Manager segreto quando connetti la tua origine OneDrive dati a. Amazon Kendra Se utilizzi l'API, devi fornire l'ARN di un IAM ruolo e di un Secrets Manager segreto esistenti e un ID di indice.

Istruzioni di connessione

Per connetterti Amazon Kendra alla tua fonte di OneDrive dati devi fornire i dettagli delle tue OneDrive credenziali in modo da Amazon Kendra poter accedere ai tuoi dati. Se non lo hai ancora configurato, OneDrive Amazon Kendra Prerequisiti consulta.

Console

Per connettersi Amazon Kendra a OneDrive

1. Accedi a AWS Management Console e apri la Amazon Kendra console.
2. Dal riquadro di navigazione a sinistra, scegli Indici, quindi scegli l'indice che desideri utilizzare dall'elenco degli indici.

   > **Note**
   >
   > Puoi scegliere di configurare o modificare le impostazioni del controllo dell'accesso degli utenti in Impostazioni dell'indice.

3. Nella pagina Guida introduttiva, scegli Aggiungi origine dati.
4. Nella pagina Aggiungi origine dati, scegli OneDrive connettore, quindi scegli Aggiungi connettore.
5. Nella pagina Specificare i dettagli dell'origine dati, inserisci le seguenti informazioni:

   a. In Nome e descrizione, per Nome dell'origine dati, inserisci un nome per l'origine dati. Puoi includere trattini ma non spazi.
   b. (Facoltativo) Descrizione: immetti una descrizione facoltativa per l'origine dati.
   c. In Lingua predefinita: scegli una lingua per filtrare i documenti per l'indice. Se non diversamente specificato, la lingua predefinita è l'inglese. La lingua specificata nei metadati del documento ha la precedenza sulla lingua selezionata.
   d. In Tag, per Aggiungi nuovo tag, includi tag opzionali per cercare e filtrare le risorse o tenere traccia dei costi. AWS
   e. Seleziona Successivo.

6. Nella pagina Definisci accesso e sicurezza, inserisci le seguenti informazioni:

   a. OneDrive ID tenant: inserire l'ID OneDrive tenant senza il protocollo.
   b. Tipo di autenticazione : scegli tra Nuova ed Esistente.
   c. i. Se scegli Esistente, seleziona un segreto esistente per Seleziona segreto.
      ii. Se scegli Nuovo, inserisci le seguenti informazioni nella sezione Nuovo AWS Secrets Manager segreto:

         A. Nome segreto: un nome per il tuo segreto. Il prefisso 'AmazonKendra- OneDrive -' viene aggiunto automaticamente al nome segreto.

B. Per l'ID dell'applicazione e la password dell'applicazione, inserisci i valori delle credenziali di autenticazione dal tuo OneDrive account, quindi scegli Salva autenticazione.

d. IAM ruolo: scegli un ruolo esistente o crea un nuovo IAM IAM ruolo per accedere alle credenziali del repository e indicizzare il contenuto.

> **Note**
>
> IAM i ruoli utilizzati per gli indici non possono essere utilizzati per le fonti di dati. Se non sei sicuro che un ruolo esistente venga utilizzato per un indice o una FAQ, scegli Crea un nuovo ruolo per evitare errori.

e. Seleziona Successivo.

7. Nella pagina Configura le impostazioni di sincronizzazione, inserisci le seguenti informazioni:

a. Scegli tra List file e Names list in base al tuo caso d'uso.

i. Se scegli List file, inserisci le seguenti informazioni:

- Seleziona posizione: inserisci il percorso del tuo Amazon S3 bucket.

  Aggiungi il file dell'elenco degli utenti a Amazon S3: seleziona per aggiungere i file dell'elenco degli utenti al tuo bucket. Amazon S3

  Mappature dei gruppi locali degli utenti: seleziona questa opzione per utilizzare la mappatura dei gruppi locali per filtrare i contenuti.

ii. Se scegli Elenco nomi, inserisci le seguenti informazioni:

- Nome utente: immettere fino a 10 unità utente da indicizzare. Per aggiungere più di 10 utenti, crea un file che contenga i nomi.

  Aggiungi un altro: scegli di aggiungere altri utenti.

  Mappature dei gruppi locali degli utenti: seleziona questa opzione per utilizzare la mappatura dei gruppi locali per filtrare i contenuti.

b. Per configurazioni aggiuntive: aggiungi modelli di espressioni regolari per includere o escludere determinati file. È possibile aggiungere fino a 100 pattern.

c. In Pianificazione di esecuzione della sincronizzazione, per Frequenza: scegli la frequenza di sincronizzazione con la tua fonte di dati. Amazon Kendra

d. Seleziona Successivo.

8. Nella pagina Imposta le mappature dei campi, inserisci le seguenti informazioni:

a. Per i campi delle origini dati predefiniti e le mappature di campo aggiuntive suggerite, seleziona uno dei campi di origine dati predefiniti Amazon Kendra generati che desideri mappare all'indice.

b. Seleziona Successivo.

9. Nella pagina Rivedi e crea, verifica che le informazioni inserite siano corrette, quindi seleziona Aggiungi origine dati. Puoi anche scegliere di modificare le tue informazioni da questa pagina. L'origine dati verrà visualizzata nella pagina Origini dati dopo che l'origine dati sarà stata aggiunta correttamente.

API

Per connettersi Amazon Kendra a OneDrive

È necessario specificare quanto segue utilizzando l'OneDriveConfigurationAPI:

- ID tenant: specifica il dominio Azure Active Directory dell'organizzazione.
- OneDrive Utenti: specifica l'elenco degli account utente i cui documenti devono essere indicizzati.
- Secret Amazon Resource Name (ARN): fornisci l'Amazon Resource Name (ARN) di un Secrets Manager segreto che contiene le credenziali di autenticazione per il tuo account. OneDrive Il segreto è archiviato in una struttura JSON con le seguenti chiavi:

```
{
    "username": "OAuth client ID",
    "password": "client secret"
}
```

> **Note**
>
> Ti consigliamo di aggiornare o ruotare regolarmente le credenziali e il segreto. Fornisci solo il livello di accesso necessario per la tua sicurezza. Non è consigliabile riutilizzare

credenziali e segreti tra diverse fonti di dati e nelle versioni 1.0 e 2.0 dei connettori (ove applicabile).

- IAM ruolo: specifica `RoleArn` quando chiami `CreateDataSource` per fornire a un IAM ruolo le autorizzazioni per accedere al tuo Secrets Manager segreto e per chiamare le API pubbliche richieste per il connettore e. OneDrive Amazon Kendra Per ulteriori informazioni, consulta i IAM ruoli per OneDrive le fonti di dati.

Puoi anche aggiungere le seguenti funzionalità opzionali:

- Filtri di inclusione ed esclusione: specifica se includere o escludere determinati documenti.

> **Note**
>
> La maggior parte delle fonti di dati utilizza modelli di espressioni regolari, che sono modelli di inclusione o esclusione denominati filtri. Se si specifica un filtro di inclusione, viene indicizzato solo il contenuto che corrisponde al filtro di inclusione. Qualsiasi documento che non corrisponde al filtro di inclusione non viene indicizzato. Se si specifica un filtro di inclusione ed esclusione, i documenti che corrispondono al filtro di esclusione non vengono indicizzati, anche se corrispondono al filtro di inclusione.

- Mappature dei campi: scegli di mappare i campi delle sorgenti OneDrive dati ai campi indice. Amazon Kendra Per ulteriori informazioni, consulta la sezione Mappatura dei campi di origine dei dati.

> **Note**
>
> Il campo del corpo del documento o l'equivalente del corpo del documento per i documenti è necessario per Amazon Kendra eseguire la ricerca nei documenti. È necessario mappare il nome del campo del corpo del documento nella fonte dati al nome del campo indice`_document_body`. Tutti gli altri campi sono facoltativi.

- Filtraggio del contesto utente e controllo degli accessi:Amazon Kendra esegue la scansione dell'elenco di controllo degli accessi (ACL) dei documenti, se disponi di un ACL per i documenti. Le informazioni ACL vengono utilizzate per filtrare i risultati della ricerca in base all'accesso dell'utente o del relativo gruppo ai documenti. Per ulteriori informazioni, consulta Filtraggio del contesto utente.

OneDrive Connettore Microsoft V2.0

Microsoft OneDrive è un servizio di archiviazione basato sul cloud che puoi utilizzare per archiviare, condividere e ospitare i tuoi contenuti. Puoi usarlo Amazon Kendra per indicizzare la tua fonte di OneDrive dati.

Puoi connetterti Amazon Kendra alla tua fonte di OneDrive dati utilizzando la Amazon Kendra console e l'OneDriveConfigurationAPI.

> **Note**
>
> La fine del supporto per OneDrive Connector OneDriveConfiguration V1.0/API è prevista entro giugno 2023. Ti consigliamo di utilizzare OneDrive Connector TemplateConfiguration V2.0/API. La versione 2.0 offre ACL aggiuntivi e funzionalità di identity crawler.

Per la risoluzione dei problemi relativi al connettore di origine Amazon Kendra OneDrive dati, consulta. Risoluzione dei problemi relativi alle origini dati

Argomenti

- Funzionalità supportate
- Prerequisiti
- Istruzioni di connessione

Funzionalità supportate

Amazon Kendra OneDrive il connettore di origine dati supporta le seguenti funzionalità:

- mappature dei campi
- Filtraggio del contesto utente
- Crawler di identità utente
- Filtri di inclusione/esclusione
- Sincronizzazione completa e incrementale dei contenuti
- Virtual Private Cloud (VPC) (Cloud privato virtuale (VPC)

Prerequisiti

Prima di poterla utilizzare Amazon Kendra per indicizzare la tua fonte di OneDrive dati, apporta queste modifiche al tuo account OneDrive e AWS ai tuoi account.

Nel OneDrive, assicurati di avere:

- Hai creato un OneDrive account in Office 365.
- Ha preso nota del tuo ID tenant di Microsoft 365. Puoi trovare il tuo ID tenant nelle proprietà del tuo portale di Azure Active Directory o nell'applicazione OAuth.
- Ha creato un'applicazione OAuth nel portale di Azure e ha annotato l'ID client e il segreto del client o le credenziali del client. Per ulteriori informazioni, consulta il tutorial Microsoft e l'esempio di app registrata.

  > **Note**
  >
  > Quando crei o registri un'app nel portale di Azure, l'ID segreto rappresenta il valore segreto effettivo. È necessario prendere nota o salvare il valore segreto effettivo immediatamente durante la creazione del segreto e dell'app. Puoi accedere al tuo segreto selezionando il nome dell'applicazione nel portale di Azure e quindi accedendo all'opzione di menu relativa a certificati e segreti.
  > Puoi accedere al tuo ID cliente selezionando il nome dell'applicazione nel portale di Azure e quindi accedendo alla pagina di panoramica. L'ID dell'applicazione (client) è l'ID del client.

- Ha utilizzato l'ID dell'applicazione AD per registrare una chiave segreta per l'applicazione sul sito AD. La chiave segreta deve contenere l'ID dell'applicazione e una chiave segreta.
- Ha copiato il dominio AD dell'organizzazione.
- Sono state aggiunte le seguenti autorizzazioni all'applicazione AD nell'opzione Microsoft Graph:
  - Leggi i file in tutte le raccolte di siti (File.Read.All)
  - Leggi i profili completi di tutti gli utenti (User.Read.All)
  - Leggi tutti i gruppi (Group.Read.All)
  - Leggi tutte le note (Notes.Read.All)
- È stato copiato l'elenco degli utenti i cui documenti devono essere indicizzati. È possibile scegliere di fornire un elenco di nomi utente oppure fornire i nomi utente in un file archiviato in un file. Amazon S3 Dopo aver creato l'origine dati, puoi:

- Modificare l'elenco degli utenti.
- Passa da un elenco di utenti a un elenco memorizzato in un Amazon S3 bucket.
- Modifica la posizione del Amazon S3 bucket di un elenco di utenti. Se modifichi la posizione del bucket, devi anche aggiornare il IAM ruolo dell'origine dati in modo che abbia accesso al bucket.

> **Note**
>
> Se memorizzi l'elenco dei nomi utente in un Amazon S3 bucket, la IAM politica per l'origine dati deve fornire l'accesso al bucket e l'accesso alla chiave con cui il bucket è stato crittografato, se presente.
> Il OneDrive connettore utilizza l'e-mail proveniente dalle informazioni di contatto presenti nelle proprietà utente di Onedrive. Assicurati che l'utente di cui desideri sottoporre a scansione i dati abbia il campo e-mail configurato nella pagina Informazioni di contatto, poiché per i nuovi utenti potrebbe essere vuoto.

Nel tuo AWS account, assicurati di avere:

- Ha creato un Amazon Kendra indice e, se si utilizza l'API, ha annotato l'ID dell'indice.
- Hai creato un IAM ruolo per la tua origine dati e, se utilizzi l'API, hai annotato l'ARN del IAM ruolo.
- Ha archiviato le credenziali di OneDrive autenticazione in un AWS Secrets Manager segreto e, se si utilizza l'API, ha annotato l'ARN del segreto.

Se non disponi di un IAM ruolo o di un segreto esistente, puoi utilizzare la console per creare un nuovo IAM ruolo e un Secrets Manager segreto quando connetti la tua fonte di OneDrive dati a. Amazon Kendra Se si utilizza l'API, è necessario fornire l'ARN di un IAM ruolo e di un Secrets Manager segreto esistenti e un ID di indice.

Istruzioni di connessione

Per connetterti Amazon Kendra alla tua fonte di OneDrive dati devi fornire i dettagli delle tue OneDrive credenziali in modo da Amazon Kendra poter accedere ai tuoi dati. Se non hai ancora configurato OneDrive per Amazon Kendra, consultaPrerequisiti.

Console

Per connettersi Amazon Kendra a OneDrive

1. Accedi a AWS Management Console e apri la Amazon Kendra console.
2. Dal riquadro di navigazione a sinistra, scegli Indici, quindi scegli l'indice che desideri utilizzare dall'elenco degli indici.

> **Note**
>
> Puoi scegliere di configurare o modificare le impostazioni del controllo dell'accesso degli utenti in Impostazioni dell'indice.

3. Nella pagina Guida introduttiva, scegli Aggiungi origine dati.
4. Nella pagina Aggiungi origine dati, scegli OneDrive connettore, quindi scegli Aggiungi connettore.
5. Nella pagina Specificare i dettagli dell'origine dati, inserisci le seguenti informazioni:
   a. In Nome e descrizione, per Nome dell'origine dati, inserisci un nome per l'origine dati. Puoi includere trattini ma non spazi.
   b. (Facoltativo) Descrizione: immetti una descrizione facoltativa per l'origine dati.
   c. In Lingua predefinita: scegli una lingua per filtrare i documenti per l'indice. Se non diversamente specificato, la lingua predefinita è l'inglese. La lingua specificata nei metadati del documento ha la precedenza sulla lingua selezionata.
   d. In Tag, per Aggiungi nuovo tag, includi tag opzionali per cercare e filtrare le risorse o tenere traccia dei costi. AWS
   e. Seleziona Successivo.
6. Nella pagina Definisci accesso e sicurezza, inserisci le seguenti informazioni:
   a. OneDrive ID tenant: inserire l'ID OneDrive tenant senza il protocollo.
   b. Autorizzazione: attiva o disattiva le informazioni dell'elenco di controllo degli accessi (ACL) per i documenti, se disponi di un ACL e desideri utilizzarlo per il controllo degli accessi. L'ACL specifica a quali documenti possono accedere utenti e gruppi. Le informazioni ACL vengono utilizzate per filtrare i risultati della ricerca in base all'accesso dell'utente o del relativo gruppo ai documenti. Per ulteriori informazioni, consulta Filtraggio del contesto utente.
   c. In Autenticazione: scegli tra Nuovo ed Esistente.
   d. i. Se scegli Esistente, seleziona un segreto esistente per Seleziona segreto.

ii. Se scegli Nuovo, inserisci le seguenti informazioni nella sezione Nuovo AWS Secrets Manager segreto:

A. Nome segreto: un nome per il tuo segreto. Il prefisso 'AmazonKendra- OneDrive -' viene aggiunto automaticamente al nome segreto.

B. Per Client ID e Client Secret: inserisci l'ID client e il segreto del client, quindi seleziona Salva autenticazione.

e. In Configura VPC e gruppo di sicurezza, opzionale, per Virtual Private Cloud (VPC), puoi scegliere di utilizzare un VPC. In tal caso, è necessario aggiungere sottoreti e gruppi di sicurezza VPC.

f. Identity crawler: specifica se attivare il crawler di identità. Amazon Kendra Il crawler di identità utilizza le informazioni dell'elenco di controllo degli accessi (ACL) per i documenti per filtrare i risultati della ricerca in base all'accesso dell'utente o del gruppo di appartenenza ai documenti. Se disponi di un ACL per i tuoi documenti e scegli di utilizzarlo, puoi anche scegliere di attivare il crawler di identità per configurare il filtraggio Amazon Kendra del contesto utente dei risultati di ricerca. Altrimenti, se il crawler di identità è disattivato, tutti i documenti possono essere ricercati pubblicamente. Se desideri utilizzare il controllo degli accessi per i tuoi documenti e il crawler di identità è disattivato, in alternativa puoi utilizzare l'PutPrincipalMappingAPI per caricare le informazioni di accesso di utenti e gruppi per il filtraggio del contesto degli utenti.

g. IAM ruolo: scegli un IAM ruolo esistente o creane uno nuovo IAM per accedere alle credenziali del repository e indicizzare il contenuto.

> **Note**
>
> IAM i ruoli utilizzati per gli indici non possono essere utilizzati per le fonti di dati. Se non sei sicuro che un ruolo esistente venga utilizzato per un indice o una FAQ, scegli Crea un nuovo ruolo per evitare errori.

h. Seleziona Successivo.

7. Nella pagina Configura le impostazioni di sincronizzazione, inserisci le seguenti informazioni:

8. a. Per l'ambito di sincronizzazione: scegli i OneDrive dati degli utenti da indicizzare. Puoi aggiungere un massimo di 10 utenti manualmente.

b. Per configurazioni aggiuntive: aggiungi modelli di espressioni regolari per includere o escludere determinati contenuti. È possibile aggiungere fino a 100 pattern.

c. Modalità di sincronizzazione: scegli come aggiornare l'indice quando il contenuto dell'origine dati cambia. Quando sincronizzi l'origine dati con Amazon Kendra per la prima volta, tutto il contenuto viene sottoposto a scansione e indicizzato per impostazione predefinita. Se la sincronizzazione iniziale non è riuscita, devi eseguire una sincronizzazione completa dei dati, anche se non scegli la sincronizzazione completa come opzione della modalità di sincronizzazione.

   - Sincronizzazione completa: indicizza di nuovo tutti i contenuti, sostituendo i contenuti esistenti ogni volta che l'origine dati si sincronizza con l'indice.
   - Nuova sincronizzazione modificata: indicizza solo i contenuti nuovi e modificati ogni volta che l'origine dati si sincronizza con l'indice. Amazon Kendra può utilizzare il meccanismo dell'origine dati per tenere traccia delle modifiche ai contenuti e indicizzare i contenuti modificati dall'ultima sincronizzazione.
   - Sincronizzazione nuova, modificata ed eliminata: indicizza solo i contenuti nuovi, modificati ed eliminati ogni volta che l'origine dati si sincronizza con l'indice. Amazon Kendra può utilizzare il meccanismo dell'origine dati per tenere traccia delle modifiche ai contenuti e indicizzare i contenuti modificati dall'ultima sincronizzazione.

d. Nella pianificazione di esecuzione della sincronizzazione, per Frequenza: scegli la frequenza con cui eseguire Amazon Kendra la sincronizzazione con la tua fonte di dati.

e. Seleziona Successivo.

9. Nella pagina Imposta le mappature dei campi, inserisci le seguenti informazioni:

   a. Per i campi delle origini dati predefiniti e le mappature di campo aggiuntive suggerite, seleziona uno dei campi di origine dati predefiniti Amazon Kendra generati che desideri mappare all'indice.

   b. Seleziona Successivo.

10. Nella pagina Rivedi e crea, verifica che le informazioni inserite siano corrette, quindi seleziona Aggiungi origine dati. Puoi anche scegliere di modificare le tue informazioni da questa pagina. L'origine dati verrà visualizzata nella pagina Origini dati dopo che l'origine dati sarà stata aggiunta correttamente.

API

Per connettersi Amazon Kendra a OneDrive

È necessario specificare un codice JSON dello schema dell'origine dati utilizzando l'TemplateConfigurationAPI. È necessario fornire le seguenti informazioni:

- Origine dati: specifica il tipo di origine dati come `ONEDRIVEV2` quando usi lo schema TemplateConfigurationJSON. Specificate anche l'origine dati come `TEMPLATE` quando chiamate l'CreateDataSourceAPI.
- ID tenant: specifica l'ID tenant di Microsoft 365. Puoi trovare il tuo ID tenant nelle proprietà del tuo portale di Azure Active Directory o nell'applicazione OAuth.
- Modalità di sincronizzazione: specifica come Amazon Kendra aggiornare l'indice quando il contenuto dell'origine dati cambia. Quando sincronizzi l'origine dati con Amazon Kendra per la prima volta, tutto il contenuto viene sottoposto a scansione e indicizzato per impostazione predefinita. Se la sincronizzazione iniziale non è riuscita, devi eseguire una sincronizzazione completa dei dati, anche se non scegli la sincronizzazione completa come opzione della modalità di sincronizzazione. Puoi scegliere tra:
  - `FORCED_FULL_CRAWL`per indicizzare nuovamente tutti i contenuti, sostituendo i contenuti esistenti ogni volta che l'origine dati si sincronizza con l'indice.
  - `FULL_CRAWL`per indicizzare solo i contenuti nuovi, modificati ed eliminati ogni volta che l'origine dati si sincronizza con l'indice. Amazon Kendra può utilizzare il meccanismo dell'origine dati per tenere traccia delle modifiche ai contenuti e indicizzare i contenuti modificati dall'ultima sincronizzazione.
  - `CHANGE_LOG`per indicizzare solo contenuti nuovi e modificati ogni volta che l'origine dati si sincronizza con l'indice. Amazon Kendra può utilizzare il meccanismo dell'origine dati per tenere traccia delle modifiche ai contenuti e indicizzare i contenuti modificati dall'ultima sincronizzazione.
- Secret Amazon Resource Name (ARN): fornisci l'Amazon Resource Name (ARN) di un Secrets Manager segreto che contiene le credenziali di autenticazione che hai creato nel tuo account. OneDrive

  Se utilizzi l'autenticazione OAuth 2.0, il segreto viene archiviato in una struttura JSON con le seguenti chiavi:

```
{
    "clientId": "client ID",
    "clientSecret": "client secret"
}
```

> **Note**
>
> Ti consigliamo di aggiornare o ruotare regolarmente le credenziali e il segreto. Fornisci solo il livello di accesso necessario per la tua sicurezza. Non è consigliabile riutilizzare credenziali e segreti tra diverse fonti di dati e nelle versioni 1.0 e 2.0 dei connettori (ove applicabile).

- IAM ruolo: specifica `RoleArn` quando chiami `CreateDataSource` per fornire a un IAM ruolo le autorizzazioni per accedere al tuo Secrets Manager segreto e per chiamare le API pubbliche richieste per il connettore e. OneDrive Amazon Kendra Per ulteriori informazioni, consulta i IAM ruoli per OneDrive le fonti di dati.

Puoi anche aggiungere le seguenti funzionalità opzionali:

- Virtual Private Cloud (VPC): `VpcConfiguration` specifica quando si chiama. `CreateDataSource` Per ulteriori informazioni, consulta Configurazione Amazon Kendra per l'utilizzo di un Amazon VPC.
- Filtri di inclusione ed esclusione: è possibile specificare se includere o escludere determinati file, OneNote sezioni e pagine. OneNote

> **Note**
>
> La maggior parte delle fonti di dati utilizza modelli di espressioni regolari, che sono modelli di inclusione o esclusione denominati filtri. Se si specifica un filtro di inclusione, viene indicizzato solo il contenuto che corrisponde al filtro di inclusione. Qualsiasi documento che non corrisponde al filtro di inclusione non viene indicizzato. Se si specifica un filtro di inclusione ed esclusione, i documenti che corrispondono al filtro di esclusione non vengono indicizzati, anche se corrispondono al filtro di inclusione.

- Identity crawler: specifica se attivare il crawler di identità. Amazon Kendra Il crawler di identità utilizza le informazioni dell'elenco di controllo degli accessi (ACL) per i documenti per filtrare i risultati della ricerca in base all'accesso dell'utente o del gruppo di appartenenza ai documenti. Se disponi di un ACL per i tuoi documenti e scegli di utilizzarlo, puoi anche scegliere di attivare il crawler di identità per configurare il filtraggio Amazon Kendra del contesto utente dei risultati di ricerca. Altrimenti, se il crawler di identità è disattivato, tutti i documenti possono essere ricercati pubblicamente. Se desideri utilizzare il controllo degli accessi per i tuoi documenti e

il crawler di identità è disattivato, in alternativa puoi utilizzare l'PutPrincipalMappingAPI per caricare le informazioni di accesso di utenti e gruppi per il filtraggio del contesto degli utenti.

- Mappature dei campi: è possibile mappare solo i campi indice incorporati o comuni per il connettore. Amazon Kendra OneDrive La mappatura personalizzata dei campi non è disponibile per il OneDrive connettore a causa delle limitazioni dell'API. Per ulteriori informazioni, consulta la sezione Mappatura dei campi di origine dei dati.

Per un elenco di altre importanti chiavi JSON da configurare, consulta. Schema OneDrive modello Microsoft

Ulteriori informazioni

Per ulteriori informazioni sull'integrazione Amazon Kendra con la tua fonte di OneDrive dati, consulta:

- Annuncio del OneDrive connettore Microsoft (V2) aggiornato per. Amazon Kendra

Microsoft SharePoint

SharePoint è un servizio collaborativo per la creazione di siti Web che è possibile utilizzare per personalizzare i contenuti Web e creare pagine, siti, raccolte di documenti ed elenchi. Puoi usarlo Amazon Kendra per indicizzare la tua fonte di SharePoint dati.

Amazon Kendra attualmente supporta SharePoint Online e SharePoint Server (versioni 2013, 2016, 2019 e Subscription Edition).

Puoi connetterti Amazon Kendra alla tua fonte di SharePoint dati utilizzando la Amazon Kendra console, l'TemplateConfigurationAPI o l'SharePointConfigurationAPI.

Amazon Kendra dispone di due versioni del SharePoint connettore. Le funzionalità supportate di ogni versione includono:

SharePoint Connettore V1.0/API SharePointConfiguration

- Log delle modifiche
- Mappature dei campi
- Filtraggio del contesto utente
- Filtri di inclusione/esclusione

- Virtual Private Cloud (VPC) (Cloud privato virtuale (VPC)

SharePoint Connettore V2.0/API TemplateConfiguration

- Mappature dei campi
- Filtraggio del contesto utente
- Scansione delle identità degli utenti
- Filtri di inclusione/esclusione
- Sincronizzazione completa e incrementale dei contenuti
- Virtual Private Cloud (VPC) (Cloud privato virtuale (VPC)

> **Note**
>
> Il supporto per il SharePoint connettore SharePointConfiguration V1.0/API dovrebbe terminare nel 2023. Ti consigliamo di eseguire la migrazione o l'utilizzo del SharePoint connettore V2.0/API. TemplateConfiguration

Per la risoluzione dei problemi relativi al connettore di origine Amazon Kendra SharePoint dati, consulta. Risoluzione dei problemi relativi alle origini dati

Argomenti

- SharePoint connettore V1.0
- SharePoint connettore V2.0

SharePoint connettore V1.0

SharePoint è un servizio collaborativo per la creazione di siti Web che è possibile utilizzare per personalizzare i contenuti Web e creare pagine, siti, raccolte di documenti ed elenchi. Se sei un SharePoint utente, puoi utilizzarlo Amazon Kendra per indicizzare la tua fonte di SharePoint dati.

> **Note**
>
> Il supporto per il SharePoint connettore SharePointConfiguration V1.0/API dovrebbe terminare nel 2023. Ti consigliamo di eseguire la migrazione o l'utilizzo del SharePoint connettore V2.0/API. TemplateConfiguration

Per la risoluzione dei problemi relativi al connettore di origine Amazon Kendra SharePoint dati, consulta. Risoluzione dei problemi relativi alle origini dati

Argomenti

- Funzionalità supportate
- Prerequisiti
- Istruzioni di connessione
- Ulteriori informazioni

Funzionalità supportate

- Log delle modifiche
- Mappature dei campi
- Filtraggio del contesto utente
- Filtri di inclusione/esclusione
- Virtual Private Cloud (VPC) (Cloud privato virtuale (VPC)

Prerequisiti

Prima di utilizzarla Amazon Kendra per indicizzare la tua fonte di SharePoint dati, apporta queste modifiche al tuo account e ai tuoi account. SharePoint AWS

Nel SharePoint, assicurati di avere:

- Hai annotato l'URL dei SharePoint siti che desideri indicizzare.
- Per SharePoint online:
  - Ho preso nota delle tue credenziali di autenticazione di base contenenti un nome utente e una password con autorizzazioni di amministratore del sito.

- Facoltativo: credenziali OAuth 2.0 generate contenenti nome utente, password, ID client e segreto del client.
- Impostazioni di sicurezza predefinite disattivate nel portale di Azure con un utente amministrativo. Per altre informazioni sulla gestione delle impostazioni di sicurezza predefinite nel portale di Azure, consulta la documentazione Microsoft su come abilitare/disabilitare le impostazioni di sicurezza predefinite.

- Per Server: SharePoint
  - Ha annotato il nome di dominio del SharePoint server (il nome NetBIOS in Active Directory). Lo usi, insieme al nome utente e alla password SharePoint di autenticazione di base, per connettere il SharePoint Server a Amazon Kendra.

> **Note**
>
> Se utilizzi SharePoint Server e devi convertire l'Access Control List (ACL) in formato e-mail per filtrare in base al contesto utente, fornisci l'URL del server LDAP e la base di ricerca LDAP. Oppure puoi usare l'override del dominio della directory. L'URL del server LDAP è il nome di dominio completo e il numero di porta (ad esempio, ldap: //example.com:389). La base di ricerca LDAP sono i controller di dominio 'example' e 'com'. Con l'override del dominio della directory, è possibile utilizzare il dominio e-mail anziché utilizzare l'URL del server LDAP e la base di ricerca LDAP. Ad esempio, il dominio di posta elettronica per username@example.com è 'example.com. Puoi utilizzare questo override se non sei preoccupato di convalidare il tuo dominio e desideri semplicemente utilizzare il tuo dominio di posta elettronica.

- Hai aggiunto le seguenti autorizzazioni al tuo account: SharePoint

  Per gli elenchi SharePoint

  - Apri elementi: visualizza l'origine dei documenti con gestori di file lato server.
  - Visualizza pagine dell'applicazione: visualizza moduli, visualizzazioni e pagine dell'applicazione. Enumera gli elenchi.
  - Visualizza elementi: visualizza gli elementi negli elenchi e i documenti nelle raccolte di documenti.
  - Visualizza versioni: visualizza le versioni precedenti di una voce di elenco o di un documento.

  Per SharePoint siti Web

  - Sfoglia le directory: enumera file e cartelle in un sito Web utilizzando l'interfaccia Designer e Web DAV. SharePoint
  - Sfoglia informazioni utente: visualizza le informazioni sugli utenti del sito Web.
  - Enumerazione delle autorizzazioni: enumera le autorizzazioni per il sito Web, l'elenco, la cartella, il documento o la voce di elenco.
  - Apri: apre un sito Web, un elenco o una cartella per accedere agli elementi all'interno del contenitore.
  - Usa le funzionalità di integrazione del client: utilizza SOAP, WebDAV, il modello a oggetti client o SharePoint le interfacce Designer per accedere al sito Web.
  - Usa interfacce remote: utilizza le funzionalità che avviano le applicazioni client.
  - Visualizza pagine: visualizza le pagine di un sito Web.
- È stato selezionato che ogni documento sia unico nelle SharePoint altre fonti di dati che intendi utilizzare per lo stesso indice. Ogni fonte di dati che desideri utilizzare per un indice non deve contenere lo stesso documento in tutte le fonti di dati. Gli ID dei documenti sono globali rispetto a un indice e devono essere univoci per indice.

Nel tuo Account AWS, assicurati di avere:

- Ha creato un Amazon Kendra indice e, se si utilizza l'API, ha annotato l'ID dell'indice.
- Hai creato un IAM ruolo per la tua origine dati e, se utilizzi l'API, hai annotato l'ARN del IAM ruolo.

> **Note**
>
> Se modifichi il tipo di autenticazione e le credenziali, devi aggiornare il IAM ruolo per accedere all'ID AWS Secrets Manager segreto corretto.

- Ha archiviato le credenziali di SharePoint autenticazione in un AWS Secrets Manager segreto e, se si utilizza l'API, ha annotato l'ARN del segreto.

> **Note**
>
> Ti consigliamo di aggiornare o ruotare regolarmente le credenziali e il segreto. Fornisci solo il livello di accesso necessario per la tua sicurezza. Non è consigliabile riutilizzare credenziali e segreti tra diverse fonti di dati e versioni dei connettori 1.0 e 2.0 (ove applicabile).

Se non disponi di un IAM ruolo o di un segreto esistente, puoi utilizzare la console per creare un nuovo IAM ruolo e un Secrets Manager segreto quando connetti la tua origine SharePoint dati a. Amazon Kendra Se utilizzi l'API, devi fornire l'ARN di un IAM ruolo e di un Secrets Manager segreto esistenti e un ID di indice.

Istruzioni di connessione

Per connetterti Amazon Kendra alla tua fonte di SharePoint dati devi fornire i dettagli delle tue SharePoint credenziali in modo da Amazon Kendra poter accedere ai tuoi dati. Se non lo hai ancora configurato, SharePoint Amazon Kendra Prerequisiti consulta.

Console

Per connettersi Amazon Kendra a SharePoint

1. Accedi alla console di AWS gestione e apri la Amazon Kendra console.
2. Dal riquadro di navigazione a sinistra, scegli Indici, quindi scegli l'indice che desideri utilizzare dall'elenco degli indici.

   > **Note**
   >
   > Puoi scegliere di configurare o modificare le impostazioni del controllo dell'accesso degli utenti in Impostazioni dell'indice.

3. Nella pagina Guida introduttiva, scegli Aggiungi origine dati.
4. Nella pagina Aggiungi origine dati, scegli il SharePoint connettore v1.0, quindi scegli Aggiungi origine dati.
5. Nella pagina Specificare i dettagli dell'origine dati, inserisci le seguenti informazioni:

   a. In Nome e descrizione, per Nome dell'origine dati, inserisci un nome per l'origine dati. Puoi includere trattini ma non spazi.
   b. (Facoltativo) Descrizione: immetti una descrizione facoltativa per la tua fonte di dati.
   c. In Lingua predefinita: scegli una lingua per filtrare i documenti per l'indice. Se non diversamente specificato, la lingua predefinita è l'inglese. La lingua specificata nei metadati del documento ha la precedenza sulla lingua selezionata.
   d. In Tag, per Aggiungi nuovo tag, includi tag opzionali per cercare e filtrare le risorse o tenere traccia dei costi. AWS
   e. Seleziona Successivo.

6. Nella pagina Definisci accesso e sicurezza, inserisci le seguenti informazioni:

   a. Per il metodo di hosting: scegli tra SharePoint Online e SharePointServer.

      i. Per SharePointOnline: inserisci gli URL del sito specifici del tuo repository. SharePoint

      ii. Per SharePointServer: scegli la tua SharePoint versione, inserisci gli URL del sito specifici del tuo SharePoint repository e inserisci il Amazon S3 percorso del certificato SSL.

   b. (Solo SharePoint server) Per il proxy Web: immetti il nome host e il numero di porta dell'istanza interna. SharePoint Il numero di porta deve essere un valore numerico compreso tra 0 e 65535.

   c. Per l'autenticazione: scegli tra le seguenti opzioni in base al tuo caso d'uso:

      i. Per SharePoint online: scegli tra l'autenticazione di base e l'autenticazione OAuth 2.0.

      ii. Per SharePoint server: scegli tra Nessuno, LDAP e Manuale.

   d. Per AWS Secrets Manager segreto: scegli un segreto esistente o creane uno nuovo per memorizzare le Secrets Manager credenziali di autenticazione. SharePoint Se scegli di creare un nuovo segreto, si apre una finestra AWS Secrets Manager segreta. Devi inserire un nome segreto. Il prefisso 'AmazonKendra- SharePoint -' viene aggiunto automaticamente al nome segreto.

   e. Inserisci le seguenti altre informazioni nella finestra Crea un AWS Secrets Manager segreto:

      i. Scegli tra le seguenti opzioni di autenticazione SharePoint cloud, in base al tuo caso d'uso:

         A. Autenticazione di base: inserisci il nome utente del tuo SharePoint account come nome utente e la password dell' SharePoint account come password.

         B. Autenticazione OAuth 2.0: inserisci il nome utente del tuo SharePoint account come nome utente, la password dell' SharePointaccount come password, il tuo SharePoint ID univoco generato automaticamente come ID cliente e la stringa segreta condivisa utilizzata da entrambi SharePoint e Amazon Kendra come segreto del cliente.

      ii. Scegli tra le seguenti opzioni di autenticazione SharePoint del server, in base al tuo caso d'uso:

A. Nessuna: inserisci il nome utente dell' SharePoint account come nome utente, la password dell' SharePoint account come password e il nome di dominio del server.

B. LDAP ***: immetti il nome utente dell' SharePoint account come nome utente, la password dell' SharePointaccount come password, l'endpoint del server LDAP (inclusi il protocollo e il numero di porta, ad esempio ldap: //example.com:389) e la base di ricerca LDAP (ad esempio, dc=example, dc=com).***

C. Manuale: immettere il nome utente dell' SharePoint account come nome utente, la password dell' SharePoint account come password e il dominio e-mail Override (dominio e-mail dell'utente o del gruppo della directory).

iii. Selezionare Salva.

f. Virtual Private Cloud (VPC) : è inoltre necessario aggiungere sottoreti e gruppi di sicurezza VPC.

> **Note**
>
> È necessario utilizzare un VPC se si utilizza SharePoint Server. Amazon VPC è facoltativo per le altre SharePoint versioni.

g. IAM ruolo: scegli un IAM ruolo esistente o crea un nuovo IAM ruolo per accedere alle credenziali del repository e indicizzare il contenuto.

> **Note**
>
> IAM i ruoli utilizzati per gli indici non possono essere utilizzati per le fonti di dati. Se non sei sicuro che un ruolo esistente venga utilizzato per un indice o una FAQ, scegli Crea un nuovo ruolo per evitare errori.

h. Seleziona Successivo.

7. Nella pagina Configura le impostazioni di sincronizzazione, inserisci le seguenti informazioni:

a. Usa Change log —Select per aggiornare l'indice anziché sincronizzare tutti i file.

b. Esplora gli allegati: seleziona questa opzione per eseguire la scansione degli allegati.

c. Usa le mappature dei gruppi locali: seleziona per assicurarti che i documenti siano filtrati correttamente.

d. Configurazione aggiuntiva: aggiungi modelli di espressioni regolari per includere o escludere determinati file. È possibile aggiungere fino a 100 pattern.

e. Pianificazione di esecuzione di In Sync per Frequency: con quale frequenza Amazon Kendra verrà eseguita la sincronizzazione con la fonte di dati.

f. Seleziona Successivo.

8. Nella pagina Imposta mappature dei campi, inserisci le seguenti informazioni:

a. Amazon Kendra mappature di campo predefinite: seleziona uno dei campi di origine dati predefiniti Amazon Kendra generati che desideri mappare all'indice.

b. Per mappature di campo personalizzate: aggiungi campi di origine dati personalizzati per creare un nome di campo indice a cui mappare e il tipo di dati del campo.

c. Seleziona Successivo.

9. Nella pagina Rivedi e crea, verifica che le informazioni inserite siano corrette, quindi seleziona Aggiungi origine dati. Puoi anche scegliere di modificare le tue informazioni da questa pagina. L'origine dati verrà visualizzata nella pagina Origini dati dopo che l'origine dati sarà stata aggiunta correttamente.

API

Per connettersi Amazon Kendra a SharePoint

È necessario specificare quanto segue utilizzando l'SharePointConfigurationAPI:

- SharePointVersione: specifica la SharePoint versione da utilizzare durante la configurazione SharePoint. Questo è il caso indipendentemente dal fatto che si utilizzi SharePoint Server 2013, SharePoint Server 2016, SharePoint Server 2019 o SharePoint Online.
- Secret Amazon Resource Name (ARN): fornisci l'Amazon Resource Name (ARN) di un Secrets Manager segreto che contiene le credenziali di autenticazione che hai creato nel tuo SharePoint account. Il segreto è archiviato in una struttura JSON.

  Per l'autenticazione di base SharePoint online, la seguente è la struttura JSON minima che deve essere inclusa nel tuo segreto:

```
{
    "userName": "user name",
    "password": "password"
}
```

Per l'autenticazione OAuth 2.0 SharePoint online, la seguente è la struttura JSON minima che deve essere inclusa nel segreto:

```
{
    "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"
}
```

Per l'autenticazione di base del SharePoint server, la seguente è la struttura JSON minima che deve essere inclusa nel segreto:

```
{
    "userName": "user name",
    "password": "password",
    "domain": "server domain name"
}
```

Per l'autenticazione LDAP SharePoint del server (se devi convertire l'elenco di controllo degli accessi (ACL) in formato e-mail per filtrare in base al contesto utente, puoi includere l'URL del server LDAP e la base di ricerca LDAP nel tuo segreto), la seguente è la struttura JSON minima che deve essere inclusa nel tuo segreto:

```
{
    "userName": "user name",
    "password": "password",
    "domain": "server domain name"
    "ldapServerUrl": "ldap://example.com:389",
    "ldapSearchBase": "dc=example,dc=com"
}
```

Per l'autenticazione manuale del SharePoint server, la seguente è la struttura JSON minima che deve essere inclusa nel segreto:

```
{
    "userName": "user name",
    "password": "password",
```

```
    "domain": "server domain name",
    "emailDomainOverride": "example.com"
}
```

> **Note**
>
> Ti consigliamo di aggiornare o ruotare regolarmente le credenziali e il segreto. Fornisci solo il livello di accesso necessario per la tua sicurezza. Non è consigliabile riutilizzare credenziali e segreti tra diverse fonti di dati e versioni dei connettori 1.0 e 2.0 (ove applicabile).

- IAM ruolo: specifica `RoleArn` quando chiami `CreateDataSource` per fornire a un IAM ruolo le autorizzazioni per accedere al tuo Secrets Manager segreto e per chiamare le API pubbliche richieste per il connettore e. SharePoint Amazon Kendra Per ulteriori informazioni, consulta i IAM ruoli per SharePoint le fonti di dati.
- Amazon VPC—Se utilizzi SharePoint Server, specifica `VpcConfiguration` come parte della configurazione dell'origine dati. Vedi Configurazione Amazon Kendra per l'uso di un VPC.

Puoi anche aggiungere le seguenti funzionalità opzionali:

- Proxy Web: indica se connettersi agli URL SharePoint del sito tramite un proxy Web. È possibile utilizzare questa opzione solo per SharePoint Server.
- Indicizzazione degli elenchi: indica Amazon Kendra se indicizzare il contenuto degli allegati agli elementi dell'elenco. SharePoint
- Registro delle modifiche: indica se Amazon Kendra utilizzare il meccanismo del registro delle modifiche dell'origine SharePoint dati per determinare se un documento deve essere aggiornato nell'indice.

> **Note**
>
> Utilizza il registro delle modifiche se non desideri Amazon Kendra scansionare tutti i documenti. Se il registro delle modifiche è di grandi dimensioni, la scansione dei documenti nella fonte SharePoint dati potrebbe richiedere Amazon Kendra meno tempo rispetto all'elaborazione del registro delle modifiche. Se sincronizzi la fonte di SharePoint dati con l'indice per la prima volta, tutti i documenti vengono scansionati.

- Filtri di inclusione ed esclusione: puoi specificare se includere o escludere determinati contenuti.

> **Note**
>
> La maggior parte delle fonti di dati utilizza modelli di espressioni regolari, che sono modelli di inclusione o esclusione denominati filtri. Se si specifica un filtro di inclusione, viene indicizzato solo il contenuto che corrisponde al filtro di inclusione. Qualsiasi documento che non corrisponde al filtro di inclusione non viene indicizzato. Se si specifica un filtro di inclusione ed esclusione, i documenti che corrispondono al filtro di esclusione non vengono indicizzati, anche se corrispondono al filtro di inclusione.

- Mappature dei campi: scegli di mappare i campi delle sorgenti SharePoint dati ai campi indice. Amazon Kendra Per ulteriori informazioni, consulta la sezione Mappatura dei campi di origine dei dati.

> **Note**
>
> Il campo del corpo del documento o l'equivalente del corpo del documento per i documenti è necessario per Amazon Kendra eseguire la ricerca nei documenti. È necessario mappare il nome del campo del corpo del documento nella fonte dati al nome del campo indice`_document_body`. Tutti gli altri campi sono facoltativi.

- Filtraggio del contesto utente e controllo degli accessi:Amazon Kendra esegue la scansione dell'elenco di controllo degli accessi (ACL) dei documenti, se disponi di un ACL per i documenti. Le informazioni ACL vengono utilizzate per filtrare i risultati della ricerca in base all'accesso dell'utente o del relativo gruppo ai documenti. Per ulteriori informazioni, consulta Filtraggio del contesto utente.

Ulteriori informazioni

Per ulteriori informazioni sull'integrazione Amazon Kendra con la tua fonte di SharePoint dati, consulta:

- Guida introduttiva al connettore Amazon Kendra SharePoint online

SharePoint connettore V2.0

SharePoint è un servizio collaborativo per la creazione di siti Web che è possibile utilizzare per personalizzare i contenuti Web e creare pagine, siti, raccolte di documenti ed elenchi. Puoi usarlo Amazon Kendra per indicizzare la tua fonte di SharePoint dati.

Amazon Kendra attualmente supporta SharePoint Online e SharePoint Server (2013, 2016, 2019 e Subscription Edition).

> **Note**
>
> Il supporto per il SharePoint connettore SharePointConfiguration V1.0/API dovrebbe terminare nel 2023. Ti consigliamo di eseguire la migrazione o l'utilizzo del SharePoint connettore V2.0/API. TemplateConfiguration

Per la risoluzione dei problemi relativi al connettore di origine Amazon Kendra SharePoint dati, consulta. Risoluzione dei problemi relativi alle origini dati

Argomenti

Funzionalità supportate

Amazon Kendra SharePoint il connettore di origine dati supporta le seguenti funzionalità:

- mappature dei campi
- Filtraggio del contesto utente
- Scansione delle identità degli utenti
- Modelli di inclusione/esclusione
- Sincronizzazione completa e incrementale dei contenuti
- Virtual Private Cloud (VPC) (Cloud privato virtuale (VPC)

Prerequisiti

Prima di poterla utilizzare Amazon Kendra per indicizzare la tua fonte di SharePoint dati, apporta queste modifiche al tuo account SharePoint e AWS ai tuoi account.

In SharePoint Online, assicurati di avere:

- Hai copiato gli URL delle tue SharePoint istanze. *`Il formato per l'URL dell'host che inserisci è https://yourdomain.sharepoint.com/sites/mysite.`* L'URL deve iniziare con `https` e contenere`sharepoint.com`.
- Hai copiato il nome di dominio dell'URL dell' SharePoint istanza.
- Ha annotato le tue credenziali di autenticazione di base contenenti il nome utente e la password con le autorizzazioni di amministratore del sito per la connessione a Online. SharePoint
- Impostazioni di sicurezza predefinite disattivate nel portale di Azure utilizzando un utente amministrativo. Per altre informazioni sulla gestione delle impostazioni di sicurezza predefinite nel portale di Azure, consulta la documentazione Microsoft su come abilitare/disabilitare le impostazioni di sicurezza predefinite.
- L'autenticazione a più fattori (MFA) Amazon Kendra è stata disattivata nel tuo SharePoint account, in modo da non impedirgli di scansionare i tuoi contenuti. SharePoint
- Se si utilizza un tipo di autenticazione diverso dall'autenticazione di base: è stato copiato l'ID tenant dell'istanza. SharePoint Per informazioni dettagliate su come trovare l'ID del tenant, vedi Trova l'ID del tenant di Microsoft 365.
- Se devi migrare all'autenticazione degli utenti nel cloud con Microsoft Entra, consulta la documentazione Microsoft sull'autenticazione cloud.
- Per l'autenticazione OAuth 2.0 e l'autenticazione con token di aggiornamento OAuth 2.0: hai annotato le tue credenziali di autenticazione di base contenenti il nome utente e la password che usi per connetterti a SharePoint Online e l'ID client e il segreto del client generati dopo la registrazione con Azure AD. SharePoint
  - Se non usi ACL, hai aggiunto le seguenti autorizzazioni:

Microsoft Graph	SharePoint
• Notes.Read.All (Application): legge tutti i taccuini OneNote • Sites.Read.All (Application): legge gli elementi in tutte le raccolte di siti	• AllSites.Read (delegato): legge gli elementi in tutte le raccolte siti

> **Note**
>
> Note.Read.All e Sites.Read.All sono obbligatori solo se si desidera eseguire la scansione dei documenti. OneNote
> Se desideri eseguire la scansione di siti specifici, l'autorizzazione può essere limitata a siti specifici anziché a tutti i siti disponibili nel dominio. L'utente configura l'autorizzazione Sites.Selected (Application). Con questa autorizzazione API, è necessario impostare l'autorizzazione di accesso su ogni sito in modo esplicito tramite l'API Microsoft Graph. Per ulteriori informazioni, consulta il blog di Microsoft su Sites.Selected permissions.

- Se utilizzi ACL, hai aggiunto le seguenti autorizzazioni:

Microsoft Graph	SharePoint
• Group.Member.Read.All (Application): legge tutte le appartenenze ai gruppi • Notes.Read.All (Application): legge tutti i OneNote taccuini • Siti. FullControl.All (delegato): necessario per recuperare gli ACL dei documenti • Sites.Read.All (Application): legge gli elementi in tutte le raccolte di siti • User.Read.All (Application): legge i profili completi di tutti gli utenti	• AllSites.Read (delegato): legge gli elementi in tutte le raccolte di siti

> **Note**
>
> GroupMember.Read.All e User.Read.All sono obbligatori solo se l'Identity crawler è attivato.
> Se desideri eseguire la scansione di siti specifici, l'autorizzazione può essere limitata a siti specifici anziché a tutti i siti disponibili nel dominio. L'utente configura l'autorizzazione Sites.Selected (Application). Con questa autorizzazione API, è necessario impostare

l'autorizzazione di accesso su ogni sito in modo esplicito tramite l'API Microsoft Graph. Per ulteriori informazioni, consulta il blog di Microsoft su Sites.Selected permissions.

- Per l'autenticazione solo per l'app Azure AD: chiave privata e ID client generati dopo la registrazione con Azure AD. SharePoint Nota anche il certificato X.509.
  - Se non utilizzi ACL, hai aggiunto le seguenti autorizzazioni:

SharePoint
• Sites.Read.All (Applicazione): necessario per accedere agli elementi e agli elenchi in tutte le raccolte siti

> **Note**
>
> Se desideri eseguire la scansione di siti specifici, l'autorizzazione può essere limitata a siti specifici anziché a tutti i siti disponibili nel dominio. L'utente configura l'autorizzazione Sites.Selected (Application). Con questa autorizzazione API, è necessario impostare l'autorizzazione di accesso su ogni sito in modo esplicito tramite l'API Microsoft Graph. Per ulteriori informazioni, consulta il blog di Microsoft su Sites.Selected permissions.

  - Se utilizzi ACL, hai aggiunto le seguenti autorizzazioni:

SharePoint
• Siti. FullControl.All (Applicazione): necessario per recuperare gli ACL dei documenti

> **Note**
>
> Se desideri eseguire la scansione di siti specifici, l'autorizzazione può essere limitata a siti specifici anziché a tutti i siti disponibili nel dominio. L'utente configura l'autorizzazione Sites.Selected (Application). Con questa autorizzazione API, è necessario impostare

l'autorizzazione di accesso su ogni sito in modo esplicito tramite l'API Microsoft Graph. Per ulteriori informazioni, consulta il blog di Microsoft su Sites.Selected permissions.

- Per l'autenticazione SharePoint solo sull'app: hai annotato l'ID SharePoint cliente e il segreto client generati durante la concessione dell'autorizzazione a Solo SharePoint app e l'ID cliente e il segreto client generati quando hai registrato l'app con Azure AD. SharePoint

> **Note**
>
> SharePoint L'autenticazione solo per app non è supportata per la versione 2013. SharePoint

- (Facoltativo) Se stai eseguendo la scansione dei OneNote documenti e utilizzi il crawler di identità, hai aggiunto le seguenti autorizzazioni:

Microsoft Graph	
• GroupMember.Read.All (Applicazione): legge tutte le appartenenze ai gruppi • Notes.Read.All (Application): legge tutti i taccuini OneNote • Sites.Read.All (Application): legge gli elementi in tutte le raccolte di siti • User.Read.All (Application): legge i profili completi di tutti gli utenti	

> **Note**
>
> Non sono richieste autorizzazioni API per la scansione delle entità utilizzando l'autenticazione di base e l'autenticazione solo tramite app. SharePoint

In SharePoint Server, assicurati di avere:

- Hai copiato gli URL delle SharePoint istanze e il nome di dominio degli URL SharePoint . *Il formato per l'URL host che inserisci è https://yourcompany/sites/mysite.* L'URL deve iniziare con`https`.

  > **Note**
  >
  > (On-premise/server) Amazon Kendra verifica se le informazioni sull'endpoint incluse sono le stesse informazioni sull'endpoint specificate nei dettagli di configurazione dell'origine dati. AWS Secrets Manager In questo modo si evita il problema del confuso vicario, ossia un problema di sicurezza in cui un utente non è autorizzato a eseguire un'azione ma lo utilizza Amazon Kendra come proxy per accedere al segreto configurato ed eseguire l'azione. Se successivamente modifichi le informazioni sull'endpoint, devi creare un nuovo segreto per sincronizzare queste informazioni.

- L'autenticazione a più fattori (MFA) Amazon Kendra è stata disattivata nel tuo SharePoint account, in modo da non impedirgli di scansionare i tuoi contenuti. SharePoint
- Se utilizzi l'autenticazione solo tramite SharePoint app per il controllo degli accessi:
  - Ha copiato l'ID SharePoint client generato durante la registrazione dell'app solo a livello di sito. Il formato dell'ID client è ClientId @TenantId. Ad esempio, *ffa956f3-8f89-44e7-b0e4-49670756342c @888d0b57 -69f1-4fb8-957f-e1f0bedf82fe*.
  - Ha SharePoint copiato il client secret generato quando hai registrato l'app solo a livello di sito.

  Nota: poiché gli ID client e i client secret vengono generati per singoli siti solo quando si registra l'autenticazione SharePoint Server for App Only, è supportato un solo URL del sito per l'autenticazione SharePoint App Only.

  > **Note**
  >
  > SharePoint L'autenticazione solo per app non è supportata per la versione SharePoint 2013.

- Se si utilizza un ID e-mail con dominio personalizzato per il controllo degli accessi:
  - *Ha annotato il valore del tuo dominio e-mail personalizzato, ad esempio: "amazon.com».*
- Se utilizzi l'autorizzazione Email ID with Domain from IDP, hai copiato il tuo:

  - Endpoint del server LDAP (endpoint del server LDAP inclusi protocollo e numero di porta). *Ad esempio: ldap: //example.com:389.*
  - Base di ricerca LDAP (base di ricerca dell'utente LDAP). Ad esempio: *CN=Users, DC=SharePoint,* DC=com.
  - Nome utente LDAP e password LDAP.
- Credenziali di autenticazione NTLM configurate o credenziali di autenticazione Kerberos configurate contenenti un nome utente (nome utente dell'account) e una password (password dell'SharePoint account). SharePoint

Nel tuo, assicurati di Account AWS avere:

- Ha creato un Amazon Kendra indice e, se si utilizza l'API, ha annotato l'ID dell'indice.
- Hai creato un IAM ruolo per la tua origine dati e, se utilizzi l'API, hai annotato l'ARN del IAM ruolo.

> **Note**
>
> Se modifichi il tipo di autenticazione e le credenziali, devi aggiornare il IAM ruolo per accedere all'ID AWS Secrets Manager segreto corretto.

- Ha archiviato le credenziali di SharePoint autenticazione in un AWS Secrets Manager segreto e, se si utilizza l'API, ha annotato l'ARN del segreto.

> **Note**
>
> Ti consigliamo di aggiornare o ruotare regolarmente le credenziali e il segreto. Fornisci solo il livello di accesso necessario per la tua sicurezza. Non è consigliabile riutilizzare credenziali e segreti tra diverse fonti di dati e versioni dei connettori 1.0 e 2.0 (ove applicabile).

Se non disponi di un IAM ruolo o di un segreto esistente, puoi utilizzare la console per creare un nuovo IAM ruolo e un Secrets Manager segreto quando connetti la tua origine SharePoint dati a. Amazon Kendra Se utilizzi l'API, devi fornire l'ARN di un IAM ruolo e di un Secrets Manager segreto esistenti e un ID di indice.

Istruzioni di connessione

Per connetterti Amazon Kendra alla tua fonte di SharePoint dati, devi fornire i dettagli delle tue SharePoint credenziali in modo da Amazon Kendra poter accedere ai tuoi dati. Se non lo hai ancora configurato SharePoint , Amazon Kendra vediPrerequisiti.

Console: SharePoint Online

Per connettersi Amazon Kendra a SharePoint Online

1. Accedi alla console di AWS gestione e apri la Amazon Kendra console.
2. Dal riquadro di navigazione a sinistra, scegli Indici, quindi scegli l'indice che desideri utilizzare dall'elenco degli indici.

> **Note**
>
> Puoi scegliere di configurare o modificare le impostazioni del controllo dell'accesso degli utenti in Impostazioni dell'indice.

3. Nella pagina Guida introduttiva, scegli Aggiungi origine dati.
4. Nella pagina Aggiungi origine dati, scegli il SharePoint connettore V2.0, quindi scegli Aggiungi origine dati.
5. Nella pagina Specificare i dettagli dell'origine dati, inserisci le seguenti informazioni:
   a. In Nome e descrizione, per Nome dell'origine dati, inserisci un nome per l'origine dati. Puoi includere trattini ma non spazi.
   b. (Facoltativo) Descrizione: immetti una descrizione facoltativa per la tua fonte di dati.
   c. In Lingua predefinita: scegli una lingua per filtrare i documenti per l'indice. Se non diversamente specificato, la lingua predefinita è l'inglese. La lingua specificata nei metadati del documento ha la precedenza sulla lingua selezionata.
   d. In Tag, per Aggiungi nuovo tag, includi tag opzionali per cercare e filtrare le risorse o tenere traccia dei costi. AWS
   e. Seleziona Successivo.
6. Nella pagina Definisci accesso e sicurezza, inserisci le seguenti informazioni:
   a. In Source, per il metodo di hosting, scegli SharePointOnline.

b. URL del sito specifici del tuo SharePoint repository: inserisci gli URL dell'host. SharePoint *Il formato per gli URL dell'host che inserisci è https://yourdomain.sharepoint.com/sites/mysite.* L'URL deve iniziare con il `https` protocollo. Separa gli URL con una nuova riga. Puoi aggiungere fino a 100 URL.

c. Dominio: inserisci il SharePoint dominio. Ad esempio, il dominio nell'URL *https://yourdomain.sharepoint.com/sites/mysite* è *yourdomain*.

d. Per l'autorizzazione, puoi scegliere tra le seguenti opzioni ACL:

- Nome principale utente: il controllo dell'accesso si baserà sul nome principale dell'utente recuperato dal portale di Azure.
- E-mail: il controllo degli accessi si baserà sugli ID di posta elettronica recuperati dal portale di Azure.

> **Note**
>
> Se non si specifica un valore, Email viene considerato il valore predefinito.

e. Per l'autenticazione, scegli tra l'autenticazione Basic, OAuth 2.0, l'autenticazione solo per app di Azure AD, l'autenticazione solo per SharePoint app e l'autenticazione con token di aggiornamento OAuth 2.0 in base al tuo caso d'uso.

i. Se usi l'autenticazione di base, inserisci le seguenti informazioni:

- Per AWS Secrets Manager segreto: scegli un segreto esistente o creane uno nuovo Secrets Manager per memorizzare le credenziali di SharePoint autenticazione. Se scegli di creare un nuovo segreto, si apre una finestra AWS Secrets Manager segreta. Inserisci le seguenti informazioni nella finestra:
  - Nome segreto: un nome per il tuo segreto. Il prefisso 'AmazonKendra-SharePoint -' viene aggiunto automaticamente al nome segreto.
  - Nome utente: nome utente per il tuo account. SharePoint
  - Password: password per il tuo SharePoint account.

ii. Se utilizzi l'autenticazione OAuth 2.0, inserisci le seguenti informazioni:

- ID tenant: ID tenant del tuo account. SharePoint
- Per AWS Secrets Manager segreto: scegli un segreto esistente o creane uno nuovo per memorizzare le Secrets Manager credenziali di autenticazione.

SharePoint Se scegli di creare un nuovo segreto, si apre una finestra AWS Secrets Manager segreta. Inserisci le seguenti informazioni nella finestra:

- Nome segreto: un nome per il tuo segreto. Il prefisso 'AmazonKendra-SharePoint -' viene aggiunto automaticamente al nome segreto.
- Nome utente: nome utente per il tuo account. SharePoint
- Password: password per il tuo SharePoint account.
- ID cliente: l'ID client di Azure AD generato al momento della registrazione SharePoint in Azure AD.
- Segreto client: il segreto del client Azure AD generato al momento della registrazione in Azure AD. SharePoint

iii. Se usi l'autenticazione solo per app di Azure AD, inserisci le seguenti informazioni:

- ID tenant: ID tenant del tuo account. SharePoint
- Certificato X.509 autofirmato di Azure AD: certificato per l'autenticazione del connettore per Azure AD.
- Per AWS Secrets Manager segreto: scegli un segreto esistente o crea un nuovo segreto per archiviare le credenziali di autenticazione. Secrets Manager SharePoint Se scegli di creare un nuovo segreto, si apre una finestra AWS Secrets Manager segreta. Inserisci le seguenti informazioni nella finestra:
  - Nome segreto: un nome per il tuo segreto. Il prefisso 'AmazonKendra-SharePoint -' viene aggiunto automaticamente al nome segreto.
  - ID client: l'ID client di Azure AD generato al momento della registrazione SharePoint in Azure AD.
  - Chiave privata: una chiave privata per autenticare il connettore per Azure AD.

iv. Se usi l'autenticazione SharePoint solo per app, inserisci le seguenti informazioni:

- ID tenant: ID tenant del tuo account. SharePoint
- Per AWS Secrets Manager segreto: scegli un segreto esistente o creane uno nuovo per memorizzare le Secrets Manager credenziali di autenticazione. SharePoint Se scegli di creare un nuovo segreto, si apre una finestra AWS Secrets Manager segreta. Inserisci le seguenti informazioni nella finestra:
  - Nome segreto: un nome per il tuo segreto. Il prefisso 'AmazonKendra-SharePoint -' viene aggiunto automaticamente al nome segreto.

- SharePoint ID cliente: l'ID SharePoint cliente che hai generato quando hai registrato l'app solo a livello di tenant. *Il formato ClientID è clientID@. TenantId* Ad esempio, *ffa956f3-8f89-44e7-b0e4-49670756342c @888d0b57 -69f1-4fb8-957f-e1f0bedf82fe*.
- SharePoint client secret: il SharePoint client secret generato al momento della registrazione all'app solo a livello di tenant.
- ID client: l'ID client di Azure AD generato quando ti registri SharePoint in Azure AD.
- Segreto client: il segreto del client di Azure AD generato al momento della registrazione ad Azure AD. SharePoint

v. Se usi l'autenticazione con token di aggiornamento OAuth 2.0, inserisci le seguenti informazioni:

- ID tenant: ID tenant del tuo account. SharePoint
- Per AWS Secrets Manager segreto: scegli un segreto esistente o creane uno nuovo per memorizzare le Secrets Manager credenziali di autenticazione. SharePoint Se scegli di creare un nuovo segreto, si apre una finestra AWS Secrets Manager segreta. Inserisci le seguenti informazioni nella finestra:
  - Nome segreto: un nome per il tuo segreto. Il prefisso 'AmazonKendra-SharePoint -' viene aggiunto automaticamente al nome segreto.
  - ID client: l'ID client di Azure AD univoco generato durante la registrazione SharePoint in Azure AD.
  - Segreto client: il segreto del client di Azure AD generato al momento della registrazione ad Azure AD. SharePoint
  - Token di aggiornamento: il token di aggiornamento generato a cui connettersi. Amazon Kendra SharePoint

f. Identity crawler - (Attivato solo quando l'ACL è abilitato) Scegli di attivare il crawler di identità per sincronizzare le informazioni Amazon Kendra sull'identità. Se scegli di disattivare il crawler di identità, devi caricare le informazioni principali utilizzando l'API. PutPrincipalMapping

Puoi anche scegliere di:

i. Esplora la mappatura dei gruppi locali: attiva questa opzione per eseguire la scansione della mappatura dei gruppi locali.

ii. Esplora la mappatura dei gruppi AD: attiva questa opzione per eseguire la scansione della mappatura dei gruppi di Azure Active Directory.

> **Note**
>
> La scansione della mappatura dei gruppi AD è disponibile solo per l'autenticazione OAuth 2.0, il token di aggiornamento OAuth 2.0 e l'autenticazione solo per app. SharePoint

g. (Facoltativo) Configura VPC e gruppo di sicurezza: seleziona un VPC da utilizzare con la tua istanza. SharePoint In tal caso, è necessario aggiungere sottoreti e gruppi di sicurezza VPC.

h. IAM ruolo: scegli un IAM ruolo esistente o creane uno nuovo IAM per accedere alle credenziali del repository e indicizzare il contenuto.

> **Note**
>
> IAM i ruoli utilizzati per gli indici non possono essere utilizzati per le fonti di dati. Se non sei sicuro che un ruolo esistente venga utilizzato per un indice o una FAQ, scegli Crea un nuovo ruolo per evitare errori.

i. Seleziona Successivo.

7. Nella pagina Configura le impostazioni di sincronizzazione, inserisci le seguenti informazioni:

a. Nell'ambito della sincronizzazione, scegli tra le seguenti opzioni:

i. Seleziona entità: scegli le entità che desideri sottoporre a scansione. È possibile scegliere di eseguire la scansione di tutte le entità o di qualsiasi combinazione di file, allegati, pagine di collegamenti, eventi, commenti ed elenchi di dati.

ii. Nella configurazione aggiuntiva, per i modelli regex delle entità: aggiungi modelli di espressioni regolari per collegamenti, pagine ed eventi per includere entità specifiche invece di sincronizzare tutti i documenti.

iii. Modelli regex: aggiungi modelli di espressioni regolari per includere o escludere i file in base al percorso del file, al nome del file, al tipo di file, al nome della OneNote sezione e al nome della OneNote pagina invece di sincronizzare tutti i documenti. Puoi aggiungerne fino a 100.

> **Note**
>
> OneNote la scansione è disponibile solo per l'autenticazione OAuth 2.0, il token di aggiornamento OAuth 2.0 e l'autenticazione solo tramite app. SharePoint

b. Per la modalità di sincronizzazione, scegli come aggiornare l'indice quando il contenuto dell'origine dati cambia. Quando sincronizzi l'origine dati con Amazon Kendra per la prima volta, tutto il contenuto viene sincronizzato per impostazione predefinita.

- Sincronizzazione completa: sincronizza tutti i contenuti indipendentemente dallo stato di sincronizzazione precedente.
- Sincronizzazione dei documenti nuovi o modificati: sincronizza solo i documenti nuovi o modificati.
- Sincronizzazione di documenti nuovi, modificati o eliminati: sincronizza solo i documenti nuovi, modificati ed eliminati.

c. Pianificazione di esecuzione di In Sync, per Frequenza: con quale frequenza Amazon Kendra verrà eseguita la sincronizzazione con la fonte di dati.

d. Seleziona Successivo.

8. Nella pagina Imposta mappature dei campi, inserisci le seguenti informazioni:

a. Per Pagine degli eventi, file, link, allegati e commenti: seleziona uno dei campi delle origini dati predefiniti Amazon Kendra generati che desideri mappare all'indice.

b. Aggiungi campo: consente di aggiungere campi di origine dati personalizzati per creare un nome di campo indice a cui mappare e il tipo di dati del campo.

c. Seleziona Successivo.

9. Nella pagina Rivedi e crea, verifica che le informazioni inserite siano corrette, quindi seleziona Aggiungi origine dati. Puoi anche scegliere di modificare le tue informazioni da questa pagina. L'origine dati verrà visualizzata nella pagina Origini dati dopo che l'origine dati sarà stata aggiunta correttamente.

Console: SharePoint Server

Per connettersi Amazon Kendra a SharePoint

1. Accedi alla console di AWS gestione e apri la Amazon Kendra console.
2. Dal riquadro di navigazione a sinistra, scegli Indici, quindi scegli l'indice che desideri utilizzare dall'elenco degli indici.

> **Note**
>
> Puoi scegliere di configurare o modificare le impostazioni del controllo dell'accesso degli utenti in Impostazioni dell'indice.

3. Nella pagina Guida introduttiva, scegli Aggiungi origine dati.
4. Nella pagina Aggiungi origine dati, scegli il SharePoint connettore V2.0, quindi scegli Aggiungi origine dati.
5. Nella pagina Specificare i dettagli dell'origine dati, inserisci le seguenti informazioni:
   a. In Nome e descrizione, per Nome dell'origine dati, inserisci un nome per l'origine dati. Puoi includere trattini ma non spazi.
   b. (Facoltativo) Descrizione: immetti una descrizione facoltativa per la tua fonte di dati.
   c. In Lingua predefinita: scegli una lingua per filtrare i documenti per l'indice. Se non diversamente specificato, la lingua predefinita è l'inglese. La lingua specificata nei metadati del documento ha la precedenza sulla lingua selezionata.
   d. In Tag, per Aggiungi nuovo tag, includi tag opzionali per cercare e filtrare le risorse o tenere traccia dei costi. AWS
   e. Seleziona Successivo.
6. Nella pagina Definisci accesso e sicurezza, inserisci le seguenti informazioni:
   a. In Source, per il metodo di hosting, scegli SharePointServer.
   b. Scegli SharePoint la versione: scegli tra SharePoint 2013, SharePoint 2016, SharePoint 2019 e SharePoint (edizione in abbonamento).
   c. URL del sito specifici del tuo SharePoint repository: inserisci gli URL dell'host. SharePoint *Il formato per gli URL host che inserisci è https://yourcompany/sites/mysite.* L'URL deve iniziare con il `https` protocollo. Separa gli URL con una nuova riga. Puoi aggiungere fino a 100 URL.
   d. Dominio: inserisci il SharePoint dominio. *Ad esempio, il dominio nell'URL https://yourcompany/sites/mysite è la tua azienda*
   e. Posizione del certificato SSL: immetti il Amazon S3 percorso del file del certificato SSL.

f. (Facoltativo) Per il proxy Web: immettere il nome host (senza il `https://` protocollo `http://` o) e il numero di porta utilizzato dal protocollo di trasporto dell'URL dell'host. Il valore numerico del numero di porta deve essere compreso tra 0 e 65535.

g. Autorizzazione: attiva o disattiva le informazioni dell'elenco di controllo degli accessi (ACL) per i documenti, se disponi di un ACL e desideri utilizzarlo per il controllo degli accessi. L'ACL specifica a quali documenti possono accedere utenti e gruppi. Le informazioni ACL vengono utilizzate per filtrare i risultati della ricerca in base all'accesso dell'utente o del relativo gruppo ai documenti. Per ulteriori informazioni, consulta Filtraggio del contesto utente.

   Per SharePoint Server puoi scegliere tra le seguenti opzioni ACL:

   i. ID e-mail con dominio di IDP: il controllo degli accessi si baserà sugli ID e-mail estratti dai domini di posta elettronica recuperati dal provider di identità (IDP) sottostante. I dettagli di connessione IDP vengono forniti in modo segreto durante l'autenticazione. Secrets Manager

   ii. ID e-mail con dominio personalizzato: il controllo degli accessi si baserà sugli ID e-mail. Vuoi fornire il valore del dominio e-mail. Ad esempio, "*amazon.com*». Il dominio e-mail verrà utilizzato per creare l'ID e-mail per il controllo degli accessi. Devi inserire il tuo dominio di posta elettronica utilizzando Aggiungi dominio e-mail.

   iii. Dominio\ Utente con dominio: il controllo degli accessi verrà strutturato utilizzando il formato Dominio\ ID utente. È necessario fornire un nome di dominio valido. Ad esempio: *«sharepoint2019"* per costruire il controllo degli accessi.

h. Per l'autenticazione, scegli tra l'autenticazione SharePoint solo per app, l'autenticazione NTLM e l'autenticazione Kerberos in base al tuo caso d'uso.

   i. Immettete le seguenti informazioni sia per l'autenticazione NTLM che per l'autenticazione Kerberos:

      Per AWS Secrets Manager segreto: scegli un segreto esistente o creane uno nuovo per memorizzare le Secrets Manager credenziali di autenticazione. SharePoint
      Se scegli di creare un nuovo segreto, si apre una finestra AWS Secrets Manager segreta. Inserisci le seguenti informazioni nella finestra:

      - Nome segreto: un nome per il tuo segreto. Il prefisso 'AmazonKendra- SharePoint -' viene aggiunto automaticamente al nome segreto.
      - Nome utente: nome utente per il tuo account. SharePoint

- Password: password per il tuo SharePoint account.

Se utilizzi Email ID with Domain di IDP, inserisci anche:

- Endpoint del server LDAP: endpoint del server LDAP, incluso il protocollo e il numero di porta. *Ad esempio: ldap: //example.com:389.*
- Base di ricerca LDAP: base di ricerca dell'utente LDAP. Ad esempio: *CN=Users, DC=SharePoint, DC=com*.
- Nome utente LDAP: il nome utente LDAP.
- Password LDAP: la tua password LDAP.

ii. Inserisci le seguenti informazioni per l'autenticazione solo tramite appSharePoint .

Per AWS Secrets Manager segreto: scegli un segreto esistente o creane uno nuovo per memorizzare le Secrets Manager SharePoint credenziali di autenticazione. Se scegli di creare un nuovo segreto, si apre una finestra AWS Secrets Manager segreta. Inserisci le seguenti informazioni nella finestra:

- Nome segreto: un nome per il tuo segreto. Il prefisso 'AmazonKendra- SharePoint -' viene aggiunto automaticamente al nome segreto.
- ID cliente: l'ID SharePoint cliente generato quando hai registrato l'app solo a livello di sito. Il formato ClientID è ClientID@. TenantId Ad esempio, *ffa956f3-8f89-44e7-b0e4-49670756342c @888d0b57 -69f1-4fb8-957f-e1f0bedf82fe*.
- SharePoint client secret SharePoint: il client secret generato quando ti registri all'app solo a livello di sito.

  Nota: poiché gli ID client e i client secret vengono generati per singoli siti solo quando si registra l'autenticazione SharePoint Server for App Only, per l'autenticazione solo tramite SharePoint app è supportato un solo URL del sito.

Se utilizzi Email ID with Domain from IDP, inserisci anche:

- Endpoint del server LDAP: endpoint del server LDAP, incluso il protocollo e il numero di porta. *Ad esempio: ldap: //example.com:389.*
- Base di ricerca LDAP: base di ricerca dell'utente LDAP. Ad esempio: *CN=Users, DC=SharePoint, DC=com*.

- Nome utente LDAP: il nome utente LDAP.
- Password LDAP: la tua password LDAP.

i. Identity crawler: specifica se attivare il crawler di identità. Amazon Kendra Il crawler di identità utilizza le informazioni dell'elenco di controllo degli accessi (ACL) per i documenti per filtrare i risultati della ricerca in base all'accesso dell'utente o del gruppo di appartenenza ai documenti. Se disponi di un ACL per i tuoi documenti e scegli di utilizzarlo, puoi anche scegliere di attivare il crawler di identità per configurare il filtraggio Amazon Kendra contestuale dell'utente dei risultati di ricerca. Altrimenti, se il crawler di identità è disattivato, tutti i documenti possono essere ricercati pubblicamente. Se desideri utilizzare il controllo degli accessi per i tuoi documenti e il crawler di identità è disattivato, in alternativa puoi utilizzare l'PutPrincipalMappingAPI per caricare le informazioni di accesso di utenti e gruppi per il filtraggio del contesto degli utenti.

   i. Esplora la mappatura dei gruppi locali: attiva questa opzione per eseguire la scansione della mappatura dei gruppi locali.

   ii. (Solo per ID e-mail con dominio di IDP) Esplora la mappatura dei gruppi AD: attiva per eseguire la scansione della mappatura di Active Directory.

> **Note**
>
> La scansione della mappatura del gruppo AD è disponibile solo per l'autenticazione tramite app. SharePoint

j. (Facoltativo) Configura VPC e gruppo di sicurezza: seleziona un VPC da utilizzare con la tua istanza. SharePoint In tal caso, è necessario aggiungere sottoreti e gruppi di sicurezza VPC.

k. IAM ruolo: scegli un IAM ruolo esistente o creane uno nuovo IAM per accedere alle credenziali del repository e indicizzare il contenuto.

> **Note**
>
> IAM i ruoli utilizzati per gli indici non possono essere utilizzati per le fonti di dati. Se non sei sicuro che un ruolo esistente venga utilizzato per un indice o una FAQ, scegli Crea un nuovo ruolo per evitare errori.

l. Seleziona Successivo.

7. Nella pagina Configura le impostazioni di sincronizzazione, inserisci le seguenti informazioni:

a. Nell'ambito della sincronizzazione, scegli tra le seguenti opzioni:

   i. Seleziona entità: scegli le entità che desideri sottoporre a scansione. È possibile scegliere di eseguire la scansione di tutte le entità o di qualsiasi combinazione di file, allegati, collegamenti, pagine, eventi e dati di elenco.

   ii. Nella configurazione aggiuntiva, per i modelli regex delle entità: aggiungi modelli di espressioni regolari per collegamenti, pagine ed eventi per includere entità specifiche invece di sincronizzare tutti i documenti.

   iii. Modelli regex: aggiungi modelli di espressioni regolari per includere o escludere i file in base al percorso del file, nome del file, tipo di file, nome della OneNotesezione e nome della OneNotepagina anziché sincronizzare tutti i documenti. Puoi aggiungerne fino a 100.

   > **Note**
   >
   > OneNote la scansione è disponibile solo per l'autenticazione solo SharePoint tramite app.

b. Modalità di sincronizzazione: scegli come aggiornare l'indice quando il contenuto dell'origine dati cambia. Quando sincronizzi l'origine dati con Amazon Kendra per la prima volta, tutto il contenuto viene sottoposto a scansione e indicizzato per impostazione predefinita. Se la sincronizzazione iniziale non è riuscita, devi eseguire una sincronizzazione completa dei dati, anche se non scegli la sincronizzazione completa come opzione della modalità di sincronizzazione.

   - Sincronizzazione completa: indicizza di nuovo tutti i contenuti, sostituendo i contenuti esistenti ogni volta che l'origine dati si sincronizza con l'indice.
   - Sincronizzazione nuova e modificata: indicizza solo i contenuti nuovi e modificati ogni volta che l'origine dati si sincronizza con l'indice. Amazon Kendra può utilizzare il meccanismo dell'origine dati per tenere traccia delle modifiche ai contenuti e indicizzare i contenuti modificati dall'ultima sincronizzazione.
   - Sincronizzazione nuova, modificata ed eliminata: indicizza solo i contenuti nuovi, modificati ed eliminati ogni volta che l'origine dati si sincronizza con l'indice. Amazon Kendra può utilizzare il meccanismo dell'origine dati per tenere traccia delle modifiche ai contenuti e indicizzare i contenuti modificati dall'ultima sincronizzazione.

c. Pianificazione di esecuzione di In Sync, per Frequenza: con quale frequenza Amazon Kendra verrà eseguita la sincronizzazione con la fonte di dati.

d. Seleziona Successivo.

8. Nella pagina Imposta mappature dei campi, inserisci le seguenti informazioni:

a. Per le pagine degli eventi, i file, i link, gli allegati e i dati degli elenchi: seleziona uno dei campi di origine dati predefiniti Amazon Kendra generati che desideri mappare all'indice.

b. Aggiungi campo: consente di aggiungere campi di origine dati personalizzati per creare un nome di campo indice a cui mappare e il tipo di dati del campo.

c. Seleziona Successivo.

9. Nella pagina Rivedi e crea, verifica che le informazioni inserite siano corrette, quindi seleziona Aggiungi origine dati. Puoi anche scegliere di modificare le tue informazioni da questa pagina. L'origine dati verrà visualizzata nella pagina Origini dati dopo che l'origine dati sarà stata aggiunta correttamente.

API

Per connettersi Amazon Kendra a SharePoint

È necessario specificare un codice JSON dello schema dell'origine dati utilizzando l'TemplateConfigurationAPI. È necessario fornire le seguenti informazioni:

- Origine dati: specifica il tipo di origine dati come `SHAREPOINTV2` quando usi lo schema TemplateConfigurationJSON. Specificate anche l'origine dati come `TEMPLATE` quando chiamate l'CreateDataSourceAPI.
- Repository Endpoint Metadata: specifica la fine dell'`tenantID`doministanza. `siteUrls` SharePoint
- Modalità di sincronizzazione: specifica come Amazon Kendra aggiornare l'indice quando il contenuto dell'origine dati cambia. Quando sincronizzi l'origine dati con Amazon Kendra per la prima volta, tutto il contenuto viene sottoposto a scansione e indicizzato per impostazione predefinita. Se la sincronizzazione iniziale non è riuscita, devi eseguire una sincronizzazione completa dei dati, anche se non scegli la sincronizzazione completa come opzione della modalità di sincronizzazione. Puoi scegliere tra:
  - `FORCED_FULL_CRAWL`per indicizzare nuovamente tutti i contenuti, sostituendo i contenuti esistenti ogni volta che l'origine dati si sincronizza con l'indice.

  - `FULL_CRAWL`per indicizzare solo i contenuti nuovi, modificati ed eliminati ogni volta che l'origine dati si sincronizza con l'indice. Amazon Kendra può utilizzare il meccanismo dell'origine dati per tenere traccia delle modifiche ai contenuti e indicizzare i contenuti modificati dall'ultima sincronizzazione.
  - `CHANGE_LOG`per indicizzare solo contenuti nuovi e modificati ogni volta che l'origine dati si sincronizza con l'indice. Amazon Kendra può utilizzare il meccanismo dell'origine dati per tenere traccia delle modifiche ai contenuti e indicizzare i contenuti modificati dall'ultima sincronizzazione.
- Identity crawler: specifica se attivare il crawler Amazon Kendra di identità. Il crawler di identità utilizza le informazioni dell'elenco di controllo degli accessi (ACL) per i documenti per filtrare i risultati della ricerca in base all'accesso dell'utente o del gruppo di appartenenza ai documenti. Se disponi di un ACL per i tuoi documenti e scegli di utilizzarlo, puoi anche scegliere di attivare il crawler di identità per configurare il filtraggio Amazon Kendra contestuale dell'utente dei risultati di ricerca. Altrimenti, se il crawler di identità è disattivato, tutti i documenti possono essere ricercati pubblicamente. Se desideri utilizzare il controllo degli accessi per i tuoi documenti e il crawler di identità è disattivato, in alternativa puoi utilizzare l'PutPrincipalMappingAPI per caricare le informazioni di accesso di utenti e gruppi per il filtraggio del contesto degli utenti.

  > **Note**
  >
  > Il crawler di identità è disponibile solo se è impostato su. `crawlAcl` `true`

- Proprietà aggiuntive del repository: specificare:
  - (Per Azure AD) `s3bucketName` e lo `s3certificateName` usi per archiviare il certificato X.509 autofirmato di Azure AD.
  - Tipo di autenticazione (`auth_Type`) che usi,,,`OAuth2`, `OAuth2App``OAuth2Certificate`, `Basic` e. `OAuth2_RefreshToken` `NTLM` `Kerberos`
  - Versione (`version`) utilizzata, indipendentemente dal fatto che `Server` sia`Online`. Se lo usi, `Server` puoi specificare ulteriormente on`PremVersion` come`2013`, `20162019`, o`SubscriptionEdition`.
- Secret Amazon Resource Name (ARN): fornisci l'Amazon Resource Name (ARN) di un Secrets Manager segreto che contiene le credenziali di autenticazione che hai creato nel tuo account. SharePoint

Se usi SharePoint Online, puoi scegliere tra l'autenticazione Basic, OAuth 2.0, solo per app Azure AD e solo app. SharePoint Di seguito è riportata la struttura JSON minima che deve essere segreta per ogni opzione di autenticazione:

- Autenticazione di base

```
{
    "userName": "SharePoint account user name",
    "password": "SharePoint account password"
}
```

- Autenticazione 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"
}
```

- Autenticazione solo per app Azure AD

```
{
    "clientId": "client id generated when registering SharePoint with Azure AD",
    "privateKey": "private key to authorize connection with Azure AD"
}
```

- SharePoint Autenticazione solo per app

```
{
    "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"
}
```

- Autenticazione con token di aggiornamento 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"
}
```

Se utilizzi SharePoint Server, puoi scegliere tra autenticazione SharePoint solo app, autenticazione NTLM e autenticazione Kerberos. Di seguito è riportata la struttura JSON minima che deve essere segreta per ogni opzione di autenticazione:

- SharePoint Autenticazione solo tramite app

```
{
    "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 Autenticazione solo tramite app con dominio proveniente dall'autorizzazione 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"
}
```

- Autenticazione NTLM o Kerberos (solo server)

```
{
    "siteUrlsHash": "Hash representation of SharePoint site URLs",
    "userName": "SharePoint account user name",
    "password": "SharePoint account password"
```

```
}
```

- (Solo server) Autenticazione NTLM o Kerberos con dominio proveniente dall'autorizzazione 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**
>
> Ti consigliamo di aggiornare o ruotare regolarmente le credenziali e il segreto. Fornisci solo il livello di accesso necessario per la tua sicurezza. Non è consigliabile riutilizzare credenziali e segreti tra diverse fonti di dati e versioni dei connettori 1.0 e 2.0 (ove applicabile).

- IAM ruolo: specifica `RoleArn` quando chiami `CreateDataSource` per fornire a un IAM ruolo le autorizzazioni per accedere al tuo Secrets Manager segreto e per chiamare le API pubbliche richieste per il connettore e. SharePoint Amazon Kendra Per ulteriori informazioni, consulta i IAM ruoli per SharePoint le fonti di dati.

Puoi anche aggiungere le seguenti funzionalità opzionali:

- Virtual Private Cloud (VPC): `VpcConfiguration` specifica quando si chiama. `CreateDataSource` Per ulteriori informazioni, consulta Configurazione Amazon Kendra per l'utilizzo di un Amazon VPC.
- Filtri di inclusione ed esclusione: è possibile specificare se includere o escludere determinati file e altri contenuti OneNotes.

> **Note**
>
> La maggior parte delle fonti di dati utilizza modelli di espressioni regolari, che sono modelli di inclusione o esclusione denominati filtri. Se si specifica un filtro di inclusione,

viene indicizzato solo il contenuto che corrisponde al filtro di inclusione. Qualsiasi documento che non corrisponde al filtro di inclusione non viene indicizzato. Se si specifica un filtro di inclusione ed esclusione, i documenti che corrispondono al filtro di esclusione non vengono indicizzati, anche se corrispondono al filtro di inclusione.

- Mappature dei campi: scegli di mappare i campi delle sorgenti SharePoint dati ai campi indice. Amazon Kendra Per ulteriori informazioni, consulta la sezione Mappatura dei campi di origine dei dati.

> **Note**
>
> Il campo del corpo del documento o l'equivalente del corpo del documento per i documenti è necessario per Amazon Kendra eseguire la ricerca nei documenti. È necessario mappare il nome del campo del corpo del documento nella fonte dati al nome del campo indice`_document_body`. Tutti gli altri campi sono facoltativi.

Per un elenco di altre importanti chiavi JSON da configurare, consultaSchema SharePoint modello Microsoft.

Note

- Il connettore supporta mappature di campo personalizzate solo per l'entità Files.
- Per tutte le versioni SharePoint del server, il token ACL deve essere in lettere minuscole. *Per **Email with Domain from IDP** e **Email ID with Custom Domain** ACL, ad esempio: user@sharepoint2019.com.* Per Domain\ User with Domain ACL, ad esempio: *sharepoint2013*\ user.
- Il connettore non supporta la modalità registro delle modifiche/la sincronizzazione dei contenuti nuovi o modificati per il 2013. SharePoint
- Se il nome di un'entità contiene un % carattere, il connettore ignorerà questi file a causa delle limitazioni dell'API.
- OneNote può essere sottoposto a scansione dal connettore solo utilizzando un Tenant ID e con l'autenticazione OAuth 2.0, il token di aggiornamento OAuth 2.0 o l'autenticazione App Only attivata per Online. SharePoint SharePoint
- Il connettore esegue la scansione della prima sezione di un OneNote documento utilizzando solo il nome predefinito, anche se il documento viene rinominato.

- Il connettore esegue la scansione dei link nelle edizioni SharePoint 2019, SharePoint Online e Subscription, solo se, oltre ai Link, sono selezionati come entità da sottoporre a scansione anche pagine e file.
- Il connettore esegue la scansione dei link nel SharePoint 2013 e SharePoint 2016 se Links è selezionato Links come entità da sottoporre a scansione.
- Il connettore esegue la scansione degli allegati e dei commenti degli elenchi solo quando List Data è selezionato anche come entità da sottoporre a scansione.
- Il connettore esegue la scansione degli allegati degli eventi solo quando Events è selezionato anche come entità da sottoporre a scansione.
- Per la versione SharePoint online, il token ACL sarà in lettere minuscole. *Ad esempio, se* ***il nome principale dell'utente*** *è MaryMajor@domain .com nel portale di Azure, il token ACL nel SharePoint connettore sarà marymajor@domain.com.*
- In Identity Crawler for SharePoint Online and Server, se desideri eseguire la scansione di gruppi annidati, devi attivare Local e AD Group Crawling.
- Se usi SharePoint Online e il nome principale dell'utente nel tuo portale di Azure è una combinazione di lettere maiuscole e minuscole, l' SharePoint API lo converte internamente in lettere minuscole. Per questo motivo, il Amazon Kendra SharePoint connettore imposta ACL in lettere minuscole.

Microsoft SQL Server

Microsoft SQL Serverè un sistema di gestione di database relazionali (RDBMS) sviluppato da Microsoft. Se sei un Microsoft SQL Server utente, puoi utilizzarlo Amazon Kendra per indicizzare la tua Microsoft SQL Server fonte di dati. Il connettore di origine Amazon Kendra Microsoft SQL Server dati supporta MS SQL Server 2019.

Puoi connetterti Amazon Kendra alla tua fonte di Microsoft SQL Server dati utilizzando la Amazon Kendra console e l'TemplateConfigurationAPI.

Per la risoluzione dei problemi relativi al connettore della sorgente Amazon Kendra Microsoft SQL Server dati, consultaRisoluzione dei problemi relativi alle origini dati.

Argomenti

- Funzionalità supportate
- Prerequisiti

- Istruzioni di connessione
- Note

Funzionalità supportate

- Mappature dei campi
- Filtraggio del contesto utente
- Filtri di inclusione/esclusione
- Sincronizzazione completa e incrementale dei contenuti
- Virtual Private Cloud (VPC) (Cloud privato virtuale (VPC)

Prerequisiti

Prima di poterla utilizzare Amazon Kendra per indicizzare la tua fonte di Microsoft SQL Server dati, apporta queste modifiche al tuo account Microsoft SQL Server e AWS ai tuoi account.

NelMicrosoft SQL Server, assicurati di avere:

- Hai annotato il nome utente e la password del database.

> **Important**
>
> È consigliabile fornire credenziali Amazon Kendra di database di sola lettura.

- Hai copiato l'URL, la porta e l'istanza dell'host del database.
- È stato verificato che ogni documento sia unico all'interno Microsoft SQL Server e tra le altre fonti di dati che intendi utilizzare per lo stesso indice. Ogni fonte di dati che desideri utilizzare per un indice non deve contenere lo stesso documento in tutte le fonti di dati. Gli ID dei documenti sono globali rispetto a un indice e devono essere univoci per indice.

Nel tuo Account AWS, assicurati di avere:

- Ha creato un Amazon Kendra indice e, se si utilizza l'API, ha annotato l'ID dell'indice.
- Hai creato un IAM ruolo per la tua origine dati e, se utilizzi l'API, hai annotato l'ARN del IAM ruolo.

> **Note**
>
> Se modifichi il tipo di autenticazione e le credenziali, devi aggiornare il IAM ruolo per accedere all'ID AWS Secrets Manager segreto corretto.

- Ha archiviato le credenziali di Microsoft SQL Server autenticazione in un AWS Secrets Manager segreto e, se si utilizza l'API, ha annotato l'ARN del segreto.

> **Note**
>
> Ti consigliamo di aggiornare o ruotare regolarmente le credenziali e il segreto. Fornisci solo il livello di accesso necessario per la tua sicurezza. Non è consigliabile riutilizzare credenziali e segreti tra diverse fonti di dati e versioni dei connettori 1.0 e 2.0 (ove applicabile).

Se non disponi di un IAM ruolo o di un segreto esistente, puoi utilizzare la console per creare un nuovo IAM ruolo e un Secrets Manager segreto quando connetti la tua origine Microsoft SQL Server dati a. Amazon Kendra Se utilizzi l'API, devi fornire l'ARN di un IAM ruolo e di un Secrets Manager segreto esistenti e un ID di indice.

Istruzioni di connessione

Per connetterti Amazon Kendra alla tua fonte di Microsoft SQL Server dati devi fornire i dettagli delle tue Microsoft SQL Server credenziali in modo da Amazon Kendra poter accedere ai tuoi dati. Se non lo hai ancora configuratoMicrosoft SQL Server, Amazon Kendra vediPrerequisiti.

Console

Per connettersi Amazon Kendra a Microsoft SQL Server

1. Accedi a AWS Management Console e apri la Amazon Kendra console.
2. Dal riquadro di navigazione a sinistra, scegli Indici, quindi scegli l'indice che desideri utilizzare dall'elenco degli indici.

> **Note**
>
> Puoi scegliere di configurare o modificare le impostazioni del controllo dell'accesso degli utenti in Impostazioni dell'indice.

3. Nella pagina Guida introduttiva, scegli Aggiungi origine dati.
4. Nella pagina Aggiungi origine dati, scegli Microsoft SQL Serverconnettore, quindi scegli Aggiungi connettore.
5. Nella pagina Specificare i dettagli dell'origine dati, inserisci le seguenti informazioni:
   a. In Nome e descrizione, per Nome dell'origine dati, inserisci un nome per l'origine dati. Puoi includere trattini ma non spazi.
   b. (Facoltativo) Descrizione: immetti una descrizione facoltativa per l'origine dati.
   c. In Lingua predefinita: scegli una lingua per filtrare i documenti per l'indice. Se non diversamente specificato, la lingua predefinita è l'inglese. La lingua specificata nei metadati del documento ha la precedenza sulla lingua selezionata.
   d. In Tag, per Aggiungi nuovo tag, includi tag opzionali per cercare e filtrare le risorse o tenere traccia dei costi. AWS
   e. Seleziona Successivo.
6. Nella pagina Definisci accesso e sicurezza, inserisci le seguenti informazioni:
   a. In Source, inserisci le seguenti informazioni:
   b. Host: immettere il nome host del database.
   c. Porta: immettere la porta del database.
   d. Istanza: immettere l'istanza del database.
   e. Abilita la posizione del certificato SSL: scegli di inserire il Amazon S3 percorso del file del certificato SSL.
   f. In Autenticazione, inserisci le seguenti informazioni:
      - AWS Secrets Manager segreto: scegli un segreto esistente o creane uno nuovo Secrets Manager per memorizzare le credenziali di Microsoft SQL Server autenticazione. Se scegli di creare un nuovo segreto, si apre una finestra AWS Secrets Manager segreta.

A. Inserisci le seguenti informazioni nella finestra Crea un AWS Secrets Manager segreto:

I. Nome segreto: un nome per il tuo segreto. Il prefisso 'AmazonKendra-Microsoft SQL Server -' viene aggiunto automaticamente al nome segreto.

II. Per nome utente e password del database, immettete i valori delle credenziali di autenticazione copiati dal database.

B. Selezionare Salva.

g. Virtual Private Cloud (VPC): puoi scegliere di utilizzare un VPC. In tal caso, è necessario aggiungere sottoreti e gruppi di sicurezza VPC.

h. IAM ruolo: scegli un IAM ruolo esistente o creane uno nuovo IAM per accedere alle credenziali del repository e indicizzare il contenuto.

> **Note**
>
> IAM i ruoli utilizzati per gli indici non possono essere utilizzati per le fonti di dati. Se non sei sicuro che un ruolo esistente venga utilizzato per un indice o una FAQ, scegli Crea un nuovo ruolo per evitare errori.

i. Seleziona Successivo.

7. Nella pagina Configura le impostazioni di sincronizzazione, inserisci le seguenti informazioni:

a. Nell'ambito della sincronizzazione, scegli tra le seguenti opzioni:

- Query SQL: immetti istruzioni di query SQL come le operazioni SELECT e JOIN. Le query SQL devono pesare meno di 32 KB. Amazon Kendra eseguirà la scansione di tutto il contenuto del database che corrisponde alla tua query.

> **Note**
>
> Se il nome di una tabella include caratteri speciali (non alfanumerici) nel nome, è necessario utilizzare parentesi quadre attorno al nome della tabella. Ad esempio, `seleziona*` da [] my-database-table

- Colonna chiave primaria: fornisce la chiave primaria per la tabella del database. Identifica una tabella all'interno del database.

- Colonna del titolo: fornisce il nome della colonna del titolo del documento all'interno della tabella del database.
- Colonna del corpo: fornisce il nome della colonna del corpo del documento all'interno della tabella del database.

b. In Configurazione aggiuntiva, facoltativa, scegli una delle seguenti opzioni per sincronizzare contenuti specifici anziché sincronizzare tutti i file:

- Colonne di rilevamento delle modifiche: inserisci i nomi delle colonne che Amazon Kendra verranno utilizzate per rilevare le modifiche al contenuto. Amazon Kendra reindicizzerà il contenuto in caso di modifica in una di queste colonne.
- Colonna ID utente: immetti il nome della colonna che contiene gli ID utente a cui consentire l'accesso ai contenuti.
- Colonna Gruppi: immetti il nome della colonna che contiene i gruppi a cui consentire l'accesso ai contenuti.
- Colonna URL di origine: inserisci il nome della colonna che contiene gli URL di origine da indicizzare.
- Colonna timestamp: immetti il nome della colonna che contiene i timestamp. Amazon Kendra utilizza le informazioni relative alla marca temporale per rilevare le modifiche ai contenuti e sincronizzare solo i contenuti modificati.
- Colonna dei fusi orari: inserisci il nome della colonna che contiene i fusi orari per il contenuto da sottoporre a scansione.
- Formato timestamp: immetti il nome della colonna che contiene i formati di timestamp da utilizzare per rilevare le modifiche ai contenuti e risincronizzare i contenuti.

c. Modalità di sincronizzazione: scegli come aggiornare l'indice quando il contenuto della fonte dati cambia. Quando sincronizzi l'origine dati con Amazon Kendra per la prima volta, tutto il contenuto viene sottoposto a scansione e indicizzato per impostazione predefinita. Se la sincronizzazione iniziale non è riuscita, devi eseguire una sincronizzazione completa dei dati, anche se non scegli la sincronizzazione completa come opzione della modalità di sincronizzazione.

- Sincronizzazione completa: indicizza di nuovo tutti i contenuti, sostituendo i contenuti esistenti ogni volta che l'origine dati si sincronizza con l'indice.
- Nuova sincronizzazione modificata: indicizza solo i contenuti nuovi e modificati ogni volta che l'origine dati si sincronizza con l'indice. Amazon Kendra può utilizzare

il meccanismo dell'origine dati per tenere traccia delle modifiche ai contenuti e indicizzare i contenuti modificati dall'ultima sincronizzazione.

- Sincronizzazione nuova, modificata ed eliminata: indicizza solo i contenuti nuovi, modificati ed eliminati ogni volta che l'origine dati si sincronizza con l'indice. Amazon Kendra può utilizzare il meccanismo dell'origine dati per tenere traccia delle modifiche ai contenuti e indicizzare i contenuti modificati dall'ultima sincronizzazione.

d. Pianificazione di esecuzione di In Sync, per Frequenza: con quale frequenza Amazon Kendra verrà eseguita la sincronizzazione con la fonte di dati.

e. Seleziona Successivo.

8. Nella pagina Imposta mappature dei campi, inserisci le seguenti informazioni:

a. Seleziona uno dei campi di origine dati predefiniti generati (ID documento, titoli dei documenti e URL di origine) che desideri mappare per indicizzare. Amazon Kendra

b. Aggiungi campo: consente di aggiungere campi di origine dati personalizzati per creare un nome di campo indice a cui mappare e il tipo di dati del campo.

c. Seleziona Successivo.

9. Nella pagina Rivedi e crea, verifica che le informazioni inserite siano corrette, quindi seleziona Aggiungi origine dati. Puoi anche scegliere di modificare le tue informazioni da questa pagina. L'origine dati verrà visualizzata nella pagina Origini dati dopo che l'origine dati sarà stata aggiunta correttamente.

API

Per connettersi Amazon Kendra a Microsoft SQL Server

È necessario specificare quanto segue utilizzando l'TemplateConfigurationAPI:

- Origine dati: specifica il tipo di origine dati come `JDBC` quando usi lo schema TemplateConfigurationJSON. Specificate anche l'origine dati come `TEMPLATE` quando chiamate l'CreateDataSourceAPI.
- Tipo di database: è necessario specificare il tipo di database come`sqlserver`.
- Query SQL: specifica le istruzioni di query SQL come le operazioni SELECT e JOIN. Le query SQL devono pesare meno di 32 KB. Amazon Kendra eseguirà la scansione di tutto il contenuto del database che corrisponde alla tua query.

> **Note**
>
> Se il nome di una tabella include caratteri speciali (non alfanumerici) nel nome, è necessario utilizzare parentesi quadre attorno al nome della tabella. Ad esempio, *seleziona** da [] my-database-table

- Modalità di sincronizzazione: specifica come Amazon Kendra aggiornare l'indice quando il contenuto dell'origine dati cambia. Quando sincronizzi l'origine dati con Amazon Kendra per la prima volta, tutto il contenuto viene sottoposto a scansione e indicizzato per impostazione predefinita. Se la sincronizzazione iniziale non è riuscita, devi eseguire una sincronizzazione completa dei dati, anche se non scegli la sincronizzazione completa come opzione della modalità di sincronizzazione. Puoi scegliere tra:
  - `FORCED_FULL_CRAWL`per indicizzare nuovamente tutti i contenuti, sostituendo i contenuti esistenti ogni volta che l'origine dati si sincronizza con l'indice.
  - `FULL_CRAWL`per indicizzare solo i contenuti nuovi, modificati ed eliminati ogni volta che l'origine dati si sincronizza con l'indice. Amazon Kendra può utilizzare il meccanismo dell'origine dati per tenere traccia delle modifiche ai contenuti e indicizzare i contenuti modificati dall'ultima sincronizzazione.
  - `CHANGE_LOG`per indicizzare solo contenuti nuovi e modificati ogni volta che l'origine dati si sincronizza con l'indice. Amazon Kendra può utilizzare il meccanismo dell'origine dati per tenere traccia delle modifiche ai contenuti e indicizzare i contenuti modificati dall'ultima sincronizzazione.
- Amazon Resource Name (ARN) segreto: fornisci l'Amazon Resource Name (ARN) di un Secrets Manager segreto che contiene le credenziali di autenticazione che hai creato nel tuo account. Microsoft SQL Server Il segreto è archiviato in una struttura JSON con le seguenti chiavi:

```
{
    "user name": "database user name",
    "password": "password"
}
```

> **Note**
>
> Ti consigliamo di aggiornare o ruotare regolarmente le credenziali e il segreto. Fornisci solo il livello di accesso necessario per la tua sicurezza. Non è consigliabile riutilizzare

credenziali e segreti tra diverse fonti di dati e versioni dei connettori 1.0 e 2.0 (ove applicabile).

- IAM ruolo: specifica `RoleArn` quando chiami `CreateDataSource` per fornire a un IAM ruolo le autorizzazioni per accedere al tuo Secrets Manager segreto e per chiamare le API pubbliche richieste per il connettore e. Microsoft SQL Server Amazon Kendra Per ulteriori informazioni, consulta i IAM ruoli per Microsoft SQL Server le fonti di dati.

Puoi anche aggiungere le seguenti funzionalità opzionali:

- Virtual Private Cloud (VPC): `VpcConfiguration` specifica quando si chiama. `CreateDataSource` Per ulteriori informazioni, consulta Configurazione Amazon Kendra per l'utilizzo di un Amazon VPC.
- Filtri di inclusione ed esclusione: puoi specificare se includere contenuti specifici utilizzando ID utente, gruppi, URL di origine, timestamp e fusi orari.
- Filtraggio del contesto utente e controllo degli accessi:Amazon Kendra esegue la ricerca per indicizzazione dell'elenco di controllo degli accessi (ACL) dei documenti, se disponi di un ACL per i documenti. Le informazioni ACL vengono utilizzate per filtrare i risultati della ricerca in base all'accesso dell'utente o del relativo gruppo ai documenti. Per ulteriori informazioni, consulta Filtraggio del contesto utente.
- Mappature dei campi: scegli di mappare i campi delle sorgenti Microsoft SQL Server dati ai campi indice. Amazon Kendra Per ulteriori informazioni, consulta la sezione Mappatura dei campi di origine dei dati.

> **Note**
>
> Il campo del corpo del documento o l'equivalente del corpo del documento per i documenti è necessario per Amazon Kendra eseguire la ricerca nei documenti. È necessario mappare il nome del campo del corpo del documento nella fonte dati al nome del campo indice`_document_body`. Tutti gli altri campi sono facoltativi.

Per un elenco di altre importanti chiavi JSON da configurare, consultaSchema del modello di Microsoft SQL Server.

Note

- Le righe del database eliminate non verranno registrate durante la Amazon Kendra verifica della presenza di contenuti aggiornati.
- La dimensione dei nomi e dei valori dei campi in una riga del database non può superare i 400 KB.
- Se l'origine dati del database contiene una grande quantità di dati e non desideri Amazon Kendra indicizzare tutto il contenuto del database dopo la prima sincronizzazione, puoi scegliere di sincronizzare solo i documenti nuovi, modificati o eliminati.
- È consigliabile fornire credenziali Amazon Kendra di database di sola lettura.
- È consigliabile evitare di aggiungere tabelle con dati sensibili o informazioni personali identificabili (PII).

Microsoft Teams

Microsoft Teams è uno strumento di collaborazione aziendale per la messaggistica, le riunioni e la condivisione di file. Se sei un utente di Microsoft Teams, puoi utilizzarlo Amazon Kendra per indicizzare la tua origine dati Microsoft Teams.

Puoi connetterti Amazon Kendra alla tua origine dati Microsoft Teams utilizzando la Amazon Kendra console e l'TemplateConfigurationAPI.

Per la risoluzione dei problemi relativi al connettore di origine dati Amazon Kendra Microsoft Teams, consultaRisoluzione dei problemi relativi alle origini dati.

Argomenti

- Funzionalità supportate
- Prerequisiti
- Istruzioni di connessione
- Ulteriori informazioni

Funzionalità supportate

- Mappature dei campi
- Filtraggio del contesto utente
- Scansione delle identità degli utenti

- Filtri di inclusione/esclusione
- Sincronizzazione completa e incrementale dei contenuti
- Virtual Private Cloud (VPC) (Cloud privato virtuale (VPC)

Prerequisiti

Prima di poterla utilizzare Amazon Kendra per indicizzare l'origine dati di Microsoft Teams, apporta queste modifiche a Microsoft Teams e AWS agli account.

In Microsoft Teams, assicurati di avere:

- Ha creato un account Microsoft Teams in Office 365.
- Ha preso nota del tuo ID tenant di Microsoft 365. Puoi trovare il tuo ID tenant nelle proprietà del tuo portale di Azure Active Directory o nell'applicazione OAuth.
- Ha creato un'applicazione OAuth nel portale di Azure e ha annotato l'ID client e il segreto del client o le credenziali del client. Per ulteriori informazioni, consulta il tutorial Microsoft e l'esempio di app registrata.

  > **Note**
  >
  > Quando crei o registri un'app nel portale di Azure, l'ID segreto rappresenta il valore segreto effettivo. È necessario prendere nota o salvare il valore segreto effettivo immediatamente durante la creazione del segreto e dell'app. Puoi accedere al tuo segreto selezionando il nome dell'applicazione nel portale di Azure e quindi accedendo all'opzione di menu relativa a certificati e segreti.
  > Puoi accedere al tuo ID cliente selezionando il nome dell'applicazione nel portale di Azure e quindi accedendo alla pagina di panoramica. L'ID dell'applicazione (client) è l'ID del client.

- Sono state aggiunte le autorizzazioni necessarie. Puoi scegliere di aggiungere tutte le autorizzazioni oppure puoi limitare l'ambito selezionando un numero inferiore di autorizzazioni in base alle entità che desideri sottoporre a scansione. La tabella seguente elenca le autorizzazioni a livello di applicazione per entità corrispondente:

Entità	Autorizzazioni richieste per la sincronizzazione dei dati	Autorizzazioni richieste per la sincronizzazione delle identità
Channel Post	• ChannelMessage.Leggi tutto • Gruppo. Leggi tutto • Utente.Leggi • Utente.Leggi tutto	TeamMember.Leggi tutto
Allegato al canale	• ChannelMessage.Leggi tutto • Gruppo. Leggi tutto • Utente.Leggi • Utente.Leggi tutto	TeamMember.Leggi tutto
Canale Wiki	• Gruppo. Leggi tutto • Utente.Leggi • Utente.Leggi tutto	TeamMember.Leggi tutto
Messaggio di chat	• Chatta. Leggi tutto • ChatMessage. Leggi tutto • ChatMember.Leggi tutto • Utente.Leggi • Utente.Leggi tutto • Gruppo. Leggi tutto	TeamMember. Leggi tutto
Chat di riunione	• Chatta. Leggi tutto • ChatMessage.Leggi • ChatMember.Leggi tutto • Utente.Leggi • Utente.Leggi tutto • Gruppo. Leggi tutto	TeamMember. Leggi tutto

Entità	Autorizzazioni richieste per la sincronizzazione dei dati	Autorizzazioni richieste per la sincronizzazione delle identità
Allegato alla chat	• Chatta. Leggi tutto • ChatMessage.Leggi • ChatMember.Leggi tutto • Utente.Leggi • Utente.Leggi tutto • Gruppo. Leggi tutto	TeamMember. Leggi tutto
File della riunione	• Chatta. Leggi tutto • ChatMessage. Leggi tutto • ChatMember.Leggi tutto • Utente.Leggi • Utente.Leggi tutto • Gruppo. Leggi tutto • File. Leggi tutto	TeamMember.Leggi tutto
Riunione del calendario	• Chatta. Leggi tutto • ChatMessage. Leggi tutto • ChatMember.Leggi tutto • Utente.Leggi • Utente.Leggi tutto • Gruppo. Leggi tutto • File. Leggi tutto	TeamMember.Leggi tutto
Note sulla riunione	• User.Read • Utente.Leggi tutto • Gruppo. Leggi tutto • File. Leggi tutto	TeamMember.Leggi tutto

- Selezionato, ogni documento è unico in Microsoft Teams e tra le altre fonti di dati che prevedi di utilizzare per lo stesso indice. Ogni fonte di dati che desideri utilizzare per un indice non deve

contenere lo stesso documento in tutte le fonti di dati. Gli ID dei documenti sono globali rispetto a un indice e devono essere univoci per indice.

Nel tuo Account AWS, assicurati di avere:

- Ha creato un Amazon Kendra indice e, se si utilizza l'API, ha annotato l'ID dell'indice.
- Hai creato un IAM ruolo per la tua origine dati e, se utilizzi l'API, hai annotato l'ARN del IAM ruolo.

> **Note**
>
> Se modifichi il tipo di autenticazione e le credenziali, devi aggiornare il IAM ruolo per accedere all'ID AWS Secrets Manager segreto corretto.

- Ha archiviato le credenziali di autenticazione di Microsoft Teams in un AWS Secrets Manager segreto e, se si utilizza l'API, ha annotato l'ARN del segreto.

> **Note**
>
> Ti consigliamo di aggiornare o ruotare regolarmente le credenziali e il segreto. Fornisci solo il livello di accesso necessario per la tua sicurezza. Non è consigliabile riutilizzare credenziali e segreti tra diverse fonti di dati e versioni dei connettori 1.0 e 2.0 (ove applicabile).

Se non disponi di un IAM ruolo o di un segreto esistente, puoi utilizzare la console per creare un nuovo IAM ruolo e un Secrets Manager segreto quando connetti l'origine dati di Microsoft Teams a Amazon Kendra. Se utilizzi l'API, devi fornire l'ARN di un IAM ruolo e di un Secrets Manager segreto esistenti e un ID di indice.

Istruzioni di connessione

Per connetterti Amazon Kendra alla tua origine dati Microsoft Teams, devi fornire i dettagli necessari dell'origine dati Microsoft Teams in modo che Amazon Kendra possa accedere ai tuoi dati. Se non hai ancora configurato Microsoft Teams per Amazon Kendra, vediPrerequisiti.

Console

Per connettersi Amazon Kendra a Microsoft Teams

1. Accedi a AWS Management Console e apri la Amazon Kendra console.
2. Dal riquadro di navigazione a sinistra, scegli Indici, quindi scegli l'indice che desideri utilizzare dall'elenco degli indici.

> **Note**
>
> Puoi scegliere di configurare o modificare le impostazioni del controllo dell'accesso degli utenti in Impostazioni dell'indice.

3. Nella pagina Guida introduttiva, scegli Aggiungi origine dati.
4. Nella pagina Aggiungi origine dati, scegli Connettore Microsoft Teams, quindi scegli Aggiungi connettore.
5. Nella pagina Specificare i dettagli dell'origine dati, inserisci le seguenti informazioni:
   a. In Nome e descrizione, per Nome dell'origine dati, inserisci un nome per l'origine dati. Puoi includere trattini ma non spazi.
   b. (Facoltativo) Descrizione: immetti una descrizione facoltativa per l'origine dati.
   c. In Lingua predefinita: scegli una lingua per filtrare i documenti per l'indice. Se non diversamente specificato, la lingua predefinita è l'inglese. La lingua specificata nei metadati del documento ha la precedenza sulla lingua selezionata.
   d. In Tag, per Aggiungi nuovo tag, includi tag opzionali per cercare e filtrare le risorse o tenere traccia dei costi. AWS
   e. Seleziona Successivo.
6. Nella pagina Definisci accesso e sicurezza, inserisci le seguenti informazioni:
   a. Fonte: inserisci il tuo ID tenant di Microsoft 365. Puoi trovare il tuo ID tenant nelle proprietà del tuo portale di Azure Active Directory o nell'applicazione OAuth.
   b. AWS Secrets Manager segreto: scegli un segreto esistente o crea un nuovo Secrets Manager segreto per archiviare le credenziali di autenticazione di Microsoft Teams. Se scegli di creare un nuovo segreto, si apre una finestra AWS Secrets Manager segreta.
      i. Inserisci le seguenti informazioni nella finestra Crea un AWS Secrets Manager segreto:
         A. Nome segreto: un nome per il tuo segreto. Il prefisso 'AmazonKendra-Microsoft Teams-' viene aggiunto automaticamente al nome segreto.

B. Per Client ID e Client secret: immetti i valori delle credenziali di autenticazione generati nel tuo account Microsoft Teams nel portale di Azure.

ii. Selezionare Salva.

c. Modello di pagamento: puoi scegliere un modello di licenza e pagamento per il tuo account Microsoft Teams. I modelli di pagamento modello A sono limitati alle licenze e ai modelli di pagamento che richiedono la conformità alla sicurezza. I modelli di pagamento modello B sono adatti per licenze e modelli di pagamento che non richiedono la conformità in materia di sicurezza.

d. Virtual Private Cloud (VPC): puoi scegliere di utilizzare un VPC. In tal caso, è necessario aggiungere sottoreti e gruppi di sicurezza VPC.

e. Identity crawler: specifica se attivare il crawler di identità. Amazon Kendra Il crawler di identità utilizza le informazioni dell'elenco di controllo degli accessi (ACL) per i documenti per filtrare i risultati della ricerca in base all'accesso dell'utente o del relativo gruppo ai documenti. Se disponi di un ACL per i tuoi documenti e scegli di utilizzarlo, puoi anche scegliere di attivare il crawler di identità per configurare il filtraggio Amazon Kendra contestuale dell'utente dei risultati di ricerca. Altrimenti, se il crawler di identità è disattivato, tutti i documenti possono essere ricercati pubblicamente. Se desideri utilizzare il controllo degli accessi per i tuoi documenti e il crawler di identità è disattivato, in alternativa puoi utilizzare l'PutPrincipalMappingAPI per caricare le informazioni di accesso di utenti e gruppi per il filtraggio del contesto degli utenti.

f. IAM ruolo: scegli un IAM ruolo esistente o creane uno nuovo IAM per accedere alle credenziali del repository e indicizzare il contenuto.

> **Note**
>
> IAM i ruoli utilizzati per gli indici non possono essere utilizzati per le fonti di dati. Se non sei sicuro che un ruolo esistente venga utilizzato per un indice o una FAQ, scegli Crea un nuovo ruolo per evitare errori.

g. Seleziona Successivo.

7. Nella pagina Configura le impostazioni di sincronizzazione, inserisci le seguenti informazioni:

a. Sincronizza contenuti: seleziona i contenuti da sincronizzare.

b. Configurazione aggiuntiva: puoi opzionalmente utilizzare queste impostazioni per indicizzare determinati contenuti anziché sincronizzare tutti i documenti.

c. Modalità di sincronizzazione: scegli come aggiornare l'indice quando il contenuto della fonte di dati cambia. Quando sincronizzi l'origine dati con Amazon Kendra per la prima volta, tutto il contenuto viene sottoposto a scansione e indicizzato per impostazione predefinita. Se la sincronizzazione iniziale non è riuscita, devi eseguire una sincronizzazione completa dei dati, anche se non scegli la sincronizzazione completa come opzione della modalità di sincronizzazione.

   - Sincronizzazione completa: indicizza di nuovo tutti i contenuti, sostituendo i contenuti esistenti ogni volta che l'origine dati si sincronizza con l'indice.
   - Nuova sincronizzazione modificata: indicizza solo i contenuti nuovi e modificati ogni volta che l'origine dati si sincronizza con l'indice. Amazon Kendra può utilizzare il meccanismo dell'origine dati per tenere traccia delle modifiche ai contenuti e indicizzare i contenuti modificati dall'ultima sincronizzazione.
   - Sincronizzazione nuova, modificata ed eliminata: indicizza solo i contenuti nuovi, modificati ed eliminati ogni volta che l'origine dati si sincronizza con l'indice. Amazon Kendra può utilizzare il meccanismo dell'origine dati per tenere traccia delle modifiche ai contenuti e indicizzare i contenuti modificati dall'ultima sincronizzazione.

8. Nella pagina Imposta mappature dei campi, inserisci le seguenti informazioni:

   a. Campi di origine dati predefiniti: seleziona uno dei campi di origine dati predefiniti Amazon Kendra generati che desideri mappare all'indice.

   b. Aggiungi campo: consente di aggiungere campi di origine dati personalizzati per creare un nome di campo indice a cui mappare e il tipo di dati del campo.

   c. Seleziona Successivo.

9. Nella pagina Rivedi e crea, verifica che le informazioni inserite siano corrette, quindi seleziona Aggiungi origine dati. Puoi anche scegliere di modificare le tue informazioni da questa pagina. L'origine dati verrà visualizzata nella pagina Origini dati dopo che l'origine dati sarà stata aggiunta correttamente.

API

Per connettersi Amazon Kendra a Microsoft Teams

È necessario specificare un codice JSON dello schema dell'origine dati utilizzando l'TemplateConfigurationAPI. È necessario fornire le seguenti informazioni:

- Origine dati: specifica il tipo di origine dati come `MSTEAMS` quando usi lo schema TemplateConfigurationJSON. Specificate anche l'origine dati come `TEMPLATE` quando chiamate l'CreateDataSourceAPI.
- ID tenant: puoi trovare il tuo ID tenant nelle proprietà del tuo portale di Azure Active Directory o nell'applicazione OAuth.
- Modalità di sincronizzazione: specifica come Amazon Kendra aggiornare l'indice quando il contenuto dell'origine dati cambia. Quando sincronizzi l'origine dati con Amazon Kendra per la prima volta, tutto il contenuto viene sottoposto a scansione e indicizzato per impostazione predefinita. Se la sincronizzazione iniziale non è riuscita, devi eseguire una sincronizzazione completa dei dati, anche se non scegli la sincronizzazione completa come opzione della modalità di sincronizzazione. Puoi scegliere tra:
  - `FORCED_FULL_CRAWL`per indicizzare nuovamente tutti i contenuti, sostituendo i contenuti esistenti ogni volta che l'origine dati si sincronizza con l'indice.
  - `FULL_CRAWL`per indicizzare solo i contenuti nuovi, modificati ed eliminati ogni volta che l'origine dati si sincronizza con l'indice. Amazon Kendra può utilizzare il meccanismo dell'origine dati per tenere traccia delle modifiche ai contenuti e indicizzare i contenuti modificati dall'ultima sincronizzazione.
  - `CHANGE_LOG`per indicizzare solo contenuti nuovi e modificati ogni volta che l'origine dati si sincronizza con l'indice. Amazon Kendra può utilizzare il meccanismo dell'origine dati per tenere traccia delle modifiche ai contenuti e indicizzare i contenuti modificati dall'ultima sincronizzazione.
- Secret Amazon Resource Name (ARN): fornisci l'Amazon Resource Name (ARN) di un Secrets Manager segreto che contiene le credenziali di autenticazione per il tuo account Microsoft Teams. Il segreto è archiviato in una struttura JSON con le seguenti chiavi:

```
{
    "clientId": "client ID",
    "clientSecret": "client secret"
}
```

> **Note**
>
> Ti consigliamo di aggiornare o ruotare regolarmente le credenziali e il segreto. Fornisci solo il livello di accesso necessario per la tua sicurezza. Non è consigliabile riutilizzare

credenziali e segreti tra diverse fonti di dati e versioni dei connettori 1.0 e 2.0 (ove applicabile).

- IAM ruolo: specifica `RoleArn` quando chiami `CreateDataSource` per fornire a un IAM ruolo le autorizzazioni per accedere al tuo Secrets Manager segreto e per chiamare le API pubbliche richieste per il connettore Microsoft Teams e. Amazon Kendra Per ulteriori informazioni, consulta IAM i ruoli per le origini dati di Microsoft Teams.

Puoi anche aggiungere le seguenti funzionalità opzionali:

- Virtual Private Cloud (VPC): `VpcConfiguration` specifica quando si chiama. `CreateDataSource` Per ulteriori informazioni, consulta Configurazione Amazon Kendra per l'utilizzo di un Amazon VPC.
- Filtri di inclusione ed esclusione: specifica se includere o escludere determinati contenuti in Microsoft Teams. Puoi includere o escludere nomi di team, nomi di canale, nomi e tipi di file, e-mail degli utenti, OneNote sezioni e OneNote pagine. Puoi anche specificare se indicizzare i messaggi e gli allegati della chat, i post e gli allegati del canale, i wiki del canale, il contenuto del calendario, le chat delle riunioni, i file e le note.

> **Note**
>
> La maggior parte delle fonti di dati utilizza modelli di espressioni regolari, che sono modelli di inclusione o esclusione denominati filtri. Se si specifica un filtro di inclusione, viene indicizzato solo il contenuto che corrisponde al filtro di inclusione. Qualsiasi documento che non corrisponde al filtro di inclusione non viene indicizzato. Se si specifica un filtro di inclusione ed esclusione, i documenti che corrispondono al filtro di esclusione non vengono indicizzati, anche se corrispondono al filtro di inclusione.

- Identity crawler: specifica se attivare il crawler di identità. Amazon Kendra Il crawler di identità utilizza le informazioni dell'elenco di controllo degli accessi (ACL) per i documenti per filtrare i risultati della ricerca in base all'accesso dell'utente o del relativo gruppo ai documenti. Se disponi di un ACL per i tuoi documenti e scegli di utilizzarlo, puoi anche scegliere di attivare il crawler di identità per configurare il filtraggio Amazon Kendra contestuale dell'utente dei risultati di ricerca. Altrimenti, se il crawler di identità è disattivato, tutti i documenti possono essere ricercati pubblicamente. Se desideri utilizzare il controllo degli accessi per i tuoi documenti e il crawler di identità è disattivato, in alternativa puoi utilizzare l'PutPrincipalMappingAPI per caricare le informazioni di accesso di utenti e gruppi per il filtraggio del contesto degli utenti.

- Mappature dei campi: scegli di mappare i campi dell'origine dati di Microsoft Teams ai Amazon Kendra campi indice. Per ulteriori informazioni, consulta la sezione Mappatura dei campi di origine dei dati.

> **Note**
>
> Il campo del corpo del documento o l'equivalente del corpo del documento per i documenti è necessario per Amazon Kendra eseguire la ricerca nei documenti. È necessario mappare il nome del campo del corpo del documento nella fonte dati al nome del campo indice`_document_body`. Tutti gli altri campi sono facoltativi.

Per un elenco di altre importanti chiavi JSON da configurare, consultaSchema del modello Microsoft Teams.

Ulteriori informazioni

Per ulteriori informazioni sull'integrazione Amazon Kendra con l'origine dati Microsoft Teams, consulta:

- Cerca in modo intelligente l'origine dati Microsoft Teams della tua organizzazione con il Amazon Kendra connettore per Microsoft Teams

Microsoft Yammer

Microsoft Yammer è uno strumento di collaborazione aziendale per la messaggistica, le riunioni e la condivisione di file. Se sei un utente di Microsoft Yammer, puoi utilizzarlo Amazon Kendra per indicizzare la tua origine dati Microsoft Yammer.

Puoi connetterti Amazon Kendra alla tua origine dati Microsoft Yammer utilizzando la Amazon Kendra console e l'TemplateConfigurationAPI.

Per la risoluzione dei problemi relativi al connettore di origine dati Amazon Kendra Microsoft Yammer, vedere. Risoluzione dei problemi relativi alle origini dati

Funzionalità supportate

- Mappature dei campi

- Filtri di inclusione/esclusione
- Sincronizzazione completa e incrementale dei contenuti
- Virtual Private Cloud (VPC) (Cloud privato virtuale (VPC)

Prerequisiti

Prima di poterla utilizzare Amazon Kendra per indicizzare l'origine dati Microsoft Yammer, apporta queste modifiche a Microsoft Yammer e agli account. AWS

In Microsoft Yammer, assicurati di avere:

- Ha creato un account amministrativo Microsoft Yammer in Office 365.
- Ha preso nota del nome utente e della password di Microsoft Yammer.
- Ha preso nota del tuo ID tenant di Microsoft 365. Puoi trovare il tuo ID tenant nelle proprietà del tuo portale di Azure Active Directory o nell'applicazione OAuth.
- Ha creato un'applicazione OAuth nel portale di Azure e ha annotato l'ID client e il segreto del client o le credenziali del client. Per ulteriori informazioni, consulta il tutorial Microsoft e l'esempio di app registrata.

  > **Note**
  >
  > Quando crei o registri un'app nel portale di Azure, l'ID segreto rappresenta il valore segreto effettivo. È necessario prendere nota o salvare il valore segreto effettivo immediatamente durante la creazione del segreto e dell'app. Puoi accedere al tuo segreto selezionando il nome dell'applicazione nel portale di Azure e quindi accedendo all'opzione di menu relativa a certificati e segreti.
  > Puoi accedere al tuo ID cliente selezionando il nome dell'applicazione nel portale di Azure e quindi accedendo alla pagina di panoramica. L'ID dell'applicazione (client) è l'ID del client.

- Selezionato, ogni documento è unico in Microsoft Yammer e tra le altre fonti di dati che si prevede di utilizzare per lo stesso indice. Ogni origine dati che si desidera utilizzare per un indice non deve contenere lo stesso documento in tutte le fonti di dati. Gli ID dei documenti sono globali rispetto a un indice e devono essere univoci per indice.

Nel tuo Account AWS, assicurati di avere:

- Ha creato un Amazon Kendra indice e, se si utilizza l'API, ha annotato l'ID dell'indice.
- Hai creato un IAM ruolo per la tua origine dati e, se utilizzi l'API, hai annotato l'ARN del IAM ruolo.

> **Note**
>
> Se modifichi il tipo di autenticazione e le credenziali, devi aggiornare il IAM ruolo per accedere all'ID AWS Secrets Manager segreto corretto.

- Ha archiviato le credenziali di autenticazione di Microsoft Yammer in un AWS Secrets Manager segreto e, se si utilizza l'API, ha annotato l'ARN del segreto.

> **Note**
>
> Ti consigliamo di aggiornare o ruotare regolarmente le credenziali e il segreto. Fornisci solo il livello di accesso necessario per la tua sicurezza. Non è consigliabile riutilizzare credenziali e segreti tra diverse fonti di dati e nelle versioni 1.0 e 2.0 dei connettori (ove applicabile).

Se non disponi di un IAM ruolo o di un segreto esistente, puoi usare la console per creare un nuovo IAM ruolo e Secrets Manager segreto quando connetti l'origine dati Microsoft Yammer a. Amazon Kendra Se utilizzi l'API, devi fornire l'ARN di un IAM ruolo e di un Secrets Manager segreto esistenti e un ID di indice.

Istruzioni di connessione

Per connettersi Amazon Kendra all'origine dati Microsoft Yammer, è necessario fornire i dettagli necessari dell'origine dati Microsoft Yammer in modo che sia Amazon Kendra possibile accedere ai dati. Se non è ancora stato configurato Microsoft Yammer per Amazon Kendra, vedere. Prerequisiti

Console

Per connettersi Amazon Kendra a Microsoft Yammer

1. Accedere a AWS Management Console e aprire la Amazon Kendra console.
2. Dal riquadro di navigazione a sinistra, scegli Indici, quindi scegli l'indice che desideri utilizzare dall'elenco degli indici.

> **Note**
>
> Puoi scegliere di configurare o modificare le impostazioni del controllo dell'accesso degli utenti in Impostazioni dell'indice.

3. Nella pagina Guida introduttiva, scegli Aggiungi origine dati.
4. Nella pagina Aggiungi origine dati, scegli Connettore Microsoft Yammer, quindi scegli Aggiungi connettore.
5. Nella pagina Specificare i dettagli dell'origine dati, inserisci le seguenti informazioni:
   a. In Nome e descrizione, per Nome dell'origine dati, inserisci un nome per l'origine dati. Puoi includere trattini ma non spazi.
   b. (Facoltativo) Descrizione: immetti una descrizione facoltativa per la tua fonte di dati.
   c. In Lingua predefinita: scegli una lingua per filtrare i documenti per l'indice. Se non diversamente specificato, la lingua predefinita è l'inglese. La lingua specificata nei metadati del documento ha la precedenza sulla lingua selezionata.
   d. In Tag, per Aggiungi nuovo tag, includi tag opzionali per cercare e filtrare le risorse o tenere traccia dei costi. AWS
   e. Seleziona Successivo.
6. Nella pagina Definisci accesso e sicurezza, inserisci le seguenti informazioni:
   a. Fonte: usa l'URL di Microsoft Yammer.
   b. AWS Secrets Manager segreto: scegli un segreto esistente o creane uno nuovo Secrets Manager per archiviare le credenziali di autenticazione di Microsoft Yammer. Se scegli di creare un nuovo segreto, si apre una finestra segreta. AWS Secrets Manager
      i. Inserisci le seguenti informazioni nella finestra Crea un AWS Secrets Manager segreto:
         A. Nome segreto: un nome per il tuo segreto. Il prefisso 'AmazonKendra-Microsoft Yammer-' viene aggiunto automaticamente al nome segreto.
         B. Per Nome utente, password: immettere il nome utente e la password di Microsoft Yammer.
         C. Per Client ID, Client secret: immetti i valori delle credenziali di autenticazione generati dal tuo account Microsoft Yammer nel portale di Azure.

ii. Selezionare Salva.

c. Virtual Private Cloud (VPC): puoi scegliere di utilizzare un VPC. In tal caso, è necessario aggiungere sottoreti e gruppi di sicurezza VPC.

d. Identity crawler: specifica se attivare il crawler di identità. Amazon Kendra Il crawler di identità utilizza le informazioni dell'elenco di controllo degli accessi (ACL) per i documenti per filtrare i risultati della ricerca in base all'accesso dell'utente o del gruppo di appartenenza ai documenti. Se disponi di un ACL per i tuoi documenti e scegli di utilizzarlo, puoi anche scegliere di attivare il crawler di identità per configurare il filtraggio Amazon Kendra contestuale dell'utente dei risultati di ricerca. Altrimenti, se il crawler di identità è disattivato, tutti i documenti possono essere ricercati pubblicamente. Se desideri utilizzare il controllo degli accessi per i tuoi documenti e il crawler di identità è disattivato, in alternativa puoi utilizzare l'PutPrincipalMappingAPI per caricare le informazioni di accesso di utenti e gruppi per il filtraggio del contesto degli utenti.

e. IAM ruolo: scegli un IAM ruolo esistente o creane uno nuovo IAM per accedere alle credenziali del repository e indicizzare il contenuto.

> **Note**
>
> IAM i ruoli utilizzati per gli indici non possono essere utilizzati per le fonti di dati. Se non sei sicuro che un ruolo esistente venga utilizzato per un indice o una FAQ, scegli Crea un nuovo ruolo per evitare errori.

f. Seleziona Successivo.

7. Nella pagina Configura le impostazioni di sincronizzazione, inserisci le seguenti informazioni:

a. Data di inizio: specifica la data di inizio della scansione dei dati in Microsoft Yammer.

b. Sincronizzazione dei contenuti: seleziona il tipo di contenuto che desideri indicizzare. Ad esempio, messaggi pubblici, messaggi privati e allegati.

c. Configurazione aggiuntiva: è possibile utilizzare facoltativamente queste opzioni per indicizzare determinati contenuti anziché sincronizzare tutti i documenti. Ad esempio, è possibile indicizzare nomi di comunità specifici e utilizzare modelli di espressioni regolari per includere o escludere determinati file.

d. Modalità di sincronizzazione: scegli come aggiornare l'indice quando il contenuto dell'origine dati cambia. Quando sincronizzi l'origine dati con Amazon Kendra per la prima volta, tutto il contenuto viene sottoposto a scansione e indicizzato per impostazione predefinita. Se la sincronizzazione iniziale non è riuscita, devi eseguire una

sincronizzazione completa dei dati, anche se non scegli la sincronizzazione completa come opzione della modalità di sincronizzazione.

- Sincronizzazione completa: indicizza di nuovo tutti i contenuti, sostituendo i contenuti esistenti ogni volta che l'origine dati si sincronizza con l'indice.
- Nuova sincronizzazione modificata: indicizza solo i contenuti nuovi e modificati ogni volta che l'origine dati si sincronizza con l'indice. Amazon Kendra può utilizzare il meccanismo dell'origine dati per tenere traccia delle modifiche ai contenuti e indicizzare i contenuti modificati dall'ultima sincronizzazione.
- Sincronizzazione nuova, modificata ed eliminata: indicizza solo i contenuti nuovi, modificati ed eliminati ogni volta che l'origine dati si sincronizza con l'indice. Amazon Kendra può utilizzare il meccanismo dell'origine dati per tenere traccia delle modifiche ai contenuti e indicizzare i contenuti modificati dall'ultima sincronizzazione.

8. Nella pagina Imposta mappature dei campi, inserisci le seguenti informazioni:

   a. Campi di origine dati predefiniti: seleziona uno dei campi di origine dati predefiniti Amazon Kendra generati che desideri mappare all'indice.

   b. Aggiungi campo: consente di aggiungere campi di origine dati personalizzati per creare un nome di campo indice a cui mappare e il tipo di dati del campo.

   c. Seleziona Successivo.

9. Nella pagina Rivedi e crea, verifica che le informazioni inserite siano corrette, quindi seleziona Aggiungi origine dati. Puoi anche scegliere di modificare le tue informazioni da questa pagina. L'origine dati verrà visualizzata nella pagina Origini dati dopo che l'origine dati sarà stata aggiunta correttamente.

API

Per connettersi Amazon Kendra a Microsoft Yammer

È necessario specificare un codice JSON dello schema dell'origine dati utilizzando l'API. TemplateConfiguration È necessario fornire le seguenti informazioni:

- Origine dati: specifica il tipo di origine dati come `YAMMER` quando usi lo schema TemplateConfigurationJSON. Specificate anche l'origine dati come `TEMPLATE` quando chiamate l'CreateDataSourceAPI.
- Modalità di sincronizzazione: specifica come Amazon Kendra aggiornare l'indice quando il contenuto dell'origine dati cambia. Quando sincronizzi l'origine dati con Amazon Kendra per

la prima volta, tutto il contenuto viene sottoposto a scansione e indicizzato per impostazione predefinita. Se la sincronizzazione iniziale non è riuscita, devi eseguire una sincronizzazione completa dei dati, anche se non scegli la sincronizzazione completa come opzione della modalità di sincronizzazione. Puoi scegliere tra:

- `FORCED_FULL_CRAWL`per indicizzare nuovamente tutti i contenuti, sostituendo i contenuti esistenti ogni volta che l'origine dati si sincronizza con l'indice.
- `FULL_CRAWL`per indicizzare solo i contenuti nuovi, modificati ed eliminati ogni volta che l'origine dati si sincronizza con l'indice. Amazon Kendra può utilizzare il meccanismo dell'origine dati per tenere traccia delle modifiche ai contenuti e indicizzare i contenuti modificati dall'ultima sincronizzazione.
- `CHANGE_LOG`per indicizzare solo contenuti nuovi e modificati ogni volta che l'origine dati si sincronizza con l'indice. Amazon Kendra può utilizzare il meccanismo dell'origine dati per tenere traccia delle modifiche ai contenuti e indicizzare i contenuti modificati dall'ultima sincronizzazione.

- Secret Amazon Resource Name (ARN): fornisci l'Amazon Resource Name (ARN) di un Secrets Manager segreto che contiene le credenziali di autenticazione per il tuo account Microsoft Yammer. Il segreto è archiviato in una struttura JSON con le seguenti chiavi:

```
{
    "username": "user name",
    "password": "password",
    "clientId": "client ID",
    "clientSecret": "client secret"
}
```

> **Note**
>
> Ti consigliamo di aggiornare o ruotare regolarmente le credenziali e il segreto. Fornisci solo il livello di accesso necessario per la tua sicurezza. Non è consigliabile riutilizzare credenziali e segreti tra diverse fonti di dati e nelle versioni 1.0 e 2.0 dei connettori (ove applicabile).

- IAM ruolo: specifica `RoleArn` quando chiami `CreateDataSource` per fornire a un IAM ruolo le autorizzazioni per accedere al tuo Secrets Manager segreto e per chiamare le API pubbliche richieste per il connettore Microsoft Yammer e. Amazon Kendra Per ulteriori informazioni, vedi IAM ruoli per le origini dati Microsoft Yammer.

È inoltre possibile aggiungere le seguenti funzionalità opzionali:

- Virtual Private Cloud (VPC): `VpcConfiguration` specifica quando si chiama. `CreateDataSource` Per ulteriori informazioni, consulta Configurazione Amazon Kendra per l'utilizzo di un Amazon VPC.
- Filtri di inclusione ed esclusione: specificano se includere o escludere determinati contenuti.

> **Note**
>
> La maggior parte delle fonti di dati utilizza modelli di espressioni regolari, che sono modelli di inclusione o esclusione denominati filtri. Se si specifica un filtro di inclusione, viene indicizzato solo il contenuto che corrisponde al filtro di inclusione. Qualsiasi documento che non corrisponde al filtro di inclusione non viene indicizzato. Se si specifica un filtro di inclusione ed esclusione, i documenti che corrispondono al filtro di esclusione non vengono indicizzati, anche se corrispondono al filtro di inclusione.

- Identity crawler: specifica se attivare il crawler di identità. Amazon Kendra Il crawler di identità utilizza le informazioni dell'elenco di controllo degli accessi (ACL) per i documenti per filtrare i risultati della ricerca in base all'accesso dell'utente o del gruppo di appartenenza ai documenti. Se disponi di un ACL per i tuoi documenti e scegli di utilizzarlo, puoi anche scegliere di attivare il crawler di identità per configurare il filtraggio Amazon Kendra contestuale dell'utente dei risultati di ricerca. Altrimenti, se il crawler di identità è disattivato, tutti i documenti possono essere ricercati pubblicamente. Se desideri utilizzare il controllo degli accessi per i tuoi documenti e il crawler di identità è disattivato, in alternativa puoi utilizzare l'PutPrincipalMappingAPI per caricare le informazioni di accesso di utenti e gruppi per il filtraggio del contesto degli utenti.
- Mappature dei campi: scegliere di mappare i campi dell'origine dati di Microsoft Yammer ai campi indice. Amazon Kendra Per ulteriori informazioni, consulta la sezione Mappatura dei campi di origine dei dati.

> **Note**
>
> Il campo del corpo del documento o l'equivalente del corpo del documento per i documenti è necessario per eseguire la ricerca nei documenti. Amazon Kendra È necessario mappare il nome del campo del corpo del documento nella fonte dati al nome del campo indice`_document_body`. Tutti gli altri campi sono facoltativi.

Ulteriori informazioni

Per ulteriori informazioni sull'integrazione Amazon Kendra con l'origine dati Microsoft Yammer, vedi:

- Annuncio del connettore Yammer per Amazon Kendra

MySQL

MySQLè un sistema di gestione di database relazionali open source. Se sei un MySQL utente, puoi utilizzarlo Amazon Kendra per indicizzare la tua fonte di MySQL dati. Il connettore di origine Amazon Kendra MySQL dati supporta MySQL 8.0. 21.

Puoi connetterti Amazon Kendra alla tua fonte di MySQL dati utilizzando la Amazon Kendra console e l'API. TemplateConfiguration

Per la risoluzione dei problemi relativi al connettore della sorgente Amazon Kendra MySQL dati, consultaRisoluzione dei problemi relativi alle origini dati.

Argomenti

- Funzionalità supportate
- Prerequisiti
- Istruzioni di connessione
- Note

Funzionalità supportate

- Mappature dei campi
- Filtraggio del contesto utente
- Filtri di inclusione/esclusione
- Sincronizzazione completa e incrementale dei contenuti
- Virtual Private Cloud (VPC) (Cloud privato virtuale (VPC)

Prerequisiti

Prima di poterla utilizzare Amazon Kendra per indicizzare la tua fonte di MySQL dati, apporta queste modifiche al tuo account MySQL e AWS ai tuoi account.

NelMySQL, assicurati di avere:

- Hai annotato il nome utente e la password del database.

> **Important**
>
> È consigliabile fornire credenziali Amazon Kendra di database di sola lettura.

- Hai copiato l'URL, la porta e l'istanza dell'host del database.
- È stato verificato che ogni documento sia unico all'interno MySQL e tra le altre fonti di dati che intendi utilizzare per lo stesso indice. Ogni fonte di dati che desideri utilizzare per un indice non deve contenere lo stesso documento in tutte le fonti di dati. Gli ID dei documenti sono globali rispetto a un indice e devono essere univoci per indice.

Nel tuo Account AWS, assicurati di avere:

- Ha creato un Amazon Kendra indice e, se si utilizza l'API, ha annotato l'ID dell'indice.
- Hai creato un IAM ruolo per la tua origine dati e, se utilizzi l'API, hai annotato l'ARN del IAM ruolo.

> **Note**
>
> Se modifichi il tipo di autenticazione e le credenziali, devi aggiornare il IAM ruolo per accedere all'ID AWS Secrets Manager segreto corretto.

- Ha archiviato le credenziali di MySQL autenticazione in un AWS Secrets Manager segreto e, se si utilizza l'API, ha annotato l'ARN del segreto.

> **Note**
>
> Ti consigliamo di aggiornare o ruotare regolarmente le credenziali e il segreto. Fornisci solo il livello di accesso necessario per la tua sicurezza. Non è consigliabile riutilizzare credenziali e segreti tra diverse fonti di dati e versioni dei connettori 1.0 e 2.0 (ove applicabile).

Se non disponi di un IAM ruolo o di un segreto esistente, puoi utilizzare la console per creare un nuovo IAM ruolo e un Secrets Manager segreto quando connetti la tua origine MySQL dati a. Amazon

Kendra Se utilizzi l'API, devi fornire l'ARN di un IAM ruolo e di un Secrets Manager segreto esistenti e un ID di indice.

Istruzioni di connessione

Per connetterti Amazon Kendra alla tua fonte di MySQL dati devi fornire i dettagli delle tue MySQL credenziali in modo da Amazon Kendra poter accedere ai tuoi dati. Se non lo hai ancora configurato, MySQL Amazon Kendra Prerequisiti consulta.

Console

Per connettersi Amazon Kendra a MySQL

1. Accedi a AWS Management Console e apri la Amazon Kendra console.
2. Dal riquadro di navigazione a sinistra, scegli Indici, quindi scegli l'indice che desideri utilizzare dall'elenco degli indici.

> **Note**
>
> Puoi scegliere di configurare o modificare le impostazioni del controllo dell'accesso degli utenti in Impostazioni dell'indice.

3. Nella pagina Guida introduttiva, scegli Aggiungi origine dati.
4. Nella pagina Aggiungi origine dati, scegli MySQLconnettore, quindi scegli Aggiungi connettore.
5. Nella pagina Specificare i dettagli dell'origine dati, inserisci le seguenti informazioni:
   a. In Nome e descrizione, per Nome dell'origine dati, inserisci un nome per l'origine dati. Puoi includere trattini ma non spazi.
   b. (Facoltativo) Descrizione: immetti una descrizione facoltativa per la tua fonte di dati.
   c. In Lingua predefinita: scegli una lingua per filtrare i documenti per l'indice. Se non diversamente specificato, la lingua predefinita è l'inglese. La lingua specificata nei metadati del documento ha la precedenza sulla lingua selezionata.
   d. In Tag, per Aggiungi nuovo tag, includi tag opzionali per cercare e filtrare le risorse o tenere traccia dei costi. AWS
   e. Seleziona Successivo.
6. Nella pagina Definisci accesso e sicurezza, inserisci le seguenti informazioni:

a. In Source, inserisci le seguenti informazioni:

b. Host: immettere il nome host del database.

c. Porta: immettere la porta del database.

d. Istanza: immettere l'istanza del database.

e. Abilita la posizione del certificato SSL: scegli di inserire il Amazon S3 percorso del file del certificato SSL.

f. In Autenticazione, inserisci le seguenti informazioni:

- AWS Secrets Manager segreto: scegli un segreto esistente o creane uno nuovo Secrets Manager per memorizzare le credenziali di MySQL autenticazione. Se scegli di creare un nuovo segreto, si apre una finestra AWS Secrets Manager segreta.

  A. Inserisci le seguenti informazioni nella finestra Crea un AWS Secrets Manager segreto:

     I. Nome segreto: un nome per il tuo segreto. Il prefisso 'AmazonKendra-MySQL -' viene aggiunto automaticamente al nome segreto.

     II. Per nome utente e password del database, immettete i valori delle credenziali di autenticazione copiati dal database.

  B. Selezionare Salva.

g. Virtual Private Cloud (VPC): puoi scegliere di utilizzare un VPC. In tal caso, è necessario aggiungere sottoreti e gruppi di sicurezza VPC.

h. IAM ruolo: scegli un IAM ruolo esistente o creane uno nuovo IAM per accedere alle credenziali del repository e indicizzare il contenuto.

> **Note**
>
> IAM i ruoli utilizzati per gli indici non possono essere utilizzati per le fonti di dati. Se non sei sicuro che un ruolo esistente venga utilizzato per un indice o una FAQ, scegli Crea un nuovo ruolo per evitare errori.

i. Seleziona Successivo.

7. Nella pagina Configura le impostazioni di sincronizzazione, inserisci le seguenti informazioni:

a. Nell'ambito della sincronizzazione, scegli tra le seguenti opzioni:

- Query SQL: immetti istruzioni di query SQL come le operazioni SELECT e JOIN. Le query SQL devono pesare meno di 32 KB. Amazon Kendra eseguirà la scansione di tutto il contenuto del database che corrisponde alla tua query.
- Colonna chiave primaria: fornisce la chiave primaria per la tabella del database. Identifica una tabella all'interno del database.
- Colonna del titolo: fornisce il nome della colonna del titolo del documento all'interno della tabella del database.
- Colonna del corpo: fornisce il nome della colonna del corpo del documento all'interno della tabella del database.

b. In Configurazione aggiuntiva, facoltativa, scegli una delle seguenti opzioni per sincronizzare contenuti specifici anziché sincronizzare tutti i file:

- Colonne di rilevamento delle modifiche: immetti i nomi delle colonne che Amazon Kendra verranno utilizzate per rilevare le modifiche al contenuto. Amazon Kendra reindicizzerà il contenuto quando viene apportata una modifica in una di queste colonne.
- Colonna ID utenti: immetti il nome della colonna che contiene gli ID utente a cui consentire l'accesso ai contenuti.
- Colonna Gruppi: immetti il nome della colonna che contiene i gruppi a cui consentire l'accesso ai contenuti.
- Colonna URL di origine: inserisci il nome della colonna che contiene gli URL di origine da indicizzare.
- Colonna timestamp: immetti il nome della colonna che contiene i timestamp. Amazon Kendra utilizza le informazioni relative alla marca temporale per rilevare le modifiche ai contenuti e sincronizzare solo i contenuti modificati.
- Colonna dei fusi orari: inserisci il nome della colonna che contiene i fusi orari per il contenuto da sottoporre a scansione.
- Formato timestamp: immetti il nome della colonna che contiene i formati di timestamp da utilizzare per rilevare le modifiche ai contenuti e risincronizzare i contenuti.

c. Modalità di sincronizzazione: scegli come aggiornare l'indice quando il contenuto della fonte dati cambia. Quando sincronizzi l'origine dati con Amazon Kendra per la prima volta, tutto il contenuto viene sottoposto a scansione e indicizzato per impostazione predefinita. Se la sincronizzazione iniziale non è riuscita, devi eseguire una

sincronizzazione completa dei dati, anche se non scegli la sincronizzazione completa come opzione della modalità di sincronizzazione.

- Sincronizzazione completa: indicizza di nuovo tutti i contenuti, sostituendo i contenuti esistenti ogni volta che l'origine dati si sincronizza con l'indice.
- Sincronizzazione nuova e modificata: indicizza solo i contenuti nuovi e modificati ogni volta che l'origine dati si sincronizza con l'indice. Amazon Kendra può utilizzare il meccanismo dell'origine dati per tenere traccia delle modifiche ai contenuti e indicizzare i contenuti modificati dall'ultima sincronizzazione.
- Sincronizzazione nuova, modificata ed eliminata: indicizza solo i contenuti nuovi, modificati ed eliminati ogni volta che l'origine dati si sincronizza con l'indice. Amazon Kendra può utilizzare il meccanismo dell'origine dati per tenere traccia delle modifiche ai contenuti e indicizzare i contenuti modificati dall'ultima sincronizzazione.

d. Pianificazione di esecuzione di In Sync, per Frequenza: con quale frequenza Amazon Kendra verrà eseguita la sincronizzazione con la fonte di dati.

e. Seleziona Successivo.

8. Nella pagina Imposta le mappature dei campi, inserisci le seguenti informazioni:

a. Seleziona uno dei campi di origine dati predefiniti generati (ID documento, titoli dei documenti e URL di origine) che desideri mappare per indicizzare. Amazon Kendra

b. Aggiungi campo: consente di aggiungere campi di origine dati personalizzati per creare un nome di campo indice a cui mappare e il tipo di dati del campo.

c. Seleziona Successivo.

9. Nella pagina Rivedi e crea, verifica che le informazioni inserite siano corrette, quindi seleziona Aggiungi origine dati. Puoi anche scegliere di modificare le tue informazioni da questa pagina. L'origine dati verrà visualizzata nella pagina Origini dati dopo che l'origine dati sarà stata aggiunta correttamente.

API

Per connettersi Amazon Kendra a MySQL

È necessario specificare quanto segue utilizzando l'TemplateConfigurationAPI:

- Origine dati: specifica il tipo di origine dati come `JDBC` quando usi lo schema TemplateConfigurationJSON. Specificate anche l'origine dati come `TEMPLATE` quando chiamate l'CreateDataSourceAPI.
- Tipo di database: è necessario specificare il tipo di database come`mySql`.
- Query SQL: specifica le istruzioni di query SQL come le operazioni SELECT e JOIN. Le query SQL devono pesare meno di 32 KB. Amazon Kendra eseguirà la scansione di tutto il contenuto del database che corrisponde alla tua query.
- Modalità di sincronizzazione: specifica come Amazon Kendra aggiornare l'indice quando il contenuto dell'origine dati cambia. Quando sincronizzi l'origine dati con Amazon Kendra per la prima volta, tutto il contenuto viene sottoposto a scansione e indicizzato per impostazione predefinita. Se la sincronizzazione iniziale non è riuscita, devi eseguire una sincronizzazione completa dei dati, anche se non scegli la sincronizzazione completa come opzione della modalità di sincronizzazione. Puoi scegliere tra:
  - `FORCED_FULL_CRAWL`per indicizzare nuovamente tutti i contenuti, sostituendo i contenuti esistenti ogni volta che l'origine dati si sincronizza con l'indice.
  - `FULL_CRAWL`per indicizzare solo i contenuti nuovi, modificati ed eliminati ogni volta che l'origine dati si sincronizza con l'indice. Amazon Kendra può utilizzare il meccanismo dell'origine dati per tenere traccia delle modifiche ai contenuti e indicizzare i contenuti modificati dall'ultima sincronizzazione.
  - `CHANGE_LOG`per indicizzare solo contenuti nuovi e modificati ogni volta che l'origine dati si sincronizza con l'indice. Amazon Kendra può utilizzare il meccanismo dell'origine dati per tenere traccia delle modifiche ai contenuti e indicizzare i contenuti modificati dall'ultima sincronizzazione.
- Amazon Resource Name (ARN) segreto: fornisci l'Amazon Resource Name (ARN) di un Secrets Manager segreto che contiene le credenziali di autenticazione che hai creato nel tuo account. MySQL Il segreto è archiviato in una struttura JSON con le seguenti chiavi:

```
{
    "user name": "database user name",
    "password": "password"
}
```

> **Note**
>
> Ti consigliamo di aggiornare o ruotare regolarmente le credenziali e il segreto. Fornisci solo il livello di accesso necessario per la tua sicurezza. Non è consigliabile riutilizzare

credenziali e segreti tra diverse fonti di dati e versioni dei connettori 1.0 e 2.0 (ove applicabile).

- IAM ruolo: specifica `RoleArn` quando chiami `CreateDataSource` per fornire a un IAM ruolo le autorizzazioni per accedere al tuo Secrets Manager segreto e per chiamare le API pubbliche richieste per il connettore e. MySQL Amazon Kendra Per ulteriori informazioni, consulta i IAM ruoli per MySQL le fonti di dati.

Puoi anche aggiungere le seguenti funzionalità opzionali:

- Virtual Private Cloud (VPC): `VpcConfiguration` specifica quando si chiama. `CreateDataSource` Per ulteriori informazioni, consulta Configurazione Amazon Kendra per l'utilizzo di un Amazon VPC.
- Filtri di inclusione ed esclusione: puoi specificare se includere contenuti specifici utilizzando ID utente, gruppi, URL di origine, timestamp e fusi orari.
- Filtraggio del contesto utente e controllo degli accessi:Amazon Kendra esegue la ricerca per indicizzazione dell'elenco di controllo degli accessi (ACL) dei documenti, se disponi di un ACL per i documenti. Le informazioni ACL vengono utilizzate per filtrare i risultati della ricerca in base all'accesso dell'utente o del relativo gruppo ai documenti. Per ulteriori informazioni, consulta Filtraggio del contesto utente.
- Mappature dei campi: scegli di mappare i campi delle sorgenti MySQL dati ai campi indice. Amazon Kendra Per ulteriori informazioni, consulta la sezione Mappatura dei campi di origine dei dati.

> **Note**
>
> Il campo del corpo del documento o l'equivalente del corpo del documento per i documenti è necessario per Amazon Kendra eseguire la ricerca nei documenti. È necessario mappare il nome del campo del corpo del documento nella fonte dati al nome del campo indice_`document_body`. Tutti gli altri campi sono facoltativi.

Note

- Le righe del database eliminate non verranno registrate durante la Amazon Kendra verifica della presenza di contenuti aggiornati.

- La dimensione dei nomi e dei valori dei campi in una riga del database non può superare i 400 KB.
- Se l'origine dati del database contiene una grande quantità di dati e non desideri Amazon Kendra indicizzare tutto il contenuto del database dopo la prima sincronizzazione, puoi scegliere di sincronizzare solo i documenti nuovi, modificati o eliminati.
- È consigliabile fornire credenziali Amazon Kendra di database di sola lettura.
- È consigliabile evitare di aggiungere tabelle con dati sensibili o informazioni personali identificabili (PII).

Oracle Database

Oracle Databaseè un sistema di gestione di database. Se sei un Oracle Database utente, puoi usarlo Amazon Kendra per indicizzare la tua fonte di Oracle Database dati. Il connettore di origine Amazon Kendra Oracle Database dati supporta Oracle Database 18c, 19c e 21c.

Puoi connetterti Amazon Kendra alla tua fonte di Oracle Database dati utilizzando la Amazon Kendra console e l'API. TemplateConfiguration

Per la risoluzione dei problemi relativi al connettore della sorgente Amazon Kendra Oracle Database dati, consultaRisoluzione dei problemi relativi alle origini dati.

Argomenti

- Funzionalità supportate
- Prerequisiti
- Istruzioni di connessione
- Note

Funzionalità supportate

- Mappature dei campi
- Filtraggio del contesto utente
- Filtri di inclusione/esclusione
- Sincronizzazione completa e incrementale dei contenuti
- Virtual Private Cloud (VPC) (Cloud privato virtuale (VPC)

Prerequisiti

Prima di poterla utilizzare Amazon Kendra per indicizzare la tua fonte di Oracle Database dati, apporta queste modifiche al tuo account Oracle Database e AWS ai tuoi account.

NelOracle Database, assicurati di avere:

- Hai annotato il nome utente e la password del database.

> **Important**
>
> È consigliabile fornire credenziali Amazon Kendra di database di sola lettura.

- Hai copiato l'URL, la porta e l'istanza dell'host del database.
- È stato verificato che ogni documento sia unico all'interno Oracle Database e tra le altre fonti di dati che intendi utilizzare per lo stesso indice. Ogni fonte di dati che desideri utilizzare per un indice non deve contenere lo stesso documento in tutte le fonti di dati. Gli ID dei documenti sono globali rispetto a un indice e devono essere univoci per indice.

Nel tuo Account AWS, assicurati di avere:

- Ha creato un Amazon Kendra indice e, se si utilizza l'API, ha annotato l'ID dell'indice.
- Hai creato un IAM ruolo per la tua origine dati e, se utilizzi l'API, hai annotato l'ARN del IAM ruolo.

> **Note**
>
> Se modifichi il tipo di autenticazione e le credenziali, devi aggiornare il IAM ruolo per accedere all'ID AWS Secrets Manager segreto corretto.

- Ha archiviato le credenziali di Oracle Database autenticazione in un AWS Secrets Manager segreto e, se si utilizza l'API, ha annotato l'ARN del segreto.

> **Note**
>
> Ti consigliamo di aggiornare o ruotare regolarmente le credenziali e il segreto. Fornisci solo il livello di accesso necessario per la tua sicurezza. Non è consigliabile riutilizzare credenziali e segreti tra diverse fonti di dati e nelle versioni 1.0 e 2.0 dei connettori (ove applicabile).

Se non disponi di un IAM ruolo o di un segreto esistente, puoi utilizzare la console per creare un nuovo IAM ruolo e un Secrets Manager segreto quando connetti la tua origine Oracle Database dati a. Amazon Kendra Se utilizzi l'API, devi fornire l'ARN di un IAM ruolo e di un Secrets Manager segreto esistenti e un ID di indice.

Istruzioni di connessione

Per connetterti Amazon Kendra alla tua fonte di Oracle Database dati devi fornire i dettagli delle tue Oracle Database credenziali in modo da Amazon Kendra poter accedere ai tuoi dati. Se non lo hai ancora configurato, Oracle Database Amazon Kendra Prerequisiti consulta.

Console

Per connettersi Amazon Kendra a Oracle Database

1. Accedi a AWS Management Console e apri la Amazon Kendra console.
2. Dal riquadro di navigazione a sinistra, scegli Indici, quindi scegli l'indice che desideri utilizzare dall'elenco degli indici.

   > **Note**
   >
   > Puoi scegliere di configurare o modificare le impostazioni del controllo dell'accesso degli utenti in Impostazioni dell'indice.

3. Nella pagina Guida introduttiva, scegli Aggiungi origine dati.
4. Nella pagina Aggiungi origine dati, scegli Oracle Databaseconnettore, quindi scegli Aggiungi connettore.
5. Nella pagina Specificare i dettagli dell'origine dati, inserisci le seguenti informazioni:

   a. In Nome e descrizione, per Nome dell'origine dati, inserisci un nome per l'origine dati. Puoi includere trattini ma non spazi.
   b. (Facoltativo) Descrizione: immetti una descrizione facoltativa per l'origine dati.
   c. In Lingua predefinita: scegli una lingua per filtrare i documenti per l'indice. Se non diversamente specificato, la lingua predefinita è l'inglese. La lingua specificata nei metadati del documento ha la precedenza sulla lingua selezionata.
   d. In Tag, per Aggiungi nuovo tag, includi tag opzionali per cercare e filtrare le risorse o tenere traccia dei costi. AWS
   e. Seleziona Successivo.

6. Nella pagina Definisci accesso e sicurezza, inserisci le seguenti informazioni:

   a. In Source, inserisci le seguenti informazioni:

   b. Host: immettere il nome host del database.

   c. Porta: immettere la porta del database.

   d. Istanza: immettere l'istanza del database.

   e. Abilita la posizione del certificato SSL: scegli di inserire il Amazon S3 percorso del file del certificato SSL.

   f. In Autenticazione, inserisci le seguenti informazioni:

      - AWS Secrets Manager segreto: scegli un segreto esistente o creane uno nuovo Secrets Manager per memorizzare le credenziali di Oracle Database autenticazione. Se scegli di creare un nuovo segreto, si apre una finestra AWS Secrets Manager segreta.

        A. Inserisci le seguenti informazioni nella finestra Crea un AWS Secrets Manager segreto:

           I. Nome segreto: un nome per il tuo segreto. Il prefisso 'AmazonKendra-Oracle Database -' viene aggiunto automaticamente al nome segreto.

           II. Per nome utente e password del database, immettete i valori delle credenziali di autenticazione copiati dal database.

        B. Selezionare Salva.

   g. Virtual Private Cloud (VPC): puoi scegliere di utilizzare un VPC. In tal caso, è necessario aggiungere sottoreti e gruppi di sicurezza VPC.

   h. IAM ruolo: scegli un IAM ruolo esistente o creane uno nuovo IAM per accedere alle credenziali del repository e indicizzare il contenuto.

      > **Note**
      >
      > IAM i ruoli utilizzati per gli indici non possono essere utilizzati per le fonti di dati. Se non sei sicuro che un ruolo esistente venga utilizzato per un indice o una FAQ, scegli Crea un nuovo ruolo per evitare errori.

   i. Seleziona Successivo.

7. Nella pagina Configura le impostazioni di sincronizzazione, inserisci le seguenti informazioni:

a. Nell'ambito della sincronizzazione, scegli tra le seguenti opzioni:

   - Query SQL: immetti istruzioni di query SQL come le operazioni SELECT e JOIN. Le query SQL devono pesare meno di 32 KB. Amazon Kendra eseguirà la scansione di tutto il contenuto del database che corrisponde alla tua query.
   - Colonna chiave primaria: fornisce la chiave primaria per la tabella del database. Identifica una tabella all'interno del database.
   - Colonna del titolo: fornisce il nome della colonna del titolo del documento all'interno della tabella del database.
   - Colonna del corpo: fornisce il nome della colonna del corpo del documento all'interno della tabella del database.

b. In Configurazione aggiuntiva, facoltativa, scegli una delle seguenti opzioni per sincronizzare contenuti specifici anziché sincronizzare tutti i file:

   - Colonne di rilevamento delle modifiche: immetti i nomi delle colonne che Amazon Kendra verranno utilizzate per rilevare le modifiche al contenuto. Amazon Kendra reindicizzerà il contenuto quando viene apportata una modifica in una di queste colonne.
   - Colonna ID utente: immetti il nome della colonna che contiene gli ID utente a cui consentire l'accesso ai contenuti.
   - Colonna Gruppi: immetti il nome della colonna che contiene i gruppi a cui consentire l'accesso ai contenuti.
   - Colonna URL di origine: inserisci il nome della colonna che contiene gli URL di origine da indicizzare.
   - Colonna timestamp: immetti il nome della colonna che contiene i timestamp. Amazon Kendra utilizza le informazioni relative alla marca temporale per rilevare le modifiche ai contenuti e sincronizzare solo i contenuti modificati.
   - Colonna dei fusi orari: inserisci il nome della colonna che contiene i fusi orari per il contenuto da sottoporre a scansione.
   - Formato timestamp: immetti il nome della colonna che contiene i formati di timestamp da utilizzare per rilevare le modifiche ai contenuti e risincronizzare i contenuti.

c. Modalità di sincronizzazione: scegli come aggiornare l'indice quando il contenuto della fonte dati cambia. Quando sincronizzi l'origine dati con Amazon Kendra per la prima volta, tutto il contenuto viene sottoposto a scansione e indicizzato per

impostazione predefinita. Se la sincronizzazione iniziale non è riuscita, devi eseguire una sincronizzazione completa dei dati, anche se non scegli la sincronizzazione completa come opzione della modalità di sincronizzazione.

- Sincronizzazione completa: indicizza di nuovo tutti i contenuti, sostituendo i contenuti esistenti ogni volta che l'origine dati si sincronizza con l'indice.
- Sincronizzazione nuova e modificata: indicizza solo i contenuti nuovi e modificati ogni volta che l'origine dati si sincronizza con l'indice. Amazon Kendra può utilizzare il meccanismo dell'origine dati per tenere traccia delle modifiche ai contenuti e indicizzare i contenuti modificati dall'ultima sincronizzazione.
- Sincronizzazione nuova, modificata ed eliminata: indicizza solo i contenuti nuovi, modificati ed eliminati ogni volta che l'origine dati si sincronizza con l'indice. Amazon Kendra può utilizzare il meccanismo dell'origine dati per tenere traccia delle modifiche ai contenuti e indicizzare i contenuti modificati dall'ultima sincronizzazione.

d. Pianificazione di esecuzione di In Sync, per Frequenza: con quale frequenza Amazon Kendra verrà eseguita la sincronizzazione con la fonte di dati.

e. Seleziona Successivo.

8. Nella pagina Imposta le mappature dei campi, inserisci le seguenti informazioni:

a. Seleziona uno dei campi di origine dati predefiniti generati (ID documento, titoli dei documenti e URL di origine) che desideri mappare per indicizzare. Amazon Kendra

b. Aggiungi campo: consente di aggiungere campi di origine dati personalizzati per creare un nome di campo indice a cui mappare e il tipo di dati del campo.

c. Seleziona Successivo.

9. Nella pagina Rivedi e crea, verifica che le informazioni inserite siano corrette, quindi seleziona Aggiungi origine dati. Puoi anche scegliere di modificare le tue informazioni da questa pagina. L'origine dati verrà visualizzata nella pagina Origini dati dopo che l'origine dati sarà stata aggiunta correttamente.

API

Per connettersi Amazon Kendra a Oracle Database

È necessario specificare quanto segue utilizzando l'TemplateConfigurationAPI:

- Origine dati: specifica il tipo di origine dati come `JDBC` quando usi lo schema TemplateConfigurationJSON. Specificate anche l'origine dati come `TEMPLATE` quando chiamate l'CreateDataSourceAPI.
- Tipo di database: è necessario specificare il tipo di database come`oracle`.
- Query SQL: specifica le istruzioni di query SQL come le operazioni SELECT e JOIN. Le query SQL devono pesare meno di 32 KB. Amazon Kendra eseguirà la scansione di tutto il contenuto del database che corrisponde alla tua query.
- Modalità di sincronizzazione: specifica come Amazon Kendra aggiornare l'indice quando il contenuto dell'origine dati cambia. Quando sincronizzi l'origine dati con Amazon Kendra per la prima volta, tutto il contenuto viene sottoposto a scansione e indicizzato per impostazione predefinita. Se la sincronizzazione iniziale non è riuscita, devi eseguire una sincronizzazione completa dei dati, anche se non scegli la sincronizzazione completa come opzione della modalità di sincronizzazione. Puoi scegliere tra:
  - `FORCED_FULL_CRAWL`per indicizzare nuovamente tutti i contenuti, sostituendo i contenuti esistenti ogni volta che l'origine dati si sincronizza con l'indice.
  - `FULL_CRAWL`per indicizzare solo i contenuti nuovi, modificati ed eliminati ogni volta che l'origine dati si sincronizza con l'indice. Amazon Kendra può utilizzare il meccanismo dell'origine dati per tenere traccia delle modifiche ai contenuti e indicizzare i contenuti modificati dall'ultima sincronizzazione.
  - `CHANGE_LOG`per indicizzare solo contenuti nuovi e modificati ogni volta che l'origine dati si sincronizza con l'indice. Amazon Kendra può utilizzare il meccanismo dell'origine dati per tenere traccia delle modifiche ai contenuti e indicizzare i contenuti modificati dall'ultima sincronizzazione.
- Amazon Resource Name (ARN) segreto: fornisci l'Amazon Resource Name (ARN) di un Secrets Manager segreto che contiene le credenziali di autenticazione che hai creato nel tuo account. Oracle Database Il segreto è archiviato in una struttura JSON con le seguenti chiavi:

```
{
    "user name": "database user name",
    "password": "password"
}
```

> **Note**
>
> Ti consigliamo di aggiornare o ruotare regolarmente le credenziali e il segreto. Fornisci solo il livello di accesso necessario per la tua sicurezza. Non è consigliabile riutilizzare

credenziali e segreti tra diverse fonti di dati e nelle versioni 1.0 e 2.0 dei connettori (ove applicabile).

- IAM ruolo: specifica `RoleArn` quando chiami `CreateDataSource` per fornire a un IAM ruolo le autorizzazioni per accedere al tuo Secrets Manager segreto e per chiamare le API pubbliche richieste per il connettore e. Oracle Database Amazon Kendra Per ulteriori informazioni, consulta i IAM ruoli per Oracle Database le fonti di dati.

Puoi anche aggiungere le seguenti funzionalità opzionali:

- Virtual Private Cloud (VPC): `VpcConfiguration` specifica quando si chiama. `CreateDataSource` Per ulteriori informazioni, consulta Configurazione Amazon Kendra per l'utilizzo di un Amazon VPC.
- Filtri di inclusione ed esclusione: puoi specificare se includere contenuti specifici utilizzando ID utente, gruppi, URL di origine, timestamp e fusi orari.
- Filtraggio del contesto utente e controllo degli accessi:Amazon Kendra esegue la ricerca per indicizzazione dell'elenco di controllo degli accessi (ACL) dei documenti, se disponi di un ACL per i documenti. Le informazioni ACL vengono utilizzate per filtrare i risultati della ricerca in base all'accesso dell'utente o del relativo gruppo ai documenti. Per ulteriori informazioni, consulta Filtraggio del contesto utente.
- Mappature dei campi: scegli di mappare i campi delle sorgenti Oracle Database dati ai campi indice. Amazon Kendra Per ulteriori informazioni, consulta la sezione Mappatura dei campi di origine dei dati.

> **Note**
>
> Il campo del corpo del documento o l'equivalente del corpo del documento per i documenti è necessario per Amazon Kendra eseguire la ricerca nei documenti. È necessario mappare il nome del campo del corpo del documento nella fonte dati al nome del campo indice`_document_body`. Tutti gli altri campi sono facoltativi.

Per un elenco di altre importanti chiavi JSON da configurare, consultaSchema del modello di database Oracle.

Note

- Le righe del database eliminate non verranno registrate durante la Amazon Kendra verifica della presenza di contenuti aggiornati.
- La dimensione dei nomi e dei valori dei campi in una riga del database non può superare i 400 KB.
- Se l'origine dati del database contiene una grande quantità di dati e non desideri Amazon Kendra indicizzare tutto il contenuto del database dopo la prima sincronizzazione, puoi scegliere di sincronizzare solo i documenti nuovi, modificati o eliminati.
- È consigliabile fornire credenziali Amazon Kendra di database di sola lettura.
- È consigliabile evitare di aggiungere tabelle con dati sensibili o informazioni personali identificabili (PII).

PostgreSQL

PostgreSQLè un sistema di gestione di database open source. Se sei un PostgreSQL utente, puoi usarlo Amazon Kendra per indicizzare la tua fonte di PostgreSQL dati. Il connettore di origine Amazon Kendra PostgreSQL dati supporta PostgreSQL 9.6.

Puoi connetterti Amazon Kendra alla tua fonte di PostgreSQL dati utilizzando la Amazon Kendra console e l'API. TemplateConfiguration

Per la risoluzione dei problemi relativi al connettore della sorgente Amazon Kendra PostgreSQL dati, consultaRisoluzione dei problemi relativi alle origini dati.

Argomenti

Funzionalità supportate

- Mappature dei campi
- Filtraggio del contesto utente
- Filtri di inclusione/esclusione

- Sincronizzazione completa e incrementale dei contenuti
- Virtual Private Cloud (VPC) (Cloud privato virtuale (VPC)

Prerequisiti

Prima di poterla utilizzare Amazon Kendra per indicizzare la tua fonte di PostgreSQL dati, apporta queste modifiche al tuo account PostgreSQL e AWS ai tuoi account.

NelPostgreSQL, assicurati di avere:

- Hai annotato il nome utente e la password del database.

> **Important**
>
> È consigliabile fornire credenziali Amazon Kendra di database di sola lettura.

- Hai copiato l'URL, la porta e l'istanza dell'host del database.
- È stato verificato che ogni documento sia unico all'interno PostgreSQL e tra le altre fonti di dati che intendi utilizzare per lo stesso indice. Ogni fonte di dati che desideri utilizzare per un indice non deve contenere lo stesso documento in tutte le fonti di dati. Gli ID dei documenti sono globali rispetto a un indice e devono essere univoci per indice.

Nel tuo Account AWS, assicurati di avere:

- Ha creato un Amazon Kendra indice e, se si utilizza l'API, ha annotato l'ID dell'indice.
- Hai creato un IAM ruolo per la tua origine dati e, se utilizzi l'API, hai annotato l'ARN del IAM ruolo.

> **Note**
>
> Se modifichi il tipo di autenticazione e le credenziali, devi aggiornare il IAM ruolo per accedere all'ID AWS Secrets Manager segreto corretto.

- Ha archiviato le credenziali di PostgreSQL autenticazione in un AWS Secrets Manager segreto e, se si utilizza l'API, ha annotato l'ARN del segreto.

> **Note**
>
> Ti consigliamo di aggiornare o ruotare regolarmente le credenziali e il segreto. Fornisci solo il livello di accesso necessario per la tua sicurezza. Non è consigliabile riutilizzare credenziali e segreti tra diverse fonti di dati e versioni dei connettori 1.0 e 2.0 (ove applicabile).

Se non disponi di un IAM ruolo o di un segreto esistente, puoi utilizzare la console per creare un nuovo IAM ruolo e un Secrets Manager segreto quando connetti la tua origine PostgreSQL dati a. Amazon Kendra Se utilizzi l'API, devi fornire l'ARN di un IAM ruolo e di un Secrets Manager segreto esistenti e un ID di indice.

Istruzioni di connessione

Per connetterti Amazon Kendra alla tua fonte di PostgreSQL dati devi fornire i dettagli delle tue PostgreSQL credenziali in modo da Amazon Kendra poter accedere ai tuoi dati. Se non lo hai ancora configurato, PostgreSQL Amazon Kendra Prerequisiti consulta.

Console

Per connettersi Amazon Kendra a PostgreSQL

1. Accedi a AWS Management Console e apri la Amazon Kendra console.
2. Dal riquadro di navigazione a sinistra, scegli Indici, quindi scegli l'indice che desideri utilizzare dall'elenco degli indici.

   > **Note**
   >
   > Puoi scegliere di configurare o modificare le impostazioni del controllo dell'accesso degli utenti in Impostazioni dell'indice.

3. Nella pagina Guida introduttiva, scegli Aggiungi origine dati.
4. Nella pagina Aggiungi origine dati, scegli PostgreSQLconnettore, quindi scegli Aggiungi connettore.
5. Nella pagina Specificare i dettagli dell'origine dati, inserisci le seguenti informazioni:

a. In Nome e descrizione, per Nome dell'origine dati, inserisci un nome per l'origine dati. Puoi includere trattini ma non spazi.

b. (Facoltativo) Descrizione: immetti una descrizione facoltativa per l'origine dati.

c. In Lingua predefinita: scegli una lingua per filtrare i documenti per l'indice. Se non diversamente specificato, la lingua predefinita è l'inglese. La lingua specificata nei metadati del documento ha la precedenza sulla lingua selezionata.

d. In Tag, per Aggiungi nuovo tag, includi tag opzionali per cercare e filtrare le risorse o tenere traccia dei costi. AWS

e. Seleziona Successivo.

6. Nella pagina Definisci accesso e sicurezza, inserisci le seguenti informazioni:

a. In Source, inserisci le seguenti informazioni:

b. Host: immettere il nome host del database.

c. Porta: immettere la porta del database.

d. Istanza: immettere l'istanza del database.

e. Abilita la posizione del certificato SSL: scegli di inserire il Amazon S3 percorso del file del certificato SSL.

f. In Autenticazione, inserisci le seguenti informazioni:

- AWS Secrets Manager segreto: scegli un segreto esistente o creane uno nuovo Secrets Manager per memorizzare le credenziali di PostgreSQL autenticazione. Se scegli di creare un nuovo segreto, si apre una finestra AWS Secrets Manager segreta.

  A. Inserisci le seguenti informazioni nella finestra Crea un AWS Secrets Manager segreto:

     I. Nome segreto: un nome per il tuo segreto. Il prefisso 'AmazonKendra-PostgreSQL -' viene aggiunto automaticamente al nome segreto.

     II. Per nome utente e password del database, immettete i valori delle credenziali di autenticazione copiati dal database.

  B. Selezionare Salva.

g. Virtual Private Cloud (VPC): puoi scegliere di utilizzare un VPC. In tal caso, è necessario aggiungere sottoreti e gruppi di sicurezza VPC.

h. IAM ruolo: scegli un IAM ruolo esistente o creane uno nuovo IAM per accedere alle credenziali del repository e indicizzare il contenuto.

> **Note**
>
> IAM i ruoli utilizzati per gli indici non possono essere utilizzati per le fonti di dati. Se non sei sicuro che un ruolo esistente venga utilizzato per un indice o una FAQ, scegli Crea un nuovo ruolo per evitare errori.

i. Seleziona Successivo.

7. Nella pagina Configura le impostazioni di sincronizzazione, inserisci le seguenti informazioni:

a. Nell'ambito della sincronizzazione, scegli tra le seguenti opzioni:

- Query SQL: immetti istruzioni di query SQL come le operazioni SELECT e JOIN. Le query SQL devono pesare meno di 32 KB. Amazon Kendra eseguirà la scansione di tutto il contenuto del database che corrisponde alla tua query.
- Colonna chiave primaria: fornisce la chiave primaria per la tabella del database. Identifica una tabella all'interno del database.
- Colonna del titolo: fornisce il nome della colonna del titolo del documento all'interno della tabella del database.
- Colonna del corpo: fornisce il nome della colonna del corpo del documento all'interno della tabella del database.

b. In Configurazione aggiuntiva, facoltativa, scegli una delle seguenti opzioni per sincronizzare contenuti specifici anziché sincronizzare tutti i file:

- Colonne di rilevamento delle modifiche: immetti i nomi delle colonne che Amazon Kendra verranno utilizzate per rilevare le modifiche al contenuto. Amazon Kendra reindicizzerà il contenuto in caso di modifica in una di queste colonne.
- Colonna ID utenti: immetti il nome della colonna che contiene gli ID utente a cui consentire l'accesso ai contenuti.
- Colonna Gruppi: immetti il nome della colonna che contiene i gruppi a cui consentire l'accesso ai contenuti.
- Colonna URL di origine: inserisci il nome della colonna che contiene gli URL di origine da indicizzare.

- Colonna timestamp: immetti il nome della colonna che contiene i timestamp. Amazon Kendra utilizza le informazioni relative alla marca temporale per rilevare le modifiche ai contenuti e sincronizzare solo i contenuti modificati.
- Colonna dei fusi orari: inserisci il nome della colonna che contiene i fusi orari per il contenuto da sottoporre a scansione.
- Formato timestamp: immetti il nome della colonna che contiene i formati di timestamp da utilizzare per rilevare le modifiche ai contenuti e risincronizzare i contenuti.

c. Modalità di sincronizzazione: scegli come aggiornare l'indice quando il contenuto della fonte dati cambia. Quando sincronizzi l'origine dati con Amazon Kendra per la prima volta, tutto il contenuto viene sottoposto a scansione e indicizzato per impostazione predefinita. Se la sincronizzazione iniziale non è riuscita, devi eseguire una sincronizzazione completa dei dati, anche se non scegli la sincronizzazione completa come opzione della modalità di sincronizzazione.

- Sincronizzazione completa: indicizza di nuovo tutti i contenuti, sostituendo i contenuti esistenti ogni volta che l'origine dati si sincronizza con l'indice.
- Nuova sincronizzazione modificata: indicizza solo i contenuti nuovi e modificati ogni volta che l'origine dati si sincronizza con l'indice. Amazon Kendra può utilizzare il meccanismo dell'origine dati per tenere traccia delle modifiche ai contenuti e indicizzare i contenuti modificati dall'ultima sincronizzazione.
- Sincronizzazione nuova, modificata ed eliminata: indicizza solo i contenuti nuovi, modificati ed eliminati ogni volta che l'origine dati si sincronizza con l'indice. Amazon Kendra può utilizzare il meccanismo dell'origine dati per tenere traccia delle modifiche ai contenuti e indicizzare i contenuti modificati dall'ultima sincronizzazione.

d. Pianificazione di esecuzione di In Sync, per Frequenza: con quale frequenza Amazon Kendra verrà eseguita la sincronizzazione con la fonte di dati.

e. Seleziona Successivo.

8. Nella pagina Imposta mappature dei campi, inserisci le seguenti informazioni:

a. Seleziona uno dei campi di origine dati predefiniti generati (ID documento, titoli dei documenti e URL di origine) che desideri mappare per indicizzare. Amazon Kendra

b. Aggiungi campo: consente di aggiungere campi di origine dati personalizzati per creare un nome di campo indice a cui mappare e il tipo di dati del campo.

c. Seleziona Successivo.

9. Nella pagina Rivedi e crea, verifica che le informazioni inserite siano corrette, quindi seleziona Aggiungi origine dati. Puoi anche scegliere di modificare le tue informazioni da questa pagina. L'origine dati verrà visualizzata nella pagina Origini dati dopo che l'origine dati sarà stata aggiunta correttamente.

API

Per connettersi Amazon Kendra a PostgreSQL

È necessario specificare quanto segue utilizzando l'TemplateConfigurationAPI:

- Origine dati: specifica il tipo di origine dati come `JDBC` quando usi lo schema TemplateConfigurationJSON. Specificate anche l'origine dati come `TEMPLATE` quando chiamate l'CreateDataSourceAPI.
- Tipo di database: è necessario specificare il tipo di database come`postgresql`.
- Query SQL: specifica le istruzioni di query SQL come le operazioni SELECT e JOIN. Le query SQL devono pesare meno di 32 KB. Amazon Kendra eseguirà la scansione di tutto il contenuto del database che corrisponde alla tua query.
- Modalità di sincronizzazione: specifica come Amazon Kendra aggiornare l'indice quando il contenuto dell'origine dati cambia. Quando sincronizzi l'origine dati con Amazon Kendra per la prima volta, tutto il contenuto viene sottoposto a scansione e indicizzato per impostazione predefinita. Se la sincronizzazione iniziale non è riuscita, devi eseguire una sincronizzazione completa dei dati, anche se non scegli la sincronizzazione completa come opzione della modalità di sincronizzazione. Puoi scegliere tra:
  - `FORCED_FULL_CRAWL`per indicizzare nuovamente tutti i contenuti, sostituendo i contenuti esistenti ogni volta che l'origine dati si sincronizza con l'indice.
  - `FULL_CRAWL`per indicizzare solo i contenuti nuovi, modificati ed eliminati ogni volta che l'origine dati si sincronizza con l'indice. Amazon Kendra può utilizzare il meccanismo dell'origine dati per tenere traccia delle modifiche ai contenuti e indicizzare i contenuti modificati dall'ultima sincronizzazione.
  - `CHANGE_LOG`per indicizzare solo contenuti nuovi e modificati ogni volta che l'origine dati si sincronizza con l'indice. Amazon Kendra può utilizzare il meccanismo dell'origine dati per tenere traccia delle modifiche ai contenuti e indicizzare i contenuti modificati dall'ultima sincronizzazione.

- Amazon Resource Name (ARN) segreto: fornisci l'Amazon Resource Name (ARN) di un Secrets Manager segreto che contiene le credenziali di autenticazione che hai creato nel tuo account. PostgreSQL Il segreto è archiviato in una struttura JSON con le seguenti chiavi:

```
{
    "user name": "database user name",
    "password": "password"
}
```

> **Note**
>
> Ti consigliamo di aggiornare o ruotare regolarmente le credenziali e il segreto. Fornisci solo il livello di accesso necessario per la tua sicurezza. Non è consigliabile riutilizzare credenziali e segreti tra diverse fonti di dati e versioni dei connettori 1.0 e 2.0 (ove applicabile).

- IAM ruolo: specifica `RoleArn` quando chiami `CreateDataSource` per fornire a un IAM ruolo le autorizzazioni per accedere al tuo Secrets Manager segreto e per chiamare le API pubbliche richieste per il connettore e. PostgreSQL Amazon Kendra Per ulteriori informazioni, consulta i IAM ruoli per PostgreSQL le fonti di dati.

Puoi anche aggiungere le seguenti funzionalità opzionali:

- Virtual Private Cloud (VPC): `VpcConfiguration` specifica quando si chiama. `CreateDataSource` Per ulteriori informazioni, consulta Configurazione Amazon Kendra per l'utilizzo di un Amazon VPC.
- Filtri di inclusione ed esclusione: puoi specificare se includere contenuti specifici utilizzando ID utente, gruppi, URL di origine, timestamp e fusi orari.
- Filtraggio del contesto utente e controllo degli accessi:Amazon Kendra esegue la ricerca per indicizzazione dell'elenco di controllo degli accessi (ACL) dei documenti, se disponi di un ACL per i documenti. Le informazioni ACL vengono utilizzate per filtrare i risultati della ricerca in base all'accesso dell'utente o del relativo gruppo ai documenti. Per ulteriori informazioni, consulta Filtraggio del contesto utente.
- Mappature dei campi: scegli di mappare i campi delle sorgenti PostgreSQL dati ai campi indice. Amazon Kendra Per ulteriori informazioni, consulta la sezione Mappatura dei campi di origine dei dati.

> **Note**
>
> Il campo del corpo del documento o l'equivalente del corpo del documento per i documenti è necessario per Amazon Kendra eseguire la ricerca nei documenti. È necessario mappare il nome del campo del corpo del documento nella fonte dati al nome del campo indice`_document_body`. Tutti gli altri campi sono facoltativi.

Per un elenco di altre importanti chiavi JSON da configurare, consultaSchema del modello PostgreSQL.

Note

- Le righe del database eliminate non verranno registrate durante la Amazon Kendra verifica della presenza di contenuti aggiornati.
- La dimensione dei nomi e dei valori dei campi in una riga del database non può superare i 400 KB.
- Se l'origine dati del database contiene una grande quantità di dati e non desideri Amazon Kendra indicizzare tutto il contenuto del database dopo la prima sincronizzazione, puoi scegliere di sincronizzare solo i documenti nuovi, modificati o eliminati.
- È consigliabile fornire credenziali Amazon Kendra di database di sola lettura.
- È consigliabile evitare di aggiungere tabelle con dati sensibili o informazioni personali identificabili (PII).

battuta

Quip è un software di produttività collaborativa che offre funzionalità di creazione di documenti in tempo reale. Puoi usarlo Amazon Kendra per indicizzare le cartelle, i file, i commenti sui file, le chat room e gli allegati di Quip.

Puoi connetterti Amazon Kendra alla tua fonte di dati Quip usando la Amazon Kendra console e l'API. QuipConfiguration

Per la risoluzione dei problemi del connettore di origine dati Amazon Kendra Quip, consulta. Risoluzione dei problemi relativi alle origini dati

Argomenti

Funzionalità supportate

Amazon Kendra Il connettore di origine dati Quip supporta le seguenti funzionalità:

- Mappature dei campi
- Filtraggio del contesto utente
- Filtri di inclusione/esclusione
- Virtual Private Cloud (VPC) (Cloud privato virtuale (VPC)

Prerequisiti

Prima di poterla utilizzare Amazon Kendra per indicizzare la tua fonte di dati Quip, apporta queste modifiche a Quip e ai tuoi account. AWS

In Quip, assicurati di avere:

- Un account Quip con autorizzazioni amministrative.
- Credenziali di autenticazione Quip create che includono un token di accesso personale. Per ulteriori informazioni, consulta la documentazione di Quip sull'autenticazione.
- Hai copiato il dominio del tuo sito Quip. Ad esempio, *`https://quip-company.quipdomain.com/browse`* dove *`quipdomain è il dominio`*.
- Selezionato, ogni documento è unico in Quip e tra le altre fonti di dati che intendi utilizzare per lo stesso indice. Ogni fonte di dati che desideri utilizzare per un indice non deve contenere lo stesso documento in tutte le fonti di dati. Gli ID dei documenti sono globali rispetto a un indice e devono essere univoci per indice.

Nel tuo Account AWS, assicurati di avere:

- Ha creato un Amazon Kendra indice e, se si utilizza l'API, ha annotato l'ID dell'indice.
- Hai creato un IAM ruolo per la tua origine dati e, se utilizzi l'API, hai annotato l'ARN del IAM ruolo.

> **Note**
>
> Se modifichi il tipo di autenticazione e le credenziali, devi aggiornare il IAM ruolo per accedere all'ID AWS Secrets Manager segreto corretto.

- Ha archiviato le credenziali di autenticazione Quip in un AWS Secrets Manager luogo segreto e, se si utilizza l'API, ha annotato l'ARN del segreto.

> **Note**
>
> Ti consigliamo di aggiornare o ruotare regolarmente le credenziali e il segreto. Fornisci solo il livello di accesso necessario per la tua sicurezza. Non è consigliabile riutilizzare credenziali e segreti tra diverse fonti di dati e versioni dei connettori 1.0 e 2.0 (ove applicabile).

Se non disponi di un IAM ruolo o di un segreto esistente, puoi utilizzare la console per creare un nuovo IAM ruolo e un Secrets Manager segreto quando connetti la tua fonte di dati Quip a. Amazon Kendra Se utilizzi l'API, devi fornire l'ARN di un IAM ruolo e di un Secrets Manager segreto esistenti e un ID di indice.

Istruzioni di connessione

Per connetterti Amazon Kendra alla tua fonte dati Quip, devi fornire i dettagli necessari della tua fonte di dati Quip in modo che Amazon Kendra possa accedere ai tuoi dati. Se non hai ancora configurato Quip per Amazon Kendra, vedi. Prerequisiti

Console

Per connettersi Amazon Kendra a Quip

1. Accedi a AWS Management Console e apri la Amazon Kendra console.
2. Dal riquadro di navigazione a sinistra, scegli Indici, quindi scegli l'indice che desideri utilizzare dall'elenco degli indici.

> **Note**
>
> Puoi scegliere di configurare o modificare le impostazioni del controllo dell'accesso degli utenti in Impostazioni dell'indice.

3. Nella pagina Guida introduttiva, scegli Aggiungi origine dati.
4. Nella pagina Aggiungi origine dati, scegli Connettore Quip, quindi scegli Aggiungi connettore.
5. Nella pagina Specificare i dettagli dell'origine dati, inserisci le seguenti informazioni:
   a. In Nome e descrizione, per Nome dell'origine dati, inserisci un nome per l'origine dati. Puoi includere trattini ma non spazi.
   b. (Facoltativo) Descrizione: immetti una descrizione facoltativa per la tua fonte di dati.
   c. In Lingua predefinita: scegli una lingua per filtrare i documenti per l'indice. Se non diversamente specificato, la lingua predefinita è l'inglese. La lingua specificata nei metadati del documento ha la precedenza sulla lingua selezionata.
   d. In Tag, per Aggiungi nuovo tag, includi tag opzionali per cercare e filtrare le risorse o tenere traccia dei costi. AWS
   e. Seleziona Successivo.
6. Nella pagina Definisci accesso e sicurezza, inserisci le seguenti informazioni:
   a. Nome di dominio Quip: inserisci il Quip che hai copiato dal tuo account Quip.
   b. AWS Secrets Manager segreto: scegli un segreto esistente o creane uno nuovo per memorizzare le tue credenziali di autenticazione Secrets Manager Quip. Se scegli di creare un nuovo segreto, si apre una finestra AWS Secrets Manager segreta.
      i. Inserisci le seguenti informazioni nella finestra Crea un AWS Secrets Manager segreto:
         A. Nome segreto: un nome per il tuo segreto. Il prefisso 'AmazonKendra-Quip-' viene aggiunto automaticamente al tuo nome segreto.
         B. Token Quip: inserisci il token di accesso personale Quip che hai creato nel tuo account Quip.
      ii. Selezionare Salva.
   c. Virtual Private Cloud (VPC): puoi scegliere di utilizzare un VPC. In tal caso, è necessario aggiungere sottoreti e gruppi di sicurezza VPC.

d. IAM ruolo: scegli un IAM ruolo esistente o creane uno nuovo IAM per accedere alle credenziali del repository e indicizzare il contenuto.

> **Note**
>
> IAM i ruoli utilizzati per gli indici non possono essere utilizzati per le fonti di dati. Se non sei sicuro che un ruolo esistente venga utilizzato per un indice o una FAQ, scegli Crea un nuovo ruolo per evitare errori.

e. Seleziona Successivo.

7. Nella pagina Configura le impostazioni di sincronizzazione, inserisci le seguenti informazioni:

a. Aggiungi gli ID delle cartelle Quip da sottoporre a scansione: gli ID delle cartelle Quip di cui desideri eseguire la scansione.

> **Note**
>
> Per eseguire la scansione di una cartella principale, incluse tutte le sottocartelle e i documenti al suo interno, inserisci l'ID della cartella principale. Per eseguire la scansione di sottocartelle specifiche, aggiungi gli ID delle sottocartelle specifiche.

b. Configurazione aggiuntiva (tipi di contenuto): inserisci i tipi di contenuto che desideri sottoporre a scansione.

c. Modelli Regex: modelli di espressioni regolari per includere o escludere determinati file. È possibile aggiungere fino a 100 pattern.

d. In Pianificazione di esecuzione della sincronizzazione, per Frequenza: scegli la frequenza di sincronizzazione di Amazon Kendra con la tua fonte di dati.

e. Seleziona Successivo.

8. Nella pagina Imposta mappature dei campi, inserisci le seguenti informazioni:

a. Seleziona uno dei campi di origine dati predefiniti generati che desideri mappare per indicizzare Amazon Kendra .

b. Aggiungi campo: consente di aggiungere campi di origine dati personalizzati per creare un nome di campo indice a cui mappare e il tipo di dati del campo.

c. Seleziona Successivo.

9. Nella pagina Rivedi e crea, verifica che le informazioni inserite siano corrette, quindi seleziona Aggiungi origine dati. Puoi anche scegliere di modificare le tue informazioni da questa pagina. L'origine dati verrà visualizzata nella pagina Origini dati dopo che l'origine dati sarà stata aggiunta correttamente.

API

Per connettersi Amazon Kendra a Quip

È necessario specificare quanto segue utilizzando l'QuipConfiguration API:

- Dominio del sito Quip: ad esempio, *`https://quip-company.quipdomain.com/browse`* dove *`quipdomain è il dominio`*.
- Secret Amazon Resource Name (ARN): fornisci l'Amazon Resource Name (ARN) di un Secrets Manager segreto che contiene le credenziali di autenticazione per il tuo account Quip. Il segreto è archiviato in una struttura JSON con le seguenti chiavi:

```
{
    "accessToken": "token"
}
```

> **Note**
>
> Ti consigliamo di aggiornare o ruotare regolarmente le credenziali e il segreto. Fornisci solo il livello di accesso necessario per la tua sicurezza. Non è consigliabile riutilizzare credenziali e segreti tra diverse fonti di dati e versioni dei connettori 1.0 e 2.0 (ove applicabile).

- IAM ruolo: specifica `RoleArn` quando chiami `CreateDataSource` per fornire a un IAM ruolo le autorizzazioni per accedere al tuo Secrets Manager segreto e per chiamare le API pubbliche richieste per il connettore Quip e. Amazon Kendra Per ulteriori informazioni, consulta i IAM ruoli per le fonti di dati Quip.

Puoi anche aggiungere le seguenti funzionalità opzionali:

- Virtual Private Cloud (VPC): specifica `VpcConfiguration` come parte della configurazione dell'origine dati. Vedi Configurazione Amazon Kendra per l'uso di un VPC.

- Filtri di inclusione ed esclusione: specifica se includere o escludere determinati file.

  > **Note**
  >
  > La maggior parte delle fonti di dati utilizza modelli di espressioni regolari, che sono modelli di inclusione o esclusione denominati filtri. Se si specifica un filtro di inclusione, viene indicizzato solo il contenuto che corrisponde al filtro di inclusione. Qualsiasi documento che non corrisponde al filtro di inclusione non viene indicizzato. Se si specifica un filtro di inclusione ed esclusione, i documenti che corrispondono al filtro di esclusione non vengono indicizzati, anche se corrispondono al filtro di inclusione.

- Cartelle: specifica le cartelle e le sottocartelle Quip che desideri indicizzare

  > **Note**
  >
  > Per eseguire la scansione di una cartella principale, incluse tutte le sottocartelle e i documenti al suo interno, inserisci l'ID della cartella principale. Per eseguire la scansione di sottocartelle specifiche, aggiungi gli ID delle sottocartelle specifiche.

- Allegati, chat room, commenti ai file: scegli se includere la scansione degli allegati, il contenuto delle chat room e i commenti sui file.
- Mappature dei campi: scegli di mappare i campi della sorgente dati di Quip ai campi indice. Amazon Kendra Per ulteriori informazioni, consulta la sezione Mappatura dei campi di origine dei dati.

  > **Note**
  >
  > Il campo relativo al corpo del documento o l'equivalente del corpo del documento è necessario per Amazon Kendra eseguire la ricerca nei documenti. È necessario mappare il nome del campo del corpo del documento nella fonte dati al nome del campo indice `_document_body`. Tutti gli altri campi sono facoltativi.

- Filtraggio del contesto utente e controllo degli accessi:Amazon Kendra esegue la scansione dell'elenco di controllo degli accessi (ACL) dei documenti, se disponi di un ACL per i documenti. Le informazioni ACL vengono utilizzate per filtrare i risultati della ricerca in base all'accesso dell'utente o del relativo gruppo ai documenti. Per ulteriori informazioni, consulta Filtraggio del contesto utente.

Ulteriori informazioni

Per saperne di più sull'integrazione Amazon Kendra con la tua fonte di dati Quip, vedi:

- Cerca informazioni nei documenti Quip con la ricerca intelligente utilizzando il connettore Quip per Amazon Kendra

Salesforce

Salesforce è uno strumento di gestione delle relazioni con i clienti (CRM) per la gestione dei team di supporto, vendita e marketing. Puoi utilizzarlo Amazon Kendra per indicizzare gli oggetti standard di Salesforce e persino gli oggetti personalizzati.

Puoi connetterti Amazon Kendra alla tua fonte di dati Salesforce utilizzando la Amazon Kendra console, l'API o l'TemplateConfigurationAPI. SalesforceConfiguration

Amazon Kendra dispone di due versioni del connettore Salesforce. Le funzionalità supportate di ogni versione includono:

Connettore Salesforce V1.0/API SalesforceConfiguration

- Mappature dei campi
- Filtraggio del contesto utente
- Filtri di inclusione/esclusione

Connettore Salesforce V2.0/API TemplateConfiguration

- Mappature dei campi
- Filtraggio del contesto utente
- Scansione delle identità degli utenti
- Filtri di inclusione/esclusione
- Sincronizzazione completa e incrementale dei contenuti
- Scansione degli allegati delle entità
- Virtual Private Cloud (VPC) (Cloud privato virtuale (VPC)

> **Note**
>
> La fine del supporto per il connettore Salesforce SalesforceConfiguration V1.0/API è prevista per il 2023. Consigliamo di eseguire la migrazione o l'utilizzo del connettore Salesforce V2.0/ API. TemplateConfiguration

Per la risoluzione dei problemi relativi al connettore di origine dati Amazon Kendra Salesforce, consulta. Risoluzione dei problemi relativi alle origini dati

Argomenti

Connettore Salesforce V1.0

Salesforce è uno strumento di gestione delle relazioni con i clienti (CRM) per la gestione dei team di supporto, vendita e marketing. Puoi utilizzarlo Amazon Kendra per indicizzare gli oggetti standard di Salesforce e persino gli oggetti personalizzati.

> **Important**
>
> Amazon Kendra utilizza la versione 48 dell'API Salesforce. L'API Salesforce limita il numero di richieste che puoi effettuare al giorno. Se Salesforce supera tali richieste, riprova finché non è in grado di continuare.

> **Note**
>
> La fine del supporto per il connettore Salesforce SalesforceConfiguration V1.0/API è prevista per il 2023. Consigliamo di eseguire la migrazione o l'utilizzo del connettore Salesforce V2.0/ API. TemplateConfiguration

Per la risoluzione dei problemi relativi al connettore di origine dati Amazon Kendra Salesforce, consulta. Risoluzione dei problemi relativi alle origini dati

Argomenti

Funzionalità supportate

Amazon Kendra Il connettore di origine dati Salesforce supporta le seguenti funzionalità:

- Mappature dei campi
- Filtraggio del contesto utente
- Filtri di inclusione/esclusione

Prerequisiti

Prima di utilizzarla Amazon Kendra per indicizzare la tua fonte di dati Salesforce, apporta queste modifiche a Salesforce e agli account. AWS

In Salesforce, assicurati di avere:

- Hai creato un account Salesforce e hai annotato il nome utente e la password che usi per connetterti a Salesforce.
- Hai creato un account Salesforce Connected App con OAuth attivato e hai copiato la chiave consumer (ID client) e il segreto del consumatore (client secret) assegnati alla tua app Salesforce Connected. Per ulteriori informazioni, consulta la documentazione di Salesforce sulle app connesse.
- Ha copiato il token di sicurezza Salesforce associato all'account utilizzato per connettersi a Salesforce.
- Ha copiato l'URL dell'istanza Salesforce che desideri indicizzare. <company>In genere, si tratta di *https:*//.salesforce.com/. Il server deve eseguire un'app connessa a Salesforce.
- Sono state aggiunte credenziali al server Salesforce per un utente con accesso in sola lettura a Salesforce clonando il ReadOnly profilo e quindi aggiungendo le autorizzazioni Visualizza tutti i dati e Gestisci articoli. Queste credenziali identificano l'utente che effettua la connessione e l'app connessa Salesforce a cui si connette. Amazon Kendra
- Controllato, ogni documento è unico in Salesforce e tra le altre fonti di dati che intendi utilizzare per lo stesso indice. Ogni fonte di dati che desideri utilizzare per un indice non deve contenere lo

stesso documento in tutte le fonti di dati. Gli ID dei documenti sono globali rispetto a un indice e devono essere univoci per indice.

Nel tuo Account AWS, assicurati di avere:

- Ha creato un Amazon Kendra indice e, se si utilizza l'API, ha annotato l'ID dell'indice.
- Hai creato un IAM ruolo per la tua origine dati e, se utilizzi l'API, hai annotato l'ARN del IAM ruolo.

> **Note**
>
> Se modifichi il tipo di autenticazione e le credenziali, devi aggiornare il IAM ruolo per accedere all'ID AWS Secrets Manager segreto corretto.

- Ha archiviato le credenziali di autenticazione Salesforce in un AWS Secrets Manager segreto e, se si utilizza l'API, ha annotato l'ARN del segreto.

> **Note**
>
> Ti consigliamo di aggiornare o ruotare regolarmente le credenziali e il segreto. Fornisci solo il livello di accesso necessario per la tua sicurezza. Non è consigliabile riutilizzare credenziali e segreti tra diverse fonti di dati e versioni dei connettori 1.0 e 2.0 (ove applicabile).

Se non disponi di un IAM ruolo o di un segreto esistente, puoi utilizzare la console per creare un nuovo IAM ruolo e un Secrets Manager segreto quando connetti la tua fonte di dati Salesforce a. Amazon Kendra Se utilizzi l'API, devi fornire l'ARN di un IAM ruolo e di un Secrets Manager segreto esistenti e un ID di indice.

Istruzioni di connessione

Per connetterti Amazon Kendra alla tua fonte dati Salesforce, devi fornire i dettagli necessari della fonte dati Salesforce in modo che Amazon Kendra possa accedere ai tuoi dati. Se non hai ancora configurato Salesforce, vedi. Amazon Kendra Prerequisiti

Console

Per connettersi Amazon Kendra a Salesforce

1. Accedi alla console di AWS gestione e apri la Amazon Kendra console.
2. Dal riquadro di navigazione a sinistra, scegli Indici, quindi scegli l'indice che desideri utilizzare dall'elenco degli indici.

> **Note**
>
> Puoi scegliere di configurare o modificare le impostazioni del controllo dell'accesso degli utenti in Impostazioni dell'indice.

3. Nella pagina Guida introduttiva, scegli Aggiungi origine dati.
4. Nella pagina Aggiungi origine dati, scegli Salesforce connector V1.0, quindi scegli Aggiungi connettore.
5. Nella pagina Specificare i dettagli dell'origine dati, inserisci le seguenti informazioni:
   a. Nome dell'origine dati: immetti un nome per l'origine dati. È possibile includere trattini ma non spazi.
   b. (Facoltativo) Descrizione: immetti una descrizione facoltativa per la tua fonte di dati.
   c. Lingua predefinita: una lingua per filtrare i documenti per l'indice. Se non diversamente specificato, la lingua predefinita è l'inglese. La lingua specificata nei metadati ha la precedenza sulla lingua selezionata.
   d. Aggiungi nuovo tag: tag per cercare e filtrare le risorse o tenere traccia dei costi condivisi.
   e. Seleziona Successivo.
6. Nella pagina Definisci accesso e sicurezza, inserisci le seguenti informazioni:
   a. URL Salesforce: immetti l'URL dell'istanza per il sito Salesforce che desideri indicizzare.
   b. Per Tipo di autenticazione, scegli tra Esistente e Nuovo per memorizzare le credenziali di autenticazione Salesforce. Se scegli di creare un nuovo segreto, si apre una finestra AWS Secrets Manager segreta.
      - Inserisci le seguenti informazioni nella finestra Crea un AWS Secrets Manager segreto:
        A. Nome segreto: un nome per il tuo segreto. Il prefisso 'AmazonKendra-Salesforce-' viene aggiunto automaticamente al nome segreto.

B. Per nome utente, password, token di sicurezza, chiave utente, segreto utente e URL di autenticazione, inserisci i valori delle credenziali di autenticazione che hai creato nel tuo account Salesforce.

C. Scegli Salva autenticazione.

c. IAM ruolo: scegli un IAM ruolo esistente o crea un nuovo IAM ruolo per accedere alle credenziali del repository e indicizzare il contenuto.

> **Note**
>
> IAM i ruoli utilizzati per gli indici non possono essere utilizzati per le fonti di dati. Se non sei sicuro che un ruolo esistente venga utilizzato per un indice o una FAQ, scegli Crea un nuovo ruolo per evitare errori.

d. Seleziona Successivo.

7. Nella pagina Configura le impostazioni di sincronizzazione, inserisci le seguenti informazioni:

a. Per indicizzare gli allegati: selezionare per eseguire la scansione di tutti gli oggetti, gli articoli e i feed allegati.

b. Per gli oggetti Standard, gli articoli di Knowledge e i feed Chatter, seleziona le entità o i tipi di contenuto di Salesforce che desideri sottoporre a scansione.

> **Note**
>
> È necessario fornire informazioni di configurazione per indicizzare almeno uno degli oggetti standard, degli articoli di conoscenza o dei feed di Chatter. Se scegli di eseguire la ricerca per indicizzazione degli articoli di Knowledge, devi specificare i tipi di articoli della Knowledge Article da indicizzare, il nome degli articoli e se indicizzare i campi standard di tutti gli articoli della Knowledge Article o solo i campi di un tipo di articolo personalizzato. Se scegli di indicizzare gli articoli personalizzati, devi specificare il nome interno del tipo di articolo. È possibile specificare fino a 10 tipi di articoli.

c. Frequenza: con quale frequenza Amazon Kendra verrà eseguita la sincronizzazione con la fonte di dati.

d. Seleziona Successivo.

8. Nella pagina Imposta le mappature dei campi, inserisci le seguenti informazioni:

a. Per gli articoli Standard Knowledge, gli allegati degli oggetti standard e le mappature di campo consigliate aggiuntive, seleziona uno dei campi di origine dati predefiniti Amazon Kendra generati che desideri mappare all'indice.

> **Note**
>
> È richiesta una mappatura dell'indice a. `_document_body` Non è possibile modificare la mappatura tra il `Salesforce ID` campo e il Amazon Kendra `_document_id` campo.

b. Aggiungi campo: consente di aggiungere campi di origine dati personalizzati per creare un nome di campo indice a cui mappare e il tipo di dati del campo.

c. Seleziona Successivo.

9. Nella pagina Rivedi e crea, verifica che le informazioni inserite siano corrette, quindi seleziona Aggiungi origine dati. Puoi anche scegliere di modificare le tue informazioni da questa pagina. L'origine dati verrà visualizzata nella pagina Origini dati dopo che l'origine dati sarà stata aggiunta correttamente.

API

Per connettersi Amazon Kendra a Salesforce

È necessario specificare quanto segue l'SalesforceConfigurationAPI:

- URL del server: l'URL dell'istanza del sito Salesforce che desideri indicizzare.
- Secret Amazon Resource Name (ARN): fornisci l'Amazon Resource Name (ARN) di un Secrets Manager segreto che contiene le credenziali di autenticazione per il tuo account Salesforce. Il segreto è archiviato in una struttura JSON con le seguenti chiavi:

```
{
    "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**
>
> Ti consigliamo di aggiornare o ruotare regolarmente le credenziali e il segreto. Fornisci solo il livello di accesso necessario per la tua sicurezza. Non è consigliabile riutilizzare credenziali e segreti tra diverse fonti di dati e versioni dei connettori 1.0 e 2.0 (ove applicabile).

- IAM ruolo: specifica `RoleArn` quando chiami `CreateDataSource` per fornire a un IAM ruolo le autorizzazioni per accedere al tuo Secrets Manager segreto e per chiamare le API pubbliche richieste per il connettore Salesforce e. Amazon Kendra Per ulteriori informazioni, consulta i IAM ruoli per le fonti di dati Salesforce.
- È necessario fornire informazioni di configurazione per l'indicizzazione di almeno uno degli oggetti standard, degli articoli di conoscenza o dei feed di chatter.
  - Oggetti standard: se si sceglie di eseguire la ricerca per indicizzazione degli oggetti standard, è necessario specificare il nome dell'oggetto standard e il nome del campo nella tabella degli oggetti standard che contiene il contenuto del documento.
  - Articoli della Knowledge: se si sceglie di eseguire la ricerca per indicizzazione degli articoli di Knowledge, è necessario specificare i tipi di articoli della Knowledge Base da indicizzare, lo stato degli articoli da indicizzare e se indicizzare i campi standard di tutti gli articoli della Knowledge Article o solo i campi di un tipo di articolo personalizzato.
  - Feed di Chatter: se scegli di eseguire la scansione dei feed di Chatter, devi specificare il nome della colonna nella tabella FeedItem Salesforce che contiene il contenuto da indicizzare.

Puoi anche aggiungere le seguenti funzionalità opzionali:

- Filtri di inclusione ed esclusione: specificano se includere o escludere determinati file allegati.

> **Note**
>
> La maggior parte delle fonti di dati utilizza modelli di espressioni regolari, che sono modelli di inclusione o esclusione denominati filtri. Se si specifica un filtro di inclusione,

viene indicizzato solo il contenuto che corrisponde al filtro di inclusione. Qualsiasi documento che non corrisponde al filtro di inclusione non viene indicizzato. Se si specifica un filtro di inclusione ed esclusione, i documenti che corrispondono al filtro di esclusione non vengono indicizzati, anche se corrispondono al filtro di inclusione.

- Mappature dei campi: scegli di mappare i campi dell'origine dati di Salesforce ai campi indice. Amazon Kendra Per ulteriori informazioni, consulta la sezione Mappatura dei campi di origine dei dati.

> **Note**
>
> Il campo del corpo del documento o l'equivalente del corpo del documento per i documenti è necessario per eseguire la ricerca nei documenti. Amazon Kendra È necessario mappare il nome del campo del corpo del documento nella fonte dati al nome del campo indice`_document_body`. Tutti gli altri campi sono facoltativi.

- Filtraggio del contesto utente e controllo degli accessi:Amazon Kendra esegue la scansione dell'elenco di controllo degli accessi (ACL) dei documenti, se disponi di un ACL per i documenti. Le informazioni ACL vengono utilizzate per filtrare i risultati della ricerca in base all'accesso dell'utente o del relativo gruppo ai documenti. Per ulteriori informazioni, consulta Filtraggio del contesto utente.

Connettore Salesforce V2.0

Salesforce è uno strumento di gestione delle relazioni con i clienti (CRM) per la gestione dei team di supporto, vendita e marketing. Puoi utilizzarlo Amazon Kendra per indicizzare gli oggetti standard di Salesforce e persino gli oggetti personalizzati.

Il connettore di origine dati Amazon Kendra Salesforce supporta le seguenti edizioni Salesforce: Developer Edition ed Enterprise Edition.

> **Note**
>
> La fine del supporto per il connettore Salesforce SalesforceConfiguration V1.0/API è prevista per il 2023. Consigliamo di eseguire la migrazione o l'utilizzo del connettore Salesforce V2.0/ API. TemplateConfiguration

Per la risoluzione dei problemi relativi al connettore di origine dati Amazon Kendra Salesforce, consulta. Risoluzione dei problemi relativi alle origini dati

Argomenti

Funzionalità supportate

Amazon Kendra Il connettore di origine dati Salesforce supporta le seguenti funzionalità:

- Mappature dei campi
- Filtraggio del contesto utente
- Scansione delle identità degli utenti
- Filtri di inclusione/esclusione
- Sincronizzazione completa e incrementale dei contenuti
- Scansione degli allegati delle entità
- Virtual Private Cloud (VPC) (Cloud privato virtuale (VPC)

Prerequisiti

Prima di poterla utilizzare Amazon Kendra per indicizzare la tua fonte di dati Salesforce, apporta queste modifiche a Salesforce e agli account. AWS

In Salesforce, assicurati di avere:

- Hai creato un account amministrativo Salesforce e hai annotato il nome utente e la password utilizzati per connetterti a Salesforce.
- Ha copiato il token di sicurezza Salesforce associato all'account utilizzato per connettersi a Salesforce.
- Hai creato un account Salesforce Connected App con OAuth attivato e hai copiato la chiave consumer (ID client) e il segreto del consumatore (segreto del cliente) assegnati alla tua app

Salesforce Connected. Per ulteriori informazioni, consulta la documentazione di Salesforce sulle app connesse.

- Hai copiato l'URL dell'istanza Salesforce che desideri indicizzare. <company>In genere, si tratta di *https:*//.salesforce.com/. Il server deve eseguire un'app connessa a Salesforce.
- Sono state aggiunte credenziali al server Salesforce per un utente con accesso in sola lettura a Salesforce clonando il ReadOnly profilo e quindi aggiungendo le autorizzazioni Visualizza tutti i dati e Gestisci articoli. Queste credenziali identificano l'utente che effettua la connessione e l'app connessa Salesforce a cui si connette. Amazon Kendra
- Controllato, ogni documento è unico in Salesforce e tra le altre fonti di dati che intendi utilizzare per lo stesso indice. Ogni fonte di dati che desideri utilizzare per un indice non deve contenere lo stesso documento in tutte le fonti di dati. Gli ID dei documenti sono globali rispetto a un indice e devono essere univoci per indice.

Nel tuo Account AWS, assicurati di avere:

- Ha creato un Amazon Kendra indice e, se si utilizza l'API, ha annotato l'ID dell'indice.
- Hai creato un IAM ruolo per la tua origine dati e, se utilizzi l'API, hai annotato l'ARN del IAM ruolo.

> **Note**
>
> Se modifichi il tipo di autenticazione e le credenziali, devi aggiornare il IAM ruolo per accedere all'ID AWS Secrets Manager segreto corretto.

- Ha archiviato le credenziali di autenticazione Salesforce in un AWS Secrets Manager segreto e, se si utilizza l'API, ha annotato l'ARN del segreto.

> **Note**
>
> Ti consigliamo di aggiornare o ruotare regolarmente le credenziali e il segreto. Fornisci solo il livello di accesso necessario per la tua sicurezza. Non è consigliabile riutilizzare credenziali e segreti tra diverse fonti di dati e versioni dei connettori 1.0 e 2.0 (ove applicabile).

Se non disponi di un IAM ruolo o di un segreto esistente, puoi utilizzare la console per creare un nuovo IAM ruolo e un Secrets Manager segreto quando connetti la tua fonte di dati Salesforce a.

Amazon Kendra Se utilizzi l'API, devi fornire l'ARN di un IAM ruolo e di un Secrets Manager segreto esistenti e un ID di indice.

Istruzioni di connessione

Per connetterti Amazon Kendra alla tua fonte dati Salesforce, devi fornire i dettagli necessari della fonte dati Salesforce in modo che Amazon Kendra possa accedere ai tuoi dati. Se non hai ancora configurato Salesforce, vedi. Amazon Kendra Prerequisiti

Console

Per connetterti a Amazon Kendra Salesforce:

1. Accedi alla console di AWS gestione e apri la Amazon Kendra console.
2. Dal riquadro di navigazione a sinistra, scegli Indici, quindi scegli l'indice che desideri utilizzare dall'elenco degli indici.

> **Note**
>
> Puoi scegliere di configurare o modificare le impostazioni del controllo dell'accesso degli utenti in Impostazioni dell'indice.

3. Nella pagina Guida introduttiva, scegli Aggiungi origine dati.
4. Nella pagina Aggiungi origine dati, scegli Salesforce connector V2.0, quindi scegli Aggiungi connettore.
5. Nella pagina Specificare i dettagli dell'origine dati, inserisci le seguenti informazioni:
   a. Nome dell'origine dati: immetti un nome per l'origine dati. È possibile includere trattini ma non spazi.
   b. (Facoltativo) Descrizione: immetti una descrizione facoltativa per la tua fonte di dati.
   c. Lingua predefinita: una lingua per filtrare i documenti per l'indice. Se non diversamente specificato, la lingua predefinita è l'inglese. La lingua specificata nei metadati ha la precedenza sulla lingua selezionata.
   d. Seleziona Successivo.
6. Nella pagina Definisci accesso e sicurezza, inserisci le seguenti informazioni:
   a. URL Salesforce: immetti l'URL dell'istanza per il sito Salesforce che desideri indicizzare.

b. Autorizzazione: attiva o disattiva le informazioni dell'elenco di controllo degli accessi (ACL) per i tuoi documenti, se disponi di un ACL e desideri utilizzarlo per il controllo degli accessi. L'ACL specifica a quali documenti possono accedere utenti e gruppi. Le informazioni ACL vengono utilizzate per filtrare i risultati della ricerca in base all'accesso dell'utente o del relativo gruppo ai documenti. Per ulteriori informazioni, consulta Filtraggio del contesto utente.

c. Inserisci un segreto esistente o se ne crei uno nuovo, si apre una finestra AWS Secrets Manager segreta.

   - Autenticazione: inserisci le seguenti informazioni nella finestra Crea un AWS Secrets Manager segreto:

     A. Nome segreto: un nome per il tuo segreto. Il prefisso 'AmazonKendra-Salesforce-' viene aggiunto automaticamente al nome segreto.

     B. Per nome utente, password, token di sicurezza, chiave utente, segreto utente e URL di autenticazione, inserisci i valori delle credenziali di autenticazione che hai generato e scaricato dal tuo account Salesforce.

     C. Scegli Salva autenticazione.

d. Virtual Private Cloud (VPC): puoi scegliere di utilizzare un VPC. In tal caso, è necessario aggiungere sottoreti e gruppi di sicurezza VPC.

e. Identity crawler: specifica se attivare il crawler di identità. Amazon Kendra Il crawler di identità utilizza le informazioni dell'elenco di controllo degli accessi (ACL) per i documenti per filtrare i risultati della ricerca in base all'accesso dell'utente o del gruppo di appartenenza ai documenti. Se disponi di un ACL per i tuoi documenti e scegli di utilizzarlo, puoi anche scegliere di attivare il crawler di identità per configurare il filtraggio Amazon Kendra contestuale dell'utente dei risultati di ricerca. Altrimenti, se il crawler di identità è disattivato, tutti i documenti possono essere ricercati pubblicamente. Se desideri utilizzare il controllo degli accessi per i tuoi documenti e il crawler di identità è disattivato, in alternativa puoi utilizzare l'PutPrincipalMappingAPI per caricare le informazioni di accesso di utenti e gruppi per il filtraggio del contesto degli utenti.

f. IAM ruolo: scegli un IAM ruolo esistente o creane uno nuovo IAM per accedere alle credenziali del repository e indicizzare il contenuto.

> **Note**
>
> IAM i ruoli utilizzati per gli indici non possono essere utilizzati per le fonti di dati. Se non sei sicuro che un ruolo esistente venga utilizzato per un indice o una FAQ, scegli Crea un nuovo ruolo per evitare errori.

g. Seleziona Successivo.

7. Nella pagina Configura le impostazioni di sincronizzazione, inserisci le seguenti informazioni:

   a. Per indicizzare gli allegati: seleziona per eseguire la scansione di tutti gli oggetti Salesforce collegati.

   b. Per gli oggetti Standard, gli oggetti Standard con allegati e gli Oggetti Standard senza allegati e Knowledge Articles, seleziona le entità o i tipi di contenuto Salesforce che desideri sottoporre a scansione.

   c. È necessario fornire informazioni di configurazione per l'indicizzazione di almeno uno degli oggetti standard, degli articoli di conoscenza o dei feed di Chatter. Se scegli di eseguire la scansione degli articoli di Knowledge, devi specificare i tipi di articoli della Knowledge Base da indicizzare. Puoi scegliere bozze e allegati pubblicati, archiviati.

      Filtro Regex: specifica un modello regex per includere elementi specifici del catalogo.

8. Per una configurazione aggiuntiva:

   - Informazioni ACL Tutti gli elenchi di controllo degli accessi sono inclusi per impostazione predefinita. La deselezione di un elenco di controllo degli accessi renderà pubblici tutti i file di quella categoria.
   - Modelli Regex: aggiungono modelli di espressioni regolari per includere o escludere determinati file. È possibile aggiungere fino a 100 pattern.

   Modalità di sincronizzazione: scegli come aggiornare l'indice quando il contenuto dell'origine dati cambia. Quando sincronizzi l'origine dati con Amazon Kendra per la prima volta, tutto il contenuto viene sottoposto a scansione e indicizzato per impostazione predefinita. Se la sincronizzazione iniziale non è riuscita, devi eseguire una sincronizzazione completa dei dati, anche se non scegli la sincronizzazione completa come opzione della modalità di sincronizzazione.

- Sincronizzazione completa: indicizza di nuovo tutti i contenuti, sostituendo i contenuti esistenti ogni volta che l'origine dati si sincronizza con l'indice.
- Nuova sincronizzazione modificata: indicizza solo i contenuti nuovi e modificati ogni volta che l'origine dati si sincronizza con l'indice. Amazon Kendra può utilizzare il meccanismo dell'origine dati per tenere traccia delle modifiche ai contenuti e indicizzare i contenuti modificati dall'ultima sincronizzazione.
- Sincronizzazione nuova, modificata ed eliminata: indicizza solo i contenuti nuovi, modificati ed eliminati ogni volta che l'origine dati si sincronizza con l'indice. Amazon Kendra può utilizzare il meccanismo dell'origine dati per tenere traccia delle modifiche ai contenuti e indicizzare i contenuti modificati dall'ultima sincronizzazione.

9. Seleziona Successivo.
10. Nella pagina Imposta mappature dei campi, inserisci le seguenti informazioni:

    a. Per gli articoli Standard Knowledge, gli allegati degli oggetti standard e le mappature di campo consigliate aggiuntive, seleziona uno dei campi di origine dati predefiniti Amazon Kendra generati che desideri mappare all'indice.

    > **Note**
    >
    > È richiesta una mappatura dell'indice a. `_document_body` Non è possibile modificare la mappatura tra il `Salesforce ID` campo e il Amazon Kendra `_document_id` campo. Puoi mappare qualsiasi campo Salesforce ai campi indice riservati/predefiniti del titolo o del corpo del documento di Amazon Kendra.

    b. Aggiungi campo: consente di aggiungere campi di origine dati personalizzati per creare un nome di campo indice a cui mappare e il tipo di dati del campo.

    c. Seleziona Successivo.

11. Nella pagina Rivedi e crea, verifica che le informazioni inserite siano corrette, quindi seleziona Aggiungi origine dati. Puoi anche scegliere di modificare le tue informazioni da questa pagina. L'origine dati verrà visualizzata nella pagina Origini dati dopo che l'origine dati sarà stata aggiunta correttamente.

API

Per connettersi Amazon Kendra a Salesforce

È necessario specificare un codice JSON dello schema dell'origine dati utilizzando l'API. TemplateConfiguration È necessario fornire le seguenti informazioni:

- Origine dati: specifica il tipo di origine dati come `SALESFORCEV2` quando usi lo schema TemplateConfigurationJSON. Specificate anche l'origine dati come `TEMPLATE` quando chiamate l'CreateDataSourceAPI.
- URL host: specifica l'URL dell'host dell'istanza Salesforce.
- Modalità di sincronizzazione: specifica come Amazon Kendra aggiornare l'indice quando il contenuto dell'origine dati cambia. Quando sincronizzi l'origine dati con Amazon Kendra per la prima volta, tutto il contenuto viene sottoposto a scansione e indicizzato per impostazione predefinita. Se la sincronizzazione iniziale non è riuscita, devi eseguire una sincronizzazione completa dei dati, anche se non scegli la sincronizzazione completa come opzione della modalità di sincronizzazione. Puoi scegliere tra:
  - `FORCED_FULL_CRAWL`per indicizzare nuovamente tutti i contenuti, sostituendo i contenuti esistenti ogni volta che l'origine dati si sincronizza con l'indice.
  - `FULL_CRAWL`per indicizzare solo i contenuti nuovi, modificati ed eliminati ogni volta che l'origine dati si sincronizza con l'indice. Amazon Kendra può utilizzare il meccanismo dell'origine dati per tenere traccia delle modifiche ai contenuti e indicizzare i contenuti modificati dall'ultima sincronizzazione.
  - `CHANGE_LOG`per indicizzare solo contenuti nuovi e modificati ogni volta che l'origine dati si sincronizza con l'indice. Amazon Kendra può utilizzare il meccanismo dell'origine dati per tenere traccia delle modifiche ai contenuti e indicizzare i contenuti modificati dall'ultima sincronizzazione.
- Secret Amazon Resource Name (ARN): fornisci l'Amazon Resource Name (ARN) di un Secrets Manager segreto che contiene le credenziali di autenticazione per il tuo account Salesforce. Il segreto è archiviato in una struttura JSON con le seguenti chiavi:

```
{
    "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**
>
> Ti consigliamo di aggiornare o ruotare regolarmente le credenziali e il segreto. Fornisci solo il livello di accesso necessario per la tua sicurezza. Non è consigliabile riutilizzare credenziali e segreti tra diverse fonti di dati e versioni dei connettori 1.0 e 2.0 (ove applicabile).

- IAM ruolo: specifica `RoleArn` quando chiami `CreateDataSource` per fornire a un IAM ruolo le autorizzazioni per accedere al tuo Secrets Manager segreto e per chiamare le API pubbliche richieste per il connettore Salesforce e. Amazon Kendra Per ulteriori informazioni, consulta i IAM ruoli per le fonti di dati Salesforce.

Puoi anche aggiungere le seguenti funzionalità opzionali:

- Virtual Private Cloud (VPC): `VpcConfiguration` specifica quando si chiama. `CreateDataSource` Per ulteriori informazioni, consulta Configurazione Amazon Kendra per l'utilizzo di un Amazon VPC.
- Filtri di inclusione ed esclusione: puoi specificare se includere o escludere determinati documenti, account, campagne, casi, contatti, lead, opportunità, soluzioni, attività, gruppi, chat e file di entità personalizzati.

> **Note**
>
> La maggior parte delle fonti di dati utilizza modelli di espressioni regolari, che sono modelli di inclusione o esclusione denominati filtri. Se si specifica un filtro di inclusione, viene indicizzato solo il contenuto che corrisponde al filtro di inclusione. Qualsiasi documento che non corrisponde al filtro di inclusione non viene indicizzato. Se si specifica un filtro di inclusione ed esclusione, i documenti che corrispondono al filtro di esclusione non vengono indicizzati, anche se corrispondono al filtro di inclusione.

- Identity crawler: specifica se attivare il crawler di identità. Amazon Kendra Il crawler di identità utilizza le informazioni dell'elenco di controllo degli accessi (ACL) per i documenti

per filtrare i risultati della ricerca in base all'accesso dell'utente o del gruppo di appartenenza ai documenti. Se disponi di un ACL per i tuoi documenti e scegli di utilizzarlo, puoi anche scegliere di attivare il crawler di identità per configurare il filtraggio Amazon Kendra contestuale dell'utente dei risultati di ricerca. Altrimenti, se il crawler di identità è disattivato, tutti i documenti possono essere ricercati pubblicamente. Se desideri utilizzare il controllo degli accessi per i tuoi documenti e il crawler di identità è disattivato, in alternativa puoi utilizzare l'PutPrincipalMappingAPI per caricare le informazioni di accesso di utenti e gruppi per il filtraggio del contesto degli utenti.

- Mappature dei campi: scegli di mappare i campi delle sorgenti dati di Salesforce ai campi indice. Amazon Kendra Per ulteriori informazioni, consulta la sezione Mappatura dei campi di origine dei dati.

> **Note**
>
> Il campo del corpo del documento o l'equivalente del corpo del documento per i documenti è necessario per eseguire la ricerca nei documenti. Amazon Kendra È necessario mappare il nome del campo del corpo del documento nella fonte dati al nome del campo indice`_document_body`. Tutti gli altri campi sono facoltativi.

Per un elenco di altre importanti chiavi JSON da configurare, consultaSchema del modello Salesforce.

Ulteriori informazioni

Per saperne di più sull'integrazione Amazon Kendra con la tua fonte di dati Salesforce, consulta:

- Annuncio del connettore Salesforce aggiornato (V2) per Amazon Kendra

ServiceNow

ServiceNow fornisce un sistema di gestione dei servizi basato sul cloud per creare e gestire flussi di lavoro a livello di organizzazione, come servizi IT, sistemi di ticketing e supporto. È possibile utilizzarlo Amazon Kendra per indicizzare i ServiceNow cataloghi, gli articoli informativi, gli incidenti e i relativi allegati.

Puoi connetterti Amazon Kendra alla tua fonte di ServiceNow dati utilizzando la Amazon Kendra console, l'TemplateConfigurationAPI o l'API. ServiceNowConfiguration

Amazon Kendra dispone di due versioni del ServiceNow connettore. Le funzionalità supportate di ogni versione includono:

ServiceNow connettore V1.0/API ServiceNowConfiguration

- Mappature dei campi
- ServiceNow versioni di istanza: London, Others
- Modelli di inclusione/esclusione: cataloghi di servizi, articoli conoscitivi, allegati

ServiceNow connettore TemplateConfigurationV2.0/API

- mappature dei campi
- Filtraggio del contesto utente
- Filtri di inclusione/esclusione
- Sincronizzazione completa e incrementale dei contenuti
- ServiceNow versioni di istanza: Roma, Sandiego, Tokyo, Altre
- Virtual Private Cloud (VPC) (Cloud privato virtuale (VPC)

> **Note**
>
> Il supporto per il ServiceNow connettore ServiceNowConfiguration V1.0/API dovrebbe terminare nel 2023. Ti consigliamo di eseguire la migrazione o l'utilizzo del ServiceNow connettore V2.0/API. TemplateConfiguration

Per la risoluzione dei problemi relativi al connettore di origine Amazon Kendra ServiceNow dati, consulta. Risoluzione dei problemi relativi alle origini dati

Argomenti

- ServiceNow connettore V1.0
- ServiceNow connettore V2.0
- Specificare i documenti da indicizzare con una query

ServiceNow connettore V1.0

ServiceNow fornisce un sistema di gestione dei servizi basato sul cloud per creare e gestire flussi di lavoro a livello di organizzazione, come servizi IT, sistemi di ticketing e supporto. È possibile utilizzarlo Amazon Kendra per indicizzare i ServiceNow cataloghi, gli articoli informativi e i relativi allegati.

> **Note**
>
> Il supporto per il ServiceNow connettore ServiceNowConfiguration V1.0/API dovrebbe terminare nel 2023. Ti consigliamo di eseguire la migrazione o l'utilizzo del ServiceNow connettore V2.0/API. TemplateConfiguration

Per la risoluzione dei problemi relativi al connettore di origine Amazon Kendra ServiceNow dati, consulta. Risoluzione dei problemi relativi alle origini dati

Argomenti

Funzionalità supportate

Amazon Kendra ServiceNow il connettore di origine dati supporta le seguenti funzionalità:

- ServiceNow versioni di istanza: London, Others
- Modelli di inclusione/esclusione: cataloghi di servizi, articoli conoscitivi e relativi allegati

Prerequisiti

Prima di utilizzarla Amazon Kendra per indicizzare la tua fonte di ServiceNow dati, apporta queste modifiche al tuo account e ai tuoi account. ServiceNow AWS

Nel ServiceNow, assicurati di avere:

- Hai creato un account ServiceNow amministratore e hai creato un' ServiceNowistanza.
- Hai copiato l'host dell'URL dell' ServiceNow istanza. Ad esempio, se l'URL dell'istanza è *https://your-domain.service-now.com*, il formato per l'URL dell'host che inserisci è *your-domain.service-now.com*.
- Hai annotato le tue credenziali di autenticazione di base contenenti un nome utente e una password per consentire la connessione all'istanza. Amazon Kendra ServiceNow
- Facoltativo: hai configurato un token di credenziali OAuth 2.0 in grado di identificare Amazon Kendra e generare un nome utente, una password, un ID client e un segreto client. Il nome utente e la password devono consentire l'accesso alla ServiceNow knowledge base e al catalogo dei servizi. Per ulteriori informazioni, ServiceNow consulta la documentazione sull'autenticazione OAuth 2.0.
- Sono state aggiunte le seguenti autorizzazioni:
  - kb_category
  - kb_conoscenza
  - kb_knowledgebase
  - kb_uc_cannot_read_mtom
  - kb_uc_can_read_mtom
  - sc_catalogo
  - sc_category
  - sc_cat_item
  - sys_attachment
  - sys_attachment_doc
  - sys_user_role
- È stato selezionato che ogni documento sia unico all'interno ServiceNow e tra le altre fonti di dati che intendi utilizzare per lo stesso indice. Ogni fonte di dati che desideri utilizzare per un indice non deve contenere lo stesso documento in tutte le fonti di dati. Gli ID dei documenti sono globali rispetto a un indice e devono essere univoci per indice.

Nel tuo Account AWS, assicurati di avere:

- Ha creato un Amazon Kendra indice e, se si utilizza l'API, ha annotato l'ID dell'indice.
- Hai creato un IAM ruolo per la tua origine dati e, se utilizzi l'API, hai annotato l'ARN del IAM ruolo.

> **Note**
>
> Se modifichi il tipo di autenticazione e le credenziali, devi aggiornare il IAM ruolo per accedere all'ID AWS Secrets Manager segreto corretto.

- Ha archiviato le credenziali di ServiceNow autenticazione in un AWS Secrets Manager segreto e, se si utilizza l'API, ha annotato l'ARN del segreto.

> **Note**
>
> Ti consigliamo di aggiornare o ruotare regolarmente le credenziali e il segreto. Fornisci solo il livello di accesso necessario per la tua sicurezza. Non è consigliabile riutilizzare credenziali e segreti tra diverse fonti di dati e versioni dei connettori 1.0 e 2.0 (ove applicabile).

Se non disponi di un IAM ruolo o di un segreto esistente, puoi utilizzare la console per creare un nuovo IAM ruolo e un Secrets Manager segreto quando connetti la tua origine ServiceNow dati a. Amazon Kendra Se utilizzi l'API, devi fornire l'ARN di un IAM ruolo e di un Secrets Manager segreto esistenti e un ID di indice.

Istruzioni di connessione

Per connetterti Amazon Kendra alla tua fonte di ServiceNow dati, devi fornire i dettagli necessari della tua origine ServiceNow dati in modo che Amazon Kendra possa accedere ai tuoi dati. Se non lo hai ancora configurato ServiceNow per Amazon Kendra seePrerequisiti.

Console

Per connettersi Amazon Kendra a ServiceNow

1. Accedi alla console di AWS gestione e apri la Amazon Kendra console.
2. Dal riquadro di navigazione a sinistra, scegli Indici, quindi scegli l'indice che desideri utilizzare dall'elenco degli indici.

> **Note**
>
> Puoi scegliere di configurare o modificare le impostazioni del controllo dell'accesso degli utenti in Impostazioni dell'indice.

3. Nella pagina Guida introduttiva, scegli Aggiungi origine dati.
4. Nella pagina Aggiungi origine dati, scegli il ServiceNowconnettore V1.0, quindi scegli Aggiungi origine dati.
5. Nella pagina Specificare i dettagli dell'origine dati, inserisci le seguenti informazioni:
   a. In Nome e descrizione, per Nome dell'origine dati, inserisci un nome per l'origine dati. Puoi includere trattini ma non spazi.
   b. (Facoltativo) Descrizione: immetti una descrizione facoltativa per l'origine dati.
   c. In Lingua predefinita: scegli una lingua per filtrare i documenti per l'indice. Se non diversamente specificato, la lingua predefinita è l'inglese. La lingua specificata nei metadati del documento ha la precedenza sulla lingua selezionata.
   d. In Tag, per Aggiungi nuovo tag, includi tag opzionali per cercare e filtrare le risorse o tenere traccia dei costi. AWS
   e. Seleziona Successivo.
6. Nella pagina Definisci accesso e sicurezza, inserisci le seguenti informazioni:
   a. ServiceNow host: immetti l'URL dell' ServiceNowhost.
   b. ServiceNow versione: seleziona la tua ServiceNow versione.
   c. Scegli tra l'autenticazione di base e l'autenticazione Oauth 2.0 in base al tuo caso d'uso.
   d. AWS Secrets Manager segreto: scegli un segreto esistente o creane uno nuovo per memorizzare le Secrets Manager ServiceNow credenziali di autenticazione. Se scegli di creare un nuovo segreto, si apre una finestra AWS Secrets Manager segreta.
      i. Nome segreto: un nome per il tuo segreto. Il prefisso 'AmazonKendra- ServiceNow -' viene aggiunto automaticamente al nome segreto.
      ii. Se utilizzi l'autenticazione di base, inserisci il nome segreto, il nome utente e la password per il tuo account. ServiceNow

Se utilizzi l'autenticazione OAuth2, inserisci il nome segreto, il nome utente, la password, l'ID cliente e il segreto del cliente che hai creato nel tuo account. ServiceNow

iii. Scegli Salva e aggiungi segreto.

e. IAM ruolo: scegli un IAM ruolo esistente o crea un nuovo IAM ruolo per accedere alle credenziali del repository e indicizzare il contenuto.

> **Note**
>
> IAM i ruoli utilizzati per gli indici non possono essere utilizzati per le fonti di dati. Se non sei sicuro che un ruolo esistente venga utilizzato per un indice o una FAQ, scegli Crea un nuovo ruolo per evitare errori.

f. Seleziona Successivo.

7. Nella pagina Configura le impostazioni di sincronizzazione, inserisci le seguenti informazioni:

a. Includi articoli informativi: scegli di indicizzare gli articoli della conoscenza.

b. Tipo di articoli informativi: scegli tra Includi solo articoli pubblici e Includi articoli in base a una query di ServiceNow filtro in base al tuo caso d'uso. Se selezioni Includi articoli in base alla query di ServiceNow filtro, devi inserire una query di filtro copiata dal tuo ServiceNow account.

c. Includi gli allegati degli articoli informativi: scegli di indicizzare gli allegati degli articoli informativi. Puoi anche selezionare tipi di file specifici da indicizzare.

d. Includi elementi del catalogo: scegli di indicizzare gli articoli del catalogo.

e. Includi gli allegati degli articoli del catalogo: scegli di indicizzare gli allegati degli articoli del catalogo. Puoi anche selezionare tipi di file specifici da indicizzare.

f. Frequenza: con quale frequenza Amazon Kendra verrà eseguita la sincronizzazione con la fonte di dati.

g. Seleziona Successivo.

8. Nella pagina Imposta le mappature dei campi, inserisci le seguenti informazioni:

a. Articoli informativi e Catalogo dei servizi: seleziona tra i campi delle origini dati predefiniti Amazon Kendra generati e le mappature di campo aggiuntive suggerite che desideri mappare all'indice.

b. Aggiungi campo: consente di aggiungere campi di origine dati personalizzati per creare un nome di campo indice a cui mappare e il tipo di dati del campo.

c. Seleziona Successivo.

9. Nella pagina Rivedi e crea, verifica che le informazioni inserite siano corrette, quindi seleziona Aggiungi origine dati. Puoi anche scegliere di modificare le tue informazioni da questa pagina. L'origine dati verrà visualizzata nella pagina Origini dati dopo che l'origine dati sarà stata aggiunta correttamente.

API

Per connettersi Amazon Kendra a ServiceNow

È necessario specificare quanto segue utilizzando l'ServiceNowConfiguration API:

- URL dell'origine dati: specificare l' ServiceNow URL. *L'endpoint host dovrebbe avere il seguente aspetto: your-domain.service-now.com.*
- Istanza host di origine dati: specifica la versione dell'istanza host come o. ServiceNow `LONDON` `OTHERS`
- Secret Amazon Resource Name (ARN): fornisci l'Amazon Resource Name (ARN) di un Secrets Manager segreto che contiene le credenziali di autenticazione che hai creato nel tuo account. ServiceNow

  Se utilizzi l'autenticazione di base, il segreto viene archiviato in una struttura JSON con le seguenti chiavi:

  ```
  {
      "username": "user name",
      "password": "password"
  }
  ```

  Se utilizzi l'autenticazione OAuth2, il segreto viene archiviato in una struttura JSON con le seguenti chiavi:

  ```
  {
      "username": "user name",
      "password": "password",
      "clientId": "client id",
      "clientSecret": "client secret"
  ```

```
}
```

> **Note**
>
> Ti consigliamo di aggiornare o ruotare regolarmente le credenziali e il segreto. Fornisci solo il livello di accesso necessario per la tua sicurezza. Non è consigliabile riutilizzare credenziali e segreti tra diverse fonti di dati e versioni dei connettori 1.0 e 2.0 (ove applicabile).

- IAM ruolo: specifica `RoleArn` quando chiami `CreateDataSource` per fornire a un IAM ruolo le autorizzazioni per accedere al tuo Secrets Manager segreto e per chiamare le API pubbliche richieste per il connettore e. ServiceNow Amazon Kendra Per ulteriori informazioni, consulta i IAM ruoli per ServiceNow le fonti di dati.

Puoi anche aggiungere le seguenti funzionalità opzionali:

- Mappature dei campi: scegli di mappare i campi delle sorgenti ServiceNow dati Amazon Kendra ai campi indice. Per ulteriori informazioni, consulta la sezione Mappatura dei campi di origine dei dati.

> **Note**
>
> Il campo del corpo del documento o l'equivalente del corpo del documento per i documenti è necessario per Amazon Kendra eseguire la ricerca nei documenti. È necessario mappare il nome del campo del corpo del documento nella fonte dati al nome del campo indice`_document_body`. Tutti gli altri campi sono facoltativi.

- Filtri di inclusione ed esclusione: specificate se includere o escludere determinati file allegati di cataloghi e articoli informativi.

> **Note**
>
> La maggior parte delle fonti di dati utilizza modelli di espressioni regolari, che sono modelli di inclusione o esclusione denominati filtri. Se si specifica un filtro di inclusione, viene indicizzato solo il contenuto che corrisponde al filtro di inclusione. Qualsiasi documento che non corrisponde al filtro di inclusione non viene indicizzato. Se si

specifica un filtro di inclusione ed esclusione, i documenti che corrispondono al filtro di esclusione non vengono indicizzati, anche se corrispondono al filtro di inclusione.

- Parametri di indicizzazione: puoi anche scegliere di specificare se:
  - Indicizza gli articoli informativi e i cataloghi di servizi, o entrambi. Se si sceglie di indicizzare gli articoli della Knowledge Base e gli elementi del catalogo dei servizi, è necessario fornire il nome del ServiceNow campo mappato al campo del contenuto del documento indicizzato nell' Amazon Kendra indice.
  - Indicizza gli allegati agli articoli di approfondimento e agli elementi del catalogo.
  - Utilizza una ServiceNow query che seleziona i documenti da una o più basi di conoscenza. Le basi di conoscenza possono essere pubbliche o private. Per ulteriori informazioni, consulta la sezione Specifica dei documenti da indicizzare con una query.

Ulteriori informazioni

Per ulteriori informazioni sull'integrazione Amazon Kendra con la tua fonte di ServiceNow dati, consulta:

- Guida introduttiva a Amazon Kendra ServiceNow Online connector

ServiceNow connettore V2.0

ServiceNow fornisce un sistema di gestione dei servizi basato sul cloud per creare e gestire flussi di lavoro a livello di organizzazione, come servizi IT, sistemi di ticketing e supporto. È possibile utilizzarlo Amazon Kendra per indicizzare i ServiceNow cataloghi, gli articoli informativi, gli incidenti e i relativi allegati.

Per la risoluzione dei problemi relativi al connettore di origine Amazon Kendra ServiceNow dati, consulta. Risoluzione dei problemi relativi alle origini dati

Argomenti

- Funzionalità supportate
- Prerequisiti
- Istruzioni di connessione
- Ulteriori informazioni

Funzionalità supportate

Amazon Kendra ServiceNow il connettore di origine dati supporta le seguenti funzionalità:

- mappature dei campi
- Filtraggio del contesto utente
- Filtri di inclusione/esclusione
- Sincronizzazione completa e incrementale dei contenuti
- ServiceNow versioni di istanza: Roma, Sandiego, Tokyo, Altre
- Virtual Private Cloud (VPC) (Cloud privato virtuale (VPC)

Prerequisiti

Prima di poterla utilizzare Amazon Kendra per indicizzare la tua fonte di ServiceNow dati, apporta queste modifiche al tuo AWS account ServiceNow e ai tuoi account.

Nel ServiceNow, assicurati di avere:

- Hai creato un'istanza Personal o Enterprise Developer e disponi di un' ServiceNowistanza con un ruolo amministrativo.
- Hai copiato l'host dell'URL dell' ServiceNow istanza. Il formato per l'URL dell'host che inserisci è *`your-domain.service-now.com`*. Ti serve l'URL dell'istanza a cui connetterti. ServiceNow Amazon Kendra
- Hai annotato le tue credenziali di autenticazione di base, un nome utente e una password per consentirti Amazon Kendra di connetterti all' ServiceNow istanza.
- Facoltativo: credenziali client OAuth 2.0 configurate che possono essere identificate Amazon Kendra utilizzando un nome utente, una password, un ID client generato e un segreto client. Per ulteriori informazioni, ServiceNow consulta la documentazione sull'autenticazione OAuth 2.0.
- È stato verificato che ogni documento sia unico nelle ServiceNow altre fonti di dati che intendi utilizzare per lo stesso indice. Ogni fonte di dati che desideri utilizzare per un indice non deve contenere lo stesso documento in tutte le fonti di dati. Gli ID dei documenti sono globali rispetto a un indice e devono essere univoci per indice.

Nel tuo Account AWS, assicurati di avere:

- Ha creato un Amazon Kendra indice e, se si utilizza l'API, ha annotato l'ID dell'indice.

- Hai creato un IAM ruolo per la tua origine dati e, se utilizzi l'API, hai annotato l'ARN del IAM ruolo.

> **Note**
>
> Se modifichi il tipo di autenticazione e le credenziali, devi aggiornare il IAM ruolo per accedere all'ID AWS Secrets Manager segreto corretto.

- Ha archiviato le credenziali di ServiceNow autenticazione in un AWS Secrets Manager segreto e, se si utilizza l'API, ha annotato l'ARN del segreto.

> **Note**
>
> Ti consigliamo di aggiornare o ruotare regolarmente le credenziali e il segreto. Fornisci solo il livello di accesso necessario per la tua sicurezza. Non è consigliabile riutilizzare credenziali e segreti tra diverse fonti di dati e versioni dei connettori 1.0 e 2.0 (ove applicabile).

Se non disponi di un IAM ruolo o di un segreto esistente, puoi utilizzare la console per creare un nuovo IAM ruolo e un Secrets Manager segreto quando connetti la tua origine ServiceNow dati a. Amazon Kendra Se utilizzi l'API, devi fornire l'ARN di un IAM ruolo e di un Secrets Manager segreto esistenti e un ID di indice.

Istruzioni di connessione

Per connetterti Amazon Kendra alla tua fonte di ServiceNow dati, devi fornire i dettagli necessari della tua origine ServiceNow dati in modo che Amazon Kendra possa accedere ai tuoi dati. Se non lo hai ancora configurato ServiceNow per Amazon Kendra seePrerequisiti.

Console

Per connettersi Amazon Kendra a ServiceNow

1. Accedi alla console di AWS gestione e apri la Amazon Kendra console.
2. Dal riquadro di navigazione a sinistra, scegli Indici, quindi scegli l'indice che desideri utilizzare dall'elenco degli indici.

> **Note**
>
> Puoi scegliere di configurare o modificare le impostazioni del controllo dell'accesso degli utenti in Impostazioni dell'indice.

3. Nella pagina Guida introduttiva, scegli Aggiungi origine dati.
4. Nella pagina Aggiungi origine dati, scegli il ServiceNowconnettore V2.0, quindi scegli Aggiungi origine dati.
5. Nella pagina Specificare i dettagli dell'origine dati, inserisci le seguenti informazioni:
   a. In Nome e descrizione, per Nome dell'origine dati, inserisci un nome per l'origine dati. Puoi includere trattini ma non spazi.
   b. (Facoltativo) Descrizione: immetti una descrizione facoltativa per l'origine dati.
   c. In Lingua predefinita: scegli una lingua per filtrare i documenti per l'indice. Se non diversamente specificato, la lingua predefinita è l'inglese. La lingua specificata nei metadati del documento ha la precedenza sulla lingua selezionata.
   d. In Tag, per Aggiungi nuovo tag, includi tag opzionali per cercare e filtrare le risorse o tenere traccia dei costi. AWS
   e. Seleziona Successivo.
6. Nella pagina Definisci accesso e sicurezza, inserisci le seguenti informazioni:
   a. ServiceNow host: immetti l'URL dell' ServiceNowhost. Il formato per l'URL dell'host che inserisci è *your-domain.service-now.com*.
   b. ServiceNow versione: seleziona ServiceNow la versione dell'istanza. Puoi scegliere tra Roma, Sandiego, Tokyo o Altri.
   c. Autorizzazione: attiva o disattiva le informazioni dell'elenco di controllo degli accessi (ACL) per i tuoi documenti, se disponi di un ACL e desideri utilizzarlo per il controllo degli accessi. L'ACL specifica a quali documenti possono accedere utenti e gruppi. Le informazioni ACL vengono utilizzate per filtrare i risultati della ricerca in base all'accesso dell'utente o del relativo gruppo ai documenti. Per ulteriori informazioni, consulta Filtraggio del contesto utente.
   d. Autenticazione: scegli tra l'autenticazione di base e l'autenticazione OAuth 2.0.
   e. AWS Secrets Manager segreto: scegli un segreto esistente o creane uno nuovo per memorizzare le Secrets Manager credenziali di autenticazione. ServiceNow Se scegli di

creare un nuovo segreto, si apre una finestra AWS Secrets Manager segreta. Inserisci le seguenti informazioni nella finestra:

i. Nome segreto: un nome per il tuo segreto. Il prefisso 'AmazonKendra- ServiceNow -' viene aggiunto automaticamente al nome segreto.

ii. Se utilizzi l'autenticazione di base, inserisci il nome segreto, il nome utente e la password per il tuo account. ServiceNow

Se utilizzi l'autenticazione OAuth2.0, inserisci il nome segreto, il nome utente, la password, l'ID cliente e il segreto del cliente che hai creato nel tuo account. ServiceNow

iii. Scegli Salva e aggiungi segreto.

f. Virtual Private Cloud (VPC): puoi scegliere di utilizzare un VPC. In tal caso, è necessario aggiungere sottoreti e gruppi di sicurezza VPC.

g. Identity crawler: specifica se attivare il crawler di identità. Amazon Kendra Il crawler di identità utilizza le informazioni dell'elenco di controllo degli accessi (ACL) per i documenti per filtrare i risultati della ricerca in base all'accesso dell'utente o del relativo gruppo ai documenti. Se disponi di un ACL per i tuoi documenti e scegli di utilizzarlo, puoi anche scegliere di attivare il crawler di identità per configurare il filtraggio Amazon Kendra contestuale dell'utente dei risultati di ricerca. Altrimenti, se il crawler di identità è disattivato, tutti i documenti possono essere ricercati pubblicamente. Se desideri utilizzare il controllo degli accessi per i tuoi documenti e il crawler di identità è disattivato, in alternativa puoi utilizzare l'PutPrincipalMappingAPI per caricare le informazioni di accesso di utenti e gruppi per il filtraggio del contesto degli utenti.

h. IAM ruolo: scegli un IAM ruolo esistente o creane uno nuovo IAM per accedere alle credenziali del repository e indicizzare il contenuto.

> **Note**
>
> IAM i ruoli utilizzati per gli indici non possono essere utilizzati per le fonti di dati. Se non sei sicuro che un ruolo esistente venga utilizzato per un indice o una FAQ, scegli Crea un nuovo ruolo per evitare errori.

i. Seleziona Successivo.

7. Nella pagina Configura le impostazioni di sincronizzazione, inserisci le seguenti informazioni:

a. Per gli articoli di Knowledge, scegli una delle seguenti opzioni:

- Articoli della conoscenza: scegli di indicizzare gli articoli della conoscenza.
- Allegati degli articoli informativi: scegli di indicizzare gli allegati degli articoli informativi.
- Tipo di articoli informativi: scegli tra Solo articoli pubblici e Articoli di Knowledge in base alla query di ServiceNow filtro in base al tuo caso d'uso. Se selezioni Includi articoli in base alla query di ServiceNow filtro, devi inserire una query di filtro copiata dal tuo ServiceNow account. *Le query di filtro di esempio includono: workflow_state=draft^eq, kb_knowledge_base=dfc19531bf2021003f07e2c1ac0739ab^text ISNOTEMPTY^EQ, article_type=text^active=true^eq.*

  > **Important**
  >
  > Se scegli di eseguire la ricerca per indicizzazione Solo articoli pubblici, Amazon Kendra esegue la ricerca per indicizzazione solo degli articoli della conoscenza a cui è stato assegnato un ruolo di accesso pubblico in ServiceNow.

- Includi articoli in base al filtro di descrizione breve: specifica i modelli di espressioni regolari per includere o escludere articoli specifici.

b. Per gli articoli del catalogo Service:

- Elementi del catalogo dei servizi: scegliere di indicizzare gli articoli del catalogo dei servizi.
- Allegati degli elementi del catalogo dei servizi: scegliere di indicizzare gli allegati degli elementi del catalogo dei servizi.
- Elementi del catalogo dei servizi attivi: scegliere di indicizzare gli articoli del catalogo dei servizi attivi.
- Elementi del catalogo dei servizi inattivi: scegliere di indicizzare gli articoli del catalogo dei servizi inattivi.
- Interrogazione di filtro: consente di includere gli elementi del catalogo dei servizi in base a un filtro definito nell'istanza. ServiceNow *Le query di filtro di esempio includono: short_descriptionLikeAccess^category=2809952237b1300054b6a3549dbe5dd4 nameStartsWithService^active=true^eq.*

- Includi gli elementi del catalogo dei servizi in base al filtro di descrizione breve: specifica un modello regex per includere elementi specifici del catalogo.

c. Per gli incidenti:

- Incidenti: scegliere di indicizzare gli incidenti di servizio.
- Allegati degli incidenti: scegliere di indicizzare gli allegati degli incidenti.
- Incidenti attivi: scegliere di indicizzare gli incidenti attivi.
- Incidenti inattivi: scegliere di indicizzare gli incidenti inattivi.
- Tipo di incidente attivo: scegli tra Tutti gli incidenti, Incidenti aperti, Incidenti aperti - non assegnati e Incidenti risolti a seconda del caso d'uso.
- Interrogazione di filtro: scegli di includere gli incidenti in base a un filtro definito nell'istanza. ServiceNow *Le query di filtro di esempio includono: short_descriptionLikeTest^urgency=3^state=1^eq, priority=2^category=software^eq.*
- Includi incidenti in base a un filtro di descrizione breve: specifica un modello regex per includere incidenti specifici.

d. Per una configurazione aggiuntiva:

- Informazioni ACL: gli elenchi di controllo degli accessi per le entità selezionate sono inclusi per impostazione predefinita. La deselezione di un elenco di controllo degli accessi renderà pubblici tutti i file di quella categoria. Le opzioni ACL vengono disattivate automaticamente per le entità non selezionate. Per gli articoli pubblici l'ACL non viene applicato.
- Per la dimensione massima del file: specifica il limite di dimensione del file in MB che Amazon Kendra scansionerà. Amazon Kendra eseguirà la scansione solo dei file entro il limite di dimensione definito. La dimensione predefinita del file è 50 MB. La dimensione massima del file deve essere superiore a 0 MB e inferiore o uguale a 50 MB.
- Schemi di espressione regolare degli allegati: aggiungono modelli di espressioni regolari per includere o escludere determinati file allegati di cataloghi, articoli informativi e incidenti. È possibile aggiungere fino a 100 pattern.

e. Modalità di sincronizzazione: scegli come aggiornare l'indice quando il contenuto dell'origine dati cambia. Quando sincronizzi l'origine dati con Amazon Kendra per la prima volta, tutto il contenuto viene sottoposto a scansione e indicizzato per impostazione predefinita. Se la sincronizzazione iniziale non è riuscita, devi eseguire una

sincronizzazione completa dei dati, anche se non scegli la sincronizzazione completa come opzione della modalità di sincronizzazione.

- Sincronizzazione completa: indicizza di nuovo tutti i contenuti, sostituendo i contenuti esistenti ogni volta che l'origine dati si sincronizza con l'indice.
- Sincronizzazione nuova, modificata ed eliminata: indicizza solo i contenuti nuovi, modificati ed eliminati ogni volta che l'origine dati si sincronizza con l'indice. Amazon Kendra può utilizzare il meccanismo dell'origine dati per tenere traccia delle modifiche ai contenuti e indicizzare i contenuti modificati dall'ultima sincronizzazione.

f. Pianificazione di esecuzione di In Sync, per Frequenza: con quale frequenza Amazon Kendra verrà eseguita la sincronizzazione con la fonte di dati.

g. Seleziona Successivo.

8. Nella pagina Imposta le mappature dei campi, inserisci le seguenti informazioni:

   a. Articoli informativi, Service Catalog, Allegati e Incidenti: seleziona uno dei campi delle origini dati predefiniti Amazon Kendra generati che desideri mappare all'indice.

   b. Aggiungi campo: consente di aggiungere campi di origine dati personalizzati per creare un nome di campo indice a cui mappare e il tipo di dati del campo.

   c. Seleziona Successivo.

9. Nella pagina Rivedi e crea, verifica che le informazioni inserite siano corrette, quindi seleziona Aggiungi origine dati. Puoi anche scegliere di modificare le tue informazioni da questa pagina. L'origine dati verrà visualizzata nella pagina Origini dati dopo che l'origine dati sarà stata aggiunta correttamente.

API

Per connettersi Amazon Kendra a ServiceNow

È necessario specificare un codice JSON dello schema dell'origine dati utilizzando l'TemplateConfigurationAPI. È necessario fornire le seguenti informazioni:

- Origine dati: specifica il tipo di origine dati come `SERVICENOWV2` quando usi lo schema TemplateConfigurationJSON. Specificate anche l'origine dati come `TEMPLATE` quando chiamate l'CreateDataSourceAPI.
- URL host: specifica la versione dell'istanza ServiceNow host. Ad esempio, *`your-domain.service-now.com`*.

- Tipo di autenticazione: specifica il tipo di autenticazione che utilizzi, indipendentemente dal fatto che sia o per la tua istanza. `basicAuth` `OAuth2` ServiceNow
- ServiceNow versione dell'istanza: specifica l' ServiceNow istanza da utilizzare, se`Tokyo`, `SandiegoRome`, o. `Others`
- Modalità di sincronizzazione: specifica come Amazon Kendra aggiornare l'indice quando il contenuto dell'origine dati cambia. Quando sincronizzi l'origine dati con Amazon Kendra per la prima volta, tutto il contenuto viene sottoposto a scansione e indicizzato per impostazione predefinita. Se la sincronizzazione iniziale non è riuscita, devi eseguire una sincronizzazione completa dei dati, anche se non scegli la sincronizzazione completa come opzione della modalità di sincronizzazione. Puoi scegliere tra:
  - `FORCED_FULL_CRAWL`per indicizzare nuovamente tutti i contenuti, sostituendo i contenuti esistenti ogni volta che l'origine dati si sincronizza con l'indice.
  - `FULL_CRAWL`per indicizzare solo i contenuti nuovi, modificati ed eliminati ogni volta che l'origine dati si sincronizza con l'indice. Amazon Kendra può utilizzare il meccanismo dell'origine dati per tenere traccia delle modifiche ai contenuti e indicizzare i contenuti modificati dall'ultima sincronizzazione.
- Secret Amazon Resource Name (ARN): fornisci l'Amazon Resource Name (ARN) di un Secrets Manager segreto che contiene le credenziali di autenticazione che hai creato nel tuo account. ServiceNow

  Se utilizzi l'autenticazione di base, il segreto viene archiviato in una struttura JSON con le seguenti chiavi:

```
{
    "username": "user name",
    "password": "password"
}
```

> **Note**
>
> Ti consigliamo di aggiornare o ruotare regolarmente le credenziali e il segreto. Fornisci solo il livello di accesso necessario per la tua sicurezza. Non è consigliabile riutilizzare credenziali e segreti tra diverse fonti di dati e versioni dei connettori 1.0 e 2.0 (ove applicabile).

- Se utilizzi le credenziali del client OAuth2, il segreto viene archiviato in una struttura JSON con le seguenti chiavi:

```
{
    "username": "user name",
    "password": "password",
    "clientId": "client id",
    "clientSecret": "client secret"
}
```

- IAM role: specifica `RoleArn` quando chiami `CreateDataSource` per fornire a un IAM ruolo le autorizzazioni per accedere al tuo Secrets Manager segreto e per chiamare le API pubbliche richieste per il connettore e. ServiceNow Amazon Kendra Per ulteriori informazioni, consulta i IAM ruoli per ServiceNow le fonti di dati.

Puoi anche aggiungere le seguenti funzionalità opzionali:

- Virtual Private Cloud (VPC): `VpcConfiguration` specifica quando si chiama. `CreateDataSource` Per ulteriori informazioni, consulta Configurazione Amazon Kendra per l'utilizzo di un Amazon VPC.
- Filtri di inclusione ed esclusione: è possibile specificare se includere o escludere determinati file allegati utilizzando i nomi dei file e i tipi di file degli articoli informativi, dei cataloghi di servizi e degli incidenti.

> **Note**
>
> La maggior parte delle fonti di dati utilizza modelli di espressioni regolari, che sono modelli di inclusione o esclusione denominati filtri. Se si specifica un filtro di inclusione, viene indicizzato solo il contenuto che corrisponde al filtro di inclusione. Qualsiasi documento che non corrisponde al filtro di inclusione non viene indicizzato. Se si specifica un filtro di inclusione ed esclusione, i documenti che corrispondono al filtro di esclusione non vengono indicizzati, anche se corrispondono al filtro di inclusione.

- Documenti specifici da indicizzare: è possibile utilizzare una ServiceNow query per specificare i documenti desiderati da una o più knowledge base, incluse le knowledge base private. L'accesso alle knowledge base è determinato dall'utente utilizzato per connettersi all' ServiceNow istanza. Per ulteriori informazioni, consulta la sezione Specifica dei documenti da indicizzare con una query.

- Parametri di indicizzazione: puoi anche scegliere di specificare se:
  - Indicizza gli articoli informativi, i cataloghi di servizi e gli incidenti o tutti questi elementi. Se si sceglie di indicizzare gli articoli informativi, gli articoli del catalogo dei servizi e gli incidenti, è necessario fornire il nome del ServiceNow campo mappato al campo del contenuto del documento indicizzato nell'indice. Amazon Kendra
  - Indicizza gli allegati agli articoli informativi, agli elementi del catalogo dei servizi e agli incidenti.
  - Includi articoli informativi, elementi del catalogo dei servizi e incidenti in base allo `short description` schema di filtro.
  - Scegli di filtrare gli elementi e gli incidenti attivi e inattivi del catalogo dei servizi.
  - Scegli di filtrare gli incidenti in base al tipo di incidente.
  - Scegli quali entità devono avere il loro ACL sottoposto a scansione.
  - È possibile utilizzare una ServiceNow query per specificare i documenti desiderati da una o più knowledge base, incluse le knowledge base private. L'accesso alle knowledge base è determinato dall'utente utilizzato per connettersi all' ServiceNowistanza. Per ulteriori informazioni, consulta la sezione Specifica dei documenti da indicizzare con una query.
- Identity crawler: specifica se attivare il crawler Amazon Kendra di identità. Il crawler di identità utilizza le informazioni dell'elenco di controllo degli accessi (ACL) per i documenti per filtrare i risultati della ricerca in base all'accesso dell'utente o del relativo gruppo ai documenti. Se disponi di un ACL per i tuoi documenti e scegli di utilizzarlo, puoi anche scegliere di attivare il crawler di identità per configurare il filtraggio Amazon Kendra contestuale dell'utente dei risultati di ricerca. Altrimenti, se il crawler di identità è disattivato, tutti i documenti possono essere ricercati pubblicamente. Se desideri utilizzare il controllo degli accessi per i tuoi documenti e il crawler di identità è disattivato, in alternativa puoi utilizzare l'PutPrincipalMappingAPI per caricare le informazioni di accesso di utenti e gruppi per il filtraggio del contesto degli utenti.
- Mappature dei campi: scegli di mappare i campi delle sorgenti ServiceNow dati ai campi indice. Amazon Kendra Per ulteriori informazioni, consulta la sezione Mappatura dei campi di origine dei dati.

> **Note**
>
> Il campo del corpo del documento o l'equivalente del corpo del documento per i documenti è necessario per Amazon Kendra eseguire la ricerca nei documenti. È

necessario mappare il nome del campo del corpo del documento nella fonte dati al nome del campo indice_`document_body`. Tutti gli altri campi sono facoltativi.

Per un elenco di altre importanti chiavi JSON da configurare, consultaServiceNow schema modello.

Ulteriori informazioni

Per ulteriori informazioni sull'integrazione Amazon Kendra con la tua fonte di ServiceNow dati, consulta:

- Guida introduttiva Amazon Kendra all'annuncio del ServiceNow connettore aggiornato (V2) per Amazon Kendra

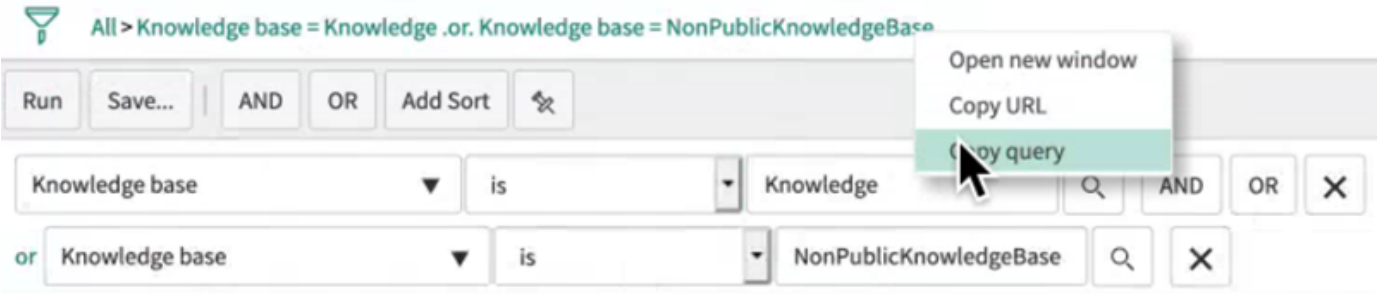
Specificare i documenti da indicizzare con una query

È possibile utilizzare un' ServiceNow interrogazione per specificare i documenti da includere in un Amazon Kendra indice. Quando si utilizza una query, è possibile specificare più basi di conoscenza, incluse le knowledge base private. L'accesso alle knowledge base è determinato dall'utente utilizzato per connettersi all' ServiceNow istanza.

Per creare una query, si utilizza il generatore di ServiceNow query. È possibile utilizzare il generatore per creare la query e verificare che la query restituisca l'elenco corretto di documenti.

Per creare una query utilizzando la console ServiceNow

1. Accedere alla ServiceNow console.
2. Dal menu a sinistra, scegli Conoscenza, quindi Articoli, quindi scegli Tutto.
3. Nella parte superiore della pagina, scegli l'icona del filtro.
4. Usa il generatore di query per creare l'interrogazione.
5. Quando la query è completa, fate clic con il pulsante destro del mouse sulla query e scegliete Copia interrogazione per copiare la query dal generatore di query. Salva questa interrogazione per utilizzarla in Amazon Kendra.



Assicuratevi di non modificare alcun parametro di interrogazione quando copiate l'interrogazione. Se uno qualsiasi dei parametri della query non viene riconosciuto, ServiceNow considera il parametro come vuoto e non lo utilizza per filtrare i risultati.

Slack

Slack è un'app di comunicazione aziendale che consente agli utenti di inviare messaggi e allegati attraverso vari canali pubblici e privati. Puoi usarla Amazon Kendra per indicizzare i canali pubblici e privati di Slack, creare bot e archiviare messaggi, file e allegati, messaggi diretti e di gruppo. Puoi anche scegliere contenuti specifici da filtrare.

> **Note**
>
> Amazon Kendra ora supporta un connettore Slack aggiornato.
> La console è stata aggiornata automaticamente per te. Tutti i nuovi connettori creati nella console utilizzeranno l'architettura aggiornata. Se utilizzi l'API, ora devi utilizzare l'TemplateConfigurationoggetto anziché l'`SlackConfiguration`oggetto per configurare il connettore.
> I connettori configurati utilizzando la console e l'architettura API precedenti continueranno a funzionare come configurato. Tuttavia, non potrai modificarli o aggiornarli. Se desideri modificare o aggiornare la configurazione del connettore, devi creare un nuovo connettore. Ti consigliamo di migrare il flusso di lavoro del connettore alla versione aggiornata. La fine del supporto per i connettori configurati utilizzando l'architettura precedente è prevista entro giugno 2024.

Puoi connetterti Amazon Kendra alla tua fonte di dati Slack utilizzando la Amazon Kendra console o l'TemplateConfigurationAPI.

Per la risoluzione dei problemi relativi al connettore di origine dati Amazon Kendra Slack, consulta. Risoluzione dei problemi relativi alle origini dati

Argomenti

Funzionalità supportate

Amazon Kendra Il connettore di origine dati Slack supporta le seguenti funzionalità:

- Mappature dei campi
- Filtraggio del contesto utente
- Scansione delle identità degli utenti
- Filtri di inclusione/esclusione
- Sincronizzazione completa e incrementale dei contenuti
- Virtual Private Cloud (VPC) (Cloud privato virtuale (VPC)

Prerequisiti

Prima di poterla utilizzare Amazon Kendra per indicizzare la tua fonte di dati Slack, apporta queste modifiche a Slack e agli account. AWS

In Slack, assicurati di avere:

- Hai creato un token OAuth per l'utente Slack Bot o un token OAuth per l'utente Slack. Puoi scegliere uno dei due token per Amazon Kendra connetterti alla tua fonte di dati Slack. Per ulteriori informazioni, consulta la documentazione di Slack sui token di accesso.

> **Note**
>
> Se utilizzi il token bot come parte delle tue credenziali Slack, non puoi indicizzare i messaggi diretti e i messaggi di gruppo e devi aggiungere il token bot al canale che desideri indicizzare.

- Hai annotato l'ID del team del tuo spazio di lavoro Slack dall'URL della pagina principale del tuo spazio di lavoro Slack. *Ad esempio, https://app.slack.com/client/T0123456789/...* dove *T0123456789* è l'ID del team.
- Sono stati aggiunti i seguenti ambiti e autorizzazioni Oauth:

Ambito del token utente	Ambito del token bot
• canali:cronologia • canali:leggi • emoji: leggi • file:leggi • gruppi:storia • gruppi: leggi • im:storia • im:read • mpim:storia • mpim: leggi • team:read • users.profile:leggi • utenti:leggi • utenti:read.email	• canali:cronologia • canali:gestire • canali:leggi • conversations.connect:gestire • conversations.connect: leggi • file:leggi • gruppi:storia • gruppi: leggi • im:storia • im:read • mpim:storia • mpim: leggi • reazioni:leggi • team:read • gruppi di utenti: leggi • users.profile:leggi • utenti:leggi • utenti:read.email

- È stato selezionato che ogni documento sia unico in Slack e tra le altre fonti di dati che intendi utilizzare per lo stesso indice. Ogni fonte di dati che desideri utilizzare per un indice non deve contenere lo stesso documento in tutte le fonti di dati. Gli ID dei documenti sono globali rispetto a un indice e devono essere univoci per indice.

Nel tuo Account AWS, assicurati di avere:

- Ha creato un Amazon Kendra indice e, se si utilizza l'API, ha annotato l'ID dell'indice.
- Hai creato un IAM ruolo per la tua origine dati e, se utilizzi l'API, hai annotato l'ARN del IAM ruolo.

> **Note**
>
> Se modifichi il tipo di autenticazione e le credenziali, devi aggiornare il IAM ruolo per accedere all'ID AWS Secrets Manager segreto corretto.

- Ha archiviato le credenziali di autenticazione Slack in un AWS Secrets Manager luogo segreto e, se si utilizza l'API, ha annotato l'ARN del segreto.

> **Note**
>
> Ti consigliamo di aggiornare o ruotare regolarmente le credenziali e il segreto. Fornisci solo il livello di accesso necessario per la tua sicurezza. Non è consigliabile riutilizzare credenziali e segreti tra diverse fonti di dati e versioni dei connettori 1.0 e 2.0 (ove applicabile).

Se non disponi di un IAM ruolo o di un segreto esistente, puoi utilizzare la console per creare un nuovo IAM ruolo e un Secrets Manager segreto quando connetti la tua fonte di dati Slack a. Amazon Kendra Se utilizzi l'API, devi fornire l'ARN di un IAM ruolo e di un Secrets Manager segreto esistenti e un ID di indice.

Istruzioni di connessione

Per connetterti Amazon Kendra alla tua fonte di dati Slack, devi fornire i dettagli necessari della tua fonte di dati Slack in modo che Amazon Kendra possa accedere ai tuoi dati. Se non hai ancora configurato Slack per Amazon Kendra, consulta. Prerequisiti

Console

Per connetterti Amazon Kendra a Slack

1. Accedi a AWS Management Console e apri la Amazon Kendra console.
2. Dal riquadro di navigazione a sinistra, scegli Indici, quindi scegli l'indice che desideri utilizzare dall'elenco degli indici.

> **Note**
>
> Puoi scegliere di configurare o modificare le impostazioni del controllo dell'accesso degli utenti in Impostazioni dell'indice.

3. Nella pagina Guida introduttiva, scegli Aggiungi origine dati.
4. Nella pagina Aggiungi origine dati, scegli Connettore Slack, quindi scegli Aggiungi connettore.
5. Nella pagina Specificare i dettagli dell'origine dati, inserisci le seguenti informazioni:
   a. In Nome e descrizione, per Nome dell'origine dati, inserisci un nome per l'origine dati. Puoi includere trattini ma non spazi.
   b. (Facoltativo) Descrizione: immetti una descrizione facoltativa per la tua fonte di dati.
   c. In Lingua predefinita: scegli una lingua per filtrare i documenti per l'indice. Se non diversamente specificato, la lingua predefinita è l'inglese. La lingua specificata nei metadati del documento ha la precedenza sulla lingua selezionata.
   d. In Tag, per Aggiungi nuovo tag, includi tag opzionali per cercare e filtrare le risorse o tenere traccia dei costi. AWS
   e. Seleziona Successivo.
6. Nella pagina Definisci accesso e sicurezza, inserisci le seguenti informazioni:
   a. In Source, per Slack Workspace Team ID: l'ID del team del tuo spazio di lavoro Slack.
   b. AWS Secrets Manager segreto: scegli un segreto esistente o creane uno nuovo per archiviare le credenziali di autenticazione Secrets Manager Slack. Se scegli di creare un nuovo segreto, si apre una finestra AWS Secrets Manager segreta.
      i. Inserisci le seguenti informazioni nella finestra Crea un AWS Secrets Manager segreto:
         A. Nome segreto: un nome per il tuo segreto. Il prefisso 'AmazonKendra-Slack-' viene aggiunto automaticamente al tuo nome segreto.
         B. Per il token Slack: inserisci i valori delle credenziali di autenticazione che hai creato nel tuo account Slack.
      ii. Selezionare Salva.
   c. Virtual Private Cloud (VPC): puoi scegliere di utilizzare un VPC. In tal caso, è necessario aggiungere sottoreti e gruppi di sicurezza VPC.

d. Identity crawler: specifica se attivare il crawler di identità. Amazon Kendra Il crawler di identità utilizza le informazioni dell'elenco di controllo degli accessi (ACL) per i documenti per filtrare i risultati della ricerca in base all'accesso dell'utente o del gruppo di appartenenza ai documenti. Se disponi di un ACL per i tuoi documenti e scegli di utilizzarlo, puoi anche scegliere di attivare il crawler di identità per configurare il filtraggio Amazon Kendra contestuale dell'utente dei risultati di ricerca. Altrimenti, se il crawler di identità è disattivato, tutti i documenti possono essere ricercati pubblicamente. Se desideri utilizzare il controllo degli accessi per i tuoi documenti e il crawler di identità è disattivato, in alternativa puoi utilizzare l'PutPrincipalMappingAPI per caricare le informazioni di accesso di utenti e gruppi per il filtraggio del contesto degli utenti.

e. IAM ruolo: scegli un IAM ruolo esistente o creane uno nuovo IAM per accedere alle credenziali del repository e indicizzare il contenuto.

> **Note**
>
> IAM i ruoli utilizzati per gli indici non possono essere utilizzati per le fonti di dati. Se non sei sicuro che un ruolo esistente venga utilizzato per un indice o una FAQ, scegli Crea un nuovo ruolo per evitare errori.

f. Seleziona Successivo.

7. Nella pagina Configura le impostazioni di sincronizzazione, inserisci le seguenti informazioni:

a. Seleziona il tipo di contenuto da sottoporre a scansione: le entità o i tipi di contenuto Slack che desideri sottoporre a scansione. Puoi scegliere tra Tutti i canali, Canali pubblici, Canali privati, Messaggi di gruppo e Messaggi privati.

b. Seleziona la data di inizio della scansione: inserisci la data a partire dalla quale Amazon Kendra eseguirai la scansione dei tuoi contenuti Slack.

c. Per la configurazione aggiuntiva, facoltativa, inserisci le seguenti informazioni:

- (Facoltativo) ID/nome del canale: se hai scelto di sincronizzare i contenuti dei canali, puoi includere contenuti da sincronizzare da canali specifici fornendo ID e nomi dei canali.
- Messaggi: scegli se includere messaggi bot o messaggi archiviati o entrambi i messaggi bot e archiviati.

> **Note**
>
> Se scegli di configurare i filtri sia per l'ID del canale che per il nome del canale, il connettore Amazon Kendra Slack darà la priorità agli ID dei canali rispetto ai nomi dei canali.
> Se scegli di configurare i filtri per l'ID del canale o il nome del canale, il connettore Amazon Kendra Slack ignorerà i messaggi privati e di gruppo anche se hai scelto di scansionare i messaggi privati e di gruppo nell'ambito di sincronizzazione.

- Modelli Regex: modelli di espressioni regolari per includere o escludere determinati file. È possibile aggiungere fino a 100 pattern. Esempi di modelli regex includono:
  - Tipo di file: .pdf, .docx
  - Nome del file: Hello*.txt,. TestFile *

d. Modalità di sincronizzazione: scegli come aggiornare l'indice quando il contenuto dell'origine dati cambia. Quando sincronizzi l'origine dati con Amazon Kendra per la prima volta, tutto il contenuto viene sottoposto a scansione e indicizzato per impostazione predefinita. Se la sincronizzazione iniziale non è riuscita, devi eseguire una sincronizzazione completa dei dati, anche se non scegli la sincronizzazione completa come opzione della modalità di sincronizzazione.

- Sincronizzazione completa: indicizza di nuovo tutti i contenuti, sostituendo i contenuti esistenti ogni volta che l'origine dati si sincronizza con l'indice.
- Sincronizzazione nuova, modificata ed eliminata: indicizza solo i contenuti nuovi, modificati ed eliminati ogni volta che l'origine dati si sincronizza con l'indice. Amazon Kendra può utilizzare il meccanismo dell'origine dati per tenere traccia delle modifiche ai contenuti e indicizzare i contenuti modificati dall'ultima sincronizzazione.

e. Pianificazione di esecuzione di In Sync, per Frequenza: con quale frequenza Amazon Kendra verrà eseguita la sincronizzazione con la fonte di dati.

f. Seleziona Successivo.

8. Nella pagina Imposta mappature dei campi, inserisci le seguenti informazioni:

a. Per le mappature dei campi di Slack: seleziona tra i campi di origine dati predefiniti Amazon Kendra generati che desideri mappare al tuo indice.

b. Aggiungi campo: consente di aggiungere campi di origine dati personalizzati per creare un nome di campo indice a cui mappare e il tipo di dati del campo.

c. Seleziona Successivo.

9. Nella pagina Rivedi e crea, verifica che le informazioni inserite siano corrette, quindi seleziona Aggiungi origine dati. Puoi anche scegliere di modificare le tue informazioni da questa pagina. L'origine dati verrà visualizzata nella pagina Origini dati dopo che l'origine dati sarà stata aggiunta correttamente.

API

Per connettersi Amazon Kendra a Slack

È necessario specificare un codice JSON dello schema dell'origine dati utilizzando l'TemplateConfigurationAPI. È necessario fornire le seguenti informazioni:

- Origine dati: specifica il tipo di origine dati come `SLACK` quando usi lo schema TemplateConfigurationJSON. Specificate anche l'origine dati come `TEMPLATE` quando chiamate l'CreateDataSourceAPI.
- ID del team di Slack Workspace: l'ID del team Slack che hai copiato dall'URL della pagina principale di Slack.
- Data di inizio: la data in cui iniziare a scansionare i dati del team dell'area di lavoro Slack. La data deve seguire questo formato:. yyyy-mm-dd
- Modalità di sincronizzazione: specifica come Amazon Kendra aggiornare l'indice quando il contenuto della fonte di dati cambia. Quando sincronizzi l'origine dati con Amazon Kendra per la prima volta, tutto il contenuto viene sottoposto a scansione e indicizzato per impostazione predefinita. Se la sincronizzazione iniziale non è riuscita, devi eseguire una sincronizzazione completa dei dati, anche se non scegli la sincronizzazione completa come opzione della modalità di sincronizzazione. Puoi scegliere tra:
  - `FORCED_FULL_CRAWL`per indicizzare nuovamente tutti i contenuti, sostituendo i contenuti esistenti ogni volta che l'origine dati si sincronizza con l'indice.
  - `FULL_CRAWL`per indicizzare solo i contenuti nuovi, modificati ed eliminati ogni volta che l'origine dati si sincronizza con l'indice. Amazon Kendra può utilizzare il meccanismo dell'origine dati per tenere traccia delle modifiche ai contenuti e indicizzare i contenuti modificati dall'ultima sincronizzazione.
  - `CHANGE_LOG`per indicizzare solo contenuti nuovi e modificati ogni volta che l'origine dati si sincronizza con l'indice. Amazon Kendra può utilizzare il meccanismo dell'origine dati

per tenere traccia delle modifiche ai contenuti e indicizzare i contenuti modificati dall'ultima sincronizzazione.

- Identity crawler: specifica se attivare il crawler Amazon Kendra di identità. Il crawler di identità utilizza le informazioni dell'elenco di controllo degli accessi (ACL) per i documenti per filtrare i risultati della ricerca in base all'accesso dell'utente o del gruppo di appartenenza ai documenti. Se disponi di un ACL per i tuoi documenti e scegli di utilizzarlo, puoi anche scegliere di attivare il crawler di identità per configurare il filtraggio Amazon Kendra contestuale dell'utente dei risultati di ricerca. Altrimenti, se il crawler di identità è disattivato, tutti i documenti possono essere ricercati pubblicamente. Se desideri utilizzare il controllo degli accessi per i tuoi documenti e il crawler di identità è disattivato, in alternativa puoi utilizzare l'PutPrincipalMappingAPI per caricare le informazioni di accesso di utenti e gruppi per il filtraggio del contesto degli utenti.
- Secret Amazon Resource Name (ARN): fornisci l'Amazon Resource Name (ARN) di un Secrets Manager segreto che contiene le credenziali di autenticazione per il tuo account Slack. Il segreto è archiviato in una struttura JSON con le seguenti chiavi:

```
{
    "slackToken": "token"
}
```

> **Note**
>
> Ti consigliamo di aggiornare o ruotare regolarmente le credenziali e il segreto. Fornisci solo il livello di accesso necessario per la tua sicurezza. Non è consigliabile riutilizzare credenziali e segreti tra diverse fonti di dati e versioni dei connettori 1.0 e 2.0 (ove applicabile).

- IAM ruolo: specifica `RoleArn` quando chiami `CreateDataSource` per fornire a un IAM ruolo le autorizzazioni per accedere al tuo Secrets Manager segreto e per chiamare le API pubbliche richieste per il connettore Slack e. Amazon Kendra Per ulteriori informazioni, consulta i IAM ruoli per le fonti di dati Slack.

Puoi anche aggiungere le seguenti funzionalità opzionali:

- Virtual Private Cloud (VPC): `VpcConfiguration` specifica quando si chiama. `CreateDataSource` Per ulteriori informazioni, consulta Configurazione Amazon Kendra per l'utilizzo di un Amazon VPC.

- Canali specifici: filtra per canali pubblici o privati e specifica determinati canali in base al relativo ID.
- Tipi di canali e messaggi: Amazon Kendra se indicizzare i canali pubblici e privati, i messaggi diretti e di gruppo, i messaggi bot e archiviati. Se utilizzi un token bot come parte delle tue credenziali di autenticazione Slack, devi aggiungere il token bot al canale che desideri indicizzare. Non puoi indicizzare i messaggi diretti e i messaggi di gruppo utilizzando un token bot.
- Guarda indietro: puoi scegliere di configurare un `lookBack` parametro in modo che il connettore Slack esegua la scansione dei contenuti aggiornati o eliminati fino a un determinato numero di ore prima dell'ultima sincronizzazione del connettore.
- Filtri di inclusione ed esclusione: specifica se includere o escludere determinati contenuti Slack. Se utilizzi un token bot come parte delle tue credenziali di autenticazione Slack, devi aggiungere il token bot al canale che desideri indicizzare. Non puoi indicizzare i messaggi diretti e i messaggi di gruppo utilizzando un token bot.

  > **Note**
  >
  > La maggior parte delle fonti di dati utilizza modelli di espressioni regolari, che sono modelli di inclusione o esclusione denominati filtri. Se si specifica un filtro di inclusione, viene indicizzato solo il contenuto che corrisponde al filtro di inclusione. Qualsiasi documento che non corrisponde al filtro di inclusione non viene indicizzato. Se si specifica un filtro di inclusione ed esclusione, i documenti che corrispondono al filtro di esclusione non vengono indicizzati, anche se corrispondono al filtro di inclusione.

- Mappature dei campi: scegli di mappare i campi delle sorgenti dati di Slack ai campi indice. Amazon Kendra Per ulteriori informazioni, consulta la sezione Mappatura dei campi di origine dei dati.

  > **Note**
  >
  > Il campo del corpo del documento o l'equivalente del corpo del documento per i tuoi documenti è obbligatorio per Amazon Kendra poter cercare i tuoi documenti. È necessario mappare il nome del campo del corpo del documento nella fonte dati al nome del campo indice_`document_body`. Tutti gli altri campi sono facoltativi.

Per un elenco di altre importanti chiavi JSON da configurare, consulta lo schema Slack del modello.

Ulteriori informazioni

Per saperne di più sull'integrazione Amazon Kendra con la tua fonte di dati Slack, consulta:

- Svela le tue conoscenze nelle aree di lavoro di Slack con la ricerca intelligente utilizzando il connettore Slack Amazon Kendra

Zendesk

Zendesk è un sistema di gestione delle relazioni con i clienti che aiuta le aziende ad automatizzare e migliorare le interazioni con l'assistenza clienti. Puoi utilizzarlo Amazon Kendra per indicizzare i ticket di assistenza Zendesk, i commenti ai ticket, gli allegati dei ticket, gli articoli del centro assistenza, i commenti agli articoli, gli allegati dei commenti agli articoli, gli argomenti della community di guide, i post della community e i commenti ai post della community.

Puoi filtrare in base al nome dell'organizzazione se desideri indicizzare i ticket che si trovano solo all'interno di un'organizzazione specifica. Puoi anche scegliere di impostare una data di scansione per quando vuoi iniziare a scansionare i dati da Zendesk.

Puoi connetterti Amazon Kendra alla tua fonte di dati Zendesk utilizzando la Amazon Kendra console e l'API. TemplateConfiguration

Per la risoluzione dei problemi relativi al connettore di origine dati Amazon Kendra Zendesk, consulta. Risoluzione dei problemi relativi alle origini dati

Argomenti

- Funzionalità supportate
- Prerequisiti
- Istruzioni di connessione
- Ulteriori informazioni

Funzionalità supportate

Amazon Kendra Il connettore per sorgenti dati Zendesk supporta le seguenti funzionalità:

- Log delle modifiche
- Mappatura dei campi
- Filtraggio del contesto utente
- Filtri di inclusione/esclusione
- Virtual Private Cloud (VPC) (Cloud privato virtuale (VPC)

Prerequisiti

Prima di poterla utilizzare Amazon Kendra per indicizzare la fonte di dati Zendesk, apporta queste modifiche a Zendesk e agli account. AWS

In Zendesk, assicurati di avere:

- Hai creato un account amministrativo Zendesk Suite (Professional/Enterprise).
- Ha annotato l'URL del tuo host Zendesk. Ad esempio, *https://{sub-domain (https://{host/)}.zendesk.com/*.

> **Note**
>
> (On-premise/server) Amazon Kendra verifica se le informazioni sull'endpoint incluse sono le stesse informazioni sull'endpoint specificate nei dettagli di configurazione dell'origine dati. AWS Secrets Manager In questo modo si evita il problema del confuso vicario, ossia un problema di sicurezza in cui un utente non è autorizzato a eseguire un'azione ma lo utilizza Amazon Kendra come proxy per accedere al segreto configurato ed eseguire l'azione. Se successivamente modifichi le informazioni sull'endpoint, devi creare un nuovo segreto per sincronizzare queste informazioni.

- Ha generato un token di credenziali OAuth 2.0 contenente un ID client, un segreto client, un nome utente e una password. Per ulteriori informazioni, consulta la documentazione di Zendesk sulla generazione di token OAuth 2.0.
- È stato aggiunto il seguente ambito OAuth 2.0:
  - read
- Facoltativo: è stato installato un certificato SSL per consentire Amazon Kendra la connessione.
- Controllato, ogni documento è unico in Zendesk e tra le altre fonti di dati che intendi utilizzare per lo stesso indice. Ogni fonte di dati che si desidera utilizzare per un indice non deve contenere lo

stesso documento in tutte le fonti di dati. Gli ID dei documenti sono globali rispetto a un indice e devono essere univoci per indice.

Nel tuo Account AWS, assicurati di avere:

- Ha creato un Amazon Kendra indice e, se si utilizza l'API, ha annotato l'ID dell'indice.
- Hai creato un IAM ruolo per la tua origine dati e, se utilizzi l'API, hai annotato l'ARN del IAM ruolo.

> **Note**
>
> Se modifichi il tipo di autenticazione e le credenziali, devi aggiornare il IAM ruolo per accedere all'ID AWS Secrets Manager segreto corretto.

- Ha archiviato le credenziali di autenticazione Zendesk in un AWS Secrets Manager luogo segreto e, se si utilizza l'API, ha annotato l'ARN del segreto.

> **Note**
>
> Ti consigliamo di aggiornare o ruotare regolarmente le credenziali e il segreto. Fornisci solo il livello di accesso necessario per la tua sicurezza. Non è consigliabile riutilizzare credenziali e segreti tra diverse fonti di dati e versioni dei connettori 1.0 e 2.0 (ove applicabile).

Se non disponi di un IAM ruolo o di un segreto esistente, puoi utilizzare la console per creare un nuovo IAM ruolo e un Secrets Manager segreto quando connetti la tua fonte di dati Zendesk a. Amazon Kendra Se utilizzi l'API, devi fornire l'ARN di un IAM ruolo e di un Secrets Manager segreto esistenti e un ID di indice.

Istruzioni di connessione

Per connetterti Amazon Kendra alla tua fonte dati Zendesk, devi fornire i dettagli necessari sulla tua fonte di dati Zendesk in modo che Amazon Kendra possa accedere ai tuoi dati. Se non hai ancora configurato Zendesk per Amazon Kendra, consulta. Prerequisiti

Console

Per connettersi a Amazon Kendra Zendesk

1. Accedi a AWS Management Console e apri la Amazon Kendra console.
2. Dal riquadro di navigazione a sinistra, scegli Indici, quindi scegli l'indice che desideri utilizzare dall'elenco degli indici.

> **Note**
>
> Puoi scegliere di configurare o modificare le impostazioni del controllo dell'accesso degli utenti in Impostazioni dell'indice.

3. Nella pagina Guida introduttiva, scegli Aggiungi origine dati.
4. Nella pagina Aggiungi origine dati, scegli Connettore Zendesk, quindi scegli Aggiungi connettore.
5. Nella pagina Specificare i dettagli dell'origine dati, inserisci le seguenti informazioni:
   a. In Nome e descrizione, per Nome dell'origine dati, inserisci un nome per l'origine dati. Puoi includere trattini ma non spazi.
   b. (Facoltativo) Descrizione: immetti una descrizione facoltativa per la tua fonte di dati.
   c. In Lingua predefinita: scegli una lingua per filtrare i documenti per l'indice. Se non diversamente specificato, la lingua predefinita è l'inglese. La lingua specificata nei metadati del documento ha la precedenza sulla lingua selezionata.
   d. In Tag, per Aggiungi nuovo tag, includi tag opzionali per cercare e filtrare le risorse o tenere traccia dei costi. AWS
   e. Seleziona Successivo.
6. Nella pagina Definisci accesso e sicurezza, inserisci le seguenti informazioni:
   a. URL Zendesk: inserisci il tuo URL Zendesk.
   b. AWS Secrets Manager segreto: scegli un segreto esistente o creane uno nuovo Secrets Manager per archiviare le credenziali di autenticazione Zendesk. Se scegli di creare un nuovo segreto, si apre una finestra AWS Secrets Manager segreta.
      i. Inserisci le seguenti informazioni nella finestra Crea un AWS Secrets Manager segreto:
         A. Nome segreto: un nome per il tuo segreto. Il prefisso 'AmazonKendra-Zendesk-' viene aggiunto automaticamente al nome segreto.

B. Per ID cliente, segreto del cliente, nome utente, password: inserisci i valori delle credenziali di autenticazione che hai creato nel tuo account Zendesk.

ii. Selezionare Salva.

c. Virtual Private Cloud (VPC): puoi scegliere di utilizzare un VPC. In tal caso, è necessario aggiungere sottoreti e gruppi di sicurezza VPC.

d. IAM ruolo: scegli un IAM ruolo esistente o creane uno nuovo IAM per accedere alle credenziali del repository e indicizzare il contenuto.

> **Note**
>
> IAM i ruoli utilizzati per gli indici non possono essere utilizzati per le fonti di dati. Se non sei sicuro che un ruolo esistente venga utilizzato per un indice o una FAQ, scegli Crea un nuovo ruolo per evitare errori.

e. Seleziona Successivo.

7. Nella pagina Configura le impostazioni di sincronizzazione, inserisci le seguenti informazioni:

a. Seleziona entità o tipi di contenuto: le entità o i tipi di contenuto Zendesk che desideri sottoporre a scansione.

b. Registro delle modifiche: seleziona questa opzione per aggiornare l'indice solo con contenuti nuovi e modificati anziché sincronizzare tutti i file.

c. Nome dell'organizzazione: inserisci i nomi delle organizzazioni Zendesk per filtrare la sincronizzazione.

d. Data di inizio della sincronizzazione: la data a partire dalla quale desideri indicizzare i tuoi contenuti.

e. Modelli Regex: modelli di espressioni regolari per includere o escludere determinati file. È possibile aggiungere fino a 100 pattern.

f. Pianificazione di esecuzione di In Sync per Frequency: scegli la frequenza di sincronizzazione con la tua fonte di dati. Amazon Kendra

g. Seleziona Successivo.

8. Nella pagina Imposta le mappature dei campi, inserisci le seguenti informazioni:

a. Per Tickets, Commento al ticket, Allegato commento al ticket, Articolo, Commento all'articolo, Allegato commento all'articolo, Argomento della community, post della

community, commento al post della community: seleziona uno dei campi Amazon Kendra generati delle origini dati predefiniti che desideri mappare al tuo indice.

b. Aggiungi campo: consente di aggiungere campi di origine dati personalizzati a cui creare un nome di campo indice a cui mappare e il tipo di dati del campo.

c. Seleziona Successivo.

9. Nella pagina Rivedi e crea, verifica che le informazioni inserite siano corrette, quindi seleziona Aggiungi origine dati. Puoi anche scegliere di modificare le tue informazioni da questa pagina. L'origine dati verrà visualizzata nella pagina Origini dati dopo che l'origine dati sarà stata aggiunta correttamente.

API

Per connettersi Amazon Kendra a Zendesk

È necessario specificare un codice JSON dello schema dell'origine dati utilizzando l'TemplateConfigurationAPI. È necessario fornire le seguenti informazioni:

- Origine dati: specifica il tipo di origine dati come `ZENDESK` quando usi lo schema TemplateConfigurationJSON. Specificate anche l'origine dati come `TEMPLATE` quando chiamate l'CreateDataSourceAPI.
- URL dell'host: fornisci l'URL dell'host Zendesk come parte della configurazione della connessione o dei dettagli dell'endpoint del repository. *`Ad esempio, https://yoursubdomain.zendesk.com.`*
- Registro delle modifiche: se Amazon Kendra utilizzare il meccanismo del registro delle modifiche all'origine dati di Zendesk per determinare se un documento deve essere aggiornato nell'indice.

> **Note**
>
> Utilizza il registro delle modifiche se non desideri Amazon Kendra scansionare tutti i documenti. Se il registro delle modifiche è di grandi dimensioni, la scansione dei documenti nella fonte dati Zendesk potrebbe richiedere Amazon Kendra meno tempo rispetto all'elaborazione del registro delle modifiche. Se sincronizzi la fonte di dati Zendesk con l'indice per la prima volta, tutti i documenti vengono scansionati.

- Secret Amazon Resource Name (ARN): fornisci l'Amazon Resource Name (ARN) di un Secrets Manager segreto che contiene le credenziali di autenticazione per il tuo account Zendesk. Il segreto è archiviato in una struttura JSON con le seguenti chiavi:

```
{
    "hostUrl": "https://yoursubdomain.zendesk.com",
    "clientId": "client ID",
    "clientSecret": "Zendesk client secret",
    "userName": "Zendesk user name",
    "password": "Zendesk password"
}
```

> **Note**
>
> Ti consigliamo di aggiornare o ruotare regolarmente le credenziali e il segreto. Fornisci solo il livello di accesso necessario per la tua sicurezza. Non è consigliabile riutilizzare credenziali e segreti tra diverse fonti di dati e versioni dei connettori 1.0 e 2.0 (ove applicabile).

- IAM ruolo: specifica `RoleArn` quando chiami `CreateDataSource` per fornire a un IAM ruolo le autorizzazioni per accedere al tuo Secrets Manager segreto e per chiamare le API pubbliche richieste per il connettore Zendesk e. Amazon Kendra Per ulteriori informazioni, consulta i IAM ruoli per le fonti di dati Zendesk.

Puoi anche aggiungere le seguenti funzionalità opzionali:

- Virtual Private Cloud (VPC): `VpcConfiguration` specifica quando si chiama. `CreateDataSource` Per ulteriori informazioni, consulta Configurazione Amazon Kendra per l'utilizzo di un Amazon VPC.
- Filtri di inclusione ed esclusione: specifica se includere o escludere:
  - Ticket di supporto, commenti sui ticket e/o allegati ai commenti dei ticket
  - Articoli del Centro assistenza, allegati agli articoli e commenti agli articoli
  - Guida gli argomenti, i post o i commenti dei post della community

> **Note**
>
> La maggior parte delle fonti di dati utilizza modelli di espressioni regolari, che sono modelli di inclusione o esclusione denominati filtri. Se si specifica un filtro di inclusione, viene indicizzato solo il contenuto che corrisponde al filtro di inclusione. Qualsiasi documento che non corrisponde al filtro di inclusione non viene indicizzato. Se si specifica un filtro di inclusione ed esclusione, i documenti che corrispondono al filtro di esclusione non vengono indicizzati, anche se corrispondono al filtro di inclusione.

- Filtro del contesto utente e controllo degli accessi:Amazon Kendra esegue la ricerca per indicizzazione dell'elenco di controllo degli accessi (ACL) dei documenti, se disponi di un ACL per i documenti. Le informazioni ACL vengono utilizzate per filtrare i risultati della ricerca in base all'accesso dell'utente o del relativo gruppo ai documenti. Per ulteriori informazioni, consulta Filtraggio del contesto utente.
- Mappature dei campi: scegli di mappare i campi delle sorgenti dati di Zendesk ai campi indice. Amazon Kendra Per ulteriori informazioni, consulta la sezione Mappatura dei campi di origine dei dati.

> **Note**
>
> Il campo del corpo del documento o l'equivalente del corpo del documento per i documenti è necessario per Amazon Kendra eseguire la ricerca nei documenti. È necessario mappare il nome del campo del corpo del documento nella fonte dati al nome del campo indice`_document_body`. Tutti gli altri campi sono facoltativi.

Per un elenco di altre importanti chiavi JSON da configurare, consultaSchema del modello Zendesk.

Ulteriori informazioni

Per saperne di più sull'integrazione Amazon Kendra con la tua fonte di dati Zendesk, consulta:

- Scopri gli approfondimenti di Zendesk con la ricerca intelligente Amazon Kendra

Mappatura dei campi delle fonti di dati

Amazon Kendra i connettori di origine dati possono mappare i campi del documento o del contenuto dall'origine dati ai campi Amazon Kendra dell'indice. Per impostazione predefinita, ogni connettore è progettato per eseguire la scansione di campi di origine dati specifici. I campi delle sorgenti dati predefiniti e le relative proprietà non possono essere modificati o personalizzati. Sulla Amazon Kendra console, i campi e le proprietà dei campi predefiniti che non possono essere modificati sono visualizzati in grigio.

Amazon Kendra i connettori consentono inoltre di mappare campi di documento o contenuto personalizzati dalla fonte di dati ai campi personalizzati dell'indice. Ad esempio, se nella fonte dati è presente un campo chiamato «reparto» che contiene informazioni sul reparto per un documento, è possibile mapparlo a un campo indice chiamato «Dipartimento». In questo modo, puoi utilizzare il campo per interrogare i documenti.

Puoi anche mappare campi Amazon Kendra riservati o comuni come`_created_at`. Se la tua fonte di dati ha un campo chiamato «creation_date», puoi mapparlo al campo Amazon Kendra riservato equivalente chiamato. `_created_at` Per ulteriori informazioni sui campi Amazon Kendra riservati, consulta Attributi o campi del documento.

Puoi mappare i campi per la maggior parte delle fonti di dati. È possibile creare mappature dei campi per le seguenti fonti di dati:

- Adobe Experience Manager
- Alfresco
- Aurora (MySQL)
- Aurora (PostgreSQL)
- Amazon FSx (Windows)
- Amazon FSx (NetApp SU TAP)
- Amazon RDS/Aurora
- Amazon RDS (Microsoft SQL Server)
- Amazon RDS (MySQL)
- Amazon RDS (Oracle)
- Amazon RDS (PostgreSQL)
- Amazon Kendra Web crawler

- Amazon WorkDocs
- Box (Cubo)
- Confluence
- Dropbox
- Drupal
- GitHub
- Unità Google Workspace
- Gmail
- IBM DB2
- Jira
- Microsoft Exchange
- Microsoft OneDrive
- Microsoft SharePoint
- Microsoft Teams
- Microsoft SQL Server
- Microsoft Yammer
- MySQL
- Oracle Database
- PostgreSQL
- battuta
- Salesforce
- ServiceNow
- Slack
- Zendesk

Se memorizzi i tuoi documenti in un bucket S3 o in una fonte di dati S3, specifichi i campi utilizzando un file di metadati JSON. Per ulteriori informazioni, consulta S3 Data Source Connector.

La mappatura dei campi della sorgente dati su un campo indice è un processo in tre fasi:

1. Creare un indice. Per ulteriori informazioni, vedere Creazione di un indice.
2. Aggiorna l'indice per aggiungere campi.

3. Crea una fonte di dati e includi le mappature dei campi per mappare i campi riservati e qualsiasi campo personalizzato per Amazon Kendra indicizzare i campi.

Per aggiornare l'indice e aggiungere campi personalizzati, utilizza la console per modificare le mappature dei campi dell'origine dati e aggiungere un campo personalizzato o utilizzare l'API. UpdateIndex Puoi aggiungere un totale di 500 campi personalizzati al tuo indice.

Per le origini dati del database, se il nome della colonna del database corrisponde al nome di un campo riservato, il campo e la colonna vengono mappati automaticamente.

Con l'UpdateIndexAPI, aggiungi campi riservati e personalizzati utilizzandoDocumentMetadataConfigurationUpdates.

Il seguente esempio JSON utilizza `DocumentMetadataConfigurationUpdates` l'aggiunta di un campo chiamato «Dipartimento» all'indice.

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

Quando crei il campo, hai la possibilità di impostare il modo in cui il campo viene utilizzato per la ricerca. Puoi scegliere tra le seguenti opzioni:

- Visualizzabile: determina se il campo viene restituito nella risposta alla query. Il valore predefinito è `true`.
- Facetable: indica che il campo può essere utilizzato per creare sfaccettature. Il valore predefinito è `false`.
- Ricercabile: determina se il campo viene utilizzato nella ricerca. L'impostazione predefinita è `true` per i campi stringa e `false` per i campi numero e data.
- Ordinabile: indica che il campo può essere utilizzato per ordinare la risposta di una query. Può essere impostato solo per i campi di data, numero e stringa. Non può essere impostato per i campi dell'elenco di stringhe.

Il seguente esempio JSON utilizza l'aggiunta `DocumentMetadataConfigurationUpdates` di un campo chiamato «Department» all'indice e lo contrassegna come facetable.

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

Utilizzo di campi di Amazon Kendra documento riservati o comuni

Con l'UpdateIndex API, è possibile creare campi riservati o comuni utilizzando `DocumentMetadataConfigurationUpdates` e specificando il nome del campo indice Amazon Kendra riservato da mappare all'attributo/nome di campo equivalente del documento. Puoi anche creare campi personalizzati. Se utilizzi un connettore di origine dati, la maggior parte include mappature di campi che mappano i campi del documento di origine dati ai campi Amazon Kendra indice. Se utilizzi la console, aggiorni i campi selezionando l'origine dati, selezionando l'azione di modifica e quindi procedendo accanto alla sezione delle mappature dei campi per configurare l'origine dati.

Puoi configurare l'`Search`oggetto per impostare un campo come visualizzabile, personalizzabile, ricercabile e ordinabile. È possibile configurare l'`Relevance`oggetto per impostare l'ordine di classificazione, la durata dell'aumento o il periodo di tempo di un campo da applicare a boosting, freshness, value di importanza e valori di importanza mappati a valori di campo specifici. Se utilizzi la console, puoi configurare le impostazioni di ricerca per un campo selezionando l'opzione facet nel menu di navigazione. Per impostare l'ottimizzazione della pertinenza, seleziona l'opzione di ricerca nell'indice nel menu di navigazione, inserisci una query e utilizza le opzioni del pannello laterale per ottimizzare la pertinenza della ricerca. Non è possibile modificare il tipo di campo dopo averlo creato.

Amazon Kendra contiene i seguenti campi di documento riservati o comuni che è possibile utilizzare:

- `_authors`—Un elenco di uno o più autori responsabili del contenuto del documento.
- `_category`—Una categoria che colloca un documento in un gruppo specifico.
- `_created_at`—La data e l'ora in formato ISO 8601 in cui è stato creato il documento. Ad esempio, 2012-03-25T12:30:10+01:00 è il formato data/ora ISO 8601 per il 25 marzo 2012 alle 12:30 (più 10 secondi) nel fuso orario dell'Europa centrale (CET).
- `_data_source_id`—L'identificatore della fonte di dati che contiene il documento.

- `_document_body`—Il contenuto del documento.
- `_document_id`—Un identificatore univoco per il documento.
- `_document_title`—Il titolo del documento.
- `_excerpt_page_number`—Il numero di pagina in un file PDF in cui viene visualizzato l'estratto del documento. Se l'indice è stato creato prima dell'8 settembre 2020, è necessario reindicizzare i documenti prima di poter utilizzare questo attributo.
- `_faq_id`—Se si tratta di un documento di tipo domanda-risposta (FAQ), un identificatore univoco per le domande frequenti.
- `_file_type`—Il tipo di file del documento, ad esempio pdf o doc.
- `_last_updated_at`—La data e l'ora in formato ISO 8601 dell'ultimo aggiornamento del documento. Ad esempio, 2012-03-25T12:30:10+01:00 è il formato data/ora ISO 8601 per il 25 marzo 2012 alle 12:30 (più 10 secondi) nel fuso orario dell'Europa centrale (CET).
- `_source_uri`—L'URI in cui è disponibile il documento. Ad esempio, l'URI del documento sul sito Web di un'azienda.
- `_version`—Un identificatore per la versione specifica di un documento.
- `_view_count`—Il numero di volte in cui il documento è stato visualizzato.
- `_language_code`(String) —Il codice per una lingua che si applica al documento. Il valore predefinito è l'inglese se non si specifica una lingua. Per ulteriori informazioni sulle lingue supportate, compresi i relativi codici, consulta Aggiungere documenti in lingue diverse dall'inglese.

Per i campi personalizzati, puoi creare questi campi utilizzando `DocumentMetadataConfigurationUpdates` l'`UpdateIndex`API, proprio come quando crei un campo riservato o comune. È necessario impostare il tipo di dati appropriato per il campo personalizzato. Se utilizzi la console, aggiorni i campi selezionando l'origine dati, selezionando l'azione di modifica e quindi procedendo accanto alla sezione delle mappature dei campi per configurare l'origine dati. Alcune fonti di dati non supportano l'aggiunta di nuovi campi o campi personalizzati. Non è possibile modificare il tipo di campo dopo averlo creato.

Di seguito sono riportati i tipi che è possibile impostare per i campi personalizzati:

- Data
- Numero
- Stringa
- Elenco stringhe

Se hai aggiunto documenti all'indice utilizzando l'BatchPutDocumentAPI, `Attributes` elenca i campi/gli attributi dei tuoi documenti e crei campi utilizzando l'oggetto. `DocumentAttribute`

Per i documenti indicizzati da un'origine Amazon S3 dati, crei campi utilizzando un file di metadati JSON che include le informazioni sui campi.

Se utilizzi un database supportato come fonte di dati, puoi configurare i campi utilizzando l'opzione di mappatura dei campi.

Aggiungere documenti in lingue diverse dall'inglese

È possibile indicizzare i documenti in più lingue. Se non specifichi una lingua, Amazon Kendra indicizza i documenti in inglese per impostazione predefinita. Il codice della lingua di un documento viene incluso nei metadati del documento come campo. Vedi Mappature dei campi e Attributi personalizzati per ulteriori informazioni sul `_language_code` campo di un documento.

Puoi specificare il codice della lingua per tutti i tuoi documenti nella tua fonte di dati quando chiami. CreateDataSource Se un documento non ha un codice di lingua specificato in un campo di metadati, il documento viene indicizzato utilizzando il codice della lingua specificato per tutti i documenti a livello di origine dati. Nella console, puoi indicizzare i documenti in una lingua supportata solo a livello di origine dati. Vai a Origini dati, quindi alla pagina Specificare i dettagli dell'origine dati e scegli una lingua dal menu a discesa Lingua.

Puoi anche cercare o interrogare documenti in una lingua supportata. Per ulteriori informazioni, vedere Ricerca nelle lingue.

Sono supportate le seguenti lingue e i relativi codici (l'inglese o `en` è supportato per impostazione predefinita se non si specifica una lingua). Questa tabella include le lingue che Amazon Kendra supportano la ricerca semantica completa, nonché le lingue che supportano solo la semplice corrispondenza di parole chiave. Le lingue che supportano la ricerca semantica completa sono contrassegnate da un asterisco e sono in grassetto nella tabella seguente. L'inglese (lingua predefinita) è supportato anche con la ricerca semantica completa.

Nome della lingua	Codice lingua
Arabo	`ar`
Armeno	hy

Nome della lingua	Codice lingua
Basco	`eu`
Bengalese	`bn`
Bulgaro	`bg`
catalano	`ca`
Cinese: semplificato e tradizionale*	`zh`
Ceco	`cs`
Danese	`da`
Olandese	`nl`
Finlandese	`fi`
Francese: include il francese (Canada) *	`fr`
Galiziano	`gl`
Tedesco*	`de`
Greco	`el`
Hindi	`hi`
Ungherese	`hu`
Indonesiano	`id`
irlandese	`ga`
Italiano	`it`
Giapponese*	`ja`
Coreano*	`ko`

Nome della lingua	Codice lingua
Lettone	`lv`
Lituano	`lt`
Norvegese	`no`
Persiano	`fa`
Portoghese	`pt`
Portoghese (Brasile) *	`pt-BR`
Romeno	`ro`
Russo	`ru`
Sorani	`ckb`
Spagnolo: include lo spagnolo (Messico) *	`es`
Svedese	`sv`
Turco	`tr`

*La ricerca semantica è supportata per la lingua.

Per le lingue che supportano la ricerca semantica, sono supportate le seguenti funzionalità.

- Rilevanza del documento oltre la semplice corrispondenza delle parole chiave.
- Domande frequenti che vanno oltre la semplice corrispondenza di parole chiave.
- Estrazione di risposte dai documenti in base alla comprensione Amazon Kendra della lettura.
- Livelli di confidenza (molto alti, alti, medi e bassi) dei risultati di ricerca.

Per le lingue che non supportano la ricerca semantica, è supportata la semplice corrispondenza di parole chiave per la pertinenza dei documenti e le domande frequenti.

I sinonimi (inclusi i sinonimi personalizzati), l'apprendimento e il feedback incrementali e i suggerimenti di query sono supportati solo per l'inglese (lingua predefinita).

Configurazione Amazon Kendra per l'utilizzo di un Amazon VPC

Amazon Kendra può connettersi a un cloud privato virtuale (VPC) con cui è stato creato Amazon Virtual Private Cloud per indicizzare i contenuti archiviati in fonti di dati in esecuzione nel cloud privato. Quando crei un connettore per l'origine dati, puoi fornire identificatori di gruppo di sicurezza e sottorete per la sottorete che contiene l'origine dati. Con queste informazioni, Amazon Kendra crea un'interfaccia di rete elastica che utilizza per comunicare in modo sicuro con la fonte di dati all'interno del VPC.

Per configurare un connettore di origine Amazon Kendra dati con Amazon VPC, puoi utilizzare l'operazione AWS Management Console o l'CreateDataSourceAPI. Se utilizzi la console, connetti un VPC durante il processo di configurazione del connettore.

> **Note**
>
> La Amazon VPC funzionalità è facoltativa quando si configura un connettore di origine Amazon Kendra dati. Se la fonte di dati è accessibile dalla rete Internet pubblica, non è necessario abilitare la Amazon VPC funzione. Non tutti i connettori di origine Amazon Kendra dati sono supportati Amazon VPC.

Se la tua origine dati non è in esecuzione Amazon VPC e non è accessibile dalla rete Internet pubblica, devi innanzitutto connetterla al tuo VPC utilizzando una rete privata virtuale (VPN). Quindi, puoi connettere la tua fonte di dati Amazon Kendra utilizzando una combinazione di Amazon VPC e AWS Virtual Private Network. Per informazioni sulla configurazione di una VPN, consulta la AWS VPN documentazione.

Argomenti

- Configurazione del Amazon VPC supporto per i connettori Amazon Kendra
- Configura un'origine Amazon Kendra dati a cui connetterti Amazon VPC
- Connessione a un database in un VPC
- Risoluzione dei problemi di connessione VPC

Configurazione del Amazon VPC supporto per i connettori Amazon Kendra

Per configurarlo Amazon VPC per l'uso con i Amazon Kendra connettori, procedi nel seguente modo.

Fasi

- Fase 1. Crea Amazon VPC sottoreti per Amazon Kendra
- Fase 2. Crea gruppi di sicurezza per Amazon VPCAmazon Kendra
- Fase 3. Configura la tua fonte di dati esterna e Amazon VPC

Fase 1. Crea Amazon VPC sottoreti per Amazon Kendra

Crea o scegli una Amazon VPC sottorete esistente che Amazon Kendra puoi utilizzare per accedere alla tua fonte di dati. Le sottoreti preparate devono trovarsi in una delle seguenti zone di disponibilità Regioni AWS e in una delle seguenti zone di disponibilità:

- Stati Uniti occidentali (Oregon) /us-west-2—usw2-az1, usw2-az2, usw2-az3
- Stati Uniti orientali (Virginia settentrionale) /us-east-1—use1-az1, use1-az2, use1-az4
- Stati Uniti orientali (Ohio) /us-east-2—use2-az1, use2-az2, use2-az3
- Asia Pacifico (Tokyo) /ap-northeast-1—apne1-az1, apne1-az2, apne1-az4
- Asia Pacifico (Mumbai) /ap-south-1—aps1-az1, aps1-az2, aps1-az3
- Asia Pacifico (Singapore) /ap-southeast-1—apse1-az1, apse1-az2, apse1-az3
- Asia Pacifico (Sydney) /ap-southeast-2—apse2-az1, apse2-az2, apse2-az3
- Canada (centrale) /ca-central-1—cac1-az1, cac1-az2, cac1-az4
- Europa (Irlanda) /eu-west-1—euw1-az1, uew1-az2, euw1-az3
- Europa (Londra) /eu-west-2—usw2-az1, usw2-az2, usw2-az3

La tua fonte di dati deve essere accessibile dalle sottoreti che hai fornito a Connector. Amazon Kendra

Per ulteriori informazioni su come configurare le Amazon VPC sottoreti, consulta Subnet for your nella Amazon VPC Amazon VPC User Guide.

Se Amazon Kendra devi instradare la connessione tra due o più sottoreti, puoi preparare più sottoreti. Ad esempio, la sottorete che contiene la fonte dei dati ha esaurito gli indirizzi IP. In tal caso, è

possibile fornire una sottorete aggiuntiva Amazon Kendra con indirizzi IP sufficienti e connessa alla prima sottorete. Se si elencano più sottoreti, queste devono essere in grado di comunicare tra loro.

Fase 2. Crea gruppi di sicurezza per Amazon VPCAmazon Kendra

Per connettere il connettore di origine Amazon Kendra dati a Amazon VPC, devi preparare uno o più gruppi di sicurezza dal tuo VPC a cui assegnare. Amazon Kendra I gruppi di sicurezza verranno associati all'interfaccia elastica di rete creata da Amazon Kendra. Questa interfaccia di rete controlla il traffico in entrata e in uscita da e verso le Amazon Kendra Amazon VPC sottoreti.

Assicurati che le regole in uscita del tuo gruppo di sicurezza consentano al traffico proveniente dai connettori delle sorgenti Amazon Kendra dati di accedere alle sottoreti e all'origine dati con cui intendi sincronizzarti. Ad esempio, potresti utilizzare un MySQL connettore per la sincronizzazione da un database. MySQL Se si utilizza la porta predefinita, i gruppi di sicurezza devono consentire l'accesso Amazon Kendra alla porta 3306 sull'host che esegue il database.

Ti consigliamo di configurare un gruppo di sicurezza predefinito con i seguenti valori Amazon Kendra da utilizzare:

- Regole in entrata: se scegli di lasciare questo campo vuoto, tutto il traffico in entrata verrà bloccato.
- Regole in uscita: aggiungi una regola per consentire tutto il traffico in uscita in modo da Amazon Kendra poter avviare le richieste di sincronizzazione dalla tua fonte di dati.
  - Versione IP: IPv4
  - Tipo: tutto il traffico
  - Protocollo: tutto il traffico
  - Intervallo di porte: tutto
  - Destinazione — 0.0.0.0/0

Per ulteriori informazioni su come configurare i gruppi Amazon VPC di sicurezza, consulta le regole dei gruppi di sicurezza nella Amazon VPC User Guide.

Fase 3. Configura la tua fonte di dati esterna e Amazon VPC

Assicurati che l'origine dati esterna disponga della configurazione delle autorizzazioni e delle impostazioni di rete corrette Amazon Kendra per accedervi. Puoi trovare istruzioni dettagliate su come configurare le tue fonti di dati nella sezione dei prerequisiti di ogni pagina del connettore.

Inoltre, controlla Amazon VPC le impostazioni e assicurati che la fonte di dati esterna sia raggiungibile dalla sottorete a cui effettuerai l'assegnazione. Amazon Kendra A tale scopo, ti consigliamo di creare un' Amazon EC2 istanza nella stessa sottorete con gli stessi gruppi di sicurezza e di testare l'accesso alla fonte di dati da questa istanza. Amazon EC2 Per ulteriori informazioni, consulta Risoluzione dei problemi di Amazon VPC connessione.

Configura un'origine Amazon Kendra dati a cui connetterti Amazon VPC

Quando aggiungi una nuova origine dati in Amazon Kendra, puoi utilizzare la Amazon VPC funzione se il connettore di origine dati selezionato supporta questa funzionalità.

Puoi configurare una nuova fonte di Amazon Kendra dati Amazon VPC abilitandola utilizzando AWS Management Console o l' Amazon Kendra API. In particolare, utilizzate l'operazione CreateDataSourceAPI, quindi utilizzate il `VpcConfiguration` parametro per fornire le seguenti informazioni:

- `SubnetIds`— Un elenco di identificatori di sottoreti Amazon VPC
- `SecurityGroupIds`— Un elenco di identificatori di gruppi di sicurezza Amazon VPC

Se si utilizza la console, si forniscono le Amazon VPC informazioni richieste durante la configurazione del connettore. Per utilizzare la console per abilitare la funzionalità Amazon VPC per un connettore, devi prima scegliere un Amazon VPC. Quindi, fornisci gli identificatori di tutte le sottoreti Amazon VPC e gli identificatori di qualsiasi gruppo di sicurezza Amazon VPC. Puoi scegliere le sottoreti Amazon VPC e i gruppi di sicurezza Amazon VPC che hai creato in Configurazione di Amazon VPC o utilizzare quelli esistenti.

Argomenti

- Visualizzazione degli identificatori Amazon VPC
- Verifica del ruolo della fonte di IAM dati

Visualizzazione degli identificatori Amazon VPC

Gli identificatori per le sottoreti e i gruppi di sicurezza sono configurati nella console. Amazon VPC Per visualizzare gli identificatori, utilizzare le seguenti procedure.

Per visualizzare gli identificatori di sottorete

1. Accedi AWS Management Console e apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Dal pannello di navigazione, scegli Subnet.
3. Dall'elenco delle sottoreti, scegli la sottorete che contiene il server del database.
4. Nella scheda Dettagli, prendi nota dell'identificatore nel campo ID sottorete.

Per visualizzare gli identificatori dei gruppi di sicurezza

1. Accedi AWS Management Console e apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Dal pannello di navigazione, scegli Gruppi di sicurezza.
3. Dall'elenco dei gruppi di sicurezza, scegli il gruppo per cui desideri l'identificatore.
4. Nella scheda Dettagli, prendi nota dell'identificatore nel campo ID del gruppo di sicurezza.

Verifica del ruolo della fonte di IAM dati

Assicurati che il ruolo Data Source Connector AWS Identity and Access Management IAM () contenga le autorizzazioni per accedere al tuo Amazon VPC.

Se utilizzi la console per creare un nuovo ruolo per il tuo IAM ruolo, aggiunge Amazon Kendra automaticamente le autorizzazioni corrette al IAM ruolo per tuo conto. Se utilizzi l'API o utilizzi un IAM ruolo esistente, verifica che il ruolo contenga le autorizzazioni di accesso. Amazon VPC Per verificare di disporre delle autorizzazioni corrette, consulta IAM ruoli per VPC.

È possibile modificare un'origine dati esistente per utilizzare una sottorete diversa Amazon VPC . Tuttavia, controlla il IAM ruolo della tua fonte di dati e, se necessario, modificala in modo che rifletta la modifica relativa al corretto funzionamento del connettore di origine Amazon Kendra dati.

Connessione a un database in un VPC

L'esempio seguente mostra come connettere un MySQL database in esecuzione in un cloud privato virtuale (VPC). L'esempio presuppone che si stia iniziando con il VPC predefinito e che sia necessario creare un MySQL database. Se hai già un VPC, assicurati che sia configurato come mostrato. Se hai un MySQL database, puoi usarlo invece di crearne uno nuovo.

Fasi

Fase 1: Configurazione di un VPC

Configura il tuo VPC in modo da avere una sottorete privata e un gruppo di sicurezza per accedere Amazon Kendra a un MySQL database in esecuzione nella sottorete. Le sottoreti fornite nella configurazione VPC devono trovarsi nella regione Stati Uniti occidentali (Oregon), nella regione Stati Uniti orientali (Virginia settentrionale) o nella regione Europa (Irlanda).

Per configurare un VPC utilizzando Amazon VPC

1. Accedi AWS Management Console e apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Dal pannello di navigazione, scegli Tabelle di percorsi, quindi scegli Crea tabella di percorsi.
3. Per il campo Nome, inserisci**`Private subnet route table`**. Dal menu a discesa VPC, seleziona il tuo VPC, quindi scegli Crea tabella di percorsi. Scegli Chiudi per tornare all'elenco delle tabelle dei percorsi.
4. Dal pannello di navigazione, scegli Gateway NAT, quindi scegli Crea gateway NAT.
5. Dal menu a discesa Subnet, scegli la sottorete che è la sottorete pubblica. Prendi nota dell'ID della sottorete.
6. Se non disponi di un indirizzo IP elastico, scegli Crea nuovo EIP, scegli Crea un gateway NAT e quindi scegli Chiudi.
7. Dal pannello di navigazione, scegli Tabelle dei percorsi.
8. Dall'elenco delle tabelle di routing, scegli la tabella di routing della sottorete privata che hai creato nel passaggio 3. Da Azioni, scegli Modifica percorsi.
9. Scegli Aggiungi route. Per la destinazione, inserisci **`0.0.0.0/0`** per consentire tutto il traffico in uscita verso Internet. Per Target, scegli NAT Gateway, quindi scegli il gateway creato nel passaggio 4. Scegli Salva modifiche, quindi scegli Chiudi.
10. In Azioni, scegli Modifica associazioni di sottoreti.

11. Scegli le sottoreti che desideri siano private. Non scegliete la sottorete con il gateway NAT che avete annotato in precedenza. Scegli Salva associazioni quando hai finito.

Passaggio 2: creare e configurare gruppi di sicurezza

Quindi, configura i gruppi di sicurezza per il tuo database.

Per creare e configurare gruppi di sicurezza

1. Accedi AWS Management Console e apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Dalla descrizione del tuo VPC, prendi nota del CIDR IPv4.
3. Dal riquadro di navigazione, scegli Gruppi di sicurezza, quindi scegli Crea gruppo di sicurezza.
4. In Security group name (Nome gruppo di sicurezza) immettere **`DataSourceInboundSecurityGroup`**. Fornisci una descrizione, quindi scegli il tuo VPC dall'elenco. Scegli Crea gruppo di sicurezza, quindi scegli Chiudi.
5. Selezionare la scheda Inbound Rules (Regole in entrata).
6. Scegli Modifica regole in entrata, quindi scegli Aggiungi regola
7. Per un database, inserisci il numero di porta per l'intervallo di porte. Ad esempio, per MySQL it è**`3306`**, e, per HTTPS, è**`443`**. Per il codice Source, digita il Classless Inter-Domain Routing (CIDR) del tuo VPC. Scegli Salva regole, quindi scegli Chiudi.

Il gruppo di sicurezza consente a chiunque all'interno del VPC di connettersi al database e consente connessioni in uscita a Internet.

Fase 3: Creare un database

Crea un database per archiviare i tuoi documenti oppure puoi utilizzare il database esistente.

Per istruzioni su come creare un MySQL database, consulta MySQL.

Fase 4: Creare un connettore per l'origine dati

Dopo aver configurato il VPC e creato il database, puoi creare un connettore di origine dati per il database. Per informazioni sui connettori di database Amazon Kendra supportati, consulta Connettori supportati.

Per il tuo database, assicurati di configurare il tuo VPC, le sottoreti private che hai creato nel tuo VPC e il gruppo di sicurezza che hai creato nel tuo VPC.

Risoluzione dei problemi di connessione VPC

In caso di problemi con la connessione al cloud privato virtuale (VPC), verifica che IAM le autorizzazioni, le impostazioni dei gruppi di sicurezza e le tabelle di routing della sottorete siano configurate correttamente.

Una possibile causa di una mancata sincronizzazione del connettore di origine dati è che l'origine dati potrebbe non essere raggiungibile dalla sottorete a cui è stata assegnata. Amazon Kendra Per risolvere questo problema, ti consigliamo di creare un' Amazon EC2 istanza con le stesse impostazioni. Amazon VPC Quindi, prova ad accedere all'origine dati da questa Amazon EC2 istanza utilizzando chiamate API REST o altri metodi (in base al tipo specifico di origine dati).

Se accedi con successo all'origine dati dall' Amazon EC2 istanza che crei, significa che l'origine dati è raggiungibile da questa sottorete. Pertanto, il problema di sincronizzazione non è correlato all'inaccessibilità della fonte di dati da. Amazon VPC

Se non riesci ad accedere all' Amazon EC2 istanza dalla configurazione del VPC e a convalidarla con l' Amazon EC2 istanza che hai creato, devi risolvere ulteriormente i problemi. Ad esempio, se hai un Amazon S3 connettore la cui sincronizzazione non è riuscita a causa di errori relativi a problemi di connessione, puoi configurare un' Amazon EC2 istanza con la stessa Amazon VPC configurazione che hai assegnato al connettore. Amazon S3 Quindi, usa questa istanza Amazon EC2 per verificare se la tua Amazon VPC è stata configurata correttamente.

Di seguito è riportato un esempio di configurazione di un' Amazon EC2 istanza per risolvere i problemi di Amazon VPC connessione con un' Amazon S3 origine dati.

Argomenti

Fase 1: Avviare un'istanza Amazon EC2

1. Accedi AWS Management Console e apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.

2. Seleziona Avvia un'istanza.
3. Scegli Impostazioni di rete, quindi scegli Modifica, quindi esegui le seguenti operazioni:

   a. Scegli lo stesso VPC e la stessa sottorete a cui hai assegnato. Amazon Kendra
   b. Per Firewall (gruppi di sicurezza), scegli Seleziona gruppo di sicurezza esistente. Quindi, seleziona il gruppo di sicurezza a cui hai assegnato Amazon Kendra.

      > **Note**
      >
      > Il gruppo di sicurezza dovrebbe consentire al traffico in uscita di Amazon S3.

   c. Imposta Assegna automaticamente l'IP pubblico su Disabilita.
   d. In Dettagli avanzati, procedi come segue:

      - Per il profilo dell'istanza IAM, seleziona Crea nuovo profilo IAM per creare e allegare un profilo di IAM istanza alla tua istanza. Assicurati che il profilo disponga delle autorizzazioni di accesso Amazon S3. Per ulteriori informazioni, vedi Come posso concedere alla mia Amazon EC2 istanza l'accesso a un Amazon S3 bucket? nel AWS re:Post.
      - Lascia tutte le altre impostazioni come predefinite.

   e. Rivedi e avvia l' Amazon EC2 istanza.

Passaggio 2: Connect all' Amazon EC2 istanza

Dopo l'esecuzione dell' Amazon EC2 istanza, vai alla pagina dei dettagli dell'istanza e connettiti all'istanza. A tale scopo, segui la procedura descritta in Connetti alle tue istanze senza richiedere un indirizzo IPv4 pubblico utilizzando l'endpoint EC2 Instance Connect nella Guida per Amazon EC2 l'utente per le istanze Linux.

Fase 3: Verifica l'accesso Amazon S3

Dopo esserti connesso al terminale dell' Amazon EC2 istanza, esegui un AWS CLI comando per testare la connessione da questa sottorete privata al tuo Amazon S3 bucket.

Per testare Amazon S3 l'accesso, digita il seguente AWS CLI comando in: AWS CLI `aws s3 ls`

Dopo l'esecuzione del AWS CLI comando, esaminate quanto segue:

- Se hai impostato correttamente le IAM autorizzazioni necessarie e la Amazon S3 configurazione è corretta, dovresti vedere un elenco dei tuoi Amazon S3 bucket.

- Se riscontri errori di autorizzazione`Access Denied`, ad esempio, è probabile che la configurazione del tuo VPC sia corretta, ma c'è qualcosa che non va nelle tue IAM autorizzazioni o nella politica del bucket. Amazon S3

Se il comando è scaduto, è probabile che la connessione stia scadendo perché la configurazione del VPC non è corretta e l'istanza Amazon EC2 non può accedere ad Amazon S3 dalla sottorete. Riconfigura il tuo VPC e riprova.

Eliminazione di un indice, di un'origine dati o di documenti caricati in batch

Questa sezione mostra come eliminare un indice, un archivio di fonti di dati dei documenti nel tuo indice o documenti nell'indice che hai caricato in batch.

Argomenti

Eliminazione di un indice

È possibile eliminare un indice da Amazon Kendra quando non lo si utilizza più. Ad esempio, elimina un indice quando:

- Non stai più utilizzando l'indice e desideri ridurre gli addebiti AWS sul tuo account. Un Amazon Kendra indice addebita commissioni durante la sua esecuzione, indipendentemente dal fatto che si effettuino o meno delle interrogazioni sull'indice.
- Vuoi riconfigurare l'indice per un'edizione diversa di. Amazon Kendra Elimina l'indice esistente e poi creane uno nuovo con l'edizione diversa.
- Hai raggiunto il numero massimo di indici nel tuo account e non vuoi superare la tua quota. Eliminare un indice esistente e aggiungerne uno nuovo. Per informazioni sul numero massimo di indici che puoi creare, consulta Quote.

Per eliminare un indice, utilizza la consoleAWS Command Line Interface, lo AWS CloudFormation script o l'`DeleteIndex`API. L'eliminazione di un indice rimuove l'indice e tutte le fonti di dati e i dati del documento associati. L'eliminazione di un indice non rimuove i documenti originali dalla memoria.

L'eliminazione di un indice è un'operazione asincrona. Quando si inizia a eliminare un indice, lo stato dell'indice cambia in`DELETING`. Rimane nello `DELETING` stato fino alla rimozione di tutte le informazioni relative all'indice. Una volta eliminato, l'indice non viene più visualizzato nei risultati di una chiamata all'ListIndicesAPI. Se chiami l'DescribeIndexAPI con l'identificatore dell'indice eliminato, ricevi `ResourceNotFound` un'eccezione.

Per eliminare un indice (console)

1. Accedi AWS Management Console e apri la Amazon Kendra console all'indirizzo https://console.aws.amazon.com/kendra/.
2. Nel riquadro di navigazione, scegli Indici, quindi scegli l'indice da eliminare.
3. Scegliete Elimina per eliminare l'indice selezionato.

Per eliminare un indice (CLI)

- Nel AWS CLI, usa il seguente comando. Il comando è formattato per Linux e macOS. Se usi Windows, sostituisci il carattere di continuazione della riga Unix (\) con un accento circonflesso (^).

```
aws kendra delete-index \
   --id index-id
```

Eliminazione di un'origine dati

Elimini un'origine dati quando desideri rimuovere dall'Amazon Kendraindice le informazioni in essa contenute. Ad esempio, elimina un'origine dati quando:

- Un'origine dati non è configurata correttamente. Elimina l'origine dati, attendi che l'origine dati finisca di essere eliminata, quindi ricreala.
- Hai migrato i documenti da un'origine dati all'altra. Eliminare l'origine dati originale e ricrearla nella nuova posizione.
- Hai raggiunto il limite di fonti di dati per un indice. Elimina una delle fonti di dati esistenti e aggiungine una nuova. Per ulteriori informazioni sul numero di fonti di dati che è possibile creare, vedereQuote.

Per eliminare un'origine dati, utilizza la console, la AWS Command Line Interface (AWS CLI), l'`DeleteDataSource`API o uno AWS CloudFormation script. L'eliminazione di un'origine dati rimuove tutte le informazioni sull'origine dati dall'indice. Se desideri interrompere solo la sincronizzazione dell'origine dati, modifica la pianificazione della sincronizzazione per l'origine dati in «esecuzione su richiesta».

L'eliminazione di un'origine dati è un'operazione asincrona. Quando inizi a eliminare un'origine dati, lo stato dell'origine dati cambia in`DELETING`. Rimane nello `DELETING` stato fino alla rimozione delle informazioni relative alla fonte dei dati. Dopo l'eliminazione, l'origine dati non viene più visualizzata nei risultati di una chiamata all'ListDataSourcesAPI. Se chiami l'DescribeDataSourceAPI con l'identificatore dell'origine dati eliminata, ricevi un'`ResourceNotFound`eccezione.

> **Note**
>
> L'eliminazione di un'intera origine dati o la risincronizzazione dell'indice dopo aver eliminato documenti specifici da un'origine dati possono richiedere fino a un'ora o più, a seconda del numero di documenti che si desidera eliminare.

Per eliminare un'origine dati (console)

1. Accedi AWS Management Console e apri la Amazon Kendra console all'indirizzo https://console.aws.amazon.com/kendra/.
2. Nel riquadro di navigazione, scegli Indici, quindi scegli l'indice che contiene l'origine dati da eliminare.
3. Nel pannello di navigazione scegli Data sources (Origini dati).
4. Scegli l'origine dei dati da rimuovere.
5. Scegliete Elimina per eliminare l'origine dati.

Per eliminare un'origine dati (CLI)

- Nel AWS Command Line Interface, usa il seguente comando. Il comando è formattato per Linux e macOS. Se usi Windows, sostituisci il carattere di continuazione della riga Unix (\) con un accento circonflesso (^).

```
aws kendra delete-data-source \
   --id data-source-id \
   --index-id index-id
```

Quando si elimina un'origine dati, Amazon Kendra rimuove tutte le informazioni memorizzate sull'origine dati. Amazon Kendrarimuove tutti i dati del documento archiviati nell'indice e tutte le

cronologie e le metriche di esecuzione associate all'origine dati. L'eliminazione di un'origine dati non rimuove i documenti originali dalla memoria.

I documenti nell'origine dati possono essere inclusi nel numero di documenti restituito dall'`DescribeIndex`API mentre si Amazon Kendra elimina un'origine dati. I documenti della fonte dati possono essere visualizzati nei risultati di ricerca mentre l'origine dati Amazon Kendra viene eliminata.

Amazon Kendrarilascia le risorse per un'origine dati non appena richiami l'`DeleteDataSource`API o scegli di eliminare l'origine dati nella console. Se stai eliminando l'origine dati per ridurre il numero di fonti di dati al di sotto del limite, puoi creare subito una nuova origine dati.

Se stai eliminando un'origine dati e quindi stai creando un'altra origine dati per i dati del documento, attendi che la prima origine dati venga eliminata prima di sincronizzare la nuova origine dati.

È possibile eliminare un'origine dati in corso di sincronizzazione conAmazon Kendra. La sincronizzazione viene interrotta e l'origine dati viene rimossa. Se si tenta di avviare una sincronizzazione quando l'origine dati viene eliminata, si ottiene un'`ConflictException`eccezione.

Non è possibile eliminare un'origine dati se l'indice associato è nello `DELETING` stato. L'eliminazione di un indice comporta l'eliminazione di tutte le fonti di dati dell'indice. Puoi iniziare a eliminare un indice mentre un'origine dati per quell'indice è nello `DELETING` stato.

Se hai due origini dati che puntano agli stessi documenti, ad esempio due origini dati che puntano allo stesso Amazon S3 bucket, i documenti nell'indice potrebbero non essere coerenti quando una delle fonti di dati viene eliminata. Quando due fonti di dati fanno riferimento agli stessi documenti, nell'indice viene memorizzata una sola copia dei dati del documento. La rimozione di un'origine dati rimuove i dati dell'indice dei documenti. L'altra fonte di dati non è a conoscenza del fatto che i documenti sono stati rimossi, quindi Amazon Kendra non li reindicizzerà correttamente alla successiva sincronizzazione. Quando hai due origini dati che puntano alla stessa posizione del documento, devi eliminare entrambe le fonti di dati e quindi ricrearne una.

Eliminazione di documenti caricati in batch

Puoi eliminare documenti direttamente da un indice utilizzando l'BatchDeleteDocumentAPI. Non puoi eliminare documenti direttamente utilizzando la console. Se utilizzi la console, puoi eliminare documenti specifici dal tuo archivio di origini dati e risincronizzarli con l'indice o eliminare l'intero connettore di origine dati.

L'eliminazione di documenti da un indice utilizzando `BatchDeleteDocument` è un'operazione asincrona. Dopo aver chiamato l'`BatchDeleteDocument`API, puoi utilizzare l'BatchGetDocumentStatusAPI per monitorare l'avanzamento dell'eliminazione dei documenti. Quando un documento viene eliminato dall'indice, viene Amazon Kendra `NOT_FOUND` restituito lo stato.

> **Note**
>
> L'eliminazione di documenti da un indice utilizzando `BatchDeleteDocument` può richiedere fino a un'ora o più, a seconda del numero di documenti che si desidera eliminare.

Per eliminare documenti caricati in batch da un indice (CLI)

- Nel AWS Command Line Interface, usa il seguente comando. Il comando è formattato per Linux e macOS. Se usi Windows, sostituisci il carattere di continuazione della riga Unix (\) con un accento circonflesso (^).

```
aws kendra batch-delete-document \
   --index-id index-id \
   --document-id-list 'doc-id-1' 'doc-id-2'
```

Arricchimento dei documenti durante l'ingestione

È possibile modificare i campi o gli attributi dei contenuti e dei metadati del documento durante il processo di inserimento del documento. Con Amazon Kendra la funzione Custom Document Enrichment, puoi creare, modificare o eliminare gli attributi e i contenuti dei documenti quando inserisci i tuoi documenti. Amazon Kendra Ciò significa che puoi manipolare e importare i tuoi dati in base alle tue esigenze.

Questa funzione consente di controllare il modo in cui i documenti vengono trattati e inseriti. Amazon Kendra Ad esempio, puoi cancellare le informazioni di identificazione personale nei metadati del documento durante l'inserimento dei documenti. Amazon Kendra

Un altro modo per utilizzare questa funzionalità consiste nel richiamare una funzione Lambda AWS Lambda per eseguire il riconoscimento ottico dei caratteri (OCR) su immagini, la traduzione sul testo e altre attività di preparazione dei dati per la ricerca o l'analisi. Ad esempio, puoi richiamare una funzione per eseguire l'OCR sulle immagini. La funzione può interpretare il testo dalle immagini e trattare ogni immagine come un documento testuale. Un'azienda che riceve sondaggi per i clienti per posta e li archivia sotto forma di immagini potrebbe inserirle come documenti testuali. Amazon Kendra L'azienda può quindi cercare informazioni preziose nei sondaggi sui clienti inAmazon Kendra.

È possibile utilizzare le operazioni di base da applicare come prima analisi dei dati, quindi utilizzare una funzione Lambda per applicare operazioni più complesse sui dati. Ad esempio, è possibile utilizzare un'operazione di base per rimuovere semplicemente tutti i valori nel campo dei metadati del documento 'Customer_ID' e quindi applicare una funzione Lambda per estrarre il testo dalle immagini del testo nei documenti.

Come funziona l'arricchimento personalizzato dei documenti

Il processo complessivo di Custom Document Enrichment è il seguente:

1. Puoi configurare Custom Document Enrichment quando crei o aggiorni la tua fonte di dati o indicizzi i tuoi documenti direttamente inAmazon Kendra.
2. Amazon Kendraapplica configurazioni in linea o logica di base per modificare i dati. Per ulteriori informazioni, consulta the section called “Operazioni di base per modificare i metadati”.
3. Se scegli di configurare la manipolazione avanzata dei dati, Amazon Kendra puoi applicarla ai tuoi documenti originali non elaborati o ai documenti strutturati e analizzati. Per ulteriori informazioni, consulta the section called “Funzioni Lambda: estrarre e modificare metadati o contenuti”.

4. I tuoi documenti alterati vengono inseriti. Amazon Kendra

In qualsiasi momento di questo processo, se la configurazione non è valida, Amazon Kendra genera un errore.

Quando chiami le BatchPutDocumentAPI CreateDataSourceUpdateDataSource, fornisci la tua configurazione personalizzata per l'arricchimento dei documenti. Se chiami`BatchPutDocument`, devi configurare Custom Document Enrichment con ogni richiesta. Se usi la console, seleziona l'indice e quindi seleziona Arricchimenti dei documenti per configurare l'arricchimento personalizzato dei documenti.

Se utilizzi Document Enrichments nella console, puoi scegliere di configurare solo le operazioni di base o solo le funzioni Lambda o entrambe, come puoi fare usando l'API. Puoi selezionare Avanti nei passaggi della console per scegliere di non configurare le operazioni di base e solo le funzioni Lambda, incluso se applicarle ai dati originali (preestrazione) o strutturati (post-estrazione). Puoi salvare le tue configurazioni solo completando tutti i passaggi nella console. Le configurazioni del documento non vengono salvate se non completi tutti i passaggi.

Operazioni di base per modificare i metadati

È possibile manipolare i campi e il contenuto del documento utilizzando la logica di base. Ciò include la rimozione di valori in un campo, la modifica dei valori in un campo utilizzando una condizione o la creazione di un campo. Per manipolazioni avanzate che vanno oltre ciò che è possibile manipolare utilizzando la logica di base, richiama una funzione Lambda. Per ulteriori informazioni, consulta the section called “Funzioni Lambda: estrarre e modificare metadati o contenuti”.

Per applicare la logica di base, è necessario specificare il campo di destinazione che si desidera manipolare utilizzando l'DocumentAttributeTargetoggetto. Fornisci la chiave dell'attributo. Ad esempio, la chiave 'Dipartimento' è un campo o un attributo che contiene tutti i nomi dei reparti associati ai documenti. È inoltre possibile specificare un valore da utilizzare nel campo di destinazione se viene soddisfatta una determinata condizione. La condizione viene impostata utilizzando l'DocumentAttributeConditionoggetto. Ad esempio, se il campo 'Source_URI' contiene 'financial' nel suo valore URI, precompila il campo di destinazione 'Dipartimento' con il valore di destinazione 'Finance' per il documento. Puoi anche eliminare i valori dell'attributo del documento di destinazione.

Per applicare la logica di base utilizzando la console, seleziona il tuo indice e quindi seleziona Arricchimenti dei documenti nel menu di navigazione. Vai a Configura le operazioni di base per applicare le manipolazioni di base ai campi e ai contenuti del documento.

Di seguito è riportato un esempio di utilizzo della logica di base per rimuovere tutti i numeri di identificazione del cliente nel campo del documento chiamato 'customer_id'.

Esempio 1: rimozione dei numeri di identificazione del cliente associati ai documenti

Dati prima della manipolazione di base applicata.

ID del documento	Corpo_testo	ID cliente
1	Lorem Ipsum.	CID1234
2	Lorem Ipsum.	CID1235
3	Lorem Ipsum.	CID1236

Dati dopo l'applicazione della manipolazione di base.

ID del documento	Corpo_testo	ID cliente
1	Lorem Ipsum.	
2	Lorem Ipsum.	
3	Lorem Ipsum.	

Di seguito è riportato un esempio di utilizzo della logica di base per creare un campo chiamato «Dipartimento» e precompilare questo campo con i nomi dei reparti in base alle informazioni del campo «Source_URI». Viene utilizzata la condizione che se il campo 'Source_URI' contiene 'financial' nel suo valore URI, precompili il campo di destinazione 'Dipartimento' con il valore di destinazione 'Finance' per il documento.

Esempio 2: creazione del campo «Reparto» e precompilazione con i nomi dei reparti associati ai documenti utilizzando una condizione.

Dati prima della manipolazione di base applicata.

ID del documento	Corpo_testo	Fonte_uri
1	Lorem Ipsum.	finanziario/1
2	Lorem Ipsum.	finanziario/2
3	Lorem Ipsum.	finanziario/3

Dati dopo l'applicazione della manipolazione di base.

ID del documento	Corpo_testo	Fonte_uri	Dipartimento
1	Lorem Ipsum.	finanziario/1	Finanza
2	Lorem Ipsum.	finanziario/2	Finanza
3	Lorem Ipsum.	finanziario/3	Finanza

> **Note**
>
> Amazon Kendranon è possibile creare un campo del documento di destinazione se non è già stato creato come campo indice. Dopo aver creato il campo indice, puoi creare un campo documento utilizzando`DocumentAttributeTarget`. Amazon Kendraquindi associa il campo dei metadati del documento appena creato al campo indice.

Il codice seguente è un esempio di configurazione della manipolazione di base dei dati per rimuovere i numeri di identificazione dei clienti associati ai documenti.

Console

Per configurare la manipolazione di base dei dati per rimuovere i numeri di identificazione del cliente

1. Nel riquadro di navigazione a sinistra, in Indici, seleziona Arricchimenti del documento, quindi seleziona Aggiungi arricchimento del documento.

2. Nella pagina Configura le operazioni di base, scegli dal menu a discesa la fonte di dati in cui desideri modificare i campi e il contenuto del documento. Quindi scegli dal menu a discesa il nome del campo del documento 'Customer_ID', seleziona dal menu a discesa il nome del campo indice 'Customer_ID' e seleziona dal menu a discesa l'azione di destinazione Elimina. Quindi seleziona Aggiungi operazione di base.

CLI

Per configurare la manipolazione di base dei dati per rimuovere i numeri di identificazione del cliente

```
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

Per configurare la manipolazione di base dei dati per rimuovere i numeri di identificazione del cliente

```
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

Per configurare la manipolazione di base dei dati per rimuovere i numeri di identificazione del cliente

```
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");
    }
}
```

Funzioni Lambda: estrarre e modificare metadati o contenuti

È possibile manipolare i campi e il contenuto del documento utilizzando le funzioni Lambda. Ciò è utile se si desidera andare oltre la logica di base e applicare manipolazioni avanzate dei dati. Ad esempio, utilizzando il riconoscimento ottico dei caratteri (OCR), che interpreta il testo dalle immagini e tratta ogni immagine come un documento testuale. Oppure, recuperando la data-ora corrente in un determinato fuso orario e inserendo la data-ora in cui è presente un valore vuoto per un campo data.

È possibile applicare prima la logica di base e quindi utilizzare una funzione Lambda per manipolare ulteriormente i dati o viceversa. Puoi anche scegliere di applicare solo una funzione Lambda.

Amazon Kendrapuò richiamare una funzione Lambda per applicare manipolazioni avanzate dei dati durante il processo di inserimento come parte del tuo. CustomDocumentEnrichmentConfiguration Specifichi un ruolo che include l'autorizzazione per eseguire la funzione Lambda e accedere al tuo Amazon S3 bucket per archiviare l'output delle tue manipolazioni IAM dei dati: vedi ruoli di accesso.

Amazon Kendrapuò applicare una funzione Lambda sui documenti originali non elaborati o sui documenti strutturati e analizzati. È possibile configurare una funzione Lambda che prende i dati originali o grezzi e applica le manipolazioni dei dati utilizzando. PreExtractionHookConfiguration Puoi anche configurare una funzione Lambda che prende i tuoi documenti strutturati e applica le tue manipolazioni dei dati utilizzando. PostExtractionHookConfiguration Amazon Kendraestrae i metadati e il testo del documento per strutturare i documenti. Le funzioni Lambda devono seguire le strutture obbligatorie di richiesta e risposta. Per ulteriori informazioni, consulta the section called “Contratti dati per funzioni Lambda”.

Per configurare una funzione Lambda nella console, seleziona il tuo indice e quindi seleziona Arricchimenti del documento nel menu di navigazione. Vai a Configura funzioni Lambda per configurare una funzione Lambda.

È possibile configurare solo una funzione Lambda per `PreExtractionHookConfiguration` e una sola funzione Lambda per. `PostExtractionHookConfiguration` Tuttavia, la funzione Lambda può richiamare altre funzioni richieste. Puoi configurare entrambi `PreExtractionHookConfiguration` `PostExtractionHookConfiguration` e/o uno dei due. La funzione Lambda per non `PreExtractionHookConfiguration` deve superare un tempo di esecuzione di 5 minuti e la funzione Lambda per non `PostExtractionHookConfiguration` deve superare un tempo di esecuzione di 1 minuto. La configurazione di Custom Document Enrichment richiede naturalmente più tempo per l'inserimento dei documenti Amazon Kendra rispetto a quando non lo si configura.

È possibile configurare Amazon Kendra per richiamare una funzione Lambda solo se viene soddisfatta una condizione. Ad esempio, è possibile specificare una condizione secondo la quale, se sono presenti valori data-ora vuoti, Amazon Kendra deve richiamare una funzione che inserisca la data e l'ora corrente.

Di seguito è riportato un esempio di utilizzo di una funzione Lambda per eseguire l'OCR per interpretare il testo dalle immagini e archiviarlo in un campo chiamato 'Document_Image_Text'.

Esempio 1: estrazione di testo dalle immagini per creare documenti testuali

Dati prima dell'applicazione della manipolazione avanzata.

ID del documento	Immagine del documento
1	image_1.png
2	image_2.png
3	image_3.png

Dati dopo l'applicazione della manipolazione avanzata.

ID del documento	Immagine del documento	Documento_immagine_testo
1	image_1.png	Risposta al sondaggio inviata per posta
2	image_2.png	Risposta al sondaggio inviata per posta
3	image_3.png	Risposta al sondaggio inviata per posta

Di seguito è riportato un esempio di utilizzo di una funzione Lambda per inserire la data-ora corrente per valori di data vuoti. Viene utilizzata la condizione che se il valore di un campo data è 'nullo', lo sostituisca con la data-ora corrente.

Esempio 2: sostituzione dei valori vuoti nel campo Last_Updated con la data-ora corrente.

Dati prima dell'applicazione della manipolazione avanzata.

ID del documento	Corpo_testo	Ultimo aggiornamento
1	Lorem Ipsum.	1 gennaio 2020
2	Lorem Ipsum.	
3	Lorem Ipsum.	1 luglio 2020

Dati dopo l'applicazione della manipolazione avanzata.

ID del documento	Corpo_testo	Ultimo aggiornamento
1	Lorem Ipsum.	1 gennaio 2020
2	Lorem Ipsum.	1° dicembre 2021
3	Lorem Ipsum.	1 luglio 2020

Il codice seguente è un esempio di configurazione di una funzione Lambda per la manipolazione avanzata dei dati sui dati grezzi e originali.

Console

Per configurare una funzione Lambda per la manipolazione avanzata dei dati sui dati grezzi e originali

1. Nel riquadro di navigazione a sinistra, in Indici, seleziona Arricchimenti del documento, quindi seleziona Aggiungi arricchimento del documento.
2. Nella pagina Configura le funzioni Lambda, nella sezione Lambda per la preestrazione, seleziona dai menu a discesa la tua funzione Lambda ARN e il tuo bucket. Amazon S3 Aggiungi il tuo ruolo di IAM accesso selezionando l'opzione per creare un nuovo ruolo dal menu a discesa. In questo modo vengono create le Amazon Kendra autorizzazioni necessarie per creare l'arricchimento del documento.

CLI

Per configurare una funzione Lambda per la manipolazione avanzata dei dati sui dati grezzi e originali

```
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

Per configurare una funzione Lambda per la manipolazione avanzata dei dati sui dati grezzi e originali

```
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

Per configurare una funzione Lambda per la manipolazione avanzata dei dati sui dati grezzi e originali

```
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");
    }
}
```

Contratti dati per funzioni Lambda

Le funzioni Lambda per la manipolazione avanzata dei dati interagiscono con Amazon Kendra i contratti dati. I contratti sono le strutture obbligatorie di richiesta e risposta delle funzioni Lambda. Se le tue funzioni Lambda non seguono queste strutture, Amazon Kendra genera un errore.

La tua funzione Lambda per `PreExtractionHookConfiguration` dovrebbe aspettarsi la seguente struttura di richiesta:

```
{
    "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>
}
```

La `metadata` struttura, che include la `CustomDocumentAttribute` struttura, è la seguente:

```
{
    "attributes": [<CustomDocumentAttribute<]
}

CustomDocumentAttribute
{
    "name": <str>,
    "value": <CustomDocumentAttributeValue>
}

CustomDocumentAttributeValue
{
    "stringValue": <str>,
    "integerValue": <int>,
    "longValue": <long>,
    "stringListValue": list<str>,
    "dateValue": <str>
}
```

La tua funzione Lambda per `PreExtractionHookConfiguration` deve rispettare la seguente struttura di risposta:

```
{
    "version": <str>,
    "dataBlobStringEncodedInBase64": <str>, //In the case of a data blob
    "s3ObjectKey": <str>, //In the case of an S3 bucket
    "metadataUpdates": [<CustomDocumentAttribute>]
}
```

La tua funzione Lambda per `PostExtractionHookConfiguration` dovrebbe aspettarsi la seguente struttura di richiesta:

```
{
    "version": <str>,
    "s3Bucket": <str>,
    "s3ObjectKey": <str>,
    "metadata": <Metadata>
}
```

La tua funzione Lambda per `PostExtractionHookConfiguration` deve rispettare la seguente struttura di risposta:

```
PostExtractionHookConfiguration Lambda Response
{
    "version": <str>,
    "s3ObjectKey": <str>,
    "metadataUpdates": [<CustomDocumentAttribute>]
}
```

Il documento modificato viene caricato nel Amazon S3 bucket. Il documento modificato deve seguire il formato mostrato inthe section called “Formato di documento strutturato”.

Formato di documento strutturato

Amazon Kendracarica il documento strutturato nel Amazon S3 bucket specificato. Il documento strutturato segue questo formato:

```
Kendra document

{
   "textContent": <TextContent>
}

TextContent
{
  "documentBodyText": <str>
}
```

Esempio di funzione Lambda che aderisce ai contratti dati

Il seguente codice Python è un esempio di funzione Lambda che applica la manipolazione avanzata dei campi `_authors` di metadati e del contenuto del corpo `_document_title` dei documenti grezzi o originali.

Nel caso in cui il contenuto corporeo risieda in un secchio 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"]}}
        ]
    }
```

Nel caso in cui il contenuto corporeo risieda in un blob di dati

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

Il seguente codice Python è un esempio di funzione Lambda che applica la manipolazione avanzata dei campi `_authors` di metadati e del contenuto del corpo `_document_title` dei documenti strutturati o analizzati.

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

Ricerca in un indice

Per cercare un Amazon Kendra indice, si utilizza l'API Query. L'`Query`API restituisce informazioni sui documenti indicizzati utilizzati nell'applicazione. Questa sezione mostra come effettuare una query, eseguire filtri e interpretare la risposta che si ottiene dall'`Query`API.

Per cercare i documenti con cui hai indicizzato Amazon Lex, usa Amazon Kendra AMAZON. KendraSearchIntent. Per un esempio di configurazione Amazon Kendra con Amazon Lex, consulta Creazione di un bot per le domande frequenti per un Amazon Kendra indice.

Argomenti

Interrogare un indice

Quando esegui una ricerca nell'indice, Amazon Kendra utilizza tutte le informazioni che hai fornito sui documenti per determinare i documenti più pertinenti ai termini di ricerca inseriti. Alcuni degli elementi che vengono presi in Amazon Kendra considerazione sono:

- Il testo o il corpo del documento.
- Il titolo del documento.
- Campi di testo personalizzati contrassegnati come ricercabili.

- Il campo della data che hai indicato deve essere usato per determinare la «freschezza» di un documento.
- Qualsiasi altro campo che possa fornire informazioni pertinenti.

Amazon Kendra può anche filtrare la risposta in base a qualsiasi filtro di campo/attributo che potresti aver impostato per la ricerca. Ad esempio, se disponi di un campo personalizzato chiamato «reparto», puoi filtrare la risposta per restituire solo i documenti di un reparto chiamato «legale». Per ulteriori informazioni, consulta Campi o attributi personalizzati.

I risultati di ricerca restituiti vengono ordinati in base alla pertinenza che Amazon Kendra determina per ogni documento. I risultati sono suddivisi in pagine in modo da poter mostrare all'utente una pagina alla volta.

Per cercare i documenti con Amazon Kendra cui hai indicizzato, usa AMAZON. Amazon Lex KendraSearchIntent. Per un esempio di configurazione Amazon Kendra con Amazon Lex, consulta Creazione di un bot per le domande frequenti per un Amazon Kendra indice.

L'esempio seguente mostra come cercare un indice. Amazon Kendra determina il tipo di risultato della ricerca (risposta, documento, domanda-risposta) più adatto alla query. Non è possibile Amazon Kendra configurare la restituzione di un tipo specifico di risposta di ricerca (risposta, documento, domanda-risposta) a una query.

Per informazioni sulle risposte alle interrogazioni, vedere. Risposte alle interrogazioni e tipi di risposta

Prerequisiti

Prima di utilizzare l'API Query per interrogare un indice:

- Configura le autorizzazioni richieste per un indice e connettiti alla tua fonte di dati o carica in batch i tuoi documenti. Per ulteriori informazioni, consulta IAM ruoli. Utilizzi l'Amazon Resource Name del ruolo quando chiami l'API per creare un connettore di indicizzazione e origine dati o per caricare documenti in batch.
- Configura un SDK o accedi alla Amazon Kendra console. AWS Command Line Interface Per ulteriori informazioni, consulta la pagina Setting up Amazon Kendra.
- Crea un indice e connettiti a una fonte di dati di documenti o carica documenti in batch. Per ulteriori informazioni, vedere Creazione di un indice e Creazione di un connettore di origine dati.

Ricerca in un indice (console)

Puoi usare la Amazon Kendra console per cercare e testare il tuo indice. Puoi fare domande e vedere i risultati.

Per cercare un indice con la console

1. Accedi AWS Management Console e apri la Amazon Kendra console all'indirizzo http://console.aws.amazon.com/kendra/.
2. Nel riquadro di navigazione, scegli Indici.
3. Scegli il tuo indice.
4. Nel menu di navigazione, scegli l'opzione per cercare nell'indice.
5. Inserisci una query nella casella di testo, quindi premi invio.
6. Amazon Kendra restituisce i risultati della ricerca.

Puoi anche ottenere l'ID della query per la ricerca selezionando l'icona a forma di lampadina nel pannello laterale.

Ricerca in un indice (SDK)

Per cercare un indice con Python o Java

- L'esempio seguente esegue una ricerca in un indice. Modificate `query` il valore della query di ricerca `index_id` e/o `indexId` dell'identificatore dell'indice in cui desiderate cercare.

  Puoi anche ottenere l'ID della query per la ricerca come parte degli elementi di risposta quando chiami l'API Query.

  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");
        }
    }
}
```

Ricerca in un indice (Postman)

Puoi usare Postman per interrogare e testare il tuo Amazon Kendra indice.

Per cercare un indice usando Postman

1. Crea una nuova raccolta in Postman e imposta il tipo di richiesta su POST.
2. Inserisci l'URL dell'endpoint. Ad esempio, https://kendra. .amazonaws.com. <region>
3. Seleziona la scheda Autorizzazione e inserisci le seguenti informazioni.

   - Tipo: seleziona la AWS firma.
   - AccessKey—Inserisci la chiave di accesso generata quando crei un IAM utente.
   - SecretKey—Immettere la chiave segreta generata quando si crea un IAM utente.
   - AWS Regione: inserire la regione dell'indice. Ad esempio, us-west-2.
   - Nome servizio: inserisci kendra. Fa distinzione tra maiuscole e minuscole, quindi deve essere minuscola.

   > **Warning**
   >
   > Se inserisci il nome di servizio errato o non usi le lettere minuscole, viene generato un errore dopo aver selezionato Invia per inviare la richiesta: «La credenziale deve essere limitata al servizio corretto 'kendra'».
   > È inoltre necessario verificare di aver inserito la chiave di accesso e la chiave segreta corrette.

4. Seleziona la scheda Intestazioni e inserisci le seguenti informazioni sulla chiave e sul valore.

   - Chiave: X-Amz-Target

     Valore: com.amazonaws.kendra. AWSKendraFrontendService.Interrogazione
   - Chiave: codifica del contenuto

     Valore: amz-1.0

5. Selezionate la scheda Corpo ed effettuate le seguenti operazioni.

   - Scegliete il tipo JSON non elaborato per il corpo della richiesta.
   - Inserisci un codice JSON che includa l'ID dell'indice e il testo della query.

```
{
    "IndexId": "index-id",
    "QueryText": "enter a query here"
```

```
}
```

> **Warning**
>
> Se il tuo JSON non utilizza l'indendazione corretta, viene generato un errore: "». SerializationException Controlla l'indendazione nel tuo codice JSON.

6. Seleziona Invia (in alto a destra).

Ricerca con sintassi di interrogazione avanzata

È possibile creare interrogazioni più specifiche delle semplici query con parole chiave o in linguaggio naturale utilizzando la sintassi o gli operatori di query avanzati. Ciò include intervalli, valori booleani, caratteri jolly e altro ancora. Utilizzando gli operatori, è possibile contestualizzare la query e rifinire ulteriormente i risultati della ricerca.

Amazon Kendra supporta i seguenti operatori.

- Boolean: logica per limitare o ampliare la ricerca. Ad esempio, `amazon AND sports` limita la ricerca alla ricerca solo di documenti contenenti entrambi i termini.
- Parentesi: legge i termini di interrogazione annidati in ordine di precedenza. Ad esempio, legge prima. `(amazon AND sports) NOT rainforest` `(amazon AND sports)` `NOT rainforest`
- Intervalli: valori di date o intervalli numerici. Gli intervalli possono essere inclusivi, esclusivi o illimitati. Ad esempio, puoi cercare i documenti che sono stati aggiornati l'ultima volta tra il 1° gennaio 2020 e il 31 dicembre 2020, comprese queste date.
- Campi: utilizza un campo specifico per limitare la ricerca. Ad esempio, puoi cercare documenti con «Stati Uniti» nel campo «posizione».
- Carte jolly: corrispondono parzialmente a una stringa di testo. Ad esempio, `Cloud*` potrebbe corrispondere CloudFormation. Amazon Kendra attualmente supporta solo i caratteri jolly finali.
- Virgolette esatte: corrispondono esattamente a una stringa di testo. Ad esempio, documenti che contengono`"Amazon Kendra" "pricing"`.

È possibile utilizzare una combinazione di uno qualsiasi degli operatori precedenti.

Tieni presente che un uso eccessivo di operatori o query estremamente complesse potrebbero influire sulla latenza delle query. Le wildcard sono alcuni degli operatori più costosi in termini di

latenza. Una regola generale è che maggiore è il numero di termini e operatori utilizzati, maggiore è il potenziale impatto sulla latenza. Altri fattori che influiscono sulla latenza includono la dimensione media dei documenti indicizzati, la dimensione dell'indice, qualsiasi filtro sui risultati di ricerca e il carico complessivo dell'indice. Amazon Kendra

Booleano

È possibile combinare o escludere parole utilizzando gli operatori booleani,. `AND` `OR` `NOT`

Di seguito sono riportati alcuni esempi di utilizzo degli operatori booleani.

`amazon AND sports`

Restituisce risultati di ricerca che contengono sia i termini «amazon» che «sport» nel testo, come Amazon Prime video sport o altri contenuti simili.

`sports OR recreation`

Restituisce risultati di ricerca che contengono i termini «sport» o «ricreazione», o entrambi, nel testo.

`amazon NOT rainforest`

Restituisce risultati di ricerca che contengono il termine «amazon» ma non il termine «foresta pluviale» nel testo. Questo serve per cercare documenti sull'azienda Amazon, non sulla foresta pluviale amazzonica.

Parentesi

È possibile interrogare le parole annidate in ordine di precedenza utilizzando le parentesi. Le parentesi indicano come deve essere letta una query. Amazon Kendra

Di seguito sono riportati alcuni esempi di utilizzo degli operatori tra parentesi.

`(amazon AND sports) NOT rainforest`

Restituisce documenti che contengono sia i termini «amazon» che «sports» nel testo, ma non il termine «foresta pluviale». Questo serve per cercare video sportivi o altri contenuti simili su Amazon Prime, non sugli sport d'avventura nella foresta pluviale amazzonica. Le parentesi aiutano a indicare che `amazon AND sports` dovrebbe essere letto prima. `NOT rainforest` L'interrogazione non deve essere letta come. `amazon AND (sports NOT rainforest)`

`(amazon AND (sports OR recreation)) NOT rainforest`

Restituisce documenti che contengono i termini «sport» o «ricreazione», o entrambi, e il termine «amazon». Ma non include il termine «foresta pluviale». Questo è per cercare video sportivi o ricreativi su Amazon Prime, non per sport d'avventura nella foresta pluviale amazzonica. Le parentesi aiutano a indicare che `sports OR recreation` deve essere letto prima di combinarlo con «amazon», che viene letto prima. `NOT rainforest` La query non deve essere letta come. `amazon AND (sports OR (recreation NOT rainforest))`

Intervalli

È possibile utilizzare un intervallo di valori per filtrare i risultati della ricerca. È possibile specificare un attributo e i valori dell'intervallo. Può essere una data o un tipo numerico.

Gli intervalli di date devono avere i seguenti formati:

- Epoch
- YYYY
- yyyy-MM
- aaaa-mm-gg
- YYYY-MM-D'T'HH

È inoltre possibile specificare se includere o escludere i valori inferiori e superiori dell'intervallo.

Di seguito sono riportati alcuni esempi di utilizzo degli operatori di intervallo.

`_processed_date:>2019-12-31 AND _processed_date:<2021-01-01`

Restituisce i documenti elaborati nel 2020, ovvero dopo il 31 dicembre 2019 e inferiori al 1° gennaio 2021.

`_processed_date:>=2020-01-01 AND _processed_date:<=2020-12-31`

Restituisce i documenti che sono stati elaborati nel 2020, maggiori o uguali al 1° gennaio 2020 e inferiori o uguali al 31 dicembre 2020.

`_document_likes:<1`

Restituisce documenti con zero Mi piace o nessun feedback da parte degli utenti, ovvero con meno di 1 like.

È possibile specificare se un intervallo deve essere considerato inclusivo o escluso dei valori dell'intervallo specificato.

Inclusivo

`_last_updated_at:[2020-01-01 TO 2020-12-31]`

Restituisce i documenti aggiornati l'ultima volta nel 2020, inclusi i giorni 1° dicembre 2020 e 31 dicembre 2020.

Esclusivo

`_last_updated_at:{2019-12-31 TO 2021-01-01}`

Restituisce i documenti aggiornati l'ultima volta nel 2020, esclusi i giorni 31 dicembre 2019 e 1 gennaio 2021.

< and **>**Per intervalli illimitati che non sono né inclusivi né esclusivi, è sufficiente utilizzare gli operatori. Ad esempio, `_last_updated_at:>2019-12-31 AND _last_updated_at:<2021-01-01`

Campi

Puoi limitare la ricerca in modo da restituire solo i documenti che soddisfano un valore in un campo specifico. Il campo può essere di qualsiasi tipo.

Di seguito sono riportati alcuni esempi di utilizzo degli operatori di contesto a livello di campo.

`status:"Incomplete" AND financial_year:2021`

Restituisce i documenti per l'esercizio finanziario 2021 con lo stato incompleto.

`(sports OR recreation) AND country:"United States" AND level:"professional"`

Restituisce documenti che trattano di sport o attività ricreative professionistiche negli Stati Uniti.

Caratteri jolly

È possibile ampliare la ricerca per tenere conto delle varianti di parole e frasi utilizzando l'operatore wildcard. Ciò è utile per la ricerca di varianti di nome. Amazon Kendra attualmente supporta solo i caratteri jolly finali. Il numero di caratteri di prefisso per un jolly finale deve essere maggiore di due.

Di seguito sono riportati alcuni esempi di utilizzo degli operatori jolly.

`Cloud*`

Restituisce documenti che contengono varianti come CloudFormation e CloudWatch.

`kendra*aws`

Restituisce documenti che contengono varianti come kendra.amazonaws.

`kendra*aws*`

Restituisce documenti che contengono varianti come kendra.amazonaws.com

Citazioni esatte

È possibile utilizzare le virgolette per cercare una corrispondenza esatta di una parte di testo.

Di seguito sono riportati alcuni esempi di utilizzo delle virgolette.

`"Amazon Kendra" "pricing"`

Restituisce documenti che contengono sia la frase 'Amazon Kendra' che il termine 'prezzo'. I documenti devono contenere sia «Amazon Kendra» che «prezzi» per poter essere restituiti nei risultati.

`"Amazon Kendra" "pricing" cost`

Restituisce documenti che contengono sia la frase «Amazon Kendra» che il termine «prezzo» e, facoltativamente, il termine «costo». I documenti devono contenere sia «Amazon Kendra» che «prezzi» per poter restituire i risultati, ma potrebbero non includere necessariamente il termine «costo».

Sintassi di interrogazione non valida

Amazon Kendra emette un avviso se ci sono problemi con la sintassi della query o se la query non è attualmente supportata da. Amazon Kendra Per ulteriori informazioni, consulta la documentazione dell'API per gli avvisi sulle query.

Le seguenti query sono esempi di sintassi di query non valida.

`_last_updated_at:<2021-12-32`

Data non valida. Il giorno 32 non esiste nel calendario gregoriano, utilizzato da. Amazon Kendra

`_view_count:ten`

Valore numerico non valido. Le cifre devono essere utilizzate per rappresentare valori numerici.

`nonExistentField:123`

Ricerca nei campi non valida. Il campo deve esistere per poter utilizzare la ricerca nei campi.

`Product:[A TO D]`

Intervallo non valido. È necessario utilizzare valori numerici o date per gli intervalli.

`OR Hello`

Valore booleano non valido. Gli operatori devono essere utilizzati con termini e collocati tra i termini.

Ricerca in lingue

È possibile cercare documenti in una lingua supportata. Inserisci il codice della lingua AttributeFilterper restituire i documenti filtrati nella lingua scelta. È possibile digitare la query in una lingua supportata.

Se non si specifica una lingua, per impostazione predefinita Amazon Kendra interroga i documenti in inglese. Per ulteriori informazioni sulle lingue supportate, compresi i relativi codici, consulta Aggiungere documenti in lingue diverse dall'inglese.

Per cercare documenti in una lingua supportata nella console, seleziona l'indice, quindi seleziona l'opzione di ricerca nell'indice dal menu di navigazione. Scegli la lingua in cui desideri restituire i documenti selezionando le impostazioni di ricerca e quindi selezionando una lingua dal menu a discesa Lingua.

Gli esempi seguenti mostrano come cercare documenti in spagnolo.

Per cercare un indice in spagnolo nella console

1. Accedi AWS Management Console e apri la Amazon Kendra console all'indirizzo http://console.aws.amazon.com/kendra/.
2. Nel menu di navigazione, scegli Indici e scegli il tuo indice.
3. Nel menu di navigazione, scegli l'opzione per cercare nell'indice.

4. Nelle impostazioni di ricerca, seleziona il menu a discesa Lingue e scegli lo spagnolo.
5. Inserisci una query nella casella di testo, quindi premi invio.
6. Amazon Kendra restituisce i risultati della ricerca in spagnolo.

Per cercare un indice in spagnolo utilizzando CLI, Python o Java

- L'esempio seguente cerca un indice in spagnolo. Modificate `searchString` il valore della query di ricerca e `indexID` il valore con l'identificatore dell'indice che desiderate cercare. Il codice della lingua per lo spagnolo è`es`. Puoi sostituirlo con il tuo codice di lingua.

  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");
```

```
        }
    }
}
```

Recupero dei passaggi

È possibile utilizzare l'RetrieveAPI come retriever per i sistemi RAG (Retrieval Augmented Generation).

I sistemi RAG utilizzano l'intelligenza artificiale generativa per creare applicazioni di risposta a domande. I sistemi RAG sono costituiti da un retriever e da modelli linguistici di grandi dimensioni (LLM). A seguito di una richiesta, il retriever identifica le porzioni di testo più rilevanti da un corpus di documenti e le invia all'LLM per fornire la risposta più utile. Quindi, l'LLM analizza i blocchi o i passaggi di testo pertinenti e genera una risposta completa alla domanda.

L'`Retrieve`API esamina le porzioni di testo o gli estratti denominati passaggi e restituisce i passaggi principali più pertinenti alla query.

Come l'QueryAPI, anche l'API cerca le informazioni `Retrieve` pertinenti utilizzando la ricerca semantica. La ricerca semantica tiene conto del contesto della query di ricerca, oltre a tutte le informazioni disponibili dai documenti indicizzati. Tuttavia, per impostazione predefinita, l'`Query`API restituisce solo passaggi estratti contenenti un massimo di 100 parole chiave. Con l'`Retrieve`API, puoi recuperare passaggi più lunghi di un massimo di 200 parole chiave e fino a 100 passaggi semanticamente rilevanti. Questo non include le risposte a domande e risposte di tipo FAQ dal tuo indice. I passaggi sono estratti di testo che possono essere estratti semanticamente da più documenti e più parti dello stesso documento. Se in casi estremi i documenti non producono passaggi utilizzando l'`Retrieve`API, in alternativa è possibile utilizzare l'API e i `Query` relativi tipi di risposte.

Con l'`Retrieve`API puoi anche fare quanto segue:

- Sostituisci il potenziamento a livello di indice
- Filtra in base ai campi o agli attributi del documento
- Filtra in base all'accesso dell'utente o del relativo gruppo ai documenti
- Visualizza il bucket del punteggio di confidenza per un risultato di passaggio recuperato. Il bucket di confidenza fornisce una classificazione relativa che indica quanto Amazon Kendra è sicuro che la risposta sia pertinente alla query.

> **Note**
>
> I bucket con il punteggio di confidenza sono attualmente disponibili solo per l'inglese.

Puoi anche includere alcuni campi nella risposta che potrebbero fornire utili informazioni aggiuntive.

L'`Retrieve`API attualmente non supporta tutte le funzionalità supportate dall'`Query`API. Le seguenti funzionalità non sono supportate: esecuzione di query utilizzando la sintassi avanzata delle query, correzioni ortografiche suggerite per le query, faceting, suggerimenti di query per il completamento automatico delle query di ricerca e apprendimento incrementale. Tieni presente che non tutte le funzionalità si applicano all'API. `Retrieve` Eventuali versioni future dell'`Retrieve`API verranno documentate in questa guida.

L'`Retrieve`API condivide il numero di unità di capacità di interrogazione impostate per l'indice. Per ulteriori informazioni su cosa è incluso in una singola unità di capacità e sulla capacità di base predefinita per un indice, consulta Adattamento della capacità.

> **Note**
>
> Non è possibile aggiungere capacità se si utilizza la Amazon Kendra Developer Edition; è possibile aggiungere capacità solo quando si utilizza Amazon Kendra Enterprise Edition. Per ulteriori informazioni su ciò che è incluso nelle edizioni Developer ed Enterprise, consulta Amazon Kendra Edizioni.

Di seguito è riportato un esempio di utilizzo dell'`Retrieve`API per recuperare i 100 passaggi più importanti dei documenti in un indice per la query "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");
        }
    }
}
```

Navigazione in un indice

Puoi sfogliare i documenti in base ai loro attributi o sfaccettature senza dover digitare una query di ricerca. Amazon Kendra Index Browse può aiutare gli utenti a scoprire i documenti sfogliando liberamente un indice senza una domanda specifica in mente. Ciò consente inoltre agli utenti di sfogliare in generale un indice come punto di partenza per la ricerca.

Index Browse può essere utilizzato solo per la ricerca in base all'attributo o al facet del documento con un tipo di ordinamento. Non è possibile cercare in un intero indice utilizzando Index Browse. Se manca il testo della query, Amazon Kendra richiede un filtro o un facet per gli attributi del documento e un tipo di ordinamento.

Per consentire la navigazione nell'indice utilizzando l'API Query, devi includere AttributeFilteror Facet e. SortingConfiguration Per consentire la navigazione nell'indice nella console, seleziona l'indice in Indici nel menu di navigazione, quindi seleziona l'opzione per la ricerca nell'indice. Nella casella di ricerca, premi due volte il tasto Invio. Seleziona il menu a discesa Filtra i risultati della ricerca per scegliere un filtro e seleziona il menu a discesa Ordina per scegliere un tipo di ordinamento.

Di seguito è riportato un esempio di visualizzazione di un indice di documenti in lingua spagnolo in ordine decrescente della data di creazione del documento.

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");
        }
    }
}
```

Presenta i risultati della ricerca

Puoi inserire determinati documenti nei risultati di ricerca quando gli utenti inviano determinate domande. Questo aiuta a rendere i risultati più visibili e importanti per gli utenti. I risultati in evidenza sono separati dal consueto elenco di risultati e visualizzati nella parte superiore della pagina di ricerca. Puoi provare a inserire documenti diversi per domande diverse o assicurarti che determinati documenti ottengano la visibilità che meritano.

Puoi mappare domande specifiche su documenti specifici per includerle nei risultati. Se una query contiene una corrispondenza esatta, nei risultati della ricerca vengono visualizzati uno o più documenti specifici.

Ad esempio, puoi specificare che se gli utenti inviano la query «nuovi prodotti 2023», seleziona i documenti intitolati «Novità» e «Prossimamente» da visualizzare nella parte superiore della pagina

dei risultati di ricerca. Questo aiuta a garantire che questi documenti sui nuovi prodotti ottengano la visibilità che meritano.

Amazon Kendra non duplica i risultati di ricerca se un risultato è già selezionato per essere visualizzato nella parte superiore della pagina dei risultati di ricerca. Un risultato in evidenza non viene nuovamente classificato come primo risultato se è già presente al di sopra di tutti gli altri risultati.

Per visualizzare determinati risultati, è necessario specificare una corrispondenza esatta di una query di testo completo, non una corrispondenza parziale di una query che utilizza una parola chiave o una frase contenuta in una query. Ad esempio, se specifichi solo la query «Kendra» in un set di risultati in primo piano, query come «Come classifica semanticamente Kendra i risultati?» non visualizzerà i risultati in evidenza. I risultati in evidenza sono progettati per query specifiche, anziché per query di ambito troppo ampio. Amazon Kendra gestisce in modo naturale le query basate su parole chiave per classificare i documenti più utili nei risultati di ricerca, evitando un'eccessiva presentazione dei risultati basata su parole chiave semplici.

Se ci sono determinate query che gli utenti utilizzano frequentemente, puoi specificarle per visualizzare i risultati in evidenza. Ad esempio, se esamini le tue query principali utilizzando Amazon Kendra Analytics e trovi quelle specifiche, come «In che modo kendra classifica semanticamente i risultati?» e 'kendra semantic search', sono usati frequentemente, quindi queste domande potrebbero essere utili da specificare per mostrare il documento intitolato 'search 101'.Amazon Kendra

Amazon Kendra considera le interrogazioni relative ai risultati in evidenza senza distinzione tra maiuscole e minuscole. Amazon Kendra converte una query in lettere minuscole e sostituisce gli spazi vuoti finali con uno spazio singolo. Amazon Kendra corrisponde a tutti gli altri caratteri così come sono quando si specificano le query per i risultati in evidenza.

Crei una serie di risultati in primo piano che mappi a determinate query utilizzando l'CreateFeaturedResultsSetAPI. Se utilizzi la console, seleziona l'indice e quindi seleziona Risultati in evidenza nel menu di navigazione per creare un set di risultati in evidenza. È possibile creare fino a 50 set di risultati in evidenza per indice, fino a quattro documenti da inserire in evidenza per set e fino a 49 testi di query per set di risultati in evidenza. Puoi richiedere di aumentare questi limiti contattando il Supporto.

Puoi selezionare lo stesso documento tra più set di risultati in evidenza. Tuttavia, non è necessario utilizzare lo stesso testo della query con corrispondenza esatta su più set. Le query specificate per i risultati in evidenza devono essere uniche per ogni set di risultati in evidenza per ogni indice.

È possibile organizzare l'ordine dei documenti selezionando fino a quattro documenti in evidenza. Se utilizzi l'API, l'ordine in cui elenchi i documenti in evidenza è lo stesso visualizzato nei risultati in evidenza. Se usi la console, puoi semplicemente trascinare l'ordine dei documenti quando selezioni i documenti da inserire nei risultati.

Il controllo degli accessi, in base al quale determinati utenti e gruppi hanno accesso a determinati documenti e altri no, viene comunque rispettato quando si configurano i risultati in evidenza. Questo vale anche per il filtraggio del contesto utente. Ad esempio, l'utente A appartiene al gruppo aziendale «Stagisti», che non dovrebbe accedere ai documenti sui segreti aziendali. Se l'utente A inserisce una query che include un documento segreto aziendale, l'utente A non vede questo documento tra i risultati. Questo vale anche per tutti gli altri risultati nella pagina dei risultati di ricerca. Puoi anche utilizzare i tag per controllare l'accesso a un set di risultati in evidenza, che è una Amazon Kendra risorsa per la quale controlli l'accesso.

Di seguito è riportato un esempio di creazione di una serie di risultati in evidenza con le query «nuovi prodotti 2023", «nuovi prodotti disponibili» mappate ai documenti intitolati «Novità» (doc-id-1) e «Prossimamente» (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.")
```

Ricerca tabulare per HTML

Amazon Kendra la funzione di ricerca tabulare può cercare ed estrarre risposte da tabelle incorporate nei documenti HTML. Quando esegui una ricerca nell'indice, Amazon Kendra include un estratto da una tabella se è pertinente alla query e fornisce informazioni utili.

Amazon Kendra esamina tutte le informazioni contenute nel corpo del testo di un documento, incluse le informazioni utili nelle tabelle. Ad esempio, un indice contiene report aziendali con tabelle su costi

operativi, ricavi e altre informazioni finanziarie. Per la domanda, «qual è il costo operativo annuo dal 2020 al 2022?» , Amazon Kendra può restituire un estratto da una tabella che contiene le colonne pertinenti della tabella «Operazioni (milioni di USD)» e «Esercizio finanziario» e le righe della tabella contenenti i valori di reddito per il 2020, 2021 e 2022. L'estratto della tabella è incluso nel risultato, insieme al titolo del documento, a un collegamento al documento completo e a qualsiasi altro campo del documento che scegli di includere.

Gli estratti delle tabelle possono essere visualizzati nei risultati della ricerca indipendentemente dal fatto che le informazioni si trovino in una cella di una tabella o in più celle. Ad esempio, Amazon Kendra può visualizzare un estratto di tabella personalizzato per ciascuno di questi tipi di interrogazioni:

- «carta di credito con il tasso di interesse più alto del 2020"
- «carta di credito con il tasso di interesse più elevato del periodo 2020-2022"
- «le 3 carte di credito con il tasso di interesse più elevato nel 2020-2022"
- «carte di credito con tassi di interesse inferiori al 10%»
- «tutte le carte di credito a basso interesse disponibili»

Amazon Kendra evidenzia la cella o le celle della tabella più pertinenti alla query. Le celle più pertinenti con le righe, le colonne e i nomi di colonna corrispondenti vengono visualizzate nei risultati della ricerca. L'estratto della tabella mostra fino a cinque colonne e tre righe, a seconda del numero di celle della tabella pertinenti alla query e del numero di colonne disponibili nella tabella originale. La prima cella più rilevante viene visualizzata nell'estratto della tabella, insieme alle celle successive più pertinenti.

La risposta include il bucket di confidenza (`MEDIUM`,`HIGH`,`VERY_HIGH`) per mostrare la pertinenza della risposta della tabella rispetto alla query. Se il valore di una cella della tabella è `VERY_HIGH` riservato, diventa la «risposta principale» e viene evidenziato. Se i valori delle celle della tabella sono `HIGH` riservati, vengono evidenziati. Se i valori delle celle della tabella sono `MEDIUM` riservati, non vengono evidenziati. La confidenza complessiva per la risposta della tabella viene restituita nella risposta. Ad esempio, se una tabella contiene principalmente celle di tabella con `HIGH` confidenza, la fiducia complessiva restituita nella risposta alla tabella è la `HIGH` fiducia.

Per impostazione predefinita, alle tabelle non viene assegnato un livello di importanza o un peso maggiore rispetto agli altri componenti di un documento. All'interno di un documento, se una tabella è solo leggermente rilevante per una query, ma contiene un paragrafo molto pertinente, Amazon Kendra restituisce un estratto del paragrafo. I risultati della ricerca mostrano il contenuto che fornisce

la migliore risposta possibile e le informazioni più utili, nello stesso documento o in altri documenti. Se la confidenza per una tabella scende al di sotto della `MEDIUM` confidenza, l'estratto della tabella non viene restituito nella risposta.

Per utilizzare la ricerca tabulare su un indice esistente, è necessario reindicizzare i contenuti.

Amazon Kendra la ricerca tabulare supporta i sinonimi (inclusi i sinonimi personalizzati). Amazon Kendra supporta solo documenti in inglese con tabelle HTML che si trovano all'interno del tag table.

L'esempio seguente mostra l'estratto della tabella incluso nel risultato della query. Per visualizzare un JSON di esempio con risposte alle query, inclusi estratti di tabella, vedi Risposte e tipi di query.

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");
        }
    }
}
```

Suggerimenti per le interrogazioni

Amazon Kendra I suggerimenti sulle query possono aiutare gli utenti a digitare le query di ricerca più velocemente e guidare la ricerca.

Amazon Kendra suggerisce domande pertinenti per gli utenti in base a una delle seguenti opzioni:

- Query più comuni nella cronologia delle query o nel registro delle query
- Il contenuto dei campi/attributi del documento

È possibile impostare la preferenza per l'utilizzo della cronologia delle interrogazioni o dei campi del documento impostando `QUERY` o `SuggestionTypes` `DOCUMENT_ATTRIBUTES` e chiamando. GetQuerySuggestions Per impostazione predefinita, Amazon Kendra utilizza la cronologia delle interrogazioni su cui basare i suggerimenti. Se la cronologia delle interrogazioni e i campi del documento sono entrambi attivati quando si chiama UpdateQuerySuggestionsConfige non è stata impostata la `SuggestionTypes` preferenza per l'utilizzo dei campi del documento, Amazon Kendra utilizza la cronologia delle query.

Se si utilizza la console, è possibile basare i suggerimenti sulle interrogazioni sulla cronologia delle query o sui campi del documento. Seleziona prima l'indice, quindi seleziona Suggerimenti di interrogazione in Arricchimenti nel menu di navigazione. Quindi seleziona Configura i suggerimenti di interrogazione. Dopo aver configurato i suggerimenti per le query, verrai indirizzato a una console di ricerca in cui puoi selezionare i campi Cronologia delle query o Documento nel pannello di destra e inserire una query di ricerca nella barra di ricerca.

Per impostazione predefinita, i suggerimenti di interrogazione che utilizzano i campi Cronologia delle interrogazioni e documento vengono entrambi attivati senza costi aggiuntivi. È possibile disattivare questi tipi di suggerimenti di interrogazione in qualsiasi momento utilizzando l'`UpdateQuerySuggestionsConfig`API. Per disattivare i suggerimenti di interrogazione in base alla cronologia delle query, imposta su `DISABLED` Quando `Mode` si chiama. `UpdateQuerySuggestionsConfig` Per disattivare i suggerimenti di interrogazione basati sui campi del documento, `AttributeSuggestionsMode` impostalo `INACTIVE` nella configurazione dei campi del documento e poi chiama. `UpdateQuerySuggestionsConfig>` Se utilizzi la console, puoi disattivare i suggerimenti di interrogazione nelle impostazioni dei suggerimenti di interrogazione.

I suggerimenti di interrogazione non fanno distinzione tra maiuscole e min Amazon Kendra converte il prefisso della query e la query suggerita in lettere minuscole, ignora tutte le virgolette singole e doppie e sostituisce più caratteri di spazio bianco con uno spazio singolo. Amazon Kendra corrisponde a tutti gli altri caratteri speciali così come sono. Amazon Kendra non mostra alcun suggerimento se un utente digita meno di due caratteri o più di 60 caratteri.

Argomenti

- Suggerimenti di interrogazione utilizzando la cronologia delle query

- Suggerimenti di interrogazione utilizzando i campi del documento
- Blocca i suggerimenti relativi a determinate domande o al contenuto dei campi del documento

Suggerimenti di interrogazione utilizzando la cronologia delle query

Argomenti

- Impostazioni per la selezione delle interrogazioni per i suggerimenti
- Suggerimenti chiari conservando la cronologia delle interrogazioni
- Nessun suggerimento disponibile

Puoi scegliere di suggerire query pertinenti agli utenti in base alle query più frequenti nella cronologia delle query o nel registro delle query. Amazon Kendra utilizza tutte le query che gli utenti cercano e impara da queste query per fornire suggerimenti agli utenti. Amazon Kendra suggerisce le query più frequenti agli utenti quando iniziano a digitare la query. Amazon Kendra suggerisce una query se il prefisso o i primi caratteri della query corrispondono a quelli che l'utente inizia a digitare come query.

Ad esempio, un utente inizia a digitare la query «eventi imminenti». Amazon Kendra ha appreso dalla cronologia delle query che molti utenti hanno cercato «eventi imminenti 2050" molte volte. L'utente vede «Eventi imminenti 2050" apparire direttamente sotto la barra di ricerca, completando automaticamente la query di ricerca. L'utente seleziona questo suggerimento di interrogazione e il documento «Nuovi eventi: cosa succede nel 2050» viene restituito nei risultati della ricerca.

Puoi specificare in che modo Amazon Kendra seleziona le query idonee da suggerire ai tuoi utenti. Ad esempio, puoi specificare che un suggerimento di query deve essere stato cercato da almeno 10 utenti unici (il valore predefinito è tre), deve essere stato cercato negli ultimi 30 giorni e non contiene parole o frasi dall'elenco di blocco. Amazon Kendra richiede che una query abbia almeno un risultato di ricerca e contenga almeno una parola di più di quattro caratteri.

Impostazioni per la selezione delle interrogazioni per i suggerimenti

È possibile configurare le seguenti impostazioni per la selezione delle query per i suggerimenti utilizzando l'UpdateQuerySuggestionsConfigAPI:

- Modalità: i suggerimenti di interrogazione che utilizzano la cronologia delle query sono o`ENABLED`. `LEARN_ONLY` Amazon Kendra attiva i suggerimenti di interrogazione per impostazione predefinita. `LEARN_ONLY`disattiva i suggerimenti di interrogazione. Se disattivata, Amazon Kendra continua a ricevere suggerimenti ma non fornisce suggerimenti di query agli utenti.

- Finestra temporale del registro delle query: quanto sono recenti le query nella finestra temporale del registro delle query. La finestra temporale è un valore intero per il numero di giorni dal giorno corrente ai giorni passati.
- Interrogazioni senza informazioni sull'utente: impostata TRUE per includere tutte le interrogazioni o impostata FALSE per includere solo le interrogazioni con informazioni sull'utente. È possibile utilizzare questa impostazione se l'applicazione di ricerca include informazioni sull'utente, ad esempio l'ID utente, quando un utente invia una query. Per impostazione predefinita, questa impostazione non filtra le interrogazioni se a esse non sono associate informazioni utente specifiche. Tuttavia, puoi utilizzare questa impostazione per fornire solo suggerimenti basati su query che includono informazioni sull'utente.
- Utenti unici: il numero minimo di utenti unici che devono cercare una query per poter essere suggeriti ai tuoi utenti. Questo numero è un valore intero.
- Numero di query: il numero minimo di volte in cui è necessario eseguire una ricerca affinché la query sia idonea a essere suggerita agli utenti. Questo numero è un valore intero.

Queste impostazioni influiscono sul modo in cui le query vengono selezionate come query popolari da suggerire agli utenti. Il modo in cui regolerai le impostazioni dipenderà dalle tue esigenze specifiche, ad esempio:

- Se gli utenti di solito effettuano ricerche in media una volta al mese, puoi impostare il numero di giorni nella finestra temporale del registro delle query su 30 giorni. Utilizzando questa impostazione, acquisisci la maggior parte delle query recenti degli utenti prima che diventino obsolete nella finestra temporale.
- Se solo un numero limitato di query include informazioni sugli utenti e non desideri suggerire query basate su un campione di dimensioni ridotte, puoi impostare le query in modo da includere tutti gli utenti.
- Se definisci le query popolari come ricerche effettuate da almeno 10 utenti unici e almeno 100 volte, imposti gli utenti unici su 10 e il conteggio delle query su 100.

> **Warning**
>
> Le modifiche alle impostazioni potrebbero non avere effetto immediato. Puoi tenere traccia delle modifiche alle impostazioni utilizzando l'DescribeQuerySuggestionsConfigAPI. La data di entrata in vigore delle impostazioni aggiornate dipende dagli aggiornamenti apportati e dal numero di query di ricerca nell'indice. Amazon Kendra aggiorna automaticamente i

suggerimenti ogni 24 ore, dopo aver modificato un'impostazione o dopo aver applicato un elenco di blocco.

CLI

Per recuperare i suggerimenti relativi alle interrogazioni

```
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
```

Per aggiornare i suggerimenti di interrogazione

Ad esempio, per modificare la finestra temporale del registro delle query e il numero minimo di volte in cui una query deve essere cercata:

```
aws kendra update-query-suggestions-config \
 --index-id index-id \
 --query-log-look-back-window-in-days 30 \
 --minimum-query-count 100
```

Python

Per recuperare i suggerimenti relativi alle interrogazioni

```
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.")
```

Per aggiornare i suggerimenti di interrogazione

Ad esempio, per modificare la finestra temporale del registro delle query e il numero minimo di volte in cui una query deve essere cercata:

```
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.")
```

Suggerimenti chiari conservando la cronologia delle interrogazioni

Puoi cancellare i suggerimenti di interrogazione utilizzando l'ClearQuerySuggestionsAPI. La cancellazione dei suggerimenti elimina solo i suggerimenti di interrogazione esistenti, non le query presenti nella cronologia delle query. Quando si eliminano i suggerimenti, Amazon Kendra ne apprende di nuovi in base alle nuove interrogazioni aggiunte al registro delle query dal momento in cui sono stati eliminati i suggerimenti.

CLI

Per cancellare i suggerimenti relativi alle interrogazioni

```
aws  kendra clear-query-suggestions \
 --index-id index-id
```

Python

Per cancellare i suggerimenti relativi alle interrogazioni

```
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.")
```

Nessun suggerimento disponibile

Se non vedi suggerimenti per una query, potrebbe essere per uno dei seguenti motivi:

- Nel tuo indice non ci sono abbastanza domande da Amazon Kendra cui imparare.

- Le impostazioni dei suggerimenti di interrogazione sono troppo rigide, di conseguenza la maggior parte delle query viene filtrata dai suggerimenti.
- Hai recentemente cancellato i suggerimenti e hai Amazon Kendra ancora bisogno di tempo per accumulare nuove domande per apprendere nuovi suggerimenti.

Puoi controllare le tue impostazioni correnti utilizzando l'API. DescribeQuerySuggestionsConfig

Suggerimenti di interrogazione utilizzando i campi del documento

Argomenti

- Impostazioni per la selezione dei campi per i suggerimenti
- Controllo utente nei campi del documento

Puoi scegliere di suggerire domande pertinenti ai tuoi utenti in base al contenuto dei campi del documento. Invece di utilizzare la cronologia delle interrogazioni per suggerire altre query pertinenti più comuni, è possibile utilizzare le informazioni contenute in un campo del documento utili per il completamento automatico della query. Amazon Kendra cerca il contenuto pertinente nei campi impostati su `Suggestable` e che siano strettamente allineati alla query dell'utente. Quindi, Amazon Kendra suggerisce questo contenuto all'utente quando inizia a digitare la query.

Ad esempio, se specifichi il campo del titolo su cui basare i suggerimenti e un utente inizia a digitare la query «How amazon ken... ', si potrebbe suggerire il titolo più pertinente 'How Amazon Kendra works' per completare automaticamente la ricerca. L'utente vede «Come Amazon Kendra funziona» apparire direttamente sotto la barra di ricerca, che completa automaticamente la query di ricerca. L'utente seleziona questo suggerimento di interrogazione e il documento «How Amazon Kendra works» viene restituito nei risultati della ricerca.

È possibile utilizzare il contenuto di qualsiasi campo `String` e `StringList` tipo di documento per suggerire una query impostando il campo `Suggestable` come parte della configurazione dei campi per i suggerimenti di interrogazione. Puoi anche utilizzare un elenco di blocco in modo che i campi di documento suggeriti che contengono determinate parole o frasi non vengano mostrati agli utenti. Puoi usare un solo elenco di blocchi. L'elenco dei blocchi si applica sia che si impostino suggerimenti di interrogazione per utilizzare la cronologia delle interrogazioni o i campi del documento.

Impostazioni per la selezione dei campi per i suggerimenti

È possibile configurare le seguenti impostazioni per selezionare i campi del documento per i suggerimenti utilizzando AttributeSuggestionsConfige richiamando l'UpdateQuerySuggestionsConfigAPI per aggiornare le impostazioni a livello di indice:

- Modalità di suggerimento di campi/attributi: i suggerimenti di interrogazione che utilizzano i campi del documento sono o. `ACTIVE` `INACTIVE` Amazon Kendra attiva i suggerimenti di interrogazione per impostazione predefinita.
- Campi/attributi suggestionabili: i nomi dei campi o le chiavi di campo su cui basare i suggerimenti. Questi campi devono essere impostati su `TRUE` for`Suggestable`, come parte della configurazione dei campi. È possibile sovrascrivere la configurazione dei campi a livello di query mantenendo la configurazione a livello di indice. Utilizza l'GetQuerySuggestionsAPI per modificare `AttributeSuggestionConfig` a livello di query. Questa configurazione a livello di query può essere utile per sperimentare rapidamente l'utilizzo di diversi campi del documento senza dover aggiornare la configurazione a livello di indice.
- Campi/attributi aggiuntivi: i campi aggiuntivi che si desidera includere nella risposta a un suggerimento di query. Questi campi vengono utilizzati per fornire informazioni aggiuntive nella risposta; tuttavia, non vengono utilizzati per basare suggerimenti.

> **Warning**
>
> Le modifiche alle impostazioni potrebbero non avere effetto immediato. Puoi tenere traccia delle modifiche alle impostazioni utilizzando l'DescribeQuerySuggestionsConfigAPI. La data di entrata in vigore delle impostazioni aggiornate dipende dagli aggiornamenti che apporti. Amazon Kendra aggiorna automaticamente i suggerimenti ogni 24 ore, dopo aver modificato un'impostazione o dopo aver applicato un elenco di blocco.

CLI

Per recuperare i suggerimenti di interrogazione e sovrascrivere la configurazione dei campi del documento a livello di query anziché dover modificare la configurazione a livello di indice.

```
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
```

Per aggiornare i suggerimenti di interrogazione

Ad esempio, per modificare la configurazione dei campi del documento a livello di indice:

```
aws kendra update-query-suggestions-config \
 --index-id index-id \
 --attribute-suggestions-config '{"SuggestableConfigList": '[{"SuggestableConfig":
 "_document_title", "Suggestable": true}]', "AttributeSuggestionsMode": "ACTIVE"}'
```

Python

Per recuperare i suggerimenti di interrogazione e sovrascrivere la configurazione dei campi del documento a livello di query invece di dover modificare la configurazione a livello di indice.

```
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.")
```

Per aggiornare i suggerimenti di interrogazione

Ad esempio, per modificare la configurazione dei campi del documento a livello di indice:

```
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.")
```

Controllo utente nei campi del documento

È possibile applicare il filtro del contesto utente ai campi del documento su cui si desidera basare i suggerimenti di interrogazione. Questo filtra le informazioni sui campi del documento in base all'accesso dell'utente o del relativo gruppo ai documenti. Ad esempio, uno stagista effettua una ricerca nel portale aziendale e non ha accesso a un documento aziendale top secret. Pertanto, le domande suggerite in base al titolo del documento top secret o a qualsiasi altro campo suggestionabile non vengono mostrate allo stagista.

È possibile indicizzare i documenti con un elenco di controllo degli accessi (ACL), che definisce a quali utenti e gruppi è assegnato l'accesso a quali documenti. Quindi, puoi applicare il filtro del contesto utente ai campi dei documenti per suggerimenti di interrogazione. Il filtro del contesto utente attualmente impostato per l'indice è lo stesso filtro del contesto utente applicato alla configurazione dei campi del documento per i suggerimenti di query. Il filtraggio del

contesto utente fa parte della configurazione dei campi del documento. Si utilizza la chiamata AttributeSuggestionsGetConfigGetQuerySuggestionsand.

Blocca i suggerimenti relativi a determinate domande o al contenuto dei campi del documento

Un elenco di blocco Amazon Kendra impedisce di suggerire determinate domande agli utenti. Un elenco di blocco è un elenco di parole o frasi che desideri escludere dai suggerimenti di interrogazione. Amazon Kendra esclude le interrogazioni che contengono una corrispondenza esatta delle parole o delle frasi nell'elenco di blocco.

È possibile utilizzare un elenco di blocco per proteggersi da parole o frasi offensive che compaiono comunemente nella cronologia delle query o nei campi del documento e che Amazon Kendra potrebbero essere selezionate come suggerimenti. Un elenco di blocco può anche Amazon Kendra impedire di suggerire domande che contengono informazioni che non sono pronte per essere rilasciate o annunciate pubblicamente. Ad esempio, gli utenti fanno spesso domande sulla prossima release di un potenziale nuovo prodotto. Tuttavia, non vuoi suggerire il prodotto perché non sei pronto a rilasciarlo. Puoi bloccare i suggerimenti per le domande che contengono il nome e le informazioni sul prodotto.

Puoi creare un elenco di blocco per le query utilizzando l'API. CreateQuerySuggestionsBlockList Metti ogni parola o frase in blocco su una riga separata in un file di testo. Quindi carichi il file di testo nel tuo bucket Amazon S3 e fornisci il percorso o la posizione del file in cui si trova. Amazon S3 Amazon Kendra attualmente supporta la creazione di un solo elenco di blocchi.

Puoi sostituire il file di testo delle parole e delle frasi bloccate nel tuo Amazon S3 bucket. Per aggiornare l'elenco dei blocchi in Amazon Kendra, usa l'UpdateQuerySuggestionsBlockListAPI.

Usa l'DescribeQuerySuggestionsBlockListAPI per conoscere lo stato della tua lista di blocco. `DescribeQuerySuggestionsBlockList`può fornirti anche altre informazioni utili, come le seguenti:

- Data dell'ultimo aggiornamento della lista di blocco
- Quante parole o frasi ci sono nella tua lista di blocco attuale
- Messaggi di errore utili durante la creazione di un elenco di blocchi

Puoi anche utilizzare l'ListQuerySuggestionsBlockListsAPI per ottenere un elenco di riepiloghi degli elenchi di blocchi per un indice.

Per eliminare la lista dei blocchi, usa l'DeleteQuerySuggestionsBlockListAPI.

Gli aggiornamenti alla lista di blocco potrebbero non avere effetto immediato. Puoi tenere traccia degli aggiornamenti utilizzando l'`DescribeQuerySuggestionsBlockList`API.

CLI

Per creare un elenco di blocchi

```
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
```

Per aggiornare un elenco di indirizzi bloccati

```
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
```

Per eliminare un elenco di indirizzi bloccati

```
aws kendra delete-query-suggestions-block-list \
 --index-id index-id \
 --id block-list-id
```

Python

Per creare una lista di blocco

```
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.")
```

Per aggiornare un elenco di indirizzi bloccati

```
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.")
```

Per eliminare un elenco di indirizzi bloccati

```
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.")
```

Interroga il correttore ortografico

Amazon Kendra Il correttore ortografico suggerisce correzioni ortografiche per una query. Questo può aiutarti a ridurre al minimo le occorrenze di zero risultati di ricerca e a restituire risultati pertinenti. I tuoi utenti potrebbero non ricevere risultati di ricerca a causa di query con errori di ortografia senza risultati corrispondenti o senza documenti restituiti. In alternativa, i tuoi utenti potrebbero ricevere risultati di ricerca non pertinenti a causa di query con errori di ortografia.

Il correttore ortografico è progettato per suggerire correzioni per le parole con errori di ortografia in base alle parole che compaiono nei documenti indicizzati e al grado di corrispondenza tra una parola corretta e una parola con errori di ortografia. Ad esempio, se la parola «rendiconti» appare nei documenti indicizzati, potrebbe corrispondere molto alla parola errata «rendiconti» nella query «rendiconti finanziari di fine anno».

Il correttore ortografico restituisce le parole desiderate o corrette che sostituiscono le parole con errori ortografici nel testo della query originale. Ad esempio, 'depoying kendre search' potrebbe restituire 'deploying Kendra search'. Puoi anche utilizzare le posizioni offset fornite nell'API per evidenziare o mettere in corsivo le parole corrette restituite in una query nella tua applicazione front-end. Nella console, le parole corrette sono evidenziate o in corsivo per impostazione predefinita. Ad esempio, «implementazione di Kendra search».

Per quanto riguarda i termini aziendali o specialistici che compaiono nei documenti indicizzati, il correttore ortografico non li interpreta erroneamente come errori di ortografia nella query. Ad esempio, 'amazon macie' non è corretto in 'amazon mace'.

Per le parole sillabate, come «fine anno», il correttore ortografico le considera come parole singole per suggerire correzioni per tali parole. Ad esempio, la correzione suggerita per «fine anno» potrebbe essere «fine anno».

Per `DOCUMENT` i tipi di risposta alle `QUESTION_ANSWER` interrogazioni, il correttore ortografico suggerisce correzioni alle parole con errori di ortografia in base alle parole presenti nel corpo del documento. Il corpo del documento è più affidabile del titolo per suggerire correzioni che si avvicinano molto alle parole con errori di ortografia. Per i tipi di risposta alle `ANSWER` interrogazioni, il correttore

ortografico suggerisce correzioni in base alle parole presenti nel documento di domande e risposte predefinito dell'indice.

È possibile attivare il correttore ortografico utilizzando l'oggetto. SpellCorrectionConfiguration Sei impostato su`IncludeQuerySpellCheckSuggestions`. `TRUE` Il correttore ortografico è attivato per impostazione predefinita nella console. Per impostazione predefinita, è integrato nella console.

Spell Checker può anche suggerire correzioni ortografiche per le query in più lingue, non solo in inglese. Per un elenco delle lingue supportate per il correttore ortografico, vedi lingue supportate.Amazon Kendra

Utilizzo del correttore ortografico delle query con limiti predefiniti

Il correttore ortografico è progettato con determinati valori o limiti predefiniti. Di seguito è riportato un elenco dei limiti correnti che si applicano quando si attivano i suggerimenti di correzione ortografica.

- Le correzioni ortografiche suggerite non possono essere restituite per parole con meno di tre caratteri o più di 30 caratteri di lunghezza. Per consentire più di 30 caratteri o meno di tre caratteri, contatta l'assistenza.
- Le correzioni ortografiche suggerite non possono limitare i suggerimenti basati sul controllo dell'accesso utente o sull'elenco di controllo degli accessi per il filtraggio del contesto utente. Le correzioni ortografiche si basano su tutte le parole presenti nei documenti indicizzati, indipendentemente dal fatto che le parole siano riservate a determinati utenti o meno. Se vuoi evitare che alcune parole compaiano nelle correzioni ortografiche suggerite per le query, non attivarle. `SpellCorrectionConfiguration`
- Le correzioni ortografiche suggerite non possono essere restituite per le parole che includono numeri. Ad esempio, 'how 2 not br8k ubun2'.
- Le correzioni ortografiche suggerite non possono utilizzare parole che non compaiono nei documenti indicizzati.
- Le correzioni ortografiche consigliate non possono utilizzare parole con una frequenza inferiore allo 0,01% nei documenti indicizzati. Per modificare la soglia dello 0,01%, contatta l'assistenza.

Filtraggio e ricerca sfaccettata

Puoi migliorare i risultati della ricerca o la risposta dall'API Query utilizzando i filtri. I filtri limitano i documenti nella risposta a quelli che si applicano direttamente alla query. Per creare suggerimenti di ricerca sfaccettati, utilizza la logica booleana per filtrare gli attributi specifici del documento dalla

risposta o i documenti che non corrispondono a criteri specifici. Puoi specificare le sfaccettature utilizzando il `Facets` parametro nell'API. `Query`

Per cercare i documenti con cui hai indicizzato Amazon Lex, usa Amazon Kendra AMAZON.KendraSearchIntent. Per un esempio di configurazione Amazon Kendra con Amazon Lex, consulta Creazione di un bot per le domande frequenti per un Amazon Kendra indice. Puoi anche fornire un filtro per la risposta utilizzando AttributeFilter. Questo è il filtro di interrogazione in JSON durante la configurazione`AMAZON.KendraSearchIntent`. Per fornire un filtro per gli attributi durante la configurazione di un intento di ricerca nella console, vai all'editor degli intenti e scegli Amazon Kendra query per fornire un filtro di query in JSON. Per ulteriori informazioni in merito`AMAZON.KendraSearchIntent`, consulta la guida alla documentazione.Amazon Lex

Facet

I facet sono visualizzazioni mirate di un insieme di risultati di ricerca. Ad esempio, puoi fornire risultati di ricerca per città di tutto il mondo, dove i documenti vengono filtrati in base a una città specifica a cui sono associati. In alternativa, puoi creare sfaccettature per visualizzare i risultati di un autore specifico.

Puoi utilizzare un attributo del documento o un campo di metadati associato a un documento come sfaccettato in modo che gli utenti possano effettuare ricerche per categorie o valori all'interno di quel facet. È inoltre possibile visualizzare i facet annidati nei risultati di ricerca in modo che gli utenti possano eseguire la ricerca non solo in base a una categoria o a un campo, ma anche in base a una sottocategoria o sottocampo.

L'esempio seguente mostra come ottenere informazioni sui facet per l'attributo personalizzato «City».

```
response=kendra.query(
        QueryText = query,
        IndexId = index,
        Facets = [
            {
                "DocumentAttributeKey" : "City"
            }
        ]
        )
```

È possibile utilizzare sfaccettature annidate per restringere ulteriormente la ricerca. Ad esempio, l'attributo o sfaccettatura del documento «Città» include un valore chiamato «Seattle». Inoltre, l'attributo o sfaccettatura del documento "CityRegion" include i valori «Nord» e «Sud» per i documenti

assegnati a «Seattle». È possibile visualizzare le sfaccettature annidate con i relativi conteggi nei risultati di ricerca in modo che i documenti possano essere cercati non solo per città ma anche per regione all'interno di una città.

Tieni presente che i facet annidati potrebbero influire sulla latenza delle query. Una regola generale è che maggiore è il numero di facet annidati utilizzati, maggiore è il potenziale impatto sulla latenza. Altri fattori che influiscono sulla latenza includono la dimensione media dei documenti indicizzati, la dimensione dell'indice, le query estremamente complesse e il carico complessivo sull'indice. Amazon Kendra

L'esempio seguente mostra come ottenere informazioni sui facet per l'attributo personalizzato "CityRegion", come facet annidato all'interno di «City».

```
response=kendra.query(
        QueryText = query,
        IndexId = index,
        Facets = [
            {
                "DocumentAttributeKey" : "City",
                "Facets": [
                    {
                        "DocumentAttributeKey" : "CityRegion"
                    }
                ]
            }
        ]
        )
```

Le informazioni sulle sfaccettature, come il conteggio dei documenti, vengono restituite nell'array di risposta. `FacetResults` I contenuti vengono utilizzati per visualizzare suggerimenti di ricerca sfaccettati nell'applicazione. Ad esempio, se l'attributo del documento «Città» contiene la città a cui può essere applicata una ricerca, utilizzate tali informazioni per visualizzare un elenco di ricerche relative alle città. Gli utenti possono scegliere una città per filtrare i risultati della ricerca. Per effettuare la ricerca sfaccettata, chiama l'API Query e utilizza l'attributo del documento scelto per filtrare i risultati.

È possibile visualizzare fino a 10 valori di sfaccettatura per sfaccettatura per una query e solo una sfaccettatura annidata all'interno di una sfaccettatura. Se desideri aumentare questi limiti, contatta l'assistenza. Se desiderate limitare il numero di valori di sfaccettatura per sfaccettatura a meno di 10, potete specificarlo nell'`Facet`oggetto.

Il seguente esempio di risposta JSON mostra le sfaccettature che rientrano nell'ambito dell'attributo del documento «City». La risposta include il numero di documenti per il valore del facet.

```
{
    'FacetResults': [
        {
            'DocumentAttributeKey': 'City',
            'DocumentAttributeValueCountPairs': [
                {
                    'Count': 3,
                    'DocumentAttributeValue': {
                        'StringValue': 'Dubai'
                    }
                },
                {
                    'Count': 3,
                    'DocumentAttributeValue': {
                        'StringValue': 'Seattle'
                    }
                },
                {
                    'Count': 1,
                    'DocumentAttributeValue': {
                        'StringValue': 'Paris'
                    }
                }
            ]
        }
    ]
```

Puoi anche visualizzare le informazioni sulle sfaccettature relative a una sfaccettatura annidata, ad esempio una regione all'interno di una città, per filtrare ulteriormente i risultati della ricerca.

Il seguente esempio di risposta JSON mostra le sfaccettature appartenenti all'attributo "CityRegion" del documento, come sfaccettature annidate all'interno di «Città». La risposta include il conteggio dei documenti per i valori dei facet annidati.

```
{
    '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'
                                    }
                                }
                            ]
                        }
                    ]
                }
            }
        ]
}
```

Quando utilizzate un campo con un elenco di stringhe per creare facet, i risultati dei facet restituiti si basano sul contenuto dell'elenco di stringhe. Ad esempio, se avete un campo con un elenco di stringhe che contiene due elementi, uno con l'elenco «bassotto», «cane da salsiccia» e uno con il valore «husky», otterrete tre sfaccettature. `FacetResults`

Per ulteriori informazioni, consulta Risposte alle interrogazioni e tipi di risposta.

Utilizzo degli attributi del documento per filtrare i risultati della ricerca

Per impostazione predefinita, `Query` restituisce tutti i risultati della ricerca. Per filtrare le risposte, è possibile eseguire operazioni logiche sugli attributi del documento. Ad esempio, se desideri solo documenti per una città specifica, puoi filtrare gli attributi personalizzati del documento «Città» e «Stato». Si utilizza AttributeFilterper creare un'operazione booleana sui filtri forniti dall'utente.

La maggior parte degli attributi può essere utilizzata per filtrare le risposte per tutti i tipi di risposta. Tuttavia, l'`_excerpt_page_number`attributo è applicabile solo ai tipi di `ANSWER` risposta quando si filtrano le risposte.

L'esempio seguente mostra come eseguire un'operazione AND logica filtrando in base a una città specifica, Seattle, e allo stato di Washington.

```
response=kendra.query(
        QueryText = query,
        IndexId = index,
        AttributeFilter = {'AndAllFilters':
            [
                {"EqualsTo": {"Key": "City","Value": {"StringValue": "Seattle"}}},
                {"EqualsTo": {"Key": "State","Value": {"StringValue": "Washington"}}}
            ]
            }
        )
```

L'esempio seguente mostra come eseguire un'operazione OR logica quando una qualsiasi delle `SourceURI` chiavi `FileformatAuthor`, o corrisponde ai valori specificati.

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

Per `StringList` i campi, utilizzate i filtri `ContainsAll` degli attributi `ContainsAny` o per restituire i documenti con la stringa specificata. L'esempio seguente mostra come restituire tutti i documenti che hanno i valori «Seattle» o «Portland» nell'attributo `Locations` personalizzato.

```
response=kendra.query(
```

```
        QueryText = query,
        IndexId = index,
        AttributeFilter = {
                "ContainsAny": { "Key": "Locations", "Value": { "StringListValue":
 [ "Seattle", "Portland"] }}
            }
        )
```

Filtrare gli attributi di ciascun documento nei risultati della ricerca

Amazon Kendra restituisce gli attributi del documento per ogni documento nei risultati della ricerca. È possibile filtrare determinati attributi del documento che si desidera includere nella risposta come parte dei risultati della ricerca. Per impostazione predefinita, tutti gli attributi del documento assegnati a un documento vengono restituiti nella risposta.

Nell'esempio seguente, solo gli attributi `_source_uri` e del `_author` documento sono inclusi nella risposta di un documento.

```
response=kendra.query(
        QueryText = query,
        IndexId = index,
        RequestedDocumentAttributes = ["_source_uri", "_author"]
        )
```

Filtraggio in base al contesto dell'utente

Puoi filtrare i risultati della ricerca di un utente in base all'accesso dell'utente o del suo gruppo ai documenti. È possibile utilizzare un token utente, un ID utente o un attributo utente per filtrare i documenti. Amazon Kendra può anche mappare gli utenti ai loro gruppi. Puoi scegliere di utilizzarlo AWS IAM Identity Center come archivio di identità o fonte.

Il filtraggio del contesto utente è un tipo di ricerca personalizzata con il vantaggio di controllare l'accesso ai documenti. Ad esempio, non tutti i team che cercano informazioni nel portale aziendale devono accedere ai documenti aziendali top secret, né tali documenti sono pertinenti per tutti gli utenti. Solo utenti o gruppi di team specifici che hanno accesso ai documenti top secret dovrebbero vedere questi documenti nei risultati di ricerca.

Quando un documento viene indicizzato in Amazon Kendra, per la maggior parte dei documenti viene inserita una corrispondente lista di controllo degli accessi (ACL). L'ACL specifica a quali nomi utente

e nomi di gruppi è consentito o negato l'accesso al documento. I documenti senza un ACL sono documenti pubblici.

Amazon Kendra può estrarre le informazioni sull'utente o sul gruppo associate a ciascun documento per la maggior parte delle fonti di dati. Ad esempio, un documento in Quip può includere un elenco «condiviso» di utenti selezionati a cui è consentito l'accesso al documento. Se utilizzi un bucket S3 come fonte di dati, fornisci un file JSON per il tuo ACL e includi il percorso S3 di questo file come parte della configurazione dell'origine dati. Se aggiungi documenti direttamente a un indice, specifichi l'ACL nell'oggetto Principal come parte dell'oggetto documento nell'API. BatchPutDocument

È possibile utilizzare l'CreateAccessControlConfigurationAPI per riconfigurare il controllo di accesso a livello di documento esistente senza indicizzare nuovamente tutti i documenti. Ad esempio, l'indice contiene documenti aziendali top secret a cui possono accedere solo determinati dipendenti o utenti. Uno di questi utenti lascia l'azienda o passa a un team a cui dovrebbe essere impedito l'accesso ai documenti top secret. L'utente ha ancora accesso ai documenti top secret perché aveva accesso quando i documenti venivano indicizzati in precedenza. È possibile creare una configurazione di controllo degli accessi specifica per l'utente con negazione dell'accesso. Successivamente è possibile aggiornare la configurazione del controllo degli accessi per consentire l'accesso nel caso in cui l'utente ritorni in azienda e si unisca nuovamente al team «top secret». Puoi riconfigurare il controllo degli accessi per i tuoi documenti man mano che le circostanze cambiano.

Per applicare la configurazione del controllo degli accessi a determinati documenti, si chiama l'BatchPutDocumentAPI con l'oggetto Document `AccessControlConfigurationId` incluso. Se usi un bucket S3 come fonte di dati, lo aggiorni `.metadata.json` con `AccessControlConfigurationId` e sincronizzi la tua origine dati. Amazon Kendra attualmente supporta solo la configurazione del controllo degli accessi per le fonti di dati e i documenti S3 indicizzati tramite l'API. `BatchPutDocument`

Filtraggio per token utente

Quando si esegue una query su un indice, è possibile utilizzare un token utente per filtrare i risultati della ricerca in base all'accesso dell'utente o del relativo gruppo ai documenti. Quando si esegue una query, Amazon Kendra estrae e convalida il token, recupera e controlla le informazioni sull'utente e sul gruppo ed esegue la query. Vengono restituiti tutti i documenti a cui l'utente ha accesso, inclusi i documenti pubblici. Per ulteriori informazioni, consulta Controllo dell'accesso utente basato su token.

Fornisci il token utente nell'UserContextoggetto e lo passi nell'API Query.

Di seguito viene illustrato come includere un token utente.

```
response = kendra.query(
    QueryText = query,
    IndexId = index,
    UserToken = {
        Token = "token"
    })
```

È possibile mappare gli utenti ai gruppi. Quando si utilizza il filtro del contesto utente, non è necessario includere tutti i gruppi a cui appartiene un utente quando si esegue la query. Con l'PutPrincipalMappingAPI, puoi mappare gli utenti ai loro gruppi. Se non desideri utilizzare l'`PutPrincipalMapping`API, devi fornire il nome utente e tutti i gruppi a cui appartiene l'utente quando effettui una query. Puoi anche recuperare i livelli di accesso di gruppi e utenti nella tua fonte di identità IAM Identity Center utilizzando l'UserGroupResolutionConfigurationoggetto.

Filtraggio per ID utente e gruppo

Quando si esegue una query su un indice, è possibile utilizzare l'ID utente e il gruppo per filtrare i risultati della ricerca in base all'accesso dell'utente o del relativo gruppo ai documenti. Quando si esegue una query, Amazon Kendra controlla le informazioni sull'utente e sul gruppo ed esegue la query. Vengono restituiti tutti i documenti pertinenti alla query a cui l'utente ha accesso, inclusi i documenti pubblici.

Puoi anche filtrare i risultati della ricerca in base alle fonti di dati a cui hanno accesso utenti e gruppi. Specificare un'origine dati è utile se un gruppo è legato a più fonti di dati, ma si desidera che il gruppo acceda solo ai documenti di una determinata origine dati. Ad esempio, i gruppi «Ricerca», «Ingegneria» e «Vendite e marketing» sono tutti collegati ai documenti dell'azienda archiviati nelle fonti di dati Confluence e Salesforce. Tuttavia, il team «Vendite e marketing» deve accedere solo ai documenti relativi ai clienti archiviati in Salesforce. Pertanto, quando gli utenti delle vendite e del marketing cercano documenti relativi ai clienti, possono visualizzare i documenti di Salesforce nei risultati. Gli utenti che non si occupano di vendite e marketing non vedono i documenti Salesforce nei risultati di ricerca.

Fornisci informazioni su utenti, gruppi e fonti di dati nell'UserContextoggetto e le passi nell'API Query. L'ID utente e l'elenco dei gruppi e delle fonti di dati devono corrispondere al nome specificato nell'oggetto Principal per identificare l'utente, i gruppi e le fonti di dati. Con l'`Principal`oggetto, è possibile aggiungere un utente, un gruppo o una fonte di dati a un elenco consentito o a un elenco di divieto per l'accesso a un documento.

È necessario fornire uno dei seguenti elementi:

- Informazioni su utenti e gruppi e (facoltative) informazioni sulle fonti di dati.
- Solo le informazioni sugli utenti se mappi gli utenti a gruppi e fonti di dati utilizzando l'PutPrincipalMappingAPI. Puoi anche recuperare i livelli di accesso di gruppi e utenti nella tua fonte di identità IAM Identity Center utilizzando l'UserGroupResolutionConfigurationoggetto.

Se queste informazioni non sono incluse nella query, Amazon Kendra restituisce tutti i documenti. Se fornite queste informazioni, vengono restituiti solo i documenti con ID utente, gruppi e fonti di dati corrispondenti.

Di seguito viene illustrato come includere ID utente, gruppi e fonti di dati.

```
response = kendra.query(
    QueryText = query,
    IndexId = index,
    UserId = {
        UserId = "user1"
    },
    Groups = {
        Groups = ["Sales and Marketing"]
    },
    DataSourceGroups = {
        DataSourceGroups = [{"DataSourceId" : "SalesforceCustomerDocsGroup", "GroupId":
 "Sales and Marketing"}]
    })
```

Filtraggio per attributo utente

Quando si esegue una query su un indice, è possibile utilizzare gli attributi incorporati `_user_id` e `_group_id` filtrare i risultati della ricerca in base all'accesso dell'utente e del relativo gruppo ai documenti. È possibile impostare fino a 100 identificatori di gruppo. Quando si esegue una query, Amazon Kendra controlla le informazioni sull'utente e sul gruppo ed esegue la query. Vengono restituiti tutti i documenti pertinenti alla query a cui l'utente ha accesso, inclusi i documenti pubblici.

Fornisci gli attributi utente e di gruppo nell'AttributeFilteroggetto e li passi nell'API Query.

L'esempio seguente mostra una richiesta che filtra la risposta alla query in base all'ID utente e ai gruppi «HR» e «IT», a cui l'utente appartiene. La query restituirà qualsiasi documento che contenga l'utente o i gruppi «HR» o «IT» nell'elenco consentito. Se l'utente o uno dei due gruppi è presente nell'elenco degli utenti non accettati per un documento, il documento non viene restituito.

```
response = kendra.query(
        QueryText = query,
        IndexId = index,
        AttributeFilter = {
            "OrAllFilters": [
                {
                    "EqualsTo": {
                        "Key": "_user_id",
                        "Value": {
                            "StringValue": "user1"
                        }
                     }
                },
                {
                    "EqualsTo": {
                        "Key": "_group_ids",
                        "Value": {
                            "StringListValue": ["HR", "IT"]
                        }
                    }
                }
            ]
        }
        )
```

È inoltre possibile specificare a quale origine dati un gruppo può accedere nell'`Principal`oggetto.

> **Note**
>
> Il filtraggio del contesto utente non è un controllo di autenticazione o autorizzazione per i tuoi contenuti. Non esegue l'autenticazione dell'utente sull'utente e sui gruppi inviati all'`Query`API. Spetta all'applicazione garantire che le informazioni su utenti e gruppi inviate all'`Query`API siano autenticate e autorizzate.

Esiste un'implementazione del filtraggio del contesto utente per ogni fonte di dati. La sezione seguente descrive ogni implementazione.

Argomenti

- Filtraggio del contesto utente per i documenti aggiunti direttamente a un indice
- Filtraggio del contesto utente per le domande frequenti

- Filtraggio del contesto utente per le fonti di dati

Filtraggio del contesto utente per i documenti aggiunti direttamente a un indice

Quando aggiungi documenti direttamente a un indice utilizzando l'BatchPutDocumentAPI, Amazon Kendra ottiene informazioni su utenti e gruppi dal `AccessControlList` campo del documento. Fornisci una lista di controllo degli accessi (ACL) per i tuoi documenti e l'ACL viene incorporata con i tuoi documenti.

L'ACL viene specificato nell'oggetto Principal come parte dell'oggetto Document nell'API. `BatchPutDocument` Fornisci le seguenti informazioni:

- L'accesso che deve avere l'utente o il gruppo. Puoi dire `ALLOW` o`DENY`.
- Il tipo di entità. Puoi dire `USER` o`GROUP`.
- Il nome dell'utente o del gruppo.

Puoi aggiungere fino a 200 voci nel `AccessControlList` campo.

Filtraggio del contesto utente per le domande frequenti

Quando aggiungi una FAQ a un indice, Amazon Kendra ottiene informazioni su utenti e gruppi dall'`AccessControlList`oggetto/campo del file JSON delle domande frequenti. Puoi anche utilizzare un file FAQ CSV con campi o attributi personalizzati per il controllo degli accessi.

Fornisci le seguenti informazioni:

- L'accesso che deve avere l'utente o il gruppo. Puoi dire `ALLOW` o`DENY`.
- Il tipo di entità. Puoi dire `USER` o`GROUP`.
- Il nome dell'utente o del gruppo.

Per ulteriori informazioni, consulta i file delle domande frequenti.

Filtraggio del contesto utente per le fonti di dati

Amazon Kendra esegue anche la scansione delle informazioni sugli elenchi di controllo degli accessi di utenti e gruppi (ACL) dai connettori di origine dati supportati. Ciò è utile per il filtraggio del contesto

degli utenti, in cui i risultati della ricerca vengono filtrati in base all'accesso dell'utente o del relativo gruppo ai documenti.

Argomenti

- Filtraggio del contesto utente per le origini dati di Microsoft SQL Server
- Filtraggio del contesto utente per le origini dati di Microsoft Teams
- Filtraggio del contesto utente per le origini dati Microsoft Yammer
- Filtraggio del contesto utente per sorgenti dati MySQL
- Filtraggio del contesto utente per le origini dati di Oracle Database
- Filtraggio del contesto utente per le fonti di dati PostgreSQL
- Filtraggio del contesto utente per le fonti di dati Quip
- Filtraggio del contesto utente per le fonti di dati Salesforce
- Filtraggio del contesto utente per le fonti di ServiceNow dati
- Filtraggio del contesto utente per le fonti di dati Slack
- Filtraggio del contesto utente per le fonti di dati Zendesk

Filtraggio del contesto utente per le fonti di dati di Adobe Experience Manager

Quando utilizzi un'origine dati di Adobe Experience Manager, Amazon Kendra ottiene le informazioni su utenti e gruppi dall'istanza di Adobe Experience Manager.

Gli ID di gruppo e utente sono mappati come segue:

- `_group_ids`—Gli ID di gruppo esistono nei contenuti di Adobe Experience Manager in cui sono presenti autorizzazioni di accesso impostate. Sono mappati in base ai nomi dei gruppi in Adobe Experience Manager.
- `_user_id`—Gli ID utente esistono nei contenuti di Adobe Experience Manager in cui sono presenti autorizzazioni di accesso impostate. Vengono mappati dalle e-mail degli utenti come ID in Adobe Experience Manager.

Puoi aggiungere fino a 200 voci nel `AccessControlList` campo.

Filtraggio del contesto utente per le fonti di dati Alfresco

Quando si utilizza un'origine dati Alfresco, Amazon Kendra ottiene le informazioni su utenti e gruppi dall'istanza Alfresco.

Gli ID di gruppo e utente sono mappati come segue:

- `_group_ids`—Gli ID di gruppo esistono in Alfresco sui file in cui sono presenti autorizzazioni di accesso impostate. Sono mappati in base ai nomi di sistema dei gruppi (non ai nomi visualizzati) in Alfresco.
- `_user_id`—Gli ID utente esistono in Alfresco sui file in cui sono presenti autorizzazioni di accesso impostate. Vengono mappati dalle e-mail degli utenti come ID in Alfresco.

È possibile aggiungere fino a 200 voci nel `AccessControlList` campo.

Filtraggio del contesto utente per sorgenti Aurora dati (MySQL)

Quando si utilizza un'origine dati Aurora (MySQL) Amazon Kendra , ottiene informazioni su utenti e gruppi da una colonna nella tabella di origine. Specificate questa colonna nella console o utilizzate l'TemplateConfigurationoggetto come parte dell'CreateDataSourceAPI.

Un'origine dati di database Aurora (MySQL) presenta le seguenti limitazioni:

- È possibile specificare solo un elenco di dati consentiti per un'origine dati del database. Non è possibile specificare un elenco di rifiuto.
- È possibile specificare solo gruppi. Non è possibile specificare singoli utenti per l'elenco degli utenti consentiti.
- La colonna del database deve essere una stringa contenente un elenco di gruppi delimitato da punto e virgola.

Filtraggio del contesto utente per sorgenti Aurora dati (PostgreSQL)

Quando si utilizza un'origine dati Aurora (PostgreSQL) Amazon Kendra , ottiene informazioni su utenti e gruppi da una colonna nella tabella di origine. Specificate questa colonna nella console o utilizzate l'TemplateConfigurationoggetto come parte dell'API. CreateDataSource

Un' Aurora origine dati di database (PostgreSQL) presenta le seguenti limitazioni:

- È possibile specificare solo un elenco di dati consentiti per un'origine dati del database. Non è possibile specificare un elenco di rifiuto.
- È possibile specificare solo gruppi. Non è possibile specificare singoli utenti per l'elenco degli utenti consentiti.
- La colonna del database deve essere una stringa contenente un elenco di gruppi delimitato da punto e virgola.

Filtraggio del contesto utente per le fonti di dati Amazon FSx

Quando utilizzi un'origine Amazon FSx dati, Amazon Kendra ottiene informazioni su utenti e gruppi dal servizio di directory dell' Amazon FSx istanza.

Gli ID Amazon FSx di gruppo e utente sono mappati come segue:

- `_group_ids`—Gli ID di gruppo sono presenti nei file Amazon FSx in cui sono presenti autorizzazioni di accesso impostate. Sono mappati in base ai nomi dei gruppi di sistema nel servizio di directory di. Amazon FSx
- `_user_id`—Gli ID utente sono presenti nei file Amazon FSx in cui sono impostate le autorizzazioni di accesso. Sono mappati dai nomi utente di sistema nel servizio di directory di. Amazon FSx

È possibile aggiungere fino a 200 voci nel `AccessControlList` campo.

Filtraggio del contesto utente per le fonti di dati del database

Quando si utilizza un'origine dati del database, ad esempio Amazon Aurora PostgreSQL, Amazon Kendra ottiene informazioni su utenti e gruppi da una colonna nella tabella di origine. Specificate questa colonna nell'AclConfigurationoggetto come parte dell'DatabaseConfigurationoggetto nell'CreateDataSourceAPI.

Un'origine dati del database presenta le seguenti limitazioni:

- È possibile specificare solo un elenco di dati consentiti per un'origine dati del database. Non è possibile specificare un elenco di rifiuto.
- È possibile specificare solo gruppi. Non è possibile specificare singoli utenti per l'elenco degli utenti consentiti.
- La colonna del database deve essere una stringa contenente un elenco di gruppi delimitato da punto e virgola.

Filtraggio del contesto utente per le origini dati Amazon RDS (Microsoft SQL Server)

Quando si utilizza un'origine dati Amazon RDS (Microsoft SQL Server), Amazon Kendra ottiene informazioni su utenti e gruppi da una colonna nella tabella di origine. Specificate questa colonna nella console o utilizzate l'TemplateConfigurationoggetto come parte dell'CreateDataSourceAPI.

Un'origine dati di database Amazon RDS (Microsoft SQL Server) presenta le seguenti limitazioni:

- È possibile specificare solo un elenco di dati consentiti per un'origine dati del database. Non è possibile specificare un elenco di rifiuto.
- È possibile specificare solo gruppi. Non è possibile specificare singoli utenti per l'elenco degli utenti consentiti.
- La colonna del database deve essere una stringa contenente un elenco di gruppi delimitato da punto e virgola.

Filtraggio del contesto utente per sorgenti Amazon RDS dati (MySQL)

Quando si utilizza un'origine dati Amazon RDS (MySQL) Amazon Kendra , ottiene informazioni su utenti e gruppi da una colonna nella tabella di origine. Specificate questa colonna nella console o utilizzate l'TemplateConfigurationoggetto come parte dell'CreateDataSourceAPI.

Un'origine dati di database Amazon RDS (MySQL) presenta le seguenti limitazioni:

- È possibile specificare solo un elenco di dati consentiti per un'origine dati del database. Non è possibile specificare un elenco di rifiuto.
- È possibile specificare solo gruppi. Non è possibile specificare singoli utenti per l'elenco degli utenti consentiti.
- La colonna del database deve essere una stringa contenente un elenco di gruppi delimitato da punto e virgola.

Filtraggio del contesto utente per le fonti di dati Amazon RDS (Oracle)

Quando si utilizza un'origine dati Amazon RDS (Oracle), Amazon Kendra ottiene informazioni su utenti e gruppi da una colonna della tabella di origine. Specificate questa colonna nella console o utilizzate l'TemplateConfigurationoggetto come parte dell'CreateDataSourceAPI.

Un'origine dati di database Amazon RDS (Oracle) presenta le seguenti limitazioni:

- È possibile specificare solo un elenco di dati consentiti per un'origine dati del database. Non è possibile specificare un elenco di rifiuto.
- È possibile specificare solo gruppi. Non è possibile specificare singoli utenti per l'elenco degli utenti consentiti.
- La colonna del database deve essere una stringa contenente un elenco di gruppi delimitato da punto e virgola.

Filtraggio del contesto utente per sorgenti Amazon RDS dati (PostgreSQL)

Quando si utilizza un'origine dati Amazon RDS (PostgreSQL) Amazon Kendra , ottiene informazioni su utenti e gruppi da una colonna nella tabella di origine. Specificate questa colonna nella console o utilizzate l'TemplateConfigurationoggetto come parte dell'API. CreateDataSource

Un' Amazon RDS origine dati di database (PostgreSQL) presenta le seguenti limitazioni:

- È possibile specificare solo un elenco di dati consentiti per un'origine dati del database. Non è possibile specificare un elenco di rifiuto.
- È possibile specificare solo gruppi. Non è possibile specificare singoli utenti per l'elenco degli utenti consentiti.
- La colonna del database deve essere una stringa contenente un elenco di gruppi delimitato da punto e virgola.

Filtraggio del contesto utente per le fonti di dati Amazon S3

Si aggiunge il filtro del contesto utente a un documento in un'origine Amazon S3 dati utilizzando un file di metadati associato al documento. Le informazioni vengono aggiunte al `AccessControlList` campo del documento JSON. Per ulteriori informazioni sull'aggiunta di metadati ai documenti indicizzati da un'origine Amazon S3 dati, consulta Metadati dei documenti S3.

Fornisci tre informazioni:

- L'accesso che l'entità dovrebbe avere. Puoi dire `ALLOW` o`DENY`.
- Il tipo di entità. Puoi dire `USER` o`GROUP`.
- Il nome dell'entità.

È possibile aggiungere fino a 200 voci nel `AccessControlList` campo.

Filtraggio del contesto utente per le fonti di Amazon WorkDocs dati

Quando utilizzi un'origine Amazon WorkDocs dati, Amazon Kendra ottiene informazioni su utenti e gruppi dall' Amazon WorkDocs istanza.

Gli ID Amazon WorkDocs di gruppo e utente sono mappati come segue:

- `_group_ids`—Gli ID di gruppo sono presenti nei file Amazon WorkDocs in cui sono presenti autorizzazioni di accesso impostate. Sono mappati in base ai nomi dei gruppi in. Amazon WorkDocs
- `_user_id`—Gli ID utente sono presenti nei file Amazon WorkDocs in cui sono presenti autorizzazioni di accesso impostate. Sono mappati dai nomi utente in. Amazon WorkDocs

È possibile aggiungere fino a 200 voci nel `AccessControlList` campo.

Filtraggio del contesto utente per le sorgenti dati Box

Quando utilizzi un'origine dati Box, Amazon Kendra ottiene informazioni su utenti e gruppi dall'istanza Box.

Il gruppo Box e gli ID utente sono mappati come segue:

- `_group_ids`—Gli ID di gruppo esistono in Box sui file in cui sono presenti autorizzazioni di accesso impostate. Sono mappati in base ai nomi dei gruppi in Box.
- `_user_id`—Gli ID utente esistono in Box nei file in cui sono presenti autorizzazioni di accesso impostate. Vengono mappati dalle e-mail degli utenti come ID utente in Box.

Puoi aggiungere fino a 200 voci nel `AccessControlList` campo.

Filtraggio del contesto utente per le fonti di dati Confluence

Quando utilizzi un'origine dati Confluence, Amazon Kendra ottiene informazioni su utenti e gruppi dall'istanza Confluence.

Puoi configurare l'accesso di utenti e gruppi agli spazi utilizzando la pagina delle autorizzazioni dello spazio. Per le pagine e i blog, si utilizza la pagina delle restrizioni. Per ulteriori informazioni sulle autorizzazioni di spazio, consulta Space Permissions Overview sul sito Web di Confluence Support. Per ulteriori informazioni sulle restrizioni relative a pagine e blog, consulta Restrizioni di pagina sul sito Web di Confluence Support.

Il gruppo e i nomi utente di Confluence sono mappati come segue:

- `_group_ids`—I nomi dei gruppi sono presenti in spazi, pagine e blog soggetti a restrizioni. Sono mappati a partire dal nome del gruppo in Confluence. I nomi dei gruppi sono sempre in minuscolo.

- `_user_id`—I nomi utente sono presenti nello spazio, nella pagina o nel blog in cui sono presenti restrizioni. Sono mappati in base al tipo di istanza Confluence che stai utilizzando.

  Per il connettore Confluence v1.0

  - Server: è il `_user_id` nome utente. Il nome utente è sempre in minuscolo.
  - Cloud: `_user_id` è l'ID dell'account dell'utente.

  Per il connettore Confluence v2.0

  - Server: è il `_user_id` nome utente. Il nome utente è sempre in minuscolo.
  - Cloud: `_user_id` è l'ID e-mail dell'utente.

  > **Important**
  >
  > Affinché il filtro del contesto utente funzioni correttamente per il tuo connettore Confluence, devi assicurarti che la visibilità di un utente a cui è stato concesso l'accesso a una pagina Confluence sia impostata su Chiunque. Per ulteriori informazioni, consulta Impostare la visibilità delle e-mail nella documentazione per sviluppatori di Atlassian.

Puoi aggiungere fino a 200 voci nel `AccessControlList` campo.

Filtraggio del contesto utente per le fonti di dati di Dropbox

Quando utilizzi una fonte di dati Dropbox, Amazon Kendra ottiene le informazioni su utenti e gruppi dall'istanza Dropbox.

Gli ID di gruppo e utente sono mappati come segue:

- `_group_ids`—Gli ID di gruppo esistono in Dropbox sui file in cui sono presenti autorizzazioni di accesso prestabilite. Sono mappati in base ai nomi dei gruppi in Dropbox.
- `_user_id`—Gli ID utente esistono in Dropbox sui file in cui sono presenti autorizzazioni di accesso prestabilite. Vengono mappati dalle email degli utenti come ID in Dropbox.

Puoi aggiungere fino a 200 voci nel `AccessControlList` campo.

Filtraggio del contesto utente per le fonti di dati Drupal

Quando si utilizza una fonte di dati Drupal, Amazon Kendra ottiene le informazioni su utenti e gruppi dall'istanza Drupal.

Gli ID di gruppo e utente sono mappati come segue:

- `_group_ids`— Gli ID di gruppo esistono in Drupal sui file in cui sono presenti autorizzazioni di accesso impostate. Sono mappati in base ai nomi dei gruppi in Drupal.
- `_user_id`— Gli ID utente esistono in Drupal sui file in cui sono impostati i permessi di accesso. Vengono mappati dalle e-mail degli utenti come ID in Drupal.

Puoi aggiungere fino a 200 voci nel campo. `AccessControlList`

Filtraggio del contesto utente per le fonti di GitHub dati

Quando utilizzi un'origine GitHub dati, Amazon Kendra ottiene le informazioni sull'utente dall' GitHub istanza.

Gli ID GitHub utente sono mappati come segue:

- `_user_id`—Gli ID utente sono presenti nei file GitHub in cui sono presenti autorizzazioni di accesso impostate. Vengono mappati dalle e-mail degli utenti come ID inseriti. GitHub

È possibile aggiungere fino a 200 voci nel `AccessControlList` campo.

Filtraggio del contesto utente per le fonti di dati di Gmail

Quando utilizzi un'origine dati Gmail, Amazon Kendra ottiene le informazioni sull'utente dall'istanza di Gmail.

Gli ID utente sono mappati come segue:

- `_user_id`— Gli ID utente esistono in Gmail nei file in cui sono presenti autorizzazioni di accesso impostate. Vengono mappati dalle e-mail degli utenti come ID in Gmail.

Puoi aggiungere fino a 200 voci nel `AccessControlList` campo.

Filtraggio del contesto utente per le fonti di dati di Google Drive

Un'origine dati Google Workspace Drive restituisce informazioni su utenti e gruppi per utenti e gruppi di Google Drive. L'appartenenza a gruppi e domini viene mappata sul campo dell'`_group_ids`indice. Il nome utente di Google Drive è mappato sul `_user_id` campo.

Quando fornisci uno o più indirizzi email utente nell'`Query`API, vengono restituiti solo i documenti che sono stati condivisi con tali indirizzi email. Il seguente `AttributeFilter` parametro restituisce solo i documenti condivisi con "martha@example.com».

```
"AttributeFilter": {
                "EqualsTo":{
                   "Key": "_user_id",
                   "Value": {
                       "StringValue": "martha@example.com"
                   }
               }
          }
```

Se si forniscono uno o più indirizzi e-mail di gruppo nella query, vengono restituiti solo i documenti condivisi con i gruppi. Il seguente `AttributeFilter` parametro restituisce solo i documenti condivisi con il gruppo "hr@example.com».

```
"AttributeFilter": {
                "EqualsTo":{
                   "Key": "_group_ids",
                   "Value": {
                       "StringListValue": ["hr@example.com"]
                   }
               }
          }
```

Se si fornisce il dominio nella query, vengono restituiti tutti i documenti condivisi con il dominio. Il seguente `AttributeFilter` parametro restituisce i documenti condivisi con il dominio «example.com».

```
"AttributeFilter": {
                "EqualsTo":{
                   "Key": "_group_ids",
                   "Value": {
                       "StringListValue": ["example.com"]
```

```
                }
            }
        }
```

È possibile aggiungere fino a 200 voci nel `AccessControlList` campo.

Filtraggio del contesto utente per le fonti di dati IBM DB2

Quando utilizzi un'origine dati IBM DB2, Amazon Kendra ottiene informazioni su utenti e gruppi da una colonna nella tabella di origine. Specificate questa colonna nella console o utilizzate l'TemplateConfigurationoggetto come parte dell'CreateDataSourceAPI.

Un'origine dati del database IBM DB2 presenta le seguenti limitazioni:

- È possibile specificare solo un elenco di dati consentiti per un'origine dati del database. Non è possibile specificare un elenco di rifiuto.
- È possibile specificare solo gruppi. Non è possibile specificare singoli utenti per l'elenco degli utenti consentiti.
- La colonna del database deve essere una stringa contenente un elenco di gruppi delimitato da punto e virgola.

Filtraggio del contesto utente per le fonti di dati Jira

Quando usi un'origine dati Jira, Amazon Kendra ottiene informazioni su utenti e gruppi dall'istanza Jira.

Gli ID utente Jira sono mappati come segue:

- `_user_id`—Gli ID utente esistono in Jira nei file in cui sono presenti autorizzazioni di accesso impostate. Vengono mappati dalle e-mail degli utenti come ID utente in Jira.

Puoi aggiungere fino a 200 voci nel `AccessControlList` campo.

Filtraggio del contesto utente per le origini dati di Microsoft Exchange

Quando si utilizza un'origine dati di Microsoft Exchange, Amazon Kendra ottiene le informazioni sull'utente dall'istanza di Microsoft Exchange.

Gli ID utente di Microsoft Exchange sono mappati come segue:

- `_user_id`—Gli ID utente sono presenti nelle autorizzazioni di Microsoft Exchange che consentono agli utenti di accedere a determinati contenuti. Vengono mappati dai nomi utente come ID in Microsoft Exchange.

È possibile aggiungere fino a 200 voci nel `AccessControlList` campo.

Filtraggio del contesto utente per le origini OneDrive dati Microsoft

Amazon Kendra recupera informazioni su utenti e gruppi da Microsoft OneDrive quando indicizza i documenti sul sito. Le informazioni su utenti e gruppi sono tratte dal SharePoint sito Microsoft sottostante che ospita OneDrive.

Quando utilizzi un OneDrive utente o un gruppo per filtrare i risultati della ricerca, calcola l'ID come segue:

1. Ottieni il nome del sito. Ad esempio, `https://host.onmicrosoft.com/sites/siteName.`
2. Prendi l'hash MD5 del nome del sito. Ad esempio, `430a6b90503eef95c89295c8999c7981`.
3. Crea l'e-mail dell'utente o l'ID del gruppo concatenando l'hash MD5 con una barra verticale (|) e l'ID. Ad esempio, se il nome di un gruppo è "localGroupName«, l'ID del gruppo sarebbe:

   ```
   "430a6b90503eef95c89295c8999c7981 | localGroupName"
   ```

   > **Note**
   >
   > Includi uno spazio prima e dopo la barra verticale. La barra verticale viene utilizzata per identificarsi `localGroupName` con il relativo hash MD5.

   Per il nome utente "someone@host.onmicrosoft.com», l'ID utente sarebbe il seguente:

   ```
   "430a6b90503eef95c89295c8999c7981 | someone@host.onmicrosoft.com"
   ```

Invia l'ID utente o di gruppo a Amazon Kendra come `_group_id` attributo `_user_id` o quando chiami l'API Query. Ad esempio, il AWS CLI comando che utilizza un gruppo per filtrare i risultati della ricerca ha il seguente aspetto:

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

```
                --query-text "query text"
                --attribute-filter '{
                   "EqualsTo":{
                     "Key": "_group_id",
                     "Value": {"StringValue": "430a6b90503eef95c89295c8999c7981 |
localGroupName"}
                  }}'
```

È possibile aggiungere fino a 200 voci nel `AccessControlList` campo.

Filtraggio del contesto utente per le origini dati Microsoft OneDrive v2.0

Un'origine dati Microsoft OneDrive v2.0 restituisce informazioni su sezioni e pagine dalle entità della lista di controllo degli OneDrive accessi (ACL). Amazon Kendra utilizza il dominio OneDrive tenant per connettersi all' OneDrive istanza e quindi può filtrare i risultati della ricerca in base all'accesso di utenti o gruppi alle sezioni e ai nomi di file.

Per gli oggetti standard, gli `_user_id` e `_group_id` vengono utilizzati come segue:

- `_user_id`— Il tuo ID e-mail OneDrive utente Microsoft è mappato sul `_user_id` campo.
- `_group_id`— L'e-mail OneDrive del gruppo Microsoft è mappata sul `_group_id` campo.

È possibile aggiungere fino a 200 voci nel `AccessControlList` campo.

Filtraggio del contesto utente per le origini SharePoint dati Microsoft

Amazon Kendra recupera informazioni su utenti e gruppi da Microsoft SharePoint quando indicizza i documenti del sito. Per filtrare i risultati della ricerca in base all'accesso di utenti o gruppi, fornisci informazioni su utenti e gruppi quando chiami l'API. `Query`

Per filtrare utilizzando un nome utente, utilizza l'indirizzo e-mail dell'utente. Ad esempio, johnstiles@example.com.

Quando utilizzi un SharePoint gruppo per filtrare i risultati della ricerca, calcola l'ID del gruppo come segue:

Per gruppi locali

1. Ottieni il nome del sito. Ad esempio, `https://host.onmicrosoft.com/sites/siteName`.
2. Prendi l'hash SHA256 del nome del sito. Ad esempio, `430a6b90503eef95c89295c8999c7981`.

3. Crea l'ID del gruppo concatenando l'hash SHA256 con una barra verticale (|) e il nome del gruppo. Ad esempio, se il nome del gruppo è "localGroupName«, l'ID del gruppo sarebbe:

   `"430a6b90503eef95c89295c8999c7981 | localGroupName"`

   > **Note**
   >
   > Includi uno spazio prima e dopo la barra verticale. La barra verticale viene utilizzata per identificarsi `localGroupName` con il relativo hash SHA256.

Invia l'ID del gruppo a Amazon Kendra come `_group_id` attributo quando chiami l'API Query. Ad esempio, il AWS CLI comando ha il seguente aspetto:

```
aws kendra  query \
                --index-id index ID
                --query-text "query text"
                --attribute-filter '{
                   "EqualsTo":{
                     "Key": "_group_id",
                     "Value": {"StringValue": "430a6b90503eef95c89295c8999c7981 |
 localGroupName"}
                  }}'
```

Per i gruppi AD

1. Utilizza l'ID del gruppo AD per configurare il filtraggio dei risultati di ricerca.

Invia l'ID del gruppo a Amazon Kendra come `_group_id` attributo quando chiami l'API Query. Ad esempio, il AWS CLI comando ha il seguente aspetto:

```
aws kendra  query \
                --index-id index ID
                --query-text "query text"
                --attribute-filter '{
                   "EqualsTo":{
                     "Key": "_group_id",
                     "Value": {"StringValue": "AD group"}
                  }}'
```

È possibile aggiungere fino a 200 voci nel `AccessControlList` campo.

Filtraggio del contesto utente per le origini dati di Microsoft SQL Server

Quando si utilizza un'origine dati Microsoft SQL Server, Amazon Kendra ottiene informazioni su utenti e gruppi da una colonna nella tabella di origine. È possibile specificare questa colonna nella console o utilizzare l'TemplateConfigurationoggetto come parte dell'CreateDataSourceAPI.

Un'origine dati di database Microsoft SQL Server presenta le seguenti limitazioni:

- È possibile specificare solo un elenco di dati consentiti per un'origine dati del database. Non è possibile specificare un elenco di rifiuto.
- È possibile specificare solo gruppi. Non è possibile specificare singoli utenti per l'elenco degli utenti consentiti.
- La colonna del database deve essere una stringa contenente un elenco di gruppi delimitato da punto e virgola.

Filtraggio del contesto utente per le origini dati di Microsoft Teams

Amazon Kendra recupera le informazioni dell'utente da Microsoft Teams quando indicizza i documenti. Le informazioni sull'utente vengono prese dall'istanza Microsoft Teams sottostante.

È possibile aggiungere fino a 200 voci nel `AccessControlList` campo.

Filtraggio del contesto utente per le origini dati Microsoft Yammer

Amazon Kendra recupera le informazioni utente da Microsoft Yammer quando indicizza i documenti. Le informazioni su utenti e gruppi vengono prese dall'istanza di Microsoft Yammer sottostante.

Gli ID utente di Microsoft Yammer sono mappati come segue:

- `_email_id`— L'ID e-mail Microsoft mappato al `_user_id` campo.

È possibile aggiungere fino a 200 voci nel `AccessControlList` campo.

Filtraggio del contesto utente per sorgenti dati MySQL

Quando si utilizza un'origine dati MySQL Amazon Kendra , ottiene informazioni su utenti e gruppi da una colonna nella tabella di origine. Specificate questa colonna nella console o utilizzate l'TemplateConfigurationoggetto come parte dell'CreateDataSourceAPI.

L'origine dati di un database MySQL presenta le seguenti limitazioni:

- È possibile specificare solo un elenco di dati consentiti per un'origine dati del database. Non è possibile specificare un elenco di rifiuto.
- È possibile specificare solo gruppi. Non è possibile specificare singoli utenti per l'elenco degli utenti consentiti.
- La colonna del database deve essere una stringa contenente un elenco di gruppi delimitato da punto e virgola.

Filtraggio del contesto utente per le origini dati di Oracle Database

Quando si utilizza un'origine dati del database Oracle, Amazon Kendra ottiene informazioni su utenti e gruppi da una colonna nella tabella di origine. È possibile specificare questa colonna nella console o utilizzare l'TemplateConfigurationoggetto come parte dell'CreateDataSourceAPI.

L'origine dati di un database Oracle Database presenta le seguenti limitazioni:

- È possibile specificare solo un elenco di dati consentiti per un'origine dati del database. Non è possibile specificare un elenco di rifiuto.
- È possibile specificare solo gruppi. Non è possibile specificare singoli utenti per l'elenco degli utenti consentiti.
- La colonna del database deve essere una stringa contenente un elenco di gruppi delimitato da punto e virgola.

Filtraggio del contesto utente per le fonti di dati PostgreSQL

Quando usi un'origine dati PostgreSQL Amazon Kendra , ottiene informazioni su utenti e gruppi da una colonna nella tabella di origine. Specificate questa colonna nella console o utilizzate l'TemplateConfigurationoggetto come parte dell'API. CreateDataSource

L'origine dati di un database PostgreSQL presenta le seguenti limitazioni:

- È possibile specificare solo un elenco di dati consentiti per un'origine dati del database. Non è possibile specificare un elenco di rifiuto.
- È possibile specificare solo gruppi. Non è possibile specificare singoli utenti per l'elenco degli utenti consentiti.

- La colonna del database deve essere una stringa contenente un elenco di gruppi delimitato da punto e virgola.

Filtraggio del contesto utente per le fonti di dati Quip

Quando si utilizza una fonte di dati Quip, Amazon Kendra ottiene le informazioni sull'utente dall'istanza Quip.

Gli ID utente Quip sono mappati come segue:

- `_user_id`—Gli ID utente esistono in Quip su file in cui sono presenti autorizzazioni di accesso impostate. Vengono mappati dalle e-mail degli utenti come ID in Quip.

Puoi aggiungere fino a 200 voci nel `AccessControlList` campo.

Filtraggio del contesto utente per le fonti di dati Salesforce

Un'origine dati Salesforce restituisce informazioni su utenti e gruppi dalle entità della Salesforce Access Control List (ACL). Puoi applicare il filtro del contesto utente agli oggetti standard di Salesforce e ai feed di chat. Il filtraggio del contesto utente non è disponibile per gli articoli di conoscenza di Salesforce.

Per gli oggetti standard, i `_user_id` e `_group_ids` vengono utilizzati come segue:

- `_user_id`—Il nome utente dell'utente Salesforce.
- `_group_ids`—
  - Nome dell'utente Salesforce `Profile`
  - Nome di Salesforce `Group`
  - Nome di Salesforce `UserRole`
  - Nome di Salesforce `PermissionSet`

Per i feed di Chatter, gli `_user_id` e `_group_ids` vengono utilizzati come segue:

- `_user_id`—Il nome utente dell'utente Salesforce. Disponibile solo se l'articolo è pubblicato nel feed dell'utente.
- `_group_ids`—Gli ID di gruppo vengono utilizzati come segue. Disponibile solo se l'elemento del feed è pubblicato in un gruppo di chat o di collaborazione.

- Il nome del gruppo di chat o di collaborazione.
- Se il gruppo è pubblico,`PUBLIC:ALL`.

È possibile aggiungere fino a 200 voci nel `AccessControlList` campo.

Filtraggio del contesto utente per le fonti di ServiceNow dati

Il filtraggio del contesto utente per ServiceNow è supportato solo per l' TemplateConfiguration API e il ServiceNow Connector v2.0. ServiceNowConfigurationAPI e ServiceNow Connector v1.0. non supportano il filtraggio del contesto utente.

Quando utilizzi un'origine ServiceNow dati, Amazon Kendra ottiene le informazioni sull'utente e sul gruppo dall'istanza. ServiceNow

Gli ID di gruppo e utente sono mappati come segue:

- `_group_ids`—Gli ID di gruppo sono presenti nei file ServiceNow in cui sono presenti autorizzazioni di accesso impostate. Sono mappati in base ai nomi dei ruoli di in. `sys_ids` ServiceNow
- `_user_id`—Gli ID utente sono presenti nei file ServiceNow in cui sono presenti autorizzazioni di accesso impostate. Vengono mappati dalle e-mail degli utenti come ID inseriti. ServiceNow

È possibile aggiungere fino a 200 voci nel `AccessControlList` campo.

Filtraggio del contesto utente per le fonti di dati Slack

Quando utilizzi un'origine dati Slack, Amazon Kendra ottiene le informazioni sull'utente dall'istanza Slack.

Gli ID utente di Slack sono mappati come segue:

- `_user_id`—Gli ID utente esistono in Slack nei messaggi e nei canali in cui sono impostate le autorizzazioni di accesso. Vengono mappati dalle e-mail degli utenti come ID in Slack.

Puoi aggiungere fino a 200 voci nel `AccessControlList` campo.

Filtraggio del contesto utente per le fonti di dati Zendesk

Quando utilizzi un'origine dati Zendesk, Amazon Kendra ottiene le informazioni su utenti e gruppi dall'istanza Zendesk.

Gli ID di gruppo e utente sono mappati come segue:

- `_group_ids`—Gli ID di gruppo sono presenti nei ticket e negli articoli Zendesk in cui sono presenti autorizzazioni di accesso prestabilite. Sono mappati in base ai nomi dei gruppi in Zendesk.
- `_user_id`—Gli ID di gruppo sono presenti nei ticket e negli articoli Zendesk in cui sono presenti autorizzazioni di accesso prestabilite. Vengono mappati dalle e-mail degli utenti come ID in Zendesk.

È possibile aggiungere fino a 200 voci nel `AccessControlList` campo.

Risposte alle interrogazioni e tipi di risposta

Amazon Kendra supporta diverse risposte alle interrogazioni e tipi di risposta.

Risposte alle interrogazioni

Una chiamata all'API Query restituisce informazioni sui risultati di una ricerca. I risultati si trovano in una serie di QueryResultItemoggetti (`ResultItems`). Ciascuno `QueryResultItem` include un riepilogo del risultato. Sono inclusi gli attributi del documento associati al risultato della query.

Informazioni di riepilogo

Le informazioni di riepilogo variano a seconda del tipo di risultato. In ogni caso, include il testo del documento che corrisponde al termine di ricerca. Include anche informazioni di evidenziazione che è possibile utilizzare per evidenziare il testo di ricerca nell'output dell'applicazione. Ad esempio, se il termine di ricerca è qual è l'altezza dello Space Needle? , le informazioni di riepilogo includono la posizione del testo per le parole height e space needle. Per informazioni sui tipi di risposta, vedereRisposte alle interrogazioni e tipi di risposta.

Attributi del documento

Ogni risultato contiene gli attributi del documento che corrisponde a una query. Alcuni attributi sono predefiniti, ad esempio `DocumentIdDocumentTitle`, e`DocumentUri`. Altri sono attributi personalizzati definiti dall'utente. È possibile utilizzare gli attributi del documento per filtrare la

risposta dall'`Query`API. Ad esempio, potresti volere solo i documenti scritti da un autore specifico o da una versione specifica di un documento. Per ulteriori informazioni, consulta Filtraggio e ricerca sfaccettata. Gli attributi del documento vengono specificati quando si aggiungono documenti a un indice. Per ulteriori informazioni, consulta Campi o attributi personalizzati.

Di seguito è riportato un esempio di codice JSON per il risultato di una query. Annotate gli attributi del documento in `DocumentAttributes` and`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
}
```

Tipi di risposta

Amazon Kendra restituisce tre tipi di risposta alla query.

- Risposta (include la risposta alla tabella)
- Documento
- Domande e risposte

Il tipo di risposta viene restituito nel campo di `Type` risposta dell'QueryResultItemoggetto.

Risposta

Amazon Kendra ha rilevato una o più risposte alle domande nella risposta. Un dato di fatto è la risposta a una domanda su chi, cosa, quando o dove, ad esempio Dov'è il centro di assistenza più vicino a me? Amazon Kendra restituisce il testo dell'indice che meglio corrisponde alla query. Il testo si trova nel `AnswerText` campo e contiene informazioni di evidenziazione per il termine di ricerca all'interno del testo della risposta. `AnswerText`include l'estratto completo del documento con testo evidenziato, mentre `DocumentExcerpt` include l'estratto del documento troncato (290 caratteri) con testo evidenziato.

Amazon Kendra restituisce solo una risposta per documento, ossia la risposta con la massima confidenza. Per restituire più risposte da un documento, è necessario suddividere il documento in più documenti.

```
{
    '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'
}
```

Documento

Amazon Kendra restituisce i documenti classificati per quelli che corrispondono al termine di ricerca. La classifica si basa sulla fiducia che si Amazon Kendra ha nell'accuratezza del risultato della ricerca. Le informazioni sul documento corrispondente vengono restituite in QueryResultItem. Include il titolo del documento. L'estratto include le informazioni di evidenziazione per il testo di ricerca e la sezione del testo corrispondente nel documento. L'URI per la corrispondenza dei documenti si trova nell'attributo `SourceURI` document. L'esempio JSON seguente mostra il riepilogo del documento per un documento corrispondente.

```
{
    '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'
}
```

Domande e risposte

Una risposta a domanda e risposta viene restituita quando una domanda Amazon Kendra corrisponde a una delle domande frequenti nell'indice. La risposta include la domanda e la risposta corrispondenti nel QueryResultItemcampo. Include anche informazioni di evidenziazione per i termini di query rilevati nella stringa di query. Il codice JSON seguente mostra una domanda e una risposta. Nota che la risposta include il testo della domanda.

```
{
    '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?'
    }
}
```

Per informazioni sull'aggiunta del testo di domande e risposte a un indice, vedi Creazione di domande frequenti.

Ottimizzazione e ordinamento delle risposte

È possibile modificare l'effetto di un campo o di un attributo sulla pertinenza della ricerca tramite l'ottimizzazione della pertinenza. È inoltre possibile ordinare i risultati della ricerca in base a un determinato attributo o campo.

Argomenti

- Ottimizzazione delle risposte
- Ordinamento delle risposte

Ottimizzazione delle risposte

È possibile modificare l'effetto di un campo o di un attributo sulla pertinenza della ricerca tramite l'ottimizzazione della pertinenza. Per testare rapidamente l'ottimizzazione della pertinenza, utilizza l'API Query per inserire le configurazioni di ottimizzazione nella query. Potrai quindi visualizzare i

diversi risultati di ricerca che ottieni da diverse configurazioni. L'ottimizzazione della pertinenza a livello di query non è supportata nella console. È inoltre possibile ottimizzare campi o attributi di questo tipo solo `StringList` a livello di indice. Per ulteriori informazioni, consulta Ottimizzazione della pertinenza della ricerca.

Per impostazione predefinita, le risposte alle interrogazioni vengono ordinate in base al punteggio di pertinenza Amazon Kendra determinato per ogni risultato della risposta.

È possibile ottimizzare i risultati per qualsiasi attributo/campo integrato o personalizzato dei seguenti tipi:

- Valore della data
- Valore lungo
- Valore di stringa

Non è possibile ordinare gli attributi del tipo seguente:

- Valori dell'elenco di stringhe

Classizza e ottimizza i risultati dei documenti (AWS SDK)

Imposta il `Searchable` parametro su true per migliorare la configurazione dei metadati del documento.

Per ottimizzare un attributo in una query, impostate il `DocumentRelevanceOverrideConfigurations` parametro dell'`Query`API e specificate il nome dell'attributo da ottimizzare.

Il seguente esempio JSON mostra un `DocumentRelevanceOverrideConfigurations` oggetto che sovrascrive l'ottimizzazione dell'attributo chiamato «department» nell'indice.

```
"DocumentRelevanceOverrideConfigurations" : [
    "Name": "department",
    "Relevance": {
        "Importance": 1,
        "ValueImportanceMap": {
            "IT": 3,
            "HR": 7
        }
    }
```

```
]
```

Ordinamento delle risposte

Amazon Kendra utilizza l'attributo o il campo di ordinamento come parte dei criteri per i documenti restituiti dalla query. Ad esempio, i risultati restituiti da una query ordinata per «_created_at» potrebbero non contenere gli stessi risultati di una query ordinata per «_version».

Per impostazione predefinita, le risposte alle interrogazioni vengono ordinate in base al punteggio di pertinenza determinato per ogni risultato della risposta. Amazon Kendra Per modificare l'ordinamento, rendi ordinabile un attributo del documento e quindi configura l'utilizzo di tale attributo Amazon Kendra per ordinare le risposte.

È possibile ordinare i risultati su qualsiasi attributo/campo integrato o personalizzato dei seguenti tipi:

- Valore della data
- Valore lungo
- Valore di stringa

Non è possibile ordinare gli attributi del tipo seguente:

- Valori dell'elenco di stringhe

È possibile eseguire l'ordinamento in base a uno o più attributi del documento in ogni query. Le interrogazioni restituiscono 100 risultati. Se sono presenti meno di 100 documenti con l'attributo di ordinamento impostato, i documenti senza un valore per l'attributo di ordinamento vengono restituiti alla fine dei risultati, ordinati in base alla pertinenza rispetto alla query.

Per ordinare i risultati dei documenti (SDK)AWS

1. Per utilizzare l'UpdateIndexAPI per rendere ordinabile un attributo, imposta il `Sortable` parametro su. `true` Il seguente esempio JSON utilizza `DocumentMetadataConfigurationUpdates` per aggiungere un attributo chiamato «Department» all'indice e renderlo ordinabile.

   ```
   "DocumentMetadataConfigurationUpdates": [
      {
          "Name": "Department",
   ```

```
        "Type": "STRING_VALUE",
        "Search": {
            "Sortable": "true"
        }
    }
]
```

2. Per utilizzare un attributo ordinabile in una query, imposta il `SortingConfiguration` parametro dell'API Query. Specificate il nome dell'attributo da ordinare e se ordinare la risposta in ordine crescente o decrescente.

   L'esempio JSON seguente mostra il `SortingConfiguration` parametro utilizzato per ordinare i risultati di una query in base all'attributo «Department» in ordine crescente.

```
   "SortingConfiguration": {
      "DocumentAttributeKey": "Department",
      "SortOrder": "ASC"
   }
```

3. Per utilizzare più di un attributo ordinabile in una query, imposta il `SortingConfigurations` parametro dell'API Query. Puoi impostare fino a 3 campi in base ai Amazon Kendra quali ordinare i risultati. È inoltre possibile specificare se i risultati devono essere ordinati in ordine crescente o decrescente. La quota del campo di ordinamento può essere aumentata.

   Se non si fornisce una configurazione di ordinamento, i risultati vengono ordinati in base alla pertinenza che Amazon Kendra determina il risultato. In caso di parità nell'ordinamento dei risultati, i risultati vengono ordinati per rilevanza.

   L'esempio JSON seguente mostra il `SortingConfigurations` parametro utilizzato per ordinare i risultati di una query in base agli attributi «Nome» e «Prezzo» in ordine crescente.

```
"CollapseConfiguration" : {
    "DocumentAttributeKey": "Name",
    "SortingConfigurations": [
        {
            "DocumentAttributeKey": "Price",
            "SortOrder": "ASC"
        }
    ],
    "MissingAttributeKeyStrategy": "IGNORE"
}
```

Per ordinare i risultati del documento (console)

> **Note**
>
> L'ordinamento con più attributi non è attualmente supportato da. AWS Management Console

1. Per rendere un attributo ordinabile nella console, scegli Ordinabile nella definizione dell'attributo. È possibile rendere ordinabile un attributo al momento della creazione dell'attributo oppure modificarlo in un secondo momento.
2. Per ordinare la risposta a una query nella console, scegli l'attributo per ordinare la risposta dal menu Ordina. Nell'elenco vengono visualizzati solo gli attributi contrassegnati come ordinabili durante la configurazione dell'origine dati.

Comprimere/espandere i risultati delle interrogazioni

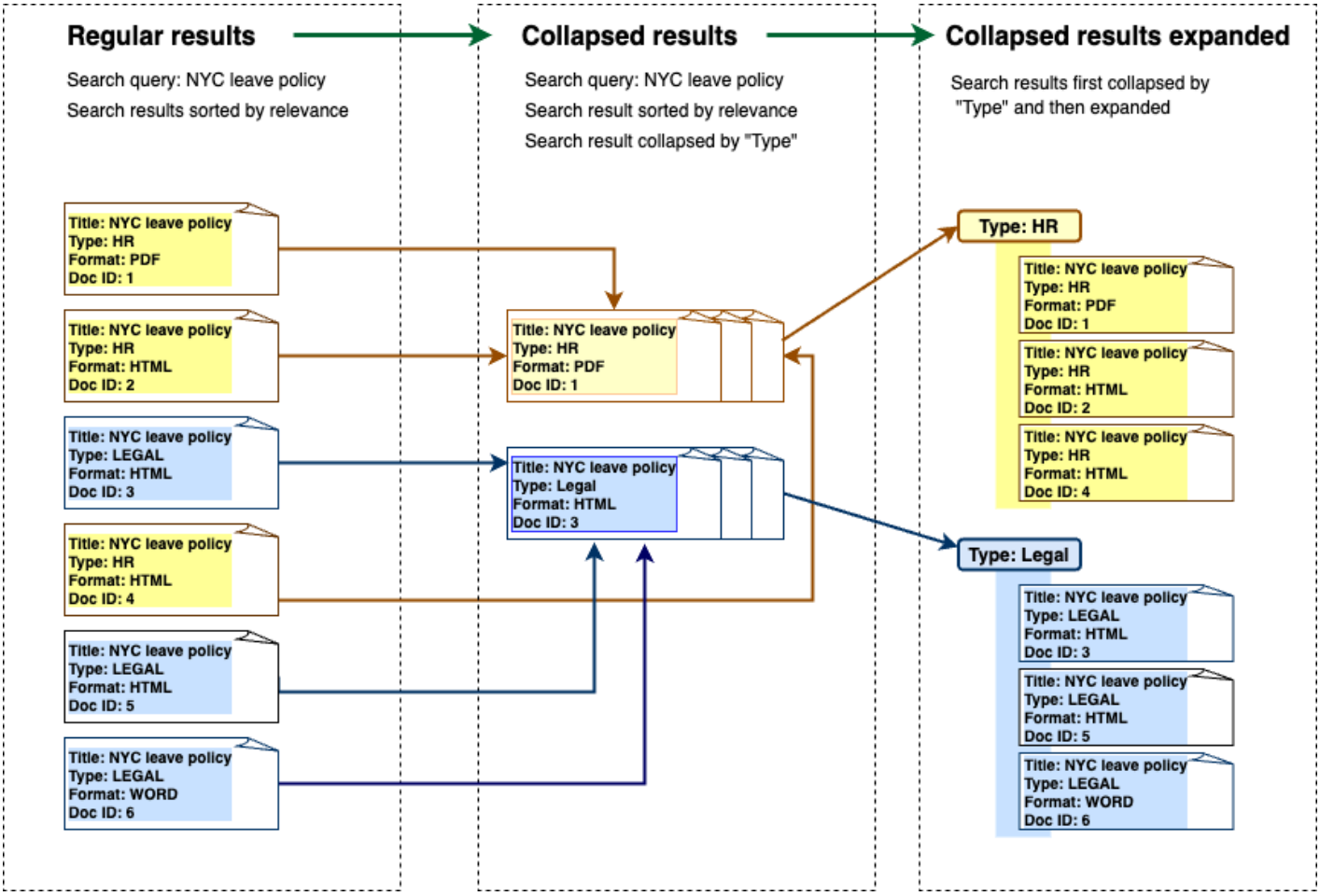
Quando ti connetti Amazon Kendra ai tuoi dati, esegue la scansione degli attributi dei metadati del documento, ad esempio`_document_title`, `e_created_at`, `_document_id` e utilizza questi attributi o campi per fornire funzionalità di ricerca avanzate durante la fase di interrogazione.

Amazon Kendra La funzionalità Comprimi ed espandi i risultati delle interrogazioni consente di raggruppare i risultati della ricerca utilizzando un attributo comune del documento e di visualizzarli, compressi o parzialmente espansi, in un documento principale designato.

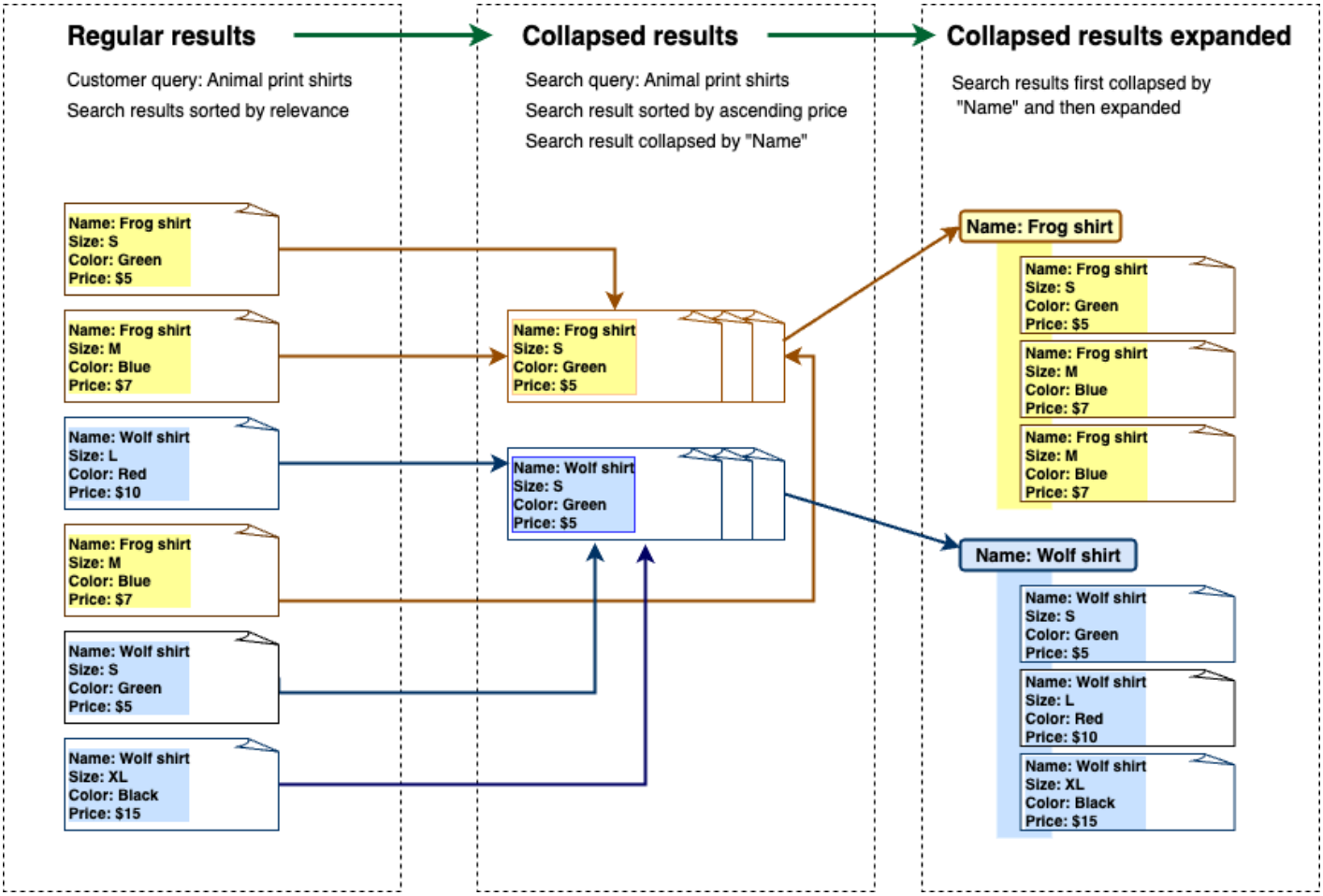
> **Note**
>
> La funzionalità di compressione ed espansione dei risultati delle query è attualmente disponibile solo tramite l'API.Amazon Kendra

Questa funzionalità è utile nei seguenti tipi di situazioni di ricerca:

- Nei documenti inclusi nell'indice esistono più versioni del contenuto. Quando l'utente finale interroga l'indice, desideri che visualizzi la versione più pertinente del documento con i duplicati nascosti/compressi. Ad esempio, se l'indice contiene più versioni di un documento denominato «Politica sui congedi di New York», puoi scegliere di comprimere i documenti per i gruppi specifici «HR» e «Legal» utilizzando l'attributo/campo «Tipo».



- L'indice contiene più documenti con informazioni uniche su un tipo di articolo o oggetto, ad esempio un inventario di prodotti. Per acquisire e ordinare comodamente le informazioni sugli articoli, è necessario che gli utenti finali accedano a tutti i documenti collegati da un elemento o oggetto come unico risultato di ricerca. Nell'esempio seguente, una ricerca effettuata da un cliente su «camicie con stampa animalier» restituisce risultati raggruppati per nome e ordinati per ordine di prezzo crescente.



Compressione dei risultati

Per raggruppare documenti simili o correlati, è necessario specificare l'attributo su cui comprimerli (ad esempio, è possibile comprimere/raggruppare documenti in base a). `_category` A tale scopo, chiamate l'API Query e utilizzate l'CollapseConfigurationoggetto per specificare su cui `DocumentAttributeKey` comprimere. I `DocumentAttributeKey` controlli in base ai quali campi verranno compressi i risultati della ricerca. I campi chiave degli attributi supportati includono `String` eNumber. `String liste` il `Date` tipo non sono supportati.

Scelta di un documento principale utilizzando l'ordinamento

Per configurare il documento principale da visualizzare per un gruppo compresso, utilizzate il `SortingConfigurations` parametro riportato di seguito. CollapseConfiguration Ad esempio, per ottenere la versione più recente di un documento, è necessario ordinare ogni gruppo compresso per. `_version` È possibile specificare fino a 3 attributi/campi in base ai quali ordinare e un criterio di

ordinamento per ogni attributo/campo utilizzato. `SortingConfigurations` È possibile richiedere un aumento della quota per il numero di attributi di ordinamento.

Per impostazione predefinita, Amazon Kendra ordina le risposte alle interrogazioni in base al punteggio di pertinenza determinato per ogni risultato della risposta. Per modificare l'ordinamento predefinito, rendi ordinabili gli attributi del documento e quindi configura l'utilizzo Amazon Kendra di questi attributi per ordinare le risposte. Per ulteriori informazioni, consulta Ordinamento delle risposte.

Strategia chiave del documento mancante

Se il documento non ha un valore per l'attributo di compressione, Amazon Kendra offre tre opzioni di personalizzazione:

- Scegli tra `COLLAPSE` tutti i documenti con valori nulli o mancanti in un unico gruppo. Questa è la configurazione predefinita.
- Scegli tra i `IGNORE` documenti con valori nulli o mancanti. I documenti ignorati non verranno visualizzati nei risultati delle query.
- Scegliete `EXPAND` ogni documento con un valore nullo o mancante in un gruppo a parte.

Espansione dei risultati

È possibile scegliere se i gruppi di risultati di ricerca compressi si espandono utilizzando il `Expand` parametro nell'CollapseConfigurationoggetto. I risultati espansi mantengono lo stesso ordinamento utilizzato per selezionare il documento principale per il gruppo.

Per configurare il numero di gruppi di risultati di ricerca compressi da espandere, utilizzate il `MaxResultItemstoExpand` parametro nell'ExpandConfigurationoggetto. Se impostate questo valore su 10, ad esempio, solo i primi 10 gruppi di risultati su 100 avranno la funzionalità di espansione.

Per configurare il numero di risultati espansi da mostrare per documento principale compresso, utilizzate il `MaxExpandResultsPerItem` parametro. Ad esempio, se imposti questo valore su 3, verranno visualizzati al massimo 3 risultati per gruppo compresso.

Interazioni con altre funzionalità Amazon Kendra

- La compressione e l'espansione dei risultati non modificano il numero di sfaccettature né influiscono sul numero totale di risultati visualizzati.

- Amazon Kendra i risultati di ricerca in evidenza non verranno compressi anche se hanno lo stesso valore di campo del campo di compressione configurato.
- La compressione e l'espansione dei risultati si applicano solo ai risultati di tipo. `DOCUMENT`

Ottimizzazione della pertinenza della ricerca

Amazon Kendra le query producono risultati di ricerca classificati in base alla loro pertinenza. I campi o gli attributi ricercabili presenti nell'indice contribuiscono tutti a questa classificazione.

È possibile modificare l'effetto di un campo o di un attributo sulla pertinenza della ricerca tramite l'ottimizzazione della pertinenza. L'ottimizzazione della pertinenza della ricerca può essere eseguita manualmente a livello di indice, dove si impostano le configurazioni di ottimizzazione per l'indice, oppure a livello di query sovrascrivendo le configurazioni impostate a livello di indice.

Quando si utilizza l'ottimizzazione della pertinenza, un risultato aumenta la risposta quando la query include termini che corrispondono al campo o all'attributo. È inoltre necessario specificare il livello di incremento che il documento riceve in caso di corrispondenza. L'ottimizzazione della pertinenza non comporta Amazon Kendra l'inclusione di un documento nella risposta alla query, ma è solo uno dei fattori Amazon Kendra utilizzati per determinare la pertinenza di un documento.

Puoi potenziare campi o attributi specifici nell'indice per assegnare maggiore importanza a risposte specifiche. Ad esempio, quando qualcuno cerca «When is re:Invent?» potresti aumentare l'importanza della freschezza dei documenti sul campo. `_last_update_at` Oppure, in un indice di rapporti di ricerca, potresti promuovere una fonte di dati specifica nel campo «fonte».

Puoi anche potenziare i documenti in base ai voti o al numero di visualizzazioni, cosa comune nei forum e in altre knowledge base di supporto. Puoi combinare i potenziamenti, ad esempio per aumentare i documenti visualizzati più spesso e quelli più recenti.

È possibile impostare la quantità di incremento che un documento riceve utilizzando il `Importance` parametro. Più è alto`Importance`, più il campo o l'attributo aumenta la pertinenza di un documento. Quando ottimizzi l'indice o esegui l'ottimizzazione a livello di query, aumenta il valore del `Importance` parametro in piccoli incrementi fino a ottenere l'effetto desiderato. Per determinare se stai migliorando i risultati della ricerca, esegui la ricerca e confronta i risultati con le query precedenti.

È possibile specificare attributi di data, numero o stringa per ottimizzare un indice o ottimizzarlo a livello di query. È possibile ottimizzare campi o attributi di questo tipo `StringList` solo a livello di indice. Ogni campo o attributo ha criteri specifici per determinare quando migliora un risultato.

- Campi o attributi data: esistono tre criteri specifici per i campi data,`Duration`, `Freshness` e. `RankOrder`

  - `Duration`imposta il periodo di tempo a cui si applica il boost. Ad esempio, se si imposta il periodo di tempo su 86400 secondi (ovvero un giorno), l'incremento inizia a diminuire dopo un giorno. Maggiore è l'importanza, più velocemente l'effetto boost diminuisce.
  - `Freshness`determina quanto è recente un documento quando viene applicato a un campo o a un attributo. Se si applica `Freshness` al campo per la data di creazione o la data dell'ultimo aggiornamento, un documento creato o aggiornato più di recente viene considerato «più recente» di un documento precedente. Ad esempio, se il documento 1 è stato creato il 14 novembre e il documento 2 è stato creato il 5 novembre, il documento 1 è «più recente» del documento 2. E se il documento 1 è stato aggiornato l'ultima volta il 14 novembre e il documento 2 è stato aggiornato l'ultima volta il 20 novembre, il documento 2 è «più fresco» del documento 1. Più il documento è fresco, più questa spinta viene applicata. Puoi avere solo un `Freshness` campo nel tuo indice.
  - `RankOrder`applica l'incremento in ordine crescente o decrescente. Se si specifica`ASCENDING`, le date successive hanno la precedenza. Se si specifica`DESCENDING`, le date precedenti hanno la precedenza.
- Campi o attributi numerici: per i campi o gli attributi numerici, è possibile specificare l'ordine di classificazione da Amazon Kendra utilizzare per determinare la pertinenza del campo o dell'attributo. Se si specifica`ASCENDING`, viene data la precedenza ai numeri più alti. Se si specifica`DESCENDING`, i numeri più bassi hanno la precedenza.
- Campi o attributi stringa: per i campi o gli attributi stringa, puoi creare categorie di un campo per dare a ciascuna categoria un impulso diverso. Ad esempio, se aumenti un campo o un attributo chiamato «Dipartimento», puoi dare un impulso diverso ai documenti di «Risorse Umane» rispetto ai documenti di «Legale». Puoi potenziare un campo o un attributo di questo tipo`String`. È possibile aumentare `StringList` i campi solo a livello di indice.

Regolazione della pertinenza a livello di indice

È possibile ottimizzare la pertinenza di un campo o di un attributo a livello di indice utilizzando la console per impostare l'ottimizzazione dei dettagli dell'indice o l'API. UpdateIndex

L'esempio seguente imposta il `_last_updated_at` campo come `Freshness` campo per un documento.

```
"DocumentMetadataConfigurationUpdates" : [
    {
        "Name": "_last_updated_at",
```

```
        "Type": "DATE_VALUE",
        "Relevance": {
            "Freshness": TRUE,
            "Importance": 2
        }
    }
]
```

L'esempio seguente attribuisce un'importanza diversa alle diverse categorie nel campo «reparto».

```
"DocumentMetadataConfigurationUpdates" : [
    {
        "Name": "department",
        "Type": "STRING_VALUE",
        "Relevance": {
            "Importance": 2,
            "ValueImportanceMap": {
                "HR": 3,
                "Legal": 1
            }
        }
    }
]
```

Ottimizzazione della pertinenza a livello di query

È possibile ottimizzare la pertinenza di un campo o di un attributo a livello di query utilizzando l'API Query.

L'ottimizzazione della pertinenza a livello di query non è supportata nella console.

L'ottimizzazione a livello di query può velocizzare il processo di ottimizzazione della pertinenza dei test, poiché non è necessario aggiornare manualmente le configurazioni di ottimizzazione nell'indice per ogni test. È possibile ottimizzare la pertinenza di un documento inserendo le configurazioni di ottimizzazione nella query. Quindi puoi vedere i diversi risultati che ottieni da diverse configurazioni. Una configurazione passata nella query ha la precedenza sulla configurazione impostata a livello di indice.

L'esempio seguente sostituisce l'importanza applicata al campo «dipartimento» e a ogni categoria di reparto impostata a livello di indice, mostrata nell'esempio precedente. Quando un utente inserisce la

propria query di ricerca, il campo «dipartimento» ha un discreto livello di importanza e l'Ufficio legale ha più importanza del dipartimento delle risorse umane.

```
"DocumentRelevanceOverrideConfigurations" : [
    {
        "Name": "department",
        "Type": "STRING_VALUE",
        "Relevance": {
            "Importance": 2,
            "ValueImportanceMap": {
                "HR": 2,
                "Legal": 8
            }
        }
    }
]
```

Ottenere informazioni dettagliate con l'analisi delle ricerche

Puoi utilizzare Amazon Kendra Search Analytics per ottenere informazioni dettagliate su come l'applicazione di ricerca aiuta con successo o meno gli utenti a trovare informazioni.

Amazon Kendra L'analisi fornisce un'istantanea del modo in cui gli utenti interagiscono con l'applicazione di ricerca e dell'efficacia della configurazione dell'applicazione di ricerca. Puoi visualizzare i dati delle metriche utilizzando l'GetSnapshotsAPI o selezionando Analytics nel pannello di navigazione della console.

Puoi eseguire il rendering dei dati generati da `GetSnapshots` sulla tua dashboard personalizzata. Oppure puoi utilizzare la dashboard delle metriche fornita nella console, che include grafici visivi. Con una dashboard visiva, puoi cercare tendenze o modelli nel comportamento degli utenti nel tempo o far emergere problemi con la configurazione dell'applicazione di ricerca. Ad esempio, un grafico a linee che mostra un numero costante di query al giorno e un aumento costante potrebbe indicare un aumento dell'adozione e dell'utilizzo. D'altra parte, un calo improvviso potrebbe indicare che c'è un problema che deve essere esaminato.

Puoi utilizzare le metriche per stabilire connessioni tra diversi punti di dati per risolvere problemi relativi al modo in cui gli utenti richiedono informazioni o scoprono opportunità di business. Ad esempio, il documento «How does AI work?» è il documento più cliccato nei risultati di ricerca e la query più cercata è «Come funziona l'apprendimento automatico?». Questo ti informa sui termini e sulla lingua preferiti utilizzati dai tuoi utenti. Puoi integrare questi termini nei tuoi documenti o utilizzare sinonimi personalizzati per questi termini per rendere i documenti più ricercabili per gli utenti.

Metriche per la ricerca

Sono disponibili 10 metriche per analizzare le prestazioni dell'applicazione di ricerca o le informazioni che gli utenti stanno cercando. Per recuperare i dati delle metriche, specificate il nome della stringa dei dati metrici che desiderate recuperare quando chiamate. `GetSnapshots`

È inoltre necessario fornire un intervallo di tempo o una finestra temporale per visualizzare i dati delle metriche. L'intervallo di tempo utilizza il fuso orario dell'indice. È possibile visualizzare i dati nelle seguenti finestre temporali:

- `THIS_WEEK`: La settimana corrente, che inizia la domenica e termina il giorno precedente alla data corrente.

- `ONE_WEEK_AGO`: La settimana precedente, che inizia la domenica e termina il sabato successivo.
- `TWO_WEEKS_AGO`: La settimana precedente, con inizio la domenica e termine il sabato successivo.
- `THIS_MONTH`: Il mese corrente, che inizia il primo giorno del mese e termina il giorno precedente la data corrente.
- `ONE_MONTH_AGO`: Il mese precedente, che inizia il primo giorno del mese e termina l'ultimo giorno del mese.
- `TWO_MONTHS_AGO`: Il mese precedente al mese precedente, che inizia il primo giorno del mese e termina l'ultimo giorno del mese.

Nella console, le finestre orarie supportate sono Questa settimana, Settimana precedente, Questo mese, Mese precedente.

Percentuale di clic

La percentuale di interrogazioni che portano a fare clic su un documento nei risultati di ricerca. Ciò consente di capire se la configurazione dell'applicazione di ricerca aiuta gli utenti a trovare informazioni pertinenti alle loro ricerche. Per le query che restituiscono risposte immediate, gli utenti potrebbero non aver bisogno di fare clic su un documento per ulteriori informazioni. Per ulteriori informazioni, consulta the section called “Percentuale di risposta istantanea”. È necessario chiamare SubmitFeedbackper assicurarsi che venga raccolto il feedback tramite clic.

Per recuperare i dati sulla percentuale di clic utilizzando l'API, specifica as. `GetSnapshots` `metricType` `AGG_QUERY_DOC_METRICS` Puoi anche visualizzare questa metrica nella console selezionando Analytics nel pannello di navigazione.

Frequenza di clic pari a zero

La percentuale di query che portano a zero clic nei risultati della ricerca. Questo ti aiuta a comprendere le lacune nei tuoi contenuti che forniscono risultati di ricerca non pertinenti. Per le query che restituiscono risposte immediate, gli utenti potrebbero non aver bisogno di fare clic su un documento per ulteriori informazioni. Per ulteriori informazioni, consulta the section called “Percentuale di risposta istantanea”. Inoltre, le impostazioni di ricerca, come l'ottimizzazione delle configurazioni, potrebbero avere un impatto sul modo in cui i documenti vengono restituiti nei risultati della ricerca.

Per recuperare dati con una percentuale di clic pari a zero utilizzando l'`GetSnapshots`API, specifica as. `metricType` `AGG_QUERY_DOC_METRICS` Puoi anche visualizzare questa metrica nella console selezionando Analytics nel pannello di navigazione.

Tasso di risultati di ricerca pari a zero

La percentuale di query che portano a zero risultati di ricerca. Questo ti aiuta a comprendere le lacune nei tuoi contenuti senza fornire risultati di ricerca pertinenti.

Per recuperare i dati sulla percentuale di risultati di ricerca pari a zero utilizzando l'`GetSnapshots`API, specifica as. `metricType` `AGG_QUERY_DOC_METRICS` Puoi anche visualizzare questa metrica nella console selezionando Analytics nel pannello di navigazione.

Percentuale di risposta istantanea

La percentuale di domande con risposta immediata o domande frequenti restituite. Questo ti aiuta a comprendere il ruolo delle risposte istantanee nella fornitura di informazioni.

Per recuperare i dati sulla percentuale di risposta istantanea utilizzando l'`GetSnapshots`API, specifica `metricType` as`AGG_QUERY_DOC_METRICS`. Puoi anche visualizzare questa metrica nella console selezionando Analytics nel pannello di navigazione.

Le domande più frequenti

Le 100 principali query ricercate dai tuoi utenti. Questo ti aiuta a capire quali sono le query più popolari e il tipo di informazioni a cui i tuoi utenti sono maggiormente interessati.

Le metriche includono il numero di volte in cui viene effettuata la ricerca nella query, la percentuale di clic su un documento, la percentuale di clic non effettuati su un documento, la profondità media di clic nei risultati di ricerca per la query, la percentuale di risposte istantanee alla query e l'affidabilità media dei primi 10 risultati di ricerca per una query.

Per recuperare i dati sulle query principali utilizzando l'API, specifica as. `GetSnapshots` `metricType` `QUERIES_BY_COUNT` Puoi anche visualizzare questa metrica nella console selezionando Analytics nel pannello di navigazione della console, quindi selezionando Prime query in Elenchi di query.

Le principali query con zero clic

Le 100 principali query che hanno portato a zero clic nei risultati di ricerca. Questo ti aiuta a comprendere eventuali lacune nei tuoi contenuti, dovute alla mancanza di documenti pertinenti

ad alcune query o alla configurazione dell'applicazione di ricerca che restituisce risultati di ricerca irrilevanti. Per le query che restituiscono risposte immediate, potrebbe non essere necessario che gli utenti facciano clic su un documento per ottenere ulteriori informazioni. Per ulteriori informazioni, consulta the section called “Percentuale di risposta istantanea”.

Le metriche includono il numero di volte in cui la query porta a zero clic, la percentuale di zero clic per la query, la percentuale di risposte istantanee per la query e l'affidabilità media dei primi 10 risultati di ricerca per una query.

Per recuperare i dati sulle query principali con zero clic utilizzando l'`GetSnapshots`API, specifica as. `metricType` `QUERIES_BY_ZERO_CLICK_RATE` Puoi anche visualizzare questa metrica nella console selezionando Analytics nel pannello di navigazione della console, quindi selezionando Prime query a zero clic in Elenchi di query.

Query principali con zero risultati di ricerca

Le 100 principali query che hanno portato a zero risultati di ricerca. Questo ti aiuta a comprendere eventuali lacune nei tuoi contenuti, laddove non ci sono documenti pertinenti per alcune domande. In alternativa, i tuoi utenti potrebbero utilizzare termini specializzati che potrebbero non portare a risultati di ricerca, richiedendoti di creare sinonimi personalizzati per gestire questa situazione.

Le metriche includono il numero di volte in cui la query porta a zero risultati di ricerca, la percentuale di zero risultati di ricerca per la query e la proporzione di volte in cui la query viene cercata rispetto a tutte le query.

Per recuperare i dati sulle query principali con zero risultati di ricerca utilizzando l'`GetSnapshots`API, specifica as. `metricType` `QUERIES_BY_ZERO_RESULT_RATE` Puoi anche visualizzare questa metrica nella console selezionando Analytics nel pannello di navigazione della console, quindi selezionando Query con i primi zero risultati in Elenchi di query.

I documenti sono stati cliccati in alto

I primi 100 documenti più cliccati nei risultati di ricerca. Questo ti aiuta a capire quali documenti o risultati di ricerca sono più pertinenti per i tuoi utenti quando richiedono informazioni.

Le metriche includono il numero di volte in cui si fa clic sul documento, il numero di Mi piace che un documento riceve dagli utenti (pollice rivolto verso l'alto), il numero di «Mi piace» che un documento riceve dagli utenti (pollice rivolto verso il basso).

Per recuperare i dati sui documenti più cliccati utilizzando l'API, specifica as. `GetSnapshots` `metricType` `DOCS_BY_CLICK_COUNT` Puoi anche visualizzare questa metrica nella console selezionando Analytics nel pannello di navigazione della console, quindi selezionando Documenti più cliccati in Elenchi Query.

Interrogazioni totali

Il numero totale di query ricercate dai tuoi utenti. Questo ti aiuta a capire il livello di coinvolgimento degli utenti con la tua applicazione di ricerca.

Per recuperare i dati sul totale delle query utilizzando l'`GetSnapshots`API, specifica as. `metricType` `AGG_QUERY_DOC_METRICS` Puoi anche visualizzare questa metrica nella console selezionando Analytics nel pannello di navigazione.

Documenti totali

Il numero totale di documenti presenti nell'indice. Ciò consente di confrontare la dimensione dell'indice con il numero totale di query per verificare se esiste un numero di documenti appropriato per il volume di query.

Per recuperare i dati sul totale dei documenti utilizzando l'`GetSnapshots`API, specifica as. `metricType` `AGG_QUERY_DOC_METRICS` Puoi anche visualizzare questa metrica nella console selezionando Analytics nel pannello di navigazione.

Esempio di recupero dei dati metrici

Il codice seguente è un esempio di recupero dei dati sulle principali query del mese precedente.

Console

Per recuperare le query principali del mese precedente

1. Nel riquadro di navigazione a sinistra, in Indici, seleziona l'indice, quindi seleziona Analytics.
2. Nella pagina Analytics, seleziona il pulsante Questa settimana per modificare la finestra temporale per il recupero dei dati impostandola su Mese precedente.
3. Nella pagina Analytics, in Elenchi di query, seleziona Query principali.

CLI

Per recuperare le query principali del mese precedente

```
aws kendra get-snapshots \
--index-id index-id \
--interval "ONE_MONTH_AGO" \
--metric-type "QUERIES_BY_COUNT"
```

Python

Per recuperare le query principali del mese precedente

```
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

Per recuperare le query principali del mese precedente

```
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()))
```

Dalle metriche agli approfondimenti utilizzabili

Le informazioni fruibili sono informazioni significative estratte da dati grezzi e vengono utilizzate per guidare le azioni o le decisioni. Per estrarre significato dalle metriche e utilizzarle per ottenere informazioni fruibili, è importante non solo esaminare le metriche in modo isolato, ma anche stabilire connessioni tra le metriche.

Ad esempio, la query principale con zero clic è «Quali aree sono attualmente disponibili?». Tuttavia, ha anche un tasso di risposta istantanea del 100%. Ciò suggerisce che gli utenti ricevano la risposta a questa domanda senza dover fare clic su un risultato di ricerca o su un documento che fornisce informazioni sulle aree disponibili. Se si considerasse solo l'utilizzo di zero clic, non si capirebbe la storia completa e si potrebbero trarre conclusioni errate sul successo della configurazione dell'applicazione di ricerca nella gestione di questa query.

Un altro esempio di intuizione utilizzabile è la scoperta di un'opportunità di business. Le aziende spesso cercano opportunità per far crescere i propri clienti analizzando le metriche di ricerca. Il documento più cliccato è «Regioni disponibili». Inoltre, la maggior parte delle domande più ricercate riguarda domande sulla disponibilità dei prodotti nella regione dell'Oceania, con percentuali di risposta istantanea del 100% e un'elevata percentuale di clic per ulteriori informazioni sulle regioni disponibili come parte della risposta. Ciò indica che c'è interesse e domanda per il tuo prodotto o servizio in questa regione.

Visualizzazione e segnalazione delle analisi di ricerca

Esistono cinque metriche che includono dati sulle tendenze che puoi visualizzare e cercare tendenze o modelli nel tempo. Se utilizzi la console, vengono forniti grafici dei dati sulle tendenze. Se utilizzi

le API, puoi recuperare i dati sulle tendenze per creare grafici o visualizzazioni personalizzati. La maggior parte dei grafici nella console riporta i punti dati giornalieri nella finestra temporale prescelta.

La console fornisce una dashboard delle metriche in cui puoi selezionare un grafico e un elenco principale che desideri visualizzare. Puoi esportare le metriche mostrate nella dashboard in formato CSV selezionando Esporta nella home page di Analytics. Puoi includere questi report nei tuoi documenti o presentazioni aziendali.

Puoi visualizzare le seguenti metriche:

Grafico delle interrogazioni totali

Un grafico a linee del numero di interrogazioni emesse ogni giorno. Il grafico ti aiuta a visualizzare i modelli di coinvolgimento quotidiano degli utenti. Alcuni esempi includono un aumento o una diminuzione costante del coinvolgimento degli utenti o un drastico calo a 0 domande a causa di un arresto anomalo dell'applicazione di ricerca o di problemi con il sito web.

Se utilizzi l'API, puoi recuperare questi dati specificando. `TREND_QUERY_DOC_METRICS` È possibile utilizzare i dati per creare grafici personalizzati o utilizzare i grafici forniti nella console.

Grafico della frequenza di clic

Un grafico a linee delle proporzioni di clic al giorno. Il grafico consente di visualizzare i modelli relativi alla percentuale di clic giornaliera. Alcuni esempi includono un aumento o una diminuzione costante della percentuale di clic o una diminuzione delle risposte istantanee che potrebbe influenzare un aumento della percentuale di clic.

Se utilizzi l'API, puoi recuperare questi dati specificando. `TREND_QUERY_DOC_METRICS` È possibile utilizzare i dati per creare grafici personalizzati o utilizzare i grafici forniti nella console.

Grafico della frequenza di clic pari a zero

Un grafico a linee della proporzione di zero clic al giorno. Il grafico ti aiuta a visualizzare i modelli con una percentuale di clic giornaliera pari a zero. Alcuni esempi includono un aumento o una diminuzione costante della percentuale di clic pari a zero o un aumento delle risposte istantanee che potrebbe influenzare un aumento della percentuale di clic pari a zero.

Se utilizzi l'API, puoi recuperare questi dati specificando. `TREND_QUERY_DOC_METRICS` È possibile utilizzare i dati per creare grafici personalizzati o utilizzare i grafici forniti nella console.

Grafico del tasso di zero risultati di ricerca

Un grafico a linee della percentuale di zero risultati di ricerca al giorno. Il grafico ti aiuta a visualizzare i modelli con una percentuale giornaliera pari a zero risultati di ricerca. Alcuni esempi includono un aumento o una diminuzione costante della percentuale di risultati di ricerca pari a zero oppure una forte diminuzione del numero di documenti nell'indice, che potrebbe influenzare un aumento della percentuale di zero risultati di ricerca.

Se utilizzi l'API, puoi recuperare questi dati specificando. `TREND_QUERY_DOC_METRICS` È possibile utilizzare i dati per creare grafici personalizzati o utilizzare i grafici forniti nella console.

Grafico del tasso di risposta istantaneo

Un grafico a linee della percentuale di domande con risposta immediata o domande frequenti restituite. Il grafico consente di visualizzare i modelli relativi alla percentuale di risposta istantanea giornaliera. Alcuni esempi includono un aumento o una diminuzione costante delle domande di tipo domanda-risposta o una diminuzione dei clic che potrebbe influenzare un aumento delle risposte istantanee.

Se utilizzi l'API, puoi recuperare questi dati specificando. `TREND_QUERY_DOC_METRICS` È possibile utilizzare i dati per creare grafici personalizzati o utilizzare i grafici forniti nella console.

Invio di feedback per l'apprendimento incrementale

Amazon Kendra utilizza l'apprendimento incrementale per migliorare i risultati di ricerca. Utilizzando il feedback delle query, l'apprendimento incrementale migliora gli algoritmi di classificazione e ottimizza i risultati di ricerca per una maggiore precisione.

Ad esempio, supponiamo che gli utenti cerchino la frase «prestazioni sanitarie». Se gli utenti scelgono sempre il secondo risultato dall'elenco, col Amazon Kendra tempo il risultato passa al primo posto. L'incremento diminuisce nel tempo, quindi se gli utenti smettono di selezionare un risultato, Amazon Kendra alla fine lo rimuove e mostra invece un altro risultato più popolare. Questo aiuta a Amazon Kendra dare priorità ai risultati in base alla pertinenza, all'età e al contenuto.

L'apprendimento incrementale è attivato per tutti gli indici e per tutti i tipi di documenti supportati.

Amazon Kendra inizia ad apprendere non appena fornisci un feedback, anche se possono essere necessarie più di 24 ore per vedere i risultati del feedback. Amazon Kendra offre tre metodi per inviare feedback: la AWS console, una JavaScript libreria che puoi includere nella pagina dei risultati di ricerca e un'API che puoi utilizzare.

Amazon Kendra accetta due tipi di feedback degli utenti:

- Clic: informazioni sui risultati della query scelti dall'utente. Il feedback include l'ID del risultato e il timestamp Unix della data e dell'ora in cui è stato scelto il risultato della ricerca.

  Per inviare feedback sui clic, l'applicazione deve raccogliere informazioni sui clic relative alle attività degli utenti e quindi inviare tali informazioni a. Amazon Kendra Puoi raccogliere informazioni sui clic con la console, la JavaScript libreria e l' Amazon Kendra API.
- Rilevanza: informazioni sulla pertinenza di un risultato di ricerca, fornite in genere dall'utente. Il feedback contiene l'ID del risultato e un indicatore di pertinenza (o). `RELEVANT` `NOT_RELEVANT` L'utente determina le informazioni pertinenti.

  Per inviare un feedback sulla pertinenza, l'applicazione deve fornire un meccanismo di feedback che consenta all'utente di scegliere la pertinenza appropriata per il risultato di una query e quindi inviare tali informazioni a. Amazon Kendra Puoi raccogliere informazioni pertinenti solo con la console e l'API. Amazon Kendra

Il feedback viene utilizzato mentre l'indice è attivo. Il feedback riguarda solo l'indice a cui è stato inviato, non può essere utilizzato su più indici o per account diversi.

È necessario fornire un contesto utente aggiuntivo quando si esegue una query Amazon Kendra sull'indice. Quando fornisci il contesto dell'utente, Amazon Kendra è in grado di stabilire se il feedback è fornito da un singolo utente o da più utenti e di modificare i risultati della ricerca di conseguenza.

Quando si fornisce un contesto all'utente, il feedback relativo alla query viene associato all'utente specifico fornito nel contesto. Se non specifichi il contesto utente, puoi fornire un ID visitatore da utilizzare per raggruppare e aggregare le query.

Se non fornisci un contesto utente o un ID visitatore, il feedback è anonimo e aggregato con altri feedback anonimi.

Il codice seguente mostra come includere il contesto utente come token o ID visitatore.

```
response = kendra.query(
    QueryText = query,
    IndexId = index,
    UserToken = {
        Token = "token"
    })

    OR

    response = kendra.query(
    QueryText = query,
    IndexId = index,
    VisitorId = "visitor-id")
```

Per le applicazioni Web, puoi utilizzare cookie, posizioni o utenti del browser per generare un ID visitatore per ogni utente.

Per quanto riguarda le domande dirette, che rappresentano il maggior volume di richieste, il feedback tramite clic fornisce informazioni sufficienti per migliorare la precisione complessiva. Per quanto riguarda le domande secondarie, quelle rare, gli esperti in materia dovrebbero inviare feedback pertinenti e non pertinenti per migliorarne la precisione.

Oltre alla console, puoi utilizzare uno dei due metodi seguenti: una JavaScript libreria o l'API. SubmitFeedback È necessario utilizzare un solo metodo per raccogliere feedback. Per ottenere risultati ottimali, è necessario inviare il feedback entro 24 ore dalla richiesta.

Argomenti

Utilizzo della Amazon Kendra JavaScript libreria per inviare feedback

Amazon Kendra fornisce una JavaScript libreria che puoi utilizzare per aggiungere feedback sui clic alla pagina dei risultati di ricerca. Per utilizzare la libreria, inserite un tag script nel codice client che visualizza i risultati della ricerca, quindi aggiungete informazioni a ciascuno dei link ai documenti nell'elenco dei risultati. Quando un utente sceglie un link per visualizzare un documento, le informazioni sui clic vengono inviate a Amazon Kendra.

La libreria funziona con i browser che supportano la JavaScript versione ES6/ES2015.

Passaggio 1: inserisci un tag script nell'applicazione di ricerca Amazon Kendra

Nel codice client che visualizza i risultati della Amazon Kendra ricerca, inserisci un <script>tag e aggiungi un riferimento alla JavaScript libreria:

```
<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>
```

Lo script scarica in modo asincrono la JavaScript libreria da un CDN Amazon Kendra ospitato e inizializza una variabile globale chiamata `kendraFeedback` che consente di impostare parametri opzionali.

Sostituisci *`l'URL di download della libreria e l'endpoint di feedback`* con un identificatore della tabella seguente in base alla regione che ospita l'indice. Amazon Kendra

Regione	Scarica il URL	Endpoint di feedback
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
ap-southeast-2	https://dopqntoe6z0ce.cloudfront.net/ksf-v1.js	https://oovf4nvjj7.execute-api.ap-southeast-2.amazonaws.com/prod/submit

Regione	Scarica il URL	Endpoint di feedback
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

Ad esempio, se l'indice si trova negli Stati Uniti orientali (Virginia settentrionale), *l'URL di download della libreria* è `https://d2zm0lpns956f8.cloudfront.net/ksf-v1.js` e l'*endpoint di feedback* è. `https://ujxwp5s92h.execute-api.us-east-1.amazonaws.com/prod/submit`

È possibile configurare due impostazioni opzionali per la Amazon Kendra JavaScript libreria:

- `disableCookies`— Per impostazione predefinita, Amazon Kendra imposta un cookie che identifica in modo univoco l'utente. Impostalo per `true` disabilitare il cookie.

  ```
  kendraFeedback('disableCookie', 'true | false');
  ```

  `searchDivClassName`— Per impostazione predefinita, Amazon Kendra monitora i clic su tutti i link nella pagina dei risultati di ricerca. Impostalo su un nome `<div>` di classe per monitorare solo i link nella classe specificata.

  ```
  kendraFeedback('searchDivClassName', 'class name');
  ```

Passaggio 2: aggiungi il token di feedback ai risultati della ricerca

Nella pagina dei risultati, aggiungi un attributo HTML chiamato `data-kendra-token` al tag anchor o al tag div principale immediato che contiene un link al documento dalla risposta alla query. Per esempio:

```
<a href="document location" data-kendra-token="feedback token value"></a>
OR
<div data-url="document location" data-kendra-token="feedback token value"></div>
```

Una risposta alla query contiene un token nel `feedbackToken` campo. Il token identifica in modo univoco la risposta se l'utente la sceglie. Assegna il valore del token all'attributo. `data-kendra-token` La Amazon Kendra JavaScript libreria cerca questo token quando l'utente sceglie il risultato e lo invia a un Amazon Kendra endpoint come feedback.

La Amazon Kendra JavaScript libreria invia solo il token di feedback e altri metadati, come l'ora in cui è stato scelto il risultato e un ID visitatore univoco.

Fase 3: Prova lo script di feedback

Per assicurarti che la JavaScript libreria sia configurata correttamente e che invii il feedback all'endpoint corretto, procedi come segue. Questo esempio utilizza il browser Chrome.

1. Apri gli strumenti per sviluppatori Web nel browser. Su Chrome, apri il menu Chrome nell'angolo in alto a destra del browser, scegli Altri strumenti, quindi scegli Strumenti per sviluppatori.
2. Assicurati che non vi siano errori relativi alla Amazon Kendra JavaScript libreria nella scheda della console.
3. Effettua una ricerca e scegli un risultato qualsiasi. Nella scheda Rete degli strumenti per sviluppatori. Dovresti vedere una richiesta inviata all'endpoint di feedback, il token del risultato e lo stato 200 OK.

Utilizzo dell' Amazon Kendra API per inviare feedback

Per utilizzare l' Amazon Kendra API per inviare feedback sulle query, utilizza l'SubmitFeedbackAPI. Per identificare la query, fornisci l'ID di indice dell'indice a cui si riferisce la query e l'ID della query restituito nella risposta dall'API Query.

L'esempio seguente mostra come inviare feedback su clic e pertinenza utilizzando l' Amazon Kendra API. È possibile inviare più set di feedback tramite gli `RelevanceFeedbackItems` array `ClickFeedbackItems` and. Questo esempio invia un solo clic e un singolo elemento di feedback pertinente. L'invio del feedback utilizza l'ora corrente.

Per inviare feedback per una ricerca (AWS SDK)

1. Puoi utilizzare il seguente codice di esempio con i valori richiesti:

   a. `index id`: l'ID dell'indice a cui si applica la query.

   b. `query id`—La query su cui si desidera fornire un feedback.

   c. `result id`—L'ID del risultato della query su cui desideri fornire un feedback. La risposta alla query contiene l'ID del risultato.

   d. `relevance value`—O `RELEVANT` (il risultato della query è rilevante) o `NOT_RELEVANT` (il risultato dell'interrogazione non è rilevante).

   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. Eseguire il codice. Dopo l'invio del feedback, il codice visualizza un messaggio.

Aggiungere sinonimi personalizzati a un indice

Per aggiungere sinonimi personalizzati a un indice, è necessario specificarli in un file del thesaurus. Nell'uso dei sinonimi è possibile includere termini aziendali specifici o specialistici. Amazon Kendra I sinonimi generici in inglese, ad esempio`leader, head`, sono incorporati Amazon Kendra e non devono essere inclusi in un file del thesaurus, compresi i sinonimi generici che utilizzano trattini. Amazon Kendra supporta i sinonimi per tutti i tipi di risposta, che includono i tipi di `DOCUMENT` risposta e/o i tipi di risposta. `QUESTION_ANSWER` `ANSWER` Amazon Kendra attualmente non supporta l'aggiunta di sinonimi contrassegnati come stopword. Questo sarà incluso in una versione futura.

Amazon Kendra crea correlazioni tra sinonimi. Ad esempio, utilizzando la coppia di sinonimi`Dynamo, Amazon DynamoDB`, Amazon Kendra correla Dynamo con. Amazon DynamoDB La domanda «Cos'è la dinamo?» quindi restituisce un documento come «Che cos'è Amazon DynamoDB?». Con i sinonimi, Amazon Kendra è possibile rilevare più facilmente la correlazione.

Il file del thesaurus è un file di testo memorizzato in un bucket. Amazon S3 Per informazioni, consulta Aggiungere un thesaurus a un indice.

Il file del thesaurus utilizza il formato dei sinonimi Solr. Amazon Kendra ha un limite al numero di thesauri per indice. Consulta l'argomento Quote.

I sinonimi possono essere utili nei seguenti scenari:

- Termini specializzati che non sono sinonimi tradizionali della lingua inglese come`NLP, Natural Language Processing`.
- Nomi propri con associazioni semantiche complesse. Si tratta di sostantivi che è improbabile che il grande pubblico comprenda, ad esempio, nell'apprendimento automatico,. `cost, loss, model performance`
- Diverse forme di nomi di prodotto, ad esempio,. `Elastic Compute Cloud, EC2`
- Termini specifici del dominio o dell'azienda, come i nomi dei prodotti. Ad esempio, `Route53, DNS`.

Non utilizzare sinonimi nei seguenti scenari:

- Sinonimi generici in lingua inglese come`leader, head`. Questi sinonimi non sono specifici del dominio e l'utilizzo di sinonimi in questi scenari potrebbe avere effetti indesiderati.
- Errori tipografici come. `teh => the`

- Varianti morfologiche come i plurali e i possessivi dei sostantivi, la forma comparativa e superlativa degli aggettivi e il passato, il participio passato e la forma progressiva dei verbi. Un esempio di `good, better, best` aggettivi comparativi e superlativi è.
- Unigram (parola singola) interrompono parole come. `WHO` Le interruzioni Unigram non sono consentite nel thesaurus e sono escluse dalla ricerca. Ad esempio, viene rifiutato. `WHO => World Health Organization` È possibile utilizzare `W.H.O.` tuttavia come termine sinonimo e interrompere le parole chiave come parte di un sinonimo composto da più parole. Ad esempio, non `of` è consentito ma `United States of America` è accettato.

I sinonimi personalizzati facilitano la comprensione Amazon Kendra della terminologia specifica dell'azienda, ampliando le query per includere i sinonimi specifici dell'azienda. Sebbene i sinonimi possano migliorare la precisione della ricerca, è importante capire in che modo i sinonimi influiscono sulla latenza in modo da poterla ottimizzare.

Una regola generale per i sinonimi è: maggiore è il numero di termini nella query che vengono abbinati e ampliati con sinonimi, maggiore è il potenziale impatto sulla latenza. Altri fattori che influiscono sulla latenza includono la dimensione media dei documenti indicizzati, la dimensione dell'indice, qualsiasi filtro sui risultati di ricerca e il carico complessivo dell'indice. Amazon Kendra Le query che non corrispondono ad alcun sinonimo non sono interessate.

Una linea guida generale su come i sinonimi influiscono sulla latenza:

Caso d'uso	Aumento della latenza*
Tipiche query in linguaggio naturale o con parole chiave composte da 3 a 5 parole ciascuna	Meno del 15 percento
1 termine di ricerca si espande a 3 sinonimi	
Indice di circa 500.000 documenti (con una media di 10,48 KB di testo estratto per documento) o 30.000 coppie di domande e domande	

* Le prestazioni variano in base all'uso specifico dei sinonimi e delle configurazioni dell'indice. È consigliabile testare le prestazioni di ricerca per ottenere benchmark più accurati per il caso d'uso specifico.

Se il thesaurus è di grandi dimensioni, ha un rapporto di espansione a lungo termine elevato e l'aumento della latenza non rientra nei limiti accettabili, potete provare una o entrambe le seguenti soluzioni:

- Taglia il thesaurus per ridurre il rapporto di espansione (numero di sinonimi per termine).
- Riduci la copertura complessiva dei termini (numero di righe nel thesaurus).

In alternativa, è possibile aumentare la capacità di provisioning (unità di archiviazione virtuali) per compensare l'aumento della latenza.

Argomenti

Creazione di un file del thesaurus

Un file Amazon Kendra del thesaurus è un file con codifica UTF-8 contenente un elenco di sinonimi nel formato di elenco dei sinonimi Solr. Il file del thesaurus deve pesare meno di 5 MB.

Esistono due modi per specificare le mappature dei sinonimi:

- I sinonimi bidirezionali vengono specificati come elenco di termini separati da virgole. Se l'utente esegue una query su uno qualsiasi dei termini, tutti i termini dell'elenco vengono utilizzati per la ricerca nei documenti, incluso il termine originale interrogato.
- I sinonimi unidirezionali sono specificati come termini separati dal simbolo «=>» tra di loro per associare i termini ai rispettivi sinonimi. Se l'utente cerca un termine a sinistra del simbolo «=>», viene mappato a un termine a destra per cercare documenti utilizzando il sinonimo. Non è mappato viceversa, il che lo rende unidirezionale.

I sinonimi stessi fanno distinzione tra maiuscole e minuscole, ma i termini a cui mappano non fanno distinzione tra maiuscole e minuscole. Ad esempio, `ML => Machine Learning` significa che se l'utente richiede «ML» o «ml» o utilizza altre maiuscole, verrà mappato a «Machine Learning». Se dovessi mapparlo viceversa`Machine Learning => ML`, allora «Machine Learning» o «machine learning» o qualche altro caso verrebbero mappati a «ML».

Un sinonimo non cerca una corrispondenza esatta su caratteri speciali. Ad esempio, se cerchi "dead-letter-queue«, Amazon Kendra puoi restituire documenti che corrispondono a «dead letter queue» (senza trattino). Se i documenti contengono trattini, ad esempio "dead-letter-queue«, Amazon Kendra elabora i documenti durante la ricerca per rimuovere i trattini. Per i sinonimi generici in inglese incorporati Amazon Kendra e che non devono essere inclusi in un file del thesaurus, Amazon Kendra puoi cercare sia nella versione con trattino del termine che nella versione senza trattini del termine. Ad esempio, se cerchi «terze parti» e «terze parti», Amazon Kendra restituisce documenti che corrispondono a entrambe le versioni di tali termini.

Per i sinonimi che contengono stopword o parole di uso comune, Amazon Kendra restituisce documenti che corrispondono a termini, compresi i stopword. Ad esempio, puoi creare una regola per i sinonimi per mappare «on boarding» e «onboarding». Non è possibile utilizzare solo le parole chiave per i sinonimi. Ad esempio, se si cerca «on», Amazon Kendra non è possibile restituire tutti i documenti che contengono «on».

Alcune regole relative ai sinonimi vengono ignorate. Ad esempio, `a => b` è una regola, ma `a => a` viene ignorata e non conta come regola.

Il conteggio dei termini è il numero di termini univoci nel file theaurus. Il file di esempio seguente include termini`AWS CodeStar`,`ML`, `Machine Learning` `autoscaling group`ASG, e altro.

È previsto un numero massimo di regole relative ai sinonimi per thesaurus e un numero massimo di sinonimi per termine. Per ulteriori informazioni, consulta Quote per Amazon Kendra.

L'esempio seguente mostra un file del thesaurus con regole relative ai sinonimi. Ogni riga contiene una singola regola per i sinonimi. Le righe e i commenti vuoti vengono ignorati.

```
# 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.
```

Aggiungere un thesaurus a un indice

Le procedure seguenti mostrano come aggiungere un file del thesaurus contenente sinonimi a un indice. La visualizzazione degli effetti del file del thesaurus aggiornato può richiedere fino a 30 minuti. Per ulteriori informazioni sul file del thesaurus, vedere. Creazione di un file del thesaurus

Console

Per aggiungere un thesaurus

1. Nel riquadro di navigazione a sinistra, sotto l'indice in cui desideri aggiungere un elenco di sinonimi, il tuo thesaurus, scegli Sinonimi.
2. Nella pagina dei sinonimi, scegli Aggiungi Thesaurus.
3. In Define thesaurus, assegnate al thesaurus un nome e una descrizione opzionale.
4. Nelle impostazioni del thesaurus, specificate il percorso del file del Amazon S3 thesaurus. Il file deve pesare meno di 5 MB.
5. Per IAM Role, seleziona un ruolo o seleziona Crea un nuovo ruolo e specifica un nome di ruolo per creare un nuovo ruolo. Amazon Kendra utilizza questo ruolo per accedere alla Amazon S3 risorsa per tuo conto. Il ruolo IAM ha il prefisso "AmazonKendra-».
6. Scegli Salva per salvare la configurazione e aggiungere il thesaurus. Una volta inserito, il thesaurus è attivo e i sinonimi vengono evidenziati nei risultati. La visualizzazione degli effetti del file del thesaurus può richiedere fino a 30 minuti.

CLI

Per aggiungere un thesarus a un indice con, chiamate: AWS CLI`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
```

Chiama `list-thesauri` per vedere un elenco di thesaurus:

```
aws kendra list-thesauri \
--index-id index-id
```

Per visualizzare i dettagli di un thesaurus, chiamate: `describe-thesaurus`

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

```
--index-id thesaurus-id
```

La visualizzazione degli effetti del file del thesaurus può richiedere fino a 30 minuti.

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.");
  }
}
```

Aggiornamento di un thesaurus

È possibile modificare la configurazione di un thesaurus dopo la sua creazione. È possibile modificare dettagli come il nome del thesaurus e le informazioni IAM. Puoi anche modificare la posizione del percorso del file del thesaurus Amazon S3. Se modifichi il percorso del file del thesaurus, Amazon Kendra sostituisce il thesaurus esistente con il thesaurus specificato nel percorso aggiornato.

La visualizzazione degli effetti del file del thesaurus aggiornato può richiedere fino a 30 minuti.

> **Note**
>
> In caso di errori di convalida o di sintassi nel file del thesaurus, viene mantenuto il file del thesaurus caricato in precedenza.

Le seguenti procedure mostrano come modificare i dettagli del thesaurus.

Console

Per modificare i dettagli del thesaurus

1. Nel riquadro di navigazione a sinistra, sotto l'indice che desideri modificare, scegli Sinonimi.
2. Nella pagina dei sinonimi, selezionate il thesaurus che desiderate modificare, quindi scegliete Modifica.
3. Nella pagina Aggiorna il thesaurus, aggiorna i dettagli del thesaurus.
4. (Facoltativo) Scegliete Modifica il percorso del file del thesaurus, quindi specificate un Amazon S3 percorso per il nuovo file del thesaurus. Il file del thesaurus esistente viene sostituito dal file specificato. Se non modificate il percorso, Amazon Kendra ricarica il thesaurus dal percorso esistente.

   Se si seleziona Mantieni il file del thesaurus corrente, Amazon Kendra non ricarica il file del thesaurus.
5. Scegli Salva per salvare la configurazione.

Puoi anche ricaricare il thesaurus dal percorso del thesaurus esistente.

Per ricaricare un thesaurus da un percorso esistente

1. Nel riquadro di navigazione a sinistra, sotto l'indice che desideri modificare, scegli Sinonimi.
2. Nella pagina dei sinonimi, seleziona il thesaurus che desideri ricaricare, quindi scegli Aggiorna.
3. Nella pagina Ricarica il file del thesaurus, confermate di voler aggiornare il file del thesaurus.

CLI

Per aggiornare un thesaurus, chiamate: `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.");
  }
}
```

Eliminazione di un thesaurus

Le seguenti procedure mostrano come eliminare un thesaurus.

Console

1. Nel riquadro di navigazione a sinistra, sotto l'indice che desideri modificare, scegli Sinonimi.
2. Nella pagina dei sinonimi, selezionate il thesaurus che desiderate eliminare.
3. Nella pagina dei dettagli del Thesaurus, scegliete Elimina, quindi confermate l'eliminazione.

CLI

Per eliminare un thesarus in un indice con, chiamate: AWS CLI`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);
  }
}
```

Punti salienti nei risultati di ricerca

L'evidenziazione dei sinonimi è attiva per impostazione predefinita. Le informazioni di evidenziazione sono incluse nei Amazon Kendra risultati delle query SDK e CLI. Se interagisci Amazon Kendra utilizzando l'SDK o la CLI, sei tu a determinare come visualizzare i risultati.

Le evidenziazioni sinonimiche avranno il tipo di evidenziazione. `THESAURUS_SYNONYM` Per ulteriori informazioni sulle evidenziazioni, vedete l'oggetto Highlight.

Tutorial: Creazione di una soluzione di ricerca intelligente arricchita di metadati con Amazon Kendra

Questo tutorial mostra come creare una soluzione di ricerca intelligente basata su linguaggio naturale e arricchita di metadati per i tuoi dati aziendali utilizzando Amazon Kendra, Amazon Comprehend, Amazon Simple Storage Service (S3) e. AWS CloudShell

Amazon Kendra è un servizio di ricerca intelligente in grado di creare un indice di ricerca per i tuoi archivi di dati in linguaggio naturale non strutturati. Per consentire ai tuoi clienti di trovare e filtrare più facilmente le risposte pertinenti, puoi utilizzare Amazon Comprehend per estrarre metadati dai tuoi dati e inserirli nel tuo indice di ricerca Amazon Kendra.

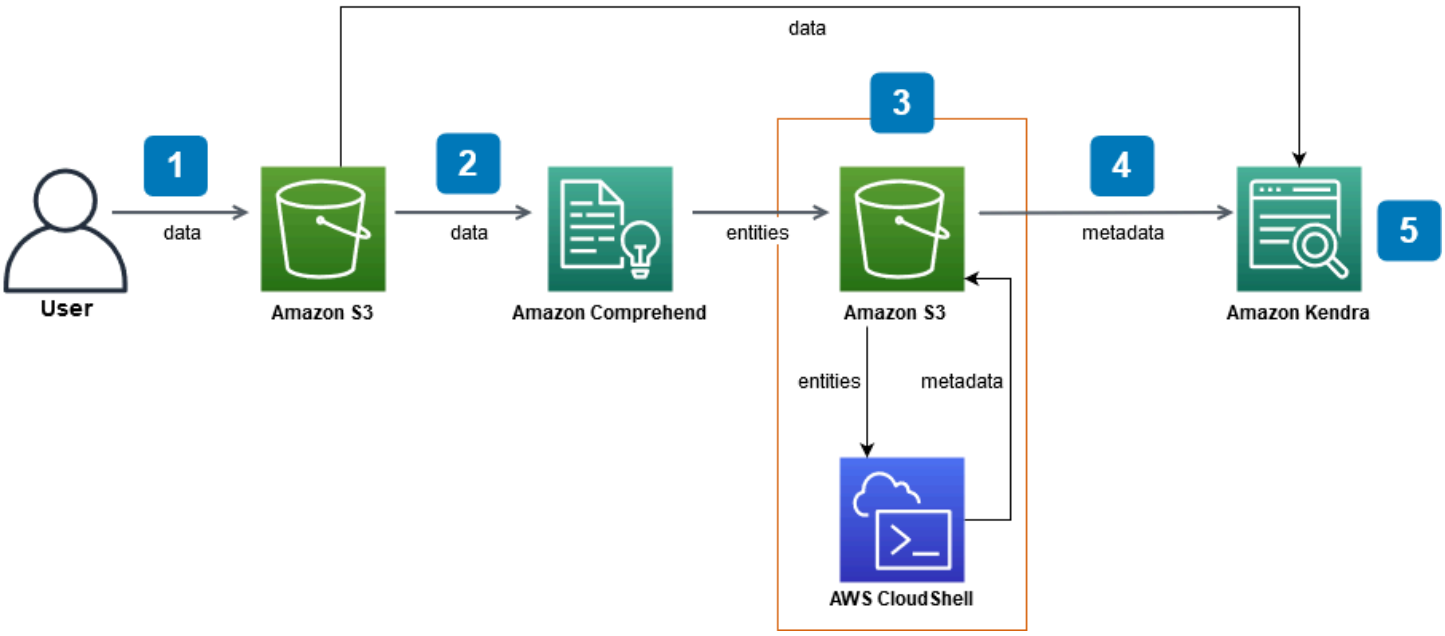
Amazon Comprehend è un servizio di elaborazione del linguaggio naturale (NLP) in grado di identificare le entità. Le entità sono riferimenti a persone, luoghi, luoghi, organizzazioni e oggetti nei tuoi dati.

Questo tutorial utilizza un set di dati di esempio di articoli di notizie per estrarre entità, convertirle in metadati e inserirle nel tuo indice Amazon Kendra per eseguire ricerche. I metadati aggiunti consentono di filtrare i risultati della ricerca utilizzando qualsiasi sottoinsieme di queste entità e migliorano la precisione della ricerca. Seguendo questo tutorial, imparerai come creare una soluzione di ricerca per i tuoi dati aziendali senza alcuna conoscenza specializzata di machine learning.

Questo tutorial mostra come creare la tua soluzione di ricerca utilizzando i seguenti passaggi:

1. Archiviazione di un set di dati di esempio di articoli di notizie in Amazon S3.
2. Utilizzo di Amazon Comprehend per estrarre entità dai tuoi dati.
3. Esecuzione di uno script Python 3 per convertire le entità nel formato dei metadati dell'indice Amazon Kendra e archiviazione di questi metadati in S3.
4. Creazione di un indice di ricerca Amazon Kendra e inserimento di dati e metadati.
5. Interrogazione dell'indice di ricerca.

Il diagramma seguente mostra il flusso di lavoro:



Tempo stimato per completare questo tutorial: 1 ora

Costo stimato: alcune delle azioni di questo tutorial comportano costi sul tuo AWS account. Per ulteriori informazioni sul costo di ciascun servizio, consulta le pagine dei prezzi di Amazon S3, Amazon Comprehend e Amazon Kendra. AWS CloudShell

Argomenti

- Prerequisiti
- Fase 1: Aggiungere documenti ad Amazon S3
- Fase 2: Esecuzione di un processo di analisi delle entità su Amazon Comprehend
- Fase 3: Formattazione dell'output dell'analisi delle entità come metadati di Amazon Kendra
- Fase 4: Creazione di un indice Amazon Kendra e inserimento dei metadati
- Fase 5: Interrogare l'indice Amazon Kendra
- Fase 6: Pulizia

Prerequisiti

Per completare questo tutorial, sono necessarie le seguenti risorse:

- Un account AWS. Se non disponi di un AWS account, segui i passaggi in Configurazione di Amazon Kendra per configurare il tuo AWS account.

- Un computer di sviluppo che esegue Windows, macOS o Linux, per accedere alla console di AWS gestione. Per ulteriori informazioni, vedere Configurazione della console AWS di gestione.
- Un utente AWS Identity and Access Management(IAM). Per scoprire come configurare un utente e un gruppo IAM per il tuo account, consulta la sezione Guida introduttiva della Guida per l'utente IAM.

  Se stai utilizzando ilAWS Command Line Interface, devi anche allegare la seguente politica al tuo utente IAM per concedergli le autorizzazioni di base necessarie per completare questo tutorial.

  Per ulteriori informazioni, consulta Creazione di policy IAM e Aggiungere e rimuovere le autorizzazioni di identità IAM.
- L'elenco dei servizi AWS regionali. Per ridurre la latenza, devi scegliere la AWS regione più vicina alla tua posizione geografica supportata sia da Amazon Comprehend che da Amazon Kendra.
- (Facoltativo) Un AWS Key Management Service. Sebbene questo tutorial non utilizzi la crittografia, potresti voler utilizzare le migliori pratiche di crittografia per il tuo caso d'uso specifico.
- (Facoltativo) Un cloud privato virtuale Amazon. Sebbene questo tutorial non utilizzi un VPC, potresti voler utilizzare le migliori pratiche VPC per garantire la sicurezza dei dati per il tuo caso d'uso specifico.

Fase 1: Aggiungere documenti ad Amazon S3

Prima di eseguire un processo di analisi delle entità Amazon Comprehend sul tuo set di dati, crei un bucket Amazon S3 per ospitare i dati, i metadati e l'output dell'analisi delle entità Amazon Comprehend.

Argomenti

- Scaricamento del set di dati di esempio
- Creazione di un bucket Amazon S3
- Creazione di cartelle di dati e metadati nel tuo bucket S3
- Caricamento dei dati di input

Scaricamento del set di dati di esempio

Prima che Amazon Comprehend possa eseguire un processo di analisi delle entità sui tuoi dati, devi scaricare ed estrarre il set di dati e caricarlo su un bucket S3.

Per scaricare ed estrarre il set di dati (Console)

1. Scarica la cartella tutorial-dataset.zip sul tuo dispositivo.
2. Estrarre la `tutorial-dataset` cartella per accedere alla `data` cartella.

Per scaricare ed estrarre il set di dati (Terminale)

1. Per scaricare il`tutorial-dataset`, esegui il seguente comando su una finestra di terminale:

   Linux

   ```
   curl -o path/tutorial-dataset.zip https://docs.aws.amazon.com/kendra/latest/dg/
   samples/tutorial-dataset.zip
   ```

   Dove:

   - *`path/`* è il percorso del file locale verso la posizione in cui si desidera salvare la cartella zip.

   macOS

   ```
   curl -o path/tutorial-dataset.zip https://docs.aws.amazon.com/kendra/latest/dg/
   samples/tutorial-dataset.zip
   ```

   Dove:

   - *`path/`* è il percorso del file locale verso la posizione in cui si desidera salvare la cartella zip.

   Windows

   ```
   curl -o path/tutorial-dataset.zip https://docs.aws.amazon.com/kendra/latest/dg/
   samples/tutorial-dataset.zip
   ```

Dove:

- *path/* è il percorso del file locale verso la posizione in cui si desidera salvare la cartella zip.

2. Per estrarre i dati dalla cartella zip, esegui il seguente comando nella finestra del terminale:

   Linux

   ```
   unzip path/tutorial-dataset.zip -d path/
   ```

   Dove:

   - *path/* è il percorso del file locale della cartella zip salvata.

   macOS

   ```
   unzip path/tutorial-dataset.zip -d path/
   ```

   Dove:

   - *path/* è il percorso del file locale della cartella zip salvata.

   Windows

   ```
   tar -xf path/tutorial-dataset.zip -C path/
   ```

   Dove:

   - *path/* è il percorso del file locale della cartella zip salvata.

Alla fine di questo passaggio, dovresti avere i file estratti in una cartella decompressa chiamata. `tutorial-dataset` Questa cartella contiene un `README` file con un'attribuzione open source Apache 2.0 e una cartella chiamata `data` contenente il set di dati per questo tutorial. Il set di dati è composto da 100 file con `.story` estensioni.

Creazione di un bucket Amazon S3

Dopo aver scaricato ed estratto la cartella di dati di esempio, la memorizzi in un bucket Amazon S3.

> **Important**
>
> Il nome di un bucket Amazon S3 deve essere univoco per tutti. AWS

Per creare un bucket S3 (console)

1. Accedi alla AWS Management Console e apri la console di Amazon S3 all'indirizzo https://console.aws.amazon.com/s3/.
2. In Bucket, scegli Crea bucket.
3. In Bucket name (Nome bucket), immettere un nome univoco.
4. Per Regione, scegli la AWS regione in cui desideri creare il bucket.

   > **Note**
   >
   > Devi scegliere una regione che supporti sia Amazon Comprehend che Amazon Kendra. Non è possibile modificare la regione di un bucket dopo averlo creato.

5. Mantieni le impostazioni predefinite per le impostazioni di blocco dell'accesso pubblico per questo bucket, Bucket Versioning e Tags.
6. Per la crittografia predefinita, scegli Disabilita.
7. Mantieni le impostazioni predefinite per le impostazioni avanzate.
8. Controlla la configurazione del bucket e scegli Crea bucket.

Per creare un bucket S3 () AWS CLI

1. Per creare un bucket S3, usa il comando create-bucket in: AWS CLI

   Linux

   ```
   aws s3api create-bucket \
           --bucket DOC-EXAMPLE-BUCKET \
           --region aws-region \
   ```

```
        --create-bucket-configuration LocationConstraint=aws-region
```

Dove:

- *DOC-EXAMPLE-BUCKET è il nome del tuo bucket*,
- *aws-region* è la regione in cui vuoi creare il tuo bucket.

macOS

```
aws s3api create-bucket \
        --bucket DOC-EXAMPLE-BUCKET \
        --region aws-region \
        --create-bucket-configuration LocationConstraint=aws-region
```

Dove:

- *DOC-EXAMPLE-BUCKET è il nome del tuo bucket*,
- *aws-region* è la regione in cui vuoi creare il tuo bucket.

Windows

```
aws s3api create-bucket ^
        --bucket DOC-EXAMPLE-BUCKET ^
        --region aws-region ^
        --create-bucket-configuration LocationConstraint=aws-region
```

Dove:

- *DOC-EXAMPLE-BUCKET è il nome del tuo bucket*,
- *aws-region* è la regione in cui vuoi creare il tuo bucket.

> **Note**
>
> Devi scegliere una regione che supporti sia Amazon Comprehend che Amazon Kendra. Non è possibile modificare la regione di un bucket dopo averlo creato.

2. Per assicurarti che il tuo bucket sia stato creato correttamente, usa il comando list:

Linux

```
aws s3 ls
```

macOS

```
aws s3 ls
```

Windows

```
aws s3 ls
```

Creazione di cartelle di dati e metadati nel tuo bucket S3

Dopo aver creato il tuo bucket S3, crei cartelle di dati e metadati al suo interno.

Per creare cartelle nel tuo bucket S3 (console)

1. Apri la console di Amazon S3 su https://console.aws.amazon.com/s3/.
2. In Buckets, fai clic sul nome del tuo bucket dall'elenco dei bucket.
3. Dalla scheda Oggetti, scegli Crea cartella.
4. Per il nuovo nome della cartella, inserisci**`data`**.
5. Per le impostazioni di crittografia, scegli Disabilita.
6. Scegliere Create folder (Crea cartella).
7. Ripeti i passaggi da 3 a 6 per creare un'altra cartella in cui archiviare i metadati di Amazon Kendra e assegna un nome alla cartella creata nel passaggio 4. **`metadata`**

Per creare cartelle nel tuo bucket S3 () AWS CLI

1. Per creare la `data` cartella nel tuo bucket S3, usa il comando put-object in: AWS CLI

   Linux

   ```
   aws s3api put-object \
           --bucket DOC-EXAMPLE-BUCKET \
   ```

```
        --key data/
```

Dove:

- *DOC-EXAMPLE-BUCKET è il nome del tuo bucket*.

macOS

```
aws s3api put-object \
        --bucket DOC-EXAMPLE-BUCKET \
        --key data/
```

Dove:

- *DOC-EXAMPLE-BUCKET è il nome del tuo bucket*.

Windows

```
aws s3api put-object ^
        --bucket DOC-EXAMPLE-BUCKET ^
        --key data/
```

Dove:

- *DOC-EXAMPLE-BUCKET è il nome del tuo bucket*.

2. Per creare la `metadata` cartella nel tuo bucket S3, usa il comando put-object in: AWS CLI

Linux

```
aws s3api put-object \
        --bucket DOC-EXAMPLE-BUCKET \
        --key metadata/
```

Dove:

- *DOC-EXAMPLE-BUCKET è il nome del tuo bucket*.

macOS

```
aws s3api put-object \
        --bucket DOC-EXAMPLE-BUCKET \
        --key metadata/
```

Dove:

- *DOC-EXAMPLE-BUCKET è il nome del tuo bucket*.

Windows

```
aws s3api put-object ^
        --bucket DOC-EXAMPLE-BUCKET ^
        --key metadata/
```

Dove:

- *DOC-EXAMPLE-BUCKET è il nome del tuo bucket*.

3. Per assicurarti che le tue cartelle siano state create correttamente, controlla il contenuto del tuo bucket usando il comando list:

Linux

```
aws s3 ls s3://DOC-EXAMPLE-BUCKET/
```

Dove:

- *DOC-EXAMPLE-BUCKET è il nome del tuo bucket*.

macOS

```
aws s3 ls s3://DOC-EXAMPLE-BUCKET/
```

Dove:

- *DOC-EXAMPLE-BUCKET è il nome del tuo bucket*.

Windows

```
aws s3 ls s3://DOC-EXAMPLE-BUCKET/
```

Dove:

- *DOC-EXAMPLE-BUCKET è il nome del tuo bucket*.

Caricamento dei dati di input

Dopo aver creato le cartelle di dati e metadati, carichi il set di dati di esempio nella cartella. `data`

Per caricare il set di dati di esempio nella cartella dei dati (Console)

1. Apri la console di Amazon S3 su https://console.aws.amazon.com/s3/.
2. In Buckets, fai clic sul nome del tuo bucket dall'elenco dei bucket, quindi fai clic su. `data`
3. Scegli Carica, quindi scegli Aggiungi file.
4. Nella finestra di dialogo, accedi alla `data` cartella all'interno della `tutorial-dataset` cartella nel tuo dispositivo locale, seleziona tutti i file e scegli Apri.
5. Mantieni le impostazioni predefinite per Destinazione, Autorizzazioni e Proprietà.
6. Scegliere Upload (Carica).

Per caricare il set di dati di esempio nella cartella dei dati () AWS CLI

1. Per caricare i dati di esempio nella `data` cartella, usa il comando copy inAWS CLI:

   Linux

   ```
   aws s3 cp path/tutorial-dataset/data s3://DOC-EXAMPLE-BUCKET/data/ --recursive
   ```

   Dove:

   - *path/* è il percorso del file della `tutorial-dataset` cartella sul tuo dispositivo,
   - *DOC-EXAMPLE-BUCKET è il nome del tuo bucket*.

macOS

```
aws s3 cp path/tutorial-dataset/data s3://DOC-EXAMPLE-BUCKET/data/ --recursive
```

Dove:

- *path/* è il percorso del file della `tutorial-dataset` cartella sul tuo dispositivo,
- *DOC-EXAMPLE-BUCKET è il nome del tuo bucket*.

Windows

```
aws s3 cp path/tutorial-dataset/data s3://DOC-EXAMPLE-BUCKET/data/ --recursive
```

Dove:

- *path/* è il percorso del file della `tutorial-dataset` cartella sul tuo dispositivo,
- *DOC-EXAMPLE-BUCKET è il nome del tuo bucket*.

2. Per assicurarti che i file del set di dati siano stati caricati correttamente `data` nella tua cartella, usa il comando list in: AWS CLI

Linux

```
aws s3 ls s3://DOC-EXAMPLE-BUCKET/data/
```

Dove:

- *DOC-EXAMPLE-BUCKET è il nome del tuo bucket S3*.

macOS

```
aws s3 ls s3://DOC-EXAMPLE-BUCKET/data/
```

Dove:

- *DOC-EXAMPLE-BUCKET è il nome del tuo bucket S3*.

Windows

```
aws s3 ls s3://DOC-EXAMPLE-BUCKET/data/
```

Dove:

- *DOC-EXAMPLE-BUCKET è il nome del tuo bucket S3*.

Alla fine di questo passaggio, avrai un bucket S3 con il tuo set di dati archiviato all'interno della `data` cartella e una `metadata` cartella vuota, in cui verranno archiviati i metadati di Amazon Kendra.

Fase 2: Esecuzione di un processo di analisi delle entità su Amazon Comprehend

Dopo aver archiviato il set di dati di esempio nel tuo bucket S3, esegui un processo di analisi delle entità Amazon Comprehend per estrarre le entità dai tuoi documenti. Queste entità formeranno gli attributi personalizzati di Amazon Kendra e ti aiuteranno a filtrare i risultati di ricerca nel tuo indice. Per ulteriori informazioni, vedere Rileva entità.

Argomenti

- Esecuzione di un processo di analisi delle entità Amazon Comprehend

Esecuzione di un processo di analisi delle entità Amazon Comprehend

Per estrarre le entità dal tuo set di dati, esegui un processo di analisi delle entità Amazon Comprehend.

Se utilizzi l'interfaccia a riga di AWS comando in questa fase, devi prima creare e associare un ruolo e una policy AWS IAM per Amazon Comprehend, quindi eseguire un processo di analisi delle entità. Per eseguire un processo di analisi delle entità sui dati di esempio, Amazon Comprehend necessita di:

- un ruolo AWS Identity and Access Management (IAM) che la riconosce come entità affidabile
- una policy AWS IAM associata al ruolo IAM che gli conferisce le autorizzazioni per accedere al tuo bucket S3

Per ulteriori informazioni, consulta Come funziona Amazon Comprehend con IAM e le politiche basate sull'identità per Amazon Comprehend.

Per eseguire un processo di analisi delle entità Amazon Comprehend (Console)

1. Apri la console Amazon Comprehend all'indirizzo https://console.aws.amazon.com/comprehend/.

   > **Important**
   >
   > Assicurati di trovarti nella stessa regione in cui hai creato il tuo bucket Amazon S3. Se ti trovi in un'altra regione, scegli la AWS regione in cui hai creato il tuo bucket S3 dal selettore della regione nella barra di navigazione in alto.

2. Scegli Launch Amazon Comprehend.
3. Nel riquadro di navigazione a sinistra, scegli Lavori di analisi.
4. Scegli Create job (Crea processo).
5. Nella sezione Impostazioni del lavoro, procedi come segue:
   a. In Name (Nome), inserire **`data-entities-analysis`**.
   b. Per Tipo di analisi, scegli Entità.
   c. Per Lingua, scegli l'inglese.
   d. Mantieni la crittografia Job disattivata.
6. Nella sezione Dati di input, procedi come segue:
   a. In Origine dati, scegli I miei documenti.
   b. Per la posizione S3, scegli Sfoglia S3.
   c. Per Scegli risorse, fai clic sul nome del tuo bucket dall'elenco dei bucket.
   d. Per Oggetti, selezionate il pulsante di opzione `data` e scegliete Scegli.
   e. Per il formato di input, scegli Un documento per file.
7. Nella sezione Dati di output, procedi come segue:
   a. Per la posizione S3, scegli Browse S3, quindi seleziona la casella di opzione per il tuo bucket dall'elenco dei bucket e scegli Scegli.
   b. Mantieni la crittografia disattivata.
8. Nella sezione Autorizzazioni di accesso, procedi come segue:

a. Per il ruolo IAM, scegli Crea un ruolo IAM.

b. Per le autorizzazioni di accesso, scegli i bucket S3 di input e output.

c. Per il suffisso Nome, immettere**`comprehend-role`**. Questo ruolo fornisce l'accesso al tuo bucket Amazon S3.

9. Mantieni le impostazioni VPC predefinite.

10. Scegli Create job (Crea processo).

Per eseguire un processo di analisi delle entità Amazon Comprehend () AWS CLI

1. Per creare e assegnare un ruolo IAM per Amazon Comprehend che lo riconosca come entità affidabile, procedi come segue:

   a. Salva la seguente politica di affidabilità come file JSON richiamato `comprehend-trust-policy.json` in un editor di testo sul tuo dispositivo locale.

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

   b. Per creare un ruolo IAM chiamato `comprehend-role` e allegare il `comprehend-trust-policy.json` file salvato, usa il comando create-role:

      Linux

```
aws iam create-role \
          --role-name comprehend-role \
          --assume-role-policy-document file://path/comprehend-trust-
policy.json
```

Dove:

- *path/* è il percorso del file `comprehend-trust-policy.json` sul tuo dispositivo locale.

macOS

```
aws iam create-role \
          --role-name comprehend-role \
          --assume-role-policy-document file://path/comprehend-trust-
policy.json
```

Dove:

- *path/* è il percorso del file `comprehend-trust-policy.json` sul tuo dispositivo locale.

Windows

```
aws iam create-role ^
          --role-name comprehend-role ^
          --assume-role-policy-document file://path/comprehend-trust-
policy.json
```

Dove:

- *path/* è il percorso del file `comprehend-trust-policy.json` sul tuo dispositivo locale.

c. Copia Amazon Resource Name (ARN) nel tuo editor di testo e salvalo localmente con nome. `comprehend-role-arn`

> **Note**
>
> L'ARN ha un formato simile a *arn:aws:iam: :123456789012:role/comprensend-role*. È necessario l'ARN salvato `comprehend-role-arn` per eseguire il processo di analisi Amazon Comprehend.

2. Per creare e allegare una policy IAM al tuo ruolo IAM che gli conceda le autorizzazioni per accedere al tuo bucket S3, procedi come segue:

   a. Salva la seguente politica di affidabilità come file JSON richiamato `comprehend-S3-access-policy.json` in un editor di testo sul tuo dispositivo locale.

```
{
    "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. Per creare una policy IAM chiamata `comprehend-S3-access-policy` ad accedere al tuo bucket S3, usa il comando create-policy:

Linux

```
aws iam create-policy \
          --policy-name comprehend-S3-access-policy \
          --policy-document file://path/comprehend-S3-access-policy.json
```

Dove:

- *path/* è il percorso del file `comprehend-S3-access-policy.json` sul tuo dispositivo locale.

macOS

```
aws iam create-policy \
          --policy-name comprehend-S3-access-policy \
          --policy-document file://path/comprehend-S3-access-policy.json
```

Dove:

- *path/* è il percorso del file `comprehend-S3-access-policy.json` sul tuo dispositivo locale.

Windows

```
aws iam create-policy ^
          --policy-name comprehend-S3-access-policy ^
          --policy-document file://path/comprehend-S3-access-policy.json
```

Dove:

- *path/* è il percorso del file `comprehend-S3-access-policy.json` sul tuo dispositivo locale.

c. Copia Amazon Resource Name (ARN) nel tuo editor di testo e salvalo localmente con nome. `comprehend-S3-access-arn`

> **Note**
>
> L'ARN ha un formato simile a *arn:aws:iam: :123456789012:role/comprensend-S3-access-policy*. Hai bisogno dell'ARN che hai salvato `comprehend-S3-access-arn` per associarlo `comprehend-S3-access-policy` al tuo ruolo IAM.

d. Per associarlo `comprehend-S3-access-policy` al tuo ruolo IAM, usa il attach-role-policycomando:

Linux

```
aws iam attach-role-policy \
          --policy-arn policy-arn \
          --role-name comprehend-role
```

Dove:

- *policy-arn* è l'ARN che hai salvato. `comprehend-S3-access-arn`

macOS

```
aws iam attach-role-policy \
          --policy-arn policy-arn \
          --role-name comprehend-role
```

Dove:

- *policy-arn* è l'ARN che hai salvato. `comprehend-S3-access-arn`

Windows

```
aws iam attach-role-policy ^
          --policy-arn policy-arn ^
          --role-name comprehend-role
```

Dove:

- *policy-arn* è l'ARN che hai salvato. comprehend-S3-access-arn

3. Per eseguire un processo di analisi delle entità Amazon Comprehend, utilizza il start-entities-detection-jobcomando:

   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
   ```

   Dove:

   - *DOC-EXAMPLE-BUCKET è il nome del tuo bucket S3,*
   - *role-arn* è l'ARN che hai salvato, comprehend-role-arn
   - *aws-region è la tua AWS regione*.

   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
   ```

   Dove:

   - *DOC-EXAMPLE-BUCKET è il nome del tuo bucket S3,*
   - *role-arn* è l'ARN che hai salvato, comprehend-role-arn
   - *aws-region è la tua AWS regione*.

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
```

Dove:

- *DOC-EXAMPLE-BUCKET è il nome del tuo bucket S3,*
- *role-arn* è l'ARN che hai salvato, `comprehend-role-arn`
- *aws-region è la tua AWS regione*.

4. Copia l'analisi delle entità `JobId` e salvala in un editor di testo come`comprehend-job-id`. Ti `JobId` aiuta a tenere traccia dello stato del tuo lavoro di analisi delle entità.
5. Per monitorare lo stato di avanzamento del processo di analisi delle entità, usa il describe-entities-detection-jobcomando:

   Linux

   ```
   aws comprehend describe-entities-detection-job \
           --job-id entities-job-id \
           --region aws-region
   ```

   Dove:

   - *entities-job-id*è il tuo salvato`comprehend-job-id`,
   - *aws-region è la tua AWS regione*.

   macOS

   ```
   aws comprehend describe-entities-detection-job \
           --job-id entities-job-id \
   ```

```
        --region aws-region
```

Dove:

- *entities-job-id*è il tuo salvatocomprehend-job-id,
- *aws-region è la tua AWS regione*.

Windows

```
aws comprehend describe-entities-detection-job ^
        --job-id entities-job-id ^
        --region aws-region
```

Dove:

- *entities-job-id*è il tuo salvatocomprehend-job-id,
- *aws-region è la tua AWS regione*.

Potrebbero essere necessari alcuni minuti `JobStatus` per passare a`COMPLETED`.

Al termine di questo passaggio, Amazon Comprehend archivia i risultati dell'analisi delle entità come `output.tar.gz` file compresso all'interno di una `output` cartella generata automaticamente nel bucket S3. Assicurati che lo stato del tuo lavoro di analisi sia completo prima di passare alla fase successiva.

Fase 3: Formattazione dell'output dell'analisi delle entità come metadati di Amazon Kendra

Per convertire le entità estratte da Amazon Comprehend nel formato di metadati richiesto da un indice Amazon Kendra, esegui uno script Python 3. I risultati della conversione vengono archiviati nella `metadata` cartella del bucket Amazon S3.

Per ulteriori informazioni sul formato e sulla struttura dei metadati di Amazon Kendra, consulta i metadati dei documenti S3.

Argomenti

- Scaricare ed estrarre l'output di Amazon Comprehend

- Caricamento dell'output nel bucket S3
- Conversione dell'output nel formato di metadati Amazon Kendra
- Pulire il bucket Amazon S3

Scaricare ed estrarre l'output di Amazon Comprehend

Per formattare l'output dell'analisi delle entità Amazon Comprehend, devi prima scaricare l'`output.tar.gz`archivio di analisi delle entità Amazon Comprehend ed estrarre il file di analisi delle entità.

Per scaricare ed estrarre il file di output (Console)

1. Nel riquadro di navigazione della console Amazon Comprehend, vai a Processi di analisi.
2. Scegli il tuo lavoro di analisi delle entità`data-entities-analysis`.
3. In Output, scegli il link visualizzato accanto a Posizione dei dati di output. Questo ti reindirizza all'`output.tar.gz`archivio nel tuo bucket S3.
4. Nella scheda Panoramica, scegli Scarica.

> **Tip**
>
> L'output di tutti i processi di analisi Amazon Comprehend ha lo stesso nome. Rinominare il tuo archivio ti aiuterà a rintracciarlo più facilmente.

5. Decomprimi ed estrai il file Amazon Comprehend scaricato sul tuo dispositivo.

Per scaricare ed estrarre il file di output (AWS CLI)

1. Per accedere al nome della cartella generata automaticamente da Amazon Comprehend nel tuo bucket S3 che contiene i risultati del processo di analisi delle entità, usa il comando: describe-entities-detection-job

   Linux

   ```
   aws comprehend describe-entities-detection-job \
             --job-id entities-job-id \
             --region aws-region
   ```

Dove:

- *entities-job-id*è il tuo salvato comprehend-job-id dathe section called “Fase 2: Rilevamento delle entità”,
- *aws-region è la tua AWS regione*.

macOS

```
aws comprehend describe-entities-detection-job \
          --job-id entities-job-id \
          --region aws-region
```

Dove:

- *entities-job-id*è il tuo salvato comprehend-job-id dathe section called “Fase 2: Rilevamento delle entità”,
- *aws-region è la tua AWS regione*.

Windows

```
aws comprehend describe-entities-detection-job ^
          --job-id entities-job-id ^
          --region aws-region
```

Dove:

- *entities-job-id*è il tuo salvato comprehend-job-id dathe section called “Fase 2: Rilevamento delle entità”,
- *aws-region è la tua AWS regione*.

2. Dall'OutputDataConfigoggetto nella descrizione del lavoro dell'entità, copia e salva il S3Uri valore come comprehend-S3uri su un editor di testo.

> **Note**
>
> Il S3Uri valore ha un formato simile a *s3://DOC-EXAMPLE-BUCKET /...* /output/output.tar.gz.

3. Per scaricare l'archivio di output delle entità, usa il comando copy:

   Linux

   ```
   aws s3 cp s3://DOC-EXAMPLE-BUCKET/.../output/output.tar.gz path/output.tar.gz
   ```

   Dove:

   - *s3://BUCKET DI ESEMPIO DI DOCUMENTO /...* /output/output.tar.gz è il `S3Uri` valore che hai salvato come`comprehend-S3uri`,
   - *path/* è la cartella locale in cui si desidera salvare l'output.

   macOS

   ```
   aws s3 cp s3://DOC-EXAMPLE-BUCKET/.../output/output.tar.gz path/output.tar.gz
   ```

   Dove:

   - *s3://BUCKET DI ESEMPIO DI DOCUMENTO /...* /output/output.tar.gz è il `S3Uri` valore che hai salvato come`comprehend-S3uri`,
   - *path/* è la cartella locale in cui si desidera salvare l'output.

   Windows

   ```
   aws s3 cp s3://DOC-EXAMPLE-BUCKET/.../output/output.tar.gz path/output.tar.gz
   ```

   Dove:

   - *s3://BUCKET DI ESEMPIO DI DOCUMENTO /...* /output/output.tar.gz è il `S3Uri` valore che hai salvato come`comprehend-S3uri`,
   - *path/* è la cartella locale in cui si desidera salvare l'output.

4. Per estrarre l'output delle entità, esegui il seguente comando su una finestra di terminale:

   Linux

   ```
   tar -xf path/output.tar.gz -C path/
   ```

Dove:

- *path/* è il percorso del file dell'`output.tar.gz`archivio scaricato sul dispositivo locale.

macOS

```
tar -xf path/output.tar.gz -C path/
```

Dove:

- *path/* è il percorso del file dell'`output.tar.gz`archivio scaricato sul dispositivo locale.

Windows

```
tar -xf path/output.tar.gz -C path/
```

Dove:

- *path/* è il percorso del file dell'`output.tar.gz`archivio scaricato sul dispositivo locale.

Al termine di questo passaggio, dovresti avere un file sul tuo dispositivo denominato `output` con un elenco di entità identificate da Amazon Comprehend.

Caricamento dell'output nel bucket S3

Dopo aver scaricato ed estratto il file di analisi delle entità Amazon Comprehend, carichi il `output` file estratto nel tuo bucket Amazon S3.

Per caricare il file di output Amazon Comprehend estratto (Console)

1. Apri la console di Amazon S3 su https://console.aws.amazon.com/s3/.
2. In Buckets, fai clic sul nome del tuo bucket e quindi scegli Carica.
3. In File e cartelle, scegli Aggiungi file.
4. Nella finestra di dialogo, accedi al `output` file estratto nel dispositivo, selezionalo e scegli Apri.
5. Mantieni le impostazioni predefinite per Destinazione, Autorizzazioni e Proprietà.
6. Scegliere Upload (Carica).

Per caricare il file di output Amazon Comprehend estratto () AWS CLI

1. Per caricare il `output` file estratto nel tuo bucket, usa il comando copy:

   Linux

   ```
   aws s3 cp path/output s3://DOC-EXAMPLE-BUCKET/output
   ```

   Dove:

   - *path/* è il percorso locale del file estratto, `output`
   - *DOC-EXAMPLE-BUCKET è il nome del tuo bucket S3*.

   macOS

   ```
   aws s3 cp path/output s3://DOC-EXAMPLE-BUCKET/output
   ```

   Dove:

   - *path/* è il percorso locale del file estratto, `output`
   - *DOC-EXAMPLE-BUCKET è il nome del tuo bucket S3*.

   Windows

   ```
   aws s3 cp path/output s3://DOC-EXAMPLE-BUCKET/output
   ```

   Dove:

   - *path/* è il percorso locale del file estratto, `output`
   - *DOC-EXAMPLE-BUCKET è il nome del tuo bucket S3*.

2. Per assicurarti che il `output` file sia stato caricato correttamente nel tuo bucket S3, controllane il contenuto usando il comando list:

   Linux

   ```
   aws s3 ls s3://DOC-EXAMPLE-BUCKET/
   ```

Dove:

- *DOC-EXAMPLE-BUCKET è il nome del tuo bucket S3*.

macOS

```
aws s3 ls s3://DOC-EXAMPLE-BUCKET/
```

Dove:

- *DOC-EXAMPLE-BUCKET è il nome del tuo bucket S3*.

Windows

```
aws s3 ls s3://DOC-EXAMPLE-BUCKET/
```

Dove:

- *DOC-EXAMPLE-BUCKET è il nome del tuo bucket S3*.

Conversione dell'output nel formato di metadati Amazon Kendra

Per convertire l'output di Amazon Comprehend in metadati Amazon Kendra, esegui uno script Python 3. Se si utilizza la Console, si utilizza AWS CloudShell per questo passaggio.

Per eseguire lo script Python 3 (console)

1. Scarica il file compresso converter.py.zip sul tuo dispositivo.
2. Estrai il file `converter.py` Python 3.
3. Accedi alla Console di AWS gestione e assicurati che la tua AWS regione sia impostata sulla stessa regione del bucket S3 e del tuo lavoro di analisi Amazon Comprehend.
4. Scegli l'AWS CloudShellicona o digita AWSCloudShellnella casella di ricerca nella barra di navigazione in alto per avviare un ambiente.

> **Note**
>
> Quando AWS CloudShell viene avviata per la prima volta in una nuova finestra del browser, viene visualizzato un pannello di benvenuto e un elenco delle funzioni chiave. La shell è pronta per l'interazione dopo la chiusura di questo pannello e la visualizzazione del prompt dei comandi.

5. Dopo aver preparato il terminale, scegli Azioni dal pannello di navigazione, quindi scegli Carica file dal menu.
6. Nella finestra di dialogo che si apre, scegli Seleziona file, quindi scegli il file Python 3 scaricato `converter.py` dal tuo dispositivo. Scegliere Upload (Carica).
7. Nell'AWS CloudShellambiente, inserisci il seguente comando:

```
python3 converter.py
```

8. Quando l'interfaccia shell richiede di inserire il nome del bucket S3, inserisci il nome del bucket S3 e premi invio.
9. Quando l'interfaccia shell richiede di immettere il percorso completo del file di output Comprehend, inserisci **`output`** e premi invio.
10. Quando l'interfaccia shell richiede di immettere il percorso completo del file nella cartella dei metadati, inserisci e premi invio. **`metadata/`**

> **Important**
>
> Affinché i metadati siano formattati correttamente, i valori di input nei passaggi 8-10 devono essere esatti.

Per eseguire lo script Python 3 () AWS CLI

1. Per scaricare il file Python 3`converter.py`, esegui il seguente comando su una finestra di terminale:

Linux

```
curl -o path/converter.py.zip https://docs.aws.amazon.com/kendra/latest/dg/
samples/converter.py.zip
```

Dove:

- *path/* è il percorso del file nella posizione in cui si desidera salvare il file compresso.

macOS

```
curl -o path/converter.py.zip https://docs.aws.amazon.com/kendra/latest/dg/
samples/converter.py.zip
```

Dove:

- *path/* è il percorso del file nella posizione in cui si desidera salvare il file compresso.

Windows

```
curl -o path/converter.py.zip https://docs.aws.amazon.com/kendra/latest/dg/
samples/converter.py.zip
```

Dove:

- *path/* è il percorso del file nella posizione in cui si desidera salvare il file compresso.

2. Per estrarre il file Python 3, esegui il seguente comando nella finestra del terminale:

Linux

```
unzip path/converter.py.zip -d path/
```

Dove:

- *path/* è il percorso del file salvato. `converter.py.zip`

macOS

```
unzip path/converter.py.zip -d path/
```

Dove:

- *path/* è il percorso del file salvato. `converter.py.zip`

Windows

```
tar -xf path/converter.py.zip -C path/
```

Dove:

- *path/* è il percorso del file salvato. `converter.py.zip`

3. Assicurati che Boto3 sia installato sul tuo dispositivo eseguendo il seguente comando.

Linux

```
pip3 show boto3
```

macOS

```
pip3 show boto3
```

Windows

```
pip3 show boto3
```

> **Note**
>
> Se non hai installato Boto3, esegui `pip3 install boto3` per installarlo.

4. Per eseguire lo script Python 3 per convertire il `output` file, esegui il seguente comando.

Linux

```
python path/converter.py
```

Dove:

- *path/* è il percorso del file salvato. `converter.py.zip`

macOS

```
python path/converter.py
```

Dove:

- *path/* è il percorso del file salvato. `converter.py.zip`

Windows

```
python path/converter.py
```

Dove:

- *path/* è il percorso del file salvato. `converter.py.zip`

5. Quando ti viene AWS CLI richiesto`Enter the name of your S3 bucket`, inserisci il nome del tuo bucket S3 e premi invio.
6. Quando AWS CLI richiesto`Enter the full filepath to your Comprehend output file`, inserisci **`output`** e premi invio.
7. Quando AWS CLI richiesto`Enter the full filepath to your metadata folder`, inserisci **`metadata/`** e premi invio.

> **Important**
>
> Affinché i metadati siano formattati correttamente, i valori di input nei passaggi 5-7 devono essere esatti.

Al termine di questo passaggio, i metadati formattati vengono depositati `metadata` nella cartella del bucket S3.

Pulire il bucket Amazon S3

Poiché l'indice Amazon Kendra sincronizza tutti i file archiviati in un bucket, ti consigliamo di ripulire il bucket Amazon S3 per evitare risultati di ricerca ridondanti.

Per pulire il tuo bucket Amazon S3 (console)

1. Apri la console di Amazon S3 su https://console.aws.amazon.com/s3/.
2. In Buckets, scegli il tuo bucket, quindi seleziona la cartella di output dell'analisi delle entità Amazon Comprehend, il file di analisi delle entità Amazon Comprehend e il `.temp` file Amazon Comprehend estratto. `output`
3. Dalla scheda Panoramica, scegli Elimina.
4. In Elimina oggetti, scegli Eliminare definitivamente gli oggetti? e inserisci il **`permanently delete`** campo di immissione del testo.
5. Scegliere Delete objects (Elimina oggetti).

Per pulire il tuo bucket Amazon S3 () AWS CLI

1. Per eliminare tutti i file e le cartelle nel tuo bucket S3 tranne le `metadata` cartelle `data` and, usa il comando remove in: AWS CLI

   Linux

   ```
   aws s3 rm s3://DOC-EXAMPLE-BUCKET/ --recursive --exclude "data/*" --exclude
    "metadata/*"
   ```

   Dove:

   - *DOC-EXAMPLE-BUCKET è il nome del tuo bucket S3*.

   macOS

   ```
   aws s3 rm s3://DOC-EXAMPLE-BUCKET/ --recursive --exclude "data/*" --exclude
    "metadata/*"
   ```

Dove:

- *DOC-EXAMPLE-BUCKET è il nome del tuo bucket S3*.

Windows

```
aws s3 rm s3://DOC-EXAMPLE-BUCKET/ --recursive --exclude "data/*" --exclude
 "metadata/*"
```

Dove:

- *DOC-EXAMPLE-BUCKET è il nome del tuo bucket S3*.

2. Per assicurarti che gli oggetti siano stati eliminati correttamente dal tuo bucket S3, controllane il contenuto usando il comando list:

Linux

```
aws s3 ls s3://DOC-EXAMPLE-BUCKET/
```

Dove:

- *DOC-EXAMPLE-BUCKET è il nome del tuo bucket S3*.

macOS

```
aws s3 ls s3://DOC-EXAMPLE-BUCKET/
```

Dove:

- *DOC-EXAMPLE-BUCKET è il nome del tuo bucket S3*.

Windows

```
aws s3 ls s3://DOC-EXAMPLE-BUCKET/
```

Dove:

- *DOC-EXAMPLE-BUCKET è il nome del tuo bucket S3*.

Al termine di questo passaggio, hai convertito l'output dell'analisi delle entità Amazon Comprehend in metadati Amazon Kendra. Ora sei pronto per creare un indice Amazon Kendra.

Fase 4: Creazione di un indice Amazon Kendra e inserimento dei metadati

Per implementare la tua soluzione di ricerca intelligente, crei un indice Amazon Kendra e inserisci i tuoi dati e metadati S3.

Prima di aggiungere metadati al tuo indice Amazon Kendra, crei campi indice personalizzati corrispondenti agli attributi del documento personalizzati, che a loro volta corrispondono ai tipi di entità Amazon Comprehend. Amazon Kendra utilizza i campi indice e gli attributi personalizzati dei documenti che crei per cercare e filtrare i tuoi documenti.

Per ulteriori informazioni, vedere Indicizzazione e creazione di attributi di documenti personalizzati.

Argomenti

- Creazione di un indice Amazon Kendra
- Aggiornamento del ruolo IAM per l'accesso ad Amazon S3
- Creazione di campi dell'indice di ricerca personalizzati di Amazon Kendra
- Aggiungere il bucket Amazon S3 come origine dati per l'indice
- Sincronizzazione dell'indice Amazon Kendra

Creazione di un indice Amazon Kendra

Per interrogare i tuoi documenti di origine, crei un indice Amazon Kendra.

Se utilizzi AWS CLI in questo passaggio, crei e alleghi un ruolo e una policy AWS IAM che consentano ad Amazon Kendra di accedere ai tuoi CloudWatch log prima di creare un indice. Per ulteriori informazioni, consulta Prerequisiti.

Per creare un indice Amazon Kendra (Console)

1. Apri la console Amazon Kendra all'indirizzo https://console.aws.amazon.com/kendra/.

> **Important**
>
> Assicurati di trovarti nella stessa regione in cui hai creato il job di analisi delle entità Amazon Comprehend e il tuo bucket Amazon S3. Se ti trovi in un'altra regione, scegli la AWS regione in cui hai creato il tuo bucket Amazon S3 dal selettore della regione nella barra di navigazione in alto.

2. Scegli Crea un indice.
3. Per i dettagli dell'indice nella pagina Specifica i dettagli dell'indice, procedi come segue:
   a. Per Index name (Nome indice), inserisci **`kendra-index`**.
   b. Mantieni vuoto il campo Descrizione.
   c. Per IAM Role (Ruolo IAM), scegliere Create a New Role (Crea un nuovo ruolo). Questo ruolo fornisce l'accesso al tuo bucket Amazon S3.
   d. Per Nome ruolo, inserisci **`kendra-role`**. Il ruolo IAM avrà il prefisso`AmazonKendra-`.
   e. Mantieni le impostazioni predefinite per Crittografia e tag e scegli Avanti.
4. Per le impostazioni del controllo d'accesso nella pagina Configura il controllo degli accessi utente, scegli No, quindi scegli Avanti.
5. Per le edizioni Provisioning nella pagina dei dettagli del provisioning, scegli Edizione per sviluppatori e scegli Crea.

Per creare un indice Amazon Kendra () AWS CLI

1. Per creare e assegnare un ruolo IAM per Amazon Kendra che la riconosca come entità affidabile, procedi come segue:
   a. Salva la seguente politica di affidabilità come file JSON richiamato `kendra-trust-policy.json` in un editor di testo sul tuo dispositivo locale.

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

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

b. Per creare un ruolo IAM chiamato `kendra-role` e allegare il `kendra-trust-policy.json` file salvato, usa il comando create-role:

Linux

```
aws iam create-role \
          --role-name kendra-role \
          --assume-role-policy-document file://path/kendra-trust-policy.json
```

Dove:

- *path/* è il percorso del file `kendra-trust-policy.json` sul tuo dispositivo locale.

macOS

```
aws iam create-role \
          --role-name kendra-role \
          --assume-role-policy-document file://path/kendra-trust-policy.json
```

Dove:

- *path/* è il percorso del file `kendra-trust-policy.json` sul tuo dispositivo locale.

Windows

```
aws iam create-role ^
          --role-name kendra-role ^
          --assume-role-policy-document file://path/kendra-trust-policy.json
```

Dove:

- *path/* è il percorso del file `kendra-trust-policy.json` sul tuo dispositivo locale.

c. Copia Amazon Resource Name (ARN) nel tuo editor di testo e salvalo localmente con nome. `kendra-role-arn`

> **Note**
>
> L'ARN ha un formato simile a *arn:aws:iam: :123456789012:role/kendra-role*. Hai bisogno dell'ARN che hai salvato `kendra-role-arn` per eseguire i job di Amazon Kendra.

2. Prima di creare un indice, devi fornire `kendra-role` il permesso di scrivere su CloudWatch Logs. Per farlo, completa le seguenti fasi.

   a. Salva la seguente politica di affidabilità come file JSON richiamato `kendra-cloudwatch-policy.json` in un editor di testo sul tuo dispositivo locale.

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

Sostituisci *aws-region* con la tua AWS regione e *aws-account-id*con il tuo ID account a 12 cifreAWS.

b. Per creare una policy IAM per accedere ai CloudWatch log, usa il comando create-policy:

Linux

```
aws iam create-policy \
          --policy-name kendra-cloudwatch-policy \
          --policy-document file://path/kendra-cloudwatch-policy.json
```

Dove:

- *path/* è il percorso del file `kendra-cloudwatch-policy.json` sul tuo dispositivo locale.

macOS

```
aws iam create-policy \
          --policy-name kendra-cloudwatch-policy \
          --policy-document file://path/kendra-cloudwatch-policy.json
```

Dove:

- *path/* è il percorso del file `kendra-cloudwatch-policy.json` sul tuo dispositivo locale.

Windows

```
aws iam create-policy ^
          --policy-name kendra-cloudwatch-policy ^
```

```
        --policy-document file://path/kendra-cloudwatch-policy.json
```

Dove:

- *path/* è il percorso del file `kendra-cloudwatch-policy.json` sul tuo dispositivo locale.

c. Copia Amazon Resource Name (ARN) nel tuo editor di testo e salvalo localmente con nome. `kendra-cloudwatch-arn`

> **Note**
>
> L'ARN ha un formato simile a *arn:aws:iam: :123456789012:role/*. kendra-cloudwatch-policy Hai bisogno dell'ARN che hai salvato `kendra-cloudwatch-arn` per associarlo `kendra-cloudwatch-policy` al tuo ruolo IAM.

d. Per associarlo `kendra-cloudwatch-policy` al tuo ruolo IAM, usa il attach-role-policycomando:

Linux

```
aws iam attach-role-policy \
          --policy-arn policy-arn \
          --role-name kendra-role
```

Dove:

- *policy-arn* è il tuo salvataggio. `kendra-cloudwatch-arn`

macOS

```
aws iam attach-role-policy \
          --policy-arn policy-arn \
          --role-name kendra-role
```

Dove:

- *policy-arn* è il tuo salvataggio. `kendra-cloudwatch-arn`

Windows

```
aws iam attach-role-policy ^
          --policy-arn policy-arn ^
          --role-name kendra-role
```

Dove:

- *policy-arn* è il tuo salvataggio. `kendra-cloudwatch-arn`

3. Per creare un indice, usa il comando create-index:

Linux

```
aws kendra create-index \
        --name kendra-index \
        --edition DEVELOPER_EDITION \
        --role-arn role-arn \
        --region aws-region
```

Dove:

- *role-arn* è il tuo salvataggio, `kendra-role-arn`
- *aws-region è la tua AWS regione*.

macOS

```
aws kendra create-index \
        --name kendra-index \
        --edition DEVELOPER_EDITION \
        --role-arn role-arn \
        --region aws-region
```

Dove:

- *role-arn* è il tuo salvataggio, `kendra-role-arn`
- *aws-region è la tua AWS regione*.

Windows

```
aws kendra create-index ^
        --name kendra-index ^
        --edition DEVELOPER_EDITION ^
        --role-arn role-arn ^
        --region aws-region
```

Dove:

- *role-arn* è il tuo salvataggio, `kendra-role-arn`
- *aws-region è la tua AWS regione*.

4. Copia l'indice `Id` e salvalo in un editor di testo come`kendra-index-id`. Ti `Id` aiuta a tenere traccia dello stato della creazione dell'indice.
5. Per monitorare l'avanzamento del processo di creazione dell'indice, usa il comando describe-index:

Linux

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

Dove:

- *kendra-index-id*è il tuo salvato`kendra-index-id`,
- *aws-region è la tua AWS regione*.

macOS

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

Dove:

- *kendra-index-id*è il tuo salvato`kendra-index-id`,

- *aws-region è la tua AWS regione*.

Windows

```
aws kendra describe-index ^
        --id kendra-index-id ^
        --region aws-region
```

Dove:

- *kendra-index-id*è il tuo salvatokendra-index-id,
- *aws-region è la tua AWS regione*.

Il processo di creazione dell'indice richiede in media 15 minuti, ma può richiedere più tempo. Quando lo stato dell'indice è attivo, l'indice è pronto per l'uso. Durante la creazione dell'indice, puoi iniziare il passaggio successivo.

Se utilizzi AWS CLI in questo passaggio, crei e alleghi una policy IAM al tuo ruolo IAM di Amazon Kendra che fornisce al tuo indice le autorizzazioni per accedere al tuo bucket S3.

Aggiornamento del ruolo IAM per l'accesso ad Amazon S3

Durante la creazione dell'indice, aggiorni il tuo ruolo IAM di Amazon Kendra per consentire all'indice creato di leggere i dati dal tuo bucket Amazon S3. Per ulteriori informazioni, consulta i ruoli di accesso IAM per Amazon Kendra.

Per aggiornare il tuo ruolo IAM (Console)

1. Aprire la console IAM all'indirizzo https://console.aws.amazon.com/iam/.
2. Nel riquadro di navigazione a sinistra, scegli Ruoli e inserisci **kendra-role** nella casella di ricerca sopra il nome del ruolo.
3. Tra le opzioni suggerite, fai clic sukendra-role.
4. In Riepilogo, scegli Allega criteri.
5. In Allega autorizzazioni, nella casella di ricerca, inserisci **S3** e seleziona la casella di controllo accanto alla ReadOnlyAccess politica di AmazonS3 tra le opzioni suggerite.
6. Scegli Attach policy (Collega policy). Nella pagina di riepilogo, ora vedrai due politiche associate al ruolo IAM.

7. Torna alla console Amazon Kendra all'indirizzo https://console.aws.amazon.com/kendra/ e attendi che lo stato dell'indice passi da Creazione a Attivo prima di continuare con il passaggio successivo.

Per aggiornare il tuo ruolo IAM (AWS CLI)

1. Salva il testo seguente in un file JSON chiamato `kendra-S3-access-policy.json` in un editor di testo sul tuo dispositivo locale.

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

```
}
```

Sostituisci *DOC-EXAMPLE-BUCKET* con il nome del tuo bucket S3, *aws-region con la tua AWS regione*, con l'ID account a 12 cifre e *aws-account-id*con quello salvato. AWS *kendra-index-id*kendra-index-id

2. Per creare una policy IAM per accedere al tuo bucket S3, usa il comando create-policy:

   Linux

   ```
   aws iam create-policy \
             --policy-name kendra-S3-access-policy \
             --policy-document file://path/kendra-S3-access-policy.json
   ```

   Dove:

   - *path/* è il percorso del file kendra-S3-access-policy.json sul tuo dispositivo locale.

   macOS

   ```
   aws iam create-policy \
             --policy-name kendra-S3-access-policy \
             --policy-document file://path/kendra-S3-access-policy.json
   ```

   Dove:

   - *path/* è il percorso del file kendra-S3-access-policy.json sul tuo dispositivo locale.

   Windows

   ```
   aws iam create-policy ^
             --policy-name kendra-S3-access-policy ^
             --policy-document file://path/kendra-S3-access-policy.json
   ```

   Dove:

   - *path/* è il percorso del file kendra-S3-access-policy.json sul tuo dispositivo locale.

3. Copia Amazon Resource Name (ARN) nel tuo editor di testo e salvalo localmente con nome. kendra-S3-access-arn

> **Note**
>
> L'ARN ha un formato simile a *arn:aws:iam: :123456789012:role/Kendra-S3-access-policy*. Hai bisogno dell'ARN che hai salvato `kendra-S3-access-arn` per associarlo `kendra-S3-access-policy` al tuo ruolo IAM.

4. Per associarlo `kendra-S3-access-policy` al tuo ruolo IAM di Amazon Kendra, usa il attach-role-policycomando:

   Linux

   ```
   aws iam attach-role-policy \
            --policy-arn policy-arn \
            --role-name kendra-role
   ```

   Dove:

   - *policy-arn* è il tuo salvataggio. `kendra-S3-access-arn`

   macOS

   ```
   aws iam attach-role-policy \
            --policy-arn policy-arn \
            --role-name kendra-role
   ```

   Dove:

   - *policy-arn* è il tuo salvataggio. `kendra-S3-access-arn`

   Windows

   ```
   aws iam attach-role-policy ^
            --policy-arn policy-arn ^
            --role-name kendra-role
   ```

   Dove:

   - *policy-arn* è il tuo salvataggio. `kendra-S3-access-arn`

Creazione di campi dell'indice di ricerca personalizzati di Amazon Kendra

Per preparare Amazon Kendra a riconoscere i tuoi metadati come attributi personalizzati del documento, crei campi personalizzati corrispondenti ai tipi di entità Amazon Comprehend. Inserisci i seguenti nove tipi di entità Amazon Comprehend come campi personalizzati:

- OGGETTO_COMMERCIALE
- DATE
- EVENT
- LOCATION
- ORGANIZZAZIONE
- OTHER
- PERSONA
- QUANTITÀ
- TITOLO

> **Important**
>
> I tipi di entità con errori di ortografia non verranno riconosciuti dall'indice.

Per creare campi personalizzati per il tuo indice Amazon Kendra (Console)

1. Apri la console Amazon Kendra all'indirizzo https://console.aws.amazon.com/kendra/.
2. Dall'elenco degli indici, fare clic su. `kendra-index`
3. Nel pannello di navigazione a sinistra, in Gestione dati, scegli Definizione delle faccette.
4. Dal menu Campi indice, scegli Aggiungi campo.
5. Nella finestra di dialogo Aggiungi campo indice, effettuate le seguenti operazioni:
   a. In Nome campo, inserisci**`COMMERCIAL_ITEM`**.
   b. In Tipo di dati, scegli Elenco stringhe.
   c. In Tipi di utilizzo, seleziona Facetable, Ricercabile e Visualizzabile, quindi scegli Aggiungi.
   d. Ripeti i passaggi da a c per ogni tipo di entità Amazon Comprehend: COMMERCIAL_ITEM, DATE, EVENT, LOCATION, ORGANIZATION, OTHER, PERSON, QUANTITY, TITLE.

La console visualizza i messaggi di corretta aggiunta dei campi. Puoi scegliere di chiuderli prima di procedere con il passaggio successivo.

Per creare campi personalizzati per il tuo indice Amazon Kendra () AWS CLI

1. Salva il testo seguente come file JSON chiamato `custom-attributes.json` in un editor di testo sul tuo dispositivo locale.

```
[
   {
       "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. Per creare campi personalizzati nel tuo indice, usa il comando update-index:

   Linux

   ```
   aws kendra update-index \
           --id kendra-index-id \
           --document-metadata-configuration-updates file://path/custom-
   attributes.json \
           --region aws-region
   ```

   Dove:

   - *kendra-index-id*è il tuo salvatokendra-index-id,
   - *path/* è il percorso del file custom-attributes.json sul tuo dispositivo locale,
   - *aws-region è la tua AWS regione*.

   macOS

   ```
   aws kendra update-index \
           --id kendra-index-id \
           --document-metadata-configuration-updates file://path/custom-
   attributes.json \
           --region aws-region
   ```

   Dove:

   - *kendra-index-id*è il tuo salvatokendra-index-id,
   - *path/* è il percorso del file custom-attributes.json sul tuo dispositivo locale,
   - *aws-region è la tua AWS regione*.

   Windows

   ```
   aws kendra update-index ^
           --id kendra-index-id ^
   ```

```
        --document-metadata-configuration-updates file://path/custom-
attributes.json ^
        --region aws-region
```

Dove:

- *kendra-index-id*è il tuo salvatokendra-index-id,
- *path/* è il percorso del file custom-attributes.json sul tuo dispositivo locale,
- *aws-region è la tua AWS regione*.

3. Per verificare che gli attributi personalizzati siano stati aggiunti al tuo indice, usa il comando describe-index:

Linux

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

Dove:

- *kendra-index-id*è il tuo salvatokendra-index-id,
- *aws-region è la tua AWS regione*.

macOS

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

Dove:

- *kendra-index-id*è il tuo salvatokendra-index-id,
- *aws-region è la tua AWS regione*.

Windows

```
aws kendra describe-index ^
```

```
        --id kendra-index-id ^
        --region aws-region
```

Dove:

- *kendra-index-id*è il tuo salvato`kendra-index-id`,
- *aws-region è la tua AWS regione*.

Aggiungere il bucket Amazon S3 come origine dati per l'indice

Prima di poter sincronizzare l'indice, devi connettere la tua sorgente dati S3 ad esso.

Per connettere un bucket S3 al tuo indice Amazon Kendra (console)

1. Apri la console Amazon Kendra all'indirizzo https://console.aws.amazon.com/kendra/.
2. Dall'elenco degli indici, fare clic su. `kendra-index`
3. Dal menu di navigazione a sinistra, in Gestione dati, scegli Origini dati.
4. Nella sezione Seleziona il tipo di connettore di origine dati, accedi ad Amazon S3 e scegli Aggiungi connettore.
5. Nella pagina Specifica i dettagli dell'origine dati, procedi come segue:
    a. In Nome e descrizione, per Nome origine dati, immettere**`S3-data-source`**.
    b. Mantieni vuota la sezione Descrizione.
    c. Mantieni le impostazioni predefinite per i tag.
    d. Seleziona Successivo.
6. Nella pagina Configurazione delle impostazioni di sincronizzazione, nella sezione Ambito della sincronizzazione, procedi come segue:
    a. In Inserisci la posizione dell'origine dei dati, scegli Sfoglia S3.
    b. In Scegli risorse, seleziona il tuo bucket S3, quindi scegli Scegli.
    c. Nella cartella del prefisso dei file di metadati, scegli Sfoglia S3.
    d. In Scegli risorse, fai clic sul nome del tuo bucket dall'elenco dei bucket.
    e. Per Oggetti, selezionate la casella di opzione `metadata` e scegliete Scegli. Il campo della posizione dovrebbe ora indicare`metadata/`.

f. Mantieni le impostazioni predefinite per la posizione del file di configurazione della lista di controllo di accesso, Seleziona la chiave di decrittografia e la configurazione aggiuntiva.

7. Per il ruolo IAM, nella pagina Configura le impostazioni di sincronizzazione, scegli`kendra-role`.
8. Nella pagina Configura le impostazioni di sincronizzazione, in Pianificazione dell'esecuzione della sincronizzazione, per Frequenza, scegli Esegui su richiesta e quindi scegli Avanti.
9. Nella pagina Rivedi e crea, rivedi le tue scelte per i dettagli dell'origine dati e scegli Aggiungi origine dati.

Per connettere un bucket S3 al tuo indice Amazon Kendra () AWS CLI

1. Salva il testo seguente come file JSON chiamato `S3-data-connector.json` in un editor di testo sul tuo dispositivo locale.

```
{
   "S3Configuration":{
      "BucketName":"DOC-EXAMPLE-BUCKET",
      "DocumentsMetadataConfiguration":{
         "S3Prefix":"metadata"
      }
   }
}
```

   Sostituisci *`DOC-EXAMPLE-BUCKET con il nome del tuo bucket S3`*.

2. Per connettere il tuo bucket S3 al tuo indice, usa il create-data-sourcecomando:

   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
```

   Dove:

   - *`kendra-index-id`*è il tuo salvato`kendra-index-id`,

- *path/* è il percorso del file S3-data-connector.json sul tuo dispositivo locale,
- *role-arn* è il tuo salvataggio, kendra-role-arn
- *aws-region è la tua AWS regione*.

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
```

Dove:

- *kendra-index-id*è il tuo salvatokendra-index-id,
- *path/* è il percorso del file S3-data-connector.json sul tuo dispositivo locale,
- *role-arn* è il tuo salvataggio, kendra-role-arn
- *aws-region è la tua AWS regione*.

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
```

Dove:

- *kendra-index-id*è il tuo salvatokendra-index-id,
- *path/* è il percorso del file S3-data-connector.json sul tuo dispositivo locale,
- *role-arn* è il tuo salvataggio, kendra-role-arn
- *aws-region è la tua AWS regione*.

3. Copia il connettore `Id` e salvalo in un editor di testo come`S3-connector-id`. Ti `Id` aiuta a tenere traccia dello stato del processo di connessione dati.
4. Per assicurarti che la tua sorgente dati S3 sia stata connessa correttamente, usa il describe-data-sourcecomando:

   Linux

   ```
   aws kendra describe-data-source \
           --id S3-connector-id \
           --index-id kendra-index-id \
           --region aws-region
   ```

   Dove:

   - *S3-connector-ID* è il tuo salvataggio, `S3-connector-id`
   - *kendra-index-id*è il tuo salvato`kendra-index-id`,
   - *aws-region è la tua AWS regione*.

   macOS

   ```
   aws kendra describe-data-source \
           --id S3-connector-id \
           --index-id kendra-index-id \
           --region aws-region
   ```

   Dove:

   - *S3-connector-ID* è il tuo salvataggio, `S3-connector-id`
   - *kendra-index-id*è il tuo salvato`kendra-index-id`,
   - *aws-region è la tua AWS regione*.

   Windows

   ```
   aws kendra describe-data-source ^
           --id S3-connector-id ^
           --index-id kendra-index-id ^
           --region aws-region
   ```

Dove:

- *S3-connector-ID* è il tuo salvataggio, `S3-connector-id`
- *kendra-index-id*è il tuo salvato`kendra-index-id`,
- *aws-region è la tua AWS regione*.

Al termine di questo passaggio, la tua origine dati Amazon S3 è connessa all'indice.

Sincronizzazione dell'indice Amazon Kendra

Con l'aggiunta della fonte dati Amazon S3, ora puoi sincronizzare il tuo indice Amazon Kendra con essa.

Per sincronizzare il tuo indice Amazon Kendra (Console)

1. Apri la console Amazon Kendra all'indirizzo https://console.aws.amazon.com/kendra/.
2. Dall'elenco degli indici, fare clic su. `kendra-index`
3. Dal menu di navigazione a sinistra, scegli Origini dati.
4. Da Origini dati, seleziona`S3-data-source`.
5. Dalla barra di navigazione in alto, scegli Sincronizza ora.

Per sincronizzare il tuo indice Amazon Kendra () AWS CLI

1. Per sincronizzare il tuo indice, usa il comando 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
   ```

   Dove:

   - *S3-connector-ID* è il tuo salvataggio, `S3-connector-id`
   - *kendra-index-id*è il tuo salvato`kendra-index-id`,
   - *aws-region è la tua AWS regione*.

macOS

```
aws kendra start-data-source-sync-job \
        --id S3-connector-id \
        --index-id kendra-index-id \
        --region aws-region
```

Dove:

- *S3-connector-ID* è il tuo salvataggio, `S3-connector-id`
- *kendra-index-id*è il tuo salvato`kendra-index-id`,
- *aws-region è la tua AWS regione*.

Windows

```
aws kendra start-data-source-sync-job ^
        --id S3-connector-id ^
        --index-id kendra-index-id ^
        --region aws-region
```

Dove:

- *S3-connector-ID* è il tuo salvataggio, `S3-connector-id`
- *kendra-index-id*è il tuo salvato`kendra-index-id`,
- *aws-region è la tua AWS regione*.

2. Per verificare lo stato della sincronizzazione dell'indice, usa il comando 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
```

Dove:

- *S3-connector-ID* è il tuo salvataggio, `S3-connector-id`
- *kendra-index-id*è il tuo salvato`kendra-index-id`,
- *aws-region è la tua AWS regione*.

macOS

```
aws kendra list-data-source-sync-jobs \
        --id S3-connector-id \
        --index-id kendra-index-id \
        --region aws-region
```

Dove:

- *S3-connector-ID* è il tuo salvataggio, `S3-connector-id`
- *kendra-index-id*è il tuo salvato`kendra-index-id`,
- *aws-region è la tua AWS regione*.

Windows

```
aws kendra list-data-source-sync-jobs ^
        --id S3-connector-id ^
        --index-id kendra-index-id ^
        --region aws-region
```

Dove:

- *S3-connector-ID* è il tuo salvataggio, `S3-connector-id`
- *kendra-index-id*è il tuo salvato`kendra-index-id`,
- *aws-region è la tua AWS regione*.

Al termine di questo passaggio, hai creato un indice Amazon Kendra ricercabile e filtrabile per il tuo set di dati.

Fase 5: Interrogare l'indice Amazon Kendra

Il tuo indice Amazon Kendra è ora pronto per le interrogazioni in linguaggio naturale. Quando effettui una ricerca nell'indice, Amazon Kendra utilizza tutti i dati e i metadati che hai fornito per restituire le risposte più accurate alla tua query di ricerca.

Esistono tre tipi di domande a cui Amazon Kendra può rispondere:

- Domande fattuali (domande su «chi», «cosa», «quando» o «dove»)
- Domande descrittive (domande «come»)
- Ricerche per parole chiave (domande il cui scopo e scopo non sono chiari)

Argomenti

Interrogare il tuo indice Amazon Kendra

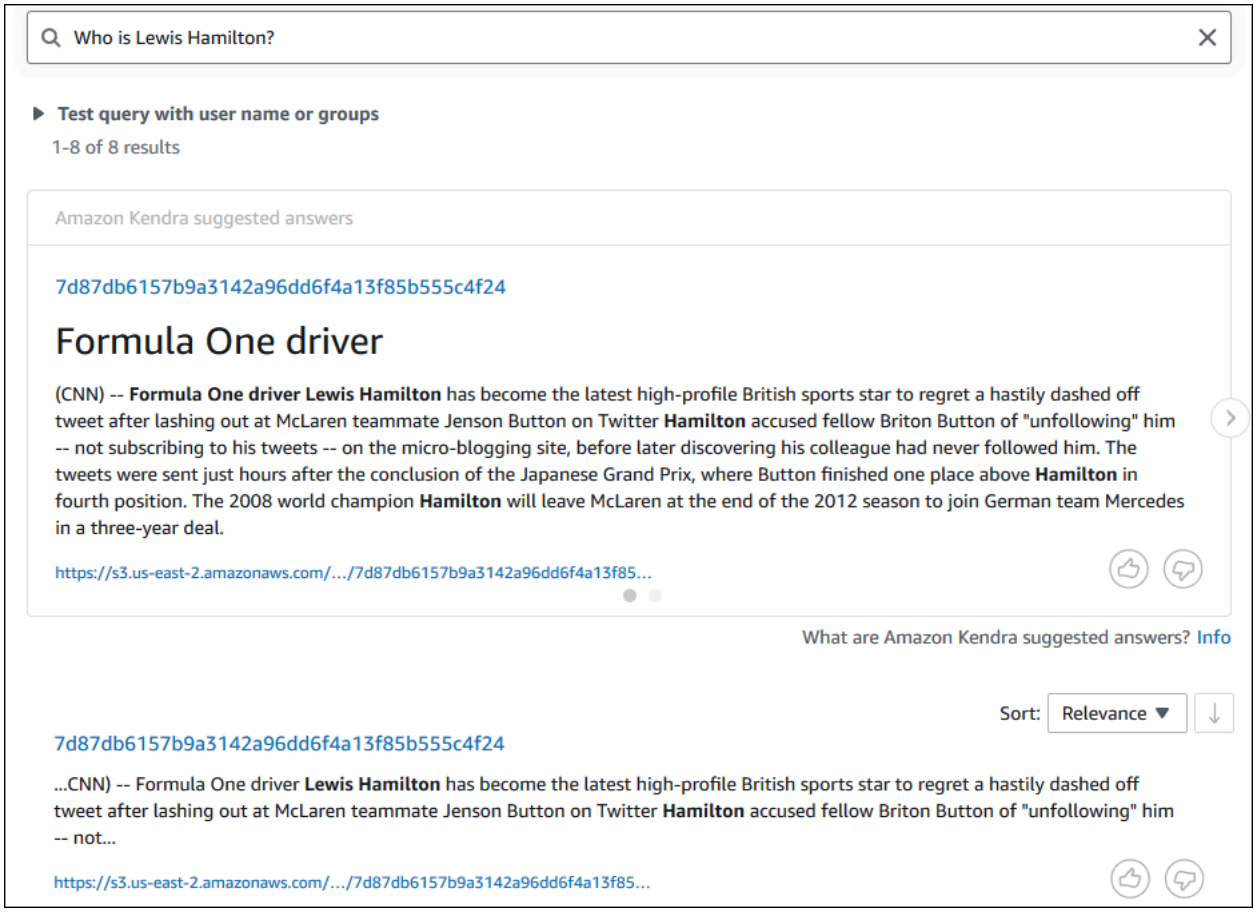
Puoi interrogare il tuo indice Amazon Kendra utilizzando domande che corrispondono ai tre tipi di query supportati da Amazon Kendra. Per ulteriori informazioni, consulta Interrogazioni.

Le domande di esempio in questa sezione sono state scelte in base al set di dati di esempio.

Per interrogare il tuo indice Amazon Kendra (Console)

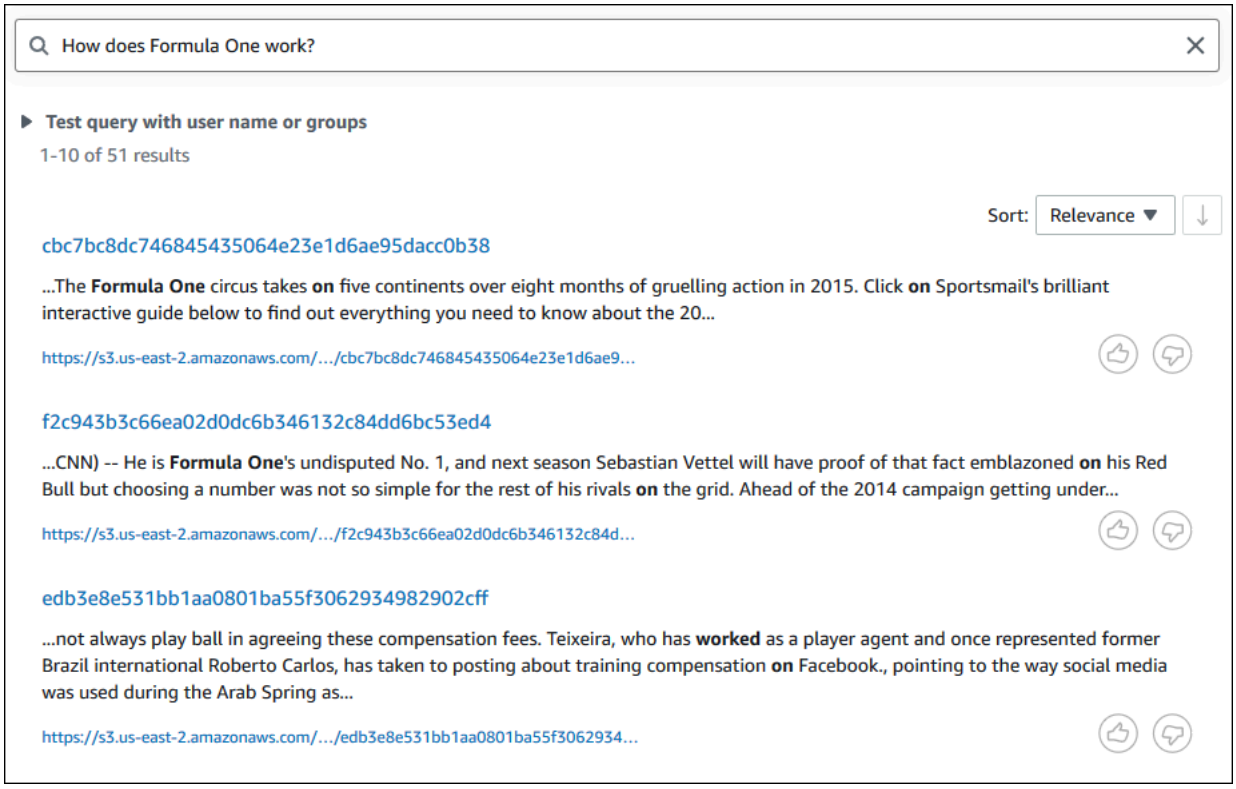
1. Apri la console Amazon Kendra all'indirizzo https://console.aws.amazon.com/kendra/.
2. Dall'elenco degli indici, fare clic su. `kendra-index`
3. Dal menu di navigazione a sinistra, scegli l'opzione per cercare nel tuo indice.
4. Per eseguire una query factoid di esempio, inserisci **`Who is Lewis Hamilton?`** nella casella di ricerca e premi invio.

   Il primo risultato restituito è la risposta suggerita da Amazon Kendra, insieme al file di dati contenente la risposta. Il resto dei risultati costituisce l'insieme dei documenti consigliati.



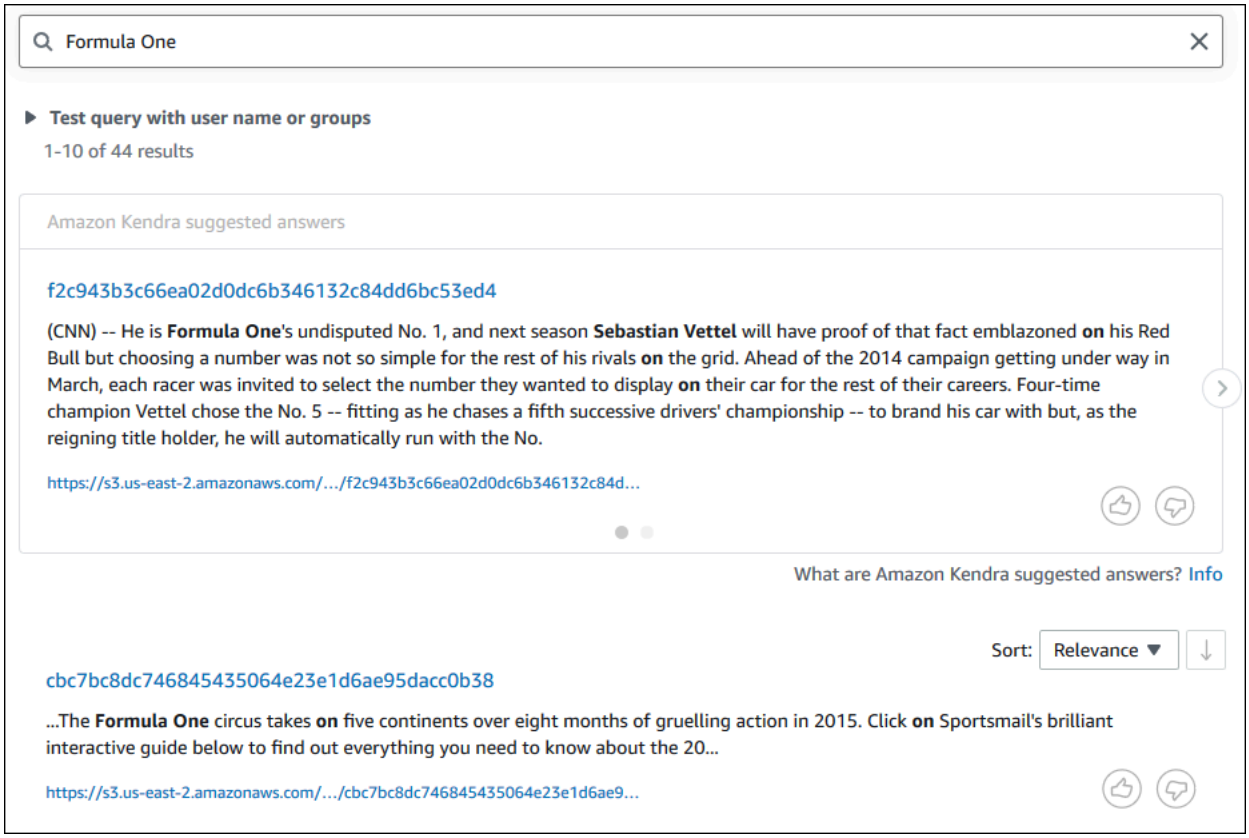
5. Per eseguire una query descrittiva, inserisci **`How does Formula One work?`** la casella di ricerca e premi invio.

   Vedrai un altro risultato restituito dalla console Amazon Kendra, questa volta con la frase pertinente evidenziata.



6. Per eseguire una ricerca per parola chiave, inserisci **`Formula One`** nella casella di ricerca e premi invio.

   Vedrai un altro risultato restituito dalla console Amazon Kendra, seguito dai risultati per tutte le altre menzioni della frase nel set di dati.



Per interrogare il tuo indice Amazon Kendra () AWS CLI

1. Per eseguire una query factoid di esempio, usa il comando query:

   Linux

   ```
   aws kendra query \
           --index-id kendra-index-id \
           --query-text "Who is Lewis Hamilton?" \
           --region aws-region
   ```

   Dove:

   - *kendra-index-id*è il tuo salvatokendra-index-id,
   - *aws-region è la tua AWS regione*.

macOS

```
aws kendra query \
        --index-id kendra-index-id \
        --query-text "Who is Lewis Hamilton?" \
        --region aws-region
```

Dove:

- *kendra-index-id*è il tuo salvatokendra-index-id,
- *aws-region è la tua AWS regione*.

Windows

```
aws kendra query ^
        --index-id kendra-index-id ^
        --query-text "Who is Lewis Hamilton?" ^
        --region aws-region
```

Dove:

- *kendra-index-id*è il tuo salvatokendra-index-id,
- *aws-region è la tua AWS regione*.

AWS CLIVisualizza i risultati della tua ricerca.

2. Per eseguire una query descrittiva di esempio, usa il comando query:

Linux

```
aws kendra query \
        --index-id kendra-index-id \
        --query-text "How does Formula One work?" \
        --region aws-region
```

Dove:

- *kendra-index-id*è il tuo salvatokendra-index-id,

- *aws-region è la tua AWS regione*.

macOS

```
aws kendra query \
        --index-id kendra-index-id \
        --query-text "How does Formula One work?" \
        --region aws-region
```

Dove:

- *kendra-index-id*è il tuo salvatokendra-index-id,
- *aws-region è la tua AWS regione*.

Windows

```
aws kendra query ^
        --index-id kendra-index-id ^
        --query-text "How does Formula One work?" ^
        --region aws-region
```

Dove:

- *kendra-index-id*è il tuo salvatokendra-index-id,
- *aws-region è la tua AWS regione*.

AWS CLIVisualizza i risultati della tua ricerca.

3. Per eseguire una ricerca di esempio per parola chiave, usa il comando query:

Linux

```
aws kendra query \
        --index-id kendra-index-id \
        --query-text "Formula One" \
        --region aws-region
```

Dove:

- *kendra-index-id*è il tuo salvatokendra-index-id,
- *aws-region è la tua AWS regione*.

macOS

```
aws kendra query \
        --index-id kendra-index-id \
        --query-text "Formula One" \
        --region aws-region
```

Dove:

- *kendra-index-id*è il tuo salvatokendra-index-id,
- *aws-region è la tua AWS regione*.

Windows

```
aws kendra query ^
        --index-id kendra-index-id ^
        --query-text "Formula One" ^
        --region aws-region
```

Dove:

- *kendra-index-id*è il tuo salvatokendra-index-id,
- *aws-region è la tua AWS regione*.

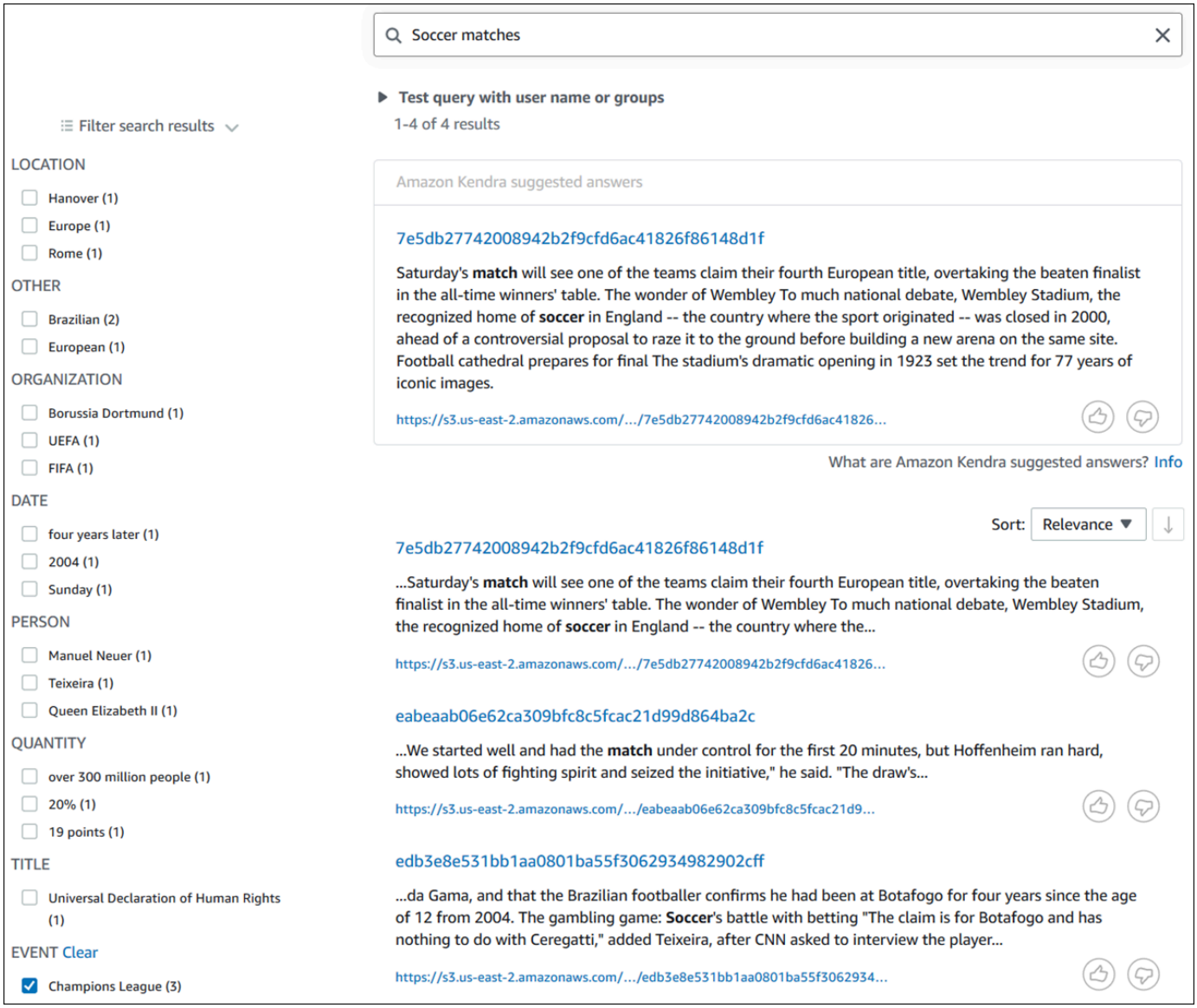
AWS CLIVisualizza le risposte restituite alla tua richiesta.

Filtrare i risultati della ricerca

Puoi filtrare e ordinare i risultati della ricerca utilizzando attributi di documento personalizzati nella console Amazon Kendra. Per ulteriori informazioni su come Amazon Kendra elabora le query, consulta Filtrare le query.

Per filtrare i risultati della ricerca (Console)

1. Apri la console Amazon Kendra all'indirizzo https://console.aws.amazon.com/kendra/.
2. Dall'elenco degli indici, fare clic su. `kendra-index`
3. Dal menu di navigazione a sinistra, scegli l'opzione per cercare nel tuo indice.
4. Nella casella di ricerca, inserisci **`Soccer matches`** come query e premi invio.
5. Dal menu di navigazione a sinistra, scegli Filtra i risultati della ricerca per visualizzare un elenco di sfaccettature che puoi utilizzare per filtrare la ricerca.
6. Seleziona la casella di controllo «Champions League» sotto il sottotitolo EVENTO, per visualizzare i risultati della ricerca filtrati solo in base ai risultati che contengono «Champions League».



Per filtrare i risultati della ricerca (AWS CLI)

1. Per visualizzare le entità di un tipo specifico (ad esempioEVENT) disponibili per una ricerca, usa il comando query:

   Linux

```
aws kendra query \
        --index-id kendra-index-id \
        --query-text "Soccer matches" \
        --facets '[{"DocumentAttributeKey":"EVENT"}]' \
        --region aws-region
```

Dove:

- *kendra-index-id*è il tuo salvatokendra-index-id,
- *aws-region è la tua AWS regione*.

macOS

```
aws kendra query \
        --index-id kendra-index-id \
        --query-text "Soccer matches" \
        --facets '[{"DocumentAttributeKey":"EVENT"}]' \
        --region aws-region
```

Dove:

- *kendra-index-id*è il tuo salvatokendra-index-id,
- *aws-region è la tua AWS regione*.

Windows

```
aws kendra query ^
        --index-id kendra-index-id ^
        --query-text "Soccer matches" ^
        --facets '[{"DocumentAttributeKey":"EVENT"}]' ^
        --region aws-region
```

Dove:

- *kendra-index-id*è il tuo salvatokendra-index-id,
- *aws-region è la tua AWS regione*.

AWS CLIVisualizza i risultati della ricerca. Per ottenere un elenco di sfaccettature di tipoEVENT, vai alla sezione "FacetResults" dell'AWS CLIoutput per visualizzare un elenco di sfaccettature filtrabili con i relativi conteggi. Ad esempio, una delle sfaccettature è la «Champions League».

> **Note**
>
> InveceEVENT, puoi scegliere uno qualsiasi dei campi indice che hai creato the section called “Creazione di un indice Amazon Kendra” per il `DocumentAttributeKey` valore.

2. Per eseguire la stessa ricerca ma filtrare solo in base ai risultati che contengono «Champions League», usa il comando di ricerca:

   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
   ```

   Dove:

   - *kendra-index-id*è il tuo salvato`kendra-index-id`,
   - *aws-region è la tua AWS regione*.

   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
   ```

   Dove:

   - *kendra-index-id*è il tuo salvato`kendra-index-id`,
   - *aws-region è la tua AWS regione*.

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
```

Dove:

- *kendra-index-id*è il tuo salvato`kendra-index-id`,
- *aws-region è la tua AWS regione*.

AWS CLIVisualizza i risultati della ricerca filtrati.

Fase 6: Pulizia

Ripulire i file

Per non incorrere più in addebiti AWS sul tuo account dopo aver completato questo tutorial, puoi seguire i seguenti passaggi:

1. Elimina il tuo bucket Amazon S3

   Per informazioni sull'eliminazione di un bucket, vedere Eliminazione di un bucket.
2. Elimina il tuo indice Amazon Kendra

   Per informazioni sull'eliminazione di un indice Amazon Kendra, consulta Eliminazione di un indice.
3. Eliminare **`converter.py`**
   - Per console: vai a AWS CloudShelle assicurati che la regione sia impostata sulla tua AWS regione. Dopo il caricamento della shell bash, digita il seguente comando nell'ambiente e premi invio.

     ```
     rm converter.py
     ```

- PerAWS CLI: Esegui il seguente comando su una finestra di terminale.

  Linux

  ```
  rm file/converter.py
  ```

  Dove:

  - *file/* è il percorso del file `converter.py` sul dispositivo locale.

  macOS

  ```
  rm file/converter.py
  ```

  Dove:

  - *file/* è il percorso del file `converter.py` sul dispositivo locale.

  Windows

  ```
  rm file/converter.py
  ```

  Dove:

  - *file/* è il percorso del file `converter.py` sul dispositivo locale.

Ulteriori informazioni

Per ulteriori informazioni sull'integrazione di Amazon Kendra nel tuo flusso di lavoro, consulta i seguenti post sul blog:

- Codifica dei metadati dei contenuti per una ricerca avanzata
- Crea una soluzione di ricerca intelligente con arricchimento automatico dei contenuti

Per ulteriori informazioni su Amazon Comprehend, puoi consultare la Amazon Comprehend Developer Guide.

Monitoraggio e log per Amazon Kendra

Argomenti

Monitoraggio dell'indice (console)

Usa la console Amazon Kendra per monitorare lo stato degli indici e delle fonti di dati. È possibile utilizzare queste informazioni per tenere traccia delle dimensioni e dei requisiti di archiviazione dell'indice e per monitorare l'avanzamento e il successo della sincronizzazione tra l'indice e le fonti di dati.

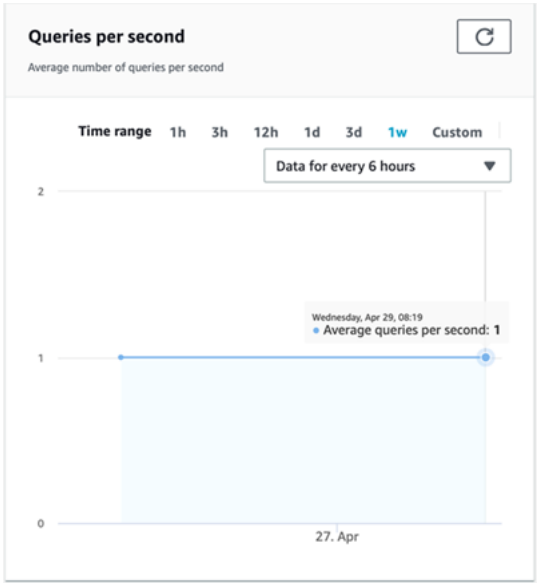
Per visualizzare le metriche dell'indice (console)

1. Accedi AWS Management Console e apri la console Amazon Kendra all'indirizzo https://console.aws.amazon.com/kendra/home.
2. Dall'elenco degli indici, scegli l'indice da visualizzare.
3. Scorri la schermata per visualizzare le metriche dell'indice.

Puoi visualizzare le seguenti metriche sul tuo indice.

- Numero di documenti: il numero totale di documenti indicizzati. Ciò include tutti i documenti provenienti da tutte le fonti di dati. Usa questa metrica per determinare se devi acquistare più o meno unità di archiviazione per il tuo indice.

- Interrogazioni al secondo: il numero di query sull'indice richieste ogni secondo. Usa questa metrica per determinare se devi acquistare più o meno unità di query per il tuo indice.



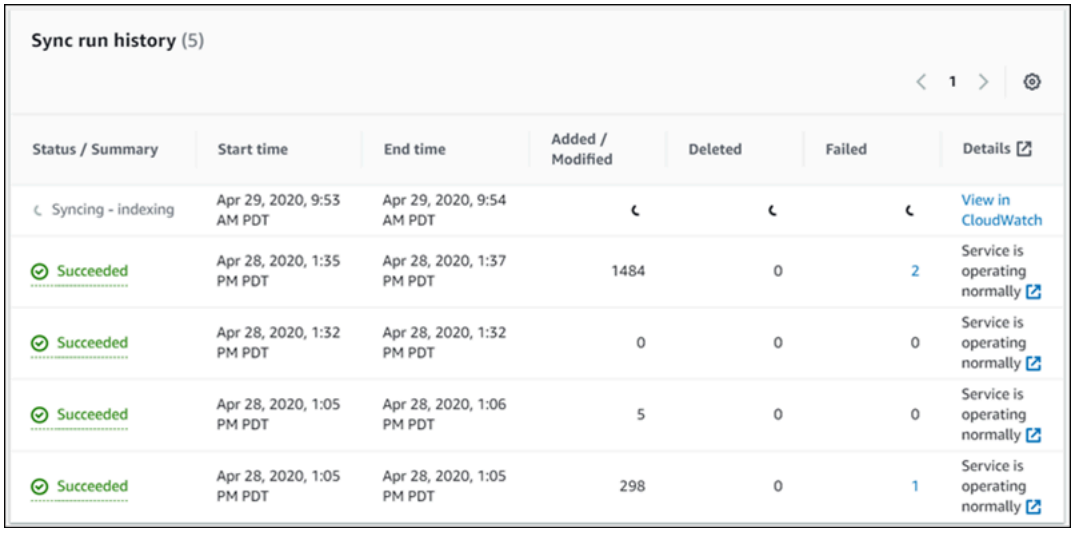
Per monitorare l'avanzamento e il successo della sincronizzazione tra il tuo indice e una fonte di dati, utilizza la console Amazon Kendra. Usa queste informazioni per determinare lo stato della tua fonte di dati.

Per visualizzare le metriche di sincronizzazione (console)

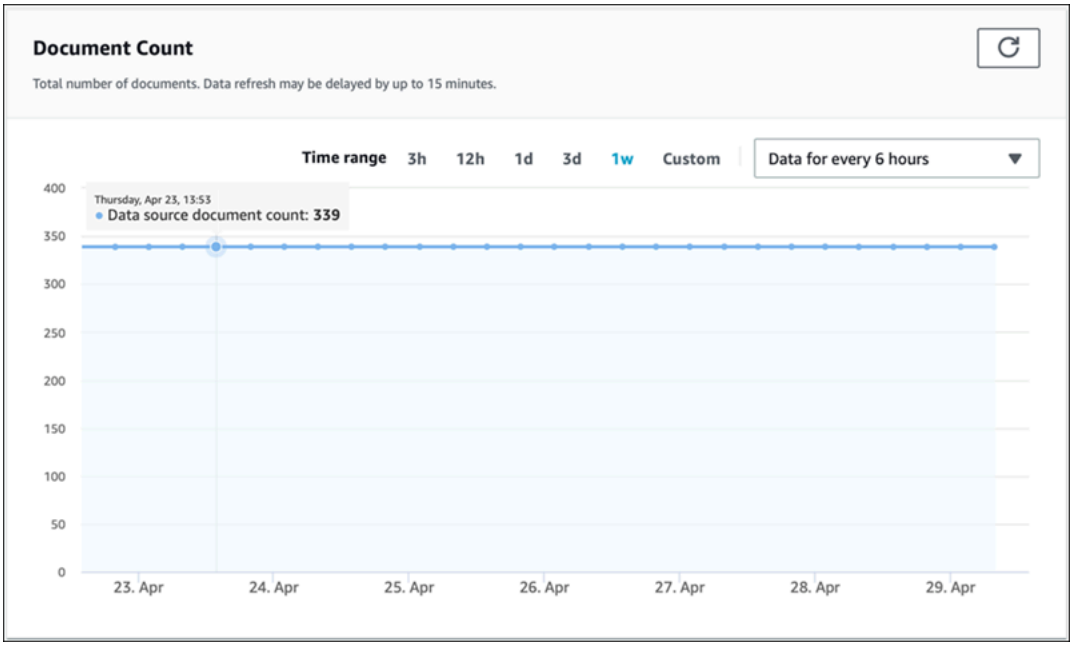
1. Accedi AWS Management Console e apri la console Amazon Kendra all'indirizzo https://console.aws.amazon.com/kendra/home.
2. Dall'elenco degli indici, scegli l'indice per cui visualizzare le metriche di sincronizzazione.
3. Dal menu a sinistra, scegli Origini dati.
4. Dall'elenco delle origini dati, scegli l'origine dati da visualizzare.
5. Scorri lo schermo per visualizzare le metriche dell'esecuzione della sincronizzazione.

È possibile visualizzare le seguenti informazioni.

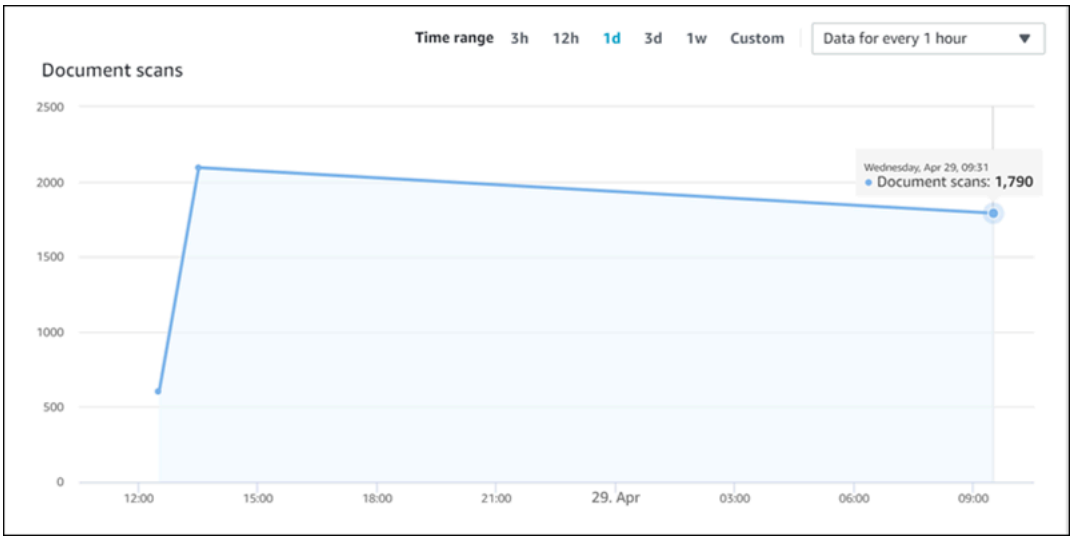
- Cronologia dell'esecuzione della sincronizzazione: statistiche sull'esecuzione della sincronizzazione, tra cui l'ora di inizio e di fine, il numero di documenti aggiunti, eliminati e non riusciti. Se l'esecuzione della sincronizzazione fallisce, è disponibile un collegamento a CloudWatch Registri con ulteriori informazioni. Scegli l'icona delle impostazioni in alto a sinistra per modificare le colonne visualizzate nella cronologia. Usa queste informazioni per determinare lo stato generale della tua fonte di dati.



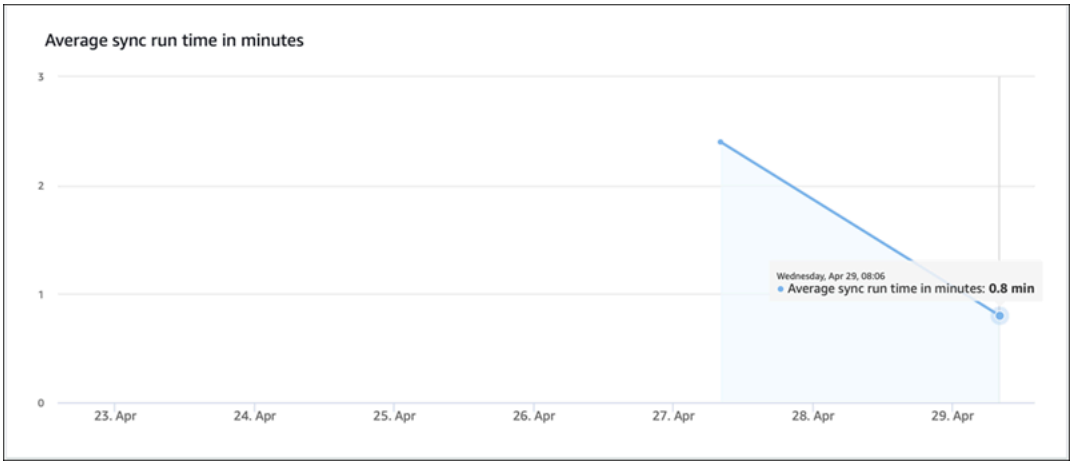
- Numero di documenti: il numero totale di documenti indicizzati da questa fonte di dati. Si tratta del totale di tutti i documenti aggiunti all'origine dati meno il totale di tutti i documenti eliminati dall'origine dati. Usa queste informazioni per determinare quanti documenti di questa fonte di dati sono inclusi nell'indice.



- Scansioni dei documenti: il numero totale di documenti scansionati durante l'esecuzione della sincronizzazione. Ciò include tutti i documenti nella fonte dei dati, inclusi quelli aggiunti, aggiornati, eliminati o immutati. Usa queste informazioni per determinare se Amazon Kendra sta scansionando tutti i documenti nella fonte di dati. Il numero di documenti scansionati influisce sull'importo addebitato per il servizio.



- Tempo medio di esecuzione della sincronizzazione in minuti: il tempo medio necessario per il completamento di un'esecuzione di sincronizzazione. Il tempo necessario per sincronizzare un'origine dati influisce sull'importo addebitato per il servizio.



Registrazione delle chiamate API di Amazon Kendra conAWS CloudTrailregistri

Amazon Kendra è integrato conAWS CloudTrail, un servizio che fornisce una registrazione delle operazioni eseguite da un utente, un ruolo o unAWSservizio in Amazon Kendra. CloudTrail acquisisce tutte le chiamate API da Amazon Kendra come eventi, incluse le chiamate dalla console di Amazon Kendra e le chiamate di codice alle API di Amazon Kendra di Amazon Kendra di Amazon Kendra. Se si crea un percorso, è possibile attivare la consegna continua di CloudTrail eventi per un bucket Amazon S3, inclusi gli eventi per Amazon Kendra. Se non si configura un percorso, è comunque possibile visualizzare gli eventi più recenti nella CloudTrail console inCronologia degli eventi. Utilizzo delle informazioni raccolte da CloudTrail, è possibile determinare la richiesta inviata ad Amazon Kendra, l'indirizzo IP da cui è stata effettuata, chi ha effettuato la richiesta, quando è stata effettuata e altri dettagli.

Per ulteriori informazioni su CloudTrail, incluso come configurarlo e attivarlo, vedi ilAWS CloudTrailGuida per l'utente.

Informazioni su Amazon Kendra possono contenere CloudTrail

CloudTrail è attivato sul tuoAWSaccount al momento della creazione dell'account. Quando si verifica un'operazione in Amazon Kendra, tale operazione viene registrata in un CloudTrail evento insieme ad altriAWSeventi di service CloudTrail cronologia degli eventi. È possibile visualizzare, cercare e scaricare gli eventi recenti nell'account AWS. Per ulteriori informazioni, consulta Visualizzazione di eventi mediante la cronologia eventi di CloudTrail.

Per una registrazione continua di tutti gli eventi dellaAWSaccount, inclusi gli eventi per Amazon Kendra, crea un percorso. UNpistaè una configurazione che consente CloudTrail per fornire eventi come file di registro a un bucket S3 specificato. Per impostazione predefinita, quando si crea un trail nella console, il trail sarà valido in tutte le regioni AWS. Il trail registra gli eventi di tutte le regioni nella partizione AWS e distribuisce i file di log nel bucket S3 specificato. Inoltre, puoi configurare altriAWSservizi per analizzare ulteriormente e agire in base ai dati degli eventi raccolti in CloudTrail registri. Per ulteriori informazioni, consultare:

- Panoramica della creazione di un percorso
- CloudTrail Servizi e integrazioni supportati
- Configurazione delle notifiche Amazon SNS per CloudTrail
- Ricezione CloudTrail I file di log di più areeeRicezione CloudTrail I file di log di più account

CloudTrail registra tutte le azioni di Amazon Kendra, che sono documentate nelRiferimento alle API. Ad esempio, le chiamate a`CreateIndex`,`CreateDataSource`, e`Query`le operazioni generano voci nel CloudTrail file di log.

Ogni evento o voce di log contiene informazioni sull'utente che ha generato la richiesta. Per ulteriori informazioni, consulta Elemento CloudTrail userIdentity.

Esempio: voci di log di Amazon Kendra

UNpistaè una configurazione che consente la consegna di eventi come file di registro a un bucket S3 specificato. CloudTrail I file di log possono contenere una o più voci di log. Uneventorappresenta una singola richiesta da qualsiasi fonte e include informazioni sull'operazione richiesta, la data e l'ora dell'operazione, i parametri della richiesta e così via. CloudTrail i file di registro non sono una traccia di stack ordinata delle chiamate API pubbliche, quindi non vengono visualizzati in un ordine specifico.

Chiamate al`Query`l'operazione può contenere la voce seguente.

```
       {
           "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"
    },
```

Registrazione delle chiamate all'API di Ranking di Amazon Kendra conAWS CloudTrailregistri

Amazon Kendra Intelligent Ranking è integrato conAWS CloudTrail, un servizio che fornisce una registrazione delle operazioni eseguite da un utente, un ruolo o unAWSservizio in Amazon Kendra Ranking di Amazon Kendra. CloudTrail acquisisce tutte le chiamate API da Amazon Kendra Intelligent Ranking di Amazon Kendra, incluse le chiamate di codice alle API di Intelligent Ranking di Amazon Kendra. Se si crea un percorso, è possibile attivare la consegna continua di CloudTrail

eventi per un bucket Amazon S3, inclusi gli eventi per Amazon Kendra Ranking di Amazon Kendra. Se non si configura un percorso, è comunque possibile visualizzare gli eventi più recenti nella CloudTrail console inCronologia degli eventi. Utilizzo delle informazioni raccolte da CloudTrail, è possibile determinare la richiesta inviata ad Amazon Kendra Intelligent Ranking, l'indirizzo IP da cui è stata effettuata, l'autore della richiesta, quando è stata effettuata e altri dettagli.

Per ulteriori informazioni su CloudTrail, incluso come configurarlo e attivarlo, vedi ilAWS CloudTrailGuida per l'utente.

Informazioni di Amazon Kendra Intelligent Ranking di Amazon Kendra in CloudTrail

CloudTrail è attivato sul tuoAWSaccount al momento della creazione dell'account. L'operazione che si verifica in Amazon Kendra Intelligent Ranking di Amazon Kendra, viene registrata in un CloudTrailevento insieme ad altriAWSeventi di service CloudTrail cronologia degli eventi. È possibile visualizzare, cercare e scaricare gli eventi recenti nell'account AWS. Per ulteriori informazioni, consulta la paginaVisualizzazione di eventi con CloudTrail Cronologia degli eventi.

Per una registrazione continua di tutti gli eventi dellaAWSaccount, inclusi gli eventi per Amazon Kendra Intelligent Ranking, crea un percorso. UNpistaè una configurazione che consente CloudTrail per fornire eventi come file di registro a un bucket S3 specificato. Per impostazione predefinita, quando si crea un trail nella console, il trail sarà valido in tutte le regioni AWS. Il trail registra gli eventi di tutte le regioni nella partizione AWS e distribuisce i file di log nel bucket S3 specificato. Inoltre, puoi configurare altriAWSservizi per analizzare ulteriormente e agire in base ai dati degli eventi raccolti in CloudTrail registri. Per ulteriori informazioni, consultare:

- Panoramica della creazione di un percorso
- CloudTrail Servizi e integrazioni supportati
- Configurazione delle notifiche Amazon SNS per CloudTrail
- Ricezione CloudTrail I file di log di più areeeRicezione CloudTrail I file di log di più account

CloudTrail registra tutte le azioni di Amazon Kendra Intelligent Ranking, documentate nelRiferimento alle API. Ad esempio, le chiamate a`CreateRescoreExecutionPlan`generare voci in CloudTrail file di log.

Ogni evento o voce di log contiene informazioni sull'utente che ha generato la richiesta. Per ulteriori informazioni, consulta Elemento CloudTrail userIdentity.

Esempio: voci dei file di log di Amazon Kendra Intelligent Ranking di Amazon Kendra Kendra

UNpistaè una configurazione che consente la consegna di eventi come file di registro a un bucket S3 specificato. CloudTrail I file di log possono contenere una o più voci di log. Uneventorappresenta una singola richiesta da qualsiasi fonte e include informazioni sull'operazione richiesta, la data e l'ora dell'operazione, i parametri della richiesta e così via. CloudTrail i file di registro non sono una traccia di stack ordinata delle chiamate API pubbliche, quindi non vengono visualizzati in un ordine specifico.

Chiamate al`CreateRescoreExecutionPlan`l'operazione può contenere la voce seguente.

```
{
            "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"
        }
    }
```

Monitoraggio di Amazon Kendra con Amazon CloudWatch

Per monitorare lo stato dei tuoi indici, usa Amazon CloudWatch. Con CloudWatch, puoi ottenere metriche per la sincronizzazione dei documenti per il tuo indice. Puoi anche configurare CloudWatch allarmi da notificare quando una o più metriche superano una soglia definita dall'utente. Ad esempio, è possibile monitorare il numero di documenti inviati per l'indicizzazione o il numero di documenti che non sono stati indicizzati.

È necessario disporre di CloudWatch autorizzazioni per monitorare Amazon Kendra con CloudWatch. Per ulteriori informazioni, consulta la paginaAutenticazione e controllo degli accessi per Amazon CloudWatchnelAmazon CloudWatchGuida per l'utente.

Visualizzazione dei parametri di Amazon Kendra

Visualizza i parametri di Amazon Kendra possono contenere CloudWatch consolle.

Per visualizzare le metriche (CloudWatch consolle)

1. Accedi aAWS Management Consolee apri CloudWatch console ahttps://console.aws.amazon.com/cloudwatch/.

2. ScegliMetriche, scegliTutte le metrichee poi scegliKendra.
3. Scegliere la dimensione, selezionare un nome parametro e scegliere Add to graph (Aggiungi a grafico).
4. Seleziona un valore per l'intervallo di date. Il numero di parametri per l'intervallo di date selezionato è visualizzato nel grafico.

Creazione di un allarme

UN CloudWatch alarm controlla una singola metrica in un periodo di tempo specificato ed esegue una o più operazioni: invio di una notifica alla policy di Auto Scaling di Amazon Scaling di Amazon Simple Notification Service (Amazon SNS) o alla policy di Auto Scaling di Amazon Scaling di Amazon Scaling di Amazon Scaling di Amazon Scaling di Amazon Scaling di Amazon Scaling di Amazon Scaling di Amazon Scaling Le operazioni o le operazioni si basano sul valore della metrica relativa a una determinata soglia per un numero di periodi di tempo specificati dall'utente. CloudWatch può anche inviarti un messaggio Amazon SNS quando l'allarme cambia stato.

CloudWatch gli allarmi richiamano le operazioni solo quando lo stato cambia e è persistito per il periodo specificato.

Impostazione di un allarme

1. Accedi aAWS Management Consolee apri CloudWatch console ahttps://console.aws.amazon.com/cloudwatch/.
2. ScegliAllarmie poi scegliCrea una sveglia.
3. Seleziona una metrica. Scegli unKendrametrica per l'indice e la fonte di dati. Imposta anche l'ora come numero prestabilito di ore, giorni, settimane o personalizzata.
4. Scegli la tua statistica. Ad esempioMedia. Scegli anche il periodo di attivazione della sveglia in base a un numero prestabilito di minuti, ore, al giorno o personalizzato.
5. Scegli la soglia per attivare l'allarme, se utilizzare un valore statico o una banda e la condizione da soddisfare per la soglia.
6. Scegli lo stato di allarme per l'attivazione, se la metrica deve rientrare al di fuori della soglia impostata o in un altro stato. Seleziona a chi/a quale email inviare la notifica di allarme.
7. Se sei soddisfatto dell'allarme, scegliCrea una sveglia.

> **Note**
>
> È necessario fornire un nome per CloudWatch allarme.

CloudWatch Metriche per i lavori di sincronizzazione degli indici

La tabella seguente descrive le metriche di Amazon Kendra per i lavori di sincronizzazione delle origini dati di Amazon Kendra.

Se si utilizza l'API o la CLI, è necessario specificare`Namespace`come 'AWS/Kendra' oltre a`MetricName`a tua scelta quando usi[GetMetricStatistics](#)API.

Parametro	Descrizione
`DocumentsCrawled`	Il numero di documenti scansionati o rilevati dal processo di sincronizzazione durante l'esecuzione. Dimensioni: • IndexId • DataSourceId Unità: numero
`DocumentsSubmittedForIndexing`	Il numero di documenti che il processo di sincronizzazione ha inviato all'indice. Dimensioni: • IndexId • DataSourceId Unità: numero
`DocumentsSubmittedForIndexingFailed`	Il numero di documenti che non sono stati indicizzati. Controlla i contenuti di CloudWatc

Parametro	Descrizione
	h registra il processo di sincronizzazione per i dettagli. Dimensioni: • IndexId • DataSourceId Unità: numero
DocumentsSubmittedForDeletion	Il numero di documenti che il processo di sincronizzazione ha richiesto di rimuovere dall'indice. Dimensioni: • IndexId • DataSourceId Unità: numero
DocumentsSubmittedForDeletionFailed	Il numero di documenti che non sono stati eliminati. Controlla i contenuti di CloudWatch registra il processo di sincronizzazione per i dettagli. Dimensioni: • IndexId • DataSourceId Unità: numero

I parametri per le fonti di dati di Amazon Kendra

La tabella seguente descrive le metriche di Amazon Kendra per i lavori di sincronizzazione delle origini dati di Amazon Kendra. Le metriche contrassegnate con un asterisco (*) vengono utilizzate solo per le sorgenti di dati Amazon S3.

Se si utilizza l'API o la CLI, è necessario specificare`Namespace`come 'AWS/Kendra' oltre a`MetricName`a tua scelta quando usiGetMetricStatisticsAPI.

Parametro	Descrizione
`DocumentsSkippedNoChange *`	Il numero di documenti esaminati e ritenuti invariati, quindi non sono stati inviati per l'indiciz zazione. Dimensioni: • IndexId • DataSourceId Unità: numero
`DocumentsSkippedInvalidMetadata *`	Il numero di documenti è stato ignorato a causa di un problema con il file di metadati associato. Controlla i contenuti di CloudWatch registra l'esecuzione della sincronizzazione per maggiori dettagli. Dimensioni: • IndexId • DataSourceId Unità: numero
`DocumentsCrawled`	Il numero di file di documenti esaminati. Dimensioni:

Parametro	Descrizione
	• IndexId • DataSourceId Unità: numero
DocumentsSubmittedForDeletion	Il numero di documenti esaminati che sono stati eliminati dalla fonte di dati e inviati per la cancellazione. Dimensioni: • IndexId • DataSourceId Unità: numero
DocumentsSubmittedForDeletionFailed	Il numero di documenti che non sono stati eliminati da una fonte di dati. Dimensioni: • IndexId • DataSourceId Unità: numero
DocumentsSubmittedForIndexing	Il numero di documenti esaminati e inviati per l'indicizzazione. Dimensioni: • IndexId • DataSourceId Unità: numero

Parametro	Descrizione
`DocumentsSubmittedForIndexingFailed`	Il numero di documenti inviati per l'indicizzazione che non è stato possibile indicizzare. Dimensioni: • IndexId • DataSourceId Unità: numero

Metriche per i documenti indicizzati

La tabella seguente descrive i parametri di Amazon Kendra per i documenti indicizzati. Per i documenti indicizzati utilizzando il BatchPutDocument operazione, solo `IndexId` la dimensione è supportata.

Se si utilizza l'API o la CLI, è necessario specificare `Namespace` come 'AWS/Kendra' oltre a `MetricName` a tua scelta quando usi GetMetricStatistics API.

Parametro	Descrizione
`DocumentsIndexed`	Il numero di documenti indicizzati. Dimensioni: • IndexId • DataSourceId Unità: numero
`DocumentsFailedToIndex`	Il numero di documenti che non è stato possibile indicizzare. Controlla i contenuti di CloudWatch log. Dimensioni:

Parametro	Descrizione
	• IndexId • DataSourceId Unità: numero
`IndexQueryCount`	Il numero di query di indicizzazione al minuto. Dimensioni: • IndexId Unità: numero

Monitoraggio di Amazon Kendra con Amazon CloudWatch Registri

Amazon Kendra può contenere CloudWatch Registri per darti informazioni dettagliate sul funzionamento delle tue fonti di dati. Amazon Kendra registra i dettagli del processo per i documenti man mano che vengono indicizzati. Registra gli errori provenienti dalla fonte di dati che si verificano durante l'indicizzazione dei documenti. Tu usi CloudWatch Registri per monitorare, archiviare e accedere ai file di registro.

CloudWatch Logs archivia gli eventi di registro in un flusso di log che fa parte di un gruppo di log. Amazon Kendra utilizza queste funzionalità come segue:

- Gruppi di log: Amazon Kendra archivia tutti i flussi di log in un unico gruppo di log per ogni indice. Amazon Kendra crea il gruppo di log al momento della creazione dell'indice. L'identificatore del gruppo di log inizia sempre con «aws/kendra/».
- Log Stream: Amazon Kendra crea un nuovo flusso di log di origine dati nel gruppo di log per ogni processo di sincronizzazione dell'indice eseguito. Inoltre, crea un nuovo flusso di log dei documenti quando un flusso raggiunge circa 500 voci.
- Voci di log: Amazon Kendra crea una voce di log nel flusso di log mentre indicizza i documenti. Ogni voce fornisce informazioni sull'elaborazione del documento o sugli eventuali errori riscontrati.

Per ulteriori informazioni sull'utilizzo CloudWatch Registri, vediChe cos'è Amazon Cloud Watch LogsnelGuida per l'utente di Amazon Cloud Watch Logs.

Amazon Kendra crea due tipi di flussi di log:

- Fonte di dati: flussi di log
- I file di log dei documenti

Fonte di dati: flussi di log

I flussi di log delle fonti di dati pubblicano voci relative ai processi di sincronizzazione degli indici. Ogni processo di sincronizzazione crea un nuovo flusso di log che utilizza per pubblicare le voci. I file di log possono contenere:

```
data source id/YYYY-MM-DD-HH/data source sync job ID
```

Viene creato un nuovo flusso di log per ogni processo di sincronizzazione eseguito.

Esistono tre tipi di messaggi di log pubblicati in un flusso di log di un'origine dati:

- Un messaggio di registro per un documento che non è stato inviato per l'indicizzazione. Di seguito è riportato un esempio di questo messaggio per un documento in una fonte di dati 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."
}
```

- Un messaggio di registro per un documento che non è stato inviato per l'eliminazione. Di seguito è riportato un esempio di questo messaggio:

```
{
    "DocumentId": "document ID",
    "Message": "Failed to delete document via BatchDeleteDocument.",
    "ErrorCode": "InvalidRequest",
    "ErrorMessage": "Document can't be deleted because it doesn't exist."
```

```
}
```

- Un messaggio di log quando viene trovato un file di metadati non valido per un documento in un bucket Amazon S3. Di seguito è riportato un esempio di questo messaggio.

```
{
    "Message": "Found invalid metadata
 file bucket/prefix/filename.extension.metadata.json."
}
```

- Per SharePoint e connettori di database, Amazon Kendra scrive messaggi nel flusso di log solo se un documento non può essere indicizzato. Di seguito è riportato un esempio del messaggio di errore registrato da Amazon Kendra.

```
{
    "DocumentID": "document ID",
    "IndexID": "index ID",
    "SourceURI": "",
    "CrawlStatus": "FAILED",
    "ErrorCode": "403",
    "ErrorMessage": "Access Denied",
    "DataSourceErrorCode": "403"
}
```

I file di log dei documenti

Amazon Kendra registra le informazioni sull'elaborazione dei documenti durante l'indicizzazione. Registra una serie di messaggi per i documenti archiviati in una fonte di dati Amazon S3. Registra gli errori solo per i documenti archiviati in un ambiente Microsoft SharePoint o una fonte di dati del database.

Se i documenti sono stati aggiunti all'indice utilizzando ilBatchPutDocumentoperazione, il flusso di log è denominato come segue:

```
YYYY-MM-DD-HH/UUID
```

Se i documenti sono stati aggiunti all'indice utilizzando un'origine dati, il flusso di log viene denominato come segue:

```
dataSourceId/YYYY-MM-DD-HH/UUID
```

Ogni flusso di log contiene fino a 500 messaggi.

Se l'indicizzazione di un documento non riesce, questo messaggio viene inviato al flusso di registro:

```
{
    "DocumentId": "document ID",
    "IndexName": "index name",
    "IndexId": "index ID"
    "SourceURI": "source URI"
    "IndexingStatus": "DocumentFailedToIndex",
    "ErrorCode": "400 | 500",
    "ErrorMessage": "message"
}
```

Sicurezza in Amazon Kendra

La sicurezza del cloud AWS è la massima priorità. In qualità di AWS cliente, puoi beneficiare di un data center e di un'architettura di rete progettati per soddisfare i requisiti delle organizzazioni più sensibili alla sicurezza.

La sicurezza è una responsabilità condivisa tra AWS te e te. Il modello di responsabilità condivisa descrive questo aspetto come sicurezza del cloud e sicurezza nel cloud:

- Sicurezza del cloud:AWS è responsabile della protezione dell'infrastruttura che gestisce AWS i servizi nel AWS cloud. AWS ti fornisce anche servizi che puoi utilizzare in modo sicuro. I revisori esterni testano e verificano regolarmente l'efficacia della nostra sicurezza nell'ambito dei AWS Programmi di AWS conformità dei Programmi di conformità dei di . Per ulteriori informazioni sui programmi di conformità applicabili ad Amazon Kendra, AWS consulta Services in Scope by Compliance AWS Program Services in Scope by Compliance .
- Sicurezza nel cloud: la tua responsabilità è determinata dal AWS servizio che utilizzi. Sei anche responsabile di altri fattori, tra cui la riservatezza dei dati, i requisiti della tua azienda e le leggi e normative vigenti.

Questa documentazione ti aiuta a capire come applicare il modello di responsabilità condivisa quando usi Amazon Kendra. I seguenti argomenti mostrano come configurare Amazon Kendra per soddisfare i tuoi obiettivi di sicurezza e conformità. Scopri anche come utilizzare altri AWS servizi che ti aiutano a monitorare e proteggere le tue risorse Amazon Kendra.

Argomenti

Protezione dei dati in Amazon Kendra

Il modello di responsabilità AWS condivisa Modello si applica alla protezione dei dati in Amazon Kendra. Come descritto in questo modello, AWS è responsabile della protezione dell'infrastruttura globale che gestisce tutti i. Cloud AWS L'utente è responsabile del controllo dei contenuti ospitati su questa infrastruttura. L'utente è inoltre responsabile della configurazione della protezione e delle attività di gestione per i Servizi AWS utilizzati. Per ulteriori informazioni sulla privacy dei dati, vedi le Domande frequenti sulla privacy dei dati. Per informazioni sulla protezione dei dati in Europa, consulta il post del blog relativo al Modello di responsabilità condivisa AWS e GDPR nel Blog sulla sicurezza AWS .

Ai fini della protezione dei dati, consigliamo di proteggere Account AWS le credenziali e configurare i singoli utenti con AWS IAM Identity Center or AWS Identity and Access Management (IAM). In tal modo, a ogni utente verranno assegnate solo le autorizzazioni necessarie per svolgere i suoi compiti. Ti suggeriamo, inoltre, di proteggere i dati nei seguenti modi:

- Utilizza l'autenticazione a più fattori (MFA) con ogni account.
- Usa SSL/TLS per comunicare con le risorse. AWS È richiesto TLS 1.2 ed è consigliato TLS 1.3.
- Configura l'API e la registrazione delle attività degli utenti con. AWS CloudTrail
- Utilizza soluzioni di AWS crittografia, insieme a tutti i controlli di sicurezza predefiniti all'interno Servizi AWS.
- Utilizza i servizi di sicurezza gestiti avanzati, come Amazon Macie, che aiutano a individuare e proteggere i dati sensibili archiviati in Amazon S3.
- Se hai bisogno di moduli crittografici convalidati FIPS 140-2 per l'accesso AWS tramite un'interfaccia a riga di comando o un'API, utilizza un endpoint FIPS. Per ulteriori informazioni sugli endpoint FIPS disponibili, consulta il Federal Information Processing Standard (FIPS) 140-2.

Ti consigliamo vivamente di non inserire mai informazioni riservate o sensibili, ad esempio gli indirizzi e-mail dei clienti, nei tag o nei campi di testo in formato libero, ad esempio nel campo Nome. Ciò include quando lavori con Amazon Kendra o Servizi AWS altri utenti utilizzando la console, l'API AWS CLI o gli SDK. AWS I dati inseriti nei tag o nei campi di testo in formato libero utilizzati per i nomi possono essere utilizzati per i la fatturazione o i log di diagnostica. Quando fornisci un URL a un server esterno, ti suggeriamo vivamente di non includere informazioni sulle credenziali nell'URL per convalidare la tua richiesta al server.

Crittografia dei dati a riposo

Amazon Kendra crittografa i tuoi dati inattivi con una chiave di crittografia a tua scelta. È possibile scegliere una delle seguenti opzioni:

- Una chiave KMS di AWS proprietà AWS . Se non specifichi una chiave di crittografia, i dati vengono crittografati con questa chiave per impostazione predefinita.
- Una chiave KMS AWS gestita nel tuo account. Questa chiave viene creata, gestita e utilizzata per tuo conto da Amazon Kendra. Il nome chiave è. `aws/kendra`
- Una chiave gestita dal cliente. Puoi fornire l'ARN di una chiave di crittografia che hai creato nel tuo account. Quando utilizzi una chiave KMS gestita dal cliente, devi fornire alla chiave una politica chiave che consenta ad Amazon Kendra di utilizzare la chiave. Seleziona una chiave KMS con crittografia simmetrica gestita dal cliente, Amazon Kendra non supporta chiavi KMS asimmetriche. Per ulteriori informazioni, consulta Gestione delle chiavi.

Crittografia dei dati in transito

Amazon Kendra utilizza il protocollo HTTPS per comunicare con l'applicazione client. Utilizza HTTPS e AWS firme per comunicare con altri servizi per conto dell'applicazione. Se utilizzi un VPC, puoi utilizzarlo AWS PrivateLink per stabilire una connessione privata tra il tuo VPC e Amazon Kendra.

Gestione delle chiavi

Amazon Kendra crittografa i contenuti del tuo indice utilizzando uno dei tre tipi di chiavi. È possibile scegliere una delle seguenti opzioni:

- Un AWS KMS di proprietà. AWS Questa è l'impostazione predefinita.
- Una chiave AWS KMS gestita. Questa chiave viene creata nel tuo account ed è gestita e utilizzata per tuo conto da Amazon Kendra.
- Una chiave KMS gestita dal cliente. Puoi creare la chiave quando crei un indice o un'origine dati Amazon Kendra oppure puoi creare la chiave utilizzando la console. AWS KMS Seleziona una chiave KMS con crittografia simmetrica gestita dal cliente. Amazon Kendra non supporta le chiavi KMS asimmetriche. Per ulteriori informazioni, consulta la sezione relativa all'uso di chiavi simmetriche e asimmetriche nella Guida per gli sviluppatori di AWS Key Management Service.

Amazon Kendra Amazon Kendra Intelligent Ranking e interfaccia VPC endpoint ()AWS PrivateLink

Puoi stabilire una connessione privata tra il tuo VPC e Amazon Kendra creando un endpoint VPC di interfaccia. Gli endpoint di interfaccia sono basati su una tecnologia che consente di accedere in modo privato alle API di Amazon Kendra senza un gateway Internet, un dispositivo NAT, una connessione VPN o una connessione Direct Connect. AWS PrivateLink AWS Le istanze nel tuo VPC non necessitano di indirizzi IP pubblici per comunicare con le API di Amazon Kendra. Il traffico tra il tuo VPC e Amazon Kendra non esce dalla rete Amazon.

Ogni endpoint dell'interfaccia è rappresentato da una o più interfacce di rete elastiche nelle tue sottoreti.

Considerazioni sugli endpoint VPC Amazon Kendra e Amazon Kendra Intelligent Ranking

Prima di configurare un endpoint VPC di interfaccia per Amazon Kendra o Amazon Kendra Intelligent Ranking, assicurati di esaminare i prerequisiti nella Amazon VPC User Guide.

Amazon Kendra e Amazon Kendra Intelligent Ranking supportano le chiamate a tutte le azioni API dal tuo VPC.

Creazione di un endpoint VPC di interfaccia per Amazon Kendra e Amazon Kendra Intelligent Ranking

Puoi creare un endpoint VPC per il servizio Amazon Kendra o Amazon Kendra Intelligent Ranking utilizzando la console Amazon VPC o il (). AWS Command Line Interface AWS CLI

Crea un endpoint VPC per Amazon Kendra utilizzando il seguente nome di servizio:

- com.amazonaws.*region*.kendra

Crea un endpoint VPC per Amazon Kendra Intelligent Ranking utilizzando il seguente nome di servizio:

- aws.api.*region*.kendra-ranking

Dopo aver creato un endpoint VPC, puoi utilizzare il seguente AWS CLI comando di esempio che utilizza il `endpoint-url` parametro per specificare un endpoint di interfaccia per l'API Amazon Kendra:

```
aws kendra list-indices --endpoint-url https://VPC endpoint
```

L'*`endpoint VPC`* è il nome DNS generato quando viene creato l'endpoint dell'interfaccia. Questo nome include l'ID dell'endpoint VPC e il nome del servizio Amazon Kendra, che include la regione. Ad esempio, `vpce-1234-abcdef.kendra.us-west-2.vpce.amazonaws.com`.

Se attivi il DNS privato per l'endpoint, puoi effettuare richieste API ad Amazon Kendra utilizzando il nome DNS predefinito per la regione. Ad esempio, `kendra.us-east-1.amazonaws.com`.

Per ulteriori informazioni, consulta Creazione di un endpoint dell'interfaccia nella Guida per l'utente di Amazon VPC.

Creazione di una policy sugli endpoint VPC per Amazon Kendra e Amazon Kendra Intelligent Ranking

Puoi allegare una policy per gli endpoint al tuo endpoint VPC che controlla l'accesso ad Amazon Kendra o Amazon Kendra Intelligent Ranking.

La politica per Amazon Kendra o Amazon Kendra Intelligent Ranking specifica le seguenti informazioni:

- L'utente principale/autorizzato che può eseguire azioni.
- Le azioni che possono essere eseguite.
- Le risorse sui cui si possono eseguire azioni.

Esempio: policy sugli endpoint VPC per le azioni di Amazon Kendra

Di seguito è riportato un esempio di policy sugli endpoint per Amazon Kendra. Se collegata a un endpoint, questa policy garantisce l'accesso a tutte le azioni Amazon Kendra disponibili per tutti i principali/utenti autorizzati su tutte le risorse.

```
{
   "Statement":[
      {
         "Principal":"*",
```

```
         "Effect":"Allow",
         "Action":[
            "kendra:*"
         ],
         "Resource":"*"
      }
   ]
}
```

Esempio: policy sugli endpoint VPC per le azioni di Amazon Kendra Intelligent Ranking

Di seguito è riportato un esempio di policy sugli endpoint per Amazon Kendra Intelligent Ranking. Se collegata a un endpoint, questa policy garantisce l'accesso a tutte le azioni di Amazon Kendra Intelligent Ranking disponibili per tutti i principali/utenti autorizzati su tutte le risorse.

```
{
   "Statement":[
      {
         "Principal":"*",
         "Effect":"Allow",
         "Action":[
            "kendra-ranking:*"
         ],
         "Resource":"*"
      }
   ]
}
```

Per ulteriori informazioni, consulta Controllare l'accesso agli endpoint VPC utilizzando le policy degli endpoint nella Amazon VPC User Guide.

Gestione delle identità e degli accessi per Amazon Kendra

AWS Identity and Access Management (IAM) è uno strumento Servizio AWS che aiuta un amministratore a controllare in modo sicuro l'accesso alle risorse. AWS Gli amministratori IAM controllano chi può essere autenticato (effettuato l'accesso) e autorizzato (disporre delle autorizzazioni) a utilizzare le risorse Amazon Kendra. IAM è uno strumento Servizio AWS che puoi utilizzare senza costi aggiuntivi.

Argomenti

- Destinatari

- Autenticazione con identità
- Gestione dell'accesso con policy
- Come funziona Amazon Kendra con IAM
- Esempi di policy basate sull'identità di Amazon Kendra
- AWS politiche gestite per Amazon Kendra
- Risoluzione dei problemi relativi a Amazon Kendra Identity and Access

Destinatari

Il modo in cui utilizzi AWS Identity and Access Management (IAM) varia a seconda del lavoro svolto in Amazon Kendra.

Utente del servizio: se utilizzi il servizio Amazon Kendra per svolgere il tuo lavoro, l'amministratore ti fornisce le credenziali e le autorizzazioni necessarie. Man mano che utilizzi più funzionalità di Amazon Kendra per svolgere il tuo lavoro, potresti aver bisogno di autorizzazioni aggiuntive. La comprensione della gestione dell'accesso ti consente di richiedere le autorizzazioni corrette all'amministratore. Se non riesci ad accedere a una funzionalità di Amazon Kendra, consulta. Risoluzione dei problemi relativi a Amazon Kendra Identity and Access

Amministratore del servizio: se sei responsabile delle risorse Amazon Kendra della tua azienda, probabilmente hai pieno accesso ad Amazon Kendra. È tuo compito determinare a quali funzionalità e risorse di Amazon Kendra devono accedere gli utenti del servizio. Devi inviare le richieste all'amministratore IAM per cambiare le autorizzazioni degli utenti del servizio. Esamina le informazioni contenute in questa pagina per comprendere i concetti di base relativi a IAM. Per ulteriori informazioni su come la tua azienda può utilizzare IAM con Amazon Kendra, consulta. Come funziona Amazon Kendra con IAM

Amministratore IAM: se sei un amministratore IAM, potresti voler saperne di più su come scrivere policy per gestire l'accesso ad Amazon Kendra. Per visualizzare esempi di policy basate sull'identità di Amazon Kendra che puoi utilizzare in IAM, consulta. Esempi di policy basate sull'identità di Amazon Kendra

Autenticazione con identità

L'autenticazione è il modo in cui accedi utilizzando le tue credenziali di identità. AWS Devi essere autenticato (aver effettuato l' Utente root dell'account AWS accesso AWS) come utente IAM o assumendo un ruolo IAM.

Puoi accedere AWS come identità federata utilizzando le credenziali fornite tramite una fonte di identità. AWS IAM Identity Center Gli utenti (IAM Identity Center), l'autenticazione Single Sign-On della tua azienda e le tue credenziali di Google o Facebook sono esempi di identità federate. Se accedi come identità federata, l'amministratore ha configurato in precedenza la federazione delle identità utilizzando i ruoli IAM. Quando accedi AWS utilizzando la federazione, assumi indirettamente un ruolo.

A seconda del tipo di utente, puoi accedere al AWS Management Console o al portale di AWS accesso. Per ulteriori informazioni sull'accesso a AWS, vedi Come accedere al tuo Account AWS nella Guida per l'Accedi ad AWS utente.

Se accedi a AWS livello di codice, AWS fornisce un kit di sviluppo software (SDK) e un'interfaccia a riga di comando (CLI) per firmare crittograficamente le tue richieste utilizzando le tue credenziali. Se non utilizzi AWS strumenti, devi firmare tu stesso le richieste. Per ulteriori informazioni sull'utilizzo del metodo consigliato per firmare autonomamente le richieste, consulta Signing AWS API request nella IAM User Guide.

A prescindere dal metodo di autenticazione utilizzato, potrebbe essere necessario specificare ulteriori informazioni sulla sicurezza. Ad esempio, ti AWS consiglia di utilizzare l'autenticazione a più fattori (MFA) per aumentare la sicurezza del tuo account. Per ulteriori informazioni, consulta Autenticazione a più fattori nella Guida per l'utente di AWS IAM Identity Center e Utilizzo dell'autenticazione a più fattori (MFA) in AWS nella Guida per l'utente di IAM.

Account AWS utente root

Quando si crea un account Account AWS, si inizia con un'identità di accesso che ha accesso completo a tutte Servizi AWS le risorse dell'account. Questa identità è denominata utente Account AWS root ed è accessibile effettuando l'accesso con l'indirizzo e-mail e la password utilizzati per creare l'account. Si consiglia vivamente di non utilizzare l'utente root per le attività quotidiane. Conserva le credenziali dell'utente root e utilizzarle per eseguire le operazioni che solo l'utente root può eseguire. Per un elenco completo delle attività che richiedono l'accesso come utente root, consulta la sezione Attività che richiedono le credenziali dell'utente root nella Guida per l'utente di IAM.

Utenti IAM e gruppi

Un utente IAM è un'identità interna Account AWS che dispone di autorizzazioni specifiche per una singola persona o applicazione. Ove possibile, consigliamo di fare affidamento a credenziali temporanee invece di creare utenti IAM con credenziali a lungo termine come le password e le

chiavi di accesso. Tuttavia, per casi d'uso specifici che richiedono credenziali a lungo termine con utenti IAM, si consiglia di ruotare le chiavi di accesso. Per ulteriori informazioni, consulta la pagina Rotazione periodica delle chiavi di accesso per casi d'uso che richiedono credenziali a lungo termine nella Guida per l'utente di IAM.

Un gruppo IAM è un'identità che specifica un insieme di utenti IAM. Non è possibile eseguire l'accesso come gruppo. È possibile utilizzare gruppi per specificare le autorizzazioni per più utenti alla volta. I gruppi semplificano la gestione delle autorizzazioni per set di utenti di grandi dimensioni. Ad esempio, è possibile avere un gruppo denominato Amministratori IAM e concedere a tale gruppo le autorizzazioni per amministrare le risorse IAM.

Gli utenti sono diversi dai ruoli. Un utente è associato in modo univoco a una persona o un'applicazione, mentre un ruolo è destinato a essere assunto da chiunque ne abbia bisogno. Gli utenti dispongono di credenziali a lungo termine permanenti, mentre i ruoli forniscono credenziali temporanee. Per ulteriori informazioni, consulta Quando creare un utente IAM (invece di un ruolo) nella Guida per l'utente di IAM.

Ruoli IAM

Un ruolo IAM è un'identità interna all'utente Account AWS che dispone di autorizzazioni specifiche. È simile a un utente IAM, ma non è associato a una persona specifica. Puoi assumere temporaneamente un ruolo IAM in AWS Management Console cambiando ruolo. Puoi assumere un ruolo chiamando un'operazione AWS CLI o AWS API o utilizzando un URL personalizzato. Per ulteriori informazioni sui metodi per l'utilizzo dei ruoli, consulta Utilizzo di ruoli IAM nella Guida per l'utente di IAM.

I ruoli IAM con credenziali temporanee sono utili nelle seguenti situazioni:

- Accesso utente federato: per assegnare le autorizzazioni a una identità federata, è possibile creare un ruolo e definire le autorizzazioni per il ruolo. Quando un'identità federata viene autenticata, l'identità viene associata al ruolo e ottiene le autorizzazioni da esso definite. Per ulteriori informazioni sulla federazione dei ruoli, consulta Creazione di un ruolo per un provider di identità di terza parte nella Guida per l'utente di IAM. Se utilizzi IAM Identity Center, configura un set di autorizzazioni. IAM Identity Center mette in correlazione il set di autorizzazioni con un ruolo in IAM per controllare a cosa possono accedere le identità dopo l'autenticazione. Per informazioni sui set di autorizzazioni, consulta Set di autorizzazioni nella Guida per l'utente di AWS IAM Identity Center .
- Autorizzazioni utente IAM temporanee: un utente IAM o un ruolo può assumere un ruolo IAM per ottenere temporaneamente autorizzazioni diverse per un'attività specifica.

- Accesso multi-account: è possibile utilizzare un ruolo IAM per permettere a un utente (un principale affidabile) con un account diverso di accedere alle risorse nell'account. I ruoli sono lo strumento principale per concedere l'accesso multi-account. Tuttavia, con alcuni Servizi AWS, è possibile allegare una policy direttamente a una risorsa (anziché utilizzare un ruolo come proxy). Per informazioni sulle differenze tra ruoli e policy basate su risorse per l'accesso multi-account, consulta Differenza tra i ruoli IAM e le policy basate su risorse nella Guida per l'utente di IAM.
- Accesso a più servizi: alcuni Servizi AWS utilizzano le funzionalità di altri Servizi AWS. Ad esempio, quando effettui una chiamata in un servizio, è comune che tale servizio esegua applicazioni in Amazon EC2 o archivi oggetti in Amazon S3. Un servizio può eseguire questa operazione utilizzando le autorizzazioni dell'entità chiamante, utilizzando un ruolo di servizio o utilizzando un ruolo collegato al servizio.
  - Sessioni di accesso diretto (FAS): quando utilizzi un utente o un ruolo IAM per eseguire azioni AWS, sei considerato un preside. Quando si utilizzano alcuni servizi, è possibile eseguire un'azione che attiva un'altra azione in un servizio diverso. FAS utilizza le autorizzazioni del principale che chiama an Servizio AWS, combinate con la richiesta Servizio AWS per effettuare richieste ai servizi downstream. Le richieste FAS vengono effettuate solo quando un servizio riceve una richiesta che richiede interazioni con altri Servizi AWS o risorse per essere completata. In questo caso è necessario disporre delle autorizzazioni per eseguire entrambe le azioni. Per i dettagli delle policy relative alle richieste FAS, consulta la pagina Forward access sessions.
  - Ruolo di servizio: un ruolo di servizio è un ruolo IAM che un servizio assume per eseguire azioni per tuo conto. Un amministratore IAM può creare, modificare ed eliminare un ruolo di servizio dall'interno di IAM. Per ulteriori informazioni, consulta la sezione Creazione di un ruolo per delegare le autorizzazioni a un Servizio AWS nella Guida per l'utente di IAM.
  - Ruolo collegato al servizio: un ruolo collegato al servizio è un tipo di ruolo di servizio collegato a un. Servizio AWS Il servizio può assumere il ruolo per eseguire un'azione per tuo conto. I ruoli collegati al servizio vengono visualizzati nel tuo account Account AWS e sono di proprietà del servizio. Un amministratore IAM può visualizzare le autorizzazioni per i ruoli collegati ai servizi, ma non modificarle.
- Applicazioni in esecuzione su Amazon EC2: puoi utilizzare un ruolo IAM per gestire le credenziali temporanee per le applicazioni in esecuzione su un'istanza EC2 e che AWS CLI effettuano richieste API. AWS Ciò è preferibile all'archiviazione delle chiavi di accesso nell'istanza EC2. Per assegnare un AWS ruolo a un'istanza EC2 e renderlo disponibile per tutte le sue applicazioni, crei un profilo di istanza collegato all'istanza. Un profilo dell'istanza contiene il ruolo e consente ai programmi in esecuzione sull'istanza EC2 di ottenere le credenziali temporanee. Per ulteriori

informazioni, consulta Utilizzo di un ruolo IAM per concedere autorizzazioni ad applicazioni in esecuzione su istanze di Amazon EC2 nella Guida per l'utente di IAM.

Per informazioni sull'utilizzo dei ruoli IAM, consulta Quando creare un ruolo IAM (invece di un utente) nella Guida per l'utente di IAM.

Gestione dell'accesso con policy

Puoi controllare l'accesso AWS creando policy e collegandole a AWS identità o risorse. Una policy è un oggetto AWS che, se associato a un'identità o a una risorsa, ne definisce le autorizzazioni. AWS valuta queste politiche quando un principale (utente, utente root o sessione di ruolo) effettua una richiesta. Le autorizzazioni nelle policy determinano l'approvazione o il rifiuto della richiesta. La maggior parte delle politiche viene archiviata AWS come documenti JSON. Per ulteriori informazioni sulla struttura e sui contenuti dei documenti delle policy JSON, consulta Panoramica delle policy JSON nella Guida per l'utente di IAM.

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. In altre parole, quale principale può eseguire azioni su quali risorse e in quali condizioni.

Per impostazione predefinita, utenti e ruoli non dispongono di autorizzazioni. Per concedere agli utenti l'autorizzazione a eseguire azioni sulle risorse di cui hanno bisogno, un amministratore IAM può creare policy IAM. Successivamente l'amministratore può aggiungere le policy IAM ai ruoli e gli utenti possono assumere i ruoli.

Le policy IAM definiscono le autorizzazioni relative a un'azione, a prescindere dal metodo utilizzato per eseguirla. Ad esempio, supponiamo di disporre di una policy che consente l'azione `iam:GetRole`. Un utente con tale policy può ottenere informazioni sul ruolo dall' AWS Management Console AWS CLI, dall'o dall' AWS API.

Policy basate su identità

Le policy basate su identità sono documenti di policy di autorizzazione JSON che è possibile allegare a un'identità (utente, gruppo di utenti o ruoli IAM). Tali policy definiscono le azioni che utenti e ruoli possono eseguire, su quali risorse e in quali condizioni. Per informazioni su come creare una policy basata su identità, consulta Creazione di policy IAM nella Guida per l'utente di IAM.

Le policy basate su identità possono essere ulteriormente classificate come policy inline o policy gestite. Le policy inline sono integrate direttamente in un singolo utente, gruppo o ruolo. Le politiche

gestite sono politiche autonome che puoi allegare a più utenti, gruppi e ruoli nel tuo Account AWS. Le politiche gestite includono politiche AWS gestite e politiche gestite dai clienti. Per informazioni su come scegliere tra una policy gestita o una policy inline, consulta Scelta fra policy gestite e policy inline nella Guida per l'utente di IAM.

Policy basate su risorse

Le policy basate su risorse sono documenti di policy JSON che è possibile collegare a una risorsa. Gli esempi più comuni di policy basate su risorse sono le policy di attendibilità dei ruoli IAM e le policy dei bucket Amazon S3. Nei servizi che supportano policy basate sulle risorse, gli amministratori dei servizi possono utilizzarle per controllare l'accesso a una risorsa specifica. Quando è collegata a una risorsa, una policy definisce le azioni che un principale può eseguire su tale risorsa e a quali condizioni. È necessario specificare un principale in una policy basata sulle risorse. I principali possono includere account, utenti, ruoli, utenti federati o. Servizi AWS

Le policy basate sulle risorse sono policy inline che si trovano in tale servizio. Non puoi utilizzare le policy AWS gestite di IAM in una policy basata sulle risorse.

Liste di controllo degli accessi (ACL)

Le liste di controllo degli accessi (ACL) controllano quali principali (membri, utenti o ruoli dell'account) hanno le autorizzazioni per accedere a una risorsa. Le ACL sono simili alle policy basate su risorse, sebbene non utilizzino il formato del documento di policy JSON.

Amazon S3 e Amazon VPC sono esempi di servizi che supportano gli ACL. AWS WAF Per maggiori informazioni sulle ACL, consulta Panoramica delle liste di controllo degli accessi (ACL) nella Guida per gli sviluppatori di Amazon Simple Storage Service.

Altri tipi di policy

AWS supporta tipi di policy aggiuntivi e meno comuni. Questi tipi di policy possono impostare il numero massimo di autorizzazioni concesse dai tipi di policy più comuni.

- Limiti delle autorizzazioni: un limite delle autorizzazioni è una funzione avanzata nella quale si imposta il numero massimo di autorizzazioni che una policy basata su identità può concedere a un'entità IAM (utente o ruolo IAM). È possibile impostare un limite delle autorizzazioni per un'entità. Le autorizzazioni risultanti sono l'intersezione delle policy basate su identità dell'entità e i relativi limiti delle autorizzazioni. Le policy basate su risorse che specificano l'utente o il ruolo nel campo `Principal` sono condizionate dal limite delle autorizzazioni. Un rifiuto esplicito in una qualsiasi

di queste policy sostituisce l'autorizzazione. Per ulteriori informazioni sui limiti delle autorizzazioni, consulta Limiti delle autorizzazioni per le entità IAM nella Guida per l'utente di IAM.

- Politiche di controllo dei servizi (SCP): le SCP sono politiche JSON che specificano le autorizzazioni massime per un'organizzazione o un'unità organizzativa (OU) in. AWS Organizations AWS Organizations è un servizio per il raggruppamento e la gestione centralizzata di più Account AWS di proprietà dell'azienda. Se abiliti tutte le funzionalità in un'organizzazione, puoi applicare le policy di controllo dei servizi (SCP) a uno o tutti i tuoi account. L'SCP limita le autorizzazioni per le entità presenti negli account dei membri, inclusa ciascuna. Utente root dell'account AWS Per ulteriori informazioni su organizzazioni e policy SCP, consulta la pagina sulle Policy di controllo dei servizi nella Guida per l'utente di AWS Organizations .
- Policy di sessione: le policy di sessione sono policy avanzate che vengono trasmesse come parametro quando si crea in modo programmatico una sessione temporanea per un ruolo o un utente federato. Le autorizzazioni della sessione risultante sono l'intersezione delle policy basate su identità del ruolo o dell'utente e le policy di sessione. Le autorizzazioni possono anche provenire da una policy basata su risorse. Un rifiuto esplicito in una qualsiasi di queste policy sostituisce l'autorizzazione. Per ulteriori informazioni, consulta Policy di sessione nella Guida per l'utente di IAM.

Più tipi di policy

Quando più tipi di policy si applicano a una richiesta, le autorizzazioni risultanti sono più complicate da comprendere. Per scoprire come si AWS determina se consentire una richiesta quando sono coinvolti più tipi di policy, consulta Logica di valutazione delle policy nella IAM User Guide.

Come funziona Amazon Kendra con IAM

Prima di utilizzare IAM per gestire l'accesso ad Amazon Kendra, è necessario comprendere quali funzionalità IAM sono disponibili per l'uso con Amazon Kendra. Per avere una visione di alto livello di come Amazon Kendra AWS e altri servizi funzionano con IAM AWS , consulta Services That Work with IAM nella IAM User Guide.

Argomenti

- Politiche basate sull'identità di Amazon Kendra
- Politiche basate sulle risorse di Amazon Kendra
- Liste di controllo degli accessi (ACL)
- Autorizzazione basata sui tag Amazon Kendra

- Ruoli IAM di Amazon Kendra

Politiche basate sull'identità di Amazon Kendra

Con le policy basate su identità di IAM, è possibile specificare quali azioni e risorse sono consentite o rifiutate, nonché le condizioni in base alle quali le azioni sono consentite o rifiutate. Amazon Kendra supporta azioni, risorse e chiavi di condizione specifiche. Per informazioni su tutti gli elementi utilizzati in una policy JSON, consulta Documentazione di riferimento degli elementi delle policy JSON IAM nella Guida per l'utente IAM.

Azioni

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. Cioè, quale principale può eseguire azioni su quali risorse, e in quali condizioni.

L'elemento `Action` di una policy JSON descrive le azioni che è possibile utilizzare per consentire o negare l'accesso a un criterio. Le azioni politiche in genere hanno lo stesso nome dell'operazione AWS API associata. Ci sono alcune eccezioni, ad esempio le azioni di sola autorizzazione che non hanno un'operazione API corrispondente. Esistono anche alcune operazioni che richiedono più operazioni in una policy. Queste operazioni aggiuntive sono denominate operazioni dipendenti.

Includi le operazioni in una policy per concedere le autorizzazioni a eseguire l'operazione associata.

Le azioni politiche in Amazon Kendra utilizzano il seguente prefisso prima dell'azione:. `kendra:` Ad esempio, per concedere a qualcuno l'autorizzazione a elencare gli indici Amazon Kendra con ListIndicesl'operazione API, `kendra:ListIndices` includi l'azione nella sua politica. Le istruzioni della policy devono includere un elemento `Action` o `NotAction`. Amazon Kendra definisce il proprio set di azioni che descrivono le attività che puoi eseguire con questo servizio.

Per specificare più azioni in una sola istruzione, separa ciascuna di esse con una virgola come mostrato di seguito:

```
"Action": [
      "kendra:action1",
      "kendra:action2"
```

È possibile specificare più azioni tramite caratteri jolly (*). Ad esempio, per specificare tutte le azioni che iniziano con la parola `Describe`, includi la seguente azione:

```
"Action": "kendra:Describe*"
```

Per visualizzare un elenco delle azioni di Amazon Kendra, consulta Actions Defined by Amazon Kendra nella IAM User Guide.

Risorse

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. Cioè, quale principale può eseguire operazioni su quali risorse, e in quali condizioni.

L'elemento JSON `Resource` della policy specifica l'oggetto o gli oggetti ai quali si applica l'azione. Le istruzioni devono includere un elemento `Resource` o un elemento `NotResource`. Come best practice, specifica una risorsa utilizzando il suo nome della risorsa Amazon (ARN). Puoi eseguire questa operazione per azioni che supportano un tipo di risorsa specifico, note come autorizzazioni a livello di risorsa.

Per le azioni che non supportano le autorizzazioni a livello di risorsa, ad esempio le operazioni di elenco, utilizza un carattere jolly (*) per indicare che l'istruzione si applica a tutte le risorse.

```
"Resource": "*"
```

La risorsa dell'indice Amazon Kendra ha il seguente ARN:

```
arn:${Partition}:kendra:${Region}:${Account}:index/${IndexId}
```

Per ulteriori informazioni sul formato degli ARN, consulta Amazon Resource Names (ARNs) e AWS Service Namespaces.

Ad esempio, per specificare un indice nella dichiarazione, utilizzate il GUID dell'indice nel seguente ARN:

```
"Resource": "arn:aws:kendra:${Region}:${Account}:index/${GUID}"
```

Per specificare tutti gli indici che appartengono a un account specifico, usa il carattere jolly (*):

```
"Resource": "arn:aws:${Region}:${Account}:index/*"
```

Alcune azioni di Amazon Kendra, come quelle per la creazione di risorse, non possono essere eseguite su una risorsa specifica. In questi casi, è necessario utilizzare il carattere jolly (*).

```
"Resource": "*"
```

Per visualizzare un elenco dei tipi di risorse Amazon Kendra e dei relativi ARN, consulta Resources Defined by Amazon Kendra nella IAM User Guide. Per sapere con quali azioni puoi specificare l'ARN di ogni risorsa, consulta Azioni definite da Amazon Kendra.

Chiavi di condizione

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. Cioè, quale principale può eseguire azioni su quali risorse, e in quali condizioni.

L'elemento `Condition` (o blocco `Condition`) consente di specificare le condizioni in cui un'istruzione è in vigore. L'elemento `Condition` è facoltativo. Puoi compilare espressioni condizionali che utilizzano operatori di condizione, ad esempio uguale a o minore di, per soddisfare la condizione nella policy con i valori nella richiesta.

Se specifichi più elementi `Condition` in un'istruzione o più chiavi in un singolo elemento `Condition`, questi vengono valutati da AWS utilizzando un'operazione `AND` logica. Se si specificano più valori per una singola chiave di condizione, AWS valuta la condizione utilizzando un'operazione logica. `OR` Tutte le condizioni devono essere soddisfatte prima che le autorizzazioni dell'istruzione vengano concesse.

Puoi anche utilizzare variabili segnaposto quando specifichi le condizioni. Ad esempio, puoi autorizzare un utente IAM ad accedere a una risorsa solo se è stata taggata con il relativo nome utente IAM. Per ulteriori informazioni, consulta Elementi delle policy IAM: variabili e tag nella Guida per l'utente di IAM.

AWS supporta chiavi di condizione globali e chiavi di condizione specifiche del servizio. Per visualizzare tutte le chiavi di condizione AWS globali, consulta le chiavi di contesto delle condizioni AWS globali nella Guida per l'utente IAM.

Amazon Kendra non fornisce chiavi di condizione specifiche del servizio, ma supporta l'utilizzo di alcune chiavi di condizione globali. Per visualizzare tutte le chiavi di condizione AWS globali, consulta AWS Global Condition Context Keys nella Guida per l'utente IAM.

Esempi

Per visualizzare esempi di politiche basate sull'identità di Amazon Kendra, consulta. Esempi di policy basate sull'identità di Amazon Kendra

Politiche basate sulle risorse di Amazon Kendra

Amazon Kendra non supporta politiche basate sulle risorse.

Liste di controllo degli accessi (ACL)

Amazon Kendra non supporta le liste di controllo degli accessi (ACL) per l'accesso AWS a servizi e risorse.

Autorizzazione basata sui tag Amazon Kendra

Puoi associare tag a determinati tipi di risorse Amazon Kendra per autorizzare l'accesso a tali risorse. Per controllare l'accesso in base ai tag, fornisci le informazioni sui tag nell'elemento condition di una policy utilizzando i tasti `aws:RequestTag/key-name` o `aws:TagKeys` condition.

La tabella seguente elenca le azioni, i tipi di risorse corrispondenti e le chiavi di condizione per il controllo degli accessi basato su tag. Ogni azione è autorizzata in base ai tag associati al tipo di risorsa corrispondente.

Azione	Tipo di risorsa	Chiavi di condizione
CreateDataSource		`aws:RequestTag` , `aws:TagKeys`
CreateFaq		`aws:RequestTag` , `aws:TagKeys`
CreateIndex		`aws:RequestTag` , `aws:TagKeys`
API_ ListTagsForResource	fonte di dati, domande frequenti, indice	
TagResource	fonte di dati, domande frequenti, indice	`aws:RequestTag` , `aws:TagKeys`
UntagResource	fonte di dati, domande frequenti, indice	`aws:TagKeys`

Per informazioni su come etichettare le risorse di Amazon Kendra, consulta. Tag Per un esempio di politica basata sull'identità che limita l'accesso a una risorsa in base ai tag delle risorse, consulta. Esempi di policy basate su tag Per ulteriori informazioni sull'utilizzo dei tag per limitare l'accesso alle risorse, consulta Controlling access using tags nella IAM User Guide.

Ruoli IAM di Amazon Kendra

Un ruolo IAM è un'entità all'interno del tuo AWS account che dispone di autorizzazioni specifiche.

Utilizzo di credenziali temporanee con Amazon Kendra

È possibile utilizzare credenziali temporanee per effettuare l'accesso con la federazione, assumere un ruolo IAM o un ruolo multi-account. Puoi ottenere credenziali di sicurezza temporanee chiamando operazioni AWS STS API come o. AssumeRoleGetFederationToken

Amazon Kendra supporta l'utilizzo di credenziali temporanee.

Ruoli dei servizi

Questa caratteristica consente a un servizio di assumere un ruolo di servizio per conto dell'utente. Questo ruolo consente al servizio di accedere alle risorse in altri servizi per completare un'azione per conto dell'utente. I ruoli dei servizi sono visualizzati nell'account IAM e sono di proprietà dell'account. Ciò significa che un amministratore IAM può modificare le autorizzazioni per questo ruolo. Tuttavia, questo potrebbe pregiudicare la funzionalità del servizio.

Amazon Kendra supporta i ruoli di servizio.

Scelta di un ruolo IAM in Amazon Kendra

Quando crei un indice, richiami l'`BatchPutDocument`operazione, crei un'origine dati o crei una FAQ, devi fornire un ruolo di accesso Amazon Resource Name (ARN) che Amazon Kendra utilizza per accedere alle risorse richieste per tuo conto. Se hai già creato un ruolo, la console Amazon Kendra ti fornisce un elenco di ruoli tra cui scegliere. È importante scegliere un ruolo che consenta l'accesso alle risorse di cui hai bisogno. Per ulteriori informazioni, consulta IAM ruoli di accesso per Amazon Kendra.

Esempi di policy basate sull'identità di Amazon Kendra

Per impostazione predefinita, gli utenti e i ruoli non dispongono dell'autorizzazione per creare o modificare risorse Amazon Kendra. Inoltre, non possono eseguire attività utilizzando l'API AWS Management Console AWS CLI, o AWS . Un amministratore IAM deve creare policy IAM che concedono a utenti e ruoli l'autorizzazione per eseguire operazioni API specifiche sulle risorse

specificate di cui hanno bisogno. L'amministratore devi quindi collegare queste policy a utenti o gruppi che richiedono tali autorizzazioni.

Per informazioni su come creare una policy basata su identità IAM utilizzando questi documenti di policy JSON di esempio, consulta Creazione di policy nella scheda JSON nella Guida per l'utente IAM.

Argomenti

Best practice delle policy

Le politiche basate sull'identità determinano se qualcuno può creare, accedere o eliminare risorse Amazon Kendra nel tuo account. Queste azioni possono comportare costi aggiuntivi per l' Account AWS. Quando crei o modifichi policy basate su identità, segui queste linee guida e raccomandazioni:

- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi: per iniziare a concedere autorizzazioni a utenti e carichi di lavoro, utilizza le politiche gestite che concedono le autorizzazioni per molti casi d'uso comuni.AWS Sono disponibili nel tuo. Account AWS Ti consigliamo di ridurre ulteriormente le autorizzazioni definendo politiche gestite dai AWS clienti specifiche per i tuoi casi d'uso. Per ulteriori informazioni, consulta Policy gestite da AWS o Policy gestite da AWS per le funzionalità dei processi nella Guida per l'utente di IAM.
- Applica le autorizzazioni con privilegi minimi: quando imposti le autorizzazioni con le policy IAM, concedi solo le autorizzazioni richieste per eseguire un'attività. Puoi farlo definendo le azioni che possono essere intraprese su risorse specifiche in condizioni specifiche, note anche come autorizzazioni con privilegi minimi. Per ulteriori informazioni sull'utilizzo di IAM per applicare le autorizzazioni, consulta Policy e autorizzazioni in IAM nella Guida per l'utente di IAM.
- Condizioni d'uso nelle policy IAM per limitare ulteriormente l'accesso: per limitare l'accesso ad azioni e risorse puoi aggiungere una condizione alle tue policy. Ad esempio, è possibile scrivere una condizione di policy per specificare che tutte le richieste devono essere inviate utilizzando SSL. Puoi anche utilizzare le condizioni per concedere l'accesso alle azioni del servizio se vengono utilizzate tramite uno specifico Servizio AWS, ad esempio AWS CloudFormation. Per ulteriori

informazioni, consulta la sezione Elementi delle policy JSON di IAM: condizione nella Guida per l'utente di IAM.

- Utilizzo di IAM Access Analyzer per convalidare le policy IAM e garantire autorizzazioni sicure e funzionali: IAM Access Analyzer convalida le policy nuove ed esistenti in modo che aderiscano alla sintassi della policy IAM (JSON) e alle best practice di IAM. IAM Access Analyzer offre oltre 100 controlli delle policy e consigli utili per creare policy sicure e funzionali. Per ulteriori informazioni, consulta Convalida delle policy per IAM Access Analyzer nella Guida per l'utente di IAM.
- Richiedi l'autenticazione a più fattori (MFA): se hai uno scenario che richiede utenti IAM o un utente root nel Account AWS tuo, attiva l'MFA per una maggiore sicurezza. Per richiedere la MFA quando vengono chiamate le operazioni API, aggiungi le condizioni MFA alle policy. Per ulteriori informazioni, consulta Configurazione dell'accesso alle API protetto con MFA nella Guida per l'utente di IAM.

Per maggiori informazioni sulle best practice in IAM, consulta Best practice di sicurezza in IAM nella Guida per l'utente di IAM.

AWS Policy gestite (predefinite) per Amazon Kendra

AWS affronta molti casi d'uso comuni fornendo politiche IAM autonome create e amministrate da. AWS Queste politiche sono chiamate politiche AWS gestite. AWS le politiche gestite semplificano l'assegnazione delle autorizzazioni a utenti, gruppi e ruoli rispetto a quando si dovessero scrivere le politiche personalmente. Per ulteriori informazioni, consulta Aggiunta di autorizzazioni a un utente nella Guida per l'utente IAM.

Le seguenti politiche AWS gestite, che puoi allegare a gruppi e ruoli nel tuo account, sono specifiche di Amazon Kendra:

- AmazonKendraReadOnly— Garantisce l'accesso in sola lettura alle risorse di Amazon Kendra.
- AmazonKendraFullAccess— Garantisce l'accesso completo per creare, leggere, aggiornare, eliminare, etichettare ed eseguire tutte le risorse Amazon Kendra.

Per quanto riguarda la console, il tuo ruolo deve inoltre disporre di`iam:CreateRole`, `iam:CreatePolicy``iam:AttachRolePolicy`, e autorizzazioni. `s3:ListBucket`

> **Note**
>
> Puoi rivedere queste autorizzazioni accedendo alla console IAM e cercando policy specifiche.

Puoi anche creare politiche personalizzate per consentire le autorizzazioni per le azioni dell'API Amazon Kendra. Puoi collegare queste policy personalizzate ai ruoli o ai gruppi IAM che richiedono le autorizzazioni. Per esempi di politiche IAM per Amazon Kendra, consulta. Esempi di policy basate sull'identità di Amazon Kendra

Consentire agli utenti di visualizzare le loro autorizzazioni

Questo esempio mostra in che modo è possibile creare una policy che consente agli utenti IAM di visualizzare le policy inline e gestite che sono cpllegate alla relativa identità utente. Questa politica include le autorizzazioni per completare questa azione sulla console o utilizzando l'API o a livello di codice. 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": "*"
        }
```

```
    ]
}
```

Accesso a un indice Amazon Kendra

In questo esempio, vuoi concedere a un utente del tuo AWS account l'accesso per interrogare un indice.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "QueryIndex",
            "Effect": "Allow",
            "Action": [
                "kendra:Query"
            ],
            "Resource": "arn:aws:kendra:${Region}:${Account}:index/${Index ID}"
        }
    ]
}
```

Esempi di policy basate su tag

Le politiche basate su tag sono documenti di policy JSON che specificano le azioni che un principale può eseguire sulle risorse con tag.

Esempio: utilizzare un tag per accedere a una risorsa

Questa politica di esempio concede a un utente o a un ruolo nell' AWS account l'autorizzazione a utilizzare l'`Query`operazione con qualsiasi risorsa etichettata con la chiave **`department`** e il valore**`finance`**.

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

```
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/department": "finance"
                }
            }
        }
    ]
}
```

Esempio: usa un tag per attivare le operazioni di Amazon Kendra

Questa politica di esempio concede a un utente o a un ruolo nel tuo AWS account l'autorizzazione a utilizzare qualsiasi operazione Amazon Kendra tranne `TagResource` l'operazione con qualsiasi risorsa etichettata con la chiave e **`department`** il valore. **`finance`**

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "kendra:*",
            "Resource": "*"
        },
        {
            "Effect": "Deny",
            "Action": [
                "kendra:TagResource"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/department": "finance"
                }
            }
        }
    ]
}
```

Esempio: usa un tag per limitare l'accesso a un'operazione

Questa politica di esempio limita l'accesso di un utente o di un ruolo del tuo AWS account all'utilizzo dell'`CreateIndex`operazione, a meno che l'utente non fornisca il **`department`** tag e non disponga dei valori consentiti **`finance`** e**`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 politiche gestite per Amazon Kendra

Per aggiungere autorizzazioni a utenti, gruppi e ruoli, è più facile utilizzare le politiche AWS gestite che scrivere le politiche da soli. Creare policy gestite dal cliente IAM per fornire al tuo team solo le autorizzazioni di cui ha bisogno richiede tempo e competenza. Per iniziare rapidamente, puoi utilizzare le nostre politiche AWS gestite. Queste politiche coprono casi d'uso comuni e sono disponibili nel tuo AWS account. Per ulteriori informazioni sulle policy AWS gestite, consulta le policy AWS gestite nella IAM User Guide.

AWS i servizi mantengono e aggiornano le politiche AWS gestite. Non è possibile modificare le autorizzazioni nelle politiche AWS gestite. I servizi occasionalmente aggiungono altre autorizzazioni a una policy gestita da AWS per supportare nuove funzionalità. Questo tipo di aggiornamento interessa tutte le identità (utenti, gruppi e ruoli) a cui è collegata la policy. È più probabile che i servizi aggiornino una policy gestita da AWS quando viene avviata una nuova funzionalità o quando diventano disponibili nuove operazioni. I servizi non rimuovono le autorizzazioni da una policy AWS gestita, quindi gli aggiornamenti delle policy non comprometteranno le autorizzazioni esistenti.

Inoltre, AWS supporta politiche gestite per le funzioni lavorative che si estendono su più servizi. Ad esempio, la policy ReadOnlyAccess AWS gestita fornisce l'accesso in sola lettura a tutti i AWS servizi e le risorse. Quando un servizio lancia una nuova funzionalità, AWS aggiunge autorizzazioni di sola lettura per nuove operazioni e risorse. Per l'elenco e la descrizione delle policy di funzione dei processi, consulta la sezione Policy gestite da AWS per funzioni di processi nella Guida per l'utente di IAM.

AWS politica gestita: AmazonKendraReadOnly

Garantisce l'accesso in sola lettura alle risorse di Amazon Kendra. Questa policy include le seguenti autorizzazioni:

- `kendra`— Consente agli utenti di eseguire azioni che restituiscono un elenco di elementi o dettagli su un elemento. Ciò include le operazioni API che iniziano con `Describe`,`List`,`Query`,`BatchGetDocumentStatus`,`GetQuerySuggestions`, o`GetSnapshots`.

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

```
            "Action": [
                "kendra:Describe*",
                "kendra:List*",
                "kendra:Query",
                "kendra:BatchGetDocumentStatus",
                "kendra:GetQuerySuggestions",
                "kendra:GetSnapshots"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

AWS politica gestita: AmazonKendraFullAccess

Garantisce l'accesso completo per creare, leggere, aggiornare, eliminare, etichettare ed eseguire tutte le risorse Amazon Kendra. Questa policy include le seguenti autorizzazioni:

- `kendra`—Consente ai principali di accedere in lettura e scrittura a tutte le azioni in Amazon Kendra.
- `s3`—Consente ai mandanti di ottenere le posizioni dei bucket Amazon S3 e di elencare i bucket.
- `iam`—Consente ai presidi di passare ed elencare i ruoli.
- `kms`—Consente ai principali di descrivere ed AWS KMS elencare chiavi e alias.
- `secretsmanager`—Consente ai mandanti di creare, descrivere ed elencare segreti.
- `ec2`—Consente ai responsabili di descrivere gruppi di sicurezza, VCP (Virtual Private Cloud) e sottoreti.
- `cloudwatch`—Consente ai dirigenti di visualizzare le metriche di 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 si aggiorna alle politiche gestite AWS

Visualizza i dettagli sugli aggiornamenti delle politiche AWS gestite per Amazon Kendra da quando questo servizio ha iniziato a tracciare queste modifiche. Per ricevere avvisi automatici sulle modifiche a questa pagina, iscriviti al feed RSS nella pagina della cronologia dei documenti di Amazon Kendra.

Modifica	Descrizione	Data
AmazonKendraReadOnly— Aggiungi l'autorizzazione al supporto, alle API GetSnapshots BatchGetDocumentStatus	Amazon Kendra ha aggiunto nuove API e. `GetSnapshots BatchGetDocumentStatus` `GetSnapshots` fornisce dati che mostrano come gli utenti interagiscono con	3 gennaio 2022

Modifica	Descrizione	Data
	l'applicazione di ricerca. `BatchGetDocumentStatus` monitora lo stato di avanzamento dell'indicizzazione dei documenti.	
AmazonKendraReadOnly—Aggiunge l'autorizzazione all'operazione di supporto GetQuerySuggestions	Amazon Kendra ha aggiunto una nuova `GetQuerySuggestions` API che consente di accedere a suggerimenti di query per le query di ricerca più comuni, aiutando a guidare la ricerca degli utenti. Quando gli utenti digitano la query di ricerca, la query suggerita aiuta a completare automaticamente la ricerca.	27 maggio 2021
Amazon Kendra ha iniziato a tracciare le modifiche	Amazon Kendra ha iniziato a tracciare le modifiche per AWS le sue politiche gestite.	27 maggio 2021

Risoluzione dei problemi relativi a Amazon Kendra Identity and Access

Utilizza le seguenti informazioni per aiutarti a diagnosticare e risolvere i problemi più comuni che potresti riscontrare quando lavori con Amazon Kendra e IAM.

Argomenti

- Non sono autorizzato a eseguire un'azione in Amazon Kendra
- Non sono autorizzato a eseguire iam: PassRole
- Sono un amministratore e desidero consentire ad altri di accedere ad Amazon Kendra
- Voglio consentire a persone esterne al mio AWS account di accedere alle mie risorse Amazon Kendra

Non sono autorizzato a eseguire un'azione in Amazon Kendra

Se ti AWS Management Console dice che non sei autorizzato a eseguire un'azione, devi contattare l'amministratore per ricevere assistenza. L'amministratore è colui che ti ha fornito le credenziali di accesso.

L'errore di esempio seguente si verifica quando l'`mateojackson`utente tenta di utilizzare la console per visualizzare i dettagli di un indice ma non dispone `kendra:DescribeIndex` delle autorizzazioni.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 kendra:DescribeIndex on resource: index ARN
```

In questo caso, Mateo richiede al suo amministratore di aggiornare le policy per poter accedere alla risorsa `index` utilizzando l'azione `kendra:DescribeIndex`.

Non sono autorizzato a eseguire iam: PassRole

Se ricevi un messaggio di errore indicante che non sei autorizzato a eseguire l'`iam:PassRole`azione, le tue politiche devono essere aggiornate per consentirti di trasferire un ruolo ad Amazon Kendra.

Alcuni Servizi AWS consentono di trasferire un ruolo esistente a quel servizio invece di creare un nuovo ruolo di servizio o un ruolo collegato al servizio. Per eseguire questa operazione, è necessario disporre delle autorizzazioni per trasmettere il ruolo al servizio.

Il seguente errore di esempio si verifica quando un utente IAM denominato `marymajor` tenta di utilizzare la console per eseguire un'azione in Amazon Kendra. Tuttavia, l'azione richiede che il servizio disponga delle autorizzazioni concesse da un ruolo di servizio. Mary non dispone delle autorizzazioni per passare il ruolo al servizio.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

In questo caso, le policy di Mary devono essere aggiornate per poter eseguire l'operazione `iam:PassRole`.

Se hai bisogno di aiuto, contatta il tuo AWS amministratore. L'amministratore è la persona che ti ha fornito le credenziali di accesso.

Sono un amministratore e desidero consentire ad altri di accedere ad Amazon Kendra

Per consentire ad altri di accedere ad Amazon Kendra, devi creare un'entità IAM (utente o ruolo) per la persona o l'applicazione che deve accedere. Tale utente o applicazione utilizzerà le credenziali dell'entità per accedere ad AWS. Devi quindi allegare una politica all'entità che concede loro le autorizzazioni corrette in Amazon Kendra.

Per iniziare immediatamente, consulta Creazione dei primi utenti e gruppi delegati IAM nella Guida per l'utente di IAM.

Voglio consentire a persone esterne al mio AWS account di accedere alle mie risorse Amazon Kendra

È possibile creare un ruolo con il quale utenti in altri account o persone esterne all'organizzazione possono accedere alle tue risorse. È possibile specificare chi è attendibile per l'assunzione del ruolo. Per servizi che supportano policy basate su risorse o liste di controllo accessi (ACL), utilizza tali policy per concedere alle persone l'accesso alle tue risorse.

Per ulteriori informazioni, consulta gli argomenti seguenti:

- Per sapere se Amazon Kendra supporta queste funzionalità, consulta. Come funziona Amazon Kendra con IAM
- Per sapere come fornire l'accesso alle tue risorse attraverso Account AWS le risorse di tua proprietà, consulta Fornire l'accesso a un utente IAM in un altro Account AWS di tua proprietà nella IAM User Guide.
- Per scoprire come fornire l'accesso alle tue risorse a terze parti Account AWS, consulta Fornire l'accesso a soggetti Account AWS di proprietà di terze parti nella Guida per l'utente IAM.
- Per informazioni su come fornire l'accesso tramite la federazione delle identità, consulta Fornire l'accesso a utenti autenticati esternamente (Federazione delle identità) nella Guida per l'utente di IAM.
- Per informazioni sulle differenze tra l'utilizzo di ruoli e policy basate su risorse per l'accesso multi-account, consulta Differenza tra i ruoli IAM e le policy basate su risorse nella Guida per l'utente IAM.

Best practice di sicurezza

Amazon Kendra offre una serie di funzionalità di sicurezza da prendere in considerazione durante lo sviluppo e l'implementazione delle proprie politiche di sicurezza. Le seguenti best practice sono linee guida generali e non rappresentano una soluzione di sicurezza completa. Poiché queste best practice potrebbero non essere appropriate o sufficienti per l'ambiente, gestiscile come considerazioni utili anziché prescrizioni.

Applicazione del principio del privilegio minimo

Amazon Kendra fornisce una policy di accesso granulare per le applicazioni che utilizzano ruoli. IAM Consigliamo di concedere ai ruoli solo il set minimo di privilegi richiesto dal lavoro, ad esempio la copertura della candidatura e l'accesso alla destinazione dei log. Si consiglia inoltre di verificare i processi per le autorizzazioni su base regolare e in caso di modifiche all'applicazione.

Autorizzazioni per il controllo degli accessi basato su ruoli (RBAC)

Gli amministratori devono controllare rigorosamente le autorizzazioni RBAC (Role-based access control) per le applicazioni Amazon Kendra.

Registrazione e monitoraggio in Amazon Kendra

Il monitoraggio è un elemento importante per mantenere l'affidabilità, la disponibilità e le prestazioni delle applicazioni Amazon Kendra. Per monitorare le chiamate all'API Amazon Kendra, puoi utilizzare. AWS CloudTrail Per monitorare lo stato dei tuoi lavori, usa Amazon CloudWatch Logs.

- Amazon CloudWatch Alarms: utilizzando gli CloudWatch allarmi, controlli una singola metrica per un periodo di tempo specificato. Se la metrica supera una policy. CloudWatch gli allarmi non richiamano azioni quando una metrica si trova in uno stato particolare. È necessario invece cambiare lo stato e mantenerlo per un numero di periodi specificato. Per ulteriori informazioni, consulta Monitoraggio di Amazon Kendra con Amazon CloudWatch.
- AWS CloudTrail Registri: CloudTrail forniscono un registro delle azioni intraprese da un utente, un ruolo o un AWS servizio in Amazon Kendra o Amazon Kendra Intelligent Ranking. Utilizzando le informazioni raccolte da CloudTrail, puoi determinare la richiesta che è stata effettuata ad Amazon Kendra, l'indirizzo IP da cui è stata effettuata la richiesta, chi ha effettuato la richiesta, quando è stata effettuata e ulteriori dettagli. Per ulteriori informazioni, consulta Registrazione delle chiamate API di Amazon Kendra conAWS CloudTrailregistri e Registrazione delle chiamate all'API di Ranking di Amazon Kendra conAWS CloudTrailregistri.

Convalida della conformità per Amazon Kendra

I revisori di terze parti valutano la sicurezza e la conformità di Amazon Kendra nell'ambito di diversi programmi di conformità di Amazon Kendra. Amazon Kendra è conforme a quanto segue:

- Health Insurance Portability and Accountability Act (HIPAA)
- Controlli di sistema e organizzazione (SOC) 2
- Programma per valutatori registrati per la sicurezza delle informazioni (IRAP)
- Programma federale di gestione dei rischi e delle autorizzazioni (FedRAMP) Moderato nelle regioni est/occidentali degli Stati Uniti
- Programma federale di gestione dei rischi e delle autorizzazioni (FedRAMP) elevato nella regione AWS (Stati Uniti occidentali) GovCloud

Per informazioni generali, vedere Programmi di AWS conformità Programmi di di .

È possibile scaricare report di audit di terze parti utilizzando AWS Artifact. Per ulteriori informazioni, consulta Scaricamento dei report in AWS Artifact Scaricamento dei . AWS

La tua responsabilità di conformità quando usi Amazon Kendra è determinata dalla sensibilità dei tuoi dati, dagli obiettivi di conformità della tua azienda e dalle leggi e dai regolamenti applicabili. AWS fornisce le seguenti risorse per contribuire alla conformità:

- Guide rapide su sicurezza e conformità Guide introduttive implementazione illustrano considerazioni sull'architettura e forniscono passaggi per implementare ambienti di base incentrati sulla sicurezza e sulla conformità. AWS
- Whitepaper sull'architettura per la sicurezza e la conformità HIPAA: questo white paper descrive in che modo le aziende possono utilizzare per creare applicazioni conformi all'HIPAA. AWS
- AWS Risorse per la conformità Risorse per la conformità: questa raccolta di cartelle di lavoro e guide potrebbe operate.
- Valutazione delle risorse con le regole nella Guida per gli AWS Config sviluppatori: il AWS Config servizio valuta la conformità delle configurazioni delle risorse alle pratiche interne, alle linee guida del settore e alle normative.
- AWS Security Hub—Questo AWS servizio offre una visione completa dello stato di sicurezza dell'utente, AWS che consente di verificare la conformità agli standard e alle best practice del settore della sicurezza.

Resilienza in Amazon Kendra

L'infrastruttura AWS globale è costruita attorno AWS a regioni e zone di disponibilità. AWS Le regioni forniscono più zone di disponibilità fisicamente separate e isolate, collegate con reti a bassa latenza, ad alto throughput e altamente ridondanti. Con le zone di disponibilità, puoi progettare e gestire applicazioni e database che eseguono automaticamente il failover tra zone di disponibilità senza interruzioni. Le zone di disponibilità sono più disponibili, tolleranti ai guasti e scalabili rispetto alle infrastrutture a data center singolo o multiplo tradizionali.

Per ulteriori informazioni su AWS regioni e zone di disponibilità, consulta Global Infrastructure.AWS

Con un'infrastruttura AWS globale, Amazon Kendra Enterprise Edition è tollerante ai guasti, scalabile e altamente disponibile. Il ripristino alle versioni precedenti di un indice non è attualmente supportato, ma puoi aggiornare o ricreare parti dell'indice eliminando e aggiungendo nuovamente le fonti di dati esistenti all'indice.

Sicurezza dell'infrastruttura in Amazon Kendra

In quanto servizio gestito, Amazon Kendra è protetto AWS dalla sicurezza di rete globale. Per informazioni sui servizi di AWS sicurezza e su come AWS protegge l'infrastruttura, consulta AWS Cloud Security. Per progettare il tuo AWS ambiente utilizzando le migliori pratiche per la sicurezza dell'infrastruttura, vedi Infrastructure Protection in Security Pillar AWS Well-Architected Framework.

Utilizzi chiamate API AWS pubblicate per accedere ad Amazon Kendra attraverso la rete. I client devono supportare quanto segue:

- Transport Layer Security (TLS). È richiesto TLS 1.2 ed è consigliato TLS 1.3.
- Suite di cifratura con Perfect Forward Secrecy (PFS), ad esempio Ephemeral Diffie-Hellman (DHE) o Elliptic Curve Ephemeral Diffie-Hellman (ECDHE). La maggior parte dei sistemi moderni, come Java 7 e versioni successive, supporta tali modalità.

Inoltre, le richieste devono essere firmate utilizzando un ID chiave di accesso e una chiave di accesso segreta associata a un principale IAM. O puoi utilizzare AWS Security Token Service (AWS STS) per generare credenziali di sicurezza temporanee per sottoscrivere le richieste.

Configurazione e analisi delle vulnerabilità in AWS Identity and Access Management

AWS gestisce le attività di sicurezza di base come l'applicazione di patch al sistema operativo guest (OS) e al database, la configurazione del firewall e il disaster recovery. Queste procedure sono state riviste e certificate dalle terze parti appropriate. Per ulteriori dettagli, consulta le seguenti risorse :

- Modello di responsabilità condivisa
- AWS: Panoramica dei processi di sicurezza (white paper)

Le seguenti risorse riguardano anche la configurazione e l'analisi delle vulnerabilità in (): AWS Identity and Access Management IAM

- Convalida della conformità per AWS Identity and Access Management
- Migliori pratiche di sicurezza e casi d'uso in AWS Identity and Access Management.

Quote per Amazon Kendra

Regioni supportate

Per un elenco delle AWS regioni in cui Amazon Kendra è disponibile, consulta Amazon Kendra le regioni e gli endpoint nell'Amazon Web Services General Reference.

Quote

Le quote di servizio, note anche come limiti, sono il numero massimo di risorse di servizio per il tuo AWS account. Per ulteriori informazioni, consulta Amazon Kendra Service Quotas in Riferimenti generali di AWS .

Quote indicizzate

Descrizione	Default	Edizione	Regolabile
Numero massimo di indici per account	10	Sviluppatore, Enterprise	Sì
Quantità di testo estratta per un indice in una singola unità (Sviluppatore). Non puoi aggiungere unità aggiuntive per l'estrazione del testo per la Developer Edition.	3 GB	Developer	No
Quantità di testo estratto per un indice in una singola unità (Enterprise). Puoi aggiungere fino a 100 unità aggiuntive per l'estrazione del	30 GB	Enterprise	Sì

Descrizione	Default	Edizione	Regolabile
testo per l'Enterprise Edition o semplicem ente contattare l'assistenza.			

Quote dei connettori di origine dati

Descrizione	Default	Edizione	Regolabile
Numero massimo di connettori di origine dati per indice (sviluppatore)	5	Developer	No
Numero massimo di connettori di origine dati per indice (Enterprise)	50	Enterprise	Sì
Dimensione massima di un singolo documento o file raw quando si utilizza un connettore di origine dati	50 MB	Sviluppatore, azienda	Sì
Numero massimo di prefissi S3 nel file di configurazione dell'elenco di controllo degli accessi incluso nel Amazon S3 connettore di origine dati	100	Sviluppatore, Enterprise	No

Descrizione	Default	Edizione	Regolabile
Dimensione massima del file di configurazione dell'elenco di controllo degli accessi incluso nel connettore di origine Amazon S3 dati	50 MB	Sviluppatore, Enterprise	Sì

Quote per domande frequenti

Descrizione	Default	Edizione	Regolabile
Numero massimo di domande frequenti per indice	30	Sviluppatore, Enterprise	Sì
Dimensione massima di 1 FAQ	5 MB	Sviluppatore, Enterprise	Sì
Numero massimo di risultati restituiti per le domande frequenti	4	Sviluppatore, Enterprise	Sì
Numero massimo di caratteri consentito per una domanda FAQ	300	Sviluppatore, Enterprise	No
Numero massimo di caratteri in una risposta alle domande frequenti	2000	Sviluppatore, Enterprise	No

Quote del thesaurus

Descrizione	Default	Edizione	Regolabile
Numero massimo di thesauri per indice	1	Sviluppatore, Enterprise	No
Dimensione massima di un file del thesaurus	5 MB	Sviluppatore, Enterprise	Sì
Numero massimo di regole relative ai sinonimi per thesaurus	10.000	Sviluppatore, Enterprise	Sì
Numero massimo di sinonimi per termine in tutti i thesauri di un indice	10	Sviluppatore, Enterprise	No

Amazon Kendra quote di esperienza

Descrizione	Default	Edizione	Regolabile
Numero massimo di Amazon Kendra esperienze per indice	50	Sviluppatore, azienda	Sì

Quote relative alle query e ai risultati di ricerca

Descrizione	Default	Edizione	Regolabile
Quantità di query al secondo per un	0,05	Developer	No

Descrizione	Default	Edizione	Regolabile
indice in una singola unità (Developer). Non puoi aggiunger e unità aggiuntive per le query per la Developer Edition.			
Quantità di query al secondo per un indice in una singola unità (Enterprise). Puoi aggiungere fino a 100 unità aggiuntive per le domande relative all'Enterprise Edition o semplicemente contattare l'assistenza.	0.1	Enterprise	Sì
Numero massimo di caratteri per testo della query	1000	Sviluppatore, Enterprise	Sì
Numero massimo di risultati di ricerca per query. L'impostazione predefinita è 100. Per consentire più di 100 risultati, contatta semplicemente l'assistenza.	100	Sviluppatore, Enterprise	Sì
Numero massimo di risultati di ricerca per pagina	100	Sviluppatore, Enterprise	Sì

Descrizione	Default	Edizione	Regolabile
Numero massimo di parole chiave per testo della query prima del troncamento. Il valore predefinito è 30. Per consentire più di 30 parole, contatta semplicemente l'assistenza.	30	Sviluppatore, Enterprise	Sì
Dimensione massima dell'elenco dei gruppi di utenti per attributo di query	10	Sviluppatore, Enterprise	Sì
Dimensione massima dell'elenco di stringhe per attributo di query	10	Sviluppatore, Enterprise	Sì

Quote, suggerimenti, suggerimenti

Descrizione	Default	Edizione	Regolabile
Numero massimo di suggerimenti di interrogazione restituiti per chiamata GetQuerySuggestions	10	Sviluppatore, Enterprise	Sì
Numero massimo di campi/attributi per i suggerimenti di interrogazione per	10	Sviluppatore, azienda	Sì

Descrizione	Default	Edizione	Regolabile
chiamata GetQuerySuggestions			
Numero massimo di campi/attributi aggiuntivi per i suggerimenti di interrogazione per chiamata GetQuerySuggestions	5	Sviluppatore, Enterprise	Sì
Numero massimo di elenchi di blocchi per indice	1	Sviluppatore, Enterprise	No
Dimensione massima di un file di testo con un elenco di blocchi	2 MB	Sviluppatore, Enterprise	Sì
Numero massimo di elementi (parole o frasi) in un elenco di blocco	20.000	Sviluppatore, Enterprise	Sì
Numero massimo di suggerimenti di interrogazione con correzione ortografica da restituire in una chiamata API. `Query`	1	Sviluppatore, Enterprise	Sì

Quote dei documenti

Descrizione	Default	Edizione	Regolabile
Quantità di testo estratto per un indice in una singola unità (Developer). Non puoi aggiungere unità aggiuntive per l'estrazione del testo per la Developer Edition.	3 GB	Developer	No
Quantità di testo estratto per un indice in una singola unità (Enterprise). Puoi aggiungere fino a 100 unità aggiuntive per l'estrazione del testo per l'Enterprise Edition o semplicemente contattare l'assistenza.	30 GB	Enterprise	Sì
Dimensione massima di un singolo documento o file raw quando si utilizza un connettore di origine dati	50 MB	Sviluppatore, azienda	Sì
Dimensione massima di un singolo documento o file raw quando si	5 MB	Sviluppatore, azienda	Sì

Descrizione	Default	Edizione	Regolabile
utilizza l'`BatchPutDocument` API			
Quantità massima di testo estratto da un singolo documento	5 MB	Sviluppatore, Enterprise	No
Numero massimo di campi/attributi personalizzati per indice	500	Sviluppatore, Enterprise	No

Quote dei risultati di ricerca in evidenza

Descrizione	Default	Edizione	Regolabile
Numero massimo di documenti in evidenza per set di risultati in evidenza	4	Enterprise	Sì
Numero massimo di testi di interrogazione per set di risultati in evidenza	49	Enterprise	No
Numero massimo di caratteri per testo di query in un set di risultati in evidenza	1000	Enterprise	Sì
Numero massimo di set di risultati in evidenza per indice	50	Enterprise	Sì

Riscrive/riordina le quote dei risultati di ricerca

Descrizione	Default	Edizione	Regolabile
Numero massimo di `Rescore` richieste al secondo per un piano di esecuzione di rescore o per una singola unità di capacità. È possibile aggiungere fino a 1000 unità aggiuntive.	0.01	Enterprise	No
Numero massimo di piani di esecuzione di rescore per account.	50	Enterprise	Sì
Numero massimo di token in ingresso `Title` per un documento in una `Rescore` richiesta.	100	Enterprise	No
Numero massimo di token in ingresso `Body` per un documento in una `Rescore` richiesta.	200	Enterprise	No
Numero massimo di documenti in una `Rescore` richiesta.	25	Enterprise	No
Numero massimo di documenti per gruppo	3	Enterprise	No

Descrizione	Default	Edizione	Regolabile
in una `Rescore` richiesta.			

Per ulteriori informazioni sulle quote di Amazon Kendra servizio e per richiedere un aumento delle quote, vedere Service Quotas.

Risoluzione dei problemi

Questa sezione può aiutarti a risolvere i problemi più comuni che potresti riscontrare quando lavori con Amazon Kendra.

Argomenti

Risoluzione dei problemi relativi alle origini dati

Questa sezione può aiutarti a risolvere i problemi più comuni relativi alla configurazione e all'utilizzo Amazon Kendra dei connettori di origine dati.

I miei documenti non sono stati indicizzati

Quando sincronizzi l' Amazon Kendra indice con un'origine dati, potresti riscontrare problemi che impediscono l'indicizzazione dei documenti. L'indicizzazione è un processo in due fasi. Innanzitutto, viene verificata la presenza di documenti nuovi e aggiornati da indicizzare e per individuare i documenti da rimuovere dall'indice. In secondo luogo, a livello di documento, ogni documento è accessibile e indicizzato.

In uno di questi passaggi può verificarsi un errore. Gli errori a livello di origine dati vengono segnalati nella console nella sezione Cronologia delle esecuzioni di sincronizzazione della pagina dei dettagli dell'origine dati. Lo stato del processo di sincronizzazione può essere Riuscito, Incompleto o Non riuscito. È inoltre possibile visualizzare il numero di documenti indicizzati ed eliminati durante il processo. Se lo stato è Fallito, viene visualizzato un messaggio nella colonna Dettagli.

Gli errori a livello di documento vengono segnalati in Amazon CloudWatch Logs. È possibile visualizzare gli errori utilizzando la CloudWatch console.

Per generare un rapporto sullo stato della sincronizzazione dei documenti, vedi Desidero generare un rapporto sullo stato della sincronizzazione per i miei documenti.

Il mio processo di sincronizzazione non è riuscito

Un processo di sincronizzazione in genere fallisce quando si verifica un errore di configurazione nell'indice o nell'origine dati. Nella console, puoi trovare il messaggio di errore nella sezione Cronologia delle esecuzioni di sincronizzazione della pagina dei dettagli dell'origine dati, nella colonna Dettagli. Gli errori a livello di documento sono segnalati in Amazon CloudWatch Logs. Il messaggio di errore fornisce informazioni su cosa è andato storto. Il problema è in genere che l'indice o l'origine dati non dispongono delle IAM autorizzazioni appropriate. Il messaggio di errore descrive le autorizzazioni mancanti. Ecco alcuni dei messaggi di errore che puoi ricevere:

```
Failed to create log group for job. Please make sure that the IAM role
provided has sufficient permissions.
```

Se il ruolo di indice non dispone dell'autorizzazione all'uso CloudWatch, l'origine dati non sarà in grado di creare un CloudWatch registro. Se viene visualizzato questo errore, è necessario aggiungere CloudWatch le autorizzazioni al ruolo di indice.

```
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.
```

Quando si utilizza una fonte di Amazon S3 dati, è Amazon Kendra necessario disporre dell'autorizzazione per accedere al bucket che contiene i documenti. È necessario aggiungere l'autorizzazione Amazon Kendra per leggere il bucket al ruolo di origine IAM dati.

```
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 necessita dell'autorizzazione per assumere i IAM ruoli di indice e origine dati. È necessario aggiungere una politica di attendibilità ai ruoli con autorizzazione per l'`sts:AssumeRole`azione.

Per le IAM politiche che Amazon Kendra richiedono l'indicizzazione di un'origine dati, consulta IAM i ruoli.

Per generare un rapporto sullo stato della sincronizzazione dei documenti, vedi Desidero generare un rapporto sullo stato della sincronizzazione per i miei documenti.

Il mio processo di sincronizzazione è incompleto

I lavori sono generalmente incompleti quando hanno completato il processo a livello di origine dati, ma presentano qualche errore durante il processo a livello di documento. Quando un lavoro è incompleto, alcuni documenti potrebbero non essere stati indicizzati correttamente. Per un'origine Amazon S3 dati, un processo incompleto è in genere causato da:

- I metadati per uno o più documenti non erano validi.
- Quando i documenti vengono inviati per l'indicizzazione ma almeno un documento non è stato inviato.
- Quando vengono inviati documenti per essere eliminati dall'indice ma almeno un documento non è stato inviato.

Per risolvere un processo di sincronizzazione incompleto, consulta innanzitutto i tuoi log. CloudWatch

1. Dalla colonna dei dettagli, scegli Visualizza dettagli in. CloudWatch
2. Esamina i messaggi di errore per vedere cosa ha causato il fallimento del documento.

Per generare un rapporto sullo stato della sincronizzazione dei documenti, vedi Desidero generare un rapporto sullo stato della sincronizzazione per i miei documenti.

Il mio processo di sincronizzazione è riuscito ma non ci sono documenti indicizzati

Occasionalmente, un processo di sincronizzazione dell'indice eseguito viene contrassegnato come Riuscito, ma non ci sono documenti nuovi o aggiornati indicizzati quando previsto. Le ragioni possibili sono:

- Controlla la CloudWatch `DocumentsSubmittedForIndexingFailed` metrica per vedere se qualche documento non è riuscito a sincronizzarsi. Controlla i tuoi CloudWatch log per i dettagli.
- Per una fonte di Amazon S3 dati, potresti aver fornito Amazon Kendra il nome o il prefisso del bucket errato. Assicurati che il bucket che stai utilizzando Amazon Kendra sia quello che contiene i documenti da indicizzare.
- Quando reindicizzi un documento che non è stato indicizzato in un lavoro precedente, non lo indicizzerà a meno che tu Amazon Kendra non abbia modificato il documento o il file di metadati associato.

Per generare un rapporto sullo stato della sincronizzazione dei documenti, vedi Desidero generare un rapporto sullo stato della sincronizzazione per i miei documenti.

Sto riscontrando problemi di formato dei file durante la sincronizzazione della mia fonte di dati

Se riscontri problemi di formato dei file durante l'aggiunta di file alla fonte dati o la sincronizzazione dell'origine dati, assicurati che i tipi di documento siano Amazon Kendra supportati. Per un elenco dei tipi di documenti supportati da, Amazon Kendra consulta Tipi o formati di documenti.

Se utilizzi l'`BatchPutDocument`API con file di testo semplice, specifica `PLAIN_TEXT` come tipo di contenuto.

Voglio generare un rapporto sulla cronologia delle sincronizzazioni per i miei documenti

Quando Amazon Kendra sincronizzi il connettore della sorgente dati, Amazon Kendra puoi generare report sullo stato della sincronizzazione per ogni documento nella tua fonte di dati e copiarli in un Amazon S3 bucket. Durante questo processo, i dati vengono crittografati tramite AWS KMS chiavi e possono essere visualizzati solo da te. Lo stato del documento segnalato può essere uno dei seguenti: Non riuscito, Completato o Riuscito con errori.

Prima di poter generare report sullo stato della sincronizzazione, è necessario effettuare le seguenti operazioni:

- Aggiungi il seguente Amazon Kendra servizio principale alla tua politica di Amazon S3 accesso

```
{
    “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/*”
        }
    ]
```

```
}
```

- Crea un Amazon S3 bucket con autorizzazioni di accesso a Amazon Kendra

Se utilizzi la console, per generare un rapporto sullo stato della sincronizzazione, scegli di attivare l'opzione di generazione della cronologia di sincronizzazione dalla pagina dei dettagli dell'origine dati. Quindi, inserisci la posizione del Amazon S3 bucket e scegli tra le opzioni di configurazione disponibili. I report verranno generati dalla sincronizzazione successiva dopo l'attivazione della funzione di generazione del rapporto.

Se elimini il Amazon S3 bucket, perderai i dati di registro e dovrai configurare un nuovo bucket per archiviare i nuovi report di sincronizzazione.

Lo stato della generazione dei report di sincronizzazione è attualmente supportato solo per il Amazon S3 connettore.

Quanto tempo richiede la sincronizzazione di una fonte di dati?

Se non ci sono aggiornamenti ai documenti, il tempo di sincronizzazione di un Amazon Kendra indice aumenta in modo lineare rispetto al numero di documenti. Ad esempio, la sincronizzazione di 1.000 documenti senza aggiornamenti richiederebbe circa cinque minuti e 2.000 documenti senza aggiornamenti circa 10 minuti. Se sono presenti aggiornamenti ai documenti, il tempo di sincronizzazione aumenterà in base al numero di documenti aggiornati.

Qual è il costo per la sincronizzazione di una fonte di dati?

Quando sincronizzi l'indice, occorrono due minuti per riscaldarsi e Amazon EC2 attivarsi per stabilire le connessioni necessarie. Non ti viene addebitato alcun costo durante questo processo. Il misuratore di utilizzo inizia solo dopo l'avvio del processo di sincronizzazione. Per ulteriori informazioni sui Amazon Kendra prezzi, consulta la pagina Amazon Kendra dei prezzi.

Ricevo un errore di Amazon EC2 autorizzazione

Se si verifica un errore di funzionamento Amazon EC2 non autorizzato durante una sincronizzazione per un'origine dati su cloud privato virtuale (VPC), è probabile che il ruolo IAM VPC non disponga delle autorizzazioni necessarie. Verifica che il IAM ruolo che utilizzi per la tua origine dati disponga delle autorizzazioni allegate. Per ulteriori informazioni, consulta IAM Ruolo nel cloud privato virtuale.

Non riesco a utilizzare i link all'indice di ricerca per aprire i miei Amazon S3 oggetti

Amazon Kendra L'indice può accedere solo ai file per i quali un'origine Amazon S3 dati gli concede le autorizzazioni di accesso. Ad esempio, Amazon Kendra non è possibile modificare le Amazon S3 autorizzazioni che determinano se un oggetto deve essere pubblico o crittografato. Amazon Kendra inoltre non dispone delle autorizzazioni predefinite per creare o restituire un link firmato per gli Amazon S3 oggetti. Se desideri attivare il collegamento firmato per Amazon S3 gli oggetti in un Amazon Kendra indice, hai due opzioni:

- È possibile utilizzare la firma dei risultati della query sull'indice con l'oggetto uri di origine prima di restituire il risultato alla pagina di ricerca. Per una descrizione step-by-step dettagliata di questo processo, consultate Condivisione di oggetti utilizzando URL predefiniti.
- È possibile sovrascrivere l'URI della fonte dei metadati Amazon S3 dell'oggetto e rendere disponibile il servizio tramite una rete per la distribuzione di CloudFront contenuti (CDN) connessa a un bucket. Amazon S3 In alternativa, puoi utilizzare un endpoint API Gateway proxy che restituisce un URL predefinito e reindirizza ad esso.

Ricevo un messaggio di errore relativo all'AccessDenied utilizzo del file del certificato SSL

Se ricevi un errore di accesso negato quando usi un certificato SSL con la tua origine dati, assicurati che il tuo IAM ruolo disponga dell'autorizzazione per accedere al file del certificato SSL nella posizione specificata. Se il certificato è crittografato con una AWS KMS chiave, il tuo IAM ruolo dovrebbe avere anche l'autorizzazione a decrittografare utilizzando la chiave. AWS KMS Per ulteriori informazioni, consulta Autenticazione e controllo degli accessi per. AWS KMS

Ricevo un errore di autorizzazione quando utilizzo una fonte di SharePoint dati

Se ricevi un errore di autorizzazione durante la sincronizzazione dell'indice con un'origine SharePoint dati, conferma che ti è stato assegnato un ruolo di amministratore del sito in SharePoint.

Il mio indice non esegue la scansione dei documenti dalla mia fonte di dati Confluence

Se l' Amazon Kendra indice non esegue la scansione dei documenti dalla fonte dati Confluence durante il processo di sincronizzazione, conferma di far parte dei gruppi di amministratori di Confluence.

Risoluzione dei problemi dei risultati della ricerca nei documenti

Questa sezione può aiutarti a risolvere i problemi nei risultati Amazon Kendra di ricerca.

I miei risultati di ricerca non sono pertinenti alla mia query di ricerca

Se i risultati della ricerca sembrano irrilevanti, potrebbe essere per i seguenti motivi:

- I risultati vengono inclusi con `LOW` sicurezza nei risultati. Puoi filtrare i risultati con `LOW` sicurezza utilizzando il `ScoreAttributes` campo QueryResultItem'per escludere qualsiasi risultato con un valore di`LOW`. Amazon Kendra assegna a ogni risultato un valore del bucket di confidenza pari a `VERY_HIGH`HIGH, `MEDIUM` e. `LOW` Questi valori indicano il livello di certezza che un risultato è rilevante per una query. Inoltre, indipendentemente dai valori di confidenza, Amazon Kendra restituisce tre tipi di risultati nel seguente ordine: `ANSWER` (estratto della risposta consigliata), (FAQ) e `QUESTION_ANSWER` `DOCUMENT` (estratto del documento). Pertanto, è possibile che un risultato di fiducia sia posizionato al di sopra di un `QUESTION_ANSWER` risultato di `LOW` fiducia. `VERY_HIGH` `DOCUMENT` Tuttavia, non è sempre necessariamente vero che `LOW` la fiducia `QUESTION_ANSWER` sia un risultato migliore della `VERY_HIGH` fiducia`DOCUMENT`.
- Alcuni campi o attributi di metadati vengono potenziati a un valore molto elevato, che influisce sulla classificazione dei risultati. Amazon Kendra esegue ricerche nell'indice utilizzando più parametri come titolo del documento, testo, data e campi o attributi di testo personalizzati. Puoi sperimentare diversi valori di potenziamento per ottenere i migliori risultati in tutte le query. Puoi anche utilizzare l'ottimizzazione dinamica della pertinenza a livello di query per utilizzare valori di incremento diversi per ogni query.
- Gli utenti utilizzano termini specializzati quando richiedono informazioni e per l'indice non è stato impostato alcun sinonimo personalizzato per la gestione di questi termini specialistici. Per ulteriori dettagli su come e quando utilizzare i sinonimi, consulta Aggiungere sinonimi personalizzati a un indice.

Perché vedo solo 100 risultati?

Amazon Kendra restituisce il conteggio totale dei documenti pertinenti. Per impostazione predefinita, vengono restituiti i primi 100 per query. I risultati sono suddivisi in pagine. È possibile utilizzare `PageNumber` per accedere a pagine diverse.

È possibile configurare Amazon Kendra per restituire fino a 1.000 documenti o risultati di ricerca per query, con un massimo di 100 risultati per pagina. Per restituire più di 100 risultati, puoi richiederlo contattando Quotas Support. L'aumento del numero di risultati di ricerca potrebbe influire sulla latenza.

Perché mancano i documenti che mi aspetto di vedere scomparsi?

Amazon Kendra supporta gli elenchi di controllo degli accessi (ACL) basati su utenti e gruppi. Amazon Kendra inserisce le politiche ACL tramite connettori. Se un indice non configura un ACL, verranno visualizzati solo i documenti che corrispondono al filtro degli attributi per utente e gruppo. Se viene fornito un filtro per gli attributi utente o di gruppo, i documenti senza un ACL non verranno visualizzati.

Se si utilizza il controllo degli accessi basato su token, verranno visualizzati i documenti senza una politica ACL e i documenti che corrispondono all'utente e ai gruppi.

Perché vedo documenti con una politica ACL?

Se un indice non configura una politica di controllo degli accessi, il filtro può fornire utenti e gruppi. Se non viene applicato alcun filtro per utenti e gruppi, verranno restituiti tutti i documenti correlati. Qualsiasi criterio ACL verrà ignorato.

Risoluzione dei problemi generali

Amazon Kendra utilizza CloudWatch metriche e registri per fornire informazioni sulla sincronizzazione delle fonti di dati. Puoi utilizzare le metriche e i log per determinare cosa è andato storto durante un'esecuzione di sincronizzazione e come risolverlo.

Per una risoluzione generale dei problemi, inizia con le tue metriche. CloudWatch

- Controlla la `DocumentsCrawled` metrica per vedere quanti documenti ha verificato la tua fonte di dati. Per un Amazon S3 bucket, se il numero è inferiore a quello previsto, verifica che la fonte di dati punti al bucket giusto.

- Controlla la `DocumentsSkippedNoChange` metrica per vedere quanti documenti sono stati ignorati perché non sono cambiati dall'ultima sincronizzazione. Se il numero non corrisponde a quello che ti aspetti, verifica che il tuo repository sia stato aggiornato correttamente.
- Controlla la `DocumentsSkippedInvalidMetadata` metrica per vedere quanti documenti contengono metadati non validi. Controlla i CloudWatch log per vedere gli errori specifici che si sono verificati.
- Controlla la `DocumentsSubmittedForIndexingFailed` metrica per vedere quanti documenti sono stati inviati dall'origine dati all'indice ma non sono stati indicizzati. Ad esempio, se utilizzi un attributo di metadati in un'origine Amazon S3 dati che non è stata definita come campo indice personalizzato, il documento non verrà indicizzato. Controlla i CloudWatch log per vedere gli errori specifici che si sono verificati.
- Controlla la `DocumentsSubmittedForDeletionFailed` metrica per vedere quanti documenti che l'origine dati ha tentato di rimuovere dall'indice non sono stati eliminati dall'indice. Controlla i CloudWatch log per vedere gli errori specifici che si sono verificati.

È possibile esaminare CloudWatch i registri di una particolare esecuzione di sincronizzazione per ottenere dettagli sugli errori che si sono verificati durante l'esecuzione. Per ulteriori informazioni sui CloudWatch registri con Amazon Kendra, vedere. CloudWatch Logs

Amazon KendraClassifica intelligente

Amazon KendraIntelligent Ranking utilizza funzionalità di ricerca Amazon Kendra semantica per riclassificare in modo intelligente i risultati di un servizio di ricerca.

Argomenti

Amazon Kendra Classificazione intelligente per l'autogestione OpenSearch

Puoi sfruttare le funzionalità Amazon Kendra di ricerca semantica di cui dispone per migliorare i risultati di ricerca grazie al servizio di OpenSearchricerca open source autogestito basato sulla licenza Apache 2.0. Il plugin Amazon Kendra Intelligent Ranking rielabora semanticamente i risultati utilizzando. OpenSearch Amazon Kendra Lo fa comprendendo il significato e il contesto di una query di ricerca utilizzando campi specifici, come il corpo o il titolo del documento, dai risultati di ricerca predefiniti. OpenSearch

Prendiamo, ad esempio, questa query: «indirizzo principale del keynote». Poiché 'indirizzo' ha diversi significati, Amazon Kendra può dedurre il significato alla base della query per restituire informazioni pertinenti in linea con il significato previsto. In questo contesto, si tratta di un discorso programmatico alla conferenza. Un servizio di ricerca più semplice potrebbe non tenere conto dell'intento e potrebbe restituire risultati per un indirizzo su Main Street, ad esempio.

Il plugin Intelligent Ranking per OpenSearch è disponibile per la versione OpenSearch (autogestita) 2.4.0 e successive. È possibile installare il plug-in utilizzando uno script Bash di avvio rapido per creare una nuova immagine Docker OpenSearch con il plug-in Intelligent Ranking incluso. VediConfigurazione del plug-in di ricerca intelligente: questo è un esempio di configurazione per renderti operativo rapidamente.

Come funziona il plugin di ricerca intelligente

Il processo complessivo del plugin Intelligent Ranking for OpenSearch (autogestito) è il seguente:

1. Un OpenSearch utente invia una query e OpenSearch fornisce una risposta alla query o un elenco di documenti pertinenti alla query.

2. Il plugin Intelligent Ranking prende la risposta alla query ed estrae le informazioni dai documenti.
3. Il plug-in Intelligent Ranking effettua una chiamata all'API Rescore di Amazon Kendra Intelligent Ranking.
4. L'`Rescore`API prende le informazioni estratte dai documenti e riordina semanticamente i risultati della ricerca.
5. L'`Rescore`API invia i risultati della ricerca riclassificati al plugin. Il plugin riorganizza i risultati della ricerca nella risposta di OpenSearch ricerca per riflettere la nuova classificazione semantica.

Il plugin Intelligent Ranking riclassifica i risultati utilizzando i campi «body» e «title». Questi campi del plug-in possono essere mappati sui campi OpenSearch dell'indice che meglio si adattano alla definizione del corpo e del titolo del documento. Ad esempio, se l'indice contiene capitoli di un libro con campi come «chapter_heading» e «chapter_contents», puoi mappare il primo a «title» e il secondo a «body» per ottenere i migliori risultati.

Configurazione del plug-in di ricerca intelligente

Di seguito viene descritto come configurare rapidamente OpenSearch (autogestito) con il plug-in Intelligent Ranking.

Configurazione OpenSearch (autogestita) con il plug-in Intelligent Ranking (configurazione rapida)

Se stai già utilizzando l'immagine Docker`opensearch:2.4.0`, puoi utilizzare questo Dockerfile per creare una nuova immagine di OpenSearch 2.4.0 con il plug-in Intelligent Ranking. Includi un contenitore per la nuova immagine nel file docker-compose.yml o nel file opensearch.yml. Includi anche l'ID del piano di esecuzione di rescore generato dalla creazione di un piano di esecuzione di rescore, insieme alle informazioni sulla regione e sull'endpoint. Vedi il passaggio 2 per creare un piano di esecuzione di rescore.

Se in precedenza hai scaricato una versione dell'immagine `opensearch` Docker precedente alla 2.4.0, devi utilizzare l'immagine Docker `opensearch:2.4.0` o una versione successiva e creare una nuova immagine con il plug-in Intelligent Ranking incluso.

1. Scarica e installa Docker Desktop per il tuo sistema operativo. Docker Desktop include Docker Compose e Docker Engine. Si consiglia di verificare se il computer soddisfa i requisiti di sistema indicati nei dettagli di installazione di Docker.

Puoi anche aumentare i requisiti di utilizzo della memoria all'interno delle impostazioni del tuo Docker Desktop. Sei responsabile dei requisiti di utilizzo di Docker al di fuori dei limiti di utilizzo disponibili gratuitamente per i servizi Docker. Vedi gli abbonamenti Docker.

Verifica che lo stato di Docker Desktop sia «in esecuzione».

2. Fornisci Amazon Kendra Intelligent Ranking e i tuoi requisiti di capacità. Una volta effettuato il provisioning di Amazon Kendra Intelligent Ranking, ti verrà addebitato ogni ora in base alle unità di capacità impostate. Consulta le informazioni sul piano gratuito e sui prezzi.

   Utilizzi l'CreateRescoreExecutionPlanAPI per fornire il`Rescore API`. Se non hai bisogno di più unità di capacità rispetto alla singola unità predefinita, non aggiungere altre unità e fornisci solo un nome per il tuo piano di esecuzione di rescore. Puoi anche aggiornare i requisiti di capacità utilizzando l'UpdateRescoreExecutionPlanAPI. Per ulteriori informazioni, consulta Classificazione semantica dei risultati di un servizio di ricerca.

   Facoltativamente, puoi andare al passaggio 3 per creare un piano di esecuzione di rescore predefinito quando esegui lo script Bash di avvio rapido.

   Nota per il passaggio 4 l'ID del piano di esecuzione di rescore incluso nella risposta.

   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. Scarica lo script Bash di avvio rapido da GitHub per la tua versione di OpenSearch selezionando il ramo della versione dal menu a discesa del ramo principale.

   Questo script utilizza immagini Docker OpenSearch e OpenSearch dashboard che utilizzano la versione selezionata nel GitHub repository per lo script. Scarica un file zip per il plug-in Intelligent Ranking e genera un file `Dockerfile` per creare una nuova immagine Docker OpenSearch che includa il plug-in. Crea anche un file docker-compose.yml che include contenitori per il plug-in Intelligent Ranking e OpenSearch le dashboard. OpenSearch Lo script aggiunge l'ID del piano di esecuzione di rescore, le informazioni sulla regione e l'endpoint (utilizza la regione) al file docker-compose.yml. Lo script viene quindi eseguito `docker-compose up` per avviare i contenitori per Intelligent Ranking incluso e Dashboards. OpenSearch OpenSearch Per fermare i contenitori senza rimuoverli, `docker-compose stop` esegui. Per rimuovere i contenitori, eseguidocker-compose down.

4. Apri il tuo terminale e nella directory dello script Bash, esegui il seguente comando.

   ```
   bash search_processing_kendra_quickstart.sh -p <execution-plan-id> -r <region>
   ```

   Quando esegui questo comando, fornisci l'ID del piano di esecuzione di rescore che hai annotato nel passaggio 2 durante il provisioning di Amazon Kendra Intelligent Ranking, insieme alle informazioni sulla tua regione. Facoltativamente, puoi invece fornire Amazon Kendra Intelligent Ranking utilizzando l'opzione. `--create-execution-plan` Questo crea un piano di esecuzione di rescore con un nome e una capacità predefiniti.

   Per non perdere l'indice quando il contenitore temporaneo predefinito viene rimosso, puoi fare in modo che l'indice persista tra le esecuzioni fornendo il nome del volume di dati utilizzando l'opzione. `--volume-name` Se in precedenza hai creato un indice, puoi specificare il volume nel tuo file docker-compose.yml o opensearch.yml. Per lasciare **`docker-compose down -v`**intatti i volumi, non eseguirli.

   Lo script Bash di avvio rapido configura AWS le credenziali nel OpenSearch keystore per la connessione a Intelligent Ranking. Amazon Kendra Per fornire le AWS credenziali allo script, utilizzate l'`--profile`opzione per specificare il profilo. AWS Se l'`--profile`opzione non è specificata, lo script Bash di avvio rapido tenta di leggere AWS le credenziali (chiave di accesso/segreta, token di sessione opzionale) dalle variabili di ambiente e quindi dal profilo predefinito. AWS Se l'`--profile`opzione non è specificata e non viene trovata alcuna credenziale, lo script non passerà le credenziali al keystore. OpenSearch Se non viene specificata alcuna credenziale nel OpenSearch keystore, il plug-in controlla comunque le credenziali nella catena di provider

di credenziali di default, incluse le credenziali del Amazon ECS contenitore o le credenziali del profilo di istanza fornite tramite il servizio di metadati. Amazon EC2

Assicurati di aver creato un IAM ruolo con le autorizzazioni necessarie per richiamare Intelligent Ranking. Amazon Kendra Di seguito è riportato un esempio di IAM politica per concedere l'autorizzazione all'uso dell'`Rescore`API per uno specifico piano di esecuzione di rescore:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "kendra-ranking:Rescore",
            "Resource": "arn:aws:kendra-ranking:${Region}:${Account}:rescore-
execution-plan/${RescoreExecutionPlanId}"
        }
    ]
}
```

Esempio di docker-compose.yml

Un esempio di file docker-compose.yml che utilizza OpenSearch 2.4.0 o versione successiva con il plug-in Intelligent Ranking e Dashboards 2.4.0 o versione successiva. 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
```

Esempio di Dockerfile e creazione di un'immagine

Un esempio di utilizzo della OpenSearch versione 2.4.0 o successiva con il plug-in Intelligent Ranking. `Dockerfile`

```
FROM opensearchproject/opensearch:<your-version>
RUN /usr/share/opensearch/bin/opensearch-plugin install --batch  https://github.com/
opensearch-project/search-processor/releases/download/<your-version>/search-
processor.zip
```

Creazione di un'immagine Docker per OpenSearch con il plug-in Intelligent Ranking.

```
docker build --tag=<Docker image tag name of OpenSearch with Intelligent Ranking
 plugin>
```

Interazione con il plugin di ricerca intelligente

Dopo aver configurato OpenSearch (gestito autonomamente) il plug-in Intelligent Ranking, puoi interagire con il plug-in utilizzando i comandi curl o le librerie OpenSearch client. Le credenziali predefinite per l'accesso OpenSearch con il plugin Intelligent Ranking sono il nome utente 'admin' e la password 'admin'.

Per applicare le impostazioni del plug-in Intelligent Ranking a un indice: OpenSearch

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)
```

È necessario includere il nome del campo di testo principale che si desidera utilizzare per modificare la classificazione, ad esempio il corpo del documento o il campo del contenuto del documento. Puoi anche includere altri campi di testo, come il titolo del documento o il riepilogo del documento.

Ora puoi inviare qualsiasi query e i risultati vengono classificati utilizzando il plug-in 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)
```

Per rimuovere le impostazioni del plug-in Intelligent Ranking per un OpenSearch indice:

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)
```

Per testare il plug-in Intelligent Ranking su una determinata query o su determinati campi del corpo e del titolo:

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)
```

Confronto OpenSearch dei risultati con Amazon Kendra i risultati

Puoi confrontare side-by-side OpenSearch (autogestiti) i risultati classificati con i risultati Amazon Kendra riclassificati. OpenSearch La versione 2.4.0 e successive di Dashboards offre side-by-side risultati che consentono di confrontare la classificazione dei documenti con quella OpenSearch dei documenti Amazon Kendra oppure il plug-in classifica i documenti per una query di ricerca.

Prima di poter confrontare i risultati OpenSearch classificati con quelli Amazon Kendra riclassificati, assicurati che le OpenSearch dashboard siano supportate da un server con il plug-in Intelligent Ranking. OpenSearch Puoi configurarlo usando Docker e uno script Bash di avvio rapido. Per informazioni, consulta Configurazione del plug-in di ricerca intelligente.

Di seguito viene descritto come confrontare OpenSearch e Amazon Kendra cercare i risultati nelle dashboard. OpenSearch Per ulteriori informazioni, consulta la OpenSearch documentazione.

Confronto dei risultati della ricerca nei OpenSearch dashboard

1. Apri http://localhost:5601 e accedi a OpenSearch Dashboards. Le credenziali predefinite sono il nome utente 'admin' e la password 'admin'.
2. Seleziona Search Relevance dai OpenSearch plugin nel menu di navigazione.
3. Inserisci il testo da cercare nella barra di ricerca.
4. Seleziona il tuo indice per Query 1 e inserisci una query in OpenSearch Query DSL. È possibile utilizzare la `%SearchText%` variabile per fare riferimento al testo di ricerca immesso nella barra di ricerca. Per un esempio di questa query, consulta OpenSearch Documentazione. I risultati restituiti per questa query sono i OpenSearch risultati senza utilizzare il plug-in Intelligent Ranking.

5. Seleziona lo stesso indice per Query 2 e inserisci la stessa query in OpenSearch Query DSL. Inoltre, includi l'estensione `kendra_intelligent_ranking` e specifica l'elemento obbligatorio in base al quale `body_field` classificare. Puoi anche specificare il campo del titolo, ma il campo body è obbligatorio. Per un esempio di questa query, vedi OpenSearch Documentazione. I risultati restituiti per questa query sono i risultati Amazon Kendra riclassificati utilizzando il plug-in Intelligent Ranking. Il plugin classifica fino a 25 risultati.
6. Seleziona Cerca per restituire e confrontare i risultati.

Classificazione semantica dei risultati di un servizio di ricerca

Amazon Kendra Intelligent Ranking utilizza le funzionalità Amazon Kendra di ricerca semantica di Intelligent Ranking per riordinare i risultati di un servizio di ricerca. Lo fa tenendo conto del contesto della query di ricerca, oltre a tutte le informazioni disponibili dai documenti del servizio di ricerca. Amazon Kendra Intelligent Ranking può migliorare la semplice corrispondenza delle parole chiave.

L'CreateRescoreExecutionPlanAPI crea una risorsa Amazon Kendra Intelligent Ranking utilizzata per il provisioning dell'API Rescore. L'`Rescore`API riordina i risultati di ricerca di un servizio di ricerca come OpenSearch (autogestito).

Quando chiami`CreateRescoreExecutionPlan`, imposti le unità di capacità richieste per riclassificare i risultati di un servizio di ricerca. Se non hai bisogno di più unità di capacità oltre a quella predefinita per la singola unità, non modificare l'impostazione predefinita. Fornisci solo un nome per il tuo piano di esecuzione di rescore. È possibile configurare fino a 1000 unità aggiuntive. Per informazioni su cosa è incluso in una singola unità di capacità, vedere Regolazione della capacità. Una volta effettuato il provisioning di Amazon Kendra Intelligent Ranking, ti verrà addebitato ogni ora in base alle unità di capacità impostate. Consulta le informazioni sul piano gratuito e sui prezzi.

Un ID del piano di esecuzione di rescore viene generato e restituito nella risposta alla chiamata`CreateRescoreExecutionPlan`. L'`Rescore`API utilizza l'ID del piano di esecuzione di rescore per riclassificare i risultati di un servizio di ricerca utilizzando la capacità impostata. Includi l'ID del piano di esecuzione di rescore nei file di configurazione del tuo servizio di ricerca. Ad esempio, se utilizzi OpenSearch (gestione automatica), includi l'ID del piano di esecuzione di rescore nel file docker-compose.yml o opensearch.yml. Vedi Risultati di classificazione intelligente (self-service). OpenSearch

Nella risposta alla chiamata viene generato anche un Amazon Resource Name (ARN). `CreateRescoreExecutionPlan` È possibile utilizzare questo ARN per creare una politica di

autorizzazioni in AWS Identity and Access Management (IAM) per limitare l'accesso degli utenti a un ARN specifico per uno specifico piano di esecuzione di rescore. Per un esempio di IAM policy per concedere l'autorizzazione all'uso dell'`RescoreAPI` per uno specifico piano di esecuzione di rescore, vedi Amazon Kendra Intelligent Ranking for self-managed. OpenSearch

Di seguito è riportato un esempio di creazione di un piano di esecuzione di rescore con unità di capacità impostate su 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.");
```

```
  }
}
```

Di seguito è riportato un esempio di aggiornamento di un piano di esecuzione di rescore per impostare le unità di capacità su 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.");
  }
}
```

Di seguito è riportato un esempio di utilizzo dell'`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());
```

```
    }
}
```

Cronologia dei documenti per Amazon Kendra

- Ultimo aggiornamento della documentazione: 27 febbraio 2024

La tabella seguente descrive le modifiche importanti in ogni versione di Amazon Kendra. Per ricevere notifiche sugli aggiornamenti della documentazione, puoi sottoscrivere il feed RSS.

Modifica	Descrizione	Data
Nuova caratteristica	Amazon Kendra ora supporta una versione aggiornata del connettore di origine GitHub dati. Per ulteriori informazioni, vedere GitHub.	27 febbraio 2024
Nuova caratteristica	Amazon Kendra ora supporta una versione aggiornata del connettore di origine Amazon FSx dati. Per ulteriori informazioni, vedete Amazon FSx (Windows) e Amazon FSx (NetAppONTAP).	8 febbraio 2024
Nuova caratteristica	Amazon Kendra ora supporta una versione aggiornata del connettore di origine dati Slack. Per ulteriori informazioni, consulta Slack.	11 gennaio 2024
Nuova caratteristica	Amazon Kendra ora supporta la compressione e l'espansione dei risultati di ricerca. Per ulteriori informazioni, consulta Comprimere/espandere i risultati di ricerca.	19 ottobre 2023

Nuova caratteristica	Amazon Kendra ora supporta un connettore di origine dati Aurora (MySQL). Per ulteriori informazioni, vedere Aurora (MySQL).	28 settembre 2023
Nuova caratteristica	Amazon Kendra ora supporta un connettore di origine dati Aurora (PostgreSQL). Per ulteriori informazioni, vedere Aurora (PostgreSQL).	28 settembre 2023
Nuova caratteristica	Amazon Kendra ora supporta un connettore di origine dati Amazon RDS (MySQL). Per ulteriori informazioni, vedere Amazon RDS (MySQL).	28 settembre 2023
Nuova caratteristica	Amazon Kendra ora supporta un connettore di origine dati Amazon RDS (Microsoft SQL Server). Per ulteriori informazioni, vedere Amazon RDS (Microsoft SQL Server).	28 settembre 2023
Nuova caratteristica	Amazon Kendra ora supporta un connettore di origine dati Amazon RDS (Oracle). Per ulteriori informazioni, vedere Amazon RDS (Oracle).	28 settembre 2023
Nuova caratteristica	Amazon Kendra ora supporta un connettore di origine dati Amazon RDS (PostgreSQL). Per ulteriori informazioni, vedere Amazon RDS (PostgreSQL).	28 settembre 2023

Nuova caratteristica	Amazon Kendra ora supporta un connettore di origine dati IBM DB2. Per ulteriori informazioni, consulta IBM DB2.	28 settembre 2023
Nuova caratteristica	Amazon Kendra ora supporta un connettore di origine dati Microsoft SQL Server. Per ulteriori informazioni, vedere Microsoft SQL Server.	28 settembre 2023
Nuova caratteristica	Amazon Kendra ora supporta un connettore di origine dati MySQL. Per ulteriori informazioni, consulta MySQL.	28 settembre 2023
Nuova caratteristica	Amazon Kendra ora supporta un connettore di origine dati del database Oracle. Per ulteriori informazioni, vedere Oracle Database.	28 settembre 2023
Nuova caratteristica	Amazon Kendra ora supporta un connettore di origine dati PostgreSQL. Per ulteriori informazioni, consulta PostgreSQL.	28 settembre 2023
Nuova caratteristica	Amazon Kendra ora fornisce un connettore di origine dati per Drupal. Per ulteriori informazioni, consulta Drupal.	6 settembre 2023

Nuova caratteristica	Recupera i passaggi semanticamente rilevanti utilizzando l'API Amazon Kendra Retrieve per i sistemi RAG (Retrieval Augmented Generation).	22 giugno 2023
Nuova caratteristica	Amazon Kendra ora supporta una versione aggiornata del connettore di origine dati Web Crawler. Amazon Kendra Per ulteriori informazioni, consulta Amazon Kendra Web Crawler v2.0.	21 giugno 2023
Espansione regionale	Amazon Kendra è ora disponibile in Europa (Londra) (eu-west-2).	5 giugno 2023
Nuova caratteristica	Amazon Kendra ora supporta una versione aggiornata del connettore di origine dati Alfresco. Per ulteriori informazioni, consulta Alfresco.	16 maggio 2023
Nuova caratteristica	Amazon Kendra ora fornisce un connettore di origine dati per Adobe Experience Manager. Per ulteriori informazioni, consulta Adobe Experience Manager.	11 maggio 2023

Nuova caratteristica	Amazon Kendra ora supporta la configurazione dei campi/attributi del documento quando si chiama. GetQuerySuggestions È ora possibile basare i suggerimenti di interrogazione sul contenuto dei campi del documento. Per ulteriori informazioni, consulta Suggerimenti per le query.	2 maggio 2023
Nuova caratteristica	Amazon Kendra ora fornisce un connettore di origine dati per Gmail. Per ulteriori informazioni, consulta Gmail.	13 aprile 2023
Nuova caratteristica	Amazon Kendra ora supporta una versione aggiornata del connettore di origine OneDrive dati Microsoft. Per ulteriori informazioni, vedere Microsoft OneDrive v2.0.	3 aprile 2023
Nuova caratteristica	Migliora la visibilità di nuovi documenti o promuovi determinati documenti quando gli utenti digitano determinate query utilizzando i risultati in evidenza.	30 marzo 2023
Nuova caratteristica	Amazon Kendra ora supporta un connettore di origine dati aggiornato per Microsoft SharePoint. Per ulteriori informazioni, vedere Microsoft SharePoint.	2 marzo 2023

Nuova caratteristica	Amazon Kendra ora supporta una versione aggiornata del connettore di origine dati Confluence. Per ulteriori informazioni, consulta Confluence.	1 marzo 2023
Espansione regionale	Amazon Kendra è ora disponibile in Asia Pacifico (Tokyo) (ap-northeast-1).	7 febbraio 2023
Nuova caratteristica	Amazon Kendra ora fornisce un connettore di origine dati per Microsoft Exchange. Per ulteriori informazioni, vedere Microsoft Exchange.	12 gennaio 2023
Nuova caratteristica	Amazon Kendra ora fornisce un connettore di origine dati per Microsoft Yammer. Per ulteriori informazioni, vedere Microsoft Yammer.	12 gennaio 2023
Nuova caratteristica	Amazon Kendra ora supporta l'indicizzazione dei tipi di documenti RTF, XML, XSLT, MS_EXCEL, CSV, JSON e MD. Per ulteriori informazioni, vedere Tipi di documenti.	11 gennaio 2023
Nuova caratteristica	Amazon Kendra ora supporta una versione aggiornata del connettore di origine Amazon S3 dati. Per ulteriori informazioni, consulta Amazon S3.	10 gennaio 2023

Nuova caratteristica	OpenSearchi risultati di ricerca (gestiti autonomamente) possono essere classificati semanticamente utilizzando Amazon Kendra Intelligent Ranking.	9 gennaio 2023
Nuova caratteristica	Amazon Kendra ora fornisce un connettore di origine dati per Microsoft Teams. Per ulteriori informazioni, consulta Microsoft Teams.	5 gennaio 2023
Nuova caratteristica	Amazon Kendra dispone di un connettore di origine dati aggiornato per Google Drive. Per ulteriori informazioni, consulta Google Drive.	5 gennaio 2023
Nuova caratteristica	Amazon Kendra dispone di un connettore di origine dati aggiornato per ServiceNo w. Per ulteriori informazioni, vedere ServiceNow.	21 dicembre 2022
Nuova caratteristica	Amazon Kendra dispone di un connettore di origine dati aggiornato per Salesforce. Per ulteriori informazioni, consulta Salesforce.	21 dicembre 2022
Espansione regionale	Amazon Kendra è ora disponibile in Asia Pacifico (Mumbai) (ap-south-1).	14 dicembre 2022

Nuova caratteristica	Amazon Kendrala funzione di ricerca tabulare può cercare ed estrarre risposte da tabelle incorporate nei documenti HTML.	27 novembre 2022
Nuova caratteristica	Amazon Kendra supporta la ricerca semantica per un insieme selezionato di lingue.	27 novembre 2022
Nuova caratteristica	Amazon Kendra ora fornisce un connettore di origine dati per Dropbox. Per ulteriori informazioni, consulta Dropbox.	27 settembre 2022
Nuova caratteristica	Amazon Kendra ora fornisce un connettore per sorgenti dati per Zendesk. Per ulteriori informazioni, consulta Zendesk.	17 agosto 2022
Nuova caratteristica	Il controllo degli accessi a livello di documento può ora essere riconfigurato dopo aver indicizzato i documenti. Per ulteriori informazioni, vedere Configurazione del controllo degli accessi.	14 luglio 2022
Nuova caratteristica	Amazon Kendra ora fornisce un connettore di origine dati per Alfresco. Per ulteriori informazioni, vedere Alfresco.	30 giugno 2022

Nuova caratteristica	Amazon Kendra ora fornisce un connettore di origine dati per GitHub. Per ulteriori informazioni, vedere GitHub.	2 giugno 2022
Nuova caratteristica	Amazon Kendra ora fornisce un connettore di origine dati per Jira. Per ulteriori informazioni, consulta Jira.	12 maggio 2022
Nuova caratteristica	Le sfaccettature annidate all'interno di una sfaccettatura possono essere visualizzate nei risultati della ricerca. Per ulteriori informazioni, consulta Facets.	5 maggio 2022
Nuova caratteristica	Amazon Kendra ora fornisce un connettore di origine dati per Quip. Per ulteriori informazioni, vedi Quip.	19 aprile 2022
Nuova caratteristica	Amazon Kendra ora fornisce un connettore di origine dati per Box. Per ulteriori informazioni, vedi Box.	6 aprile 2022
Nuova caratteristica	Amazon Kendra ora fornisce un connettore di origine dati per Slack. Per ulteriori informazioni, consulta Slack.	14 marzo 2022
Nuova caratteristica	Amazon Kendra ora fornisce un connettore di origine dati per Amazon FSx. Per ulteriori informazioni, consulta Amazon FSx.	8 febbraio 2022

AWS aggiornamenti delle politiche gestite: nuove politiche	Amazon Kendra sono state aggiunte nuove politiche AWS gestite. Per ulteriori informazioni, consulta Politiche AWS gestite per Amazon Kendra.	3 gennaio 2022
Nuova caratteristica	Amazon Kendra l'applicazione di ricerca può essere implementata in pochi clic senza la necessità di alcun codice front-end. Per ulteriori informazioni, consulta Distribuzione di un'applicazione di ricerca senza codice.	1° dicembre 2021
Nuova caratteristica	I metadati e i contenuti dei documenti possono essere arricchiti durante il processo di inserimento del documento. Per ulteriori informazioni, consulta la sezione Personalizzazione dei metadati del documento durante il processo di importazione.	1° dicembre 2021
Nuova caratteristica	Amazon Kendra offre analisi di ricerca per ottenere informazioni utili sulla vostra applicazione di ricerca. Per ulteriori informazioni, consulta Acquisire informazioni con l'analisi di ricerca.	1° dicembre 2021
Espansione regionale	Amazon Kendra è ora disponibile in AWS GovCloud (Stati Uniti occidentali) (us-gov-west-1).	13 ottobre 2021

Nuova caratteristica	Amazon Kendra ora può indicizzare i documenti in più lingue e filtrare i risultati della ricerca per lingua. Vedi Aggiungere documenti in lingue diverse dall'inglese e Ricerca in lingue.	7 ottobre 2021
Nuova caratteristica	Amazon Kendra ora si integra con la directory Identity Center per recuperare i livelli di accesso di gruppi e utenti per il filtraggio del contesto degli utenti. Vedi Configurazione dei gruppi di utenti per IAM Identity Center.	6 ottobre 2021
Nuovo tutorial	Amazon Kendra ora fornisce un tutorial che illustra come creare una soluzione di ricerca arricchita di metadati. Vedi Creazione di una soluzione di ricerca intelligente.	13 agosto 2021
Nuova caratteristica	Amazon Kendra ora fornisce un connettore di origine dati per Amazon WorkDocs. Per ulteriori informazioni, consulta Amazon WorkDocs.	20 luglio 2021
Nuova caratteristica	Amazon Kendra ora fornisce un web crawler per eseguire la scansione e l'indicizzazione delle pagine Web. Per ulteriori informazioni, consulta Web crawler.	17 giugno 2021

Espansione regionale	Amazon Kendra è ora disponibile in Canada (Central) (ca-central-1).	16 giugno 2021
Espansione regionale	Amazon Kendra è ora disponibile negli Stati Uniti orientali (Ohio) (us-east-2).	7 giugno 2021
Nuova caratteristica	Amazon Kendra ora supporta i suggerimenti di interrogazione, in cui agli utenti vengono suggerite le query più frequenti pertinenti alla loro ricerca. Per ulteriori informazioni, consulta Suggerimento di query di ricerca popolari.	27 maggio 2021
AWS aggiornamenti delle politiche gestite: nuove politiche	Amazon Kendra sono state aggiunte nuove politiche AWS gestite. Per ulteriori informazi oni, consulta Politiche AWS gestite per Amazon Kendra.	27 maggio 2021
Espansione regionale	Amazon Kendra è ora disponibile in Asia Pacifico (Singapore) (ap-southeast-1).	5 maggio 2021
Nuova caratteristica	Amazon Kendra ora supporta l'ottimizzazione della pertinenz a della ricerca nella query sovrascrivendo le configura zioni di ottimizzazione impostate a livello di indice. Per ulteriori informazioni, consulta Ottimizzazione della pertinenza della ricerca e Ottimizzazione delle risposte.	20 aprile 2021

Nuova caratteristica	Amazon Kendra ora supporta l'autenticazione OAuth 2.0 e l'utilizzo di ServiceNo w query per selezionare i documenti da indicizzare. Per ulteriori informazioni, vedere. ServiceNow	1 aprile 2021
Nuova caratteristica	Amazon Kendra ora supporta l'apprendimento increment ale per i documenti delle domande frequenti. Per ulteriori informazioni, consulta Invio di feedback per l'apprend imento incrementale.	17 febbraio 2021
Nuova caratteristica	Amazon Kendra ora supporta i sinonimi di indice. Per ulteriori informazioni, consulta Aggiungere sinonimi a un indice.	10 dicembre 2020
Nuova caratteristica	Amazon Kendra ora fornisce un connettore di database per Google Workspace Drive. Per ulteriori informazioni, vedere Utilizzo di un'origine dati di Google Workspace Drive.	8 dicembre 2020
Nuova caratteristica	Amazon Kendra ora fornisce una JavaScript libreria che semplifica l'invio di feedback sulle query. Amazon Kendra Per ulteriori informazioni, consulta Invio di feedback.	8 dicembre 2020

Nuova caratteristica	Amazon Kendra ora supporta il controllo degli accessi degli utenti basato su token. Per ulteriori informazioni, vedere Controllo dell'accesso ai documenti in un indice.	5 novembre 2020
Nuova caratteristica	Il connettore di origine dati Amazon Kendra Confluence ora funziona con Confluence cloud. Per ulteriori informazioni, consulta la sezione Utilizzo di un'origine dei dati Confluence.	5 novembre 2020
Espansione regionale	Amazon Kendra è ora disponibile in Asia Pacifico (Sydney) (ap-southeast-2).	2 novembre 2020
Nuova caratteristica	Amazon Kendra ora fornisce un connettore di origine dati per il server Confluence. Per ulteriori informazioni, consulta la sezione Utilizzo di un'origine dei dati Confluence.	26 ottobre 2020
Nuova caratteristica	Amazon Kendra ora fornisce una fonte di dati che puoi usare per generare statistiche per i tuoi connettori personalizzati. Per ulteriori informazioni, consulta Utilizzo di un'origine dati personalizzata.	21 ottobre 2020

Nuova caratteristica	Amazon Kendra ora supporta gli attributi personalizzati per le domande frequenti . Per ulteriori informazioni, consulta Aggiungere domande e risposte.	17 settembre 2020
Nuova caratteristica	Amazon Kendra ora restituis ce punteggi di confidenza per i risultati delle query. Per ulteriori informazioni, vedere QueryResultItem.	15 settembre 2020
Nuova caratteristica	AWS CloudFormation ora supporta Amazon Kendra. Per ulteriori informazioni, vedere riferimento al tipo di Amazon Kendra risorsa - AWS CloudFormation.	10 settembre 2020
Nuova caratteristica	Amazon Kendra aggiunge il supporto per AWS PrivateLi nk. Per ulteriori informazioni consulta Amazon Kendra ed endpoint VPC di interfaccia (AWS PrivateLink).	7 luglio 2020
Nuova guida	Questa è la prima versione della Guida per sviluppatori di Amazon Kendra .	11 maggio 2020

Riferimento API

La documentazione di riferimento sulle API è ora una guida separata.

Glossario per AWS

Per la terminologia AWS più recente, consultare il glossario AWS nella documentazione di riferimento per Glossario AWS.

Le traduzioni sono generate tramite traduzione automatica. In caso di conflitto tra il contenuto di una traduzione e la versione originale in Inglese, quest'ultima prevarrà.