aws

Entwicklerhandbuch

Amazon Kendra

Amazon Kendra: Entwicklerhandbuch

Table of Contents

Was ist Amazon Kendra?

Amazon Kendraist ein intelligenter Suchdienst, der natürliche Sprachverarbeitung und fortschrittliche Algorithmen für maschinelles Lernen verwendet, um spezifische Antworten auf Suchfragen aus Ihren Daten zurückzugeben.

Im Gegensatz zur herkömmlichen schlüsselwortbasierten Suche werden hier die semantischen und kontextuellen Fähigkeiten Amazon Kendra genutzt, um zu entscheiden, ob ein Dokument für eine Suchabfrage relevant ist. Es gibt spezifische Antworten auf Fragen und bietet Benutzern eine Erfahrung, die der Interaktion mit einem menschlichen Experten nahe kommt.

> **Note**
>
> Sie können auch die Amazon Kendra semantischen Suchfunktionen verwenden, um die Ergebnisse eines anderen Suchdienstes neu zu bewerten. Weitere Informationen finden Sie unter Amazon KendraIntelligentes Ranking.

Mit können Sie ein einheitliches Sucherlebnis schaffenAmazon Kendra, indem Sie mehrere Datenrepositorys mit einem Index verbinden und Dokumente aufnehmen und durchsuchen.
Sie können Ihre Dokumentmetadaten verwenden, um Ihren Benutzern ein funktionsreiches und angepasstes Sucherlebnis zu bieten, das ihnen hilft, effizient die richtigen Antworten auf ihre Fragen zu finden.

Was ist Amazon Kendra?

Abfragen von Amazon Kendra

Sie können Amazon Kendra die folgenden Arten von Abfragen stellen:

Faktoid-Fragen — Einfache Fragen zu wem, was, wann oder wo, z. B. Wo ist das nächstgelegene Servicecenter zu Seattle? Faktoid-Fragen haben faktenbasierte Antworten, die als einzelnes Wort oder Ausdruck zurückgegeben werden können. Die Antwort wird aus einer FAQ oder aus Ihren indexierten Dokumenten abgerufen.

Beschreibende Fragen — Fragen, bei denen die Antwort ein Satz, eine Passage oder ein ganzes Dokument sein kann. Zum Beispiel: Wie verbinde ich mein Echo Plus mit meinem Netzwerk? Oder, Wie erhalte ich Steuervorteile für Familien mit niedrigerem Einkommen?

Fragen nach Schlüsselwörtern und natürlicher Sprache — Fragen, die komplexe Konversationsinhalte beinhalten, bei denen die Bedeutung möglicherweise nicht klar ist. Zum Beispiel Keynote Address. Wenn Sie Amazon Kendra auf ein Wort wie „Adresse“ stoßen, das mehrere kontextuelle Bedeutungen hat, leitet es korrekt auf die Bedeutung der Suchabfrage ab und gibt relevante Informationen zurück.

Vorteile von Amazon Kendra

Amazon Kendraist hochgradig skalierbar, kann Leistungsanforderungen erfüllen, ist eng in andere AWS Dienste wie Amazon S3und integriert und Amazon Lexbietet Sicherheit auf Unternehmensniveau. Die Nutzung von Amazon Kendra bietet unter anderem folgende Vorteile:

Einfachheit — Amazon Kendra bietet eine Konsole und eine API für die Verwaltung der Dokumente, die Sie durchsuchen möchten. Sie können eine einfache Such-API verwenden, um Amazon Kendra sie in Ihre Kundenanwendungen wie Websites oder mobile Anwendungen zu integrieren.

Konnektivität — Amazon Kendra kann eine Verbindung zu Datenrepositorien oder Datenquellen von Drittanbietern wie Microsoft herstellen. SharePoint Mithilfe Ihrer Datenquelle können Sie Ihre Dokumente einfach indexieren und durchsuchen.

Genauigkeit — Im Gegensatz zu herkömmlichen Suchdiensten, die Stichwortsuchen verwenden, Amazon Kendra versucht dieser, den Kontext der Frage zu verstehen und gibt das relevanteste Wort, den Textausschnitt oder das Dokument für Ihre Anfrage zurück. Amazon Kendranutzt maschinelles Lernen, um die Suchergebnisse im Laufe der Zeit zu verbessern.

Sicherheit — Amazon Kendra bietet ein hochsicheres Sucherlebnis für Unternehmen. Ihre Suchergebnisse spiegeln das Sicherheitsmodell Ihrer Organisation wider und können nach dem Benutzer- oder Gruppenzugriff auf Dokumente gefiltert werden. Kunden sind für die Authentifizierung und Autorisierung des Benutzerzugriffs verantwortlich.

Amazon KendraAusgaben

Amazon Kendrahat zwei Versionen: Developer Edition und Enterprise Edition. In der folgenden Tabelle werden ihre Funktionen und die Unterschiede zwischen den beiden beschrieben.

Amazon KendraAusgabe für Entwickler	Amazon KendraEnterprise-Ausgabe
Amazon KendraDie Developer Edition bietet alle Funktionen von Amazon Kendra zu einem geringeren Preis. Idealer Anwendungsfall • Erfahren Sie, wie Ihre Amazon Kendra Dokumente indexiert werden • Funktionen ausprobieren • Entwickeln von Anwendungen, die Amazon Kendra Funktionen • Ein kostenloses Kontingent mit 750 Stunden Nutzung • Bis zu 5 Indizes mit jeweils bis zu 5 Datenquellen • 10.000 Dokumente oder 3 GB extrahierter Text • Ungefähr 4.000 Abfragen pro Tag oder 0,05 Abfragen pro Sekunde • Läuft in einer Availability Zone (AZ) — siehe Availability Zones (Rechenzentren in AWS Regionen) Einschränkungen • Nicht für Produktionsanwendungen • Keine Garantie für Latenz oder Verfügbarkeit	Amazon KendraDie Enterprise Edition bietet alle Funktionen von Amazon Kendra und ist für Produktionskontexte konzipiert. Idealer Anwendungsfall • Indexierung Ihrer gesamten Unternehm ensdokumentenbibliothek • Bereitstellung Ihrer Anwendung in einer Produktionsumgebung Funktionen • Bis zu 5 Indizes mit jeweils bis zu 50 Datenquellen • 100.000 Dokumente oder 30 GB extrahierter Text • Ungefähr 8.000 Abfragen pro Tag oder 0,1 Abfragen pro Sekunde • Läuft in 3 Availability Zones (AZ) — siehe Availability Zones (Rechenzentren in AWS Regionen) Note Sie können dieses Kontingent mithilfe der Service Quotas-Konsole erhöhen. Einschränkungen • Keine

> **Note**
>
> Eine Liste der Regionen, Endpunkte und Servicekontingente, die von unterstützt werdenAmazon Kendra, finden Sie unter Amazon KendraEndpoints und Kontingente.

Preise für Amazon Kendra

Sie können kostenlos mit der Amazon Kendra Developer Edition beginnen, die eine Nutzung von bis zu 750 Stunden in den ersten 30 Tagen bietet.

Nach Ablauf Ihrer Testphase werden Ihnen alle bereitgestellten Amazon Kendra Indizes in Rechnung gestellt, auch wenn sie leer sind und keine Abfragen ausgeführt werden. Nach Ablauf der Testphase fallen zusätzliche Gebühren für das Scannen und Synchronisieren von Dokumenten mithilfe der Amazon Kendra Datenquellen an.

Eine vollständige Liste der Gebühren und Preise finden Sie unter Amazon KendraPreise.

Verwenden Sie Amazon Kendra zum ersten Mal?

Wenn Sie Amazon Kendra zum ersten Mal verwenden, empfehlen wir Ihnen, nacheinander die folgenden Abschnitte zu lesen:

1	2	3	4	5	6
Funktionsweise von Amazon Kendra	Erste Schritte	Erstellen eines Index	Hinzufügen von Dokumenten direkt zu einem Index mit Batch-Upload	Erstellen eines Datenquellen-Connectors	Einen Index durchsuchen
Stellt Amazon Kendra Komponenten vor und beschreibt,	Erläutert, wie Sie Ihr Konto einrichten und die Amazon	Erläutert, wie Amazon Kendra Sie einen Suchindex	Erläutert, wie Dokumente direkt zu einem Amazon	Erläutert, wie Sie Dokumente aus Ihrem Datenspei	Erläutert, wie die Amazon Kendra Such-API verwendet

1	2	3	4	5	6
Funktionsweise von Amazon Kendra	Erste Schritte	Erstellen eines Index	Hinzufügen von Dokumenten direkt zu einem Index mit Batch-Upload	Erstellen eines Datenquellen-Connectors	Einen Index durchsuchen
wie Sie sie verwenden, um eine Suchlösung zu erstellen.	Kendra Such-API testen.	erstellen und Datenquellen hinzufügen, um Ihre Dokumente zu synchronisieren.	Kendra Index hinzugefügt werden.	cher zu einem Amazon Kendra Index hinzufügen.	wird, um einen Index zu durchsuchen.

Funktionsweise von Amazon Kendra

Amazon Kendra stellt Suchfunktionen für Ihre Anwendung bereit. Es indexiert Ihre Dokumente direkt oder aus Ihrem Dokumentenspeicher eines Drittanbieters und stellt Ihren Benutzern auf intelligente Weise relevante Informationen zur Verfügung. Sie können Amazon Kendra damit einen aktualisierbaren Index von Dokumenten verschiedener Typen erstellen. Eine Liste der von unterstützten Dokumenttypen Amazon Kendra finden Sie unter Dokumenttypen.

Amazon Kendra lässt sich in andere Dienste integrieren. Sie können beispielsweise Amazon Lex Chat-Bots mit Amazon Kendra Suchfunktionen unterstützen, um nützliche Antworten auf die Fragen der Benutzer zu geben. Sie können einen Amazon Simple Storage Service Bucket als Datenquelle verwenden, um eine Verbindung Amazon Kendra zu Ihren Dokumenten herzustellen und diese zu indizieren. Und Sie können mithilfe von... Zugriffsrichtlinien oder Berechtigungen für Ressourcen einrichten AWS Identity and Access Management.

Amazon Kendra besteht aus den folgenden Komponenten:

- Ein Index, der Ihre Dokumente enthält und sie durchsuchbar macht.
- Eine Datenquelle, die Ihre Dokumente speichert und zu der Amazon Kendra eine Verbindung hergestellt wird. Sie können eine Datenquelle automatisch mit einem Amazon Kendra Index synchronisieren, sodass Ihr Index stets mit Ihrem Quell-Repository aktualisiert wird.
- Eine API zum Hinzufügen von Dokumenten, die Dokumente direkt zu einem Index hinzufügt.

Sie können es Amazon Kendra über die Konsole oder die API verwenden. Sie können Indizes erstellen, aktualisieren und löschen. Durch das Löschen eines Indexes werden alle zugehörigen Datenquellenkonnektoren und alle Ihre Dokumentinformationen dauerhaft aus gelöscht. Amazon Kendra

Themen

Index

Ein Index enthält den Inhalt Ihrer Dokumente und ist so strukturiert, dass die Dokumente durchsuchbar sind. Wie Sie Dokumente zum Index hinzufügen, hängt davon ab, wie Sie Ihre Dokumente speichern.

- Wenn Sie Ihre Dokumente in einem Repository speichern, z. B. in einem Amazon S3 Bucket oder einer SharePoint Microsoft-Site, verwenden Sie einen Datenquellen-Connector, um Ihre Dokumente aus Ihrem Repository zu indizieren.
- Wenn Sie Ihre Dokumente nicht in einem Repository speichern, verwenden Sie die BatchPutDocumentAPI, um Ihre Dokumente direkt zu indizieren.
- Häufig gestellte Fragen und Antworten, die in einem Amazon Kendra (Amazon S3) -Bucket gespeichert werden müssen, laden Sie sie aus dem Bucket hoch

Sie können Indizes mit der Amazon Kendra Konsole AWS CLI, dem oder einem AWS SDK erstellen. Informationen zu den Dokumenttypen, die indexiert werden können, finden Sie unter Dokumenttypen.

Verwenden von Amazon Kendra reservierten oder allgemeinen Dokumentfeldern

Mit der UpdateIndex API können Sie reservierte oder allgemeine Felder erstellen, indem Sie den Namen des Amazon Kendra reservierten Indexfeldes verwenden `DocumentMetadataConfigurationUpdates` und angeben, um ihn Ihrem entsprechenden Dokumentattribut/Feldnamen zuzuordnen. Sie können auch benutzerdefinierte Felder erstellen. Wenn Sie einen Datenquellenconnector verwenden, enthalten die meisten Feldzuordnungen, die die Felder Ihres Datenquellendokuments Amazon Kendra Indexfeldern zuordnen. Wenn Sie die Konsole verwenden, aktualisieren Sie Felder, indem Sie Ihre Datenquelle auswählen, die Aktion Bearbeiten auswählen und dann mit dem Abschnitt Feldzuordnungen zur Konfiguration der Datenquelle fortfahren.

Sie können das `Search` Objekt so konfigurieren, dass ein Feld entweder als anzeigbar, facettierbar, durchsuchbar oder sortierbar festgelegt wird. Sie können das `Relevance` Objekt so konfigurieren, dass die Rangfolge, die Boost-Dauer oder der Zeitraum eines Felds so festgelegt werden, dass sie auf Boosting, Aktualität, Wichtigkeitswert und Wichtigkeitswerte angewendet werden, die bestimmten Feldwerten zugeordnet sind. Wenn Sie die Konsole verwenden, können Sie die Sucheinstellungen für ein Feld festlegen, indem Sie im Navigationsmenü die Option Facette auswählen. Um die

Relevanzoptimierung einzustellen, wählen Sie im Navigationsmenü die Option zum Durchsuchen Ihres Index aus, geben Sie eine Abfrage ein und verwenden Sie die Optionen im Seitenbereich, um die Suchrelevanz zu optimieren. Sie können den Feldtyp nicht mehr ändern, nachdem Sie das Feld erstellt haben.

Amazon Kendra hat die folgenden reservierten oder allgemeinen Dokumentfelder, die Sie verwenden können:

- `_authors`—Eine Liste mit einem oder mehreren Autoren, die für den Inhalt des Dokuments verantwortlich sind.
- `_category`— Eine Kategorie, die ein Dokument einer bestimmten Gruppe zuordnet.
- `_created_at`— Datum und Uhrzeit im ISO 8601-Format, an dem das Dokument erstellt wurde. Beispiel: 2012-03-25T12:30:10+01:00 ist das ISO-8601-Datums-/Uhrzeitformat für den 25. März 2012 um 12:30 Uhr (plus 10 Sekunden) in mitteleuropäischer Zeit (CET).
- `_data_source_id`— Der Bezeichner der Datenquelle, die das Dokument enthält.
- `_document_body`— Der Inhalt des Dokuments.
- `_document_id`— Eine eindeutige Kennung für das Dokument.
- `_document_title`— Der Titel des Dokuments.
- `_excerpt_page_number`— Die Seitenzahl in einer PDF-Datei, auf der der Dokumentauszug erscheint. Wenn Ihr Index vor dem 8. September 2020 erstellt wurde, müssen Sie Ihre Dokumente erneut indizieren, bevor Sie dieses Attribut verwenden können.
- `_faq_id`— Wenn es sich um ein Dokument vom Typ Frage-Antwort (FAQ) handelt, eine eindeutige Kennung für die häufig gestellten Fragen.
- `_file_type`— Der Dateityp des Dokuments, z. B. PDF oder Dokument.
- `_last_updated_at`— Datum und Uhrzeit der letzten Aktualisierung des Dokuments im Format ISO 8601. Beispiel: 2012-03-25T12:30:10+01:00 ist das ISO-8601-Datums-/Uhrzeitformat für den 25. März 2012 um 12:30 Uhr (plus 10 Sekunden) in mitteleuropäischer Zeit (CET).
- `_source_uri`— Die URI, unter der das Dokument verfügbar ist. Zum Beispiel der URI des Dokuments auf einer Unternehmenswebsite.
- `_version`— Ein Bezeichner für die spezifische Version eines Dokuments.
- `_view_count`— Wie oft das Dokument angesehen wurde.
- `_language_code`(String) — Der Code für eine Sprache, die für das Dokument gilt. Dies ist standardmäßig Englisch, wenn Sie keine Sprache angeben. Weitere Informationen zu den

unterstützten Sprachen, einschließlich ihrer Codes, finden Sie unter Dokumente in anderen Sprachen als Englisch hinzufügen.

Bei benutzerdefinierten Feldern erstellen Sie diese Felder `DocumentMetadataConfigurationUpdates` mithilfe der `UpdateIndex` API, genau wie bei der Erstellung eines reservierten oder gemeinsamen Felds. Sie müssen den entsprechenden Datentyp für Ihr benutzerdefiniertes Feld festlegen. Wenn Sie die Konsole verwenden, aktualisieren Sie Felder, indem Sie Ihre Datenquelle auswählen, die Aktion Bearbeiten auswählen und dann mit dem Abschnitt Feldzuordnungen zur Konfiguration der Datenquelle fortfahren. Einige Datenquellen unterstützen das Hinzufügen neuer Felder oder benutzerdefinierter Felder nicht. Sie können den Feldtyp nicht mehr ändern, nachdem Sie das Feld erstellt haben.

Die folgenden Typen können Sie für benutzerdefinierte Felder festlegen:

- Datum
- Zahl
- String
- Zeichenfolgenliste

Wenn Sie dem Index mithilfe der BatchPutDocumentAPI Dokumente hinzugefügt haben, `Attributes` listet die Felder/Attribute Ihrer Dokumente auf und Sie erstellen Felder mithilfe des `DocumentAttribute` Objekts.

Für Dokumente, die aus einer Amazon S3 Datenquelle indexiert wurden, erstellen Sie Felder mithilfe einer JSON-Metadatendatei, die die Feldinformationen enthält.

Wenn Sie eine unterstützte Datenbank als Datenquelle verwenden, können Sie Ihre Felder mithilfe der Option Feldzuordnungen konfigurieren.

Indizes durchsuchen

Nachdem Sie einen Index erstellt haben, können Sie mit der Suche in Ihren Dokumenten beginnen. Weitere Informationen finden Sie unter Indizes durchsuchen.

-Documents

In diesem Abschnitt wird erklärt, wie die vielen unterstützten Dokumentformate und die verschiedenen Felder/Attribute von Dokumenten Amazon Kendra indexiert werden.

Themen

Dokumenttypen oder -formate

Amazon Kendra unterstützt gängige Dokumenttypen oder Formate wie PDF, HTML PowerPoint, Word und mehr. Ein Index kann mehrere Dokumentformate enthalten.

Amazon Kendra extrahiert den Inhalt der Dokumente, um die Dokumente durchsuchbar zu machen. Die Dokumente werden so analysiert, dass die Suche nach dem extrahierten Text und allen tabellarischen Inhalten (HTML-Tabellen) in den Dokumenten optimiert wird. Das bedeutet, die Dokumente in Felder oder Attribute zu strukturieren, die für die Suche verwendet werden. Die Metadaten des Dokuments, z. B. das Datum der letzten Änderung, können nützliche Felder für die Suche sein.

Dokumente können in Zeilen und Spalten organisiert werden. Beispielsweise ist jedes Dokument eine Zeile und jedes Dokumentfeld/jedes Dokumentattribut, z. B. der Titel und der Hauptteil, ist eine Spalte. Wenn Sie beispielsweise eine Datenbank als Datenquelle verwenden, sollten die Daten strukturiert oder in Zeilen und Spalten organisiert sein.

Sie können Ihrem Index auf folgende Weise Dokumente hinzufügen:

- BatchPutDocument-API
- Datenquellen-Konnektor

Wenn Sie eine FAQ-Datei hinzufügen möchten, verwenden Sie die CreateFaqAPI, um die in einem Amazon S3 Bucket gespeicherte Datei hinzuzufügen. Sie können zwischen einem grundlegenden CSV-Format, einem CSV-Format, das benutzerdefinierte Felder/Attribute in einer Kopfzeile enthält, und einem JSON-Format, das benutzerdefinierte Felder enthält, wählen. Das Standardformat ist das grundlegende CSV-Format.

Im Folgenden finden Sie Informationen zu den einzelnen unterstützten Dokumentformaten und dazu, wie die einzelnen Formate bei der Indizierung von Dokumenten Amazon Kendra behandelt werden.

Format des Dokuments	Behandelt als	Wie wird das Dokument behandelt	Ursprüngliche Struktur
Tragbares Dokumentenformat (PDF)	HTML	In HTML konvertiert, dann wird der Inhalt extrahiert.	Unstrukturiert
HyperText Auszeichnungssprache (HTML)	HTML	HTML-Tags werden herausgefiltert, um Inhalte zu extrahieren. Der Inhalt muss zwischen den `HTML` Haupt-Start- und Schlusstags (`<HTML>content</HTML>`) liegen.	Semistrukturiert
Erweiterbare Markup Language (XML)	XML	XML-Tags werden herausgefiltert, um Inhalte zu extrahieren.	Semistrukturiert
Erweiterbare Stylesheet-Sprachtransformation (XSLT)	XSLT	Tags werden herausgefiltert, um Inhalte zu extrahieren.	Halbstrukturiert
MarkDown (MD)	Klartext	Der Inhalt wird mit der enthaltenen MarkDown Syntax extrahiert.	Halbstrukturiert
Comma Separated Values (CSV)	CSV	Aus jeder Zelle extrahierter Inhalt, wobei eine einzelne Datei als einzelnes Dokumentergebnis behandelt wird.	Strukturiert für FAQ-Dateien, ansonsten halbstrukturiert

Format des Dokuments	Behandelt als	Wie wird das Dokument behandelt	Ursprüngliche Struktur
Microsoft Excel (XLS und XLSX)	XLS und XLSX	Aus jeder Zelle extrahierter Inhalt, wobei eine einzelne Datei als einzelnes Dokumentergebnis behandelt wird.	Teilweise strukturiert
JavaScript Objektnotation (JSON)	Klarer Text	Der Inhalt wird inklusive JSON-Syntax extrahiert.	Halbstrukturiert
Rich-Text-Format (RTF)	RTF	Die RTF-Syntax wird herausgefiltert, um Inhalte zu extrahieren.	Semistrukturiert
Microsoft PowerPoint (PPT)	PPT	Nur Textinhalte werden für die Suche aus PowerPoint Folien extrahiert. Bilder und andere Inhalte werden nicht extrahiert.	Unstrukturiert
Microsoft Word (DOCX)	DOCX	Nur Textinhalte werden für die Suche aus Word-Seiten extrahiert. Bilder und andere Inhalte werden nicht extrahiert.	Unstrukturiert
Klartext (TXT)	TXT	Der gesamte Text im Textdokument wird extrahiert.	Unstrukturiert

Attribute oder Felder des Dokuments

Einem Dokument sind Attribute oder Felder zugeordnet. Felder eines Dokuments sind die Eigenschaften eines Dokuments oder das, was in der Struktur eines Dokuments enthalten ist. Beispielsweise kann jedes Ihrer Dokumente Titel, Haupttext und Autor enthalten. Sie können auch benutzerdefinierte Felder für Ihre speziellen Dokumente hinzufügen. Wenn Ihr Index beispielsweise nach Steuerdokumenten sucht, können Sie ein benutzerdefiniertes Feld für den Typ des Steuerdokuments angeben, z. B. W-2, 1099 usw.

Bevor Sie ein Dokumentfeld in einer Abfrage verwenden können, muss es einem Indexfeld zugeordnet werden. Beispielsweise kann das Titelfeld dem Feld zugeordnet werden. `_document_title` Weitere Informationen finden Sie unter Felder zuordnen. Um ein neues Feld hinzuzufügen, müssen Sie ein Indexfeld erstellen, dem das Feld zugeordnet werden soll. Sie erstellen Indexfelder mithilfe der Konsole oder mithilfe der UpdateIndexAPI.

Sie können Dokumentfelder verwenden, um Antworten zu filtern und facettierte Suchergebnisse zu erstellen. Sie können beispielsweise eine Antwort so filtern, dass nur eine bestimmte Version eines Dokuments zurückgegeben wird, oder Sie können Suchanfragen so filtern, dass nur Steuerdokumente vom Typ 1099 zurückgegeben werden, die dem Suchbegriff entsprechen. Weitere Informationen finden Sie unter Filtern und Facettensuche.

Sie können auch Dokumentfelder verwenden, um die Abfrageantwort manuell zu optimieren. Sie können sich beispielsweise dafür entscheiden, die Bedeutung des Titelfeldes zu erhöhen, um die Gewichtung zu erhöhen, die dem Feld Amazon Kendra zugewiesen wird, wenn es darum geht, zu bestimmen, welche Dokumente in der Antwort zurückgegeben werden sollen. Weitere Informationen finden Sie unter Suchrelevanz optimieren.

Wenn Sie ein Dokument direkt zu einem Index hinzufügen, geben Sie die Felder im Eingabeparameter Dokument für die BatchPutDocumentAPI an. Sie geben die benutzerdefinierten Feldwerte in einem DocumentAttributeObjekt-Array an. Wenn Sie eine Datenquelle verwenden, hängt die Methode, mit der Sie die Dokumentfelder hinzufügen, von der Datenquelle ab. Weitere Informationen finden Sie unter Zuweisen von Datenquellenfeldern.

Verwenden von Amazon Kendra reservierten oder gemeinsamen Dokumentfeldern

Mit der UpdateIndex API können Sie reservierte oder allgemeine Felder erstellen, indem Sie den Namen des Amazon Kendra reservierten Indexfeldes verwenden `DocumentMetadataConfigurationUpdates` und angeben, um ihn Ihrem entsprechenden

Dokumentattribut/Feldnamen zuzuordnen. Sie können auch benutzerdefinierte Felder erstellen. Wenn Sie einen Datenquellenconnector verwenden, enthalten die meisten Feldzuordnungen, die die Felder Ihres Datenquellendokuments Amazon Kendra Indexfeldern zuordnen. Wenn Sie die Konsole verwenden, aktualisieren Sie Felder, indem Sie Ihre Datenquelle auswählen, die Aktion Bearbeiten auswählen und dann mit dem Abschnitt Feldzuordnungen zur Konfiguration der Datenquelle fortfahren.

Sie können das `Search` Objekt so konfigurieren, dass ein Feld entweder als anzeigbar, facettierbar, durchsuchbar oder sortierbar festgelegt wird. Sie können das `Relevance` Objekt so konfigurieren, dass die Rangfolge, die Boost-Dauer oder der Zeitraum eines Felds so festgelegt werden, dass sie auf Boosting, Aktualität, Wichtigkeitswert und Wichtigkeitswerte angewendet werden, die bestimmten Feldwerten zugeordnet sind. Wenn Sie die Konsole verwenden, können Sie die Sucheinstellungen für ein Feld festlegen, indem Sie im Navigationsmenü die Option Facette auswählen. Um die Relevanzoptimierung einzustellen, wählen Sie im Navigationsmenü die Option zum Durchsuchen Ihres Index aus, geben Sie eine Abfrage ein und verwenden Sie die Optionen im Seitenbereich, um die Suchrelevanz zu optimieren. Sie können den Feldtyp nicht mehr ändern, nachdem Sie das Feld erstellt haben.

Amazon Kendra hat die folgenden reservierten oder allgemeinen Dokumentfelder, die Sie verwenden können:

- `_authors`—Eine Liste mit einem oder mehreren Autoren, die für den Inhalt des Dokuments verantwortlich sind.
- `_category`— Eine Kategorie, die ein Dokument einer bestimmten Gruppe zuordnet.
- `_created_at`— Datum und Uhrzeit im ISO 8601-Format, an dem das Dokument erstellt wurde. Beispiel: 2012-03-25T12:30:10+01:00 ist das ISO-8601-Datums-/Uhrzeitformat für den 25. März 2012 um 12:30 Uhr (plus 10 Sekunden) in mitteleuropäischer Zeit (CET).
- `_data_source_id`— Der Bezeichner der Datenquelle, die das Dokument enthält.
- `_document_body`— Der Inhalt des Dokuments.
- `_document_id`— Eine eindeutige Kennung für das Dokument.
- `_document_title`— Der Titel des Dokuments.
- `_excerpt_page_number`— Die Seitenzahl in einer PDF-Datei, auf der der Dokumentauszug erscheint. Wenn Ihr Index vor dem 8. September 2020 erstellt wurde, müssen Sie Ihre Dokumente erneut indizieren, bevor Sie dieses Attribut verwenden können.
- `_faq_id`— Wenn es sich um ein Dokument vom Typ Frage-Antwort (FAQ) handelt, eine eindeutige Kennung für die häufig gestellten Fragen.

- `_file_type`— Der Dateityp des Dokuments, z. B. PDF oder Dokument.
- `_last_updated_at`— Datum und Uhrzeit der letzten Aktualisierung des Dokuments im Format ISO 8601. Beispiel: 2012-03-25T12:30:10+01:00 ist das ISO-8601-Datums-/Uhrzeitformat für den 25. März 2012 um 12:30 Uhr (plus 10 Sekunden) in mitteleuropäischer Zeit (CET).
- `_source_uri`— Die URI, unter der das Dokument verfügbar ist. Zum Beispiel der URI des Dokuments auf einer Unternehmenswebsite.
- `_version`— Ein Bezeichner für die spezifische Version eines Dokuments.
- `_view_count`— Wie oft das Dokument angesehen wurde.
- `_language_code`(String) — Der Code für eine Sprache, die für das Dokument gilt. Dies ist standardmäßig Englisch, wenn Sie keine Sprache angeben. Weitere Informationen zu den unterstützten Sprachen, einschließlich ihrer Codes, finden Sie unter Dokumente in anderen Sprachen als Englisch hinzufügen.

Bei benutzerdefinierten Feldern erstellen Sie diese Felder `DocumentMetadataConfigurationUpdates` mithilfe der `UpdateIndex` API, genau wie bei der Erstellung eines reservierten oder gemeinsamen Felds. Sie müssen den entsprechenden Datentyp für Ihr benutzerdefiniertes Feld festlegen. Wenn Sie die Konsole verwenden, aktualisieren Sie Felder, indem Sie Ihre Datenquelle auswählen, die Aktion Bearbeiten auswählen und dann mit dem Abschnitt Feldzuordnungen zur Konfiguration der Datenquelle fortfahren. Einige Datenquellen unterstützen das Hinzufügen neuer Felder oder benutzerdefinierter Felder nicht. Sie können den Feldtyp nicht mehr ändern, nachdem Sie das Feld erstellt haben.

Die folgenden Typen können Sie für benutzerdefinierte Felder festlegen:

- Datum
- Zahl
- String
- Zeichenfolgenliste

Wenn Sie dem Index mithilfe der BatchPutDocumentAPI Dokumente hinzugefügt haben, `Attributes` listet die Felder/Attribute Ihrer Dokumente auf und Sie erstellen Felder mithilfe des `DocumentAttribute` Objekts.

Für Dokumente, die aus einer Amazon S3 Datenquelle indexiert wurden, erstellen Sie Felder mithilfe einer JSON-Metadatendatei, die die Feldinformationen enthält.

Wenn Sie eine unterstützte Datenbank als Datenquelle verwenden, können Sie Ihre Felder mithilfe der Option Feldzuordnungen konfigurieren.

Datenquellen

Eine Datenquelle ist ein Datenrepository oder ein Speicherort, der eine Amazon Kendra Verbindung zu Ihren Dokumenten oder Inhalten herstellt und diese indexiert. Sie können beispielsweise so konfigurieren, Amazon Kendra dass eine Verbindung zu Microsoft hergestellt wird SharePoint , um Ihre in dieser Quelle gespeicherten Dokumente zu crawlen und zu indizieren. Sie können Webseiten auch indizieren, indem Sie die URLs angeben, die gecrawlt werden Amazon Kendra sollen. Sie können eine Datenquelle automatisch mit einem Amazon Kendra Index synchronisieren, sodass hinzugefügte, aktualisierte oder gelöschte Dokumente in der Datenquelle auch im Index hinzugefügt, aktualisiert oder gelöscht werden.

Unterstützte Datenquellen sind:

- Adobe Experience Manager
- Alfresco
- Aurora (MySQL)
- Aurora (PostgreSQL)
- Amazon FSx (Windows)
- Amazon FSx (NetApp ONTAP)
- Datenbank-Datenquellen
- Amazon RDS (Microsoft SQL Server)
- Amazon RDS (MySQL)
- Amazon RDS (Orakel)
- Amazon RDS (PostgreSQL)
- Amazon S3 Eimer
- Amazon Kendra Webcrawler
- Amazon WorkDocs
- Box (Kasten)
- Zusammenfluss
- Benutzerdefinierte Datenquellen

- Dropbox
- Drupal
- GitHub
- Gmail
- Google Workspace-Laufwerke
- IBM DB2
- Jira
- Microsoft Exchange
- Microsoft OneDrive
- Microsoft SharePoint
- Microsoft Teams
- Microsoft SQL Server
- Microsoft Yammer
- MySQL
- Oracle-Datenbank
- PostgreSQL
- Quip
- Salesforce
- ServiceNow
- Slack
- Zendesk

Eine Liste der von unterstützten Dokumenttypen oder -formate Amazon Kendra finden Sie unter Dokumenttypen. Sie müssen zuerst einen Index erstellen, bevor Sie einen Datenquellenconnector erstellen können, um Ihre Dokumente aus Ihrer Datenquelle zu indizieren.

> **Note**
>
> Um einen Dokumentenindex zu erstellen, müssen Sie keine Datenquelle verwenden. Sie können Dokumente per Batch-Upload direkt zu einem Index hinzufügen. Weitere Informationen finden Sie unter Dokumente direkt zu einem Index hinzufügen.

Eine exemplarische Vorgehensweise zur Verwendung der Amazon Kendra Konsole, der AWS CLI oder der SDKs finden Sie unter Erste Schritte.

Abfragen

Um Antworten zu erhalten, fragen Benutzer einen Index ab. Benutzer können in ihren Abfragen natürliche Sprache verwenden. Die Antwort enthält Informationen wie den Titel, einen Textauszug und die Position der Dokumente im Index, die die beste Antwort liefern.

Amazon Kendra verwendet alle Informationen, die Sie zu Ihren Dokumenten angeben, nicht nur den Inhalt der Dokumente, um zu ermitteln, ob ein Dokument für die Abfrage relevant ist. Wenn Ihr Index beispielsweise Informationen darüber enthält, wann Dokumente zuletzt aktualisiert wurden, können Sie festlegen, dass Dokumenten, Amazon Kendra die in jüngerer Zeit aktualisiert wurden, eine höhere Relevanz zugewiesen werden sollen.

Eine Abfrage kann auch Kriterien für das Filtern der Antwort enthalten, sodass nur Dokumente Amazon Kendra zurückgegeben werden, die die Filterkriterien erfüllen. Wenn Sie beispielsweise ein Indexfeld mit dem Namen Abteilung erstellt haben, können Sie die Antwort so filtern, dass nur Dokumente zurückgegeben werden, deren Abteilungsfeld auf Rechtlich festgelegt ist. Weitere Informationen finden Sie unter Suche filtern.

Sie können die Ergebnisse einer Abfrage beeinflussen, indem Sie die Relevanz einzelner Felder im Index optimieren. Durch die Optimierung ändert sich die Bedeutung eines Felds für die Ergebnisse. Wenn Sie beispielsweise die Wichtigkeit von Dokumenten mit der Kategorie neu hervorheben, ist es wahrscheinlicher, dass Dokumente dieser Kategorie in der Antwort enthalten sind. Weitere Informationen finden Sie unter Suchrelevanz optimieren.

Weitere Informationen zur Verwendung von Abfragen finden Sie unter Einen Index durchsuchen.

Tags

Verwalten Sie Ihre Indizes, Datenquellen und häufig gestellte Fragen, indem Sie Tags oder Labels zuweisen. Sie können Tags verwenden, um Ihre Amazon Kendra Ressourcen auf verschiedene Weise zu kategorisieren. Zum Beispiel nach Zweck, Eigentümer oder Anwendung oder einer beliebigen Kombination. Jedes Tag besteht aus einem Schlüssel und einem Wert, die Sie beide selbst definieren.

Tags helfen Ihnen bei Folgendem:

- Identifizieren und organisieren Sie Ihre AWS Ressourcen. Viele AWS Dienste unterstützen Tagging, sodass Sie Ressourcen in verschiedenen Diensten dasselbe Tag zuweisen können, um anzuzeigen, dass die Ressourcen miteinander verknüpft sind. Sie können beispielsweise einen Index und den Amazon Lex Bot, der den Index verwendet, mit demselben Tag kennzeichnen.
- Zuordnen von Kosten. Sie aktivieren Tags auf dem AWS Billing and Cost Management Dashboard. AWS verwendet Tags, um Ihre Kosten zu kategorisieren und Ihnen einen monatlichen Kostenverteilungsbericht zu liefern. Weitere Informationen finden Sie unter Kostenzuweisung und Tagging in Über AWS Billing and Cost Management.
- Kontrollieren Sie den Zugriff auf Ihre -Ressourcen. Sie können Tags in Richtlinien AWS Identity and Access Management (IAM) verwenden, die den Zugriff auf Amazon Kendra Ressourcen steuern. Sie können diese Richtlinien einer IAM Rolle oder einem Benutzer zuordnen, um die Tag-basierte Zugriffskontrolle zu aktivieren. Weitere Informationen finden Sie unter Autorisierung auf der Grundlage von Stichwörtern.

Sie können Tags mithilfe der AWS Management Console, der AWS Command Line Interface (AWS CLI) oder der Amazon Kendra API erstellen und verwalten.

Markieren von Ressourcen

Wenn Sie die Amazon Kendra Konsole verwenden, können Sie Ressourcen bei der Erstellung taggen oder sie später hinzufügen. Sie können die Konsole auch verwenden, um Tags zu aktualisieren oder zu entfernen.

Wenn Sie die AWS Command Line Interface (AWS CLI) oder die Amazon Kendra API verwenden, verwenden Sie die folgenden Operationen, um Tags für Ihre Ressourcen zu verwalten:

- CreateDataSource— Wenden Sie Tags an, wenn Sie eine Datenquelle erstellen.
- CreateFaq— Wenden Sie Tags an, wenn Sie eine häufig gestellte Frage erstellen.
- CreateIndex— Wendet Tags an, wenn Sie einen Index erstellen.
- ListTagsForResource— Zeigt die mit einer Ressource verknüpften Tags an.
- TagResource— Fügen Sie Tags für eine Ressource hinzu und ändern Sie sie.
- UntagResource— Tags aus einer Ressource entfernen.

Tag (Markierung)-Einschränkungen

Die folgenden Einschränkungen gelten für Tags auf Amazon Kendra Ressourcen:

- Maximale Anzahl von Stichworten: 50
- Maximale Schlüssellänge: 128 Zeichen
- Die maximale Länge des Werts beträgt 256 Zeichen
- Gültige Zeichen für Schlüssel und Wert — a—z, A—Z, Leerzeichen und die folgenden Zeichen: _.:/ = + - und @
- Schlüssel und Werte unterscheiden zwischen Groß- und Kleinschreibung.
- Verwenden Sie nicht `aws:` als Präfix für Schlüssel. Dieses Präfix ist für AWS reserviert.

Einrichten von Amazon Kendra

Bevor Sie Amazon Kendra verwenden, benötigen Sie ein Amazon Web Services (AWS)-Konto. Nachdem Sie ein - AWS Konto haben, können Sie über die Amazon-Kendra-Konsole, die AWS Command Line Interface (AWS CLI) oder die AWS SDKs auf Amazon Kendra zugreifen.

Dieses Handbuch enthält Beispiele für AWS CLI, Java und Python.

Themen

Registrieren für AWS

Bei der Registrierung für Amazon Web Services (AWS) wird Ihr -Konto automatisch für alle Services in registriert AWS, einschließlich Amazon Kendra. Berechnet werden Ihnen aber nur die Services, die Sie nutzen.

Wenn Sie bereits über ein - AWS Konto verfügen, fahren Sie mit der nächsten Aufgabe fort. Wenn Sie kein AWS -Konto haben, führen Sie die folgenden Schritte zum Erstellen eines Kontos aus.

So registrieren Sie sich bei AWS

1. Öffnen Sie https://aws.amazon.com und wählen Sie dann AWS Konto erstellen aus.
2. Folgen Sie den Anweisungen auf dem Bildschirm, um die Kontoerstellung durchzuführen. Notieren Sie sich Ihre 12-stellige AWS Kontonummer. Der Anmeldeprozess beinhaltet auch einen Telefonanruf und die Eingabe einer PIN über die Telefontastatur.
3. Erstellen Sie einen AWS Identity and Access Management (IAM)-Administratorbenutzer. Eine entsprechende Anleitung finden Sie unter Erstellen Ihres ersten Administratorbenutzers und Ihrer ersten Administratorgruppe in IAM im AWS Identity and Access Management Benutzerhandbuch.

Regionen und Endpunkte

Ein Endpunkt ist eine URL, die als Eintrittspunkt für einen Webservice fungiert. Jeder Endpunkt ist einer bestimmten AWS Region zugeordnet. Wenn Sie eine Kombination aus der Amazon-Kendra-Konsole AWS CLI, der und den Amazon-Kendra-SDKs verwenden, achten Sie auf ihre Standardregionen, da alle Amazon-Kendra-Komponenten einer bestimmten Kampagne (Index, Abfrage usw.) in derselben Region erstellt werden müssen. Die von Amazon Kendra unterstützten Regionen und Endpunkte finden Sie unter Regionen und Endpunkte.

Einrichten der AWS CLI

Die - AWS Befehlszeilenschnittstelle (AWS CLI) ist ein einheitliches Entwicklertool für die Verwaltung von AWS -Services, einschließlich Amazon Kendra. Wir empfehlen Ihnen, sie zu installieren.

1. Um die zu installieren AWS CLI, folgen Sie den Anweisungen unter Installieren der - AWS Befehlszeilenschnittstelle im AWS -Befehlszeilenschnittstellen-Benutzerhandbuch.
2. Um die zu konfigurieren AWS CLI und ein Profil für den Aufruf der einzurichten AWS CLI, folgen Sie den Anweisungen unter Konfigurieren der AWS CLI im AWS Benutzerhandbuch für die - Befehlszeilenschnittstelle.
3. Führen Sie den folgenden Befehl aus, um zu bestätigen, dass das AWS CLI Profil ordnungsgemäß konfiguriert ist:

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

   Wenn das Profil korrekt konfiguriert wurde, wird die Ausgabe etwa wie folgt aussehen:

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

4. Führen Sie die folgenden Befehle aus, um zu überprüfen, ob für die Verwendung mit Amazon Kendra konfiguriert AWS CLI ist:

   ```
   aws kendra help
   ```

   Wenn der korrekt konfiguriert AWS CLI ist, wird eine Liste der AWS CLI unterstützten Befehle für Amazon Kendra-, Amazon Kendra-Laufzeit- und Amazon Kendra-Ereignisse angezeigt.

Einrichten der AWS SDKs

Laden Sie die zu verwendenden AWS SDKs herunter und installieren Sie sie. Dieses Handbuch enthält Beispiele für Python. Weitere Informationen zu anderen AWS SDKs finden Sie unter Tools für Amazon Web Services.

Das Paket für das Python SDK heißt Boto3.

Bevor Sie die folgenden Python-Befehle ausführen, müssen Sie Python 3.6 oder höher zuerst für Ihr Betriebssystem herunterladen und installieren. Die Unterstützung für Python 3.5 und früher ist veraltet. Wenn Sie pip nicht in Ihrem Python-Scripts-Verzeichnis enthalten haben, können Sie get-pip.py herunterladen und in Ihrem Skripts-Verzeichnis speichern. Sie können Ihr Python-Verzeichnis auch mithilfe eines Terminalprogramms als Pfad oder Umgebungsvariable festlegen.

```
# 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
```

Um Boto3 verwenden zu können, müssen Sie mithilfe der IAM-Konsole Authentifizierungsanmeldeinformationen für Ihr AWS Konto einrichten.

IAM -Zugriffsrollen für Amazon Kendra

Wenn Sie einen Index, eine Datenquelle oder eine häufig gestellte Frage erstellen, Amazon Kendra benötigt Zugriff auf die AWS Ressourcen, die zum Erstellen der Amazon Kendra Ressource erforderlich sind. Sie müssen eine AWS Identity and Access Management (IAM)-Richtlinie erstellen, bevor Sie die Amazon Kendra Ressource erstellen. Wenn Sie die -Operation aufrufen, geben Sie den Amazon-Ressourcennamen (ARN) der Rolle mit der angehängten Richtlinie an. Wenn Sie beispielsweise die BatchPutDocument-API aufrufen, um Dokumente aus einem - Amazon S3 Bucket hinzuzufügen, stellen Sie eine Rolle Amazon Kendra mit einer Richtlinie bereit, die Zugriff auf den Bucket hat.

Sie können eine neue IAM Rolle in der Amazon Kendra Konsole erstellen oder eine IAM vorhandene Rolle auswählen, die verwendet werden soll. Die Konsole zeigt Rollen mit der Zeichenfolge „kendra“ oder „Kendra“ im Rollennamen an.

Die folgenden Themen enthalten Details zu den erforderlichen Richtlinien. Wenn Sie IAM Rollen mit der Amazon Kendra Konsole erstellen, werden diese Richtlinien für Sie erstellt.

Themen

IAM -Rollen für Indizes

Wenn Sie einen Index erstellen, müssen Sie eine - IAM Rolle mit der Berechtigung zum Schreiben in einen bereitstellen Amazon CloudWatch. Sie müssen auch eine Vertrauensrichtlinie angeben, die es

ermöglicht, die Rolle Amazon Kendra zu übernehmen. Im Folgenden sind die Richtlinien aufgeführt, die bereitgestellt werden müssen.

IAM -Rollen für Indizes

Eine Rollenrichtlinie, die Amazon Kendra den Zugriff auf ein CloudWatch Protokoll ermöglicht.

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

Eine Rollenrichtlinie, die Amazon Kendra den Zugriff auf ermöglicht AWS Secrets Manager. Wenn Sie den Benutzerkontext mit Secrets Manager als Schlüsselspeicherort verwenden, können Sie die folgende Richtlinie verwenden.

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

Eine Vertrauensrichtlinie, Amazon Kendra mit der eine Rolle übernehmen kann.

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

IAM -Rollen für die BatchPutDocument API

> **Warning**
>
> Amazon Kendra verwendet keine Bucket-Richtlinie, die einem - Amazon Kendra Prinzipal Berechtigungen zur Interaktion mit einem S3-Bucket erteilt. Stattdessen werden Rollen verwendet IAM . Stellen Sie sicher, dass nicht als vertrauenswürdiges Mitglied in Ihrer Bucket-Richtlinie enthalten Amazon Kendra ist, um Datensicherheitsprobleme beim versehentlichen Erteilen von Berechtigungen für beliebige Prinzipale zu vermeiden. Sie können jedoch eine Bucket-Richtlinie hinzufügen, um einen - Amazon S3 Bucket über verschiedene Konten hinweg zu verwenden. Weitere Informationen finden Sie unter Zu verwendende Richtlinien Amazon S3 für -Konten. Informationen zu IAM Rollen für S3-Datenquellen finden Sie unter IAM Rollen .

Wenn Sie die BatchPutDocument-API verwenden, um Dokumente in einem - Amazon S3 Bucket zu indizieren, müssen Sie eine - IAM Rolle Amazon Kendra mit Zugriff auf den Bucket bereitstellen. Sie müssen auch eine Vertrauensrichtlinie angeben, die es ermöglicht, die Rolle Amazon Kendra zu übernehmen. Wenn die Dokumente im Bucket verschlüsselt sind, müssen Sie die Berechtigung erteilen, den AWS KMS Kundenmasterschlüssel (CMK) zum Entschlüsseln der Dokumente zu verwenden.

IAM -Rollen für die BatchPutDocument API

Eine erforderliche Rollenrichtlinie, um den Zugriff auf einen Amazon S3 -Bucket Amazon Kendra zu ermöglichen.

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

```
    ]
}
```

Eine Vertrauensrichtlinie, Amazon Kendra mit der eine Rolle übernehmen kann.

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

Es wird empfohlen, dass Sie `aws:sourceAccount` und `aws:sourceArn` in die Vertrauensrichtlinie aufnehmen. Dadurch `aws:sourceArn` werden Berechtigungen eingeschränkt und sicher geprüft, ob `aws:sourceAccount` und mit denen in der IAM Rollenrichtlinie für die `sts:AssumeRole` Aktion übereinstimmen. Dadurch wird verhindert, dass nicht autorisierte Entitäten auf Ihre IAM Rollen und deren Berechtigungen zugreifen. Weitere Informationen finden Sie im AWS Identity and Access Management Leitfaden zum Confused-Deputy-Problem .

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

Eine optionale Rollenrichtlinie, die es ermöglicht Amazon Kendra , einen AWS KMS - Kundenmasterschlüssel (CMK) zum Entschlüsseln von Dokumenten in einem - Amazon S3 Bucket zu verwenden.

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

IAM -Rollen für Datenquellen

Wenn Sie die CreateDataSource-API verwenden, müssen Sie Amazon Kendra eine - IAM Rolle erteilen, die über die Berechtigung für den Zugriff auf die Ressourcen verfügt. Die spezifischen erforderlichen Berechtigungen hängen von der Datenquelle ab.

IAM -Rollen für Adobe Experience Manager-Datenquellen

Wenn Sie Adobe Experience Manager verwenden, geben Sie eine Rolle mit den folgenden Richtlinien an.

- Berechtigung zum Zugriff auf Ihr AWS Secrets Manager Secret zur Authentifizierung Ihres Adobe Experience Manager.

- Berechtigung zum Aufrufen der erforderlichen öffentlichen APIs für den Adobe Experience Manager-Konnektor.
- Berechtigung zum Aufrufen der APIs `BatchPutDocument`, `BatchDeleteDocument`, `DeletePrincipalMapping`, `PutPrincipalMappingDescribePrincipalMapping`, und `ListGroupsOlderThanOrderingId` APIs.

> **Note**
>
> Sie können eine Adobe Experience Manager-Datenquelle über mit Amazon Kendra verbinden Amazon VPC. Wenn Sie eine verwenden Amazon VPC, müssen Sie zusätzliche Berechtigungen hinzufügen.

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

Eine Vertrauensrichtlinie, Amazon Kendra mit der eine Rolle übernehmen kann.

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

IAM -Rollen für Alfresco-Datenquellen

Wenn Sie Alfresco verwenden, geben Sie eine Rolle mit den folgenden Richtlinien an.

- Berechtigung zum Zugriff auf Ihr AWS Secrets Manager Secret zur Authentifizierung Ihres Alfresco.
- Berechtigung zum Aufrufen der erforderlichen öffentlichen APIs für den Alfresco-Konnektor.
- Berechtigung zum Aufrufen der APIs `BatchPutDocument`, `BatchDeleteDocument`, `DeletePrincipalMapping`, `PutPrincipalMappingDescribePrincipalMapping`, und `ListGroupsOlderThanOrderingId` APIs.

> **Note**
>
> Sie können eine Alfresco-Datenquelle Amazon Kendra über mit verbinden Amazon VPC. Wenn Sie eine verwenden Amazon VPC, müssen Sie zusätzliche Berechtigungen hinzufügen.

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

Eine Vertrauensrichtlinie, Amazon Kendra mit der eine Rolle übernehmen kann.

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

IAM -Rollen für Aurora (MySQL)-Datenquellen

Wenn Sie Aurora (MySQL) verwenden, stellen Sie eine Rolle mit den folgenden Richtlinien bereit.

- Berechtigung zum Zugriff auf Ihr AWS Secrets Manager Secret zur Authentifizierung Ihres Aurora (MySQL).
- Berechtigung zum Aufrufen der erforderlichen öffentlichen APIs für den Aurora (MySQL)-Konnektor.
- Berechtigung zum Aufrufen der APIs `BatchPutDocument`, `BatchDeleteDocument`, `DeletePrincipalMapping`, `PutPrincipalMappingDescribePrincipalMapping`, und `ListGroupsOlderThanOrderingId` APIs.

> **Note**
>
> Sie können eine Aurora (MySQL)-Datenquelle über mit Amazon Kendra verbinden Amazon VPC. Wenn Sie eine verwenden Amazon VPC, müssen Sie zusätzliche Berechtigungen hinzufügen.

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

Eine Vertrauensrichtlinie, Amazon Kendra mit der eine Rolle übernehmen kann.

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

IAM -Rollen für Aurora (PostgreSQL)-Datenquellen

Wenn Sie Aurora (PostgreSQL) verwenden, stellen Sie eine Rolle mit den folgenden Richtlinien bereit.

- Berechtigung zum Zugriff auf Ihr AWS Secrets Manager Secret zur Authentifizierung Ihres Aurora (PostgreSQL).
- Berechtigung zum Aufrufen der erforderlichen öffentlichen APIs für den Aurora (PostgreSQL)-Konnektor.
- Berechtigung zum Aufrufen der APIs `BatchPutDocument`, `BatchDeleteDocument`, `DeletePrincipalMapping`, `PutPrincipalMappingDescribePrincipalMapping`, und `ListGroupsOlderThanOrderingId` APIs.

> **Note**
>
> Sie können eine Aurora (PostgreSQL)-Datenquelle über mit Amazon Kendra verbinden Amazon VPC. Wenn Sie eine verwenden Amazon VPC, müssen Sie zusätzliche Berechtigungen hinzufügen.

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

Eine Vertrauensrichtlinie, Amazon Kendra mit der eine Rolle übernehmen kann.

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

```
}
```

IAM -Rollen für Amazon FSx Datenquellen

Wenn Sie verwenden Amazon FSx, geben Sie eine Rolle mit den folgenden Richtlinien an.

- Berechtigung zum Zugriff auf Ihr AWS Secrets Manager Secret zur Authentifizierung Ihres Amazon FSx Dateisystems.
- Berechtigung für den Zugriff auf Amazon Virtual Private Cloud (VPC), in dem sich Ihr Amazon FSx Dateisystem befindet.
- Berechtigung zum Abrufen des Domänennamens Ihres Active Directory für Ihr Amazon FSx Dateisystem.
- Berechtigung zum Aufrufen der erforderlichen öffentlichen APIs für den Amazon FSx Konnektor.
- Berechtigung zum Aufrufen der `BatchDeleteDocument` APIs `BatchPutDocument` und , um den Index zu aktualisieren.

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

Eine Vertrauensrichtlinie, Amazon Kendra mit der eine Rolle übernehmen kann.

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

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

IAM -Rollen für Datenbankdatenquellen

Wenn Sie eine Datenbank als Datenquelle verwenden, stellen Sie eine Rolle Amazon Kendra bereit, die über die erforderlichen Berechtigungen für die Verbindung mit dem verfügt. Dazu zählen:

- Berechtigung für den Zugriff auf das AWS Secrets Manager Secret, das den Benutzernamen und das Passwort für die Website enthält. Weitere Informationen zum Inhalt des Secrets finden Sie unter Datenquellen .
- Berechtigung zur Verwendung des AWS KMS Kundenmasterschlüssels (CMK) zum Entschlüsseln des von gespeicherten Benutzernamens und Passwort-Secrets Secrets Manager.
- Berechtigung zur Verwendung der `BatchDeleteDocument` Operationen `BatchPutDocument` und zum Aktualisieren des Index.
- Berechtigung für den Zugriff auf den Amazon S3 Bucket, der das SSL-Zertifikat enthält, das für die Kommunikation mit der Website verwendet wird.

> **Note**
>
> Sie können Datenbankdatenquellen Amazon Kendra über mit verbinden Amazon VPC. Wenn Sie eine verwenden Amazon VPC, müssen Sie zusätzliche Berechtigungen hinzufügen.

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

Es gibt zwei optionale Richtlinien, die Sie mit einer Datenquelle verwenden können.

Wenn Sie den Amazon S3 Bucket verschlüsselt haben, der das SSL-Zertifikat enthält, das für die Kommunikation mit der verwendet wird, geben Sie eine Richtlinie an, um Amazon Kendra Zugriff auf den Schlüssel zu gewähren.

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

Wenn Sie eine VPC verwenden, geben Sie eine Richtlinie an, die Amazon Kendra Zugriff auf die erforderlichen Ressourcen gewährt. Die erforderliche Richtlinie finden Sie unter IAM Rollen für Datenquellen, VPC.

Eine Vertrauensrichtlinie, Amazon Kendra mit der eine Rolle übernehmen kann.

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

IAM -Rollen für Amazon RDS (Microsoft SQL Server)-Datenquellen

Wenn Sie einen Amazon RDS (Microsoft SQL Server) Datenquellen-Connector verwenden, stellen Sie eine Rolle mit den folgenden Richtlinien bereit.

- Berechtigung zum Zugriff auf Ihr AWS Secrets Manager Secret zur Authentifizierung Ihrer Amazon RDS (Microsoft SQL Server)-Datenquellen-Instance.
- Berechtigung zum Aufrufen der erforderlichen öffentlichen APIs für den Amazon RDS (Microsoft SQL Server)-Datenquellen-Konnektor.
- Berechtigung zum Aufrufen der APIs `BatchPutDocument`, `BatchDeleteDocument`, `DeletePrincipalMapping`, `PutPrincipalMappingDescribePrincipalMapping`, und `ListGroupsOlderThanOrderingId` APIs.

> **Note**
>
> Sie können eine Amazon RDS (Microsoft SQL Server)-Datenquelle Amazon Kendra über mit verbinden Amazon VPC. Wenn Sie eine verwenden Amazon VPC, müssen Sie zusätzliche Berechtigungen hinzufügen.

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

Eine Vertrauensrichtlinie, Amazon Kendra mit der eine Rolle übernehmen kann.

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

IAM -Rollen für Amazon RDS (MySQL)-Datenquellen

Wenn Sie einen Amazon RDS (MySQL)-Datenquellen-Konnektor verwenden, stellen Sie eine Rolle mit den folgenden Richtlinien bereit.

- Berechtigung zum Zugriff auf Ihr AWS Secrets Manager Secret zur Authentifizierung Ihrer Amazon RDS (MySQL)-Datenquellen-Instance.
- Berechtigung zum Aufrufen der erforderlichen öffentlichen APIs für den Amazon RDS (MySQL)-Datenquellen-Konnektor.
- Berechtigung zum Aufrufen der APIs `BatchPutDocument`, `BatchDeleteDocument`, `DeletePrincipalMappingPutPrincipalMapping`, `DescribePrincipalMapping`, und `ListGroupsOlderThanOrderingId` APIs.

> **Note**
>
> Sie können eine Amazon RDS (MySQL)-Datenquelle über mit Amazon Kendra verbinden Amazon VPC. Wenn Sie eine verwenden Amazon VPC, müssen Sie zusätzliche Berechtigungen hinzufügen.

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

Eine Vertrauensrichtlinie, Amazon Kendra mit der eine Rolle übernehmen kann.

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

```
}
```

IAM -Rollen für Amazon RDS (Oracle)-Datenquellen

Wenn Sie einen Amazon RDS Oracle-Datenquellen-Konnektor verwenden, stellen Sie eine Rolle mit den folgenden Richtlinien bereit.

- Berechtigung zum Zugriff auf Ihr AWS Secrets Manager Secret zur Authentifizierung Ihrer Amazon RDS (Oracle)-Datenquellen-Instance.
- Berechtigung zum Aufrufen der erforderlichen öffentlichen APIs für den Amazon RDS (Oracle)-Datenquellen-Konnektor.
- Berechtigung zum Aufrufen der APIs `BatchPutDocument`, `BatchDeleteDocument`, `DeletePrincipalMappingPutPrincipalMapping`, `DescribePrincipalMapping`, und `ListGroupsOlderThanOrderingId` APIs.

> **Note**
>
> Sie können eine Amazon RDS Oracle-Datenquelle über mit Amazon Kendra verbinden Amazon VPC. Wenn Sie eine verwenden Amazon VPC, müssen Sie zusätzliche Berechtigungen hinzufügen.

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

Eine Vertrauensrichtlinie, Amazon Kendra mit der eine Rolle übernehmen kann.

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

```
      }
    ]
}
```

IAM -Rollen für Amazon RDS (PostgreSQL)-Datenquellen

Wenn Sie einen Amazon RDS (PostgreSQL)-Datenquellen-Konnektor verwenden, stellen Sie eine Rolle mit den folgenden Richtlinien bereit.

- Berechtigung zum Zugriff auf Ihr AWS Secrets Manager Secret zur Authentifizierung Ihrer Amazon RDS (PostgreSQL)-Datenquellen-Instance.
- Berechtigung zum Aufrufen der erforderlichen öffentlichen APIs für den Amazon RDS (PostgreSQL)-Datenquellen-Konnektor.
- Berechtigung zum Aufrufen der APIs `BatchPutDocument`, `BatchDeleteDocument`, `DeletePrincipalMappingPutPrincipalMapping`, `DescribePrincipalMapping`, und `ListGroupsOlderThanOrderingId` APIs.

> **Note**
>
> Sie können eine Amazon RDS (PostgreSQL)-Datenquelle über mit Amazon Kendra verbinden Amazon VPC. Wenn Sie eine verwenden Amazon VPC, müssen Sie zusätzliche Berechtigungen hinzufügen.

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

Eine Vertrauensrichtlinie, Amazon Kendra mit der eine Rolle übernehmen kann.

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

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

IAM -Rollen für Amazon S3 Datenquellen

> **Warning**
>
> Amazon Kendra verwendet keine Bucket-Richtlinie, die einem - Amazon Kendra Prinzipal Berechtigungen zur Interaktion mit einem S3-Bucket erteilt. Stattdessen werden IAM Rollen verwendet. Stellen Sie sicher, dass nicht als vertrauenswürdiges Mitglied in Ihrer Bucket-Richtlinie enthalten Amazon Kendra ist, um Datensicherheitsprobleme beim versehentlichen Erteilen von Berechtigungen für beliebige Prinzipale zu vermeiden. Sie können jedoch eine Bucket-Richtlinie hinzufügen, um einen Amazon S3 -Bucket über verschiedene Konten hinweg zu verwenden. Weitere Informationen finden Sie unter Zu Amazon S3 verwendende Richtlinien für alle Konten (herunterscrollen).

Wenn Sie einen - Amazon S3 Bucket als Datenquelle verwenden, stellen Sie eine Rolle bereit, die über die Berechtigung zum Zugriff auf den Bucket und zur Verwendung der `BatchDeleteDocument` Operationen `BatchPutDocument` und verfügt. Wenn die Dokumente im Bucket verschlüsselt sind, müssen Sie die Amazon S3 Berechtigung erteilen, den AWS KMS Kundenmasterschlüssel (CMK) zum Entschlüsseln der Dokumente zu verwenden.

Die folgenden Rollenrichtlinien müssen zulassen Amazon Kendra , dass eine Rolle annimmt. Scrollen Sie weiter nach unten, um eine Vertrauensrichtlinie zur Übernahme einer Rolle anzuzeigen.

Eine erforderliche Rollenrichtlinie, damit einen Amazon Kendra - Amazon S3 Bucket als Datenquelle verwenden kann.

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

Eine optionale Rollenrichtlinie, die es ermöglicht Amazon Kendra , einen AWS KMS - Kundenmasterschlüssel (CMK) zum Entschlüsseln von Dokumenten in einem - Amazon S3 Bucket zu verwenden.

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

```
}
```

Eine optionale Rollenrichtlinie, die Amazon Kendra den Zugriff auf einen Amazon S3 -Bucket ermöglicht, während ein verwendet wird Amazon VPCund ohne Aktivierungs- AWS KMS oder AWS KMS Freigabeberechtigungen.

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

Eine optionale Rollenrichtlinie, die den Zugriff Amazon Kendra auf einen Amazon S3 -Bucket ermöglicht Amazon VPC, während ein und mit aktivierten AWS KMS Berechtigungen verwendet werden.

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

Eine Vertrauensrichtlinie, Amazon Kendra mit der eine Rolle übernehmen kann.

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

Zu Amazon S3 verwendende Richtlinien für alle Konten

Wenn sich Ihr Amazon S3 Bucket in einem anderen Konto befindet als das Konto, das Sie für Ihren Amazon Kendra Index verwenden, können Sie Richtlinien erstellen, um ihn kontenübergreifend zu verwenden.

Eine Rollenrichtlinie zur Verwendung Ihres Amazon S3 Buckets als Datenquelle, wenn sich der Bucket in einem anderen Konto als Ihr Amazon Kendra Index befindet. Beachten Sie, dass `s3:PutObject` und optional `s3:PutObjectAcl` sind, und verwenden Sie diese Option, wenn Sie eine Konfigurationsdatei für Ihre Zugriffskontrollliste einschließen möchten.

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

Eine Bucket-Richtlinie, die der Amazon S3 Datenquellenrolle den kontenübergreifenden Zugriff auf den Amazon S3 Bucket ermöglicht. Beachten Sie, dass `s3:PutObject` und optional `s3:PutObjectAcl` sind, und verwenden Sie dies, wenn Sie eine Konfigurationsdatei für Ihre Zugriffskontrollliste einschließen möchten.

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

Eine Vertrauensrichtlinie, Amazon Kendra mit der eine Rolle übernehmen kann.

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

IAM -Rollen für Amazon Kendra Web-Crawler-Datenquellen

Wenn Sie Amazon Kendra Web Crawler verwenden, geben Sie eine Rolle mit den folgenden Richtlinien an:

- Berechtigung für den Zugriff auf das AWS Secrets Manager Secret, das die Anmeldeinformationen für die Verbindung mit Websites oder einem Web-Proxy-Server enthält, der durch die Standardauthentifizierung unterstützt wird. Weitere Informationen zum Inhalt des Secrets finden Sie unter Verwenden einer Web-Crawler-Datenquelle.
- Berechtigung zur Verwendung des AWS KMS Kundenmasterschlüssels (CMK) zum Entschlüsseln des von gespeicherten Benutzernamens und Passwort-Secrets Secrets Manager.

- Berechtigung zur Verwendung der `BatchDeleteDocument` Operationen `BatchPutDocument` und zum Aktualisieren des Index.
- Wenn Sie einen - Amazon S3 Bucket verwenden, um Ihre Liste von Seed-URLs oder Sitemaps zu speichern, fügen Sie die Berechtigung für den Zugriff auf den Amazon S3 Bucket hinzu.

> **Note**
>
> Sie können eine - Amazon Kendra Web-Crawler-Datenquelle über mit Amazon Kendra verbinden Amazon VPC. Wenn Sie eine verwenden Amazon VPC, müssen Sie zusätzliche Berechtigungen hinzufügen.

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

Wenn Sie Ihre Seed-URLs oder Sitemaps in einem - Amazon S3 Bucket speichern, müssen Sie diese Berechtigung der Rolle hinzufügen.

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

Eine Vertrauensrichtlinie, Amazon Kendra mit der eine Rolle übernehmen kann.

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

IAM -Rollen für Amazon WorkDocs Datenquellen

Wenn Sie verwenden Amazon WorkDocs, stellen Sie eine Rolle mit den folgenden Richtlinien bereit

- Berechtigung zum Überprüfen der Verzeichnis-ID (Organisations-ID), die Ihrem Amazon WorkDocs Website-Repository entspricht.
- Berechtigung zum Abrufen des Domänennamens Ihres Active Directory, das Ihr Amazon WorkDocs Website-Verzeichnis enthält.
- Berechtigung zum Aufrufen der erforderlichen öffentlichen APIs für den Amazon WorkDocs Konnektor.
- Berechtigung zum Aufrufen der `BatchDeleteDocument` APIs `BatchPutDocument` und , um den Index zu aktualisieren.

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

Eine Vertrauensrichtlinie, Amazon Kendra mit der eine Rolle übernehmen kann.

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

IAM -Rollen für Box-Datenquellen

Wenn Sie Box verwenden, geben Sie eine Rolle mit den folgenden Richtlinien an.

- Berechtigung zum Zugriff auf Ihr AWS Secrets Manager Secret zur Authentifizierung Ihres Slack.
- Berechtigung zum Aufrufen der erforderlichen öffentlichen APIs für den Box-Konnektor.
- Berechtigung zum Aufrufen der APIs `BatchPutDocument`, `BatchDeleteDocument`, `DeletePrincipalMappingPutPrincipalMapping`, `DescribePrincipalMapping`, und `ListGroupsOlderThanOrderingId` APIs.

> **Note**
>
> Sie können eine Box-Datenquelle Amazon Kendra über mit verbinden Amazon VPC. Wenn Sie eine verwenden Amazon VPC, müssen Sie zusätzliche Berechtigungen hinzufügen.

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

Eine Vertrauensrichtlinie, Amazon Kendra mit der eine Rolle übernehmen kann.

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

IAM -Rollen für Confluence-Datenquellen

IAM -Rollen für Confluence Connector v1.0

Wenn Sie einen Confluence-Server als Datenquelle verwenden, stellen Sie eine Rolle mit den folgenden Richtlinien bereit:

- Berechtigung für den Zugriff auf das AWS Secrets Manager Secret, das die Anmeldeinformationen enthält, die für die Verbindung mit Confluence erforderlich sind. Weitere Informationen zum Inhalt des Secrets finden Sie unter Confluence-Datenquellen.
- Berechtigung zur Verwendung des AWS KMS Kundenmasterschlüssels (CMK) zum Entschlüsseln des von gespeicherten Benutzernamens und Passwort-Secrets Secrets Manager.
- Berechtigung zur Verwendung der `BatchDeleteDocument` Operationen `BatchPutDocument` und zum Aktualisieren des Index.

> **Note**
>
> Sie können eine Confluence-Datenquelle Amazon Kendra über mit verbinden Amazon VPC. Wenn Sie eine verwenden Amazon VPC, müssen Sie zusätzliche Berechtigungen hinzufügen.

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

Wenn Sie eine VPC verwenden, geben Sie eine Richtlinie an, die Amazon Kendra Zugriff auf die erforderlichen Ressourcen gewährt. Die erforderliche Richtlinie finden Sie unter IAM Rollen für Datenquellen, VPC.

Eine Vertrauensrichtlinie, Amazon Kendra mit der eine Rolle übernehmen kann.

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

IAM -Rollen für Confluence Connector v2.0

Für eine Confluence-Connector-v2.0-Datenquelle geben Sie eine Rolle mit den folgenden Richtlinien an.

- Berechtigung für den Zugriff auf das AWS Secrets Manager Secret, das die Authentifizierungsanmeldeinformationen für Confluence enthält. Weitere Informationen zum Inhalt des Secrets finden Sie unter Confluence-Datenquellen.
- Berechtigung zur Verwendung des AWS KMS Kundenmasterschlüssels (CMK) zum Entschlüsseln des von gespeicherten Benutzernamens und Passwort-Secrets AWS Secrets Manager.
- Berechtigung zur Verwendung der `BatchDeleteDocument` Operationen `BatchPutDocument` und zum Aktualisieren des Index.

Sie müssen auch eine Vertrauensrichtlinie anfügen, die es erlaubt, die Rolle Amazon Kendra zu übernehmen.

> **Note**
>
> Sie können eine Confluence-Datenquelle Amazon Kendra über mit verbinden Amazon VPC. Wenn Sie eine verwenden Amazon VPC, müssen Sie zusätzliche Berechtigungen hinzufügen.

Eine Rollenrichtlinie, die es ermöglicht Amazon Kendra , eine Verbindung zu Confluence herzustellen.

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

Eine Vertrauensrichtlinie, Amazon Kendra mit der eine Rolle übernehmen kann.

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

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

IAM -Rollen für Dropbox-Datenquellen

Wenn Sie Dropbox verwenden, geben Sie eine Rolle mit den folgenden Richtlinien an.

- Berechtigung zum Zugriff auf Ihr AWS Secrets Manager Secret zur Authentifizierung Ihrer Dropbox.
- Berechtigung zum Aufrufen der erforderlichen öffentlichen APIs für den Dropbox-Konnektor.
- Berechtigung zum Aufrufen der APIs `BatchPutDocument`, `BatchDeleteDocument`, `DeletePrincipalMapping`, `PutPrincipalMappingDescribePrincipalMapping`, und `ListGroupsOlderThanOrderingId` APIs.

> **Note**
>
> Sie können eine Dropbox-Datenquelle Amazon Kendra über mit verbinden Amazon VPC. Wenn Sie eine verwenden Amazon VPC, müssen Sie zusätzliche Berechtigungen hinzufügen.

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

Eine Vertrauensrichtlinie, Amazon Kendra mit der eine Rolle übernehmen kann.

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

IAM -Rollen für Drupal-Datenquellen

Wenn Sie Drupal verwenden, geben Sie eine Rolle mit den folgenden Richtlinien an.

- Berechtigung zum Zugriff auf Ihr AWS Secrets Manager Secret zur Authentifizierung Ihres Drupal.
- Berechtigung zum Aufrufen der erforderlichen öffentlichen APIs für den Drupal-Konnektor.
- Berechtigung zum Aufrufen der APIs `BatchPutDocument`, `BatchDeleteDocument`, `DeletePrincipalMapping`, `PutPrincipalMappingDescribePrincipalMapping`, und `ListGroupsOlderThanOrderingId` APIs.

> **Note**
>
> Sie können eine Drupal-Datenquelle Amazon Kendra über mit verbinden Amazon VPC. Wenn Sie eine verwenden Amazon VPC, müssen Sie zusätzliche Berechtigungen hinzufügen.

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

Eine Vertrauensrichtlinie, Amazon Kendra mit der eine Rolle übernehmen kann.

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

IAM -Rollen für GitHub Datenquellen

Wenn Sie verwenden GitHub, geben Sie eine Rolle mit den folgenden Richtlinien an.

- Berechtigung zum Zugriff auf Ihr AWS Secrets Manager Secret zur Authentifizierung Ihres GitHub.
- Berechtigung zum Aufrufen der erforderlichen öffentlichen APIs für den GitHub Konnektor.
- Berechtigung zum Aufrufen der APIs `BatchPutDocument`, `BatchDeleteDocument`, `DeletePrincipalMapping`, `PutPrincipalMappingDescribePrincipalMapping`, und `ListGroupsOlderThanOrderingId` APIs.

> **Note**
>
> Sie können eine GitHub Datenquelle Amazon Kendra über mit verbinden Amazon VPC. Wenn Sie eine verwenden Amazon VPC, müssen Sie zusätzliche Berechtigungen hinzufügen.

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

Eine Vertrauensrichtlinie, Amazon Kendra mit der eine Rolle übernehmen kann.

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

IAM -Rollen für Gmail-Datenquellen

Wenn Sie Gmail verwenden, geben Sie eine Rolle mit den folgenden Richtlinien an.

- Berechtigung zum Zugriff auf Ihr AWS Secrets Manager Secret zur Authentifizierung Ihrer Gmail.
- Berechtigung zum Aufrufen der erforderlichen öffentlichen APIs für den Gmailconnector.
- Berechtigung zum Aufrufen der APIs `BatchPutDocument`, `BatchDeleteDocument`, `DeletePrincipalMapping`, `PutPrincipalMappingDescribePrincipalMapping`, und `ListGroupsOlderThanOrderingId` APIs.

> **Note**
>
> Sie können eine Gmail-Datenquelle Amazon Kendra über mit verbinden Amazon VPC. Wenn Sie eine verwenden Amazon VPC, müssen Sie zusätzliche Berechtigungen hinzufügen.

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

Eine Vertrauensrichtlinie, Amazon Kendra mit der eine Rolle übernehmen kann.

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

IAM -Rollen für Google-Drive-Datenquellen

Wenn Sie eine Google Workspace Drive-Datenquelle verwenden, stellen Sie eine Rolle Amazon Kendra bereit, die über die erforderlichen Berechtigungen für die Verbindung mit der Website verfügt. Dazu zählen:

- Berechtigung zum Abrufen und Entschlüsseln des AWS Secrets Manager Geheimnisses, das die Clientkonto-E-Mail, die Adminkonto-E-Mail und den privaten Schlüssel enthält, die für die Verbindung mit der Google-Drive-Website erforderlich sind. Weitere Informationen zum Inhalt des Secrets finden Sie unter Google Drive-Datenquellen.
- Berechtigung zur Verwendung der BatchPutDocument APIs und BatchDeleteDocument APIs.

> **Note**
>
> Sie können eine Google-Drive-Datenquelle Amazon Kendra über mit verbinden Amazon VPC. Wenn Sie eine verwenden Amazon VPC, müssen Sie zusätzliche Berechtigungen hinzufügen.

Die folgende IAM Richtlinie stellt die erforderlichen Berechtigungen bereit:

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

Eine Vertrauensrichtlinie, Amazon Kendra mit der eine Rolle übernehmen kann.

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

IAM -Rollen für IBM DB2-Datenquellen

Wenn Sie einen IBM DB2-Datenquellen-Connector verwenden, stellen Sie eine Rolle mit den folgenden Richtlinien bereit.

- Berechtigung zum Zugriff auf Ihr AWS Secrets Manager Secret zur Authentifizierung Ihrer IBM DB2-Datenquellen-Instance.
- Berechtigung zum Aufrufen der erforderlichen öffentlichen APIs für den IBM DB2-Datenquellen-Konnektor.
- Berechtigung zum Aufrufen der APIs `BatchPutDocument`, `BatchDeleteDocument`, `DeletePrincipalMapping`, `PutPrincipalMappingDescribePrincipalMapping`, und `ListGroupsOlderThanOrderingId` APIs.

> **Note**
>
> Sie können eine IBM DB2-Datenquelle Amazon Kendra über mit verbinden Amazon VPC. Wenn Sie eine verwenden Amazon VPC, müssen Sie zusätzliche Berechtigungen hinzufügen.

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

Eine Vertrauensrichtlinie, Amazon Kendra mit der eine Rolle übernehmen kann.

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

IAM -Rollen für JCCP-Datenquellen

Wenn Sie Jpir verwenden, geben Sie eine Rolle mit den folgenden Richtlinien an.

- Berechtigung zum Zugriff auf Ihr AWS Secrets Manager Secret zur Authentifizierung Ihrer Jura.
- Berechtigung zum Aufrufen der erforderlichen öffentlichen APIs für den Jura-Konnektor.
- Berechtigung zum Aufrufen der APIs `BatchPutDocument`, `BatchDeleteDocument`, `DeletePrincipalMapping`, `PutPrincipalMappingDescribePrincipalMapping`, und `ListGroupsOlderThanOrderingId` APIs.

> **Note**
>
> Sie können eine JCCP-Datenquelle Amazon Kendra über mit verbinden Amazon VPC. Wenn Sie eine verwenden Amazon VPC, müssen Sie zusätzliche Berechtigungen hinzufügen.

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

Eine Vertrauensrichtlinie, Amazon Kendra mit der eine Rolle übernehmen kann.

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

IAM -Rollen für Microsoft-Exchange-Datenquellen

Wenn Sie eine Microsoft Exchange-Datenquelle verwenden, stellen Sie eine Rolle Amazon Kendra bereit, die über die erforderlichen Berechtigungen für die Verbindung mit der Website verfügt. Dazu zählen:

- Berechtigung zum Abrufen und Entschlüsseln des AWS Secrets Manager Secrets, das die Anwendungs-ID und den geheimen Schlüssel enthält, die für die Verbindung mit der Microsoft-Exchange-Website erforderlich sind. Weitere Informationen zum Inhalt des Secrets finden Sie unter Microsoft Exchange-Datenquellen.
- Berechtigung zur Verwendung der BatchPutDocument APIs und BatchDeleteDocument APIs.

> **Note**
>
> Sie können eine Microsoft-Exchange-Datenquelle Amazon Kendra über mit verbinden Amazon VPC. Wenn Sie eine verwenden Amazon VPC, müssen Sie zusätzliche Berechtigungen hinzufügen.

Die folgende IAM Richtlinie stellt die erforderlichen Berechtigungen bereit:

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

Wenn Sie die Liste der zu indizierenden Benutzer in einem - Amazon S3 Bucket speichern, müssen Sie auch die Berechtigung zur Verwendung der S3-`GetObject`Operation erteilen. Die folgende IAM Richtlinie stellt die erforderlichen Berechtigungen bereit:

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

Eine Vertrauensrichtlinie, Amazon Kendra mit der eine Rolle übernehmen kann.

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

IAM -Rollen für Microsoft- OneDrive Datenquellen

Wenn Sie eine Microsoft- OneDrive Datenquelle verwenden, stellen Sie eine Rolle Amazon Kendra bereit, die über die erforderlichen Berechtigungen für die Verbindung mit der Website verfügt. Dazu zählen:

- Berechtigung zum Abrufen und Entschlüsseln des AWS Secrets Manager Secrets, das die Anwendungs-ID und den geheimen Schlüssel enthält, die für die Verbindung mit der OneDrive Website erforderlich sind. Weitere Informationen zum Inhalt des Secrets finden Sie unter Microsoft-OneDrive Datenquellen.
- Berechtigung zur Verwendung der BatchPutDocument APIs und BatchDeleteDocument APIs.

> **Note**
>
> Sie können eine Microsoft- OneDrive Datenquelle Amazon Kendra über mit verbinden Amazon VPC. Wenn Sie eine verwenden Amazon VPC, müssen Sie zusätzliche Berechtigungen hinzufügen.

Die folgende IAM Richtlinie stellt die erforderlichen Berechtigungen bereit:

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

Wenn Sie die Liste der zu indizierenden Benutzer in einem - Amazon S3 Bucket speichern, müssen Sie auch die Berechtigung zur Verwendung der S3-`GetObject`Operation erteilen. Die folgende IAM Richtlinie stellt die erforderlichen Berechtigungen bereit:

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

Eine Vertrauensrichtlinie, Amazon Kendra mit der eine Rolle übernehmen kann.

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

IAM -Rollen für Microsoft- SharePoint Datenquellen

IAM -Rollen für SharePoint Connector v1.0

Für eine Microsoft SharePoint Connector v1.0-Datenquelle stellen Sie eine Rolle mit den folgenden Richtlinien bereit.

- Berechtigung für den Zugriff auf das AWS Secrets Manager Secret, das den Benutzernamen und das Passwort für die SharePoint Website enthält. Weitere Informationen zum Inhalt des Secrets finden Sie unter Microsoft- SharePoint Datenquellen.
- Berechtigung zur Verwendung des AWS KMS Kundenmasterschlüssels (CMK) zum Entschlüsseln des von gespeicherten Benutzernamens und Passwort-Secrets AWS Secrets Manager.

- Berechtigung zur Verwendung der `BatchDeleteDocument` Operationen `BatchPutDocument` und zum Aktualisieren des Index.
- Berechtigung für den Zugriff auf den Amazon S3 Bucket, der das SSL-Zertifikat enthält, das für die Kommunikation mit der SharePoint Website verwendet wird.

Sie müssen auch eine Vertrauensrichtlinie anfügen, die es erlaubt, die Rolle Amazon Kendra zu übernehmen.

> **Note**
>
> Sie können eine Microsoft- SharePoint Datenquelle Amazon Kendra über mit verbinden Amazon VPC. Wenn Sie eine verwenden Amazon VPC, müssen Sie zusätzliche Berechtigungen hinzufügen.

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

Wenn Sie den Amazon S3 Bucket verschlüsselt haben, der das SSL-Zertifikat enthält, das für die Kommunikation mit der SharePoint Website verwendet wurde, geben Sie eine Richtlinie an, um Amazon Kendra Zugriff auf den Schlüssel zu gewähren.

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

```
}
```

Eine Vertrauensrichtlinie, Amazon Kendra mit der eine Rolle übernehmen kann.

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

IAM -Rollen für SharePoint Connector v2.0

Für eine Microsoft SharePoint Connector v2.0-Datenquelle stellen Sie eine Rolle mit den folgenden Richtlinien bereit.

- Berechtigung für den Zugriff auf das AWS Secrets Manager Secret, das die Authentifizierungsanmeldeinformationen für die SharePoint Website enthält. Weitere Informationen zum Inhalt des Secrets finden Sie unter Microsoft- SharePoint Datenquellen.
- Berechtigung zur Verwendung des AWS KMS Kundenmasterschlüssels (CMK) zum Entschlüsseln des von gespeicherten Benutzernamens und Passwort-Secrets AWS Secrets Manager.
- Berechtigung zur Verwendung der `BatchDeleteDocument` Operationen `BatchPutDocument` und zum Aktualisieren des Index.
- Berechtigung für den Zugriff auf den Amazon S3 Bucket, der das SSL-Zertifikat enthält, das für die Kommunikation mit der SharePoint Website verwendet wird.

Sie müssen auch eine Vertrauensrichtlinie anfügen, die es erlaubt, die Rolle Amazon Kendra zu übernehmen.

> **Note**
>
> Sie können eine Microsoft- SharePoint Datenquelle Amazon Kendra über mit verbinden Amazon VPC. Wenn Sie eine verwenden Amazon VPC, müssen Sie zusätzliche Berechtigungen hinzufügen.

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

Wenn Sie den Amazon S3 Bucket verschlüsselt haben, der das SSL-Zertifikat enthält, das für die Kommunikation mit der SharePoint Website verwendet wurde, geben Sie eine Richtlinie an, um Amazon Kendra Zugriff auf den Schlüssel zu gewähren.

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

Eine Vertrauensrichtlinie, Amazon Kendra mit der eine Rolle übernehmen kann.

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

IAM -Rollen für Microsoft SQL Server-Datenquellen

Wenn Sie Microsoft SQL Server verwenden, stellen Sie eine Rolle mit den folgenden Richtlinien bereit.

- Berechtigung zum Zugriff auf Ihr AWS Secrets Manager Secret zur Authentifizierung Ihrer Microsoft SQL Server-Instance.

- Berechtigung zum Aufrufen der erforderlichen öffentlichen APIs für den Microsoft SQL Server-Konnektor.
- Berechtigung zum Aufrufen der APIs `BatchPutDocument`, `BatchDeleteDocument`, `DeletePrincipalMapping`, `PutPrincipalMappingDescribePrincipalMapping`, und `ListGroupsOlderThanOrderingId` APIs.

> **Note**
>
> Sie können eine Microsoft SQL Server-Datenquelle Amazon Kendra über mit verbinden Amazon VPC. Wenn Sie eine verwenden Amazon VPC, müssen Sie zusätzliche Berechtigungen hinzufügen.

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

Eine Vertrauensrichtlinie, Amazon Kendra mit der eine Rolle übernehmen kann.

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

IAM -Rollen für Microsoft Teams-Datenquellen

Wenn Sie eine Microsoft Teams-Datenquelle verwenden, stellen Sie eine Rolle Amazon Kendra bereit, die über die erforderlichen Berechtigungen für die Verbindung mit der Website verfügt. Dazu zählen:

- Berechtigung zum Abrufen und Entschlüsseln des AWS Secrets Manager Secrets, das die Client-ID und das Client-Secret enthält, die für die Verbindung mit Microsoft Teams erforderlich sind. Weitere Informationen zum Inhalt des Secrets finden Sie unter Microsoft Teams-Datenquellen.

> **Note**
>
> Sie können eine Microsoft Teams-Datenquelle Amazon Kendra über mit verbinden Amazon VPC. Wenn Sie eine verwenden Amazon VPC, müssen Sie zusätzliche Berechtigungen hinzufügen.

Die folgende IAM Richtlinie stellt die erforderlichen Berechtigungen bereit:

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

Eine Vertrauensrichtlinie, Amazon Kendra mit der eine Rolle übernehmen kann.

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

IAM -Rollen für Microsoft-Yammer-Datenquellen

Wenn Sie eine Microsoft-Yammer-Datenquelle verwenden, stellen Sie eine Rolle Amazon Kendra bereit, die über die erforderlichen Berechtigungen für die Verbindung mit der Website verfügt. Dazu zählen:

- Berechtigung zum Abrufen und Entschlüsseln des AWS Secrets Manager Secrets, das die Anwendungs-ID und den geheimen Schlüssel enthält, die für die Verbindung mit der Microsoft-Yammer-Website erforderlich sind. Weitere Informationen zum Inhalt des Secrets finden Sie unter Microsoft-Yammer-Datenquellen.
- Berechtigung zur Verwendung der BatchPutDocument APIs und BatchDeleteDocument APIs.

> **Note**
>
> Sie können eine Microsoft-Yammer-Datenquelle Amazon Kendra über mit verbinden Amazon VPC. Wenn Sie eine verwenden Amazon VPC, müssen Sie zusätzliche Berechtigungen hinzufügen.

Die folgende IAM Richtlinie stellt die erforderlichen Berechtigungen bereit:

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

Wenn Sie die Liste der zu indizierenden Benutzer in einem - Amazon S3 Bucket speichern, müssen Sie auch die Berechtigung zur Verwendung der S3-`GetObject`Operation erteilen. Die folgende IAM Richtlinie stellt die erforderlichen Berechtigungen bereit:

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

Eine Vertrauensrichtlinie, Amazon Kendra mit der eine Rolle übernehmen kann.

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

IAM -Rollen für MySQL-Datenquellen

Wenn Sie einen My SQL-Datenquellen-Konnektor verwenden, stellen Sie eine Rolle mit den folgenden Richtlinien bereit.

- Berechtigung zum Zugriff auf Ihr AWS Secrets Manager Secret zur Authentifizierung Ihrer My SQL-Datenquellen-Instance.
- Berechtigung zum Aufrufen der erforderlichen öffentlichen APIs für den My SQL-Datenquellen-Konnektor.
- Berechtigung zum Aufrufen der APIs `BatchPutDocument`, `BatchDeleteDocument`, `DeletePrincipalMapping`, `PutPrincipalMappingDescribePrincipalMapping`, und `ListGroupsOlderThanOrderingId` APIs.

> **Note**
>
> Sie können eine MySQL-Datenquelle Amazon Kendra über mit verbinden Amazon VPC. Wenn Sie eine verwenden Amazon VPC, müssen Sie zusätzliche Berechtigungen hinzufügen.

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

Eine Vertrauensrichtlinie, Amazon Kendra mit der eine Rolle übernehmen kann.

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

IAM -Rollen für Oracle-Datenquellen

Wenn Sie einen Oracle-Datenquellen-Konnektor verwenden, stellen Sie eine Rolle mit den folgenden Richtlinien bereit.

- Berechtigung zum Zugriff auf Ihr AWS Secrets Manager Secret zur Authentifizierung Ihrer Oracle-Datenquellen-Instance.
- Berechtigung zum Aufrufen der erforderlichen öffentlichen APIs für den Oracle-Datenquellen-Konnektor.
- Berechtigung zum Aufrufen der APIs `BatchPutDocument`, `BatchDeleteDocument`, `DeletePrincipalMapping`, `PutPrincipalMappingDescribePrincipalMapping`, und `ListGroupsOlderThanOrderingId` APIs.

> **Note**
>
> Sie können eine Oracle-Datenquelle Amazon Kendra über mit verbinden Amazon VPC. Wenn Sie eine verwenden Amazon VPC, müssen Sie zusätzliche Berechtigungen hinzufügen.

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

Eine Vertrauensrichtlinie, Amazon Kendra mit der eine Rolle übernehmen kann.

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

IAM -Rollen für PostgreSQL-Datenquellen

Wenn Sie einen PostgreSQL-Datenquellen-Konnektor verwenden, stellen Sie eine Rolle mit den folgenden Richtlinien bereit.

- Berechtigung zum Zugriff auf Ihr AWS Secrets Manager Secret zur Authentifizierung Ihrer PostgreSQL-Datenquellen-Instance.
- Berechtigung zum Aufrufen der erforderlichen öffentlichen APIs für den PostgreSQL-Datenquellen-Konnektor.
- Berechtigung zum Aufrufen der APIs `BatchPutDocument`, `BatchDeleteDocument`, `DeletePrincipalMapping`, `PutPrincipalMappingDescribePrincipalMapping`, und `ListGroupsOlderThanOrderingId` APIs.

> **Note**
>
> Sie können eine PostgreSQL-Datenquelle Amazon Kendra über mit verbinden Amazon VPC. Wenn Sie eine verwenden Amazon VPC, müssen Sie zusätzliche Berechtigungen hinzufügen.

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

Eine Vertrauensrichtlinie, Amazon Kendra mit der eine Rolle übernehmen kann.

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

IAM -Rollen für Quip-Datenquellen

Wenn Sie Quip verwenden, geben Sie eine Rolle mit den folgenden Richtlinien an.

- Berechtigung zum Zugriff auf Ihr AWS Secrets Manager Secret zur Authentifizierung Ihrer Warteschlange.
- Berechtigung zum Aufrufen der erforderlichen öffentlichen APIs für den Quip-Konnektor.
- Berechtigung zum Aufrufen der APIs `BatchPutDocument`, `BatchDeleteDocument`, `DeletePrincipalMapping`, `PutPrincipalMappingDescribePrincipalMapping`, und `ListGroupsOlderThanOrderingId` APIs.

> **Note**
>
> Sie können eine Quip-Datenquelle Amazon Kendra über mit verbinden Amazon VPC. Wenn Sie eine verwenden Amazon VPC, müssen Sie zusätzliche Berechtigungen hinzufügen.

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

Eine Vertrauensrichtlinie, Amazon Kendra mit der eine Rolle übernehmen kann.

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

IAM -Rollen für Salesforce-Datenquellen

Wenn Sie Salesforce als Datenquelle verwenden, stellen Sie eine Rolle mit den folgenden Richtlinien bereit:

- Berechtigung für den Zugriff auf das AWS Secrets Manager Secret, das den Benutzernamen und das Passwort für die Salesforce-Website enthält. Weitere Informationen zum Inhalt des Secrets finden Sie unter Salesforce-Datenquellen.
- Berechtigung zur Verwendung des AWS KMS Kundenmasterschlüssels (CMK) zum Entschlüsseln des von gespeicherten Benutzernamens und Passwort-Secrets Secrets Manager.
- Berechtigung zur Verwendung der `BatchDeleteDocument` Operationen `BatchPutDocument` und zum Aktualisieren des Index.

> **Note**
>
> Sie können eine Salesforce-Datenquelle Amazon Kendra über mit verbinden Amazon VPC. Wenn Sie eine verwenden Amazon VPC, müssen Sie zusätzliche Berechtigungen hinzufügen.

```
{
  "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"
```

```
  }]
}
```

Eine Vertrauensrichtlinie, Amazon Kendra mit der eine Rolle übernehmen kann.

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

IAM -Rollen für ServiceNow Datenquellen

Wenn Sie einen ServiceNow als Datenquelle verwenden, stellen Sie eine Rolle mit den folgenden Richtlinien bereit:

- Berechtigung für den Zugriff auf das Secrets Manager Secret, das den Benutzernamen und das Passwort für die ServiceNow Website enthält. Weitere Informationen zum Inhalt des Secrets finden Sie unter ServiceNow Datenquellen .
- Berechtigung zur Verwendung des AWS KMS Kundenmasterschlüssels (CMK) zum Entschlüsseln des von gespeicherten Benutzernamens und Passwort-Secrets Secrets Manager.
- Berechtigung zur Verwendung der `BatchDeleteDocument` Operationen `BatchPutDocument` und zum Aktualisieren des Index.

> **Note**
>
> Sie können eine ServiceNow Datenquelle Amazon Kendra über mit verbinden Amazon VPC. Wenn Sie eine verwenden Amazon VPC, müssen Sie zusätzliche Berechtigungen hinzufügen.

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

Eine Vertrauensrichtlinie, Amazon Kendra mit der eine Rolle übernehmen kann.

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

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

IAM -Rollen für Slack-Datenquellen

Wenn Sie Slack verwenden, geben Sie eine Rolle mit den folgenden Richtlinien an.

- Berechtigung zum Zugriff auf Ihr AWS Secrets Manager Secret zur Authentifizierung Ihres Slack.
- Berechtigung zum Aufrufen der erforderlichen öffentlichen APIs für den Slack-Konnektor.
- Berechtigung zum Aufrufen der APIs `BatchPutDocument`, `BatchDeleteDocument`, `DeletePrincipalMapping`, `PutPrincipalMappingDescribePrincipalMapping`, und `ListGroupsOlderThanOrderingId` APIs.

> **Note**
>
> Sie können eine Slack-Datenquelle Amazon Kendra über mit verbinden Amazon VPC. Wenn Sie eine verwenden Amazon VPC, müssen Sie zusätzliche Berechtigungen hinzufügen.

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

Eine Vertrauensrichtlinie, Amazon Kendra mit der eine Rolle übernehmen kann.

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

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

IAM -Rollen für Zendesk-Datenquellen

Wenn Sie Zendesk verwenden, geben Sie eine Rolle mit den folgenden Richtlinien an.

- Berechtigung zum Zugriff auf Ihr AWS Secrets Manager Secret zur Authentifizierung Ihrer Zendesk Suite.
- Berechtigung zum Aufrufen der erforderlichen öffentlichen APIs für den Zendesk-Konnektor.
- Berechtigung zum Aufrufen der APIs `BatchPutDocument`, `BatchDeleteDocument`, `DeletePrincipalMapping`, `PutPrincipalMappingDescribePrincipalMapping`, und `ListGroupsOlderThanOrderingId` APIs.

> **Note**
>
> Sie können eine Zendesk-Datenquelle Amazon Kendra über mit verbinden Amazon VPC. Wenn Sie eine verwenden Amazon VPC, müssen Sie zusätzliche Berechtigungen hinzufügen.

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

Eine Vertrauensrichtlinie, Amazon Kendra mit der eine Rolle übernehmen kann.

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

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

Virtual Private Cloud (VPC)- IAM Rolle

Wenn Sie eine Virtual Private Cloud (VPC) verwenden, um eine Verbindung zu Ihrer Datenquelle herzustellen, müssen Sie die folgenden zusätzlichen Berechtigungen bereitstellen.

VPC- IAM Rolle

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

Eine Vertrauensrichtlinie, Amazon Kendra mit der eine Rolle übernehmen kann.

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

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

IAM -Rollen für häufig gestellte Fragen (FAQs)

Wenn Sie die CreateFaq-API verwenden, um Fragen und Antworten in einen Index zu laden, müssen Sie eine - IAM Rolle Amazon Kendra mit Zugriff auf den Amazon S3 Bucket bereitstellen, der die Quelldateien enthält. Wenn die Quelldateien verschlüsselt sind, müssen Sie die Berechtigung erteilen, den AWS KMS Kundenmasterschlüssel (CMK) zum Entschlüsseln der Dateien zu verwenden.

IAM -Rollen für FAQs Fragen

Eine erforderliche Rollenrichtlinie, um den Zugriff auf einen Amazon S3 -Bucket Amazon Kendra zu ermöglichen.

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

Eine optionale Rollenrichtlinie, die es ermöglicht Amazon Kendra , einen AWS KMS - Kundenmasterschlüssel (CMK) zum Entschlüsseln von Dateien in einem - Amazon S3 Bucket zu verwenden.

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

Eine Vertrauensrichtlinie, Amazon Kendra mit der eine Rolle übernehmen kann.

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

IAM -Rollen für Abfragevorschläge

Wenn Sie eine - Amazon S3 Datei als Blockliste für Abfragevorschläge verwenden, geben Sie eine Rolle an, die über die Berechtigung für den Zugriff auf die Amazon S3 Datei und den Amazon S3

Bucket verfügt. Wenn die Blocklistentextdatei (die - Amazon S3 Datei) im Bucket verschlüsselt ist, müssen Sie die Amazon S3 Berechtigung erteilen, den AWS KMS Kundenmasterschlüssel (CMK) zum Entschlüsseln der Dokumente zu verwenden.

IAM -Rollen für Abfragevorschläge

Eine erforderliche Rollenrichtlinie, damit die Amazon Kendra - Amazon S3 Datei als Blockliste für Abfragevorschläge verwenden kann.

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

Eine optionale Rollenrichtlinie, die es ermöglicht Amazon Kendra , einen AWS KMS - Kundenmasterschlüssel (CMK) zum Entschlüsseln von Dokumenten in einem - Amazon S3 Bucket zu verwenden.

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

Eine Vertrauensrichtlinie, Amazon Kendra mit der eine Rolle übernehmen kann.

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

IAM -Rollen für die Prinzipalzuordnung von Benutzern und Gruppen

Wenn Sie die PutPrincipalMapping-API verwenden, um Benutzer ihren Gruppen zum Filtern von Suchergebnissen nach Benutzerkontext zuzuordnen, müssen Sie eine Liste der Benutzer oder Untergruppen bereitstellen, die zu einer Gruppe gehören. Wenn Ihre Liste mehr als 1000 Benutzer oder Untergruppen für eine Gruppe umfasst, müssen Sie eine Rolle bereitstellen, die über die Berechtigung zum Zugriff auf die Amazon S3 Datei Ihrer Liste und des Amazon S3 Buckets verfügt. Wenn die Textdatei (die Amazon S3 -Datei) der Liste im Amazon S3 Bucket verschlüsselt ist, müssen Sie die Berechtigung erteilen, den AWS KMS Kundenmasterschlüssel (CMK) zum Entschlüsseln der Dokumente zu verwenden.

IAM -Rollen für die Prinzipalzuordnung

Eine erforderliche Rollenrichtlinie Amazon Kendra , damit die Amazon S3 Datei als Liste der Benutzer und Untergruppen verwenden kann, die zu einer Gruppe gehören.

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

```
            ]
        }
    ]
}
```

Eine optionale Rollenrichtlinie, die es ermöglicht Amazon Kendra , einen AWS KMS - Kundenmasterschlüssel (CMK) zum Entschlüsseln von Dokumenten in einem - Amazon S3 Bucket zu verwenden.

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

Eine Vertrauensrichtlinie, Amazon Kendra mit der eine Rolle übernehmen kann.

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

Es wird empfohlen, dass Sie `aws:sourceAccount` und `aws:sourceArn` in die Vertrauensrichtlinie aufnehmen. Dadurch `aws:sourceArn` werden Berechtigungen eingeschränkt und sicher überprüft, ob `aws:sourceAccount` und mit denen in der IAM Rollenrichtlinie für die `sts:AssumeRole` Aktion

übereinstimmen. Dadurch wird verhindert, dass nicht autorisierte Entitäten auf Ihre IAM Rollen und deren Berechtigungen zugreifen. Weitere Informationen finden Sie im AWS Identity and Access Management Leitfaden zum Confused-Deputy-Problem .

```
{
    "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 -Rollen für AWS IAM Identity Center

Wenn Sie das -UserGroupResolutionConfigurationObjekt verwenden, um Zugriffsebenen von Gruppen und Benutzern aus einer AWS IAM Identity Center Identitätsquelle abzurufen, müssen Sie eine Rolle bereitstellen, die über die Berechtigung für den Zugriff auf verfügt IAM Identity Center.

IAM -Rollen für AWS IAM Identity Center

Eine erforderliche Rollenrichtlinie, um den Zugriff auf Amazon Kendra zu ermöglichen 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"
              ]
            }
          }
        }
    ]
}
```

Eine Vertrauensrichtlinie, Amazon Kendra mit der eine Rolle übernehmen kann.

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

```
}
```

IAM -Rollen für - Amazon Kendra Erlebnisse

Wenn Sie die CreateExperience oder UpdateExperience APIs verwenden, um eine Suchanwendung zu erstellen oder zu aktualisieren, müssen Sie eine Rolle bereitstellen, die über die Berechtigung für den Zugriff auf die erforderlichen Operationen und IAM Identity Center verfügt.

IAM -Rollen für die Amazon Kendra Sucherfahrung

Eine erforderliche Rollenrichtlinie, um Amazon Kendra den Zugriff auf `Query` -Operationen, -`QuerySuggestions`Operationen, -`SubmitFeedback`Operationen und IAM Identity Center zu ermöglichen, das Ihre Benutzer- und Gruppeninformationen speichert.

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

Eine Vertrauensrichtlinie, Amazon Kendra mit der eine Rolle übernehmen kann.

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

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

Es wird empfohlen, dass Sie `aws:sourceAccount` und `aws:sourceArn` in die Vertrauensrichtlinie aufnehmen. Dadurch `aws:sourceArn` werden Berechtigungen eingeschränkt und sicher überprüft, ob `aws:sourceAccount` und mit denen in der IAM Rollenrichtlinie für die `sts:AssumeRole` Aktion übereinstimmen. Dadurch wird verhindert, dass nicht autorisierte Entitäten auf Ihre IAM Rollen und deren Berechtigungen zugreifen. Weitere Informationen finden Sie im AWS Identity and Access Management Leitfaden zum Confused-Deputy-Problem .

```
{
    "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 -Rollen für die Anreicherung benutzerdefinierter Dokumente

Wenn Sie das -CustomDocumentEnrichmentConfigurationObjekt verwenden, um erweiterte Änderungen an Ihren Dokumentmetadaten und -inhalten vorzunehmen, müssen Sie eine Rolle bereitstellen, die über die erforderlichen Berechtigungen zum Ausführen von

`PreExtractionHookConfiguration` und/oder verfügt`PostExtractionHookConfiguration`. Sie konfigurieren eine Lambda-Funktion für `PreExtractionHookConfiguration` und/oder `PostExtractionHookConfiguration`, um während des Erfassungsprozesses erweiterte Änderungen an Ihren Dokumentmetadaten und -inhalten vorzunehmen. Wenn Sie die serverseitige Verschlüsselung für Ihren Amazon S3 Bucket aktivieren möchten, müssen Sie die Berechtigung erteilen, den AWS KMS -Kundenmasterschlüssel (CMK) zum Verschlüsseln und Entschlüsseln der in Ihrem Amazon S3 Bucket gespeicherten Objekte zu verwenden.

IAM -Rollen für die Anreicherung benutzerdefinierter Dokumente

Eine erforderliche Rollenrichtlinie, damit `PreExtractionHookConfiguration` und `PostExtractionHookConfiguration` mit Verschlüsselung für Ihren Amazon S3 Bucket Amazon Kendra ausführen kann.

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

Eine optionale Rollenrichtlinie, Amazon Kendra mit der `PreExtractionHookConfiguration` und `PostExtractionHookConfiguration` ohne Verschlüsselung für Ihren Amazon S3 Bucket ausgeführt werden können.

```
{
  "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"
```

```
  }]
}
```

Eine Vertrauensrichtlinie, Amazon Kendra mit der eine Rolle übernehmen kann.

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

Es wird empfohlen, dass Sie `aws:sourceAccount` und `aws:sourceArn` in die Vertrauensrichtlinie aufnehmen. Dadurch `aws:sourceArn` werden Berechtigungen eingeschränkt und sicher überprüft, ob `aws:sourceAccount` und mit denen in der IAM Rollenrichtlinie für die `sts:AssumeRole` Aktion übereinstimmen. Dadurch wird verhindert, dass nicht autorisierte Entitäten auf Ihre IAM Rollen und deren Berechtigungen zugreifen. Weitere Informationen finden Sie im AWS Identity and Access Management Leitfaden zum Confused-Deputy-Problem .

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

Bereitstellen von Amazon Kendra

Wenn es an der Zeit ist, sie bereitzustellenAmazon KendraWenn Sie auf Ihrer Website suchen, stellen wir Quellcode zur Verfügung, den Sie mit React verwenden können, um Ihrer Anwendung einen Vorsprung zu verschaffen. Der Quellcode wird kostenlos unter einer modifizierten MIT-Lizenz bereitgestellt. Sie können auch das Tutorial in ansehen. Die mitgelieferte React-App ist ein Beispiel für den Einstieg. Es ist keine produktionsreife App.

Informationen zum Bereitstellen einer Suchanwendung ohne Code und zum Generieren einer Endpunkt-URL zu Ihrer Suchseite mit Zugriffskontrolle finden Sie unterAmazon KendraErstelle das Tutorial.

Der folgende Beispielcode fügtAmazon Kendrasuche nach einer vorhandenen React-Webanwendung:

- https://kendrasamples.s3.amazonaws.com/kendrasamples-react-app.zip—Beispieldateien, mit denen Entwickler ein funktionales Sucherlebnis in ihre bestehende React-Webanwendung integrieren können.

Die Beispiele sind der Suchseite des nachempfundenAmazon KendraKonsole. Sie haben dieselben Funktionen zum Suchen und Anzeigen von Suchergebnissen. Sie können das gesamte Beispiel verwenden oder Sie können nur eine der Funktionen für Ihren eigenen Gebrauch auswählen.

Um die drei Komponenten der Suchseite in derAmazon KendraKonsole, wählen Sie das Codesymbol (</>) aus dem rechten Menü. Bewegen Sie den Mauszeiger über die einzelnen Abschnitte, um eine kurze Beschreibung der Komponente und die URL der Quelle der Komponente anzuzeigen.

Themen

- Komponente „Paginierung“
- Aufbau eines Sucherlebnisses ohne Code

Übersicht

Sie fügen den Beispielcode zu einer vorhandenen React-Webanwendung hinzu, um die Suche zu aktivieren. Der Beispielcode enthält eine Readme-Datei mit Schritten zum Einrichten einer neuen React-Entwicklungsumgebung. Die Beispieldaten im Codebeispiel können verwendet werden, um eine Suche zu demonstrieren. Die Suchdateien und Komponenten im Beispielcode sind wie folgt strukturiert:

- Hauptsuchseite (`Search.tsx`) — Dies ist die Hauptseite, die alle Komponenten enthält. Hier integrieren Sie Ihre Anwendung inAmazon KendraAPI.
- Suchleiste — Dies ist die Komponente, in der ein Benutzer einen Suchbegriff eingibt und die Suchfunktion aufruft.
- Ergebnisse — Dies ist die Komponente, die die Ergebnisse von anzeigtAmazon Kendra. Es besteht aus drei Komponenten: Antwortvorschläge, FAQ-Ergebnisse und empfohlene Dokumente.
- Facetten — Dies ist die Komponente, die die Facetten in den Suchergebnissen anzeigt und es Ihnen ermöglicht, eine Facette auszuwählen, um die Suche einzugrenzen.
- Paginierung — Dies ist die Komponente, die die Antwort paginiertAmazon Kendra.

Voraussetzungen

Bevor Sie beginnen, muss Folgendes sichergestellt sein:

- Node.js und npminstalliert. Node.js Version 19 oder älter ist erforderlich.
- Python 3 oder Python 2heruntergeladen und installiert.
- SDK for JavaoderAWS SDK for JavaScriptum API-Aufrufe in ansehen.Amazon Kendra.
- Eine bestehende React-Webanwendung. Der Beispielcode enthält eine Readme-Datei mit Schritten zum Einrichten einer neuen React-Entwicklungsumgebung, einschließlich der Verwendung der erforderlichen Frameworks/Bibliotheken. Sie können auch das Tutorial in ansehen.React-Dokumentation zur Erstellung einer React-Web-App.
- Die erforderlichen Bibliotheken und Abhängigkeiten, die in Ihrer Entwicklungsumgebung konfiguriert sind. Der Beispielcode enthält eine Readme-Datei, in der die erforderlichen Bibliotheken und Paketabhängigkeiten aufgeführt sind. Beachten Sie, dass`sass`ist erforderlich,

danode-sassist nicht mehr in ansehen. Wenn Sie zuvor installiert habennode-sass, deinstalliere das und installieresass.

Das Beispiel in ansehen.

Ein vollständiges Verfahren zum HinzufügenAmazon KendraDie Suche nach einer React-Anwendung ist in der Readme-Datei enthalten, die im Codebeispiel enthalten ist.

Um das Tutorial in ansehen kendrasamples-react-app.zip

1. Sie können auch das ansehen.Voraussetzungen, einschließlich des Herunterladens und der Installation von Node.js und npm.
2. Herunterladen kendrasamples-react-app.zip und entpacken.
3. Öffne dein Terminal und gehe zuaws-kendra-example-react-app/src/services/. Öffnenlocal-dev-credentials.jsonund geben Sie auch das Tutorial in ansehen. Sie können auch das Tutorial in ansehen.
4. Gehe zuaws-kendra-example-react-appund installiere die Abhängigkeiten inpackage.json. Führen Sie `npm install`.
5. Sie können auch das Tutorial in ansehen. Führen Sie `npm start`. Sie können den lokalen Server beenden, indem Sie auf Ihrer Tastatur etwas eingebenCmd/Ctrl + C.
6. Sie können den Port oder den Host (z. B. die IP-Adresse) ändern, indem Sie zupackage.jsonund aktualisieren Sie den Host und den Port:`"start": "HOST=[host] PORT=[port] react-scripts start"`. Wenn Sie Windows verwenden:`"start": "set HOST=[host] && set PORT=[port] && react-scripts start"`.
7. Wenn Sie eine registrierte Website-Domain haben, können Sie dies in angebenpackage.jsonnach auch das App-Name. Zum Beispiel `"homepage": "https://mywebsite.com"`. Du musst rennen`npm install`erneut, um neue Abhängigkeiten zu aktualisieren, und dann ausführen`npm start`.
8. Um die App zu erstellen, führe folgenden Befehl aus`npm build`. Laden Sie den Inhalt des Build-Verzeichnisses auf Ihren Hosting-Anbieter hoch.

> **Warning**
>
> Die React-App istnichtbereit für die Produktion. Es ist ein Beispiel für die Bereitstellung einer App fürAmazon Kendrasuchen.

Haupt-Suchseite

Die Hauptsuchseite (`Search.tsx`) enthält alle Beispiel-Suchkomponenten. Es enthält die Suchleistenkomponente für die Ausgabe, die Ergebniskomponenten zur Anzeige der Antwort vonAbfrageAPI und eine Paginierungskomponente zum Durchblättern der Antwort.

Komponente ansehen

Die Suchkomponente bietet ein Textfeld zur Eingabe von Abfragetext. Dieon`Search`Funktion ist ein Hook, der die Hauptfunktion aufruft in`Search.tsx`um dasAmazon Kendra AbfrageAPI-Aufruf.

Komponente „Ergebnisse“

Die Ergebniskomponente zeigt die Antwort von`Query`API. Die Ergebnisse werden in drei separaten Bereichen angezeigt.

- Vorgeschlagene Antworten — Dies sind die besten Ergebnisse, die von`Query`API. Es enthält bis zu drei Antwortvorschläge. In der Antwort haben sie den Ergebnistyp`ANSWER`.
- Antworten auf häufig gestellte Fragen — Dies sind die Ergebnisse der Antwort auf häufig gestellte Fragen. Häufig gestellte Fragen werden dem Index separat hinzugefügt. In der Antwort haben sie den Typ`QUESTION_ANSWER`. Weitere Informationen finden Sie unterFragen und Antworten.
- Empfohlene Dokumente — Dies sind zusätzliche Dokumente, dieAmazon Kendragibt in auch das Tutorial in ansehen. In der Antwort von`Query`API, sie haben den Typ`DOCUMENT`.

Die Ergebniskomponenten teilen sich eine Reihe von Komponenten für Funktionen wie Hervorhebungen, Titel, Links und mehr. Die gemeinsam genutzten Komponenten müssen vorhanden sein, damit die Ergebniskomponenten funktionieren.

Komponente „Facetten“

Die Facettenkomponente listet die in den Suchergebnissen verfügbaren Facetten auf. Jede Facette klassifiziert die Antwort nach einer bestimmten Dimension, z. B. nach dem Autor. Sie können die Suche auf eine bestimmte Facette eingrenzen, indem Sie eine Facette aus der Liste auswählen.

Nachdem Sie eine Facette ausgewählt haben, ruft die Komponente auf`Query`mit einem Attributfilter, der die Suche auf Dokumente beschränkt, die der Facette entsprechen.

Komponente „Paginierung“

Mit der Paginierungskomponente können Sie die Suchergebnisse aus dem anzeigen`Query`API auf mehreren Seiten. Es ruft die`Query`API mit dem`PageSize`und`PageNumber`Parameter, um eine bestimmte Ergebnisseite zu erhalten.

Aufbau eines Sucherlebnisses ohne Code

Sie können eine erstellen und bereitstellenAmazon KendraSuchanwendung, ohne dass Frontend-Code erforderlich ist.Amazon Kendra Erstelle das Tutorialhilft Ihnen dabei, mit wenigen Klicks eine voll funktionsfähige Suchanwendung zu erstellen und bereitzustellen, sodass Sie sofort mit der Suche beginnen können. Sie können Ihre Suchseite individuell gestalten und Ihre Suche optimieren, um das Erlebnis an die Bedürfnisse Ihrer Benutzer anzupassen.Amazon Kendrageneriert eine eindeutige, vollständig gehostete Endpunkt-URL Ihrer Suchseite, um mit der Suche in Ihren Dokumenten und häufig gestellten Fragen zu beginnen. Sie können schnell einen Machbarkeitsnachweis für Ihr Sucherlebnis erstellen und ihn mit anderen teilen.

Sie verwenden die im Builder verfügbare Vorlage für Sucherlebnisse, um Ihre Suche anzupassen. Sie können andere einladen, gemeinsam an der Gestaltung Ihres Sucherlebnisses zu arbeiten, oder die Suchergebnisse zu Optimierungszwecken auswerten. Sobald Ihr Sucherlebnis bereit ist, damit Ihre Benutzer mit der Suche beginnen können, geben Sie einfach die URL des sicheren Endpunkts weiter.

So funktioniert die Suche — Experience Builder

Der Gesamtprozess beim Aufbau eines Sucherlebnisses sieht wie folgt aus:

1. Sie erstellen Ihr Sucherlebnis, indem Sie ihm einen Namen und eine Beschreibung geben und Ihre Datenquellen auswählen, die Sie für Ihr Sucherlebnis verwenden möchten.
2. Sie können auch das Tutorial in ansehen.AWS IAM Identity Centerund weisen Sie ihnen dann Zugriffsrechte für Ihr Sucherlebnis zu. Sie beziehen sich selbst als Eigentümer des Erlebnisses ein. Weitere Informationen finden Sie unter the section called “Sie können auch das Tutorial in ansehen.”.
3. Sie können auch das ansehen.Amazon KendraExperience Builder zum Entwerfen und Optimieren Ihrer Suchseite. Sie können Ihre Endpunkt-URL Ihres Sucherlebnisses mit anderen teilen, denen Sie eigene Zugriffsrechte zum Bearbeiten oder zum Anzeigen von Suchvorgängen zuweisen.

Sie rufen denCreateExperienceAPI zur Erstellung und Konfiguration Ihres Sucherlebnisses. Wenn Sie die Konsole verwenden, wählen Sie Ihren Index aus und wählen dannErlebnissein das Navigationsmenü ansehen.

Gestalten und optimieren Sie Ihr Sucherlebnis

Sobald Sie Ihr Sucherlebnis erstellt und konfiguriert haben, öffnen Sie das Sucherlebnis mithilfe einer Endpunkt-URL, um als Eigentümer mit Editor-Zugriffsrechten mit der Anpassung Ihrer Suche zu beginnen. Sie geben Ihre Suchanfrage in das Suchfeld ein und passen dann Ihre Suche mithilfe der Bearbeitungsoptionen im Seitenbereich an, um zu sehen, wie sie auf Ihre Seite zutreffen. Wenn Sie das Tutorial in ansehen.Veröffentlichen. Sie können auch das Tutorial in ansehen.Zur Live-Ansicht ansehen, um die neueste veröffentlichte Version Ihrer Suchseite zu sehen, undIn das Build-Modus ansehen, um Ihre Suchseite zu bearbeiten oder anzupassen.

Im Folgenden finden Sie Möglichkeiten, wie Sie Ihr Sucherlebnis anpassen können.

Filter

Fügen Sie eine facettierte Suche hinzu oder filtern Sie nach Dokumentattributen. Sie können auch das Tutorial in ansehen. Sie können mithilfe Ihrer eigenen konfigurierten Metadatenfelder einen Filter hinzufügen. Um beispielsweise eine Facettensuche nach jeder Stadtkategorie durchzuführen, verwenden Sie`_category`benutzerdefiniertes Dokumentattribut, das alle Stadtkategorien enthält.

Vorgeschlagene Antwort

Fügen Sie durch maschinelles Lernen generierte Antworten auf die Fragen Ihrer Benutzer hinzu. Sie können auch das ansehen.„Wie schwierig ist dieser Kurs?“.Amazon Kendrakann aus allen Dokumenten, die sich auf den Schwierigkeitsgrad eines Kurses beziehen, den relevantesten Text abrufen und die relevanteste Antwort vorschlagen.

Häufig gestellte Fragen

Fügen Sie ein FAQ-Dokument hinzu, um Antworten auf häufig gestellte Fragen zu geben. Sie können auch das ansehen.„Wie viele Stunden muss ich für diesen Kurs absolvieren?“.Amazon Kendrakann das FAQ-Dokument mit der Antwort auf diese Frage verwenden und die richtige Antwort geben.

Sortierung

Fügen Sie eine Sortierung der Suchergebnisse hinzu, sodass Ihre Benutzer die Ergebnisse nach Relevanz, Erstellungszeit, Uhrzeit der letzten Aktualisierung und anderen Sortierkriterien organisieren können.

-Documents

Konfigurieren Sie, wie Dokumente oder Suchergebnisse auf Ihrer Suchseite angezeigt werden. Sie können konfigurieren, wie viele Ergebnisse auf der Seite angezeigt werden, Seitennummerierung wie Seitenzahlen einbeziehen, eine Schaltfläche für Benutzerfeedback aktivieren und festlegen, wie Metadatenfelder von Dokumenten in Suchergebnissen angezeigt werden.

Sprache

Wählen Sie eine Sprache aus, um die Suchergebnisse oder Dokumente in der ausgewählten Sprache zu filtern.

Suchfeld

Konfigurieren Sie die Größe und den Platzhaltertext Ihres Suchfeldes und lassen Sie Abfragevorschläge zu.

Abstimmung der Relevanz

Fügen Sie den Metadatenfeldern von Dokumenten eine Erhöhung hinzu, um diesen Feldern mehr Gewicht zu verleihen, wenn Ihre Benutzer nach Dokumenten suchen. Sie können eine Gewichtung hinzufügen, die bei 1 beginnt und schrittweise auf 10 erhöht wird. Sie können die Feldtypen Text, Datum und Zahl erhöhen. Zum Beispiel um zu geben`_last_updated_at`und`_created_at`mehr Gewicht oder Wichtigkeit als andere Felder, geben Sie diesen Feldern je nach Wichtigkeit eine Gewichtung von 1 bis 10. Sie können für jede Suchanwendung oder jedes Erlebnis unterschiedliche Konfigurationen zur Relevanzoptimierung anwenden.

Sie können auch das Tutorial in ansehen.

Der Zugriff auf Ihr Sucherlebnis erfolgt über das IAM Identity Center. Wenn Sie Ihr Sucherlebnis konfigurieren, gewähren Sie anderen Personen, die in Ihrem Identity Center-Verzeichnis aufgeführt sind, Zugriff auf IhrAmazon KendraSuchseite. Sie erhalten eine E-Mail, in der sie aufgefordert werden, sich mit ihren Anmeldeinformationen im IAM Identity Center anzumelden, um auf die Suchseite zuzugreifen. Sie müssen IAM Identity Center auf Organisations- oder Kontoinhaberebene einrichten inAWS Organizations. Weitere Informationen zur Einrichtung von IAM Identity Center finden Sie unterErste Schritte mit IAM Identity Center.

Sie aktivieren Benutzeridentitäten im IAM Identity Center mit Ihrer Sucherfahrung und weisen sie zuZuschaueroderBesitzerZugriffsberechtigungen über die API oder die Konsole.

- Zuschauer: Erlaubt es, Fragen zu stellen, Antwortvorschläge zu erhalten, die für ihre Suche relevant sind, und ihr Feedback dazu beizutragenAmazon Kendradamit die Suche weiter verbessert wird.
- Besitzer: Erlaubt es, das Design der Suchseite anzupassen, die Suche zu optimieren und die Suchanwendung alsZuschauer. Das Deaktivieren des Zugriffs auf Zuschauer in der Konsole wird derzeit nicht unterstützt.

Um anderen Personen Zugriff auf Ihr Sucherlebnis zuzuweisen, aktivieren Sie zunächst Benutzeridentitäten im IAM Identity Center mit IhremAmazon Kendraerleben Sie mit demExperienceConfigurationObjekt. Sie geben den Feldnamen an, der die Identifikatoren Ihrer Benutzer wie Benutzername oder E-Mail-Adresse enthält. Anschließend gewähren Sie Ihrer Benutzerliste Zugriff auf Ihr Sucherlebnis mithilfe derAssociateEntitiesToExperienceAPI und definieren Sie ihre Berechtigungen alsZuschaueroderBesitzerunter Verwendung derAssociatePersonasToEntitiesAPI. Sie spezifizieren jeden Benutzer oder jede Gruppe mit demEntityConfigurationObjekt und ob es sich bei diesem Benutzer oder dieser Gruppe um einZuschaueroderBesitzerunter Verwendung derEntityPersonaConfiguratonObjekt.

Um anderen Personen mithilfe der Konsole Zugriff auf Ihr Sucherlebnis zu gewähren, müssen Sie zunächst ein Erlebnis erstellen und Ihre Identität sowie die Tatsache, dass Sie der Eigentümer sind, bestätigen. Anschließend können Sie andere Benutzer oder Gruppen als Zuschauer oder Eigentümer zuweisen. Sie können auch das Tutorial in ansehen.Erlebnisseein das Navigationsmenü ansehen. Nachdem Sie Ihr Erlebnis erstellt haben, können Sie es aus der Liste auswählen. Gehe zuVerwaltung von Zugriffenum Benutzer oder Gruppen als Zuschauer oder Eigentümer zuzuweisen.

Konfiguration eines Sucherlebnisses

Im Folgenden finden Sie ein Beispiel für die Konfiguration oder Erstellung eines Sucherlebnisses.

Console

Um einAmazon Kendradas Erlebnis in ansehen.

1. Sie können auch das linke Navigationsfenster in ansehen.Indizes, wählenErlebnisseund dann dasErfahrung in ansehen.
2. Auf derErlebnis ansehenSeite, Geben Sie einen Namen und eine Beschreibung für Ihr Erlebnis ein, und wählen Sie Ihre Inhaltsquellen und die IAM-Rolle für Ihr Erlebnis aus. Sie können auch das Tutorial in ansehen.IAM-Rollen fürAmazon KendraErfahrungen.

3. Auf derBestätigen Sie Ihre Identität anhand eines Identity Center-VerzeichnissesWählen Sie auf der Seite Ihre Benutzer-ID aus, z. B. Ihre E-Mail-Adresse. Wenn Sie kein Identity Center-Verzeichnis haben, geben Sie einfach Ihren vollständigen Namen und Ihre E-Mail-Adresse ein, um ein Identity Center-Verzeichnis zu erstellen. Dies schließt Sie als Benutzer des Erlebnisses ein und weist Ihnen automatisch Eigentümerzugriffsrechte zu.
4. Auf derÜberprüfen Sie, um Experience Builder zu öffnenSeite ansehen. Sie können auch das Tutorial in ansehen.Erstellen Sie ein Erlebnis und öffnen Sie Experience Builderum mit der Bearbeitung Ihrer Suchseite zu beginnen.

CLI

Um einAmazon KendraErfahrung

```
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

Um einAmazon KendraErfahrung

```
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

Erstellen einer 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.");
    }
}
```

Kapazität anpassen

Amazon Kendra stellt Ressourcen für Ihren Index in Kapazitätseinheiten bereit. Jede Kapazitätseinheit stellt zusätzliche Ressourcen für Ihren Index bereit. Es gibt separate Kapazitätseinheiten für die Speicherung von Dokumenten und für Abfragen. Sie können nur Kapazitätseinheiten zu Amazon Kendra Enterprise Edition-Indizes hinzufügen. Sie können einem Developer Edition-Index keine Kapazität hinzufügen.

Eine Dokumentenspeicherkapazitätseinheit bietet den folgenden zusätzlichen Speicherplatz für Ihren Index.

- 100.000 Dokumente oder 30 GB Speicherplatz.

Eine Abfragekapazitätseinheit stellt die folgenden zusätzlichen Abfragen für Ihren Index bereit.

- 0,1 Abfragen pro Sekunde oder ungefähr 8.000 Abfragen pro Tag.

Jeder Index hat eine Basiskapazität, die 1 Kapazitätseinheit entspricht (30 GB Speicher und 0,1 Abfragen pro Sekunde). Für jede zusätzliche Kapazitätseinheit fallen zusätzliche Kosten an. Weitere Details finden Sie unter Amazon Kendra -Preise.

Sie können Ihrem Speicher bis zu 100 zusätzliche Kapazitätseinheiten hinzufügen und Ressourcen für einen Index abfragen. Wenn Sie mehr Einheiten benötigen, wenden Sie sich einfach an den Support.

Sie können die Kapazitätseinheiten bis zu fünfmal täglich an Ihre Nutzungsanforderungen anpassen. Sie können die Speicherkapazität für Dokumente nicht unter die Anzahl der in Ihrem Index gespeicherten Dokumente reduzieren. Wenn Sie beispielsweise 150.000 Dokumente speichern, können Sie die Speicherkapazität nicht auf eine zusätzliche Einheit reduzieren.

Sie können die Ressourcen, die ein Index verwendet, in der Konsole anzeigen, indem Sie den Namen des Indexes auswählen, um die Indexeinstellungen und andere Informationen zu öffnen, oder Sie können die DescribeIndexAPI verwenden.

Amazon Kendra gibt auch Ausnahmen zurück, wenn Sie die Kapazität eines Indexes überschreiten. Sie erhalten eine`ServiceQuotaExceededException`, wenn die gesamte extrahierte Größe aller Dokumente den Grenzwert für einen Index überschreitet. Sie erhalten a `InvalidRequest` für jedes Dokument, wenn die Anzahl der Dokumente das Limit für einen Index überschreitet. Sie

erhalten eine`ThrottlingException`, wenn die Anzahl der Abfragen pro Sekunde den Grenzwert überschreitet. Weitere Informationen zu Grenzwerten finden Sie unter Kontingente für Amazon Kendra.

Kumulierte Abfragen dauern bis zu 24 Stunden.

Kapazität für die Anzeige

Zeigen Sie mit der Amazon Kendra Konsole die Ressourcen an, die Ihr Index verwendet, indem Sie den Namen Ihres Indexes auswählen, um auf die Details zuzugreifen. Die Konsole bietet auch Nutzungsdiagramme, mit denen Sie ermitteln können, wie viel Speicher- und Abfragekapazität Ihr Index verwendet. Sie können diese Informationen verwenden, um zu planen, wann zusätzliche Kapazität hinzugefügt werden sollte.

So zeigen Sie den Dokumentenspeicher und die Verwendung von Abfragen an (Konsole)

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die Amazon Kendra Konsole unter https://console.aws.amazon.com/kendra/home.
2. Wählen Sie aus der Liste der Indizes den Index aus, auf den Sie zugreifen möchten.
3. Scrollen Sie zum Bereich Einstellungen, um die aktuelle Gesamtspeicher- und Abfragekapazität für Dokumente anzuzeigen.

Verwenden Sie den `CapacityUnits` Parameter in der Amazon Kendra API, um die Kapazität mithilfe der DescribeIndexAPI anzuzeigen.

Kapazität hinzufügen und entfernen

Wenn Sie zusätzliche Kapazität für Ihren Index benötigen, können Sie diese über die Konsole oder die Amazon Kendra API hinzufügen.

Um Speicher- oder Abfragekapazität hinzuzufügen oder zu entfernen (Konsole)

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die Amazon Kendra Konsole unter https://console.aws.amazon.com/kendra/home.
2. Wählen Sie aus der Liste der Indizes den Index aus, auf den Sie zugreifen möchten.
3. Wählen Sie Bearbeiten aus oder wählen Sie Bearbeiten aus der Dropdownliste Aktionen aus.
4. Wählen Sie Weiter aus, um zur Seite mit den Bereitstellungsdetails zu gelangen.

5. Fügen Sie Kapazitätseinheiten für Dokumentenspeicher und/oder Abfragen hinzu oder entfernen Sie sie.
6. Wählen Sie weiterhin Weiter aus, um zur Überprüfungsseite zu gelangen, und wählen Sie dann Aktualisieren aus, um Ihre Änderungen zu speichern.

Nachdem Sie die Kapazität Ihres Index aktualisiert haben, kann es mehrere Minuten dauern, bis die Änderungen wirksam werden.

Verwenden Sie den `CapacityUnits` Parameter in der Amazon Kendra API, um Kapazität mithilfe der UpdateIndexAPI hinzuzufügen oder zu entfernen.

Amazon Kendra Kapazität für intelligentes Ranking

Eine Kapazitätseinheit stellt die folgenden zusätzlichen Rescore-Anfragen pro Sekunde für einen Rescore-Ausführungsplan bereit. Ein Rescore-Ausführungsplan ist eine Ressource, die zur Bereitstellung der Rescore-API verwendet wird.

- 0,01 Anfragen pro Sekunde.

Jeder Rescore-Ausführungsplan hat eine Basiskapazität, die 1 Kapazitätseinheit (0,01 Anfragen pro Sekunde) entspricht. Für jede zusätzliche Kapazitätseinheit fallen zusätzliche Kosten an. Weitere Details finden Sie unter Amazon Kendra -Preise.

Sie können bis zu 1000 zusätzliche Kapazitätseinheiten für einen Rescore-Ausführungsplan hinzufügen. Wenn Sie mehr Einheiten benötigen, wenden Sie sich einfach an den Support.

Kapazität für Vorschläge abfragen

Bei der Verwendung von Abfragevorschlägen gibt es eine Basisabfragekapazität von 2,5 GetQuerySuggestionsAufrufen pro Sekunde. Die `GetQuerySuggestions` Kapazität entspricht dem Fünffachen der bereitgestellten Abfragekapazität für einen Index oder der Basiskapazität von 2,5 Aufrufen pro Sekunde, je nachdem, welcher Wert höher ist. Zum Beispiel beträgt die Basiskapazität für einen Index 0,1 Abfragen pro Sekunde, und die `GetQuerySuggestions`-Kapazität hat eine Basis von 2,5 Anrufen pro Sekunde. Wenn Sie weitere 0,1 Abfragen pro Sekunde hinzufügen, um insgesamt 0,2 Abfragen pro Sekunde für einen Index zu erhalten, ist die `GetQuerySuggestions`-Kapazität 2,5 Aufrufe pro Sekunde (höher als fünf mal 0,2 Abfragen pro Sekunde).

Amazon Kendra Kapazität erleben

Kapazität für Sucherlebnisse

Amazon Kendra beginnt `QueryQuerySuggestions`, `SubmitFeedback` Ihrer Amazon Kendra Erfahrung nach auf 15 Anfragen pro Sekunde und 40 Anfragen pro Sekunde beim Abfrage-Bursting zu drosseln. Für einen Index mit mehr als 150 Abfragekapazitätseinheiten gelten diese Grenzwerte weiterhin.

Ihre Abfragekapazitätseinheiten für Ihren Index sind beispielsweise 150, sodass Ihre Search Experience-Anwendung 15 Anfragen pro Sekunde verarbeiten kann. Wenn Sie jedoch auf 200 Kapazitätseinheiten für Abfragen skalieren würden, würde Ihre Search Experience-App immer noch nur 15 Anfragen pro Sekunde verarbeiten. Wenn Sie Ihren Index auf 100 Kapazitätseinheiten für Abfragen beschränken, würde Ihre Search Experience-App nur 10 Anfragen pro Sekunde verarbeiten.

Adaptives Abfrage-Bursting

Amazon Kendra hat eine bereitgestellte Basiskapazität von 1 Abfragekapazitätseinheit. Sie können bis zu 8.000 Abfragen pro Tag mit einem Mindestdurchsatz von 0,1 Abfragen pro Sekunde (pro Abfragekapazitätseinheit) verwenden. Kumulierte Abfragen dauern bis zu 24 Stunden und können Datenfluten bewältigen. Die Anzahl der zulässigen Bursts variiert, da sie von der Auslastung des Clusters zu einem bestimmten Zeitpunkt abhängt. Stellen Sie genügend Abfragekapazitätseinheiten bereit, um Ihre Spitzenlastwerte zu bewältigen.

Ein adaptiver Ansatz für den Umgang mit unerwarteten Datenverkehrsspitzen, die über den bereitgestellten Durchsatz hinausgehen, Amazon Kendra ist das integrierte adaptive Query-Bursting. Adaptives Query-Bursting ist in der Enterprise Edition von verfügbar. Amazon Kendra

Adaptives Query-Bursting ist eine integrierte Funktion, mit der Sie ungenutzte Abfragekapazität nutzen können, um unerwarteten Datenverkehr zu verarbeiten. Amazon Kendra sammelt Ihre ungenutzten Abfragen mit der Rate Ihrer bereitgestellten Abfragen pro Sekunde, jede Sekunde, bis zu der maximalen Anzahl von Abfragen, die Sie für Ihren Index bereitgestellt haben. Amazon Kendra Diese gesammelten Abfragen werden für unerwarteten Datenverkehr verwendet, der die zugewiesene Kapazität übersteigt. Die optimale Leistung von adaptivem Query-Bursting kann variieren und hängt von verschiedenen Faktoren ab, wie z. B. der Gesamtgröße Ihres Indexes, der Komplexität der Abfragen, der Anzahl ungenutzter Abfragen und der Gesamtauslastung Ihres

Indexes. Es wird empfohlen, dass Sie Ihre eigenen Lasttests durchführen, um die Bursting-Kapazität genau zu messen.

Erste Schritte

In diesem Abschnitt erfahren Sie, wie Sie eine Datenquelle erstellen und Ihre Dokumente zu einem Amazon Kendra Index hinzufügen. Es werden Anweisungen für die AWS Konsole bereitgestellt, dieAWS CLI, ein Python-Programm, das die verwendetAWS SDK for Python (Boto3), und ein Java-Programm, das die verwendetAWS SDK for Java.

Themen

Voraussetzungen

Die folgenden Schritte sind Voraussetzungen für die Übungen „Erste Schritte“. Die Schritte zeigen Ihnen, wie Sie Ihr Konto einrichten, eine IAM Rolle erstellen, die Ihnen die Amazon Kendra Erlaubnis erteilt, in Ihrem Namen Anrufe zu tätigen, und Dokumente aus einem Amazon S3 Bucket indexieren. Ein S3-Bucket wird als Beispiel verwendet, aber Sie können auch andere Datenquellen verwenden, die dies Amazon Kendra unterstützen. Siehe Datenquellen.

So melden Sie sich für ein AWS-Konto an

Wenn Sie kein AWS-Konto haben, führen Sie die folgenden Schritte zum Erstellen durch.

Anmeldung für ein AWS-Konto

1. Öffnen Sie https://portal.aws.amazon.com/billing/signup.
2. Folgen Sie den Online-Anweisungen.

   Bei der Anmeldung müssen Sie auch einen Telefonanruf entgegennehmen und einen Verifizierungscode über die Telefontasten eingeben.

Wenn Sie sich für ein AWS-Konto anmelden, wird ein Root-Benutzer des AWS-Kontos erstellt. Der Root-Benutzer hat Zugriff auf alle AWS-Services und Ressourcen des Kontos. Als bewährte Sicherheitsmethode weisen Sie einem Administratorbenutzer Administratorzugriff zu und verwenden Sie nur den Root-Benutzer, um Aufgaben auszuführen, die Root-Benutzerzugriff erfordern.

AWS sendet Ihnen eine Bestätigungs-E-Mail, sobald die Anmeldung abgeschlossen ist. Sie können jederzeit Ihre aktuelle Kontoaktivität anzeigen und Ihr Konto verwalten. Rufen Sie dazu https://aws.amazon.com/ auf und klicken Sie auf Mein Konto.

Einen Administratorbenutzer erstellen

Nachdem Sie sich für einen angemeldet habenAWS-Konto, sichern Sie Ihren Root-Benutzer des AWS-KontosAWS IAM Identity Center, aktivieren und erstellen Sie einen Administratorbenutzer, sodass Sie den Root-Benutzer nicht für alltägliche Aufgaben verwenden.

Schützen Ihres Root-Benutzer des AWS-Kontos

1. Melden Sie sich bei der AWS Management Console als Kontobesitzer an, indem Sie Root-Benutzer auswählen und Ihre AWS-Konto E-Mail-Adresse eingeben. Geben Sie auf der nächsten Seite Ihr Passwort ein.

   Hilfe bei der Anmeldung mit dem Root-Benutzer finden Sie unter Anmelden als Root-Benutzer im AWS-AnmeldungBenutzerhandbuch zu .
2. Aktivieren Sie die Multi-Faktor-Authentifizierung (MFA) für den Root-Benutzer.

   Anweisungen dazu finden Sie unter Aktivieren eines virtuellen MFA-Geräts für den Root-Benutzer Ihres AWS-Konto (Konsole) im IAM-Benutzerhandbuch.

Erstellen eines Administratorbenutzers

1. Aktivieren Sie IAM Identity Center.

   Anweisungen finden Sie unter Aktivieren AWS IAM Identity Center im AWS IAM Identity CenterBenutzerhandbuch.
2. Gewähren Sie in IAM Identity Center einem Administratorbenutzer Administratorzugriff.

Ein Tutorial zur Verwendung von IAM-Identity-Center-Verzeichnis als Identitätsquelle finden Sie unter Benutzerzugriff mit der Standardeinstellung konfigurieren IAM-Identity-Center-Verzeichnis im AWS IAM Identity CenterBenutzerhandbuch.

Als Administratorbenutzer anmelden

- Um sich mit Ihrem IAM-Identity-Center-Benutzer anzumelden, verwenden Sie die Anmelde-URL, die an Ihre E-Mail-Adresse gesendet wurde, als Sie den IAM-Identity-Center-Benutzer erstellt haben.

  Hilfe bei der Anmeldung mit einem IAM-Identity-Center-Benutzer finden Sie unter Anmelden beim AWS-Zugangsportal im AWS-Anmeldung Benutzerhandbuch zu.

- Wenn Sie einen S3-Bucket verwenden, der Dokumente zum Testen enthältAmazon Kendra, erstellen Sie einen S3-Bucket in derselben Region, die Sie verwendenAmazon Kendra. Anweisungen finden Sie unter Erstellen und Konfigurieren eines S3-Buckets im Amazon Simple Storage Service-Benutzerhandbuch.

  Laden Sie Ihre Dokumente in Ihren S3-Bucket hoch. Anweisungen finden Sie unter Hochladen, Herunterladen und Verwalten von Objekten im Amazon Simple Storage Service-Benutzerhandbuch.

  Wenn Sie eine andere Datenquelle verwenden, benötigen Sie eine aktive Site und Anmeldeinformationen, um eine Verbindung mit der Datenquelle herzustellen.

Wenn Sie zunächst die Konsole verwenden, beginnen Sie mitErste Schritte mit der Amazon Kendra Konsole.

Amazon KendraRessourcen:AWS CLI, SDK, Konsole

Wenn Sie CLI, SDK oder die Konsole verwenden, sind bestimmte Berechtigungen erforderlich.

Um sie Amazon Kendra für die CLI, das SDK oder die Konsole verwenden zu können, müssen Sie über die erforderlichen Berechtigungen verfügenAmazon Kendra, um Ressourcen in Ihrem Namen erstellen und verwalten zu können. Je nach Anwendungsfall umfassen diese Berechtigungen den Zugriff auf die Amazon Kendra API selbst, AWS KMS keys wenn Sie Ihre Daten über ein benutzerdefiniertes CMK verschlüsseln möchten, oder auf das Identity Center-Verzeichnis, wenn Sie

ein Search Experience integrieren AWS IAM Identity Center oder ein solches erstellen möchten. Eine vollständige Liste der Berechtigungen für verschiedene Anwendungsfälle finden Sie unter IAM Rollen.

Zunächst müssen Sie Ihrem IAM-Benutzer die folgenden Berechtigungen zuweisen.

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

Zweitens müssen Sie, wenn Sie die CLI oder das SDK verwenden, auch eine IAM Rolle und eine Richtlinie für den Zugriff erstellenAmazon CloudWatch Logs. Wenn Sie die Konsole verwenden, müssen Sie dafür keine IAM Rolle und Richtlinie erstellen. Sie erstellen dies im Rahmen der Konsolenprozedur.

Um eine IAM Rolle und eine Richtlinie für das AWS CLI SDK zu erstellen, die den Amazon Kendra Zugriff auf Ihre ermöglichenAmazon CloudWatch Logs.

1. Melden Sie sich bei der AWS Management Console an und öffnen Sie die IAM-Konsole unter https://console.aws.amazon.com/iam/.
2. Wählen Sie im linken Menü Richtlinien und dann Richtlinie erstellen aus.
3. Wählen Sie JSON und ersetzen Sie dann die Standardrichtlinie durch Folgendes:

```
{
    "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. Wählen Sie Richtlinie prüfen.
5. Geben Sie der Richtlinie einen Namen "KendraPolicyForGettingStartedIndex" und wählen Sie dann Richtlinie erstellen aus.
6. Wählen Sie im linken Menü Rollen und dann Rolle erstellen aus.

7. Wählen Sie Anderes AWS Konto und geben Sie dann Ihre Konto-ID in das Feld Konto-ID ein. Wählen Sie Weiter: Berechtigungen aus.
8. Wählen Sie die Richtlinie aus, die Sie oben erstellt haben, und klicken Sie dann auf Weiter: Tags
9. Fügen Sie keine Tags hinzu. Wählen Sie Weiter: Prüfen aus.
10. Geben Sie der Rolle einen Namen "KendraRoleForGettingStartedIndex" und wählen Sie dann Rolle erstellen aus.
11. Suchen Sie die Rolle, die Sie gerade erstellt haben. Wählen Sie den Rollennamen, um die Zusammenfassung zu öffnen. Wählen Sie Vertrauensbeziehungen und dann Vertrauensbeziehung bearbeiten aus.
12. Ersetzen Sie die bestehende Vertrauensbeziehung durch Folgendes:

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

13. Wählen Sie Update trust policy (Vertrauensrichtlinie aktualisieren) aus.

Drittens müssen Sie, wenn Sie eine Amazon S3 zum Speichern Ihrer Dokumente verwenden oder S3 zum Testen verwendenAmazon Kendra, auch eine IAM Rolle und eine Richtlinie für den Zugriff auf Ihren Bucket erstellen. Wenn Sie eine andere Datenquelle verwenden, finden Sie weitere Informationen unter IAMRollen für Datenquellen.

Um eine IAM Rolle und eine Richtlinie zu erstellen, die Amazon Kendra den Zugriff auf Ihren Amazon S3 Bucket und dessen Indexierung ermöglichen.

1. Melden Sie sich bei der AWS Management Console an und öffnen Sie die IAM-Konsole unter https://console.aws.amazon.com/iam/.
2. Wählen Sie im linken Menü Richtlinien und dann Richtlinie erstellen aus.
3. Wählen Sie JSON und ersetzen Sie dann die Standardrichtlinie durch Folgendes:

```
{
    "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. Wählen Sie Richtlinie prüfen.
5. Geben Sie der Richtlinie den Namen KendraPolicyForGettingStartedDataSource "" und wählen Sie dann Richtlinie erstellen aus.
6. Wählen Sie im linken Menü Rollen und dann Rolle erstellen aus.
7. Wählen Sie Anderes AWS Konto und geben Sie dann Ihre Konto-ID in das Feld Konto-ID ein. Wählen Sie Weiter: Berechtigungen aus.
8. Wählen Sie die Richtlinie aus, die Sie oben erstellt haben, und klicken Sie dann auf Weiter: Tags
9. Fügen Sie keine Tags hinzu. Wählen Sie Weiter: Prüfen aus.

10. Geben Sie der Rolle den Namen KendraRoleForGettingStartedDataSource "" und wählen Sie dann Rolle erstellen aus.
11. Suchen Sie die Rolle, die Sie gerade erstellt haben. Wählen Sie den Rollennamen, um die Zusammenfassung zu öffnen. Wählen Sie Vertrauensbeziehungen und dann Vertrauensbeziehung bearbeiten aus.
12. Ersetzen Sie die bestehende Vertrauensbeziehung durch Folgendes:

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

13. Wählen Sie Update trust policy (Vertrauensrichtlinie aktualisieren) aus.

Je nachdem, wie Sie die Amazon Kendra API verwenden möchten, führen Sie einen der folgenden Schritte aus.

- Erste Schritte (AWS CLI)
- Erste Schritte (AWS SDK for Java)
- Erste Schritte (AWS SDK for Python (Boto3))

Erste Schritte mit der Amazon Kendra Konsole

Die folgenden Verfahren zeigen, wie Sie einen Amazon Kendra Index mithilfe der AWS Konsole erstellen und testen. In den Verfahren erstellen Sie einen Index und eine Datenquelle für einen Index. Schließlich testen Sie Ihren Index, indem Sie eine Suchanfrage stellen.

Schritt 1: So erstellen Sie einen Index (Konsole)

1. Melden Sie sich bei der AWS Management Console an und öffnen Sie die Amazon Kendra Konsole unter https://console.aws.amazon.com/kendra/.
2. Wählen Sie im Bereich Indizes die Option Index erstellen aus.
3. Geben Sie auf der Seite Indexdetails angeben Ihrem Index einen Namen und eine Beschreibung.
4. Wählen Sie unter IAMRolle die Option Neue Rolle erstellen aus und geben Sie der Rolle dann einen Namen. Die IAM Rolle wird das Präfix "AmazonKendra-“ haben.
5. Behalten Sie für alle anderen Felder ihre Standardwerte bei. Wählen Sie Weiter.
6. Wählen Sie auf der Seite Benutzerzugriffskontrolle konfigurieren die Option Weiter aus.
7. Wählen Sie auf der Seite mit den Bereitstellungsdetails die Developer Edition aus.
8. Wählen Sie Erstellen, um Ihren Index zu erstellen.
9. Warten Sie, bis Ihr Index erstellt wurde. Amazon Kendrastellt die Hardware für Ihren Index bereit. Dieser Vorgang kann einige Zeit in Anspruch nehmen.

Schritt 2: So fügen Sie einem Index eine Datenquelle hinzu (Konsole)

1. Sehen Sie sich die verfügbaren Datenquellen an, um eine Verbindung Amazon Kendra zu Ihren Dokumenten herzustellen und sie zu indizieren.
2. Wählen Sie im Navigationsbereich Datenquellen und dann Datenquelle hinzufügen für die gewählte Datenquelle aus.
3. Folgen Sie den Schritten, um die Datenquelle zu konfigurieren.

Schritt 3: So durchsuchen Sie einen Index (Konsole)

1. Wählen Sie im Navigationsbereich die Option zum Durchsuchen Ihres Index aus.
2. Geben Sie einen Suchbegriff ein, der zu Ihrem Index passt. Die besten Ergebnisse und die besten Dokumentergebnisse werden angezeigt.

Erste Schritte (AWS CLI)

Das folgende Verfahren zeigt, wie Sie einen Amazon Kendra Index mit dem erstellenAWS CLI. Die Prozedur erstellt eine Datenquelle, einen Index, und führt eine Abfrage für den Index aus.

So erstellen Sie einen Amazon Kendra Index (CLI)

1. Mach dasVoraussetzungen.
2. Geben Sie den folgenden Befehl ein, um einen Index zu erstellen.

```
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. Warten SieAmazon Kendra, bis der Index erstellt wurde. Überprüfen Sie den Fortschritt mit dem folgenden Befehl. Wenn das Statusfeld angezeigt wirdACTIVE, fahren Sie mit dem nächsten Schritt fort.

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

4. Geben Sie in der Befehlszeile den folgenden Befehl ein, um eine Datenquelle zu erstellen.

```
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"}}'
```

   Wenn Sie mithilfe eines Vorlagenschemas eine Verbindung zu Ihrer Datenquelle herstellen, konfigurieren Sie das Vorlagenschema.

```
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. Das Erstellen der Datenquelle dauert Amazon Kendra eine Weile. Geben Sie den folgenden Befehl ein, um den Fortschritt zu überprüfen. Wenn der Status lautetACTIVE, fahren Sie mit dem nächsten Schritt fort.

```
aws kendra describe-data-source \
```

```
 --id data source ID \
 --index-id index ID
```

6. Geben Sie den folgenden Befehl ein, um die Datenquelle zu synchronisieren.

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

7. Amazon Kendraindexiert Ihre Datenquelle. Die dafür benötigte Zeit hängt von der Anzahl der Dokumente ab. Sie können den Status des Synchronisierungsauftrags mit dem folgenden Befehl überprüfen. Wenn der Status lautet`ACTIVE`, fahren Sie mit dem nächsten Schritt fort.

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

8. Geben Sie den folgenden Befehl ein, um eine Abfrage zu stellen.

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

   Die Ergebnisse der Suche werden im JSON-Format angezeigt.

Erste Schritte (AWS SDK for Python (Boto3))

Das folgende Programm ist ein Beispiel für die Verwendung Amazon Kendra in einem Python-Programm. Das Programm führt die folgenden Aktionen aus:

1. Erstellt mithilfe der CreateIndexOperation einen neuen Index.
2. Wartet auf den Abschluss der Indexerstellung. Es verwendet den DescribeIndexVorgang, um den Status des Indexes zu überwachen.
3. Sobald der Index aktiv ist, erstellt er mithilfe der CreateDataSourceOperation eine Datenquelle.
4. Wartet, bis die Erstellung der Datenquelle abgeschlossen ist. Es verwendet den DescribeDataSourceVorgang, um den Status der Datenquelle zu überwachen.
5. Wenn die Datenquelle aktiv ist, synchronisiert sie den Index mithilfe der StartDataSourceSyncJobOperation mit dem Inhalt der Datenquelle.

```
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.")
```

Erste Schritte (AWS SDK for Java)

Das folgende Programm ist ein Beispiel für die Verwendung Amazon Kendra in einem Java-Programm. Das Programm führt die folgenden Aktionen aus:

1. Erstellt mithilfe der CreateIndexOperation einen neuen Index.
2. Wartet auf den Abschluss der Indexerstellung. Es verwendet den DescribeIndexVorgang, um den Status des Indexes zu überwachen.
3. Sobald der Index aktiv ist, erstellt er mithilfe der CreateDataSourceOperation eine Datenquelle.
4. Wartet, bis die Erstellung der Datenquelle abgeschlossen ist. Es verwendet den DescribeDataSourceVorgang, um den Status der Datenquelle zu überwachen.
5. Wenn die Datenquelle aktiv ist, synchronisiert sie den Index mithilfe der StartDataSourceSyncJobOperation mit dem Inhalt der Datenquelle.

```
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");
    }
```

```
}
```

Erste Schritte mit einer Amazon S3 Datenquelle (Konsole)

Sie können die Amazon Kendra Konsole verwenden, um mit der Verwendung eines Amazon S3 Buckets als Datenspeicher zu beginnen. Wenn Sie die Konsole verwenden, geben Sie alle Verbindungsinformationen an, die Sie benötigen, um den Inhalt des Buckets zu indexieren. Weitere Informationen finden Sie unter Amazon S3.

Gehen Sie wie folgt vor, um mithilfe der Standardkonfiguration eine einfache S3-Bucket-Datenquelle zu erstellen. Das Verfahren geht davon aus, dass Sie einen Index gemäß den Schritten in Schritt 1 von erstellt habenErste Schritte mit der Amazon Kendra Konsole.

So erstellen Sie eine S3-Bucket-Datenquelle mithilfe der Amazon Kendra Konsole

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die Amazon Kendra Konsole unter https://console.aws.amazon.com/kendra/home.
2. Wählen Sie aus der Liste der Indizes den Index aus, zu dem Sie die Datenquelle hinzufügen möchten.
3. Wählen Sie Datenquellen hinzufügen aus.
4. Wählen Sie aus der Liste der Datenquellenkonnektoren aus Amazon S3.
5. Geben Sie auf der Seite „Attribute definieren“ Ihrer Datenquelle einen Namen und optional eine Beschreibung. Lassen Sie das Feld Tags leer. Wählen Sie Next (Weiter), um fortzufahren.
6. Geben Sie im Feld Speicherort der Datenquelle den Namen des S3-Buckets ein, der Ihre Dokumente enthält. Sie können den Namen direkt eingeben, oder Sie können nach dem Namen suchen, indem Sie Durchsuchen wählen. Der Bucket muss sich in derselben Region wie der Index befinden.
7. Wählen Sie IAMunter Rolle die Option Neue Rolle erstellen aus und geben Sie dann einen Rollennamen ein. Weitere Informationen finden Sie unter IAMRollen für Amazon S3 Datenquellen.
8. Wählen Sie im Abschnitt Zeitplan für die Synchronisierung festlegen die Option Bei Bedarf ausführen aus.
9. Wählen Sie Next (Weiter), um fortzufahren.
10. Überprüfen Sie auf der Seite Überprüfen und erstellen die Details Ihrer S3-Datenquelle. Wenn Sie Änderungen vornehmen möchten, klicken Sie neben dem Element, das Sie ändern möchten,

auf die Schaltfläche Bearbeiten. Wenn Sie mit Ihrer Auswahl zufrieden sind, wählen Sie Erstellen, um Ihre S3-Datenquelle zu erstellen.

Nachdem Sie Erstellen ausgewählt haben, Amazon Kendra wird mit der Erstellung der Datenquelle begonnen. Es kann mehrere Minuten dauern, bis die Datenquelle erstellt ist. Wenn der Vorgang abgeschlossen ist, ändert sich der Status der Datenquelle von Erstellt in Aktiv.

Nachdem Sie die Datenquelle erstellt haben, müssen Sie den Amazon Kendra Index mit der Datenquelle synchronisieren. Wählen Sie Jetzt synchronisieren, um den Synchronisierungsvorgang zu starten. Die Synchronisierung der Datenquelle kann je nach Anzahl und Größe der Dokumente mehrere Minuten bis mehrere Stunden dauern.

Erste Schritte mit einer MySQL-Datenbankdatenquelle (Konsole)

Sie können die Amazon Kendra Konsole verwenden, um mit der Verwendung einer MySQL-Datenbank als Datenquelle zu beginnen. Wenn Sie die Konsole verwenden, geben Sie die Verbindungsinformationen an, die Sie benötigen, um den Inhalt einer MySQL-Datenbank zu indexieren. Weitere Informationen finden Sie unter Verwenden einer Datenbank-Datenquelle.

Sie müssen zuerst eine MySQL-Datenbank erstellen, dann können Sie eine Datenquelle für die Datenbank erstellen.

Gehen Sie wie folgt vor, um eine grundlegende MySQL-Datenbank zu erstellen. Das Verfahren geht davon aus, dass Sie nach Schritt 1 von bereits einen Index erstellt habenErste Schritte mit der Amazon Kendra Konsole.

Um eine MySQL-Datenbank zu erstellen

1. Melden Sie sich bei der AWS Management Console an und öffnen Sie die Amazon-RDS-Konsole unter https://console.aws.amazon.com/rds/.
2. Wählen Sie im Navigationsbereich Subnetzgruppen und dann Create DB Subnet Group aus.
3. Benennen Sie die Gruppe und wählen Sie Ihre Virtual Private Cloud (VPC). Weitere Informationen zur Konfiguration einer VPC finden Sie unter Konfiguration Amazon Kendra zur Verwendung einer VPC.
4. Fügen Sie die privaten Subnetze Ihrer VPC hinzu. Ihre privaten Subnetze sind diejenigen, die nicht mit Ihrem NAT verbunden sind. Wählen Sie Create (Erstellen) aus.
5. Wählen Sie im Navigationsbereich Datenbanken und dann Datenbank erstellen aus.

6. Verwenden Sie die folgenden Parameter, um die Datenbank zu erstellen. Belassen Sie alle anderen Parameter auf ihren Standardwerten.

   - Engine-Optionen — MySQL
   - Vorlagen — Kostenloses Kontingent
   - Einstellungen für Anmeldeinformationen — Geben Sie ein Passwort ein und bestätigen Sie es
   - Wählen Sie unter Konnektivität die Option Zusätzliche Verbindungskonfiguration aus. Treffen Sie die folgenden Entscheidungen.
     - Subnetzgruppe — Wählen Sie die Subnetzgruppe aus, die Sie in Schritt 4 erstellt haben.
     - VPC-Sicherheitsgruppe — Wählen Sie die Gruppe aus, die sowohl eingehende als auch ausgehende Regeln enthält, die Sie in Ihrer VPC erstellt haben. Zum Beispiel **`DataSourceSecurityGroup`**. Weitere Informationen zur Konfiguration einer VPC finden Sie unter Konfiguration Amazon Kendra zur Verwendung einer VPC.
   - Legen Sie unter Zusätzliche Konfiguration den ursprünglichen Datenbanknamen auf fest**`content`**.
7. Wählen Sie Datenbank erstellen aus.
8. Wählen Sie aus der Liste der Datenbanken Ihre neue Datenbank aus. Notieren Sie sich den Datenbankendpunkt.
9. Nachdem Sie Ihre Datenbank erstellt haben, müssen Sie eine Tabelle für Ihre Dokumente erstellen. Das Erstellen einer Tabelle ist nicht Gegenstand dieser Anleitung. Beachten Sie beim Erstellen Ihrer Tabelle Folgendes:

   - Datenbankname— **`content`**
   - Tabellenname— **`documents`**
   - Spalten— **`IDTitle`**,**`Body`**, und**`LastUpdate`**. Sie können zusätzliche Spalten hinzufügen, wenn Sie möchten.

Nachdem Sie Ihre MySQL-Datenbank erstellt haben, können Sie eine Datenquelle für die Datenbank erstellen.

Um eine MySQL-Datenquelle zu erstellen

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die Amazon Kendra Konsole unter https://console.aws.amazon.com/kendra/home.
2. Wählen Sie im Navigationsbereich Indizes und dann Ihren Index aus.

3. Wählen Sie Datenquellen hinzufügen und dann Amazon RDS aus.
4. Geben Sie einen Namen und eine Beschreibung für die Datenquelle ein und wählen Sie dann Weiter.
5. Wählen Sie MySQL.
6. Geben Sie unter Verbindungszugriff die folgenden Informationen ein:
   - Endpunkt — Der Endpunkt der Datenbank, die Sie zuvor erstellt haben.
   - Port — Die Portnummer für die Datenbank. Für MySQL ist die Standardeinstellung 3306.
   - Art der Authentifizierung — Wählen Sie Neu.
   - Neuer geheimer Containername — Ein Name für den Secrets Manager Container für die Datenbankanmeldeinformationen.
   - Benutzername — Der Name eines Benutzers mit Administratorzugriff auf die Datenbank.
   - Passwort — Das Passwort für den Benutzer, und wählen Sie dann Authentifizierung speichern.
   - Datenbankname —**`content`**.
   - Tabellenname —**`documents`**.
   - IAM-Rolle — Wählen Sie Neue Rolle erstellen aus, und geben Sie dann einen Namen für die Rolle ein.
7. Geben Sie unter Spaltenkonfiguration Folgendes ein:
   - Name der Dokument-ID-Spalte — **`ID`**
   - Titel und Spaltenname des Dokuments — **`Title`**
   - Name der Dokumentdatenspalte — **`Body`**
8. Geben Sie im Feld Erkennung von Spaltenänderungen Folgendes ein:
   - Erkennungsspalten ändern — **`LastUpdate`**
9. Geben Sie unter „VPC und Sicherheitsgruppe konfigurieren“ Folgendes an:
   - Wählen Sie in Virtual Private Cloud (VPC) Ihre VPC aus.
   - Wählen Sie unter Subnetze die privaten Subnetze aus, die Sie in Ihrer VPC erstellt haben.
   - Wählen Sie unter VPC-Sicherheitsgruppen die Sicherheitsgruppe aus, die sowohl eingehende als auch ausgehende Regeln enthält, die Sie in Ihren VPC für MySQL-Datenbanken erstellt haben. Zum Beispiel **`DataSourceSecurityGroup`**.
10. Wählen Sie unter „Zeitplan für die Synchronisierung festlegen“ die Option „Bei Bedarf ausführen“ und dann „Weiter“.

11. Wählen Sie unter Datenquellenfeldzuordnung die Option Weiter aus.
12. Überprüfen Sie die Konfiguration Ihrer Datenquelle, um sicherzustellen, dass sie korrekt ist. Wenn Sie davon überzeugt sind, dass alles korrekt ist, wählen Sie Erstellen.

Erste Schritte mit einer AWS IAM Identity Center Identitätsquelle (Konsole)

Eine AWS IAM Identity Center Identitätsquelle enthält Informationen zu Ihren Benutzern und Gruppen. Dies ist nützlich für die Einrichtung der Benutzerkontextfilterung, bei der Suchergebnisse für verschiedene Benutzer basierend auf dem Zugriff des Benutzers oder seiner Gruppe auf Dokumente Amazon Kendra filtert.

Um eine IAM-Identity-Center-Identitätsquelle zu erstellen, müssen Sie IAM Identity Center aktivieren und eine Organisation in erstellen AWS Organizations. Wenn Sie IAM Identity Center aktivieren und zum ersten Mal eine Organisation erstellen, wird automatisch das Identity-Center-Verzeichnis als Identitätsquelle verwendet. Sie können zu Active Directory (von Amazon verwaltet oder selbstverwaltet) oder einem externen Identitätsanbieter als Identitätsquelle wechseln. Sie müssen dazu die richtigen Anweisungen befolgen – siehe Ändern Ihrer IAM-Identity-Center-Identitätsquelle. Sie können nur eine Identitätsquelle pro Organisation haben.

Damit Ihren Benutzern und Gruppen unterschiedliche Zugriffsebenen auf Dokumente zugewiesen werden können, müssen Sie Ihre Benutzer und Gruppen in Ihre Zugriffskontrollliste aufnehmen, wenn Sie Dokumente in Ihren Index aufnehmen. Auf diese Weise können Ihre Benutzer und Gruppen entsprechend ihrer Zugriffsebene Amazon Kendra nach Dokumenten in suchen. Wenn Sie eine Abfrage ausgeben, muss die Benutzer-ID genau mit dem Benutzernamen im IAM Identity Center übereinstimmen.

Sie müssen auch die erforderlichen Berechtigungen erteilen, um IAM Identity Center mit verwenden zu können Amazon Kendra. Weitere Informationen finden Sie unter IAM Rollen für IAM Identity Center.

So richten Sie eine IAM-Identity-Center-Identitätsquelle ein

1. Öffnen Sie die IAM-Identity-Center-Konsole .
2. Wählen Sie IAM Identity Center aktivieren und dann AWS Organisation erstellen aus.

   Identity-Center-Verzeichnis wird standardmäßig erstellt und Sie erhalten eine E-Mail, um die mit der Organisation verknüpfte E-Mail-Adresse zu verifizieren.

3. Um Ihrer AWS Organisation eine Gruppe hinzuzufügen, wählen Sie im Navigationsbereich Gruppen aus.
4. Wählen Sie auf der Seite Gruppen die Option Gruppe erstellen aus und geben Sie einen Gruppennamen und eine Beschreibung in das Dialogfeld ein. Wählen Sie Erstellen.
5. Um einen Benutzer zu Ihren Organizations hinzuzufügen, wählen Sie im Navigationsbereich Benutzer aus.
6. Wählen Sie auf der Seite Users (Benutzer) die Option Add user (Benutzer hinzufügen) aus. Geben Sie unter User details (Benutzerdetails) alle erforderlichen Felder an. Wählen Sie unter Password (Kennwort) Send an email to the user (Eine E-Mail-Nachricht an den Benutzer senden aus. Wählen Sie Weiter aus.
7. Um einen Benutzer zu einer Gruppe hinzuzufügen, wählen Sie Gruppen und dann eine Gruppe aus.
8. Wählen Sie auf der Seite Details unter Gruppenmitglieder die Option Benutzer hinzufügen aus.
9. Wählen Sie auf der Seite Benutzer zur Gruppe hinzufügen den Benutzer aus, den Sie als Mitglied der Gruppe hinzufügen möchten. Sie können mehrere Benutzer auswählen, die einer Gruppe hinzugefügt werden sollen.
10. Um Ihre Benutzer- und Gruppenliste mit IAM Identity Center zu synchronisieren, ändern Sie Ihre Identitätsquelle in Active Directory oder Externer Identitätsanbieter.

    Identity-Center-Verzeichnis ist die Standardidentitätsquelle und erfordert, dass Sie Ihre Benutzer und Gruppen mithilfe dieser Quelle manuell hinzufügen, wenn Sie nicht über eine eigene Liste verfügen, die von einem Anbieter verwaltet wird. Um Ihre Identitätsquelle zu ändern, müssen Sie dazu die richtigen Anweisungen befolgen – siehe Ändern Ihrer IAM-Identity-Center-Identitätsquelle.

> **Note**
>
> Wenn Sie Active Directory oder einen externen Identitätsanbieter als Identitätsquelle verwenden, müssen Sie die E-Mail-Adressen Ihrer Benutzer IAM-Identity-Center-Benutzernamen zuordnen, wenn Sie das System for Cross-Domain Identity Management (SCIM)-Protokoll angeben. Weitere Informationen finden Sie im IAM-Identity-Center-Leitfaden zu SCIM zum Aktivieren von IAM Identity Center .

Sobald Sie Ihre IAM-Identity-Center-Identitätsquelle eingerichtet haben, können Sie diese in der Konsole aktivieren, wenn Sie Ihren Index erstellen oder bearbeiten. Gehen Sie in Ihren Indexeinstellungen zu Benutzerzugriffskontrolle und bearbeiten Sie Ihre Einstellungen, um das Abrufen von Benutzergruppeninformationen aus dem IAM Identity Center zu ermöglichen.

Sie können IAM Identity Center auch mit dem -UserGroupResolutionConfigurationObjekt aktivieren. Sie geben `UserGroupResolutionMode` als an `AWS_SSO` und erstellen eine - IAM Rolle, die die Berechtigung zum Aufrufen von `sso:ListDirectoryAssociations`, `sso-directory:SearchUsers`, `sso-directory:ListGroupsForUser`, erteilt`sso-directory:DescribeGroups`.

> **Warning**
>
> Amazon Kendra unterstützt derzeit nicht die Verwendung von `UserGroupResolutionConfiguration` mit einem AWS Organisationsmitgliedkonto für Ihre IAM-Identity-Center-Identitätsquelle. Sie müssen Ihren Index im Verwaltungskonto der Organisation erstellen, um verwenden zu können`UserGroupResolutionConfiguration`.

Im Folgenden finden Sie eine Übersicht darüber, wie Sie eine Datenquelle mit `UserGroupResolutionConfiguration` und Benutzerzugriffskontrolle einrichten, um Suchergebnisse nach Benutzerkontext zu filtern. Dies setzt voraus, dass Sie bereits einen Index und eine - IAM Rolle für Indizes erstellt haben. Sie erstellen einen Index und stellen die IAM Rolle mithilfe der CreateIndex API bereit.

Einrichten einer Datenquelle mit **`UserGroupResolutionConfiguration`** und Benutzerkontextfilterung

1. Erstellen Sie eine -IAM Rolle, die die Berechtigung zum Zugriff auf Ihre IAM-Identity-Center-Identitätsquelle erteilt.
2. Konfigurieren Sie , `UserGroupResolutionConfiguration` indem Sie den -Modus auf setzen `AWS_SSO` und aufrufenUpdateIndex, um Ihren Index für die Verwendung von IAM Identity Center zu aktualisieren.
3. Wenn Sie die tokenbasierte Benutzerzugriffssteuerung verwenden möchten, um Suchergebnisse nach Benutzerkontext zu filtern, legen Sie `USER_TOKEN` beim Aufrufen von UserContextPolicy auf fest`UpdateIndex`. Andernfalls Amazon Kendra durchsucht die Zugriffskontrollliste für jedes Ihrer Dokumente für die meisten Datenquellen-Konnektoren. Sie können Suchergebnisse auch nach Benutzerkontext in der Abfrage-API filtern, indem Sie Benutzer- und Gruppeninformationen

in bereitstellen`UserContext`. Sie können Benutzer auch mit ihren Gruppen zuordnen, PutPrincipalMapping sodass Sie die Benutzer-ID nur beim Ausgeben der Abfrage angeben müssen.

4. Erstellen Sie eine -IAM Rolle, die die Berechtigung zum Zugriff auf Ihre Datenquelle erteilt.
5. Konfigurieren Sie Ihre Datenquelle. Sie müssen die erforderlichen Verbindungsinformationen angeben, um eine Verbindung zu Ihrer Datenquelle herzustellen.
6. Erstellen Sie eine Datenquelle mit der CreateDataSource-API. Geben Sie das `DataSourceConfiguration` Objekt an, das `TemplateConfiguration`, die ID Ihres Index, die IAM Rolle für Ihre Datenquelle und den Datenquellentyp enthält, und geben Sie Ihrer Datenquelle einen Namen. Sie können auch Ihre Datenquelle aktualisieren.

Ändern Ihrer IAM-Identity-Center-Identitätsquelle

> **Warning**
>
> Das Ändern Ihrer Identitätsquelle in den IAM-Identity-Center-Einstellungen kann sich auf die Beibehaltung von Benutzer- und Gruppeninformationen auswirken. Um dies sicher zu tun, wird empfohlen, Überlegungen zum Ändern Ihrer Identitätsquelle zu lesen. Wenn Sie Ihre Identitätsquelle ändern, wird eine neue Identitätsquellen-ID generiert. Überprüfen Sie, ob Sie die richtige ID verwenden, bevor Sie den Modus `AWS_SSO` in auf setzenUserGroupResolutionConfiguration.

So ändern Sie Ihre IAM-Identity-Center-Identitätsquelle

1. Öffnen Sie die IAM Identity Center>-Konsole.
2. Wählen Sie Settings (Einstellungen) aus.
3. Wählen Sie auf der Seite Einstellungen unter Identitätsquelle die Option Ändern aus.
4. Wählen Sie auf der Seite Identitätsquelle ändern Ihre bevorzugte Identitätsquelle und dann Weiter aus.

Erstellen eines Index

Sie können einen Index über die -Konsole oder durch Aufrufen der CreateIndex-API erstellen. Sie können die AWS Command Line Interface (AWS CLI) oder das SDK mit der API verwenden. Nachdem Sie Ihren Index erstellt haben, können Sie Dokumente direkt zu ihm oder aus einer Datenquelle hinzufügen.

Um einen Index zu erstellen, müssen Sie den Amazon-Ressourcennamen (ARN) einer AWS Identity and Access Management (IAM)-Rolle angeben, damit Indizes auf zugreifen können CloudWatch. Weitere Informationen finden Sie unter IAM Rollen für Indizes.

Die folgenden Registerkarten stellen ein Verfahren zum Erstellen eines Index mithilfe der AWS Management Consoleund Codebeispiele für die Verwendung der AWS CLIsowie Python- und Java-SDKs bereit.

Console

So erstellen Sie einen Index

1. Melden Sie sich bei der - AWS Managementkonsole an und öffnen Sie die - Amazon Kendra Konsole unter https://console.aws.amazon.com/kendra/.
2. Wählen Sie im Abschnitt Indizes die Option Index erstellen aus.
3. Geben Sie unter Indexdetails angeben einen Namen und eine Beschreibung für Ihren Index an.
4. Geben Sie IAM in Rolle eine - IAM Rolle an. Um eine Rolle zu finden, wählen Sie aus Rollen in Ihrem Konto, die das Wort „kendra“ enthalten, oder geben Sie den Namen einer anderen Rolle ein. Weitere Informationen zu den Berechtigungen, die die Rolle benötigt, finden Sie unter IAM Rollen für Indizes.
5. Wählen Sie Weiter aus.
6. Wählen Sie auf der Seite Benutzerzugriffskontrolle konfigurieren die Option Weiter aus. Sie können Ihren Index aktualisieren, um Token für die Zugriffskontrolle zu verwenden, nachdem Sie einen Index erstellt haben. Weitere Informationen finden Sie unter Steuern des Zugriffs auf Dokumente.
7. Wählen Sie auf der Seite mit den Bereitstellungsdetails die Option Erstellen aus.

8. Es kann einige Zeit dauern, bis der Index erstellt ist. Überprüfen Sie die Liste der Indizes, um den Fortschritt der Indexerstellung zu überwachen. Wenn der Status des Index lautet`ACTIVE`, ist Ihr Index einsatzbereit.

AWS CLI

So erstellen Sie einen Index

1. Verwenden Sie den folgenden Befehl, um einen Index zu erstellen. Der `role-arn` muss der Amazon-Ressourcenname (ARN) einer - IAM Rolle sein, die Amazon Kendra Aktionen ausführen kann. Weitere Informationen finden Sie unter IAM Rollen .

   Der Befehl ist für Linux und macOS formatiert. Wenn Sie Windows verwenden, ersetzen Sie das Unix-Zeilenfortsetzungszeichen (\) durch ein caret (^).

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

2. Es kann einige Zeit dauern, bis der Index erstellt ist. Um den Status Ihres Index zu überprüfen, verwenden Sie die von zurückgegebene Index-ID `create-index` mit dem folgenden Befehl. Wenn der Status des Index lautet`ACTIVE`, ist Ihr Index einsatzbereit.

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

Python

So erstellen Sie einen Index

- Geben Sie Werte für die folgenden Variablen im folgenden Codebeispiel an:
  - `description`– Eine Beschreibung des Index, den Sie erstellen. Dieser Schritt ist optional.
  - `index_name`– Der Name des Index, den Sie erstellen.
  - `role_arn`– Der Amazon-Ressourcenname (ARN) einer Rolle, die Amazon Kendra APIs ausführen kann. Weitere Informationen finden Sie unter IAM Rollen .

```
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

So erstellen Sie einen Index

- Geben Sie Werte für die folgenden Variablen im folgenden Codebeispiel an:
  - `description`– Eine Beschreibung des Index, den Sie erstellen. Dieser Schritt ist optional.
  - `index_name`– Der Name des Index, den Sie erstellen.
  - `role_arn`– Der Amazon-Ressourcenname (ARN) einer Rolle, die Amazon Kendra APIs ausführen kann. Weitere Informationen finden Sie unter IAM Rollen .

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

Nachdem Sie Ihren Index erstellt haben, fügen Sie ihm Dokumente hinzu. Sie können sie direkt hinzufügen oder eine Datenquelle erstellen, die Ihren Index regelmäßig aktualisiert.

Themen

- Hinzufügen von Dokumenten direkt zu einem Index mit Batch-Upload
- Hinzufügen häufig gestellter Fragen (FAQs) zu einem Index
- Erstellen von benutzerdefinierten Dokumentfeldern
- Steuern des Benutzerzugriffs auf Dokumente mit Tokens

Hinzufügen von Dokumenten direkt zu einem Index mit Batch-Upload

Sie können Dokumente mithilfe der BatchPutDocument API direkt zu einem Index hinzufügen. Sie können Dokumente nicht direkt über die Konsole hinzufügen. Wenn Sie die Konsole verwenden, stellen Sie eine Verbindung zu einer Datenquelle her, um Ihrem Index Dokumente hinzuzufügen. Dokumente können aus einem S3-Bucket hinzugefügt oder als Binärdaten bereitgestellt werden. Eine Liste der von unterstützten Dokumenttypen Amazon Kendra finden Sie unter Dokumenttypen.

Das Hinzufügen von Dokumenten zu einem Index mit `BatchPutDocument` ist eine asynchrone Operation. Nachdem Sie die `BatchPutDocument` API aufgerufen haben, verwenden Sie die BatchGetDocumentStatus API, um den Fortschritt der Indizierung Ihrer Dokumente zu überwachen. Wenn Sie die `BatchGetDocumentStatus` API mit einer Liste von Dokument-IDs aufrufen, wird der Status des Dokuments zurückgegeben. Wenn der Status des Dokuments `INDEXED` oder lautet`FAILED`, ist die Verarbeitung des Dokuments abgeschlossen. Wenn der Status lautet`FAILED`, gibt die `BatchGetDocumentStatus` API den Grund zurück, warum das Dokument nicht indiziert werden konnte.

Wenn Sie Ihre Inhalte und Dokumentmetadatenfelder oder Attribute während der Dokumentenerfassung ändern möchten, finden Sie weitere Informationen unter Amazon Kendra Anreicherung benutzerdefinierter Dokumente. Wenn Sie eine benutzerdefinierte Datenquelle verwenden möchten, benötigt jedes Dokument, das Sie mit der `BatchPutDocument` API einreichen, eine Datenquellen-ID und eine Ausführungs-ID als Attribute oder Felder. Weitere Informationen finden Sie unter Erforderliche Attribute für benutzerdefinierte Datenquellen.

> **Note**
>
> Jede Dokument-ID muss pro Index eindeutig sein. Sie können keine Datenquelle erstellen, um Ihre Dokumente mit ihren eindeutigen IDs zu indizieren, und dann die `BatchPutDocument`-API verwenden, um dieselben Dokumente zu indizieren, oder umgekehrt. Sie können eine Datenquelle löschen und dann die `BatchPutDocument` - API verwenden, um dieselben Dokumente zu indizieren, oder umgekehrt. Die Verwendung der `BatchDeleteDocument` APIs `BatchPutDocument` und in Kombination mit einem Amazon Kendra Datenquellen-Connector für denselben Satz von Dokumenten kann zu Inkonsistenzen bei Ihren Daten führen. Stattdessen empfehlen wir, den Amazon Kendra benutzerdefinierten Datenquellen-Konnektor zu verwenden.

Die folgenden Dokumente im Entwicklerhandbuch zeigen, wie Dokumente direkt zu einem Index hinzugefügt werden.

Themen

Hinzufügen von Dokumenten mit der BatchPutDocument API

Im folgenden Beispiel wird einem Index ein Textblob hinzugefügt, indem aufgerufen wirdBatchPutDocument. Sie können die `BatchPutDocument`-API verwenden, um Dokumente direkt zu Ihrem Index hinzuzufügen. Eine Liste der von unterstützten Dokumenttypen Amazon Kendra finden Sie unter Dokumenttypen.

Ein Beispiel für das Erstellen eines Index mit der AWS CLI und SDKs finden Sie unter Erstellen eines Index. Informationen zum Einrichten der CLI und der SDKs finden Sie unter Einrichten von Amazon Kendra.

> **Note**
>
> Dateien, die dem Index hinzugefügt werden, müssen sich in einem UTF-8-kodierten Byte-Stream befinden.

In den folgenden Beispielen wird dem Index UTF-8-kodierter Text hinzugefügt.

CLI

AWS Command Line InterfaceVerwenden Sie in der den folgenden Befehl. Der Befehl ist für Linux und macOS formatiert. Wenn Sie Windows verwenden, ersetzen Sie das Unix-Zeilenfortsetzungszeichen (\) durch ein caret (^).

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

Python

```
import boto3

kendra = boto3.client("kendra")

# Provide the index ID
index_id = "index-id"

# Provide the title and text
title = "Information about Amazon.com"
text = "Amazon.com is an online retailer."

document = {
    "Id": "1",
    "Blob": text,
    "ContentType": "PLAIN_TEXT",
    "Title": title
}

documents = [
    document
]

result = kendra.batch_put_document(
    IndexId = index_id,
    Documents = documents
)

print(result)
```

Java

```
package com.amazonaws.kendra;


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

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

        String indexId = "yourIndexId";

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

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

        BatchPutDocumentResponse result =
 kendra.batchPutDocument(batchPutDocumentRequest);

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

Hinzufügen von Dokumenten aus einem S3-Bucket

Sie können Dokumente mithilfe der API direkt aus einem BatchPutDocument- Amazon S3 Bucket zu Ihrem Index hinzufügen. Sie können bis zu 10 Dokumente in demselben Aufruf hinzufügen. Wenn Sie einen S3-Bucket verwenden, müssen Sie eine - IAM Rolle mit der Berechtigung für den Zugriff auf den Bucket bereitstellen, der Ihre Dokumente enthält. Sie geben die Rolle im `RoleArn` Parameter an.

Die Verwendung der BatchPutDocument API zum Hinzufügen von Dokumenten aus einem - Amazon S3 Bucket ist ein einmaliger Vorgang. Um einen Index mit dem Inhalt eines Buckets zu synchronisieren, erstellen Sie eine - Amazon S3 Datenquelle. Weitere Informationen finden Sie unter Amazon S3 Datenquelle .

Ein Beispiel für das Erstellen eines Index mit der AWS CLI und SDKs finden Sie unter Erstellen eines Index. Informationen zum Einrichten der CLI und der SDKs finden Sie unter Einrichten von Amazon

Kendra. Informationen zum Erstellen eines S3-Buckets finden Sie in der Amazon Simple Storage Service -Dokumentation.

Im folgenden Beispiel werden dem Index mithilfe der API zwei Microsoft Word`BatchPutDocument`-Dokumente hinzugefügt.

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));
    }
}
```

Hinzufügen häufig gestellter Fragen (FAQs) zu einem Index

Sie können häufig gestellte Fragen (FAQs) direkt über die Konsole oder die CreateFaq API zu Ihrem Index hinzufügen. Das Hinzufügen von FAQs Fragen zu einem Index ist eine asynchrone Operation. Sie speichern die Daten für die häufig gestellten Fragen in einer Datei, die Sie in einem - Amazon Simple Storage Service Bucket speichern. Sie können CSV- oder JSON-Dateien als Eingabe für Ihre häufig gestellten Fragen verwenden:

- Basic CSV – Eine CSV-Datei, in der jede Zeile eine Frage, eine Antwort und einen optionalen Quell-URI enthält.
- Benutzerdefiniertes CSV – Eine CSV-Datei, die Fragen, Antworten und Kopfzeilen für benutzerdefinierte Felder/Attribute enthält, die Sie verwenden können, um Antworten auf häufig gestellte Fragen zu Facetten, anzuzeigen oder zu sortieren. Sie können auch Zugriffskontrollfelder definieren, um die Antwort auf häufig gestellte Fragen auf bestimmte Benutzer und Gruppen zu beschränken, die die Antwort auf häufig gestellte Fragen sehen dürfen.
- JSON – Eine JSON-Datei mit Fragen, Antworten und benutzerdefinierten Feldern/Attributen, die Sie verwenden können, um Antworten auf häufig gestellte Fragen zu Facetten, anzuzeigen oder zu sortieren. Sie können auch Zugriffskontrollfelder definieren, um die Antwort auf häufig gestellte Fragen auf bestimmte Benutzer und Gruppen zu beschränken, die die Antwort auf häufig gestellte Fragen sehen dürfen.

Im Folgenden finden Sie beispielsweise eine einfache CSV-Datei, die Antworten auf Fragen zu kostenlosen Unterhaltungen in Spokane, Puerto USA und Lake View, Missouri, USA bietet.

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

> **Note**
>
> Die Datei mit häufig gestellten Fragen muss eine UTF-8-encoded Datei sein.

Themen

Erstellen von Indexfeldern für eine FAQ-Datei

Wenn Sie eine benutzerdefinierte CSV- oder JSON-Datei für die Eingabe verwenden, können Sie benutzerdefinierte Felder für Ihre häufig gestellten Fragen deklarieren. Sie können beispielsweise ein benutzerdefiniertes Feld erstellen, das jede häufig gestellte Frage einer Geschäftsabteilung zuweist. Wenn die häufig gestellten Fragen als Antwort zurückgegeben werden, können Sie die Abteilung als Facette verwenden, um die Suche beispielsweise auf „Personal“ oder „Finanzen“ zu beschränken.

Ein benutzerdefiniertes Feld muss einem Indexfeld zugeordnet werden. In der Konsole verwenden Sie die Facet-Definitionsseite, um ein Indexfeld zu erstellen. Wenn Sie die API verwenden, müssen Sie zunächst ein Indexfeld mit der UpdateIndex API erstellen.

Der Feld-/Attributtyp in der Datei mit häufig gestellten Fragen muss mit dem Typ des zugehörigen Indexfelds übereinstimmen. Das Feld „Abteilung“ ist beispielsweise ein `STRING_LIST` Typfeld. Daher müssen Sie Werte für das Abteilungsfeld als Zeichenfolgenliste in Ihrer Datei mit häufig gestellten Fragen angeben. Sie können den Typ der Indexfelder auf der Facet-Definitionsseite in der Konsole oder mithilfe der DescribeIndex API überprüfen.

Wenn Sie ein Indexfeld erstellen, das einem benutzerdefinierten Attribut zugeordnet ist, können Sie es als anzeigbar, Facettenbar oder sortierbar markieren. Sie können ein benutzerdefiniertes Attribut nicht durchsuchbar machen.

Zusätzlich zu den benutzerdefinierten Attributen können Sie auch die Amazon Kendra reservierten oder allgemeinen Felder in einer benutzerdefinierten CSV- oder JSON-Datei verwenden. Weitere Informationen finden Sie unter Dokumentattribute oder Felder.

Grundlegende CSV-Datei

Verwenden Sie eine einfache CSV-Datei, wenn Sie eine einfache Struktur für Ihre FAQs verwenden möchten. In einer einfachen CSV-Datei hat jede Zeile zwei oder drei Felder: eine Frage, eine Antwort und eine optionale Quell-URI, die auf ein Dokument mit weiteren Informationen verweist.

Der Inhalt der Datei muss dem RFC 4180 Common Format und dem MIME-Typ für CSV-Dateien (Comma-Separated Values) entsprechen.

Im Folgenden finden Sie eine FAQ-Datei im grundlegenden CSV-Format.

```
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
```

Benutzerdefinierte CSV-Datei

Verwenden Sie eine benutzerdefinierte CSV-Datei, wenn Sie Ihren häufig gestellten Fragen benutzerdefinierte Felder/Attribute hinzufügen möchten. Für eine benutzerdefinierte CSV-Datei verwenden Sie eine Kopfzeile in Ihrer CSV-Datei, um die zusätzlichen Attribute zu definieren.

Die CSV-Datei muss die folgenden zwei Pflichtfelder enthalten:

- `_question`– Die häufig gestellte Frage
- `_answer`– Die Antwort auf die häufig gestellte Frage

Ihre -Datei kann sowohl Amazon Kendra reservierte Felder als auch benutzerdefinierte Felder enthalten. Im Folgenden finden Sie ein Beispiel für eine benutzerdefinierte CSV-Datei.

```
_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
```

Der Inhalt der benutzerdefinierten Datei muss dem RFC 4180 Common Format und dem MIME-Typ für CSV-Dateien (Comma-Separated Values) entsprechen.

Im Folgenden werden die Typen von benutzerdefinierten Feldern aufgeführt:

- Datum – ISO 8601-kodierte Datums- und Zeitwerte.

  Beispiel: 2012-03-25T12:30:10+01:00 ist das ISO 8601-Datum-Uhrzeit-Format für den 25. März 2012 um 23:30 Uhr (plus 10 Sekunden) in der mittelEuropazeitzone.
- Lang – Zahlen, z. B. `1234`.
- Zeichenfolge – Zeichenfolgenwerte. Wenn Ihre Zeichenfolge Kommas enthält, schließen Sie den gesamten Wert in doppelte Anführungszeichen (") ein (z. B. `"custom attribute, and more"`).
- Zeichenfolgenliste – Eine Liste von Zeichenfolgenwerten. Listen Sie die Werte in einer durch Komma getrennten Liste auf, die in Anführungszeichen (") eingeschlossen ist (z. B. `"item1, item2, item3"`). Wenn die Liste nur einen einzigen Eintrag enthält, können Sie die Anführungszeichen weglassen (z. B. `item1`).

Eine benutzerdefinierte CSV-Datei kann Benutzerzugriffskontrollfelder enthalten. Sie können diese Felder verwenden, um den Zugriff auf die häufig gestellten Fragen auf bestimmte Benutzer und Gruppen zu beschränken. Um nach Benutzerkontext zu filtern, muss der Benutzer Benutzer Benutzer- und Gruppeninformationen in der Abfrage angeben. Andernfalls werden alle relevanten FAQs Fragen zurückgegeben. Weitere Informationen finden Sie unter Filterung des Benutzerkontexts.

Im Folgenden werden die Benutzerkontextfilter für FAQs Fragen aufgeführt:

- `_acl_user_allow`– Benutzer in der Zulassungsliste können die häufig gestellten Fragen in der Abfrageantwort sehen. Die häufig gestellten Fragen werden nicht an andere Benutzer zurückgegeben.
- `_acl_user_deny`– Benutzer in der Sperrliste können die häufig gestellten Fragen in der Abfrageantwort nicht sehen. Die häufig gestellten Fragen werden an alle anderen Benutzer zurückgegeben, wenn sie für die Abfrage relevant sind.

- `_acl_group_allow`– Benutzer, die Mitglieder einer zulässigen Gruppe sind, können die häufig gestellten Fragen in der Abfrageantwort sehen. Die häufig gestellten Fragen werden nicht an Benutzer zurückgegeben, die Mitglieder einer anderen Gruppe sind.
- `_acl_group_deny`– Benutzer, die Mitglieder einer verweigerten Gruppe sind, können die häufig gestellten Fragen in der Abfrageantwort nicht sehen. Die häufig gestellten Fragen werden an andere Gruppen zurückgegeben, wenn sie für die Abfrage relevant sind.

Geben Sie die Werte für die Zulassungs- und Verweigerungslisten in kommagetrennten Listen an, die in Anführungszeichen eingeschlossen sind (z. B. `"user1,user2,user3"`). Sie können einen Benutzer oder eine Gruppe entweder in eine Zulassungsliste oder eine Sperrliste aufnehmen, aber nicht beide, bei denen derselbe Benutzer einzeln zugelassen, aber auch die Gruppe verweigert wird. Wenn Sie einen Benutzer oder eine Gruppe in beide einschließen, erhalten Sie eine Fehlermeldung.

Im Folgenden finden Sie ein Beispiel für eine benutzerdefinierte CSV-Datei mit Benutzerkontextinformationen.

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

JSON-Datei

Sie können eine JSON-Datei verwenden, um Fragen, Antworten und Felder für Ihren Index bereitzustellen. Sie können jedes der Amazon Kendra reservierten Felder oder benutzerdefinierten Felder zu den häufig gestellten Fragen hinzufügen.

Im Folgenden finden Sie das Schema für die JSON-Datei.

```
{
    "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
    ]
}
```

Die folgende JSON-Beispieldatei zeigt zwei häufig gestellte Fragen. Eines der Dokumente enthält nur die erforderliche Frage und Antwort. Das andere Dokument enthält auch zusätzliche Informationen zum Feld- und Benutzerkontext oder zur Zugriffskontrolle.

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

```
    ]
}
```

Im Folgenden werden die Typen von benutzerdefinierten Feldern aufgeführt:

- Datum – Ein JSON-Zeichenfolgenwert mit ISO 8601-kodierten Datums- und Zeitwerten. Beispiel: 2012-03-25T12:30:10+01:00 ist das ISO 8601-Datum-Uhrzeit-Format für den 25. März 2012 um 23:30 Uhr (plus 10 Sekunden) in der mittelEuropazeitzone.
- Lang – Ein JSON-Nummernwert, z. B. `1234`.
- Zeichenfolge – Ein JSON-Zeichenfolgenwert (z. B. `"custom attribute"`).
- Zeichenfolgenliste – Ein JSON-Array von Zeichenfolgenwerten (z. B. `["item1,item2,item3"]`).

Eine JSON-Datei kann Benutzerzugriffskontrollfelder enthalten. Sie können diese Felder verwenden, um den Zugriff auf die häufig gestellten Fragen auf bestimmte Benutzer und Gruppen zu beschränken. Um nach Benutzerkontext zu filtern, muss der Benutzer Benutzer Benutzer- und Gruppeninformationen in der Abfrage angeben. Andernfalls werden alle relevanten FAQs Fragen zurückgegeben. Weitere Informationen finden Sie unter Filtern des Benutzerkontexts.

Sie können einen Benutzer oder eine Gruppe entweder in eine Zulassungsliste oder eine Sperrliste aufnehmen, aber nicht beide, bei denen derselbe Benutzer einzeln zugelassen, aber auch die Gruppe verweigert wird. Wenn Sie einen Benutzer oder eine Gruppe in beide einschließen, erhalten Sie eine Fehlermeldung.

Im Folgenden finden Sie ein Beispiel für die Einbindung der Benutzerzugriffssteuerung in eine JSON-FAQ.

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

Verwenden Ihrer FAQ-Datei

Nachdem Sie Ihre Eingabedatei mit häufig gestellten Fragen in einem S3-Bucket gespeichert haben, verwenden Sie die -Konsole oder die `CreateFaq`-API, um die Fragen und Antworten in Ihren Index zu speichern. Wenn Sie eine häufig gestellte Frage aktualisieren möchten, löschen Sie die häufig gestellten Fragen und erstellen Sie sie erneut. Sie verwenden die `DeleteFaq`-API, um häufig gestellte Fragen zu löschen.

Sie müssen eine - IAM Rolle bereitstellen, die Zugriff auf den S3-Bucket hat, der Ihre Quelldateien enthält. Sie geben die Rolle in der -Konsole oder im -`RoleArn`Parameter an. Im Folgenden finden Sie ein Beispiel für das Hinzufügen einer FAQ-Datei zu einem Index.

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));

    }
}
```

Häufig gestellte Fragen zu Dateien in anderen Sprachen als Englisch

Sie können häufig gestellte Fragen in einer unterstützten Sprache indizieren. Amazon Kendra Indiziert häufig gestellte FAQs standardmäßig auf Englisch, wenn Sie keine Sprache angeben. Sie geben den Sprachcode an, wenn Sie die -CreateFaqOperation aufrufen, oder Sie können den Sprachcode für eine häufig gestellte Frage in die Metadaten der häufig gestellten Fragen als Feld aufnehmen. Wenn für eine häufig gestellte Frage in ihren Metadaten kein Sprachcode in einem Metadatenfeld angegeben ist, werden die häufig gestellten Fragen mit dem Sprachcode indiziert, der

beim Aufrufen der `CreateFAQ` Operation angegeben wird. Um ein Dokument mit häufig gestellten Fragen in einer unterstützten Sprache in der Konsole zu indizieren, gehen Sie zu FAQs Fragen und wählen Sie Häufig gestellte Fragen hinzufügen aus. Sie wählen eine Sprache aus der Dropdown-Liste Sprache aus.

Erstellen von benutzerdefinierten Dokumentfeldern

Sie können benutzerdefinierte Attribute oder Felder für Ihre Dokumente in Ihrem Amazon-Kendra-Index erstellen. Sie können beispielsweise ein benutzerdefiniertes Feld oder Attribut namens „Abteilung“ mit den Werten „Personal“, „Vertrieb“ und „Produktion“ erstellen. Wenn Sie diese benutzerdefinierten Felder oder Attribute Ihrem Amazon-Kendra-Index zuordnen, können Sie sie verwenden, um die Suchergebnisse so zu filtern, dass Dokumente nach dem Abteilungsattribut „HR“ eingeschlossen werden.

Bevor Sie ein benutzerdefiniertes Feld oder Attribut verwenden können, müssen Sie zuerst das Feld im Index erstellen. Verwenden Sie die -Konsole, um die Zuordnungen von Datenquellenfeldern zu bearbeiten und ein benutzerdefiniertes Feld hinzuzufügen, oder verwenden Sie die UpdateIndex -API, um das Indexfeld zu erstellen. Sie können den Felddatentyp nicht mehr ändern, nachdem Sie das Feld erstellt haben.

Für die meisten Datenquellen ordnen Sie Felder in der externen Datenquelle den entsprechenden Feldern in zu Amazon Kendra. Weitere Informationen finden Sie unter Zuweisen von Datenquellenfeldern. Für S3-Datenquellen können Sie benutzerdefinierte Felder oder Attribute mithilfe einer JSON-Metadatendatei erstellen.

Sie können bis zu 500 benutzerdefinierte Felder oder Attribute erstellen.

Sie können auch Amazon Kendra reservierte oder allgemeine Felder verwenden. Weitere Informationen finden Sie unter Dokumentattribute oder Felder.

Themen

- Aktualisieren von benutzerdefinierten Dokumentfeldern

Aktualisieren von benutzerdefinierten Dokumentfeldern

Mit der `UpdateIndex` -API fügen Sie benutzerdefinierte Felder oder Attribute mithilfe des `-DocumentMetadataConfigurationUpdates`Parameters hinzu.

Im folgenden JSON-Beispiel wird verwendet`DocumentMetadataConfigurationUpdates`, um dem Index ein Feld namens „Abteilung“ hinzuzufügen.

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

Die folgenden Abschnitte enthalten Beispiele für das Hinzufügen benutzerdefinierter Attribute oder Felder mithilfe der BatchPutDocument und für eine Amazon S3-Datenquelle.

Themen

- Hinzufügen von benutzerdefinierten Attributen oder Feldern mit der BatchPutDocument API
- Hinzufügen von benutzerdefinierten Attributen oder Feldern zu einer Amazon S3 Datenquelle

Hinzufügen von benutzerdefinierten Attributen oder Feldern mit der BatchPutDocument API

Wenn Sie die BatchPutDocument-API verwenden, um Ihrem Index ein Dokument hinzuzufügen, geben Sie benutzerdefinierte Felder oder Attribute als Teil von an`Attributes`. Sie können mehrere Felder oder Attribute hinzufügen, wenn Sie die -API aufrufen. Sie können bis zu 500 benutzerdefinierte Felder oder Attribute erstellen. Das folgende Beispiel ist ein benutzerdefiniertes Feld oder Attribut, das einem Dokument „Abteilung“ hinzufügt.

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

Hinzufügen von benutzerdefinierten Attributen oder Feldern zu einer Amazon S3 Datenquelle

Wenn Sie einen S3-Bucket als Datenquelle für Ihren Index verwenden, fügen Sie den Dokumenten Metadaten mit zugehörigen Metadatendateien hinzu. Sie speichern die Metadaten-JSON-Dateien

in einer Verzeichnisstruktur, die parallel zu Ihren Dokumenten ist. Weitere Informationen finden Sie unter S3-Dokumentmetadaten.

Sie geben benutzerdefinierte Felder oder Attribute in der `Attributes` JSON-Struktur an. Sie können bis zu 500 benutzerdefinierte Felder oder Attribute erstellen. Im folgenden Beispiel wird beispielsweise verwendet, `Attributes` um drei benutzerdefinierte Felder oder Attribute und ein reserviertes Feld zu definieren.

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

Die folgenden Schritte führen Sie durch das Hinzufügen benutzerdefinierter Attribute zu einer Amazon S3-Datenquelle.

Themen

- Schritt 1: Erstellen eines Amazon-Kendra-Index
- Schritt 2: Aktualisieren des Index, um benutzerdefinierte Dokumentfelder hinzuzufügen
- Schritt 3: Erstellen einer Amazon S3-Datenquelle und Zuordnen von Datenquellenfeldern zu benutzerdefinierten Attributen

Schritt 1: Erstellen eines Amazon-Kendra-Index

Führen Sie die Schritte unter ausErstellen eines Index, um Ihren Amazon-Kendra-Index zu erstellen.

Schritt 2: Aktualisieren des Index, um benutzerdefinierte Dokumentfelder hinzuzufügen

Nachdem Sie einen Index erstellt haben, fügen Sie ihm Felder hinzu. Das folgende Verfahren zeigt, wie Sie mithilfe der Konsole und der CLI Felder zu einem Index hinzufügen.

Console

So erstellen Sie Indexfelder

1. Stellen Sie sicher, dass Sie einen Index erstellt haben.
2. Wählen Sie dann im linken Navigationsmenü unter Datenverwaltung die Option Facettendefinition aus.

3. Wählen Sie im Leitfaden Indexfeldeinstellungen unter Indexfelder die Option Feld hinzufügen aus, um benutzerdefinierte Felder hinzuzufügen.
4. Gehen Sie im Dialogfeld Indexfeld hinzufügen wie folgt vor:

   - Feldname – Fügen Sie einen Feldnamen hinzu.
   - Datentyp – Wählen Sie den Datentyp aus, unabhängig davon, ob Zeichenfolge , Zeichenfolgenliste oder Datum .
   - Verwendungstypen – Wählen Sie Nutzungstypen aus, unabhängig davon, ob Facetable ,Searchable ,Displayable und Sortable ist.

     Wählen Sie dann Hinzufügen aus.

   Wiederholen Sie den letzten Schritt für alle anderen Felder, die Sie zuordnen möchten.

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
        }
```

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

Schritt 3: Erstellen einer Amazon S3-Datenquelle und Zuordnen von Datenquellenfeldern zu benutzerdefinierten Attributen

Um eine Amazon S3-Datenquelle zu erstellen und ihr Felder zuzuordnen, folgen Sie den Anweisungen unter Amazon S3.

Wenn Sie die API verwenden, verwenden Sie das `fieldMappings` Attribut unter , `configuration` wenn Sie die CreateDataSource API verwenden.

Eine Übersicht über die Zuordnung von Datenquellenfeldern finden Sie unter Zuordnen von Datenquellenfeldern.

Steuern des Benutzerzugriffs auf Dokumente mit Tokens

Sie können steuern, welche Benutzer oder Gruppen auf bestimmte Dokumente in Ihrem Index zugreifen oder bestimmte Dokumente in ihren Suchergebnissen sehen können. Dies wird als Benutzerkontextfilterung bezeichnet. Es handelt sich um eine Art personalisierte Suche mit dem Vorteil, den Zugriff auf Dokumente zu kontrollieren. Beispielsweise sollten nicht alle Teams, die das Unternehmensportal nach Informationen durchsuchen, auf streng geheime Unternehmensdokumente zugreifen, und diese Dokumente sind auch nicht für alle Benutzer relevant. Nur bestimmte Benutzer oder Gruppen von Teams, die Zugriff auf streng geheime Dokumente haben, sollten diese Dokumente in ihren Suchergebnissen sehen.

Amazon Kendraunterstützt die tokenbasierte Benutzerzugriffskontrolle mithilfe der folgenden Tokentypen:

- ID öffnen
- JWT mit einem gemeinsamen Geheimnis
- JWT mit einem öffentlichen Schlüssel
- JSON

Amazon Kendrabietet eine hochsichere Unternehmenssuche für Ihre Suchanwendungen. Ihre Suchergebnisse spiegeln das Sicherheitsmodell Ihres Unternehmens wider. Kunden sind dafür

verantwortlich, Benutzer zu authentifizieren und zu autorisieren, um Zugriff auf ihre Suchanwendung zu erhalten. Zur Suchzeit ist derAmazon KendraDer Dienst filtert Suchergebnisse auf der Grundlage der Benutzer-ID, die von der Suchanwendung des Kunden bereitgestellt wird, und anhand von Zugriffskontrolllisten (ACLs) für Dokumente, die von derAmazon KendraKonnektoren während der Crawl-/Indizierungszeit. Die Suchergebnisse enthalten URLs, die auf die ursprünglichen Dokumentablagen verweisen, sowie kurze Auszüge. Der Zugriff auf das vollständige Dokument wird weiterhin vom ursprünglichen Repository erzwungen.

Themen

OpenID verwenden

Um einen Amazon Kendra Index so zu konfigurieren, dass er ein OpenID-Token für die Zugriffskontrolle verwendet, benötigen Sie die JWKS-URL (JSON Web Key Set) vom OpenID-Anbieter. In den meisten Fällen hat die JWKS-URL das folgende Format (sofern sie der OpenID-Erkennung folgen). `https://domain-name/.well_known/jwks.json`

Die folgenden Beispiele zeigen, wie Sie ein OpenID-Token für die Benutzerzugriffskontrolle verwenden, wenn Sie einen Index erstellen.

Console

1. Wählen Sie Index erstellen, um mit der Erstellung eines neuen Indexes zu beginnen.
2. Geben Sie auf der Seite Indexdetails angeben Ihrem Index einen Namen und eine Beschreibung.
3. Wählen Sie IAM unter Rolle eine Rolle aus, oder wählen Sie Neue Rolle erstellen für und geben Sie einen Rollennamen an, um eine neue Rolle zu erstellen. Die IAM-Rolle wird das Präfix "AmazonKendra-“ haben.
4. Behalten Sie für alle anderen Felder die Standardwerte bei. Wählen Sie Weiter aus.
5. Wählen Sie auf der Seite Benutzerzugriffskontrolle konfigurieren unter Einstellungen für die Zugriffskontrolle die Option Ja aus, um Token für die Zugriffskontrolle zu verwenden.
6. Wählen Sie unter Token-Konfiguration OpenID als Token-Typ aus.

7. Geben Sie eine URL für den Signaturschlüssel an. Die URL sollte auf eine Reihe von JSON-Webschlüsseln verweisen.
8. Optional unter „Erweiterte Konfiguration“:
    a. Geben Sie einen Benutzernamen an, der bei der ACL-Prüfung verwendet werden soll.
    b. Geben Sie eine oder mehrere Gruppen an, die bei der ACL-Prüfung verwendet werden sollen.
    c. Geben Sie den Aussteller an, der den Token-Aussteller validieren wird.
    d. Geben Sie die Client-ID (s) an. Sie müssen einen regulären Ausdruck angeben, der der Zielgruppe im JWT entspricht.
9. Wählen Sie auf der Seite mit den Bereitstellungsdetails die Developer Edition aus.
10. Wählen Sie Erstellen, um Ihren Index zu erstellen.
11. Warten Sie, bis Ihr Index erstellt wurde. Amazon Kendra stellt die Hardware für Ihren Index bereit. Dieser Vorgang kann einige Zeit in Anspruch nehmen.

CLI

Um AWS CLI mithilfe einer JSON-Eingabedatei einen Index zu erstellen, erstellen Sie zunächst eine JSON-Datei mit den gewünschten Parametern:

```
{
    "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"
}
```

Sie können die standardmäßigen Benutzer- und Gruppenfeldnamen überschreiben. Der Standardwert für `UserNameAttributeField` ist „Benutzer“. Der Standardwert für `GroupAttributeField` ist „Gruppen“.

Rufen Sie als Nächstes `create-index` mit der Eingabedatei auf. Wenn der Name Ihrer JSON-Datei beispielsweise lautet`create-index-openid.json`, können Sie Folgendes verwenden:

```
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'
)
```

Verwenden eines JSON-Web-Tokens (JWT) mit einem gemeinsamen geheimen Schlüssel

Die folgenden Beispiele zeigen, wie Sie JSON Web Token (JWT) mit einem Shared Secret-Token für die Benutzerzugriffskontrolle verwenden, wenn Sie einen Index erstellen.

Console

1. Wählen Sie Create Index aus, um mit der Erstellung eines neuen Indexes zu beginnen.

2. Geben Sie auf der Seite Indexdetails angeben Ihrem Index einen Namen und eine Beschreibung.
3. Wählen Sie für die IAM-Rolle eine Rolle aus, oder wählen Sie Neue Rolle erstellen für und geben Sie einen Rollennamen an, um eine neue Rolle zu erstellen. Die IAM Rolle wird das Präfix "AmazonKendra-“ haben.
4. Behalten Sie für alle anderen Felder ihre Standardwerte bei. Wählen Sie Weiter aus.
5. Wählen Sie auf der Seite Benutzerzugriffskontrolle konfigurieren unter Einstellungen für die Zugriffskontrolle die Option Ja aus, um Token für die Zugriffskontrolle zu verwenden.
6. Wählen Sie unter Tokenkonfiguration JWT with Shared Secret als Tokentyp aus.
7. Wählen Sie unter Parameter für das Signieren von Shared Secret den Typ des Geheimnisses aus. Sie können einen vorhandenen AWS Secrets Manager gemeinsamen geheimen Schlüssel verwenden oder einen neuen gemeinsamen geheimen Schlüssel erstellen.

   Um einen neuen gemeinsamen geheimen Schlüssel zu erstellen, wählen Sie Neu und gehen Sie dann wie folgt vor:

   a. Geben Sie unter Neuer AWS Secrets Manager geheimer Schlüssel einen geheimen Namen an. Das Präfix `AmazonKendra-` wird hinzugefügt, wenn Sie den öffentlichen Schlüssel speichern.
   b. Geben Sie eine Schlüssel-ID an. Die Schlüssel-ID ist ein Hinweis, der angibt, welcher Schlüssel verwendet wurde, um die JSON-Websignatur des Tokens zu sichern.
   c. Wählen Sie den Signaturalgorithmus für das Token. Dies ist der kryptografische Algorithmus, der zur Sicherung des ID-Tokens verwendet wird. For more information on RSA, see RSA Cryptography.
   d. Geben Sie einen gemeinsamen geheimen Schlüssel an, indem Sie einen Base64-URL-codierten Schlüssel eingeben. Sie können auch „Geheim generieren“ auswählen, um ein Geheimnis für Sie generieren zu lassen. Sie müssen sicherstellen, dass es sich bei dem Secret um ein Base64-URL-kodiertes Geheimnis handelt.
   e. (Optional) Geben Sie an, wann der gemeinsame geheime Schlüssel gültig ist. Sie können das Datum und die Uhrzeit angeben, ab dem ein Geheimnis gültig ist, bis wann es gültig ist oder beides. Das Geheimnis ist in dem angegebenen Intervall gültig.
   f. Wählen Sie Geheim speichern, um das neue Geheimnis zu speichern.
8. (Optional) Gehen Sie unter Erweiterte Konfiguration wie folgt vor:

   a. Geben Sie einen Benutzernamen an, der bei der ACL-Prüfung verwendet werden soll.

b. Geben Sie eine oder mehrere Gruppen an, die bei der ACL-Prüfung verwendet werden sollen.

c. Geben Sie den Aussteller an, der den Token-Aussteller validieren wird.

d. Geben Sie die Antragsnummer (n) an. Sie müssen einen regulären Ausdruck angeben, der der Zielgruppe im JWT entspricht.

9. Wählen Sie auf der Seite mit den Bereitstellungsdetails die Developer Edition aus.
10. Wählen Sie Erstellen, um Ihren Index zu erstellen.
11. Warten Sie, bis Ihr Index erstellt wurde. Amazon Kendra stellt die Hardware für Ihren Index bereit. Dieser Vorgang kann einige Zeit in Anspruch nehmen.

CLI

Sie können das JWT-Token mit einem gemeinsamen geheimen Schlüssel verwenden. AWS Secrets Manager Das Geheimnis muss ein Base64-URL-kodiertes Geheimnis sein. Sie benötigen den Secrets Manager ARN, und Ihre Amazon Kendra Rolle muss Zugriff `GetSecretValue` auf die Secrets Manager Ressource haben. Wenn Sie die Secrets Manager Ressource mit verschlüsseln AWS KMS, muss die Rolle auch Zugriff auf die Entschlüsselungsaktion haben.

Um AWS CLI mithilfe einer JSON-Eingabedatei einen Index zu erstellen, erstellen Sie zunächst eine JSON-Datei mit den gewünschten Parametern:

```
{
    "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"
```

```
}
```

Sie können die standardmäßigen Benutzer- und Gruppenfeldnamen überschreiben. Der Standardwert für `UserNameAttributeField` ist „Benutzer“. Der Standardwert für `GroupAttributeField` ist „Gruppen“.

Rufen Sie als Nächstes `create-index` mit der Eingabedatei auf. Wenn der Name Ihrer JSON-Datei beispielsweise lautet`create-index-openid.json`, können Sie Folgendes verwenden:

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

Das Geheimnis muss das folgende Format haben 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"
    }
  ]
}
```

Weitere Informationen zu JWT finden Sie unter jwt.io.

Python

Sie können das JWT-Token mit einem gemeinsamen geheimen Schlüssel darin verwenden. AWS Secrets Manager Das Geheimnis muss ein Base64-URL-kodiertes Geheimnis sein. Sie benötigen den Secrets Manager ARN, und Ihre Amazon Kendra Rolle muss Zugriff `GetSecretValue` auf die Secrets Manager Ressource haben. Wenn Sie die Secrets Manager Ressource mit verschlüsseln AWS KMS, muss die Rolle auch Zugriff auf die Entschlüsselungsaktion haben.

```
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'
)
```

Verwenden eines JSON Web Tokens (JWT) mit einem öffentlichen Schlüssel

Die folgenden Beispiele zeigen, wie Sie JSON Web Token (JWT) mit einem öffentlichen Schlüssel für die Benutzerzugriffskontrolle verwenden, wenn Sie einen Index erstellen. Weitere Informationen zu JWT finden Sie unter jwt.io.

Console

1. Wählen Sie Create index, um mit der Erstellung eines neuen Indexes zu beginnen.
2. Geben Sie auf der Seite Indexdetails angeben Ihrem Index einen Namen und eine Beschreibung.
3. Wählen Sie für die IAM-Rolle eine Rolle aus, oder wählen Sie Neue Rolle erstellen für und geben Sie einen Rollennamen an, um eine neue Rolle zu erstellen. Die IAM Rolle wird das Präfix "AmazonKendra-“ haben.
4. Behalten Sie für alle anderen Felder ihre Standardwerte bei. Wählen Sie Weiter aus.
5. Wählen Sie auf der Seite Benutzerzugriffskontrolle konfigurieren unter Einstellungen für die Zugriffskontrolle die Option Ja aus, um Token für die Zugriffskontrolle zu verwenden.
6. Wählen Sie unter Tokenkonfiguration JWT mit öffentlichem Schlüssel als Tokentyp aus.
7. Wählen Sie unter Parameter für das Signieren eines öffentlichen Schlüssels den Typ des Geheimnisses aus. Sie können ein vorhandenes AWS Secrets Manager Geheimnis verwenden oder ein neues Geheimnis erstellen.

Um ein neues Geheimnis zu erstellen, wählen Sie Neu und gehen Sie dann wie folgt vor:

a. Geben Sie unter Neues AWS Secrets Manager Geheimnis einen geheimen Namen ein. Das Präfix `AmazonKendra-` wird hinzugefügt, wenn Sie den öffentlichen Schlüssel speichern.

b. Geben Sie eine Schlüssel-ID an. Die Schlüssel-ID ist ein Hinweis, der angibt, welcher Schlüssel verwendet wurde, um die JSON-Websignatur des Tokens zu sichern.

c. Wählen Sie den Signaturalgorithmus für das Token. Dies ist der kryptografische Algorithmus, der zur Sicherung des ID-Tokens verwendet wird. For more information on RSA, see RSA Cryptography.

d. Geben Sie unter Zertifikatattribute eine optionale Zertifikatskette an. Die Zertifikatskette besteht aus einer Liste von Zertifikaten. Sie beginnt mit einem Serverzertifikat und endet mit dem Stammzertifikat.

e. Optional: Geben Sie den Fingerabdruck oder Fingerabdruck an. Es sollte sich um einen Hash eines Zertifikats handeln, der aus allen Zertifikatsdaten und der zugehörigen Signatur berechnet wird.

f. Geben Sie den Exponenten an. Dies ist der Exponentenwert für den öffentlichen RSA-Schlüssel. Er wird als Base64urlUInt-kodierten Wert dargestellt.

g. Geben Sie den Modulus an. Dies ist der Exponentenwert für den öffentlichen RSA-Schlüssel. Er wird als Base64urlUInt-kodierten Wert dargestellt.

h. Wählen Sie Schlüssel speichern, um den neuen Schlüssel zu speichern.

8. Optional unter „Erweiterte Konfiguration“:

a. Geben Sie einen Benutzernamen an, der bei der ACL-Prüfung verwendet werden soll.

b. Geben Sie eine oder mehrere Gruppen an, die bei der ACL-Prüfung verwendet werden sollen.

c. Geben Sie den Aussteller an, der den Token-Aussteller validieren wird.

d. Geben Sie die Client-ID (s) an. Sie müssen einen regulären Ausdruck angeben, der der Zielgruppe im JWT entspricht.

9. Wählen Sie auf der Seite mit den Bereitstellungsdetails die Developer Edition aus.

10. Wählen Sie Erstellen, um Ihren Index zu erstellen.

11. Warten Sie, bis Ihr Index erstellt wurde. Amazon Kendra stellt die Hardware für Ihren Index bereit. Dieser Vorgang kann einige Zeit in Anspruch nehmen.

CLI

Sie können JWT mit einem öffentlichen Schlüssel in einem AWS Secrets Manager verwenden. Sie benötigen den Secrets Manager ARN, und Ihre Amazon Kendra Rolle muss Zugriff `GetSecretValue` auf die Secrets Manager Ressource haben. Wenn Sie die Secrets Manager Ressource mit verschlüsseln AWS KMS, muss die Rolle auch Zugriff auf die Entschlüsselungsaktion haben.

Um AWS CLI mithilfe einer JSON-Eingabedatei einen Index zu erstellen, erstellen Sie zunächst eine JSON-Datei mit den gewünschten Parametern:

```
{
    "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"
}
```

Sie können die standardmäßigen Benutzer- und Gruppenfeldnamen überschreiben. Der Standardwert für `UserNameAttributeField` ist „Benutzer“. Der Standardwert für `GroupAttributeField` ist „Gruppen“.

Rufen Sie als Nächstes `create-index` mit der Eingabedatei auf. Wenn der Name Ihrer JSON-Datei beispielsweise lautet`create-index-openid.json`, können Sie Folgendes verwenden:

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

Das Geheimnis muss das folgende Format haben 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"
      ]
    }
  ]
}
```

Weitere Informationen zu JWT finden Sie unter 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'
)
```

Verwendung von JSON:

Die folgenden Beispiele zeigen, wie Sie JSON für die Benutzerzugriffskontrolle verwenden, wenn Sie einen Index erstellen.

> **Warning**
>
> Das JSON-Token ist eine nicht validierte Nutzlast. Dies sollte nur verwendet werden, wenn Anfragen von einem vertrauenswürdigen Server Amazon Kendra kommen, und niemals von einem Browser.

Console

1. Wählen Sie Index erstellen, um mit der Erstellung eines neuen Indexes zu beginnen.
2. Geben Sie auf der Seite Indexdetails angeben Ihrem Index einen Namen und eine Beschreibung.
3. Wählen Sie IAM unter Rolle eine Rolle aus oder wählen Sie Neue Rolle erstellen für und geben Sie einen Rollennamen an, um eine neue Rolle zu erstellen. Die IAM Rolle wird das Präfix "AmazonKendra-“ haben.
4. Behalten Sie für alle anderen Felder ihre Standardwerte bei. Wählen Sie Weiter aus.
5. Wählen Sie auf der Seite Benutzerzugriffskontrolle konfigurieren unter Einstellungen für die Zugriffskontrolle die Option Ja aus, um Token für die Zugriffskontrolle zu verwenden.
6. Wählen Sie unter Token-Konfiguration JSON als Tokentyp aus.
7. Geben Sie einen Benutzernamen an, der bei der ACL-Prüfung verwendet werden soll.
8. Geben Sie eine oder mehrere Gruppen an, die bei der ACL-Prüfung verwendet werden sollen.
9. Wählen Sie Weiter aus.
10. Wählen Sie auf der Seite mit den Provisioning-Details die Developer Edition aus.
11. Wählen Sie Erstellen, um Ihren Index zu erstellen.
12. Warten Sie, bis Ihr Index erstellt wurde. Amazon Kendra stellt die Hardware für Ihren Index bereit. Dieser Vorgang kann einige Zeit in Anspruch nehmen.

CLI

Um AWS CLI mithilfe einer JSON-Eingabedatei einen Index zu erstellen, erstellen Sie zunächst eine JSON-Datei mit den gewünschten Parametern:

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

Rufen Sie als Nächstes `create-index` mit der Eingabedatei auf. Wenn der Name Ihrer JSON-Datei beispielsweise lautet`create-index-openid.json`, können Sie Folgendes verwenden:

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

Wenn Sie Open ID for nicht verwenden AWS IAM Identity Center, können Sie uns das Token im JSON-Format senden. In diesem Fall müssen Sie angeben, welches Feld im JSON-Token den Benutzernamen und welches Feld die Gruppen enthält. Die Gruppenfeldwerte müssen ein JSON-String-Array sein. Wenn Sie beispielsweise SAML verwenden, würde Ihr Token dem folgenden ähneln:

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

Das `TokenConfiguration` würde den Benutzernamen und die Gruppenfeldnamen angeben:

```
{
    "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'
)
```

Erstellen eines Datenquellen-Connectors

Sie können einen Datenquellen-Connector für erstellen Amazon Kendra , um eine Verbindung zu Ihren Dokumenten herzustellen und diese zu indizieren. Amazon Kendra kann eine Verbindung zu Microsoft SharePoint, Google Drive und vielen anderen Anbietern herstellen. Wenn Sie einen Datenquellen-Konnektor erstellen, geben Sie Amazon Kendra die Konfigurationsinformationen an, die für die Verbindung mit Ihrem Quell-Repository erforderlich sind. Im Gegensatz zum Hinzufügen von Dokumenten direkt zu einem Index können Sie die Datenquelle regelmäßig scannen, um den Index zu aktualisieren.

Angenommen, Sie haben ein Repository mit Steuerdokumenten in einem - Amazon S3 Bucket gespeichert. Von Zeit zu Zeit werden vorhandene Dokumente geändert und dem Repository neue Dokumente hinzugefügt. Wenn Sie das Repository Amazon Kendra als Datenquelle zu hinzufügen, können Sie Ihren Index auf dem neuesten Stand halten, indem Sie regelmäßige Synchronisationen zwischen Ihrer Datenquelle und dem Index einrichten.

Sie können einen Index manuell mithilfe der Konsole oder der StartDataSourceSyncJob API aktualisieren. Andernfalls richten Sie einen Zeitplan ein, um einen Index zu aktualisieren und ihn mit Ihrer Datenquelle synchronisieren zu lassen.

Ein Index kann mehr als eine Datenquelle haben. Jede Datenquelle kann ihren eigenen Aktualisierungsplan haben. Sie können beispielsweise den Index Ihrer Arbeitsdokumente täglich oder sogar stündlich aktualisieren, während Sie Ihre archivierten Dokumente manuell aktualisieren, wenn sich das Archiv ändert.

Wenn Sie Ihre Dokumentmetadaten oder Attribute und Inhalte während der Dokumentenerfassung ändern möchten, finden Sie weitere Informationen unter Amazon Kendra Anreicherung benutzerdefinierter Dokumente.

> **Note**
>
> Jede Dokument-ID muss pro Index eindeutig sein. Sie können keine Datenquelle erstellen, um Ihre Dokumente mit ihren eindeutigen IDs zu indizieren, und dann die `BatchPutDocument`-API verwenden, um dieselben Dokumente zu indizieren, oder umgekehrt. Sie können eine Datenquelle löschen und dann die `BatchPutDocument` - API verwenden, um dieselben Dokumente zu indizieren, oder umgekehrt. Die Verwendung der `BatchDeleteDocument` APIs `BatchPutDocument` und in Kombination mit einem

Amazon Kendra Datenquellen-Connector für denselben Satz von Dokumenten kann zu Inkonsistenzen bei Ihren Daten führen. Stattdessen empfehlen wir die Verwendung des Amazon Kendra benutzerdefinierten Datenquellen-Konnektors .

> **Note**
>
> Dateien, die dem Index hinzugefügt werden, müssen sich in einem UTF-8-kodierten Byte-Stream befinden. Weitere Informationen zu Dokumenten in finden Sie Amazon Kendraunter Dokumente.

Festlegen eines Aktualisierungszeitplans

Konfigurieren Sie Ihre Datenquelle so, dass sie regelmäßig mit der Konsole oder mithilfe des `Schedule` Parameters aktualisiert wird, wenn Sie eine Datenquelle erstellen oder aktualisieren. Der Inhalt des Parameters ist eine Zeichenfolge, die entweder eine Zeitplanzeichenfolge im `cron`-Format oder eine leere Zeichenfolge enthält, um anzugeben, dass der Index bei Bedarf aktualisiert wird. Informationen zum Format eines Cron-Ausdrucks finden Sie unter Planen von Ausdrücken für Regeln im Amazon CloudWatch Events -Benutzerhandbuch. Amazon Kendra unterstützt nur Cron-Ausdrücke. Rate-Ausdrücke werden nicht unterstützt.

Festlegen einer Sprache

Sie können alle Ihre Dokumente in einer Datenquelle in einer unterstützten Sprache indizieren. Sie geben den Sprachcode für alle Ihre Dokumente in Ihrer Datenquelle an, wenn Sie aufrufenCreateDataSource. Wenn für ein Dokument kein Sprachcode in einem Metadatenfeld angegeben ist, wird das Dokument mit dem Sprachcode indiziert, der für alle Dokumente auf Datenquellenebene angegeben ist. Wenn Sie keine Sprache angeben, Amazon Kendra indiziert Dokumente standardmäßig in einer Datenquelle in Englisch. Weitere Informationen zu unterstützten Sprachen, einschließlich ihrer Codes, finden Sie unter Hinzufügen von Dokumenten in anderen Sprachen als Englisch.

Sie indizieren alle Ihre Dokumente in einer Datenquelle in einer unterstützten Sprache mithilfe der Konsole. Gehen Sie zu Datenquellen und bearbeiten Sie Ihre Datenquelle oder Datenquelle hinzufügen, wenn Sie eine neue Datenquelle hinzufügen. Wählen Sie auf der Seite Datenquellendetails angeben eine Sprache aus der Dropdown-Liste Sprache aus. Sie wählen

Aktualisieren aus oder geben die Konfigurationsinformationen weiter ein, um eine Verbindung zu Ihrer Datenquelle herzustellen.

Datenquellen-Konnektoren

In diesem Abschnitt erfahren Sie, wie Sie mithilfe von Amazon Kendra in der und den Amazon Kendra APIs eine Verbindung Amazon Kendra zu unterstützten Datenbanken AWS Management Console und Datenquellen-Repositorys herstellen.

Themen

- Google Drive
- IBM DB2
- Jira
- Microsoft Exchange
- Microsoft OneDrive
- Microsoft SharePoint
- Microsoft SQL Server
- Microsoft Teams
- Microsoft Yammer
- MySQL
- Oracle Database
- PostgreSQL
- Quip
- Salesforce
- ServiceNow
- Slack
- Zendesk

Schemas für Datenquellenvorlagen

Im Folgenden finden Sie Vorlagenschemas für Datenquellen, für die Vorlagen unterstützt werden.

Themen

- Adobe Experience ManagerVorlagenschema
- Amazon FSx (Windows) Vorlagenschema
- Amazon FSx (NetApp ONTAP) -Vorlagenschema
- AlfrescoVorlagenschema
- Aurora (MySQL) Vorlagenschema
- Aurora (PostgreSQL) -Vorlagenschema
- Amazon RDS (Microsoft SQL Server) -Vorlagenschema
- Amazon RDS (MySQL) Vorlagenschema

- Amazon RDS (Oracle) Vorlagenschema
- Amazon RDS (PostgreSQL) -Vorlagenschema
- Amazon S3 Vorlagenschema
- Amazon Kendra Web Crawler-Vorlagenschema
- Confluence-Vorlagenschema
- Dropbox-Vorlagenschema
- Drupal-Vorlagenschema
- GitHub Vorlagenschema
- Gmail-Vorlagenschema
- Google Drive-Vorlagenschema
- IBM DB2-Vorlagenschema
- Microsoft Exchange-Vorlagenschema
- OneDrive Microsoft-Vorlagenschema
- SharePoint Microsoft-Vorlagenschema
- Microsoft SQL Server-Vorlagenschema
- Microsoft Teams-Vorlagenschema
- Microsoft Yammer-Vorlagenschema
- MySQL-Vorlagenschema
- Oracle-Datenbank-Vorlagenschema
- PostgreSQL-Vorlagenschema
- Salesforce-Vorlagenschema
- ServiceNow Vorlagenschema
- Slack-Vorlagenschema
- Zendesk-Vorlagenschema

Adobe Experience ManagerVorlagenschema

Sie fügen eine JSON-Datei ein, die das Datenquellenschema als Teil des TemplateConfigurationObjekts enthält. Sie geben die Adobe Experience Manager Host-URL, den Authentifizierungstyp und die Angabe, ob Sie Adobe Experience Manager (AEM) als Cloud-Dienst oder AEM On-Premise verwenden, als Teil der Verbindungskonfiguration oder der Repository-Endpunktdetails an. Geben Sie außerdem den Typ der Datenquelle`AEM`, ein Geheimnis für Ihre

Authentifizierungsdaten und andere erforderliche Konfigurationen an. Geben Sie dann `TEMPLATE` an`Type`, wann Sie anrufen CreateDataSource.

Sie können die in diesem Entwicklerhandbuch enthaltene Vorlage verwenden. Weitere Informationen finden Sie unter Adobe Experience ManagerJSON-Schema.

In der folgenden Tabelle werden die Parameter des AEM-JSON-Schemas beschrieben.

Konfiguration	Beschreibung
Verbindung/Konfiguration	Konfigurationsinformationen für den Endpunkt für die Datenquelle.
repositoryEndpointMetadata	Die Endpunktinformationen für die Datenquelle.
AEM-URL	Die Adobe Experience Manager Host-URL. Wenn Sie beispielsweise AEM On-Premise verwenden, geben Sie den Hostnamen und den Port an:. https://hostname:port Oder, wenn Sie AEM als Cloud-Service verwenden, können Sie die URL des Autors verwenden:. https://author-xxxxxx-xxxxxxx.adobeaemcloud.com
authType	Die Art der Authentifizierung, die Sie verwenden, ob `Basic` oder`OAuth2`.
deploymentType	Der TypAdobe Experience Manager, den Sie verwenden, entweder oder`CLOUD`. `ON_PREMIS E`
Repository-Konfigurationen	Konfigurationsinformationen für den Inhalt der Datenquelle. Beispielsweise die Konfiguration bestimmter Inhaltstypen und Feldzuordnungen.
• angezeigten • Komponente	Eine Liste von Objekten, die die Attribute oder Feldnamen Ihrer Adobe Experience Manager Seiten und Assets Amazon Kendra Indexfeld namen zuordnen. Weitere Informationen finden Sie unter Zuweisen von Datenquellenfeldern.

Konfiguration	Beschreibung
Zusätzliche Eigenschaften	Zusätzliche Konfigurationsoptionen für Ihre Inhalte in Ihrer Datenquelle.
timeZoneId	Wenn Sie AEM On-Premise verwenden und sich die Zeitzone Ihres Servers von der Zeitzone des Amazon Kendra AEM-Connectors oder -Indexes unterscheidet, können Sie die Serverzeitzone so angeben, dass sie mit dem AEM-Connector oder Index übereinstimmt. Die Standardzeitzone für AEM On-Premise ist die Zeitzone des AEM-Connectors oder -Indexes. Amazon Kendra Die Standardzeitzone für AEM as a Cloud Service ist Greenwich Mean Time.
• pageRootPaths • assetRootPaths	Eine Liste von Stammpfaden für Seiten und Assets. Beispielsweise könnte der Stammpfad für eine Seite /content/sub und der Stammpfad für ein Asset /content/sub/asset1 lauten.
Assets crawlen	`true`um Vermögenswerte zu crawlen.
Seiten crawlen	`true`um Seiten zu crawlen.

Konfiguration	Beschreibung
• pagePathInclusionMuster • pageNameInclusionMuster • assetPathInclusionMuster • assetTypeInclusionMuster • assetNameInclusionMuster	Eine Liste von Mustern mit regulären Ausdrücken, um bestimmte Seiten und Elemente in Ihre Adobe Experience Manager Datenquelle aufzunehmen. Seiten und Elemente, die den Mustern entsprechen, werden in den Index aufgenommen. Seiten und Inhalte, die den Mustern nicht entsprech en, werden aus dem Index ausgeschlossen. Wenn eine Seite oder ein Asset sowohl einem Einschluss- als auch einem Ausschlus smuster entspricht, hat das Ausschlussmuster Vorrang und der Inhalt wird nicht in den Index aufgenommen.
• pagePathExclusionMuster • pageNameExclusionMuster • assetPathExclusionMuster • assetTypeInclusionMuster • assetNameInclusionMuster	Eine Liste von Mustern mit regulären Ausdrücken, um bestimmte Seiten und Elemente in Ihrer Adobe Experience Manager Datenquelle auszuschließen. Seiten und Elemente, die den Mustern entsprechen, werden aus dem Index ausgeschlossen. Seiten und Inhalte, die den Mustern nicht entsprechen, werden in den Index aufgenommen. Wenn eine Seite oder ein Asset sowohl einem Einschlus s- als auch einem Ausschlussmuster entsprich t, hat das Ausschlussmuster Vorrang und der Inhalt wird nicht in den Index aufgenommen.
Seitenkomponenten	Eine Liste mit Namen für die spezifischen Seitenkomponenten, die Sie indexieren möchten.
contentFragmentVariations	Eine Liste mit Namen für die spezifischen gespeicherten Varianten von Adobe Experienc e Manager Inhaltsfragmenten, die Sie indiziere n möchten.

Konfiguration	Beschreibung
Typ	Der Typ der Datenquelle. Geben Sie `AEM` als Datenquellentyp an.
enableIdentityCrawler	`true`um den Identity Crawler zu verwenden, um Amazon Kendra Identitäts- und Hauptinformationen von Benutzern und Gruppen zu synchronisieren, die Zugriff auf bestimmte Dokumente haben. Wenn Identity Crawler ausgeschaltet ist, können alle Dokumente öffentlich durchsucht werden. Wenn Sie die Zugriffskontrolle für Ihre Dokumente verwenden möchten und Identity Crawler ausgeschaltet ist, können Sie alternativ die PutPrincipalMappingAPI verwenden, um Benutzer- und Gruppenzugriffsinformationen hochzuladen.

Konfiguration	Beschreibung
SyncMode	Geben Sie an, wie Ihr Index aktualisiert Amazon Kendra werden soll, wenn sich der Inhalt Ihrer Datenquelle ändert. Sie können wählen zwischen: • `FORCED_FULL_CRAWL` um den gesamten Inhalt neu zu indizieren und vorhandene Inhalte jedes Mal zu ersetzen, wenn Ihre Datenquelle mit Ihrem Index synchronisiert wird. • `FULL_CRAWL` um bei jeder Synchronisierung Ihrer Datenquelle mit Ihrem Index nur neue, geänderte und gelöschte Inhalte zu indiziere n. Amazon Kendra kann den Mechanismus Ihrer Datenquelle verwenden, um Inhaltsän derungen nachzuverfolgen und Inhalte zu indexieren, die sich seit der letzten Synchroni sierung geändert haben. • `CHANGE_LOG` um bei jeder Synchroni sierung Ihrer Datenquelle mit Ihrem Index nur neue und geänderte Inhalte zu indiziere n. Amazon Kendra kann den Mechanismus Ihrer Datenquelle verwenden, um Inhaltsän derungen nachzuverfolgen und Inhalte zu indexieren, die sich seit der letzten Synchroni sierung geändert haben.

Konfiguration	Beschreibung
SecreN	Der Amazon-Ressourcenname (ARN) eines AWS Secrets Manager Geheimnisses, das die Schlüssel-Wert-Paare enthält, die für die Verbindung mit Ihrem Adobe Experienc e Manager erforderlich sind. Informationen zu diesen Schlüssel-Wert-Paaren finden Sie in den Verbindungsanweisungen für Adobe Experience Manager.
version	Die Version dieser Vorlage, die derzeit unterstützt wird.

Adobe Experience ManagerJSON-Schema

```
{
  "$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 (Windows) Vorlagenschema

Sie fügen eine JSON-Datei ein, die das Datenquellenschema als Teil des TemplateConfigurationObjekts enthält. Sie geben die Dateisystem-ID als Teil der Verbindungskonfiguration oder der Repository-Endpunktdetails an. Sie müssen auch den Typ der Datenquelle als FSX geheimen Schlüssel für Ihre Authentifizierungsdaten und andere erforderliche Konfigurationen angeben. Anschließend geben Sie TEMPLATE anType, wann Sie anrufen CreateDataSource.

Sie können die in diesem Entwicklerhandbuch enthaltene Vorlage verwenden. Siehe Amazon FSx (Windows) JSON-Schema.

In der folgenden Tabelle werden die Parameter des Amazon FSx (Windows-) JSON-Schemas beschrieben.

Konfiguration	Beschreibung
Verbindung/Konfiguration	Konfigurationsinformationen für den Endpunkt für die Datenquelle.
repositoryEndpointMetadata	Die Endpunktinformationen für die Datenquelle.
fileSystemId	Der Bezeichner des Amazon FSx Dateisyst ems. Sie finden Ihre Dateisystem-ID im Dateisystem-Dashboard in der Amazon FSx Konsole.

Konfiguration	Beschreibung
fileSystemType	Der Amazon FSx Dateisystemtyp. Geben Sie an, ob Sie es Windows File Server als Dateisystemtyp verwenden möchten`WINDOWS`.
Repository-Konfigurationen	Konfigurationsinformationen für den Inhalt der Datenquelle. Beispielsweise die Konfiguration bestimmter Inhaltstypen und Feldzuordnungen.
Alle	Eine Liste von Objekten, die Attribute oder Feldnamen Ihrer Dateien in Ihrer Amazon FSx Datenquelle Amazon Kendra Indexfeldnamen zuordnen. Weitere Informationen finden Sie unter Zuweisen von Datenquellenfeldern.
Zusätzliche Eigenschaften	Zusätzliche Konfigurationsoptionen für Ihre Inhalte in Ihrer Datenquelle.
isCrawlAcl	`true`um die Informationen der Zugriffskontrollliste (ACL) für Ihre Dokumente zu durchsuchen, falls Sie über eine ACL verfügen und diese für die Zugriffskontrolle verwenden möchten. Die ACL gibt an, auf welche Dokumente Benutzer und Gruppen zugreifen können. Die ACL-Informationen werden verwendet, um Suchergebnisse nach dem Benutzer- oder Gruppenzugriff auf Dokumente zu filtern. Weitere Informationen finden Sie unter Benutzerkontextfilterung.

Konfiguration	Beschreibung
Einschlussmuster	Eine Liste von Mustern für reguläre Ausdrücke , um bestimmte Dateien in Ihre Amazon FSx Datenquelle aufzunehmen. Dateien, die dem Muster entsprechen, sind im Index enthalten . Dateien, die nicht dem Muster entsprech en, werden aus dem Index ausgeschlossen. Wenn eine Datei sowohl einem Ein- als auch einem Ausschlussmuster entspricht, hat das Ausschlussmuster Vorrang und die Datei ist nicht im Index enthalten.
Ausschlussmuster	Eine Liste von Mustern für reguläre Ausdrücke , um bestimmte Dateien in Ihrer Amazon FSx Datenquelle auszuschließen. Dateien, die dem Muster entsprechen, werden aus dem Index ausgeschlossen. Dateien, die den Mustern nicht entsprechen, werden in den Index aufgenommen. Wenn eine Datei sowohl einem Ausschluss- als auch einem Einschlus smuster entspricht, hat das Ausschlussmuster Vorrang und die Datei wird nicht in den Index aufgenommen.
enableIdentityCrawler	`true`um den Identity Crawler zu verwenden, um Amazon Kendra Identitäts- und Hauptinfo rmationen von Benutzern und Gruppen mit Zugriff auf bestimmte Dokumente zu synchroni sieren. Wenn Identity Crawler ausgeschaltet ist, können alle Dokumente öffentlich durchsucht werden. Wenn Sie die Zugriffskontrolle für Ihre Dokumente verwenden möchten und Identity Crawler ausgeschaltet ist, können Sie alternati v die PutPrincipalMappingAPI verwenden, um Benutzer- und Gruppenzugriffsinformationen hochzuladen.

Konfiguration	Beschreibung
SyncMode	Geben Sie an, wie Ihr Index aktualisiert Amazon Kendra werden soll, wenn sich der Inhalt Ihrer Datenquelle ändert. Sie können wählen zwischen: • `FORCED_FULL_CRAWL` um den gesamten Inhalt neu zu indizieren und vorhandene Inhalte jedes Mal zu ersetzen, wenn Ihre Datenquelle mit Ihrem Index synchronisiert wird. • `FULL_CRAWL` um bei jeder Synchronisierung Ihrer Datenquelle mit Ihrem Index nur neue, geänderte und gelöschte Inhalte zu indiziere n. Amazon Kendra kann den Mechanismus Ihrer Datenquelle verwenden, um Inhaltsän derungen nachzuverfolgen und Inhalte zu indexieren, die sich seit der letzten Synchroni sierung geändert haben.
Typ	Der Typ der Datenquelle. Geben Sie für Windows-Dateisystem-Datenquellen an`FSX`.

Amazon FSx (Windows) JSON-Schema

```
{
  "$schema": "http://json-schema.org/draft-04/schema#",
  "type": "object",
  "properties": {
    "connectionConfiguration": {
      "type": "object",
      "properties": {
        "repositoryEndpointMetadata": {
          "type": "object",
          "properties": {
            "fileSystemId": {
              "type": "string",
```

```
            "pattern": "fs-.*"
          },
          "fileSystemType": {
            "type": "string",
            "pattern": "WINDOWS"
          }
        },
        "required": ["fileSystemId", "fileSystemType"]
      }
    }
  },
  "repositoryConfigurations": {
    "type": "object",
    "properties": {
      "All": {
        "type": "object",
        "properties": {
          "fieldMappings": {
            "type": "array",
            "items": [
              {
                "type": "object",
                "properties": {
                  "indexFieldName": {
                    "type": "string"
                  },
                  "indexFieldType": {
                    "type": "string",
                    "enum": ["STRING", "STRING_LIST", "DATE"]
                  },
                  "dataSourceFieldName": {
                    "type": "string"
                  },
                  "dateFieldFormat": {
                    "type": "string",
                    "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                  }
                },
                "required": [
                  "indexFieldName",
                  "indexFieldType",
                  "dataSourceFieldName"
                ]
              }
```

```
            ]
          }
        },
        "required": ["fieldMappings"]
      }
    },
    "required": ["All"]
  },
  "additionalProperties": {
    "type": "object",
    "properties": {
      "isCrawlAcl": {
        "type": "boolean"
      },
      "exclusionPatterns": {
        "type": "array",
        "items": {
          "type": "string"
        }
      },
      "inclusionPatterns": {
        "type": "array",
        "items": {
          "type": "string"
        }
      }
    },
    "required": []
  },
  "enableIdentityCrawler": {
    "type": "boolean"
  },
  "syncMode": {
    "type": "string",
    "enum": [
      "FORCED_FULL_CRAWL",
      "FULL_CRAWL"
    ]
  },
  "type" : {
    "type" : "string",
    "pattern": "FSX"
  }
},
```

```
  "version": {
    "type": "string",
    "anyOf": [
      {
        "pattern": "1.0.0"
      }
    ]
  },
  "required": [
    "connectionConfiguration",
    "repositoryConfigurations",
    "syncMode",
    "enableIdentityCrawler",
    "additionalProperties",
    "type"
  ]
}
```

Amazon FSx (NetApp ONTAP) -Vorlagenschema

Sie fügen ein JSON hinzu, das das Datenquellenschema als Teil des TemplateConfigurationObjekts enthält. Sie geben die Dateisystem-ID und die virtuelle Speichermaschine (SVM) als Teil der Verbindungskonfiguration oder der Repository-Endpunktdetails an. Sie müssen auch den Typ der Datenquelle angebenFSXONTAP, ein Geheimnis für Ihre Authentifizierungsdaten und andere erforderliche Konfigurationen. Anschließend geben Sie `TEMPLATE` an`Type`, wann Sie anrufen CreateDataSource.

Sie können die in diesem Entwicklerhandbuch enthaltene Vorlage verwenden. Siehe Amazon FSx (NetApp ONTAP) JSON-Schema.

In der folgenden Tabelle werden die Parameter des Amazon FSx (NetApp ONTAP) JSON-Schemas beschrieben.

Konfiguration	Beschreibung
Verbindung/Konfiguration	Konfigurationsinformationen für den Endpunkt für die Datenquelle.
repositoryEndpointMetadata	Die Endpunktinformationen für die Datenquelle.

Konfiguration	Beschreibung
fileSystemId	Der Bezeichner des Amazon FSx Dateisyst ems. Sie finden Ihre Dateisystem-ID im Dateisystem-Dashboard in der Amazon FSx Konsole. Informationen zum Erstellen eines Dateisystems in der Amazon FSx Konsole für NetApp ONTAP finden Sie im Benutzerh andbuch unter Erste Schritte für NetApp ONTAP.FSx for ONTAP
fileSystemType	Der Amazon FSx Dateisystemtyp. Geben Sie an, ob Sie es NetApp ONTAP als Dateisyst emtyp verwenden möchten`ONTAP`.
SVMid	Die ID der virtuellen Speichermaschine (SVM), die mit Ihrem Amazon FSx Dateisystem für verwendet wird. NetApp ONTAP Sie finden Ihre SVM-ID, indem Sie in der Amazon FSx Konsole das Dateisystem-Dashboard aufrufen, Ihre Dateisystem-ID und dann virtuelle Speicherm aschinen auswählen. Informationen zum Erstellen eines Dateisystems in der Amazon FSx Konsole für NetApp ONTAP finden Sie im Benutzerhandbuch unter Erste Schritte für NetApp ONTAP.FSx for ONTAP
Typ des Protokolls	Ob Sie das Common Internet File System (CIFS) -Protokoll für Windows oder das Network File System (NFS) -Protokoll für Linux verwenden.
Repository-Konfigurationen	Konfigurationsinformationen für den Inhalt der Datenquelle. Beispielsweise die Konfiguration bestimmter Inhaltstypen und Feldzuordnungen.

Konfiguration	Beschreibung
file	Eine Liste von Objekten, die Attribute oder Feldnamen Ihrer Dateien in Ihrer Amazon FSx Datenquelle Amazon Kendra Indexfeldnamen zuordnen. Weitere Informationen finden Sie unter Zuweisen von Datenquellenfeldern. Die Feldnamen der Datenquelle müssen in den benutzerdefinierten Metadaten Ihrer Datei vorhanden sein.
Zusätzliche Eigenschaften	Zusätzliche Konfigurationsoptionen für Ihre Inhalte in Ihrer Datenquelle.
Cl crawlen	`true`um die Informationen der Zugriffskontrollliste (ACL) für Ihre Dokumente zu durchsuchen, falls Sie über eine ACL verfügen und diese für die Zugriffskontrolle verwenden möchten. Die ACL gibt an, auf welche Dokumente Benutzer und Gruppen zugreifen können. Die ACL-Informationen werden verwendet, um Suchergebnisse nach dem Benutzer- oder Gruppenzugriff auf Dokumente zu filtern. Weitere Informationen finden Sie unter Benutzerkontextfilterung.
Einschlussmuster	Eine Liste von Mustern für reguläre Ausdrücke, um bestimmte Dateien in Ihre Amazon FSx Datenquelle aufzunehmen. Dateien, die dem Muster entsprechen, sind im Index enthalten. Dateien, die nicht dem Muster entsprechen, werden aus dem Index ausgeschlossen. Wenn eine Datei sowohl einem Ein- als auch einem Ausschlussmuster entspricht, hat das Ausschlussmuster Vorrang und die Datei ist nicht im Index enthalten.

Konfiguration	Beschreibung
Ausschlussmuster	Eine Liste von Mustern für reguläre Ausdrücke , um bestimmte Dateien in Ihrer Amazon FSx Datenquelle auszuschließen. Dateien, die dem Muster entsprechen, werden aus dem Index ausgeschlossen. Dateien, die den Mustern nicht entsprechen, werden in den Index aufgenommen. Wenn eine Datei sowohl einem Ausschluss- als auch einem Einschlus smuster entspricht, hat das Ausschlussmuster Vorrang und die Datei wird nicht in den Index aufgenommen.
Typ	Der Typ der Datenquelle. Geben NetApp ONTAP Sie für Dateisystem-Datenquellen an`FSXONTAP`.
Sync-Modus	Geben Sie an, wie Ihr Index aktualisiert Amazon Kendra werden soll, wenn sich der Inhalt Ihrer Datenquelle ändert. Sie können wählen zwischen: • `FORCED_FULL_CRAWL` um den gesamten Inhalt neu zu indizieren und vorhandene Inhalte jedes Mal zu ersetzen, wenn Ihre Datenquelle mit Ihrem Index synchronisiert wird. • `FULL_CRAWL` um bei jeder Synchronisierung Ihrer Datenquelle mit Ihrem Index nur neue, geänderte und gelöschte Inhalte zu indiziere n. Amazon Kendra kann den Mechanismus Ihrer Datenquelle verwenden, um Inhaltsän derungen nachzuverfolgen und Inhalte zu indexieren, die sich seit der letzten Synchroni sierung geändert haben.

Konfiguration	Beschreibung

SecreN	Der Amazon-Ressourcenname (ARN) eines AWS Secrets Manager Geheimnisses, das die Schlüssel-Wert-Paare enthält, die für die Verbindung mit Ihrem Amazon FSx Dateisyst em erforderlich sind. Das Geheimnis muss eine JSON-Struktur mit den folgenden Schlüsseln enthalten:
	
	`{ "username": " user@corp.example. com ", "password": " password" }`
	
	Wenn Sie das NFS-Protokoll für Ihr Amazon FSx Dateisystem verwenden, wird das Geheimnis in einer JSON-Struktur mit den folgenden Schlüsseln gespeichert:
	
	`{ "leftId": "left ID", "rightId": " right ID", "preSharedKey": " pre-shared key " }`

Amazon FSx (NetApp ONTAP) JSON-Schema

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

AlfrescoVorlagenschema

Sie fügen eine JSON-Datei ein, die das Datenquellenschema als Teil des TemplateConfigurationObjekts enthält. Sie geben die Alfresco Site-ID, die Repository-URL, die URL der Benutzeroberfläche, den Authentifizierungstyp an, ob Sie die Cloud oder lokal verwenden, und den Inhaltstyp, den Sie crawlen möchten. Sie geben dies als Teil der Verbindungskonfiguration oder der Repository-Endpunktdetails an. Geben Sie außerdem den Typ der DatenquelleALFRESCO, ein Geheimnis für Ihre Authentifizierungsdaten und andere erforderliche Konfigurationen an. Geben Sie dann TEMPLATE anType, wann Sie anrufen CreateDataSource.

Sie können die in diesem Entwicklerhandbuch enthaltene Vorlage verwenden. Siehe AlfrescoJSON-Schema.

In der folgenden Tabelle werden die Parameter des Alfresco JSON-Schemas beschrieben.

Konfiguration	Beschreibung
Verbindung/Konfiguration	Konfigurationsinformationen für den Endpunkt für die Datenquelle.
repositoryEndpointMetadata	Die Endpunktinformationen für die Datenquelle.
SiteID	Die Kennung der Alfresco-Site.
URL erneut eingeben	Die URL Ihres Alfresco Repositorys. Sie können die Repository-URL von Ihrem Alfresco Administrator erhalten. Wenn Sie beispiels weise Alfresco Cloud (PaaS) verwenden, könnte die Repository-URL lauten https://c ompany.alfrescocloud.com. Oder, wenn Sie Alfresco On-Premise verwenden, könnte die Repository-URL lauten. https://company-al fresco-instance.company-domain.suffix:port
webAppUrl	Die URL Ihrer Alfresco Benutzeroberfläche. Die URL der Alfresco Benutzeroberfläche erhalten Sie von Ihrem Alfresco Administrator. Die URL der Benutzeroberfläche könnte beispielsweise https://example.com lauten.

Konfiguration	Beschreibung
repositoryAdditionalProperties	Zusätzliche Eigenschaften für die Verbindung mit dem Endpunkt des Repository/der Datenquelle.
authType	Die Art der Authentifizierung, die Sie verwenden, ob oder. `0Auth2` `Basic`
Typ (Bereitstellung)	Der TypAlfresco, den Sie verwenden, ob `PAAS` oder`ON-PREM`.
CrawlType	Der Inhaltstyp, den Sie crawlen möchten, sei es `ASPECT` (mit „Aspekten“ markierter InhaltAlfresco), `SITE_ID` (Inhalt innerhalb einer bestimmten Alfresco Website) oder `ALL_SITES` (Inhalt auf all Ihren Alfresco Websites).
Repository-Konfigurationen	Konfigurationsinformationen für den Inhalt der Datenquelle. Beispielsweise die Konfiguration bestimmter Inhaltstypen und Feldzuordnungen.
• document • Kommentar	Eine Liste von Objekten, die die Attribute oder Feldnamen Ihrer Alfresco-Dokumente und Kommentare den Indexfeldnamen zuordnen. Amazon Kendra Weitere Informationen finden Sie unter Zuweisen von Datenquellenfeldern.
Zusätzliche Eigenschaften	Zusätzliche Konfigurationsoptionen für Ihre Inhalte in Ihrer Datenquelle.
Name eines Aussehens	Der Name eines bestimmten „Aspects“, den Sie indexieren möchten.
Aspect-Eigenschaften	Eine Liste bestimmter Inhaltseigenschaften von „Aspect“, die Sie indexieren möchten.
enableFineGrainedSteuerung	`true`um „Aspekte“ zu crawlen.

Konfiguration	Beschreibung
isCrawlComment	`true`um Kommentare zu crawlen.
• inclusionFileNameMuster • inclusionFileTypeMuster • inclusionFilePathMuster	Eine Liste von Mustern für reguläre Ausdrücke , um bestimmte Dateien in Ihre Alfresco Datenquelle aufzunehmen. Dateien, die dem Muster entsprechen, sind im Index enthalten . Dateien, die nicht dem Muster entsprechen, werden aus dem Index ausgeschlossen. Wenn eine Datei sowohl einem Einschluss- als auch einem Ausschlussmuster entspricht, hat das Ausschlussmuster Vorrang, und die Datei wird nicht in den Index aufgenommen.
• exclusionFileNameMuster • exclusionFileTypeMuster • exclusionFilePathMuster	Eine Liste von Mustern mit regulären Ausdrücken, um bestimmte Dateien in Ihrer Alfresco Datenquelle auszuschließen. Dateien, die dem Muster entsprechen, werden aus dem Index ausgeschlossen. Dateien, die den Mustern nicht entsprechen, werden in den Index aufgenommen. Wenn eine Datei sowohl einem Einschluss- als auch einem Ausschlus smuster entspricht, hat das Ausschlussmuster Vorrang, und die Datei wird nicht in den Index aufgenommen.
Typ	Der Typ der Datenquelle. Geben Sie `ALFRESCO` als Datenquellentyp an.

Konfiguration	Beschreibung

Sekretär N	Der Amazon-Ressourcenname (ARN) eines AWS Secrets Manager Geheimnisses, das die Schlüssel-Wert-Paare enthält, die für die Verbindung mit Ihrem erforderlich sind. Alfresco Das Geheimnis muss eine JSON-Struktur mit den folgenden Schlüsseln enthalten:
	
	Wenn Sie die Standardauthentifizierung verwenden:
	
	`{ "username": " user name", "password": " password" }`
	
	Wenn Sie die OAuth 2.0-Authentifizierung verwenden:
	
	`{ "clientId": " client ID", "clientSecret": " client secret", "tokenUrl": " token URL" }`

Konfiguration	Beschreibung
Sync-Modus	Geben Sie an, wie Ihr Index aktualisiert Amazon Kendra werden soll, wenn sich der Inhalt Ihrer Datenquelle ändert. Sie können wählen zwischen: • `FORCED_FULL_CRAWL` um den gesamten Inhalt neu zu indizieren und vorhandene Inhalte jedes Mal zu ersetzen, wenn Ihre Datenquelle mit Ihrem Index synchronisiert wird. • `FULL_CRAWL` um bei jeder Synchronisierung Ihrer Datenquelle mit Ihrem Index nur neue, geänderte und gelöschte Inhalte zu indiziere n. Amazon Kendra kann den Mechanismus Ihrer Datenquelle verwenden, um Inhaltsän derungen nachzuverfolgen und Inhalte zu indexieren, die sich seit der letzten Synchroni sierung geändert haben.
enableIdentityCrawler	`true`um den Identity Crawler zu verwenden, um Amazon Kendra Identitäts- und Hauptinfo rmationen von Benutzern und Gruppen mit Zugriff auf bestimmte Dokumente zu synchroni sieren. Wenn Identity Crawler ausgeschaltet ist, können alle Dokumente öffentlich durchsucht werden. Wenn Sie die Zugriffskontrolle für Ihre Dokumente verwenden möchten und Identity Crawler ausgeschaltet ist, können Sie alternati v die PutPrincipalMappingAPI verwenden, um Benutzer- und Gruppenzugriffsinformationen hochzuladen.
version	Die Version dieser Vorlage, die derzeit unterstützt wird.

AlfrescoJSON-Schema

```
{
  "$schema": "http://json-schema.org/draft-04/schema#",
  "type": "object",
  "properties": {
    "connectionConfiguration": {
      "type": "object",
      "properties": {
        "repositoryEndpointMetadata": {
          "type": "object",
          "properties": {
            "siteId": {
              "type": "string"
            },
            "repoUrl": {
              "type": "string"
            },
            "webAppUrl": {
              "type": "string"
            },
            "repositoryAdditionalProperties": {
              "type": "object",
              "properties": {
                "authType": {
                  "type": "string",
                  "enum": [
                    "OAuth2",
                    "Basic"
                  ]
                },
                "type": {
                  "type": "string",
                  "enum": [
                    "PAAS",
                    "ON_PREM"
                  ]
                },
                "crawlType": {
                  "type": "string",
                  "enum": [
                    "ASPECT",
                    "SITE_ID",
                    "ALL_SITES"
```

```
                ]
              }
            }
          }
        }
      }
    },
    "required": [
      "repositoryEndpointMetadata"
    ]
  },
  "repositoryConfigurations": {
    "type": "object",
    "properties": {
      "document": {
        "type": "object",
        "properties": {
          "fieldMappings": {
            "type": "array",
            "items": {
              "anyOf": [
                {
                  "type": "object",
                  "properties": {
                    "indexFieldName": {
                      "type": "string"
                    },
                    "indexFieldType": {
                      "type": "string",
                      "enum": [
                        "STRING",
                        "DATE",
                        "STRING_LIST",
                        "LONG"
                      ]
                    },
                    "dataSourceFieldName": {
                      "type": "string"
                    },
                    "dateFieldFormat": {
                      "type": "string",
                      "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                    }
                  },
```

```
                "required": [
                  "indexFieldName",
                  "indexFieldType",
                  "dataSourceFieldName"
                ]
              }
            ]
          }
        }
      },
      "required": [
        "fieldMappings"
      ]
    },
    "comment": {
      "type": "object",
      "properties": {
        "fieldMappings": {
          "type": "array",
          "items": {
            "anyOf": [
              {
                "type": "object",
                "properties": {
                  "indexFieldName": {
                    "type": "string"
                  },
                  "indexFieldType": {
                    "type": "string",
                    "enum": [
                      "STRING",
                      "DATE",
                      "STRING_LIST",
                      "LONG"
                    ]
                  },
                  "dataSourceFieldName": {
                    "type": "string"
                  },
                  "dateFieldFormat": {
                    "type": "string",
                    "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                  }
                },
```

```
                  "required": [
                    "indexFieldName",
                    "indexFieldType",
                    "dataSourceFieldName"
                  ]
                }
              ]
            }
          }
        },
        "required": [
          "fieldMappings"
        ]
      }
    }
  },
  "additionalProperties": {
    "type": "object",
    "properties": {
      "aspectName": {
        "type": "string"
      },
      "aspectProperties": {
        "type": "array"
      },
      "enableFineGrainedControl": {
        "type": "boolean"
      },
      "isCrawlComment": {
        "type": "boolean"
      },
      "inclusionFileNamePatterns": {
        "type": "array"
      },
      "exclusionFileNamePatterns": {
        "type": "array"
      },
      "inclusionFileTypePatterns": {
        "type": "array"
      },
      "exclusionFileTypePatterns": {
        "type": "array"
      },
      "inclusionFilePathPatterns": {
```

```
          "type": "array"
        },
        "exclusionFilePathPatterns": {
          "type": "array"
        }
      }
    },
    "type": {
      "type": "string",
      "pattern": "ALFRESCO"
    },
    "secretArn": {
      "type": "string",
      "minLength": 20,
      "maxLength": 2048
    },
    "syncMode": {
      "type": "string",
      "enum": [
        "FORCED_FULL_CRAWL",
        "FULL_CRAWL"
      ]
    },
    "enableIdentityCrawler": {
      "type": "boolean"
    },
    "version": {
      "type": "string",
      "anyOf": [
        {
          "pattern": "1.0.0"
        }
      ]
    }
  },
  "required": [
    "connectionConfiguration",
    "repositoryConfigurations",
    "additionalProperties",
    "type",
    "secretArn"
  ]
}
```

Aurora (MySQL) Vorlagenschema

Sie fügen eine JSON-Datei ein, die das Datenquellenschema als Teil des TemplateConfigurationObjekts enthält. Geben Sie den Typ der Datenquelle als`JDBC`, den Datenbanktyp als`mysql`, ein Geheimnis für Ihre Authentifizierungsdaten und andere erforderliche Konfigurationen an. Geben Sie dann `TEMPLATE` an`Type`, wann Sie anrufen CreateDataSource.

Sie können die in diesem Entwicklerhandbuch enthaltene Vorlage verwenden. Siehe Aurora (MySQL) JSON-Schema.

In der folgenden Tabelle werden die Parameter des Aurora (MySQL) JSON-Schemas beschrieben.

Konfiguration	Beschreibung
Verbindung/Konfiguration	Konfigurationsinformationen für den Endpunkt für die Datenquelle.
repositoryEndpointMetadata	Erforderliche Konfigurationsinformationen für die Verbindung mit Ihrer Datenquelle. • dbType — Der Typ der Java-Date nbank, die Sie verwenden, unabhängig davon`mysql`,`db2`, `postgresql oracle`, oder. `sqlserver` • DBHost — Der Datenbank-Hostname. • DBPort — Der Datenbankport. • dbInstance — Die Datenbankinstanz.
Repository-Konfigurationen	Konfigurationsinformationen für den Inhalt der Datenquelle. Beispielsweise die Konfiguration bestimmter Inhaltstypen und Feldzuordnungen. Geben Sie den Typ der Datenquelle und den geheimen ARN an.
document	Eine Liste von Objekten, die die Attribute oder Feldnamen Ihres Datenbankinhalts Amazon Kendra Indexfeldnamen zuordnen. Weitere

Konfiguration	Beschreibung
	Informationen finden Sie unter Zuweisen von Datenquellenfeldern.
Zusätzliche Eigenschaften	Zusätzliche Konfigurationsoptionen für Ihre Inhalte in Ihrer Datenquelle. Dient zum Ein- oder Ausschließen bestimmter Inhalte in Ihrer Datenbankdatenquelle.
Primärschlüssel	Geben Sie den Primärschlüssel für die Datenbanktabelle an. Dies identifiziert eine Tabelle in Ihrer Datenbank.
Titel/Spalte	Geben Sie den Namen der Titelspalte des Dokuments in Ihrer Datenbanktabelle ein.
BodyColumn	Geben Sie den Namen der Titelspalte des Dokuments in Ihrer Datenbanktabelle ein.
sqlQuery	Geben Sie SQL-Abfrageanweisungen wie SELECT- und JOIN-Operationen ein. SQL-Abfragen müssen weniger als 32 KB groß sein. Amazon Kendra durchsucht den gesamten Datenbankinhalt, der Ihrer Abfrage entspricht.
Spalte „Zeitstempel“	Geben Sie den Namen der Spalte ein, die Zeitstempel enthält. Amazon Kendra verwendet Zeitstempelinformationen, um Änderungen an Ihrem Inhalt zu erkennen und nur geänderte Inhalte zu synchronisieren.
Zeitstempelformat	Geben Sie den Namen der Spalte ein, die Zeitstempelformate enthält, anhand derer Inhaltsänderungen erkannt und Ihre Inhalte erneut synchronisiert werden sollen.

Konfiguration	Beschreibung
Zeitzone	Geben Sie den Namen der Spalte ein, die Zeitzonen für den Inhalt enthält, der gecrawlt werden soll.
changeDetectingColumns	Geben Sie die Namen der Spalten ein, anhand derer Inhaltsänderungen erkannt Amazon Kendra werden sollen. Amazon Kendra indexiert den Inhalt neu, wenn sich eine dieser Spalten ändert
allowedUsersColumns	Geben Sie den Namen der Spalte ein, die Benutzer-IDs enthält, um Zugriff auf Inhalte zu erhalten.
allowedGroupsColumn	Geben Sie den Namen der Spalte ein, die Benutzer-IDs enthält, denen der Zugriff auf Inhalte gewährt werden soll.
Quelle-URI-Spalte	Geben Sie den Namen der Spalte ein, die Quell-URLs enthält, die indexiert werden sollen.
isSslEnabled	Geben Sie SQL-Abfrageanweisungen wie SELECT- und JOIN-Operationen ein. SQL-Abfragen müssen weniger als 32 KB groß sein. Amazon Kendra durchsucht den gesamten Datenbankinhalt, der Ihrer Abfrage entspricht.
Typ	Der Typ der Datenquelle. Geben Sie `JDBC` als Datenquellentyp an.

Konfiguration	Beschreibung
Sync-Modus	Geben Sie an, wie Ihr Index aktualisiert Amazon Kendra werden soll, wenn sich der Inhalt Ihrer Datenquelle ändert. Sie können wählen zwischen: • `FORCED_FULL_CRAWL` um den gesamten Inhalt neu zu indizieren und vorhandene Inhalte jedes Mal zu ersetzen, wenn Ihre Datenquelle mit Ihrem Index synchronisiert wird. • `FULL_CRAWL` um bei jeder Synchronisierung Ihrer Datenquelle mit Ihrem Index nur neue, geänderte und gelöschte Inhalte zu indiziere n. Amazon Kendra kann den Mechanismus Ihrer Datenquelle verwenden, um Inhaltsän derungen nachzuverfolgen und Inhalte zu indexieren, die sich seit der letzten Synchroni sierung geändert haben. • `CHANGE_LOG` um bei jeder Synchroni sierung Ihrer Datenquelle mit Ihrem Index nur neue und geänderte Inhalte zu indiziere n. Amazon Kendra kann den Mechanismus Ihrer Datenquelle verwenden, um Inhaltsän derungen nachzuverfolgen und Inhalte zu indexieren, die sich seit der letzten Synchroni sierung geändert haben.

Konfiguration	Beschreibung
SecreN	Der Amazon-Ressourcenname (ARN) eines Secrets Manager Manager-Geheimnisses, das den Benutzernamen und das Passwort enthält, die für die Verbindung mit Ihrer Datenbank erforderlich sind. Das Geheimnis muss eine JSON-Struktur mit den folgenden Schlüsseln enthalten: `{ "user name": "database user name", "password": " password" }`
version	Die Version der Vorlage, die derzeit unterstützt wird.

Aurora (MySQL) JSON-Schema

```
{
  "$schema": "http://json-schema.org/draft-04/schema#",
  "type": "object",
  "properties": {
    "connectionConfiguration": {
      "type": "object",
      "properties": {
        "repositoryEndpointMetadata": {
          "type": "object",
          "properties": {
            "dbType": {
              "type": "string",
              "enum": [
                "mysql",
                "db2",
                "postgresql",
                "oracle",
                "sqlserver"
              ]
            },
```

```
            "dbHost": {
              "type": "string"
            },
            "dbPort": {
              "type": "string"
            },
            "dbInstance": {
              "type": "string"
            }
          },
          "required": [
            "dbType",
            "dbHost",
            "dbPort",
            "dbInstance"
          ]
        }
      },
      "required": [
        "repositoryEndpointMetadata"
      ]
    },
    "repositoryConfigurations": {
      "type": "object",
      "properties": {
        "document": {
          "type": "object",
          "properties": {
            "fieldMappings": {
              "type": "array",
              "items": [
                {
                  "type": "object",
                  "properties": {
                    "indexFieldName": {
                      "type": "string"
                    },
                    "indexFieldType": {
                      "type": "string"
                    },
                    "dataSourceFieldName": {
                      "type": "string"
                    }
                  },
```

```
                "required": [
                  "indexFieldName",
                  "indexFieldType",
                  "dataSourceFieldName"
                ]
              }
            ]
          }
        },
        "required": [
          "fieldMappings"
        ]
      }
    },
    "required": [
    ]
  },
  "additionalProperties": {
    "type": "object",
    "properties": {
      "primaryKey": {
        "type": "string"
      },
      "titleColumn": {
        "type": "string"
      },
      "bodyColumn": {
        "type": "string"
      },
      "sqlQuery": {
        "type": "string",
        "not": {
          "pattern": ";+"
        }
      },
      "timestampColumn": {
        "type": "string"
      },
      "timestampFormat": {
        "type": "string"
      },
      "timezone": {
        "type": "string"
      },
```

```
        "changeDetectingColumns": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "allowedUsersColumn": {
          "type": "string"
        },
        "allowedGroupsColumn": {
          "type": "string"
        },
        "sourceURIColumn": {
          "type": "string"
        },
        "isSslEnabled": {
          "type": "boolean"
        }
      },
      "required": ["primaryKey", "titleColumn", "bodyColumn", "sqlQuery"]
    },
    "type" : {
      "type" : "string",
      "pattern": "JDBC"
    },
    "syncMode": {
      "type": "string",
      "enum": [
        "FORCED_FULL_CRAWL",
        "FULL_CRAWL",
        "CHANGE_LOG"
      ]
    },
    "secretArn": {
      "type": "string"
    }
  },
  "version": {
    "type": "string",
    "anyOf": [
      {
        "pattern": "1.0.0"
      }
    ]
```

```
  },
  "required": [
      "connectionConfiguration",
      "repositoryConfigurations",
      "syncMode",
      "additionalProperties",
      "secretArn",
      "type"
  ]
}
```

Aurora (PostgreSQL) -Vorlagenschema

Sie fügen eine JSON-Datei ein, die das Datenquellenschema als Teil des TemplateConfigurationObjekts enthält. Geben Sie den Typ der Datenquelle als`JDBC`, den Datenbanktyp als`postgresql`, ein Geheimnis für Ihre Authentifizierungsdaten und andere erforderliche Konfigurationen an. Geben Sie dann `TEMPLATE` an`Type`, wann Sie anrufen CreateDataSource.

Sie können die in diesem Entwicklerhandbuch enthaltene Vorlage verwenden. Siehe Aurora (PostgreSQL) JSON-Schema.

In der folgenden Tabelle werden die Parameter des Aurora (PostgreSQL) JSON-Schemas beschrieben.

Konfiguration	Beschreibung
Verbindung/Konfiguration	Konfigurationsinformationen für den Endpunkt für die Datenquelle.
repositoryEndpointMetadata	Erforderliche Konfigurationsinformationen für die Verbindung mit Ihrer Datenquelle. • dbType — Der Typ der Java-Date nbank, die Sie verwenden, unabhängig davon`mysql`,`db2`, `postgresql` `oracle`, oder. `sqlserver` • DBHost — Der Datenbank-Hostname. • DBPort — Der Datenbankport.

Konfiguration	Beschreibung
	• dbInstance — Die Datenbankinstanz.
Repository-Konfigurationen	Konfigurationsinformationen für den Inhalt der Datenquelle. Beispielsweise die Konfiguration bestimmter Inhaltstypen und Feldzuordnungen. Geben Sie den Typ der Datenquelle und den geheimen ARN an.
document	Eine Liste von Objekten, die die Attribute oder Feldnamen Ihres Datenbankinhalts Amazon Kendra Indexfeldnamen zuordnen. Weitere Informationen finden Sie unter Zuweisen von Datenquellenfeldern.
Zusätzliche Eigenschaften	Zusätzliche Konfigurationsoptionen für Ihre Inhalte in Ihrer Datenquelle. Dient zum Ein- oder Ausschließen bestimmter Inhalte in Ihrer Datenbankdatenquelle.
Primärschlüssel	Geben Sie den Primärschlüssel für die Datenbanktabelle an. Dies identifiziert eine Tabelle in Ihrer Datenbank.
Titel/Spalte	Geben Sie den Namen der Titelspalte des Dokuments in Ihrer Datenbanktabelle ein.
BodyColumn	Geben Sie den Namen der Titelspalte des Dokuments in Ihrer Datenbanktabelle ein.
sqlQuery	Geben Sie SQL-Abfrageanweisungen wie SELECT- und JOIN-Operationen ein. SQL-Abfragen müssen weniger als 32 KB groß sein. Amazon Kendra durchsucht den gesamten Datenbankinhalt, der Ihrer Abfrage entspricht.

Konfiguration	Beschreibung
Spalte „Zeitstempel“	Geben Sie den Namen der Spalte ein, die Zeitstempel enthält. Amazon Kendra verwendet Zeitstempelinformationen, um Änderungen an Ihrem Inhalt zu erkennen und nur geänderte Inhalte zu synchronisieren.
Zeitstempelformat	Geben Sie den Namen der Spalte ein, die Zeitstempelformate enthält, anhand derer Inhaltsänderungen erkannt und Ihre Inhalte erneut synchronisiert werden sollen.
Zeitzone	Geben Sie den Namen der Spalte ein, die Zeitzonen für den Inhalt enthält, der gecrawlt werden soll.
changeDetectingColumns	Geben Sie die Namen der Spalten ein, anhand derer Inhaltsänderungen erkannt Amazon Kendra werden sollen. Amazon Kendra indexiert den Inhalt neu, wenn sich eine dieser Spalten ändert
allowedUsersColumns	Geben Sie den Namen der Spalte ein, die Benutzer-IDs enthält, um Zugriff auf Inhalte zu erhalten.
allowedGroupsColumn	Geben Sie den Namen der Spalte ein, die Benutzer-IDs enthält, denen der Zugriff auf Inhalte gewährt werden soll.
Quelle-URI-Spalte	Geben Sie den Namen der Spalte ein, die Quell-URLs enthält, die indexiert werden sollen.

Konfiguration	Beschreibung
isSslEnabled	Geben Sie SQL-Abfrageanweisungen wie SELECT- und JOIN-Operationen ein. SQL-Abfragen müssen weniger als 32 KB groß sein. Amazon Kendra durchsucht den gesamten Datenbankinhalt, der Ihrer Abfrage entspricht.
Typ	Der Typ der Datenquelle. Geben Sie `JDBC` als Datenquellentyp an.
Sync-Modus	Geben Sie an, wie Ihr Index aktualisiert Amazon Kendra werden soll, wenn sich der Inhalt Ihrer Datenquelle ändert. Sie können wählen zwischen: • `FORCED_FULL_CRAWL` um den gesamten Inhalt neu zu indizieren und vorhandene Inhalte jedes Mal zu ersetzen, wenn Ihre Datenquelle mit Ihrem Index synchronisiert wird. • `FULL_CRAWL` um bei jeder Synchronisierung Ihrer Datenquelle mit Ihrem Index nur neue, geänderte und gelöschte Inhalte zu indiziere n. Amazon Kendra kann den Mechanismus Ihrer Datenquelle verwenden, um Inhaltsän derungen nachzuverfolgen und Inhalte zu indexieren, die sich seit der letzten Synchroni sierung geändert haben. • `CHANGE_LOG` um bei jeder Synchroni sierung Ihrer Datenquelle mit Ihrem Index nur neue und geänderte Inhalte zu indiziere n. Amazon Kendra kann den Mechanismus Ihrer Datenquelle verwenden, um Inhaltsän derungen nachzuverfolgen und Inhalte zu indexieren, die sich seit der letzten Synchroni sierung geändert haben.

Konfiguration	Beschreibung
SecreN	Der Amazon-Ressourcenname (ARN) eines Secrets Manager Manager-Geheimnisses, das den Benutzernamen und das Passwort enthält, die für die Verbindung mit Ihrer Datenbank erforderlich sind. Das Geheimnis muss eine JSON-Struktur mit den folgenden Schlüsseln enthalten: `{ "user name": "database user name", "password": " password" }`
version	Die Version der Vorlage, die derzeit unterstützt wird.

Aurora (PostgreSQL) JSON-Schema

```
{
  "$schema": "http://json-schema.org/draft-04/schema#",
  "type": "object",
  "properties": {
    "connectionConfiguration": {
      "type": "object",
      "properties": {
        "repositoryEndpointMetadata": {
          "type": "object",
          "properties": {
            "dbType": {
              "type": "string",
              "enum": [
                "mysql",
                "db2",
                "postgresql",
                "oracle",
                "sqlserver"
              ]
            },
```

```
            "dbHost": {
              "type": "string"
            },
            "dbPort": {
              "type": "string"
            },
            "dbInstance": {
              "type": "string"
            }
          },
          "required": [
            "dbType",
            "dbHost",
            "dbPort",
            "dbInstance"
          ]
        }
      },
      "required": [
        "repositoryEndpointMetadata"
      ]
    },
    "repositoryConfigurations": {
      "type": "object",
      "properties": {
        "document": {
          "type": "object",
          "properties": {
            "fieldMappings": {
              "type": "array",
              "items": [
                {
                  "type": "object",
                  "properties": {
                    "indexFieldName": {
                      "type": "string"
                    },
                    "indexFieldType": {
                      "type": "string"
                    },
                    "dataSourceFieldName": {
                      "type": "string"
                    }
                  },
```

```
                "required": [
                  "indexFieldName",
                  "indexFieldType",
                  "dataSourceFieldName"
                ]
              }
            ]
          }
        },
        "required": [
          "fieldMappings"
        ]
      }
    },
    "required": [
    ]
  },
  "additionalProperties": {
    "type": "object",
    "properties": {
      "primaryKey": {
        "type": "string"
      },
      "titleColumn": {
        "type": "string"
      },
      "bodyColumn": {
        "type": "string"
      },
      "sqlQuery": {
        "type": "string",
        "not": {
          "pattern": ";+"
        }
      },
      "timestampColumn": {
        "type": "string"
      },
      "timestampFormat": {
        "type": "string"
      },
      "timezone": {
        "type": "string"
      },
```

```
        "changeDetectingColumns": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "allowedUsersColumn": {
          "type": "string"
        },
        "allowedGroupsColumn": {
          "type": "string"
        },
        "sourceURIColumn": {
          "type": "string"
        },
        "isSslEnabled": {
          "type": "boolean"
        }
      },
      "required": ["primaryKey", "titleColumn", "bodyColumn", "sqlQuery"]
    },
    "type" : {
      "type" : "string",
      "pattern": "JDBC"
    },
    "syncMode": {
      "type": "string",
      "enum": [
        "FORCED_FULL_CRAWL",
        "FULL_CRAWL",
        "CHANGE_LOG"
      ]
    },
    "secretArn": {
      "type": "string"
    }
  },
  "version": {
    "type": "string",
    "anyOf": [
      {
        "pattern": "1.0.0"
      }
    ]
```

```
  },
  "required": [
      "connectionConfiguration",
      "repositoryConfigurations",
      "syncMode",
      "additionalProperties",
      "secretArn",
      "type"
  ]
}
```

Amazon RDS (Microsoft SQL Server) -Vorlagenschema

Sie fügen eine JSON-Datei ein, die das Datenquellenschema als Teil des TemplateConfigurationObjekts enthält. Geben Sie den Typ der Datenquelle als`JDBC`, den Datenbanktyp als`sqlserver`, ein Geheimnis für Ihre Authentifizierungsdaten und andere erforderliche Konfigurationen an. Geben Sie dann `TEMPLATE` an`Type`, wann Sie anrufen CreateDataSource.

Sie können die in diesem Entwicklerhandbuch enthaltene Vorlage verwenden. Siehe Amazon RDS (Microsoft SQL Server) JSON-Schema.

In der folgenden Tabelle werden die Parameter des Amazon RDS (Microsoft SQL Server) JSON-Schemas beschrieben.

Konfiguration	Beschreibung
Verbindung/Konfiguration	Konfigurationsinformationen für den Endpunkt für die Datenquelle.
repositoryEndpointMetadata	Erforderliche Konfigurationsinformationen für die Verbindung Ihrer Datenquelle. • dbType — Der Typ der Java-Date nbank, die Sie verwenden, unabhängig davon`mysql`,`db2`, `postgresql oracle`, oder. `sqlserver` • DBHost — Der Datenbank-Hostname. • DBPort — Der Datenbankport.

Konfiguration	Beschreibung
	• dbInstance — Die Datenbankinstanz.
Repository-Konfigurationen	Konfigurationsinformationen für den Inhalt der Datenquelle. Beispielsweise die Konfiguration bestimmter Inhaltstypen und Feldzuordnungen. Geben Sie den Typ der Datenquelle und den geheimen ARN an.
document	Eine Liste von Objekten, die die Attribute oder Feldnamen Ihres Datenbankinhalts Amazon Kendra Indexfeldnamen zuordnen. Weitere Informationen finden Sie unter Zuweisen von Datenquellenfeldern.
Zusätzliche Eigenschaften	Zusätzliche Konfigurationsoptionen für Ihre Inhalte in Ihrer Datenquelle. Dient zum Ein- oder Ausschließen bestimmter Inhalte in Ihrer Datenbankdatenquelle.
Primärschlüssel	Geben Sie den Primärschlüssel für die Datenbanktabelle an. Dies identifiziert eine Tabelle in Ihrer Datenbank.
Titel/Spalte	Geben Sie den Namen der Titelspalte des Dokuments in Ihrer Datenbanktabelle ein.
BodyColumn	Geben Sie den Namen der Titelspalte des Dokuments in Ihrer Datenbanktabelle ein.
sqlQuery	Geben Sie SQL-Abfrageanweisungen wie SELECT- und JOIN-Operationen ein. SQL-Abfragen müssen weniger als 32 KB groß sein. Amazon Kendra durchsucht den gesamten Datenbankinhalt, der Ihrer Abfrage entspricht.

Konfiguration	Beschreibung
Spalte „Zeitstempel“	Geben Sie den Namen der Spalte ein, die Zeitstempel enthält. Amazon Kendra verwendet Zeitstempelinformationen, um Änderungen an Ihrem Inhalt zu erkennen und nur geänderte Inhalte zu synchronisieren.
Zeitstempelformat	Geben Sie den Namen der Spalte ein, die Zeitstempelformate enthält, anhand derer Inhaltsänderungen erkannt und Ihre Inhalte erneut synchronisiert werden sollen.
Zeitzone	Geben Sie den Namen der Spalte ein, die Zeitzonen für den Inhalt enthält, der gecrawlt werden soll.
changeDetectingColumns	Geben Sie die Namen der Spalten ein, anhand derer Inhaltsänderungen erkannt Amazon Kendra werden sollen. Amazon Kendra indexiert den Inhalt neu, wenn sich eine dieser Spalten ändert
allowedUsersColumns	Geben Sie den Namen der Spalte ein, die Benutzer-IDs enthält, um Zugriff auf Inhalte zu erhalten.
allowedGroupsColumn	Geben Sie den Namen der Spalte ein, die Benutzer-IDs enthält, denen der Zugriff auf Inhalte gewährt werden soll.
Quelle-URI-Spalte	Geben Sie den Namen der Spalte ein, die Quell-URLs enthält, die indexiert werden sollen.

Konfiguration	Beschreibung
isSslEnabled	Geben Sie SQL-Abfrageanweisungen wie SELECT- und JOIN-Operationen ein. SQL-Abfragen müssen weniger als 32 KB groß sein. Amazon Kendra durchsucht den gesamten Datenbankinhalt, der Ihrer Abfrage entspricht.
Typ	Der Typ der Datenquelle. Geben Sie `JDBC` als Datenquellentyp an.
Sync-Modus	Geben Sie an, wie Ihr Index aktualisiert Amazon Kendra werden soll, wenn sich der Inhalt Ihrer Datenquelle ändert. Sie können wählen zwischen: • `FORCED_FULL_CRAWL` um den gesamten Inhalt neu zu indizieren und vorhandene Inhalte jedes Mal zu ersetzen, wenn Ihre Datenquelle mit Ihrem Index synchronisiert wird. • `FULL_CRAWL` um bei jeder Synchronisierung Ihrer Datenquelle mit Ihrem Index nur neue, geänderte und gelöschte Inhalte zu indiziere n. Amazon Kendra kann den Mechanismus Ihrer Datenquelle verwenden, um Inhaltsän derungen nachzuverfolgen und Inhalte zu indexieren, die sich seit der letzten Synchroni sierung geändert haben. • `CHANGE_LOG` um bei jeder Synchroni sierung Ihrer Datenquelle mit Ihrem Index nur neue und geänderte Inhalte zu indiziere n. Amazon Kendra kann den Mechanismus Ihrer Datenquelle verwenden, um Inhaltsän derungen nachzuverfolgen und Inhalte zu indexieren, die sich seit der letzten Synchroni sierung geändert haben.

Konfiguration	Beschreibung
SecreN	Der Amazon-Ressourcenname (ARN) eines Secrets Manager Manager-Geheimnisses, das den Benutzernamen und das Passwort enthält, die für die Verbindung mit Ihrer Datenbank erforderlich sind. Das Geheimnis muss eine JSON-Struktur mit den folgenden Schlüsseln enthalten: `{ "user name": "database user name", "password": " password" }`
version	Die Version der Vorlage, die derzeit unterstützt wird.

Amazon RDS (Microsoft SQL Server) JSON-Schema

```
{
  "$schema": "http://json-schema.org/draft-04/schema#",
  "type": "object",
  "properties": {
    "connectionConfiguration": {
      "type": "object",
      "properties": {
        "repositoryEndpointMetadata": {
          "type": "object",
          "properties": {
            "dbType": {
              "type": "string",
              "enum": [
                "mysql",
                "db2",
                "postgresql",
                "oracle",
                "sqlserver"
              ]
            },
```

```
            "dbHost": {
              "type": "string"
            },
            "dbPort": {
              "type": "string"
            },
            "dbInstance": {
              "type": "string"
            }
          },
          "required": [
            "dbType",
            "dbHost",
            "dbPort",
            "dbInstance"
          ]
        }
      },
      "required": [
        "repositoryEndpointMetadata"
      ]
    },
    "repositoryConfigurations": {
      "type": "object",
      "properties": {
        "document": {
          "type": "object",
          "properties": {
            "fieldMappings": {
              "type": "array",
              "items": [
                {
                  "type": "object",
                  "properties": {
                    "indexFieldName": {
                      "type": "string"
                    },
                    "indexFieldType": {
                      "type": "string"
                    },
                    "dataSourceFieldName": {
                      "type": "string"
                    }
                  },
```

```
                "required": [
                  "indexFieldName",
                  "indexFieldType",
                  "dataSourceFieldName"
                ]
              }
            ]
          }
        },
        "required": [
          "fieldMappings"
        ]
      }
    },
    "required": [
    ]
  },
  "additionalProperties": {
    "type": "object",
    "properties": {
      "primaryKey": {
        "type": "string"
      },
      "titleColumn": {
        "type": "string"
      },
      "bodyColumn": {
        "type": "string"
      },
      "sqlQuery": {
        "type": "string",
        "not": {
          "pattern": ";+"
        }
      },
      "timestampColumn": {
        "type": "string"
      },
      "timestampFormat": {
        "type": "string"
      },
      "timezone": {
        "type": "string"
      },
```

```
        "changeDetectingColumns": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "allowedUsersColumn": {
          "type": "string"
        },
        "allowedGroupsColumn": {
          "type": "string"
        },
        "sourceURIColumn": {
          "type": "string"
        },
        "isSslEnabled": {
          "type": "boolean"
        }
      },
      "required": ["primaryKey", "titleColumn", "bodyColumn", "sqlQuery"]
    },
    "type" : {
      "type" : "string",
      "pattern": "JDBC"
    },
    "syncMode": {
      "type": "string",
      "enum": [
        "FORCED_FULL_CRAWL",
        "FULL_CRAWL",
        "CHANGE_LOG"
      ]
    },
    "secretArn": {
      "type": "string"
    }
  },
  "version": {
    "type": "string",
    "anyOf": [
      {
        "pattern": "1.0.0"
      }
    ]
```

```
  },
  "required": [
      "connectionConfiguration",
      "repositoryConfigurations",
      "syncMode",
      "additionalProperties",
      "secretArn",
      "type"
  ]
}
```

Amazon RDS (MySQL) Vorlagenschema

Sie fügen eine JSON-Datei ein, die das Datenquellenschema als Teil des TemplateConfigurationObjekts enthält. Geben Sie den Typ der Datenquelle als`JDBC`, den Datenbanktyp als`mysql`, ein Geheimnis für Ihre Authentifizierungsdaten und andere erforderliche Konfigurationen an. Geben Sie dann `TEMPLATE` an`Type`, wann Sie anrufen CreateDataSource.

Sie können die in diesem Entwicklerhandbuch enthaltene Vorlage verwenden. Siehe Amazon RDS (MySQL) JSON-Schema.

In der folgenden Tabelle werden die Parameter des Amazon RDS (MySQL) JSON-Schemas beschrieben.

Konfiguration	Beschreibung
Verbindung/Konfiguration	Konfigurationsinformationen für den Endpunkt für die Datenquelle.
repositoryEndpointMetadata	Erforderliche Konfigurationsinformationen für die Verbindung Ihrer Datenquelle. • dbType — Der Typ der Java-Date nbank, die Sie verwenden, unabhängig davon`mysql`,`db2`, `postgresql oracle`, oder. `sqlserver` • DBHost — Der Datenbank-Hostname. • DBPort — Der Datenbankport. • dbInstance — Die Datenbankinstanz.

Konfiguration	Beschreibung
Repository-Konfigurationen	Konfigurationsinformationen für den Inhalt der Datenquelle. Beispielsweise die Konfiguration bestimmter Inhaltstypen und Feldzuordnungen. Geben Sie den Typ der Datenquelle und den geheimen ARN an.
document	Eine Liste von Objekten, die die Attribute oder Feldnamen Ihres Datenbankinhalts Amazon Kendra Indexfeldnamen zuordnen. Weitere Informationen finden Sie unter Zuweisen von Datenquellenfeldern.
Zusätzliche Eigenschaften	Zusätzliche Konfigurationsoptionen für Ihre Inhalte in Ihrer Datenquelle. Dient zum Ein- oder Ausschließen bestimmter Inhalte in Ihrer Datenbankdatenquelle.
Primärschlüssel	Geben Sie den Primärschlüssel für die Datenbanktabelle an. Dies identifiziert eine Tabelle in Ihrer Datenbank.
Titel/Spalte	Geben Sie den Namen der Titelspalte des Dokuments in Ihrer Datenbanktabelle ein.
BodyColumn	Geben Sie den Namen der Titelspalte des Dokuments in Ihrer Datenbanktabelle ein.
sqlQuery	Geben Sie SQL-Abfrageanweisungen wie SELECT- und JOIN-Operationen ein. SQL-Abfragen müssen weniger als 32 KB groß sein. Amazon Kendra durchsucht den gesamten Datenbankinhalt, der Ihrer Abfrage entspricht.

Konfiguration	Beschreibung
Spalte „Zeitstempel“	Geben Sie den Namen der Spalte ein, die Zeitstempel enthält. Amazon Kendra verwendet Zeitstempelinformationen, um Änderungen an Ihrem Inhalt zu erkennen und nur geänderte Inhalte zu synchronisieren.
Zeitstempelformat	Geben Sie den Namen der Spalte ein, die Zeitstempelformate enthält, anhand derer Inhaltsänderungen erkannt und Ihre Inhalte erneut synchronisiert werden sollen.
Zeitzone	Geben Sie den Namen der Spalte ein, die Zeitzonen für den Inhalt enthält, der gecrawlt werden soll.
changeDetectingColumns	Geben Sie die Namen der Spalten ein, anhand derer Inhaltsänderungen erkannt Amazon Kendra werden sollen. Amazon Kendra indexiert den Inhalt neu, wenn sich eine dieser Spalten ändert
allowedUsersColumns	Geben Sie den Namen der Spalte ein, die Benutzer-IDs enthält, um Zugriff auf Inhalte zu erhalten.
allowedGroupsColumn	Geben Sie den Namen der Spalte ein, die Benutzer-IDs enthält, denen der Zugriff auf Inhalte gewährt werden soll.
Quelle-URI-Spalte	Geben Sie den Namen der Spalte ein, die Quell-URLs enthält, die indexiert werden sollen.

Konfiguration	Beschreibung
isSslEnabled	Geben Sie SQL-Abfrageanweisungen wie SELECT- und JOIN-Operationen ein. SQL-Abfragen müssen weniger als 32 KB groß sein. Amazon Kendra durchsucht den gesamten Datenbankinhalt, der Ihrer Abfrage entspricht.
Typ	Der Typ der Datenquelle. Geben Sie `JDBC` als Datenquellentyp an.
Sync-Modus	Geben Sie an, wie Ihr Index aktualisiert Amazon Kendra werden soll, wenn sich der Inhalt Ihrer Datenquelle ändert. Sie können wählen zwischen: • `FORCED_FULL_CRAWL` um den gesamten Inhalt neu zu indizieren und vorhandene Inhalte jedes Mal zu ersetzen, wenn Ihre Datenquelle mit Ihrem Index synchronisiert wird. • `FULL_CRAWL` um bei jeder Synchronisierung Ihrer Datenquelle mit Ihrem Index nur neue, geänderte und gelöschte Inhalte zu indiziere n. Amazon Kendra kann den Mechanismus Ihrer Datenquelle verwenden, um Inhaltsän derungen nachzuverfolgen und Inhalte zu indexieren, die sich seit der letzten Synchroni sierung geändert haben. • `CHANGE_LOG` um bei jeder Synchroni sierung Ihrer Datenquelle mit Ihrem Index nur neue und geänderte Inhalte zu indiziere n. Amazon Kendra kann den Mechanismus Ihrer Datenquelle verwenden, um Inhaltsän derungen nachzuverfolgen und Inhalte zu indexieren, die sich seit der letzten Synchroni sierung geändert haben.

Konfiguration	Beschreibung
SecreN	Der Amazon-Ressourcenname (ARN) eines Secrets Manager Manager-Geheimnisses, das den Benutzernamen und das Passwort enthält, die für die Verbindung mit Ihrer Datenbank erforderlich sind. Das Geheimnis muss eine JSON-Struktur mit den folgenden Schlüsseln enthalten: `{ "user name": "database user name", "password": " password" }`
version	Die Version der Vorlage, die derzeit unterstützt wird.

Amazon RDS (MySQL) JSON-Schema

```
{
  "$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 (Oracle) Vorlagenschema

Sie fügen eine JSON-Datei ein, die das Datenquellenschema als Teil des TemplateConfigurationObjekts enthält. Geben Sie den Typ der Datenquelle als`JDBC`, den Datenbanktyp als`oracle`, ein Geheimnis für Ihre Authentifizierungsdaten und andere erforderliche Konfigurationen an. Geben Sie dann `TEMPLATE` an`Type`, wann Sie anrufen CreateDataSource.

Sie können die in diesem Entwicklerhandbuch enthaltene Vorlage verwenden. Siehe Amazon RDS (Oracle) JSON-Schema.

In der folgenden Tabelle werden die Parameter des Amazon RDS (Oracle) JSON-Schemas beschrieben.

Konfiguration	Beschreibung
Verbindung/Konfiguration	Konfigurationsinformationen für den Endpunkt für die Datenquelle.
repositoryEndpointMetadata	Erforderliche Konfigurationsinformationen für die Verbindung Ihrer Datenquelle. • dbType — Der Typ der Java-Date nbank, die Sie verwenden, unabhängig davon`mysql`,`db2`, `postgresql` `oracle`, oder. `sqlserver` • DBHost — Der Datenbank-Hostname. • DBPort — Der Datenbankport. • dbInstance — Die Datenbankinstanz.

Konfiguration	Beschreibung
Repository-Konfigurationen	Konfigurationsinformationen für den Inhalt der Datenquelle. Beispielsweise die Konfiguration bestimmter Inhaltstypen und Feldzuordnungen. Geben Sie den Typ der Datenquelle und den geheimen ARN an.
document	Eine Liste von Objekten, die die Attribute oder Feldnamen Ihres Datenbankinhalts Amazon Kendra Indexfeldnamen zuordnen. Weitere Informationen finden Sie unter Zuweisen von Datenquellenfeldern.
Zusätzliche Eigenschaften	Zusätzliche Konfigurationsoptionen für Ihre Inhalte in Ihrer Datenquelle. Dient zum Ein- oder Ausschließen bestimmter Inhalte in Ihrer Datenbankdatenquelle.
Primärschlüssel	Geben Sie den Primärschlüssel für die Datenbanktabelle an. Dies identifiziert eine Tabelle in Ihrer Datenbank.
Titel/Spalte	Geben Sie den Namen der Titelspalte des Dokuments in Ihrer Datenbanktabelle ein.
BodyColumn	Geben Sie den Namen der Titelspalte des Dokuments in Ihrer Datenbanktabelle ein.
sqlQuery	Geben Sie SQL-Abfrageanweisungen wie SELECT- und JOIN-Operationen ein. SQL-Abfragen müssen weniger als 32 KB groß sein. Amazon Kendra durchsucht den gesamten Datenbankinhalt, der Ihrer Abfrage entspricht.

Konfiguration	Beschreibung
Spalte „Zeitstempel“	Geben Sie den Namen der Spalte ein, die Zeitstempel enthält. Amazon Kendra verwendet Zeitstempelinformationen, um Änderungen an Ihrem Inhalt zu erkennen und nur geänderte Inhalte zu synchronisieren.
Zeitstempelformat	Geben Sie den Namen der Spalte ein, die Zeitstempelformate enthält, anhand derer Inhaltsänderungen erkannt und Ihre Inhalte erneut synchronisiert werden sollen.
Zeitzone	Geben Sie den Namen der Spalte ein, die Zeitzonen für den Inhalt enthält, der gecrawlt werden soll.
changeDetectingColumns	Geben Sie die Namen der Spalten ein, anhand derer Inhaltsänderungen erkannt Amazon Kendra werden sollen. Amazon Kendra indexiert den Inhalt neu, wenn sich eine dieser Spalten ändert
allowedUsersColumns	Geben Sie den Namen der Spalte ein, die Benutzer-IDs enthält, um Zugriff auf Inhalte zu erhalten.
allowedGroupsColumn	Geben Sie den Namen der Spalte ein, die Benutzer-IDs enthält, denen der Zugriff auf Inhalte gewährt werden soll.
Quelle-URI-Spalte	Geben Sie den Namen der Spalte ein, die Quell-URLs enthält, die indexiert werden sollen.

Konfiguration	Beschreibung
isSslEnabled	Geben Sie SQL-Abfrageanweisungen wie SELECT- und JOIN-Operationen ein. SQL-Abfragen müssen weniger als 32 KB groß sein. Amazon Kendra durchsucht den gesamten Datenbankinhalt, der Ihrer Abfrage entspricht.
Typ	Der Typ der Datenquelle. Geben Sie `JDBC` als Datenquellentyp an.
Sync-Modus	Geben Sie an, wie Ihr Index aktualisiert Amazon Kendra werden soll, wenn sich der Inhalt Ihrer Datenquelle ändert. Sie können wählen zwischen: • `FORCED_FULL_CRAWL` um den gesamten Inhalt neu zu indizieren und vorhandene Inhalte jedes Mal zu ersetzen, wenn Ihre Datenquelle mit Ihrem Index synchronisiert wird. • `FULL_CRAWL` um bei jeder Synchronisierung Ihrer Datenquelle mit Ihrem Index nur neue, geänderte und gelöschte Inhalte zu indiziere n. Amazon Kendra kann den Mechanismus Ihrer Datenquelle verwenden, um Inhaltsän derungen nachzuverfolgen und Inhalte zu indexieren, die sich seit der letzten Synchroni sierung geändert haben. • `CHANGE_LOG` um bei jeder Synchroni sierung Ihrer Datenquelle mit Ihrem Index nur neue und geänderte Inhalte zu indiziere n. Amazon Kendra kann den Mechanismus Ihrer Datenquelle verwenden, um Inhaltsän derungen nachzuverfolgen und Inhalte zu indexieren, die sich seit der letzten Synchroni sierung geändert haben.

Konfiguration	Beschreibung
SecreN	Der Amazon-Ressourcenname (ARN) eines Secrets Manager Manager-Geheimnisses, das den Benutzernamen und das Passwort enthält, die für die Verbindung mit Ihrer Datenbank erforderlich sind. Das Geheimnis muss eine JSON-Struktur mit den folgenden Schlüsseln enthalten: `{ "user name": "database user name", "password": " password" }`
version	Die Version der Vorlage, die derzeit unterstützt wird.

Amazon RDS (Oracle) JSON-Schema

```
{
  "$schema": "http://json-schema.org/draft-04/schema#",
  "type": "object",
  "properties": {
    "connectionConfiguration": {
      "type": "object",
      "properties": {
        "repositoryEndpointMetadata": {
          "type": "object",
          "properties": {
            "dbType": {
              "type": "string",
              "enum": [
                "mysql",
                "db2",
                "postgresql",
                "oracle",
                "sqlserver"
              ]
            },
```

```
            "dbHost": {
              "type": "string"
            },
            "dbPort": {
              "type": "string"
            },
            "dbInstance": {
              "type": "string"
            }
          },
          "required": [
            "dbType",
            "dbHost",
            "dbPort",
            "dbInstance"
          ]
        }
      },
      "required": [
        "repositoryEndpointMetadata"
      ]
    },
    "repositoryConfigurations": {
      "type": "object",
      "properties": {
        "document": {
          "type": "object",
          "properties": {
            "fieldMappings": {
              "type": "array",
              "items": [
                {
                  "type": "object",
                  "properties": {
                    "indexFieldName": {
                      "type": "string"
                    },
                    "indexFieldType": {
                      "type": "string"
                    },
                    "dataSourceFieldName": {
                      "type": "string"
                    }
                  },
```

```
                "required": [
                  "indexFieldName",
                  "indexFieldType",
                  "dataSourceFieldName"
                ]
              }
            ]
          }
        },
        "required": [
          "fieldMappings"
        ]
      }
    },
    "required": [
    ]
  },
  "additionalProperties": {
    "type": "object",
    "properties": {
      "primaryKey": {
        "type": "string"
      },
      "titleColumn": {
        "type": "string"
      },
      "bodyColumn": {
        "type": "string"
      },
      "sqlQuery": {
        "type": "string",
        "not": {
          "pattern": ";+"
        }
      },
      "timestampColumn": {
        "type": "string"
      },
      "timestampFormat": {
        "type": "string"
      },
      "timezone": {
        "type": "string"
      },
```

```
        "changeDetectingColumns": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "allowedUsersColumn": {
          "type": "string"
        },
        "allowedGroupsColumn": {
          "type": "string"
        },
        "sourceURIColumn": {
          "type": "string"
        },
        "isSslEnabled": {
          "type": "boolean"
        }
      },
      "required": ["primaryKey", "titleColumn", "bodyColumn", "sqlQuery"]
    },
    "type" : {
      "type" : "string",
      "pattern": "JDBC"
    },
    "syncMode": {
      "type": "string",
      "enum": [
        "FORCED_FULL_CRAWL",
        "FULL_CRAWL",
        "CHANGE_LOG"
      ]
    },
    "secretArn": {
      "type": "string"
    }
  },
  "version": {
    "type": "string",
    "anyOf": [
      {
        "pattern": "1.0.0"
      }
    ]
```

```
  },
  "required": [
      "connectionConfiguration",
      "repositoryConfigurations",
      "syncMode",
      "additionalProperties",
      "secretArn",
      "type"
  ]
}
```

Amazon RDS (PostgreSQL) -Vorlagenschema

Sie fügen eine JSON-Datei ein, die das Datenquellenschema als Teil des TemplateConfigurationObjekts enthält. Geben Sie den Typ der Datenquelle als`JDBC`, den Datenbanktyp als`postgresql`, ein Geheimnis für Ihre Authentifizierungsdaten und andere erforderliche Konfigurationen an. Geben Sie dann `TEMPLATE` an`Type`, wann Sie anrufen CreateDataSource.

Sie können die in diesem Entwicklerhandbuch enthaltene Vorlage verwenden. Siehe Amazon RDS (PostgreSQL) JSON-Schema.

In der folgenden Tabelle werden die Parameter des Amazon RDS (PostgreSQL) JSON-Schemas beschrieben.

Konfiguration	Beschreibung
Verbindung/Konfiguration	Konfigurationsinformationen für den Endpunkt für die Datenquelle.
repositoryEndpointMetadata	Erforderliche Konfigurationsinformationen für die Verbindung Ihrer Datenquelle. • dbType — Der Typ der Java-Date nbank, die Sie verwenden, unabhängig davon`mysql`,`db2`, `postgresql` `oracle`, oder. `sqlserver` • DBHost — Der Datenbank-Hostname. • DBPort — Der Datenbankport.

Konfiguration	Beschreibung
	• dbInstance — Die Datenbankinstanz.
Repository-Konfigurationen	Konfigurationsinformationen für den Inhalt der Datenquelle. Beispielsweise die Konfiguration bestimmter Inhaltstypen und Feldzuordnungen. Geben Sie den Typ der Datenquelle und den geheimen ARN an.
document	Eine Liste von Objekten, die die Attribute oder Feldnamen Ihres Datenbankinhalts Amazon Kendra Indexfeldnamen zuordnen. Weitere Informationen finden Sie unter Zuweisen von Datenquellenfeldern.
Zusätzliche Eigenschaften	Zusätzliche Konfigurationsoptionen für Ihre Inhalte in Ihrer Datenquelle. Dient zum Ein- oder Ausschließen bestimmter Inhalte in Ihrer Datenbankdatenquelle.
Primärschlüssel	Geben Sie den Primärschlüssel für die Datenbanktabelle an. Dies identifiziert eine Tabelle in Ihrer Datenbank.
Titel/Spalte	Geben Sie den Namen der Titelspalte des Dokuments in Ihrer Datenbanktabelle ein.
BodyColumn	Geben Sie den Namen der Titelspalte des Dokuments in Ihrer Datenbanktabelle ein.
sqlQuery	Geben Sie SQL-Abfrageanweisungen wie SELECT- und JOIN-Operationen ein. SQL-Abfragen müssen weniger als 32 KB groß sein. Amazon Kendra durchsucht den gesamten Datenbankinhalt, der Ihrer Abfrage entspricht.

Konfiguration	Beschreibung
Spalte „Zeitstempel“	Geben Sie den Namen der Spalte ein, die Zeitstempel enthält. Amazon Kendra verwendet Zeitstempelinformationen, um Änderungen an Ihrem Inhalt zu erkennen und nur geänderte Inhalte zu synchronisieren.
Zeitstempelformat	Geben Sie den Namen der Spalte ein, die Zeitstempelformate enthält, anhand derer Inhaltsänderungen erkannt und Ihre Inhalte erneut synchronisiert werden sollen.
Zeitzone	Geben Sie den Namen der Spalte ein, die Zeitzonen für den Inhalt enthält, der gecrawlt werden soll.
changeDetectingColumns	Geben Sie die Namen der Spalten ein, anhand derer Inhaltsänderungen erkannt Amazon Kendra werden sollen. Amazon Kendra indexiert den Inhalt neu, wenn sich eine dieser Spalten ändert
allowedUsersColumns	Geben Sie den Namen der Spalte ein, die Benutzer-IDs enthält, um Zugriff auf Inhalte zu erhalten.
allowedGroupsColumn	Geben Sie den Namen der Spalte ein, die Benutzer-IDs enthält, denen der Zugriff auf Inhalte gewährt werden soll.
Quelle-URI-Spalte	Geben Sie den Namen der Spalte ein, die Quell-URLs enthält, die indexiert werden sollen.

Konfiguration	Beschreibung
isSslEnabled	Geben Sie SQL-Abfrageanweisungen wie SELECT- und JOIN-Operationen ein. SQL-Abfragen müssen weniger als 32 KB groß sein. Amazon Kendra durchsucht den gesamten Datenbankinhalt, der Ihrer Abfrage entspricht.
Typ	Der Typ der Datenquelle. Geben Sie `JDBC` als Datenquellentyp an.
Sync-Modus	Geben Sie an, wie Ihr Index aktualisiert Amazon Kendra werden soll, wenn sich der Inhalt Ihrer Datenquelle ändert. Sie können wählen zwischen: • `FORCED_FULL_CRAWL` um den gesamten Inhalt neu zu indizieren und vorhandene Inhalte jedes Mal zu ersetzen, wenn Ihre Datenquelle mit Ihrem Index synchronisiert wird. • `FULL_CRAWL` um bei jeder Synchronisierung Ihrer Datenquelle mit Ihrem Index nur neue, geänderte und gelöschte Inhalte zu indiziere n. Amazon Kendra kann den Mechanismus Ihrer Datenquelle verwenden, um Inhaltsän derungen nachzuverfolgen und Inhalte zu indexieren, die sich seit der letzten Synchroni sierung geändert haben. • `CHANGE_LOG` um bei jeder Synchroni sierung Ihrer Datenquelle mit Ihrem Index nur neue und geänderte Inhalte zu indiziere n. Amazon Kendra kann den Mechanismus Ihrer Datenquelle verwenden, um Inhaltsän derungen nachzuverfolgen und Inhalte zu indexieren, die sich seit der letzten Synchroni sierung geändert haben.

Konfiguration	Beschreibung
SecreN	Der Amazon-Ressourcenname (ARN) eines Secrets Manager Manager-Geheimnisses, das den Benutzernamen und das Passwort enthält, die für die Verbindung mit Ihrer Datenbank erforderlich sind. Das Geheimnis muss eine JSON-Struktur mit den folgenden Schlüsseln enthalten: `{ "user name": "database user name", "password": " password" }`
version	Die Version der Vorlage, die derzeit unterstützt wird.

Amazon RDS (PostgreSQL) JSON-Schema

```
{
  "$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 Vorlagenschema

Sie fügen eine JSON-Datei, die das Datenquellenschema enthält, als Teil der Vorlagenkonfiguration hinzu. Sie geben den Namen des S3-Buckets als Teil der Verbindungskonfiguration oder der Repository-Endpunktdetails an. Geben Sie auch den Typ der Datenquelle als `S3` und andere erforderliche Konfigurationen an. Sie geben dann `TEMPLATE` an`Type`, wann Sie anrufen CreateDataSource.

Sie können die in diesem Entwicklerhandbuch enthaltene Vorlage verwenden. Siehe S3-JSON-Schema.

In der folgenden Tabelle werden die Parameter des Amazon S3 JSON-Schemas beschrieben.

Konfiguration	Beschreibung
Verbindung/Konfiguration	Konfigurationsinformationen für den Endpunkt für die Datenquelle.
repositoryEndpointMetadata	Die Endpunktinformationen für die Datenquelle.
BucketName	Der Name Ihres Amazon S3 Buckets.
Repository-Konfigurationen	Konfigurationsinformationen für den Inhalt der Datenquelle. Beispielsweise die Konfiguration bestimmter Inhaltstypen und Feldzuordnungen.
Zusätzliche Eigenschaften	Zusätzliche Konfigurationsoptionen für Ihre Inhalte in Ihrer Datenquelle

Konfiguration	Beschreibung
• Inklusionsmuster • Ausschlussmuster • Präfixe für Inklusion • Präfixe für Ausschlüsse	Eine Liste von Mustern für reguläre Ausdrücke , mit denen Sie bestimmte Dateien in Ihre Amazon S3 Datenquelle ein- oder ausschließen können. Dateien, die dem Muster entsprechen, sind im Index enthalten. Dateien, die nicht dem Muster entsprechen, werden aus dem Index ausgeschlossen. Wenn eine Datei sowohl einem Ein- als auch einem Ausschlussmuster entspricht, hat das Ausschlussmuster Vorrang und die Datei ist nicht im Index enthalten.
aclConfigurationFilePfad	Der Dateipfad, der den Zugriff auf Dokumente in einem Amazon Kendra Index steuert.
metadataFilesPrefix	Der Speicherort für Metadatendateien in Ihrem Bucket.
Sync-Modus	Geben Sie an, wie Ihr Index aktualisiert Amazon Kendra werden soll, wenn sich der Inhalt Ihrer Datenquelle ändert. Sie können wählen zwischen: • `FORCED_FULL_CRAWL` um den gesamten Inhalt neu zu indizieren und vorhandene Inhalte jedes Mal zu ersetzen, wenn Ihre Datenquelle mit Ihrem Index synchronisiert wird. • `FULL_CRAWL` um bei jeder Synchronisierung Ihrer Datenquelle mit Ihrem Index nur neue, geänderte und gelöschte Inhalte zu indiziere n. Amazon Kendra kann den Mechanismus Ihrer Datenquelle verwenden, um Inhaltsän derungen nachzuverfolgen und Inhalte zu indexieren, die sich seit der letzten Synchroni sierung geändert haben.

Konfiguration	Beschreibung
Typ	Der Typ der Datenquelle. Geben Sie S3 als Datenquellentyp an.
version	Die Version der Vorlage, die unterstützt wird.

S3-JSON-Schema

```
{
  "$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 Web Crawler-Vorlagenschema

Sie fügen eine JSON-Datei ein, die das Datenquellenschema als Teil des TemplateConfigurationObjekts enthält.

Sie geben die Seed- oder Startpunkt-URLs an, oder Sie können die Sitemap-URLs als Teil der Verbindungskonfiguration oder der Repository-Endpunktdetails angeben. Anstatt alle Ihre URLs manuell aufzulisten, können Sie den Pfad zu dem Amazon S3 Bucket angeben, in dem eine Textdatei für Ihre Liste von Seed-URLs oder Sitemap-XML-Dateien gespeichert ist, die Sie in S3 in einer ZIP-Datei zusammenfassen können.

Sie geben auch den Typ der Datenquelle`WEBCRAWLERV2`, die Anmeldeinformationen für die Website-Authentifizierung und den Authentifizierungstyp an, falls Ihre Websites eine Authentifizierung erfordern, sowie andere erforderliche Konfigurationen.

Sie geben dann `TEMPLATE` anType, wann Sie anrufen CreateDataSource.

> **Important**
>
> Die Erstellung von Web Crawler v2.0-Connectoren wird von nicht unterstützt. AWS CloudFormation Verwenden Sie den Web Crawler v1.0-Connector, wenn Sie Unterstützung benötigen. AWS CloudFormation

Bei der Auswahl der zu indizierenden Websites müssen Sie die Amazon Acceptable Use Policy (Richtlinie zur zulässigen Nutzung) und alle anderen Amazon-Bedingungen einhalten. Denken Sie daran, dass Sie Amazon Kendra Web Crawler nur verwenden dürfen, um Ihre eigenen Webseiten oder Webseiten zu indizieren, für deren Indexierung Sie autorisiert sind. Informationen dazu, wie Sie verhindern können, dass Amazon Kendra Web Crawler Ihre Websites indexiert, finden Sie unter. Konfiguration der *`robots.txt`* Datei für Amazon Kendra Web Crawler

Sie können die in diesem Entwicklerhandbuch bereitgestellte Vorlage verwenden. Siehe Amazon Kendra JSON-Schema für Web Crawler.

In der folgenden Tabelle werden die Parameter des Amazon Kendra Web Crawler-JSON-Schemas beschrieben.

Konfiguration	Beschreibung
Verbindung/Konfiguration	Konfigurationsinformationen für den Endpunkt für die Datenquelle.
repositoryEndpointMetadata	Die Endpunktinformationen für die Datenquelle.
siteMapUrls	Die Liste der Sitemap-URLs für die Websites, die Sie crawlen möchten. Sie können bis zu drei Sitemap-URLs auflisten.
s3 SeedUrl	Der S3-Pfad zur Textdatei, in der die Liste der Seed- oder Startpunkt-URLs gespeichert ist. z. B. s3://bucket-name/directory/. Jede URL in der Textdatei muss in einer separaten Zeile formatiert werden. Sie können bis zu 100 Seed-URLs in einer Datei auflisten.
s3 SiteMapUrl	Der S3-Pfad zu den Sitemap-XML-Dateien. z. B. s3://bucket-name/directory/. Sie können bis zu drei Sitemap-XML-Dateien auflisten. Sie können mehrere Sitemap-Dateien zu einer ZIP-Datei zusammenfassen und die ZIP-Datei in Ihrem Amazon S3 Bucket speichern.
seedUrlConnections	Die Liste der Seed- oder Startpunkt-URLs für die Websites, die Sie crawlen möchten. Sie können bis zu 100 Seed-URLs auflisten.
Seed-URL	Die Startpunkt-URL oder die Startpunkt-URL.
Authentifizierung	Der Authentifizierungstyp, wenn Ihre Websites dieselbe Authentifizierung erfordern, andernfal ls geben Sie ihn an`NoAuthentication` .
Repository-Konfigurationen	Konfigurationsinformationen für den Inhalt der Datenquelle. Beispielsweise die Konfiguration bestimmter Inhaltstypen und Feldzuordnungen.

Konfiguration	Beschreibung
• Webseite • attachment	Eine Liste von Objekten, die die Attribute oder Feldnamen Ihrer Webseiten und Webseiten dateien Amazon Kendra Indexfeldnamen zuordnen. Beispielsweise kann das Titel-Tag der HTML-Webseite dem `_document_title` Indexfeld zugeordnet werden. Weitere Informati onen finden Sie unter Zuweisen von Datenquel lenfeldern.
SyncMode	Geben Sie an, wie Ihr Index aktualisiert Amazon Kendra werden soll, wenn sich der Inhalt Ihrer Datenquelle ändert. Sie können wählen zwischen: • `FORCED_FULL_CRAWL` um den gesamten Inhalt neu zu indizieren und vorhandene Inhalte jedes Mal zu ersetzen, wenn Ihre Datenquelle mit Ihrem Index synchronisiert wird. • `FULL_CRAWL` um bei jeder Synchronisierung Ihrer Datenquelle mit Ihrem Index nur neue, geänderte und gelöschte Inhalte zu indiziere n. Amazon Kendra kann den Mechanismus Ihrer Datenquelle verwenden, um Inhaltsän derungen nachzuverfolgen und Inhalte zu indexieren, die sich seit der letzten Synchroni sierung geändert haben.
Zusätzliche Eigenschaften	Zusätzliche Konfigurationsoptionen für Ihre Inhalte in Ihrer Datenquelle.
RateLimit	Die maximale Anzahl an URLs, die pro Website-Host pro Minute gecrawlt werden.

Konfiguration	Beschreibung
maxFileSize	Die maximale Größe (in MB) einer Webseite oder eines Anhangs, die gecrawlt werden soll.
CrawlDepth	Die Anzahl der Ebenen von der Seed-URL bis zum Crawl. Beispielsweise hat die Seed-URL-Seite Tiefe 1 und alle Hyperlinks auf dieser Seite, die ebenfalls gecrawlt werden, haben Tiefe 2.
maxLinksPerUrl	Die maximale Anzahl von URLs auf einer Webseite, die beim Crawlen einer Website berücksichtigt werden sollen. Diese Zahl gilt pro Webseite. Wenn die Webseiten einer Website gecrawlt werden, werden auch alle URLs gecrawlt, auf die die Webseiten verweisen . URLs auf einer Webseite werden in der Reihenfolge ihres Auftretens gecrawlt.
crawlSubDomain	`true`um die Domains der Website mit Subdomains zu crawlen. Wenn die Seed-URL beispielsweise "" lautet, werden abc.examp le.com "" und a.abc.example.com "b.abc.ex ample.com" ebenfalls gecrawlt. Wenn Sie `crawlSubDomain` oder nicht `crawlAllD omain` auf festlegen`true`, werden Amazon Kendra nur die Domains der Websites gecrawlt, die Sie crawlen möchten.
crawlAllDomain	`true`zum Crawlen der Website-Domains mit Subdomains und anderen Domains, auf die die Webseiten verweisen. Wenn Sie `crawlSubD omain` oder `crawlAllDomain` auf nicht festlegen`true`, werden Amazon Kendra nur die Domains der Websites gecrawlt, die Sie crawlen möchten.

Konfiguration	Beschreibung
HonorRobots	`true`um die Anweisungen von robots.txt der Websites zu respektieren, die Sie crawlen möchten. Diese Anweisungen steuern, wie Amazon Kendra Web Crawler die Websites crawlt, d. h., ob nur bestimmte Inhalte gecrawlt werden Amazon Kendra können oder keine Inhalte.
Dateianhänge crawlen	`true`um Dateien zu crawlen, auf die die Webseiten verweisen.
• Inklusions-URL CrawlPatterns • Inklusions-URL IndexPatterns	Eine Liste mit Mustern für reguläre Ausdrücke , einschließlich des Crawlens bestimmter URLs und der Indexierung aller Hyperlinks auf diesen URL-Webseiten. URLs, die dem Muster entsprechen, sind im Index enthalten . URLs, die nicht dem Muster entsprechen, werden aus dem Index ausgeschlossen. Wenn eine URL sowohl einem Einschluss- als auch einem Ausschlussmuster entspricht, hat das Ausschlussmuster Vorrang, und die Webseiten der URL/Website werden nicht in den Index aufgenommen.

Konfiguration	Beschreibung
• Ausschluss-URL CrawlPatterns • Ausschluss-URL IndexPatterns	Eine Liste von Mustern mit regulären Ausdrücken, um das Crawlen bestimmter URLs und das Indexieren von Hyperlinks auf diesen URL-Webseiten auszuschließen. URLs, die dem Muster entsprechen, werden aus dem Index ausgeschlossen. URLs, die nicht dem Muster entsprechen, sind im Index enthalten . Wenn eine URL sowohl einem Einschluss- als auch einem Ausschlussmuster entsprich t, hat das Ausschlussmuster Vorrang, und die Webseiten der URL/Website werden nicht in den Index aufgenommen.
inclusionFileIndexMuster	Eine Liste von Mustern für reguläre Ausdrücke , die bestimmte Webseitendateien enthalten sollen. Dateien, die dem Muster entsprechen, sind im Index enthalten. Dateien, die nicht dem Muster entsprechen, werden aus dem Index ausgeschlossen. Wenn eine Datei sowohl einem Einschluss- als auch einem Ausschlus smuster entspricht, hat das Ausschlussmuster Vorrang, und die Datei wird nicht in den Index aufgenommen.
exclusionFileIndexMuster	Eine Liste von Mustern mit regulären Ausdrücken, um bestimmte Webseitendateien auszuschließen. Dateien, die dem Muster entsprechen, werden aus dem Index ausgeschl ossen. Dateien, die den Mustern nicht entsprechen, werden in den Index aufgenomm en. Wenn eine Datei sowohl einem Einschlus s- als auch einem Ausschlussmuster entsprich t, hat das Ausschlussmuster Vorrang, und die Datei wird nicht in den Index aufgenommen.

Konfiguration	Beschreibung
Proxy	Konfigurationsinformationen, die erforderlich sind, um über einen Webproxy eine Verbindung zu Ihren internen Websites herzustellen.
Host	Der Hostname des Proxyservers, den Sie für die Verbindung zu internen Websites verwenden möchten. Der Hostname von https://a.example.com/page1.htmlist beispielsweise "a.example.com“.
port	Die Portnummer des Proxyservers, den Sie für die Verbindung zu internen Websites verwenden möchten. Beispielsweise ist 443 der Standardport für HTTPS.
SecreTrann (Proxy)	Wenn Web-Proxy-Anmeldeinformationen erforderlich sind, um eine Verbindung zu einem Website-Host herzustellen, können Sie ein AWS Secrets Manager Geheimnis erstellen, in dem die Anmeldeinformationen gespeichert werden. Geben Sie den Amazon-Ressourcennamen (ARN) des Geheimnisses an.
Typ	Der Typ der Datenquelle. Geben Sie `WEBCRAWLERV2` als Datenquellentyp an.

Konfiguration	Beschreibung
Sekretär N	Der Amazon-Ressourcenname (ARN) eines AWS Secrets Manager Geheimnisses, das verwendet wird, wenn für Ihre Websites eine Authentifizierung für den Zugriff auf die Websites erforderlich ist. Sie speichern die Authentifizierungsdaten für die Website in dem Secret, das JSON-Schlüssel-Wert-Paare enthält. Wenn Sie Basic oder NTML/Kerberos verwenden, geben Sie den Benutzernamen und das Passwort ein. Die JSON-Schlüssel im Secret müssen und sein. `userName` `password` Das NTLM-Authentifizierungsprotokoll beinhaltet Passwort-Hashing, und das Kerberos-Authentifizierungsprotokoll beinhaltet Passwortverschlüsselung. Wenn Sie die SAML- oder Formularauthentifizierung verwenden, geben Sie den Benutzernamen und das Passwort, XPath für das Benutzernamenfeld (und die Benutzernamenschaltfläche bei Verwendung von SAML), XPaths für das Kennwortfeld und die Schaltfläche sowie die URL der Anmeldeseite ein. Die JSON-Schlüssel im Secret müssen`userName`,,,, `password` `userNameFieldXpath` `userNameButtonXpath` , `passwordFieldXpath` und lauten. `passwordButtonXpath` `loginPageUrl` Sie können die XPaths (XML Path Language) von Elementen mithilfe der Entwicklertools Ihres Webbrowsers finden. XPaths folgen normalerweise diesem Format:. `//tagname[@Attribute='Value']`

Konfiguration	Beschreibung
	Amazon Kendra prüft außerdem, ob die im Secret enthaltenen Endpunktinformationen (Seed-URLs) mit den Endpunktinformationen übereinstimmen, die in den Konfigurationsdeta ils Ihres Datenquellen-Endpunkts angegeben sind.
version	Die Version dieser Vorlage, die derzeit unterstützt wird.

Amazon Kendra JSON-Schema für 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"
  ]
}
```

Confluence-Vorlagenschema

Sie fügen eine JSON-Datei ein, die das Datenquellenschema als Teil des TemplateConfigurationObjekts enthält. Sie geben die Confluence-Host-URL, die Hosting-Methode und den Authentifizierungstyp als Teil der Verbindungskonfiguration oder der Repository-Endpunktdetails an. Geben Sie außerdem den Typ der DatenquelleCONFLUENCEV2, ein Geheimnis für Ihre Authentifizierungsdaten und andere erforderliche Konfigurationen an. Geben Sie dann TEMPLATE anType, wann Sie anrufen CreateDataSource.

Sie können die in diesem Entwicklerhandbuch enthaltene Vorlage verwenden. Siehe Confluence-JSON-Schema.

In der folgenden Tabelle werden die Parameter des Confluence-JSON-Schemas beschrieben.

Konfiguration	Beschreibung
Verbindung/Konfiguration	Konfigurationsinformationen für den Endpunkt für die Datenquelle.
repositoryEndpointMetadata	Die Endpunktinformationen für die Datenquelle.
Host-URL	Die URL für Ihre Confluence-Instanz. *Zum Beispiel https://example.confluence.com.*
Typ	Die Hosting-Methode für Ihre Confluence-Instanz, ob `SAAS` und. `ON_PREM`
authType	Die Authentifizierungsmethode für Ihre Confluence-Instanz, ob, oder`Basic`. `OAuth2` `Personal-token`
Repository-Konfigurationen	Konfigurationsinformationen für den Inhalt der Datenquelle. Beispielsweise die Konfiguration bestimmter Inhaltstypen und Feldzuordnungen.
• Leerzeichen • angezeigten • Blog • Kommentar • attachment	Eine Liste von Objekten, die die Attribute oder Feldnamen Ihrer Confluence-Spaces, -Seiten, Blogs, Kommentare und Anlagen Amazon Kendra Indexfeldnamen zuordnen. Weitere Informationen finden Sie unter Zuweisen von Datenquellenfeldern. Die Feldnamen der Confluence-Datenquelle müssen in Ihren benutzerdefinierten Confluence-Metadaten vorhanden sein.
Zusätzliche Eigenschaften	Zusätzliche Konfigurationsoptionen für Ihre Inhalte in Ihrer Datenquelle.
isCrawlAcl	`true`um die Informationen der Zugriffskontrollliste (ACL) für Ihre Dokumente zu durchsuchen,

Konfiguration	Beschreibung
	falls Sie über eine ACL verfügen und diese für die Zugriffskontrolle verwenden möchten. Die ACL gibt an, auf welche Dokumente Benutzer und Gruppen zugreifen können. Die ACL-Informationen werden verwendet, um Suchergebnisse nach dem Benutzer- oder Gruppenzugriff auf Dokumente zu filtern. Weitere Informationen finden Sie unter Benutzerkontextfilterung.
fieldForUserID	Geben Sie an, `email` ob Sie die Benutzer-E-Mail als Benutzer-ID verwenden möchten. `email`wird standardmäßig verwendet und ist derzeit der einzige unterstützte Benutzer-ID-Typ.
• inclusionSpaceKeyFilter • exclusionSpaceKeyFiltern • pageTitleRegEX • blogTitleRegEX • commentTitleRegEX • attachmentTitleRegEX • inclusionFileTypeMuster • exclusionFileTypeMuster • inclusionUrlPatterns • exclusionUrlPatterns	Eine Liste von Mustern für reguläre Ausdrücke, mit denen Sie bestimmte Dateien in Ihre Confluence-Datenquelle ein- und/oder ausschließen können. Dateien, die dem Muster entsprechen, sind im Index enthalten. Dateien, die nicht dem Muster entsprechen, werden aus dem Index ausgeschlossen. Wenn eine Datei sowohl einem Ein- als auch einem Ausschlusmuster entspricht, hat das Ausschlussmuster Vorrang und die Datei ist nicht im Index enthalten.
ProxyHost	Der Hostname des Web-Proxys, den Sie verwenden, ohne das `http://` `https://` OR-Protokoll.
ProxyPort	Die vom Host-URL-Transportprotokoll verwendete Portnummer. Muss ein numerischer Wert zwischen 0 und 65535 sein.

Konfiguration	Beschreibung
• isCrawlPersonalLeertaste • isCrawlArchivedWeltall • isCrawlArchivedSeite • isCrawlPage • isCrawlBlog • isCrawlPageKommentar • isCrawlPageAnlage • isCrawlBlogKommentar • isCrawlBlogAnlage	`true`um Dateien in Ihren persönlichen Bereichen, Seiten, Blogs, Seitenkommentaren, Seitenanhängen, Blogkommentaren und Bloganhängen von Confluence zu crawlen.
maxFileSizeInMegaBytes	Geben Sie die Dateigrößenbeschränkung in MB an, die gecrawlt werden können. Amazon Kendra Amazon Kendra durchsucht nur die Dateien innerhalb der von Ihnen definierten Größenbeschränkung. Die Standarddateigröße ist 50 MB. Die maximale Dateigröße sollte größer als 0 MB und kleiner oder gleich 50 MB sein.
Typ	Der Typ der Datenquelle. Geben Sie `CONFLUENCEV2` als Datenquellentyp an.

Konfiguration	Beschreibung
enableIdentityCrawler	`true`um den Identity Crawler zu verwenden, um Amazon Kendra Identitäts- und Hauptinfo rmationen von Benutzern und Gruppen zu synchronisieren, die Zugriff auf bestimmte Dokumente haben. Wenn Identity Crawler ausgeschaltet ist, können alle Dokumente öffentlich durchsucht werden. Wenn Sie die Zugriffskontrolle für Ihre Dokumente verwenden möchten und Identity Crawler ausgeschaltet ist, können Sie alternativ die PutPrincipalMappin gAPI verwenden, um Benutzer- und Gruppenzu griffsinformationen hochzuladen.
SyncMode	Geben Sie an, wie Ihr Index aktualisiert Amazon Kendra werden soll, wenn sich der Inhalt Ihrer Datenquelle ändert. Sie können wählen zwischen: • `FORCED_FULL_CRAWL` um den gesamten Inhalt neu zu indizieren und vorhandene Inhalte jedes Mal zu ersetzen, wenn Ihre Datenquelle mit Ihrem Index synchronisiert wird. • `FULL_CRAWL` um bei jeder Synchronisierung Ihrer Datenquelle mit Ihrem Index nur neue, geänderte und gelöschte Inhalte zu indiziere n. Amazon Kendra kann den Mechanismus Ihrer Datenquelle verwenden, um Inhaltsän derungen nachzuverfolgen und Inhalte zu indexieren, die sich seit der letzten Synchroni sierung geändert haben.

Konfiguration	Beschreibung
SecreN	Der Amazon-Ressourcenname (ARN) eines AWS Secrets Manager Geheimnisses, das die Schlüssel-Wert-Paare enthält, die für die Verbindung mit Ihrem Confluence erforderlich sind. Informationen zu diesen Schlüssel-Wert-Paaren finden Sie in den Verbindungsanweisungen für Confluence.
version	Die Version dieser Vorlage, die derzeit unterstützt wird.

Confluence-JSON-Schema

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

Dropbox-Vorlagenschema

Sie fügen eine JSON-Datei ein, die das Datenquellenschema als Teil des TemplateConfigurationObjekts enthält. Sie geben den Dropbox-App-Key, den geheimen App-Schlüssel und das Zugriffstoken als Teil Ihres Secrets an, in dem Ihre Authentifizierungsdaten gespeichert werden. Geben Sie außerdem den Typ der DatenquelleDROPBOX, den Typ des Zugriffstokens, das Sie verwenden möchten (temporär oder permanent), und andere erforderliche Konfigurationen an. Geben Sie dann `TEMPLATE` an`Type`, wann Sie anrufen CreateDataSource.

Sie können die in diesem Entwicklerhandbuch enthaltene Vorlage verwenden. Siehe Dropbox-JSON-Schema.

In der folgenden Tabelle werden die Parameter des Dropbox-JSON-Schemas beschrieben.

Konfiguration	Beschreibung
Verbindung/Konfiguration	Konfigurationsinformationen für den Endpunkt für die Datenquelle.
repositoryEndpointMetadata	Die Endpunktinformationen für die Datenquelle. Diese Datenquelle gibt keinen Endpunkt in an`repositoryEndpointMetadata` . Vielmehr sind die Verbindungsinformationen in einem AWS Secrets Manager Geheimnis enthalten, das Sie angeben`secretArn` .
Repository-Konfigurationen	Konfigurationsinformationen für den Inhalt der Datenquelle. Beispielsweise die Konfiguration bestimmter Inhaltstypen und Feldzuordnungen.
• file • paper • Papier • Abkürzung	Eine Liste von Objekten, die die Attribute oder Feldnamen Ihrer Dropbox-Dateien, Dropbox Paper und Verknüpfungen den Namen von Amazon Kendra Indexfeldern zuordnen. Weitere Informationen finden Sie unter Zuweisen von Datenquellenfeldern.
SecreN	Der Amazon-Ressourcenname (ARN) eines AWS Secrets Manager Geheimnisses, das die Schlüssel-Wert-Paare enthält, die für die Verbindung mit Ihrer Dropbox erforderlich sind. Das Geheimnis muss eine JSON-Struktur mit den folgenden Schlüsseln enthalten: `{ "appKey": "Dropbox app key", "appSecret": " Dropbox app secret", "accesstoken": " temporary access token or refresh access token" }`

Konfiguration	Beschreibung
Zusätzliche Eigenschaften	Zusätzliche Konfigurationsoptionen für Ihre Inhalte in Ihrer Datenquelle.
• inclusionFileNameMuster • inclusionFileTypeMuster	Eine Liste mit Mustern für reguläre Ausdrücke , um bestimmte Dateinamen und -typen in Ihre Dropbox-Datenquelle aufzunehmen. Dateien, die dem Muster entsprechen, sind im Index enthalten. Dateien, die nicht dem Muster entsprechen, werden aus dem Index ausgeschl ossen. Wenn eine Datei sowohl einem Ein- als auch einem Ausschlussmuster entspricht, hat das Ausschlussmuster Vorrang und die Datei ist nicht im Index enthalten.
• exclusionFileNameMuster • exclusionFileTypeMuster	Eine Liste mit Mustern für reguläre Ausdrücke , mit denen Sie bestimmte Dateinamen und -typen aus Ihrer Dropbox-Datenquell e ausschließen können. Dateien, die dem Muster entsprechen, werden aus dem Index ausgeschlossen. Dateien, die den Mustern nicht entsprechen, werden in den Index aufgenommen. Wenn eine Datei sowohl einem Ausschluss- als auch einem Einschlus smuster entspricht, hat das Ausschlussmuster Vorrang und die Datei wird nicht in den Index aufgenommen.
• Datei crawlen • Papier kriechen • CrawlPaper T • Abkürzung zum Crawlen	`true`um Dateien in Ihrer Dropbox, Dropbox Paper-Dokumente, Dropbox Paper-Vorlagen und in Ihrer Dropbox gespeicherte Webseiten verknüpfungen zu crawlen.
Typ	Der Typ der Datenquelle. Geben Sie `DROPBOX` als Datenquellentyp an.

Konfiguration	Beschreibung
useChangeLog	`true`um anhand des Dropbox-Änderungsprotokolls zu ermitteln, welche Dokumente im Index hinzugefügt, aktualisiert oder gelöscht werden müssen. Je nach Größe des Änderungsprotokolls kann es länger dauern, das Änderungsprotokoll Amazon Kendra zu verwenden, als alle Ihre Dokumente in Ihrer Dropbox zu scannen.
Token-Typ	Geben Sie den Typ Ihres Zugriffstokens an: permanentes oder temporäres Zugriffstoken. Es wird empfohlen, ein Zugriffstoken für die Aktualisierung zu erstellen, das in Dropbox nie abläuft, anstatt sich auf ein einmaliges Zugriffstoken zu verlassen, das nach 4 Stunden abläuft. Sie erstellen eine App und ein Zugriffstoken für die Aktualisierung in der Dropbox-Entwicklerkonsole und geben das Zugriffstoken geheim an.
version	Die Version dieser Vorlage, die derzeit unterstützt wird.

Dropbox-JSON-Schema

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

Drupal-Vorlagenschema

Sie fügen eine JSON-Datei ein, die das Datenquellenschema als Teil des TemplateConfigurationObjekts enthält. Sie geben die Drupal-Host-URL und den Authentifizierungstyp als Teil der Verbindungskonfiguration oder der Repository-Endpunktdetails an. Geben Sie außerdem

den Typ der Datenquelle als DRUPAL an, ein Geheimnis für Ihre Authentifizierungsdaten und andere erforderliche Konfigurationen. Sie geben dann an`TEMPLATE`, `Type` wann Sie anrufen. CreateDataSource

Sie können die in diesem Entwicklerhandbuch enthaltene Vorlage verwenden. Siehe Drupal-JSON-Schema.

In der folgenden Tabelle werden die Parameter des Drupal-JSON-Schemas beschrieben.

Konfiguration	Beschreibung
Verbindung/Konfiguration	Konfigurationsinformationen für den Endpunkt für die Datenquelle.
repositoryEndpointMetadata	Die Endpunktinformationen für die Datenquelle.
Host-URL	Die Host-URL Ihrer Drupal-Website. <drupalsitename>Zum Beispiel *https:///* <hostname>.
Repository-Konfigurationen	Konfigurationsinformationen für den Inhalt der Datenquelle.
• Inhalt • Kommentar • attachment	Eine Liste von Objekten, die die Attribute oder Feldnamen Ihrer Drupal-Dateien zuordnen. Weitere Informationen finden Sie unter Zuweisen von Datenquellenfeldern. Die Feldnamen der Drupal-Datenquelle müssen in Ihren benutzerdefinierten Drupal-Metadaten vorhanden sein.
Zusätzliche Eigenschaften	Zusätzliche Konfigurationsoptionen für Ihre Inhalte in Ihrer Datenquelle.
• inclusionFileNameMuster • articleTitleInclusionMuster • pageTitleInclusionMuster • customContentTitleInclusionPatterns • basicBlockTitleInclusionPatterns	Eine Liste von Mustern für reguläre Ausdrücke, um bestimmte Dateien in Ihre Drupal-Datenquelle aufzunehmen. Dateien, die dem Muster entsprechen, sind im Index enthalten. Dateien, die nicht dem Muster entsprech

Konfiguration	Beschreibung
• customBlockTitleInclusionPatterns	en, werden aus dem Index ausgeschlossen. Wenn eine Datei sowohl einem Ein- als auch einem Ausschlussmuster entspricht, hat das Ausschlussmuster Vorrang und die Datei ist nicht im Index enthalten.
• exclusionFileNameMuster • articleTitleExclusionMuster • pageTitleExclusionMuster • customContentTitleExclusionPatterns • basicBlockTitleExclusionPatterns • customBlockTitleExclusionPatterns	Eine Liste von Mustern für reguläre Ausdrücke , um bestimmte Dateien in Ihrer Drupal-Da tenquelle auszuschließen. Dateien, die dem Muster entsprechen, werden aus dem Index ausgeschlossen. Dateien, die den Mustern nicht entsprechen, werden in den Index aufgenommen. Wenn eine Datei sowohl einem Ausschluss- als auch einem Einschlus smuster entspricht, hat das Ausschlussmuster Vorrang und die Datei wird nicht in den Index aufgenommen.
Inhaltsdefinitionen • contentType • Felddefinition • isCrawlComments • isCrawlFiles • isCrawlArticle • isCrawlBasicSeite • isCrawlBasicBlockieren • isCrawlCustomContentTypesList	Geben Sie an, welche Inhaltstypen gecrawlt werden sollen, und ob Kommentare und Anlagen für die ausgewählten Inhaltstypen gecrawlt werden sollen.
Typ	Der Typ der Datenquelle. Geben Sie `DRUPAL` als Datenquellentyp an.
authType	Die Art der Authentifizierung, die Sie verwenden, ob `BASIC-AUTH` oder`OAUTH2`.

Konfiguration	Beschreibung
Sync-Modus	Geben Sie an, wie Ihr Index aktualisiert Amazon Kendra werden soll, wenn sich der Inhalt Ihrer Datenquelle ändert. Sie können wählen zwischen: • `FORCED_FULL_CRAWL` um den gesamten Inhalt neu zu indizieren und vorhandene Inhalte jedes Mal zu ersetzen, wenn Ihre Datenquelle mit Ihrem Index synchronisiert wird. • `FULL_CRAWL` um bei jeder Synchronisierung Ihrer Datenquelle mit Ihrem Index nur neue, geänderte und gelöschte Inhalte zu indiziere n. Amazon Kendra kann den Mechanismus Ihrer Datenquelle verwenden, um Inhaltsän derungen nachzuverfolgen und Inhalte zu indexieren, die sich seit der letzten Synchroni sierung geändert haben. • `CHANGE_LOG` um bei jeder Synchroni sierung Ihrer Datenquelle mit Ihrem Index nur neue und geänderte Inhalte zu indiziere n. Amazon Kendra kann den Mechanismus Ihrer Datenquelle verwenden, um Inhaltsän derungen nachzuverfolgen und Inhalte zu indexieren, die sich seit der letzten Synchroni sierung geändert haben.

Konfiguration	Beschreibung
enableIdentityCrawler	`true`um den Identity Crawler zu verwenden, um Amazon Kendra Identitäts- und Hauptinfo rmationen von Benutzern und Gruppen mit Zugriff auf bestimmte Dokumente zu synchroni sieren. Wenn Identity Crawler ausgeschaltet ist, können alle Dokumente öffentlich durchsucht werden. Wenn Sie die Zugriffskontrolle für Ihre Dokumente verwenden möchten und Identity Crawler ausgeschaltet ist, können Sie alternati v die PutPrincipalMappingAPI verwenden, um Benutzer- und Gruppenzugriffsinformationen hochzuladen.

Konfiguration	Beschreibung

SecreN	Der Amazon-Ressourcenname (ARN) eines AWS Secrets Manager Geheimnisses, das die Schlüssel-Wert-Paare enthält, die für die Verbindung mit Ihrem Drupal erforderlich sind. Das Geheimnis muss eine JSON-Struktur mit den folgenden Schlüsseln enthalten:
	
	Wenn Sie die Standardauthentifizierung verwenden:
	
	`{ "username": "user name", "passwords": "password" }`
	
	Wenn Sie die OAuth 2.0-Authentifizierung verwenden:
	
	`{ "username": "user name", "password": "password" , "clientId": "client id", "clientSecret": "client secret" }`

version	Die Version dieser Vorlage, die derzeit unterstützt wird.

Drupal-JSON-Schema

```
{
 "$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 Vorlagenschema

Sie fügen eine JSON-Datei ein, die das Datenquellenschema als Teil des TemplateConfigurationObjekts enthält. Sie geben die GitHub Host-URL, den Namen der Organisation und die Angabe, ob Sie GitHub Cloud oder GitHub lokal verwenden, als Teil der Verbindungskonfiguration oder der Repository-Endpunktdetails an. Geben Sie außerdem den Typ der Datenquelle`GITHUB`, ein Geheimnis für Ihre Authentifizierungsdaten und andere erforderliche Konfigurationen an. Geben Sie dann `TEMPLATE` an`Type`, wann Sie anrufen CreateDataSource.

Sie können die in diesem Entwicklerhandbuch enthaltene Vorlage verwenden. Siehe GitHub JSON-Schema.

In der folgenden Tabelle werden die Parameter des GitHub JSON-Schemas beschrieben.

Konfiguration	Beschreibung
Verbindung/Konfiguration	Konfigurationsinformationen für den Endpunkt für die Datenquelle.
repositoryEndpointMetadata	Die Endpunktinformationen für die Datenquelle.
Typ	Geben Sie den Typ entweder als `SAAS` oder an`ON_PREMISE` .
Host-URL	Die GitHub Host-URL. Wenn Sie beispielsweise GitHub SaaS/Enterprise Cloud verwenden:. https://api.github.com Oder, wenn Sie einen GitHub lokalen Server/Enterprise Server verwenden:. https://on-prem-host-url/api/v3/
Name der Organisation	Sie finden den Namen Ihrer Organisation, wenn Sie sich bei GitHub Desktop anmelden und in der Dropdownliste Ihres Profilbilds zu Ihre Organisationen gehen.
Repository-Konfigurationen	Konfigurationsinformationen für den Inhalt der Datenquelle. Beispielsweise die Konfiguration bestimmter Inhaltstypen und Feldzuordnungen.
• GH-Repository • GH-Commit • ghIssueDocument • ghIssueComment • ghIssueAttachment • GHPR-Dokument • GHPR-Kommentar	Eine Liste von Objekten, die die Attribute oder Feldnamen Ihres GitHub Inhalts Amazon Kendra Indexfeldnamen zuordnen. Weitere Informationen finden Sie unter Zuweisen von Datenquellenfeldern.

Konfiguration	Beschreibung
• GHPR-Anlage	
Zusätzliche Eigenschaften	Zusätzliche Konfigurationsoptionen für Ihre Inhalte in Ihrer Datenquelle.
isCrawlAcl	`true`um die Informationen der Zugriffskontrollliste (ACL) für Ihre Dokumente zu durchsuchen, falls Sie über eine ACL verfügen und diese für die Zugriffskontrolle verwenden möchten. Die ACL gibt an, auf welche Dokumente Benutzer und Gruppen zugreifen und welche sie durchsuchen können. Die ACL-Informationen werden verwendet, um Suchergebnisse nach dem Benutzer- oder Gruppenzugriff auf Dokumente zu filtern. Weitere Informationen finden Sie unter Benutzerkontextfilterung.
fieldForUserID	Geben Sie den Typ der Benutzer-ID an, die Sie für das ACL-Crawling verwenden möchten. Geben Sie an, `email` ob Sie die Benutzer-E-Mail für die Benutzer-ID verwenden möchten, oder `username` ob Sie den Benutzernamen für die Benutzer-ID verwenden möchten. Wenn Sie keine Option angeben, `email` wird diese Option standardmäßig verwendet.
RepositoryFilter	Eine Liste mit Namen der spezifischen Repositorys und Branchennamen, die Sie indexieren möchten.
Repository crawlen	`true`um Repositorys zu crawlen.
crawlRepositoryDocuments	`true`um Repository-Dokumente zu crawlen.
Problem crawlen	`true`um Probleme zu crawlen.
crawlIssueComment	`true`um Problemkommentare zu crawlen.

Konfiguration	Beschreibung
crawlIssueCommentAnlage	`true`um Dateianhänge zu crawlen.
crawlPullRequest	`true`um Pull-Requests zu crawlen.
crawlPullRequestKommentar	`true`um Kommentare zu Pull-Requests zu crawlen.
crawlPullRequestCommentAttachment	`true`zum Crawlen von Anhängen von Pull-Request-Kommentaren.
• inclusionFolderNameMuster • inclusionFileTypeMuster • inclusionFileNameMuster	Eine Liste von Mustern für reguläre Ausdrücke, um bestimmte Inhalte in Ihre GitHub Datenquelle aufzunehmen. Elemente, die den Mustern entsprechen, sind im Index enthalten. Inhalte, die den Mustern nicht entsprechen, werden aus dem Index ausgeschlossen. Wenn ein Inhalt sowohl einem Einschluss- als auch einem Ausschlussmuster entspricht, hat das Ausschlussmuster Vorrang, und der Inhalt wird nicht in den Index aufgenommen.
• exclusionFolderNameMuster • exclusionFileTypeMuster • exclusionFileNameMuster	Eine Liste von Mustern mit regulären Ausdrücken, um bestimmte Inhalte in Ihrer GitHub Datenquelle auszuschließen. Inhalte, die den Mustern entsprechen, werden aus dem Index ausgeschlossen. Inhalte, die den Mustern nicht entsprechen, werden in den Index aufgenommen. Wenn Inhalte sowohl einem Inklusions- als auch einem Ausschlussmuster entsprechen, hat das Ausschlussmuster Vorrang, und der Inhalt wird nicht in den Index aufgenommen.
Typ	Der Typ der Datenquelle. Geben Sie `GITHUB` als Datenquellentyp an.

Konfiguration	Beschreibung
enableIdentityCrawler	`true`um den Identity Crawler zu verwenden, um Amazon Kendra Identitäts- und Hauptinformationen von Benutzern und Gruppen zu synchronisieren, die Zugriff auf bestimmte Dokumente haben. Wenn Identity Crawler ausgeschaltet ist, können alle Dokumente öffentlich durchsucht werden. Wenn Sie die Zugriffskontrolle für Ihre Dokumente verwenden möchten und Identity Crawler ausgeschaltet ist, können Sie alternativ die PutPrincipalMappingAPI verwenden, um Benutzer- und Gruppenzugriffsinformationen hochzuladen.

Konfiguration	Beschreibung
SyncMode	Geben Sie an, wie Ihr Index aktualisiert Amazon Kendra werden soll, wenn sich der Inhalt Ihrer Datenquelle ändert. Sie können wählen zwischen: • `FORCED_FULL_CRAWL` um den gesamten Inhalt neu zu indizieren und vorhandene Inhalte jedes Mal zu ersetzen, wenn Ihre Datenquelle mit Ihrem Index synchronisiert wird. • `FULL_CRAWL` um bei jeder Synchronisierung Ihrer Datenquelle mit Ihrem Index nur neue, geänderte und gelöschte Inhalte zu indiziere n. Amazon Kendra kann den Mechanismus Ihrer Datenquelle verwenden, um Inhaltsän derungen nachzuverfolgen und Inhalte zu indexieren, die sich seit der letzten Synchroni sierung geändert haben. • `CHANGE_LOG` um bei jeder Synchroni sierung Ihrer Datenquelle mit Ihrem Index nur neue und geänderte Inhalte zu indiziere n. Amazon Kendra kann den Mechanismus Ihrer Datenquelle verwenden, um Inhaltsän derungen nachzuverfolgen und Inhalte zu indexieren, die sich seit der letzten Synchroni sierung geändert haben.

Konfiguration	Beschreibung
SecreN	Der Amazon-Ressourcenname (ARN) eines AWS Secrets Manager Geheimnisses, das die Schlüssel-Wert-Paare enthält, die für die Verbindung mit Ihrem erforderlich sind. GitHub Das Geheimnis muss eine JSON-Struktur mit den folgenden Schlüsseln enthalten: `{ "personalToken": " token" }`
version	Die Version dieser Vorlage, die derzeit unterstützt wird.

GitHub JSON-Schema

Das Folgende ist das GitHub JSON-Schema:

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

Gmail-Vorlagenschema

Sie fügen eine JSON-Datei ein, die das Datenquellenschema als Teil des TemplateConfigurationObjekts enthält. Geben Sie den Typ der Datenquelle als`GMAIL`, ein Geheimnis für Ihre Authentifizierungsdaten und andere erforderliche Konfigurationen an. Geben Sie dann `TEMPLATE` anType, wann Sie anrufen CreateDataSource.

Sie können die in diesem Entwicklerhandbuch enthaltene Vorlage verwenden. Siehe Gmail-JSON-Schema.

In der folgenden Tabelle werden die Parameter des Gmail-JSON-Schemas beschrieben.

Konfiguration	Beschreibung
Verbindung/Konfiguration	Konfigurationsinformationen für den Endpunkt für die Datenquelle.
Repository-Konfigurationen	Konfigurationsinformationen für den Inhalt der Datenquelle. Beispielsweise die Konfiguration bestimmter Inhaltstypen und Feldzuordnungen. Geben Sie den Typ der Datenquelle und den geheimen ARN an.
• Nachricht • Anhänge	Eine Liste von Objekten, die die Attribute oder Feldnamen Ihrer Gmail-Nachrichten und -Anlagen Amazon Kendra Indexfeldnamen zuordnen. Weitere Informationen finden Sie unter Zuweisen von Datenquellenfeldern.
Zusätzliche Eigenschaften	Zusätzliche Konfigurationsoptionen für Ihre Inhalte in Ihrer Datenquelle.
• inclusionLabelNameMuster • exclusionLabelNameMuster • inclusionAttachmentTypeMuster • exclusionAttachmentTypeMuster • inclusionAttachmentNameMuster • exclusionAttachmentNameMuster • inclusionSubjectFilter • exclusionSubjectFilter • isSubjectAnd • inclusionFromFilter • exclusionFromFilter • inclusionToFilter • exclusionToFilter	Eine Liste mit Mustern für reguläre Ausdrücke , mit denen Sie Nachrichten mit bestimmte n Betreffnamen in Ihre Gmail-Datenquelle aufnehmen oder ausschließen können. Dateien, die dem Muster entsprechen, sind im Index enthalten. Wenn eine Datei sowohl einem Einschluss- als auch einem Ausschlus smuster entspricht, hat das Ausschlussmuster Vorrang und die Datei wird nicht in den Index aufgenommen.

Konfiguration	Beschreibung
• inclusionCcFilter • exclusionCcFilter • inclusionBccFilter • exclusionBccFilter	
beforeDateFilter	Geben Sie Nachrichten und Anlagen an, die vor einem bestimmten Datum aufgenommen werden sollen.
afterDateFilter	Geben Sie Nachrichten und Anlagen an, die nach einem bestimmten Datum hinzugefügt werden sollen.
isCrawlAttachment	Ein boolescher Wert, mit dem Sie auswählen können, ob Anlagen gecrawlt werden sollen. Nachrichten werden automatisch gecrawlt.
Typ	Der Typ der Datenquelle. Geben Sie `GMAIL` als Datenquellentyp an.
shouldCrawlDraftNachrichten	Ein boolescher Wert, mit dem Sie auswählen können, ob Nachrichtenentwürfe gecrawlt werden sollen.

Konfiguration	Beschreibung
SyncMode	Geben Sie an, wie Ihr Index aktualisiert Amazon Kendra werden soll, wenn sich der Inhalt Ihrer Datenquelle ändert. Sie können wählen zwischen: • `FORCED_FULL_CRAWL` um den gesamten Inhalt neu zu indizieren und vorhandene Inhalte jedes Mal zu ersetzen, wenn Ihre Datenquelle mit Ihrem Index synchronisiert wird. • `FULL_CRAWL` um bei jeder Synchronisierung Ihrer Datenquelle mit Ihrem Index nur neue, geänderte und gelöschte Inhalte zu indiziere n. Amazon Kendra kann den Mechanismus Ihrer Datenquelle verwenden, um Inhaltsän derungen nachzuverfolgen und Inhalte zu indexieren, die sich seit der letzten Synchroni sierung geändert haben. **Important** Da es keine API zum Aktualisieren dauerhaft gelöschter Gmail-Nachrichten gibt, werden alle neuen, geänderten oder gelöschten Inhalte synchronisiert: • Nachrichten, die dauerhaft aus Gmail gelöscht wurden, werden nicht aus Ihrem Amazon Kendra Index entfernt • Synchronisiert keine Änderungen an Gmail-E-Mail-Labels Um die Änderungen an den Labels Ihrer Gmail-Datenquelle und dauerhaft

Konfiguration	Beschreibung
	gelöschte E-Mail-Nachrichten mit Ihrem Amazon Kendra Index zu synchronisieren, müssen Sie regelmäßig vollständige Crawls ausführen.
Sekretär N	Der Amazon-Ressourcenname (ARN) eines Secrets Manager Manager-Geheimnisses, das die Schlüssel-Wert-Paare enthält, die für die Verbindung mit Ihrem Gmail erforderlich sind. Das Geheimnis muss eine JSON-Struktur mit den folgenden Schlüsseln enthalten: `{ "adminAccountEmailId": " service account email", "clientEmailId": " user account email", "privateKey": " private key" }`
version	Die Version der Vorlage, die derzeit unterstützt wird.

Gmail-JSON-Schema

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

Google Drive-Vorlagenschema

Sie fügen eine JSON-Datei ein, die das Datenquellenschema als Teil des TemplateConfigurationObjekts enthält. Geben Sie den Typ der Datenquelle alsGOOGLEDRIVE2, ein Geheimnis für Ihre Authentifizierungsdaten und andere erforderliche Konfigurationen an. Geben Sie dann TEMPLATE anType, wann Sie anrufen CreateDataSource.

Sie können die in diesem Entwicklerhandbuch enthaltene Vorlage verwenden. Siehe Google Drive-JSON-Schema.

In der folgenden Tabelle werden die Parameter des Google Drive-JSON-Schemas beschrieben.

Konfiguration	Beschreibung
Verbindung/Konfiguration	Konfigurationsinformationen für die Datenquel le.
repositoryEndpointMetadata	Die Endpunktinformationen für die Datenquel le. Diese Datenquelle gibt keinen Endpunkt an. Sie wählen Ihren Authentifizierungs typ: `serviceAccount` und`OAuth2`. Die Verbindungsinformationen sind in einem AWS

Konfiguration	Beschreibung
	Secrets Manager Geheimnis enthalten, das Sie angeben`secretArn` .
authType	Wählen Sie `OAuth2` je nach Anwendungsfall zwischen `serviceAccount` und.
Repository-Konfigurationen	Konfigurationsinformationen für den Inhalt der Datenquelle. Beispielsweise die Konfiguration bestimmter Inhaltstypen und Feldzuordnungen.
• file • Kommentar	Eine Liste von Objekten, die die Attribute oder Feldnamen Ihres Google Drives Amazon Kendra Indexfeldnamen zuordnen. Weitere Informationen finden Sie unter Zuweisen von Datenquellenfeldern.
Zusätzliche Eigenschaften	Zusätzliche Konfigurationsoptionen für Ihre Inhalte in Ihrer Datenquelle
• maxFileSizeInMegaBytes	Geben Sie eine Dateigrößenbeschränkung in MB an, die gecrawlt Amazon Kendra werden soll.
• iscrawlComment	`true`um Kommentare in Ihrer Google Drive-Datenquelle zu crawlen.
• isCrawlMyDriveAndSharedWithMe	`true`um Drive-Laufwerke in Ihrer Google Drive-Datenquelle zu crawlen MyDrive und mit mir geteilt zu haben.
• isCrawlSharedLaufwerke	`true`um Shared Drives in Ihrer Google Drive-Datenquelle zu crawlen.

Konfiguration	Beschreibung
isCrawlAcl	`true`um die Informationen der Zugriffskontrollliste (ACL) für Ihre Dokumente zu durchsuchen, falls Sie über eine ACL verfügen und diese für die Zugriffskontrolle verwenden möchten. Die ACL gibt an, auf welche Dokumente Benutzer und Gruppen zugreifen und welche sie durchsuchen können. Die ACL-Informationen werden verwendet, um Suchergebnisse nach dem Benutzer- oder Gruppenzugriff auf Dokumente zu filtern. Weitere Informationen finden Sie unter Benutzerkontextfilterung.
• excludeUserAccounts • excludeSharedDrives • excludeMimeTypes • exclusionFileTypeMuster • exclusionFileNameMuster • exclusionFilePathFiltern	Eine Liste mit Mustern für reguläre Ausdrücke, um bestimmte Dateien in Ihrer Google Drive-Datenquelle auszuschließen. Dateien, die dem Muster entsprechen, werden aus dem Index ausgeschlossen. Dateien, die den Mustern nicht entsprechen, werden in den Index aufgenommen. Wenn eine Datei sowohl einem Ausschluss- als auch einem Einschlussmuster entspricht, hat das Ausschlussmuster Vorrang, und die Datei wird nicht in den Index aufgenommen.
• includeUserAccounts • includeSharedDrives • includeMimeTypes • inclusionFileTypeMuster • inclusionFileNameMuster • inclusionFilePathFiltern	Eine Liste mit Mustern für reguläre Ausdrücke, um bestimmte Dateien in Ihre Google Drive-Datenquelle aufzunehmen. Dateien, die dem Muster entsprechen, sind im Index enthalten. Dateien, die nicht dem Muster entsprechen, werden aus dem Index ausgeschlossen. Wenn eine Datei sowohl einem Einschluss- als auch einem Ausschlussmuster entspricht, hat das Ausschlussmuster Vorrang und die Datei wird nicht in den Index aufgenommen.

Konfiguration	Beschreibung
Typ	Der Typ der Datenquelle. Geben Sie `GOOGLEDRIVEV2` als Datenquellentyp an.
enableIdentityCrawler	`true`um den Identity Crawler zu verwenden, um Amazon Kendra Identitäts- und Hauptinformationen von Benutzern und Gruppen zu synchronisieren, die Zugriff auf bestimmte Dokumente haben. Wenn Identity Crawler ausgeschaltet ist, können alle Dokumente öffentlich durchsucht werden. Wenn Sie die Zugriffskontrolle für Ihre Dokumente verwenden möchten und Identity Crawler ausgeschaltet ist, können Sie alternativ die PutPrincipalMappingAPI verwenden, um Benutzer- und Gruppenzugriffsinformationen hochzuladen.

Konfiguration	Beschreibung
SyncMode	Geben Sie an, wie Ihr Index aktualisiert Amazon Kendra werden soll, wenn sich der Inhalt Ihrer Datenquelle ändert. Sie können wählen zwischen: • `FORCED_FULL_CRAWL` um den gesamten Inhalt neu zu indizieren und vorhandene Inhalte jedes Mal zu ersetzen, wenn Ihre Datenquelle mit Ihrem Index synchronisiert wird. • `FULL_CRAWL` um bei jeder Synchronisierung Ihrer Datenquelle mit Ihrem Index nur neue, geänderte und gelöschte Inhalte zu indiziere n. Amazon Kendra kann den Mechanismus Ihrer Datenquelle verwenden, um Inhaltsän derungen nachzuverfolgen und Inhalte zu indexieren, die sich seit der letzten Synchroni sierung geändert haben. • `CHANGE_LOG` um bei jeder Synchroni sierung Ihrer Datenquelle mit Ihrem Index nur neue und geänderte Inhalte zu indiziere n. Amazon Kendra kann den Mechanismus Ihrer Datenquelle verwenden, um Inhaltsän derungen nachzuverfolgen und Inhalte zu indexieren, die sich seit der letzten Synchroni sierung geändert haben.

Konfiguration	Beschreibung

SecreN	Der Amazon-Ressourcenname (ARN) eines AWS Secrets Manager Geheimnisses, das die Schlüssel-Wert-Paare enthält, die für die Verbindung mit Ihrem Google Drive erforderlich sind. Das Geheimnis muss eine JSON-Struktur mit den folgenden Schlüsseln enthalten:
	
	Wenn Sie die Authentifizierung für das Google-Dienstkonto verwenden:
	
	`{ "clientEmail": " user account email", "adminAccountEmail": " service account email", "privateKey": " private key" }`
	
	Wenn Sie die OAuth 2.0-Authentifizierung verwenden:
	
	`{ "clientID": " OAuth client ID", "clientSecret": " client secret", "refreshToken": " refresh token" }`

version	Die Version dieser Vorlage, die derzeit unterstützt wird.

Google Drive-JSON-Schema

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

IBM DB2-Vorlagenschema

Sie fügen eine JSON-Datei ein, die das Datenquellenschema als Teil des TemplateConfigurationObjekts enthält. Geben Sie den Typ der Datenquelle als`JDBC`, den Datenbanktyp als`db2`, ein Geheimnis für Ihre Authentifizierungsdaten und andere erforderliche Konfigurationen an. Geben Sie dann `TEMPLATE` an`Type`, wann Sie anrufen CreateDataSource.

Sie können die in diesem Entwicklerhandbuch enthaltene Vorlage verwenden. Siehe IBM DB2 JSON-Schema.

In der folgenden Tabelle werden die Parameter des IBM DB2 JSON-Schemas beschrieben.

Konfiguration	Beschreibung
Verbindung/Konfiguration	Konfigurationsinformationen für den Endpunkt für die Datenquelle.
repositoryEndpointMetadata	Erforderliche Konfigurationsinformationen für die Verbindung Ihrer Datenquelle. • dbType — Der Typ der Java-Datenbank, die Sie verwenden, unabhängig davon `mysql`, `db2`, `postgresql` `oracle`, oder. `sqlserver` • DBHost — Der Datenbank-Hostname. • DBPort — Der Datenbankport. • dbInstance — Die Datenbankinstanz.
Repository-Konfigurationen	Konfigurationsinformationen für den Inhalt der Datenquelle. Beispielsweise die Konfiguration bestimmter Inhaltstypen und Feldzuordnungen. Geben Sie den Typ der Datenquelle und den geheimen ARN an.
document	Eine Liste von Objekten, die die Attribute oder Feldnamen Ihres Datenbankinhalts Amazon Kendra Indexfeldnamen zuordnen. Weitere Informationen finden Sie unter Zuweisen von Datenquellenfeldern.
Zusätzliche Eigenschaften	Zusätzliche Konfigurationsoptionen für Ihre Inhalte in Ihrer Datenquelle. Dient zum Ein- oder Ausschließen bestimmter Inhalte in Ihrer Datenbankdatenquelle.
Primärschlüssel	Geben Sie den Primärschlüssel für die Datenbanktabelle an. Dies identifiziert eine Tabelle in Ihrer Datenbank.

Konfiguration	Beschreibung
Titel/Spalte	Geben Sie den Namen der Titelspalte des Dokuments in Ihrer Datenbanktabelle ein.
BodyColumn	Geben Sie den Namen der Titelspalte des Dokuments in Ihrer Datenbanktabelle ein.
sqlQuery	Geben Sie SQL-Abfrageanweisungen wie SELECT- und JOIN-Operationen ein. SQL-Abfragen müssen weniger als 32 KB groß sein. Amazon Kendra durchsucht den gesamten Datenbankinhalt, der Ihrer Abfrage entspricht.
Spalte „Zeitstempel“	Geben Sie den Namen der Spalte ein, die Zeitstempel enthält. Amazon Kendra verwendet Zeitstempelinformationen, um Änderungen an Ihrem Inhalt zu erkennen und nur geänderte Inhalte zu synchronisieren.
Zeitstempelformat	Geben Sie den Namen der Spalte ein, die Zeitstempelformate enthält, anhand derer Inhaltsänderungen erkannt und Ihre Inhalte erneut synchronisiert werden sollen.
Zeitzone	Geben Sie den Namen der Spalte ein, die Zeitzonen für den Inhalt enthält, der gecrawlt werden soll.
changeDetectingColumns	Geben Sie die Namen der Spalten ein, anhand derer Inhaltsänderungen erkannt Amazon Kendra werden sollen. Amazon Kendra indexiert den Inhalt neu, wenn sich eine dieser Spalten ändert
allowedUsersColumns	Geben Sie den Namen der Spalte ein, die Benutzer-IDs enthält, um Zugriff auf Inhalte zu erhalten.

Konfiguration	Beschreibung
allowedGroupsColumn	Geben Sie den Namen der Spalte ein, die Benutzer-IDs enthält, denen der Zugriff auf Inhalte gewährt werden soll.
Quelle-URI-Spalte	Geben Sie den Namen der Spalte ein, die Quell-URLs enthält, die indexiert werden sollen.
isSslEnabled	Geben Sie SQL-Abfrageanweisungen wie SELECT- und JOIN-Operationen ein. SQL-Abfragen müssen weniger als 32 KB groß sein. Amazon Kendra durchsucht den gesamten Datenbankinhalt, der Ihrer Abfrage entspricht.
Typ	Der Typ der Datenquelle. Geben Sie `JDBC` als Datenquellentyp an.

Konfiguration	Beschreibung
Sync-Modus	Geben Sie an, wie Ihr Index aktualisiert Amazon Kendra werden soll, wenn sich der Inhalt Ihrer Datenquelle ändert. Sie können wählen zwischen: • `FORCED_FULL_CRAWL` um den gesamten Inhalt neu zu indizieren und vorhandene Inhalte jedes Mal zu ersetzen, wenn Ihre Datenquelle mit Ihrem Index synchronisiert wird. • `FULL_CRAWL` um bei jeder Synchronisierung Ihrer Datenquelle mit Ihrem Index nur neue, geänderte und gelöschte Inhalte zu indiziere n. Amazon Kendra kann den Mechanismus Ihrer Datenquelle verwenden, um Inhaltsän derungen nachzuverfolgen und Inhalte zu indexieren, die sich seit der letzten Synchroni sierung geändert haben. • `CHANGE_LOG` um bei jeder Synchroni sierung Ihrer Datenquelle mit Ihrem Index nur neue und geänderte Inhalte zu indiziere n. Amazon Kendra kann den Mechanismus Ihrer Datenquelle verwenden, um Inhaltsän derungen nachzuverfolgen und Inhalte zu indexieren, die sich seit der letzten Synchroni sierung geändert haben.

Konfiguration	Beschreibung
SecreN	Der Amazon-Ressourcenname (ARN) eines Secrets Manager Manager-Geheimnisses, das den Benutzernamen und das Passwort enthält, die für die Verbindung mit Ihrer Datenbank erforderlich sind. Das Geheimnis muss eine JSON-Struktur mit den folgenden Schlüsseln enthalten: `{ "user name": "database user name", "password": " password" }`
version	Die Version der Vorlage, die derzeit unterstützt wird.

IBM DB2 JSON-Schema

```
{
  "$schema": "http://json-schema.org/draft-04/schema#",
  "type": "object",
  "properties": {
    "connectionConfiguration": {
      "type": "object",
      "properties": {
        "repositoryEndpointMetadata": {
          "type": "object",
          "properties": {
            "dbType": {
              "type": "string",
              "enum": [
                "mysql",
                "db2",
                "postgresql",
                "oracle",
                "sqlserver"
              ]
            },
```

```
            "dbHost": {
              "type": "string"
            },
            "dbPort": {
              "type": "string"
            },
            "dbInstance": {
              "type": "string"
            }
          },
          "required": [
            "dbType",
            "dbHost",
            "dbPort",
            "dbInstance"
          ]
        }
      },
      "required": [
        "repositoryEndpointMetadata"
      ]
    },
    "repositoryConfigurations": {
      "type": "object",
      "properties": {
        "document": {
          "type": "object",
          "properties": {
            "fieldMappings": {
              "type": "array",
              "items": [
                {
                  "type": "object",
                  "properties": {
                    "indexFieldName": {
                      "type": "string"
                    },
                    "indexFieldType": {
                      "type": "string"
                    },
                    "dataSourceFieldName": {
                      "type": "string"
                    }
                  },
```

```
                "required": [
                  "indexFieldName",
                  "indexFieldType",
                  "dataSourceFieldName"
                ]
              }
            ]
          }
        },
        "required": [
          "fieldMappings"
        ]
      }
    },
    "required": [
    ]
  },
  "additionalProperties": {
    "type": "object",
    "properties": {
      "primaryKey": {
        "type": "string"
      },
      "titleColumn": {
        "type": "string"
      },
      "bodyColumn": {
        "type": "string"
      },
      "sqlQuery": {
        "type": "string",
        "not": {
          "pattern": ";+"
        }
      },
      "timestampColumn": {
        "type": "string"
      },
      "timestampFormat": {
        "type": "string"
      },
      "timezone": {
        "type": "string"
      },
```

```
        "changeDetectingColumns": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "allowedUsersColumn": {
          "type": "string"
        },
        "allowedGroupsColumn": {
          "type": "string"
        },
        "sourceURIColumn": {
          "type": "string"
        },
        "isSslEnabled": {
          "type": "boolean"
        }
      },
      "required": ["primaryKey", "titleColumn", "bodyColumn", "sqlQuery"]
    },
    "type" : {
      "type" : "string",
      "pattern": "JDBC"
    },
    "syncMode": {
      "type": "string",
      "enum": [
        "FORCED_FULL_CRAWL",
        "FULL_CRAWL",
        "CHANGE_LOG"
      ]
    },
    "secretArn": {
      "type": "string"
    }
  },
  "version": {
    "type": "string",
    "anyOf": [
      {
        "pattern": "1.0.0"
      }
    ]
```

```
  },
  "required": [
      "connectionConfiguration",
      "repositoryConfigurations",
      "syncMode",
      "additionalProperties",
      "secretArn",
      "type"
  ]
}
```

Microsoft Exchange-Vorlagenschema

Sie fügen eine JSON-Datei ein, die das Datenquellenschema als Teil des TemplateConfigurationObjekts enthält. Sie geben die Mandanten-ID als Teil der Verbindungskonfiguration oder der Repository-Endpunktdetails an. Geben Sie außerdem den Typ der DatenquelleMSEXCHANGE, ein Geheimnis für Ihre Authentifizierungsdaten und andere erforderliche Konfigurationen an. Geben Sie dann TEMPLATE anType, wann Sie anrufen CreateDataSource.

Sie können die in diesem Entwicklerhandbuch enthaltene Vorlage verwenden. Siehe Microsoft Exchange-JSON-Schema.

In der folgenden Tabelle werden die Parameter des Microsoft Exchange JSON-Schemas beschrieben.

Konfiguration	Beschreibung
Verbindung/Konfiguration	Konfigurationsinformationen für den Endpunkt für die Datenquelle.
repositoryEndpointMetadata	Die Endpunktinformationen für die Datenquelle.
TenantID	Die Microsoft 365-Mandanten-ID. Sie finden Ihre Mandanten-ID in den Eigenschaften Ihres Azure Active Directory-Portals oder in Ihrer OAuth-Anwendung.
Repository-Konfigurationen	Konfigurationsinformationen für den Inhalt der Datenquelle. Beispielsweise die Konfiguration bestimmter Inhaltstypen und Feldzuordnungen.

Konfiguration	Beschreibung
• email • attachment • calendar • Kontakte • notes	Eine Liste von Objekten, die die Attribute oder Feldnamen Ihrer Microsoft Exchange-Datenquelle Amazon Kendra Indexfeldern zuordnen. Weitere Informationen finden Sie unter Zuweisen von Datenquellenfeldern.
Zusätzliche Eigenschaften	Zusätzliche Konfigurationsoptionen für Inhalte in Ihrer Datenquelle
Einschlussmuster	Eine Liste von Mustern für reguläre Ausdrücke , um bestimmte Dateien in Ihre Microsoft Exchange-Datenquelle aufzunehmen. Dateien, die dem Muster entsprechen, sind im Index enthalten. Dateien, die nicht dem Muster entsprechen, werden aus dem Index ausgeschl ossen. Wenn eine Datei sowohl einem Ein- als auch einem Ausschlussmuster entspricht, hat das Ausschlussmuster Vorrang und die Datei ist nicht im Index enthalten.
Ausschlussmuster	Eine Liste von Mustern für reguläre Ausdrücke , um bestimmte Dateien in Ihrer Microsoft Exchange-Datenquelle auszuschließen. Dateien, die dem Muster entsprechen, werden aus dem Index ausgeschlossen. Dateien, die den Mustern nicht entsprechen, werden in den Index aufgenommen. Wenn eine Datei sowohl einem Ausschluss- als auch einem Einschlus smuster entspricht, hat das Ausschlussmuster Vorrang und die Datei wird nicht in den Index aufgenommen.

Konfiguration	Beschreibung
• inclusionUsersList • inclusionUsersFileName • inclusionDomainUsers	Eine Liste von Mustern für reguläre Ausdrücke , um bestimmte Benutzer und Benutzerd ateien in Ihre Microsoft Exchange-Datenquel le aufzunehmen. Benutzer, die den Mustern entsprechen, werden in den Index aufgenomm en. Benutzer, die den Mustern nicht entsprech en, werden aus dem Index ausgeschlossen. Wenn ein Benutzer sowohl einem Inklusions- als auch einem Ausschlussmuster entsprich t, hat das Ausschlussmuster Vorrang und der Benutzer wird nicht in den Index aufgenommen.
• exclusionUsersList • exclusionUsersFileName • exclusionDomainUsers	Eine Liste von Mustern für reguläre Ausdrücke , um bestimmte Benutzer und Benutzerd ateien in Ihrer Microsoft Exchange-Datenquel le auszuschließen. Benutzer, die den Mustern entsprechen, werden aus dem Index ausgeschl ossen. Benutzer, die den Mustern nicht entsprechen, werden in den Index aufgenomm en. Wenn ein Benutzer sowohl einem Ausschluss- als auch einem Einschlussmuster entspricht, hat das Ausschlussmuster Vorrang und der Benutzer wird nicht in den Index aufgenommen.
S3-Bucket-Name	Der Name Ihres S3-Buckets, falls Sie diesen verwenden möchten.
• CrawlCalendar • CrawlNotizen • CrawlKontakte • crawlFolderAcl	`true`um diese Arten von Inhalts- und Zugriffskontrollinformationen in Ihrer Microsoft Exchange-Datenquelle zu crawlen.

Konfiguration	Beschreibung
startCalendarDateZeit	Sie können ein bestimmtes Startdatum und eine bestimmte Startzeit für Ihren Kalenderinhalt konfigurieren.
endCalendarDateUhrzeit	Sie können ein bestimmtes Enddatum und eine bestimmte Endzeit für Kalenderinhalte konfigurieren.
subject	Sie können eine bestimmte Betreffzeile für Ihren E-Mail-Inhalt konfigurieren.
EmailFrom	Sie können eine bestimmte E-Mail für den Inhalt Ihrer Absender- oder Absendermail konfigurieren.
E-Mail an	Sie können eine bestimmte E-Mail für den Inhalt Ihrer „An“ -E-Mail oder Empfänger-Mail konfigurieren.

Konfiguration	Beschreibung
Synchronisierungsmodus	Geben Sie an, wie Ihr Index aktualisiert Amazon Kendra werden soll, wenn sich der Inhalt Ihrer Datenquelle ändert. Sie können wählen zwischen: • `FORCED_FULL_CRAWL` um den gesamten Inhalt neu zu indizieren und vorhandene Inhalte jedes Mal zu ersetzen, wenn Ihre Datenquelle mit Ihrem Index synchronisiert wird. • `FULL_CRAWL` um bei jeder Synchronisierung Ihrer Datenquelle mit Ihrem Index nur neue, geänderte und gelöschte Inhalte zu indiziere n. Amazon Kendra kann den Mechanismus Ihrer Datenquelle verwenden, um Inhaltsän derungen nachzuverfolgen und Inhalte zu indexieren, die sich seit der letzten Synchroni sierung geändert haben. • `CHANGE_LOG` um bei jeder Synchroni sierung Ihrer Datenquelle mit Ihrem Index nur neue und geänderte Inhalte zu indiziere n. Amazon Kendra kann den Mechanismus Ihrer Datenquelle verwenden, um Inhaltsän derungen nachzuverfolgen und Inhalte zu indexieren, die sich seit der letzten Synchroni sierung geändert haben.
Typ	Der Typ der Datenquelle. Geben Sie `MSEXCHANGE` als Datenquellentyp an.

Konfiguration	Beschreibung
Sekretär N	Der Amazon-Ressourcenname (ARN) eines AWS Secrets Manager Geheimnisses, das die Schlüssel-Wert-Paare enthält, die für die Verbindung mit Ihrem Microsoft Exchange erforderlich sind. Dazu gehören Ihre Client-ID und Ihr geheimer Client-Schlüssel, der generiert wird, wenn Sie eine OAuth-Anw endung im Azure-Portal erstellen.
version	Die Version dieser Vorlage, die derzeit unterstützt wird.

Microsoft Exchange-JSON-Schema

```
{
  "$schema": "http://json-schema.org/draft-04/schema#",
  "type": "object",
  "properties": {
    "connectionConfiguration": {
      "type": "object",
      "properties": {
        "repositoryEndpointMetadata": {
          "type": "object",
          "properties": {
            "tenantId": {
              "type": "string",
              "pattern": "^[0-9a-f]{8}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]
{12}$",
              "minLength": 36,
              "maxLength": 36
            }
          },
          "required": ["tenantId"]
        }
      }
    },
    "repositoryConfigurations": {
      "type": "object",
```

```
      "properties": {
        "email": {
          "type": "object",
          "properties": {
            "fieldMappings": {
              "type": "array",
              "items": [
                {
                  "type": "object",
                  "properties": {
                    "indexFieldName": {
                      "type": "string"
                    },
                    "indexFieldType": {
                      "type": "string",
                      "enum": ["STRING", "STRING_LIST", "DATE"]
                    },
                    "dataSourceFieldName": {
                      "type": "string"
                    },
                    "dateFieldFormat": {
                      "type": "string",
                      "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                    }
                  },
                  "required": [
                    "indexFieldName",
                    "indexFieldType",
                    "dataSourceFieldName"
                  ]
                }
              ]
            }
          },
          "required": [
            "fieldMappings"
          ]
        },
        "attachment": {
          "type": "object",
          "properties": {
            "fieldMappings": {
              "type": "array",
              "items": [
```

```
            {
              "type": "object",
              "properties": {
                "indexFieldName": {
                  "type": "string"
                },
                "indexFieldType": {
                  "type": "string",
                  "enum": ["STRING", "DATE","LONG"]
                },
                "dataSourceFieldName": {
                  "type": "string"
                },
                "dateFieldFormat": {
                  "type": "string",
                  "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                }
              },
              "required": [
                "indexFieldName",
                "indexFieldType",
                "dataSourceFieldName"
              ]
            }
          ]
        }
      },
      "required": [
        "fieldMappings"
      ]
    },
    "calendar": {
      "type": "object",
      "properties": {
        "fieldMappings": {
          "type": "array",
          "items": [
            {
              "type": "object",
              "properties": {
                "indexFieldName": {
                  "type": "string"
                },
                "indexFieldType": {
```

```
                    "type": "string",
                    "enum": ["STRING", "STRING_LIST", "DATE"]
                  },
                  "dataSourceFieldName": {
                    "type": "string"
                  },
                  "dateFieldFormat": {
                    "type": "string",
                    "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                  }
                },
                "required": [
                  "indexFieldName",
                  "indexFieldType",
                  "dataSourceFieldName"
                ]
              }
            ]
          }
        },
        "required": [
          "fieldMappings"
        ]
      },
      "contacts": {
        "type": "object",
        "properties": {
          "fieldMappings": {
            "type": "array",
            "items": [
              {
                "type": "object",
                "properties": {
                  "indexFieldName": {
                    "type": "string"
                  },
                  "indexFieldType": {
                    "type": "string",
                    "enum": ["STRING", "STRING_LIST", "DATE"]
                  },
                  "dataSourceFieldName": {
                    "type": "string"
                  },
                  "dateFieldFormat": {
```

```
                    "type": "string",
                    "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                  }
                },
                "required": [
                  "indexFieldName",
                  "indexFieldType",
                  "dataSourceFieldName"
                ]
              }
            ]
          }
        },
        "required": [
          "fieldMappings"
        ]
      },
      "notes": {
        "type": "object",
        "properties": {
          "fieldMappings": {
            "type": "array",
            "items": [
              {
                "type": "object",
                "properties": {
                  "indexFieldName": {
                    "type": "string"
                  },
                  "indexFieldType": {
                    "type": "string",
                    "enum": ["STRING", "DATE"]
                  },
                  "dataSourceFieldName": {
                    "type": "string"
                  },
                  "dateFieldFormat": {
                    "type": "string",
                    "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                  }
                },
                "required": [
                  "indexFieldName",
                  "indexFieldType",
```

```
                  "dataSourceFieldName"
                ]
              }
            ]
          }
        },
        "required": [
          "fieldMappings"
        ]
      }
    },
    "required": ["email"
    ]
  },
  "additionalProperties": {
    "type": "object",
    "properties": {
      "inclusionPatterns": {
        "type": "array",
        "items": {
          "type": "string"
        }
      },
      "exclusionPatterns": {
        "type": "array",
        "items": {
          "type": "string"
        }
      },
      "inclusionUsersList": {
        "type": "array",
        "items": {
          "type": "string",
          "format": "email"
        }
      },
      "exclusionUsersList": {
        "type": "array",
        "items": {
          "type": "string",
          "format": "email"
        }
      },
      "s3bucketName": {
```

```
          "type": "string"
        },
        "inclusionUsersFileName": {
          "type": "string"
        },
        "exclusionUsersFileName": {
          "type": "string"
        },
        "inclusionDomainUsers": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "exclusionDomainUsers": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "crawlCalendar": {
          "type": "boolean"
        },
        "crawlNotes": {
          "type": "boolean"
        },
        "crawlContacts": {
          "type": "boolean"
        },
        "crawlFolderAcl": {
          "type": "boolean"
        },
        "startCalendarDateTime": {
          "anyOf": [
            {
              "type": "string",
              "pattern": "^[0-9]{4}-[0-9]{2}-[0-9]{2}T[0-9]{2}:[0-9]{2}:[0-9]{2}Z$"
            },
            {
              "type": "string",
              "pattern": ""
            }
          ]
        },
```

```
        "endCalendarDateTime": {
          "anyOf": [
            {
            "type": "string",
            "pattern": "^[0-9]{4}-[0-9]{2}-[0-9]{2}T[0-9]{2}:[0-9]{2}:[0-9]{2}Z$"
            },
            {
              "type": "string",
              "pattern": ""
            }
          ]
        },
        "subject": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "emailFrom": {
          "type": "array",
          "items": {
            "type": "string",
            "format": "email"
          }
        },
        "emailTo": {
          "type": "array",
          "items": {
            "type": "string",
            "format": "email"
          }
        }
      },
      "required": [
      ]
    },
    "syncMode": {
      "type": "string",
      "enum": [
        "FORCED_FULL_CRAWL",
        "FULL_CRAWL",
        "CHANGE_LOG"
      ]
    },
```

```
    "type" : {
      "type" : "string",
      "pattern": "MSEXCHANGE"
    },
    "secretArn": {
      "type": "string"
    }
  },
  "version": {
    "type": "string",
    "anyOf": [
      {
        "pattern": "1.0.0"
      }
    ]
  },
  "required": [
    "connectionConfiguration",
    "repositoryConfigurations",
    "syncMode",
    "additionalProperties",
    "secretArn",
    "type"
  ]
}
```

OneDrive Microsoft-Vorlagenschema

Sie fügen eine JSON-Datei ein, die das Datenquellenschema als Teil des TemplateConfigurationObjekts enthält. Sie geben die Mandanten-ID als Teil der Verbindungskonfiguration oder der Repository-Endpunktdetails an. Geben Sie außerdem den Typ der Datenquelle und ein Geheimnis für Ihre Authentifizierungsdaten sowie andere erforderliche Konfigurationen an. `ONEDRIVEV2` Geben Sie dann `TEMPLATE` an`Type`, wann Sie anrufen CreateDataSource.

Sie können die in diesem Entwicklerhandbuch enthaltene Vorlage verwenden. Siehe Microsoft OneDrive JSON-Schema.

In der folgenden Tabelle werden die Parameter des Microsoft OneDrive JSON-Schemas beschrieben.

Konfiguration	Beschreibung
Verbindung/Konfiguration	Konfigurationsinformationen für den Endpunkt für die Datenquelle.
repositoryEndpointMetadata	Die Endpunktinformationen für die Datenquelle.
TenantID	Die Microsoft 365-Mandanten-ID. Sie finden Ihre Mandanten-ID in den Eigenschaften Ihres Azure Active Directory-Portals oder in Ihrer OAuth-Anwendung.
Repository-Konfigurationen	Konfigurationsinformationen für den Inhalt der Datenquelle. Beispielsweise die Konfiguration bestimmter Inhaltstypen und Feldzuordnungen.
file	Eine Liste von Objekten, die die Attribute oder Feldnamen Ihrer OneDrive Microsoft -Dateien Amazon Kendra Indexfeldnamen zuordnen. Weitere Informationen finden Sie unter Zuweisen von Datenquellenfeldern.
Zusätzliche Eigenschaften	Zusätzliche Konfigurationsoptionen für Ihre Inhalte in Ihrer Datenquelle
• userNameFilter • userFilterPath • inclusionFileTypeMuster • exclusionFileTypeMuster • inclusionFileNameMuster • exclusionFileNameMuster • inclusionFilePathMuster • exclusionFilePathMuster • inclusionOneNoteSectionNamePatterns • exclusionOneNoteSectionNamePatterns • inclusionOneNotePageNamePatterns	Sie können wählen, ob Sie bestimmte Dateien, OneNote Abschnitte und OneNote Seiten indizieren und nach Benutzernamen filtern möchten.

Konfiguration	Beschreibung
• exclusionOneNotepageNamePatterns	
isUserNameAuf S3	`true`um eine Liste von Benutzernamen in einer Datei bereitzustellen, die in einem gespeichert ist Amazon S3.
Typ	Der Typ der Datenquelle. Geben Sie `ONEDRIVEV2` als Datenquellentyp an.
enableIdentityCrawler	`true`um den Identity Crawler zu verwenden, um Amazon Kendra Identitäts- und Hauptinfo rmationen von Benutzern und Gruppen zu synchronisieren, die Zugriff auf bestimmte Dokumente haben. Wenn Identity Crawler ausgeschaltet ist, können alle Dokumente öffentlich durchsucht werden. Wenn Sie die Zugriffskontrolle für Ihre Dokumente verwenden möchten und Identity Crawler ausgeschaltet ist, können Sie alternativ die PutPrincipalMappin gAPI verwenden, um Benutzer- und Gruppenzu griffsinformationen hochzuladen.
Typ	Der Typ der Datenquelle. Geben Sie `ONEDRIVEV2` als Datenquellentyp an.

Konfiguration	Beschreibung
Sync-Modus	Geben Sie an, wie Ihr Index aktualisiert Amazon Kendra werden soll, wenn sich der Inhalt Ihrer Datenquelle ändert. Sie können wählen zwischen: • `FORCED_FULL_CRAWL` um den gesamten Inhalt neu zu indizieren und vorhandene Inhalte jedes Mal zu ersetzen, wenn Ihre Datenquelle mit Ihrem Index synchronisiert wird. • `FULL_CRAWL` um bei jeder Synchronisierung Ihrer Datenquelle mit Ihrem Index nur neue, geänderte und gelöschte Inhalte zu indiziere n. Amazon Kendra kann den Mechanismus Ihrer Datenquelle verwenden, um Inhaltsän derungen nachzuverfolgen und Inhalte zu indexieren, die sich seit der letzten Synchroni sierung geändert haben. • `CHANGE_LOG` um bei jeder Synchroni sierung Ihrer Datenquelle mit Ihrem Index nur neue und geänderte Inhalte zu indiziere n. Amazon Kendra kann den Mechanismus Ihrer Datenquelle verwenden, um Inhaltsän derungen nachzuverfolgen und Inhalte zu indexieren, die sich seit der letzten Synchroni sierung geändert haben.

Konfiguration	Beschreibung
SecreN	Der Amazon-Ressourcenname (ARN) eines AWS Secrets Manager Geheimnisses, das die Schlüssel-Wert-Paare enthält, die für die Verbindung mit Ihrem Microsoft erforderlich sind. OneDrive Das Geheimnis muss eine JSON-Struktur mit den folgenden Schlüsseln enthalten: `{ "clientId": " client ID", "clientSecret": " client secret" }`
version	Die Version dieser Vorlage, die derzeit unterstützt wird.

Microsoft OneDrive JSON-Schema

```
{
 "$schema": "http://json-schema.org/draft-04/schema#",
 "type": "object",
 "properties": {
  "connectionConfiguration": {
   "type": "object",
   "properties": {
    "repositoryEndpointMetadata": {
     "type": "object",
     "properties": {
      "tenantId": {
       "type": "string",
       "pattern": "^[0-9a-f]{8}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{12}$",
       "minLength": 36,
       "maxLength": 36
      }
     },
     "required": [
      "tenantId"
     ]
```

```
    }
   },
   "required": [
    "repositoryEndpointMetadata"
   ]
  },
  "repositoryConfigurations": {
   "type": "object",
   "properties": {
    "file": {
     "type": "object",
     "properties": {
      "fieldMappings": {
       "type": "array",
       "items": [
        {
         "type": "object",
         "properties": {
          "indexFieldName": {
           "type": "string"
          },
          "indexFieldType": {
           "type": "string",
           "enum": [
            "STRING",
            "STRING_LIST",
            "DATE",
            "LONG"
           ]
          },
          "dataSourceFieldName": {
           "type": "string"
          },
          "dateFieldFormat": {
           "type": "string",
           "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
          }
         },
         "required": [
          "indexFieldName",
          "indexFieldType",
          "dataSourceFieldName"
         ]
        }
```

```
        ]
       }
      },
      "required": [
       "fieldMappings"
      ]
     }
    }
   },
   "additionalProperties": {
    "type": "object",
    "properties": {
     "userNameFilter": {
      "type": "array",
      "items": {
       "type": "string"
      }
     },
     "userFilterPath": {
      "type": "string"
     },
     "isUserNameOnS3": {
      "type": "boolean"
     },
     "inclusionFileTypePatterns": {
      "type": "array",
      "items": {
       "type": "string"
      }
     },
     "exclusionFileTypePatterns": {
      "type": "array",
      "items": {
       "type": "string"
      }
     },
     "inclusionFileNamePatterns": {
      "type": "array",
      "items": {
       "type": "string"
      }
     },
     "exclusionFileNamePatterns": {
      "type": "array",
```

```
     "items": {
      "type": "string"
     }
    },
    "inclusionFilePathPatterns": {
     "type": "array",
     "items": {
      "type": "string"
     }
    },
    "exclusionFilePathPatterns": {
     "type": "array",
     "items": {
      "type": "string"
     }
    },
    "inclusionOneNoteSectionNamePatterns": {
     "type": "array",
     "items": {
      "type": "string"
     }
    },
    "exclusionOneNoteSectionNamePatterns": {
     "type": "array",
     "items": {
      "type": "string"
     }
    },
    "inclusionOneNotePageNamePatterns": {
     "type": "array",
     "items": {
      "type": "string"
     }
    },
    "exclusionOneNotePageNamePatterns": {
     "type": "array",
     "items": {
      "type": "string"
     }
    }
   },
   "required": []
  },
```

```
  "enableIdentityCrawler": {
   "type": "boolean"
  },
  "type": {
   "type": "string",
   "pattern": "ONEDRIVEV2"
  },
  "syncMode": {
   "type": "string",
   "enum": [
    "FULL_CRAWL",
    "FORCED_FULL_CRAWL",
    "CHANGE_LOG"
   ]
  },
  "secretArn": {
   "type": "string",
   "minLength": 20,
   "maxLength": 2048
  }
 },
 "version": {
  "type": "string",
  "anyOf": [
   {
    "pattern": "1.0.0"
   }
  ]
 },
 "required": [
  "connectionConfiguration",
  "repositoryConfigurations",
  "syncMode",
  "additionalProperties",
  "secretArn",
  "type"
 ]
}
```

SharePoint Microsoft-Vorlagenschema

Sie fügen eine JSON-Datei ein, die das Datenquellenschema als Teil des TemplateConfigurationObjekts enthält. Sie geben die SharePoint Site-URL/URLs, die Domäne und,

falls erforderlich, auch eine Mandanten-ID als Teil der Verbindungskonfiguration oder der Repository-Endpunktdetails an. Geben Sie außerdem den Typ der Datenquelle`SHAREPOINTV2`, ein Geheimnis für Ihre Authentifizierungsdaten und andere erforderliche Konfigurationen an. Sie geben dann `TEMPLATE` den Typ an, wenn Sie anrufen CreateDataSource.

Sie können die in diesem Entwicklerhandbuch enthaltene Vorlage verwenden. Siehe SharePoint JSON-Schema.

In der folgenden Tabelle werden die Parameter des Microsoft SharePoint JSON-Schemas beschrieben.

Konfiguration	Beschreibung
Verbindung/Konfiguration	Konfigurationsinformationen für den Endpunkt für die Datenquelle
repositoryEndpointMetadata	Die Endpunktinformationen für die Datenquelle
TenantID	Die Mieter-ID Ihres SharePoint Kontos.
Domain	Die Domain Ihres SharePoint Kontos.
URLs der Website	Die Host-URLs Ihres SharePoint Kontos.
repositoryAdditionalProperties	Zusätzliche Eigenschaften für die Verbindung mit dem Endpunkt des Repository/der Datenquelle.
S3-Bucket-Name	Der Name des Amazon S3 Buckets, in dem Ihr selbstsigniertes Azure AD-X.509-Zertifikat gespeichert ist.
Name des S3-Zertifikats	Der Name des selbstsignierten Azure AD-X.509-Zertifikats, das in Ihrem Bucket gespeichert ist. Amazon S3
authType	Die Art der Authentifizierung, die Sie verwenden, ob`OAuth2`,`OAuth2Certificate` ,,`OAuth2App` , `Basic` `OAuth2_RefreshToken` `NTLM`, oder. `Kerberos`

Konfiguration	Beschreibung
version	Die SharePoint Version, die Sie verwenden, ob `Server` oder`Online`.
onPremVersion	Die SharePoint Serverversion, die Sie verwenden`2013`, ob `2016`oder`2019`, oder`SubscriptionEdition` .
Repository-Konfigurationen	Konfigurationsinformationen für den Inhalt der Datenquelle. Beispielsweise die Konfiguration bestimmter Inhaltstypen und Feldzuordnungen.
• event • angezeigten • file • Verknüpfung • attachment • Kommentar	Eine Liste von Objekten, die die Attribute oder Feldnamen Ihres SharePoint Inhalts Amazon Kendra Indexfeldnamen zuordnen. Weitere Informationen finden Sie unter Zuweisen von Datenquellenfeldern.
Zusätzliche Eigenschaften	Zusätzliche Konfigurationsoptionen für Ihre Inhalte in Ihrer Datenquelle.

Konfiguration	Beschreibung
• eventTitleFilterRegEx • pageTitleFilterRegEx • linkTitleFilterRegEx • inclusionFilePath • exclusionFilePath • inclusionFileTypeMuster • exclusionFileTypeMuster • inclusionFileNameMuster • exclusionFileNameMuster • inclusionOneNoteSectionNamePatterns • exclusionOneNoteSectionNamePatterns • inclusionOneNotePageNamePatterns • exclusionOneNotePageNamePatterns	Eine Liste von Mustern für reguläre Ausdrücke , mit denen Sie bestimmte Inhalte in Ihre SharePoint Datenquelle einschließen/aussc hließen können. Inhaltselemente, die den Einschlussmustern entsprechen, werden in den Index aufgenommen. Inhaltselemente, die nicht den Inklusionsmustern entsprechen, werden aus dem Index ausgeschlossen. Wenn eine Datei sowohl einem Einschluss- als auch einem Ausschlussmuster entspricht, hat das Ausschlussmuster Vorrang, und die Datei wird nicht in den Index aufgenommen.
• Dateien durchforsten • Seiten crawlen • Ereignisse crawlen • Kommentare crawlen • Links crawlen • Crawl-Anhänge	`true`um diese Art von Inhalten zu crawlen.

Konfiguration	Beschreibung
CI crawlen	`true`um die Informationen der Zugriffskontrollliste (ACL) für Ihre Dokumente zu durchsuchen, falls Sie über eine ACL verfügen und diese für die Zugriffskontrolle verwenden möchten. Die ACL gibt an, auf welche Dokumente Benutzer und Gruppen zugreifen und welche sie durchsuchen können. Die ACL-Informationen werden verwendet, um Suchergebnisse nach dem Benutzer- oder Gruppenzugriff auf Dokumente zu filtern. Weitere Informationen finden Sie unter Benutzerkontextfilterung.
fieldForUserID	Geben Sie an, `email` ob Sie die Benutzer-E-Mail für die Benutzer-ID verwenden möchten, oder `userPrincipalName` ob Sie einen Benutzernamen für die Benutzer-ID verwenden möchten. Wenn Sie keine Option angeben, `email` wird diese Option standardmäßig verwendet.
ACL-Konfiguration	Geben Sie entweder `ACLWithLDAPEmailFmt` `ACLWithManualEmailFmt` , oder an. `ACLWithUsernameFmtM`
E-Mail-Domäne	Die Domain der E-Mail. Zum Beispiel "*`amazon.com`* “.
• isCrawlLocalGroupMapping • isCrawlAdGroupMapping	`true`um Informationen zur Gruppenzuweisung zu crawlen.
ProxyHost	Der Hostname des Webproxys, den Sie verwenden, ohne das Protokoll http:// oder https://.

Konfiguration	Beschreibung
ProxyPort	Die vom Host-URL-Transportprotokoll verwendete Portnummer. Muss ein numerisch er Wert zwischen 0 und 65535 sein.
Typ	Geben Sie `SHAREPOINTV2` als Datenquel lentyp an
enableIdentityCrawler	`true`um den Identity Crawler zu verwenden , um Amazon Kendra Identitäts- und Prinzipal informationen von Benutzern und Gruppen mit Zugriff auf bestimmte Dokumente zu synchroni sieren. Wenn Identity Crawler ausgeschaltet ist, können alle Dokumente öffentlich durchsucht werden. Wenn Sie die Zugriffskontrolle für Ihre Dokumente verwenden möchten und Identity Crawler ausgeschaltet ist, können Sie alternati v die PutPrincipalMappingAPI verwenden, um Benutzer- und Gruppenzugriffsinformationen hochzuladen.

Konfiguration	Beschreibung
SyncMode	Geben Sie an, wie Ihr Index aktualisiert Amazon Kendra werden soll, wenn sich der Inhalt Ihrer Datenquelle ändert. Sie können wählen zwischen: • `FORCED_FULL_CRAWL` um den gesamten Inhalt neu zu indizieren und vorhandene Inhalte jedes Mal zu ersetzen, wenn Ihre Datenquelle mit Ihrem Index synchronisiert wird. • `FULL_CRAWL` um bei jeder Synchronisierung Ihrer Datenquelle mit Ihrem Index nur neue, geänderte und gelöschte Inhalte zu indiziere n. Amazon Kendra kann den Mechanismus Ihrer Datenquelle verwenden, um Inhaltsän derungen nachzuverfolgen und Inhalte zu indexieren, die sich seit der letzten Synchroni sierung geändert haben. • `CHANGE_LOG` um bei jeder Synchroni sierung Ihrer Datenquelle mit Ihrem Index nur neue und geänderte Inhalte zu indiziere n. Amazon Kendra kann den Mechanismus Ihrer Datenquelle verwenden, um Inhaltsän derungen nachzuverfolgen und Inhalte zu indexieren, die sich seit der letzten Synchroni sierung geändert haben.

Konfiguration	Beschreibung
SecreN	Der Amazon-Ressourcenname (ARN) eines AWS Secrets Manager Geheimnisses, das die Schlüssel-Wert-Paare enthält, die für die Verbindung mit Ihrem erforderlich sind. SharePoint Informationen zu diesen Schlüssel -Wert-Paaren finden Sie unter Verbindungsanweisungen für SharePoint Online und Server. SharePoint
version	Die Version dieser Vorlage, die derzeit unterstützt wird.

SharePoint JSON-Schema

```
{
 "$schema": "http://json-schema.org/draft-04/schema#",
 "type": "object",
 "properties": {
  "connectionConfiguration": {
   "type": "object",
   "properties": {
    "repositoryEndpointMetadata": {
     "type": "object",
     "properties": {
      "tenantId": {
       "type": "string",
       "pattern": "^[0-9a-f]{8}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{12}$",
       "minLength": 36,
       "maxLength": 36
      },
      "domain": {
       "type": "string"
      },
      "siteUrls": {
       "type": "array",
       "items": {
        "type": "string",
        "pattern": "https://.*"
```

```
        }
       },
       "repositoryAdditionalProperties": {
        "type": "object",
        "properties": {
         "s3bucketName": {
          "type": "string"
         },
         "s3certificateName": {
          "type": "string"
         },
         "authType": {
          "type": "string",
          "enum": [
           "OAuth2",
           "OAuth2Certificate",
           "OAuth2App",
           "Basic",
           "OAuth2_RefreshToken",
           "NTLM",
           "Kerberos"
          ]
         },
         "version": {
          "type": "string",
          "enum": [
           "Server",
           "Online"
          ]
         },
         "onPremVersion": {
          "type": "string",
          "enum": [
           "",
           "2013",
           "2016",
           "2019",
           "SubscriptionEdition"
          ]
         }
        },
        "required": [
         "authType",
         "version"
```

```
      ]
     }
    },
    "required": [
     "siteUrls",
     "domain",
     "repositoryAdditionalProperties"
    ]
   }
  },
  "required": [
   "repositoryEndpointMetadata"
  ]
 },
 "repositoryConfigurations": {
  "type": "object",
  "properties": {
   "event": {
    "type": "object",
    "properties": {
     "fieldMappings": {
      "type": "array",
      "items": [
       {
        "type": "object",
        "properties": {
         "indexFieldName": {
          "type": "string"
         },
         "indexFieldType": {
          "type": "string",
          "enum": [
           "STRING",
           "STRING_LIST",
           "DATE"
          ]
         },
         "dataSourceFieldName": {
          "type": "string"
         },
         "dateFieldFormat": {
          "type": "string",
          "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
         }
```

```
        },
        "required": [
         "indexFieldName",
         "indexFieldType",
         "dataSourceFieldName"
        ]
       }
      ]
     }
    },
    "required": [
     "fieldMappings"
    ]
   },
   "page": {
    "type": "object",
    "properties": {
     "fieldMappings": {
      "type": "array",
      "items": [
       {
        "type": "object",
        "properties": {
         "indexFieldName": {
          "type": "string"
         },
         "indexFieldType": {
          "type": "string",
          "enum": [
           "STRING",
           "DATE",
           "LONG"
          ]
         },
         "dataSourceFieldName": {
          "type": "string"
         },
         "dateFieldFormat": {
          "type": "string",
          "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
         }
        },
        "required": [
         "indexFieldName",
```

```
          "indexFieldType",
          "dataSourceFieldName"
         ]
        }
       ]
      }
     },
     "required": [
      "fieldMappings"
     ]
    },
    "file": {
     "type": "object",
     "properties": {
      "fieldMappings": {
       "type": "array",
       "items": [
        {
         "type": "object",
         "properties": {
          "indexFieldName": {
           "type": "string"
          },
          "indexFieldType": {
           "type": "string",
           "enum": [
            "STRING",
            "DATE",
            "LONG"
           ]
          },
          "dataSourceFieldName": {
           "type": "string"
          },
          "dateFieldFormat": {
           "type": "string",
           "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
          }
         },
         "required": [
          "indexFieldName",
          "indexFieldType",
          "dataSourceFieldName"
         ]
```

```
        }
       ]
      }
     },
     "required": [
      "fieldMappings"
     ]
    },
    "link": {
     "type": "object",
     "properties": {
      "fieldMappings": {
       "type": "array",
       "items": [
        {
         "type": "object",
         "properties": {
          "indexFieldName": {
           "type": "string"
          },
          "indexFieldType": {
           "type": "string",
           "enum": [
            "STRING",
            "STRING_LIST",
            "DATE"
           ]
          },
          "dataSourceFieldName": {
           "type": "string"
          },
          "dateFieldFormat": {
           "type": "string",
           "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
          }
         },
         "required": [
          "indexFieldName",
          "indexFieldType",
          "dataSourceFieldName"
         ]
        }
       ]
      }
```

```
    },
    "required": [
     "fieldMappings"
    ]
   },
   "attachment": {
    "type": "object",
    "properties": {
     "fieldMappings": {
      "type": "array",
      "items": [
       {
        "type": "object",
        "properties": {
         "indexFieldName": {
          "type": "string"
         },
         "indexFieldType": {
          "type": "string",
          "enum": [
           "STRING",
           "STRING_LIST",
           "DATE"
          ]
         },
         "dataSourceFieldName": {
          "type": "string"
         },
         "dateFieldFormat": {
          "type": "string",
          "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
         }
        },
        "required": [
         "indexFieldName",
         "indexFieldType",
         "dataSourceFieldName"
        ]
       }
      ]
     }
    },
    "required": [
     "fieldMappings"
```

```
      ]
     },
     "comment": {
      "type": "object",
      "properties": {
       "fieldMappings": {
        "type": "array",
        "items": [
         {
          "type": "object",
          "properties": {
           "indexFieldName": {
            "type": "string"
           },
           "indexFieldType": {
            "type": "string",
            "enum": [
             "STRING",
             "STRING_LIST",
             "DATE"
            ]
           },
           "dataSourceFieldName": {
            "type": "string"
           },
           "dateFieldFormat": {
            "type": "string",
            "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
           }
          },
          "required": [
           "indexFieldName",
           "indexFieldType",
           "dataSourceFieldName"
          ]
         }
        ]
       }
      },
      "required": [
       "fieldMappings"
      ]
     }
    }
```

```
  },
  "additionalProperties": {
   "type": "object",
   "properties": {
    "eventTitleFilterRegEx": {
     "type": "array",
     "items": {
      "type": "string"
     }
    },
    "pageTitleFilterRegEx": {
     "type": "array",
     "items": {
      "type": "string"
     }
    },
    "linkTitleFilterRegEx": {
     "type": "array",
     "items": {
      "type": "string"
     }
    },
    "inclusionFilePath": {
     "type": "array",
     "items": {
      "type": "string"
     }
    },
    "exclusionFilePath": {
     "type": "array",
     "items": {
      "type": "string"
     }
    },
    "inclusionFileTypePatterns": {
     "type": "array",
     "items": {
      "type": "string"
     }
    },
    "exclusionFileTypePatterns": {
     "type": "array",
     "items": {
      "type": "string"
```

```
      }
     },
     "inclusionFileNamePatterns": {
      "type": "array",
      "items": {
       "type": "string"
      }
     },
     "exclusionFileNamePatterns": {
      "type": "array",
      "items": {
       "type": "string"
      }
     },
     "inclusionOneNoteSectionNamePatterns": {
      "type": "array",
      "items": {
       "type": "string"
      }
     },
     "exclusionOneNoteSectionNamePatterns": {
      "type": "array",
      "items": {
       "type": "string"
      }
     },
     "inclusionOneNotePageNamePatterns": {
      "type": "array",
      "items": {
       "type": "string"
      }
     },
     "exclusionOneNotePageNamePatterns": {
      "type": "array",
      "items": {
       "type": "string"
      }
     },
     "crawlFiles": {
      "type": "boolean"
     },
     "crawlPages": {
      "type": "boolean"
     },
```

```
    "crawlEvents": {
     "type": "boolean"
    },
    "crawlComments": {
     "type": "boolean"
    },
    "crawlLinks": {
     "type": "boolean"
    },
    "crawlAttachments": {
     "type": "boolean"
    },
    "crawlListData": {
     "type": "boolean"
    },
    "crawlAcl": {
     "type": "boolean"
    },
    "fieldForUserId": {
     "type": "string"
    },
    "aclConfiguration": {
     "type": "string",
     "enum": [
      "ACLWithLDAPEmailFmt",
      "ACLWithManualEmailFmt",
      "ACLWithUsernameFmt"
     ]
    },
    "emailDomain": {
     "type": "string"
    },
    "isCrawlLocalGroupMapping": {
     "type": "boolean"
    },
    "isCrawlAdGroupMapping": {
     "type": "boolean"
    },
    "proxyHost": {
     "type": "string"
    },
    "proxyPort": {
     "type": "string"
    }
```

```
    },
    "required": [
    ]
   },
   "type": {
    "type": "string",
    "pattern": "SHAREPOINTV2"
   },
   "enableIdentityCrawler": {
    "type": "boolean"
   },
   "syncMode": {
    "type": "string",
    "enum": [
     "FULL_CRAWL",
     "FORCED_FULL_CRAWL",
     "CHANGE_LOG"
    ]
   },
   "secretArn": {
    "type": "string",
    "minLength": 20,
    "maxLength": 2048
   }
  },
  "version": {
   "type": "string",
   "anyOf": [
    {
     "pattern": "1.0.0"
    }
   ]
  },
  "required": [
   "connectionConfiguration",
   "repositoryConfigurations",
   "enableIdentityCrawler",
   "syncMode",
   "additionalProperties",
   "secretArn",
   "type"
  ]
}
```

Microsoft SQL Server-Vorlagenschema

Sie fügen eine JSON-Datei ein, die das Datenquellenschema als Teil des TemplateConfigurationObjekts enthält. Geben Sie den Typ der Datenquelle als`JDBC`, den Datenbanktyp als`sqlserver`, ein Geheimnis für Ihre Authentifizierungsdaten und andere erforderliche Konfigurationen an. Geben Sie dann `TEMPLATE` an`Type`, wann Sie anrufen CreateDataSource.

Sie können die in diesem Entwicklerhandbuch enthaltene Vorlage verwenden. Siehe JSON-Schema für Microsoft SQL Server.

In der folgenden Tabelle werden die Parameter des Microsoft SQL Server-JSON-Schemas beschrieben.

Konfiguration	Beschreibung
Verbindungskonfiguration	Konfigurationsinformationen für den Endpunkt für die Datenquelle.
repositoryEndpointMetadata	Erforderliche Konfigurationsinformationen für die Verbindung Ihrer Datenquelle. • dbType — Der Typ der Java-Date nbank, die Sie verwenden, unabhängig davon`mysql`,`db2`, `postgresql oracle`, oder. `sqlserver` • DBHost — Der Datenbank-Hostname. • DBPort — Der Datenbankport. • dbInstance — Die Datenbankinstanz.
Repository-Konfigurationen	Konfigurationsinformationen für den Inhalt der Datenquelle. Beispielsweise die Konfiguration bestimmter Inhaltstypen und Feldzuordnungen. Geben Sie den Typ der Datenquelle und den geheimen ARN an.
document	Eine Liste von Objekten, die die Attribute oder Feldnamen Ihres Datenbankinhalts Amazon

Konfiguration	Beschreibung
	Kendra Indexfeldnamen zuordnen. Weitere Informationen finden Sie unter Zuweisen von Datenquellenfeldern.
Zusätzliche Eigenschaften	Zusätzliche Konfigurationsoptionen für Ihre Inhalte in Ihrer Datenquelle. Dient zum Ein- oder Ausschließen bestimmter Inhalte in Ihrer Datenbankdatenquelle.
Primärschlüssel	Geben Sie den Primärschlüssel für die Datenbanktabelle an. Dies identifiziert eine Tabelle in Ihrer Datenbank.
Titel/Spalte	Geben Sie den Namen der Titelspalte des Dokuments in Ihrer Datenbanktabelle ein.
BodyColumn	Geben Sie den Namen der Titelspalte des Dokuments in Ihrer Datenbanktabelle ein.
sqlQuery	Geben Sie SQL-Abfrageanweisungen wie SELECT- und JOIN-Operationen ein. SQL-Abfragen müssen weniger als 32 KB groß sein. Amazon Kendra durchsucht den gesamten Datenbankinhalt, der Ihrer Abfrage entspricht.
Spalte „Zeitstempel“	Geben Sie den Namen der Spalte ein, die Zeitstempel enthält. Amazon Kendra verwendet Zeitstempelinformationen, um Änderungen an Ihrem Inhalt zu erkennen und nur geänderte Inhalte zu synchronisieren.
Zeitstempelformat	Geben Sie den Namen der Spalte ein, die Zeitstempelformate enthält, anhand derer Inhaltsänderungen erkannt und Ihre Inhalte erneut synchronisiert werden sollen.

Konfiguration	Beschreibung
Zeitzone	Geben Sie den Namen der Spalte ein, die Zeitzonen für den Inhalt enthält, der gecrawlt werden soll.
changeDetectingColumns	Geben Sie die Namen der Spalten ein, anhand derer Inhaltsänderungen erkannt Amazon Kendra werden sollen. Amazon Kendra indexiert den Inhalt neu, wenn sich eine dieser Spalten ändert
allowedUsersColumns	Geben Sie den Namen der Spalte ein, die Benutzer-IDs enthält, um Zugriff auf Inhalte zu erhalten.
allowedGroupsColumn	Geben Sie den Namen der Spalte ein, die Benutzer-IDs enthält, denen der Zugriff auf Inhalte gewährt werden soll.
Quelle-URI-Spalte	Geben Sie den Namen der Spalte ein, die Quell-URLs enthält, die indexiert werden sollen.
isSslEnabled	Geben Sie SQL-Abfrageanweisungen wie SELECT- und JOIN-Operationen ein. SQL-Abfragen müssen weniger als 32 KB groß sein. Amazon Kendra durchsucht den gesamten Datenbankinhalt, der Ihrer Abfrage entspricht.
Typ	Der Typ der Datenquelle. Geben Sie `JDBC` als Datenquellentyp an.

Konfiguration	Beschreibung
Sync-Modus	Geben Sie an, wie Ihr Index aktualisiert Amazon Kendra werden soll, wenn sich der Inhalt Ihrer Datenquelle ändert. Sie können wählen zwischen: • `FORCED_FULL_CRAWL` um den gesamten Inhalt neu zu indizieren und vorhandene Inhalte jedes Mal zu ersetzen, wenn Ihre Datenquelle mit Ihrem Index synchronisiert wird. • `FULL_CRAWL` um bei jeder Synchronisierung Ihrer Datenquelle mit Ihrem Index nur neue, geänderte und gelöschte Inhalte zu indiziere n. Amazon Kendra kann den Mechanismus Ihrer Datenquelle verwenden, um Inhaltsän derungen nachzuverfolgen und Inhalte zu indexieren, die sich seit der letzten Synchroni sierung geändert haben. • `CHANGE_LOG` um bei jeder Synchroni sierung Ihrer Datenquelle mit Ihrem Index nur neue und geänderte Inhalte zu indiziere n. Amazon Kendra kann den Mechanismus Ihrer Datenquelle verwenden, um Inhaltsän derungen nachzuverfolgen und Inhalte zu indexieren, die sich seit der letzten Synchroni sierung geändert haben.

Konfiguration	Beschreibung
SecreN	Der Amazon-Ressourcenname (ARN) eines Secrets Manager Manager-Geheimnisses, das den Benutzernamen und das Passwort enthält, die für die Verbindung mit Ihrer Datenbank erforderlich sind. Das Geheimnis muss eine JSON-Struktur mit den folgenden Schlüsseln enthalten: `{ "user name": "database user name", "password": " password" }`
version	Die Version der Vorlage, die derzeit unterstützt wird.

JSON-Schema für 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"
  ]
}
```

Microsoft Teams-Vorlagenschema

Sie fügen eine JSON-Datei ein, die das Datenquellenschema als Teil des TemplateConfigurationObjekts enthält. Sie geben die Mandanten-ID als Teil der Verbindungskonfiguration oder der Repository-Endpunktdetails an. Geben Sie außerdem den Typ der Datenquelle`MSTEAMS`, ein Geheimnis für Ihre Authentifizierungsdaten und andere erforderliche Konfigurationen an. Geben Sie dann `TEMPLATE` an`Type`, wann Sie anrufen CreateDataSource.

Sie können die in diesem Entwicklerhandbuch enthaltene Vorlage verwenden. Siehe JSON-Schema für Microsoft Teams.

In der folgenden Tabelle werden die Parameter des Microsoft Teams JSON-Schemas beschrieben.

Konfiguration	Beschreibung
Verbindung/Konfiguration	Konfigurationsinformationen für den Endpunkt der Datenquelle.
repositoryEndpointMetadata	Die Endpunktinformationen für die Datenquelle.
TenantID	Die Microsoft 365-Mandanten-ID. Sie finden Ihre Mandanten-ID in den Eigenschaften Ihres Azure Active Directory-Portals oder in Ihrer OAuth-Anwendung.
Repository-Konfigurationen	Konfigurationsinformationen für den Inhalt der Datenquelle. Beispielsweise die Konfiguration bestimmter Inhaltstypen und Feldzuordnungen.

Konfiguration	Beschreibung
• Chat-Nachricht • Chat-Anhang • Beitrag auf dem Kanal • KanalWiki • Kanalanhang • Besprechung-Chat • Meeting-Datei • Notiz zur Besprechung • Besprechungskalender	Eine Liste von Objekten, die die Attribute oder Feldnamen Ihrer Microsoft Teams-Inhalte Amazon Kendra Indexfeldnamen zuordnen. Weitere Informationen finden Sie unter Zuweisen von Datenquellenfeldern.
Zusätzliche Eigenschaften	Zusätzliche Konfigurationsoptionen für Ihre Inhalte in Ihrer Datenquelle.
Zahlungsmodell	Gibt an, welche Art von Zahlungsmodell mit Ihrer Microsoft Teams-Datenquelle verwendet werden soll. Zahlungsmodelle nach Modell A sind auf Lizenz- und Zahlungsmodelle beschränkt, für die Sicherheitsbestimmungen eingehalten werden müssen. Die Zahlungsm odelle des Modells B eignen sich für Lizenz- und Zahlungsmodelle, für die keine Einhaltung von Sicherheitsvorschriften erforderlich ist.
• inclusionTeamNameFiltern • inclusionChannelNameFiltern • inclusionFileNameMuster • inclusionFileTypeMuster • inclusionUserEmailFiltern • inclusionOneNoteSectionNamePatterns • inclusionOneNotePageNamePatterns	Eine Liste von Mustern für reguläre Ausdrücke, um bestimmte Inhalte in Ihre Microsoft Teams-Datenquelle aufzunehmen. Elemente, die den Mustern entsprechen, sind im Index enthalten . Inhalte, die den Mustern nicht entsprech en, werden aus dem Index ausgeschlossen. Wenn Inhalt sowohl einem Einschluss- als auch einem Ausschlussmuster entspricht, hat das Ausschlussmuster Vorrang, und der Inhalt wird nicht in den Index aufgenommen.

Konfiguration	Beschreibung
• exclusionTeamNameFiltern • exclusionChannelNameFiltern • exclusionFileNameMuster • exclusionFileTypeMuster • exclusionUserEmailFiltern • exclusionOneNoteSectionNamePatterns • exclusionOneNotePageNamePatterns	Eine Liste von Mustern mit regulären Ausdrücken, um bestimmte Inhalte in Ihrer Microsoft Teams-Datenquelle auszuschließen. Inhalte, die den Mustern entsprechen, werden aus dem Index ausgeschlossen. Inhalte, die den Mustern nicht entsprechen, werden in den Index aufgenommen. Wenn Inhalte sowohl einem Inklusions- als auch einem Ausschlus smuster entsprechen, hat das Ausschlus smuster Vorrang, und der Inhalt wird nicht in den Index aufgenommen.
• isCrawlChatNachricht • isCrawlChatAnlage • isCrawlChannelBeitrag • isCrawlChannelAnlage • isCrawlChannelWiki • isCrawlCalendarTreffen • isCrawlMeetingPlaudern • isCrawlMeetingDatei • isCrawlMeetingNotiz	`true`um diese Arten von Inhalten in Ihrer Microsoft Teams-Datenquelle zu crawlen.
startCalendarDateZeit	Sie können ein bestimmtes Startdatum und eine bestimmte Startzeit für Ihren Kalenderi nhalt konfigurieren.
endCalendarDateUhrzeit	Sie können ein bestimmtes Enddatum und eine bestimmte Endzeit für Kalenderinhalte konfiguri eren.
Typ	Der Typ der Datenquelle. Geben Sie `MSTEAMS` als Datenquellentyp an.

Konfiguration	Beschreibung
enableIdentityCrawler	`true`um den Identity Crawler zu verwenden, um Amazon Kendra Identitäts- und Hauptinformationen von Benutzern und Gruppen zu synchronisieren, die Zugriff auf bestimmte Dokumente haben. Wenn Identity Crawler ausgeschaltet ist, können alle Dokumente öffentlich durchsucht werden. Wenn Sie die Zugriffskontrolle für Ihre Dokumente verwenden möchten und Identity Crawler ausgeschaltet ist, können Sie alternativ die PutPrincipalMappingAPI verwenden, um Benutzer- und Gruppenzugriffsinformationen hochzuladen.

Konfiguration	Beschreibung
SyncMode	Geben Sie an, wie Ihr Index aktualisiert Amazon Kendra werden soll, wenn sich der Inhalt Ihrer Datenquelle ändert. Sie können wählen zwischen: • `FORCED_FULL_CRAWL` um den gesamten Inhalt neu zu indizieren und vorhandene Inhalte jedes Mal zu ersetzen, wenn Ihre Datenquelle mit Ihrem Index synchronisiert wird. • `FULL_CRAWL` um bei jeder Synchronisierung Ihrer Datenquelle mit Ihrem Index nur neue, geänderte und gelöschte Inhalte zu indiziere n. Amazon Kendra kann den Mechanismus Ihrer Datenquelle verwenden, um Inhaltsän derungen nachzuverfolgen und Inhalte zu indexieren, die sich seit der letzten Synchroni sierung geändert haben. • `CHANGE_LOG` um bei jeder Synchroni sierung Ihrer Datenquelle mit Ihrem Index nur neue und geänderte Inhalte zu indiziere n. Amazon Kendra kann den Mechanismus Ihrer Datenquelle verwenden, um Inhaltsän derungen nachzuverfolgen und Inhalte zu indexieren, die sich seit der letzten Synchroni sierung geändert haben.

Konfiguration	Beschreibung
SecreN	Der Amazon-Ressourcenname (ARN) eines AWS Secrets Manager Geheimnisses, das die Schlüssel-Wert-Paare enthält, die für die Verbindung mit Ihren Microsoft Teams erforderl ich sind. Dazu gehören Ihre Client-ID und Ihr geheimer Client-Schlüssel, der generiert wird, wenn Sie eine OAuth-Anwendung im Azure-Por tal erstellen.
version	Die Version dieser Vorlage, die derzeit unterstützt wird.

JSON-Schema für 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"
  ]
}
```

Microsoft Yammer-Vorlagenschema

Sie fügen eine JSON-Datei hinzu, die das Datenquellenschema als Teil des TemplateConfigurationObjekts enthält. Geben Sie den Typ der Datenquelle als`YAMMER`, ein Geheimnis für Ihre Authentifizierungsdaten und andere erforderliche Konfigurationen an. Sie geben dann `TEMPLATE` den Typ an, wenn Sie anrufen CreateDataSource.

Sie können die in diesem Entwicklerhandbuch enthaltene Vorlage verwenden.

In der folgenden Tabelle werden die Parameter des Microsoft Yammer-JSON-Schemas beschrieben.

Konfiguration	Beschreibung
Verbindung/Konfiguration	Konfigurationsinformationen für die Datenquel le.
repositoryEndpointMetadata	Die Endpunktinformationen für die Datenquel le. Diese Datenquelle gibt keinen Endpunkt in an`repositoryEndpointMetadata` . Vielmehr sind die Verbindungsinformationen in einem AWS Secrets Manager Geheimnis enthalten, das Sie angeben`secretArn` .
Repository-Konfigurationen	Konfigurationsinformationen für den Inhalt der Datenquelle. Beispielsweise die Konfiguration bestimmter Inhaltstypen und Feldzuordnungen.
• Gemeinschaft • user • Nachricht • attachment	Eine Liste von Objekten, die Attribute oder Feldnamen von Microsoft Yammer-Inhalten Amazon Kendra Kendra-Indexfeldnamen zuordnen. Weitere Informationen finden Sie unter Zuweisen von Datenquellenfeldern.
Zusätzliche Eigenschaften	Zusätzliche Konfigurationsoptionen für Ihre Inhalte in Ihrer Datenquelle
Inklusionsmuster	Eine Liste von Mustern für reguläre Ausdrücke , um bestimmte Dateien in Ihre Microsoft Yammer-Datenquelle aufzunehmen. Dateien, die dem Muster entsprechen, sind im Index enthalten. Dateien, die den Mustern nicht entsprechen, werden aus dem Index ausgeschl ossen. Wenn eine Datei sowohl einem Ein- als auch einem Ausschlussmuster entspricht, hat das Ausschlussmuster Vorrang und die Datei ist nicht im Index enthalten.
Ausschlussmuster	Eine Liste von Mustern für reguläre Ausdrücke zum Ausschließen bestimmter Dateien in

Konfiguration	Beschreibung
	Ihrer Microsoft Yammer-Datenquelle. Dateien, die dem Muster entsprechen, werden aus dem Index ausgeschlossen. Dateien, die den Mustern nicht entsprechen, werden in den Index aufgenommen. Wenn eine Datei sowohl einem Ausschluss- als auch einem Einschlus smuster entspricht, hat das Ausschlussmuster Vorrang und die Datei wird nicht in den Index aufgenommen.
Seit Datum	Sie können einen `sinceDate` Parameter so konfigurieren, dass der Microsoft Yammer-Connector Inhalte auf der Grundlage eines bestimmten Inhalts crawlt. `sinceDate`
communityNameFilter	Sie können wählen, ob bestimmte Community-Inhalte indexiert werden sollen.
• isCrawlMessage • isCrawlAttachment • isCrawlPrivateNachricht	`true`um Nachrichten, Nachrichtenanhänge und private Nachrichten zu crawlen.
Typ	Geben Sie `YAMMER` als Datenquellentyp an.
Sekretär N	Der Amazon-Ressourcenname (ARN) eines AWS Secrets Manager Geheimnisses, das die Schlüssel-Wert-Paare enthält, die für die Verbindung mit Ihrem Microsoft Yammer erforderlich sind. Dazu gehören Ihr Microsoft Yammer-Benutzername und Ihr Passwort sowie Ihre Client-ID und Ihr Client-Geheimnis, die generiert werden, wenn Sie eine OAuth-Anwendung im Azure-Portal erstellen.

Konfiguration	Beschreibung
useChangeLog	`true`um anhand des Microsoft Yammer-Änderungsprotokolls zu ermitteln, welche Dokumente im Index aktualisiert werden müssen.
Sync-Modus	Geben Sie an, wie Ihr Index aktualisiert Amazon Kendra werden soll, wenn sich der Inhalt Ihrer Datenquelle ändert. Sie können wählen zwischen: • `FORCED_FULL_CRAWL` um den gesamten Inhalt neu zu indizieren und vorhandene Inhalte jedes Mal zu ersetzen, wenn Ihre Datenquelle mit Ihrem Index synchronisiert wird. • `FULL_CRAWL` um bei jeder Synchronisierung Ihrer Datenquelle mit Ihrem Index nur neue, geänderte und gelöschte Inhalte zu indiziere n. Amazon Kendra kann den Mechanismus Ihrer Datenquelle verwenden, um Inhaltsän derungen nachzuverfolgen und Inhalte zu indexieren, die sich seit der letzten Synchroni sierung geändert haben. • `CHANGE_LOG` um bei jeder Synchroni sierung Ihrer Datenquelle mit Ihrem Index nur neue und geänderte Inhalte zu indiziere n. Amazon Kendra kann den Mechanismus Ihrer Datenquelle verwenden, um Inhaltsän derungen nachzuverfolgen und Inhalte zu indexieren, die sich seit der letzten Synchroni sierung geändert haben.

Konfiguration	Beschreibung
enableIdentityCrawler	`true`um den Identity Crawler zu verwenden, um Amazon Kendra Identitäts- und Hauptinfo rmationen von Benutzern und Gruppen mit Zugriff auf bestimmte Dokumente zu synchroni sieren. Wenn Identity Crawler ausgeschaltet ist, können alle Dokumente öffentlich durchsucht werden. Wenn Sie die Zugriffskontrolle für Ihre Dokumente verwenden möchten und Identity Crawler ausgeschaltet ist, können Sie alternati v die PutPrincipalMappingAPI verwenden, um Benutzer- und Gruppenzugriffsinformationen hochzuladen.

Microsoft Yammer-JSON-Schema

```
{
  "$schema": "http://json-schema.org/draft-04/schema#",
  "type": "object",
  "properties": {
    "connectionConfiguration": {
      "type": "object",
      "properties": {
        "repositoryEndpointMetadata": {
          "type": "object",
          "properties": {
          }
        }
      },
      "required": [
        "repositoryEndpointMetadata"
      ]
    },
    "repositoryConfigurations": {
      "type": "object",
      "properties": {
        "community": {
          "type": "object",
          "properties": {
```

```
            "fieldMappings": {
              "type": "array",
              "items": {
                "anyOf": [
                  {
                    "type": "object",
                    "properties": {
                      "indexFieldName": {
                        "type": "string"
                      },
                      "indexFieldType": {
                        "type": "string",
                        "enum": [
                          "STRING",
                          "DATE"
                        ]
                      },
                      "dataSourceFieldName": {
                        "type": "string"
                      },
                      "dateFieldFormat": {
                        "type": "string",
                        "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                      }
                    },
                    "required": [
                      "indexFieldName",
                      "indexFieldType",
                      "dataSourceFieldName"
                    ]
                  }
                ]
              }
            }
          },
          "required": [
            "fieldMappings"
          ]
        },
        "user": {
          "type": "object",
          "properties": {
            "fieldMappings": {
              "type": "array",
```

```
            "items": {
              "anyOf": [
                {
                  "type": "object",
                  "properties": {
                    "indexFieldName": {
                      "type": "string"
                    },
                    "indexFieldType": {
                      "type": "string",
                      "enum": [
                        "STRING",
                        "DATE"
                      ]
                    },
                    "dataSourceFieldName": {
                      "type": "string"
                    },
                    "dateFieldFormat": {
                      "type": "string",
                      "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                    }
                  },
                  "required": [
                    "indexFieldName",
                    "indexFieldType",
                    "dataSourceFieldName"
                  ]
                }
              ]
            }
          }
        },
        "required": [
          "fieldMappings"
        ]
      },
      "message": {
        "type": "object",
        "properties": {
          "fieldMappings": {
            "type": "array",
            "items": {
              "anyOf": [
```

```
                {
                  "type": "object",
                  "properties": {
                    "indexFieldName": {
                      "type": "string"
                    },
                    "indexFieldType": {
                      "type": "string",
                      "enum": [
                        "STRING",
                        "DATE"
                      ]
                    },
                    "dataSourceFieldName": {
                      "type": "string"
                    },
                    "dateFieldFormat": {
                      "type": "string",
                      "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                    }
                  },
                  "required": [
                    "indexFieldName",
                    "indexFieldType",
                    "dataSourceFieldName"
                  ]
                }
              ]
            }
          }
        },
        "required": [
          "fieldMappings"
        ]
      },
      "attachment": {
        "type": "object",
        "properties": {
          "fieldMappings": {
            "type": "array",
            "items": {
              "anyOf": [
                {
                  "type": "object",
```

```
                  "properties": {
                    "indexFieldName": {
                      "type": "string"
                    },
                    "indexFieldType": {
                      "type": "string",
                      "enum": [
                        "STRING",
                        "DATE"
                      ]
                    },
                    "dataSourceFieldName": {
                      "type": "string"
                    },
                    "dateFieldFormat": {
                      "type": "string",
                      "pattern": "yyyy-MM-dd'T'HH:mm:ss'Z'"
                    }
                  },
                  "required": [
                    "indexFieldName",
                    "indexFieldType",
                    "dataSourceFieldName"
                  ]
                }
              ]
            }
          }
        },
        "required": [
          "fieldMappings"
        ]
      }
    }
  },
  "additionalProperties": {
    "type": "object",
    "properties": {
      "inclusionPatterns": {
        "type": "array"
      },
      "exclusionPatterns": {
        "type": "array"
      },
```

```
        "sinceDate": {
          "type": "string",
          "pattern": "^(19|2[0-9])[0-9]{2}-(0[1-9]|1[012])-(0[1-9]|[12][0-9]|
3[01])T(0[0-9]|1[0-9]|2[0-3]):([0-5][0-9]):([0-5][0-9])((\\+|-)(0[0-9]|1[0-9]|2[0-3]):
([0-5][0-9]))?$"
        },
        "communityNameFilter": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "isCrawlMessage": {
          "type": "boolean"
        },
        "isCrawlAttachment": {
          "type": "boolean"
        },
        "isCrawlPrivateMessage": {
          "type": "boolean"
        }
      },
      "required": [
        "sinceDate"
      ]
    },
    "type": {
      "type": "string",
      "pattern": "YAMMER"
    },
    "secretArn": {
      "type": "string",
      "minLength": 20,
      "maxLength": 2048
    },
    "useChangeLog": {
      "type": "string",
      "enum": [
        "true",
        "false"
      ]
    },
    "syncMode": {
      "type": "string",
```

```
      "enum": [
        "FORCED_FULL_CRAWL",
        "FULL_CRAWL",
        "CHANGE_LOG"
      ]
    },
    "enableIdentityCrawler": {
      "type": "boolean"
    },
    "version": {
      "type": "string",
      "anyOf": [
        {
          "pattern": "1.0.0"
        }
      ]
    }
  },
  "required": [
    "connectionConfiguration",
    "repositoryConfigurations",
    "additionalProperties",
    "type",
    "secretArn",
    "syncMode"
  ]
}
```

MySQL-Vorlagenschema

Sie fügen eine JSON-Datei ein, die das Datenquellenschema als Teil des TemplateConfigurationObjekts enthält. Geben Sie den Typ der Datenquelle als`JDBC`, den Datenbanktyp als`mysql`, ein Geheimnis für Ihre Authentifizierungsdaten und andere erforderliche Konfigurationen an. Geben Sie dann `TEMPLATE` an`Type`, wann Sie anrufen CreateDataSource.

Sie können die in diesem Entwicklerhandbuch enthaltene Vorlage verwenden. Siehe MySQL JSON-Schema.

In der folgenden Tabelle werden die Parameter des MySQL-JSON-Schemas beschrieben.

Konfiguration	Beschreibung
Verbindung/Konfiguration	Konfigurationsinformationen für den Endpunkt für die Datenquelle.
repositoryEndpointMetadata	Erforderliche Konfigurationsinformationen für die Verbindung Ihrer Datenquelle. • dbType — Der Typ der Java-Datenbank, die Sie verwenden, unabhängig davon `mysql`, `db2`, `postgresql` `oracle`, oder. `sqlserver` • DBHost — Der Datenbank-Hostname. • DBPort — Der Datenbankport. • dbInstance — Die Datenbankinstanz.
Repository-Konfigurationen	Konfigurationsinformationen für den Inhalt der Datenquelle. Beispielsweise die Konfiguration bestimmter Inhaltstypen und Feldzuordnungen. Geben Sie den Typ der Datenquelle und den geheimen ARN an.
document	Eine Liste von Objekten, die die Attribute oder Feldnamen Ihres Datenbankinhalts Amazon Kendra Indexfeldnamen zuordnen. Weitere Informationen finden Sie unter Zuweisen von Datenquellenfeldern.
Zusätzliche Eigenschaften	Zusätzliche Konfigurationsoptionen für Ihre Inhalte in Ihrer Datenquelle. Dient zum Ein- oder Ausschließen bestimmter Inhalte in Ihrer Datenbankdatenquelle.
Primärschlüssel	Geben Sie den Primärschlüssel für die Datenbanktabelle an. Dies identifiziert eine Tabelle in Ihrer Datenbank.

Konfiguration	Beschreibung
Titel/Spalte	Geben Sie den Namen der Titelspalte des Dokuments in Ihrer Datenbanktabelle ein.
BodyColumn	Geben Sie den Namen der Titelspalte des Dokuments in Ihrer Datenbanktabelle ein.
sqlQuery	Geben Sie SQL-Abfrageanweisungen wie SELECT- und JOIN-Operationen ein. SQL-Abfragen müssen weniger als 32 KB groß sein. Amazon Kendra durchsucht den gesamten Datenbankinhalt, der Ihrer Abfrage entspricht.
Spalte „Zeitstempel“	Geben Sie den Namen der Spalte ein, die Zeitstempel enthält. Amazon Kendra verwendet Zeitstempelinformationen, um Änderungen an Ihrem Inhalt zu erkennen und nur geänderte Inhalte zu synchronisieren.
Zeitstempelformat	Geben Sie den Namen der Spalte ein, die Zeitstempelformate enthält, anhand derer Inhaltsänderungen erkannt und Ihre Inhalte erneut synchronisiert werden sollen.
Zeitzone	Geben Sie den Namen der Spalte ein, die Zeitzonen für den Inhalt enthält, der gecrawlt werden soll.
changeDetectingColumns	Geben Sie die Namen der Spalten ein, anhand derer Inhaltsänderungen erkannt Amazon Kendra werden sollen. Amazon Kendra indexiert den Inhalt neu, wenn sich eine dieser Spalten ändert
allowedUsersColumns	Geben Sie den Namen der Spalte ein, die Benutzer-IDs enthält, um Zugriff auf Inhalte zu erhalten.

Konfiguration	Beschreibung
allowedGroupsColumn	Geben Sie den Namen der Spalte ein, die Benutzer-IDs enthält, denen der Zugriff auf Inhalte gewährt werden soll.
Quelle-URI-Spalte	Geben Sie den Namen der Spalte ein, die Quell-URLs enthält, die indexiert werden sollen.
isSslEnabled	Geben Sie SQL-Abfrageanweisungen wie SELECT- und JOIN-Operationen ein. SQL-Abfragen müssen weniger als 32 KB groß sein. Amazon Kendra durchsucht den gesamten Datenbankinhalt, der Ihrer Abfrage entspricht.
Typ	Der Typ der Datenquelle. Geben Sie `JDBC` als Datenquellentyp an.

Konfiguration	Beschreibung
Sync-Modus	Geben Sie an, wie Ihr Index aktualisiert Amazon Kendra werden soll, wenn sich der Inhalt Ihrer Datenquelle ändert. Sie können wählen zwischen: • `FORCED_FULL_CRAWL` um den gesamten Inhalt neu zu indizieren und vorhandene Inhalte jedes Mal zu ersetzen, wenn Ihre Datenquelle mit Ihrem Index synchronisiert wird. • `FULL_CRAWL` um bei jeder Synchronisierung Ihrer Datenquelle mit Ihrem Index nur neue, geänderte und gelöschte Inhalte zu indiziere n. Amazon Kendra kann den Mechanismus Ihrer Datenquelle verwenden, um Inhaltsän derungen nachzuverfolgen und Inhalte zu indexieren, die sich seit der letzten Synchroni sierung geändert haben. • `CHANGE_LOG` um bei jeder Synchroni sierung Ihrer Datenquelle mit Ihrem Index nur neue und geänderte Inhalte zu indiziere n. Amazon Kendra kann den Mechanismus Ihrer Datenquelle verwenden, um Inhaltsän derungen nachzuverfolgen und Inhalte zu indexieren, die sich seit der letzten Synchroni sierung geändert haben.

Konfiguration	Beschreibung
SecreN	Der Amazon-Ressourcenname (ARN) eines Secrets Manager Manager-Geheimnisses, das den Benutzernamen und das Passwort enthält, die für die Verbindung mit Ihrer Datenbank erforderlich sind. Das Geheimnis muss eine JSON-Struktur mit den folgenden Schlüsseln enthalten: `{ "user name": "database user name", "password": " password" }`
version	Die Version der Vorlage, die derzeit unterstützt wird.

MySQL JSON-Schema

```
{
  "$schema": "http://json-schema.org/draft-04/schema#",
  "type": "object",
  "properties": {
    "connectionConfiguration": {
      "type": "object",
      "properties": {
        "repositoryEndpointMetadata": {
          "type": "object",
          "properties": {
            "dbType": {
              "type": "string",
              "enum": [
                "mysql",
                "db2",
                "postgresql",
                "oracle",
                "sqlserver"
              ]
            },
```

```
            "dbHost": {
              "type": "string"
            },
            "dbPort": {
              "type": "string"
            },
            "dbInstance": {
              "type": "string"
            }
          },
          "required": [
            "dbType",
            "dbHost",
            "dbPort",
            "dbInstance"
          ]
        }
      },
      "required": [
        "repositoryEndpointMetadata"
      ]
    },
    "repositoryConfigurations": {
      "type": "object",
      "properties": {
        "document": {
          "type": "object",
          "properties": {
            "fieldMappings": {
              "type": "array",
              "items": [
                {
                  "type": "object",
                  "properties": {
                    "indexFieldName": {
                      "type": "string"
                    },
                    "indexFieldType": {
                      "type": "string"
                    },
                    "dataSourceFieldName": {
                      "type": "string"
                    }
                  },
```

```
                "required": [
                  "indexFieldName",
                  "indexFieldType",
                  "dataSourceFieldName"
                ]
              }
            ]
          }
        },
        "required": [
          "fieldMappings"
        ]
      }
    },
    "required": [
    ]
  },
  "additionalProperties": {
    "type": "object",
    "properties": {
      "primaryKey": {
        "type": "string"
      },
      "titleColumn": {
        "type": "string"
      },
      "bodyColumn": {
        "type": "string"
      },
      "sqlQuery": {
        "type": "string",
        "not": {
          "pattern": ";+"
        }
      },
      "timestampColumn": {
        "type": "string"
      },
      "timestampFormat": {
        "type": "string"
      },
      "timezone": {
        "type": "string"
      },
```

```
        "changeDetectingColumns": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "allowedUsersColumn": {
          "type": "string"
        },
        "allowedGroupsColumn": {
          "type": "string"
        },
        "sourceURIColumn": {
          "type": "string"
        },
        "isSslEnabled": {
          "type": "boolean"
        }
      },
      "required": ["primaryKey", "titleColumn", "bodyColumn", "sqlQuery"]
    },
    "type" : {
      "type" : "string",
      "pattern": "JDBC"
    },
    "syncMode": {
      "type": "string",
      "enum": [
        "FORCED_FULL_CRAWL",
        "FULL_CRAWL",
        "CHANGE_LOG"
      ]
    },
    "secretArn": {
      "type": "string"
    }
  },
  "version": {
    "type": "string",
    "anyOf": [
      {
        "pattern": "1.0.0"
      }
    ]
```

```
  },
  "required": [
      "connectionConfiguration",
      "repositoryConfigurations",
      "syncMode",
      "additionalProperties",
      "secretArn",
      "type"
  ]
}
```

Oracle-Datenbank-Vorlagenschema

Sie fügen eine JSON-Datei ein, die das Datenquellenschema als Teil des TemplateConfigurationObjekts enthält. Geben Sie den Typ der Datenquelle als`JDBC`, den Datenbanktyp als`oracle`, ein Geheimnis für Ihre Authentifizierungsdaten und andere erforderliche Konfigurationen an. Geben Sie dann `TEMPLATE` an`Type`, wann Sie anrufen CreateDataSource.

Sie können die in diesem Entwicklerhandbuch enthaltene Vorlage verwenden. Siehe JSON-Schema der Oracle-Datenbank.

In der folgenden Tabelle werden die Parameter des Oracle Database-JSON-Schemas beschrieben.

Konfiguration	Beschreibung
Verbindung/Konfiguration	Konfigurationsinformationen für den Endpunkt für die Datenquelle.
repositoryEndpointMetadata	Erforderliche Konfigurationsinformationen für die Verbindung Ihrer Datenquelle. • dbType — Der Typ der Java-Date nbank, die Sie verwenden, unabhängig davon`mysql`,`db2`, `postgresql` `oracle`, oder. `sqlserver` • DBHost — Der Datenbank-Hostname. • DBPort — Der Datenbankport. • dbInstance — Die Datenbankinstanz.

Konfiguration	Beschreibung
Repository-Konfigurationen	Konfigurationsinformationen für den Inhalt der Datenquelle. Beispielsweise die Konfiguration bestimmter Inhaltstypen und Feldzuordnungen. Geben Sie den Typ der Datenquelle und den geheimen ARN an.
document	Eine Liste von Objekten, die die Attribute oder Feldnamen Ihres Datenbankinhalts Amazon Kendra Indexfeldnamen zuordnen. Weitere Informationen finden Sie unter Zuweisen von Datenquellenfeldern.
Zusätzliche Eigenschaften	Zusätzliche Konfigurationsoptionen für Ihre Inhalte in Ihrer Datenquelle. Dient zum Ein- oder Ausschließen bestimmter Inhalte in Ihrer Datenbankdatenquelle.
Primärschlüssel	Geben Sie den Primärschlüssel für die Datenbanktabelle an. Dies identifiziert eine Tabelle in Ihrer Datenbank.
Titel/Spalte	Geben Sie den Namen der Titelspalte des Dokuments in Ihrer Datenbanktabelle ein.
BodyColumn	Geben Sie den Namen der Titelspalte des Dokuments in Ihrer Datenbanktabelle ein.
sqlQuery	Geben Sie SQL-Abfrageanweisungen wie SELECT- und JOIN-Operationen ein. SQL-Abfragen müssen weniger als 32 KB groß sein. Amazon Kendra durchsucht den gesamten Datenbankinhalt, der Ihrer Abfrage entspricht.

Konfiguration	Beschreibung
Spalte „Zeitstempel“	Geben Sie den Namen der Spalte ein, die Zeitstempel enthält. Amazon Kendra verwendet Zeitstempelinformationen, um Änderungen an Ihrem Inhalt zu erkennen und nur geänderte Inhalte zu synchronisieren.
Zeitstempelformat	Geben Sie den Namen der Spalte ein, die Zeitstempelformate enthält, anhand derer Inhaltsänderungen erkannt und Ihre Inhalte erneut synchronisiert werden sollen.
Zeitzone	Geben Sie den Namen der Spalte ein, die Zeitzonen für den Inhalt enthält, der gecrawlt werden soll.
changeDetectingColumns	Geben Sie die Namen der Spalten ein, anhand derer Inhaltsänderungen erkannt Amazon Kendra werden sollen. Amazon Kendra indexiert den Inhalt neu, wenn sich eine dieser Spalten ändert
allowedUsersColumns	Geben Sie den Namen der Spalte ein, die Benutzer-IDs enthält, um Zugriff auf Inhalte zu erhalten.
allowedGroupsColumn	Geben Sie den Namen der Spalte ein, die Benutzer-IDs enthält, denen der Zugriff auf Inhalte gewährt werden soll.
Quelle-URI-Spalte	Geben Sie den Namen der Spalte ein, die Quell-URLs enthält, die indexiert werden sollen.

Konfiguration	Beschreibung
isSslEnabled	Geben Sie SQL-Abfrageanweisungen wie SELECT- und JOIN-Operationen ein. SQL-Abfragen müssen weniger als 32 KB groß sein. Amazon Kendra durchsucht den gesamten Datenbankinhalt, der Ihrer Abfrage entspricht.
Typ	Der Typ der Datenquelle. Geben Sie `JDBC` als Datenquellentyp an.
Sync-Modus	Geben Sie an, wie Ihr Index aktualisiert Amazon Kendra werden soll, wenn sich der Inhalt Ihrer Datenquelle ändert. Sie können wählen zwischen: • `FORCED_FULL_CRAWL` um den gesamten Inhalt neu zu indizieren und vorhandene Inhalte jedes Mal zu ersetzen, wenn Ihre Datenquelle mit Ihrem Index synchronisiert wird. • `FULL_CRAWL` um bei jeder Synchronisierung Ihrer Datenquelle mit Ihrem Index nur neue, geänderte und gelöschte Inhalte zu indiziere n. Amazon Kendra kann den Mechanismus Ihrer Datenquelle verwenden, um Inhaltsän derungen nachzuverfolgen und Inhalte zu indexieren, die sich seit der letzten Synchroni sierung geändert haben. • `CHANGE_LOG` um bei jeder Synchroni sierung Ihrer Datenquelle mit Ihrem Index nur neue und geänderte Inhalte zu indiziere n. Amazon Kendra kann den Mechanismus Ihrer Datenquelle verwenden, um Inhaltsän derungen nachzuverfolgen und Inhalte zu indexieren, die sich seit der letzten Synchroni sierung geändert haben.

Konfiguration	Beschreibung
SecreN	Der Amazon-Ressourcenname (ARN) eines Secrets Manager Manager-Geheimnisses, das den Benutzernamen und das Passwort enthält, die für die Verbindung mit Ihrer Datenbank erforderlich sind. Das Geheimnis muss eine JSON-Struktur mit den folgenden Schlüsseln enthalten: `{ "user name": "database user name", "password": " password" }`
version	Die Version der Vorlage, die derzeit unterstützt wird.

JSON-Schema der Oracle-Datenbank

```
{
  "$schema": "http://json-schema.org/draft-04/schema#",
  "type": "object",
  "properties": {
    "connectionConfiguration": {
      "type": "object",
      "properties": {
        "repositoryEndpointMetadata": {
          "type": "object",
          "properties": {
            "dbType": {
              "type": "string",
              "enum": [
                "mysql",
                "db2",
                "postgresql",
                "oracle",
                "sqlserver"
              ]
            },
```

```
            "dbHost": {
              "type": "string"
            },
            "dbPort": {
              "type": "string"
            },
            "dbInstance": {
              "type": "string"
            }
          },
          "required": [
            "dbType",
            "dbHost",
            "dbPort",
            "dbInstance"
          ]
        }
      },
      "required": [
        "repositoryEndpointMetadata"
      ]
    },
    "repositoryConfigurations": {
      "type": "object",
      "properties": {
        "document": {
          "type": "object",
          "properties": {
            "fieldMappings": {
              "type": "array",
              "items": [
                {
                  "type": "object",
                  "properties": {
                    "indexFieldName": {
                      "type": "string"
                    },
                    "indexFieldType": {
                      "type": "string"
                    },
                    "dataSourceFieldName": {
                      "type": "string"
                    }
                  },
```

```
                "required": [
                  "indexFieldName",
                  "indexFieldType",
                  "dataSourceFieldName"
                ]
              }
            ]
          }
        },
        "required": [
          "fieldMappings"
        ]
      }
    },
    "required": [
    ]
  },
  "additionalProperties": {
    "type": "object",
    "properties": {
      "primaryKey": {
        "type": "string"
      },
      "titleColumn": {
        "type": "string"
      },
      "bodyColumn": {
        "type": "string"
      },
      "sqlQuery": {
        "type": "string",
        "not": {
          "pattern": ";+"
        }
      },
      "timestampColumn": {
        "type": "string"
      },
      "timestampFormat": {
        "type": "string"
      },
      "timezone": {
        "type": "string"
      },
```

```
        "changeDetectingColumns": {
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "allowedUsersColumn": {
          "type": "string"
        },
        "allowedGroupsColumn": {
          "type": "string"
        },
        "sourceURIColumn": {
          "type": "string"
        },
        "isSslEnabled": {
          "type": "boolean"
        }
      },
      "required": ["primaryKey", "titleColumn", "bodyColumn", "sqlQuery"]
    },
    "type" : {
      "type" : "string",
      "pattern": "JDBC"
    },
    "syncMode": {
      "type": "string",
      "enum": [
        "FORCED_FULL_CRAWL",
        "FULL_CRAWL",
        "CHANGE_LOG"
      ]
    },
    "secretArn": {
      "type": "string"
    }
  },
  "version": {
    "type": "string",
    "anyOf": [
      {
        "pattern": "1.0.0"
      }
    ]
```

```
  },
  "required": [
      "connectionConfiguration",
      "repositoryConfigurations",
      "syncMode",
      "additionalProperties",
      "secretArn",
      "type"
  ]
}
```

PostgreSQL-Vorlagenschema

Sie fügen eine JSON-Datei ein, die das Datenquellenschema als Teil des TemplateConfigurationObjekts enthält. Geben Sie den Typ der Datenquelle als`JDBC`, den Datenbanktyp als`postgresql`, ein Geheimnis für Ihre Authentifizierungsdaten und andere erforderliche Konfigurationen an. Geben Sie dann `TEMPLATE` an`Type`, wann Sie anrufen CreateDataSource.

Sie können die in diesem Entwicklerhandbuch enthaltene Vorlage verwenden. Siehe PostgreSQL JSON-Schema.

In der folgenden Tabelle werden die Parameter des PostgreSQL-JSON-Schemas beschrieben.

Konfiguration	Beschreibung
Verbindung/Konfiguration	Konfigurationsinformationen für den Endpunkt für die Datenquelle.
repositoryEndpointMetadata	Erforderliche Konfigurationsinformationen für die Verbindung Ihrer Datenquelle. • dbType — Der Typ der Java-Date nbank, die Sie verwenden, unabhängig davon`mysql`,`db2`, `postgresql oracle`, oder. `sqlserver` • DBHost — Der Datenbank-Hostname. • DBPort — Der Datenbankport. • dbInstance — Die Datenbankinstanz.

Konfiguration	Beschreibung
Repository-Konfigurationen	Konfigurationsinformationen für den Inhalt der Datenquelle. Beispielsweise die Konfiguration bestimmter Inhaltstypen und Feldzuordnungen. Geben Sie den Typ der Datenquelle und den geheimen ARN an.
document	Eine Liste von Objekten, die die Attribute oder Feldnamen Ihres Datenbankinhalts Amazon Kendra Indexfeldnamen zuordnen. Weitere Informationen finden Sie unter Zuweisen von Datenquellenfeldern.
Zusätzliche Eigenschaften	Zusätzliche Konfigurationsoptionen für Ihre Inhalte in Ihrer Datenquelle. Dient zum Ein- oder Ausschließen bestimmter Inhalte in Ihrer Datenbankdatenquelle.
Primärschlüssel	Geben Sie den Primärschlüssel für die Datenbanktabelle an. Dies identifiziert eine Tabelle in Ihrer Datenbank.
Titel/Spalte	Geben Sie den Namen der Titelspalte des Dokuments in Ihrer Datenbanktabelle ein.
BodyColumn	Geben Sie den Namen der Titelspalte des Dokuments in Ihrer Datenbanktabelle ein.
sqlQuery	Geben Sie SQL-Abfrageanweisungen wie SELECT- und JOIN-Operationen ein. SQL-Abfragen müssen weniger als 32 KB groß sein. Amazon Kendra durchsucht den gesamten Datenbankinhalt, der Ihrer Abfrage entspricht.

Konfiguration	Beschreibung
Spalte „Zeitstempel“	Geben Sie den Namen der Spalte ein, die Zeitstempel enthält. Amazon Kendra verwendet Zeitstempelinformationen, um Änderungen an Ihrem Inhalt zu erkennen und nur geänderte Inhalte zu synchronisieren.
Zeitstempelformat	Geben Sie den Namen der Spalte ein, die Zeitstempelformate enthält, anhand derer Inhaltsänderungen erkannt und Ihre Inhalte erneut synchronisiert werden sollen.
Zeitzone	Geben Sie den Namen der Spalte ein, die Zeitzonen für den Inhalt enthält, der gecrawlt werden soll.
changeDetectingColumns	Geben Sie die Namen der Spalten ein, anhand derer Inhaltsänderungen erkannt Amazon Kendra werden sollen. Amazon Kendra indexiert den Inhalt neu, wenn sich eine dieser Spalten ändert
allowedUsersColumns	Geben Sie den Namen der Spalte ein, die Benutzer-IDs enthält, um Zugriff auf Inhalte zu erhalten.
allowedGroupsColumn	Geben Sie den Namen der Spalte ein, die Benutzer-IDs enthält, denen der Zugriff auf Inhalte gewährt werden soll.
Quelle-URI-Spalte	Geben Sie den Namen der Spalte ein, die Quell-URLs enthält, die indexiert werden sollen.

Konfiguration	Beschreibung
isSslEnabled	Geben Sie SQL-Abfrageanweisungen wie SELECT- und JOIN-Operationen ein. SQL-Abfragen müssen weniger als 32 KB groß sein. Amazon Kendra durchsucht den gesamten Datenbankinhalt, der Ihrer Abfrage entspricht.
Typ	Der Typ der Datenquelle. Geben Sie `JDBC` als Datenquellentyp an.
Sync-Modus	Geben Sie an, wie Ihr Index aktualisiert Amazon Kendra werden soll, wenn sich der Inhalt Ihrer Datenquelle ändert. Sie können wählen zwischen: • `FORCED_FULL_CRAWL` um den gesamten Inhalt neu zu indizieren und vorhandene Inhalte jedes Mal zu ersetzen, wenn Ihre Datenquelle mit Ihrem Index synchronisiert wird. • `FULL_CRAWL` um bei jeder Synchronisierung Ihrer Datenquelle mit Ihrem Index nur neue, geänderte und gelöschte Inhalte zu indiziere n. Amazon Kendra kann den Mechanismus Ihrer Datenquelle verwenden, um Inhaltsän derungen nachzuverfolgen und Inhalte zu indexieren, die sich seit der letzten Synchroni sierung geändert haben. • `CHANGE_LOG` um bei jeder Synchroni sierung Ihrer Datenquelle mit Ihrem Index nur neue und geänderte Inhalte zu indiziere n. Amazon Kendra kann den Mechanismus Ihrer Datenquelle verwenden, um Inhaltsän derungen nachzuverfolgen und Inhalte zu indexieren, die sich seit der letzten Synchroni sierung geändert haben.

Konfiguration	Beschreibung
SecreN	Der Amazon-Ressourcenname (ARN) eines Secrets Manager Manager-Geheimnisses, das den Benutzernamen und das Passwort enthält, die für die Verbindung mit Ihrer Datenbank erforderlich sind. Das Geheimnis muss eine JSON-Struktur mit den folgenden Schlüsseln enthalten: `{ "user name": "database user name", "password": " password" }`
version	Die Version der Vorlage, die derzeit unterstützt wird.

PostgreSQL JSON-Schema

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

Salesforce-Vorlagenschema

Sie fügen eine JSON-Datei ein, die das Datenquellenschema als Teil des TemplateConfigurationObjekts enthält. Sie geben die Salesforce-Host-URL als Teil der Verbindungskonfiguration oder der Repository-Endpunktdetails an. Geben Sie außerdem den Typ der Datenquelle als `SALESFORCEV2` ein Geheimnis für Ihre Authentifizierungsdaten und andere erforderliche Konfigurationen an. Geben Sie dann `TEMPLATE` an`Type`, wann Sie anrufen CreateDataSource.

Sie können die in diesem Entwicklerhandbuch enthaltene Vorlage verwenden. Siehe Salesforce-JSON-Schema.

In der folgenden Tabelle werden die Parameter des Salesforce-JSON-Schemas beschrieben.

Konfiguration	Beschreibung
Verbindung/Konfiguration	Konfigurationsinformationen für den Endpunkt für die Datenquelle.
repositoryEndpointMetadata	Die Endpunktinformationen für die Datenquelle.
Host-URL	Die URL der Salesforce-Instanz, die indexiert werden soll.
Repository-Konfigurationen	Konfigurationsinformationen für den Inhalt der Datenquelle. Beispielsweise die Konfiguration bestimmter Inhaltstypen und Feldzuordnungen.
• Konto • contact	Eine Liste von Objekten, die die Attribute oder Feldnamen Ihrer Salesforce-Entitäten Amazon

Konfiguration	Beschreibung
• Kampagne • Fall • Produkt • lead • Vertrag • Partner • Profil • Idee • Preisbuch • Aufgabe • Lösung • attachment • user • document • Artikel zum Thema Wissen • Gruppe • Gelegenheit • schwatzen • Benutzerdefinierte Entität	Kendra Indexfeldnamen zuordnen. Weitere Informationen finden Sie unter Zuweisen von Datenquellenfeldern.

Konfiguration	Beschreibung
SecreN	Der Amazon-Ressourcenname (ARN) eines AWS Secrets Manager Geheimnisses, das die Schlüssel-Wert-Paare enthält, die für die Verbindung mit Ihrem Salesforce erforderlich sind. Das Geheimnis muss eine JSON-Struktur mit den folgenden Schlüsseln enthalten: `{ "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" }`
Zusätzliche Eigenschaften	Zusätzliche Konfigurationsoptionen für Ihre Inhalte in Ihrer Datenquelle

Konfiguration	Beschreibung
• AccountFilter • Kontaktfilter • Fallfilter • Kampagnenfilter • Vertragsfilter • Gruppenfilter • Lead-Filter • Produktfilter • Opportunitätsfilter • Partnerfilter • Preisbuchfilter • IdeaFilter • Profilfilter • Aufgabenfilter • Lösungsfilter • Benutzerfilter • Chatter-Filter • Dokumentfilter • knowledgeArticleFilter • Benutzerdefinierte Entitäten	Eine Sammlung von Zeichenfolgen, die angibt, welche Entitäten gefiltert werden sollen.

Konfiguration	Beschreibung
Einschlussmuster • inclusionDocumentFileTypePatterns • inclusionDocumentFileNamePatterns • inclusionAccountFileTypePatterns • inclusionCampaignFileTypePatterns • inclusionDocumentFileNamePatterns • inclusionCampaignFileNamePatterns • inclusionCaseFileTypePatterns • inclusionCaseFileNamePatterns • inclusionContactFileTypePatterns • inclusionContractFileNamePatterns • inclusionLeadFileTypePatterns • inclusionLeadFileNamePatterns • inclusionOpportunityFileTypePatterns • inclusionOpportunityFileNamePatterns • inclusionSolutionFileTypePatterns • inclusionSolutionFileNamePatterns • inclusionTaskFileTypePatterns • inclusionTaskFileNamePatterns • inclusionGroupFileTypePatterns • inclusionGroupFileNamePatterns • inclusionChatterFileTypePatterns • inclusionChatterFileNamePatterns • inclusionCustomEntityFileTypePatterns • inclusionCustomEntityFileNamePatterns	Eine Liste von Mustern für reguläre Ausdrücke , um bestimmte Dateien in Ihre Salesforce-Datenquelle aufzunehmen. Dateien, die dem Muster entsprechen, sind im Index enthalten . Dateien, die nicht dem Muster entsprech en, werden aus dem Index ausgeschlossen. Wenn eine Datei sowohl einem Ein- als auch einem Ausschlussmuster entspricht, hat das Ausschlussmuster Vorrang und die Datei ist nicht im Index enthalten.

Konfiguration	Beschreibung
Ausschlussmuster • exclusionDocumentFileTypePatterns • exclusionDocumentFileNamePatterns • exclusionAccountFileTypePatterns • exclusionCampaignFileTypePatterns • exclusionCampaignFileNamePatterns • exclusionCaseFileTypePatterns • exclusionCaseFileNamePatterns • exclusionContactFileTypePatterns • exclusionContractFileNamePatterns • exclusionLeadFileTypePatterns • exclusionLeadFileNamePatterns • exclusionOpportunityFileTypePatterns • exclusionOpportunityFileNamePatterns • exclusionSolutionFileTypePatterns • exclusionSolutionFileNamePatterns • exclusionTaskFileTypePatterns • exclusionTaskFileNamePatterns • exclusionGroupFileTypePatterns • exclusionGroupFileNamePatterns • exclusionChatterFileTypePatterns • exclusionChatterFileNamePatterns • exclusionCustomEntityFileTypePatterns • exclusionCustomEntityFileNamePatterns	Eine Liste von Mustern mit regulären Ausdrücken, um bestimmte Dateien in Ihrer Salesforce-Datenquelle auszuschließen. Dateien, die dem Muster entsprechen, werden aus dem Index ausgeschlossen. Dateien, die den Mustern nicht entsprechen, werden in den Index aufgenommen. Wenn eine Datei sowohl einem Ausschluss- als auch einem Einschlus smuster entspricht, hat das Ausschlussmuster Vorrang und die Datei wird nicht in den Index aufgenommen.

Konfiguration	Beschreibung
• isCrawlAccount • isCrawlContact • isCrawlCase • isCrawlCampaign • isCrawlProduct • isCrawlLead • isCrawlContract • isCrawlPartner • isCrawlProfile • isCrawlIdea • isCrawlPricebook • isCrawlDocument • crawlSharedDocument • isCrawlGroup • isCrawlOpportunity • isCrawlChatter • isCrawlUser • isCrawlSolution • isCrawlTask • isCrawlAccountAnlagen • isCrawlContactAnlagen • isCrawlCaseAnlagen • isCrawlCampaignAnlagen • isCrawlLeadAnlagen • isCrawlContractAnlagen • isCrawlGroupAnlagen • isCrawlOpportunityAnlagen • isCrawlChatterAnlagen • isCrawlSolutionAnlagen	`true`um diese Arten von Dateien in Ihrem Salesforce-Konto zu crawlen.

Konfiguration	Beschreibung

• isCrawlTaskAnlagen
• isCrawlCustomEntityAttachments
• isCrawlKnowledgeArtikel
  • isCrawlDraft
  • isCrawlPublish
  • isCrawlArchived	

Typ	Der Typ der Datenquelle. Geben Sie `SALESFORCEV2` als Datenquellentyp an.
enableIdentityCrawler	`true`um den Identity Crawler zu verwenden, um Amazon Kendra Identitäts- und Hauptinformationen von Benutzern und Gruppen zu synchronisieren, die Zugriff auf bestimmte Dokumente haben. Wenn Identity Crawler ausgeschaltet ist, können alle Dokumente öffentlich durchsucht werden. Wenn Sie die Zugriffskontrolle für Ihre Dokumente verwenden möchten und Identity Crawler ausgeschaltet ist, können Sie alternativ die PutPrincipalMappingAPI verwenden, um Benutzer- und Gruppenzugriffsinformationen hochzuladen.

Konfiguration	Beschreibung
SyncMode	Geben Sie an, wie Ihr Index aktualisiert Amazon Kendra werden soll, wenn sich der Inhalt Ihrer Datenquelle ändert. Sie können wählen zwischen: • `FORCED_FULL_CRAWL` um den gesamten Inhalt neu zu indizieren und vorhandene Inhalte jedes Mal zu ersetzen, wenn Ihre Datenquelle mit Ihrem Index synchronisiert wird. • `FULL_CRAWL` um bei jeder Synchronisierung Ihrer Datenquelle mit Ihrem Index nur neue, geänderte und gelöschte Inhalte zu indiziere n. Amazon Kendra kann den Mechanismus Ihrer Datenquelle verwenden, um Inhaltsän derungen nachzuverfolgen und Inhalte zu indexieren, die sich seit der letzten Synchroni sierung geändert haben. • `CHANGE_LOG` um jedes Mal, wenn Ihre Datenquelle mit Ihrem Index synchroni siert wird, nur neue und geänderte Inhalte zu indizieren. Amazon Kendra kann den Mechanismus Ihrer Datenquelle verwenden, um Inhaltsänderungen nachzuverfolgen und Inhalte zu indexieren, die sich seit der letzten Synchronisierung geändert haben.
version	Die Version dieser Vorlage, die derzeit unterstützt wird.

Salesforce-JSON-Schema

```
{
  "$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 Vorlagenschema

Sie fügen eine JSON-Datei ein, die das Datenquellenschema als Teil des TemplateConfigurationObjekts enthält. Sie geben die ServiceNow Host-URL, den Authentifizierungstyp und die Instanzversion als Teil der Verbindungskonfiguration oder der Repository-Endpunktdetails an. Geben Sie außerdem den Typ der Datenquelle als`SERVICENOWV2`, ein Geheimnis für Ihre Authentifizierungsdaten und andere erforderliche Konfigurationen an. Geben Sie dann `TEMPLATE` an`Type`, wann Sie anrufen CreateDataSource.

Sie können die in diesem Entwicklerhandbuch enthaltene Vorlage verwenden. Siehe ServiceNow JSON-Schema.

In der folgenden Tabelle werden die Parameter des ServiceNow JSON-Schemas beschrieben.

Konfiguration	Beschreibung
Verbindung/Konfiguration	Konfigurationsinformationen für den Endpunkt für die Datenquelle.
repositoryEndpointMetadata	Die Endpunktinformationen für die Datenquelle.
Host-URL	Die ServiceNow Host-URL. Zum Beispiel *`your-domain.service-now.com`* .
authType	Die Art der Authentifizierung, die Sie verwenden, ob oder. `basicAuth` `OAuth2`
servicenowInstanceVersion	Die ServiceNow Version, die Sie verwenden. Sie können zwischen`Tokyo`, `SandiegoRome`, und wählen`Others`.

Konfiguration	Beschreibung
Repository-Konfigurationen	Konfigurationsinformationen für den Inhalt der Datenquelle. Beispielsweise die Konfiguration bestimmter Inhaltstypen und Feldzuordnungen.
• Artikel zum Thema Wissen • attachment • Servicekatalog • Vorfall	Eine Liste von Objekten, die die Attribute oder Feldnamen Ihrer ServiceNow Wissensartikel, Anlagen, Servicekataloge und Vorfälle den Amazon Kendra Indexfeldnamen zuordnen. Weitere Informationen finden Sie unter Zuweisen von Datenquellenfeldern. Die Feldnamen der ServiceNow Datenquellen müssen in Ihren ServiceNow benutzerdefinierten Metadaten vorhanden sein.
zusätzliche Eigenschaften	Zusätzliche Konfigurationsoptionen für Ihre Inhalte in Ihrer Datenquelle.
maxFileSizeInMegaBytes	Geben Sie die Dateigrößenbeschränkung in MB an, die Amazon Kendra crawlt. Amazon Kendra crawlt nur die Dateien innerhalb der von Ihnen definierten Größenbeschränkung. Die Standarddateigröße ist 50 MB. Die maximale Dateigröße sollte größer als 0 MB und kleiner oder gleich 50 MB sein.

Konfiguration	Beschreibung
• knowledgeArticleFilter • incidentQueryFilter • serviceCatalogQueryFiltern • knowledgeArticleTitleRegExp • serviceCatalogTitleRegExp • incidentTitleRegExp • inclusionFileTypeMuster • exclusionFileTypeMuster • inclusionFileNameMuster • exclusionFileNameMuster • incidentStateType	Eine Liste von Mustern für reguläre Ausdrücke, mit denen Sie bestimmte Dateien in Ihre ServiceNow Datenquelle ein- und/oder ausschließen können. Dateien, die dem Muster entsprechen, sind im Index enthalten. Dateien, die nicht dem Muster entsprechen, werden aus dem Index ausgeschlossen. Wenn eine Datei sowohl einem Ein- als auch einem Ausschlus smuster entspricht, hat das Ausschlussmuster Vorrang und die Datei ist nicht im Index enthalten.
• isCrawlKnowledgeArtikel • isCrawlKnowledgeArticleAttachment • includePublicArticlesNur • isCrawlServiceKatalog • isCrawlServiceCatalogAttachment • isCrawlActiveServiceCatalog • isCrawlInactiveServiceCatalog • isCrawlIncident • isCrawlIncidentAnlage • isCrawlActiveVorfall • isCrawlInactiveVorfall • ACL anwenden ForKnowledgeArticl e • ACL anwenden ForServiceCatalog • ACL anwenden ForIncident	`true`um ServiceNow Wissensartikel, Servicekataloge, Vorfälle und Anlagen zu crawlen.
Typ	Der Typ der Datenquelle. Geben Sie `SERVICENOWV2` als Datenquellentyp an.

Konfiguration	Beschreibung
enableIdentityCrawler	`true`um den Identity Crawler zu verwenden, um Amazon Kendra Identitäts- und Hauptinformationen von Benutzern und Gruppen zu synchronisieren, die Zugriff auf bestimmte Dokumente haben. Wenn Identity Crawler ausgeschaltet ist, können alle Dokumente öffentlich durchsucht werden. Wenn Sie die Zugriffskontrolle für Ihre Dokumente verwenden möchten und Identity Crawler ausgeschaltet ist, können Sie alternativ die PutPrincipalMappingAPI verwenden, um Benutzer- und Gruppenzugriffsinformationen hochzuladen.
SyncMode	Geben Sie an, wie Ihr Index aktualisiert Amazon Kendra werden soll, wenn sich der Inhalt Ihrer Datenquelle ändert. Sie können wählen zwischen: • `FORCED_FULL_CRAWL` um den gesamten Inhalt neu zu indizieren und vorhandene Inhalte jedes Mal zu ersetzen, wenn Ihre Datenquelle mit Ihrem Index synchronisiert wird. • `FULL_CRAWL` um bei jeder Synchronisierung Ihrer Datenquelle mit Ihrem Index nur neue, geänderte und gelöschte Inhalte zu indizieren. Amazon Kendra kann den Mechanismus Ihrer Datenquelle verwenden, um Inhaltsänderungen nachzuverfolgen und Inhalte zu indexieren, die sich seit der letzten Synchronisierung geändert haben.

Konfiguration	Beschreibung

SecreN	Der Amazon-Ressourcenname (ARN) eines AWS Secrets Manager Geheimnisses, das die Schlüssel-Wert-Paare enthält, die für die Verbindung mit Ihrem erforderlich sind. ServiceNow Das Geheimnis muss eine JSON-Struktur mit den folgenden Schlüsseln enthalten:
	`{ "username": " user name", "password": " password" }`
	Wenn Sie die OAuth2-Authentifizierung verwenden, muss Ihr Secret eine JSON-Struktur mit den folgenden Schlüsseln enthalten:
	`{ "username": " user name", "password": " password", "clientId": " client id", "clientSecret": " client secret" }`

version	Die Version der Vorlage, die derzeit unterstützt wird.

ServiceNow JSON-Schema

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

Slack-Vorlagenschema

Du fügst eine JSON-Datei ein, die das Datenquellenschema als Teil des TemplateConfigurationObjekts enthält. Sie geben die Host-URL als Teil der Verbindungskonfiguration

oder der Repository-Endpunktdetails an. Geben Sie außerdem den Typ der DatenquelleSLACK, ein Geheimnis für Ihre Authentifizierungsdaten und andere erforderliche Konfigurationen an. Geben Sie dann TEMPLATE anType, wann Sie anrufen CreateDataSource.

Sie können die in diesem Entwicklerhandbuch enthaltene Vorlage verwenden. Siehe JSON-Schema von Slack.

In der folgenden Tabelle werden die Parameter des JSON-Schemas von Slack beschrieben.

Konfiguration	Beschreibung
Verbindung/Konfiguration	Konfigurationsinformationen für den Endpunkt für die Datenquelle.
repositoryEndpointMetadata	Die Endpunktinformationen für die Datenquelle.
TeamID	Die Slack-Team-ID, die du von der URL deiner Slack-Hauptseite kopiert hast.
Repository-Konfigurationen	Konfigurationsinformationen für den Inhalt der Datenquelle. Beispielsweise die Konfiguration bestimmter Inhaltstypen und Feldzuordnungen.
Alle	Eine Liste von Objekten, die die Attribute oder Feldnamen Ihres Slack Inhalts Amazon Kendra Indexfeldnamen zuordnen.
Zusätzliche Eigenschaften	Zusätzliche Konfigurationsoptionen für Ihre Inhalte in Ihrer Datenquelle.
Inklusionsmuster	Eine Liste von Mustern für reguläre Ausdrücke , um bestimmte Inhalte in Ihre Slack Datenquel le aufzunehmen. Elemente, die den Mustern entsprechen, sind im Index enthalten. Inhalte, die den Mustern nicht entsprechen, werden aus dem Index ausgeschlossen. Wenn ein Inhalt sowohl einem Einschluss- als auch einem Ausschlussmuster entspricht, hat das

Konfiguration	Beschreibung
	Ausschlussmuster Vorrang, und der Inhalt wird nicht in den Index aufgenommen.
Ausschlussmuster	Eine Liste von Mustern für reguläre Ausdrücke , um bestimmte Inhalte in Ihrer Slack Datenquelle auszuschließen. Inhalte, die den Mustern entsprechen, werden aus dem Index ausgeschlossen. Inhalte, die den Mustern nicht entsprechen, werden in den Index aufgenommen. Wenn Inhalte sowohl einem Inklusions- als auch einem Ausschlussmuster entsprechen, hat das Ausschlussmuster Vorrang, und der Inhalt wird nicht in den Index aufgenommen.
crawlBotMessages	`true`um Bot-Nachrichten zu crawlen.
Archivierte ausschließen	`true`um das Crawlen archivierter Nachrichten auszuschließen.
Art der Konversation	Die Art der Konversation, die Sie indizieren möchten`PUBLIC_CHANNEL` , ob`PRIVATE_CHANNEL` , `GROUP_MESSAGE` und. `DIRECT_MESSAGE`
ChannelFilter	Der Kanaltyp, den Sie indizieren möchten, ob oder`private_channel` . `public_channel`
SinceDate	Sie können einen `sinceDate` Parameter so konfigurieren, dass der Slack Connector Inhalte basierend auf einem bestimmten Wert crawlt. `sinceDate`

Konfiguration	Beschreibung
LookBack	Sie können einen `lookBack` Parameter so konfigurieren, dass der Slack Connector aktualisierte oder gelöschte Inhalte bis zu einer bestimmten Anzahl von Stunden vor Ihrer letzten Connector-Synchronisierung crawlt.
Synchronisierungsmodus	Geben Sie an, wie Ihr Index aktualisiert Amazon Kendra werden soll, wenn sich der Inhalt Ihrer Datenquelle ändert. Sie können wählen zwischen: • `FORCED_FULL_CRAWL` um den gesamten Inhalt neu zu indizieren und vorhandene Inhalte jedes Mal zu ersetzen, wenn Ihre Datenquelle mit Ihrem Index synchronisiert wird. • `FULL_CRAWL` um bei jeder Synchronisierung Ihrer Datenquelle mit Ihrem Index nur neue, geänderte und gelöschte Inhalte zu indiziere n. Amazon Kendra kann den Mechanismus Ihrer Datenquelle verwenden, um Inhaltsän derungen nachzuverfolgen und Inhalte zu indexieren, die sich seit der letzten Synchroni sierung geändert haben. • `CHANGE_LOG` um jedes Mal, wenn Ihre Datenquelle mit Ihrem Index synchroni siert wird, nur neue und geänderte Inhalte zu indizieren. Amazon Kendra kann den Mechanismus Ihrer Datenquelle verwenden, um Inhaltsänderungen nachzuverfolgen und Inhalte zu indexieren, die sich seit der letzten Synchronisierung geändert haben.
Typ	Der Typ der Datenquelle. Geben Sie `SLACK` als Datenquellentyp an.

Konfiguration	Beschreibung
enableIdentityCrawler	`true`um den Identity Crawler zu verwenden, um Amazon Kendra Identitäts- und Hauptinfo rmationen von Benutzern und Gruppen zu synchronisieren, die Zugriff auf bestimmte Dokumente haben. Wenn Identity Crawler ausgeschaltet ist, können alle Dokumente öffentlich durchsucht werden. Wenn Sie die Zugriffskontrolle für Ihre Dokumente verwenden möchten und Identity Crawler ausgeschaltet ist, können Sie alternativ die PutPrincipalMappin gAPI verwenden, um Benutzer- und Gruppenzu griffsinformationen hochzuladen.
SecreN	Der Amazon-Ressourcenname (ARN) eines AWS Secrets Manager Geheimnisses, das die Schlüssel-Wert-Paare enthält, die für die Verbindung mit Ihrem erforderlich sind. Slack Das Geheimnis muss eine JSON-Struktur mit den folgenden Schlüsseln enthalten: `{ "slackToken": " token" }`
version	Die Version dieser Vorlage, die derzeit unterstützt wird.

JSON-Schema von 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"
  ]
}
```

Zendesk-Vorlagenschema

Sie fügen eine JSON-Datei hinzu, die das Datenquellenschema als Teil des TemplateConfigurationObjekts enthält. Sie geben die Host-URL als Teil der Verbindungskonfiguration oder der Repository-Endpunktdetails an. Geben Sie außerdem den Typ der Datenquelle`ZENDESK`,

ein Geheimnis für Ihre Authentifizierungsdaten und andere erforderliche Konfigurationen an. Geben Sie dann `TEMPLATE` an`Type`, wann Sie anrufen CreateDataSource.

Sie können die in diesem Entwicklerhandbuch enthaltene Vorlage verwenden. Siehe Zendesk-JSON-Schema.

In der folgenden Tabelle werden die Parameter des Zendesk-JSON-Schemas beschrieben.

Konfiguration	Beschreibung
Verbindung/Konfiguration	Konfigurationsinformationen für den Endpunkt für die Datenquelle.
repositoryEndpointMetadata	Die Endpunktinformationen für die Datenquelle.
Host-URL	Die Zendesk-Host-URL. Zum Beispiel https://yoursubdomain.zendesk.com.
Repository-Konfigurationen	Konfigurationsinformationen für den Inhalt der Datenquelle. Beispielsweise die Konfiguration bestimmter Inhaltstypen und Feldzuordnungen.
• Fahrkarte • Ticket/Kommentar • ticketCommentAttachment • article • Kommentar zum Artikel • Anlage zum Artikel • Community-Thema • communityPostComment	Eine Liste von Objekten, die Attribute oder Feldnamen von Zendesk-Tickets den Indexfeld namen von Amazon Kendra zuordnen. Weitere Informationen finden Sie unter Zuweisen von Datenquellenfeldern.
Sekretär N	Der Amazon-Ressourcenname (ARN) eines AWS Secrets Manager Geheimnisses, das die Schlüssel-Wert-Paare enthält, die für die Verbindung mit Ihrem Zendesk erforderlich sind. Das Geheimnis muss eine JSON-Struktur mit den folgenden Schlüsseln enthalten: Host-

Konfiguration	Beschreibung
	URL, Client-ID, Client-Geheimnis, Benutzern ame und Passwort.
Zusätzliche Eigenschaften	Zusätzliche Konfigurationsoptionen für Ihre Inhalte in Ihrer Datenquelle
organizationNameFilter	Sie können sich dafür entscheiden, Tickets zu indexieren, die innerhalb einer bestimmten Organisation existieren.
Seit Datum	Sie können einen `sinceDate` Parameter so konfigurieren, dass der Zendesk-Connector Inhalte anhand eines bestimmten Inhalts crawlt. `sinceDate`
Einschlussmuster	Eine Liste von Mustern für reguläre Ausdrücke , um bestimmte Dateien in Ihre Zendesk-D atenquelle aufzunehmen. Dateien, die dem Muster entsprechen, sind im Index enthalten . Dateien, die nicht dem Muster entsprechen, werden aus dem Index ausgeschlossen. Wenn eine Datei sowohl einem Einschluss- als auch einem Ausschlussmuster entspricht, hat das Ausschlussmuster Vorrang und die Datei wird nicht in den Index aufgenommen.

Konfiguration	Beschreibung
Ausschlussmuster	Eine Liste mit Mustern für reguläre Ausdrücke , mit denen Sie bestimmte Dateien in Ihrer Zendesk-Datenquelle ausschließen können. Dateien, die dem Muster entsprechen, werden aus dem Index ausgeschlossen. Dateien, die den Mustern nicht entsprechen, werden in den Index aufgenommen. Wenn eine Datei sowohl einem Ausschluss- als auch einem Einschlus smuster entspricht, hat das Ausschlussmuster Vorrang, und die Datei wird nicht in den Index aufgenommen.
• isCrawlTicket • isCrawlTicketKommentar • isCrawlTicketCommentAttachment • isCrawlArticle • isCrawlArticleKommentar • isCrawlArticleAnlage • isCrawlCommunityThema • isCrawlCommunityBeitrag • isCrawlCommunityPostComment	Geben Sie "`true`" ein, um diese Arten von Inhalten zu crawlen.
Typ	Geben Sie `ZENDESK` als Datenquellentyp an.
useChangeLog	Geben Sie "`true`" ein, um anhand des Zendesk-Änderungsprotokolls zu ermitteln, welche Dokumente im Index aktualisiert werden müssen. Je nach Größe des Änderungs protokolls ist es möglicherweise schneller, die Dokumente in Zendesk zu scannen. Wenn Sie Ihre Zendesk-Datenquelle zum ersten Mal mit Ihrem Index synchronisieren, werden alle Dokumente gescannt.

Zendesk-JSON-Schema

```
{
  "$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 Managerist ein Content-Management-System, das für die Erstellung von Inhalten für Websites oder mobile Apps verwendet wird. Sie können Amazon Kendra es verwenden, um eine Verbindung zu Ihren Seiten Adobe Experience Manager und Inhaltsressourcen herzustellen und diese zu indizieren.

Amazon Kendra unterstützt Adobe Experience Manager (AEM) als Cloud Service-Autoreninstanz und als Adobe Experience Manager On-Premise-Instanz zum Verfassen und Veröffentlichen.

Sie können über Amazon Kendra die Amazon Kendra Konsole oder die API eine Verbindung zu Ihrer Adobe Experience Manager Datenquelle herstellen. TemplateConfiguration

Informationen zur Fehlerbehebung bei Ihrem Amazon Kendra Adobe Experience Manager-Datenquellen-Connector finden Sie unterProblembehandlung bei Datenquellen.

Themen

Unterstützte Features

Adobe Experience ManagerDer Datenquellen-Connector unterstützt die folgenden Funktionen:

- Feldzuordnungen
- Filterung des Benutzerkontextes
- Einschluss-/Ausschlussfilter
- Vollständige und inkrementelle Inhaltssynchronisierung
- OAuth 2.0 und Standardauthentifizierung
- Virtual Private Cloud (VPC)

Voraussetzungen

Bevor Sie Ihre Adobe Experience Manager Datenquelle Amazon Kendra zum Indizieren verwenden können, nehmen Sie diese Änderungen in Ihren Konten Adobe Experience Manager und AWS Konten vor.

Stellen Sie sicherAdobe Experience Manager, dass Sie Folgendes haben:

- Zugriff auf ein Konto mit Administratorrechten oder auf einen Admin-Benutzer.
- Deine Adobe Experience Manager Host-URL wurde kopiert.

> **Note**
>
> (On-Premise/Server) Amazon Kendra überprüft, ob die in AWS Secrets Manager der Datei enthaltenen Endpunktinformationen mit den Endpunktinformationen übereinstimmen, die in den Konfigurationsdetails Ihrer Datenquelle angegeben sind. Dies trägt zum Schutz vor dem Problem des verwirrten Stellvertreters bei, bei dem es sich um ein Sicherheitsproblem handelt, bei dem ein Benutzer nicht berechtigt ist, eine Aktion auszuführen, sondern ihn Amazon Kendra als Proxy verwendet, um auf das konfigurierte Geheimnis zuzugreifen und

die Aktion auszuführen. Wenn Sie Ihre Endpunktinformationen später ändern, müssen Sie ein neues Geheimnis erstellen, um diese Informationen zu synchronisieren.

- Haben Sie sich Ihre grundlegenden Authentifizierungsdaten mit Admin-Benutzername und Passwort notiert.
- Optional: Generierte OAuth 2.0-Anmeldeinformationen in Adobe Experience Manager (AEM) als Cloud-Dienst oder AEM On-Premise. Wenn Sie AEM On-Premise verwenden, umfassen die Anmeldeinformationen die Client-ID, den geheimen Client-Schlüssel und den privaten Schlüssel. Wenn Sie AEM als Cloud-Dienst verwenden, umfassen die Anmeldeinformationen die Client-ID, den geheimen Client-Schlüssel, den privaten Schlüssel, die Organisations-ID, die technische Konto-ID und den Adobe Identity Management System (IMS-) Host. Weitere Informationen zum Generieren dieser Anmeldeinformationen für AEM as a Cloud Service finden Sie Adobe Experience Manager in der Dokumentation. Für AEM On-Premise bietet die Adobe Granite OAuth 2.0-Serverimplementierung (com.adobe.granite.oauth.server) die Unterstützung für OAuth 2.0-Serverfunktionen in AEM.
- Aktiviert, dass jedes Dokument in Adobe Experience Manager und in anderen Datenquellen, die Sie für denselben Index verwenden möchten, einzigartig ist. Jede Datenquelle, die Sie für einen Index verwenden möchten, darf nicht dasselbe Dokument in allen Datenquellen enthalten. Dokument-IDs gelten für einen Index global und müssen pro Index eindeutig sein.

Stellen Sie sicher AWS-Konto, dass Sie Folgendes in Ihrem haben:

- Hat einen Amazon Kendra Index erstellt und bei Verwendung der API die Index-ID notiert.
- Sie haben eine IAM Rolle für Ihre Datenquelle erstellt und, falls Sie die API verwenden, den ARN der IAM Rolle notiert.

> **Note**
>
> Wenn Sie Ihren Authentifizierungstyp und Ihre Anmeldeinformationen ändern, müssen Sie Ihre IAM Rolle aktualisieren, um auf die richtige AWS Secrets Manager geheime ID zugreifen zu können.

- Sie haben Ihre Adobe Experience Manager-Authentifizierungsdaten AWS Secrets Manager geheim gespeichert und, falls Sie die API verwenden, den ARN des Geheimnisses notiert.

> **Note**
>
> Wir empfehlen Ihnen, Ihre Anmeldeinformationen und Ihr Geheimnis regelmäßig zu aktualisieren oder zu wechseln. Stellen Sie zu Ihrer eigenen Sicherheit nur die Zugriffsebene bereit, die erforderlich ist. Wir raten davon ab, Anmeldeinformationen und geheime Daten für alle Datenquellen und Connector-Versionen 1.0 und 2.0 (sofern zutreffend) wiederzuverwenden.

Wenn Sie noch keine IAM Rolle oder keinen Schlüssel haben, können Sie die Konsole verwenden, um eine neue IAM Rolle und ein neues Secrets Manager Geheimnis zu erstellen, wenn Sie Ihre Adobe Experience Manager-Datenquelle mit verbinden. Amazon Kendra Wenn Sie die API verwenden, müssen Sie den ARN einer vorhandenen IAM Rolle und eines Secrets Manager Geheimnisses sowie eine Index-ID angeben.

Anweisungen zur Verbindung

Amazon Kendra Um eine Verbindung mit Ihrer Adobe Experience Manager Datenquelle herzustellen, müssen Sie die erforderlichen Details zu Ihrer Adobe Experience Manager Datenquelle angeben, damit Sie auf Ihre Daten zugreifen Amazon Kendra können. Falls Sie noch keine Konfiguration Adobe Experience Manager für vorgenommen haben Amazon Kendra, finden Sie weitere Informationen unterVoraussetzungen.

Console

Um eine Verbindung Amazon Kendra herzustellen Adobe Experience Manager

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die Amazon Kendra Konsole.
2. Wählen Sie im linken Navigationsbereich Indizes und dann den Index, den Sie verwenden möchten, aus der Indexliste aus.

   > **Note**
   >
   > Sie können Ihre Einstellungen für die Benutzerzugriffskontrolle unter Indexeinstellungen konfigurieren oder bearbeiten.

3. Wählen Sie auf der Seite Erste Schritte die Option Datenquelle hinzufügen aus.

4. Wählen Sie auf der Seite „Datenquelle hinzufügen“ die Option „Adobe Experience Manager-Connector“ und anschließend „Konnektor hinzufügen“.
5. Geben Sie auf der Seite „Datenquellendetails angeben“ die folgenden Informationen ein:

   a. Geben Sie im Feld Name und Beschreibung für Datenquellenname einen Namen für Ihre Datenquelle ein. Sie können Bindestriche, aber keine Leerzeichen verwenden.

   b. (Optional) Beschreibung — Geben Sie eine optionale Beschreibung für Ihre Datenquelle ein.

   c. In Standardsprache — Wählen Sie eine Sprache aus, um Ihre Dokumente nach dem Index zu filtern. Sofern Sie nichts anderes angeben, ist die Standardsprache Englisch. Die in den Metadaten des Dokuments angegebene Sprache hat Vorrang vor der ausgewählten Sprache.

   d. Unter Tags für Neues Tag hinzufügen — Fügen Sie optionale Tags hinzu, um Ihre Ressourcen zu durchsuchen und zu filtern oder Ihre Kosten nachzuverfolgen. AWS

   e. Wählen Sie Weiter aus.
6. Geben Sie auf der Seite Zugriff und Sicherheit definieren die folgenden Informationen ein:

   a. Quelle — Wählen Sie entweder AEM On-Premise oder AEM as a Cloud Service.

      Geben Sie Ihre Host-URL ein. Adobe Experience Manager Wenn Sie beispielsweise AEM On-Premise verwenden, geben Sie den Hostnamen und den Port an:. https://hostname:port Oder, wenn Sie AEM als Cloud-Service verwenden, können Sie die URL des Autors verwenden:. https://author-xxxxxx-xxxxxxx.adobeaemcloud.com

   b. Speicherort des SSL-Zertifikats — Geben Sie den Pfad zu dem in einem Bucket gespeicherten SSL-Zertifikat ein Amazon S3 . Sie verwenden dies, um über eine sichere SSL-Verbindung eine Verbindung zu AEM On-Premise herzustellen.

   c. Autorisierung — Aktivieren oder deaktivieren Sie die Informationen der Zugriffskontrollliste (ACL) für Ihre Dokumente, wenn Sie über eine ACL verfügen und diese für die Zugriffskontrolle verwenden möchten. Die ACL gibt an, auf welche Dokumente Benutzer und Gruppen zugreifen können. Die ACL-Informationen werden verwendet, um Suchergebnisse nach dem Benutzer- oder Gruppenzugriff auf Dokumente zu filtern. Weitere Informationen finden Sie unter Benutzerkontextfilterung.

   d. Authentifizierung — Wählen Sie Standardauthentifizierung oder OAuth 2.0-Authentifizierung. Wählen Sie dann ein vorhandenes AWS Secrets Manager Geheimnis aus oder erstellen Sie ein neues Geheimnis, um Ihre Anmeldeinformationen zu

speichern. Adobe Experience Manager Wenn Sie sich dafür entscheiden, ein neues Geheimnis zu erstellen, wird ein AWS Secrets Manager geheimes Fenster geöffnet.

Wenn Sie sich für die Standardauthentifizierung entschieden haben, geben Sie einen Namen für das Geheimnis, den Adobe Experience Manager Site-Benutzernamen und das Passwort ein. Der Benutzer muss über Administratorrechte verfügen oder ein Admin-Benutzer sein.

Wenn Sie sich für die OAuth 2.0-Authentifizierung entschieden haben und AEM On-Premise verwenden, geben Sie einen Namen für das Geheimnis, die Client-ID, den geheimen Client-Schlüssel und den privaten Schlüssel ein. Wenn Sie AEM als Cloud-Dienst verwenden, geben Sie einen Namen für das Geheimnis, die Client-ID, den geheimen Client-Schlüssel, den privaten Schlüssel, die Organisations-ID, die technische Konto-ID und den (IMS-Adobe Identity Management System) Host ein.

Wählen Sie Speichern.

e. Virtual Private Cloud (VPC) — Sie können wählen, ob Sie eine VPC verwenden möchten. In diesem Fall müssen Sie Subnetze und VPC-Sicherheitsgruppen hinzufügen.

f. Identity Crawler — Geben Sie an, ob der Identity Crawler aktiviert Amazon Kendra werden soll. Der Identity Crawler verwendet die Informationen der Zugriffskontrollliste (ACL) für Ihre Dokumente, um Suchergebnisse nach dem Benutzer- oder Gruppenzugriff auf Dokumente zu filtern. Wenn Sie über eine ACL für Ihre Dokumente verfügen und Ihre ACL verwenden möchten, können Sie auch den Identity Crawler aktivieren, um die Benutzerkontextfilterung der Suchergebnisse zu konfigurieren. Amazon Kendra Andernfalls können alle Dokumente öffentlich durchsucht werden, wenn Identity Crawler ausgeschaltet ist. Wenn Sie die Zugriffskontrolle für Ihre Dokumente verwenden möchten und Identity Crawler ausgeschaltet ist, können Sie alternativ die PutPrincipalMappingAPI verwenden, um Benutzer- und Gruppenzugriffsinformationen für die Benutzerkontextfilterung hochzuladen.

g. IAM Rolle — Wählen Sie eine bestehende IAM Rolle oder erstellen Sie eine neue IAM Rolle, um auf Ihre Repository-Anmeldeinformationen und Indexinhalte zuzugreifen.

> **Note**
>
> IAM Rollen, die für Indizes verwendet werden, können nicht für Datenquellen verwendet werden. Wenn Sie sich nicht sicher sind, ob eine vorhandene Rolle für

einen Index oder eine häufig gestellte Frage verwendet wird, wählen Sie Neue Rolle erstellen, um Fehler zu vermeiden.

h. Wählen Sie Weiter aus.

7. Geben Sie auf der Seite „Synchronisierungseinstellungen konfigurieren“ die folgenden Informationen ein:

   a. Synchronisierungsbereich — Legen Sie Grenzwerte für das Crawlen bestimmter Inhaltstypen, Seitenkomponenten und Stammpfade fest und filtern Sie Inhalte mithilfe von Regex-Ausdrucksmustern.

      i. Inhaltstypen — Wählen Sie aus, ob nur Seiten oder Assets oder beides gecrawlt werden sollen.

      ii. (Optional) Zusätzliche Konfiguration — Konfigurieren Sie die folgenden Einstellungen:

         - Seitenkomponenten — Die spezifischen Namen der Seitenkomponenten. Die Seitenkomponente ist eine erweiterbare Seitenkomponente, die für die Zusammenarbeit mit dem Adobe Experience Manager Vorlageneditor entwickelt wurde. Sie ermöglicht das Zusammenstellen von Kopf- und Fußzeilen sowie Strukturkomponenten von Seiten mit dem Vorlageneditor.
         - Inhaltsfragmentvariationen — Die spezifischen Namen der Inhaltsfragmentvarianten. Inhaltsfragmente ermöglichen es Ihnen, seitenunabhängige Inhalte in zu entwerfen, zu erstellen, zu kuratieren und zu veröffentlichen. Adobe Experience Manager Sie ermöglichen es Ihnen, Inhalte für die Verwendung an mehreren Orten/über mehrere Kanäle vorzubereiten.
         - Stammpfade — Die Stammpfade zu bestimmten Inhalten.
         - Regex-Muster — Die regulären Ausdrucksmuster zum Ein- oder Ausschließen bestimmter Seiten und Elemente.

   b. Synchronisierungsmodus — Wählen Sie aus, wie Sie Ihren Index aktualisieren möchten, wenn sich der Inhalt Ihrer Datenquelle ändert. Wenn Sie Ihre Datenquelle Amazon Kendra zum ersten Mal synchronisieren, werden alle Inhalte standardmäßig gecrawlt und indexiert. Sie müssen eine vollständige Synchronisierung Ihrer Daten durchführen, falls Ihre erste Synchronisierung fehlgeschlagen ist, auch wenn Sie die Option Vollsynchronisierung nicht als Synchronisierungsmodusoption wählen.

- Vollständige Synchronisierung: Indizieren Sie den gesamten Inhalt neu und ersetzen die vorhandenen Inhalte jedes Mal, wenn Ihre Datenquelle mit Ihrem Index synchronisiert wird.
- Neue, geänderte Synchronisierung: Indizieren Sie jedes Mal, wenn Ihre Datenquelle mit Ihrem Index synchronisiert wird, nur neue und geänderte Inhalte. Amazon Kendra kann den Mechanismus Ihrer Datenquelle verwenden, um Inhaltsänderungen nachzuverfolgen und Inhalte zu indexieren, die sich seit der letzten Synchronisierung geändert haben.
- Neue, geänderte, gelöschte Synchronisierung: Indizieren Sie bei jeder Synchronisierung Ihrer Datenquelle mit Ihrem Index nur neue, geänderte und gelöschte Inhalte. Amazon Kendra kann den Mechanismus Ihrer Datenquelle verwenden, um Inhaltsänderungen nachzuverfolgen und Inhalte zu indexieren, die sich seit der letzten Synchronisierung geändert haben.

c. Zeitzonen-ID — Wenn Sie AEM On-Premise verwenden und sich die Zeitzone Ihres Servers von der Zeitzone des Amazon Kendra AEM-Connectors oder -Indexes unterscheidet, können Sie die Serverzeitzone so angeben, dass sie mit dem AEM-Connector oder Index übereinstimmt. Die Standardzeitzone für AEM On-Premise ist die Zeitzone des AEM-Connectors oder -Indexes. Amazon Kendra Die Standardzeitzone für AEM as a Cloud Service ist Greenwich Mean Time.

d. Zeitplan für die Synchronisierungsausführung — Wählen Sie unter Frequenz aus, wie oft mit Ihrer Amazon Kendra Datenquelle synchronisiert werden soll.

e. Wählen Sie Weiter aus.

8. Geben Sie auf der Seite Feldzuordnungen festlegen die folgenden Informationen ein:

   a. Wählen Sie aus den Amazon Kendra generierten Standard-Datenquellenfeldern aus, die Sie Ihrem Index zuordnen möchten. Um benutzerdefinierte Datenquellenfelder hinzuzufügen, erstellen Sie einen Indexfeldnamen für die Zuordnung und den Felddatentyp.

   b. Wählen Sie Weiter aus.

9. Überprüfen Sie auf der Seite Überprüfen und erstellen, ob die von Ihnen eingegebenen Informationen korrekt sind, und wählen Sie dann Datenquelle hinzufügen aus. Sie können Ihre Informationen auch auf dieser Seite bearbeiten. Ihre Datenquelle wird auf der Seite Datenquellen angezeigt, nachdem die Datenquelle erfolgreich hinzugefügt wurde.

API

Um eine Verbindung Amazon Kendra herzustellen Adobe Experience Manager

Sie müssen mithilfe der TemplateConfigurationAPI einen JSON-Wert des Datenquellenschemas angeben. Sie müssen die folgenden Informationen angeben:

- Datenquelle — Geben Sie den Datenquellentyp wie `AEM` bei der Verwendung des TemplateConfigurationJSON-Schemas an. Geben Sie außerdem die Datenquelle so an`TEMPLATE`, wie Sie die CreateDataSourceAPI aufrufen.
- AEM-Host-URL — Geben Sie die Adobe Experience Manager Host-URL an. Wenn Sie beispielsweise AEM On-Premise verwenden, geben Sie den Hostnamen und den Port an:. https://hostname:port Oder, wenn Sie AEM als Cloud-Service verwenden, können Sie die URL des Autors verwenden:. https://author-xxxxxx-xxxxxxx.adobeaemcloud.com
- Synchronisierungsmodus — Geben Sie an, wie Ihr Index aktualisiert Amazon Kendra werden soll, wenn sich der Inhalt Ihrer Datenquelle ändert. Wenn Sie Ihre Datenquelle Amazon Kendra zum ersten Mal synchronisieren, werden alle Inhalte standardmäßig gecrawlt und indexiert. Sie müssen eine vollständige Synchronisierung Ihrer Daten durchführen, falls Ihre erste Synchronisierung fehlgeschlagen ist, auch wenn Sie die Option Vollsynchronisierung nicht als Synchronisierungsmodusoption wählen. Sie können wählen zwischen:
  - `FORCED_FULL_CRAWL`um den gesamten Inhalt neu zu indizieren und vorhandene Inhalte jedes Mal zu ersetzen, wenn Ihre Datenquelle mit Ihrem Index synchronisiert wird.
  - `FULL_CRAWL`um bei jeder Synchronisierung Ihrer Datenquelle mit Ihrem Index nur neue, geänderte und gelöschte Inhalte zu indizieren. Amazon Kendra kann den Mechanismus Ihrer Datenquelle verwenden, um Inhaltsänderungen nachzuverfolgen und Inhalte zu indexieren, die sich seit der letzten Synchronisierung geändert haben.
  - `CHANGE_LOG`um jedes Mal, wenn Ihre Datenquelle mit Ihrem Index synchronisiert wird, nur neue und geänderte Inhalte zu indizieren. Amazon Kendra kann den Mechanismus Ihrer Datenquelle verwenden, um Inhaltsänderungen nachzuverfolgen und Inhalte zu indexieren, die sich seit der letzten Synchronisierung geändert haben.
- Authentifizierungstyp — Geben Sie an, welchen Authentifizierungstyp Sie verwenden möchten, entweder `Basic` oder`OAuth2`.
- AEM-Typ — Geben Sie an, welchen Typ Adobe Experience Manager Sie verwenden, entweder oder. `CLOUD` `ON_PREMISE`
- Geheimer Amazon-Ressourcenname (ARN) — Wenn Sie die Standardauthentifizierung für AEM On-Premise oder Cloud verwenden möchten, geben Sie ein Geheimnis an, in dem Ihre

Authentifizierungsdaten mit Ihrem Benutzernamen und Passwort gespeichert werden. Sie geben den Amazon-Ressourcennamen (ARN) eines AWS Secrets Manager Geheimnisses an. Das Geheimnis wird in einer JSON-Struktur mit den folgenden Schlüsseln gespeichert:

```
{
    "aemUrl": "Adobe Experience Manager On-Premise host URL",
    "username": "user name with admin permissions",
    "password": "password with admin permissions"
}
```

Wenn Sie die OAuth 2.0-Authentifizierung für AEM On-Premise verwenden möchten, wird das Geheimnis in einer JSON-Struktur mit den folgenden Schlüsseln gespeichert:

```
{
    "aemUrl": "Adobe Experience Manager host URL",
    "clientId": "client ID",
    "clientSecret": "client secret",
    "privateKey": "private key"
}
```

Wenn Sie die OAuth 2.0-Authentifizierung für AEM as a Cloud Service verwenden möchten, wird das Geheimnis in einer JSON-Struktur mit den folgenden Schlüsseln gespeichert:

```
{
    "clientId": "client ID",
    "clientSecret": "client secret",
    "privateKey": "private key",
    "orgId": "organization ID",
    "technicalAccountId": "technical account ID",
    "imsHost": "Adobe Identity Management System (IMS) host"
}
```

- IAM Rolle — Geben Sie an`RoleArn`, wann Sie anrufen`CreateDataSource`, um einer IAM Rolle Berechtigungen für den Zugriff auf Ihr Secrets Manager Geheimnis und den Aufruf der erforderlichen öffentlichen APIs für den Adobe Experience Manager-Connector und zuzuweisen. Amazon Kendra Weitere Informationen finden Sie unter IAM Rollen für Adobe Experience Manager-Datenquellen.

Sie können auch die folgenden optionalen Funktionen hinzufügen:

- Virtual Private Cloud (VPC) — Geben Sie an, `VpcConfiguration` wann Sie anrufen. `CreateDataSource` Weitere Informationen finden Sie unter Konfigurieren von Amazon Kendra für die Verwendung eines Amazon VPC.
- Zeitzonen-ID — Wenn Sie AEM On-Premise verwenden und sich die Zeitzone Ihres Servers von der Zeitzone des Amazon Kendra AEM-Connectors oder -Indexes unterscheidet, können Sie die Serverzeitzone so angeben, dass sie mit dem AEM-Connector oder Index übereinstimmt.

  Die Standardzeitzone für AEM On-Premise ist die Zeitzone des AEM-Connectors oder -Indexes. Amazon Kendra Die Standardzeitzone für AEM as a Cloud Service ist Greenwich Mean Time.

  Informationen zu den unterstützten Zeitzonen-IDs finden Sie unter Adobe Experience ManagerJSON-Schema.
- Inklusions- und Ausschlussfilter — Geben Sie an, ob bestimmte Seiten und Inhalte ein- oder ausgeschlossen werden sollen.

  > **Note**
  >
  > Die meisten Datenquellen verwenden Muster für reguläre Ausdrücke, bei denen es sich um Ein- oder Ausschlussmuster handelt, die als Filter bezeichnet werden. Wenn Sie einen Einschlussfilter angeben, werden nur Inhalte indexiert, die dem Einschlussfilter entsprechen. Jedes Dokument, das nicht dem Einschlussfilter entspricht, wird nicht indexiert. Wenn Sie einen Ein- und Ausschlussfilter angeben, werden Dokumente, die dem Ausschlussfilter entsprechen, nicht indexiert, auch wenn sie dem Einschlussfilter entsprechen.
- Identity Crawler — Geben Sie an, ob der Identity Crawler aktiviert Amazon Kendra werden soll. Der Identity Crawler verwendet die Informationen der Zugriffskontrollliste (ACL) für Ihre Dokumente, um Suchergebnisse nach dem Benutzer- oder Gruppenzugriff auf Dokumente zu filtern. Wenn Sie über eine ACL für Ihre Dokumente verfügen und Ihre ACL verwenden möchten, können Sie auch den Identity Crawler aktivieren, um die Benutzerkontextfilterung der Suchergebnisse zu konfigurieren. Amazon Kendra Andernfalls können alle Dokumente öffentlich durchsucht werden, wenn Identity Crawler ausgeschaltet ist. Wenn Sie die Zugriffskontrolle für Ihre Dokumente verwenden möchten und Identity Crawler ausgeschaltet ist, können Sie alternativ die PutPrincipalMappingAPI verwenden, um Benutzer- und Gruppenzugriffsinformationen für die Benutzerkontextfilterung hochzuladen.

- Feldzuordnungen — Wählen Sie diese Option, um Ihre Adobe Experience Manager-Datenquellenfelder Ihren Indexfeldern zuzuordnen. Amazon Kendra Weitere Informationen finden Sie unter Zuweisen von Datenquellenfeldern.

  > **Note**
  >
  > Das Textfeld oder das entsprechende Textfeld für Ihre Dokumente ist erforderlich, um Ihre Dokumente durchsuchen Amazon Kendra zu können. Sie müssen den Feldnamen Ihres Dokumenthauptteils in Ihrer Datenquelle dem Namen des Indexfeldes zuordnen`_document_body`. Alle anderen Felder sind optional.

Eine Liste weiterer wichtiger JSON-Schlüssel, die konfiguriert werden müssen, finden Sie unter Adobe Experience ManagerVorlagenschema.

Alfresco

Alfrescoist ein Content-Management-Service, der Kunden dabei unterstützt, ihre Inhalte zu speichern und zu verwalten. Sie können Amazon Kendra es verwenden, um Ihre Alfresco Dokumentbibliothek, Ihr Wiki und Ihren Blog zu indizieren.

Amazon Kendra unterstützt Alfresco On-Premise und Alfresco Cloud (Platform as a Service).

Sie können über Amazon Kendra die Amazon Kendra Konsole oder die TemplateConfigurationAPI eine Verbindung zu Ihrer Alfresco Datenquelle herstellen.

Informationen zur Fehlerbehebung bei Ihrem Amazon Kendra Alfresco-Datenquellen-Connector finden Sie unter. Problembehandlung bei Datenquellen

Themen

- Unterstützte Features
- Voraussetzungen
- Anweisungen zur Verbindung
- Weitere Informationen

Unterstützte Features

Amazon Kendra AlfrescoDer Datenquellen-Connector unterstützt die folgenden Funktionen:

- Feldzuordnungen
- Einschluss-/Ausschlussfilter
- Vollständige und inkrementelle Inhaltssynchronisierung
- Virtual Private Cloud (VPC)
- Filterung des Benutzerkontextes
- OAuth 2.0 und Standardauthentifizierung

Voraussetzungen

Bevor Sie Ihre Alfresco-Datenquelle Amazon Kendra zur Indexierung verwenden können, nehmen Sie diese Änderungen in Ihrem und vor. Alfresco AWS-Konten

Stellen Sie sicherAlfresco, dass Sie Folgendes haben:

- Ihre Alfresco Repository-URL und die URL Ihrer Webanwendung wurden kopiert. Wenn Sie nur eine bestimmte Alfresco Site indexieren möchten, kopieren Sie auch die Site-ID.
- Notieren Sie sich Ihre Alfresco Authentifizierungsdaten, die einen Benutzernamen und ein Passwort mit mindestens Leseberechtigungen beinhalten. Wenn Sie die OAuth 2.0-Authentifizierung verwenden möchten, sollten Sie den Benutzer der Alfresco Administratorgruppe hinzufügen.
- Optional: Generierte OAuth 2.0-Anmeldeinformationen in. Alfresco Zu den Anmeldeinformationen gehören die Client-ID, der geheime Client-Schlüssel und die Token-URL. Weitere Informationen zur Konfiguration von Clients für Alfresco On-Premises finden Sie in der Alfresco-Dokumentation. Wenn Sie Alfresco Cloud (PaaS) verwenden, müssen Sie sich für die OAuth 2.0-Authentifizierung an den Hyland-Support wenden. Alfresco
- Geprüft, ob jedes Dokument in Alfresco und in anderen Datenquellen, die Sie für denselben Index verwenden möchten, einzigartig ist. Jede Datenquelle, die Sie für einen Index verwenden möchten, darf nicht dasselbe Dokument in allen Datenquellen enthalten. Dokument-IDs gelten für einen Index global und müssen pro Index eindeutig sein.

Stellen Sie sicher AWS-Konto, dass Sie Folgendes in Ihrem haben:

- Hat einen Amazon Kendra Index erstellt und bei Verwendung der API die Index-ID notiert.
- Sie haben eine IAM Rolle für Ihre Datenquelle erstellt und, falls Sie die API verwenden, den ARN der IAM Rolle notiert.

> **Note**
>
> Wenn Sie Ihren Authentifizierungstyp und Ihre Anmeldeinformationen ändern, müssen Sie Ihre IAM Rolle aktualisieren, um auf die richtige AWS Secrets Manager geheime ID zugreifen zu können.

- Ihre Alfresco-Authentifizierungsdaten AWS Secrets Manager geheim gespeichert und, falls Sie die API verwenden, den ARN des Geheimnisses notiert.

> **Note**
>
> Wir empfehlen Ihnen, Ihre Zugangsdaten und Ihr Secret regelmäßig zu aktualisieren oder zu wechseln. Stellen Sie zu Ihrer eigenen Sicherheit nur die Zugriffsebene bereit, die erforderlich ist. Wir raten davon ab, Anmeldeinformationen und geheime Daten für alle Datenquellen und Connector-Versionen 1.0 und 2.0 (sofern zutreffend) wiederzuverwenden.

Wenn Sie noch keine IAM Rolle oder keinen Schlüssel haben, können Sie die Konsole verwenden, um eine neue IAM Rolle und ein neues Secrets Manager Geheimnis zu erstellen, wenn Sie Ihre Alfresco-Datenquelle mit verbinden. Amazon Kendra Wenn Sie die API verwenden, müssen Sie den ARN einer vorhandenen IAM Rolle und eines Secrets Manager Geheimnisses sowie eine Index-ID angeben.

Anweisungen zur Verbindung

Um eine Verbindung Amazon Kendra zu Ihrer Alfresco-Datenquelle herzustellen, müssen Sie die erforderlichen Details zu Ihrer Alfresco-Datenquelle angeben, damit Sie auf Ihre Daten zugreifen Amazon Kendra können. Falls Sie Alfresco für noch nicht konfiguriert haben, finden Sie weitere Informationen unter. Amazon KendraVoraussetzungen

Console

Um eine Verbindung herzustellen Amazon Kendra Alfresco

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die Amazon Kendra Konsole.
2. Wählen Sie im linken Navigationsbereich Indizes und dann den Index, den Sie verwenden möchten, aus der Indexliste aus.

   > **Note**
   >
   > Sie können Ihre Einstellungen für die Benutzerzugriffskontrolle unter Indexeinstellungen konfigurieren oder bearbeiten.

3. Wählen Sie auf der Seite Erste Schritte die Option Datenquelle hinzufügen aus.
4. Wählen Sie auf der Seite Datenquelle hinzufügen die Option Alfresco Connector und dann Connector hinzufügen aus.
5. Geben Sie auf der Seite „Datenquellendetails angeben“ die folgenden Informationen ein:

   a. Geben Sie im Feld Name und Beschreibung für Datenquellenname einen Namen für Ihre Datenquelle ein. Sie können Bindestriche, aber keine Leerzeichen verwenden.

   b. (Optional) Beschreibung — Geben Sie eine optionale Beschreibung für Ihre Datenquelle ein.

   c. In Standardsprache — Wählen Sie eine Sprache aus, um Ihre Dokumente nach dem Index zu filtern. Sofern Sie nichts anderes angeben, ist die Standardsprache Englisch. Die in den Metadaten des Dokuments angegebene Sprache hat Vorrang vor der ausgewählten Sprache.

   d. Unter Tags für Neues Tag hinzufügen — Fügen Sie optionale Tags hinzu, um Ihre Ressourcen zu durchsuchen und zu filtern oder Ihre Kosten nachzuverfolgen. AWS

   e. Wählen Sie Weiter aus.

6. Geben Sie auf der Seite Zugriff und Sicherheit definieren die folgenden Informationen ein:

   a. Alfrescotype — Wählen Sie aus, ob Sie Alfresco On-Premise oder Alfresco Cloud (Platform as a Service) verwenden möchten.

   b. Alfresco-Repository-URL — Geben Sie Ihre Alfresco-Repository-URL ein. Wenn Sie beispielsweise Alfresco Cloud (PaaS) verwenden, könnte die Repository-URL lauten. https://company.alfrescocloud.com Oder, wenn Sie Alfresco On-Premises verwenden, könnte die Repository-URL lauten. https://company-alfresco-instance.company-domain.suffix:port

c. Alfresco-Benutzeranwendung. URL — Geben Sie die URL Ihrer Alfresco Benutzeroberfläche ein. Sie können die Repository-URL von Ihrem Alfresco Administrator erhalten. Die URL der Benutzeroberfläche könnte beispielsweise https://example.com lauten.

d. Speicherort des SSL-Zertifikats — Geben Sie den Pfad zu dem in einem Amazon S3 Bucket gespeicherten SSL-Zertifikat ein. Sie verwenden dies, um über eine sichere SSL-Verbindung eine Verbindung zu Alfresco On-Premises herzustellen.

e. Autorisierung — Aktivieren oder deaktivieren Sie die Informationen der Zugriffskontrollliste (ACL) für Ihre Dokumente, wenn Sie über eine ACL verfügen und diese für die Zugriffskontrolle verwenden möchten. Die ACL gibt an, auf welche Dokumente Benutzer und Gruppen zugreifen können. Die ACL-Informationen werden verwendet, um Suchergebnisse nach dem Benutzer- oder Gruppenzugriff auf Dokumente zu filtern. Weitere Informationen finden Sie unter Benutzerkontextfilterung.

f. Authentifizierung — Wählen Sie Standardauthentifizierung oder OAuth 2.0-Authentifizierung. Wählen Sie dann ein vorhandenes Secrets Manager Geheimnis aus oder erstellen Sie ein neues Geheimnis, um Ihre Anmeldeinformationen zu speichern. Alfresco Wenn Sie sich dafür entscheiden, ein neues Geheimnis zu erstellen, wird ein AWS Secrets Manager geheimes Fenster geöffnet.

   Wenn Sie sich für die Standardauthentifizierung entschieden haben, geben Sie einen Namen für das Geheimnis, den Alfresco Benutzernamen und das Passwort ein.

   Wenn Sie sich für die OAuth 2.0-Authentifizierung entschieden haben, geben Sie einen Namen für das Geheimnis, die Client-ID, den geheimen Client-Schlüssel und die Token-URL ein.

g. Virtual Private Cloud (VPC) — Sie können wählen, ob Sie eine VPC verwenden möchten. In diesem Fall müssen Sie Subnetze und VPC-Sicherheitsgruppen hinzufügen.

h. Identity Crawler — Geben Sie an, ob der Identity Crawler aktiviert Amazon Kendra werden soll. Der Identity Crawler verwendet die Informationen der Zugriffskontrollliste (ACL) für Ihre Dokumente, um Suchergebnisse nach dem Benutzer- oder Gruppenzugriff auf Dokumente zu filtern. Wenn Sie über eine ACL für Ihre Dokumente verfügen und sich dafür entscheiden, Ihre ACL zu verwenden, können Sie auch den Identity Crawler aktivieren, um die Benutzerkontextfilterung von Suchergebnissen zu konfigurieren. Amazon Kendra Andernfalls können alle Dokumente öffentlich durchsucht werden, wenn Identity Crawler ausgeschaltet ist. Wenn Sie die Zugriffskontrolle für Ihre Dokumente verwenden möchten und Identity Crawler ausgeschaltet ist, können Sie alternativ die

PutPrincipalMappingAPI verwenden, um Benutzer- und Gruppenzugriffsinformationen für die Benutzerkontextfilterung hochzuladen.

i. IAM Rolle — Wählen Sie eine bestehende IAM Rolle oder erstellen Sie eine neue IAM Rolle, um auf Ihre Repository-Anmeldeinformationen und Indexinhalte zuzugreifen.

> **Note**
>
> IAM Rollen, die für Indizes verwendet werden, können nicht für Datenquellen verwendet werden. Wenn Sie sich nicht sicher sind, ob eine vorhandene Rolle für einen Index oder eine häufig gestellte Frage verwendet wird, wählen Sie Neue Rolle erstellen, um Fehler zu vermeiden.

j. Wählen Sie Weiter aus.

7. Geben Sie auf der Seite „Synchronisierungseinstellungen konfigurieren“ die folgenden Informationen ein:

a. Synchronisierungsbereich — Legen Sie Grenzwerte für das Crawlen bestimmter Inhalte fest und filtern Sie Inhalte mithilfe von Regex-Ausdrucksmustern.

b. i. Inhalt — Wählen Sie aus, ob Inhalte, die mit „Aspekten“ gekennzeichnet sindAlfresco, Inhalte innerhalb einer bestimmten Alfresco Website oder Inhalte auf all Ihren Websites gecrawlt werden sollen. Alfresco

ii. (Optional) Zusätzliche Konfiguration — Legen Sie die folgenden Einstellungen fest:

- Kommentare einbeziehen — Wählen Sie aus, ob Kommentare in die Alfresco Dokumentbibliothek und den Blog aufgenommen werden sollen.
- Regex-Muster — Reguläre Ausdrucksmuster zum Ein- oder Ausschließen bestimmter Dateien.

c. Synchronisierungsmodus — Wählen Sie aus, wie Sie Ihren Index aktualisieren möchten, wenn sich der Inhalt Ihrer Datenquelle ändert. Wenn Sie Ihre Datenquelle Amazon Kendra zum ersten Mal synchronisieren, werden alle Inhalte standardmäßig gecrawlt und indexiert. Sie müssen eine vollständige Synchronisierung Ihrer Daten durchführen, falls Ihre erste Synchronisierung fehlgeschlagen ist, auch wenn Sie die Option Vollsynchronisierung nicht als Synchronisierungsmodusoption wählen.

- Vollständige Synchronisierung: Indizieren Sie den gesamten Inhalt neu und ersetzen die vorhandenen Inhalte jedes Mal, wenn Ihre Datenquelle mit Ihrem Index synchronisiert wird.

- Neue, geänderte, gelöschte Synchronisierung: Indizieren Sie bei jeder Synchronisierung Ihrer Datenquelle mit Ihrem Index nur neue, geänderte und gelöschte Inhalte. Amazon Kendra kann den Mechanismus Ihrer Datenquelle verwenden, um Inhaltsänderungen nachzuverfolgen und Inhalte zu indexieren, die sich seit der letzten Synchronisierung geändert haben.

d. Wählen Sie im Zeitplan für die Synchronisierungsausführung unter Frequenz aus, wie oft mit Ihrer Datenquelle synchronisiert Amazon Kendra werden soll.

e. Wählen Sie Weiter aus.

8. Geben Sie auf der Seite Feldzuordnungen festlegen die folgenden Informationen ein:

a. Wählen Sie aus den Amazon Kendra generierten Standard-Datenquellenfeldern aus, die Sie Ihrem Index zuordnen möchten.

b. Um benutzerdefinierte Datenquellenfelder hinzuzufügen, erstellen Sie einen Indexfeldnamen für die Zuordnung und den Felddatentyp.

c. Wählen Sie Weiter aus.

9. Überprüfen Sie auf der Seite Überprüfen und erstellen, ob die von Ihnen eingegebenen Informationen korrekt sind, und wählen Sie dann Datenquelle hinzufügen aus. Sie können Ihre Informationen auch auf dieser Seite bearbeiten. Ihre Datenquelle wird auf der Seite Datenquellen angezeigt, nachdem die Datenquelle erfolgreich hinzugefügt wurde.

API

Um eine Verbindung Amazon Kendra herzustellen Alfresco

Sie müssen mithilfe der TemplateConfigurationAPI einen JSON-Wert des Datenquellenschemas angeben. Sie müssen die folgenden Informationen angeben:

- Datenquelle — Geben Sie den Datenquellentyp wie `ALFRESCO` bei der Verwendung des TemplateConfigurationJSON-Schemas an. Geben Sie außerdem die Datenquelle so an`TEMPLATE`, wie Sie die CreateDataSourceAPI aufrufen.
- AlfrescoSite-ID — Geben Sie die Alfresco-Site-ID an.
- AlfrescoRepository-URL — Geben Sie die Repository-URL an. Alfresco Sie können die Repository-URL von Ihrem Alfresco Administrator erhalten. Wenn Sie beispielsweise Alfresco Cloud (PaaS) verwenden, könnte die Repository-URL lauten https://company.alfrescocloud.com. Oder, wenn Sie Alfresco On-Premises verwenden, könnte die Repository-URL lauten. https://company-alfresco-instance.company-domain.suffix:port

- AlfrescoURL der Webanwendung — Geben Sie die URL der Alfresco Benutzeroberfläche an. Sie können die Repository-URL von Ihrem Alfresco Administrator abrufen. Die URL der Benutzeroberfläche könnte beispielsweise https://example.com lauten.
- Authentifizierungstyp — Geben Sie an, welchen Authentifizierungstyp Sie verwenden möchten, ob `OAuth2` oder`Basic`.
- AlfrescoTyp — Geben Sie an, welchen Typ Alfresco Sie verwenden, ob `PAAS` (Cloud/Platform as a Service) oder `ON_PREM` (On-Premise).
- Geheimer Amazon-Ressourcenname (ARN) — Wenn Sie die Standardauthentifizierung verwenden möchten, geben Sie ein Geheimnis an, in dem Ihre Authentifizierungsdaten mit Ihrem Benutzernamen und Passwort gespeichert werden. Sie geben den Amazon-Ressourcennamen (ARN) eines AWS Secrets Manager Geheimnisses an. Das Geheimnis wird in einer JSON-Struktur mit den folgenden Schlüsseln gespeichert:

  ```
  {
      "username": "user name",
      "password": "password"
  }
  ```

  Wenn Sie die OAuth 2.0-Authentifizierung verwenden möchten, wird das Geheimnis in einer JSON-Struktur mit den folgenden Schlüsseln gespeichert:

  ```
  {
      "clientId": "client ID",
      "clientSecret": "client secret",
      "tokenUrl": "token URL"
  }
  ```

- IAM role — Geben Sie an`RoleArn`, wann Sie anrufen`CreateDataSource`, um einer IAM Rolle Berechtigungen für den Zugriff auf Ihr Secrets Manager Geheimnis und den Aufruf der erforderlichen öffentlichen APIs für den Alfresco-Connector und zu erteilen. Amazon Kendra Weitere Informationen finden Sie unter IAM Rollen für Alfresco-Datenquellen.

Sie können auch die folgenden optionalen Funktionen hinzufügen:

- Virtual Private Cloud (VPC) — Geben Sie an, `VpcConfiguration` wann Sie anrufen. `CreateDataSource` Weitere Informationen finden Sie unter Konfigurieren von Amazon Kendra für die Verwendung eines Amazon VPC.

- Inhaltstyp — Der Inhaltstyp, den Sie crawlen möchten, unabhängig davon, ob es sich um Inhalte handelt, die mit „Aspekten“ gekennzeichnet sindAlfresco, Inhalte innerhalb einer bestimmten Alfresco Website oder Inhalte auf all Ihren Websites. Alfresco Sie können auch bestimmte „Aspekte“ -Inhalte auflisten.
- Inklusions- und Ausschlussfilter — Geben Sie an, ob bestimmte Dateien ein- oder ausgeschlossen werden sollen.

  > **Note**
  >
  > Die meisten Datenquellen verwenden Muster mit regulären Ausdrücken, bei denen es sich um Ein- oder Ausschlussmuster handelt, die als Filter bezeichnet werden. Wenn Sie einen Einschlussfilter angeben, werden nur Inhalte indexiert, die dem Einschlussfilter entsprechen. Jedes Dokument, das nicht dem Einschlussfilter entspricht, wird nicht indexiert. Wenn Sie einen Ein- und Ausschlussfilter angeben, werden Dokumente, die dem Ausschlussfilter entsprechen, nicht indexiert, auch wenn sie dem Einschlussfilter entsprechen.

- Synchronisierungsmodus — Geben Sie an, wie Ihr Index aktualisiert Amazon Kendra werden soll, wenn sich der Inhalt Ihrer Datenquelle ändert. Wenn Sie Ihre Datenquelle Amazon Kendra zum ersten Mal synchronisieren, werden alle Inhalte standardmäßig gecrawlt und indexiert. Sie müssen eine vollständige Synchronisierung Ihrer Daten durchführen, falls Ihre erste Synchronisierung fehlgeschlagen ist, auch wenn Sie die Option Vollsynchronisierung nicht als Synchronisierungsmodusoption wählen. Sie können wählen zwischen:
  - `FORCED_FULL_CRAWL`um den gesamten Inhalt neu zu indizieren und vorhandene Inhalte jedes Mal zu ersetzen, wenn Ihre Datenquelle mit Ihrem Index synchronisiert wird.
  - `FULL_CRAWL`um bei jeder Synchronisierung Ihrer Datenquelle mit Ihrem Index nur neue, geänderte und gelöschte Inhalte zu indizieren. Amazon Kendra kann den Mechanismus Ihrer Datenquelle verwenden, um Inhaltsänderungen nachzuverfolgen und Inhalte zu indexieren, die sich seit der letzten Synchronisierung geändert haben.
- Identity Crawler — Geben Sie an, ob der Identity Crawler aktiviert Amazon Kendra werden soll. Der Identity Crawler verwendet die Informationen der Zugriffskontrollliste (ACL) für Ihre Dokumente, um Suchergebnisse nach dem Benutzer- oder Gruppenzugriff auf Dokumente zu filtern. Wenn Sie über eine ACL für Ihre Dokumente verfügen und sich dafür entscheiden, Ihre ACL zu verwenden, können Sie auch den Identity Crawler aktivieren, um die Benutzerkontextfilterung von Suchergebnissen zu konfigurieren. Amazon Kendra Andernfalls können alle Dokumente öffentlich durchsucht werden, wenn Identity Crawler ausgeschaltet ist.

Wenn Sie die Zugriffskontrolle für Ihre Dokumente verwenden möchten und Identity Crawler ausgeschaltet ist, können Sie alternativ die PutPrincipalMappingAPI verwenden, um Benutzer- und Gruppenzugriffsinformationen für die Benutzerkontextfilterung hochzuladen.

- Feldzuordnungen — Wählen Sie diese Option, um Ihre Alfresco-Datenquellenfelder Ihren Indexfeldern zuzuordnen. Amazon Kendra Weitere Informationen finden Sie unter Zuweisen von Datenquellenfeldern.

> **Note**
>
> Das Textfeld oder das entsprechende Textfeld für Ihre Dokumente ist erforderlich, um Ihre Dokumente durchsuchen zu können. Amazon Kendra Sie müssen den Feldnamen Ihres Dokumenthauptteils in Ihrer Datenquelle dem Namen des Indexfeldes zuordnen`_document_body`. Alle anderen Felder sind optional.

Eine Liste weiterer wichtiger JSON-Schlüssel, die konfiguriert werden müssen, finden Sie unter AlfrescoVorlagenschema.

Weitere Informationen

Weitere Informationen zur Integration Amazon Kendra mit Ihrer Alfresco-Datenquelle finden Sie unter:

- Suchen Sie intelligent nach Inhalten mit AlfrescoAmazon Kendra

Aurora (MySQL)

Aurora ist ein relationales Datenbankmanagementsystem (RDBMS), das für die Cloud entwickelt wurde. Wenn Sie ein Aurora Benutzer sind, können Sie es verwenden, um Ihre Aurora (MySQL) Datenquelle Amazon Kendra zu indizieren. Der Amazon Kendra Aurora (MySQL) Datenquellenconnector unterstützt Aurora MySQL 3 und Aurora Serverless MySQL 8.0.

Sie können über Amazon Kendra die Amazon Kendra Konsole und die TemplateConfigurationAPI eine Verbindung zu Ihrer Aurora (MySQL) Datenquelle herstellen.

Informationen zur Fehlerbehebung bei Ihrem Amazon Kendra Aurora (MySQL) Datenquellen-Connector finden Sie unterProblembehandlung bei Datenquellen.

Themen

Unterstützte Features

- Feldzuordnungen
- Filterung des Benutzerkontextes
- Einschluss-/Ausschlussfilter
- Vollständige und inkrementelle Inhaltssynchronisierung
- Virtual Private Cloud (VPC)

Voraussetzungen

Bevor Sie Ihre Aurora (MySQL) Datenquelle Amazon Kendra zum Indizieren verwenden können, nehmen Sie diese Änderungen in Ihren Konten Aurora (MySQL) und AWS Konten vor.

Stellen Sie sicherAurora (MySQL), dass Sie Folgendes haben:

- Notiert Ihren Datenbank-Benutzernamen und Ihr Passwort.

> **Important**
>
> Es hat sich bewährt, nur lesbare Amazon Kendra Datenbankanmeldeinformationen zur Verfügung zu stellen.

- Die URL, der Port und die Instanz Ihres Datenbank-Hosts wurden kopiert. Sie finden diese Informationen auf der Amazon RDS Konsole.
- Vergewissert, dass jedes Dokument in Aurora (MySQL) und zwischen anderen Datenquellen, die Sie für denselben Index verwenden möchten, einzigartig ist. Jede Datenquelle, die Sie für einen Index verwenden möchten, darf nicht dasselbe Dokument in allen Datenquellen enthalten. Dokument-IDs gelten für einen Index global und müssen pro Index eindeutig sein.

Stellen Sie sicher AWS-Konto, dass Sie Folgendes in Ihrem haben:

- Hat einen Amazon Kendra Index erstellt und bei Verwendung der API die Index-ID notiert.
- Sie haben eine IAM Rolle für Ihre Datenquelle erstellt und, falls Sie die API verwenden, den ARN der IAM Rolle notiert.

> **Note**
>
> Wenn Sie Ihren Authentifizierungstyp und Ihre Anmeldeinformationen ändern, müssen Sie Ihre IAM Rolle aktualisieren, um auf die richtige AWS Secrets Manager geheime ID zugreifen zu können.

- Wir haben Ihre Aurora (MySQL) Authentifizierungsdaten AWS Secrets Manager geheim gespeichert und, falls Sie die API verwenden, den ARN des Geheimnisses notiert.

> **Note**
>
> Wir empfehlen Ihnen, Ihre Anmeldeinformationen und Ihr Geheimnis regelmäßig zu aktualisieren oder zu wechseln. Stellen Sie zu Ihrer eigenen Sicherheit nur die Zugriffsebene bereit, die erforderlich ist. Wir raten davon ab, Anmeldeinformationen und geheime Daten für alle Datenquellen und Connector-Versionen 1.0 und 2.0 (sofern zutreffend) wiederzuverwenden.

Wenn Sie noch keine IAM Rolle oder keinen Schlüssel haben, können Sie die Konsole verwenden, um eine neue IAM Rolle und ein neues Secrets Manager Geheimnis zu erstellen, wenn Sie Ihre Aurora (MySQL) Datenquelle mit verbinden. Amazon Kendra Wenn Sie die API verwenden, müssen Sie den ARN einer vorhandenen IAM Rolle und eines Secrets Manager Geheimnisses sowie eine Index-ID angeben.

Anweisungen zur Verbindung

Um eine Verbindung Amazon Kendra zu Ihrer Aurora (MySQL) Datenquelle herzustellen, müssen Sie Details zu Ihren Aurora (MySQL) Anmeldeinformationen angeben, damit Sie auf Ihre Daten zugreifen Amazon Kendra können. Falls Sie das noch nicht konfiguriert haben, Amazon Kendra finden Sie Aurora (MySQL) weitere Informationen unterVoraussetzungen.

Console

Um eine Verbindung Amazon Kendra herzustellen Aurora (MySQL)

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die Amazon Kendra Konsole.
2. Wählen Sie im linken Navigationsbereich Indizes und dann den Index, den Sie verwenden möchten, aus der Indexliste aus.

   > **Note**
   >
   > Sie können Ihre Einstellungen für die Benutzerzugriffskontrolle unter Indexeinstellungen konfigurieren oder bearbeiten.

3. Wählen Sie auf der Seite Erste Schritte die Option Datenquelle hinzufügen aus.
4. Wählen Sie auf der Seite Datenquelle hinzufügen die Option Aurora (MySQL)Connector und dann Connector hinzufügen aus.
5. Geben Sie auf der Seite „Datenquellendetails angeben“ die folgenden Informationen ein:

   a. Geben Sie im Feld Name und Beschreibung für Datenquellenname einen Namen für Ihre Datenquelle ein. Sie können Bindestriche, aber keine Leerzeichen verwenden.

   b. (Optional) Beschreibung — Geben Sie eine optionale Beschreibung für Ihre Datenquelle ein.

   c. In Standardsprache — Wählen Sie eine Sprache aus, um Ihre Dokumente nach dem Index zu filtern. Sofern Sie nichts anderes angeben, ist die Standardsprache Englisch. Die in den Metadaten des Dokuments angegebene Sprache hat Vorrang vor der ausgewählten Sprache.

   d. Unter Tags für Neues Tag hinzufügen — Fügen Sie optionale Tags hinzu, um Ihre Ressourcen zu durchsuchen und zu filtern oder Ihre Kosten nachzuverfolgen. AWS

   e. Wählen Sie Weiter aus.

6. Geben Sie auf der Seite Zugriff und Sicherheit definieren die folgenden Informationen ein:

   a. Geben Sie im Feld Quelle die folgenden Informationen ein:

   b. Host — Geben Sie die URL des Datenbank-Hosts ein, zum Beispiel:`http://`*`instance URL`*`.`*`region`*`.rds.amazonaws.com`.

   c. Port — Geben Sie den Datenbankport ein, zum Beispiel`5432`.

   d. Instanz — Geben Sie die Datenbankinstanz ein.

   e. Geben Sie im Feld Authentifizierung die folgenden Informationen ein:

- AWS Secrets Manager geheim — Wählen Sie ein vorhandenes Geheimnis aus, oder erstellen Sie ein neues Secrets Manager Geheimnis, um Ihre Aurora (MySQL) Authentifizierungsdaten zu speichern. Wenn Sie ein neues Geheimnis erstellen möchten, wird ein AWS Secrets Manager geheimes Fenster geöffnet.

  A. Geben Sie die folgenden Informationen in das Fenster Create an AWS Secrets Manager Secret ein:

     I. Geheimer Name — Ein Name für Ihr Geheimnis. Das Präfix 'AmazonKendra- Aurora (MySQL) -' wird Ihrem geheimen Namen automatisch hinzugefügt.

     II. Für Datenbankbenutzername und Passwort — Geben Sie die Werte der Authentifizierungsdaten ein, die Sie aus Ihrer Datenbank kopiert haben.

  B. Wählen Sie Speichern.

f. Virtual Private Cloud (VPC) — Sie können wählen, ob Sie eine VPC verwenden möchten. In diesem Fall müssen Sie Subnetze und VPC-Sicherheitsgruppen hinzufügen.

g. IAM Rolle — Wählen Sie eine bestehende IAM Rolle oder erstellen Sie eine neue IAM Rolle, um auf Ihre Repository-Anmeldeinformationen und Indexinhalte zuzugreifen.

> **Note**
>
> IAM Rollen, die für Indizes verwendet werden, können nicht für Datenquellen verwendet werden. Wenn Sie sich nicht sicher sind, ob eine vorhandene Rolle für einen Index oder eine häufig gestellte Frage verwendet wird, wählen Sie Neue Rolle erstellen, um Fehler zu vermeiden.

h. Wählen Sie Weiter aus.

7. Geben Sie auf der Seite „Synchronisierungseinstellungen konfigurieren“ die folgenden Informationen ein:

   a. Wählen Sie unter Synchronisierungsbereich eine der folgenden Optionen aus:

   - SQL-Abfrage — Geben Sie SQL-Abfrageanweisungen wie SELECT- und JOIN-Operationen ein. SQL-Abfragen müssen weniger als 32 KB groß sein. SQL-Abfragen müssen weniger als 32 KB groß sein und dürfen keine Semikolons (;) enthalten. Amazon Kendra durchsucht den gesamten Datenbankinhalt, der Ihrer Abfrage entspricht.

- Primärschlüsselspalte — Geben Sie den Primärschlüssel für die Datenbanktabelle an. Dies identifiziert eine Tabelle in Ihrer Datenbank.
- Titelspalte — Geben Sie den Namen der Titelspalte des Dokuments in Ihrer Datenbanktabelle an.
- Hauptspalte — Geben Sie den Namen der Hauptspalte des Dokuments in Ihrer Datenbanktabelle an.

b. Wählen Sie unter Zusätzliche Konfiguration — optional aus den folgenden Optionen, um bestimmte Inhalte zu synchronisieren, anstatt alle Dateien zu synchronisieren:

- Spalten zur Erkennung von Änderungen — Geben Sie die Namen der Spalten ein, anhand derer Inhaltsänderungen erkannt Amazon Kendra werden sollen. Amazon Kendra indexiert den Inhalt neu, wenn sich eine dieser Spalten ändert.
- Spalte mit Benutzer-IDs — Geben Sie den Namen der Spalte ein, die Benutzer-IDs enthält, um Zugriff auf Inhalte zu erhalten.
- Spalte „Gruppen“ — Geben Sie den Namen der Spalte ein, die Gruppen enthält, denen der Zugriff auf Inhalte gewährt werden soll.
- Spalte Quell-URLs — Geben Sie den Namen der Spalte ein, die Quell-URLs enthält, die indexiert werden sollen.
- Spalte mit Zeitstempeln — Geben Sie den Namen der Spalte ein, die Zeitstempel enthält. Amazon Kendra verwendet Zeitstempelinformationen, um Änderungen an Ihren Inhalten zu erkennen und nur geänderte Inhalte zu synchronisieren.
- Spalte „Zeitzonen“ — Geben Sie den Namen der Spalte ein, die Zeitzonen für den Inhalt enthält, der gecrawlt werden soll.
- Zeitstempelformat — Geben Sie den Namen der Spalte ein, die Zeitstempelformate enthält, anhand derer Inhaltsänderungen erkannt und Ihre Inhalte erneut synchronisiert werden sollen.

c. Synchronisierungsmodus — Wählen Sie aus, wie Sie Ihren Index aktualisieren möchten, wenn sich der Inhalt Ihrer Datenquelle ändert. Wenn Sie Ihre Datenquelle Amazon Kendra zum ersten Mal synchronisieren, werden alle Inhalte standardmäßig gecrawlt und indexiert. Sie müssen eine vollständige Synchronisierung Ihrer Daten durchführen, falls Ihre erste Synchronisierung fehlgeschlagen ist, auch wenn Sie die Option Vollsynchronisierung nicht als Synchronisierungsmodusoption wählen.

- Vollständige Synchronisierung: Indizieren Sie den gesamten Inhalt neu und ersetzen die vorhandenen Inhalte jedes Mal, wenn Ihre Datenquelle mit Ihrem Index synchronisiert wird.
- Neue, geänderte Synchronisierung: Indizieren Sie jedes Mal, wenn Ihre Datenquelle mit Ihrem Index synchronisiert wird, nur neue und geänderte Inhalte. Amazon Kendra kann den Mechanismus Ihrer Datenquelle verwenden, um Inhaltsänderungen nachzuverfolgen und Inhalte zu indexieren, die sich seit der letzten Synchronisierung geändert haben.
- Neue, geänderte, gelöschte Synchronisierung: Indizieren Sie bei jeder Synchronisierung Ihrer Datenquelle mit Ihrem Index nur neue, geänderte und gelöschte Inhalte. Amazon Kendra kann den Mechanismus Ihrer Datenquelle verwenden, um Inhaltsänderungen nachzuverfolgen und Inhalte zu indexieren, die sich seit der letzten Synchronisierung geändert haben.

d. Im Synchronisierungslaufplan für Frequenz — Wie oft Amazon Kendra wird mit Ihrer Datenquelle synchronisiert?

e. Wählen Sie Weiter aus.

8. Geben Sie auf der Seite Feldzuordnungen festlegen die folgenden Informationen ein:

   a. Wählen Sie aus den generierten Standard-Datenquellenfeldern — Dokument-IDs, Dokumenttitel und Quell-URLs — aus, die Sie dem Index zuordnen möchten. Amazon Kendra

   b. Feld hinzufügen — Um benutzerdefinierte Datenquellenfelder hinzuzufügen, um einen Indexfeldnamen für die Zuordnung und den Felddatentyp zu erstellen.

   c. Wählen Sie Weiter aus.

9. Überprüfen Sie auf der Seite Überprüfen und erstellen, ob die von Ihnen eingegebenen Informationen korrekt sind, und wählen Sie dann Datenquelle hinzufügen aus. Sie können Ihre Informationen auch auf dieser Seite bearbeiten. Ihre Datenquelle wird auf der Seite Datenquellen angezeigt, nachdem die Datenquelle erfolgreich hinzugefügt wurde.

API

Um eine Verbindung Amazon Kendra herzustellen Aurora (MySQL)

Mithilfe der TemplateConfigurationAPI müssen Sie Folgendes angeben:

- Datenquelle — Geben Sie den Datenquellentyp wie `JDBC` bei der Verwendung des TemplateConfigurationJSON-Schemas an. Geben Sie außerdem die Datenquelle so an`TEMPLATE`, wie Sie die CreateDataSourceAPI aufrufen.
- Datenbanktyp — Sie müssen den Datenbanktyp als `mySql` angeben.
- SQL-Abfrage — Geben Sie SQL-Abfrageanweisungen wie SELECT- und JOIN-Operationen an. SQL-Abfragen müssen weniger als 32 KB groß sein. Amazon Kendra durchsucht den gesamten Datenbankinhalt, der Ihrer Abfrage entspricht.
- Synchronisierungsmodus — Geben Sie an, wie Ihr Index aktualisiert Amazon Kendra werden soll, wenn sich der Inhalt Ihrer Datenquelle ändert. Wenn Sie Ihre Datenquelle Amazon Kendra zum ersten Mal synchronisieren, werden alle Inhalte standardmäßig gecrawlt und indexiert. Sie müssen eine vollständige Synchronisierung Ihrer Daten durchführen, falls Ihre erste Synchronisierung fehlgeschlagen ist, auch wenn Sie die Option Vollsynchronisierung nicht als Synchronisierungsmodusoption wählen. Sie können wählen zwischen:
  - `FORCED_FULL_CRAWL`um den gesamten Inhalt neu zu indizieren und vorhandene Inhalte jedes Mal zu ersetzen, wenn Ihre Datenquelle mit Ihrem Index synchronisiert wird.
  - `FULL_CRAWL`um bei jeder Synchronisierung Ihrer Datenquelle mit Ihrem Index nur neue, geänderte und gelöschte Inhalte zu indizieren. Amazon Kendra kann den Mechanismus Ihrer Datenquelle verwenden, um Inhaltsänderungen nachzuverfolgen und Inhalte zu indexieren, die sich seit der letzten Synchronisierung geändert haben.
  - `CHANGE_LOG`um jedes Mal, wenn Ihre Datenquelle mit Ihrem Index synchronisiert wird, nur neue und geänderte Inhalte zu indizieren. Amazon Kendra kann den Mechanismus Ihrer Datenquelle verwenden, um Inhaltsänderungen nachzuverfolgen und Inhalte zu indexieren, die sich seit der letzten Synchronisierung geändert haben.
- Geheimer Amazon-Ressourcenname (ARN) — Geben Sie den Amazon-Ressourcennamen (ARN) eines Secrets Manager Geheimnisses ein, das die Authentifizierungsdaten enthält, die Sie in Ihrem Aurora (MySQL) Konto erstellt haben. Das Geheimnis wird in einer JSON-Struktur mit den folgenden Schlüsseln gespeichert:

```
{
    "user name": "database user name",
    "password": "password"
}
```

> **Note**
>
> Wir empfehlen Ihnen, Ihre Anmeldeinformationen und Ihr Geheimnis regelmäßig zu aktualisieren oder zu wechseln. Stellen Sie zu Ihrer eigenen Sicherheit nur die Zugriffsebene bereit, die erforderlich ist. Wir raten davon ab, Anmeldeinformationen und geheime Daten für alle Datenquellen und Connector-Versionen 1.0 und 2.0 (sofern zutreffend) wiederzuverwenden.

- IAM Rolle — Geben Sie an`RoleArn`, wann Sie anrufen`CreateDataSource`, um einer IAM Rolle Berechtigungen für den Zugriff auf Ihr Secrets Manager Geheimnis und für den Aufruf der erforderlichen öffentlichen APIs für den Aurora (MySQL) Connector und zum Aufrufen der erforderlichen öffentlichen APIs zu erteilen. Amazon Kendra Weitere Informationen finden Sie unter IAM Rollen für Aurora (MySQL) Datenquellen.

Sie können auch die folgenden optionalen Funktionen hinzufügen:

- Virtual Private Cloud (VPC) — Geben Sie an, `VpcConfiguration` wann Sie anrufen. `CreateDataSource` Weitere Informationen finden Sie unter Konfigurieren von Amazon Kendra für die Verwendung eines Amazon VPC.
- Inklusions- und Ausschlussfilter — Sie können mithilfe von Benutzer-IDs, Gruppen, Quell-URLs, Zeitstempeln und Zeitzonen angeben, ob bestimmte Inhalte eingeschlossen werden sollen.
- Benutzerkontextfilterung und Zugriffskontrolle —Amazon Kendra durchsucht die Zugriffskontrollliste (ACL) für Ihre Dokumente, sofern Sie über eine ACL für Ihre Dokumente verfügen. Die ACL-Informationen werden verwendet, um Suchergebnisse nach dem Benutzer- oder Gruppenzugriff auf Dokumente zu filtern. Weitere Informationen finden Sie unter Benutzerkontextfilterung.
- Feldzuordnungen — Wählen Sie diese Option, um Ihre Aurora (MySQL) Datenquellenfelder Ihren Indexfeldern zuzuordnen. Amazon Kendra Weitere Informationen finden Sie unter Zuweisen von Datenquellenfeldern.

> **Note**
>
> Das Textfeld oder das entsprechende Textfeld für Ihre Dokumente ist erforderlich, um Ihre Dokumente durchsuchen Amazon Kendra zu können. Sie müssen den

Feldnamen Ihres Dokumenthauptteils in Ihrer Datenquelle dem Namen des Indexfeldes zuordnen_document_body. Alle anderen Felder sind optional.

Eine Liste weiterer wichtiger JSON-Schlüssel, die konfiguriert werden müssen, finden Sie unterAurora (MySQL) Vorlagenschema.

Hinweise

- Gelöschte Datenbankzeilen werden nicht nachverfolgt, wenn nach Amazon Kendra aktualisierten Inhalten gesucht wird.
- Die Größe von Feldnamen und Werten in einer Zeile Ihrer Datenbank darf 400 KB nicht überschreiten.
- Wenn Ihre Datenbankdatenquelle eine große Datenmenge enthält und Sie nicht möchten Amazon Kendra , dass Ihr gesamter Datenbankinhalt nach der ersten Synchronisierung indexiert wird, können Sie wählen, ob nur neue, geänderte oder gelöschte Dokumente synchronisiert werden sollen.
- Es hat sich bewährt, nur lesbare Amazon Kendra Datenbankanmeldeinformationen zur Verfügung zu stellen.
- Es hat sich bewährt, das Hinzufügen von Tabellen mit sensiblen Daten oder personenbezogenen Daten (PII) zu vermeiden.

Aurora (PostgreSQL)

Aurora ist ein relationales Datenbankmanagementsystem (RDBMS), das für die Cloud entwickelt wurde. Wenn Sie ein Aurora Benutzer sind, können Sie es verwenden, um Ihre Aurora (PostgreSQL) Datenquelle Amazon Kendra zu indizieren. Der Amazon Kendra Aurora (PostgreSQL) Datenquellenconnector unterstützt Aurora PostgreSQL 1.

Sie können über Amazon Kendra die Amazon Kendra Konsole und die API eine Verbindung zu Ihrer Aurora (PostgreSQL) Datenquelle herstellen. TemplateConfiguration

Informationen zur Fehlerbehebung bei Ihrem Amazon Kendra Aurora (PostgreSQL) Datenquellen-Connector finden Sie unterProblembehandlung bei Datenquellen.

Themen

Unterstützte Features

- Feldzuordnungen
- Filterung des Benutzerkontextes
- Einschluss-/Ausschlussfilter
- Vollständige und inkrementelle Inhaltssynchronisierung
- Virtual Private Cloud (VPC)

Voraussetzungen

Bevor Sie Ihre Aurora (PostgreSQL) Datenquelle Amazon Kendra zum Indizieren verwenden können, nehmen Sie diese Änderungen in Ihren Konten Aurora (PostgreSQL) und AWS Konten vor.

Stellen Sie sicherAurora (PostgreSQL), dass Sie Folgendes haben:

- Haben Sie sich Ihren Datenbank-Benutzernamen und Ihr Passwort notiert.

> **Important**
>
> Es hat sich bewährt, nur lesbare Amazon Kendra Datenbankanmeldeinformationen zur Verfügung zu stellen.

- Die URL, der Port und die Instanz Ihres Datenbank-Hosts wurden kopiert.
- Vergewissert, dass jedes Dokument in Aurora (PostgreSQL) und zwischen anderen Datenquellen, die Sie für denselben Index verwenden möchten, einzigartig ist. Jede Datenquelle, die Sie für einen Index verwenden möchten, darf nicht dasselbe Dokument in allen Datenquellen enthalten. Dokument-IDs gelten für einen Index global und müssen pro Index eindeutig sein.

Stellen Sie sicher AWS-Konto, dass Sie Folgendes in Ihrem haben:

- Hat einen Amazon Kendra Index erstellt und bei Verwendung der API die Index-ID notiert.

- Sie haben eine IAM Rolle für Ihre Datenquelle erstellt und, falls Sie die API verwenden, den ARN der IAM Rolle notiert.

> **Note**
>
> Wenn Sie Ihren Authentifizierungstyp und Ihre Anmeldeinformationen ändern, müssen Sie Ihre IAM Rolle aktualisieren, um auf die richtige AWS Secrets Manager geheime ID zugreifen zu können.

- Wir haben Ihre Aurora (PostgreSQL) Authentifizierungsdaten AWS Secrets Manager geheim gespeichert und, falls Sie die API verwenden, den ARN des Geheimnisses notiert.

> **Note**
>
> Wir empfehlen Ihnen, Ihre Anmeldeinformationen und Ihr Geheimnis regelmäßig zu aktualisieren oder zu wechseln. Stellen Sie zu Ihrer eigenen Sicherheit nur die Zugriffsebene bereit, die erforderlich ist. Wir raten davon ab, Anmeldeinformationen und geheime Daten für alle Datenquellen und Connector-Versionen 1.0 und 2.0 (sofern zutreffend) wiederzuverwenden.

Wenn Sie noch keine IAM Rolle oder keinen Schlüssel haben, können Sie die Konsole verwenden, um eine neue IAM Rolle und ein neues Secrets Manager Geheimnis zu erstellen, wenn Sie Ihre Aurora (PostgreSQL) Datenquelle mit verbinden. Amazon Kendra Wenn Sie die API verwenden, müssen Sie den ARN einer vorhandenen IAM Rolle und eines Secrets Manager Geheimnisses sowie eine Index-ID angeben.

Anweisungen zur Verbindung

Um eine Verbindung Amazon Kendra zu Ihrer Aurora (PostgreSQL) Datenquelle herzustellen, müssen Sie Details zu Ihren Aurora (PostgreSQL) Anmeldeinformationen angeben, damit Sie auf Ihre Daten zugreifen Amazon Kendra können. Falls Sie das noch nicht konfiguriert haben, Amazon Kendra sehen Sie Aurora (PostgreSQL) nachVoraussetzungen.

Console

Um eine Verbindung Amazon Kendra herzustellen Aurora (PostgreSQL)

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die Amazon Kendra Konsole.
2. Wählen Sie im linken Navigationsbereich Indizes und dann den Index, den Sie verwenden möchten, aus der Indexliste aus.

> **Note**
>
> Sie können Ihre Einstellungen für die Benutzerzugriffskontrolle unter Indexeinstellungen konfigurieren oder bearbeiten.

3. Wählen Sie auf der Seite Erste Schritte die Option Datenquelle hinzufügen aus.
4. Wählen Sie auf der Seite Datenquelle hinzufügen die Option Aurora (PostgreSQL)Connector und dann Connector hinzufügen aus.
5. Geben Sie auf der Seite „Datenquellendetails angeben“ die folgenden Informationen ein:
   a. Geben Sie im Feld Name und Beschreibung für Datenquellenname einen Namen für Ihre Datenquelle ein. Sie können Bindestriche, aber keine Leerzeichen verwenden.
   b. (Optional) Beschreibung — Geben Sie eine optionale Beschreibung für Ihre Datenquelle ein.
   c. In Standardsprache — Wählen Sie eine Sprache aus, um Ihre Dokumente nach dem Index zu filtern. Sofern Sie nichts anderes angeben, ist die Standardsprache Englisch. Die in den Metadaten des Dokuments angegebene Sprache hat Vorrang vor der ausgewählten Sprache.
   d. Unter Tags für Neues Tag hinzufügen — Fügen Sie optionale Tags hinzu, um Ihre Ressourcen zu durchsuchen und zu filtern oder Ihre Kosten nachzuverfolgen. AWS
   e. Wählen Sie Weiter aus.
6. Geben Sie auf der Seite Zugriff und Sicherheit definieren die folgenden Informationen ein:
   a. Geben Sie im Feld Quelle die folgenden Informationen ein:
   b. Host — Geben Sie die URL des Datenbank-Hosts ein, zum Beispiel:`http://`*`instance URL`*`.`*`region`*`.rds.amazonaws.com`.
   c. Port — Geben Sie den Datenbankport ein, zum Beispiel`5432`.
   d. Instanz — Geben Sie zum Beispiel die Datenbankinstanz ein`postgres`.
   e. Speicherort für SSL-Zertifikate aktivieren — Geben Sie hier den Amazon S3 Pfad zu Ihrer SSL-Zertifikatsdatei ein.

f. Geben Sie im Feld Authentifizierung die folgenden Informationen ein:

- AWS Secrets Manager geheim — Wählen Sie ein vorhandenes Geheimnis aus, oder erstellen Sie ein neues Secrets Manager Geheimnis, um Ihre Aurora (PostgreSQL) Authentifizierungsdaten zu speichern. Wenn Sie ein neues Geheimnis erstellen möchten, wird ein AWS Secrets Manager geheimes Fenster geöffnet.

  A. Geben Sie die folgenden Informationen in das Fenster Create an AWS Secrets Manager Secret ein:

     I. Geheimer Name — Ein Name für Ihr Geheimnis. Das Präfix 'AmazonKendra- Aurora (PostgreSQL) -' wird Ihrem geheimen Namen automatisch hinzugefügt.

     II. Für Datenbankbenutzername und Passwort — Geben Sie die Werte der Authentifizierungsdaten ein, die Sie aus Ihrer Datenbank kopiert haben.

  B. Wählen Sie Speichern.

g. Virtual Private Cloud (VPC) — Sie können wählen, ob Sie eine VPC verwenden möchten. In diesem Fall müssen Sie Subnetze und VPC-Sicherheitsgruppen hinzufügen.

h. IAM Rolle — Wählen Sie eine bestehende IAM Rolle oder erstellen Sie eine neue IAM Rolle, um auf Ihre Repository-Anmeldeinformationen und Indexinhalte zuzugreifen.

> **Note**
>
> IAM Rollen, die für Indizes verwendet werden, können nicht für Datenquellen verwendet werden. Wenn Sie sich nicht sicher sind, ob eine vorhandene Rolle für einen Index oder eine häufig gestellte Frage verwendet wird, wählen Sie Neue Rolle erstellen, um Fehler zu vermeiden.

i. Wählen Sie Weiter aus.

7. Geben Sie auf der Seite „Synchronisierungseinstellungen konfigurieren“ die folgenden Informationen ein:

a. Wählen Sie unter Synchronisierungsbereich eine der folgenden Optionen aus:

- SQL-Abfrage — Geben Sie SQL-Abfrageanweisungen wie SELECT- und JOIN-Operationen ein. SQL-Abfragen müssen weniger als 32 KB groß sein. SQL-Abfragen müssen weniger als 32 KB groß sein und dürfen keine Semikolons (;) enthalten.

Amazon Kendra durchsucht den gesamten Datenbankinhalt, der Ihrer Abfrage entspricht.

- Primärschlüsselspalte — Geben Sie den Primärschlüssel für die Datenbanktabelle an. Dies identifiziert eine Tabelle in Ihrer Datenbank.
- Titelspalte — Geben Sie den Namen der Titelspalte des Dokuments in Ihrer Datenbanktabelle an.
- Hauptspalte — Geben Sie den Namen der Hauptspalte des Dokuments in Ihrer Datenbanktabelle an.

b. Wählen Sie unter Zusätzliche Konfiguration — optional aus den folgenden Optionen, um bestimmte Inhalte zu synchronisieren, anstatt alle Dateien zu synchronisieren:

- Spalten zur Erkennung von Änderungen — Geben Sie die Namen der Spalten ein, anhand derer Inhaltsänderungen erkannt Amazon Kendra werden sollen. Amazon Kendra indexiert den Inhalt neu, wenn sich eine dieser Spalten ändert.
- Spalte mit Benutzer-IDs — Geben Sie den Namen der Spalte ein, die Benutzer-IDs enthält, um Zugriff auf Inhalte zu erhalten.
- Spalte „Gruppen“ — Geben Sie den Namen der Spalte ein, die Gruppen enthält, denen der Zugriff auf Inhalte gewährt werden soll.
- Spalte Quell-URLs — Geben Sie den Namen der Spalte ein, die Quell-URLs enthält, die indexiert werden sollen.
- Spalte mit Zeitstempeln — Geben Sie den Namen der Spalte ein, die Zeitstempel enthält. Amazon Kendra verwendet Zeitstempelinformationen, um Änderungen an Ihren Inhalten zu erkennen und nur geänderte Inhalte zu synchronisieren.
- Spalte „Zeitzonen“ — Geben Sie den Namen der Spalte ein, die Zeitzonen für den Inhalt enthält, der gecrawlt werden soll.
- Zeitstempelformat — Geben Sie den Namen der Spalte ein, die Zeitstempelformate enthält, anhand derer Inhaltsänderungen erkannt und Ihre Inhalte erneut synchronisiert werden sollen.

c. Synchronisierungsmodus — Wählen Sie aus, wie Sie Ihren Index aktualisieren möchten, wenn sich der Inhalt Ihrer Datenquelle ändert. Wenn Sie Ihre Datenquelle Amazon Kendra zum ersten Mal synchronisieren, werden alle Inhalte standardmäßig gecrawlt und indexiert. Sie müssen eine vollständige Synchronisierung Ihrer Daten durchführen, falls Ihre erste Synchronisierung fehlgeschlagen ist, auch wenn Sie die Option Vollsynchronisierung nicht als Synchronisierungsmodusoption wählen.

- Vollständige Synchronisierung: Indizieren Sie alle Inhalte neu und ersetzen vorhandene Inhalte jedes Mal, wenn Ihre Datenquelle mit Ihrem Index synchronisiert wird.
- Neue, geänderte Synchronisierung: Indizieren Sie bei jeder Synchronisierung Ihrer Datenquelle mit Ihrem Index nur neue und geänderte Inhalte. Amazon Kendra kann den Mechanismus Ihrer Datenquelle verwenden, um Inhaltsänderungen nachzuverfolgen und Inhalte zu indexieren, die sich seit der letzten Synchronisierung geändert haben.
- Neue, geänderte, gelöschte Synchronisierung: Indizieren Sie bei jeder Synchronisierung Ihrer Datenquelle mit Ihrem Index nur neue, geänderte und gelöschte Inhalte. Amazon Kendra kann den Mechanismus Ihrer Datenquelle verwenden, um Inhaltsänderungen nachzuverfolgen und Inhalte zu indexieren, die sich seit der letzten Synchronisierung geändert haben.

d. Im Synchronisierungslaufplan für Frequenz — Wie oft Amazon Kendra wird mit Ihrer Datenquelle synchronisiert?

e. Wählen Sie Weiter aus.

8. Geben Sie auf der Seite Feldzuordnungen festlegen die folgenden Informationen ein:

   a. Wählen Sie aus den generierten Standard-Datenquellenfeldern — Dokument-IDs, Dokumenttitel und Quell-URLs — aus, die Sie dem Index zuordnen möchten. Amazon Kendra

   b. Feld hinzufügen — Um benutzerdefinierte Datenquellenfelder hinzuzufügen, um einen Indexfeldnamen für die Zuordnung und den Felddatentyp zu erstellen.

   c. Wählen Sie Weiter aus.

9. Überprüfen Sie auf der Seite Überprüfen und erstellen, ob die von Ihnen eingegebenen Informationen korrekt sind, und wählen Sie dann Datenquelle hinzufügen aus. Sie können Ihre Informationen auch auf dieser Seite bearbeiten. Ihre Datenquelle wird auf der Seite Datenquellen angezeigt, nachdem die Datenquelle erfolgreich hinzugefügt wurde.

API

Um eine Verbindung Amazon Kendra herzustellen Aurora (PostgreSQL)

Mithilfe der TemplateConfigurationAPI müssen Sie Folgendes angeben:

- Datenquelle — Geben Sie den Datenquellentyp wie `JDBC` bei der Verwendung des TemplateConfigurationJSON-Schemas an. Geben Sie außerdem die Datenquelle so an`TEMPLATE`, wie Sie die CreateDataSourceAPI aufrufen.
- Datenbanktyp — Sie müssen den Datenbanktyp als `postgresql` angeben.
- SQL-Abfrage — Geben Sie SQL-Abfrageanweisungen wie SELECT- und JOIN-Operationen an. SQL-Abfragen müssen weniger als 32 KB groß sein. Amazon Kendra durchsucht den gesamten Datenbankinhalt, der Ihrer Abfrage entspricht.
- Synchronisierungsmodus — Geben Sie an, wie Ihr Index aktualisiert Amazon Kendra werden soll, wenn sich der Inhalt Ihrer Datenquelle ändert. Wenn Sie Ihre Datenquelle Amazon Kendra zum ersten Mal synchronisieren, werden alle Inhalte standardmäßig gecrawlt und indexiert. Sie müssen eine vollständige Synchronisierung Ihrer Daten durchführen, falls Ihre erste Synchronisierung fehlgeschlagen ist, auch wenn Sie die Option Vollsynchronisierung nicht als Synchronisierungsmodusoption wählen. Sie können wählen zwischen:
  - `FORCED_FULL_CRAWL`um den gesamten Inhalt neu zu indizieren und vorhandene Inhalte jedes Mal zu ersetzen, wenn Ihre Datenquelle mit Ihrem Index synchronisiert wird.
  - `FULL_CRAWL`um bei jeder Synchronisierung Ihrer Datenquelle mit Ihrem Index nur neue, geänderte und gelöschte Inhalte zu indizieren. Amazon Kendra kann den Mechanismus Ihrer Datenquelle verwenden, um Inhaltsänderungen nachzuverfolgen und Inhalte zu indexieren, die sich seit der letzten Synchronisierung geändert haben.
  - `CHANGE_LOG`um jedes Mal, wenn Ihre Datenquelle mit Ihrem Index synchronisiert wird, nur neue und geänderte Inhalte zu indizieren. Amazon Kendra kann den Mechanismus Ihrer Datenquelle verwenden, um Inhaltsänderungen nachzuverfolgen und Inhalte zu indexieren, die sich seit der letzten Synchronisierung geändert haben.
- Geheimer Amazon-Ressourcenname (ARN) — Geben Sie den Amazon-Ressourcennamen (ARN) eines Secrets Manager Geheimnisses ein, das die Authentifizierungsdaten enthält, die Sie in Ihrem Aurora (PostgreSQL) Konto erstellt haben. Das Geheimnis wird in einer JSON-Struktur mit den folgenden Schlüsseln gespeichert:

```
{
    "user name": "database user name",
    "password": "password"
}
```

> **Note**
>
> Wir empfehlen Ihnen, Ihre Anmeldeinformationen und Ihr Geheimnis regelmäßig zu aktualisieren oder zu wechseln. Stellen Sie zu Ihrer eigenen Sicherheit nur die Zugriffsebene bereit, die erforderlich ist. Wir raten davon ab, Anmeldeinformationen und geheime Daten für alle Datenquellen und Connector-Versionen 1.0 und 2.0 (sofern zutreffend) wiederzuverwenden.

- IAM Rolle — Geben Sie an`RoleArn`, wann Sie anrufen`CreateDataSource`, um einer IAM Rolle Berechtigungen für den Zugriff auf Ihr Secrets Manager Geheimnis und für den Aufruf der erforderlichen öffentlichen APIs für den Aurora (PostgreSQL) Connector und zum Aufrufen der erforderlichen öffentlichen APIs zu erteilen. Amazon Kendra Weitere Informationen finden Sie unter IAM Rollen für Aurora (PostgreSQL) Datenquellen.

Sie können auch die folgenden optionalen Funktionen hinzufügen:

- Virtual Private Cloud (VPC) — Geben Sie an, `VpcConfiguration` wann Sie anrufen. `CreateDataSource` Weitere Informationen finden Sie unter Konfigurieren von Amazon Kendra für die Verwendung eines Amazon VPC.
- Inklusions- und Ausschlussfilter — Sie können mithilfe von Benutzer-IDs, Gruppen, Quell-URLs, Zeitstempeln und Zeitzonen angeben, ob bestimmte Inhalte eingeschlossen werden sollen.
- Benutzerkontextfilterung und Zugriffskontrolle —Amazon Kendra durchsucht die Zugriffskontrollliste (ACL) für Ihre Dokumente, sofern Sie über eine ACL für Ihre Dokumente verfügen. Die ACL-Informationen werden verwendet, um Suchergebnisse nach dem Benutzer- oder Gruppenzugriff auf Dokumente zu filtern. Weitere Informationen finden Sie unter Benutzerkontextfilterung.
- Feldzuordnungen — Wählen Sie diese Option, um Ihre Aurora (PostgreSQL) Datenquellenfelder Ihren Indexfeldern zuzuordnen. Amazon Kendra Weitere Informationen finden Sie unter Zuweisen von Datenquellenfeldern.

> **Note**
>
> Das Textfeld oder das entsprechende Textfeld für Ihre Dokumente ist erforderlich, um Ihre Dokumente durchsuchen Amazon Kendra zu können. Sie müssen den

Feldnamen Ihres Dokumenthauptteils in Ihrer Datenquelle dem Namen des Indexfeldes zuordnen_document_body. Alle anderen Felder sind optional.

Eine Liste weiterer wichtiger JSON-Schlüssel, die konfiguriert werden müssen, finden Sie unterAurora (PostgreSQL) -Vorlagenschema.

Hinweise

- Gelöschte Datenbankzeilen werden nicht nachverfolgt, wenn nach Amazon Kendra aktualisierten Inhalten gesucht wird.
- Die Größe von Feldnamen und Werten in einer Zeile Ihrer Datenbank darf 400 KB nicht überschreiten.
- Wenn Ihre Datenbankdatenquelle eine große Datenmenge enthält und Sie nicht möchten Amazon Kendra , dass Ihr gesamter Datenbankinhalt nach der ersten Synchronisierung indexiert wird, können Sie wählen, ob nur neue, geänderte oder gelöschte Dokumente synchronisiert werden sollen.
- Es hat sich bewährt, nur lesbare Amazon Kendra Datenbankanmeldeinformationen zur Verfügung zu stellen.
- Es hat sich bewährt, das Hinzufügen von Tabellen mit sensiblen Daten oder personenbezogenen Daten (PII) zu vermeiden.

Amazon FSx (Fenster)

Amazon FSx (Windows) ist ein vollständig verwaltetes, Cloud-basiertes Dateiserversystem, das gemeinsam genutzte Speicherfunktionen bietet. Wenn Sie ein Amazon FSx (Windows-) Benutzer sind, können Sie Amazon Kendra damit Ihre Amazon FSx (Windows-) Datenquelle indizieren.

Note

Amazon Kendra unterstützt jetzt einen aktualisierten Amazon FSx (Windows-) Connector. Die Konsole wurde automatisch für Sie aktualisiert. Alle neuen Connectors, die Sie auf der Konsole erstellen, verwenden die aktualisierte Architektur. Wenn Sie die API verwenden, müssen Sie jetzt das TemplateConfigurationObjekt anstelle des FSxConfiguration Objekts verwenden, um Ihren Connector zu konfigurieren.

Konnektoren, die mit der älteren Konsolen- und API-Architektur konfiguriert wurden, funktionieren weiterhin wie konfiguriert. Sie können sie jedoch nicht bearbeiten oder aktualisieren. Wenn Sie Ihre Connectorkonfiguration bearbeiten oder aktualisieren möchten, müssen Sie einen neuen Connector erstellen.
Wir empfehlen, Ihren Connector-Workflow auf die aktualisierte Version zu migrieren. Die Support für Konnektoren, die mit der älteren Architektur konfiguriert wurden, soll bis Juni 2024 eingestellt werden.

Sie können über Amazon Kendra die Amazon Kendra Konsole oder die TemplateConfigurationAPI eine Verbindung zu Ihrer Amazon FSx (Windows-) Datenquelle herstellen.

Informationen zur Problembehandlung Ihres Amazon Kendra Amazon FSx (Windows-) Datenquellen-Connectors finden Sie unterProblembehandlung bei Datenquellen.

Themen

- Unterstützte Features
- Voraussetzungen
- Anweisungen zur Verbindung
- Weitere Informationen

Unterstützte Features

Amazon Kendra Amazon FSx Der (Windows-) Datenquellenconnector unterstützt die folgenden Funktionen:

- Feldzuordnungen
- Steuerung des Benutzerzugriffs
- Crawling der Benutzeridentität
- Inklusions- und Ausschlussfilter
- Vollständige und inkrementelle Inhaltssynchronisierung
- Virtual Private Cloud (VPC)

Voraussetzungen

Bevor Sie Ihre Amazon FSx (Windows-) Datenquelle Amazon Kendra zum Indizieren verwenden können, überprüfen Sie die Details Ihrer Amazon FSx (Windows) und. AWS-Konten

Stellen Sie für Amazon FSx (Windows) sicher, dass Sie über Folgendes verfügen:

- Richten Sie Amazon FSx (Windows) mit Lese- und Mount-Rechten ein.
- Notiert Ihre Dateisystem-ID. Sie finden Ihre Dateisystem-ID im Dateisystem-Dashboard in der Amazon FSx (Windows-) Konsole.
- Sie haben eine virtuelle private Cloud konfiguriert Amazon VPC , in der sich Ihr Amazon FSx (Windows-) Dateisystem befindet.
- Haben Ihre Amazon FSx (Windows-) Authentifizierungsdaten für ein Active Directory Benutzerkonto notiert. Dazu gehören Ihr Active Directory-Benutzername mit Ihrem DNS-Domänennamen (z. B. user@corp.example.com) und Ihrem Passwort.

  > **Note**
  >
  > Verwenden Sie nur die erforderlichen Anmeldeinformationen, damit der Connector funktioniert. Verwenden Sie keine privilegierten Anmeldeinformationen wie den Domänenadministrator.

- Vergewissert, dass jedes Dokument in Amazon FSx (Windows) und anderen Datenquellen, die Sie für denselben Index verwenden möchten, einzigartig ist. Jede Datenquelle, die Sie für einen Index verwenden möchten, darf nicht dasselbe Dokument in allen Datenquellen enthalten. Dokument-IDs gelten für einen Index global und müssen pro Index eindeutig sein.

Stellen Sie sicher AWS-Konto, dass Sie Folgendes in Ihrem haben:

- Hat einen Amazon Kendra Index erstellt und bei Verwendung der API die Index-ID notiert.
- Sie haben eine IAM Rolle für Ihre Datenquelle erstellt und, falls Sie die API verwenden, den ARN der IAM Rolle notiert.

> **Note**
>
> Wenn Sie Ihren Authentifizierungstyp und Ihre Anmeldeinformationen ändern, müssen Sie Ihre IAM Rolle aktualisieren, um auf die richtige AWS Secrets Manager geheime ID zugreifen zu können.

- Ihre Amazon FSx (Windows-) Authentifizierungsdaten AWS Secrets Manager geheim gespeichert und, falls Sie die API verwenden, den ARN des Geheimnisses notiert.

> **Note**
>
> Wir empfehlen Ihnen, Ihre Anmeldeinformationen und Ihr Geheimnis regelmäßig zu aktualisieren oder zu wechseln. Stellen Sie zu Ihrer eigenen Sicherheit nur die erforderliche Zugriffsebene bereit. Wir raten davon ab, Anmeldeinformationen und geheime Daten für alle Datenquellen und Connector-Versionen 1.0 und 2.0 (sofern zutreffend) wiederzuverwenden.

Wenn Sie noch keine IAM Rolle oder keinen Schlüssel haben, können Sie die Konsole verwenden, um eine neue IAM Rolle und ein neues Secrets Manager Geheimnis zu erstellen, wenn Sie Ihre Amazon FSx (Windows-) Datenquelle mit verbinden. Amazon Kendra Wenn Sie die API verwenden, müssen Sie den ARN einer vorhandenen IAM Rolle und eines Secrets Manager Geheimnisses sowie eine Index-ID angeben.

Anweisungen zur Verbindung

Um eine Verbindung Amazon Kendra zu Ihrer Amazon FSx (Windows-) Datenquelle herzustellen, müssen Sie die erforderlichen Details zu Ihrer Amazon FSx (Windows-) Datenquelle angeben, damit Sie auf Ihre Daten zugreifen Amazon Kendra können. Falls Sie Amazon FSx (Windows) noch nicht konfiguriert haben Amazon Kendra, finden Sie weitere Informationen unterVoraussetzungen.

Console

So stellen Sie eine Verbindung Amazon Kendra zu Ihrem Amazon FSx (Windows-) Dateisystem her

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die Amazon Kendra Konsole.

2. Wählen Sie im linken Navigationsbereich Indizes und dann den Index, den Sie verwenden möchten, aus der Indexliste aus.

> **Note**
>
> Sie können Ihre Einstellungen für die Benutzerzugriffskontrolle unter Indexeinstellungen konfigurieren oder bearbeiten.

3. Wählen Sie auf der Seite Erste Schritte die Option Datenquelle hinzufügen aus.
4. Wählen Sie auf der Seite Datenquelle hinzufügen die Option Amazon FSx (Windows) - Connector und dann Connector hinzufügen aus.
5. Geben Sie auf der Seite „Datenquellendetails angeben“ die folgenden Informationen ein:

   a. Geben Sie im Feld Name und Beschreibung für Datenquellenname einen Namen für Ihre Datenquelle ein. Sie können Bindestriche, aber keine Leerzeichen verwenden.

   b. (Optional) Beschreibung — Geben Sie eine optionale Beschreibung für Ihre Datenquelle ein.

   c. In Standardsprache — Wählen Sie eine Sprache aus, um Ihre Dokumente nach dem Index zu filtern. Sofern Sie nichts anderes angeben, ist die Standardsprache Englisch. Die in den Metadaten des Dokuments angegebene Sprache hat Vorrang vor der ausgewählten Sprache.

   d. Unter Tags für Neues Tag hinzufügen — Fügen Sie optionale Tags hinzu, um Ihre Ressourcen zu durchsuchen und zu filtern oder Ihre Kosten nachzuverfolgen. AWS

   e. Wählen Sie Weiter aus.

6. Geben Sie auf der Seite Zugriff und Sicherheit definieren die folgenden Informationen ein:

   a. Amazon FSx (Windows) Dateisystem-ID — Wählen Sie aus der Dropdownliste Ihre bestehende Dateisystem-ID aus, die von Amazon FSx (Windows) abgerufen wurde. Oder erstellen Sie ein Amazon FSx (Windows-) Dateisystem. Sie finden Ihre Dateisystem-ID im Dateisystem-Dashboard in der Amazon FSx (Windows-) Konsole.

   b. Autorisierung — Aktivieren oder deaktivieren Sie die Informationen der Zugriffskontrollliste (ACL) für Ihre Dokumente, wenn Sie über eine ACL verfügen und diese für die Zugriffskontrolle verwenden möchten. Die ACL gibt an, auf welche Dokumente Benutzer und Gruppen zugreifen können. Die ACL-Informationen werden verwendet, um Suchergebnisse nach dem Benutzer- oder Gruppenzugriff auf Dokumente zu filtern. Weitere Informationen finden Sie unter Benutzerkontextfilterung.

c. Authentifizierung — Wählen Sie ein vorhandenes AWS Secrets Manager Geheimnis aus, oder erstellen Sie ein neues Geheimnis, um Ihre Dateisystem-Anmeldeinformationen zu speichern. Wenn Sie sich dafür entscheiden, ein neues Geheimnis zu erstellen, wird ein AWS Secrets Manager geheimes Fenster geöffnet.

   Geben Sie ein Geheimnis ein, in dem Ihre Authentifizierungsdaten mit Ihrem Benutzernamen und Passwort gespeichert werden. Der Benutzername muss Ihren DNS-Domainnamen enthalten. Zum Beispiel user@corp.example.com.

   Speichern Sie Ihr Geheimnis und fügen Sie es hinzu.

d. Virtual Private Cloud (VPC) — Sie müssen einen Standort auswählen, an Amazon VPC dem sich Ihr Amazon FSx (Windows) befindet. Sie schließen das VPC-Subnetz und die Sicherheitsgruppen ein. Siehe Konfiguration eines. Amazon VPC

e. IAM Rolle — Wählen Sie eine bestehende IAM Rolle oder erstellen Sie eine neue IAM Rolle, um auf Ihre Repository-Anmeldeinformationen und Indexinhalte zuzugreifen.

   > **Note**
   >
   > IAM Rollen, die für Indizes verwendet werden, können nicht für Datenquellen verwendet werden. Wenn Sie sich nicht sicher sind, ob eine vorhandene Rolle für einen Index oder eine häufig gestellte Frage verwendet wird, wählen Sie Neue Rolle erstellen, um Fehler zu vermeiden.

f. Wählen Sie Weiter aus.

7. Geben Sie auf der Seite „Synchronisierungseinstellungen konfigurieren“ die folgenden Informationen ein:

   a. Synchronisierungsbereich, Regex-Muster — Fügen Sie Muster für reguläre Ausdrücke hinzu, um bestimmte Dateien ein- oder auszuschließen.

   b. Synchronisierungsmodus — Wählen Sie aus, wie Sie Ihren Index aktualisieren möchten, wenn sich der Inhalt Ihrer Datenquelle ändert. Wenn Sie Ihre Datenquelle Amazon Kendra zum ersten Mal synchronisieren, werden alle Inhalte standardmäßig gecrawlt und indexiert. Sie müssen eine vollständige Synchronisierung Ihrer Daten durchführen, falls Ihre erste Synchronisierung fehlgeschlagen ist, auch wenn Sie die Option Vollsynchronisierung nicht als Synchronisierungsmodusoption wählen.

- Vollständige Synchronisierung: Indizieren Sie den gesamten Inhalt neu und ersetzen die vorhandenen Inhalte jedes Mal, wenn Ihre Datenquelle mit Ihrem Index synchronisiert wird.
- Neue, geänderte, gelöschte Synchronisierung: Indizieren Sie bei jeder Synchronisierung Ihrer Datenquelle mit Ihrem Index nur neue, geänderte und gelöschte Inhalte. Amazon Kendra kann den Mechanismus Ihrer Datenquelle verwenden, um Inhaltsänderungen nachzuverfolgen und Inhalte zu indexieren, die sich seit der letzten Synchronisierung geändert haben.

c. Zeitplan für Synchronisierungsläufe — Wählen Sie unter Häufigkeit aus, wie oft Ihre Datenquelleninhalte synchronisiert und Ihr Index aktualisiert werden soll.

d. Wählen Sie Weiter aus.

8. Geben Sie auf der Seite Feldzuordnungen festlegen die folgenden Informationen ein:

   a. Wählen Sie aus den Amazon Kendra generierten Standardfeldern Ihrer Dateien aus, die Sie Ihrem Index zuordnen möchten. Um benutzerdefinierte Datenquellenfelder hinzuzufügen, erstellen Sie einen Indexfeldnamen für die Zuordnung und den Felddatentyp.

   b. Wählen Sie Weiter aus.

9. Überprüfen Sie auf der Seite Überprüfen und erstellen, ob die von Ihnen eingegebenen Informationen korrekt sind, und wählen Sie dann Datenquelle hinzufügen aus. Sie können Ihre Informationen auch auf dieser Seite bearbeiten. Ihre Datenquelle wird auf der Seite Datenquellen angezeigt, nachdem die Datenquelle erfolgreich hinzugefügt wurde.

API

Um eine Verbindung Amazon Kendra zu Ihrem Amazon FSx (Windows-) Dateisystem herzustellen

Sie müssen mithilfe der TemplateConfigurationAPI eine JSON-Datei des Datenquellenschemas angeben. Sie müssen die folgenden Informationen angeben:

- Datenquelle — Geben Sie den Datenquellentyp wie `FSX` bei der Verwendung des TemplateConfigurationJSON-Schemas an. Geben Sie außerdem die Datenquelle so an`TEMPLATE`, wie Sie die CreateDataSourceAPI aufrufen.
- Dateisystem-ID — Die Kennung des Amazon FSx (Windows-) Dateisystems. Sie finden Ihre Dateisystem-ID im Dateisystem-Dashboard in der Amazon FSx (Windows-) Konsole.

- Dateisystemtyp — Geben Sie den Typ des Dateisystems als `WINDOWS` an.
- Virtual Private Cloud (VPC) — Geben Sie an, `VpcConfiguration` wann Sie anrufen. `CreateDataSource` Weitere Informationen finden Sie unter Konfigurieren von Amazon Kendra für die Verwendung eines Amazon VPC.

  > **Note**
  >
  > Sie müssen einen Standort auswählen Amazon VPC , an dem sich Ihr Amazon FSx (Windows) befindet. Sie schließen das VPC-Subnetz und die Sicherheitsgruppen ein.

- Synchronisierungsmodus — Geben Sie an, wie Ihr Index aktualisiert Amazon Kendra werden soll, wenn sich der Inhalt Ihrer Datenquelle ändert. Wenn Sie Ihre Datenquelle Amazon Kendra zum ersten Mal synchronisieren, werden alle Inhalte standardmäßig gecrawlt und indexiert. Sie müssen eine vollständige Synchronisierung Ihrer Daten durchführen, falls Ihre erste Synchronisierung fehlgeschlagen ist, auch wenn Sie die Option Vollsynchronisierung nicht als Synchronisierungsmodusoption wählen. Sie können wählen zwischen:
  - `FORCED_FULL_CRAWL`um den gesamten Inhalt neu zu indizieren und vorhandene Inhalte jedes Mal zu ersetzen, wenn Ihre Datenquelle mit Ihrem Index synchronisiert wird.
  - `FULL_CRAWL`um bei jeder Synchronisierung Ihrer Datenquelle mit Ihrem Index nur neue, geänderte und gelöschte Inhalte zu indizieren. Amazon Kendra kann den Mechanismus Ihrer Datenquelle verwenden, um Inhaltsänderungen nachzuverfolgen und Inhalte zu indexieren, die sich seit der letzten Synchronisierung geändert haben.
- Identity Crawler — Geben Sie an, ob der Identity Crawler aktiviert Amazon Kendra werden soll. Der Identity Crawler verwendet die Informationen der Zugriffskontrollliste (ACL) für Ihre Dokumente, um Suchergebnisse nach dem Benutzer- oder Gruppenzugriff auf Dokumente zu filtern. Wenn Sie über eine ACL für Ihre Dokumente verfügen und Ihre ACL verwenden möchten, können Sie auch den Identity Crawler aktivieren, um die Benutzerkontextfilterung der Suchergebnisse zu konfigurieren. Amazon Kendra Andernfalls können alle Dokumente öffentlich durchsucht werden, wenn Identity Crawler ausgeschaltet ist. Wenn Sie die Zugriffskontrolle für Ihre Dokumente verwenden möchten und Identity Crawler ausgeschaltet ist, können Sie alternativ die PutPrincipalMappingAPI verwenden, um Benutzer- und Gruppenzugriffsinformationen für die Benutzerkontextfilterung hochzuladen.
- Geheimer Amazon-Ressourcenname (ARN) — Geben Sie den Amazon-Ressourcennamen (ARN) eines Secrets Manager Geheimnisses ein, das die Authentifizierungsdaten für Ihr Amazon FSx (Windows-) Konto enthält. Das Geheimnis wird in einer JSON-Struktur mit den folgenden Schlüsseln gespeichert:

```
{
    "username": "user@corp.example.com",
    "password": "password"
}
```

- IAM role — Geben Sie an`RoleArn`, wann Sie aufrufen`CreateDataSource`, um einer IAM Rolle Berechtigungen für den Zugriff auf Ihr Secrets Manager Geheimnis und den Aufruf der erforderlichen öffentlichen APIs für den Amazon FSx (Windows-) Connector und Amazon Kendra zu erteilen. Weitere Informationen finden Sie unter IAM Rollen für Amazon FSx (Windows-) Datenquellen.

Sie können auch die folgenden optionalen Funktionen hinzufügen:

- Inklusions- und Ausschlussfilter — Geben Sie an, ob bestimmte Dateien ein- oder ausgeschlossen werden sollen.

> **Note**
>
> Die meisten Datenquellen verwenden Muster mit regulären Ausdrücken, bei denen es sich um Ein- oder Ausschlussmuster handelt, die als Filter bezeichnet werden. Wenn Sie einen Einschlussfilter angeben, werden nur Inhalte indexiert, die dem Einschlussfilter entsprechen. Jedes Dokument, das nicht dem Einschlussfilter entspricht, wird nicht indexiert. Wenn Sie einen Ein- und Ausschlussfilter angeben, werden Dokumente, die dem Ausschlussfilter entsprechen, nicht indexiert, auch wenn sie dem Einschlussfilter entsprechen.

- Zugriffskontrollliste (ACL) — Geben Sie an, ob die ACL-Informationen für Ihre Dokumente gecrawlt werden sollen, wenn Sie über eine ACL verfügen und diese für die Zugriffskontrolle verwenden möchten. Die ACL gibt an, auf welche Dokumente Benutzer und Gruppen zugreifen können. Die ACL-Informationen werden verwendet, um Suchergebnisse nach dem Benutzer- oder Gruppenzugriff auf Dokumente zu filtern. Weitere Informationen finden Sie unter Benutzerkontextfilterung.

> **Note**
>
> Um die Benutzerkontextfilterung für einen Benutzer zu testen, müssen Sie den DNS-Domänennamen als Teil des Benutzernamens angeben, wenn Sie die Abfrage

ausgeben. Sie müssen über Administratorrechte für die Active Directory-Domäne verfügen. Sie können die Benutzerkontextfilterung auch anhand eines Gruppennamens testen.

- Feldzuordnungen — Wählen Sie, ob Sie Ihre Amazon FSx (Windows-) Datenquellenfelder Ihren Amazon Kendra Indexfeldern zuordnen möchten. Weitere Informationen finden Sie unter Zuweisen von Datenquellenfeldern.

> **Note**
>
> Das Textfeld oder das entsprechende Textfeld für Ihre Dokumente ist erforderlich, um Ihre Dokumente durchsuchen Amazon Kendra zu können. Sie müssen den Feldnamen Ihres Dokumenthauptteils in Ihrer Datenquelle dem Namen des Indexfeldes zuordnen `_document_body`. Alle anderen Felder sind optional.

Eine Liste weiterer wichtiger JSON-Schlüssel, die konfiguriert werden müssen, finden Sie unter Amazon FSx (Windows) -Vorlagenschema.

Weitere Informationen

Weitere Informationen zur Integration Amazon Kendra mit Ihrer Amazon FSx (Windows-) Datenquelle finden Sie unter:

- Suchen Sie sicher nach unstrukturierten Daten auf Windows-Dateisystemen mit dem Amazon Kendra Connector für Amazon FSx (Windows) für Windows File Server.

Amazon FSx (IM NetApp TAP)

Amazon FSx (NetApp ONTAP) ist ein vollständig verwaltetes, Cloud-basiertes Dateiserversystem, das gemeinsam genutzte Speicherfunktionen bietet. Wenn Sie ein Amazon FSx (NetApp ONTAP-) Benutzer sind, können Sie Amazon Kendra damit Ihre Amazon FSx (NetApp ONTAP-) Datenquelle indizieren.

Sie können über Amazon Kendra die Amazon Kendra Konsole oder die API eine Verbindung zu Ihrer Amazon FSx (NetApp ONTAP-) Datenquelle herstellen. TemplateConfiguration

Informationen zur Fehlerbehebung bei Ihrem Amazon Kendra Amazon FSx (NetApp ONTAP-) Datenquellenconnector finden Sie unter. Problembehandlung bei Datenquellen

Themen

Unterstützte Features

Amazon Kendra Amazon FSx Der (NetApp ONTAP) -Datenquellen-Connector unterstützt die folgenden Funktionen:

- Feldzuordnungen
- Steuerung des Benutzerzugriffs
- Inklusions- und Ausschlussfilter
- Vollständige und inkrementelle Inhaltssynchronisierung
- Virtual Private Cloud (VPC)

Voraussetzungen

Bevor Sie Ihre Amazon FSx (NetApp ONTAP-) Datenquelle Amazon Kendra zum Indizieren verwenden können, überprüfen Sie die Details Ihrer Amazon FSx (NetApp ONTAP) und. AWS-Konten

Stellen Sie für Amazon FSx (NetApp ONTAP) sicher, dass Sie über Folgendes verfügen:

- Richten Sie Amazon FSx (NetApp ONTAP) mit Lese- und Montageberechtigungen ein.
- Notiert Ihre Dateisystem-ID. Sie finden Ihre Dateisystem-ID im Dateisystem-Dashboard in der Amazon FSx (NetApp ONTAP-) Konsole.
- Notiert die SVM-ID (Storage Virtual Machine), die mit Ihrem Dateisystem verwendet wird. Sie finden Ihre SVM-ID, indem Sie das Dateisystem-Dashboard in der Amazon FSx (NetApp ONTAP-) Konsole aufrufen, Ihre Dateisystem-ID und dann virtuelle Speichermaschinen auswählen.
- Sie haben eine virtuelle private Cloud konfiguriert, Amazon VPC in der sich Ihr Amazon FSx (NetApp ONTAP-) Dateisystem befindet.

- Haben Ihre Amazon FSx (NetApp ONTAP-) Authentifizierungsdaten für ein Active Directory Benutzerkonto notiert. Dazu gehören Ihr Active Directory-Benutzername mit Ihrem DNS-Domainnamen (z. B. user@corp.example.com) und Ihrem Passwort. Wenn Sie das Network File System (NFS) -Protokoll für Ihr Amazon FSx (NetApp ONTAP) -Dateisystem verwenden, enthalten die Authentifizierungsdaten eine linke ID, eine rechte ID und einen vorinstallierten Schlüssel.

  > **Note**
  >
  > Verwenden Sie nur die erforderlichen Anmeldeinformationen, damit der Connector funktioniert. Verwenden Sie keine privilegierten Anmeldeinformationen wie den Domänenadministrator.

- Vergewissert, dass jedes Dokument in Amazon FSx (NetApp ONTAP) und in anderen Datenquellen, die Sie für denselben Index verwenden möchten, einzigartig ist. Jede Datenquelle, die Sie für einen Index verwenden möchten, darf nicht dasselbe Dokument in allen Datenquellen enthalten. Dokument-IDs gelten für einen Index global und müssen pro Index eindeutig sein.

Stellen Sie sicher AWS-Konto, dass Sie Folgendes in Ihrem haben:

- Hat einen Amazon Kendra Index erstellt und bei Verwendung der API die Index-ID notiert.
- Sie haben eine IAM Rolle für Ihre Datenquelle erstellt und, falls Sie die API verwenden, den ARN der IAM Rolle notiert.

  > **Note**
  >
  > Wenn Sie Ihren Authentifizierungstyp und Ihre Anmeldeinformationen ändern, müssen Sie Ihre IAM Rolle aktualisieren, um auf die richtige AWS Secrets Manager geheime ID zugreifen zu können.

- Ihre Amazon FSx (NetApp ONTAP-) Authentifizierungsdaten AWS Secrets Manager geheim gespeichert und, falls Sie die API verwenden, den ARN des Geheimnisses notiert.

  > **Note**
  >
  > Wir empfehlen Ihnen, Ihre Anmeldeinformationen und Ihr Geheimnis regelmäßig zu aktualisieren oder zu wechseln. Stellen Sie zu Ihrer eigenen Sicherheit nur die erforderliche Zugriffsebene bereit. Wir raten davon ab, Anmeldeinformationen und geheime

Daten für alle Datenquellen und Connector-Versionen 1.0 und 2.0 (sofern zutreffend) wiederzuverwenden.

Wenn Sie noch keine IAM Rolle oder keinen Schlüssel haben, können Sie die Konsole verwenden, um eine neue IAM Rolle und ein neues Secrets Manager Geheimnis zu erstellen, wenn Sie Ihre Amazon FSx (NetApp ONTAP-) Datenquelle mit verbinden. Amazon Kendra Wenn Sie die API verwenden, müssen Sie den ARN einer vorhandenen IAM Rolle und eines Secrets Manager Geheimnisses sowie eine Index-ID angeben.

Anweisungen zur Verbindung

Um eine Verbindung Amazon Kendra zu Ihrer Amazon FSx (NetApp ONTAP-) Datenquelle herzustellen, müssen Sie die erforderlichen Angaben zu Ihrer Amazon FSx (NetApp ONTAP-) Datenquelle angeben, damit Sie auf Ihre Daten zugreifen Amazon Kendra können. Falls Sie Amazon FSx (NetApp ONTAP) für Amazon Kendra noch nicht konfiguriert haben, finden Sie weitere Informationen unter. Voraussetzungen

Console

So stellen Sie eine Verbindung Amazon Kendra zu Ihrem Amazon FSx (NetApp ONTAP-) Dateisystem her

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die Amazon Kendra Konsole.
2. Wählen Sie im linken Navigationsbereich Indizes und dann den Index, den Sie verwenden möchten, aus der Indexliste aus.

   > **Note**
   >
   > Sie können Ihre Einstellungen für die Benutzerzugriffskontrolle unter Indexeinstellungen konfigurieren oder bearbeiten.

3. Wählen Sie auf der Seite Erste Schritte die Option Datenquelle hinzufügen aus.
4. Wählen Sie auf der Seite Datenquelle hinzufügen die Option Amazon FSx (NetApp ONTAP) - Connector und dann Connector hinzufügen aus.
5. Geben Sie auf der Seite „Datenquellendetails angeben“ die folgenden Informationen ein:

a. Geben Sie im Feld Name und Beschreibung für Datenquellenname einen Namen für Ihre Datenquelle ein. Sie können Bindestriche, aber keine Leerzeichen verwenden.

b. (Optional) Beschreibung — Geben Sie eine optionale Beschreibung für Ihre Datenquelle ein.

c. In Standardsprache — Wählen Sie eine Sprache aus, um Ihre Dokumente nach dem Index zu filtern. Sofern Sie nichts anderes angeben, ist die Standardsprache Englisch. Die in den Metadaten des Dokuments angegebene Sprache hat Vorrang vor der ausgewählten Sprache.

d. Unter Tags für Neues Tag hinzufügen — Fügen Sie optionale Tags hinzu, um Ihre Ressourcen zu durchsuchen und zu filtern oder Ihre Kosten nachzuverfolgen. AWS

e. Wählen Sie Weiter aus.

6. Geben Sie auf der Seite Zugriff und Sicherheit definieren die folgenden Informationen ein:

a. Quelle — Geben Sie Ihre Dateisysteminformationen ein.

- Dateisystemprotokoll — Wählen Sie das Protokoll Ihres Amazon FSx (NetApp ONTAP-) Dateisystems. Sie können entweder das Common Internet File System (CIFS) -Protokoll oder das Network File System (NFS) -Protokoll für Linux wählen.
- Amazon FSx (NetApp ONTAP) -Dateisystem-ID — Wählen Sie aus der Drop-down-Liste Ihre bestehende Dateisystem-ID aus, die von (ONTAP) abgerufen wurde. Amazon FSx NetApp Oder erstellen Sie ein Amazon FSx (ONTAP-) Dateisystem NetApp . Sie finden Ihre Dateisystem-ID im Dateisystem-Dashboard in der Amazon FSx (NetApp ONTAP-) Konsole.
- SVM-ID (Amazon FSx (NetApp ONTAPnur NetApp ONTAP) für) — Geben Sie die SVM-ID (Storage Virtual Machine) Ihrer (ONTAP) an. Amazon FSx NetApp NetApp ONTAP Sie finden Ihre SVM-ID, indem Sie das Dateisystem-Dashboard in der Amazon FSx (NetApp ONTAP-) Konsole aufrufen, Ihre Dateisystem-ID auswählen und dann Virtuelle Speichermaschinen auswählen.

b. Autorisierung — Aktivieren oder deaktivieren Sie die Informationen der Zugriffskontrollliste (ACL) für Ihre Dokumente, wenn Sie über eine ACL verfügen und diese für die Zugriffskontrolle verwenden möchten. Die ACL gibt an, auf welche Dokumente Benutzer und Gruppen zugreifen können. Die ACL-Informationen werden verwendet, um Suchergebnisse nach dem Benutzer- oder Gruppenzugriff auf Dokumente zu filtern. Weitere Informationen finden Sie unter Benutzerkontextfilterung.

c. Authentifizierung — Wählen Sie ein vorhandenes AWS Secrets Manager Geheimnis aus, oder erstellen Sie ein neues Geheimnis, um Ihre Dateisystem-Anmeldeinformationen zu speichern. Wenn Sie sich dafür entscheiden, ein neues Geheimnis zu erstellen, wird ein AWS Secrets Manager geheimes Fenster geöffnet.

   Geben Sie ein Geheimnis ein, in dem Ihre Authentifizierungsdaten mit Ihrem Benutzernamen und Passwort gespeichert werden. Der Benutzername muss Ihren DNS-Domainnamen enthalten. Zum Beispiel user@corp.example.com.

   Wenn Sie das NFS-Protokoll für Ihr Amazon FSx (NetApp ONTAP-) Dateisystem verwenden, geben Sie ein Geheimnis an, in dem Ihre Authentifizierungsdaten mit linker ID, rechter ID und Pre-Shared Key gespeichert werden.

   Speichern Sie Ihr Geheimnis und fügen Sie es hinzu.

d. Virtual Private Cloud (VPC) — Sie müssen einen Standort auswählen, an Amazon VPC dem sich Ihr Amazon FSx (NetApp ONTAP) befindet. Sie schließen das VPC-Subnetz und die Sicherheitsgruppen ein. Siehe Konfiguration eines. Amazon VPC

e. IAM Rolle — Wählen Sie eine bestehende IAM Rolle oder erstellen Sie eine neue IAM Rolle, um auf Ihre Repository-Anmeldeinformationen und Indexinhalte zuzugreifen.

   > **Note**
   >
   > IAM Rollen, die für Indizes verwendet werden, können nicht für Datenquellen verwendet werden. Wenn Sie sich nicht sicher sind, ob eine vorhandene Rolle für einen Index oder eine häufig gestellte Frage verwendet wird, wählen Sie Neue Rolle erstellen, um Fehler zu vermeiden.

f. Wählen Sie Weiter aus.

7. Geben Sie auf der Seite „Synchronisierungseinstellungen konfigurieren“ die folgenden Informationen ein:

   a. Synchronisierungsbereich, Regex-Muster — Fügen Sie Muster für reguläre Ausdrücke hinzu, um bestimmte Dateien ein- oder auszuschließen.

   b. Synchronisierungsmodus — Wählen Sie aus, wie Sie Ihren Index aktualisieren möchten, wenn sich der Inhalt Ihrer Datenquelle ändert. Wenn Sie Ihre Datenquelle Amazon Kendra zum ersten Mal synchronisieren, werden alle Inhalte standardmäßig gecrawlt und indexiert. Sie müssen eine vollständige Synchronisierung Ihrer Daten

durchführen, falls Ihre erste Synchronisierung fehlgeschlagen ist, auch wenn Sie die Option Vollsynchronisierung nicht als Synchronisierungsmodusoption wählen.

- Vollständige Synchronisierung: Indizieren Sie den gesamten Inhalt neu und ersetzen die vorhandenen Inhalte jedes Mal, wenn Ihre Datenquelle mit Ihrem Index synchronisiert wird.
- Neue, geänderte, gelöschte Synchronisierung: Indizieren Sie bei jeder Synchronisierung Ihrer Datenquelle mit Ihrem Index nur neue, geänderte und gelöschte Inhalte. Amazon Kendra kann den Mechanismus Ihrer Datenquelle verwenden, um Inhaltsänderungen nachzuverfolgen und Inhalte zu indexieren, die sich seit der letzten Synchronisierung geändert haben.

c. Zeitplan für Synchronisierungsläufe — Wählen Sie unter Häufigkeit aus, wie oft Ihre Datenquelleninhalte synchronisiert und Ihr Index aktualisiert werden soll.

d. Wählen Sie Weiter aus.

8. Geben Sie auf der Seite Feldzuordnungen festlegen die folgenden Informationen ein:

   a. Wählen Sie aus den Amazon Kendra generierten Standardfeldern Ihrer Dateien aus, die Sie Ihrem Index zuordnen möchten. Um benutzerdefinierte Datenquellenfelder hinzuzufügen, erstellen Sie einen Indexfeldnamen für die Zuordnung und den Felddatentyp.

   b. Wählen Sie Weiter aus.

9. Überprüfen Sie auf der Seite Überprüfen und erstellen, ob die von Ihnen eingegebenen Informationen korrekt sind, und wählen Sie dann Datenquelle hinzufügen aus. Sie können Ihre Informationen auch auf dieser Seite bearbeiten. Ihre Datenquelle wird auf der Seite Datenquellen angezeigt, nachdem die Datenquelle erfolgreich hinzugefügt wurde.

API

Um eine Verbindung Amazon Kendra zu Ihrem Amazon FSx (NetApp ONTAP-) Dateisystem herzustellen

Sie müssen mithilfe der TemplateConfigurationAPI ein JSON des Datenquellenschemas angeben. Sie müssen die folgenden Informationen angeben:

- Datenquelle — Geben Sie den Datenquellentyp wie `FSXONTAP` bei der Verwendung des TemplateConfigurationJSON-Schemas an. Geben Sie außerdem die Datenquelle so an`TEMPLATE`, wie Sie die CreateDataSourceAPI aufrufen.

- Dateisystem-ID — Die Kennung des Amazon FSx (NetApp ONTAP-) Dateisystems. Sie finden Ihre Dateisystem-ID im Dateisystem-Dashboard in der Amazon FSx (NetApp ONTAP-) Konsole.
- SVM-ID — Die ID der virtuellen Speichermaschine (SVM), die mit Ihrem Dateisystem verwendet wird. Sie finden Ihre SVM-ID, indem Sie das Dateisystem-Dashboard in der Amazon FSx (NetApp ONTAP-) Konsole aufrufen, Ihre Dateisystem-ID und dann virtuelle Speichermaschinen auswählen.
- Protokolltyp — Geben Sie an, ob Sie das CIFS-Protokoll (Common Internet File System) oder das NFS-Protokoll (Network File System) für Linux verwenden.
- Dateisystemtyp — Geben Sie entweder den Typ des Dateisystems an. `FSXONTAP`
- Virtual Private Cloud (VPC) — Geben Sie an, `VpcConfiguration` wann Sie anrufen. `CreateDataSource` Weitere Informationen finden Sie unter Konfigurieren von Amazon Kendra für die Verwendung eines Amazon VPC.

  > **Note**
  >
  > Sie müssen einen Standort auswählen, an Amazon VPC dem sich Ihr Amazon FSx (NetApp ONTAP) befindet. Sie schließen das VPC-Subnetz und die Sicherheitsgruppen ein.

- Geheimer Amazon-Ressourcenname (ARN) — Geben Sie den Amazon-Ressourcennamen (ARN) eines Secrets Manager Geheimnisses ein, das die Authentifizierungsdaten für Ihr Amazon FSx (NetApp ONTAP) -Konto enthält. Das Geheimnis wird in einer JSON-Struktur mit den folgenden Schlüsseln gespeichert:

  ```
  {
      "username": "user@corp.example.com",
      "password": "password"
  }
  ```

  Wenn Sie das NFS-Protokoll für Ihr Amazon FSx (NetApp ONTAP-) Dateisystem verwenden, wird das Geheimnis in einer JSON-Struktur mit den folgenden Schlüsseln gespeichert:

  ```
  {
      "leftId": "left ID",
      "rightId": "right ID",
      "preSharedKey": "pre-shared key"
  }
  ```

- IAM role — Geben Sie an`RoleArn`, wann Sie anrufen`CreateDataSource`, um einer IAM Rolle Berechtigungen für den Zugriff auf Ihr Secrets Manager Secret und den Aufruf der erforderlichen öffentlichen APIs für den Amazon FSx (NetApp ONTAP-) Connector und zu erteilen. Amazon Kendra Weitere Informationen finden Sie unter IAM Rollen für Amazon FSx (NetApp ONTAP-) Datenquellen.

Sie können auch die folgenden optionalen Funktionen hinzufügen:

- Synchronisierungsmodus — Geben Sie an, wie Ihr Index aktualisiert Amazon Kendra werden soll, wenn sich der Inhalt Ihrer Datenquelle ändert. Wenn Sie Ihre Datenquelle Amazon Kendra zum ersten Mal synchronisieren, werden alle Inhalte standardmäßig gecrawlt und indexiert. Sie müssen eine vollständige Synchronisierung Ihrer Daten durchführen, falls Ihre erste Synchronisierung fehlgeschlagen ist, auch wenn Sie die Option Vollsynchronisierung nicht als Synchronisierungsmodusoption wählen. Sie können wählen zwischen:
  - `FORCED_FULL_CRAWL`um den gesamten Inhalt neu zu indizieren und vorhandene Inhalte jedes Mal zu ersetzen, wenn Ihre Datenquelle mit Ihrem Index synchronisiert wird.
  - `FULL_CRAWL`um bei jeder Synchronisierung Ihrer Datenquelle mit Ihrem Index nur neue, geänderte und gelöschte Inhalte zu indizieren. Amazon Kendra kann den Mechanismus Ihrer Datenquelle verwenden, um Inhaltsänderungen nachzuverfolgen und Inhalte zu indexieren, die sich seit der letzten Synchronisierung geändert haben.
- Inklusions- und Ausschlussfilter — Geben Sie an, ob bestimmte Dateien ein- oder ausgeschlossen werden sollen.

  > **Note**
  >
  > Die meisten Datenquellen verwenden Muster mit regulären Ausdrücken, bei denen es sich um Ein- oder Ausschlussmuster handelt, die als Filter bezeichnet werden. Wenn Sie einen Einschlussfilter angeben, werden nur Inhalte indexiert, die dem Einschlussfilter entsprechen. Jedes Dokument, das nicht dem Einschlussfilter entspricht, wird nicht indexiert. Wenn Sie einen Ein- und Ausschlussfilter angeben, werden Dokumente, die dem Ausschlussfilter entsprechen, nicht indexiert, auch wenn sie dem Einschlussfilter entsprechen.
- Zugriffskontrollliste (ACL) — Geben Sie an, ob die ACL-Informationen für Ihre Dokumente gecrawlt werden sollen, wenn Sie über eine ACL verfügen und diese für die Zugriffskontrolle verwenden möchten. Die ACL gibt an, auf welche Dokumente Benutzer und Gruppen

zugreifen können. Die ACL-Informationen werden verwendet, um Suchergebnisse nach dem Benutzer- oder Gruppenzugriff auf Dokumente zu filtern. Weitere Informationen finden Sie unter Benutzerkontextfilterung.

> **Note**
>
> Um die Benutzerkontextfilterung für einen Benutzer zu testen, müssen Sie den DNS-Domänennamen als Teil des Benutzernamens angeben, wenn Sie die Abfrage ausgeben. Sie müssen über Administratorrechte für die Active Directory-Domäne verfügen. Sie können die Benutzerkontextfilterung auch anhand eines Gruppennamens testen.

- Feldzuordnungen — Wählen Sie, ob Sie Ihre Amazon FSx (NetApp ONTAP-) Datenquellenfelder Ihren Indexfeldern zuordnen möchten. Amazon Kendra Weitere Informationen finden Sie unter Zuweisen von Datenquellenfeldern.

> **Note**
>
> Das Textfeld oder das entsprechende Textfeld für Ihre Dokumente ist erforderlich, um Ihre Dokumente durchsuchen Amazon Kendra zu können. Sie müssen den Feldnamen Ihres Dokumenthauptteils in Ihrer Datenquelle dem Namen des Indexfeldes zuordnen`_document_body`. Alle anderen Felder sind optional.

Eine Liste weiterer wichtiger JSON-Schlüssel, die konfiguriert werden müssen, finden Sie unter Amazon FSx (NetApp ONTAP) -Vorlagenschema.

Amazon RDS/Aurora

Sie können Dokumente, die in einer Datenbank gespeichert sind, mithilfe einer Datenbankdatenquelle indizieren. Nachdem Sie Verbindungsinformationen für die Datenbank angegeben haben, Amazon Kendra verbindet und indexiert Dokumente.

Amazon Kendra unterstützt die folgenden Datenbanken:

- Amazon Aurora MySQL
- Amazon Aurora PostgreSQL

- Amazon RDS für MySQL
- Amazon RDS für PostgreSQL

> **Note**
>
> Serverlose Aurora-Datenbanken werden nicht unterstützt.

> **Important**
>
> Dieser Amazon RDS/Aurora-Connector wird voraussichtlich Ende 2023 nicht mehr unterstützt.
> Amazon Kendra unterstützt jetzt neue Konnektoren für Datenbank-Datenquellen. Für eine bessere Benutzererfahrung empfehlen wir Ihnen, für Ihren Anwendungsfall aus den folgenden neuen Konnektoren zu wählen:
>
> - Aurora (MySQL)
> - Aurora (PostgreSQL)
> - Amazon RDS (MySQL)
> - Amazon RDS (Microsoft SQL Server)
> - Amazon RDS (Orakel)
> - Amazon RDS (PostgreSQL)
> - IBM DB2
> - Microsoft SQL Server
> - MySQL
> - Oracle-Datenbank
> - PostgreSQL

Sie können über Amazon Kendra die Amazon Kendra Konsole und die DatabaseConfigurationAPI eine Verbindung zu Ihrer Datenbank-Datenquelle herstellen.

Informationen zur Problembehandlung Ihres Amazon Kendra Datenbank-Datenquellen-Connectors finden Sie unterProblembehandlung bei Datenquellen.

Themen

Unterstützte Features

Amazon Kendra Der Datenbank-Datenquellen-Connector unterstützt die folgenden Funktionen:

- Feldzuordnungen
- Filterung des Benutzerkontextes
- Virtual Private Cloud (VPC)

Voraussetzungen

Bevor Sie Ihre Datenbankdatenquelle Amazon Kendra zum Indizieren verwenden können, müssen Sie diese Änderungen an Ihrer Datenbank und Ihren AWS Konten vornehmen.

Stellen Sie sicher, dass Sie in Ihrer Datenbank Folgendes haben:

- Notieren Sie sich Ihre grundlegenden Authentifizierungsdaten mit Benutzername und Passwort für Ihre Datenbank.
- Der Hostname, die Portnummer, die Hostadresse, der Name der Datenbank und der Name der Datentabelle, die die Dokumentdaten enthält, wurden kopiert. Für PostgreSQL muss die Datentabelle eine öffentliche Tabelle oder ein öffentliches Schema sein.

  > **Note**
  >
  > Der Host und der Port geben an Amazon Kendra , wo der Datenbankserver im Internet zu finden ist. Der Datenbankname und der Tabellenname geben an, Amazon Kendra wo sich die Dokumentdaten auf dem Datenbankserver befinden.

- Die Namen der Spalten in der Datentabelle, die die Dokumentdaten enthalten, wurden kopiert. Sie müssen die Dokument-ID, den Hauptteil des Dokuments, Spalten, um festzustellen, ob sich ein Dokument geändert hat (z. B. die Spalte mit der letzten Aktualisierung), und optionale Spalten in der Datentabelle angeben, die benutzerdefinierten Indexfeldern zugeordnet sind. Sie können auch jeden der Amazon Kendra reservierten Feldnamen einer Tabellenspalte zuordnen.

- Die Typinformationen der Datenbank-Engine wurden kopiert, z. B. ob Sie sie Amazon RDS für MySQL oder einen anderen Typ verwenden.
- Aktiviert, dass jedes Dokument in der Datenbank und in anderen Datenquellen, die Sie für denselben Index verwenden möchten, eindeutig ist. Jede Datenquelle, die Sie für einen Index verwenden möchten, darf nicht dasselbe Dokument in allen Datenquellen enthalten. Dokument-IDs gelten für einen Index global und müssen pro Index eindeutig sein.

Stellen Sie sicher AWS-Konto, dass Sie Folgendes in Ihrem haben:

- Hat einen Amazon Kendra Index erstellt und bei Verwendung der API die Index-ID notiert.
- Sie haben eine IAM Rolle für Ihre Datenquelle erstellt und, falls Sie die API verwenden, den ARN der IAM Rolle notiert.

> **Note**
>
> Wenn Sie Ihren Authentifizierungstyp und Ihre Anmeldeinformationen ändern, müssen Sie Ihre IAM Rolle aktualisieren, um auf die richtige AWS Secrets Manager geheime ID zugreifen zu können.

- Ihre Anmeldeinformationen für die Datenbankauthentifizierung AWS Secrets Manager geheim gespeichert und, falls Sie die API verwenden, den ARN des Geheimnisses notiert.

> **Note**
>
> Wir empfehlen Ihnen, Ihre Anmeldeinformationen und Ihr Geheimnis regelmäßig zu aktualisieren oder zu wechseln. Stellen Sie zu Ihrer eigenen Sicherheit nur die erforderliche Zugriffsebene bereit. Wir raten davon ab, Anmeldeinformationen und geheime Daten für alle Datenquellen und Connector-Versionen 1.0 und 2.0 (sofern zutreffend) wiederzuverwenden.

Wenn Sie noch keine IAM Rolle oder keinen Schlüssel haben, können Sie die Konsole verwenden, um eine neue IAM Rolle und ein neues Secrets Manager Geheimnis zu erstellen, wenn Sie Ihre Datenbankdatenquelle mit verbinden. Amazon Kendra Wenn Sie die API verwenden, müssen Sie den ARN einer vorhandenen IAM Rolle und eines Secrets Manager Geheimnisses sowie eine Index-ID angeben.

Anweisungen zur Verbindung

Um eine Verbindung Amazon Kendra zu Ihrer Datenbankdatenquelle herzustellen, müssen Sie die erforderlichen Details zu Ihrer Datenbankdatenquelle angeben, damit auf Ihre Daten zugegriffen werden Amazon Kendra kann. Wenn Sie die Datenbank für noch nicht konfiguriert haben Amazon Kendra, finden Sie weitere Informationen unterVoraussetzungen.

Console

So stellen Sie eine Verbindung Amazon Kendra zu einer Datenbank her

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die Amazon Kendra Konsole.
2. Wählen Sie im linken Navigationsbereich Indizes und dann den Index, den Sie verwenden möchten, aus der Indexliste aus.

   > **Note**
   >
   > Sie können Ihre Einstellungen für die Benutzerzugriffskontrolle unter Indexeinstellungen konfigurieren oder bearbeiten.

3. Wählen Sie auf der Seite Erste Schritte die Option Datenquelle hinzufügen aus.
4. Wählen Sie auf der Seite Datenquelle hinzufügen die Option Datenbank-Connector und dann Connector hinzufügen aus.
5. Geben Sie auf der Seite „Datenquellendetails angeben“ die folgenden Informationen ein:

   a. Geben Sie im Feld Name und Beschreibung für Datenquellenname einen Namen für Ihre Datenquelle ein. Sie können Bindestriche, aber keine Leerzeichen verwenden.

   b. (Optional) Beschreibung — Geben Sie eine optionale Beschreibung für Ihre Datenquelle ein.

   c. In Standardsprache — Wählen Sie eine Sprache aus, um Ihre Dokumente nach dem Index zu filtern. Sofern Sie nichts anderes angeben, ist die Standardsprache Englisch. Die in den Metadaten des Dokuments angegebene Sprache hat Vorrang vor der ausgewählten Sprache.

   d. Unter Tags für Neues Tag hinzufügen — Fügen Sie optionale Tags hinzu, um Ihre Ressourcen zu durchsuchen und zu filtern oder Ihre Kosten nachzuverfolgen. AWS

   e. Wählen Sie Weiter aus.

6. Geben Sie auf der Seite Zugriff und Sicherheit definieren die folgenden Informationen ein:

   a. Endpunkt — Ein DNS-Hostname, eine IPv4-Adresse oder eine IPv6-Adresse.

   b. Port — Eine Portnummer.

   c. Datenbank — Datenbankname.

   d. Tabellenname —Tabellenname.

   e. Wählen Sie für Authentifizierungstyp zwischen Existiert und Neu, um Ihre Anmeldeinformationen für die Datenbankauthentifizierung zu speichern. Wenn Sie sich dafür entscheiden, ein neues Geheimnis zu erstellen, wird ein AWS Secrets Manager geheimes Fenster geöffnet.

      - Geben Sie die folgenden Informationen in das Fenster Create an AWS Secrets Manager Secret ein:

        A. Geheimer Name — Ein Name für Ihr Geheimnis. Das Präfix 'AmazonKendra-database' wird automatisch zu Ihrem geheimen Namen hinzugefügt.

        B. Für Benutzername und Passwort — Geben Sie die Authentifizierungsdaten aus Ihrem Datenbankkonto ein.

        C. Wählen Sie Authentifizierung speichern aus.

   f. Virtual Private Cloud (VPC) — Sie können wählen, ob Sie eine VPC verwenden möchten. In diesem Fall müssen Sie Subnetze und VPC-Sicherheitsgruppen hinzufügen.

      > **Note**
      >
      > Sie müssen ein privates Subnetz verwenden. Wenn sich Ihre RDS-Instance in einem öffentlichen Subnetz in Ihrer VPC befindet, können Sie ein privates Subnetz erstellen, das ausgehenden Zugriff auf ein NAT-Gateway im öffentlichen Subnetz hat. Die in der VPC-Konfiguration bereitgestellten Subnetze müssen sich entweder in USA West (Oregon), USA Ost (Nord-Virginia) oder EU (Irland) befinden.

   g. IAM Rolle — Wählen Sie eine bestehende IAM Rolle oder erstellen Sie eine neue IAM Rolle, um auf Ihre Repository-Anmeldeinformationen und Indexinhalte zuzugreifen.

> **Note**
>
> IAM Rollen, die für Indizes verwendet werden, können nicht für Datenquellen verwendet werden. Wenn Sie sich nicht sicher sind, ob eine vorhandene Rolle für einen Index oder eine häufig gestellte Frage verwendet wird, wählen Sie Neue Rolle erstellen, um Fehler zu vermeiden.

h. Wählen Sie Weiter aus.

7. Geben Sie auf der Seite „Synchronisierungseinstellungen konfigurieren“ die folgenden Informationen ein:

   a. Wählen Sie je nach Anwendungsfall zwischen Aurora MySQL , MySQL, Aurora PostgreSQL und PostgreSQL.

   b. SQL-Bezeichner in doppelte Anführungszeichen einschließen — Wählen Sie diese Option, um SQL-Bezeichner in doppelte Anführungszeichen zu setzen. Zum Beispiel „ColumnName“.

   c. ACL-Spalte und Spalten mit Änderungserkennung — Konfigurieren Sie die Spalten, die für die Änderungserkennung Amazon Kendra verwendet werden (z. B. die Spalte mit der letzten Aktualisierung), und Ihre Zugriffskontrollliste.

   d. Wählen Sie im Synchronisierungslaufplan für Häufigkeit aus, wie oft die Synchronisierung mit Ihrer Datenquelle erfolgen Amazon Kendra soll.

   e. Wählen Sie Weiter aus.

8. Geben Sie auf der Seite Feldzuordnungen festlegen die folgenden Informationen ein:

   a. Amazon Kendra Standard-Feldzuordnungen — Wählen Sie eines der Amazon Kendra generierten Standard-Datenquellenfelder aus, die Sie Ihrem Index zuordnen möchten. Sie müssen die Datenbankspaltenwerte für und hinzufügen `document_id` `document_body`

   b. Benutzerdefinierte Feldzuordnungen — Um benutzerdefinierte Datenquellenfelder hinzuzufügen, um einen Indexfeldnamen für die Zuordnung und den Felddatentyp zu erstellen.

   c. Wählen Sie Weiter aus.

9. Überprüfen Sie auf der Seite Überprüfen und erstellen, ob die von Ihnen eingegebenen Informationen korrekt sind, und wählen Sie dann Datenquelle hinzufügen aus. Sie können

Ihre Informationen auch auf dieser Seite bearbeiten. Ihre Datenquelle wird auf der Seite Datenquellen angezeigt, nachdem die Datenquelle erfolgreich hinzugefügt wurde.

API

Um eine Verbindung Amazon Kendra zu einer Datenbank herzustellen

Sie müssen die folgende DatabaseConfigurationAPI angeben:

- ColumnConfiguration— Informationen darüber, wo der Index die Dokumentinformationen aus der Datenbank abrufen soll. Weitere Details finden Sie unter ColumnConfiguration. Sie müssen die Felder `DocumentDataColumnName` (Hauptteil des Dokuments oder Haupttext) und `DocumentIdColumnName` und `ChangeDetectingColumn` (z. B. Spalte mit der letzten Aktualisierung) angeben. Die dem `DocumentIdColumnName` Feld zugeordnete Spalte muss eine Ganzzahlspalte sein. Das folgende Beispiel zeigt eine einfache Spaltenkonfiguration für eine Datenbankdatenquelle:

```
"ColumnConfiguration": {
    "ChangeDetectingColumns": [
        "LastUpdateDate",
        "LastUpdateTime"
    ],
    "DocumentDataColumnName": "TextColumn",
    "DocumentIdColumnName": "IdentifierColumn",
    "DocoumentTitleColumnName": "TitleColumn",
    "FieldMappings": [
        {
            "DataSourceFieldName": "AbstractColumn",
            "IndexFieldName": "Abstract"
        }
    ]
}
```

- ConnectionConfiguration— Konfigurationsinformationen, die für die Verbindung mit einer Datenbank erforderlich sind. Weitere Details finden Sie unter ConnectionConfiguration.
- DatabaseEngineType— Der Typ der Datenbank-Engine, die die Datenbank ausführt. Das `DatabaseHost` Feld für `ConnectionConfiguration` muss der Instanzendpunkt Amazon Relational Database Service (Amazon RDS) für die Datenbank sein. Verwenden Sie nicht den Cluster-Endpunkt.

- Geheimer Amazon-Ressourcenname (ARN) — Geben Sie den Amazon-Ressourcennamen (ARN) eines Secrets Manager Geheimnisses ein, das die Authentifizierungsdaten für Ihr Datenbankkonto enthält. Das Geheimnis wird in einer JSON-Struktur mit den folgenden Schlüsseln gespeichert:

```
{
    "username": "user name",
    "password": "password"
}
```

Das folgende Beispiel zeigt eine Datenbankkonfiguration, einschließlich des geheimen ARN.

```
"DatabaseConfiguration": {
"ConnectionConfiguration": {
"DatabaseHost": "host.subdomain.domain.tld",
        "DatabaseName": "DocumentDatabase",
        "DatabasePort": 3306,
        "SecretArn": "arn:aws:secretmanager:region:account ID:secret/secret name",
        "TableName": "DocumentTable"
    }
}
```

> **Note**
>
> Wir empfehlen Ihnen, Ihre Anmeldeinformationen und Ihren geheimen Schlüssel regelmäßig zu aktualisieren oder zu wechseln. Stellen Sie zu Ihrer eigenen Sicherheit nur die erforderliche Zugriffsebene bereit. Wir raten davon ab, Anmeldeinformationen und geheime Daten für alle Datenquellen und Connector-Versionen 1.0 und 2.0 (sofern zutreffend) wiederzuverwenden.

- IAM Rolle — Geben Sie an`RoleArn`, wann Sie anrufen`CreateDataSource`, um einer IAM Rolle Berechtigungen für den Zugriff auf Ihr Secrets Manager Geheimnis und für den Aufruf der erforderlichen öffentlichen APIs für den Datenbank-Connector und zu erteilen. Amazon Kendra Weitere Informationen finden Sie unter IAM Rollen für Datenbankdatenquellen.

Sie können auch die folgenden optionalen Funktionen hinzufügen:

- Virtual Private Cloud (VPC) — Geben Sie dies `VpcConfiguration` als Teil der Datenquellenkonfiguration an. Siehe Konfiguration Amazon Kendra für die Verwendung einer VPC.

  > **Note**
  >
  > Sie dürfen nur ein privates Subnetz verwenden. Wenn sich Ihre RDS-Instance in einem öffentlichen Subnetz in Ihrer VPC befindet, können Sie ein privates Subnetz erstellen, das ausgehenden Zugriff auf ein NAT-Gateway im öffentlichen Subnetz hat. Die in der VPC-Konfiguration bereitgestellten Subnetze müssen sich entweder in USA West (Oregon), USA Ost (Nord-Virginia) oder EU (Irland) befinden.

- Feldzuordnungen — Wählen Sie diese Option, um Ihre Datenbank-Datenquellenfelder Ihren Indexfeldern zuzuordnen. Amazon Kendra Weitere Informationen finden Sie unter Zuweisen von Datenquellenfeldern.

  > **Note**
  >
  > Das Textfeld oder das entsprechende Textfeld für Ihre Dokumente ist erforderlich, um Ihre Dokumente durchsuchen Amazon Kendra zu können. Sie müssen den Feldnamen Ihres Dokumenthauptteils in Ihrer Datenquelle dem Namen des Indexfeldes zuordnen_`document_body`. Alle anderen Felder sind optional.

- Benutzerkontextfilterung und ZugriffskontrolleAmazon Kendra — durchsucht die Zugriffskontrollliste (ACL) für Ihre Dokumente, sofern Sie über eine ACL für Ihre Dokumente verfügen. Die ACL-Informationen werden verwendet, um Suchergebnisse nach dem Benutzer- oder Gruppenzugriff auf Dokumente zu filtern. Weitere Informationen finden Sie unter Benutzerkontextfilterung.

Amazon RDS (Microsoft SQL Server)

SQL Server ist ein von Microsoft entwickeltes Datenbankverwaltungssystem. Amazon RDS for SQL Server macht es einfach, SQL Server-Bereitstellungen in der Cloud einzurichten, zu betreiben und zu skalieren. Wenn Sie ein Amazon RDS (Microsoft SQL Server) -Benutzer sind, können Amazon Kendra Sie Ihre Amazon RDS (Microsoft SQL Server-) Datenquelle indizieren. Der Amazon Kendra JDBC-Datenquellenconnector unterstützt Microsoft SQL Server 2019.

Sie können über Amazon Kendra die Amazon Kendra Konsole und die TemplateConfigurationAPI eine Verbindung zu Ihrer Datenquelle Amazon RDS (Microsoft SQL Server) herstellen.

Informationen zur Problembehandlung Ihres Datenquellenconnectors Amazon Kendra Amazon RDS (Microsoft SQL Server) finden Sie unterProblembehandlung bei Datenquellen.

Themen

Unterstützte Features

- Feldzuordnungen
- Filterung des Benutzerkontextes
- Einschluss-/Ausschlussfilter
- Vollständige und inkrementelle Inhaltssynchronisierung
- Virtual Private Cloud (VPC)

Voraussetzungen

Bevor Sie Ihre Amazon RDS (Microsoft SQL Server) Datenquelle Amazon Kendra zum Indizieren verwenden können, nehmen Sie diese Änderungen in Ihren Amazon RDS (Microsoft SQL Server) und AWS Konten vor.

Stellen Sie in Amazon RDS (Microsoft SQL Server) sicher, dass Sie über Folgendes verfügen:

- Notiert Ihren Datenbankbenutzernamen und Ihr Passwort.

> **Important**
>
> Es hat sich bewährt, nur lesbare Amazon Kendra Datenbankanmeldeinformationen zur Verfügung zu stellen.

- Die URL, der Port und die Instanz Ihres Datenbank-Hosts wurden kopiert.

- Geprüft, ob jedes Dokument in Amazon RDS (Microsoft SQL Server) und in anderen Datenquellen, die Sie für denselben Index verwenden möchten, einzigartig ist. Jede Datenquelle, die Sie für einen Index verwenden möchten, darf nicht dasselbe Dokument in allen Datenquellen enthalten. Dokument-IDs gelten für einen Index global und müssen pro Index eindeutig sein.

Stellen Sie sicher AWS-Konto, dass Sie Folgendes in Ihrem haben:

- Hat einen Amazon Kendra Index erstellt und bei Verwendung der API die Index-ID notiert.
- Sie haben eine IAM Rolle für Ihre Datenquelle erstellt und, falls Sie die API verwenden, den ARN der IAM Rolle notiert.

> **Note**
>
> Wenn Sie Ihren Authentifizierungstyp und Ihre Anmeldeinformationen ändern, müssen Sie Ihre IAM Rolle aktualisieren, um auf die richtige AWS Secrets Manager geheime ID zugreifen zu können.

- Ihre Amazon RDS (Microsoft SQL Server-) Authentifizierungsdaten AWS Secrets Manager geheim gespeichert und, falls Sie die API verwenden, den ARN des Geheimnisses notiert.

> **Note**
>
> Wir empfehlen Ihnen, Ihre Anmeldeinformationen und Ihr Geheimnis regelmäßig zu aktualisieren oder zu wechseln. Stellen Sie zu Ihrer eigenen Sicherheit nur die erforderliche Zugriffsebene bereit. Wir raten davon ab, Anmeldeinformationen und geheime Daten für alle Datenquellen und Connector-Versionen 1.0 und 2.0 (sofern zutreffend) wiederzuverwenden.

Wenn Sie noch keine IAM Rolle oder keinen Schlüssel haben, können Sie die Konsole verwenden, um eine neue IAM Rolle und ein neues Secrets Manager Geheimnis zu erstellen, wenn Sie Ihre Amazon RDS (Microsoft SQL Server-) Datenquelle mit verbinden Amazon Kendra. Wenn Sie die API verwenden, müssen Sie den ARN einer vorhandenen IAM Rolle und eines Secrets Manager Geheimnisses sowie eine Index-ID angeben.

Anweisungen zur Verbindung

Um eine Verbindung Amazon Kendra zu Ihrer Amazon RDS (Microsoft SQL Server-) Datenquelle herzustellen, müssen Sie Details zu Ihren Amazon RDS (Microsoft SQL Server-) Anmeldeinformationen angeben, damit Sie auf Ihre Daten zugreifen Amazon Kendra können. Wenn Sie Amazon RDS (Microsoft SQL Server) noch nicht konfiguriert haben, Amazon Kendra sieheVoraussetzungen.

Console

Um eine Verbindung Amazon Kendra herzustellen mit Amazon RDS (Microsoft SQL Server)

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die Amazon Kendra Konsole.
2. Wählen Sie im linken Navigationsbereich Indizes und dann den Index, den Sie verwenden möchten, aus der Indexliste aus.

   > **Note**
   >
   > Sie können Ihre Einstellungen für die Benutzerzugriffskontrolle unter Indexeinstellungen konfigurieren oder bearbeiten.

3. Wählen Sie auf der Seite Erste Schritte die Option Datenquelle hinzufügen aus.
4. Wählen Sie auf der Seite Datenquelle hinzufügen die Option Amazon RDS (Microsoft SQL Server) Connector und dann Connector hinzufügen aus.
5. Geben Sie auf der Seite „Datenquellendetails angeben“ die folgenden Informationen ein:

   a. Geben Sie im Feld Name und Beschreibung für Datenquellenname einen Namen für Ihre Datenquelle ein. Sie können Bindestriche, aber keine Leerzeichen verwenden.

   b. (Optional) Beschreibung — Geben Sie eine optionale Beschreibung für Ihre Datenquelle ein.

   c. In Standardsprache — Wählen Sie eine Sprache aus, um Ihre Dokumente nach dem Index zu filtern. Sofern Sie nichts anderes angeben, ist die Standardsprache Englisch. Die in den Metadaten des Dokuments angegebene Sprache hat Vorrang vor der ausgewählten Sprache.

   d. Unter Tags für Neues Tag hinzufügen — Fügen Sie optionale Tags hinzu, um Ihre Ressourcen zu durchsuchen und zu filtern oder Ihre Kosten nachzuverfolgen. AWS

e. Wählen Sie Weiter aus.

6. Geben Sie auf der Seite Zugriff und Sicherheit definieren die folgenden Informationen ein:

   a. Geben Sie im Feld Quelle die folgenden Informationen ein:

   b. Host — Geben Sie den Datenbank-Hostnamen ein.

   c. Port — Geben Sie den Datenbankport ein.

   d. Instanz — Geben Sie die Datenbankinstanz ein.

   e. Speicherort für SSL-Zertifikate aktivieren — Geben Sie hier den Amazon S3 Pfad zu Ihrer SSL-Zertifikatsdatei ein.

   f. Geben Sie im Feld Authentifizierung die folgenden Informationen ein:

      - AWS Secrets Manager geheim — Wählen Sie ein vorhandenes Geheimnis oder erstellen Sie ein neues Secrets Manager Geheimnis, um Ihre Anmeldeinformationen Amazon RDS (Microsoft SQL Server) zu speichern. Wenn Sie ein neues Geheimnis erstellen möchten, wird ein AWS Secrets Manager geheimes Fenster geöffnet.

        A. Geben Sie die folgenden Informationen in das Fenster Create an AWS Secrets Manager Secret ein:

           I. Geheimer Name — Ein Name für Ihr Geheimnis. Das Präfix 'AmazonKendra-Amazon RDS (Microsoft SQL Server) -' wird Ihrem geheimen Namen automatisch hinzugefügt.

           II. Geben Sie für Datenbankbenutzername und Passwort die Werte der Authentifizierungsdaten ein, die Sie aus Ihrer Datenbank kopiert haben.

        B. Wählen Sie Speichern.

   g. Virtual Private Cloud (VPC) — Sie können wählen, ob Sie eine VPC verwenden möchten. In diesem Fall müssen Sie Subnetze und VPC-Sicherheitsgruppen hinzufügen.

   h. IAM Rolle — Wählen Sie eine bestehende IAM Rolle oder erstellen Sie eine neue IAM Rolle, um auf Ihre Repository-Anmeldeinformationen und Indexinhalte zuzugreifen.

> **Note**
>
> IAM Rollen, die für Indizes verwendet werden, können nicht für Datenquellen verwendet werden. Wenn Sie sich nicht sicher sind, ob eine vorhandene Rolle für

einen Index oder eine häufig gestellte Frage verwendet wird, wählen Sie Neue Rolle erstellen, um Fehler zu vermeiden.

i. Wählen Sie Weiter aus.

7. Geben Sie auf der Seite Synchronisierungseinstellungen konfigurieren die folgenden Informationen ein:

a. Wählen Sie unter Synchronisierungsbereich eine der folgenden Optionen aus:

- SQL-Abfrage — Geben Sie SQL-Abfrageanweisungen wie SELECT- und JOIN-Operationen ein. SQL-Abfragen müssen weniger als 32 KB groß sein. Amazon Kendra durchsucht den gesamten Datenbankinhalt, der Ihrer Abfrage entspricht.

> **Note**
>
> Wenn ein Tabellenname Sonderzeichen (nicht alphanumerisch) enthält, müssen Sie den Tabellennamen in eckige Klammern setzen. *Wählen Sie beispielsweise * aus [] my-database-table*

- Primärschlüsselspalte — Geben Sie den Primärschlüssel für die Datenbanktabelle an. Dies identifiziert eine Tabelle in Ihrer Datenbank.
- Titelspalte — Geben Sie den Namen der Titelspalte des Dokuments in Ihrer Datenbanktabelle an.
- Hauptspalte — Geben Sie den Namen der Hauptspalte des Dokuments in Ihrer Datenbanktabelle an.

b. Wählen Sie unter Zusätzliche Konfiguration — optional aus den folgenden Optionen, um bestimmte Inhalte zu synchronisieren, anstatt alle Dateien zu synchronisieren:

- Spalten zur Erkennung von Änderungen — Geben Sie die Namen der Spalten ein, anhand derer Inhaltsänderungen erkannt Amazon Kendra werden sollen. Amazon Kendra indexiert den Inhalt neu, wenn sich eine dieser Spalten ändert.
- Spalte mit Benutzer-IDs — Geben Sie den Namen der Spalte ein, die Benutzer-IDs enthält, um Zugriff auf Inhalte zu erhalten.
- Spalte „Gruppen“ — Geben Sie den Namen der Spalte ein, die Gruppen enthält, denen der Zugriff auf Inhalte gewährt werden soll.
- Spalte Quell-URLs — Geben Sie den Namen der Spalte ein, die Quell-URLs enthält, die indexiert werden sollen.

- Spalte mit Zeitstempeln — Geben Sie den Namen der Spalte ein, die Zeitstempel enthält. Amazon Kendra verwendet Zeitstempelinformationen, um Änderungen an Ihren Inhalten zu erkennen und nur geänderte Inhalte zu synchronisieren.
- Spalte „Zeitzonen“ — Geben Sie den Namen der Spalte ein, die Zeitzonen für den Inhalt enthält, der gecrawlt werden soll.
- Zeitstempelformat — Geben Sie den Namen der Spalte ein, die Zeitstempelformate enthält, anhand derer Inhaltsänderungen erkannt und Ihre Inhalte erneut synchronisiert werden sollen.

c. Synchronisierungsmodus — Wählen Sie aus, wie Sie Ihren Index aktualisieren möchten, wenn sich der Inhalt Ihrer Datenquelle ändert. Wenn Sie Ihre Datenquelle Amazon Kendra zum ersten Mal synchronisieren, werden alle Inhalte standardmäßig gecrawlt und indexiert. Sie müssen eine vollständige Synchronisierung Ihrer Daten durchführen, falls Ihre erste Synchronisierung fehlgeschlagen ist, auch wenn Sie die Option Vollsynchronisierung nicht als Synchronisierungsmodusoption wählen.

- Vollständige Synchronisierung: Indizieren Sie alle Inhalte neu und ersetzen vorhandene Inhalte jedes Mal, wenn Ihre Datenquelle mit Ihrem Index synchronisiert wird.
- Neue, geänderte Synchronisierung: Indizieren Sie bei jeder Synchronisierung Ihrer Datenquelle mit Ihrem Index nur neue und geänderte Inhalte. Amazon Kendra kann den Mechanismus Ihrer Datenquelle verwenden, um Inhaltsänderungen nachzuverfolgen und Inhalte zu indexieren, die sich seit der letzten Synchronisierung geändert haben.
- Neue, geänderte, gelöschte Synchronisierung: Indizieren Sie bei jeder Synchronisierung Ihrer Datenquelle mit Ihrem Index nur neue, geänderte und gelöschte Inhalte. Amazon Kendra kann den Mechanismus Ihrer Datenquelle verwenden, um Inhaltsänderungen nachzuverfolgen und Inhalte zu indexieren, die sich seit der letzten Synchronisierung geändert haben.

d. Im Synchronisierungslaufplan für Frequenz — Wie oft Amazon Kendra wird mit Ihrer Datenquelle synchronisiert?

e. Wählen Sie Weiter aus.

8. Geben Sie auf der Seite Feldzuordnungen festlegen die folgenden Informationen ein:

a. Wählen Sie aus den generierten Standard-Datenquellenfeldern — Dokument-IDs, Dokumenttitel und Quell-URLs — aus, die Sie dem Index zuordnen möchten. Amazon Kendra

b. Feld hinzufügen — Um benutzerdefinierte Datenquellenfelder hinzuzufügen, um einen Indexfeldnamen für die Zuordnung und den Felddatentyp zu erstellen.

c. Wählen Sie Weiter aus.

9. Überprüfen Sie auf der Seite Überprüfen und erstellen, ob die von Ihnen eingegebenen Informationen korrekt sind, und wählen Sie dann Datenquelle hinzufügen aus. Sie können Ihre Informationen auch auf dieser Seite bearbeiten. Ihre Datenquelle wird auf der Seite Datenquellen angezeigt, nachdem die Datenquelle erfolgreich hinzugefügt wurde.

API

Um eine Verbindung Amazon Kendra herzustellen mit Amazon RDS (Microsoft SQL Server)

Mithilfe der TemplateConfigurationAPI müssen Sie Folgendes angeben:

- Datenquelle — Geben Sie den Datenquellentyp wie `JDBC` bei der Verwendung des TemplateConfigurationJSON-Schemas an. Geben Sie außerdem die Datenquelle so an`TEMPLATE`, wie Sie die CreateDataSourceAPI aufrufen.
- Datenbanktyp — Sie müssen den Datenbanktyp als `sqlserver` angeben.
- SQL-Abfrage — Geben Sie SQL-Abfrageanweisungen wie SELECT- und JOIN-Operationen an. SQL-Abfragen müssen weniger als 32 KB groß sein. Amazon Kendra durchsucht den gesamten Datenbankinhalt, der Ihrer Abfrage entspricht.

> **Note**
>
> Wenn ein Tabellenname Sonderzeichen (nicht alphanumerisch) enthält, müssen Sie den Tabellennamen in eckige Klammern setzen. *`Wählen Sie beispielsweise * aus [] my-database-table`*

- Synchronisierungsmodus — Geben Sie an, wie Ihr Index aktualisiert Amazon Kendra werden soll, wenn sich der Inhalt Ihrer Datenquelle ändert. Wenn Sie Ihre Datenquelle Amazon Kendra zum ersten Mal synchronisieren, werden alle Inhalte standardmäßig gecrawlt und indexiert. Sie müssen eine vollständige Synchronisierung Ihrer Daten durchführen, falls Ihre erste

Synchronisierung fehlgeschlagen ist, auch wenn Sie die Option Vollsynchronisierung nicht als Synchronisierungsmodusoption wählen. Sie können wählen zwischen:

- `FORCED_FULL_CRAWL`um den gesamten Inhalt neu zu indizieren und vorhandene Inhalte jedes Mal zu ersetzen, wenn Ihre Datenquelle mit Ihrem Index synchronisiert wird.
- `FULL_CRAWL`um bei jeder Synchronisierung Ihrer Datenquelle mit Ihrem Index nur neue, geänderte und gelöschte Inhalte zu indizieren. Amazon Kendra kann den Mechanismus Ihrer Datenquelle verwenden, um Inhaltsänderungen nachzuverfolgen und Inhalte zu indexieren, die sich seit der letzten Synchronisierung geändert haben.
- `CHANGE_LOG`um bei jeder Synchronisierung Ihrer Datenquelle mit Ihrem Index nur neue und geänderte Inhalte zu indizieren. Amazon Kendra kann den Mechanismus Ihrer Datenquelle verwenden, um Inhaltsänderungen nachzuverfolgen und Inhalte zu indexieren, die sich seit der letzten Synchronisierung geändert haben.

- Geheimer Amazon-Ressourcenname (ARN) — Geben Sie den Amazon-Ressourcennamen (ARN) eines Secrets Manager Geheimnisses ein, das die Authentifizierungsdaten enthält, die Sie in Ihrem Konto Amazon RDS (Microsoft SQL Server) erstellt haben. Das Geheimnis wird in einer JSON-Struktur mit den folgenden Schlüsseln gespeichert:

```
{
    "user name": "database user name",
    "password": "password"
}
```

> **Note**
>
> Wir empfehlen Ihnen, Ihre Anmeldeinformationen und Ihr Geheimnis regelmäßig zu aktualisieren oder zu wechseln. Stellen Sie zu Ihrer eigenen Sicherheit nur die erforderliche Zugriffsebene bereit. Wir raten davon ab, Anmeldeinformationen und geheime Daten für alle Datenquellen und Connector-Versionen 1.0 und 2.0 (sofern zutreffend) wiederzuverwenden.

- IAM role — Geben Sie an, `RoleArn` wann Sie aufrufen`CreateDataSource`, um einer IAM Rolle Berechtigungen für den Zugriff auf Ihr Secrets Manager Geheimnis und den Aufruf der erforderlichen öffentlichen APIs für den Connector Amazon RDS (Microsoft SQL Server) zu gewähren und Amazon Kendra. Weitere Informationen finden Sie unter IAM Rollen für Amazon RDS (Microsoft SQL Server-) Datenquellen.

Sie können auch die folgenden optionalen Funktionen hinzufügen:

- Virtual Private Cloud (VPC) — Geben Sie an, `VpcConfiguration` wann Sie anrufen. `CreateDataSource` Weitere Informationen finden Sie unter Konfigurieren von Amazon Kendra für die Verwendung eines Amazon VPC.
- Inklusions- und Ausschlussfilter — Sie können mithilfe von Benutzer-IDs, Gruppen, Quell-URLs, Zeitstempeln und Zeitzonen angeben, ob bestimmte Inhalte eingeschlossen werden sollen.
- Benutzerkontextfilterung und Zugriffskontrolle —Amazon Kendra durchsucht die Zugriffskontrollliste (ACL) für Ihre Dokumente, sofern Sie über eine ACL für Ihre Dokumente verfügen. Die ACL-Informationen werden verwendet, um Suchergebnisse nach dem Benutzer- oder Gruppenzugriff auf Dokumente zu filtern. Weitere Informationen finden Sie unter Benutzerkontextfilterung.
- Feldzuordnungen — Wählen Sie diese Option, um Ihre Datenquellenfelder Amazon RDS (Microsoft SQL Server) Ihren Amazon Kendra Indexfeldern zuzuordnen. Weitere Informationen finden Sie unter Zuweisen von Datenquellenfeldern.

> **Note**
>
> Das Textfeld oder das entsprechende Textfeld für Ihre Dokumente ist erforderlich, um Ihre Dokumente durchsuchen Amazon Kendra zu können. Sie müssen den Feldnamen Ihres Dokumenthauptteils in Ihrer Datenquelle dem Namen des Indexfeldes zuordnen`_document_body`. Alle anderen Felder sind optional.

Eine Liste weiterer wichtiger JSON-Schlüssel, die konfiguriert werden müssen, finden Sie unterAmazon RDS (Microsoft SQL Server) -Vorlagenschema.

Hinweise

- Gelöschte Datenbankzeilen werden nicht nachverfolgt, wenn nach Amazon Kendra aktualisierten Inhalten gesucht wird.
- Die Größe von Feldnamen und Werten in einer Zeile Ihrer Datenbank darf 400 KB nicht überschreiten.
- Wenn Ihre Datenbankdatenquelle eine große Datenmenge enthält und Sie nicht Ihren gesamten Datenbankinhalt nach der ersten Synchronisierung indizieren möchten Amazon Kendra , können Sie wählen, ob nur neue, geänderte oder gelöschte Dokumente synchronisiert werden sollen.

- Es hat sich bewährt, nur lesbare Amazon Kendra Datenbankanmeldeinformationen zur Verfügung zu stellen.
- Es hat sich bewährt, das Hinzufügen von Tabellen mit sensiblen Daten oder personenbezogenen Daten (PII) zu vermeiden.

Amazon RDS (MySQL)

Amazon RDS (Amazon Relational Database Service) ist ein Webservice, der die Einrichtung, den Betrieb und die Skalierung einer relationalen Datenbank in der AWS Cloud erleichtert. Wenn Sie ein Amazon RDS Benutzer sind, können Sie ihn verwenden, um Ihre Amazon Kendra Amazon RDS (MySQL) Datenquelle zu indizieren. Der Amazon Kendra Datenquellen-Connector unterstützt Amazon RDS MySql 5.6, 5.7 und 8.0.

Sie können über Amazon Kendra die Amazon Kendra Konsole und die TemplateConfigurationAPI eine Verbindung zu Ihrer Amazon RDS (MySQL) Datenquelle herstellen.

Informationen zur Fehlerbehebung bei Ihrem Amazon Kendra Amazon RDS (MySQL) Datenquellen-Connector finden Sie unterProblembehandlung bei Datenquellen.

Themen

- Unterstützte Features
- Voraussetzungen
- Anweisungen zur Verbindung
- Hinweise

Unterstützte Features

- Feldzuordnungen
- Filterung des Benutzerkontextes
- Einschluss-/Ausschlussfilter
- Vollständige und inkrementelle Inhaltssynchronisierung
- Virtual Private Cloud (VPC)

Voraussetzungen

Bevor Sie Ihre Amazon RDS (MySQL) Datenquelle Amazon Kendra zum Indizieren verwenden können, nehmen Sie diese Änderungen in Ihren Konten Amazon RDS (MySQL) und AWS Konten vor.

Stellen Sie sicherAmazon RDS (MySQL), dass Sie Folgendes haben:

- Haben Sie sich Ihren Datenbank-Benutzernamen und Ihr Passwort notiert.

> **Important**
>
> Es hat sich bewährt, nur lesbare Amazon Kendra Datenbankanmeldeinformationen zur Verfügung zu stellen.

- Die URL, der Port und die Instanz Ihres Datenbank-Hosts wurden kopiert. Sie finden diese Informationen auf der Amazon RDS Konsole.
- Vergewissert, dass jedes Dokument in Amazon RDS (MySQL) und zwischen anderen Datenquellen, die Sie für denselben Index verwenden möchten, einzigartig ist. Jede Datenquelle, die Sie für einen Index verwenden möchten, darf nicht dasselbe Dokument in allen Datenquellen enthalten. Dokument-IDs gelten für einen Index global und müssen pro Index eindeutig sein.

Stellen Sie sicher AWS-Konto, dass Sie Folgendes in Ihrem haben:

- Hat einen Amazon Kendra Index erstellt und bei Verwendung der API die Index-ID notiert.
- Sie haben eine IAM Rolle für Ihre Datenquelle erstellt und, falls Sie die API verwenden, den ARN der IAM Rolle notiert.

> **Note**
>
> Wenn Sie Ihren Authentifizierungstyp und Ihre Anmeldeinformationen ändern, müssen Sie Ihre IAM Rolle aktualisieren, um auf die richtige AWS Secrets Manager geheime ID zugreifen zu können.

- Wir haben Ihre Amazon RDS (MySQL) Authentifizierungsdaten AWS Secrets Manager geheim gespeichert und, falls Sie die API verwenden, den ARN des Geheimnisses notiert.

> **Note**
>
> Wir empfehlen Ihnen, Ihre Anmeldeinformationen und Ihr Geheimnis regelmäßig zu aktualisieren oder zu wechseln. Stellen Sie zu Ihrer eigenen Sicherheit nur die Zugriffsebene bereit, die erforderlich ist. Wir raten davon ab, Anmeldeinformationen und geheime Daten für alle Datenquellen und Connector-Versionen 1.0 und 2.0 (sofern zutreffend) wiederzuverwenden.

Wenn Sie noch keine IAM Rolle oder keinen Schlüssel haben, können Sie die Konsole verwenden, um eine neue IAM Rolle und ein neues Secrets Manager Geheimnis zu erstellen, wenn Sie Ihre Amazon RDS (MySQL) Datenquelle mit verbinden. Amazon Kendra Wenn Sie die API verwenden, müssen Sie den ARN einer vorhandenen IAM Rolle und eines Secrets Manager Geheimnisses sowie eine Index-ID angeben.

Anweisungen zur Verbindung

Um eine Verbindung Amazon Kendra zu Ihrer Amazon RDS (MySQL) Datenquelle herzustellen, müssen Sie Details zu Ihren Amazon RDS (MySQL) Anmeldeinformationen angeben, damit Sie auf Ihre Daten zugreifen Amazon Kendra können. Falls Sie das noch nicht konfiguriert haben, Amazon Kendra finden Sie Amazon RDS (MySQL) weitere Informationen unterVoraussetzungen.

Console

Um eine Verbindung Amazon Kendra herzustellen Amazon RDS (MySQL)

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die Amazon Kendra Konsole.
2. Wählen Sie im linken Navigationsbereich Indizes und dann den Index, den Sie verwenden möchten, aus der Indexliste aus.

   > **Note**
   >
   > Sie können Ihre Einstellungen für die Benutzerzugriffskontrolle unter Indexeinstellungen konfigurieren oder bearbeiten.

3. Wählen Sie auf der Seite Erste Schritte die Option Datenquelle hinzufügen aus.

4. Wählen Sie auf der Seite Datenquelle hinzufügen die Option Amazon RDS (MySQL)Connector und dann Connector hinzufügen aus.
5. Geben Sie auf der Seite „Datenquellendetails angeben“ die folgenden Informationen ein:
    a. Geben Sie im Feld Name und Beschreibung für Datenquellenname einen Namen für Ihre Datenquelle ein. Sie können Bindestriche, aber keine Leerzeichen verwenden.
    b. (Optional) Beschreibung — Geben Sie eine optionale Beschreibung für Ihre Datenquelle ein.
    c. In Standardsprache — Wählen Sie eine Sprache aus, um Ihre Dokumente nach dem Index zu filtern. Sofern Sie nichts anderes angeben, ist die Standardsprache Englisch. Die in den Metadaten des Dokuments angegebene Sprache hat Vorrang vor der ausgewählten Sprache.
    d. Unter Tags für Neues Tag hinzufügen — Fügen Sie optionale Tags hinzu, um Ihre Ressourcen zu durchsuchen und zu filtern oder Ihre Kosten nachzuverfolgen. AWS
    e. Wählen Sie Weiter aus.
6. Geben Sie auf der Seite Zugriff und Sicherheit definieren die folgenden Informationen ein:
    a. Geben Sie im Feld Quelle die folgenden Informationen ein:
    b. Host — Geben Sie die URL des Datenbank-Hosts ein, zum Beispiel:`http://`*`instance URL`*`.`*`region`*`.rds.amazonaws.com`.
    c. Port — Geben Sie den Datenbankport ein, zum Beispiel`5432`.
    d. Instanz — Geben Sie zum Beispiel die Datenbankinstanz ein`postgres`.
    e. Speicherort für SSL-Zertifikate aktivieren — Geben Sie hier den Amazon S3 Pfad zu Ihrer SSL-Zertifikatsdatei ein.
    f. Geben Sie im Feld Authentifizierung die folgenden Informationen ein:
        - AWS Secrets Manager geheim — Wählen Sie ein vorhandenes Geheimnis aus, oder erstellen Sie ein neues Secrets Manager Geheimnis, um Ihre Amazon RDS (MySQL) Authentifizierungsdaten zu speichern. Wenn Sie ein neues Geheimnis erstellen möchten, wird ein AWS Secrets Manager geheimes Fenster geöffnet.
            A. Geben Sie die folgenden Informationen in das Fenster Create an AWS Secrets Manager Secret ein:

I. Geheimer Name — Ein Name für Ihr Geheimnis. Das Präfix 'AmazonKendra- Amazon RDS (MySQL) -' wird automatisch zu Ihrem geheimen Namen hinzugefügt.

II. Für Datenbankbenutzername und Passwort — Geben Sie die Werte der Authentifizierungsdaten ein, die Sie aus Ihrer Datenbank kopiert haben.

B. Wählen Sie Speichern.

g. Virtual Private Cloud (VPC) — Sie können wählen, ob Sie eine VPC verwenden möchten. In diesem Fall müssen Sie Subnetze und VPC-Sicherheitsgruppen hinzufügen.

h. IAM Rolle — Wählen Sie eine bestehende IAM Rolle oder erstellen Sie eine neue IAM Rolle, um auf Ihre Repository-Anmeldeinformationen und Indexinhalte zuzugreifen.

> **Note**
>
> IAM Rollen, die für Indizes verwendet werden, können nicht für Datenquellen verwendet werden. Wenn Sie sich nicht sicher sind, ob eine vorhandene Rolle für einen Index oder eine häufig gestellte Frage verwendet wird, wählen Sie Neue Rolle erstellen, um Fehler zu vermeiden.

i. Wählen Sie Weiter aus.

7. Geben Sie auf der Seite „Synchronisierungseinstellungen konfigurieren“ die folgenden Informationen ein:

a. Wählen Sie unter Synchronisierungsbereich eine der folgenden Optionen aus:

- SQL-Abfrage — Geben Sie SQL-Abfrageanweisungen wie SELECT- und JOIN-Operationen ein. SQL-Abfragen müssen weniger als 32 KB groß sein. SQL-Abfragen müssen weniger als 32 KB groß sein und dürfen keine Semikolons (;) enthalten. Amazon Kendra durchsucht den gesamten Datenbankinhalt, der Ihrer Abfrage entspricht.
- Primärschlüsselspalte — Geben Sie den Primärschlüssel für die Datenbanktabelle an. Dadurch wird eine Tabelle in Ihrer Datenbank identifiziert.
- Titelspalte — Geben Sie den Namen der Titelspalte des Dokuments in Ihrer Datenbanktabelle an.
- Hauptspalte — Geben Sie den Namen der Hauptspalte des Dokuments in Ihrer Datenbanktabelle an.

b. Wählen Sie unter Zusätzliche Konfiguration — optional aus den folgenden Optionen, um bestimmte Inhalte zu synchronisieren, anstatt alle Dateien zu synchronisieren:

- Spalten zur Erkennung von Änderungen — Geben Sie die Namen der Spalten ein, anhand derer Inhaltsänderungen erkannt Amazon Kendra werden sollen. Amazon Kendra indexiert den Inhalt neu, wenn sich eine dieser Spalten ändert.
- Spalte mit Benutzer-IDs — Geben Sie den Namen der Spalte ein, die Benutzer-IDs enthält, um Zugriff auf Inhalte zu erhalten.
- Spalte „Gruppen“ — Geben Sie den Namen der Spalte ein, die Gruppen enthält, denen der Zugriff auf Inhalte gewährt werden soll.
- Spalte Quell-URLs — Geben Sie den Namen der Spalte ein, die Quell-URLs enthält, die indexiert werden sollen.
- Spalte mit Zeitstempeln — Geben Sie den Namen der Spalte ein, die Zeitstempel enthält. Amazon Kendra verwendet Zeitstempelinformationen, um Änderungen an Ihren Inhalten zu erkennen und nur geänderte Inhalte zu synchronisieren.
- Spalte „Zeitzonen“ — Geben Sie den Namen der Spalte ein, die Zeitzonen für den Inhalt enthält, der gecrawlt werden soll.
- Zeitstempelformat — Geben Sie den Namen der Spalte ein, die Zeitstempelformate enthält, anhand derer Inhaltsänderungen erkannt und Ihre Inhalte erneut synchronisiert werden sollen.

c. Synchronisierungsmodus — Wählen Sie aus, wie Sie Ihren Index aktualisieren möchten, wenn sich der Inhalt Ihrer Datenquelle ändert. Wenn Sie Ihre Datenquelle Amazon Kendra zum ersten Mal synchronisieren, werden alle Inhalte standardmäßig gecrawlt und indexiert. Sie müssen eine vollständige Synchronisierung Ihrer Daten durchführen, falls Ihre erste Synchronisierung fehlgeschlagen ist, auch wenn Sie die Option Vollsynchronisierung nicht als Synchronisierungsmodusoption wählen.

- Vollständige Synchronisierung: Indizieren Sie den gesamten Inhalt neu und ersetzen die vorhandenen Inhalte jedes Mal, wenn Ihre Datenquelle mit Ihrem Index synchronisiert wird.
- Neue, geänderte Synchronisierung: Indizieren Sie jedes Mal, wenn Ihre Datenquelle mit Ihrem Index synchronisiert wird, nur neue und geänderte Inhalte. Amazon Kendra kann den Mechanismus Ihrer Datenquelle verwenden, um Inhaltsänderungen nachzuverfolgen und Inhalte zu indexieren, die sich seit der letzten Synchronisierung geändert haben.

- Neue, geänderte, gelöschte Synchronisierung: Indizieren Sie bei jeder Synchronisierung Ihrer Datenquelle mit Ihrem Index nur neue, geänderte und gelöschte Inhalte. Amazon Kendra kann den Mechanismus Ihrer Datenquelle verwenden, um Inhaltsänderungen nachzuverfolgen und Inhalte zu indexieren, die sich seit der letzten Synchronisierung geändert haben.

d. Im Synchronisierungslaufplan für Frequenz — Wie oft Amazon Kendra wird mit Ihrer Datenquelle synchronisiert?

e. Wählen Sie Weiter aus.

8. Geben Sie auf der Seite Feldzuordnungen festlegen die folgenden Informationen ein:

a. Wählen Sie aus den generierten Standard-Datenquellenfeldern — Dokument-IDs, Dokumenttitel und Quell-URLs — aus, die Sie dem Index zuordnen möchten. Amazon Kendra

b. Feld hinzufügen — Um benutzerdefinierte Datenquellenfelder hinzuzufügen, um einen Indexfeldnamen für die Zuordnung und den Felddatentyp zu erstellen.

c. Wählen Sie Weiter aus.

9. Überprüfen Sie auf der Seite Überprüfen und erstellen, ob die von Ihnen eingegebenen Informationen korrekt sind, und wählen Sie dann Datenquelle hinzufügen aus. Sie können Ihre Informationen auch auf dieser Seite bearbeiten. Ihre Datenquelle wird auf der Seite Datenquellen angezeigt, nachdem die Datenquelle erfolgreich hinzugefügt wurde.

API

Um eine Verbindung Amazon Kendra herzustellen Amazon RDS (MySQL)

Mithilfe der TemplateConfigurationAPI müssen Sie Folgendes angeben:

- Datenquelle — Geben Sie den Datenquellentyp wie `JDBC` bei der Verwendung des TemplateConfigurationJSON-Schemas an. Geben Sie außerdem die Datenquelle so an`TEMPLATE`, wie Sie die CreateDataSourceAPI aufrufen.
- Datenbanktyp — Sie müssen den Datenbanktyp als `mySql` angeben.
- SQL-Abfrage — Geben Sie SQL-Abfrageanweisungen wie SELECT- und JOIN-Operationen an. SQL-Abfragen müssen weniger als 32 KB groß sein. Amazon Kendra durchsucht den gesamten Datenbankinhalt, der Ihrer Abfrage entspricht.
- Synchronisierungsmodus — Geben Sie an, wie Ihr Index aktualisiert Amazon Kendra werden soll, wenn sich der Inhalt Ihrer Datenquelle ändert. Wenn Sie Ihre Datenquelle Amazon Kendra

zum ersten Mal synchronisieren, werden alle Inhalte standardmäßig gecrawlt und indexiert. Sie müssen eine vollständige Synchronisierung Ihrer Daten durchführen, falls Ihre erste Synchronisierung fehlgeschlagen ist, auch wenn Sie die Option Vollsynchronisierung nicht als Synchronisierungsmodusoption wählen. Sie können wählen zwischen:

- `FORCED_FULL_CRAWL`um den gesamten Inhalt neu zu indizieren und vorhandene Inhalte jedes Mal zu ersetzen, wenn Ihre Datenquelle mit Ihrem Index synchronisiert wird.
- `FULL_CRAWL`um bei jeder Synchronisierung Ihrer Datenquelle mit Ihrem Index nur neue, geänderte und gelöschte Inhalte zu indizieren. Amazon Kendra kann den Mechanismus Ihrer Datenquelle verwenden, um Inhaltsänderungen nachzuverfolgen und Inhalte zu indexieren, die sich seit der letzten Synchronisierung geändert haben.
- `CHANGE_LOG`um jedes Mal, wenn Ihre Datenquelle mit Ihrem Index synchronisiert wird, nur neue und geänderte Inhalte zu indizieren. Amazon Kendra kann den Mechanismus Ihrer Datenquelle verwenden, um Inhaltsänderungen nachzuverfolgen und Inhalte zu indexieren, die sich seit der letzten Synchronisierung geändert haben.

- Geheimer Amazon-Ressourcenname (ARN) — Geben Sie den Amazon-Ressourcennamen (ARN) eines Secrets Manager Geheimnisses ein, das die Authentifizierungsdaten enthält, die Sie in Ihrem Amazon RDS (MySQL) Konto erstellt haben. Das Geheimnis wird in einer JSON-Struktur mit den folgenden Schlüsseln gespeichert:

```
{
    "user name": "database user name",
    "password": "password"
}
```

> **Note**
>
> Wir empfehlen Ihnen, Ihre Anmeldeinformationen und Ihr Geheimnis regelmäßig zu aktualisieren oder zu wechseln. Stellen Sie zu Ihrer eigenen Sicherheit nur die Zugriffsebene bereit, die erforderlich ist. Wir raten davon ab, Anmeldeinformationen und geheime Daten für alle Datenquellen und Connector-Versionen 1.0 und 2.0 (sofern zutreffend) wiederzuverwenden.

- IAM Rolle — Geben Sie an`RoleArn`, wann Sie anrufen`CreateDataSource`, um einer IAM Rolle Berechtigungen für den Zugriff auf Ihr Secrets Manager Geheimnis und für den Aufruf der erforderlichen öffentlichen APIs für den Amazon RDS (MySQL) Connector und zum Aufrufen

der erforderlichen öffentlichen APIs zu erteilen. Amazon Kendra Weitere Informationen finden Sie unter IAM Rollen für Amazon RDS (MySQL) Datenquellen.

Sie können auch die folgenden optionalen Funktionen hinzufügen:

- Virtual Private Cloud (VPC) — Geben Sie an, `VpcConfiguration` wann Sie anrufen. `CreateDataSource` Weitere Informationen finden Sie unter Konfigurieren von Amazon Kendra für die Verwendung eines Amazon VPC.
- Inklusions- und Ausschlussfilter — Sie können mithilfe von Benutzer-IDs, Gruppen, Quell-URLs, Zeitstempeln und Zeitzonen angeben, ob bestimmte Inhalte eingeschlossen werden sollen.
- Feldzuordnungen — Wählen Sie diese Option, um Ihre Amazon RDS (MySQL) Datenquellenfelder Ihren Indexfeldern zuzuordnen. Amazon Kendra Weitere Informationen finden Sie unter Zuweisen von Datenquellenfeldern.

  > **Note**
  >
  > Das Textfeld oder das entsprechende Textfeld für Ihre Dokumente ist erforderlich, um Ihre Dokumente durchsuchen Amazon Kendra zu können. Sie müssen den Feldnamen Ihres Dokumenthauptteils in Ihrer Datenquelle dem Namen des Indexfeldes zuordnen`_document_body`. Alle anderen Felder sind optional.

- Benutzerkontextfilterung und ZugriffskontrolleAmazon Kendra — durchsucht die Zugriffskontrollliste (ACL) für Ihre Dokumente, sofern Sie über eine ACL für Ihre Dokumente verfügen. Die ACL-Informationen werden verwendet, um Suchergebnisse nach dem Benutzer- oder Gruppenzugriff auf Dokumente zu filtern. Weitere Informationen finden Sie unter Benutzerkontextfilterung.

Eine Liste weiterer wichtiger JSON-Schlüssel, die konfiguriert werden müssen, finden Sie unterAmazon RDS (MySQL) Vorlagenschema.

Hinweise

- Gelöschte Datenbankzeilen werden nicht nachverfolgt, wenn nach Amazon Kendra aktualisiertem Inhalt gesucht wird.
- Die Größe von Feldnamen und Werten in einer Zeile Ihrer Datenbank darf 400 KB nicht überschreiten.

- Wenn Ihre Datenbankdatenquelle eine große Datenmenge enthält und Sie nicht Ihren gesamten Datenbankinhalt nach der ersten Synchronisierung indizieren möchten Amazon Kendra , können Sie wählen, ob nur neue, geänderte oder gelöschte Dokumente synchronisiert werden sollen.
- Es hat sich bewährt, nur lesbare Amazon Kendra Datenbankanmeldeinformationen zur Verfügung zu stellen.
- Es hat sich bewährt, das Hinzufügen von Tabellen mit sensiblen Daten oder personenbezogenen Daten (PII) zu vermeiden.

Amazon RDS (Oracle)

Amazon RDS (Amazon Relational Database Service) ist ein Webservice, der die Einrichtung, den Betrieb und die Skalierung einer relationalen Datenbank in der AWS Cloud erleichtert. Wenn Sie ein Amazon RDS (Oracle) Benutzer sind, können Sie ihn verwenden, um Ihre Amazon Kendra Amazon RDS (Oracle) Datenquelle zu indizieren. Der Amazon Kendra Amazon RDS (Oracle) Datenquellen-Connector unterstützt Amazon RDS Oracle Database 21c, Oracle Database 19c, Oracle Database 12c.

Sie können über Amazon Kendra die Amazon Kendra Konsole und die API eine Verbindung zu Ihrer Amazon RDS (Oracle) Datenquelle herstellen. TemplateConfiguration

Informationen zur Fehlerbehebung bei Ihrem Amazon Kendra Amazon RDS (Oracle) Datenquellen-Connector finden Sie unterProblembehandlung bei Datenquellen.

Themen

- Unterstützte Features
- Voraussetzungen
- Anweisungen zur Verbindung
- Hinweise

Unterstützte Features

- Feldzuordnungen
- Filterung des Benutzerkontextes
- Einschluss-/Ausschlussfilter
- Vollständige und inkrementelle Inhaltssynchronisierung

- Virtual Private Cloud (VPC)

Voraussetzungen

Bevor Sie Ihre Amazon RDS (Oracle) Datenquelle Amazon Kendra zum Indizieren verwenden können, nehmen Sie diese Änderungen in Ihren Konten Amazon RDS (Oracle) und AWS Konten vor.

Stellen Sie sicherAmazon RDS (Oracle), dass Sie Folgendes haben:

- Haben Sie sich Ihren Datenbank-Benutzernamen und Ihr Passwort notiert.

> **Important**
>
> Es hat sich bewährt, nur lesbare Amazon Kendra Datenbankanmeldeinformationen zur Verfügung zu stellen.

- Die URL, der Port und die Instanz Ihres Datenbank-Hosts wurden kopiert.
- Vergewissert, dass jedes Dokument in Amazon RDS (Oracle) und zwischen anderen Datenquellen, die Sie für denselben Index verwenden möchten, einzigartig ist. Jede Datenquelle, die Sie für einen Index verwenden möchten, darf nicht dasselbe Dokument in allen Datenquellen enthalten. Dokument-IDs gelten für einen Index global und müssen pro Index eindeutig sein.

Stellen Sie sicher AWS-Konto, dass Sie Folgendes in Ihrem haben:

- Hat einen Amazon Kendra Index erstellt und bei Verwendung der API die Index-ID notiert.
- Sie haben eine IAM Rolle für Ihre Datenquelle erstellt und, falls Sie die API verwenden, den ARN der IAM Rolle notiert.

> **Note**
>
> Wenn Sie Ihren Authentifizierungstyp und Ihre Anmeldeinformationen ändern, müssen Sie Ihre IAM Rolle aktualisieren, um auf die richtige AWS Secrets Manager geheime ID zugreifen zu können.

- Wir haben Ihre Amazon RDS (Oracle) Authentifizierungsdaten AWS Secrets Manager geheim gespeichert und, falls Sie die API verwenden, den ARN des Geheimnisses notiert.

> **Note**
>
> Wir empfehlen Ihnen, Ihre Anmeldeinformationen und Ihr Geheimnis regelmäßig zu aktualisieren oder zu wechseln. Stellen Sie zu Ihrer eigenen Sicherheit nur die Zugriffsebene bereit, die erforderlich ist. Wir raten davon ab, Anmeldeinformationen und geheime Daten für alle Datenquellen und Connector-Versionen 1.0 und 2.0 (sofern zutreffend) wiederzuverwenden.

Wenn Sie noch keine IAM Rolle oder keinen Schlüssel haben, können Sie die Konsole verwenden, um eine neue IAM Rolle und ein neues Secrets Manager Geheimnis zu erstellen, wenn Sie Ihre Amazon RDS (Oracle) Datenquelle mit verbinden. Amazon Kendra Wenn Sie die API verwenden, müssen Sie den ARN einer vorhandenen IAM Rolle und eines Secrets Manager Geheimnisses sowie eine Index-ID angeben.

Anweisungen zur Verbindung

Um eine Verbindung Amazon Kendra zu Ihrer Amazon RDS (Oracle) Datenquelle herzustellen, müssen Sie Details zu Ihren Amazon RDS (Oracle) Anmeldeinformationen angeben, damit Sie auf Ihre Daten zugreifen Amazon Kendra können. Falls Sie das noch nicht konfiguriert haben, Amazon Kendra finden Sie Amazon RDS (Oracle) weitere Informationen unterVoraussetzungen.

Console

Um eine Verbindung Amazon Kendra herzustellen Amazon RDS (Oracle)

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die Amazon Kendra Konsole.
2. Wählen Sie im linken Navigationsbereich Indizes und dann den Index, den Sie verwenden möchten, aus der Indexliste aus.

   > **Note**
   >
   > Sie können Ihre Einstellungen für die Benutzerzugriffskontrolle unter Indexeinstellungen konfigurieren oder bearbeiten.

3. Wählen Sie auf der Seite Erste Schritte die Option Datenquelle hinzufügen aus.

4. Wählen Sie auf der Seite Datenquelle hinzufügen die Option Amazon RDS (Oracle)Connector und dann Connector hinzufügen aus.
5. Geben Sie auf der Seite „Datenquellendetails angeben“ die folgenden Informationen ein:
    a. Geben Sie im Feld Name und Beschreibung für Datenquellenname einen Namen für Ihre Datenquelle ein. Sie können Bindestriche, aber keine Leerzeichen verwenden.
    b. (Optional) Beschreibung — Geben Sie eine optionale Beschreibung für Ihre Datenquelle ein.
    c. In Standardsprache — Wählen Sie eine Sprache aus, um Ihre Dokumente nach dem Index zu filtern. Sofern Sie nichts anderes angeben, ist die Standardsprache Englisch. Die in den Metadaten des Dokuments angegebene Sprache hat Vorrang vor der ausgewählten Sprache.
    d. Unter Tags für Neues Tag hinzufügen — Fügen Sie optionale Tags hinzu, um Ihre Ressourcen zu durchsuchen und zu filtern oder Ihre Kosten nachzuverfolgen. AWS
    e. Wählen Sie Weiter aus.
6. Geben Sie auf der Seite Zugriff und Sicherheit definieren die folgenden Informationen ein:
    a. Geben Sie im Feld Quelle die folgenden Informationen ein:
    b. Host — Geben Sie den Datenbank-Hostnamen ein.
    c. Port — Geben Sie den Datenbankport ein.
    d. Instanz — Geben Sie die Datenbankinstanz ein.
    e. Speicherort für SSL-Zertifikate aktivieren — Geben Sie hier den Amazon S3 Pfad zu Ihrer SSL-Zertifikatsdatei ein.
    f. Geben Sie im Feld Authentifizierung die folgenden Informationen ein:
        - AWS Secrets Manager geheim — Wählen Sie ein vorhandenes Geheimnis aus, oder erstellen Sie ein neues Secrets Manager Geheimnis, um Ihre Amazon RDS (Oracle) Authentifizierungsdaten zu speichern. Wenn Sie sich dafür entscheiden, ein neues Geheimnis zu erstellen, wird ein AWS Secrets Manager geheimes Fenster geöffnet.
            A. Geben Sie die folgenden Informationen in das Fenster Create an AWS Secrets Manager Secret ein:

I. Geheimer Name — Ein Name für Ihr Geheimnis. Das Präfix 'AmazonKendra- Amazon RDS (Oracle) -' wird Ihrem geheimen Namen automatisch hinzugefügt.

II. Für Datenbankbenutzername und Passwort — Geben Sie die Werte der Authentifizierungsdaten ein, die Sie aus Ihrer Datenbank kopiert haben.

B. Wählen Sie Speichern.

g. Virtual Private Cloud (VPC) — Sie können wählen, ob Sie eine VPC verwenden möchten. In diesem Fall müssen Sie Subnetze und VPC-Sicherheitsgruppen hinzufügen.

h. IAM Rolle — Wählen Sie eine bestehende IAM Rolle oder erstellen Sie eine neue IAM Rolle, um auf Ihre Repository-Anmeldeinformationen und Indexinhalte zuzugreifen.

> **Note**
>
> IAM Rollen, die für Indizes verwendet werden, können nicht für Datenquellen verwendet werden. Wenn Sie sich nicht sicher sind, ob eine vorhandene Rolle für einen Index oder eine häufig gestellte Frage verwendet wird, wählen Sie Neue Rolle erstellen, um Fehler zu vermeiden.

i. Wählen Sie Weiter aus.

7. Geben Sie auf der Seite „Synchronisierungseinstellungen konfigurieren“ die folgenden Informationen ein:

a. Wählen Sie unter Synchronisierungsbereich eine der folgenden Optionen aus:

- SQL-Abfrage — Geben Sie SQL-Abfrageanweisungen wie SELECT- und JOIN-Operationen ein. SQL-Abfragen müssen weniger als 32 KB groß sein. Amazon Kendra durchsucht den gesamten Datenbankinhalt, der Ihrer Abfrage entspricht.
- Primärschlüsselspalte — Geben Sie den Primärschlüssel für die Datenbanktabelle an. Dies identifiziert eine Tabelle in Ihrer Datenbank.
- Titelspalte — Geben Sie den Namen der Titelspalte des Dokuments in Ihrer Datenbanktabelle an.
- Hauptspalte — Geben Sie den Namen der Hauptspalte des Dokuments in Ihrer Datenbanktabelle an.

b. Wählen Sie unter Zusätzliche Konfiguration — optional aus den folgenden Optionen, um bestimmte Inhalte zu synchronisieren, anstatt alle Dateien zu synchronisieren:

- Spalten zur Erkennung von Änderungen — Geben Sie die Namen der Spalten ein, anhand derer Inhaltsänderungen erkannt Amazon Kendra werden sollen. Amazon Kendra indexiert den Inhalt neu, wenn sich eine dieser Spalten ändert.
- Spalte mit Benutzer-IDs — Geben Sie den Namen der Spalte ein, die Benutzer-IDs enthält, um Zugriff auf Inhalte zu erhalten.
- Spalte „Gruppen“ — Geben Sie den Namen der Spalte ein, die Gruppen enthält, denen der Zugriff auf Inhalte gewährt werden soll.
- Spalte Quell-URLs — Geben Sie den Namen der Spalte ein, die Quell-URLs enthält, die indexiert werden sollen.
- Spalte mit Zeitstempeln — Geben Sie den Namen der Spalte ein, die Zeitstempel enthält. Amazon Kendra verwendet Zeitstempelinformationen, um Änderungen an Ihren Inhalten zu erkennen und nur geänderte Inhalte zu synchronisieren.
- Spalte „Zeitzonen“ — Geben Sie den Namen der Spalte ein, die Zeitzonen für den Inhalt enthält, der gecrawlt werden soll.
- Zeitstempelformat — Geben Sie den Namen der Spalte ein, die Zeitstempelformate enthält, anhand derer Inhaltsänderungen erkannt und Ihre Inhalte erneut synchronisiert werden sollen.

c. Synchronisierungsmodus — Wählen Sie aus, wie Sie Ihren Index aktualisieren möchten, wenn sich der Inhalt Ihrer Datenquelle ändert. Wenn Sie Ihre Datenquelle Amazon Kendra zum ersten Mal synchronisieren, werden alle Inhalte standardmäßig gecrawlt und indexiert. Sie müssen eine vollständige Synchronisierung Ihrer Daten durchführen, falls Ihre erste Synchronisierung fehlgeschlagen ist, auch wenn Sie die Option Vollsynchronisierung nicht als Synchronisierungsmodusoption wählen.

   - Vollständige Synchronisierung: Indizieren Sie den gesamten Inhalt neu und ersetzen die vorhandenen Inhalte jedes Mal, wenn Ihre Datenquelle mit Ihrem Index synchronisiert wird.
   - Neue, geänderte Synchronisierung: Indizieren Sie jedes Mal, wenn Ihre Datenquelle mit Ihrem Index synchronisiert wird, nur neue und geänderte Inhalte. Amazon Kendra kann den Mechanismus Ihrer Datenquelle verwenden, um Inhaltsänderungen nachzuverfolgen und Inhalte zu indexieren, die sich seit der letzten Synchronisierung geändert haben.
   - Neue, geänderte, gelöschte Synchronisierung: Indizieren Sie bei jeder Synchronisierung Ihrer Datenquelle mit Ihrem Index nur neue, geänderte und

gelöschte Inhalte. Amazon Kendra kann den Mechanismus Ihrer Datenquelle verwenden, um Inhaltsänderungen nachzuverfolgen und Inhalte zu indexieren, die sich seit der letzten Synchronisierung geändert haben.

d. Im Synchronisierungslaufplan für Frequenz — Wie oft Amazon Kendra wird mit Ihrer Datenquelle synchronisiert?

e. Wählen Sie Weiter aus.

8. Geben Sie auf der Seite Feldzuordnungen festlegen die folgenden Informationen ein:

a. Wählen Sie aus den generierten Standard-Datenquellenfeldern — Dokument-IDs, Dokumenttitel und Quell-URLs — aus, die Sie dem Index zuordnen möchten. Amazon Kendra

b. Feld hinzufügen — Um benutzerdefinierte Datenquellenfelder hinzuzufügen, um einen Indexfeldnamen für die Zuordnung und den Felddatentyp zu erstellen.

c. Wählen Sie Weiter aus.

9. Überprüfen Sie auf der Seite Überprüfen und erstellen, ob die von Ihnen eingegebenen Informationen korrekt sind, und wählen Sie dann Datenquelle hinzufügen aus. Sie können Ihre Informationen auch auf dieser Seite bearbeiten. Ihre Datenquelle wird auf der Seite Datenquellen angezeigt, nachdem die Datenquelle erfolgreich hinzugefügt wurde.

API

Um eine Verbindung Amazon Kendra herzustellen Amazon RDS (Oracle)

Mithilfe der TemplateConfigurationAPI müssen Sie Folgendes angeben:

- Datenquelle — Geben Sie den Datenquellentyp wie `JDBC` bei der Verwendung des TemplateConfigurationJSON-Schemas an. Geben Sie außerdem die Datenquelle so an`TEMPLATE`, wie Sie die CreateDataSourceAPI aufrufen.
- Datenbanktyp — Sie müssen den Datenbanktyp als `oracle` angeben.
- SQL-Abfrage — Geben Sie SQL-Abfrageanweisungen wie SELECT- und JOIN-Operationen an. SQL-Abfragen müssen weniger als 32 KB groß sein. Amazon Kendra durchsucht den gesamten Datenbankinhalt, der Ihrer Abfrage entspricht.
- Synchronisierungsmodus — Geben Sie an, wie Ihr Index aktualisiert Amazon Kendra werden soll, wenn sich der Inhalt Ihrer Datenquelle ändert. Wenn Sie Ihre Datenquelle Amazon Kendra zum ersten Mal synchronisieren, werden alle Inhalte standardmäßig gecrawlt und indexiert. Sie müssen eine vollständige Synchronisierung Ihrer Daten durchführen, falls Ihre erste

Synchronisierung fehlgeschlagen ist, auch wenn Sie die Option Vollsynchronisierung nicht als Synchronisierungsmodusoption wählen. Sie können wählen zwischen:

- `FORCED_FULL_CRAWL`um den gesamten Inhalt neu zu indizieren und vorhandene Inhalte jedes Mal zu ersetzen, wenn Ihre Datenquelle mit Ihrem Index synchronisiert wird.
- `FULL_CRAWL`um bei jeder Synchronisierung Ihrer Datenquelle mit Ihrem Index nur neue, geänderte und gelöschte Inhalte zu indizieren. Amazon Kendra kann den Mechanismus Ihrer Datenquelle verwenden, um Inhaltsänderungen nachzuverfolgen und Inhalte zu indexieren, die sich seit der letzten Synchronisierung geändert haben.
- `CHANGE_LOG`um jedes Mal, wenn Ihre Datenquelle mit Ihrem Index synchronisiert wird, nur neue und geänderte Inhalte zu indizieren. Amazon Kendra kann den Mechanismus Ihrer Datenquelle verwenden, um Inhaltsänderungen nachzuverfolgen und Inhalte zu indexieren, die sich seit der letzten Synchronisierung geändert haben.

- Geheimer Amazon-Ressourcenname (ARN) — Geben Sie den Amazon-Ressourcennamen (ARN) eines Secrets Manager Geheimnisses ein, das die Authentifizierungsdaten enthält, die Sie in Ihrem Amazon RDS (Oracle) Konto erstellt haben. Das Geheimnis wird in einer JSON-Struktur mit den folgenden Schlüsseln gespeichert:

```
{
    "user name": "database user name",
    "password": "password"
}
```

> **Note**
>
> Wir empfehlen Ihnen, Ihre Anmeldeinformationen und Ihr Geheimnis regelmäßig zu aktualisieren oder zu wechseln. Stellen Sie zu Ihrer eigenen Sicherheit nur die Zugriffsebene bereit, die erforderlich ist. Wir raten davon ab, Anmeldeinformationen und geheime Daten für alle Datenquellen und Connector-Versionen 1.0 und 2.0 (sofern zutreffend) wiederzuverwenden.

- IAM Rolle — Geben Sie an`RoleArn`, wann Sie anrufen`CreateDataSource`, um einer IAM Rolle Berechtigungen für den Zugriff auf Ihr Secrets Manager Geheimnis und für den Aufruf der erforderlichen öffentlichen APIs für den Amazon RDS (Oracle) Connector und zum Aufrufen der erforderlichen öffentlichen APIs zu erteilen. Amazon Kendra Weitere Informationen finden Sie unter IAM Rollen für Amazon RDS (Oracle) Datenquellen.

Sie können auch die folgenden optionalen Funktionen hinzufügen:

- Virtual Private Cloud (VPC) — Geben Sie an, `VpcConfiguration` wann Sie anrufen. `CreateDataSource` Weitere Informationen finden Sie unter Konfigurieren von Amazon Kendra für die Verwendung eines Amazon VPC.
- Inklusions- und Ausschlussfilter — Sie können mithilfe von Benutzer-IDs, Gruppen, Quell-URLs, Zeitstempeln und Zeitzonen angeben, ob bestimmte Inhalte eingeschlossen werden sollen.
- Benutzerkontextfilterung und Zugriffskontrolle —Amazon Kendra durchsucht die Zugriffskontrollliste (ACL) für Ihre Dokumente, sofern Sie über eine ACL für Ihre Dokumente verfügen. Die ACL-Informationen werden verwendet, um Suchergebnisse nach dem Benutzer- oder Gruppenzugriff auf Dokumente zu filtern. Weitere Informationen finden Sie unter Benutzerkontextfilterung.
- Feldzuordnungen — Wählen Sie diese Option, um Ihre Amazon RDS (Oracle) Datenquellenfelder Ihren Indexfeldern zuzuordnen. Amazon Kendra Weitere Informationen finden Sie unter Zuweisen von Datenquellenfeldern.

> **Note**
>
> Das Textfeld oder das entsprechende Textfeld für Ihre Dokumente ist erforderlich, um Ihre Dokumente durchsuchen Amazon Kendra zu können. Sie müssen den Feldnamen Ihres Dokumenthauptteils in Ihrer Datenquelle dem Namen des Indexfeldes zuordnen`_document_body`. Alle anderen Felder sind optional.

Eine Liste weiterer wichtiger JSON-Schlüssel, die konfiguriert werden müssen, finden Sie unterAmazon RDS (Oracle) Vorlagenschema.

Hinweise

- Gelöschte Datenbankzeilen werden nicht nachverfolgt, wenn nach Amazon Kendra aktualisiertem Inhalt gesucht wird.
- Die Größe von Feldnamen und Werten in einer Zeile Ihrer Datenbank darf 400 KB nicht überschreiten.
- Wenn Ihre Datenbankdatenquelle eine große Datenmenge enthält und Sie nicht möchten Amazon Kendra , dass Ihr gesamter Datenbankinhalt nach der ersten Synchronisierung indexiert wird,

können Sie wählen, ob nur neue, geänderte oder gelöschte Dokumente synchronisiert werden sollen.

- Es hat sich bewährt, nur lesbare Amazon Kendra Datenbankanmeldeinformationen zur Verfügung zu stellen.
- Es hat sich bewährt, das Hinzufügen von Tabellen mit sensiblen Daten oder personenbezogenen Daten (PII) zu vermeiden.

Amazon RDS (PostgreSQL)

Amazon RDS ist ein Webservice, der es einfacher macht, eine relationale Datenbank in der AWS Cloud einzurichten, zu betreiben und zu skalieren. Wenn Sie ein Amazon RDS Benutzer sind, können Sie Amazon Kendra damit Ihre Amazon RDS (PostgreSQL) Datenquelle indizieren. Der Amazon Kendra Amazon RDS (PostgreSQL) Datenquellenconnector unterstützt PostgreSQL 9.6.

Sie können über Amazon Kendra die Amazon Kendra Konsole und die API eine Verbindung zu Ihrer Amazon RDS (PostgreSQL) Datenquelle herstellen. TemplateConfiguration

Informationen zur Fehlerbehebung bei Ihrem Amazon Kendra Amazon RDS (PostgreSQL) Datenquellen-Connector finden Sie unterProblembehandlung bei Datenquellen.

Themen

- Unterstützte Features
- Voraussetzungen
- Anweisungen zur Verbindung
- Hinweise

Unterstützte Features

- Feldzuordnungen
- Filterung des Benutzerkontextes
- Einschluss-/Ausschlussfilter
- Vollständige und inkrementelle Inhaltssynchronisierung
- Virtual Private Cloud (VPC)

Voraussetzungen

Bevor Sie Ihre Amazon RDS (PostgreSQL) Datenquelle Amazon Kendra zum Indizieren verwenden können, nehmen Sie diese Änderungen in Ihren Konten Amazon RDS (PostgreSQL) und AWS Konten vor.

Stellen Sie sicherAmazon RDS (PostgreSQL), dass Sie Folgendes haben:

- Haben Sie sich Ihren Datenbank-Benutzernamen und Ihr Passwort notiert.

> **Important**
>
> Es hat sich bewährt, nur lesbare Amazon Kendra Datenbankanmeldeinformationen zur Verfügung zu stellen.

- Die URL, der Port und die Instanz Ihres Datenbank-Hosts wurden kopiert. Sie finden diese Informationen auf der Amazon RDS Konsole.
- Vergewissert, dass jedes Dokument in Amazon RDS (PostgreSQL) und zwischen anderen Datenquellen, die Sie für denselben Index verwenden möchten, einzigartig ist. Jede Datenquelle, die Sie für einen Index verwenden möchten, darf nicht dasselbe Dokument in allen Datenquellen enthalten. Dokument-IDs gelten für einen Index global und müssen pro Index eindeutig sein.

Stellen Sie sicher AWS-Konto, dass Sie Folgendes in Ihrem haben:

- Hat einen Amazon Kendra Index erstellt und bei Verwendung der API die Index-ID notiert.
- Sie haben eine IAM Rolle für Ihre Datenquelle erstellt und, falls Sie die API verwenden, den ARN der IAM Rolle notiert.

> **Note**
>
> Wenn Sie Ihren Authentifizierungstyp und Ihre Anmeldeinformationen ändern, müssen Sie Ihre IAM Rolle aktualisieren, um auf die richtige AWS Secrets Manager geheime ID zugreifen zu können.

- Wir haben Ihre Amazon RDS (PostgreSQL) Authentifizierungsdaten AWS Secrets Manager geheim gespeichert und, falls Sie die API verwenden, den ARN des Geheimnisses notiert.

> **Note**
>
> Wir empfehlen Ihnen, Ihre Anmeldeinformationen und Ihr Geheimnis regelmäßig zu aktualisieren oder zu wechseln. Stellen Sie zu Ihrer eigenen Sicherheit nur die Zugriffsebene bereit, die erforderlich ist. Wir raten davon ab, Anmeldeinformationen und geheime Daten für alle Datenquellen und Connector-Versionen 1.0 und 2.0 (sofern zutreffend) wiederzuverwenden.

Wenn Sie noch keine IAM Rolle oder keinen Schlüssel haben, können Sie die Konsole verwenden, um eine neue IAM Rolle und ein neues Secrets Manager Geheimnis zu erstellen, wenn Sie Ihre Amazon RDS (PostgreSQL) Datenquelle mit verbinden. Amazon Kendra Wenn Sie die API verwenden, müssen Sie den ARN einer vorhandenen IAM Rolle und eines Secrets Manager Geheimnisses sowie eine Index-ID angeben.

Anweisungen zur Verbindung

Um eine Verbindung Amazon Kendra zu Ihrer Amazon RDS (PostgreSQL) Datenquelle herzustellen, müssen Sie Details zu Ihren Amazon RDS (PostgreSQL) Anmeldeinformationen angeben, damit Sie auf Ihre Daten zugreifen Amazon Kendra können. Falls Sie das noch nicht konfiguriert haben, Amazon Kendra finden Sie Amazon RDS (PostgreSQL) weitere Informationen unterVoraussetzungen.

Console

Um eine Verbindung Amazon Kendra herzustellen Amazon RDS (PostgreSQL)

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die Amazon Kendra Konsole.
2. Wählen Sie im linken Navigationsbereich Indizes und dann den Index, den Sie verwenden möchten, aus der Indexliste aus.

   > **Note**
   >
   > Sie können Ihre Einstellungen für die Benutzerzugriffskontrolle unter Indexeinstellungen konfigurieren oder bearbeiten.

3. Wählen Sie auf der Seite Erste Schritte die Option Datenquelle hinzufügen aus.

4. Wählen Sie auf der Seite Datenquelle hinzufügen die Option Amazon RDS (PostgreSQL)Connector und dann Connector hinzufügen aus.
5. Geben Sie auf der Seite „Datenquellendetails angeben“ die folgenden Informationen ein:
    a. Geben Sie im Feld Name und Beschreibung für Datenquellenname einen Namen für Ihre Datenquelle ein. Sie können Bindestriche, aber keine Leerzeichen verwenden.
    b. (Optional) Beschreibung — Geben Sie eine optionale Beschreibung für Ihre Datenquelle ein.
    c. In Standardsprache — Wählen Sie eine Sprache aus, um Ihre Dokumente nach dem Index zu filtern. Sofern Sie nichts anderes angeben, ist die Standardsprache Englisch. Die in den Metadaten des Dokuments angegebene Sprache hat Vorrang vor der ausgewählten Sprache.
    d. Unter Tags für Neues Tag hinzufügen — Fügen Sie optionale Tags hinzu, um Ihre Ressourcen zu durchsuchen und zu filtern oder Ihre Kosten nachzuverfolgen. AWS
    e. Wählen Sie Weiter aus.
6. Geben Sie auf der Seite Zugriff und Sicherheit definieren die folgenden Informationen ein:
    a. Geben Sie im Feld Quelle die folgenden Informationen ein:
    b. Host — Geben Sie die URL des Datenbank-Hosts ein, zum Beispiel:`http://`*`instance URL`*`.`*`region`*`.rds.amazonaws.com`.
    c. Port — Geben Sie den Datenbankport ein, zum Beispiel`5432`.
    d. Instanz — Geben Sie zum Beispiel die Datenbankinstanz ein`postgres`.
    e. Speicherort für SSL-Zertifikate aktivieren — Geben Sie hier den Amazon S3 Pfad zu Ihrer SSL-Zertifikatsdatei ein.
    f. Geben Sie im Feld Authentifizierung die folgenden Informationen ein:
        - AWS Secrets Manager geheim — Wählen Sie ein vorhandenes Geheimnis aus, oder erstellen Sie ein neues Secrets Manager Geheimnis, um Ihre Amazon RDS (PostgreSQL) Authentifizierungsdaten zu speichern. Wenn Sie ein neues Geheimnis erstellen möchten, wird ein AWS Secrets Manager geheimes Fenster geöffnet.
            A. Geben Sie die folgenden Informationen in das Fenster Create an AWS Secrets Manager Secret ein:

I. Geheimer Name — Ein Name für Ihr Geheimnis. Das Präfix 'AmazonKendra- Amazon RDS (PostgreSQL) -' wird automatisch zu Ihrem geheimen Namen hinzugefügt.

II. Für Datenbankbenutzername und Passwort — Geben Sie die Werte der Authentifizierungsdaten ein, die Sie aus Ihrer Datenbank kopiert haben.

B. Wählen Sie Speichern.

g. Virtual Private Cloud (VPC) — Sie können wählen, ob Sie eine VPC verwenden möchten. In diesem Fall müssen Sie Subnetze und VPC-Sicherheitsgruppen hinzufügen.

h. IAM Rolle — Wählen Sie eine bestehende IAM Rolle oder erstellen Sie eine neue IAM Rolle, um auf Ihre Repository-Anmeldeinformationen und Indexinhalte zuzugreifen.

> **Note**
>
> IAM Rollen, die für Indizes verwendet werden, können nicht für Datenquellen verwendet werden. Wenn Sie sich nicht sicher sind, ob eine vorhandene Rolle für einen Index oder eine häufig gestellte Frage verwendet wird, wählen Sie Neue Rolle erstellen, um Fehler zu vermeiden.

i. Wählen Sie Weiter aus.

7. Geben Sie auf der Seite „Synchronisierungseinstellungen konfigurieren“ die folgenden Informationen ein:

a. Wählen Sie unter Synchronisierungsbereich eine der folgenden Optionen aus:

- SQL-Abfrage — Geben Sie SQL-Abfrageanweisungen wie SELECT- und JOIN-Operationen ein. SQL-Abfragen müssen weniger als 32 KB groß sein. SQL-Abfragen müssen weniger als 32 KB groß sein und dürfen keine Semikolons (;) enthalten. Amazon Kendra durchsucht den gesamten Datenbankinhalt, der Ihrer Abfrage entspricht.
- Primärschlüsselspalte — Geben Sie den Primärschlüssel für die Datenbanktabelle an. Dadurch wird eine Tabelle in Ihrer Datenbank identifiziert.
- Titelspalte — Geben Sie den Namen der Titelspalte des Dokuments in Ihrer Datenbanktabelle an.
- Hauptspalte — Geben Sie den Namen der Hauptspalte des Dokuments in Ihrer Datenbanktabelle an.

b. Wählen Sie unter Zusätzliche Konfiguration — optional aus den folgenden Optionen, um bestimmte Inhalte zu synchronisieren, anstatt alle Dateien zu synchronisieren:

- Spalten zur Erkennung von Änderungen — Geben Sie die Namen der Spalten ein, anhand derer Inhaltsänderungen erkannt Amazon Kendra werden sollen. Amazon Kendra indexiert den Inhalt neu, wenn sich eine dieser Spalten ändert.
- Spalte mit Benutzer-IDs — Geben Sie den Namen der Spalte ein, die Benutzer-IDs enthält, um Zugriff auf Inhalte zu erhalten.
- Spalte „Gruppen“ — Geben Sie den Namen der Spalte ein, die Gruppen enthält, denen der Zugriff auf Inhalte gewährt werden soll.
- Spalte Quell-URLs — Geben Sie den Namen der Spalte ein, die Quell-URLs enthält, die indexiert werden sollen.
- Spalte mit Zeitstempeln — Geben Sie den Namen der Spalte ein, die Zeitstempel enthält. Amazon Kendra verwendet Zeitstempelinformationen, um Änderungen an Ihren Inhalten zu erkennen und nur geänderte Inhalte zu synchronisieren.
- Spalte „Zeitzonen“ — Geben Sie den Namen der Spalte ein, die Zeitzonen für den Inhalt enthält, der gecrawlt werden soll.
- Zeitstempelformat — Geben Sie den Namen der Spalte ein, die Zeitstempelformate enthält, anhand derer Inhaltsänderungen erkannt und Ihre Inhalte erneut synchronisiert werden sollen.

c. Synchronisierungsmodus — Wählen Sie aus, wie Sie Ihren Index aktualisieren möchten, wenn sich der Inhalt Ihrer Datenquelle ändert. Wenn Sie Ihre Datenquelle Amazon Kendra zum ersten Mal synchronisieren, werden alle Inhalte standardmäßig gecrawlt und indexiert. Sie müssen eine vollständige Synchronisierung Ihrer Daten durchführen, falls Ihre erste Synchronisierung fehlgeschlagen ist, auch wenn Sie die Option Vollsynchronisierung nicht als Synchronisierungsmodusoption wählen.

- Vollständige Synchronisierung: Indizieren Sie den gesamten Inhalt neu und ersetzen die vorhandenen Inhalte jedes Mal, wenn Ihre Datenquelle mit Ihrem Index synchronisiert wird.
- Neue, geänderte Synchronisierung: Indizieren Sie jedes Mal, wenn Ihre Datenquelle mit Ihrem Index synchronisiert wird, nur neue und geänderte Inhalte. Amazon Kendra kann den Mechanismus Ihrer Datenquelle verwenden, um Inhaltsänderungen nachzuverfolgen und Inhalte zu indexieren, die sich seit der letzten Synchronisierung geändert haben.

- Neue, geänderte, gelöschte Synchronisierung: Indizieren Sie bei jeder Synchronisierung Ihrer Datenquelle mit Ihrem Index nur neue, geänderte und gelöschte Inhalte. Amazon Kendra kann den Mechanismus Ihrer Datenquelle verwenden, um Inhaltsänderungen nachzuverfolgen und Inhalte zu indexieren, die sich seit der letzten Synchronisierung geändert haben.

d. Im Synchronisierungslaufplan für Frequenz — Wie oft Amazon Kendra wird mit Ihrer Datenquelle synchronisiert?

e. Wählen Sie Weiter aus.

8. Geben Sie auf der Seite Feldzuordnungen festlegen die folgenden Informationen ein:

a. Wählen Sie aus den generierten Standard-Datenquellenfeldern — Dokument-IDs, Dokumenttitel und Quell-URLs — aus, die Sie dem Index zuordnen möchten. Amazon Kendra

b. Feld hinzufügen — Um benutzerdefinierte Datenquellenfelder hinzuzufügen, um einen Indexfeldnamen für die Zuordnung und den Felddatentyp zu erstellen.

c. Wählen Sie Weiter aus.

9. Überprüfen Sie auf der Seite Überprüfen und erstellen, ob die von Ihnen eingegebenen Informationen korrekt sind, und wählen Sie dann Datenquelle hinzufügen aus. Sie können Ihre Informationen auch auf dieser Seite bearbeiten. Ihre Datenquelle wird auf der Seite Datenquellen angezeigt, nachdem die Datenquelle erfolgreich hinzugefügt wurde.

API

Um eine Verbindung Amazon Kendra herzustellen Amazon RDS (PostgreSQL)

Mithilfe der TemplateConfigurationAPI müssen Sie Folgendes angeben:

- Datenquelle — Geben Sie den Datenquellentyp wie `JDBC` bei der Verwendung des TemplateConfigurationJSON-Schemas an. Geben Sie außerdem die Datenquelle so an`TEMPLATE`, wie Sie die CreateDataSourceAPI aufrufen.
- Datenbanktyp — Sie müssen den Datenbanktyp als `postgresql` angeben.
- SQL-Abfrage — Geben Sie SQL-Abfrageanweisungen wie SELECT- und JOIN-Operationen an. SQL-Abfragen müssen weniger als 32 KB groß sein. Amazon Kendra durchsucht den gesamten Datenbankinhalt, der Ihrer Abfrage entspricht.
- Synchronisierungsmodus — Geben Sie an, wie Ihr Index aktualisiert Amazon Kendra werden soll, wenn sich der Inhalt Ihrer Datenquelle ändert. Wenn Sie Ihre Datenquelle Amazon Kendra

zum ersten Mal synchronisieren, werden alle Inhalte standardmäßig gecrawlt und indexiert. Sie müssen eine vollständige Synchronisierung Ihrer Daten durchführen, falls Ihre erste Synchronisierung fehlgeschlagen ist, auch wenn Sie die Option Vollsynchronisierung nicht als Synchronisierungsmodusoption wählen. Sie können wählen zwischen:

- `FORCED_FULL_CRAWL`um den gesamten Inhalt neu zu indizieren und vorhandene Inhalte jedes Mal zu ersetzen, wenn Ihre Datenquelle mit Ihrem Index synchronisiert wird.
- `FULL_CRAWL`um bei jeder Synchronisierung Ihrer Datenquelle mit Ihrem Index nur neue, geänderte und gelöschte Inhalte zu indizieren. Amazon Kendra kann den Mechanismus Ihrer Datenquelle verwenden, um Inhaltsänderungen nachzuverfolgen und Inhalte zu indexieren, die sich seit der letzten Synchronisierung geändert haben.
- `CHANGE_LOG`um jedes Mal, wenn Ihre Datenquelle mit Ihrem Index synchronisiert wird, nur neue und geänderte Inhalte zu indizieren. Amazon Kendra kann den Mechanismus Ihrer Datenquelle verwenden, um Inhaltsänderungen nachzuverfolgen und Inhalte zu indexieren, die sich seit der letzten Synchronisierung geändert haben.

- Geheimer Amazon-Ressourcenname (ARN) — Geben Sie den Amazon-Ressourcennamen (ARN) eines Secrets Manager Geheimnisses ein, das die Authentifizierungsdaten enthält, die Sie in Ihrem Amazon RDS (PostgreSQL) Konto erstellt haben. Das Geheimnis wird in einer JSON-Struktur mit den folgenden Schlüsseln gespeichert:

```
{
    "user name": "database user name",
    "password": "password"
}
```

> **Note**
>
> Wir empfehlen Ihnen, Ihre Anmeldeinformationen und Ihr Geheimnis regelmäßig zu aktualisieren oder zu wechseln. Stellen Sie zu Ihrer eigenen Sicherheit nur die Zugriffsebene bereit, die erforderlich ist. Wir raten davon ab, Anmeldeinformationen und geheime Daten für alle Datenquellen und Connector-Versionen 1.0 und 2.0 (sofern zutreffend) wiederzuverwenden.

- IAM Rolle — Geben Sie an`RoleArn`, wann Sie anrufen`CreateDataSource`, um einer IAM Rolle Berechtigungen für den Zugriff auf Ihr Secrets Manager Geheimnis und für den Aufruf der erforderlichen öffentlichen APIs für den Amazon RDS (PostgreSQL) Connector und zum

Aufrufen der erforderlichen öffentlichen APIs zu erteilen. Amazon Kendra Weitere Informationen finden Sie unter IAM Rollen für Amazon RDS (PostgreSQL) Datenquellen.

Sie können auch die folgenden optionalen Funktionen hinzufügen:

- Virtual Private Cloud (VPC) — Geben Sie an, `VpcConfiguration` wann Sie anrufen. `CreateDataSource` Weitere Informationen finden Sie unter Konfigurieren von Amazon Kendra für die Verwendung eines Amazon VPC.
- Inklusions- und Ausschlussfilter — Sie können mithilfe von Benutzer-IDs, Gruppen, Quell-URLs, Zeitstempeln und Zeitzonen angeben, ob bestimmte Inhalte eingeschlossen werden sollen.
- Benutzerkontextfilterung und Zugriffskontrolle —Amazon Kendra durchsucht die Zugriffskontrollliste (ACL) für Ihre Dokumente, sofern Sie über eine ACL für Ihre Dokumente verfügen. Die ACL-Informationen werden verwendet, um Suchergebnisse nach dem Benutzer- oder Gruppenzugriff auf Dokumente zu filtern. Weitere Informationen finden Sie unter Benutzerkontextfilterung.
- Feldzuordnungen — Wählen Sie diese Option, um Ihre Amazon RDS (PostgreSQL) Datenquellenfelder Ihren Indexfeldern zuzuordnen. Amazon Kendra Weitere Informationen finden Sie unter Zuweisen von Datenquellenfeldern.

> **Note**
>
> Das Textfeld oder das entsprechende Textfeld für Ihre Dokumente ist erforderlich, um Ihre Dokumente durchsuchen Amazon Kendra zu können. Sie müssen den Feldnamen Ihres Dokumenthauptteils in Ihrer Datenquelle dem Namen des Indexfeldes zuordnen`_document_body`. Alle anderen Felder sind optional.

Eine Liste weiterer wichtiger JSON-Schlüssel, die konfiguriert werden müssen, finden Sie unterAmazon RDS (PostgreSQL) -Vorlagenschema.

Hinweise

- Gelöschte Datenbankzeilen werden nicht nachverfolgt, wenn nach Amazon Kendra aktualisiertem Inhalt gesucht wird.
- Die Größe von Feldnamen und Werten in einer Zeile Ihrer Datenbank darf 400 KB nicht überschreiten.

- Wenn Ihre Datenbankdatenquelle eine große Datenmenge enthält und Sie nicht möchten Amazon Kendra , dass Ihr gesamter Datenbankinhalt nach der ersten Synchronisierung indexiert wird, können Sie wählen, ob nur neue, geänderte oder gelöschte Dokumente synchronisiert werden sollen.
- Es hat sich bewährt, nur lesbare Amazon Kendra Datenbankanmeldeinformationen zur Verfügung zu stellen.
- Es hat sich bewährt, das Hinzufügen von Tabellen mit sensiblen Daten oder personenbezogenen Daten (PII) zu vermeiden.

Amazon S3

Amazon S3 ist ein Objektspeicherdienst, der Daten als Objekte in Buckets speichert. Sie können es verwenden Amazon Kendra , um Ihr Amazon S3 Bucket-Repository mit Dokumenten zu indizieren.

> **Warning**
>
> Amazon Kendra verwendet keine Bucket-Richtlinie, die einem Amazon Kendra Principal die Erlaubnis erteilt, mit einem S3-Bucket zu interagieren. Stattdessen verwendet es IAM Rollen. Stellen Sie sicher, dass dies Amazon Kendra nicht als vertrauenswürdiges Mitglied in Ihrer Bucket-Richtlinie enthalten ist, um Datensicherheitsprobleme zu vermeiden, die durch die versehentliche Vergabe von Berechtigungen an beliebige Prinzipale entstehen. Sie können jedoch eine Bucket-Richtlinie hinzufügen, um einen Amazon S3 Bucket für verschiedene Konten zu verwenden. Weitere Informationen finden Sie unter Richtlinien zur Amazon S3 kontenübergreifenden Verwendung (auf der Registerkarte IAM S3-Rollen unter IAM Rollen für Datenquellen). Informationen zu IAM Rollen für S3-Datenquellen finden Sie unter IAM Rollen.

> **Note**
>
> Amazon Kendra unterstützt jetzt einen aktualisierten Amazon S3 Connector.
> Die Konsole wurde automatisch für Sie aktualisiert. Alle neuen Konnektoren, die
> Sie in der Konsole erstellen, verwenden die aktualisierte Architektur. Wenn Sie die
> API verwenden, müssen Sie jetzt das TemplateConfigurationObjekt anstelle des
> `S3DataSourceConfiguration` Objekts verwenden, um Ihren Connector zu konfigurieren.
> Konnektoren, die mit der älteren Konsolen- und API-Architektur konfiguriert wurden,
> funktionieren weiterhin wie konfiguriert. Sie können sie jedoch nicht bearbeiten oder

aktualisieren. Wenn Sie Ihre Connectorkonfiguration bearbeiten oder aktualisieren möchten, müssen Sie einen neuen Connector erstellen.
Wir empfehlen, Ihren Connector-Workflow auf die aktualisierte Version zu migrieren. Die Support für Konnektoren, die mit der älteren Architektur konfiguriert wurden, soll bis Juni 2024 eingestellt werden.

Sie können über die Amazon Kendra Konsole oder die TemplateConfigurationAPI eine Verbindung zu Ihrer Amazon S3 Datenquelle herstellen.

> **Note**
>
> Informationen zum Generieren eines Synchronisierungsstatusberichts für Ihre Amazon S3 Datenquelle finden Sie unter Problembehandlung bei Datenquellen.

Informationen zur Fehlerbehebung bei Ihrem Amazon Kendra S3-Datenquellen-Connector finden Sie unterProblembehandlung bei Datenquellen.

Themen

Unterstützte Features

- Feldzuordnungen
- Filterung des Benutzerkontextes
- Einschluss-/Ausschlussfilter
- Vollständige und inkrementelle Inhaltssynchronisierung
- Virtual Private Cloud (VPC)

Voraussetzungen

Bevor Sie Ihre S3-Datenquelle Amazon Kendra zum Indizieren verwenden können, nehmen Sie diese Änderungen in Ihrem S3 und AWS Ihren Konten vor.

Stellen Sie in S3 sicher, dass Sie über Folgendes verfügen:

- Der Name Ihres Amazon S3 Bucket-Namens wurde kopiert.

> **Note**
>
> Ihr Bucket muss sich in derselben Region wie Ihr Amazon Kendra Index befinden und Ihr Index muss berechtigt sein, auf den Bucket zuzugreifen, der Ihre Dokumente enthält.

- Aktiviert, dass jedes Dokument in S3 und in anderen Datenquellen, die Sie für denselben Index verwenden möchten, einzigartig ist. Jede Datenquelle, die Sie für einen Index verwenden möchten, darf nicht dasselbe Dokument in allen Datenquellen enthalten. Dokument-IDs gelten für einen Index global und müssen pro Index eindeutig sein.

Stellen Sie in Ihrem AWS Konto sicher, dass Sie über Folgendes verfügen:

- Hat einen Amazon Kendra Index erstellt und bei Verwendung der API die Index-ID notiert.
- Sie haben eine IAM Rolle für Ihre Datenquelle erstellt und, falls Sie die API verwenden, den ARN der IAM Rolle notiert.

Wenn Sie noch keine IAM Rolle haben, können Sie die Konsole verwenden, um eine neue IAM Rolle zu erstellen, wenn Sie Ihre S3-Datenquelle mit verbinden Amazon Kendra. Wenn Sie die API verwenden, müssen Sie den ARN einer vorhandenen IAM Rolle und eine Index-ID angeben.

Anweisungen zur Verbindung

Um eine Verbindung Amazon Kendra zu Ihrer S3-Datenquelle herzustellen, müssen Sie die erforderlichen Details zu Ihrer S3-Datenquelle angeben, damit Sie auf Ihre Daten zugreifen Amazon Kendra können. Wenn Sie S3 noch nicht für konfiguriert haben Amazon Kendra, finden Sie weitere Informationen unterVoraussetzungen.

Console

Um eine Verbindung Amazon Kendra herzustellen Amazon S3

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die Amazon Kendra Konsole.
2. Wählen Sie im linken Navigationsbereich Indizes und dann den Index, den Sie verwenden möchten, aus der Indexliste aus.

> **Note**
>
> Sie können Ihre Einstellungen für die Benutzerzugriffskontrolle unter Indexeinstellungen konfigurieren oder bearbeiten.

3. Wählen Sie auf der Seite Erste Schritte die Option Datenquelle hinzufügen aus.
4. Wählen Sie auf der Seite Datenquelle hinzufügen die Option S3-Connector und dann Connector hinzufügen aus.
5. Geben Sie auf der Seite „Datenquellendetails angeben“ die folgenden Informationen ein:
   a. Geben Sie im Feld Name und Beschreibung für Datenquellenname einen Namen für Ihre Datenquelle ein. Sie können Bindestriche, aber keine Leerzeichen verwenden.
   b. (Optional) Beschreibung — Geben Sie eine optionale Beschreibung für Ihre Datenquelle ein.
   c. In Standardsprache — Wählen Sie eine Sprache aus, um Ihre Dokumente nach dem Index zu filtern. Sofern Sie nichts anderes angeben, ist die Standardsprache Englisch. Die in den Metadaten des Dokuments angegebene Sprache hat Vorrang vor der ausgewählten Sprache.
   d. Unter Tags für Neues Tag hinzufügen — Fügen Sie optionale Tags hinzu, um Ihre Ressourcen zu durchsuchen und zu filtern oder Ihre Kosten nachzuverfolgen. AWS
   e. Wählen Sie Weiter aus.
6. Geben Sie auf der Seite Zugriff und Sicherheit definieren die folgenden optionalen Informationen ein:
   a. IAM Rolle — Wählen Sie eine bestehende IAM Rolle oder erstellen Sie eine neue IAM Rolle, um auf Ihre Repository-Anmeldeinformationen und Indexinhalte zuzugreifen.

> **Note**
>
> IAM Rollen, die für Indizes verwendet werden, können nicht für Datenquellen verwendet werden. Wenn Sie sich nicht sicher sind, ob eine vorhandene Rolle für

einen Index oder eine häufig gestellte Frage verwendet wird, wählen Sie Neue Rolle erstellen, um Fehler zu vermeiden.

b. Virtual Private Cloud (VPC) — Sie können wählen, ob Sie a Amazon VPC für Ihren Amazon S3 Bucket verwenden möchten, wenn er nicht über das öffentliche Internet zugänglich ist. Wenn ja, müssen Sie Subnetze und Amazon VPC Sicherheitsgruppen hinzufügen.

> **Important**
>
> Stellen Sie sicher, dass Sie:
>
> - Amazon VPC Gemäß den Schritten unter Amazon S3 Gateway-Endpunkte für Amazon S3 wurde Ihrem ein Endpunkt hinzugefügt.
> - Es wurde ein privates Subnetz in einer Amazon Kendra unterstützten Availability Zone ausgewählt. Weitere Informationen finden Amazon Kendra Sie unter Konfiguration Amazon VPC für die Verwendung von.
> - Ihre Sicherheitsgruppe wurde so konfiguriert, dass sie den Amazon Kendra Zugriff auf den Amazon S3 Endpunkt ermöglicht. Weitere Informationen finden Amazon Kendra Sie unter Konfiguration Amazon VPC zur Verwendung.

c. Wählen Sie Weiter aus.

7. Geben Sie auf der Seite „Synchronisierungseinstellungen konfigurieren“ die folgenden Informationen ein:

   a. Im Synchronisierungsbereich für Speicherort der Datenquelle — Der Pfad zu dem Amazon S3 Bucket, in dem Ihre Daten gespeichert sind. Wählen Sie Browse S3 aus, um Ihren Bucket auszuwählen.

   b. (Optional) Präfix für den Ordnerspeicherort für Metadatendateien — Der Pfad zu dem Ordner, in dem Ihre Metadaten gespeichert sind. Wählen Sie S3 durchsuchen aus, um Ihren Metadatenordner zu finden.

   c. (Optional) Speicherort der Konfigurationsdatei für die Zugriffskontrollliste — Der Pfad zum Speicherort einer Datei, die eine JSON-Struktur enthält, die die Zugriffseinstellungen für die in Ihrer S3-Datenquelle gespeicherten Dateien angibt. Wählen Sie „S3 durchsuchen“ aus, um Ihre ACL-Datei zu suchen.

d. (Optional) Entschlüsselungsschlüssel wählen — Wählen Sie diese Option, um einen Entschlüsselungsschlüssel zu verwenden. Sie können wählen, ob Sie einen vorhandenen Schlüssel verwenden möchten. AWS KMS

e. (Optional) Fügen Sie unter Zusätzliche Konfiguration für Muster Muster hinzu, um Dokumente in Ihren Index aufzunehmen oder daraus auszuschließen. Alle Pfade beziehen sich auf den S3-Bucket mit dem Speicherort der Datenquelle. Sie können bis zu 100 Muster hinzufügen.

f. Synchronisierungsmodus — Wählen Sie aus, wie Sie Ihren Index aktualisieren möchten, wenn sich der Inhalt Ihrer Datenquelle ändert. Wenn Sie Ihre Datenquelle Amazon Kendra zum ersten Mal synchronisieren, werden alle Inhalte standardmäßig gecrawlt und indexiert. Sie müssen eine vollständige Synchronisierung Ihrer Daten durchführen, falls Ihre erste Synchronisierung fehlgeschlagen ist, auch wenn Sie die Option Vollsynchronisierung nicht als Synchronisierungsmodusoption wählen.

   - Vollständige Synchronisierung: Indizieren Sie den gesamten Inhalt neu und ersetzen die vorhandenen Inhalte jedes Mal, wenn Ihre Datenquelle mit Ihrem Index synchronisiert wird.
   - Neue, geänderte, gelöschte Synchronisierung: Indizieren Sie bei jeder Synchronisierung Ihrer Datenquelle mit Ihrem Index nur neue, geänderte und gelöschte Inhalte. Amazon Kendra kann den Mechanismus Ihrer Datenquelle verwenden, um Inhaltsänderungen nachzuverfolgen und Inhalte zu indexieren, die sich seit der letzten Synchronisierung geändert haben.

g. Wählen Sie im Zeitplan für die Synchronisierungsausführung unter Frequenz aus, wie oft mit Ihrer Datenquelle synchronisiert Amazon Kendra werden soll.

h. Wählen Sie Weiter aus.

8. Geben Sie auf der Seite Feldzuordnungen festlegen die folgenden optionalen Informationen ein:

   a. S3-Feldzuordnung — Wählen Sie aus den Amazon Kendra generierten Standard-Datenquellenfeldern aus, die Sie Ihrem Index zuordnen möchten.

   b. Feld hinzufügen — Wählen Sie diese Option, um benutzerdefinierte Datenquellenfelder hinzuzufügen, um einen Indexfeldnamen für die Zuordnung und den Felddatentyp zu erstellen.

   c. Wählen Sie Weiter aus.

9. Überprüfen Sie auf der Seite Überprüfen und erstellen, ob die von Ihnen eingegebenen Informationen korrekt sind, und wählen Sie dann Datenquelle hinzufügen aus. Sie können Ihre Informationen auch auf dieser Seite bearbeiten. Ihre Datenquelle wird auf der Seite Datenquellen angezeigt, nachdem die Datenquelle erfolgreich hinzugefügt wurde.

API

Um eine Verbindung Amazon Kendra herzustellen Amazon S3

Sie müssen mithilfe der TemplateConfigurationAPI einen JSON-Wert des Datenquellenschemas angeben. Sie müssen die folgenden Informationen angeben:

- BucketName— Der Name des Buckets, der die Dokumente enthält.
- Synchronisierungsmodus — Geben Sie an, wie Ihr Index aktualisiert Amazon Kendra werden soll, wenn sich der Inhalt Ihrer Datenquelle ändert. Wenn Sie Ihre Datenquelle Amazon Kendra zum ersten Mal synchronisieren, werden alle Inhalte standardmäßig gecrawlt und indexiert. Sie müssen eine vollständige Synchronisierung Ihrer Daten durchführen, falls Ihre erste Synchronisierung fehlgeschlagen ist, auch wenn Sie die Option Vollsynchronisierung nicht als Synchronisierungsmodusoption wählen. Sie können wählen zwischen:
  - `FORCED_FULL_CRAWL`um den gesamten Inhalt neu zu indizieren und vorhandene Inhalte jedes Mal zu ersetzen, wenn Ihre Datenquelle mit Ihrem Index synchronisiert wird.
  - `FULL_CRAWL`um bei jeder Synchronisierung Ihrer Datenquelle mit Ihrem Index nur neue, geänderte und gelöschte Inhalte zu indizieren. Amazon Kendra kann den Mechanismus Ihrer Datenquelle verwenden, um Inhaltsänderungen nachzuverfolgen und Inhalte zu indexieren, die sich seit der letzten Synchronisierung geändert haben.
- IAM Rolle — Geben Sie an`RoleArn`, wann Sie anrufen`CreateDataSource`, um einer IAM Rolle Berechtigungen für den Zugriff auf Ihr Secrets Manager Geheimnis und für den Aufruf der erforderlichen öffentlichen APIs für den S3-Connector und Amazon Kendra zu erteilen. Weitere Informationen finden Sie unter IAM Rollen für S3-Datenquellen.

Sie können auch die folgenden optionalen Funktionen hinzufügen:

- Virtual Private Cloud (VPC) — Geben Sie an, `VpcConfiguration` wann Sie anrufen. `CreateDataSource` Weitere Informationen finden Sie unter Konfigurieren von Amazon Kendra für die Verwendung eines Amazon VPC.

- Inklusions- und Ausschlussfilter — Geben Sie an, ob bestimmte Dateinamen, Dateitypen und Dateipfade ein- oder ausgeschlossen werden sollen. Sie verwenden Glob-Muster (Muster, mit denen ein Platzhaltermuster zu einer Liste von Pfadnamen erweitert werden kann, die dem angegebenen Muster entsprechen). Beispiele finden Sie unter Verwendung von Ausschluss- und Include-Filtern in der AWS CLI-Befehlsreferenz.
- Konfiguration von Dokumentmetadaten — Fügen Sie Dokument-Metadatendateien hinzu, die Informationen wie die Informationen zur Zugriffskontrolle für Dokumente, den Quell-URI, den Autor des Dokuments und benutzerdefinierte Attribute enthalten. Jede Metadatendatei enthält Metadaten zu einem einzelnen Dokument.
- Feldzuordnungen — Wählen Sie diese Option, um Ihre S3-Datenquellenfelder Ihren Indexfeldern zuzuordnen. Amazon Kendra Weitere Informationen finden Sie unter Zuweisen von Datenquellenfeldern.

  > **Note**
  >
  > Das Textfeld oder das entsprechende Textfeld für Ihre Dokumente ist erforderlich, um Ihre Dokumente durchsuchen Amazon Kendra zu können. Sie müssen den Feldnamen Ihres Dokumenthauptteils in Ihrer Datenquelle dem Namen des Indexfeldes zuordnen`_document_body`. Alle anderen Felder sind optional.

Eine Liste weiterer wichtiger JSON-Schlüssel, die konfiguriert werden müssen, finden Sie unterAmazon S3 Vorlagenschema.

Weitere Informationen

Weitere Informationen zur Integration Amazon Kendra mit Ihrer S3-Datenquelle finden Sie unter:

- Suchen Sie mit Amazon Kendra S3 Connector mit VPC-Unterstützung genau nach Antworten

Eine Amazon S3 Datenquelle erstellen

Die folgenden Beispiele veranschaulichen das Erstellen einer Amazon S3 Datenquelle. In den Beispielen wird davon ausgegangen, dass Sie bereits einen Index und eine IAM Rolle mit der Berechtigung zum Lesen der Daten aus dem Index erstellt haben. Weitere Informationen zu der IAM Rolle finden Sie unter IAM Zugriffsrollen. Weitere Informationen zum Erstellen eines Indexes finden Sie unter Index erstellen.

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

Der folgende Python-Codeausschnitt erstellt eine Amazon S3 Datenquelle. Das vollständige Beispiel finden Sie unter. Erste Schritte (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
    )
```

Das Erstellen Ihrer Datenquelle kann einige Zeit in Anspruch nehmen. Sie können den Fortschritt mithilfe der DescribeDataSourceAPI überwachen. Wenn der Status der Datenquelle lautet, ist `ACTIVE` die Datenquelle einsatzbereit.

Die folgenden Beispiele zeigen, wie der Status einer Datenquelle abgerufen werden kann.

CLI

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

Python

Der folgende Python-Codeausschnitt enthält Informationen über eine S3-Datenquelle. Das vollständige Beispiel finden Sie unter. Erste Schritte (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
```

Diese Datenquelle hat keinen Zeitplan und wird daher nicht automatisch ausgeführt. Um die Datenquelle zu indizieren, rufen Sie auf, StartDataSourceSyncJobum den Index mit der Datenquelle zu synchronisieren.

Die folgenden Beispiele veranschaulichen die Synchronisation einer Datenquelle.

CLI

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

Python

Der folgende Python-Codeausschnitt synchronisiert eine Amazon S3 Datenquelle. Das vollständige Beispiel finden Sie unter. Erste Schritte (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 Metadaten des Dokuments

Mithilfe einer Metadatendatei können Sie Metadaten, zusätzliche Informationen zu einem Dokument, zu Dokumenten in einem Amazon S3 Bucket hinzufügen. Jede Metadatendatei ist einem indizierten Dokument zugeordnet.

Ihre Metadatendateien müssen in demselben Bucket wie Ihre indizierten Dateien gespeichert werden. Sie können einen Speicherort innerhalb des Buckets für Ihre Metadatendateien angeben, indem Sie die Konsole oder das `S3Prefix` Feld des `DocumentsMetadataConfiguration` Parameters verwenden, wenn Sie eine Amazon S3 Datenquelle erstellen. Wenn Sie kein Amazon S3 Präfix angeben, müssen Ihre Metadatendateien am selben Ort wie Ihre indizierten Dokumente gespeichert werden.

Wenn Sie ein Amazon S3 Präfix für Ihre Metadatendateien angeben, befinden sie sich in einer Verzeichnisstruktur parallel zu Ihren indizierten Dokumenten. Amazon Kendra sucht nur im angegebenen Verzeichnis nach Ihren Metadaten. Wenn die Metadaten nicht gelesen werden, überprüfen Sie, ob der Speicherort des Verzeichnisses mit dem Speicherort Ihrer Metadaten übereinstimmt.

Die folgenden Beispiele zeigen, wie der Speicherort des indizierten Dokuments dem Speicherort der Metadatendatei zugeordnet wird. Beachten Sie, dass der Amazon S3 Schlüssel des Dokuments an das Amazon S3 Präfix der Metadaten und dann das Suffix mit angehängt wird, um den Pfad der Metadatendatei `.metadata.json` zu bilden. Amazon S3 Der kombinierte Amazon S3 Schlüssel mit dem Amazon S3 Präfix und `.metadata.json` Suffix der Metadaten darf insgesamt nicht mehr als 1024 Zeichen lang sein. Es wird empfohlen, dass Sie Ihren Amazon S3 Schlüssel unter 1000 Zeichen halten, um zusätzliche Zeichen bei der Kombination Ihres Schlüssels mit dem Präfix und dem Suffix zu berücksichtigen.

```
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
```

Die Metadaten Ihres Dokuments sind in einer JSON-Datei definiert. Die Datei muss eine UTF-8-Textdatei ohne BOM-Markierung sein. Der Dateiname der JSON-Datei muss lauten. `<document>.<extension>.metadata.json` In diesem Beispiel ist „Dokument“ der Name des Dokuments, für das sich die Metadaten beziehen, und „Erweiterung“ ist die Dateierweiterung für das Dokument. Die Dokument-ID muss eindeutig sein`<document>.<extension>.metadata.json`.

Der Inhalt der JSON-Datei folgt dieser Vorlage. Alle Attribute/Felder sind optional, sodass es nicht erforderlich ist, alle Attribute einzubeziehen. Sie müssen für jedes Attribut, das Sie einbeziehen möchten, einen Wert angeben. Der Wert darf nicht leer sein. Wenn Sie den nicht angeben`_source_uri`, verweisen die von Amazon Kendra in den Suchergebnissen zurückgegebenen Links auf den Amazon S3 Bucket, der das Dokument enthält. `DocumentId`ist dem Feld zugeordnet `s3_document_id` und ist der absolute Pfad zum Dokument 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."
}
```

Die Felder `_created_at` und `_last_updated_at` Metadaten sind nach ISO 8601 kodierte Datumsangaben. Beispielsweise ist 2012-03-25T 12:30:10 + 01:00 das ISO-8601-Datums-/Uhrzeitformat für den 25. März 2012 um 12:30 Uhr (plus 10 Sekunden) in der mitteleuropäischen Zeitzone.

Sie können dem `Attributes` Feld über ein Dokument zusätzliche Informationen hinzufügen, die Sie zum Filtern von Abfragen oder zum Gruppieren von Abfrageantworten verwenden. Weitere Informationen finden Sie unter Erstellen von benutzerdefinierten Dokumentfeldern.

Sie können das `AccessControlList` Feld verwenden, um die Antwort aus einer Abfrage zu filtern. Auf diese Weise haben nur bestimmte Benutzer und Gruppen Zugriff auf Dokumente. Weitere Informationen finden Sie unter Nach Benutzerkontext filtern.

Zugriffskontrolle für Amazon S3 Datenquellen

Sie können den Zugriff auf Dokumente in einer Amazon S3 Datenquelle mithilfe einer Konfigurationsdatei steuern. Sie geben die Datei in der Konsole oder als `AccessControlListConfiguration` Parameter an, wenn Sie die UpdateDataSourceAPI CreateDataSourceoder aufrufen.

Die Konfigurationsdatei enthält eine JSON-Struktur, die ein S3-Präfix identifiziert und die Zugriffseinstellungen für das Präfix auflistet. Das Präfix kann ein Pfad oder eine einzelne Datei sein. Wenn das Präfix ein Pfad ist, gelten die Zugriffseinstellungen für alle Dateien in diesem Pfad. In der JSON-Konfigurationsdatei gibt es eine maximale Anzahl von S3-Präfixen und eine standardmäßige maximale Dateigröße. Weitere Informationen finden Sie unter Kontingente für Amazon Kendra.

Sie können in den Zugriffseinstellungen sowohl Benutzer als auch Gruppen angeben. Wenn Sie den Index abfragen, geben Sie Benutzer- und Gruppeninformationen an. Weitere Informationen finden Sie unter Nach Benutzerattribut filtern.

Die JSON-Struktur für die Konfigurationsdatei muss das folgende Format haben:

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

Verwendung Amazon VPC mit einer Amazon S3 Datenquelle

Dieses Thema enthält ein step-by-step Beispiel, das zeigt, wie Sie mithilfe eines Amazon S3 S3-Connectors über Amazon VPC eine Verbindung zu einem Amazon S3 S3-Bucket herstellen. Das Beispiel geht davon aus, dass Sie mit einem vorhandenen S3-Bucket beginnen. Wir empfehlen, dass Sie nur einige Dokumente in Ihren S3-Bucket hochladen, um das Beispiel zu testen.

Sie können über eine Verbindung Amazon Kendra zu Ihrem Amazon S3 Bucket eine Verbindung herstellen Amazon VPC. Dazu müssen Sie bei der Erstellung Ihres Amazon S3 Datenquellenconnectors das Amazon VPC Subnetz und die Amazon VPC Sicherheitsgruppen angeben.

> **Important**
>
> Damit ein Amazon Kendra Amazon S3 Connector auf Ihren Amazon S3 Bucket zugreifen kann, stellen Sie sicher, dass Sie Ihrer Virtual Private Cloud (VPC) einen Amazon S3 Endpunkt zugewiesen haben.

Amazon Kendra Um Dokumente aus Ihrem Amazon S3 Bucket zu synchronisieren Amazon VPC, müssen Sie die folgenden Schritte ausführen:

- Richten Sie einen Amazon S3 Endpunkt für ein Amazon VPC. Weitere Informationen zum Einrichten eines Amazon S3 Endpunkts finden Sie Amazon S3 im AWS PrivateLink Handbuch unter Gateway-Endpunkte für.
- (Optional) Sie haben Ihre Amazon S3 Bucket-Richtlinien überprüft, um sicherzustellen, dass der Amazon S3 Bucket von der Virtual Private Cloud (VPC) aus zugänglich ist, der Sie zugewiesen Amazon Kendra haben. Weitere Informationen finden Sie unter Steuern des Zugriffs von VPC-Endpunkten mit Bucket-Richtlinien im Amazon S3 S3-Benutzerhandbuch

Schritte

- Schritt 1: Konfigurieren Sie ein Amazon VPC
- (Optional) Schritt 2: Amazon S3 Bucket-Richtlinie konfigurieren
- Schritt 3: Erstellen Sie einen Amazon S3 Testdatenquellen-Connector

Schritt 1: Konfigurieren Sie ein Amazon VPC

Erstellen Sie ein VPC-Netzwerk mit einem privaten Subnetz mit einem Amazon S3 Gateway-Endpunkt und einer Sicherheitsgruppe für Amazon Kendra die spätere Verwendung.

So konfigurieren Sie eine VPC mit einem privaten Subnetz, einem S3-Endpunkt und einer Sicherheitsgruppe

1. Melden Sie sich bei an AWS Management Console und öffnen Sie die Amazon VPC Konsole unter. https://console.aws.amazon.com/vpc/
2. Erstellen Sie eine VPC mit einem privaten Subnetz und einem S3-Endpunkt Amazon Kendra zur Verwendung von:

   Wählen Sie im Navigationsbereich Ihre VPCs und dann Create VPC aus.

   a. Wählen Sie unter Zu erstellende Ressourcen die Option VPC und mehr aus.
   b. Aktivieren Sie für Namenstag die Option Automatisch generieren und geben Sie dann ein. **`kendra-s3-example`**
   c. Behalten Sie für den IPv4/IPv6-CIDR-Block die Standardwerte bei.
   d. Wählen Sie für Anzahl der Availability Zones (AZs) die Zahl 1.
   e. Wählen Sie AZs anpassen und wählen Sie dann eine Availability Zone aus der Liste Erste Availability Zone aus.

      Amazon Kendra unterstützt nur eine bestimmte Gruppe von Availability Zones.
   f. Wählen Sie für Anzahl der öffentlichen Subnetze die Zahl 0 aus.
   g. Wählen Sie für Anzahl der privaten Subnetze die Zahl 1 aus.
   h. Wählen Sie für NAT gateways (NAT-Gateways) None (Keine) aus.
   i. Wählen Amazon S3 Sie für VPC-Endpoints Gateway. .
   j. Belassen Sie die übrigen Werte auf ihren Standardeinstellungen.
   k. Wählen Sie Create VPC (VPC erstellen).

      Warten Sie, bis der Workflow Create VPC abgeschlossen ist. Wählen Sie dann View VPC aus, um die VPC zu überprüfen, die Sie gerade erstellt haben.

   Sie haben jetzt ein VPC-Netzwerk mit einem privaten Subnetz erstellt, das keinen Zugriff auf das öffentliche Internet hat.

3. Kopieren Sie Ihre VPC-Endpunkt-ID Ihres Amazon S3 S3-Endpunkts:

    a. Wählen Sie im Navigationsbereich Endpunkte aus.

    b. Suchen Sie in der Liste Endpoints den Amazon S3 S3-Endpunkt`kendra-s3-example-vpce-s3`, den Sie gerade zusammen mit Ihrer VPC erstellt haben.

    c. Notieren Sie sich die VPC-Endpunkt-ID.

    Sie haben jetzt einen Amazon S3 S3-Gateway-Endpunkt erstellt, um über ein Subnetz auf Ihren Amazon S3 S3-Bucket zuzugreifen.

4. Erstellen Sie eine Sicherheitsgruppe Amazon Kendra zur Verwendung von:

    a. Wählen Sie im Navigationsbereich Sicherheitsgruppen und anschließend Sicherheitsgruppe erstellen aus.

    b. Geben Sie für Security group name (Name der Sicherheitsgruppe) **`s3-data-source-security-group`** ein.

    c. Wählen Sie Ihre VPC aus der Amazon VPCListe aus.

    d. Behalten Sie die Standardregeln für eingehenden und ausgehenden Datenverkehr bei.

    e. Wählen Sie Sicherheitsgruppe erstellen aus.

    Sie haben jetzt eine VPC-Sicherheitsgruppe erstellt.

Sie weisen das Subnetz und die Sicherheitsgruppe, die Sie während der Connector-Konfiguration erstellt haben, Ihrem Amazon Kendra Amazon S3 S3-Datenquellen-Connector zu.

(Optional) Schritt 2: Amazon S3 Bucket-Richtlinie konfigurieren

In diesem optionalen Schritt erfahren Sie, wie Sie eine Amazon S3 S3-Bucket-Richtlinie so konfigurieren, dass Ihr Amazon S3 S3-Bucket nur von der VPC aus zugänglich ist, der Sie ihn zuweisen Amazon Kendra.

Amazon Kendra verwendet IAM-Rollen für den Zugriff auf Ihren Amazon S3 S3-Bucket und erfordert nicht, dass Sie eine Amazon S3 S3-Bucket-Richtlinie konfigurieren. Möglicherweise finden Sie es jedoch nützlich, eine Bucket-Richtlinie zu erstellen, wenn Sie einen Amazon S3 Connector mithilfe eines Amazon S3 S3-Buckets konfigurieren möchten, für den bereits Richtlinien bestehen, die den Zugriff aus dem öffentlichen Internet darauf einschränken.

Um Ihre Amazon S3 Bucket-Richtlinie zu konfigurieren

1. Öffnen Sie die Amazon S3 S3-Konsole unterhttps://console.aws.amazon.com/s3/.
2. Wählen Sie im Navigationsbereich Buckets aus.
3. Wählen Sie den Namen des Amazon S3 S3-Buckets, mit dem Sie synchronisieren möchten Amazon Kendra.
4. Wählen Sie den Tab Berechtigungen, scrollen Sie nach unten zu Bucket-Richtlinie und klicken Sie dann auf Bearbeiten.
5. Fügen Sie Ihre Bucket-Richtlinie hinzu oder ändern Sie sie, sodass der Zugriff nur von dem VPC-Endpunkt aus möglich ist, den Sie erstellt haben.

   Hier finden Sie ein Beispiel für eine Bucket-Richtlinie. Ersetzen Sie *bucket-name*und *vpce-id*durch Ihren Amazon S3 S3-Bucket-Namen und die Amazon S3 S3-Endpunkt-ID, die Sie sich zuvor notiert haben.

   ```
   {
     "Version": "2012-10-17",
     "Statement": [
       {
         "Effect": "Deny",
         "Principal": "*",
         "Action": "s3:*",
         "Resource": "arn:aws:s3:::bucket-name/*",
         "Condition": {
           "StringNotEquals": {
             "aws:SourceVpce": "vpce-id"
           }
         }
       }
     ]
   }
   ```

6. Wählen Sie Änderungen speichern aus.

Ihr S3-Bucket ist jetzt nur von der spezifischen VPC aus zugänglich, die Sie erstellt haben.

Schritt 3: Erstellen Sie einen Amazon S3 Testdatenquellen-Connector

Um Ihre Amazon VPC Konfiguration zu testen, erstellen Sie einen Amazon S3 Connector. Konfigurieren Sie es dann mit der VPC, die Sie erstellt haben, indem Sie die unter beschriebenen Schritte ausführen. Amazon S3

Wählen Sie für Amazon VPC Konfigurationswerte die Werte aus, die Sie in diesem Beispiel erstellt haben:

- Amazon VPC(VPC) — `kendra-s3-example-vpc`
- Subnetze — `kendra-s3-example-subnet-private1-[availability zone]`
- Sicherheitsgruppen — `s3-data-source-security-group`

Warten Sie, bis Ihr Connector mit der Erstellung fertig ist. Nachdem der Amazon S3 Connector erstellt wurde, wählen Sie Jetzt synchronisieren, um eine Synchronisierung zu starten.

Je nachdem, wie viele Dokumente sich in Ihrem Amazon S3 Bucket befinden, kann es mehrere Minuten bis mehrere Stunden dauern, bis die Synchronisierung abgeschlossen ist. Um das Beispiel zu testen, empfehlen wir Ihnen, nur einige Dokumente in Ihren S3-Bucket hochzuladen. Wenn Ihre Konfiguration korrekt ist, sollte irgendwann der Synchronisierungsstatus Abgeschlossen angezeigt werden.

Wenn Sie auf Fehler stoßen, finden Sie weitere Informationen unter Amazon VPC Verbindungsprobleme.

Amazon Kendra Webcrawler

Sie können den Amazon Kendra Web Crawler verwenden, um Webseiten zu crawlen und zu indizieren.

Sie können nur öffentlich zugängliche Websites oder interne Unternehmenswebsites crawlen, die das sichere Kommunikationsprotokoll Hypertext Transfer Protocol Secure (HTTPS) verwenden. Wenn Sie beim Crawling einer Website einen Fehler erhalten, kann es sein, dass die Website für das Crawling gesperrt ist. Um interne Websites zu crawlen, können Sie einen Webproxy einrichten. Der Web-Proxy muss öffentlich zugänglich sein. Sie können die Authentifizierung auch verwenden, um auf Websites zuzugreifen und diese zu crawlen.

Bei der Auswahl der zu indizierenden Websites müssen Sie die Amazon Acceptable Use Policy (Richtlinie zur zulässigen Nutzung) und alle anderen Amazon-Bedingungen einhalten. Denken Sie

daran, dass Sie Amazon Kendra Web Crawler nur verwenden dürfen, um Ihre eigenen Webseiten oder Webseiten zu indizieren, für deren Indexierung Sie autorisiert sind. Informationen dazu, wie Sie verhindern können, dass Amazon Kendra Web Crawler Ihre Website (s) indexiert, finden Sie unter. Konfiguration der *robots.txt* Datei für Amazon Kendra Web Crawler

> **Note**
>
> Der Missbrauch von Amazon Kendra Web Crawler zum aggressiven Crawlen von Websites oder Webseiten, die Ihnen nicht gehören, gilt nicht als zulässige Nutzung.

Amazon Kendra hat zwei Versionen des Connectors. web crawler Zu den unterstützten Funktionen jeder Version gehören:

Amazon Kendra Web Crawler-Konnektor v1.0//API WebCrawlerConfiguration

- Webproxy
- Einschluss-/Ausschlussfilter

Amazon Kendra Webcrawler-Konnektor v2.0/API TemplateConfiguration

- Feldzuordnungen
- Einschluss-/Ausschlussfilter
- Vollständige und inkrementelle Inhaltssynchronisierung
- Web-Proxy
- Basic-, NTLM/Kerberos-, SAML- und Formularauthentifizierung für Ihre Websites
- Virtual Private Cloud (VPC)

> **Important**
>
> Die Erstellung von Web Crawler v2.0-Connectoren wird von nicht unterstützt. AWS CloudFormation Verwenden Sie den Web Crawler v1.0-Connector, wenn Sie Unterstützung benötigen. AWS CloudFormation

Informationen zur Problembehandlung Ihres Amazon Kendra Webcrawler-Datenquellen-Connectors finden Sie unter. Problembehandlung bei Datenquellen

Themen

- Amazon Kendra Web Crawler-Konnektor v1.0
- Amazon Kendra Web Crawler-Konnektor v2.0
- Konfiguration der robots.txt Datei für Amazon Kendra Web Crawler

Amazon Kendra Web Crawler-Konnektor v1.0

Sie können Amazon Kendra Web Crawler verwenden, um Webseiten zu crawlen und zu indizieren.

Sie können nur öffentlich zugängliche Websites und Websites crawlen, die das sichere Kommunikationsprotokoll Hypertext Transfer Protocol Secure (HTTPS) verwenden. Wenn Sie beim Crawling einer Website einen Fehler erhalten, kann es sein, dass die Website für das Crawling gesperrt ist. Um interne Websites zu crawlen, können Sie einen Webproxy einrichten. Der Web-Proxy muss öffentlich zugänglich sein.

Bei der Auswahl der zu indizierenden Websites müssen Sie die Amazon Acceptable Use Policy (Richtlinie zur zulässigen Nutzung) und alle anderen Amazon-Bedingungen einhalten. Denken Sie daran, dass Sie Amazon Kendra Web Crawler nur verwenden dürfen, um Ihre eigenen Webseiten oder Webseiten zu indizieren, für deren Indexierung Sie autorisiert sind. Informationen dazu, wie Sie verhindern können, dass Amazon Kendra Web Crawler Ihre Website (s) indexiert, finden Sie unter. Konfiguration der *robots.txt* Datei für Amazon Kendra Web Crawler

> **Note**
>
> Der Missbrauch von Amazon Kendra Web Crawler zum aggressiven Crawlen von Websites oder Webseiten, die Ihnen nicht gehören, gilt nicht als zulässige Nutzung.

Informationen zur Problembehandlung Ihres Amazon Kendra Webcrawler-Datenquellen-Connectors finden Sie unter. Problembehandlung bei Datenquellen

Themen

- Unterstützte Features
- Voraussetzungen

- Anweisungen zur Verbindung
- Weitere Informationen

Unterstützte Features

- Web-Proxy
- Einschluss-/Ausschlussfilter

Voraussetzungen

Bevor Sie Ihre Websites Amazon Kendra indexieren können, überprüfen Sie die Details Ihrer Websites und Konten. AWS

Stellen Sie für Ihre Websites sicher, dass Sie über Folgendes verfügen:

- Die Seed- oder Sitemap-URLs der Websites, die Sie indexieren möchten, wurden kopiert.
- Für Websites, die eine Standardauthentifizierung erfordern: Notiert den Benutzernamen und das Passwort und kopiert den Hostnamen der Website und die Portnummer.
- Optional: Der Hostname der Website und die Portnummer wurden kopiert, wenn Sie einen Webproxy verwenden möchten, um eine Verbindung zu internen Websites herzustellen, die Sie crawlen möchten. Der Web-Proxy muss öffentlich zugänglich sein. Amazon Kendra unterstützt die Verbindung zu Web-Proxyservern, die über eine Standardauthentifizierung verfügen, oder Sie können eine Verbindung ohne Authentifizierung herstellen.
- Vergewissert, dass jedes Webseitendokument, das Sie indexieren möchten, einzigartig ist und auch für andere Datenquellen gilt, die Sie für denselben Index verwenden möchten. Jede Datenquelle, die Sie für einen Index verwenden möchten, darf nicht dasselbe Dokument in allen Datenquellen enthalten. Dokument-IDs gelten für einen Index global und müssen pro Index eindeutig sein.

Stellen Sie in Ihrem AWS Konto sicher, dass Sie über Folgendes verfügen:

- Hat einen Amazon Kendra Index erstellt und bei Verwendung der API die Index-ID notiert.
- Sie haben eine IAM Rolle für Ihre Datenquelle erstellt und, falls Sie die API verwenden, den ARN der IAM Rolle notiert.

> **Note**
>
> Wenn Sie Ihren Authentifizierungstyp und Ihre Anmeldeinformationen ändern, müssen Sie Ihre IAM Rolle aktualisieren, um auf die richtige AWS Secrets Manager geheime ID zugreifen zu können.

- Für Websites, die eine Authentifizierung erfordern, oder wenn Sie einen Webproxy mit Authentifizierung verwenden, haben Sie Ihre Authentifizierungsdaten AWS Secrets Manager geheim gespeichert und, falls Sie die API verwenden, den ARN des Geheimnisses notiert.

> **Note**
>
> Wir empfehlen Ihnen, Ihre Anmeldeinformationen und Ihr Geheimnis regelmäßig zu aktualisieren oder zu wechseln. Stellen Sie zu Ihrer eigenen Sicherheit nur die Zugriffsebene bereit, die erforderlich ist. Wir raten davon ab, Anmeldeinformationen und geheime Daten für alle Datenquellen und Connector-Versionen 1.0 und 2.0 (sofern zutreffend) wiederzuverwenden.

Wenn Sie noch keine IAM Rolle oder keinen Schlüssel haben, können Sie die Konsole verwenden, um eine neue IAM Rolle und ein neues Secrets Manager Geheimnis zu erstellen, wenn Sie Ihre web crawler Datenquelle mit verbinden. Amazon Kendra Wenn Sie die API verwenden, müssen Sie den ARN einer vorhandenen IAM Rolle und eines Secrets Manager Geheimnisses sowie eine Index-ID angeben.

Anweisungen zur Verbindung

Um eine Verbindung Amazon Kendra zu Ihrer web crawler Datenquelle herzustellen, müssen Sie die erforderlichen Details zu Ihrer web crawler Datenquelle angeben, damit Sie auf Ihre Daten zugreifen Amazon Kendra können. Falls Sie das noch nicht konfiguriert web crawler haben, Amazon Kendra sieheVoraussetzungen.

Console

Um eine Verbindung Amazon Kendra herzustellen web crawler

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die Amazon Kendra Konsole.

2. Wählen Sie im linken Navigationsbereich Indizes und dann den Index, den Sie verwenden möchten, aus der Indexliste aus.

> **Note**
>
> Sie können Ihre Einstellungen für die Benutzerzugriffskontrolle unter Indexeinstellungen konfigurieren oder bearbeiten.

3. Wählen Sie auf der Seite Erste Schritte die Option Datenquelle hinzufügen aus.
4. Wählen Sie auf der Seite Datenquelle hinzufügen die Option Webcrawler-Connector und dann Connector hinzufügen aus.
5. Geben Sie auf der Seite „Datenquellendetails angeben“ die folgenden Informationen ein:

   a. Geben Sie im Feld Name und Beschreibung für Datenquellenname einen Namen für Ihre Datenquelle ein. Sie können Bindestriche, aber keine Leerzeichen verwenden.

   b. (Optional) Beschreibung — Geben Sie eine optionale Beschreibung für Ihre Datenquelle ein.

   c. In Standardsprache — Wählen Sie eine Sprache aus, um Ihre Dokumente nach dem Index zu filtern. Sofern Sie nichts anderes angeben, ist die Standardsprache Englisch. Die in den Metadaten des Dokuments angegebene Sprache hat Vorrang vor der ausgewählten Sprache.

   d. Unter Tags für Neues Tag hinzufügen — Fügen Sie optionale Tags hinzu, um Ihre Ressourcen zu durchsuchen und zu filtern oder Ihre Kosten nachzuverfolgen. AWS

   e. Wählen Sie Weiter aus.

6. Geben Sie auf der Seite Zugriff und Sicherheit definieren die folgenden Informationen ein:

   a. Wählen Sie für Quelle je nach Anwendungsfall zwischen Quell-URLs und Quell-Sitemaps und geben Sie jeweils die Werte ein.

      Sie können bis zu 10 Quell-URLs und drei Sitemaps hinzufügen.

      > **Note**
      >
      > Wenn du eine Sitemap crawlen möchtest, überprüfe, ob die Basis- oder Stamm-URL mit den URLs auf deiner Sitemap-Seite übereinstimmt. Wenn Ihre Sitemap-URL beispielsweise lautet https://example.com/sitemap-page.html, sollten

die auf dieser Sitemap-Seite aufgeführten URLs auch die Basis-URL "https://example.com/" verwenden.

b. (Optional) Geben Sie für Web-Proxy die folgenden Informationen ein:

i. Hostname — Der Hostname, für den ein Webproxy erforderlich ist.

ii. Portnummer — Der vom Host-URL-Transportprotokoll verwendete Port. Die Portnummer sollte ein numerischer Wert zwischen 0 und 65535 sein.

iii. Für Web-Proxy-Anmeldeinformationen — Wenn Ihre Web-Proxyverbindung eine Authentifizierung erfordert, wählen Sie ein vorhandenes Geheimnis oder erstellen Sie ein neues Geheimnis, um Ihre Authentifizierungsdaten zu speichern. Wenn Sie ein neues Geheimnis erstellen möchten, wird ein AWS Secrets Manager geheimes Fenster geöffnet.

iv. Geben Sie die folgenden Informationen in das Fenster Create an AWS Secrets Manager Secrets Manager Secret ein:

A. Geheimer Name — Ein Name für Ihr Geheimnis. Das Präfix AmazonKendra-WebCrawler- " wird automatisch zu Ihrem geheimen Namen hinzugefügt.

B. Für Benutzername und Passwort — Geben Sie diese grundlegenden Authentifizierungsdaten für Ihre Websites ein.

C. Wählen Sie Speichern.

c. (Optional) Hosts mit Authentifizierung — Wählen Sie diese Option, um weitere Hosts mit Authentifizierung hinzuzufügen.

d. IAM Rolle — Wählen Sie eine bestehende IAM Rolle oder erstellen Sie eine neue IAM Rolle, um auf Ihre Repository-Anmeldeinformationen und Indexinhalte zuzugreifen.

> **Note**
>
> IAM Rollen, die für Indizes verwendet werden, können nicht für Datenquellen verwendet werden. Wenn Sie sich nicht sicher sind, ob eine vorhandene Rolle für einen Index oder eine häufig gestellte Frage verwendet wird, wählen Sie Neue Rolle erstellen, um Fehler zu vermeiden.

e. Wählen Sie Weiter aus.

7. Geben Sie auf der Seite „Synchronisierungseinstellungen konfigurieren“ die folgenden Informationen ein:

a. Crawlbereich — Wählen Sie die Art der Webseiten aus, die Sie crawlen möchten.

b. Crawl-Tiefe — Wählen Sie aus der Seed-URL die Anzahl der Ebenen aus, die gecrawlt werden sollen. Amazon Kendra

c. In den erweiterten Crawling-Einstellungen und der Option Zusätzliche Konfiguration werden die folgenden Informationen eingegeben:

   i. Maximale Dateigröße — Die maximale Webseite- oder Anhangsgröße für das Crawlen. Mindestens 0,000001 MB (1 Byte). Maximal 50 MB.

   ii. Maximale Anzahl an Links pro Seite — Die maximale Anzahl von Links, die pro Seite gecrawlt wurden. Links werden in der Reihenfolge ihres Auftretens gecrawlt. Mindestens 1 Link/Seite. Maximal 1000 Links/Seite.

   iii. Maximale Drosselung — Die maximale Anzahl von URLs, die pro Hostname pro Minute gecrawlt werden. Mindestens 1 URLs/Hostname/Minute. Maximal 300 URLs/Hostname/Minute.

   iv. Regex-Muster — Fügen Sie Muster für reguläre Ausdrücke hinzu, um bestimmte URLs ein- oder auszuschließen. Sie können bis zu 100 Muster hinzufügen.

d. Wählen Sie im Zeitplan für die Synchronisierungsausführung für Frequenz aus, wie oft mit Ihrer Datenquelle synchronisiert Amazon Kendra werden soll.

e. Wählen Sie Weiter aus.

8. Überprüfen Sie auf der Seite Überprüfen und erstellen, ob die von Ihnen eingegebenen Informationen korrekt sind, und wählen Sie dann Datenquelle hinzufügen aus. Sie können Ihre Informationen auch auf dieser Seite bearbeiten. Ihre Datenquelle wird auf der Seite Datenquellen angezeigt, nachdem die Datenquelle erfolgreich hinzugefügt wurde.

API

Um eine Verbindung Amazon Kendra herzustellen web crawler

Mithilfe der WebCrawlerConfigurationAPI müssen Sie Folgendes angeben:

- URLs — Geben Sie die Seed- oder Startpunkt-URLs der Websites oder die Sitemap-URLs der Websites an, mit SeedUrlConfigurationdenen Sie crawlen möchten, und. SiteMapsConfiguration

> **Note**
>
> Wenn Sie eine Sitemap crawlen möchten, überprüfen Sie, ob die Basis- oder Stamm-URL mit den URLs übereinstimmt, die auf Ihrer Sitemap-Seite aufgeführt sind. Wenn Ihre Sitemap-URL beispielsweise lautet https://example.com/sitemap-page.html, sollten die auf dieser Sitemap-Seite aufgeführten URLs auch die Basis-URL "https://example.com/" verwenden.

- Geheimer Amazon-Ressourcenname (ARN) — Wenn für eine Website eine Standardauthentifizierung erforderlich ist, geben Sie den Hostnamen, die Portnummer und ein Geheimnis an, in dem Ihre grundlegenden Authentifizierungsdaten mit Ihrem Benutzernamen und Passwort gespeichert werden. Sie geben den geheimen ARN mithilfe der AuthenticationConfigurationAPI an. Das Geheimnis wird in einer JSON-Struktur mit den folgenden Schlüsseln gespeichert:

  ```
  {
      "username": "user name",
      "password": "password"
  }
  ```

  Sie können Webproxy-Anmeldeinformationen auch mithilfe eines AWS Secrets Manager Geheimnisses angeben. Sie verwenden die ProxyConfigurationAPI, um den Hostnamen und die Portnummer der Website sowie optional das Geheimnis anzugeben, in dem Ihre Web-Proxy-Anmeldeinformationen gespeichert werden.

- IAM Rolle — Geben Sie an`RoleArn`, wann Sie anrufen`CreateDataSource`, um einer IAM Rolle Berechtigungen für den Zugriff auf Ihr Secrets Manager Geheimnis und für den Aufruf der erforderlichen öffentlichen APIs für den Webcrawler-Connector und zuzuweisen. Amazon Kendra Weitere Informationen finden Sie unter IAM Rollen für Webcrawler-Datenquellen.

Sie können auch die folgenden optionalen Funktionen hinzufügen:

- Crawlmodus — Wählen Sie aus, ob nur Hostnamen von Websites oder Hostnamen mit Subdomänen oder auch andere Domains gecrawlt werden sollen, auf die die Webseiten verweisen.

- Die „Tiefe“ oder die Anzahl der Ebenen von der Seed-Ebene bis zum Crawl. Beispielsweise hat die Seed-URL-Seite Tiefe 1 und alle Hyperlinks auf dieser Seite, die ebenfalls gecrawlt werden, haben Tiefe 2.
- Die maximale Anzahl von URLs auf einer einzelnen Webseite, die gecrawlt werden sollen.
- Die maximale Größe einer Webseite, die gecrawlt werden soll, in MB.
- Die maximale Anzahl an URLs, die pro Website-Host pro Minute gecrawlt werden.
- Der Webproxyhost und die Portnummer für die Verbindung zu internen Websites und das Crawlen dieser Websites. Der Hostname von https://a.example.com/page1.htmlist beispielsweise "a.example.com" und die Portnummer ist 443, der Standardport für HTTPS. Wenn Web-Proxy-Anmeldeinformationen erforderlich sind, um eine Verbindung zu einem Website-Host herzustellen, können Sie einen erstellen AWS Secrets Manager , der die Anmeldeinformationen speichert.
- Die Authentifizierungsinformationen für den Zugriff auf und das Crawlen von Websites, für die eine Benutzerauthentifizierung erforderlich ist.
- Mit dem Tool Custom Document Enrichment können Sie HTML-Metatags als Felder extrahieren. Weitere Informationen finden Sie unter Anpassen der Metadaten von Dokumenten während des Erfassungsprozesses. Ein Beispiel für das Extrahieren von HTML-Metatags finden Sie unter CDE-Beispiele.
- Inklusions- und Ausschlussfilter — Geben Sie an, ob bestimmte URLs ein- oder ausgeschlossen werden sollen.

> **Note**
>
> Die meisten Datenquellen verwenden Muster für reguläre Ausdrücke, bei denen es sich um Ein- oder Ausschlussmuster handelt, die als Filter bezeichnet werden. Wenn Sie einen Einschlussfilter angeben, werden nur Inhalte indexiert, die dem Einschlussfilter entsprechen. Jedes Dokument, das nicht dem Einschlussfilter entspricht, wird nicht indexiert. Wenn Sie einen Ein- und Ausschlussfilter angeben, werden Dokumente, die dem Ausschlussfilter entsprechen, nicht indexiert, auch wenn sie dem Einschlussfilter entsprechen.

Weitere Informationen

Weitere Informationen zur Integration Amazon Kendra mit Ihrer web crawler Datenquelle finden Sie unter:

- Stellen Sie sich die Wissensfindung mit dem Web Amazon Kendra Crawler neu vor

Amazon Kendra Web Crawler-Konnektor v2.0

Sie können Amazon Kendra Web Crawler verwenden, um Webseiten zu crawlen und zu indizieren.

Sie können nur öffentlich zugängliche Websites oder interne Unternehmenswebsites crawlen, die das sichere Kommunikationsprotokoll Hypertext Transfer Protocol Secure (HTTPS) verwenden. Wenn Sie beim Crawling einer Website einen Fehler erhalten, kann es sein, dass die Website für das Crawling gesperrt ist. Um interne Websites zu crawlen, können Sie einen Webproxy einrichten. Der Web-Proxy muss öffentlich zugänglich sein. Sie können die Authentifizierung auch verwenden, um auf Websites zuzugreifen und diese zu crawlen.

Amazon Kendra Web Crawler v2.0 verwendet das Selenium-Webcrawler-Paket und einen Chromium-Treiber. Amazon Kendra aktualisiert automatisch die Version von Selenium und den Chromium-Treiber mithilfe von Continuous Integration (CI).

Bei der Auswahl der zu indizierenden Websites müssen Sie die Amazon Acceptable Use Policy (Richtlinie zur zulässigen Nutzung) und alle anderen Amazon-Bedingungen einhalten. Denken Sie daran, dass Sie Amazon Kendra Web Crawler nur verwenden dürfen, um Ihre eigenen Webseiten oder Webseiten zu indizieren, für deren Indexierung Sie autorisiert sind. Informationen dazu, wie Sie verhindern können, dass Amazon Kendra Web Crawler Ihre Website (s) indexiert, finden Sie unter. Konfiguration der *robots.txt* Datei für Amazon Kendra Web Crawler . Der Missbrauch von Amazon Kendra Web Crawler zum aggressiven Crawlen von Websites oder Webseiten, die Ihnen nicht gehören, wird nicht als akzeptable Nutzung angesehen.

Informationen zur Problembehandlung Ihres Amazon Kendra Webcrawler-Datenquellen-Connectors finden Sie unter. Problembehandlung bei Datenquellen

> **Note**
>
> Web Crawler Connector v2.0 unterstützt das Crawlen von Website-Listen aus verschlüsselten Buckets nicht. AWS KMS Amazon S3 Er unterstützt nur serverseitige Verschlüsselung mit verwalteten Schlüsseln. Amazon S3

> **Important**
>
> Die Erstellung von Web Crawler v2.0-Connectoren wird von nicht unterstützt. AWS CloudFormation Verwenden Sie den Web Crawler v1.0-Connector, wenn Sie Unterstützung benötigen. AWS CloudFormation

Themen

Unterstützte Features

- Feldzuordnungen
- Einschluss-/Ausschlussfilter
- Vollständige und inkrementelle Inhaltssynchronisierung
- Web-Proxy
- Basic-, NTLM/Kerberos-, SAML- und Formularauthentifizierung für Ihre Websites
- Virtual Private Cloud (VPC)

Voraussetzungen

Bevor Sie Ihre Websites Amazon Kendra indexieren können, sollten Sie die Details Ihrer Websites und Konten überprüfen. AWS

Stellen Sie für Ihre Websites sicher, dass Sie über Folgendes verfügen:

- Die Seed- oder Sitemap-URLs der Websites, die Sie indexieren möchten, wurden kopiert. Sie können die URLs in einer Textdatei speichern und diese in einen Amazon S3 Bucket hochladen. Jede URL in der Textdatei muss in einer separaten Zeile formatiert werden. Wenn Sie Ihre Sitemaps in einem Amazon S3 Bucket speichern möchten, stellen Sie sicher, dass Sie das Sitemap-XML kopiert und in einer XML-Datei gespeichert haben. Sie können auch mehrere Sitemap-XML-Dateien in einer ZIP-Datei zusammenfassen.

> **Note**
>
> (On-Premise/Server) Amazon Kendra überprüft, ob die in AWS Secrets Manager der Datei enthaltenen Endpunktinformationen mit den Endpunktinformationen übereinstimmen, die in den Konfigurationsdetails Ihrer Datenquelle angegeben sind. Dies trägt zum Schutz vor dem Problem des verwirrten Stellvertreters bei, bei dem es sich um ein Sicherheitsproblem handelt, bei dem ein Benutzer nicht berechtigt ist, eine Aktion auszuführen, sondern ihn Amazon Kendra als Proxy verwendet, um auf das konfigurierte Geheimnis zuzugreifen und die Aktion auszuführen. Wenn Sie Ihre Endpunktinformationen später ändern, müssen Sie ein neues Geheimnis erstellen, um diese Informationen zu synchronisieren.

- Für Websites, die eine Basic-, NTLM- oder Kerberos-Authentifizierung erfordern:
  - Notieren Sie sich Ihre Anmeldeinformationen für die Website-Authentifizierung, die einen Benutzernamen und ein Passwort enthalten.

    > **Note**
    >
    > Amazon Kendra Web Crawler v2.0 unterstützt das NTLM-Authentifizierungsprotokoll, das Passwort-Hashing beinhaltet, und das Kerberos-Authentifizierungsprotokoll, das Passwortverschlüsselung beinhaltet.

- Für Websites, die eine SAML- oder Anmeldeformularauthentifizierung erfordern:
  - Notieren Sie sich Ihre Anmeldeinformationen für die Website-Authentifizierung, die einen Benutzernamen und ein Passwort enthalten.
  - Die XPaths (XML Path Language) des Benutzernamenfeldes (und der Benutzernamenschaltfläche bei Verwendung von SAML), des Passwortfeldes und der Schaltfläche wurden kopiert und die URL der Anmeldeseite kopiert. Sie können die XPaths von Elementen mithilfe der Entwicklertools Ihres Webbrowsers finden. XPaths folgen normalerweise diesem Format:. `//tagname[@Attribute='Value']`

    > **Note**
    >
    > Amazon Kendra Web Crawler v2.0 verwendet einen Headless-Chrome-Browser und die Informationen aus dem Formular, um den Zugriff mit einer durch OAuth 2.0 geschützten URL zu authentifizieren und zu autorisieren.

- Optional: Der Hostname und die Portnummer des Web-Proxyservers wurden kopiert, wenn Sie einen Webproxy verwenden möchten, um eine Verbindung zu internen Websites herzustellen, die Sie crawlen möchten. Der Web-Proxy muss öffentlich zugänglich sein. Amazon Kendra unterstützt die Verbindung zu Web-Proxyservern, die über eine Standardauthentifizierung verfügen, oder Sie können eine Verbindung ohne Authentifizierung herstellen.
- Optional: Die Subnetz-ID der Virtual Private Cloud (VPC) wurde kopiert, wenn Sie eine VPC verwenden möchten, um eine Verbindung zu internen Websites herzustellen, die Sie crawlen möchten. Weitere Informationen finden Sie unter Konfiguration eines. Amazon VPC
- Es wurde überprüft, ob jedes Webseitendokument, das Sie indizieren möchten, einzigartig ist und dass es sich um ein und dasselbe Dokument aus anderen Datenquellen handelt, die Sie für denselben Index verwenden möchten. Jede Datenquelle, die Sie für einen Index verwenden möchten, darf nicht dasselbe Dokument in allen Datenquellen enthalten. Dokument-IDs gelten für einen Index global und müssen pro Index eindeutig sein.

Stellen Sie in Ihrem AWS Konto sicher, dass Sie über Folgendes verfügen:

- Hat einen Amazon Kendra Index erstellt und bei Verwendung der API die Index-ID notiert.
- Sie haben eine IAM Rolle für Ihre Datenquelle erstellt und, falls Sie die API verwenden, den ARN der IAM Rolle notiert.

> **Note**
>
> Wenn Sie Ihren Authentifizierungstyp und Ihre Anmeldeinformationen ändern, müssen Sie Ihre IAM Rolle aktualisieren, um auf die richtige AWS Secrets Manager geheime ID zugreifen zu können.

- Für Websites, die eine Authentifizierung erfordern, oder wenn Sie einen Webproxy mit Authentifizierung verwenden, haben Sie Ihre Authentifizierungsdaten AWS Secrets Manager geheim gespeichert und, falls Sie die API verwenden, den ARN des Geheimnisses notiert.

> **Note**
>
> Wir empfehlen Ihnen, Ihre Anmeldeinformationen und Ihr Geheimnis regelmäßig zu aktualisieren oder zu wechseln. Stellen Sie zu Ihrer eigenen Sicherheit nur die Zugriffsebene bereit, die erforderlich ist. Wir raten davon ab, Anmeldeinformationen

und geheime Daten für alle Datenquellen und Connector-Versionen 1.0 und 2.0 (sofern zutreffend) wiederzuverwenden.

Wenn Sie noch keine IAM Rolle oder keinen Schlüssel haben, können Sie die Konsole verwenden, um eine neue IAM Rolle und ein neues Secrets Manager Geheimnis zu erstellen, wenn Sie Ihre web crawler Datenquelle mit verbinden. Amazon Kendra Wenn Sie die API verwenden, müssen Sie den ARN einer vorhandenen IAM Rolle und eines Secrets Manager Geheimnisses sowie eine Index-ID angeben.

Anweisungen zur Verbindung

Um eine Verbindung Amazon Kendra zu Ihrer web crawler Datenquelle herzustellen, müssen Sie die erforderlichen Details zu Ihrer web crawler Datenquelle angeben, damit Sie auf Ihre Daten zugreifen Amazon Kendra können. Falls Sie das noch nicht konfiguriert web crawler haben, Amazon Kendra sieheVoraussetzungen.

Console

Um eine Verbindung Amazon Kendra herzustellen web crawler

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die Amazon Kendra Konsole.
2. Wählen Sie im linken Navigationsbereich Indizes und dann den Index, den Sie verwenden möchten, aus der Indexliste aus.

   > **Note**
   >
   > Sie können Ihre Einstellungen für die Benutzerzugriffskontrolle unter Indexeinstellungen konfigurieren oder bearbeiten.

3. Wählen Sie auf der Seite Erste Schritte die Option Datenquelle hinzufügen aus.
4. Wählen Sie auf der Seite Datenquelle hinzufügen die Option Webcrawler-Connector und dann Connector hinzufügen aus.
5. Geben Sie auf der Seite „Datenquellendetails angeben“ die folgenden Informationen ein:

   a. Geben Sie im Feld Name und Beschreibung für Datenquellenname einen Namen für Ihre Datenquelle ein. Sie können Bindestriche, aber keine Leerzeichen verwenden.

b. (Optional) Beschreibung — Geben Sie eine optionale Beschreibung für Ihre Datenquelle ein.

c. In Standardsprache — Wählen Sie eine Sprache aus, um Ihre Dokumente nach dem Index zu filtern. Sofern Sie nichts anderes angeben, ist die Standardsprache Englisch. Die in den Metadaten des Dokuments angegebene Sprache hat Vorrang vor der ausgewählten Sprache.

d. Unter Tags für Neues Tag hinzufügen — Fügen Sie optionale Tags hinzu, um Ihre Ressourcen zu durchsuchen und zu filtern oder Ihre Kosten nachzuverfolgen. AWS

e. Wählen Sie Weiter aus.

6. Geben Sie auf der Seite Zugriff und Sicherheit definieren die folgenden Informationen ein:

a. Quelle — Wählen Sie entweder Quell-URLs, Quell-Sitemaps, Quell-URL-Datei, Quell-Sitemaps-Datei aus. Wenn Sie eine Textdatei verwenden möchten, die eine Liste mit bis zu 100 Seed-URLs enthält, geben Sie den Pfad zu dem Amazon S3 Bucket an, in dem Ihre Datei gespeichert ist. Wenn Sie sich für die Verwendung einer XML-Sitemap-Datei entscheiden, geben Sie den Pfad zu dem Amazon S3 Bucket an, in dem Ihre Datei gespeichert ist. Sie können auch mehrere XML-Sitemap-Dateien in einer ZIP-Datei zusammenfassen. Andernfalls können Sie manuell bis zu 10 Seed- oder Startpunkt-URLs und bis zu drei Sitemap-URLs eingeben.

> **Note**
>
> Wenn du eine Sitemap crawlen möchtest, überprüfe, ob die Basis- oder Stamm-URL mit den URLs übereinstimmt, die auf deiner Sitemap-Seite aufgeführt sind. Wenn Ihre Sitemap-URL beispielsweise lautet https://example.com/sitemap-page.html, sollten die auf dieser Sitemap-Seite aufgeführten URLs auch die Basis-URL "https://example.com/" verwenden.

Wenn für Ihre Websites eine Authentifizierung für den Zugriff auf die Websites erforderlich ist, können Sie zwischen Basic-, NTLM/Kerberos-, SAML- oder Formularauthentifizierung wählen. Wählen Sie andernfalls die Option „Keine Authentifizierung“.

> **Note**
>
> Wenn Sie Ihre Datenquelle später bearbeiten möchten, um Ihre Seed-URLs mit Authentifizierung in Sitemaps zu ändern, müssen Sie eine neue Datenquelle erstellen. Amazon Kendra konfiguriert die Datenquelle mithilfe der Endpunktinformationen der Seed-URLs im Secrets Manager Secret für die Authentifizierung und kann daher die Datenquelle nicht neu konfigurieren, wenn zu Sitemaps gewechselt wird.

- AWS Secrets Manager geheim — Wenn Ihre Websites dieselbe Authentifizierung für den Zugriff auf die Websites benötigen, wählen Sie ein vorhandenes Geheimnis oder erstellen Sie ein neues Secrets Manager Geheimnis, um Ihre Website-Anmeldeinformationen zu speichern. Wenn Sie ein neues Geheimnis erstellen möchten, wird ein AWS Secrets Manager geheimes Fenster geöffnet.

  Wenn Sie sich für Basic - oder NTML/Kerberos-Authentifizierung entschieden haben, geben Sie einen Namen für das Geheimnis sowie den Benutzernamen und das Passwort ein. Das NTLM-Authentifizierungsprotokoll umfasst Kennwort-Hashing, und das Kerberos-Authentifizierungsprotokoll beinhaltet Kennwortverschlüsselung.

  Wenn Sie sich für SAML oder Formularauthentifizierung entschieden haben, geben Sie einen Namen für das Geheimnis sowie den Benutzernamen und das Passwort ein. Verwenden Sie XPath für das Benutzernamenfeld (und XPath für die Benutzernamenschaltfläche, wenn Sie SAML verwenden). Verwenden Sie XPaths für das Passwortfeld und die Schaltfläche sowie die URL der Anmeldeseite. Sie können die XPaths (XML Path Language) von Elementen mithilfe der Entwicklertools Ihres Webbrowsers finden. XPaths folgen normalerweise diesem Format:. `//tagname[@Attribute='Value']`

b. (Optional) Web-Proxy — Geben Sie den Hostnamen und die Portnummer des Proxyservers ein, den Sie für die Verbindung zu internen Websites verwenden möchten. Der Hostname von https://a.example.com/page1.htmlist beispielsweise "a.example.com" und die Portnummer ist 443, der Standardport für HTTPS. Wenn Web-Proxy-Anmeldeinformationen erforderlich sind, um eine Verbindung zu einem

Website-Host herzustellen, können Sie einen erstellen AWS Secrets Manager , der die Anmeldeinformationen speichert.

c. Virtual Private Cloud (VPC) — Sie können wählen, ob Sie eine VPC verwenden möchten. In diesem Fall müssen Sie Subnetze und VPC-Sicherheitsgruppen hinzufügen.

d. IAM Rolle — Wählen Sie eine bestehende IAM Rolle oder erstellen Sie eine neue IAM Rolle, um auf Ihre Repository-Anmeldeinformationen und Indexinhalte zuzugreifen.

> **Note**
>
> IAM Rollen, die für Indizes verwendet werden, können nicht für Datenquellen verwendet werden. Wenn Sie sich nicht sicher sind, ob eine vorhandene Rolle für einen Index oder eine häufig gestellte Frage verwendet wird, wählen Sie Neue Rolle erstellen, um Fehler zu vermeiden.

e. Wählen Sie Weiter aus.

7. Geben Sie auf der Seite „Synchronisierungseinstellungen konfigurieren“ die folgenden Informationen ein:

   a. Synchronisierungsbereich — Legen Sie Grenzwerte für das Crawlen von Webseiten fest, einschließlich ihrer Domains, Dateigrößen und Links, und filtern Sie URLs mithilfe von Regex-Mustern.

      i. (Optional) Domainbereich crawlen — Wählen Sie aus, ob nur Website-Domains, Domains mit Subdomänen oder auch andere Domains gecrawlt werden sollen, auf die die Webseiten verweisen. Standardmäßig werden Amazon Kendra nur die Domains der Websites gecrawlt, die Sie crawlen möchten.

      ii. (Optional) Zusätzliche Konfiguration — Legen Sie die folgenden Einstellungen fest:

      - Crawl-Tiefe — Die 'Tiefe' oder die Anzahl der Stufen von der Ausgangsebene bis zur Durchforstung. Beispielsweise hat die Seed-URL-Seite Tiefe 1 und alle Hyperlinks auf dieser Seite, die ebenfalls gecrawlt werden, haben Tiefe 2.
      - Maximale Dateigröße — Die maximale Größe einer Webseite oder eines Anhangs, die gecrawlt werden soll, in MB.
      - Maximale Anzahl an Links pro Seite — Die maximale Anzahl von URLs auf einer einzelnen Webseite, die gecrawlt werden können.
      - Maximale Drosselung der Crawling-Geschwindigkeit — Die maximale Anzahl von URLs, die pro Website-Host pro Minute gecrawlt werden.

- Dateien — Wählen Sie diese Option, um Dateien zu crawlen, auf die die Webseiten verweisen.
- URLs crawlen und indexieren — Fügen Sie Muster für reguläre Ausdrücke hinzu, um das Crawlen bestimmter URLs und die Indexierung aller Hyperlinks auf diesen URL-Webseiten ein- oder auszuschließen.

b. Synchronisierungsmodus — Wählen Sie aus, wie Sie Ihren Index aktualisieren möchten, wenn sich der Inhalt Ihrer Datenquelle ändert. Wenn Sie Ihre Datenquelle Amazon Kendra zum ersten Mal synchronisieren, werden alle Inhalte standardmäßig gecrawlt und indexiert. Sie müssen eine vollständige Synchronisierung Ihrer Daten durchführen, falls Ihre erste Synchronisierung fehlgeschlagen ist, auch wenn Sie die Option Vollsynchronisierung nicht als Synchronisierungsmodusoption wählen.

- Vollständige Synchronisierung: Indizieren Sie alle Inhalte neu und ersetzen vorhandene Inhalte jedes Mal, wenn Ihre Datenquelle mit Ihrem Index synchronisiert wird.
- Neue, geänderte, gelöschte Synchronisierung: Indizieren Sie bei jeder Synchronisierung Ihrer Datenquelle mit Ihrem Index nur neue, geänderte und gelöschte Inhalte. Amazon Kendra kann den Mechanismus Ihrer Datenquelle verwenden, um Inhaltsänderungen nachzuverfolgen und Inhalte zu indexieren, die sich seit der letzten Synchronisierung geändert haben.

c. Zeitplan für Synchronisierungsläufe — Wählen Sie unter Häufigkeit aus, wie oft mit Ihrer Datenquelle synchronisiert Amazon Kendra werden soll.

d. Wählen Sie Weiter aus.

8. Geben Sie auf der Seite Feldzuordnungen festlegen die folgenden Informationen ein:

a. Wählen Sie aus den Amazon Kendra generierten Standardfeldern von Webseiten und Dateien aus, die Sie Ihrem Index zuordnen möchten.

b. Wählen Sie Weiter aus.

9. Überprüfen Sie auf der Seite Überprüfen und erstellen, ob die von Ihnen eingegebenen Informationen korrekt sind, und wählen Sie dann Datenquelle hinzufügen aus. Sie können Ihre Informationen auch auf dieser Seite bearbeiten. Ihre Datenquelle wird auf der Seite Datenquellen angezeigt, nachdem die Datenquelle erfolgreich hinzugefügt wurde.

API

Um eine Verbindung Amazon Kendra herzustellen web crawler

Sie müssen mithilfe der TemplateConfigurationAPI einen JSON-Wert des Datenquellenschemas angeben. Sie müssen die folgenden Informationen angeben:

- Datenquelle — Geben Sie den Datenquellentyp wie `WEBCRAWLERV2` bei der Verwendung des TemplateConfigurationJSON-Schemas an. Geben Sie außerdem die Datenquelle so an`TEMPLATE`, wie Sie die CreateDataSourceAPI aufrufen.
- URLs — Geben Sie die Seed- oder Startpunkt-URLs der Websites oder die Sitemap-URLs der Websites an, die Sie crawlen möchten. Sie können den Pfad zu einem Amazon S3 Bucket angeben, in dem Ihre Liste von Seed-URLs gespeichert ist. Jede URL in der Textdatei für Seed-URLs muss in einer separaten Zeile formatiert werden. Sie können auch den Pfad zu einem Amazon S3 Bucket angeben, in dem Ihre Sitemap-XML-Dateien gespeichert sind. Sie können mehrere Sitemap-Dateien zu einer ZIP-Datei zusammenfassen und die ZIP-Datei in Ihrem Amazon S3 Bucket speichern.

  > **Note**
  >
  > Wenn du eine Sitemap crawlen möchtest, überprüfe, ob die Basis- oder Stamm-URL mit den URLs auf deiner Sitemap-Seite übereinstimmt. Wenn Ihre Sitemap-URL beispielsweise lautet https://example.com/sitemap-page.html, sollten die auf dieser Sitemap-Seite aufgeführten URLs auch die Basis-URL "https://example.com/" verwenden.

- Synchronisierungsmodus — Geben Sie an, wie Ihr Index aktualisiert Amazon Kendra werden soll, wenn sich der Inhalt Ihrer Datenquelle ändert. Wenn Sie Ihre Datenquelle Amazon Kendra zum ersten Mal synchronisieren, werden alle Inhalte standardmäßig gecrawlt und indexiert. Sie müssen eine vollständige Synchronisierung Ihrer Daten durchführen, falls Ihre erste Synchronisierung fehlgeschlagen ist, auch wenn Sie die Option Vollsynchronisierung nicht als Synchronisierungsmodusoption wählen. Sie können wählen zwischen:
  - `FORCED_FULL_CRAWL`um den gesamten Inhalt neu zu indizieren und vorhandene Inhalte jedes Mal zu ersetzen, wenn Ihre Datenquelle mit Ihrem Index synchronisiert wird.
  - `FULL_CRAWL`um bei jeder Synchronisierung Ihrer Datenquelle mit Ihrem Index nur neue, geänderte und gelöschte Inhalte zu indizieren. Amazon Kendra kann den Mechanismus Ihrer Datenquelle verwenden, um Inhaltsänderungen nachzuverfolgen und Inhalte zu indexieren, die sich seit der letzten Synchronisierung geändert haben.

- Authentifizierung — Wenn Ihre Websites dieselbe Authentifizierung erfordern, geben Sie entweder`BasicAuth`, `NTLM_KerberosSAML`, oder `Form` Authentifizierung an. Wenn für Ihre Websites keine Authentifizierung erforderlich ist, geben Sie `NoAuthentication` dies an.
- Geheimer Amazon-Ressourcenname (ARN) — Wenn für Ihre Websites eine Basic-, NTLM- oder Kerberos-Authentifizierung erforderlich ist, geben Sie ein Geheimnis an, in dem Ihre Authentifizierungsdaten mit Ihrem Benutzernamen und Passwort gespeichert werden. Sie geben den Amazon-Ressourcennamen (ARN) eines AWS Secrets Manager Geheimnisses an. Das Geheimnis wird in einer JSON-Struktur mit den folgenden Schlüsseln gespeichert:

```
{
    "seedUrlsHash": "Hash representation of all seed URLs",
    "userName": "user name",
    "password": "password"
}
```

Wenn für Ihre Websites eine SAML-Authentifizierung erforderlich ist, wird das Geheimnis in einer JSON-Struktur mit den folgenden Schlüsseln gespeichert:

```
{
    "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"
}
```

Wenn für Ihre Websites eine Formularauthentifizierung erforderlich ist, wird das Geheimnis in einer JSON-Struktur mit den folgenden Schlüsseln gespeichert:

```
{
    "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"
}
```

Sie können die XPaths (XML Path Language) von Elementen mithilfe der Entwicklertools Ihres Webbrowsers finden. XPaths folgen normalerweise diesem Format:. `//tagname[@Attribute='Value']`

Sie können Web-Proxy-Anmeldeinformationen auch mithilfe von und AWS Secrets Manager secret angeben.

- IAM Rolle — Geben Sie an`RoleArn`, wann Sie anrufen`CreateDataSource`, um einer IAM Rolle Berechtigungen für den Zugriff auf Ihr Secrets Manager Geheimnis und den Aufruf der erforderlichen öffentlichen APIs für den Webcrawler-Connector und zuzuweisen. Amazon Kendra Weitere Informationen finden Sie unter IAM Rollen für Webcrawler-Datenquellen.

Sie können auch die folgenden optionalen Funktionen hinzufügen:

- Virtual Private Cloud (VPC) — Geben Sie an, `VpcConfiguration` wann Sie anrufen. `CreateDataSource` Weitere Informationen finden Sie unter Konfigurieren von Amazon Kendra für die Verwendung eines Amazon VPC.
- Domainbereich — Wählen Sie aus, ob nur Website-Domains mit Subdomänen oder auch andere Domains, auf die die Webseiten verweisen, gecrawlt werden sollen. Standardmäßig werden Amazon Kendra nur die Domains der Websites gecrawlt, die Sie crawlen möchten.
- Die „Tiefe“ oder Anzahl der Ebenen von der Seed-Ebene bis zum Crawl. Beispielsweise hat die Seed-URL-Seite Tiefe 1 und alle Hyperlinks auf dieser Seite, die ebenfalls gecrawlt werden, haben Tiefe 2.
- Die maximale Anzahl von URLs auf einer einzelnen Webseite, die gecrawlt werden sollen.
- Die maximale Größe einer Webseite oder eines Anhangs, die gecrawlt werden soll, in MB.
- Die maximale Anzahl an URLs, die pro Website-Host pro Minute gecrawlt werden.
- Der Webproxyhost und die Portnummer für die Verbindung zu internen Websites und das Crawlen dieser Websites. Der Hostname von https://a.example.com/page1.htmlist beispielsweise "a.example.com" und die Portnummer ist 443, der Standardport für HTTPS. Wenn Web-Proxy-Anmeldeinformationen erforderlich sind, um eine Verbindung zu einem Website-Host herzustellen, können Sie einen erstellen AWS Secrets Manager , der die Anmeldeinformationen speichert.

- Inklusions- und Ausschlussfilter — Geben Sie an, ob das Crawlen bestimmter URLs und die Indexierung von Hyperlinks auf diesen URL-Webseiten ein- oder ausgeschlossen werden sollen.

  > **Note**
  >
  > Die meisten Datenquellen verwenden Muster für reguläre Ausdrücke. Dabei handelt es sich um Ein- oder Ausschlussmuster, die als Filter bezeichnet werden. Wenn Sie einen Einschlussfilter angeben, werden nur Inhalte indexiert, die dem Einschlussfilter entsprechen. Jedes Dokument, das nicht dem Einschlussfilter entspricht, wird nicht indexiert. Wenn Sie einen Ein- und Ausschlussfilter angeben, werden Dokumente, die dem Ausschlussfilter entsprechen, nicht indexiert, auch wenn sie dem Einschlussfilter entsprechen.

- Feldzuordnungen — Wählen Sie diese Option, um die Felder von Webseiten und Webseitendateien Ihren Indexfeldern zuzuordnen. Amazon Kendra Weitere Informationen finden Sie unter Zuweisen von Datenquellenfeldern.

Eine Liste weiterer wichtiger JSON-Schlüssel, die konfiguriert werden müssen, finden Sie unter Amazon Kendra Web Crawler-Vorlagenschema.

Konfiguration der **`robots.txt`** Datei für Amazon Kendra Web Crawler

Amazon Kendra ist ein intelligenter Suchdienst, mit dem AWS Kunden Dokumente ihrer Wahl indexieren und durchsuchen können. Um Dokumente im Internet zu indexieren, können Kunden den Amazon Kendra Web Crawler verwenden, der angibt, welche URL (s) indexiert werden sollen und welche Betriebsparameter angegeben werden sollen. Amazon Kendra Kunden müssen vor der Indexierung einer bestimmten Website eine Genehmigung einholen.

Amazon Kendra Web Crawler respektiert die Standardanweisungen von robots.txt wie `Allow` und. `Disallow` Sie können die `robots.txt` Datei Ihrer Website ändern, um zu steuern, wie Amazon Kendra Web Crawler Ihre Website crawlt.

Konfigurieren Sie, wie Amazon Kendra Web Crawler auf Ihre Website zugreift

Sie können mithilfe von AND-Anweisungen steuern, wie der Amazon Kendra Web Crawler Ihre Website indexiert. `Allow` `Disallow` Sie können auch steuern, welche Webseiten indexiert werden und welche Webseiten nicht gecrawlt werden.

Verwenden Sie die folgende Direktive, damit Amazon Kendra Web Crawler alle Webseiten mit Ausnahme unzulässiger Webseiten crawlen kann:

```
User-agent: amazon-kendra    # Amazon Kendra Web Crawler
Disallow: /credential-pages/ # disallow access to specific pages
```

Verwenden Sie die folgende Direktive, damit Amazon Kendra Web Crawler nur bestimmte Webseiten crawlen kann:

```
User-agent: amazon-kendra    # Amazon Kendra Web Crawler
Allow: /pages/ # allow access to specific pages
```

Verwenden Sie die folgende Anweisung, um Amazon Kendra Web Crawler das Crawlen aller Website-Inhalte zu ermöglichen und das Crawlen für andere Roboter zu verbieten:

```
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
```

Web Crawler daran hindern, Amazon Kendra Ihre Website zu crawlen

Mithilfe der Direktive können Sie verhindern, dass Amazon Kendra Web Crawler Ihre Website indexiert. `Disallow` Sie können auch steuern, welche Webseiten gecrawlt werden und welche nicht.

Verwenden Sie die folgende Anweisung, um zu verhindern, dass Amazon Kendra Web Crawler die Website crawlt:

```
User-agent: amazon-kendra # Amazon Kendra Web Crawler
Disallow: / # disallow access to any pages
```

Amazon Kendra Web Crawler unterstützt auch die Robots `noindex` und `nofollow` Direktiven in Metatags auf HTML-Seiten. Diese Direktiven verhindern, dass der Webcrawler eine Webseite indexiert, und er folgt keinen Links auf der Webseite mehr. Sie fügen die Metatags in den Abschnitt des Dokuments ein, um die Regeln der Robots-Regeln festzulegen.

Die folgende Webseite enthält beispielsweise die Direktiven Robots `noindex` und`nofollow`:

```
<html>
<head>
```

```
        <meta name="robots" content="noindex, nofollow"/>
        ...
    </head>
    <body>...</body>
    </html>
```

Wenn Sie Fragen oder Bedenken zu Amazon Kendra Web Crawler haben, können Sie sich an das AWS Support-Team wenden.

Amazon WorkDocs

Amazon WorkDocs ist ein sicherer Service für die Zusammenarbeit an Inhalten zum Erstellen, Bearbeiten, Speichern und Teilen von Inhalten. Sie können ihn verwenden Amazon Kendra , um Ihre Amazon WorkDocs Datenquelle zu indizieren.

Sie können über Amazon Kendra die Amazon Kendra Konsole und die WorkDocsConfigurationAPI eine Verbindung zu Ihrer Amazon WorkDocs Datenquelle herstellen.

Amazon WorkDocs ist in den Regionen Oregon, Nord-Virginia, Sydney, Singapur und Irland verfügbar.

Informationen zur Fehlerbehebung bei Ihrem Amazon Kendra WorkDocs Datenquellen-Connector finden Sie unterProblembehandlung bei Datenquellen.

Themen

- Unterstützte Features
- Voraussetzungen
- Anweisungen zur Verbindung
- Weitere Informationen

Unterstützte Features

Amazon Kendra WorkDocs Ein Datenquellenconnector unterstützt die folgenden Funktionen:

- Änderungsprotokoll
- Feldzuordnungen
- Filterung des Benutzerkontextes
- Einschluss-/Ausschlussfilter

Voraussetzungen

Bevor Sie Ihre WorkDocs Datenquelle Amazon Kendra zum Indizieren verwenden können, nehmen Sie diese Änderungen in Ihren WorkDocs Konten und Konten vor. AWS

Stellen Sie sicher WorkDocs, dass Sie Folgendes haben:

- Haben Sie sich die Amazon WorkDocs Verzeichnis-ID (Organisations-ID) für Ihr Amazon WorkDocs Repository notiert.
- Aktiviert, dass jedes Dokument in WorkDocs und zwischen anderen Datenquellen, die Sie für denselben Index verwenden möchten, einzigartig ist. Jede Datenquelle, die Sie für einen Index verwenden möchten, darf nicht dasselbe Dokument in allen Datenquellen enthalten. Dokument-IDs gelten für einen Index global und müssen pro Index eindeutig sein.

Stellen Sie in Ihrem AWS Konto sicher, dass Sie über Folgendes verfügen:

- Hat einen Amazon Kendra Index erstellt und bei Verwendung der API die Index-ID notiert.
- Sie haben eine IAM Rolle für Ihre Datenquelle erstellt und, falls Sie die API verwenden, den ARN der IAM Rolle notiert.

Wenn Sie noch keine IAM Rolle haben, können Sie die Konsole verwenden, um eine neue IAM Rolle zu erstellen, wenn Sie Ihre WorkDocs Datenquelle mit verbinden Amazon Kendra. Wenn Sie die API verwenden, müssen Sie den ARN einer vorhandenen IAM Rolle und eine Index-ID angeben.

Anweisungen zur Verbindung

Um eine Verbindung Amazon Kendra zu Ihrer WorkDocs Datenquelle herzustellen, müssen Sie die erforderlichen Details zu Ihrer WorkDocs Datenquelle angeben, damit Sie auf Ihre Daten zugreifen Amazon Kendra können. Falls Sie noch keine Konfiguration WorkDocs für vorgenommen haben Amazon Kendra, finden Sie weitere Informationen unterVoraussetzungen.

Console

Um eine Verbindung Amazon Kendra herzustellen Amazon WorkDocs

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die Amazon Kendra Konsole.
2. Wählen Sie im linken Navigationsbereich Indizes und dann den Index, den Sie verwenden möchten, aus der Indexliste aus.

> **Note**
>
> Sie können Ihre Einstellungen für die Benutzerzugriffskontrolle unter Indexeinstellungen konfigurieren oder bearbeiten.

3. Wählen Sie auf der Seite Erste Schritte die Option Datenquelle hinzufügen aus.
4. Wählen Sie auf der Seite Datenquelle hinzufügen die Option WorkDocs Connector und dann Connector hinzufügen aus.
5. Geben Sie auf der Seite „Datenquellendetails angeben“ die folgenden Informationen ein:

   a. Geben Sie im Feld Name und Beschreibung für Datenquellenname einen Namen für Ihre Datenquelle ein. Sie können Bindestriche, aber keine Leerzeichen verwenden.

   b. (Optional) Beschreibung — Geben Sie eine optionale Beschreibung für Ihre Datenquelle ein.

   c. In Standardsprache — Wählen Sie eine Sprache aus, um Ihre Dokumente nach dem Index zu filtern. Sofern Sie nichts anderes angeben, ist die Standardsprache Englisch. Die in den Metadaten des Dokuments angegebene Sprache hat Vorrang vor der ausgewählten Sprache.

   d. Unter Tags für Neues Tag hinzufügen — Fügen Sie optionale Tags hinzu, um Ihre Ressourcen zu durchsuchen und zu filtern oder Ihre Kosten nachzuverfolgen. AWS

   e. Wählen Sie Weiter aus.
6. Geben Sie auf der Seite Zugriff und Sicherheit definieren die folgenden Informationen ein:

   a. Spezifische Organisations-ID für Ihre Amazon WorkDocs Site — Wählen Sie die ID der Amazon WorkDocs Site aus, die Sie indexieren möchten. Sie müssen bereits eine Site erstellt haben.

   b. IAM Rolle — Wählen Sie eine bestehende IAM Rolle oder erstellen Sie eine neue IAM Rolle, um auf Ihre Repository-Anmeldeinformationen und Indexinhalte zuzugreifen.

   > **Note**
   >
   > IAM Rollen, die für Indizes verwendet werden, können nicht für Datenquellen verwendet werden. Wenn Sie sich nicht sicher sind, ob eine vorhandene Rolle für einen Index oder eine häufig gestellte Frage verwendet wird, wählen Sie Neue Rolle erstellen, um Fehler zu vermeiden.

c. Wählen Sie Weiter aus.

7. Geben Sie auf der Seite „Synchronisierungseinstellungen konfigurieren“ die folgenden Informationen ein:

   a. Dokumentkommentare durchforsten — Die Amazon WorkDocs Entitäten oder Inhaltstypen, die Sie crawlen möchten.

   b. Änderungsprotokolle verwenden — Wählen Sie diese Option, um Ihren Index nur mit neuen oder geänderten Inhalten zu aktualisieren, anstatt alle Ihre Dateien zu synchronisieren.

   c. Regex-Muster — Reguläre Ausdrucksmuster zum Ein- oder Ausschließen bestimmter Dateien. Sie können bis zu 100 Muster hinzufügen.

   d. Zeitplan für Synchronisierungsläufe für Häufigkeit — Wählen Sie aus, wie oft Amazon Kendra die Synchronisierung mit Ihrer Datenquelle erfolgen soll.

   e. Wählen Sie Weiter aus.

8. Geben Sie auf der Seite Feldzuordnungen festlegen die folgenden Informationen ein:

   a. Standard-Datenquellenfelder — Wählen Sie eines der Amazon Kendra generierten Standard-Datenquellenfelder aus, die Sie Ihrem Index zuordnen möchten.

   b. Feld hinzufügen — Um benutzerdefinierte Datenquellenfelder hinzuzufügen, um einen Indexfeldnamen für die Zuordnung und den Felddatentyp zu erstellen.

   c. Wählen Sie Weiter aus.

9. Überprüfen Sie auf der Seite Überprüfen und erstellen, ob die von Ihnen eingegebenen Informationen korrekt sind, und wählen Sie dann Datenquelle hinzufügen aus. Sie können Ihre Informationen auch auf dieser Seite bearbeiten. Ihre Datenquelle wird auf der Seite Datenquellen angezeigt, nachdem die Datenquelle erfolgreich hinzugefügt wurde.

API

Um eine Verbindung Amazon Kendra herzustellen Amazon WorkDocs

Mithilfe der WorkDocsConfigurationAPI müssen Sie Folgendes angeben:

- Amazon WorkDocs Verzeichnis-ID — Geben Sie die Organisations-ID Ihres Amazon WorkDocs Verzeichnisses an. Sie finden die Organisations-ID im AWS Directory Service, indem Sie zu Active Directory und dann zu Verzeichnissen gehen.

- IAM-Rolle — Geben Sie an, `RoleArn` wann Sie anrufen`CreateDataSource`, um einer IAM Rolle Berechtigungen für den Zugriff auf das WorkDocs Verzeichnis und für den Aufruf der erforderlichen öffentlichen APIs für den Connector und zum Aufrufen der erforderlichen öffentlichen APIs zu erteilen. WorkDocs Amazon Kendra Weitere Informationen finden Sie unter IAM-Rollen für Datenquellen. WorkDocs

Sie können auch die folgenden optionalen Funktionen hinzufügen:

- Änderungsprotokoll — Gibt an, ob der Mechanismus für das Änderungsprotokoll der WorkDocs Datenquelle verwendet werden Amazon Kendra soll, um zu ermitteln, ob ein Dokument im Index aktualisiert werden muss.

> **Note**
>
> Verwenden Sie das Änderungsprotokoll, wenn Sie nicht alle Dokumente scannen Amazon Kendra möchten. Wenn Ihr Änderungsprotokoll umfangreich ist, nimmt das Scannen der Dokumente in der WorkDocs Datenquelle möglicherweise Amazon Kendra weniger Zeit in Anspruch als das Verarbeiten des Änderungsprotokolls. Wenn Sie Ihre WorkDocs Datenquelle zum ersten Mal mit Ihrem Index synchronisieren, werden alle Dokumente gescannt.

- Inklusions- und Ausschlussfilter — Geben Sie an, ob bestimmte Dokumente und Dokumentkommentare ein- oder ausgeschlossen werden sollen. Jeder Kommentar wird als separates Dokument indexiert.

> **Note**
>
> Die meisten Datenquellen verwenden Muster für reguläre Ausdrücke, bei denen es sich um Ein- oder Ausschlussmuster handelt, die als Filter bezeichnet werden. Wenn Sie einen Einschlussfilter angeben, werden nur Inhalte indexiert, die dem Einschlussfilter entsprechen. Jedes Dokument, das nicht dem Einschlussfilter entspricht, wird nicht indexiert. Wenn Sie einen Ein- und Ausschlussfilter angeben, werden Dokumente, die dem Ausschlussfilter entsprechen, nicht indexiert, auch wenn sie dem Einschlussfilter entsprechen.

- Benutzerkontextfilterung und Zugriffskontrolle —Amazon Kendra durchsucht die Zugriffskontrollliste (ACL) für Ihre Dokumente, sofern Sie über eine ACL für Ihre Dokumente

verfügen. Die ACL-Informationen werden verwendet, um Suchergebnisse nach dem Benutzer- oder Gruppenzugriff auf Dokumente zu filtern. Weitere Informationen finden Sie unter Benutzerkontextfilterung.

- Feldzuordnungen — Wählen Sie diese Option, um Ihre WorkDocs Datenquellenfelder Ihren Indexfeldern zuzuordnen. Amazon Kendra Weitere Informationen finden Sie unter Zuweisen von Datenquellenfeldern.

> **Note**
>
> Das Textfeld oder das entsprechende Textfeld für Ihre Dokumente ist erforderlich, um Ihre Dokumente durchsuchen Amazon Kendra zu können. Sie müssen den Feldnamen Ihres Dokumenthauptteils in Ihrer Datenquelle dem Namen des Indexfeldes zuordnen`_document_body`. Alle anderen Felder sind optional.

Weitere Informationen

Weitere Informationen zur Integration Amazon Kendra mit Ihrer WorkDocs Datenquelle finden Sie unter:

- Erste Schritte mit dem Amazon Kendra WorkDocs Amazon-Connector

Box (Kasten)

Box ist ein Cloud-Speicherdienst, der Funktionen zum Hosten von Dateien bietet. Sie können ihn verwenden Amazon Kendra , um Inhalte in Ihren Box-Inhalten zu indizieren, einschließlich Kommentare, Aufgaben und Weblinks.

Sie können über Amazon Kendra die Amazon Kendra Konsole und die BoxConfigurationAPI eine Verbindung zu Ihrer Box-Datenquelle herstellen.

Informationen zur Fehlerbehebung bei Ihrem Amazon Kendra Box-Datenquellen-Connector finden Sie unterProblembehandlung bei Datenquellen.

Themen

- Unterstützte Features
- Voraussetzungen
- Anweisungen zur Verbindung

- Weitere Informationen

Unterstützte Features

Amazon Kendra Der Box-Datenquellen-Connector unterstützt die folgenden Funktionen:

- Änderungsprotokoll
- Feldzuordnungen
- Filterung des Benutzerkontextes
- Einschluss-/Ausschlussfilter
- Virtual Private Cloud (VPC)

Voraussetzungen

Bevor Sie Ihre Box-Datenquelle Amazon Kendra zum Indizieren verwenden können, nehmen Sie diese Änderungen in Ihrer Box und Ihren Konten vor. AWS

Stellen Sie in Box sicher, dass Sie über Folgendes verfügen:

- Ein Box Enterprise- oder Box Enterprise Plus-Konto.
- In der Box Developer Console wurde eine benutzerdefinierte Box-App erstellt und für die Verwendung der Serverauthentifizierung (mit JWT) konfiguriert.
- Stellen Sie Ihre App-Zugriffsebene auf App + Enterprise Access ein und erlauben Sie ihr, API-Aufrufe über den as-user-Header zu tätigen.
- Hat den Admin-Benutzer verwendet, um die folgenden Anwendungsbereiche zu Ihrer Box-App hinzuzufügen:
  - Schreiben Sie alle in einer Box gespeicherten Dateien und Ordner
  - Benutzer verwalten
  - Gruppen verwalten
  - Unternehmensimmobilien verwalten
- Generiertes und heruntergeladenes öffentliches/privates key pair, einschließlich einer Client-ID, eines geheimen Client-Schlüssels, einer öffentlichen Schlüssel-ID, einer privaten Schlüssel-ID, einer Passphrase und einer Unternehmens-ID zur Verwendung als Authentifizierungsdaten. Weitere Informationen finden Sie unter Öffentliches und privates Schlüsselpaar.

- Sie haben Ihre Box Enterprise ID entweder aus den Einstellungen der Box Developer Console oder aus Ihrer Box-App kopiert. Zum Beispiel *801234567*.
- Aktiviert, dass jedes Dokument in Box und in anderen Datenquellen, die Sie für denselben Index verwenden möchten, eindeutig ist. Jede Datenquelle, die Sie für einen Index verwenden möchten, darf nicht dasselbe Dokument in allen Datenquellen enthalten. Dokument-IDs gelten für einen Index global und müssen pro Index eindeutig sein.

Stellen Sie sicher AWS-Konto, dass Sie Folgendes in Ihrem haben:

- Hat einen Amazon Kendra Index erstellt und bei Verwendung der API die Index-ID notiert.
- Sie haben eine IAM Rolle für Ihre Datenquelle erstellt und, falls Sie die API verwenden, den ARN der IAM Rolle notiert.

> **Note**
>
> Wenn Sie Ihren Authentifizierungstyp und Ihre Anmeldeinformationen ändern, müssen Sie Ihre IAM Rolle aktualisieren, um auf die richtige AWS Secrets Manager geheime ID zugreifen zu können.

- Ihre Box-Authentifizierungsdaten AWS Secrets Manager geheim gespeichert und, falls Sie die API verwenden, den ARN des Geheimnisses notiert.

> **Note**
>
> Wir empfehlen Ihnen, Ihre Anmeldeinformationen und Ihr Geheimnis regelmäßig zu aktualisieren oder zu wechseln. Stellen Sie zu Ihrer eigenen Sicherheit nur die Zugriffsebene bereit, die erforderlich ist. Wir raten davon ab, Anmeldeinformationen und geheime Daten für alle Datenquellen und Connector-Versionen 1.0 und 2.0 (sofern zutreffend) wiederzuverwenden.

Wenn Sie noch keine IAM Rolle oder keinen Schlüssel haben, können Sie die Konsole verwenden, um eine neue IAM Rolle und ein neues Secrets Manager Geheimnis zu erstellen, wenn Sie Ihre Box-Datenquelle mit verbinden. Amazon Kendra Wenn Sie die API verwenden, müssen Sie den ARN einer vorhandenen IAM Rolle und eines Secrets Manager Geheimnisses sowie eine Index-ID angeben.

Anweisungen zur Verbindung

Um eine Verbindung Amazon Kendra zu Ihrer Box-Datenquelle herzustellen, müssen Sie die erforderlichen Details zu Ihrer Box-Datenquelle angeben, damit Sie auf Ihre Daten zugreifen Amazon Kendra können. Wenn Sie Box für noch nicht konfiguriert haben Amazon Kendra, finden Sie weitere Informationen unterVoraussetzungen.

Console

Um eine Verbindung Amazon Kendra zu Box herzustellen

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die Amazon Kendra Konsole.
2. Wählen Sie im linken Navigationsbereich Indizes und dann den Index, den Sie verwenden möchten, aus der Indexliste aus.

> **Note**
>
> Sie können Ihre Einstellungen für die Benutzerzugriffskontrolle unter Indexeinstellungen konfigurieren oder bearbeiten.

3. Wählen Sie auf der Seite Erste Schritte die Option Datenquelle hinzufügen aus.
4. Wählen Sie auf der Seite Datenquelle hinzufügen die Option Box-Konnektor und dann Konnektor hinzufügen aus.
5. Geben Sie auf der Seite „Datenquellendetails angeben“ die folgenden Informationen ein:

   a. Geben Sie im Feld Name und Beschreibung für Datenquellenname einen Namen für Ihre Datenquelle ein. Sie können Bindestriche, aber keine Leerzeichen verwenden.

   b. (Optional) Beschreibung — Geben Sie eine optionale Beschreibung für Ihre Datenquelle ein.

   c. In Standardsprache — Wählen Sie eine Sprache aus, um Ihre Dokumente nach dem Index zu filtern. Sofern Sie nichts anderes angeben, ist die Standardsprache Englisch. Die in den Metadaten des Dokuments angegebene Sprache hat Vorrang vor der ausgewählten Sprache.

   d. Unter Tags für Neues Tag hinzufügen — Fügen Sie optionale Tags hinzu, um Ihre Ressourcen zu durchsuchen und zu filtern oder Ihre Kosten nachzuverfolgen. AWS

   e. Wählen Sie Weiter aus.

6. Geben Sie auf der Seite Zugriff und Sicherheit definieren die folgenden Informationen ein:

   a. Box Enterprise ID — Geben Sie Ihre Box Enterprise ID ein.

   b. AWS Secrets Manager geheim — Wählen Sie ein vorhandenes Geheimnis oder erstellen Sie ein neues Secrets Manager Geheimnis, um Ihre Box-Authentifizierungsdaten zu speichern. Wenn Sie sich dafür entscheiden, ein neues Geheimnis zu erstellen, wird ein AWS Secrets Manager geheimes Fenster geöffnet.

      i. Geheimer Name — Ein Name für Ihr Geheimnis. Das Präfix 'AmazonKendra-Box' wird Ihrem geheimen Namen automatisch hinzugefügt.

      ii. Für Client-ID, Client Secret, Public Key-ID, Private Key-ID und Passphrase — Geben Sie die Werte aus dem öffentlichen/privaten Schlüssel ein, den Sie in Ihrem Box-Konto generiert und von Ihrem Box-Konto heruntergeladen haben.

      iii. Wählen Sie Speichern.

   c. Virtual Private Cloud (VPC) — Sie können wählen, ob Sie eine VPC verwenden möchten. In diesem Fall müssen Sie Subnetze und VPC-Sicherheitsgruppen hinzufügen.

   d. IAM Rolle — Wählen Sie eine bestehende IAM Rolle oder erstellen Sie eine neue IAM Rolle, um auf Ihre Repository-Anmeldeinformationen und Indexinhalte zuzugreifen.

      > **Note**
      >
      > IAM Rollen, die für Indizes verwendet werden, können nicht für Datenquellen verwendet werden. Wenn Sie sich nicht sicher sind, ob eine vorhandene Rolle für einen Index oder eine häufig gestellte Frage verwendet wird, wählen Sie Neue Rolle erstellen, um Fehler zu vermeiden.

   e. Wählen Sie Weiter aus.

7. Geben Sie auf der Seite „Synchronisierungseinstellungen konfigurieren“ die folgenden Informationen ein:

   a. Entitäten oder Inhaltstypen auswählen — Die Box-Entitäten oder Inhaltstypen, die Sie crawlen möchten. Jeder Kommentar wird als separates Dokument indexiert.

   b. Änderungsprotokoll — Wählen Sie diese Option, um Ihren Index nur für neue oder geänderte Inhalte zu aktualisieren, anstatt alle Ihre Dateien zu synchronisieren.

   c. Regex-Muster — Reguläre Ausdrucksmuster zum Ein- oder Ausschließen bestimmter Dateien. Sie können bis zu 100 Muster hinzufügen.

d. Wählen Sie im Zeitplan für die Synchronisierungsausführung für Frequenz aus, wie oft mit Ihrer Datenquelle synchronisiert Amazon Kendra werden soll.

e. Wählen Sie Weiter aus.

8. Geben Sie auf der Seite Feldzuordnungen festlegen die folgenden Informationen ein:

a. Für Dateien und Ordner, Kommentare, Aufgaben und Weblinks — Wählen Sie aus den Amazon Kendra generierten Standard-Datenquellenfeldern aus, die Sie Ihrem Index zuordnen möchten.

b. Feld hinzufügen — Um benutzerdefinierte Datenquellenfelder hinzuzufügen, um einen Indexfeldnamen für die Zuordnung und den Felddatentyp zu erstellen.

c. Wählen Sie Weiter aus.

9. Überprüfen Sie auf der Seite Überprüfen und erstellen, ob die von Ihnen eingegebenen Informationen korrekt sind, und wählen Sie dann Datenquelle hinzufügen aus. Sie können Ihre Informationen auch auf dieser Seite bearbeiten. Ihre Datenquelle wird auf der Seite Datenquellen angezeigt, nachdem die Datenquelle erfolgreich hinzugefügt wurde.

API

Um eine Verbindung Amazon Kendra zu Box herzustellen

Mithilfe der BoxConfigurationAPI müssen Sie Folgendes angeben:

Box Enterprise ID — Geben Sie Ihre Box Enterprise ID an. Sie finden die Unternehmens-ID in den Einstellungen der Box Developer Console oder wenn Sie eine App in Box erstellen.

- Geheimer Amazon-Ressourcenname (ARN) — Geben Sie den Amazon-Ressourcennamen (ARN) eines Secrets Manager Geheimnisses ein, das die Authentifizierungsdaten für Ihr Box-Konto enthält. Das Geheimnis wird in einer JSON-Struktur mit den folgenden Schlüsseln gespeichert:

```
{
    "clientID": "client-id",
    "clientSecret": "client-secret",
    "publicKeyID": "public-key-id",
    "privateKey": "private-key",
    "passphrase": "pass-phrase"
}
```

> **Note**
>
> Wir empfehlen Ihnen, Ihre Anmeldeinformationen und Ihr Geheimnis regelmäßig zu aktualisieren oder zu wechseln. Stellen Sie zu Ihrer eigenen Sicherheit nur die Zugriffsebene bereit, die erforderlich ist. Wir raten davon ab, Anmeldeinformationen und geheime Daten für alle Datenquellen und Connector-Versionen 1.0 und 2.0 (sofern zutreffend) wiederzuverwenden.

- IAM Rolle — Geben Sie an`RoleArn`, wann Sie anrufen`CreateDataSource`, um einer IAM Rolle Berechtigungen für den Zugriff auf Ihr Secrets Manager Geheimnis und den Aufruf der erforderlichen öffentlichen APIs für den Box-Connector und zum Aufrufen der erforderlichen öffentlichen APIs zu erteilen. Amazon Kendra Weitere Informationen finden Sie unter IAM Rollen für Box-Datenquellen.

Sie können auch die folgenden optionalen Funktionen hinzufügen:

- Virtual Private Cloud (VPC) — Geben Sie dies `VpcConfiguration` als Teil der Datenquellenkonfiguration an. Siehe Konfiguration Amazon Kendra für die Verwendung einer VPC.
- Änderungsprotokoll — Gibt an, ob der Change-Log-Mechanismus der Box-Datenquelle verwendet werden Amazon Kendra soll, um festzustellen, ob ein Dokument im Index aktualisiert werden muss.

> **Note**
>
> Verwenden Sie das Änderungsprotokoll, wenn Sie nicht alle Dokumente scannen Amazon Kendra möchten. Wenn Ihr Änderungsprotokoll umfangreich ist, nimmt das Scannen der Dokumente in der Box-Datenquelle möglicherweise Amazon Kendra weniger Zeit in Anspruch als das Verarbeiten des Änderungsprotokolls. Wenn Sie Ihre Box-Datenquelle zum ersten Mal mit Ihrem Index synchronisieren, werden alle Dokumente gescannt.

- Kommentare, Aufgaben, Weblinks — Geben Sie an, ob diese Inhaltstypen gecrawlt werden sollen.

> **Note**
>
> Die meisten Datenquellen verwenden Muster für reguläre Ausdrücke, bei denen es sich um Ein- oder Ausschlussmuster handelt, die als Filter bezeichnet werden. Wenn Sie einen Einschlussfilter angeben, werden nur Inhalte indexiert, die dem Einschlussfilter entsprechen. Jedes Dokument, das nicht dem Einschlussfilter entspricht, wird nicht indexiert. Wenn Sie einen Ein- und Ausschlussfilter angeben, werden Dokumente, die dem Ausschlussfilter entsprechen, nicht indexiert, auch wenn sie dem Einschlussfilter entsprechen.

- Ein- und Ausschlussfilter — Geben Sie an, ob bestimmte Box-Dateien und -Ordner ein- oder ausgeschlossen werden sollen.

> **Note**
>
> Die meisten Datenquellen verwenden Muster für reguläre Ausdrücke, bei denen es sich um Ein- oder Ausschlussmuster handelt, die als Filter bezeichnet werden. Wenn Sie einen Einschlussfilter angeben, werden nur Inhalte indexiert, die dem Einschlussfilter entsprechen. Jedes Dokument, das nicht dem Einschlussfilter entspricht, wird nicht indexiert. Wenn Sie einen Ein- und Ausschlussfilter angeben, werden Dokumente, die dem Ausschlussfilter entsprechen, nicht indexiert, auch wenn sie dem Einschlussfilter entsprechen.

- Benutzerkontextfilterung und Zugriffskontrolle —Amazon Kendra durchsucht die Zugriffskontrollliste (ACL) für Ihre Dokumente, sofern Sie über eine ACL für Ihre Dokumente verfügen. Die ACL-Informationen werden verwendet, um Suchergebnisse nach dem Benutzer- oder Gruppenzugriff auf Dokumente zu filtern. Weitere Informationen finden Sie unter Benutzerkontextfilterung.
- Feldzuordnungen — Wählen Sie diese Option, um Ihre Box-Datenquellenfelder Ihren Amazon Kendra Indexfeldern zuzuordnen. Weitere Informationen finden Sie unter Zuweisen von Datenquellenfeldern.

> **Note**
>
> Das Textfeld oder das entsprechende Textfeld für Ihre Dokumente ist erforderlich, um Ihre Dokumente durchsuchen Amazon Kendra zu können. Sie müssen den

Feldnamen Ihres Dokumenthauptteils in Ihrer Datenquelle dem Namen des Indexfeldes zuordnen_document_body. Alle anderen Felder sind optional.

Weitere Informationen

Weitere Informationen zur Integration Amazon Kendra mit Ihrer Box-Datenquelle finden Sie unter:

- Erste Schritte mit dem Amazon Kendra Box Connector

Confluence

Confluence ist ein kollaboratives Arbeitsmanagement-Tool, das für die gemeinsame Nutzung, Speicherung und Bearbeitung von Projekten, Softwareentwicklung und Produktmanagement entwickelt wurde. Sie können Amazon Kendra es verwenden, um Ihre Confluence-Bereiche, Seiten (einschließlich verschachtelter Seiten), Blogs sowie Kommentare und Anhänge zu indexierten Seiten und Blogs zu indizieren.

Amazon Kendra unterstützt sowohl Confluence Server als auch Confluence Cloud.

> **Note**
>
> Indiziert standardmäßig Amazon Kendra keine Confluence-Archive und persönlichen Bereiche. Sie können wählen, ob sie bei der Erstellung der Datenquelle indexiert werden sollen. Wenn Sie einen Bereich nicht Amazon Kendra indexieren möchten, markieren Sie ihn in Confluence als privat.

Du kannst dich entweder über Amazon Kendra die Amazon Kendra Konsole, die API oder die TemplateConfigurationAPI mit deiner Confluence-Datenquelle verbinden. ConfluenceConfiguration

Amazon Kendra hat zwei Versionen des Confluence-Connectors. Zu den unterstützten Funktionen jeder Version gehören:

Confluence-Konnektor V1.0//API ConfluenceConfiguration

- Feldzuordnungen
- Filterung des Benutzerkontextes

- Einschluss-/Ausschlussfilter
- (Nur für Confluence Server) Virtuelle private Cloud (VPC)

Confluence-Konnektor V2.0//API TemplateConfiguration

- Feldzuordnungen
- Filterung des Benutzerkontextes
- Virtual Private Cloud (VPC)
- Alle Dokumente synchronisieren/Nur neue, geänderte oder gelöschte Dokumente synchronisieren
- Einschluss-/Ausschlussmuster

> **Note**
>
> Die Support für Confluence Connector V1.0/ ConfluenceConfiguration API wird voraussichtlich 2023 enden. Wir empfehlen, zu Confluence Connector V2.0/ API zu migrieren oder diesen zu verwenden. TemplateConfiguration

Informationen zur Fehlerbehebung bei Ihrem Amazon Kendra Confluence-Datenquellen-Connector finden Sie unter. Problembehandlung bei Datenquellen

Themen

- Confluence-Konnektor V1.0
- Confluence-Konnektor V2.0

Confluence-Konnektor V1.0

Confluence ist ein kollaboratives Arbeitsmanagement-Tool, das für die gemeinsame Nutzung, Speicherung und Bearbeitung von Projekten, Softwareentwicklung und Produktmanagement entwickelt wurde. Sie können Amazon Kendra es verwenden, um Ihre Confluence-Bereiche, Seiten (einschließlich verschachtelter Seiten), Blogs sowie Kommentare und Anhänge zu indexierten Seiten und Blogs zu indizieren.

> **Note**
>
> Die Support für Confluence Connector V1.0/ ConfluenceConfiguration API wird voraussichtlich 2023 enden. Wir empfehlen, zu Confluence Connector V2.0/ API zu migrieren oder diesen zu verwenden. TemplateConfiguration

Informationen zur Fehlerbehebung bei Ihrem Amazon Kendra Confluence-Datenquellen-Connector finden Sie unter. Problembehandlung bei Datenquellen

Themen

Unterstützte Features

Amazon Kendra Der Confluence-Datenquellen-Connector unterstützt die folgenden Funktionen:

- Feldzuordnungen
- Filterung des Benutzerkontextes
- Einschluss-/Ausschlussfilter
- (Nur für Confluence Server) Virtuelle private Cloud (VPC)

Voraussetzungen

Bevor Sie Ihre Confluence-Datenquelle Amazon Kendra zum Indizieren verwenden können, nehmen Sie diese Änderungen in Ihrem Confluence und Ihren Konten vor. AWS

Stellen Sie in Confluence sicher, dass Sie über Folgendes verfügen:

- Du hast mir die Amazon Kendra Erlaubnis erteilt, alle Inhalte in deiner Confluence-Instanz anzusehen, indem du:
  - Mitglied Amazon Kendra einer Gruppe werden. `confluence-administrators`
  - Gewährung von Site-Admin-Rechten für alle vorhandenen Bereiche, Blogs und Seiten.

- Die URL deiner Confluence-Instanz wurde kopiert.
- Für SSO-Benutzer (Single Sign-On): Bei der Konfiguration der Confluence-Authentifizierungsmethoden in Confluence Data Center wurde die Option Auf der Anmeldeseite anzeigen für den Benutzernamen und das Passwort aktiviert.
- Für Confluence Server
  - Haben Sie Ihre grundlegenden Authentifizierungsdaten notiert, die den Benutzernamen und das Passwort Ihres Confluence-Administratorkontos enthalten, mit dem Sie sich verbinden möchten. Amazon Kendra
  - Optional: In Ihrem Confluence-Konto wurde ein persönliches Zugriffstoken generiert, mit dem Sie sich verbinden können. Amazon Kendra Weitere Informationen finden Sie in der Confluence-Dokumentation zur Generierung persönlicher Zugriffstoken.
- Für Confluence Cloud
  - Du hast dir deine grundlegenden Authentifizierungsdaten notiert, die den Benutzernamen und das Passwort deines Confluence-Administratorkontos für die Verbindung enthalten. Amazon Kendra
- Aktiviert, dass jedes Dokument in Confluence und in anderen Datenquellen, die Sie für denselben Index verwenden möchten, einzigartig ist. Jede Datenquelle, die Sie für einen Index verwenden möchten, darf nicht dasselbe Dokument in allen Datenquellen enthalten. Dokument-IDs gelten für einen Index global und müssen pro Index eindeutig sein.

Stellen Sie sicher AWS-Konto, dass Sie Folgendes in Ihrem haben:

- Hat einen Amazon Kendra Index erstellt und bei Verwendung der API die Index-ID notiert.
- Sie haben eine IAM Rolle für Ihre Datenquelle erstellt und, falls Sie die API verwenden, den ARN der IAM Rolle notiert.

> **Note**
>
> Wenn Sie Ihren Authentifizierungstyp und Ihre Anmeldeinformationen ändern, müssen Sie Ihre IAM Rolle aktualisieren, um auf die richtige AWS Secrets Manager geheime ID zugreifen zu können.

- Du hast deine Confluence-Authentifizierungsdaten AWS Secrets Manager geheim gespeichert und, falls du die API verwendest, den ARN des Secrets notiert.

> **Note**
>
> Wir empfehlen dir, deine Anmeldedaten und dein Secret regelmäßig zu aktualisieren oder zu wechseln. Stellen Sie zu Ihrer eigenen Sicherheit nur die erforderliche Zugriffsebene bereit. Wir raten davon ab, Anmeldeinformationen und geheime Daten für alle Datenquellen und Connector-Versionen 1.0 und 2.0 (sofern zutreffend) wiederzuverwenden.

Wenn du noch keine IAM Rolle oder keinen Schlüssel hast, kannst du die Konsole verwenden, um eine neue IAM Rolle und ein neues Secrets Manager Geheimnis zu erstellen, wenn du deine Confluence-Datenquelle mit verbindest. Amazon Kendra Wenn Sie die API verwenden, müssen Sie den ARN einer vorhandenen IAM Rolle und eines Secrets Manager Geheimnisses sowie eine Index-ID angeben.

Anweisungen zur Verbindung

Um eine Verbindung Amazon Kendra zu Ihrer Confluence-Datenquelle herzustellen, müssen Sie Details zu Ihren Confluence-Anmeldeinformationen angeben, damit Sie auf Ihre Daten zugreifen Amazon Kendra können. Falls Sie Confluence noch nicht konfiguriert haben, finden Sie weitere Informationen unter. Amazon Kendra Voraussetzungen

Console

Um eine Verbindung zu Confluence herzustellen Amazon Kendra

1. Melden Sie sich bei der AWS Management Console an und öffnen Sie die Amazon Kendra Konsole.
2. Wählen Sie im linken Navigationsbereich Indizes und dann den Index, den Sie verwenden möchten, aus der Indexliste aus.

   > **Note**
   >
   > Sie können Ihre Einstellungen für die Benutzerzugriffskontrolle unter Indexeinstellungen konfigurieren oder bearbeiten.

3. Wählen Sie auf der Seite Erste Schritte die Option Datenquelle hinzufügen aus.
4. Wählen Sie auf der Seite Datenquelle hinzufügen die Option Confluence Connector V1.0 und dann Datenquelle hinzufügen aus.

5. Geben Sie auf der Seite „Datenquellendetails angeben“ die folgenden Informationen ein:

   a. Geben Sie im Feld Name und Beschreibung für Datenquellenname einen Namen für Ihre Datenquelle ein. Sie können Bindestriche, aber keine Leerzeichen verwenden.

   b. (Optional) Beschreibung — Geben Sie eine optionale Beschreibung für Ihre Datenquelle ein.

   c. In Standardsprache — Wählen Sie eine Sprache aus, um Ihre Dokumente nach dem Index zu filtern. Sofern Sie nichts anderes angeben, ist die Standardsprache Englisch. Die in den Metadaten des Dokuments angegebene Sprache hat Vorrang vor der ausgewählten Sprache.

   d. Unter Tags für Neues Tag hinzufügen — Fügen Sie optionale Tags hinzu, um Ihre Ressourcen zu durchsuchen und zu filtern oder Ihre Kosten nachzuverfolgen. AWS

   e. Wählen Sie Weiter aus.

6. Geben Sie auf der Seite Zugriff und Sicherheit definieren die folgenden Informationen ein:

   a. Wählen Sie je nach Anwendungsfall zwischen Confluence Cloud und Confluence Server.

   b. Wenn Sie sich für Confluence Cloud entscheiden, geben Sie die folgenden Informationen ein:

      i. Confluence-URL — Ihre Confluence-URL.

      ii. AWS Secrets Manager geheim — Wählen Sie ein vorhandenes Geheimnis oder erstellen Sie ein neues Secrets Manager Geheimnis, um Ihre Confluence-Authentifizierungsdaten zu speichern. Wenn Sie sich dafür entscheiden, ein neues Geheimnis zu erstellen, wird ein AWS Secrets Manager geheimes Fenster geöffnet.

         - Geben Sie die folgenden Informationen in das Fenster Create an AWS Secrets Manager Secret ein:

            I. Geheimer Name — Ein Name für Ihr Geheimnis. Das Präfix 'AmazonKendra-Confluence-' wird Ihrem geheimen Namen automatisch hinzugefügt.

            II. Für Benutzername und Passwort — Geben Sie Ihren Confluence-Benutzernamen und Ihr Confluence-API-Token als Passwort ein.

            III. Wählen Sie Authentifizierung speichern.

   c. Wenn Sie Confluence Server wählen, geben Sie die folgenden Informationen ein:

i. Confluence-URL — Ihr Confluence-Benutzername und Ihr Passwort.

ii. (Optional) Geben Sie für den Web-Proxy die folgenden Informationen ein:

A. Hostname — Hostname für Ihr Confluence-Konto.

B. Portnummer — Port, der vom Host-URL-Transportprotokoll verwendet wird.

iii. Wählen Sie zwischen Standardauthentifizierung und Personal Access Token.

iv. AWS Secrets Manager geheim — Wählen Sie ein vorhandenes Geheimnis oder erstellen Sie ein neues Secrets Manager Geheimnis, um Ihre Confluence-Authentifizierungsdaten zu speichern. Wenn Sie sich dafür entscheiden, ein neues Geheimnis zu erstellen, wird ein AWS Secrets Manager geheimes Fenster geöffnet.

- Geben Sie die folgenden Informationen in das Fenster Create an AWS Secrets Manager Secret ein:

I. Geheimer Name — Ein Name für Ihr Geheimnis. Das Präfix 'AmazonKendra-Confluence-' wird Ihrem geheimen Namen automatisch hinzugefügt.

II. Für Benutzername und Passwort — Geben Sie die Werte für die Authentifizierungsdaten ein, die Sie generiert und von Ihrem Confluence-Konto heruntergeladen haben. Wenn Sie die Standardauthentifizierung verwenden, verwenden Sie Ihren Confluence-Benutzernamen und Ihr Passwort als Anmeldeinformationen. Wenn Sie ein persönliches Zugriffstoken verwenden, geben Sie die Details des persönlichen Zugriffstokens ein, das Sie in Ihrem Confluence-Konto erstellt haben.

III. Wählen Sie Authentifizierung speichern.

d. IAM Rolle — Wählen Sie eine bestehende IAM Rolle oder erstellen Sie eine neue IAM Rolle, um auf Ihre Repository-Anmeldeinformationen und Indexinhalte zuzugreifen.

> **Note**
>
> IAM Rollen, die für Indizes verwendet werden, können nicht für Datenquellen verwendet werden. Wenn Sie sich nicht sicher sind, ob eine vorhandene Rolle für einen Index oder eine häufig gestellte Frage verwendet wird, wählen Sie Neue Rolle erstellen, um Fehler zu vermeiden.

e. Wählen Sie Weiter aus.

7. Geben Sie auf der Seite „Synchronisierungseinstellungen konfigurieren“ die folgenden Informationen ein:

   a. Für Persönliche Bereiche einbeziehen und Archivierte Bereiche einbeziehen — Wählen Sie die optionalen Bereichstypen aus, die in diese Datenquelle aufgenommen werden sollen.

   b. Für zusätzliche Konfigurationen — Geben Sie Muster für reguläre Ausdrücke an, um bestimmte Inhalte ein- oder auszuschließen. Sie können bis zu 100 Muster hinzufügen.

   c. Sie können auch festlegen, dass Anlagen innerhalb bestimmter Bereiche gecrawlt werden.

   d. Wählen Sie im Zeitplan für die Synchronisierungsausführung unter Häufigkeit aus, wie oft mit Ihrer Datenquelle synchronisiert Amazon Kendra werden soll.

   e. Wählen Sie Weiter aus.

8. Geben Sie auf der Seite Feldzuordnungen festlegen die folgenden Informationen ein:

   a. Für Space, Page, Blog — Wählen Sie aus den Amazon Kendra generierten Standard-Datenquellenfeldern oder Zusätzliche vorgeschlagene Feldzuordnungen, um Indexfelder hinzuzufügen.

   b. Feld hinzufügen — Um benutzerdefinierte Datenquellenfelder hinzuzufügen, um einen Indexfeldnamen für die Zuordnung und den Felddatentyp zu erstellen.

   c. Wählen Sie Weiter aus.

9. Überprüfen Sie auf der Seite Überprüfen und erstellen, ob die von Ihnen eingegebenen Informationen korrekt sind, und wählen Sie dann Datenquelle hinzufügen aus. Sie können Ihre Informationen auch auf dieser Seite bearbeiten. Ihre Datenquelle wird auf der Seite Datenquellen angezeigt, nachdem die Datenquelle erfolgreich hinzugefügt wurde.

API

Um eine Verbindung Amazon Kendra zu Confluence herzustellen

Sie müssen mithilfe ConfluenceConfigurationder API Folgendes angeben:

- Confluence-Version — Geben Sie die Version der Confluence-Instanz an, die Sie als oder verwenden. `CLOUD` `SERVER`

- Geheimer Amazon-Ressourcenname (ARN) — Geben Sie den Amazon-Ressourcennamen (ARN) eines Secrets Manager Geheimnisses ein, das die Authentifizierungsdaten enthält, die Sie in Ihrem Confluence-Konto erstellt haben.

  Wenn Sie Confluence Server verwenden, können Sie entweder Ihren Confluence-Benutzernamen und Ihr Passwort oder Ihr persönliches Zugriffstoken als Anmeldeinformationen verwenden.

  Wenn Sie Ihren Confluence-Benutzernamen und Ihr Passwort als Authentifizierungsdaten verwenden, speichern Sie die folgenden Anmeldeinformationen als JSON-Struktur in Ihrem Secret: Secrets Manager

  ```
  {
      "username": "user name",
      "password": "password"
  }
  ```

  Wenn Sie ein persönliches Zugriffstoken verwenden, um eine Verbindung zu Confluence Server herzustellen Amazon Kendra, speichern Sie die folgenden Anmeldeinformationen als JSON-Struktur in Ihrem Secret: Secrets Manager

  ```
  {
      "patToken": "personal access token"
  }
  ```

  Wenn Sie Confluence Cloud als Amazon Kendra Datenquelle verwenden, verwenden Sie Ihren Confluence-Benutzernamen und ein in Ihrem Confluence-Konto generiertes API-Token als Passwort. Sie speichern die folgenden Anmeldeinformationen als JSON-Struktur in Ihrem Secret: Secrets Manager

  ```
  {
      "username": "user name",
      "password": "API token"
  }
  ```

  > **Note**
  >
  > Wir empfehlen Ihnen, Ihre Anmeldeinformationen und Ihr Geheimnis regelmäßig zu aktualisieren oder zu wechseln. Stellen Sie zu Ihrer eigenen Sicherheit nur die

erforderliche Zugriffsebene bereit. Wir raten davon ab, Anmeldeinformationen und geheime Daten für alle Datenquellen und Connector-Versionen 1.0 und 2.0 (sofern zutreffend) wiederzuverwenden.

- IAM role — Geben Sie an`RoleArn`, wann Sie anrufen`CreateDataSource`, um einer IAM Rolle Berechtigungen für den Zugriff auf Ihr Secrets Manager Secret und den Aufruf der erforderlichen öffentlichen APIs für den Confluence-Connector und zum Aufrufen der erforderlichen öffentlichen APIs zu erteilen. Amazon Kendra Weitere Informationen finden Sie unter IAM Rollen für Confluence-Datenquellen.

Sie können auch die folgenden optionalen Funktionen hinzufügen:

- Web-Proxy — Gibt an, ob Sie über einen Web-Proxy eine Verbindung zu Ihrer Confluence-URL-Instanz herstellen möchten. Sie können diese Option für Confluence Server verwenden.
- (Nur für Confluence Server) Virtual Private Cloud (VPC) — Geben Sie dies `VpcConfiguration` als Teil der Datenquellenkonfiguration an. Siehe Konfiguration Amazon Kendra für die Verwendung einer VPC.
- Inklusions- und Ausschlussfilter — Geben Sie Muster für reguläre Ausdrücke an, um bestimmte Bereiche, Blogbeiträge, Seiten, Bereiche und Anlagen ein- oder auszuschließen. Wenn Sie Anlagen indexieren möchten, werden nur Anlagen zu den indizierten Seiten und Blogs indexiert.

> **Note**
>
> Die meisten Datenquellen verwenden Muster für reguläre Ausdrücke, bei denen es sich um Ein- oder Ausschlussmuster handelt, die als Filter bezeichnet werden. Wenn Sie einen Einschlussfilter angeben, werden nur Inhalte indexiert, die dem Einschlussfilter entsprechen. Jedes Dokument, das nicht dem Einschlussfilter entspricht, wird nicht indexiert. Wenn Sie einen Ein- und Ausschlussfilter angeben, werden Dokumente, die dem Ausschlussfilter entsprechen, nicht indexiert, auch wenn sie dem Einschlussfilter entsprechen.

- Feldzuordnungen — Wählen Sie diese Option, um Ihre Confluence-Datenquellenfelder Ihren Indexfeldern zuzuordnen. Amazon Kendra Weitere Informationen finden Sie unter Zuweisen von Datenquellenfeldern.

> **Note**
>
> Das Textfeld oder das entsprechende Textfeld für Ihre Dokumente ist erforderlich, um Ihre Dokumente durchsuchen zu können. Amazon Kendra Sie müssen den Feldnamen Ihres Dokumenthauptteils in Ihrer Datenquelle dem Namen des Indexfeldes zuordnen`_document_body`. Alle anderen Felder sind optional.

- Benutzerkontextfilterung und ZugriffskontrolleAmazon Kendra — durchsucht die Zugriffskontrollliste (ACL) für Ihre Dokumente, sofern Sie über eine ACL für Ihre Dokumente verfügen. Die ACL-Informationen werden verwendet, um Suchergebnisse nach dem Benutzer- oder Gruppenzugriff auf Dokumente zu filtern. Weitere Informationen finden Sie unter Benutzerkontextfilterung.

Weitere Informationen

Weitere Informationen zur Integration Amazon Kendra mit Ihrer Confluence-Datenquelle finden Sie unter:

- Konfiguration Ihres Amazon Kendra Confluence Server-Connectors

Confluence-Konnektor V2.0

Confluence ist ein kollaboratives Arbeitsmanagement-Tool, das für die gemeinsame Nutzung, Speicherung und Bearbeitung von Projekten, Softwareentwicklung und Produktmanagement entwickelt wurde. Sie können Amazon Kendra es verwenden, um Ihre Confluence-Bereiche, Seiten (einschließlich verschachtelter Seiten), Blogs sowie Kommentare und Anhänge zu indexierten Seiten und Blogs zu indizieren.

Informationen zur Fehlerbehebung bei Ihrem Amazon Kendra Confluence-Datenquellen-Connector finden Sie unter. Problembehandlung bei Datenquellen

Themen

- Unterstützte Features
- Voraussetzungen
- Anweisungen zur Verbindung

Unterstützte Features

Amazon Kendra Der Confluence-Datenquellen-Connector unterstützt die folgenden Funktionen:

- Feldzuordnungen
- Filterung des Benutzerkontextes
- Einschluss-/Ausschlussmuster
- Vollständige und inkrementelle Inhaltssynchronisierung
- Virtual Private Cloud (VPC)

Voraussetzungen

Bevor Sie Ihre Confluence-Datenquelle Amazon Kendra zum Indizieren verwenden können, nehmen Sie diese Änderungen in Ihrem Confluence und Ihren Konten vor. AWS

Stellen Sie in Confluence sicher, dass Sie über Folgendes verfügen:

- Die URL deiner Confluence-Instanz wurde kopiert. Zum Beispiel: *https://example.confluence.com* oder *https://www.example.confluence.com/* oder *https://*atlassian.net/. Du benötigst die URL deiner Confluence-Instanz, mit der du dich verbinden möchtest. Amazon Kendra

  Wenn du Confluence Cloud verwendest, muss deine Host-URL auf atlassian.net/ enden.

  > **Note**
  >
  > Die folgenden URL-Formate werden nicht unterstützt:
  >
  > - *https://example.confluence.com/xyz*
  > - *https://www.example.confluence.com//wiki/spacekey/xxx*
  > - *https://atlassian.net/xyz*

  > **Note**
  >
  > (On-Premise/Server) Amazon Kendra überprüft, ob die in der Datei enthaltenen Endpunktinformationen mit den Endpunktinformationen übereinstimmen, die in AWS

Secrets Manager den Konfigurationsdetails deiner Datenquelle angegeben sind. Dies trägt zum Schutz vor dem Problem des verwirrten Stellvertreters bei, bei dem es sich um ein Sicherheitsproblem handelt, bei dem ein Benutzer nicht berechtigt ist, eine Aktion auszuführen, sondern ihn Amazon Kendra als Proxy verwendet, um auf das konfigurierte Geheimnis zuzugreifen und die Aktion auszuführen. Wenn Sie Ihre Endpunktinformationen später ändern, müssen Sie ein neues Geheimnis erstellen, um diese Informationen zu synchronisieren.

- Konfigurierte Basisauthentifizierungsdaten, die einen Benutzernamen (E-Mail-ID, mit der Sie sich bei Confluence angemeldet haben) und ein Passwort (Confluence-Serverpasswort) enthalten, um eine Verbindung Amazon Kendra zu Ihrer Confluence-Instanz herzustellen. Informationen zur Erstellung eines Confluence-API-Tokens findest du unter API-Token für dein Atlassian-Konto verwalten.
- Optional: Konfigurierte OAuth 2.0-Anmeldeinformationen, die einen Confluence-App-Schlüssel, ein Confluence-App-Secret, ein Confluence-Zugriffstoken und ein Confluence-Aktualisierungstoken enthalten, um eine Verbindung zu deiner Confluence-Instanz herzustellen. Amazon Kendra Wenn Ihr Zugriffstoken abläuft, können Sie entweder das Aktualisierungstoken verwenden, um Ihr Zugriffstoken und Ihr Aktualisierungstokenpaar neu zu generieren. Oder Sie können den Autorisierungsvorgang wiederholen. Weitere Informationen zu Zugriffstoken finden Sie unter OAuth-Zugriffstoken verwalten.
- (Nur für Confluence Server) Optional: Es wurde ein Personal Access Token (PAT) konfiguriert, das ein Confluence-Token enthält, um eine Verbindung zu Ihrer Confluence-Instanz Amazon Kendra herzustellen. Informationen zur Erstellung eines PAT-Tokens finden Sie unter Persönliche Zugriffstoken verwenden.

Stellen Sie sicher AWS-Konto, dass Sie in Ihrem haben:

- Hat einen Amazon Kendra Index erstellt und bei Verwendung der API die Index-ID notiert.
- Sie haben eine IAM Rolle für Ihre Datenquelle erstellt und, falls Sie die API verwenden, den ARN der IAM Rolle notiert.

> **Note**
>
> Wenn Sie Ihren Authentifizierungstyp und Ihre Anmeldeinformationen ändern, müssen Sie Ihre IAM Rolle aktualisieren, um auf die richtige AWS Secrets Manager geheime ID zugreifen zu können.

- Du hast deine Confluence-Authentifizierungsdaten AWS Secrets Manager geheim gespeichert und, falls du die API verwendest, den ARN des Secrets notiert.

> **Note**
>
> Wir empfehlen dir, deine Anmeldedaten und dein Secret regelmäßig zu aktualisieren oder zu wechseln. Stellen Sie zu Ihrer eigenen Sicherheit nur die erforderliche Zugriffsebene bereit. Wir raten davon ab, Anmeldeinformationen und geheime Daten für alle Datenquellen und Connector-Versionen 1.0 und 2.0 (sofern zutreffend) wiederzuverwenden.

Wenn du noch keine IAM Rolle oder keinen Schlüssel hast, kannst du die Konsole verwenden, um eine neue IAM Rolle und ein neues Secrets Manager Geheimnis zu erstellen, wenn du deine Confluence-Datenquelle mit verbindest. Amazon Kendra Wenn Sie die API verwenden, müssen Sie den ARN einer vorhandenen IAM Rolle und eines Secrets Manager Geheimnisses sowie eine Index-ID angeben.

Anweisungen zur Verbindung

Um eine Verbindung Amazon Kendra zu Ihrer Confluence-Datenquelle herzustellen, müssen Sie Details zu Ihren Confluence-Anmeldeinformationen angeben, damit Sie auf Ihre Daten zugreifen Amazon Kendra können. Falls Sie Confluence noch nicht konfiguriert haben, finden Sie weitere Informationen unter. Amazon Kendra Voraussetzungen

Console

Um eine Verbindung zu Confluence herzustellen Amazon Kendra

1. Melden Sie sich bei der AWS Management Console an und öffnen Sie die Amazon Kendra Konsole.
2. Wählen Sie im linken Navigationsbereich Indizes und dann den Index, den Sie verwenden möchten, aus der Indexliste aus.

   > **Note**
   >
   > Sie können Ihre Einstellungen für die Benutzerzugriffskontrolle unter Indexeinstellungen konfigurieren oder bearbeiten.

3. Wählen Sie auf der Seite Erste Schritte die Option Datenquelle hinzufügen aus.

4. Wählen Sie auf der Seite Datenquelle hinzufügen die Option Confluence Connector V2.0 und dann Connector hinzufügen aus.
5. Geben Sie auf der Seite „Datenquellendetails angeben“ die folgenden Informationen ein:
   a. Geben Sie im Feld Name und Beschreibung für Datenquellenname einen Namen für Ihre Datenquelle ein. Sie können Bindestriche, aber keine Leerzeichen verwenden.
   b. (Optional) Beschreibung — Geben Sie eine optionale Beschreibung für Ihre Datenquelle ein.
   c. In Standardsprache — Wählen Sie eine Sprache aus, um Ihre Dokumente nach dem Index zu filtern. Sofern Sie nichts anderes angeben, ist die Standardsprache Englisch. Die in den Metadaten des Dokuments angegebene Sprache hat Vorrang vor der ausgewählten Sprache.
   d. Unter Tags für Neues Tag hinzufügen — Fügen Sie optionale Tags hinzu, um Ihre Ressourcen zu durchsuchen und zu filtern oder Ihre Kosten nachzuverfolgen. AWS
   e. Wählen Sie Weiter aus.
6. Geben Sie auf der Seite Zugriff und Sicherheit definieren die folgenden Informationen ein:
   a. Wählen Sie unter Quelle je nach Ihrer Hosting-Methode für Confluence-Datenquellen zwischen Confluence Cloud und Confluence Server.
   b. Confluence-URL — Geben Sie die Confluence-Host-URL ein. *Das Format für die Host-URL, die Sie eingeben, ist https://example.confluence.com.*
   c. (Nur für Confluence Server) Speicherort des SSL-Zertifikats — optional — Geben Sie den Amazon S3 Pfad zu Ihrer SSL-Zertifikatsdatei für Confluence Server ein.
   d. (Nur für Confluence Server) Web-Proxy — optional — Geben Sie den Hostnamen des Web-Proxys (ohne das `http://` `https://` OR-Protokoll) und die Portnummer (Port, der vom Host-URL-Transportprotokoll verwendet wird) ein. Die Portnummer sollte ein numerischer Wert zwischen 0 und 65535 sein.
   e. (Nur für Confluence Server) Autorisierung — Wählen Sie diese Option, um die Access Control List (ACL) zu aktivieren. Wählen Sie dann zwischen Benutzername und E-Mail, um das Feld auszuwählen, das Sie für die Zugriffskontrolle verwenden möchten.
   f. Wählen Sie je nach Anwendungsfall zwischen Standardauthentifizierung, OAuth 2.0-Authentifizierung und (nur für Confluence-Server) Authentifizierung mit Personal Access Token.
   g. AWS Secrets Manager geheim — Wählen Sie ein vorhandenes Geheimnis oder erstellen Sie ein neues Secrets Manager Geheimnis, um Ihre Confluence-Authentifizierungsdaten

zu speichern. Wenn Sie sich dafür entscheiden, ein neues Geheimnis zu erstellen, wird ein AWS Secrets Manager geheimes Fenster geöffnet. Geben Sie die folgenden Informationen in das Fenster ein:

i. Geheimer Name — Ein Name für Ihr Geheimnis. Das Präfix 'AmazonKendra-Confluence-' wird Ihrem geheimen Namen automatisch hinzugefügt.

ii. Wenn Sie die Standardauthentifizierung verwenden — Geben Sie den geheimen Namen, den Benutzernamen und das Passwort (Confluence Server-Passwort) ein, die Sie von Ihrem Confluence-Konto generiert und heruntergeladen haben.

Wenn Sie die OAuth2.0-Authentifizierung verwenden — Geben Sie den geheimen Namen, den App-Schlüssel, den geheimen App-Schlüssel, das Zugriffstoken und das Aktualisierungstoken ein, die Sie in Ihrem Confluence-Konto erstellt haben.

(Nur Confluence-Server) Wenn Sie die Authentifizierung mit dem Personal Access Token verwenden — Geben Sie den geheimen Namen und das Confluence-Token ein, die Sie in Ihrem Confluence-Konto erstellt haben.

iii. Wählen Sie Speichern und Geheimnis hinzufügen.

h. Unter VPC und Sicherheitsgruppe konfigurieren — optional, für Virtual Private Cloud (VPC) — können Sie wählen, ob Sie eine VPC verwenden möchten. In diesem Fall müssen Sie Subnetze und VPC-Sicherheitsgruppen hinzufügen.

i. Identity Crawler — Geben Sie an, ob der Identity Crawler aktiviert Amazon Kendra werden soll. Der Identity Crawler verwendet die Informationen der Zugriffskontrollliste (ACL) für Ihre Dokumente, um Suchergebnisse nach dem Benutzer- oder Gruppenzugriff auf Dokumente zu filtern. Wenn Sie über eine ACL für Ihre Dokumente verfügen und Ihre ACL verwenden möchten, können Sie auch den Identity Crawler aktivieren, um die Benutzerkontextfilterung von Suchergebnissen zu konfigurieren. Amazon Kendra Andernfalls können alle Dokumente öffentlich durchsucht werden, wenn Identity Crawler ausgeschaltet ist. Wenn Sie die Zugriffskontrolle für Ihre Dokumente verwenden möchten und Identity Crawler ausgeschaltet ist, können Sie alternativ die PutPrincipalMappingAPI verwenden, um Benutzer- und Gruppenzugriffsinformationen für die Benutzerkontextfilterung hochzuladen.

j. IAM Rolle — Wählen Sie eine bestehende IAM Rolle oder erstellen Sie eine neue IAM Rolle, um auf Ihre Repository-Anmeldeinformationen und Indexinhalte zuzugreifen.

> **Note**
>
> IAM Rollen, die für Indizes verwendet werden, können nicht für Datenquellen verwendet werden. Wenn Sie sich nicht sicher sind, ob eine vorhandene Rolle für einen Index oder eine häufig gestellte Frage verwendet wird, wählen Sie Neue Rolle erstellen, um Fehler zu vermeiden.

k. Wählen Sie Weiter aus.

7. Geben Sie auf der Seite „Synchronisierungseinstellungen konfigurieren“ die folgenden Informationen ein:

   a. Wählen Sie unter Synchronisierungsbereich für Synchronisierungsinhalte die Synchronisierung aus den folgenden Entitätstypen aus: Seiten, Seitenkommentare, Seitenanhänge, Blogs, Blogkommentare, Bloganhänge, Persönliche Bereiche und Archivierte Bereiche.

   > **Note**
   >
   > Seitenkommentare und Seitenanhänge können nur ausgewählt werden, wenn Sie Seiten synchronisieren möchten. Blogkommentare und Bloganhänge können nur ausgewählt werden, wenn Sie Blogs synchronisieren möchten.

   > **Important**
   >
   > Wenn Sie unter Zusätzliche Konfiguration kein Regex-Muster für die Leertaste angeben, werden standardmäßig alle Seiten und Blogs gecrawlt.

   b. Geben Sie unter Zusätzliche Konfiguration für Spaces-Regex-Muster an, ob bestimmte Leerzeichen in Ihren Index aufgenommen oder ausgeschlossen werden sollen. Verwenden Sie dazu:

   - Leertaste – *Zum Beispiel my-space-123.*

> **Note**
>
> Wenn Sie unter Zusätzliche Konfiguration kein Regex-Muster für die Leertaste angeben, werden standardmäßig alle Seiten und Blogs gecrawlt.

- URL — Zum *Beispiel. *//MySite/MyDocuments*.
- Dateityp — Zum Beispiel .*\ *.pdf, .*\ .txt.*

- Für Maximale Dateigröße — Geben Sie die Dateigrößenbeschränkung in MB an, die Amazon Kendra crawlt. Amazon Kendra crawlt nur die Dateien innerhalb der von Ihnen definierten Größenbeschränkung. Die Standarddateigröße ist 50 MB. Die maximale Dateigröße sollte größer als 0 MB und kleiner oder gleich 50 MB sein.

- Für Regex-Muster für Entitätstitel — Geben Sie Muster für reguläre Ausdrücke an, um bestimmte Blogs, Seiten, Kommentare und Anlagen nach Titeln ein- oder auszuschließen.

> **Note**
>
> Wenn Sie eine bestimmte Seite oder Unterseite crawlen möchten, können Sie Regex-Muster für Seitentitel verwenden, um diese Seite entweder ein- oder auszuschließen.

c. Synchronisierungsmodus — Wählen Sie aus, wie Sie Ihren Index aktualisieren möchten, wenn sich der Inhalt Ihrer Datenquelle ändert. Wenn Sie Ihre Datenquelle Amazon Kendra zum ersten Mal synchronisieren, werden alle Inhalte standardmäßig gecrawlt und indexiert. Sie müssen eine vollständige Synchronisierung Ihrer Daten durchführen, falls Ihre erste Synchronisierung fehlgeschlagen ist, auch wenn Sie die Option Vollsynchronisierung nicht als Synchronisierungsmodusoption wählen.

- Vollständige Synchronisierung: Indizieren Sie alle Inhalte neu und ersetzen vorhandene Inhalte jedes Mal, wenn Ihre Datenquelle mit Ihrem Index synchronisiert wird.
- Neue, geänderte, gelöschte Synchronisierung: Indizieren Sie bei jeder Synchronisierung Ihrer Datenquelle mit Ihrem Index nur neue, geänderte und

gelöschte Inhalte. Amazon Kendra kann den Mechanismus Ihrer Datenquelle verwenden, um Inhaltsänderungen nachzuverfolgen und Inhalte zu indexieren, die sich seit der letzten Synchronisierung geändert haben.

d. Im Synchronisierungslaufplan für Frequenz — Wie oft Amazon Kendra wird mit Ihrer Datenquelle synchronisiert?

e. Wählen Sie Weiter aus.

8. Geben Sie auf der Seite Feldzuordnungen festlegen die folgenden Informationen ein:

a. Für Space, Page, Blog, Comment und Attachment — Wählen Sie aus den Amazon Kendra generierten Standard-Datenquellenfeldern aus, die Sie Ihrem Index zuordnen möchten.

b. Feld hinzufügen — Um benutzerdefinierte Datenquellenfelder hinzuzufügen, um einen Indexfeldnamen für die Zuordnung und den Felddatentyp zu erstellen.

c. Wählen Sie Weiter aus.

9. Überprüfen Sie auf der Seite Überprüfen und erstellen, ob die von Ihnen eingegebenen Informationen korrekt sind, und wählen Sie dann Datenquelle hinzufügen aus. Sie können Ihre Informationen auch auf dieser Seite bearbeiten. Ihre Datenquelle wird auf der Seite Datenquellen angezeigt, nachdem die Datenquelle erfolgreich hinzugefügt wurde.

API

Um eine Verbindung Amazon Kendra zu Confluence herzustellen

Sie müssen mithilfe der API ein JSON des Datenquellenschemas angeben. TemplateConfiguration Sie müssen die folgenden Informationen angeben:

- Datenquelle — Geben Sie den Datenquellentyp wie `CONFLUENCEV2` bei der Verwendung des TemplateConfigurationJSON-Schemas an. Geben Sie außerdem die Datenquelle so an`TEMPLATE`, wie Sie die CreateDataSourceAPI aufrufen.
- Host-URL — Geben Sie die Version der Confluence-Host-Instanz an. *Zum Beispiel `https://example.confluence.com`.*
- Synchronisierungsmodus — Geben Sie an, wie Ihr Index aktualisiert Amazon Kendra werden soll, wenn sich der Inhalt Ihrer Datenquelle ändert. Wenn Sie Ihre Datenquelle Amazon Kendra zum ersten Mal synchronisieren, werden alle Inhalte standardmäßig gecrawlt und indexiert. Sie müssen eine vollständige Synchronisierung Ihrer Daten durchführen, falls Ihre erste

Synchronisierung fehlgeschlagen ist, auch wenn Sie die Option Vollsynchronisierung nicht als Synchronisierungsmodusoption wählen. Sie können wählen zwischen:

- `FORCED_FULL_CRAWL`um den gesamten Inhalt neu zu indizieren und vorhandene Inhalte jedes Mal zu ersetzen, wenn Ihre Datenquelle mit Ihrem Index synchronisiert wird.
- `FULL_CRAWL`um bei jeder Synchronisierung Ihrer Datenquelle mit Ihrem Index nur neue, geänderte und gelöschte Inhalte zu indizieren. Amazon Kendra kann den Mechanismus Ihrer Datenquelle verwenden, um Inhaltsänderungen nachzuverfolgen und Inhalte zu indexieren, die sich seit der letzten Synchronisierung geändert haben.

- Authentifizierungstyp — Geben Sie den Authentifizierungstyp (ob `BasicOAuth2`,) `Personal-token` für Ihre Confluence-Instanz an.
- (Optional — Nur für Confluence Server) Speicherort des SSL-Zertifikats — Geben Sie das Land an, auf dem Sie Ihr SSL-Zertifikat gespeichert haben. `S3bucketName` `s3certificateName`
- Geheimer Amazon-Ressourcenname (ARN) — Geben Sie den Amazon-Ressourcennamen (ARN) eines Secrets Manager Geheimnisses ein, das die Authentifizierungsdaten enthält, die Sie in Ihrem Confluence-Konto erstellt haben. Wenn Sie die grundlegende Kontoauthentifizierung verwenden, wird das Geheimnis in einer JSON-Struktur mit den folgenden Schlüsseln gespeichert:

```
{
    "username": "Confluence account user name",
    "password": "Confluence API token"
}
```

Wenn Sie die OAuth 2.0-Authentifizierung verwenden, wird das Geheimnis in einer JSON-Struktur mit den folgenden Schlüsseln gespeichert:

```
{
    "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"
}
```

(Nur für Confluence Server) Wenn Sie die Standardauthentifizierung verwenden, wird das Geheimnis in einer JSON-Struktur mit den folgenden Schlüsseln gespeichert:

```
{
```

```
    "hostUrl": "Confluence Server host URL",
    "username": "Confluence Server user name",
    "password": "Confluence Server password"
}
```

(Nur für Confluence Server) Wenn Sie die Authentifizierung mit dem Personal Access Token verwenden, wird das Geheimnis in einer JSON-Struktur mit den folgenden Schlüsseln gespeichert:

```
{
    "hostUrl": "Confluence Server host URL",
    "patToken": "Confluence token"
}
```

> **Note**
>
> Wir empfehlen Ihnen, Ihre Anmeldeinformationen und Ihr Geheimnis regelmäßig zu aktualisieren oder zu wechseln. Stellen Sie zu Ihrer eigenen Sicherheit nur die erforderliche Zugriffsebene bereit. Wir raten davon ab, Anmeldeinformationen und geheime Daten für alle Datenquellen und Connector-Versionen 1.0 und 2.0 (sofern zutreffend) wiederzuverwenden.

- IAM role — Geben Sie an`RoleArn`, wann Sie anrufen`CreateDataSource`, um einer IAM Rolle Berechtigungen für den Zugriff auf Ihr Secrets Manager Secret und den Aufruf der erforderlichen öffentlichen APIs für den Confluence-Connector und zum Aufrufen der erforderlichen öffentlichen APIs zu erteilen. Amazon Kendra Weitere Informationen finden Sie unter IAM Rollen für Confluence-Datenquellen.

Sie können auch die folgenden optionalen Funktionen hinzufügen:

- Virtual Private Cloud (VPC) — Geben Sie an, `VpcConfiguration` wann Sie anrufen. `CreateDataSource` Weitere Informationen finden Sie unter Konfigurieren von Amazon Kendra für die Verwendung eines Amazon VPC.
- Inklusions- und Ausschlussfilter — Sie können angeben, ob bestimmte Bereiche, Seiten, Blogs sowie deren Kommentare und Anlagen ein- oder ausgeschlossen werden sollen.

> **Note**
>
> Die meisten Datenquellen verwenden Muster für reguläre Ausdrücke, bei denen es sich um Ein- oder Ausschlussmuster handelt, die als Filter bezeichnet werden. Wenn Sie einen Einschlussfilter angeben, werden nur Inhalte indexiert, die dem Einschlussfilter entsprechen. Jedes Dokument, das nicht dem Einschlussfilter entspricht, wird nicht indexiert. Wenn Sie einen Ein- und Ausschlussfilter angeben, werden Dokumente, die dem Ausschlussfilter entsprechen, nicht indexiert, auch wenn sie dem Einschlussfilter entsprechen.

- Identity Crawler — Geben Sie an, ob der Identity Crawler aktiviert Amazon Kendra werden soll. Der Identity Crawler verwendet die Informationen der Zugriffskontrollliste (ACL) für Ihre Dokumente, um Suchergebnisse nach dem Benutzer- oder Gruppenzugriff auf Dokumente zu filtern. Wenn Sie über eine ACL für Ihre Dokumente verfügen und Ihre ACL verwenden möchten, können Sie auch den Identity Crawler aktivieren, um die Benutzerkontextfilterung von Suchergebnissen zu konfigurieren. Amazon Kendra Andernfalls können alle Dokumente öffentlich durchsucht werden, wenn Identity Crawler ausgeschaltet ist. Wenn Sie die Zugriffskontrolle für Ihre Dokumente verwenden möchten und Identity Crawler ausgeschaltet ist, können Sie alternativ die PutPrincipalMappingAPI verwenden, um Benutzer- und Gruppenzugriffsinformationen für die Benutzerkontextfilterung hochzuladen.
- Feldzuordnungen — Wählen Sie, ob Sie Ihre Confluence-Datenquellenfelder Ihren Indexfeldern zuordnen möchten. Amazon Kendra Weitere Informationen finden Sie unter Zuweisen von Datenquellenfeldern.

> **Note**
>
> Das Textfeld oder das entsprechende Textfeld für Ihre Dokumente ist erforderlich, um Ihre Dokumente durchsuchen zu können. Amazon Kendra Sie müssen den Feldnamen Ihres Dokumenthauptteils in Ihrer Datenquelle dem Namen des Indexfeldes zuordnen`_document_body`. Alle anderen Felder sind optional.

Eine Liste weiterer wichtiger JSON-Schlüssel, die konfiguriert werden müssen, finden Sie unterConfluence-Vorlagenschema.

Hinweise

- Personal Access Token (PAT) ist für Confluence Cloud nicht verfügbar.

Benutzerdefinierter Datenquellen-Konnektor

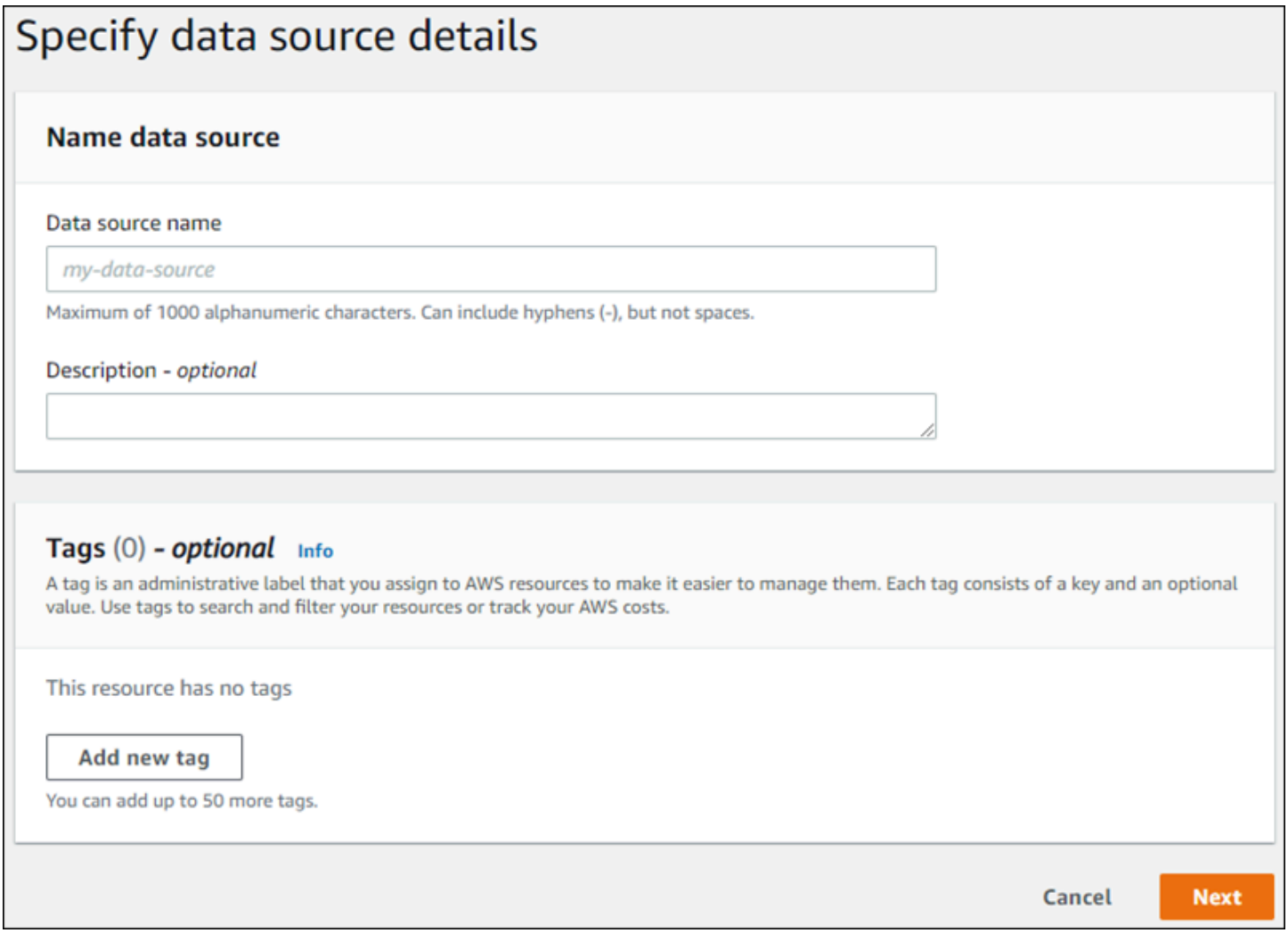
Verwenden Sie eine benutzerdefinierte Datenquelle, wenn Sie über ein Repository verfügen, für das noch Amazon Kendra keinen Datenquellen-Connector bereitstellt. Sie können es verwenden, um dieselben Metriken für den Ausführungsverlauf anzuzeigen, die Amazon Kendra Datenquellen auch dann bereitstellen, wenn Sie die Datenquellen von nicht zum Synchronisieren Ihrer Amazon KendraRepositorys verwenden können. Verwenden Sie dies, um eine konsistente Synchronisierungsüberwachung zwischen Amazon Kendra Datenquellen und benutzerdefinierten zu ermöglichen. Verwenden Sie insbesondere eine benutzerdefinierte Datenquelle, um Synchronisierungsmetriken für einen Datenquellen-Connector anzuzeigen, den Sie mit den BatchDeleteDocument APIs BatchPutDocument und erstellt haben.

Informationen zur Fehlerbehebung Ihres benutzerdefinierten Amazon Kendra-Datenquellen-Konnektors finden Sie unter Problembehandlung bei Datenquellen.

Wenn Sie eine benutzerdefinierte Datenquelle erstellen, haben Sie die vollständige Kontrolle darüber, wie die zu indizierenden Dokumente ausgewählt werden. stellt Amazon Kendra nur Metrikinformationen bereit, mit denen Sie Ihre Datenquellen-Synchronisierungsaufträge überwachen können. Sie müssen den Crawler erstellen und ausführen, der die Dokumente bestimmt, die Ihre Datenquellenindizes enthalten.

Sie müssen den Haupttitel Ihrer Dokumente mithilfe des Dokumentobjekts und angeben, `_source_uri` DocumentAttribute damit `DocumentTitle` und in die Antwort des `Query` Ergebnisses `DocumentURI` aufgenommen werden.

Sie erstellen eine Kennung für Ihre benutzerdefinierte Datenquelle mithilfe der -Konsole oder mithilfe der CreateDataSource-API. Um die Konsole zu verwenden, geben Sie Ihrer Datenquelle einen Namen und optional eine Beschreibung und Ressourcen-Tags. Nachdem die Datenquelle erstellt wurde, wird eine Datenquellen-ID angezeigt. Kopieren Sie diese ID, die Sie verwenden möchten, wenn Sie die Datenquelle mit dem Index synchronisieren.



Sie können eine benutzerdefinierte Datenquelle auch mit der `CreateDataSource`-API erstellen. Die API gibt eine ID zurück, die beim Synchronisieren der Datenquelle verwendet werden soll. Wenn Sie die `CreateDataSource`-API verwenden, um eine benutzerdefinierte Datenquelle zu erstellen, können Sie die `Schedule` Parameter `Configuration`, `RoleArn` oder nicht festlegen. Wenn Sie diese Parameter festlegen, Amazon Kendra gibt eine `ValidationException` Ausnahme zurück.

Um eine benutzerdefinierte Datenquelle zu verwenden, erstellen Sie eine Anwendung, die für die Aktualisierung des Amazon Kendra Index verantwortlich ist. Die Anwendung hängt von einem Crawler ab, den Sie erstellen. Der Crawler liest die Dokumente in Ihrem Repository und bestimmt, welche an gesendet werden sollenAmazon Kendra. Ihre Anwendung sollte die folgenden Schritte ausführen:

1. Crawlen Sie Ihr Repository und erstellen Sie eine Liste der Dokumente in Ihrem Repository, die hinzugefügt, aktualisiert oder gelöscht werden.

2. Rufen Sie die StartDataSourceSyncJob -API auf, um zu signalisieren, dass ein Synchronisierungsauftrag gestartet wird. Sie geben eine Datenquellen-ID an, um die Datenquelle zu identifizieren, die synchronisiert wird. Amazon Kendra gibt eine Ausführungs-ID zurück, um einen bestimmten Synchronisierungsauftrag zu identifizieren.
3. Rufen Sie die BatchDeleteDocument -API auf, um Dokumente aus dem Index zu entfernen. Sie geben die Datenquellen-ID und die Ausführungs-ID an, um die zu synchronisierende Datenquelle und den Auftrag zu identifizieren, dem diese Aktualisierung zugeordnet ist.
4. Rufen Sie die StopDataSourceSyncJob -API auf, um das Ende des Synchronisierungsauftrags zu signalisieren. Nachdem Sie die `StopDataSourceSyncJob` API aufgerufen haben, ist die zugehörige Ausführungs-ID nicht mehr gültig.
5. Rufen Sie die ListDataSourceSyncJobs API mit den Index- und Datenquellenkennungen auf, um die Synchronisierungsaufträge für die Datenquelle aufzulisten und Metriken für die Synchronisierungsaufträge anzuzeigen.

Nachdem Sie einen Synchronisierungsauftrag beendet haben, können Sie einen neuen Synchronisierungsauftrag starten. Es kann einen gewissen Zeitraum geben, bis alle übermittelten Dokumente zum Index hinzugefügt werden. Verwenden Sie die `ListDataSourceSyncJobs` API, um den Status des Synchronisierungsauftrags anzuzeigen. Wenn der für den Synchronisierungsauftrag `Status` zurückgegebene lautet`SYNCING_INDEXING`, werden einige Dokumente immer noch indiziert. Sie können einen neuen Synchronisierungsauftrag starten, wenn der Status des vorherigen Auftrags `FAILED` oder lautet`SUCCEEDED`.

Nachdem Sie die `StopDataSourceSyncJob` -API aufgerufen haben, können Sie in einem Aufruf der - `BatchPutDocument` oder -`BatchDeleteDocument`APIs keine Synchronisierungsauftragskennung verwenden. APIs Wenn Sie dies tun, werden alle übermittelten Dokumente in der `FailedDocuments` Antwortnachricht der API zurückgegeben.

Erforderliche Attribute

Wenn Sie ein Dokument Amazon Kendra mithilfe der `BatchPutDocument`-API an senden, benötigt jedes Dokument zwei Attribute, um die Datenquelle und den Synchronisationslauf zu identifizieren, zu dem es gehört. Sie müssen die folgenden beiden Attribute angeben, um Dokumente aus Ihrer benutzerdefinierten Datenquelle korrekt einem Amazon Kendra Index zuzuordnen:

- `_data_source_id`– Die Kennung der Datenquelle. Dies wird zurückgegeben, wenn Sie die Datenquelle mit der Konsole oder der `CreateDataSource` API erstellen.

- `_data_source_sync_job_execution_id`– Die ID der Synchronisierungsausführung. Dies wird zurückgegeben, wenn Sie die Indexsynchronisierung mit der `StartDataSourceSyncJob` API starten.

Im Folgenden finden Sie den erforderlichen JSON-Code, um ein Dokument mithilfe einer benutzerdefinierten Datenquelle zu indizieren.

```
{
    "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"
}
```

Wenn Sie mithilfe der `BatchDeleteDocument` API ein Dokument aus dem Index entfernen, müssen Sie die folgenden beiden Felder im `DataSourceSyncJobMetricTarget` Parameter angeben:

- `DataSourceId`– Die Kennung der Datenquelle. Dies wird zurückgegeben, wenn Sie die Datenquelle mit der Konsole oder der `CreateDataSource` API erstellen.
- `DataSourceSyncJobId`– Die ID der Synchronisierungsausführung. Dies wird zurückgegeben, wenn Sie die Indexsynchronisierung mit der `StartDataSourceSyncJob` API starten.

Im Folgenden finden Sie den erforderlichen JSON-Code, um ein Dokument mithilfe der `BatchDeleteDocument` API aus dem Index zu löschen.

```
{
    "DataSourceSyncJobMetricTarget": {
        "DataSourceId": "data source identifier",
        "DataSourceSyncJobId": "sync job identifier"
    },
    "DocumentIdList": [
        "document identifier"
    ],
    "IndexId": "index identifier"
}
```

Anzeigen von -Metriken

Nachdem ein Synchronisierungsauftrag abgeschlossen ist, können Sie die DataSourceSyncJobMetrics-API verwenden, um die dem Synchronisierungsauftrag zugeordneten Metriken abzurufen. Verwenden Sie dies, um Ihre benutzerdefinierten Datenquellensynchronisierungen zu überwachen.

Wenn Sie dasselbe Dokument mehrmals einreichen, entweder als Teil der `BatchPutDocument` API, der `BatchDeleteDocument` API oder wenn das Dokument sowohl zum Hinzufügen als auch zum Löschen eingereicht wird, wird das Dokument nur einmal in den Metriken gezählt.

- `DocumentsAdded`– Die Anzahl der Dokumente, die mit der diesem Synchronisierungsauftrag zugeordneten `BatchPutDocument` API zum ersten Mal zum Index hinzugefügt wurden. Wenn ein Dokument mehr als einmal in einer Synchronisierung zur Ergänzung eingereicht wird, wird das Dokument nur einmal in den Metriken gezählt.
- `DocumentsDeleted`– Die Anzahl der Dokumente, die mit der `BatchDeleteDocument` API übermittelt wurden, die diesem Synchronisierungsauftrag zugeordnet ist, wurde aus dem Index gelöscht. Wenn ein Dokument mehr als einmal in einer Synchronisierung zum Löschen eingereicht wird, wird das Dokument nur einmal in den Metriken gezählt.
- `DocumentsFailed`– Die Anzahl der Dokumente, die mit diesem Synchronisierungsauftrag verknüpft sind und bei denen die Indizierung fehlgeschlagen ist. Dies sind Dokumente, die von Amazon Kendra für die Indizierung akzeptiert wurden, aber nicht indiziert oder gelöscht werden konnten. Wenn ein Dokument von nicht akzeptiert wirdAmazon Kendra, wird die Kennung für das Dokument in der `FailedDocuments` Antworteigenschaft der `BatchDeleteDocument` APIs `BatchPutDocument` und zurückgegeben.

- `DocumentsModified`– Die Anzahl der geänderten Dokumente, die mit der `BatchPutDocument` API übermittelt wurden, die diesem Synchronisierungsauftrag zugeordnet ist und im Amazon Kendra Index geändert wurden.

Amazon Kendra gibt bei der Indizierung von Dokumenten auch Amazon CloudWatch Metriken aus. Weitere Informationen finden Sie unter Überwachung Amazon Kendra mit Amazon CloudWatch.

Amazon Kendra gibt die Metrik `DocumentsScanned` für benutzerdefinierte Datenquellen nicht zurück. Es gibt auch die Metriken aus, die im Dokument Metriken für Datenquellen CloudWatch aufgeführt sind. Amazon Kendra

Weitere Informationen

Weitere Informationen zur Integration Amazon Kendra in Ihre benutzerdefinierte Datenquelle finden Sie unter:

- Hinzufügen benutzerdefinierter Datenquellen zu Amazon Kendra

Benutzerdefinierte Datenquelle (Java)

Der folgende Code bietet eine Beispielimplementierung einer benutzerdefinierten Datenquelle mit Java. Das Programm erstellt zunächst eine benutzerdefinierte Datenquelle und synchronisiert dann neu hinzugefügte Dokumente mit dem Index mit der benutzerdefinierten Datenquelle.

Der folgende Code veranschaulicht das Erstellen und Verwenden einer benutzerdefinierten Datenquelle. Wenn Sie eine benutzerdefinierte Datenquelle in Ihrer Anwendung verwenden, müssen Sie nicht jedes Mal, wenn Sie Ihren Index mit Ihrer Datenquelle synchronisieren, eine neue Datenquelle (einmaliger Prozess) erstellen. Sie verwenden die Index-ID und die Datenquellen-ID, um Ihre Daten zu synchronisieren.

```
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 ist ein Datei-Hosting-Dienst, der Cloud-Speicher, Dokumentenorganisation und Dokumentenvorlagen anbietet. Wenn Sie ein Dropbox-Nutzer sind, können Sie Amazon Kendra damit Ihre Dropbox-Dateien, Dropbox Paper, Dropbox Paper-Vorlagen und gespeicherte Verknüpfungen zu Webseiten indexieren. Sie können auch so konfigurieren Amazon Kendra , dass bestimmte Dropbox-Dateien, Dropbox Paper, Dropbox Paper-Vorlagen und gespeicherte Verknüpfungen zu Webseiten indexiert werden.

Amazon Kendra unterstützt sowohl Dropbox als auch Dropbox Advanced für Dropbox Business.

Sie können über Amazon Kendra die Amazon Kendra Konsole und die TemplateConfigurationAPI eine Verbindung zu Ihrer Dropbox-Datenquelle herstellen.

Informationen zur Fehlerbehebung bei Ihrem Amazon Kendra Dropbox-Datenquellen-Connector finden Sie unterProblembehandlung bei Datenquellen.

Themen

- Unterstützte Features
- Voraussetzungen
- Anweisungen zur Verbindung
- Weitere Informationen

Unterstützte Features

Amazon Kendra Der Dropbox-Datenquellen-Connector unterstützt die folgenden Funktionen:

- Änderungsprotokoll
- Feldzuordnungen
- Filterung des Benutzerkontextes
- Einschluss-/Ausschlussfilter
- Virtual Private Cloud (VPC)

Voraussetzungen

Bevor Sie Ihre Dropbox-Datenquelle Amazon Kendra zum Indizieren verwenden können, müssen Sie diese Änderungen in Ihrer Dropbox und Ihren Konten vornehmen. AWS

Stellen Sie in Dropbox sicher, dass Sie über Folgendes verfügen:

- Sie haben ein Dropbox Advanced-Konto erstellt und einen Admin-Benutzer eingerichtet.
- Hat eine Dropbox-App mit einem eindeutigen App-Namen erstellt und Scoped Access aktiviert. Informationen zum Erstellen einer App finden Sie in der Dropbox-Dokumentation.
- Die vollständigen Dropbox-Berechtigungen wurden auf der Dropbox-Konsole aktiviert und die folgenden Berechtigungen hinzugefügt:
  - files.content.read
  - files.metadata.read
  - teilen.lesen
  - Dateianforderungen.lesen
  - gruppen.lesen
  - team_info.lesen
  - team_data.content.read
- Sie haben Ihren Dropbox-App-Schlüssel, den geheimen Dropbox-App-Schlüssel und das Dropbox-Zugriffstoken für die Basisauthentifizierung zur Kenntnis genommen.
- Es wurde ein temporäres OAuth 2.0-Zugriffstoken für Ihre Dropbox-App generiert und kopiert. Dieses Token ist temporär und läuft nach 4 Stunden ab. Weitere Informationen zur OAuth-Authentifizierung finden Sie in der Dropbox-Dokumentation.

> **Note**
>
> Es wird empfohlen, ein Dropbox-Zugriffstoken für die Aktualisierung zu erstellen, das nie abläuft, anstatt sich auf ein einmaliges Zugriffstoken zu verlassen, das nach 4 Stunden

abläuft. Ein Aktualisierungszugriffstoken ist permanent und läuft nie ab, sodass Sie Ihre Datenquelle auch in future synchronisieren können.

- Empfehlung: Es wurde ein permanentes Dropbox-Aktualisierungstoken konfiguriert, das nie abläuft, damit Amazon Kendra Sie Ihre Datenquelle weiterhin ohne Unterbrechungen synchronisieren können. Informationen zu Aktualisierungstoken finden Sie in der Dropbox-Dokumentation.
- Aktiviert, dass jedes Dokument in Dropbox und in anderen Datenquellen, die Sie für denselben Index verwenden möchten, einzigartig ist. Jede Datenquelle, die Sie für einen Index verwenden möchten, darf nicht dasselbe Dokument in allen Datenquellen enthalten. Dokument-IDs gelten für einen Index global und müssen pro Index eindeutig sein.

Stellen Sie sicher AWS-Konto, dass Sie Folgendes in Ihrem haben:

- Hat einen Amazon Kendra Index erstellt und bei Verwendung der API die Index-ID notiert.
- Sie haben eine IAM Rolle für Ihre Datenquelle erstellt und, falls Sie die API verwenden, den ARN der IAM Rolle notiert.

> **Note**
>
> Wenn Sie Ihren Authentifizierungstyp und Ihre Anmeldeinformationen ändern, müssen Sie Ihre IAM Rolle aktualisieren, um auf die richtige AWS Secrets Manager geheime ID zugreifen zu können.

- Haben Ihre Dropbox-Authentifizierungsdaten AWS Secrets Manager geheim gespeichert und, falls Sie die API verwenden, den ARN des Geheimnisses notiert.

> **Note**
>
> Wir empfehlen Ihnen, Ihre Anmeldedaten und Ihr Passwort regelmäßig zu aktualisieren oder zu wechseln. Stellen Sie zu Ihrer eigenen Sicherheit nur die Zugriffsebene bereit, die erforderlich ist. Wir raten davon ab, Anmeldeinformationen und geheime Daten für alle Datenquellen und Connector-Versionen 1.0 und 2.0 (sofern zutreffend) wiederzuverwenden.

Wenn Sie noch keine IAM Rolle oder keinen Schlüssel haben, können Sie die Konsole verwenden, um eine neue IAM Rolle und ein neues Secrets Manager Geheimnis zu erstellen, wenn Sie Ihre

Dropbox-Datenquelle mit verbinden. Amazon Kendra Wenn Sie die API verwenden, müssen Sie den ARN einer vorhandenen IAM Rolle und eines Secrets Manager Geheimnisses sowie eine Index-ID angeben.

Anweisungen zur Verbindung

Um eine Verbindung Amazon Kendra zu Ihrer Dropbox-Datenquelle herzustellen, müssen Sie die erforderlichen Details zu Ihrer Dropbox-Datenquelle angeben, damit Sie auf Ihre Daten zugreifen Amazon Kendra können. Falls Sie Dropbox noch nicht für konfiguriert haben Amazon Kendra, finden Sie weitere Informationen unterVoraussetzungen.

Console

So stellen Sie eine Verbindung Amazon Kendra zu Dropbox her

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die Amazon Kendra Konsole.
2. Wählen Sie im linken Navigationsbereich Indizes und dann den Index, den Sie verwenden möchten, aus der Indexliste aus.

   > **Note**
   >
   > Sie können Ihre Einstellungen für die Benutzerzugriffskontrolle unter Indexeinstellungen konfigurieren oder bearbeiten.

3. Wählen Sie auf der Seite Erste Schritte die Option Datenquelle hinzufügen aus.
4. Wählen Sie auf der Seite Datenquelle hinzufügen die Option Dropbox-Connector und dann Connector hinzufügen aus.
5. Geben Sie auf der Seite „Datenquellendetails angeben“ die folgenden Informationen ein:

   a. Geben Sie im Feld Name und Beschreibung für Datenquellenname einen Namen für Ihre Datenquelle ein. Sie können Bindestriche, aber keine Leerzeichen verwenden.

   b. (Optional) Beschreibung — Geben Sie eine optionale Beschreibung für Ihre Datenquelle ein.

   c. In Standardsprache — Wählen Sie eine Sprache aus, um Ihre Dokumente nach dem Index zu filtern. Sofern Sie nichts anderes angeben, ist die Standardsprache Englisch. Die in den Metadaten des Dokuments angegebene Sprache hat Vorrang vor der ausgewählten Sprache.

d. Unter Tags für Neues Tag hinzufügen — Fügen Sie optionale Tags hinzu, um Ihre Ressourcen zu durchsuchen und zu filtern oder Ihre Kosten nachzuverfolgen. AWS

e. Wählen Sie Weiter aus.

6. Geben Sie auf der Seite Zugriff und Sicherheit definieren die folgenden Informationen ein:

   a. Art des Authentifizierungstokens — Wählen Sie je nach Anwendungsfall zwischen Permanent Token (empfohlen) und Access Token (temporäre Verwendung).

   b. AWS Secrets Manager geheim — Wählen Sie ein vorhandenes Geheimnis oder erstellen Sie ein neues Secrets Manager Geheimnis, um Ihre Dropbox-Authentifizierungsdaten zu speichern. Wenn Sie sich dafür entscheiden, ein neues Geheimnis zu erstellen, wird ein AWS Secrets Manager geheimes Fenster geöffnet.

      i. Geben Sie die folgenden Informationen in das Fenster Create an AWS Secrets Manager Secret ein:

         A. Geheimer Name — Ein Name für Ihr Geheimnis. Das Präfix 'AmazonKendra-Dropbox' wird automatisch zu Ihrem geheimen Namen hinzugefügt.

         B. Für Informationen zum App-Schlüssel, zum geheimen App-Schlüssel und zum Token (permanent oder temporär): Geben Sie die Werte der Authentifizierungsdaten ein, die Sie mit Ihrem Dropbox-Konto generiert haben.

      ii. Wählen Sie Speichern.

   c. Virtual Private Cloud (VPC) — Sie können wählen, ob Sie eine VPC verwenden möchten. In diesem Fall müssen Sie Subnetze und VPC-Sicherheitsgruppen hinzufügen.

   d. IAM Rolle — Wählen Sie eine bestehende IAM Rolle oder erstellen Sie eine neue IAM Rolle, um auf Ihre Repository-Anmeldeinformationen und Indexinhalte zuzugreifen.

      > **Note**
      >
      > IAM Rollen, die für Indizes verwendet werden, können nicht für Datenquellen verwendet werden. Wenn Sie sich nicht sicher sind, ob eine vorhandene Rolle für einen Index oder eine häufig gestellte Frage verwendet wird, wählen Sie Neue Rolle erstellen, um Fehler zu vermeiden.

   e. Wählen Sie Weiter aus.

7. Geben Sie auf der Seite „Synchronisierungseinstellungen konfigurieren“ die folgenden Informationen ein:

a. Für Entitäten oder Inhaltstypen auswählen — Wählen Sie Entitäten oder Inhaltstypen aus, die Sie crawlen möchten.

b. Protokollmodus ändern — Wählen Sie, ob Sie Ihren Index nur mit neuen und geänderten Inhalten aktualisieren möchten, anstatt alle Dateien zu synchronisieren.

c. In Zusätzliche Konfiguration für Regex-Muster — Fügen Sie Muster für reguläre Ausdrücke hinzu, um bestimmte Dateien ein- oder auszuschließen.

d. Wählen Sie im Zeitplan für die Synchronisierungsausführung unter Frequenz aus, wie oft mit Ihrer Amazon Kendra Datenquelle synchronisiert werden soll.

e. Wählen Sie Weiter aus.

8. Geben Sie auf der Seite Feldzuordnungen festlegen die folgenden Informationen ein:

a. Vorlagen für Dateien, Dropbox Paper und Dropbox Paper — Wählen Sie aus den Amazon Kendra generierten Standard-Datenquellenfeldern, die Sie Ihrem Index zuordnen möchten.

b. Feld hinzufügen — Um benutzerdefinierte Datenquellenfelder hinzuzufügen, um einen Indexfeldnamen für die Zuordnung und den Felddatentyp zu erstellen.

c. Wählen Sie Weiter aus.

9. Überprüfen Sie auf der Seite Überprüfen und erstellen, ob die von Ihnen eingegebenen Informationen korrekt sind, und wählen Sie dann Datenquelle hinzufügen aus. Sie können Ihre Informationen auch auf dieser Seite bearbeiten. Ihre Datenquelle wird auf der Seite Datenquellen angezeigt, nachdem die Datenquelle erfolgreich hinzugefügt wurde.

API

Um eine Verbindung Amazon Kendra zu Dropbox herzustellen

Sie müssen mithilfe der TemplateConfigurationAPI einen JSON-Wert des Datenquellenschemas angeben. Sie müssen die folgenden Informationen angeben:

- Datenquelle — Geben Sie den Datenquellentyp wie `DROPBOX` bei der Verwendung des TemplateConfigurationJSON-Schemas an. Geben Sie außerdem die Datenquelle so an`TEMPLATE`, wie Sie die CreateDataSourceAPI aufrufen.
- Änderungsprotokoll — Gibt an, ob der Dropbox-Mechanismus für das Änderungsprotokoll der Datenquelle verwendet werden Amazon Kendra soll, um festzustellen, ob ein Dokument im Index aktualisiert werden muss.

> **Note**
>
> Verwenden Sie das Änderungsprotokoll, wenn Sie nicht alle Dokumente scannen Amazon Kendra möchten. Wenn Ihr Änderungsprotokoll umfangreich ist, nimmt das Scannen der Dokumente in der Dropbox-Datenquelle möglicherweise Amazon Kendra weniger Zeit in Anspruch als das Verarbeiten des Änderungsprotokolls. Wenn Sie Ihre Dropbox-Datenquelle zum ersten Mal mit Ihrem Index synchronisieren, werden alle Dokumente gescannt.

- Geheimer Amazon-Ressourcenname (ARN) — Geben Sie den Amazon-Ressourcennamen (ARN) eines Secrets Manager Geheimnisses ein, das die Authentifizierungsdaten für Ihr Dropbox-Konto enthält. Das Geheimnis wird in einer JSON-Struktur mit den folgenden Schlüsseln gespeichert:

```
{
    "appKey": "Dropbox app key",
    "appSecret": "Dropbox app secret",
    "accesstoken": "temporary access token or refresh access token"
}
```

> **Note**
>
> Wir empfehlen Ihnen, Ihre Anmeldeinformationen und Ihr Geheimnis regelmäßig zu aktualisieren oder zu wechseln. Stellen Sie zu Ihrer eigenen Sicherheit nur die Zugriffsebene bereit, die erforderlich ist. Wir raten davon ab, Anmeldeinformationen und geheime Daten für alle Datenquellen und Connector-Versionen 1.0 und 2.0 (sofern zutreffend) wiederzuverwenden.

- IAM Rolle — Geben Sie an`RoleArn`, wann Sie anrufen`CreateDataSource`, um einer IAM Rolle Berechtigungen für den Zugriff auf Ihr Secrets Manager Geheimnis und den Aufruf der erforderlichen öffentlichen APIs für den Dropbox-Connector und zum Aufrufen der erforderlichen öffentlichen APIs zu erteilen. Amazon Kendra Weitere Informationen finden Sie unter IAM Rollen für Dropbox-Datenquellen.

Sie können auch die folgenden optionalen Funktionen hinzufügen:

- Virtual Private Cloud (VPC) — Geben Sie an, `VpcConfiguration` wann Sie anrufen. `CreateDataSource` Weitere Informationen finden Sie unter Konfigurieren von Amazon Kendra für die Verwendung eines Amazon VPC.
- Inklusions- und Ausschlussfilter — Geben Sie an, ob bestimmte Dateien ein- oder ausgeschlossen werden sollen.

  > **Note**
  >
  > Die meisten Datenquellen verwenden Muster mit regulären Ausdrücken, bei denen es sich um Ein- oder Ausschlussmuster handelt, die als Filter bezeichnet werden. Wenn Sie einen Einschlussfilter angeben, werden nur Inhalte indexiert, die dem Einschlussfilter entsprechen. Jedes Dokument, das nicht dem Einschlussfilter entspricht, wird nicht indexiert. Wenn Sie einen Ein- und Ausschlussfilter angeben, werden Dokumente, die dem Ausschlussfilter entsprechen, nicht indexiert, auch wenn sie dem Einschlussfilter entsprechen.

- Benutzerkontextfilterung und Zugriffskontrolle —Amazon Kendra durchsucht die Zugriffskontrollliste (ACL) für Ihre Dokumente, sofern Sie über eine ACL für Ihre Dokumente verfügen. Die ACL-Informationen werden verwendet, um Suchergebnisse nach dem Benutzer- oder Gruppenzugriff auf Dokumente zu filtern. Weitere Informationen finden Sie unter Benutzerkontextfilterung.
- Feldzuordnungen — Wählen Sie, ob Sie Ihre Dropbox-Datenquellenfelder Ihren Amazon Kendra Indexfeldern zuordnen möchten. Weitere Informationen finden Sie unter Zuweisen von Datenquellenfeldern.

  > **Note**
  >
  > Das Textfeld oder das entsprechende Textfeld für Ihre Dokumente ist erforderlich, um Ihre Dokumente durchsuchen Amazon Kendra zu können. Sie müssen den Feldnamen Ihres Dokumenthauptteils in Ihrer Datenquelle dem Namen des Indexfeldes zuordnen`_document_body`. Alle anderen Felder sind optional.

Eine Liste weiterer wichtiger JSON-Schlüssel, die konfiguriert werden müssen, finden Sie unterDropbox-Vorlagenschema.

Weitere Informationen

Weitere Informationen zur Integration von Amazon Kendra in Ihre Dropbox-Datenquelle finden Sie unter:

- Indizieren Sie Ihre Dropbox-Inhalte mithilfe des Dropbox-Connectors für Amazon Kendra

Drupal

Drupal ist ein Open-Source-Content-Management-System (CMS), mit dem Sie Websites und Webanwendungen erstellen können. Sie können Folgendes verwenden Amazon Kendra , um in Drupal Folgendes zu indizieren:

- Inhalt — Artikel, Standardseiten, Basisblöcke, Benutzerdefinierte Inhaltstypen, Benutzerdefinierte Blocktypen, Benutzerdefinierte Inhaltstypen, Benutzerdefinierte Blocktypen
- Kommentar — Für jeden Inhaltstyp und Blocktyp
- Anlagen — Für jeden Inhaltstyp und Blocktyp

Sie können über Amazon Kendra die Amazon Kendra Konsole oder die API eine Verbindung zu Ihrer Drupal-Datenquelle herstellen. TemplateConfiguration

Informationen zur Fehlerbehebung bei Ihrem Amazon Kendra Drupal-Datenquellen-Connector finden Sie unter. Problembehandlung bei Datenquellen

Themen

- Unterstützte Features
- Voraussetzungen
- Anweisungen zur Verbindung
- Hinweise

Unterstützte Features

Amazon Kendra Der Drupal-Datenquellen-Connector unterstützt die folgenden Funktionen:

- Feldzuordnungen
- Filterung des Benutzerkontextes

- Einschluss-/Ausschlussfilter
- Vollständige und inkrementelle Inhaltssynchronisierung
- Virtual Private Cloud (VPC)

Voraussetzungen

Bevor Sie Ihre Drupal-Datenquelle Amazon Kendra zum Indizieren verwenden können, nehmen Sie diese Änderungen in Ihrem Drupal und Ihren Konten vor. AWS

Stellen Sie in Drupal sicher, dass Sie:

- Sie haben ein Drupal (Standard) Suite-Konto und einen Benutzer mit Administratorrolle erstellt.
- Der Name Ihrer Drupal-Site wurde kopiert und eine Host-URL konfiguriert. <drupalsitename>Zum Beispiel *https:///*<hostname>.
- Konfigurierte Basisauthentifizierungsdaten, die einen Benutzernamen (Anmeldename für die Drupal-Website) und ein Passwort (Drupal-Website-Passwort) enthalten.
- Empfohlen: Es wurde ein OAuth 2.0-Anmeldeinformationstoken konfiguriert. Verwenden Sie dieses Token zusammen mit Ihrem Drupal-Passwort, Ihrer Client-ID, Ihrem Kundengeheimnis, Ihrem Benutzernamen (Login-Benutzername für die Drupal-Website) und Ihrem Passwort (Drupal-Website-Passwort), um eine Verbindung herzustellen. Amazon Kendra
- Mit einer Administratorrolle wurden Ihrem Drupal-Konto die folgenden Berechtigungen hinzugefügt:
  - Blöcke verwalten
  - block_content-Anzeige verwalten
  - block_content-Felder verwalten
  - die Block_Content-Formularanzeige verwalten
  - Ansichten verwalten
  - E-Mail-Adressen von Benutzern anzeigen
  - eigene unveröffentlichte Inhalte anzeigen
  - Seitenrevisionen ansehen
  - Artikelüberarbeitungen anzeigen
  - alle Überarbeitungen ansehen
  - das Administrationsdesign ansehen
  - auf Inhalte zugreifen

- auf die Inhaltsübersicht zugreifen
- auf Kommentare zugreifen
- Inhalt suchen
- Übersicht über Dateien aufrufen
- auf kontextbezogene Links zugreifen

> **Note**
>
> Wenn es benutzerdefinierte Inhaltstypen oder benutzerdefinierte Blocktypen gibt oder Ansichten und Blöcke zur Drupal-Website hinzugefügt werden, müssen diese mit Administratorzugriff ausgestattet werden.

Stellen Sie sicher AWS-Konto, dass Sie in Ihrem haben:

- Hat einen Amazon Kendra Index erstellt und bei Verwendung der API die Index-ID notiert.
- Sie haben eine IAM Rolle für Ihre Datenquelle erstellt und, falls Sie die API verwenden, den ARN der IAM Rolle notiert.

> **Note**
>
> Wenn Sie Ihren Authentifizierungstyp und Ihre Anmeldeinformationen ändern, müssen Sie Ihre IAM Rolle aktualisieren, um auf die richtige AWS Secrets Manager geheime ID zugreifen zu können.

- Haben Ihre Drupal-Authentifizierungsdaten AWS Secrets Manager geheim gespeichert und, falls Sie die API verwenden, den ARN des Geheimnisses notiert.

> **Note**
>
> Wir empfehlen Ihnen, Ihre Anmeldeinformationen und Ihr Geheimnis regelmäßig zu aktualisieren oder zu wechseln. Stellen Sie zu Ihrer eigenen Sicherheit nur die Zugriffsebene bereit, die erforderlich ist. Wir raten davon ab, Anmeldeinformationen und geheime Daten für alle Datenquellen und Connector-Versionen 1.0 und 2.0 (sofern zutreffend) wiederzuverwenden.

Wenn Sie noch keine IAM Rolle oder keinen Schlüssel haben, können Sie die Konsole verwenden, um eine neue IAM Rolle und ein neues Secrets Manager Geheimnis zu erstellen, wenn Sie Ihre Drupal-Datenquelle mit verbinden. Amazon Kendra Wenn Sie die API verwenden, müssen Sie den ARN einer vorhandenen IAM Rolle und eines Secrets Manager Geheimnisses sowie eine Index-ID angeben.

Anweisungen zur Verbindung

Um eine Verbindung Amazon Kendra zu Ihrer Drupal-Datenquelle herzustellen, müssen Sie Details zu Ihren Drupal-Anmeldeinformationen angeben, damit Sie auf Ihre Daten zugreifen Amazon Kendra können. Wenn Sie Drupal noch nicht konfiguriert haben, finden Sie weitere Informationen. Amazon Kendra Voraussetzungen

Console

Um eine Verbindung zu Amazon Kendra Drupal herzustellen

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die Amazon Kendra Konsole.
2. Wählen Sie im linken Navigationsbereich Indizes und dann den Index, den Sie verwenden möchten, aus der Indexliste aus.

   > **Note**
   >
   > Sie können Ihre Einstellungen für die Benutzerzugriffskontrolle unter Indexeinstellungen konfigurieren oder bearbeiten.

3. Wählen Sie auf der Seite Erste Schritte die Option Datenquelle hinzufügen aus.
4. Wählen Sie auf der Seite Datenquelle hinzufügen die Option Drupal-Konnektor und dann Konnektor hinzufügen aus.
5. Geben Sie auf der Seite „Datenquellendetails angeben“ die folgenden Informationen ein:

   a. Geben Sie im Feld Name und Beschreibung für Datenquellenname einen Namen für Ihre Datenquelle ein. Sie können Bindestriche, aber keine Leerzeichen verwenden.

   b. (Optional) Beschreibung — Geben Sie eine optionale Beschreibung für Ihre Datenquelle ein.

   c. In Standardsprache — Wählen Sie eine Sprache aus, um Ihre Dokumente nach dem Index zu filtern. Sofern Sie nichts anderes angeben, ist die Standardsprache Englisch.

Die in den Metadaten des Dokuments angegebene Sprache hat Vorrang vor der ausgewählten Sprache.

d. Unter Tags für Neues Tag hinzufügen — Fügen Sie optionale Tags hinzu, um Ihre Ressourcen zu durchsuchen und zu filtern oder Ihre Kosten nachzuverfolgen. AWS

e. Wählen Sie Weiter aus.

6. Geben Sie auf der Seite Zugriff und Sicherheit definieren die folgenden Informationen ein:

a. Im Feld Quelle für Host-URL — Die Host-URL Ihrer Drupal-Site. <drupalsitename>Zum Beispiel *https:///*<hostname>.

b. Für den Speicherort des SSL-Zertifikats — Geben Sie den Pfad zu dem in Ihrem Amazon S3 Bucket gespeicherten SSL-Zertifikat ein.

c. Autorisierung — Aktivieren oder deaktivieren Sie die Informationen der Zugriffskontrollliste (ACL) für Ihre Dokumente, wenn Sie über eine ACL verfügen und diese für die Zugriffskontrolle verwenden möchten. Die ACL gibt an, auf welche Dokumente Benutzer und Gruppen zugreifen können. Die ACL-Informationen werden verwendet, um Suchergebnisse nach dem Benutzer- oder Gruppenzugriff auf Dokumente zu filtern. Weitere Informationen finden Sie unter Benutzerkontextfilterung.

d. Für Authentifizierung — Wählen Sie je nach Anwendungsfall zwischen Standardauthentifizierung und OAuth 2.0-Authentifizierung.

e. AWS Secrets Manager geheim — Wählen Sie ein vorhandenes Geheimnis oder erstellen Sie ein neues Secrets Manager Geheimnis, um Ihre Drupal-Authentifizierungsdaten zu speichern. Wenn Sie ein neues Geheimnis erstellen möchten, wird ein AWS Secrets Manager geheimes Fenster geöffnet.

i. Geben Sie die folgenden Informationen in das Fenster Create an AWS Secrets Manager Secret ein:

A. Wenn Sie die Standardauthentifizierung gewählt haben, geben Sie einen geheimen Namen, den Benutzernamen (Drupal-Site-Benutzername) und das Passwort (Drupal-Site-Passwort) ein, die Sie kopiert haben, und wählen Sie Speichern und Geheimnis hinzufügen.

B. Wenn Sie sich für die OAuth 2.0-Authentifizierung entschieden haben, geben Sie einen geheimen Namen, einen Benutzernamen (Drupal-Site-Benutzername), ein Passwort (Drupal-Site-Passwort), eine Client-ID und einen geheimen Client-Schlüssel ein, die in Ihrem Drupal-Konto generiert wurden, und wählen Sie Speichern und Geheimnis hinzufügen.

ii. Wählen Sie Speichern.

f. Virtual Private Cloud (VPC) — Sie können wählen, ob Sie eine VPC verwenden möchten. In diesem Fall müssen Sie Subnetze und VPC-Sicherheitsgruppen hinzufügen.

g. Identity Crawler — Geben Sie an, ob der Identity Crawler aktiviert Amazon Kendra werden soll. Der Identity Crawler verwendet die Informationen der Zugriffskontrollliste (ACL) für Ihre Dokumente, um Suchergebnisse nach dem Benutzer- oder Gruppenzugriff auf Dokumente zu filtern. Wenn Sie über eine ACL für Ihre Dokumente verfügen und Ihre ACL verwenden möchten, können Sie auch den Identity Crawler aktivieren, um die Benutzerkontextfilterung von Suchergebnissen zu konfigurieren. Amazon Kendra Andernfalls können alle Dokumente öffentlich durchsucht werden, wenn Identity Crawler ausgeschaltet ist. Wenn Sie die Zugriffskontrolle für Ihre Dokumente verwenden möchten und Identity Crawler ausgeschaltet ist, können Sie alternativ die PutPrincipalMappingAPI verwenden, um Benutzer- und Gruppenzugriffsinformationen für die Benutzerkontextfilterung hochzuladen.

h. IAM Rolle — Wählen Sie eine bestehende IAM Rolle oder erstellen Sie eine neue IAM Rolle, um auf Ihre Repository-Anmeldeinformationen und Indexinhalte zuzugreifen.

> **Note**
>
> IAM Rollen, die für Indizes verwendet werden, können nicht für Datenquellen verwendet werden. Wenn Sie sich nicht sicher sind, ob eine vorhandene Rolle für einen Index oder eine häufig gestellte Frage verwendet wird, wählen Sie Neue Rolle erstellen, um Fehler zu vermeiden.

i. Wählen Sie Weiter aus.

7. Geben Sie auf der Seite Synchronisierungseinstellungen konfigurieren die folgenden Informationen ein:

a. Wählen Sie für den Synchronisierungsbereich eine der folgenden Optionen aus:

> **Note**
>
> Wenn Sie Artikel, Standardseiten und Basisblöcke crawlen möchten, werden deren Standardfelder automatisch synchronisiert. Sie können sich auch dafür entscheiden, ihre Kommentare, Anlagen, benutzerdefinierten Felder und andere benutzerdefinierte Entitäten zu synchronisieren.

- Für ausgewählte Entitäten:
  - Artikel — Wählen Sie aus, ob Artikel, ihre Kommentare und ihre Anlagen gecrawlt werden sollen.
  - Standardseiten — Wählen Sie aus, ob Standardseiten, ihre Kommentare und ihre Anlagen gecrawlt werden sollen.
  - Standardblöcke — Wählen Sie aus, ob Standardblöcke, ihre Kommentare und ihre Anlagen gecrawlt werden sollen.
  - Sie können auch benutzerdefinierte Inhaltstypen und benutzerdefinierte Blöcke hinzufügen.

b. Für zusätzliche Konfigurationen — optional:

- Für Regex-Muster — Fügen Sie Muster für reguläre Ausdrücke hinzu, um bestimmte Entitätstitel und Dateinamen ein- oder auszuschließen. Sie können bis zu 100 Muster hinzufügen.

c. Synchronisierungsmodus — Wählen Sie aus, wie Sie Ihren Index aktualisieren möchten, wenn sich der Inhalt Ihrer Datenquelle ändert. Wenn Sie Ihre Datenquelle Amazon Kendra zum ersten Mal synchronisieren, werden alle Inhalte standardmäßig gecrawlt und indexiert. Sie müssen eine vollständige Synchronisierung Ihrer Daten durchführen, falls Ihre erste Synchronisierung fehlgeschlagen ist, auch wenn Sie die Option Vollsynchronisierung nicht als Synchronisierungsmodusoption wählen.

- Vollständige Synchronisierung: Indizieren Sie den gesamten Inhalt neu und ersetzen die vorhandenen Inhalte jedes Mal, wenn Ihre Datenquelle mit Ihrem Index synchronisiert wird.
- Neue, geänderte, gelöschte Synchronisierung: Indizieren Sie bei jeder Synchronisierung Ihrer Datenquelle mit Ihrem Index nur neue, geänderte und gelöschte Inhalte. Amazon Kendra kann den Mechanismus Ihrer Datenquelle verwenden, um Inhaltsänderungen nachzuverfolgen und Inhalte zu indexieren, die sich seit der letzten Synchronisierung geändert haben.

d. Im Zeitplan für die Synchronisierungsausführung, Häufigkeit — Wie oft Amazon Kendra wird mit Ihrer Datenquelle synchronisiert?

e. Wählen Sie Weiter aus.

8. Geben Sie auf der Seite Feldzuordnungen festlegen die folgenden Informationen ein:

a. Für Inhalte, Kommentare und Anlagen — Wählen Sie aus den Amazon Kendra generierten Standard-Datenquellenfeldern aus, die Sie Ihrem Index zuordnen möchten.

b. Feld hinzufügen — Um benutzerdefinierte Datenquellenfelder hinzuzufügen, um einen Indexfeldnamen für die Zuordnung und den Felddatentyp zu erstellen.

c. Wählen Sie Weiter aus.

9. Überprüfen Sie auf der Seite Überprüfen und erstellen, ob die von Ihnen eingegebenen Informationen korrekt sind, und wählen Sie dann Datenquelle hinzufügen aus. Sie können Ihre Informationen auch auf dieser Seite bearbeiten. Ihre Datenquelle wird auf der Seite Datenquellen angezeigt, nachdem die Datenquelle erfolgreich hinzugefügt wurde.

API

Um eine Verbindung Amazon Kendra zu Drupal herzustellen

Sie müssen mithilfe der TemplateConfigurationAPI ein JSON des Datenquellenschemas angeben. Sie müssen die folgenden Informationen angeben:

- Datenquelle — Geben Sie den Datenquellentyp wie `DRUPAL` bei der Verwendung des TemplateConfigurationJSON-Schemas an. Geben Sie außerdem die Datenquelle so an`TEMPLATE`, wie Sie die CreateDataSourceAPI aufrufen.
- Synchronisierungsmodus — Geben Sie an, wie Ihr Index aktualisiert Amazon Kendra werden soll, wenn sich der Inhalt Ihrer Datenquelle ändert. Wenn Sie Ihre Datenquelle Amazon Kendra zum ersten Mal synchronisieren, werden alle Inhalte standardmäßig gecrawlt und indexiert. Sie müssen eine vollständige Synchronisierung Ihrer Daten durchführen, falls Ihre erste Synchronisierung fehlgeschlagen ist, auch wenn Sie die Option Vollsynchronisierung nicht als Synchronisierungsmodusoption wählen. Sie können wählen zwischen:
  - `FORCED_FULL_CRAWL`um den gesamten Inhalt neu zu indizieren und vorhandene Inhalte jedes Mal zu ersetzen, wenn Ihre Datenquelle mit Ihrem Index synchronisiert wird.
  - `FULL_CRAWL`um bei jeder Synchronisierung Ihrer Datenquelle mit Ihrem Index nur neue, geänderte und gelöschte Inhalte zu indizieren. Amazon Kendra kann den Mechanismus Ihrer Datenquelle verwenden, um Inhaltsänderungen nachzuverfolgen und Inhalte zu indexieren, die sich seit der letzten Synchronisierung geändert haben.
  - `CHANGE_LOG`um bei jeder Synchronisierung Ihrer Datenquelle mit Ihrem Index nur neue und geänderte Inhalte zu indizieren. Amazon Kendra kann den Mechanismus Ihrer Datenquelle

verwenden, um Inhaltsänderungen nachzuverfolgen und Inhalte zu indexieren, die sich seit der letzten Synchronisierung geändert haben.

- Geheimer Amazon-Ressourcenname (ARN) — Geben Sie den Amazon-Ressourcennamen (ARN) eines Secrets Manager Geheimnisses ein, das die Authentifizierungsdaten enthält, die Sie in Ihrem Drupal-Konto erstellt haben.

  Wenn Sie die Standardauthentifizierung verwenden, wird das Geheimnis in einer JSON-Struktur mit den folgenden Schlüsseln gespeichert:

  ```
  {
      "username": "user name",
      "password": "password"
  }
  ```

  Wenn Sie die OAuth 2.0-Authentifizierung verwenden, wird das Geheimnis in einer JSON-Struktur mit den folgenden Schlüsseln gespeichert:

  ```
  {
      "username": "user name",
      "password": "password",
      "clientId": "client id",
      "clientSecret": "client secret"
  }
  ```

  > **Note**
  >
  > > **Note**
  > >
  > > Wir empfehlen Ihnen, Ihre Anmeldeinformationen und Ihr Geheimnis regelmäßig zu aktualisieren oder zu wechseln. Stellen Sie zu Ihrer eigenen Sicherheit nur die Zugriffsebene bereit, die erforderlich ist. Wir raten davon ab, Anmeldeinformationen und geheime Daten für alle Datenquellen und Connector-Versionen 1.0 und 2.0 (sofern zutreffend) wiederzuverwenden.

- IAM Rolle — Geben Sie an`RoleArn`, wann Sie anrufen`CreateDataSource`, um einer IAM Rolle Berechtigungen für den Zugriff auf Ihr Secrets Manager Geheimnis und den Aufruf der

erforderlichen öffentlichen APIs für den Drupal-Connector und zu erteilen. Amazon Kendra Weitere Informationen finden Sie unter IAM Rollen für Drupal-Datenquellen.

Sie können auch die folgenden optionalen Funktionen hinzufügen:

- Virtual Private Cloud (VPC) — Geben Sie an, `VpcConfiguration` wann Sie anrufen. `CreateDataSource` Weitere Informationen finden Sie unter Konfigurieren von Amazon Kendra für die Verwendung eines Amazon VPC.
- Inklusions- und Ausschlussfilter — Sie können angeben, ob Inhalte, Kommentare und Anlagen eingeschlossen werden sollen. Sie können auch Muster für reguläre Ausdrücke angeben, um Inhalte, Kommentare und Anlagen ein- oder auszuschließen.

  > **Note**
  >
  > Die meisten Datenquellen verwenden Muster für reguläre Ausdrücke, bei denen es sich um Ein- oder Ausschlussmuster handelt, die als Filter bezeichnet werden. Wenn Sie einen Einschlussfilter angeben, werden nur Inhalte indexiert, die dem Einschlussfilter entsprechen. Jedes Dokument, das nicht dem Einschlussfilter entspricht, wird nicht indexiert. Wenn Sie einen Ein- und Ausschlussfilter angeben, werden Dokumente, die dem Ausschlussfilter entsprechen, nicht indexiert, auch wenn sie dem Einschlussfilter entsprechen.

- Identity Crawler — Geben Sie an, ob der Identity Crawler aktiviert Amazon Kendra werden soll. Der Identity Crawler verwendet die Informationen der Zugriffskontrollliste (ACL) für Ihre Dokumente, um Suchergebnisse nach dem Benutzer- oder Gruppenzugriff auf Dokumente zu filtern. Wenn Sie über eine ACL für Ihre Dokumente verfügen und Ihre ACL verwenden möchten, können Sie auch den Identity Crawler aktivieren, um die Benutzerkontextfilterung von Suchergebnissen zu konfigurieren. Amazon Kendra Andernfalls können alle Dokumente öffentlich durchsucht werden, wenn Identity Crawler ausgeschaltet ist. Wenn Sie die Zugriffskontrolle für Ihre Dokumente verwenden möchten und Identity Crawler ausgeschaltet ist, können Sie alternativ die PutPrincipalMappingAPI verwenden, um Benutzer- und Gruppenzugriffsinformationen für die Benutzerkontextfilterung hochzuladen.
- Feldzuordnungen — Wählen Sie diese Option, um Ihre Drupal-Datenquellenfelder Ihren Indexfeldern zuzuordnen. Amazon Kendra Weitere Informationen finden Sie unter Zuweisen von Datenquellenfeldern.

> **Note**
>
> Das Textfeld oder das entsprechende Textfeld für Ihre Dokumente ist erforderlich, um Ihre Dokumente durchsuchen Amazon Kendra zu können. Sie müssen den Feldnamen Ihres Dokumenthauptteils in Ihrer Datenquelle dem Namen des Indexfeldes zuordnen`_document_body`. Alle anderen Felder sind optional.

Eine Liste weiterer wichtiger JSON-Schlüssel, die konfiguriert werden müssen, finden Sie unterDrupal-Vorlagenschema.

Hinweise

- Drupal-APIs haben keine offiziellen Drosselungsgrenzen.
- Java-SDKs sind für Drupal nicht verfügbar.
- Drupal-Daten können nur mit nativen JSON-APIs abgerufen werden.
- Inhaltstypen, die keiner Drupal-Ansicht zugeordnet sind, können nicht gecrawlt werden.
- Sie benötigen Administratorzugriff, um Daten aus Drupal-Blöcken zu crawlen.
- Es ist keine JSON-API verfügbar, um den benutzerdefinierten Inhaltstyp mithilfe von HTTP-Verben zu erstellen.
- Der Dokumenttext und die Kommentare für Artikel, Standardseiten, Basisblöcke, den benutzerdefinierten Inhaltstyp und den benutzerdefinierten Blocktyp werden im HTML-Format angezeigt. Wenn der HTML-Inhalt nicht wohlgeformt ist, werden die HTML-bezogenen Tags im Hauptteil und in den Kommentaren des Dokuments angezeigt und sind in den Amazon Kendra Suchergebnissen sichtbar.
- Inhaltstypen und Blocktypen ohne Beschreibung oder Hauptteil werden nicht übernommen. Amazon Kendra Nur Kommentare und Anlagen mit solchen Inhalts - oder Blocktypen werden in Ihren Amazon Kendra Index aufgenommen.

GitHub

GitHub ist ein webbasierter Hosting-Dienst für die Softwareentwicklung, der Codespeicher und Verwaltungsdienste mit Versionskontrolle bereitstellt. Sie können Amazon Kendra damit Ihre GitHub Enterprise Cloud (SaaS) und GitHub Enterprise Server (On Prem) Repository-Dateien,

Issue- und Pull-Requests, Issue- und Pull-Request-Kommentare sowie Issue- und Pull-Request-Kommentaranhänge indizieren. Sie können auch wählen, ob Sie bestimmte Dateien ein- oder ausschließen möchten.

> **Note**
>
> Amazon Kendra unterstützt jetzt einen aktualisierten GitHub Connector.
> Die Konsole wurde automatisch für Sie aktualisiert. Alle neuen Konnektoren, die Sie in der Konsole erstellen, verwenden die aktualisierte Architektur. Wenn Sie die API verwenden, müssen Sie jetzt das TemplateConfigurationObjekt anstelle des `GitHubConfiguration` Objekts verwenden, um Ihren Connector zu konfigurieren.
> Konnektoren, die mit der älteren Konsolen- und API-Architektur konfiguriert wurden, funktionieren weiterhin wie konfiguriert. Sie können sie jedoch nicht bearbeiten oder aktualisieren. Wenn Sie Ihre Connectorkonfiguration bearbeiten oder aktualisieren möchten, müssen Sie einen neuen Connector erstellen.
> Wir empfehlen, Ihren Connector-Workflow auf die aktualisierte Version zu migrieren. Die Support für Konnektoren, die mit der älteren Architektur konfiguriert wurden, soll bis Juni 2024 eingestellt werden.

Sie können über Amazon Kendra die Amazon Kendra Konsole und die TemplateConfigurationAPI eine Verbindung zu Ihrer GitHub Datenquelle herstellen.

Informationen zur Fehlerbehebung bei Ihrem Amazon Kendra GitHub Datenquellen-Connector finden Sie unterProblembehandlung bei Datenquellen.

Themen

- Unterstützte Features
- Voraussetzungen
- Anweisungen zur Verbindung
- Weitere Informationen

Unterstützte Features

Amazon Kendra GitHub Ein Datenquellenconnector unterstützt die folgenden Funktionen:

- Feldzuordnungen

- Filterung des Benutzerkontextes
- Crawling der Benutzeridentität
- Einschluss-/Ausschlussfilter
- Vollständige und inkrementelle Inhaltssynchronisierung
- Virtual Private Cloud (VPC)

Voraussetzungen

Bevor Sie Ihre GitHub Datenquelle Amazon Kendra zum Indizieren verwenden können, nehmen Sie diese Änderungen in Ihren Konten GitHub und AWS Konten vor.

Stellen Sie sicher GitHub, dass Sie Folgendes haben:

- Es wurde ein GitHub Benutzer mit Administratorrechten für die GitHub Organisation erstellt.
- Es wurde ein klassisches persönliches Zugriffstoken für Authentifizierungsdaten erstellt. Informationen zum Erstellen eines persönlichen Zugriffstokens finden Sie in der GitHub Dokumentation.
- Empfehlung: Es wurde ein OAuth-Token für Authentifizierungsdaten erstellt. Verwenden Sie das OAuth-Token, um die API-Drosselungsgrenzen und die Konnektorleistung zu verbessern. Weitere Informationen finden Sie in der GitHub Dokumentation zur OAuth-Autorisierung.
- Notieren Sie sich die GitHub Host-URL für den von Ihnen GitHub verwendeten Diensttyp. Beispielsweise könnte die Host-URL für die GitHub Cloud `https://api.github.com` und die Host-URL für den GitHub Server `https://on-prem-host-url/api/v3/` lauten.
- Notieren Sie sich den Namen Ihrer Organisation für GitHub das GitHub Enterprise Cloud (SaaS) -Konto oder das GitHub Enterprise Server-Konto (lokal), mit dem Sie eine Verbindung herstellen möchten. Sie finden den Namen Ihrer Organisation, indem Sie sich bei GitHub Desktop anmelden und Ihre Organisationen in der Dropdownliste Ihres Profilbilds auswählen.
- Optional (nur Server): Es wurde ein SSL-Zertifikat generiert und der Pfad zu dem in einem Amazon S3 Bucket gespeicherten Zertifikat kopiert. Sie verwenden dies, um eine Verbindung herzustellen, GitHub falls Sie eine sichere SSL-Verbindung benötigen. Sie können mit OpenSSL einfach ein selbstsigniertes X509-Zertifikat auf jedem Computer generieren. Ein Beispiel für die Verwendung von OpenSSL zur Erstellung eines X509-Zertifikats finden Sie unter X509-Zertifikat erstellen und signieren.
- Die folgenden Berechtigungen wurden hinzugefügt:

  Für GitHub Enterprise Cloud (SaaS)

- repo: Status
- public_repo
- repo: einladen
- lesen:org
- Benutzer:E-Mail
- lesen:Benutzer

Für GitHub Enterprise Server (vor Ort)

- repo:status
- public_repo
- repo: einladen
- lesen:org
- Benutzer:E-Mail
- lesen:Benutzer
- site_admin

- Vergewissert, dass jedes Dokument in GitHub und zwischen anderen Datenquellen, die Sie für denselben Index verwenden möchten, einzigartig ist. Jede Datenquelle, die Sie für einen Index verwenden möchten, darf nicht dasselbe Dokument in allen Datenquellen enthalten. Dokument-IDs gelten für einen Index global und müssen pro Index eindeutig sein.

Stellen Sie sicher AWS-Konto, dass Sie Folgendes in Ihrem haben:

- Hat einen Amazon Kendra Index erstellt und bei Verwendung der API die Index-ID notiert.
- Sie haben eine IAM Rolle für Ihre Datenquelle erstellt und, falls Sie die API verwenden, den ARN der IAM Rolle notiert.

> **Note**
>
> Wenn Sie Ihren Authentifizierungstyp und Ihre Anmeldeinformationen ändern, müssen Sie Ihre IAM Rolle aktualisieren, um auf die richtige AWS Secrets Manager geheime ID zugreifen zu können.

- Wir haben Ihre GitHub Authentifizierungsdaten AWS Secrets Manager geheim gespeichert und, falls Sie die API verwenden, den ARN des Geheimnisses notiert.

> **Note**
>
> Wir empfehlen Ihnen, Ihre Anmeldeinformationen und Ihr Geheimnis regelmäßig zu aktualisieren oder zu wechseln. Stellen Sie zu Ihrer eigenen Sicherheit nur die Zugriffsebene bereit, die erforderlich ist. Wir raten davon ab, Anmeldeinformationen und geheime Daten für alle Datenquellen und Connector-Versionen 1.0 und 2.0 (sofern zutreffend) wiederzuverwenden.

Wenn Sie noch keine IAM Rolle oder keinen Schlüssel haben, können Sie die Konsole verwenden, um eine neue IAM Rolle und ein neues Secrets Manager Geheimnis zu erstellen, wenn Sie Ihre GitHub Datenquelle mit verbinden. Amazon Kendra Wenn Sie die API verwenden, müssen Sie den ARN einer vorhandenen IAM Rolle und eines Secrets Manager Geheimnisses sowie eine Index-ID angeben.

Anweisungen zur Verbindung

Um eine Verbindung Amazon Kendra zu Ihrer GitHub Datenquelle herzustellen, müssen Sie die erforderlichen Details zu Ihrer GitHub Datenquelle angeben, damit Sie auf Ihre Daten zugreifen Amazon Kendra können. Falls Sie noch keine Konfiguration GitHub für vorgenommen haben Amazon Kendra, finden Sie weitere Informationen unterVoraussetzungen.

Console

Um eine Verbindung Amazon Kendra herzustellen GitHub

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die Amazon Kendra Konsole.
2. Wählen Sie im linken Navigationsbereich Indizes und dann den Index, den Sie verwenden möchten, aus der Indexliste aus.

   > **Note**
   >
   > Sie können Ihre Einstellungen für die Benutzerzugriffskontrolle unter Indexeinstellungen konfigurieren oder bearbeiten.

3. Wählen Sie auf der Seite Erste Schritte die Option Datenquelle hinzufügen aus.

4. Wählen Sie auf der Seite Datenquelle hinzufügen die Option GitHub Connector und dann Connector hinzufügen aus.
5. Geben Sie auf der Seite „Datenquellendetails angeben“ die folgenden Informationen ein:
    a. Geben Sie im Feld Name und Beschreibung für Datenquellenname einen Namen für Ihre Datenquelle ein. Sie können Bindestriche, aber keine Leerzeichen verwenden.
    b. (Optional) Beschreibung — Geben Sie eine optionale Beschreibung für Ihre Datenquelle ein.
    c. In Standardsprache — Wählen Sie eine Sprache aus, um Ihre Dokumente nach dem Index zu filtern. Sofern Sie nichts anderes angeben, ist die Standardsprache Englisch. Die in den Metadaten des Dokuments angegebene Sprache hat Vorrang vor der ausgewählten Sprache.
    d. Unter Tags für Neues Tag hinzufügen — Fügen Sie optionale Tags hinzu, um Ihre Ressourcen zu durchsuchen und zu filtern oder Ihre Kosten nachzuverfolgen. AWS
    e. Wählen Sie Weiter aus.
6. Geben Sie auf der Seite Zugriff und Sicherheit definieren die folgenden Informationen ein:
    a. GitHubsource — Wählen Sie zwischen GitHub Enterprise Cloud und GitHubEnterprise Server.
    b. GitHub Host-URL — Geben Sie Ihren GitHub Hostnamen ein.
    c. GitHub Name der Organisation — Geben Sie den Namen Ihrer GitHub Organisation ein. Die Informationen zu Ihrer Organisation finden Sie in Ihrem GitHub Konto.
    d. Autorisierung — Aktivieren oder deaktivieren Sie die Informationen der Zugriffskontrollliste (ACL) für Ihre Dokumente, wenn Sie über eine ACL verfügen und diese für die Zugriffskontrolle verwenden möchten. Die ACL gibt an, auf welche Dokumente Benutzer und Gruppen zugreifen können. Die ACL-Informationen werden verwendet, um Suchergebnisse nach dem Benutzer- oder Gruppenzugriff auf Dokumente zu filtern. Weitere Informationen finden Sie unter Benutzerkontextfilterung.
    e. AWS Secrets Manager geheim — Wählen Sie ein vorhandenes Geheimnis aus, oder erstellen Sie ein neues Secrets Manager Geheimnis, um Ihre GitHub Authentifizierungsdaten zu speichern. Wenn Sie ein neues Geheimnis erstellen möchten, wird ein AWS Secrets Manager geheimes Fenster geöffnet.
        i. Geben Sie die folgenden Informationen in das Fenster Create an AWS Secrets Manager Secret ein:

A. Geheimer Name — Ein Name für Ihr Geheimnis. Das Präfix 'AmazonKendra-GitHub -' wird automatisch zu Ihrem geheimen Namen hinzugefügt.

B. Für GitHubToken — Geben Sie die Werte für die Authentifizierungsdaten ein, die Sie in Ihrem Konto erstellt haben. GitHub

ii. Wählen Sie Speichern.

f. Virtual Private Cloud (VPC) — Sie können wählen, ob Sie eine VPC verwenden möchten. In diesem Fall müssen Sie Subnetze und VPC-Sicherheitsgruppen hinzufügen.

g. Identity Crawler — Geben Sie an, ob der Identity Crawler aktiviert Amazon Kendra werden soll. Der Identity Crawler verwendet die Informationen der Zugriffskontrollliste (ACL) für Ihre Dokumente, um Suchergebnisse nach dem Benutzer- oder Gruppenzugriff auf Dokumente zu filtern. Wenn Sie über eine ACL für Ihre Dokumente verfügen und Ihre ACL verwenden möchten, können Sie auch den Identity Crawler aktivieren, um die Benutzerkontextfilterung von Suchergebnissen zu konfigurieren. Amazon Kendra Andernfalls können alle Dokumente öffentlich durchsucht werden, wenn Identity Crawler ausgeschaltet ist. Wenn Sie die Zugriffskontrolle für Ihre Dokumente verwenden möchten und Identity Crawler ausgeschaltet ist, können Sie alternativ die PutPrincipalMappingAPI verwenden, um Benutzer- und Gruppenzugriffsinformationen für die Benutzerkontextfilterung hochzuladen.

h. IAM Rolle — Wählen Sie eine bestehende IAM Rolle oder erstellen Sie eine neue IAM Rolle, um auf Ihre Repository-Anmeldeinformationen und Indexinhalte zuzugreifen.

> **Note**
>
> IAM Rollen, die für Indizes verwendet werden, können nicht für Datenquellen verwendet werden. Wenn Sie sich nicht sicher sind, ob eine vorhandene Rolle für einen Index oder eine häufig gestellte Frage verwendet wird, wählen Sie Neue Rolle erstellen, um Fehler zu vermeiden.

i. Wählen Sie Weiter aus.

7. Geben Sie auf der Seite „Synchronisierungseinstellungen konfigurieren“ die folgenden Informationen ein:

a. Repositorys zum Crawlen auswählen — Wählen Sie zwischen „Alle Repositorys durchforsten“ oder „Repositorys auswählen“.

Wenn Sie Repositorys auswählen wählen, fügen Sie Namen für die Repositorys im Feld Name des Repositorys und optional die Namen bestimmter Branches im Feld Name des Branches hinzu.

b. Inhaltstypen — Wählen Sie die Inhaltstypen aus, die Sie einbeziehen möchten.

c. Regex-Muster — Reguläre Ausdrucksmuster zum Ein- oder Ausschließen bestimmter Dateien. Sie können bis zu 100 Muster hinzufügen.

d. Geben Sie im Zeitplan für die Synchronisierungsausführung die Option Frequenz ein: Wie oft Amazon Kendra wird mit Ihrer Datenquelle synchronisiert?

e. Wählen Sie Weiter aus.

8. Synchronisierungsmodus — Wählen Sie aus, wie Sie Ihren Index aktualisieren möchten, wenn sich der Inhalt Ihrer Datenquelle ändert. Wenn Sie Ihre Datenquelle Amazon Kendra zum ersten Mal synchronisieren, werden alle Inhalte standardmäßig gecrawlt und indexiert. Sie müssen eine vollständige Synchronisierung Ihrer Daten durchführen, falls Ihre erste Synchronisierung fehlgeschlagen ist, auch wenn Sie die Option Vollsynchronisierung nicht als Synchronisierungsmodusoption wählen.

   - Vollständige Synchronisierung: Indizieren Sie den gesamten Inhalt neu und ersetzen die vorhandenen Inhalte jedes Mal, wenn Ihre Datenquelle mit Ihrem Index synchronisiert wird.
   - Neue, geänderte Synchronisierung: Indizieren Sie jedes Mal, wenn Ihre Datenquelle mit Ihrem Index synchronisiert wird, nur neue und geänderte Inhalte. Amazon Kendra kann den Mechanismus Ihrer Datenquelle verwenden, um Inhaltsänderungen nachzuverfolgen und Inhalte zu indexieren, die sich seit der letzten Synchronisierung geändert haben.
   - Neue, geänderte, gelöschte Synchronisierung: Indizieren Sie bei jeder Synchronisierung Ihrer Datenquelle mit Ihrem Index nur neue, geänderte und gelöschte Inhalte. Amazon Kendra kann den Mechanismus Ihrer Datenquelle verwenden, um Inhaltsänderungen nachzuverfolgen und Inhalte zu indexieren, die sich seit der letzten Synchronisierung geändert haben.

9. Im Synchronisierungslaufplan für Frequenz — Wie oft Amazon Kendra mit Ihrer Datenquelle synchronisiert.

10. Wählen Sie Weiter aus.

11. Geben Sie auf der Seite Feldzuordnungen festlegen die folgenden Informationen ein:

    a. Für Repository, Repository Commit, Issue-Dokument, Issue-Kommentar, Issue-Anhang, Pull-Request-Kommentar, Pull-Request-Dokument, Pull-Request-Anhang — Wählen Sie

aus den Amazon Kendra generierten Standard-Datenquellenfeldern, die Sie Ihrem Index zuordnen möchten.

b. Feld hinzufügen — Um benutzerdefinierte Datenquellenfelder hinzuzufügen, um einen Indexfeldnamen für die Zuordnung und den Felddatentyp zu erstellen.

c. Wählen Sie Weiter aus.

12. Überprüfen Sie auf der Seite Überprüfen und erstellen, ob die von Ihnen eingegebenen Informationen korrekt sind, und wählen Sie dann Datenquelle hinzufügen aus. Sie können Ihre Informationen auch auf dieser Seite bearbeiten. Ihre Datenquelle wird auf der Seite Datenquellen angezeigt, nachdem die Datenquelle erfolgreich hinzugefügt wurde.

API

Um eine Verbindung Amazon Kendra herzustellen GitHub

Sie müssen mithilfe der TemplateConfigurationAPI einen JSON-Wert des Datenquellenschemas angeben. Sie müssen die folgenden Informationen angeben:

- Datenquelle — Geben Sie den Datenquellentyp wie `GITHUB` bei der Verwendung des TemplateConfigurationJSON-Schemas an. Geben Sie außerdem die Datenquelle so an`TEMPLATE`, wie Sie die CreateDataSourceAPI aufrufen.
- GitHubtype — Geben Sie den Typ entweder als `SAAS` oder `ON_PREMISE` an.
- Host-URL — Geben Sie die GitHub Host-URL oder die API-Endpunkt-URL an. Wenn Sie beispielsweise GitHub SaaS/Enterprise Cloud verwenden, könnte die Host-URL lauten`https://api.github.com`, und für GitHub On-Premises/Enterprise Server könnte die Host-URL lauten. `https://on-prem-host-url/api/v3/`
- Name der Organisation — Geben Sie den Namen der Organisation des Kontos an. GitHub Sie finden den Namen Ihrer Organisation, indem Sie sich bei GitHub Desktop anmelden und in der Dropdownliste Ihres Profilbilds Ihre Organisationen auswählen.
- Synchronisierungsmodus — Geben Sie an, wie Ihr Index aktualisiert Amazon Kendra werden soll, wenn sich der Inhalt Ihrer Datenquelle ändert. Wenn Sie Ihre Datenquelle Amazon Kendra zum ersten Mal synchronisieren, werden alle Inhalte standardmäßig gecrawlt und indexiert. Sie müssen eine vollständige Synchronisierung Ihrer Daten durchführen, falls Ihre erste Synchronisierung fehlgeschlagen ist, auch wenn Sie die Option Vollsynchronisierung nicht als Synchronisierungsmodusoption wählen. Sie können wählen zwischen:
  - `FORCED_FULL_CRAWL`um den gesamten Inhalt neu zu indizieren und vorhandene Inhalte jedes Mal zu ersetzen, wenn Ihre Datenquelle mit Ihrem Index synchronisiert wird.

  - `FULL_CRAWL`um bei jeder Synchronisierung Ihrer Datenquelle mit Ihrem Index nur neue, geänderte und gelöschte Inhalte zu indizieren. Amazon Kendra kann den Mechanismus Ihrer Datenquelle verwenden, um Inhaltsänderungen nachzuverfolgen und Inhalte zu indexieren, die sich seit der letzten Synchronisierung geändert haben.
  - `CHANGE_LOG`um jedes Mal, wenn Ihre Datenquelle mit Ihrem Index synchronisiert wird, nur neue und geänderte Inhalte zu indizieren. Amazon Kendra kann den Mechanismus Ihrer Datenquelle verwenden, um Inhaltsänderungen nachzuverfolgen und Inhalte zu indexieren, die sich seit der letzten Synchronisierung geändert haben.
- Identity Crawler — Geben Sie an, ob der Identity Crawler aktiviert Amazon Kendra werden soll. Der Identity Crawler verwendet die Informationen der Zugriffskontrollliste (ACL) für Ihre Dokumente, um Suchergebnisse nach dem Benutzer- oder Gruppenzugriff auf Dokumente zu filtern. Wenn Sie über eine ACL für Ihre Dokumente verfügen und Ihre ACL verwenden möchten, können Sie auch den Identity Crawler aktivieren, um die Benutzerkontextfilterung von Suchergebnissen zu konfigurieren. Amazon Kendra Andernfalls können alle Dokumente öffentlich durchsucht werden, wenn Identity Crawler ausgeschaltet ist. Wenn Sie die Zugriffskontrolle für Ihre Dokumente verwenden möchten und Identity Crawler ausgeschaltet ist, können Sie alternativ die PutPrincipalMappingAPI verwenden, um Benutzer- und Gruppenzugriffsinformationen für die Benutzerkontextfilterung hochzuladen.
- Geheimer Amazon-Ressourcenname (ARN) — Geben Sie den Amazon-Ressourcennamen (ARN) eines Secrets Manager Geheimnisses ein, das die Authentifizierungsdaten für Ihr GitHub Konto enthält. Das Geheimnis wird in einer JSON-Struktur mit den folgenden Schlüsseln gespeichert:

```
{
    "personalToken": "token"
}
```

> **Note**
>
> Wir empfehlen Ihnen, Ihre Anmeldeinformationen und Ihr Geheimnis regelmäßig zu aktualisieren oder zu wechseln. Stellen Sie zu Ihrer eigenen Sicherheit nur die Zugriffsebene bereit, die erforderlich ist. Wir raten davon ab, Anmeldeinformationen und geheime Daten für alle Datenquellen und Connector-Versionen 1.0 und 2.0 (sofern zutreffend) wiederzuverwenden.

- IAM Rolle — Geben Sie an`RoleArn`, wann Sie anrufen`CreateDataSource`, um einer IAM Rolle Berechtigungen für den Zugriff auf Ihr Secrets Manager Geheimnis und für den Aufruf der erforderlichen öffentlichen APIs für den GitHub Connector und zum Aufrufen der erforderlichen öffentlichen APIs zu erteilen. Amazon Kendra Weitere Informationen finden Sie unter IAM Rollen für GitHub Datenquellen.

Sie können auch die folgenden optionalen Funktionen hinzufügen:

- Virtual Private Cloud (VPC) — Geben Sie an, `VpcConfiguration` wann Sie anrufen. `CreateDataSource` Weitere Informationen finden Sie unter Konfigurieren von Amazon Kendra für die Verwendung eines Amazon VPC.

> **Note**
>
> Wenn Sie einen GitHub Server verwenden, müssen Sie einen verwenden, Amazon VPC um eine Verbindung zu Ihrem GitHub Server herzustellen.

- Repository-Filter — Filtert Repositorys nach ihrem Namen und ihren Zweignamen.
- Dokument-/Inhaltstypen — Geben Sie an, ob Repository-Dokumente, Issues, Issue-Kommentare, Issue-Kommentar-Anlagen, Pull-Requests, Pull-Request-Kommentare und Pull-Request-Kommentaranhänge gecrawlt werden sollen.
- Inklusions- und Ausschlussfilter — Geben Sie an, ob bestimmte Dateien und Ordner ein- oder ausgeschlossen werden sollen.

> **Note**
>
> Die meisten Datenquellen verwenden Muster für reguläre Ausdrücke, bei denen es sich um Ein- oder Ausschlussmuster handelt, die als Filter bezeichnet werden. Wenn Sie einen Einschlussfilter angeben, werden nur Inhalte indexiert, die dem Einschlussfilter entsprechen. Jedes Dokument, das nicht dem Einschlussfilter entspricht, wird nicht indexiert. Wenn Sie einen Ein- und Ausschlussfilter angeben, werden Dokumente, die dem Ausschlussfilter entsprechen, nicht indexiert, auch wenn sie dem Einschlussfilter entsprechen.

- Zugriffskontrollliste (ACL) — Geben Sie an, ob die ACL-Informationen für Ihre Dokumente gecrawlt werden sollen, wenn Sie über eine ACL verfügen und diese für die Zugriffskontrolle verwenden möchten. Die ACL gibt an, auf welche Dokumente Benutzer und Gruppen

zugreifen können. Die ACL-Informationen werden verwendet, um Suchergebnisse nach dem Benutzer- oder Gruppenzugriff auf Dokumente zu filtern. Weitere Informationen finden Sie unter Benutzerkontextfilterung.

- Feldzuordnungen — Wählen Sie diese Option, um Ihre GitHub Datenquellenfelder Ihren Indexfeldern zuzuordnen. Amazon Kendra Sie können Felder mit Dokumenten, Commits, Issues, Issue-Anhängen, Issue-Kommentaren, Pull-Requests, Pull-Request-Anhängen und Pull-Request-Kommentaren einbeziehen. Weitere Informationen finden Sie unter Zuweisen von Datenquellenfeldern.

  > **Note**
  >
  > Das Textfeld oder das entsprechende Dokument für Ihre Dokumente ist erforderlich, damit Amazon Kendra Ihre Dokumente durchsuchen kann. Sie müssen den Feldnamen des Hauptteils Ihres Dokuments in Ihrer Datenquelle dem Indexfeldnamen _document_body zuordnen. Alle anderen Felder sind optional.

Eine Liste weiterer wichtiger JSON-Schlüssel, die konfiguriert werden müssen, finden Sie unter GitHub Template-Schema.

Weitere Informationen

Weitere Informationen zur Integration Amazon Kendra mit Ihrer GitHub Datenquelle finden Sie unter:

- Stellen Sie sich die Suche in GitHub Repositorys mit der Leistung des Connectors neu vor Amazon Kendra GitHub

Gmail

Gmail ist ein von Google entwickelter E-Mail-Client, über den Sie E-Mail-Nachrichten mit Dateianhängen senden können. Gmail-Nachrichten können mithilfe von Ordnern und Labels sortiert und in Ihrem E-Mail-Posteingang gespeichert werden. Sie können Amazon Kendra damit Ihre E-Mail-Nachrichten und Nachrichtenanhänge indizieren. Sie können auch konfigurieren Amazon Kendra , dass bestimmte E-Mail-Nachrichten, Nachrichtenanhänge und Labels für die Indizierung ein- oder ausgeschlossen werden.

Sie können über Amazon Kendra die Amazon Kendra Konsole und die TemplateConfigurationAPI eine Verbindung zu Ihrer Gmail-Datenquelle herstellen.

Informationen zur Fehlerbehebung bei Ihrem Amazon Kendra Gmail-Datenquellen-Connector finden Sie unterProblembehandlung bei Datenquellen.

Themen

Unterstützte Features

- Feldzuordnungen
- Filterung des Benutzerkontextes
- Einschluss-/Ausschlussfilter
- Vollständige und inkrementelle Inhaltssynchronisierung
- Virtual Private Cloud (VPC)

Voraussetzungen

Bevor Sie Ihre Gmail-Datenquelle Amazon Kendra zum Indizieren verwenden können, müssen Sie diese Änderungen in Ihrem Gmail-Konto und AWS Ihren Konten vornehmen.

Stellen Sie in Gmail sicher, dass Sie über Folgendes verfügen:

- Sie haben ein Google Cloud Platform-Administratorkonto und ein Google Cloud-Projekt erstellt.
- Gmail API und Admin SDK API in Ihrem Admin-Konto aktiviert.
- Sie haben ein Dienstkonto erstellt und einen privaten JSON-Schlüssel für Ihr Gmail heruntergeladen. Informationen dazu, wie Sie Ihren privaten Schlüssel erstellen und darauf zugreifen, finden Sie in der Google Cloud-Dokumentation zum Erstellen eines Dienstkontoschlüssels und zu den Anmeldeinformationen für das Dienstkonto.

- Die E-Mail-Adresse Ihres Administratorkontos, die E-Mail-Adresse Ihres Dienstkontos und Ihr privater Schlüssel zur Authentifizierung wurden kopiert.
- Die folgenden Oauth-Bereiche (mit einer Administratorrolle) wurden für Ihren Benutzer und die gemeinsam genutzten Verzeichnisse, die Sie indexieren möchten, hinzugefügt:
  - https://www.googleapis.com/auth/admin.directory.user.readonly
  - https://www.googleapis.com/auth/gmail.readonly
- Vergewissert, dass jedes Dokument in Gmail und allen anderen Datenquellen, die Sie für denselben Index verwenden möchten, einzigartig ist. Jede Datenquelle, die Sie für einen Index verwenden möchten, darf nicht dasselbe Dokument in allen Datenquellen enthalten. Dokument-IDs gelten für einen Index global und müssen pro Index eindeutig sein.

Stellen Sie sicher AWS-Konto, dass Sie Folgendes in Ihrem haben:

- Hat einen Amazon Kendra Index erstellt und bei Verwendung der API die Index-ID notiert.
- Sie haben eine IAM Rolle für Ihre Datenquelle erstellt und, falls Sie die API verwenden, den ARN der IAM Rolle notiert.

> **Note**
>
> Wenn Sie Ihren Authentifizierungstyp und Ihre Anmeldeinformationen ändern, müssen Sie Ihre IAM Rolle aktualisieren, um auf die richtige AWS Secrets Manager geheime ID zugreifen zu können.

- Haben Ihre Gmail-Authentifizierungsdaten AWS Secrets Manager geheim gespeichert und, falls Sie die API verwenden, den ARN des Geheimnisses notiert.

> **Note**
>
> Wir empfehlen Ihnen, Ihre Anmeldeinformationen und Ihr Passwort regelmäßig zu aktualisieren oder zu wechseln. Stellen Sie zu Ihrer eigenen Sicherheit nur die Zugriffsebene bereit, die erforderlich ist. Wir raten davon ab, Anmeldeinformationen und geheime Daten für alle Datenquellen und Connector-Versionen 1.0 und 2.0 (sofern zutreffend) wiederzuverwenden.

Wenn Sie noch keine IAM Rolle oder keinen Schlüssel haben, können Sie die Konsole verwenden, um eine neue IAM Rolle und ein neues Secrets Manager Geheimnis zu erstellen, wenn Sie Ihre Gmail-Datenquelle mit verbinden. Amazon Kendra Wenn Sie die API verwenden, müssen Sie den ARN einer vorhandenen IAM Rolle und eines Secrets Manager Geheimnisses sowie eine Index-ID angeben.

Anweisungen zur Verbindung

Um eine Verbindung Amazon Kendra zu Ihrer Gmail-Datenquelle herzustellen, müssen Sie Details zu Ihren Gmail-Anmeldeinformationen angeben, damit Sie auf Ihre Daten zugreifen Amazon Kendra können. Falls Sie Gmail noch nicht für konfiguriert haben Amazon Kendra, finden Sie weitere Informationen unterVoraussetzungen.

Console

So stellen Sie eine Verbindung Amazon Kendra zu Gmail her

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die Amazon Kendra Konsole.
2. Wählen Sie im linken Navigationsbereich Indizes und dann den Index, den Sie verwenden möchten, aus der Indexliste aus.

   > **Note**
   >
   > Sie können Ihre Einstellungen für die Benutzerzugriffskontrolle unter Indexeinstellungen konfigurieren oder bearbeiten.

3. Wählen Sie auf der Seite Erste Schritte die Option Datenquelle hinzufügen aus.
4. Wählen Sie auf der Seite Datenquelle hinzufügen die Option Gmail-Connector und dann Connector hinzufügen aus.
5. Geben Sie auf der Seite „Datenquellendetails angeben“ die folgenden Informationen ein:

   a. Geben Sie im Feld Name und Beschreibung für Datenquellenname einen Namen für Ihre Datenquelle ein. Sie können Bindestriche, aber keine Leerzeichen verwenden.

   b. (Optional) Beschreibung — Geben Sie eine optionale Beschreibung für Ihre Datenquelle ein.

   c. In Standardsprache — Wählen Sie eine Sprache aus, um Ihre Dokumente nach dem Index zu filtern. Sofern Sie nichts anderes angeben, ist die Standardsprache Englisch.

Die in den Metadaten des Dokuments angegebene Sprache hat Vorrang vor der ausgewählten Sprache.

d. Unter Tags für Neues Tag hinzufügen — Fügen Sie optionale Tags hinzu, um Ihre Ressourcen zu durchsuchen und zu filtern oder Ihre Kosten nachzuverfolgen. AWS

e. Wählen Sie Weiter aus.

6. Geben Sie auf der Seite Zugriff und Sicherheit definieren die folgenden Informationen ein:

a. Unter Authentifizierung für AWS Secrets Manager geheime Daten — Wählen Sie ein vorhandenes Geheimnis aus, oder erstellen Sie ein neues Secrets Manager Geheimnis, um Ihre Gmail-Authentifizierungsdaten zu speichern. Wenn Sie sich dafür entscheiden, ein neues Geheimnis zu erstellen, wird ein AWS Secrets Manager geheimes Fenster geöffnet.

- Geben Sie die folgenden Informationen in das Fenster Create an AWS Secrets Manager Secret ein:

A. Geheimer Name — Ein Name für Ihr Geheimnis.

B. Kunden-E-Mail — Die Kunden-E-Mail, die Sie aus Ihrem Google-Dienstkonto kopiert haben.

C. E-Mail-Adresse des Administratorkontos: Die E-Mail-Adresse des Administratorkontos, die Sie verwenden möchten.

D. Privater Schlüssel — Der private Schlüssel, den Sie aus Ihrem Google-Dienstkonto kopiert haben.

E. Wählen Sie Speichern.

b. Virtual Private Cloud (VPC) — Sie können wählen, ob Sie eine VPC verwenden möchten. In diesem Fall müssen Sie Subnetze und VPC-Sicherheitsgruppen hinzufügen.

c. IAM Rolle — Wählen Sie eine bestehende IAM Rolle oder erstellen Sie eine neue IAM Rolle, um auf Ihre Repository-Anmeldeinformationen und Indexinhalte zuzugreifen.

> **Note**
>
> IAM Rollen, die für Indizes verwendet werden, können nicht für Datenquellen verwendet werden. Wenn Sie sich nicht sicher sind, ob eine vorhandene Rolle für einen Index oder eine häufig gestellte Frage verwendet wird, wählen Sie Neue Rolle erstellen, um Fehler zu vermeiden.

d. Wählen Sie Weiter aus.

7. Geben Sie auf der Seite „Synchronisierungseinstellungen konfigurieren“ die folgenden Informationen ein:

   a. Wählen Sie unter Synchronisierungsbereich für Entitätstypen die Option Nachrichtenanhänge aus, um Nachrichtenanhänge zu synchronisieren. Nachrichten werden standardmäßig synchronisiert.

   b. (Optional) Geben Sie für die zusätzliche Konfiguration die folgenden Informationen ein:

      i. Datumsbereich — Geben Sie einen Datumsbereich ein, um das Start- und Enddatum von E-Mails anzugeben, die gecrawlt werden sollen.

      ii. E-Mail-Domänen — Schließen Sie E-Mails basierend auf Domänen ein oder aus.

      iii. Schlüsselwörter in Betreffs — Schließen Sie E-Mails auf der Grundlage von Schlüsselwörtern in ihren Betreffs ein oder aus.

      > **Note**
      >
      > Sie können sich auch dafür entscheiden, alle Dokumente einzubeziehen, die allen von Ihnen eingegebenen Betreff-Schlüsselwörtern entsprechen.

      iv. Beschriftungen — Fügen Sie Muster für reguläre Ausdrücke hinzu, um bestimmte Beschriftungen ein- oder auszuschließen. Sie können bis zu 100 Muster hinzufügen.

      v. Anlagen — Fügen Sie Muster für reguläre Ausdrücke hinzu, um bestimmte Anlagen ein- oder auszuschließen. Sie können bis zu 100 Muster hinzufügen.

   c. Synchronisierungsmodus — Wählen Sie aus, wie Sie Ihren Index aktualisieren möchten, wenn sich der Inhalt Ihrer Datenquelle ändert. Wenn Sie Ihre Datenquelle Amazon Kendra zum ersten Mal synchronisieren, werden alle Inhalte standardmäßig gecrawlt und indexiert. Sie müssen eine vollständige Synchronisierung Ihrer Daten durchführen, falls Ihre erste Synchronisierung fehlgeschlagen ist, auch wenn Sie die Option Vollsynchronisierung nicht als Synchronisierungsmodusoption wählen.

      - Vollständige Synchronisierung: Indizieren Sie den gesamten Inhalt neu und ersetzen die vorhandenen Inhalte jedes Mal, wenn Ihre Datenquelle mit Ihrem Index synchronisiert wird.
      - Neue, geänderte, gelöschte Synchronisierung: Indizieren Sie bei jeder Synchronisierung Ihrer Datenquelle mit Ihrem Index nur neue, geänderte und

gelöschte Inhalte. Amazon Kendra kann den Mechanismus Ihrer Datenquelle verwenden, um Inhaltsänderungen nachzuverfolgen und Inhalte zu indexieren, die sich seit der letzten Synchronisierung geändert haben.

> **Important**
>
> Da es keine API zum Aktualisieren dauerhaft gelöschter Gmail-Nachrichten gibt, werden neue, geänderte oder gelöschte Inhalte synchronisiert:
>
> - Nachrichten, die dauerhaft aus Gmail gelöscht wurden, werden nicht aus Ihrem Amazon Kendra Index entfernt
> - Synchronisiert keine Änderungen an Gmail-E-Mail-Labels
>
> Um die Änderungen an den Labels Ihrer Gmail-Datenquelle und dauerhaft gelöschte E-Mail-Nachrichten mit Ihrem Amazon Kendra Index zu synchronisieren, müssen Sie regelmäßig vollständige Crawls ausführen.

d. Im Synchronisierungszeitplan für Frequenz — Wie oft Amazon Kendra wird mit Ihrer Datenquelle synchronisiert?

e. Wählen Sie Weiter aus.

8. Geben Sie auf der Seite Feldzuordnungen festlegen die folgenden Informationen ein:

   a. Für Nachrichten und Nachrichtenanhänge — Wählen Sie aus den Amazon Kendra generierten Standard-Datenquellenfeldern aus, die Sie Ihrem Index zuordnen möchten.

   > **Note**
   >
   > Amazon Kendra Der Gmail-Datenquellen-Connector unterstützt die Erstellung von benutzerdefinierten Indexfeldern aufgrund von API-Einschränkungen nicht.

   b. Wählen Sie Weiter aus.

9. Überprüfen Sie auf der Seite Überprüfen und erstellen, ob die von Ihnen eingegebenen Informationen korrekt sind, und wählen Sie dann Datenquelle hinzufügen aus. Sie können Ihre Informationen auch auf dieser Seite bearbeiten. Ihre Datenquelle wird auf der Seite Datenquellen angezeigt, nachdem die Datenquelle erfolgreich hinzugefügt wurde.

API

Um eine Verbindung Amazon Kendra zu Gmail herzustellen

Sie müssen mithilfe der TemplateConfigurationAPI ein JSON des Datenquellenschemas angeben. Sie müssen die folgenden Informationen angeben:

- Datenquelle — Geben Sie den Datenquellentyp wie `GMAIL` bei der Verwendung des TemplateConfigurationJSON-Schemas an. Geben Sie außerdem die Datenquelle so an`TEMPLATE`, wie Sie die CreateDataSourceAPI aufrufen.
- Synchronisierungsmodus — Geben Sie an, wie Ihr Index aktualisiert Amazon Kendra werden soll, wenn sich der Inhalt Ihrer Datenquelle ändert. Wenn Sie Ihre Datenquelle Amazon Kendra zum ersten Mal synchronisieren, werden alle Inhalte standardmäßig gecrawlt und indexiert. Sie müssen eine vollständige Synchronisierung Ihrer Daten durchführen, falls Ihre erste Synchronisierung fehlgeschlagen ist, auch wenn Sie die Option Vollsynchronisierung nicht als Synchronisierungsmodusoption wählen. Sie können wählen zwischen:
  - `FORCED_FULL_CRAWL`um den gesamten Inhalt neu zu indizieren und vorhandene Inhalte jedes Mal zu ersetzen, wenn Ihre Datenquelle mit Ihrem Index synchronisiert wird.
  - `FULL_CRAWL`um bei jeder Synchronisierung Ihrer Datenquelle mit Ihrem Index nur neue, geänderte und gelöschte Inhalte zu indizieren. Amazon Kendra kann den Mechanismus Ihrer Datenquelle verwenden, um Inhaltsänderungen nachzuverfolgen und Inhalte zu indexieren, die sich seit der letzten Synchronisierung geändert haben.

  > **Important**
  >
  > Da es keine API zum Aktualisieren dauerhaft gelöschter Gmail-Nachrichten gibt, werden neue, geänderte oder gelöschte Inhalte synchronisiert:
  >
  > - Nachrichten, die dauerhaft aus Gmail gelöscht wurden, werden nicht aus Ihrem Amazon Kendra Index entfernt
  > - Synchronisiert keine Änderungen an Gmail-E-Mail-Labels
  >
  > Um die Änderungen an den Labels Ihrer Gmail-Datenquelle und dauerhaft gelöschte E-Mail-Nachrichten mit Ihrem Amazon Kendra Index zu synchronisieren, müssen Sie regelmäßig vollständige Crawls ausführen.
- Geheimer Amazon-Ressourcenname (ARN) — Geben Sie den Amazon-Ressourcennamen (ARN) eines Secrets Manager Geheimnisses ein, das die Authentifizierungsdaten für Ihr Gmail-

Konto enthält. Das Geheimnis wird in einer JSON-Struktur mit den folgenden Schlüsseln gespeichert:

```
{
    "adminAccountEmailId": "service account email",
    "clientEmailId": "user account email",
    "privateKey": "private key"
}
```

> **Note**
>
> Wir empfehlen Ihnen, Ihre Anmeldeinformationen und Ihr Geheimnis regelmäßig zu aktualisieren oder zu wechseln. Stellen Sie zu Ihrer eigenen Sicherheit nur die Zugriffsebene bereit, die erforderlich ist. Wir raten davon ab, Anmeldeinformationen und geheime Daten für alle Datenquellen und Connector-Versionen 1.0 und 2.0 (sofern zutreffend) wiederzuverwenden.

- IAM Rolle — Geben Sie an`RoleArn`, wann Sie anrufen`CreateDataSource`, um einer IAM Rolle Berechtigungen für den Zugriff auf Ihr Secrets Manager Geheimnis und für den Aufruf der erforderlichen öffentlichen APIs für den Gmail-Connector und zum Aufrufen der erforderlichen öffentlichen APIs zu erteilen. Amazon Kendra Weitere Informationen finden Sie unter IAM Rollen für Gmail-Datenquellen.

Sie können auch die folgenden optionalen Funktionen hinzufügen:

- Virtual Private Cloud (VPC) — Geben Sie an, `VpcConfiguration` wann Sie anrufen. `CreateDataSource` Weitere Informationen finden Sie unter Konfigurieren von Amazon Kendra für die Verwendung eines Amazon VPC.
- Inklusions- und Ausschlussfilter — Sie können angeben, ob Nachrichten und Anlagen ein- oder ausgeschlossen werden sollen.

> **Note**
>
> Die meisten Datenquellen verwenden Muster für reguläre Ausdrücke, bei denen es sich um Ein- oder Ausschlussmuster handelt, die als Filter bezeichnet werden. Wenn Sie einen Einschlussfilter angeben, werden nur Inhalte indexiert, die dem Einschlussfilter entsprechen. Jedes Dokument, das nicht dem Einschlussfilter entspricht, wird nicht

indexiert. Wenn Sie einen Ein- und Ausschlussfilter angeben, werden Dokumente, die dem Ausschlussfilter entsprechen, nicht indexiert, auch wenn sie dem Einschlussfilter entsprechen.

- Benutzerkontextfilterung und Zugriffskontrolle —Amazon Kendra durchsucht die Zugriffskontrollliste (ACL) für Ihre Dokumente, sofern Sie über eine ACL für Ihre Dokumente verfügen. Die ACL-Informationen werden verwendet, um Suchergebnisse nach dem Benutzer- oder Gruppenzugriff auf Dokumente zu filtern. Weitere Informationen finden Sie unter Benutzerkontextfilterung.
- Feldzuordnungen — Wählen Sie aus, ob Sie Ihre Gmail-Datenquellenfelder Ihren Amazon Kendra Indexfeldern zuordnen möchten. Weitere Informationen finden Sie unter Zuweisen von Datenquellenfeldern.

> **Note**
>
> Das Textfeld oder das entsprechende Textfeld für Ihre Dokumente ist erforderlich, um Ihre Dokumente durchsuchen Amazon Kendra zu können. Sie müssen den Feldnamen Ihres Dokumenthauptteils in Ihrer Datenquelle dem Namen des Indexfeldes zuordnen_`document_body`. Alle anderen Felder sind optional.

> **Note**
>
> Amazon Kendra Der Gmail-Datenquellen-Connector unterstützt die Erstellung von benutzerdefinierten Indexfeldern aufgrund von API-Einschränkungen nicht.

Weitere Informationen

Weitere Informationen zur Integration Amazon Kendra mit Ihrer Gmail-Datenquelle finden Sie unter:

- Führen Sie mithilfe des Gmail-Connectors für eine intelligente Suche in allen E-Mails in Ihrem Google-Workspace durch Amazon Kendra.

Hinweise

- Da es keine API zum Aktualisieren dauerhaft gelöschter Gmail-Nachrichten gibt, erfolgt die Synchronisation mit**`FULL_CRAWL`**//Neue, geänderte oder gelöschte Inhalte:
  - Nachrichten, die dauerhaft aus Gmail gelöscht wurden, werden nicht aus Ihrem Amazon Kendra Index entfernt
  - Synchronisiert keine Änderungen an Gmail-E-Mail-Labels

  Um die Änderungen an den Labels Ihrer Gmail-Datenquelle und dauerhaft gelöschte E-Mail-Nachrichten mit Ihrem Amazon Kendra Index zu synchronisieren, müssen Sie regelmäßig vollständige Crawls ausführen.
- Amazon Kendra Der Gmail-Datenquellen-Connector unterstützt die Erstellung von benutzerdefinierten Indexfeldern aufgrund von API-Einschränkungen nicht.

Google Drive

Google Drive ist ein Cloud-basierter Dateispeicherdienst. Sie können ihn verwenden Amazon Kendra , um Dokumente zu indizieren, die in den Ordnern „Geteilte Ablagen“, „Meine Ablagen“ und „Für mich freigegeben“ in Ihrer Google Drive-Datenquelle gespeichert sind. Sie können sowohl Google Workspace-Dokumente als auch Dokumente indizieren, die unter Dokumentationstypen aufgeführt sind. Sie können auch Inklusions- und Ausschlussfilter verwenden, um Inhalte nach Dateiname, Dateityp und Dateipfad zu indizieren.

Sie können über Amazon Kendra die Amazon Kendra Konsole, die API oder die TemplateConfigurationAPI eine Verbindung zu Ihrer Google Drive-Datenquelle herstellen. GoogleDriveConfiguration

Amazon Kendra hat zwei Versionen des Google Drive-Connectors. Zu den unterstützten Funktionen jeder Version gehören:

Google Drive-Konnektor V1.0/ API GoogleDriveConfiguration

- Feldzuordnungen
- Steuerung des Benutzerzugriffs
- Einschluss-/Ausschlussfilter

Google Drive-Konnektor V2.0/API TemplateConfiguration

- Feldzuordnungen
- Steuerung des Benutzerzugriffs
- Einschluss-/Ausschlussfilter
- Vollständige und inkrementelle Inhaltssynchronisierung
- Virtual Private Cloud (VPC)

> **Note**
>
> Die Support für Google Drive Connector V1.0/Google DriveConfiguration API wird voraussichtlich 2023 enden. Wir empfehlen, zu Google Drive Connector V2.0/ API zu migrieren oder diesen zu verwenden. TemplateConfiguration

Informationen zur Fehlerbehebung bei Ihrem Amazon Kendra Google Drive-Datenquellen-Connector finden Sie unter. Problembehandlung bei Datenquellen

Themen

- Google Drive-Konnektor V1.0
- Google Drive-Anschluss V2.0

Google Drive-Konnektor V1.0

Google Drive ist ein Cloud-basierter Dateispeicherdienst. Sie können ihn verwenden Amazon Kendra , um Dokumente und Kommentare zu indizieren, die in den Ordnern „Geteilte Ablagen“, „Meine Ablagen“ und „Für mich freigegeben“ in Ihrer Google Drive-Datenquelle gespeichert sind. Sie können Google Workspace-Dokumente sowie Dokumente indizieren, die unter Dokumentationstypen aufgeführt sind. Sie können auch Inklusions- und Ausschlussfilter verwenden, um Inhalte nach Dateiname, Dateityp und Dateipfad zu indizieren.

> **Note**
>
> Die Support für Google Drive Connector V1.0/Google DriveConfiguration API wird voraussichtlich 2023 enden. Wir empfehlen, zu Google Drive Connector V2.0/ API zu migrieren oder diesen zu verwenden. TemplateConfiguration

Informationen zur Fehlerbehebung bei Ihrem Amazon Kendra Google Drive-Datenquellen-Connector finden Sie unter. Problembehandlung bei Datenquellen

Themen

Unterstützte Features

- Feldzuordnungen
- Steuerung des Benutzerzugriffs
- Einschluss-/Ausschlussfilter

Voraussetzungen

Bevor Sie Ihre Google Drive-Datenquelle Amazon Kendra zum Indizieren verwenden können, nehmen Sie diese Änderungen in Ihrem Google Drive und Ihren Konten vor. AWS

Stellen Sie in Google Drive sicher, dass Sie über Folgendes verfügen:

- Entweder wurde der Zugriff durch eine Super-Admin-Rolle gewährt oder Sie sind ein Benutzer mit Administratorrechten. Sie benötigen keine Super-Admin-Rolle für sich selbst, wenn Ihnen der Zugriff durch eine Super-Admin-Rolle gewährt wurde.
- Mit dem Konto wurde ein Dienstkonto mit aktivierter Option Domänenweite G Suite-Delegierung aktivieren und ein JSON-Schlüssel als privater Schlüssel erstellt.
- Die E-Mail-Adresse Ihres Benutzerkontos und die E-Mail-Adresse Ihres Dienstkontos wurden kopiert. Wenn Sie eine Verbindung herstellen, geben Amazon Kendra Sie die E-Mail-Adresse Ihres Benutzerkontos als Administratorkonto-E-Mail und die E-Mail-Adresse Ihres Dienstkontos als Kunden-E-Mail in Ihrem Secrets Manager Geheimen ein.
- Admin-SDK-API und Google Drive-API wurden zu Ihrem Konto hinzugefügt.
- Die folgenden Berechtigungen wurden Ihrem Dienstkonto mithilfe einer Super-Admin-Rolle hinzugefügt (oder ein Benutzer mit einer Super-Admin-Rolle wurde gebeten, sie hinzuzufügen):
  - 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
- Vergewissert, dass jedes Dokument in Google Drive und in anderen Datenquellen, die Sie für denselben Index verwenden möchten, einzigartig ist. Jede Datenquelle, die Sie für einen Index verwenden möchten, darf nicht dasselbe Dokument in allen Datenquellen enthalten. Dokument-IDs gelten für einen Index global und müssen pro Index eindeutig sein.

Stellen Sie sicher AWS-Konto, dass Sie Folgendes in Ihrem haben:

- Hat einen Amazon Kendra Index erstellt und bei Verwendung der API die Index-ID notiert.
- Sie haben eine IAM Rolle für Ihre Datenquelle erstellt und, falls Sie die API verwenden, den ARN der IAM Rolle notiert.

> **Note**
>
> Wenn Sie Ihren Authentifizierungstyp und Ihre Anmeldeinformationen ändern, müssen Sie Ihre IAM Rolle aktualisieren, um auf die richtige AWS Secrets Manager geheime ID zugreifen zu können.

- Haben Ihre Google Drive-Authentifizierungsdaten AWS Secrets Manager geheim gespeichert und, falls Sie die API verwenden, den ARN des Geheimnisses notiert.

> **Note**
>
> Wir empfehlen Ihnen, Ihre Anmeldedaten und Ihr Passwort regelmäßig zu aktualisieren oder zu wechseln. Stellen Sie zu Ihrer eigenen Sicherheit nur die Zugriffsebene bereit, die erforderlich ist. Wir raten davon ab, Anmeldeinformationen und geheime Daten für alle Datenquellen und Connector-Versionen 1.0 und 2.0 (sofern zutreffend) wiederzuverwenden.

Wenn Sie noch keine IAM Rolle oder keinen Schlüssel haben, können Sie die Konsole verwenden, um eine neue IAM Rolle und ein neues Secrets Manager Geheimnis zu erstellen, wenn Sie Ihre Google Drive-Datenquelle mit verbinden. Amazon Kendra Wenn Sie die API verwenden, müssen Sie

den ARN einer vorhandenen IAM Rolle und eines Secrets Manager Geheimnisses sowie eine Index-ID angeben.

Anweisungen zur Verbindung

Um eine Verbindung Amazon Kendra zu Ihrer Google Drive-Datenquelle herzustellen, müssen Sie die erforderlichen Details zu Ihrer Google Drive-Datenquelle angeben, damit Sie auf Ihre Daten zugreifen Amazon Kendra können. Wenn Sie Google Drive noch nicht konfiguriert haben, Amazon Kendra sehen Sie nachVoraussetzungen.

Console

Um eine Verbindung Amazon Kendra zu Google Drive herzustellen

1. Melden Sie sich bei der AWS Management Console an und öffnen Sie die Amazon Kendra Konsole.
2. Wählen Sie im linken Navigationsbereich Indizes und dann den Index, den Sie verwenden möchten, aus der Indexliste aus.

> **Note**
>
> Sie können Ihre Einstellungen für die Benutzerzugriffskontrolle unter Indexeinstellungen konfigurieren oder bearbeiten.

3. Wählen Sie auf der Seite Erste Schritte die Option Datenquelle hinzufügen aus.
4. Wählen Sie auf der Seite Datenquelle hinzufügen die Option Google Drive-Connector V1.0 und dann Connector hinzufügen aus.
5. Geben Sie auf der Seite „Datenquellendetails angeben“ die folgenden Informationen ein:

   a. Geben Sie im Feld Name und Beschreibung für Datenquellenname einen Namen für Ihre Datenquelle ein. Sie können Bindestriche, aber keine Leerzeichen verwenden.

   b. (Optional) Beschreibung — Geben Sie eine optionale Beschreibung für Ihre Datenquelle ein.

   c. In Standardsprache — Wählen Sie eine Sprache aus, um Ihre Dokumente nach dem Index zu filtern. Sofern Sie nichts anderes angeben, ist die Standardsprache Englisch. Die in den Metadaten des Dokuments angegebene Sprache hat Vorrang vor der ausgewählten Sprache.

d. Unter Tags für Neues Tag hinzufügen — Fügen Sie optionale Tags hinzu, um Ihre Ressourcen zu durchsuchen und zu filtern oder Ihre Kosten nachzuverfolgen. AWS

e. Wählen Sie Weiter aus.

6. Geben Sie auf der Seite Zugriff und Sicherheit definieren die folgenden Informationen ein:

a. Als Authentifizierungstyp — Wählen Sie zwischen „Bestehend“ und „Neu“. Wenn Sie ein vorhandenes Geheimnis verwenden möchten, verwenden Sie Select Secret, um Ihr Geheimnis auszuwählen.

b. Wenn Sie ein neues Geheimnis erstellen möchten, wird eine AWS Secrets Manager geheime Option geöffnet.

- Geben Sie die folgenden Informationen in das Fenster Create an AWS Secrets Manager Secret ein:

A. Geheimer Name — Ein Name für Ihr Geheimnis. Das Präfix 'AmazonKendra-Google Drive-' wird Ihrem geheimen Namen automatisch hinzugefügt.

B. Für Admin-Konto-E-Mail, Kunden-E-Mail und privaten Schlüssel: Geben Sie die Werte für die Authentifizierungsdaten ein, die Sie generiert und von Ihrem Google Drive-Konto heruntergeladen haben.

C. Wählen Sie Authentifizierung speichern aus.

c. IAM Rolle — Wählen Sie eine bestehende IAM Rolle oder erstellen Sie eine neue IAM Rolle, um auf Ihre Repository-Anmeldeinformationen und Indexinhalte zuzugreifen.

> **Note**
>
> IAM Rollen, die für Indizes verwendet werden, können nicht für Datenquellen verwendet werden. Wenn Sie sich nicht sicher sind, ob eine vorhandene Rolle für einen Index oder eine häufig gestellte Frage verwendet wird, wählen Sie Neue Rolle erstellen, um Fehler zu vermeiden.

d. Wählen Sie Weiter aus.

7. Geben Sie auf der Seite Synchronisierungseinstellungen konfigurieren die folgenden Informationen ein:

a. Benutzerkonten ausschließen — Die Google Drive-Nutzer, die Sie aus dem Index ausschließen möchten. Sie können bis zu 100 Benutzerkonten hinzufügen.

b. Geteilte Ablagen ausschließen — Die geteilten Google Drive-Ablagen, die Sie aus Ihrem Index ausschließen möchten. Sie können bis zu 100 geteilte Ablagen hinzufügen.

c. Laufwerke mit Dateitypen ausschließen — Die Google Drive-Dateitypen, die Sie aus Ihrem Index ausschließen möchten. Sie können sich auch dafür entscheiden, die MIME-Typauswahl zu bearbeiten.

d. Zusätzliche Konfigurationen — Reguläre Ausdrucksmuster zum Ein- oder Ausschließen bestimmter Inhalte. Sie können bis zu 100 Muster hinzufügen.

e. Häufigkeit — Wie oft Amazon Kendra wird die Synchronisierung mit Ihrer Datenquelle durchgeführt?

f. Wählen Sie Weiter aus.

8. Geben Sie auf der Seite Feldzuordnungen festlegen die folgenden Informationen ein:

a. Für GoogleDrive Feldnamen und Zusätzliche vorgeschlagene Feldzuordnungen — Wählen Sie eines der Amazon Kendra generierten Standarddatenquellenfelder aus, die Sie Ihrem Index zuordnen möchten.

b. Feld hinzufügen — Um benutzerdefinierte Datenquellenfelder hinzuzufügen, um einen Indexfeldnamen für die Zuordnung und den Felddatentyp zu erstellen.

c. Wählen Sie Weiter aus.

9. Überprüfen Sie auf der Seite Überprüfen und erstellen, ob die von Ihnen eingegebenen Informationen korrekt sind, und wählen Sie dann Datenquelle hinzufügen aus. Sie können Ihre Informationen auch auf dieser Seite bearbeiten. Ihre Datenquelle wird auf der Seite Datenquellen angezeigt, nachdem die Datenquelle erfolgreich hinzugefügt wurde.

API

Um eine Verbindung Amazon Kendra zu Google Drive herzustellen

Mithilfe der GoogleDriveConfigurationAPI müssen Sie Folgendes angeben:

- Geheimer Amazon-Ressourcenname (ARN) — Geben Sie den Amazon-Ressourcennamen (ARN) eines Secrets Manager Geheimnisses ein, das die Authentifizierungsdaten für Ihr Google Drive-Konto enthält. Das Geheimnis wird in einer JSON-Struktur mit den folgenden Schlüsseln gespeichert:

```
{
    "clientAccount": "service account email",
```

```
    "adminAccount": "user account email"",
    "privateKey": "private key"
}
```

> **Note**
>
> Wir empfehlen Ihnen, Ihre Anmeldeinformationen und Ihr Geheimnis regelmäßig zu aktualisieren oder zu wechseln. Stellen Sie zu Ihrer eigenen Sicherheit nur die Zugriffsebene bereit, die erforderlich ist. Wir raten davon ab, Anmeldeinformationen und geheime Daten für alle Datenquellen und Connector-Versionen 1.0 und 2.0 (sofern zutreffend) wiederzuverwenden.

- IAM Rolle — Geben Sie an`RoleArn`, wann Sie anrufen`CreateDataSource`, um einer IAM Rolle Berechtigungen für den Zugriff auf Ihr Secrets Manager Geheimnis und für den Aufruf der erforderlichen öffentlichen APIs für den Google Drive-Connector und zu erteilen. Amazon Kendra Weitere Informationen finden Sie unter IAM Rollen für Google Drive-Datenquellen.

Sie können auch die folgenden optionalen Funktionen hinzufügen:

- Inklusions- und Ausschlussfilter — Amazon Kendra Indiziert standardmäßig alle Dokumente in Google Drive. Sie können angeben, ob bestimmte Inhalte in geteilten Ablagen, Benutzerkonten, MIME-Typen für Dokumente und Dateien ein- oder ausgeschlossen werden sollen. Wenn Sie Benutzerkonten ausschließen, wird keine der Dateien in „Meine Ablage“, die dem Konto gehören, indexiert. Mit dem Nutzer geteilte Dateien werden indexiert, es sei denn, der Eigentümer der Datei wird ebenfalls ausgeschlossen.

> **Note**
>
> Die meisten Datenquellen verwenden Muster für reguläre Ausdrücke, bei denen es sich um Ein- oder Ausschlussmuster handelt, die als Filter bezeichnet werden. Wenn Sie einen Einschlussfilter angeben, werden nur Inhalte indexiert, die dem Einschlussfilter entsprechen. Jedes Dokument, das nicht dem Einschlussfilter entspricht, wird nicht indexiert. Wenn Sie einen Ein- und Ausschlussfilter angeben, werden Dokumente, die dem Ausschlussfilter entsprechen, nicht indexiert, auch wenn sie dem Einschlussfilter entsprechen.

- Feldzuordnungen — Wählen Sie diese Option, um Ihre Google Drive-Datenquellenfelder Ihren Indexfeldern zuzuordnen. Amazon Kendra Weitere Informationen finden Sie unter Zuweisen von Datenquellenfeldern.

  > **Note**
  >
  > Das Textfeld oder das entsprechende Textfeld für Ihre Dokumente ist erforderlich, um Ihre Dokumente durchsuchen Amazon Kendra zu können. Sie müssen den Feldnamen Ihres Dokumenthauptteils in Ihrer Datenquelle dem Namen des Indexfeldes zuordnen`_document_body`. Alle anderen Felder sind optional.

- Benutzerkontextfilterung und ZugriffskontrolleAmazon Kendra — durchsucht die Zugriffskontrollliste (ACL) für Ihre Dokumente, sofern Sie über eine ACL für Ihre Dokumente verfügen. Die ACL-Informationen werden verwendet, um Suchergebnisse nach dem Benutzer- oder Gruppenzugriff auf Dokumente zu filtern. Weitere Informationen finden Sie unter Benutzerkontextfilterung.

Weitere Informationen

Weitere Informationen zur Integration Amazon Kendra mit Ihrer Google Drive-Datenquelle finden Sie unter:

- Erste Schritte mit dem Amazon Kendra Google Drive-Connector

Google Drive-Anschluss V2.0

Google Drive ist ein Cloud-basierter Dateispeicherdienst. Sie können ihn verwenden Amazon Kendra , um Dokumente und Kommentare zu indizieren, die in den Ordnern „Geteilte Ablagen“, „Meine Ablagen“ und „Für mich freigegeben“ in Ihrer Google Drive-Datenquelle gespeichert sind. Sie können Google Workspace-Dokumente sowie Dokumente indizieren, die unter Dokumentationstypen aufgeführt sind. Sie können auch Inklusions- und Ausschlussfilter verwenden, um Inhalte nach Dateiname, Dateityp und Dateipfad zu indizieren.

> **Note**
>
> Die Support für Google Drive Connector V1.0/Google DriveConfiguration API wird voraussichtlich 2023 enden. Wir empfehlen, zu Google Drive Connector V2.0/ API zu migrieren oder diesen zu verwenden. TemplateConfiguration

Informationen zur Fehlerbehebung bei Ihrem Amazon Kendra Google Drive-Datenquellen-Connector finden Sie unter. Problembehandlung bei Datenquellen

Themen

Unterstützte Features

- Feldzuordnungen
- Steuerung des Benutzerzugriffs
- Einschluss-/Ausschlussfilter
- Vollständige und inkrementelle Inhaltssynchronisierung
- Virtual Private Cloud (VPC)

Voraussetzungen

Bevor Sie Ihre Google Drive-Datenquelle Amazon Kendra zum Indizieren verwenden können, müssen Sie diese Änderungen in Ihrem Google Drive und AWS Ihren Konten vornehmen.

Stellen Sie in Google Drive sicher, dass Sie über Folgendes verfügen:

- Entweder wurde der Zugriff durch eine Super-Admin-Rolle gewährt oder Sie sind ein Benutzer mit Administratorrechten. Sie benötigen keine Super-Admin-Rolle für sich selbst, wenn Ihnen der Zugriff durch eine Super-Admin-Rolle gewährt wurde.
- Die Verbindungsdaten für das Google Drive-Dienstkonto wurden konfiguriert, die die E-Mail-Adresse Ihres Administratorkontos, die Kunden-E-Mail-Adresse (E-Mail-Adresse des

Dienstkontos) und den privaten Schlüssel enthalten. Informationen zum Erstellen und Löschen von Dienstkontoschlüsseln finden Sie in der Google Cloud-Dokumentation.

- Es wurde ein Google Cloud-Dienstkonto (ein Konto mit delegierter Befugnis zur Annahme einer Benutzeridentität) mit aktivierter Option Domänenweite G Suite-Delegierung aktivieren für die server-to-server Authentifizierung erstellt und anschließend mithilfe des Kontos ein privater JSON-Schlüssel generiert.

> **Note**
>
> Der private Schlüssel sollte nach der Erstellung des Dienstkontos generiert werden.

- Admin SDK API und Google Drive API zu Ihrem Benutzerkonto hinzugefügt.
- Optional: Konfigurierte Google Drive OAuth 2.0-Verbindungsanmeldedaten, die Client-ID, Client-Geheimnis und Aktualisierungstoken als Verbindungsanmeldeinformationen für einen bestimmten Benutzer enthalten. Sie benötigen dies, um einzelne Kontodaten zu crawlen. Informationen zur Verwendung von OAuth 2.0 für den Zugriff auf APIs finden Sie in der Google-Dokumentation.
- Die folgenden OAuth-Bereiche wurden Ihrem Dienstkonto mithilfe einer Super-Admin-Rolle hinzugefügt (oder ein Nutzer mit einer Super-Admin-Rolle wurde gebeten, sie hinzuzufügen). Diese API-Bereiche werden benötigt, um alle Dokumente und Informationen zur Zugriffskontrolle (ACL) für alle Nutzer in einer Google Workspace-Domain zu crawlen:
  - https://www.googleapis.com/auth/drive.readonly—View und laden Sie all Ihre Google Drive-Dateien herunter
  - https://www.googleapis.com/auth/drive.metadata.readonly—View Metadaten für Dateien in Ihrem Google Drive
  - https://www.googleapis.com/auth/admin.directory.group.readonly—Scope, um nur Gruppen-, Gruppenalias- und Mitgliederinformationen abzurufen. Dies wird für den Amazon Kendra Identity Crawler benötigt.
  - https://www.googleapis.com/auth/admin.directory.user.readonly—Scope, um nur Benutzer oder Benutzeraliase abzurufen. Dies ist erforderlich, um Benutzer im Amazon Kendra Identity Crawler aufzulisten und ACLs festzulegen.
  - https://www.googleapis.com/auth/cloud-platform—Scope zum Generieren eines Zugriffstokens zum Abrufen von Inhalten großer Google Drive-Dateien.
  - https://www.googleapis.com/auth/forms.body.readonly—Scope zum Abrufen von Daten aus Google Forms.

Um die Forms-API zu unterstützen, fügen Sie den folgenden zusätzlichen Bereich hinzu:

  - https://www.googleapis.com/auth/forms.body.readonly
- Vergewissert, dass jedes Dokument in Google Drive und in anderen Datenquellen, die Sie für denselben Index verwenden möchten, einzigartig ist. Jede Datenquelle, die Sie für einen Index verwenden möchten, darf nicht dasselbe Dokument in allen Datenquellen enthalten. Dokument-IDs gelten für einen Index global und müssen pro Index eindeutig sein.

Stellen Sie sicher AWS-Konto, dass Sie Folgendes in Ihrem haben:

- Hat einen Amazon Kendra Index erstellt und bei Verwendung der API die Index-ID notiert.
- Sie haben eine IAM Rolle für Ihre Datenquelle erstellt und, falls Sie die API verwenden, den ARN der IAM Rolle notiert.

> **Note**
>
> Wenn Sie Ihren Authentifizierungstyp und Ihre Anmeldeinformationen ändern, müssen Sie Ihre IAM Rolle aktualisieren, um auf die richtige AWS Secrets Manager geheime ID zugreifen zu können.

- Haben Ihre Google Drive-Authentifizierungsdaten AWS Secrets Manager geheim gespeichert und, falls Sie die API verwenden, den ARN des Geheimnisses notiert.

> **Note**
>
> Wir empfehlen Ihnen, Ihre Anmeldedaten und Ihr Passwort regelmäßig zu aktualisieren oder zu wechseln. Stellen Sie zu Ihrer eigenen Sicherheit nur die Zugriffsebene bereit, die erforderlich ist. Wir raten davon ab, Anmeldeinformationen und geheime Daten für alle Datenquellen und Connector-Versionen 1.0 und 2.0 (sofern zutreffend) wiederzuverwenden.

Wenn Sie noch keine IAM Rolle oder keinen Schlüssel haben, können Sie die Konsole verwenden, um eine neue IAM Rolle und ein neues Secrets Manager Geheimnis zu erstellen, wenn Sie Ihre Google Drive-Datenquelle mit verbinden. Amazon Kendra Wenn Sie die API verwenden, müssen Sie den ARN einer vorhandenen IAM Rolle und eines Secrets Manager Geheimnisses sowie eine Index-ID angeben.

Anweisungen zur Verbindung

Um eine Verbindung Amazon Kendra zu Ihrer Google Drive-Datenquelle herzustellen, müssen Sie die erforderlichen Details zu Ihrer Google Drive-Datenquelle angeben, damit Sie auf Ihre Daten zugreifen Amazon Kendra können. Wenn Sie Google Drive noch nicht konfiguriert haben, Amazon Kendra sehen Sie nachVoraussetzungen.

Console

Um eine Verbindung Amazon Kendra zu Google Drive herzustellen

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die Amazon Kendra Konsole.
2. Wählen Sie im linken Navigationsbereich Indizes und dann den Index, den Sie verwenden möchten, aus der Indexliste aus.

> **Note**
>
> Sie können Ihre Einstellungen für die Benutzerzugriffskontrolle unter Indexeinstellungen konfigurieren oder bearbeiten.

3. Wählen Sie auf der Seite Erste Schritte die Option Datenquelle hinzufügen aus.
4. Wählen Sie auf der Seite Datenquelle hinzufügen die Option Google Drive-Connector und dann Connector hinzufügen aus.
5. Geben Sie auf der Seite „Datenquellendetails angeben“ die folgenden Informationen ein:
   a. Geben Sie im Feld Name und Beschreibung für Datenquellenname einen Namen für Ihre Datenquelle ein. Sie können Bindestriche, aber keine Leerzeichen verwenden.
   b. (Optional) Beschreibung — Geben Sie eine optionale Beschreibung für Ihre Datenquelle ein.
   c. In Standardsprache — Wählen Sie eine Sprache aus, um Ihre Dokumente nach dem Index zu filtern. Sofern Sie nichts anderes angeben, ist die Standardsprache Englisch. Die in den Metadaten des Dokuments angegebene Sprache hat Vorrang vor der ausgewählten Sprache.
   d. Unter Tags für Neues Tag hinzufügen — Fügen Sie optionale Tags hinzu, um Ihre Ressourcen zu durchsuchen und zu filtern oder Ihre Kosten nachzuverfolgen. AWS
   e. Wählen Sie Weiter aus.

6. Geben Sie auf der Seite Zugriff und Sicherheit definieren die folgenden Informationen ein:

   a. Autorisierung — Aktivieren oder deaktivieren Sie die Informationen der Zugriffskontrollliste (ACL) für Ihre Dokumente, wenn Sie über eine ACL verfügen und diese für die Zugriffskontrolle verwenden möchten. Die ACL gibt an, auf welche Dokumente Benutzer und Gruppen zugreifen können. Die ACL-Informationen werden verwendet, um Suchergebnisse nach dem Benutzer- oder Gruppenzugriff auf Dokumente zu filtern. Weitere Informationen finden Sie unter Benutzerkontextfilterung.

   b. Zur Authentifizierung — Wählen Sie je nach Anwendungsfall zwischen Google-Dienstkonto und OAuth 2.0-Authentifizierung.

   c. AWS Secrets Manager geheim — Wählen Sie ein vorhandenes Geheimnis oder erstellen Sie ein neues Secrets Manager Geheimnis, um Ihre Google Drive-Authentifizierungsdaten zu speichern. Wenn Sie ein neues Geheimnis erstellen möchten, wird ein AWS Secrets Manager geheimes Fenster geöffnet.

      i. Wenn Sie sich für ein Google-Dienstkonto entschieden haben, geben Sie einen Namen für Ihr Geheimnis, die E-Mail-ID des Administratorbenutzers oder „Dienstkontonutzers“ in Ihrer Dienstkontokonfiguration (Admin-E-Mail), die E-Mail-ID des Dienstkontos (Kunden-E-Mail) und den privaten Schlüssel ein, den Sie in Ihrem Dienstkonto erstellt haben.

         Speichern Sie Ihr Geheimnis und fügen Sie es hinzu

      ii. Wenn Sie sich für die OAuth 2.0-Authentifizierung entschieden haben, geben Sie einen Namen für Ihr Geheimnis, Ihre Client-ID, Ihr Client-Geheimnis und das Aktualisierungstoken ein, das Sie in Ihrem OAuth-Konto erstellt haben.

         Speichern Sie Ihr Geheimnis und fügen Sie es hinzu.

   d. Virtual Private Cloud (VPC) — Sie können wählen, ob Sie eine VPC verwenden möchten. In diesem Fall müssen Sie Subnetze und VPC-Sicherheitsgruppen hinzufügen.

   e. (Nur für Nutzer der Google-Dienstkontoauthentifizierung)

      Identity Crawler — Geben Sie an, ob der Identity Crawler aktiviert Amazon Kendra werden soll. Der Identity Crawler verwendet die Informationen der Zugriffskontrollliste (ACL) für Ihre Dokumente, um Suchergebnisse nach dem Benutzer- oder Gruppenzugriff auf Dokumente zu filtern. Wenn Sie über eine ACL für Ihre Dokumente verfügen und Ihre ACL verwenden möchten, können Sie auch den Identity Crawler aktivieren, um die Benutzerkontextfilterung von Suchergebnissen zu konfigurieren. Amazon

Kendra Andernfalls können alle Dokumente öffentlich durchsucht werden, wenn Identity Crawler ausgeschaltet ist. Wenn Sie die Zugriffskontrolle für Ihre Dokumente verwenden möchten und Identity Crawler ausgeschaltet ist, können Sie alternativ die PutPrincipalMappingAPI verwenden, um Benutzer- und Gruppenzugriffsinformationen für die Benutzerkontextfilterung hochzuladen.

f. IAM Rolle — Wählen Sie eine bestehende IAM Rolle oder erstellen Sie eine neue IAM Rolle, um auf Ihre Repository-Anmeldeinformationen und Indexinhalte zuzugreifen.

> **Note**
>
> IAM Rollen, die für Indizes verwendet werden, können nicht für Datenquellen verwendet werden. Wenn Sie sich nicht sicher sind, ob eine vorhandene Rolle für einen Index oder eine häufig gestellte Frage verwendet wird, wählen Sie Neue Rolle erstellen, um Fehler zu vermeiden.

g. Wählen Sie Weiter aus.

7. Geben Sie auf der Seite Synchronisierungseinstellungen konfigurieren die folgenden Informationen ein:

   a. Inhalte synchronisieren — Wählen Sie aus, welche Optionen oder Inhalte Sie crawlen möchten. Sie können wählen, ob Sie Meine Ablage (persönliche Ordner), Geteilte Ablage (für Sie geteilte Ordner) oder beides crawlen möchten. Sie können auch Dateikommentare hinzufügen.

   b. Unter Zusätzliche Konfiguration — optional können Sie auch die folgenden optionalen Informationen eingeben:

      i. Zielgruppen — Fügen Sie spezifische Zielgruppen für die Dokumente hinzu, die Sie crawlen möchten.

      ii. Maximale Dateigröße — Legen Sie die maximale Größenbeschränkung für zu durchforstende Dateien in MB fest.

      iii. Benutzer-E-Mail — Fügen Sie Benutzer-E-Mails hinzu, die Sie ein- oder ausschließen möchten.

      iv. Geteilte Ablagen — Fügen Sie die Namen der geteilten Ablagen hinzu, die Sie ein- oder ausschließen möchten.

      v. MIME-Typen — Fügen Sie MIME-Typen hinzu, die Sie ein- oder ausschließen möchten.

vi. Regex-Muster für Entitäten — Fügen Sie Muster für reguläre Ausdrücke hinzu, um bestimmte Anlagen für alle unterstützten Entitäten ein- oder auszuschließen. Sie können bis zu 100 Muster hinzufügen.

c. Synchronisierungsmodus — Wählen Sie aus, wie Sie Ihren Index aktualisieren möchten, wenn sich der Inhalt Ihrer Datenquelle ändert. Wenn Sie Ihre Datenquelle Amazon Kendra zum ersten Mal synchronisieren, werden alle Inhalte standardmäßig gecrawlt und indexiert. Sie müssen eine vollständige Synchronisierung Ihrer Daten durchführen, falls Ihre erste Synchronisierung fehlgeschlagen ist, auch wenn Sie die Option Vollsynchronisierung nicht als Synchronisierungsmodusoption wählen.

- Vollständige Synchronisierung: Indizieren Sie den gesamten Inhalt neu und ersetzen die vorhandenen Inhalte jedes Mal, wenn Ihre Datenquelle mit Ihrem Index synchronisiert wird.
- Neue, geänderte Synchronisierung: Indizieren Sie jedes Mal, wenn Ihre Datenquelle mit Ihrem Index synchronisiert wird, nur neue und geänderte Inhalte. Amazon Kendra kann den Mechanismus Ihrer Datenquelle verwenden, um Inhaltsänderungen nachzuverfolgen und Inhalte zu indexieren, die sich seit der letzten Synchronisierung geändert haben.
- Neue, geänderte, gelöschte Synchronisierung: Indizieren Sie bei jeder Synchronisierung Ihrer Datenquelle mit Ihrem Index nur neue, geänderte und gelöschte Inhalte. Amazon Kendra kann den Mechanismus Ihrer Datenquelle verwenden, um Inhaltsänderungen nachzuverfolgen und Inhalte zu indexieren, die sich seit der letzten Synchronisierung geändert haben.

> **Important**
>
> Die Google Drive-API unterstützt das Abrufen von Kommentaren aus einer dauerhaft gelöschten Datei nicht. Kommentare aus gelöschten Dateien können abgerufen werden. Wenn eine Datei in den Papierkorb verschoben wird, löscht der Connector Kommentare aus dem Index. Amazon Kendra

d. Wählen Sie im Zeitplan für die Synchronisierungsausführung für Häufigkeit aus, wie oft Ihre Datenquelleninhalte synchronisiert und Ihr Index aktualisiert werden soll.

e. Wählen Sie im Synchronisierungslaufverlauf aus, ob Amazon S3 beim Synchronisieren Ihrer Datenquelle automatisch generierte Berichte in einer gespeichert werden sollen. Dies ist nützlich, um Probleme beim Synchronisieren Ihrer Datenquelle nachzuverfolgen.

f. Wählen Sie Weiter aus.

8. Geben Sie auf der Seite Feldzuordnungen festlegen die folgenden Informationen ein:

   a. Für Dateien — Wählen Sie aus den Amazon Kendra generierten Standard-Datenquellenfeldern aus, die Sie Ihrem Index zuordnen möchten.

   > **Note**
   >
   > Die Google Drive-API unterstützt das Erstellen benutzerdefinierter Felder nicht. Die Zuordnung benutzerdefinierter Felder ist für den Google Drive-Connector nicht verfügbar.

   b. Wählen Sie Weiter aus.

9. Überprüfen Sie auf der Seite Überprüfen und erstellen, ob die von Ihnen eingegebenen Informationen korrekt sind, und wählen Sie dann Datenquelle hinzufügen aus. Sie können Ihre Informationen auch auf dieser Seite bearbeiten. Ihre Datenquelle wird auf der Seite Datenquellen angezeigt, nachdem die Datenquelle erfolgreich hinzugefügt wurde.

API

Um eine Verbindung Amazon Kendra zu Google Drive herzustellen

Sie müssen mithilfe der TemplateConfigurationAPI ein JSON des Datenquellenschemas angeben. Sie müssen die folgenden Informationen angeben:

- Datenquelle — Geben Sie den Datenquellentyp wie `GOOGLEDRIVEV2` bei der Verwendung des TemplateConfigurationJSON-Schemas an. Geben Sie außerdem die Datenquelle so an`TEMPLATE`, wie Sie die CreateDataSourceAPI aufrufen.
- Authentifizierungstyp — Geben Sie an, ob die Dienstkontoauthentifizierung oder die OAuth 2.0-Authentifizierung verwendet werden soll.
- Synchronisierungsmodus — Geben Sie an, wie Ihr Index aktualisiert Amazon Kendra werden soll, wenn sich der Inhalt Ihrer Datenquelle ändert. Wenn Sie Ihre Datenquelle Amazon Kendra zum ersten Mal synchronisieren, werden alle Inhalte standardmäßig gecrawlt und indexiert. Sie müssen eine vollständige Synchronisierung Ihrer Daten durchführen, falls Ihre erste Synchronisierung fehlgeschlagen ist, auch wenn Sie die Option Vollsynchronisierung nicht als Synchronisierungsmodusoption wählen. Sie können wählen zwischen:

- `FORCED_FULL_CRAWL`um den gesamten Inhalt neu zu indizieren und vorhandene Inhalte jedes Mal zu ersetzen, wenn Ihre Datenquelle mit Ihrem Index synchronisiert wird.
- `FULL_CRAWL`um bei jeder Synchronisierung Ihrer Datenquelle mit Ihrem Index nur neue, geänderte und gelöschte Inhalte zu indizieren. Amazon Kendra kann den Mechanismus Ihrer Datenquelle verwenden, um Inhaltsänderungen nachzuverfolgen und Inhalte zu indexieren, die sich seit der letzten Synchronisierung geändert haben.
- `CHANGE_LOG`um jedes Mal, wenn Ihre Datenquelle mit Ihrem Index synchronisiert wird, nur neue und geänderte Inhalte zu indizieren. Amazon Kendra kann den Mechanismus Ihrer Datenquelle verwenden, um Inhaltsänderungen nachzuverfolgen und Inhalte zu indexieren, die sich seit der letzten Synchronisierung geändert haben.

> **Important**
>
> Die Google Drive-API unterstützt das Abrufen von Kommentaren aus einer dauerhaft gelöschten Datei nicht. Kommentare aus gelöschten Dateien können abgerufen werden. Wenn eine Datei in den Papierkorb verschoben wird, löscht der Connector Kommentare aus dem Index. Amazon Kendra

- Geheimer Amazon-Ressourcenname (ARN) — Geben Sie den Amazon-Ressourcennamen (ARN) eines Secrets Manager Geheimnisses ein, das die Authentifizierungsdaten enthält, die Sie in Ihrem Google Drive-Konto erstellt haben. Wenn Sie die Google-Dienstkonto-Authentifizierung verwenden, wird das Geheimnis in einer JSON-Struktur mit den folgenden Schlüsseln gespeichert:

```
{
    "clientEmail": "user account email",
    "adminAccountEmail": "service account email",
    "privateKey": "private key"
}
```

Wenn Sie die OAuth 2.0-Authentifizierung verwenden, wird das Geheimnis in einer JSON-Struktur mit den folgenden Schlüsseln gespeichert:

```
{
    "clientID": "OAuth client ID",
    "clientSecret": "client secret",
    "refreshToken": "refresh token"
```

```
}
```

> **Note**
>
> Wir empfehlen Ihnen, Ihre Anmeldeinformationen und Ihr Geheimnis regelmäßig zu aktualisieren oder zu wechseln. Stellen Sie zu Ihrer eigenen Sicherheit nur die Zugriffsebene bereit, die erforderlich ist. Wir raten davon ab, Anmeldeinformationen und geheime Daten für alle Datenquellen und Connector-Versionen 1.0 und 2.0 (sofern zutreffend) wiederzuverwenden.

- IAM Rolle — Geben Sie an`RoleArn`, wann Sie anrufen`CreateDataSource`, um einer IAM Rolle Berechtigungen für den Zugriff auf Ihr Secrets Manager Geheimnis und für den Aufruf der erforderlichen öffentlichen APIs für den Google Drive-Connector und zu erteilen. Amazon Kendra Weitere Informationen finden Sie unter IAM Rollen für Google Drive-Datenquellen.

Sie können auch die folgenden optionalen Funktionen hinzufügen:

- Virtual Private Cloud (VPC) — Geben Sie an, `VpcConfiguration` wann Sie anrufen. `CreateDataSource` Weitere Informationen finden Sie unter Konfigurieren von Amazon Kendra für die Verwendung eines Amazon VPC.
- Meine Ablagen, Geteilte Ablagen, Kommentare — Sie können angeben, ob diese Arten von Inhalten gecrawlt werden sollen.
- Inklusions- und Ausschlussfilter — Sie können angeben, ob bestimmte Benutzerkonten, geteilte Ablagen und MIME-Typen ein- oder ausgeschlossen werden sollen.

> **Note**
>
> Die meisten Datenquellen verwenden Muster für reguläre Ausdrücke. Dabei handelt es sich um Ein- oder Ausschlussmuster, die als Filter bezeichnet werden. Wenn Sie einen Einschlussfilter angeben, werden nur Inhalte indexiert, die dem Einschlussfilter entsprechen. Jedes Dokument, das nicht dem Einschlussfilter entspricht, wird nicht indexiert. Wenn Sie einen Ein- und Ausschlussfilter angeben, werden Dokumente, die dem Ausschlussfilter entsprechen, nicht indexiert, auch wenn sie dem Einschlussfilter entsprechen.

- Zugriffskontrollliste (ACL) — Geben Sie an, ob die ACL-Informationen für Ihre Dokumente gecrawlt werden sollen, wenn Sie über eine ACL verfügen und diese für die Zugriffskontrolle

verwenden möchten. Die ACL gibt an, auf welche Dokumente Benutzer und Gruppen zugreifen können. Die ACL-Informationen werden verwendet, um Suchergebnisse nach dem Benutzer- oder Gruppenzugriff auf Dokumente zu filtern. Weitere Informationen finden Sie unter Benutzerkontextfilterung.

- Identity Crawler — Geben Sie an, ob der Identity Crawler aktiviert Amazon Kendra werden soll. Der Identity Crawler verwendet die Informationen der Zugriffskontrollliste (ACL) für Ihre Dokumente, um Suchergebnisse nach dem Benutzer- oder Gruppenzugriff auf Dokumente zu filtern. Wenn Sie über eine ACL für Ihre Dokumente verfügen und Ihre ACL verwenden möchten, können Sie auch den Identity Crawler aktivieren, um die Benutzerkontextfilterung von Suchergebnissen zu konfigurieren. Amazon Kendra Andernfalls können alle Dokumente öffentlich durchsucht werden, wenn Identity Crawler ausgeschaltet ist. Wenn Sie die Zugriffskontrolle für Ihre Dokumente verwenden möchten und Identity Crawler ausgeschaltet ist, können Sie alternativ die PutPrincipalMappingAPI verwenden, um Benutzer- und Gruppenzugriffsinformationen für die Benutzerkontextfilterung hochzuladen.
- Feldzuordnungen — Wählen Sie diese Option, um Ihre Google Drive-Datenquellenfelder Ihren Indexfeldern zuzuordnen. Amazon Kendra Weitere Informationen finden Sie unter Zuweisen von Datenquellenfeldern.

> **Note**
>
> Das Textfeld oder das entsprechende Textfeld für Ihre Dokumente ist erforderlich, um Ihre Dokumente durchsuchen Amazon Kendra zu können. Sie müssen den Feldnamen Ihres Dokumenthauptteils in Ihrer Datenquelle dem Namen des Indexfeldes zuordnen`_document_body`. Alle anderen Felder sind optional.

Eine Liste weiterer wichtiger JSON-Schlüssel, die konfiguriert werden müssen, finden Sie unter Google Drive-Vorlagenschema.

Hinweise

- Die Zuordnung benutzerdefinierter Felder ist für den Google Drive-Connector nicht verfügbar, da die Google Drive-Benutzeroberfläche das Erstellen benutzerdefinierter Felder nicht unterstützt.
- Die Google Drive-API unterstützt das Abrufen von Kommentaren aus einer dauerhaft gelöschten Datei nicht. Kommentare können jedoch für gelöschte Dateien abgerufen werden. Wenn eine Datei

in den Papierkorb verschoben wird, löscht der Amazon Kendra Connector Kommentare aus dem Index. Amazon Kendra

- Die Google Drive-API gibt keine Kommentare zurück, die in einer DOCX-Datei vorhanden sind.

IBM DB2

IBM DB2ist ein relationales Datenbankverwaltungssystem, das von IBM entwickelt wurde. Wenn Sie ein IBM DB2 Benutzer sind, können Sie es verwenden, Amazon Kendra um Ihre IBM DB2 Datenquelle zu indizieren. Der Amazon Kendra IBM DB2 Datenquellenconnector unterstützt DB2 11.5.7.

Sie können über Amazon Kendra die Amazon Kendra Konsole und die API eine Verbindung zu Ihrer IBM DB2 Datenquelle herstellen. TemplateConfiguration

Informationen zur Fehlerbehebung bei Ihrem Amazon Kendra IBM DB2 Datenquellen-Connector finden Sie unterProblembehandlung bei Datenquellen.

Themen

- Unterstützte Features
- Voraussetzungen
- Anweisungen zur Verbindung
- Hinweise

Unterstützte Features

- Feldzuordnungen
- Filterung des Benutzerkontextes
- Einschluss-/Ausschlussfilter
- Vollständige und inkrementelle Inhaltssynchronisierung
- Virtual Private Cloud (VPC)

Voraussetzungen

Bevor Sie Ihre IBM DB2 Datenquelle Amazon Kendra zum Indizieren verwenden können, nehmen Sie diese Änderungen in Ihren Konten IBM DB2 und AWS Konten vor.

Stellen Sie sicherIBM DB2, dass Sie Folgendes haben:

- Notiert Ihren Datenbank-Benutzernamen und Ihr Passwort.

> **Important**
>
> Es hat sich bewährt, nur lesbare Amazon Kendra Datenbankanmeldeinformationen zur Verfügung zu stellen.

- Die URL, der Port und die Instanz Ihres Datenbank-Hosts wurden kopiert.
- Vergewissert, dass jedes Dokument in IBM DB2 und zwischen anderen Datenquellen, die Sie für denselben Index verwenden möchten, einzigartig ist. Jede Datenquelle, die Sie für einen Index verwenden möchten, darf nicht dasselbe Dokument in allen Datenquellen enthalten. Dokument-IDs gelten für einen Index global und müssen pro Index eindeutig sein.

Stellen Sie sicher AWS-Konto, dass Sie Folgendes in Ihrem haben:

- Hat einen Amazon Kendra Index erstellt und bei Verwendung der API die Index-ID notiert.
- Sie haben eine IAM Rolle für Ihre Datenquelle erstellt und, falls Sie die API verwenden, den ARN der IAM Rolle notiert.

> **Note**
>
> Wenn Sie Ihren Authentifizierungstyp und Ihre Anmeldeinformationen ändern, müssen Sie Ihre IAM Rolle aktualisieren, um auf die richtige AWS Secrets Manager geheime ID zugreifen zu können.

- Wir haben Ihre IBM DB2 Authentifizierungsdaten AWS Secrets Manager geheim gespeichert und, falls Sie die API verwenden, den ARN des Geheimnisses notiert.

> **Note**
>
> Wir empfehlen Ihnen, Ihre Anmeldeinformationen und Ihr Geheimnis regelmäßig zu aktualisieren oder zu wechseln. Stellen Sie zu Ihrer eigenen Sicherheit nur die Zugriffsebene bereit, die erforderlich ist. Wir raten davon ab, Anmeldeinformationen und geheime Daten für alle Datenquellen und Connector-Versionen 1.0 und 2.0 (sofern zutreffend) wiederzuverwenden.

Wenn Sie noch keine IAM Rolle oder keinen Schlüssel haben, können Sie die Konsole verwenden, um eine neue IAM Rolle und ein neues Secrets Manager Geheimnis zu erstellen, wenn Sie Ihre IBM DB2 Datenquelle mit verbinden. Amazon Kendra Wenn Sie die API verwenden, müssen Sie den ARN einer vorhandenen IAM Rolle und eines Secrets Manager Geheimnisses sowie eine Index-ID angeben.

Anweisungen zur Verbindung

Um eine Verbindung Amazon Kendra zu Ihrer IBM DB2 Datenquelle herzustellen, müssen Sie Details zu Ihren IBM DB2 Anmeldeinformationen angeben, damit Sie auf Ihre Daten zugreifen Amazon Kendra können. Falls Sie das noch nicht konfiguriert haben, Amazon Kendra finden Sie IBM DB2 weitere Informationen unterVoraussetzungen.

Console

Um eine Verbindung Amazon Kendra herzustellen IBM DB2

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die Amazon Kendra Konsole.
2. Wählen Sie im linken Navigationsbereich Indizes und dann den Index, den Sie verwenden möchten, aus der Indexliste aus.

> **Note**
>
> Sie können Ihre Einstellungen für die Benutzerzugriffskontrolle unter Indexeinstellungen konfigurieren oder bearbeiten.

3. Wählen Sie auf der Seite Erste Schritte die Option Datenquelle hinzufügen aus.
4. Wählen Sie auf der Seite Datenquelle hinzufügen die Option IBM DB2Connector und dann Connector hinzufügen aus.
5. Geben Sie auf der Seite „Datenquellendetails angeben“ die folgenden Informationen ein:

   a. Geben Sie im Feld Name und Beschreibung für Datenquellenname einen Namen für Ihre Datenquelle ein. Sie können Bindestriche, aber keine Leerzeichen verwenden.

   b. (Optional) Beschreibung — Geben Sie eine optionale Beschreibung für Ihre Datenquelle ein.

   c. In Standardsprache — Wählen Sie eine Sprache aus, um Ihre Dokumente nach dem Index zu filtern. Sofern Sie nichts anderes angeben, ist die Standardsprache Englisch.

Die in den Metadaten des Dokuments angegebene Sprache hat Vorrang vor der ausgewählten Sprache.

d. Unter Tags für Neues Tag hinzufügen — Fügen Sie optionale Tags hinzu, um Ihre Ressourcen zu durchsuchen und zu filtern oder Ihre Kosten nachzuverfolgen. AWS

e. Wählen Sie Weiter aus.

6. Geben Sie auf der Seite Zugriff und Sicherheit definieren die folgenden Informationen ein:

a. Geben Sie im Feld Quelle die folgenden Informationen ein:

b. Host — Geben Sie den Datenbank-Hostnamen ein.

c. Port — Geben Sie den Datenbankport ein.

d. Instanz — Geben Sie die Datenbankinstanz ein.

e. Speicherort für SSL-Zertifikate aktivieren — Geben Sie hier den Amazon S3 Pfad zu Ihrer SSL-Zertifikatsdatei ein.

f. Geben Sie im Feld Authentifizierung die folgenden Informationen ein:

- AWS Secrets Manager geheim — Wählen Sie ein vorhandenes Geheimnis aus, oder erstellen Sie ein neues Secrets Manager Geheimnis, um Ihre IBM DB2 Authentifizierungsdaten zu speichern. Wenn Sie ein neues Geheimnis erstellen möchten, wird ein AWS Secrets Manager geheimes Fenster geöffnet.

  A. Geben Sie die folgenden Informationen in das Fenster Create an AWS Secrets Manager Secret ein:

     I. Geheimer Name — Ein Name für Ihr Geheimnis. Das Präfix 'AmazonKendra- IBM DB2 -' wird Ihrem geheimen Namen automatisch hinzugefügt.

     II. Für Datenbankbenutzername und Passwort — Geben Sie die Werte der Authentifizierungsdaten ein, die Sie aus Ihrer Datenbank kopiert haben.

  B. Wählen Sie Speichern.

g. Virtual Private Cloud (VPC) — Sie können wählen, ob Sie eine VPC verwenden möchten. In diesem Fall müssen Sie Subnetze und VPC-Sicherheitsgruppen hinzufügen.

h. IAM Rolle — Wählen Sie eine bestehende IAM Rolle oder erstellen Sie eine neue IAM Rolle, um auf Ihre Repository-Anmeldeinformationen und Indexinhalte zuzugreifen.

> **Note**
>
> IAM Rollen, die für Indizes verwendet werden, können nicht für Datenquellen verwendet werden. Wenn Sie sich nicht sicher sind, ob eine vorhandene Rolle für einen Index oder eine häufig gestellte Frage verwendet wird, wählen Sie Neue Rolle erstellen, um Fehler zu vermeiden.

i. Wählen Sie Weiter aus.

7. Geben Sie auf der Seite „Synchronisierungseinstellungen konfigurieren“ die folgenden Informationen ein:

   a. Wählen Sie unter Synchronisierungsbereich eine der folgenden Optionen aus:

      - SQL-Abfrage — Geben Sie SQL-Abfrageanweisungen wie SELECT- und JOIN-Operationen ein. SQL-Abfragen müssen weniger als 32 KB groß sein. Amazon Kendra durchsucht den gesamten Datenbankinhalt, der Ihrer Abfrage entspricht.
      - Primärschlüsselspalte — Geben Sie den Primärschlüssel für die Datenbanktabelle an. Dies identifiziert eine Tabelle in Ihrer Datenbank.
      - Titelspalte — Geben Sie den Namen der Titelspalte des Dokuments in Ihrer Datenbanktabelle an.
      - Hauptspalte — Geben Sie den Namen der Hauptspalte des Dokuments in Ihrer Datenbanktabelle an.

   b. Wählen Sie unter Zusätzliche Konfiguration — optional aus den folgenden Optionen, um bestimmte Inhalte zu synchronisieren, anstatt alle Dateien zu synchronisieren:

      - Spalten zur Erkennung von Änderungen — Geben Sie die Namen der Spalten ein, anhand derer Inhaltsänderungen erkannt Amazon Kendra werden sollen. Amazon Kendra indexiert den Inhalt neu, wenn sich eine dieser Spalten ändert.
      - Spalte mit Benutzer-IDs — Geben Sie den Namen der Spalte ein, die Benutzer-IDs enthält, um Zugriff auf Inhalte zu erhalten.
      - Spalte „Gruppen“ — Geben Sie den Namen der Spalte ein, die Gruppen enthält, denen der Zugriff auf Inhalte gewährt werden soll.
      - Spalte Quell-URLs — Geben Sie den Namen der Spalte ein, die Quell-URLs enthält, die indexiert werden sollen.

- Spalte mit Zeitstempeln — Geben Sie den Namen der Spalte ein, die Zeitstempel enthält. Amazon Kendra verwendet Zeitstempelinformationen, um Änderungen an Ihren Inhalten zu erkennen und nur geänderte Inhalte zu synchronisieren.
- Spalte „Zeitzonen“ — Geben Sie den Namen der Spalte ein, die Zeitzonen für den Inhalt enthält, der gecrawlt werden soll.
- Zeitstempelformat — Geben Sie den Namen der Spalte ein, die Zeitstempelformate enthält, anhand derer Inhaltsänderungen erkannt und Ihre Inhalte erneut synchronisiert werden sollen.

c. Synchronisierungsmodus — Wählen Sie aus, wie Sie Ihren Index aktualisieren möchten, wenn sich der Inhalt Ihrer Datenquelle ändert. Wenn Sie Ihre Datenquelle Amazon Kendra zum ersten Mal synchronisieren, werden alle Inhalte standardmäßig gecrawlt und indexiert. Sie müssen eine vollständige Synchronisierung Ihrer Daten durchführen, falls Ihre erste Synchronisierung fehlgeschlagen ist, auch wenn Sie die Option Vollsynchronisierung nicht als Synchronisierungsmodusoption wählen.

- Vollständige Synchronisierung: Indizieren Sie den gesamten Inhalt neu und ersetzen die vorhandenen Inhalte jedes Mal, wenn Ihre Datenquelle mit Ihrem Index synchronisiert wird.
- Neue, geänderte Synchronisierung: Indizieren Sie jedes Mal, wenn Ihre Datenquelle mit Ihrem Index synchronisiert wird, nur neue und geänderte Inhalte. Amazon Kendra kann den Mechanismus Ihrer Datenquelle verwenden, um Inhaltsänderungen nachzuverfolgen und Inhalte zu indexieren, die sich seit der letzten Synchronisierung geändert haben.
- Neue, geänderte, gelöschte Synchronisierung: Indizieren Sie bei jeder Synchronisierung Ihrer Datenquelle mit Ihrem Index nur neue, geänderte und gelöschte Inhalte. Amazon Kendra kann den Mechanismus Ihrer Datenquelle verwenden, um Inhaltsänderungen nachzuverfolgen und Inhalte zu indexieren, die sich seit der letzten Synchronisierung geändert haben.

d. Im Synchronisierungslaufplan für Frequenz — Wie oft Amazon Kendra wird mit Ihrer Datenquelle synchronisiert?

e. Wählen Sie Weiter aus.

8. Geben Sie auf der Seite Feldzuordnungen festlegen die folgenden Informationen ein:

a. Wählen Sie aus den generierten Standard-Datenquellenfeldern — Dokument-IDs, Dokumenttitel und Quell-URLs — aus, die Sie dem Index zuordnen möchten. Amazon Kendra

b. Feld hinzufügen — Um benutzerdefinierte Datenquellenfelder hinzuzufügen, um einen Indexfeldnamen für die Zuordnung und den Felddatentyp zu erstellen.

c. Wählen Sie Weiter aus.

9. Überprüfen Sie auf der Seite Überprüfen und erstellen, ob die von Ihnen eingegebenen Informationen korrekt sind, und wählen Sie dann Datenquelle hinzufügen aus. Sie können Ihre Informationen auch auf dieser Seite bearbeiten. Ihre Datenquelle wird auf der Seite Datenquellen angezeigt, nachdem die Datenquelle erfolgreich hinzugefügt wurde.

API

Um eine Verbindung Amazon Kendra herzustellen IBM DB2

Mithilfe der TemplateConfigurationAPI müssen Sie Folgendes angeben:

- Datenquelle — Geben Sie den Datenquellentyp wie `JDBC` bei der Verwendung des TemplateConfigurationJSON-Schemas an. Geben Sie außerdem die Datenquelle so an`TEMPLATE`, wie Sie die CreateDataSourceAPI aufrufen.
- Datenbanktyp — Sie müssen den Datenbanktyp als `db2` angeben.
- SQL-Abfrage — Geben Sie SQL-Abfrageanweisungen wie SELECT- und JOIN-Operationen an. SQL-Abfragen müssen weniger als 32 KB groß sein. Amazon Kendra durchsucht den gesamten Datenbankinhalt, der Ihrer Abfrage entspricht.
- Synchronisierungsmodus — Geben Sie an, wie Ihr Index aktualisiert Amazon Kendra werden soll, wenn sich der Inhalt Ihrer Datenquelle ändert. Wenn Sie Ihre Datenquelle Amazon Kendra zum ersten Mal synchronisieren, werden alle Inhalte standardmäßig gecrawlt und indexiert. Sie müssen eine vollständige Synchronisierung Ihrer Daten durchführen, falls Ihre erste Synchronisierung fehlgeschlagen ist, auch wenn Sie die Option Vollsynchronisierung nicht als Synchronisierungsmodusoption wählen. Sie können wählen zwischen:
  - `FORCED_FULL_CRAWL`um den gesamten Inhalt neu zu indizieren und vorhandene Inhalte jedes Mal zu ersetzen, wenn Ihre Datenquelle mit Ihrem Index synchronisiert wird.
  - `FULL_CRAWL`um bei jeder Synchronisierung Ihrer Datenquelle mit Ihrem Index nur neue, geänderte und gelöschte Inhalte zu indizieren. Amazon Kendra kann den Mechanismus Ihrer

Datenquelle verwenden, um Inhaltsänderungen nachzuverfolgen und Inhalte zu indexieren, die sich seit der letzten Synchronisierung geändert haben.

- `CHANGE_LOG`um jedes Mal, wenn Ihre Datenquelle mit Ihrem Index synchronisiert wird, nur neue und geänderte Inhalte zu indizieren. Amazon Kendra kann den Mechanismus Ihrer Datenquelle verwenden, um Inhaltsänderungen nachzuverfolgen und Inhalte zu indexieren, die sich seit der letzten Synchronisierung geändert haben.

- Geheimer Amazon-Ressourcenname (ARN) — Geben Sie den Amazon-Ressourcennamen (ARN) eines Secrets Manager Geheimnisses ein, das die Authentifizierungsdaten enthält, die Sie in Ihrem IBM DB2 Konto erstellt haben. Das Geheimnis wird in einer JSON-Struktur mit den folgenden Schlüsseln gespeichert:

```
{
    "user name": "database user name",
    "password": "password"
}
```

> **Note**
>
> Wir empfehlen Ihnen, Ihre Anmeldeinformationen und Ihr Geheimnis regelmäßig zu aktualisieren oder zu wechseln. Stellen Sie zu Ihrer eigenen Sicherheit nur die Zugriffsebene bereit, die erforderlich ist. Wir raten davon ab, Anmeldeinformationen und geheime Daten für alle Datenquellen und Connector-Versionen 1.0 und 2.0 (sofern zutreffend) wiederzuverwenden.

- IAM Rolle — Geben Sie an`RoleArn`, wann Sie anrufen`CreateDataSource`, um einer IAM Rolle Berechtigungen für den Zugriff auf Ihr Secrets Manager Geheimnis und für den Aufruf der erforderlichen öffentlichen APIs für den IBM DB2 Connector und zum Aufrufen der erforderlichen öffentlichen APIs zu erteilen. Amazon Kendra Weitere Informationen finden Sie unter IAM Rollen für IBM DB2 Datenquellen.

Sie können auch die folgenden optionalen Funktionen hinzufügen:

- Virtual Private Cloud (VPC) — Geben Sie an, `VpcConfiguration` wann Sie anrufen. `CreateDataSource` Weitere Informationen finden Sie unter Konfigurieren von Amazon Kendra für die Verwendung eines Amazon VPC.

- Inklusions- und Ausschlussfilter — Sie können mithilfe von Benutzer-IDs, Gruppen, Quell-URLs, Zeitstempeln und Zeitzonen angeben, ob bestimmte Inhalte eingeschlossen werden sollen.
- Benutzerkontextfilterung und Zugriffskontrolle —Amazon Kendra durchsucht die Zugriffskontrollliste (ACL) für Ihre Dokumente, sofern Sie über eine ACL für Ihre Dokumente verfügen. Die ACL-Informationen werden verwendet, um Suchergebnisse nach dem Benutzer- oder Gruppenzugriff auf Dokumente zu filtern. Weitere Informationen finden Sie unter Benutzerkontextfilterung.
- Feldzuordnungen — Wählen Sie diese Option, um Ihre IBM DB2 Datenquellenfelder Ihren Indexfeldern zuzuordnen. Amazon Kendra Weitere Informationen finden Sie unter Zuweisen von Datenquellenfeldern.

> **Note**
>
> Das Textfeld oder das entsprechende Textfeld für Ihre Dokumente ist erforderlich, um Ihre Dokumente durchsuchen Amazon Kendra zu können. Sie müssen den Feldnamen Ihres Dokumenthauptteils in Ihrer Datenquelle dem Namen des Indexfeldes zuordnen`_document_body`. Alle anderen Felder sind optional.

Eine Liste weiterer wichtiger JSON-Schlüssel, die konfiguriert werden müssen, finden Sie unterIBM DB2-Vorlagenschema.

Hinweise

- Gelöschte Datenbankzeilen werden nicht nachverfolgt, wenn nach Amazon Kendra aktualisierten Inhalten gesucht wird.
- Die Größe von Feldnamen und Werten in einer Zeile Ihrer Datenbank darf 400 KB nicht überschreiten.
- Wenn Ihre Datenbankdatenquelle eine große Datenmenge enthält und Sie nicht möchten Amazon Kendra , dass Ihr gesamter Datenbankinhalt nach der ersten Synchronisierung indexiert wird, können Sie wählen, ob nur neue, geänderte oder gelöschte Dokumente synchronisiert werden sollen.
- Es hat sich bewährt, nur lesbare Amazon Kendra Datenbankanmeldeinformationen zur Verfügung zu stellen.

- Es hat sich bewährt, das Hinzufügen von Tabellen mit sensiblen Daten oder personenbezogenen Daten (PII) zu vermeiden.

Jira

Jira ist ein Projektmanagement-Tool für Softwareentwicklung, Produktmanagement und Bugtracking. Sie können Amazon Kendra es verwenden, um Ihre Jira-Projekte, Probleme, Kommentare, Anhänge, Worklogs und Status zu indizieren.

Amazon Kendra unterstützt derzeit nur Jira Cloud.

Sie können entweder über Amazon Kendra die Amazon Kendra Konsole oder die API eine Verbindung zu Ihrer Jira-Datenquelle herstellen. JiraConfiguration Eine Liste der Funktionen, die von den einzelnen Funktionen unterstützt werden, finden Sie unterUnterstützte Features.

Informationen zur Fehlerbehebung bei Ihrem Amazon Kendra Jira-Datenquellen-Connector finden Sie unterProblembehandlung bei Datenquellen.

Themen

Unterstützte Features

Amazon Kendra Der Jira-Datenquellen-Connector unterstützt die folgenden Funktionen:

- Änderungsprotokoll
- Feldzuordnungen
- Filterung des Benutzerkontextes
- Einschluss-/Ausschlussfilter
- Virtual Private Cloud (VPC)

Voraussetzungen

Bevor Sie Ihre Jira-Datenquelle Amazon Kendra zum Indizieren verwenden können, nehmen Sie diese Änderungen in Ihrem Jira und Ihren Konten vor. AWS

Stellen Sie in Jira sicher, dass Sie über Folgendes verfügen:

- Es wurden Anmeldeinformationen für die Jira-API-Token-Authentifizierung erstellt, die eine Jira-ID (Benutzername oder E-Mail) und Jira-Anmeldeinformationen (Jira-API-Token) enthalten. Weitere Informationen zur Verwaltung von API-Token findest du in der Atlassian-Dokumentation.
- Du hast dir die URL deines Jira-Kontos in deinen Jira-Kontoeinstellungen notiert. *Zum Beispiel https://company.atlassian.net/.*
- Aktiviert, dass jedes Dokument in Jira und in anderen Datenquellen, die Sie für denselben Index verwenden möchten, einzigartig ist. Jede Datenquelle, die Sie für einen Index verwenden möchten, darf nicht dasselbe Dokument in allen Datenquellen enthalten. Dokument-IDs gelten für einen Index global und müssen pro Index eindeutig sein.

Stellen Sie sicher AWS-Konto, dass Sie Folgendes in Ihrem haben:

- Hat einen Amazon Kendra Index erstellt und bei Verwendung der API die Index-ID notiert.
- Sie haben eine IAM Rolle für Ihre Datenquelle erstellt und, falls Sie die API verwenden, den ARN der IAM Rolle notiert.

> **Note**
>
> Wenn Sie Ihren Authentifizierungstyp und Ihre Anmeldeinformationen ändern, müssen Sie Ihre IAM Rolle aktualisieren, um auf die richtige AWS Secrets Manager geheime ID zugreifen zu können.

- Du hast deine Jira-Authentifizierungsdaten AWS Secrets Manager geheim gespeichert und, falls du die API verwendest, den ARN des Geheimnisses notiert.

> **Note**
>
> Wir empfehlen Ihnen, Ihre Anmeldeinformationen und Ihr Geheimnis regelmäßig zu aktualisieren oder zu wechseln. Stellen Sie zu Ihrer eigenen Sicherheit nur die Zugriffsebene bereit, die erforderlich ist. Wir raten davon ab, Anmeldeinformationen

und geheime Daten für alle Datenquellen und Connector-Versionen 1.0 und 2.0 (sofern zutreffend) wiederzuverwenden.

Wenn Sie noch keine IAM Rolle oder keinen Schlüssel haben, können Sie die Konsole verwenden, um eine neue IAM Rolle und ein neues Secrets Manager Geheimnis zu erstellen, wenn Sie Ihre Jira-Datenquelle mit verbinden. Amazon Kendra Wenn Sie die API verwenden, müssen Sie den ARN einer vorhandenen IAM Rolle und eines Secrets Manager Geheimnisses sowie eine Index-ID angeben.

Anweisungen zur Verbindung

Um eine Verbindung Amazon Kendra zu Ihrer Jira-Datenquelle herzustellen, müssen Sie die erforderlichen Details zu Ihrer Jira-Datenquelle angeben, damit Sie auf Ihre Daten zugreifen Amazon Kendra können. Wenn Sie Jira für Amazon Kendra noch nicht konfiguriert haben, finden Sie weitere Informationen unter. Voraussetzungen

Console

So stellen Sie eine Verbindung Amazon Kendra zu Jira her

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die Amazon Kendra Konsole.
2. Wählen Sie im linken Navigationsbereich Indizes und dann den Index, den Sie verwenden möchten, aus der Indexliste aus.

   > **Note**
   >
   > Sie können Ihre Einstellungen für die Benutzerzugriffskontrolle unter Indexeinstellungen konfigurieren oder bearbeiten.

3. Wählen Sie auf der Seite Erste Schritte die Option Datenquelle hinzufügen aus.
4. Wählen Sie auf der Seite Datenquelle hinzufügen die Option Jira-Connector und dann Connector hinzufügen aus.
5. Geben Sie auf der Seite „Datenquellendetails angeben“ die folgenden Informationen ein:

   a. Geben Sie im Feld Name und Beschreibung für Datenquellenname einen Namen für Ihre Datenquelle ein. Sie können Bindestriche, aber keine Leerzeichen verwenden.

b. (Optional) Beschreibung — Geben Sie eine optionale Beschreibung für Ihre Datenquelle ein.

c. In Standardsprache — Wählen Sie eine Sprache aus, um Ihre Dokumente nach dem Index zu filtern. Sofern Sie nichts anderes angeben, ist die Standardsprache Englisch. Die in den Metadaten des Dokuments angegebene Sprache hat Vorrang vor der ausgewählten Sprache.

d. Unter Tags für Neues Tag hinzufügen — Fügen Sie optionale Tags hinzu, um Ihre Ressourcen zu durchsuchen und zu filtern oder Ihre Kosten nachzuverfolgen. AWS

e. Wählen Sie Weiter aus.

6. Geben Sie auf der Seite Zugriff und Sicherheit definieren die folgenden Informationen ein:

a. Jira-Konto-URL — Geben Sie die URL Ihres Jira-Kontos ein. *Zum Beispiel: https://company.atlassian.net/.*

b. AWS Secrets Manager geheim — Wählen Sie ein vorhandenes Geheimnis aus oder erstellen Sie ein neues Secrets Manager Geheimnis, um Ihre Jira-Authentifizierungsdaten zu speichern. Wenn Sie sich dafür entscheiden, ein neues Geheimnis zu erstellen, wird ein AWS Secrets Manager geheimes Fenster geöffnet.

i. Geben Sie die folgenden Informationen in das Fenster Create an AWS Secrets Manager Secret ein:

A. Geheimer Name — Ein Name für Ihr Geheimnis. Das Präfix 'AmazonKendra-Jira-' wird automatisch zu Ihrem geheimen Namen hinzugefügt.

B. Für Jira ID — Geben Sie den Jira-Benutzernamen oder die Jira-E-Mail-Adresse ein.

C. Für Passwort/Token — Geben Sie das Jira-API-Token ein, das Sie mit Ihrem Jira-Konto erstellt haben.

ii. Wählen Sie Speichern.

c. Virtual Private Cloud (VPC) — Sie können wählen, ob Sie eine VPC verwenden möchten. In diesem Fall müssen Sie Subnetze und VPC-Sicherheitsgruppen hinzufügen.

d. IAM Rolle — Wählen Sie eine bestehende IAM Rolle oder erstellen Sie eine neue IAM Rolle, um auf Ihre Repository-Anmeldeinformationen und Indexinhalte zuzugreifen.

> **Note**
>
> IAM Rollen, die für Indizes verwendet werden, können nicht für Datenquellen verwendet werden. Wenn Sie sich nicht sicher sind, ob eine vorhandene Rolle für einen Index oder eine häufig gestellte Frage verwendet wird, wählen Sie Neue Rolle erstellen, um Fehler zu vermeiden.

e. Wählen Sie Weiter aus.

7. Geben Sie auf der Seite „Synchronisierungseinstellungen konfigurieren“ die folgenden Informationen ein:

   a. Wählen Sie aus, welche Jira-Projekte indexiert werden sollen — Die Jira-Entitäten oder Inhaltstypen, die Sie crawlen möchten.

   b. Status, Zusätzliche Elemente und Problemtypen — Wählen Sie Inhalte aus, um den Umfang Ihres Indexes zu verfeinern.

   c. Änderungsprotokoll — Wählen Sie diese Option, um Ihren Index nur mit neuen oder geänderten Inhalten zu aktualisieren, anstatt alle Ihre Dateien zu synchronisieren.

   d. Regex-Muster — Reguläre Ausdrucksmuster zum Ein- oder Ausschließen bestimmter Dateien. Sie können bis zu 100 Muster hinzufügen.

   e. Wählen Sie im Synchronisierungslaufplan für Frequenz aus, wie oft Amazon Kendra mit Ihrer Datenquelle synchronisiert.

   f. Wählen Sie Weiter aus.

8. Geben Sie auf der Seite Feldzuordnungen festlegen die folgenden Informationen ein:

   a. Für Projekt, Problem, Kommentar, Anlage, Arbeitsprotokoll — Wählen Sie eines der Amazon Kendra generierten Standard-Datenquellenfelder aus, die Sie Ihrem Index zuordnen möchten.

   b. Feld hinzufügen — Um benutzerdefinierte Datenquellenfelder hinzuzufügen, um einen Indexfeldnamen für die Zuordnung und den Felddatentyp zu erstellen.

   c. Wählen Sie Weiter aus.

9. Überprüfen Sie auf der Seite Überprüfen und erstellen, ob die von Ihnen eingegebenen Informationen korrekt sind, und wählen Sie dann Datenquelle hinzufügen aus. Sie können Ihre Informationen auch auf dieser Seite bearbeiten. Ihre Datenquelle wird auf der Seite Datenquellen angezeigt, nachdem die Datenquelle erfolgreich hinzugefügt wurde.

API

Um eine Verbindung Amazon Kendra zu Jira herzustellen

Mithilfe der JiraConfiguration API müssen Sie Folgendes angeben:

- Datenquellen-URL — Geben Sie die URL Ihres Jira-Kontos an. *Zum Beispiel company.atlassian.net.*
- Geheimer Amazon-Ressourcenname (ARN) — Geben Sie den Amazon-Ressourcennamen (ARN) eines Secrets Manager Geheimnisses ein, das die Authentifizierungsdaten für Ihr Jira-Konto enthält. Das Geheimnis wird in einer JSON-Struktur mit den folgenden Schlüsseln gespeichert:

```
{
    "jiraId": "Jira user name or email",
    "jiraCredential": "Jira API token"
}
```

> **Note**
>
> Wir empfehlen Ihnen, Ihre Anmeldeinformationen und Ihr Geheimnis regelmäßig zu aktualisieren oder zu wechseln. Stellen Sie zu Ihrer eigenen Sicherheit nur die Zugriffsebene bereit, die erforderlich ist. Wir raten davon ab, Anmeldeinformationen und geheime Daten für alle Datenquellen und Connector-Versionen 1.0 und 2.0 (sofern zutreffend) wiederzuverwenden.

- IAM role — Geben Sie an`RoleArn`, wann Sie anrufen`CreateDataSource`, um einer IAM Rolle Berechtigungen für den Zugriff auf Ihr Secrets Manager Secret und den Aufruf der erforderlichen öffentlichen APIs für den Jira-Connector und zum Aufrufen der erforderlichen öffentlichen APIs zu erteilen. Amazon Kendra Weitere Informationen finden Sie unter IAM Rollen für Jira-Datenquellen.

Sie können auch die folgenden optionalen Funktionen hinzufügen:

- Virtual Private Cloud (VPC) — Geben Sie dies `VpcConfiguration` als Teil der Datenquellenkonfiguration an. Siehe Konfiguration Amazon Kendra für die Verwendung einer VPC.

- Änderungsprotokoll — Gibt an, ob der Änderungsprotokollmechanismus der Jira-Datenquelle verwendet werden Amazon Kendra soll, um festzustellen, ob ein Dokument im Index aktualisiert werden muss.

  > **Note**
  >
  > Verwenden Sie das Änderungsprotokoll, wenn Sie nicht alle Dokumente scannen Amazon Kendra möchten. Wenn Ihr Änderungsprotokoll umfangreich ist, nimmt das Scannen der Dokumente in der Jira-Datenquelle möglicherweise Amazon Kendra weniger Zeit in Anspruch als das Verarbeiten des Änderungsprotokolls. Wenn Sie Ihre Jira-Datenquelle zum ersten Mal mit Ihrem Index synchronisieren, werden alle Dokumente gescannt.

- Inklusions- und Ausschlussfilter — Sie können angeben, ob bestimmte Dateien ein- oder ausgeschlossen werden sollen.

  > **Note**
  >
  > Die meisten Datenquellen verwenden Muster für reguläre Ausdrücke, bei denen es sich um Ein- oder Ausschlussmuster handelt, die als Filter bezeichnet werden. Wenn Sie einen Einschlussfilter angeben, werden nur Inhalte indexiert, die dem Einschlussfilter entsprechen. Jedes Dokument, das nicht dem Einschlussfilter entspricht, wird nicht indexiert. Wenn Sie einen Ein- und Ausschlussfilter angeben, werden Dokumente, die dem Ausschlussfilter entsprechen, nicht indexiert, auch wenn sie dem Einschlussfilter entsprechen.

- Kommentar, Anlagen und Arbeitsprotokolle — Sie können angeben, ob bestimmte Kommentare, Anlagen und Arbeitsprotokolle zu Problemen gecrawlt werden sollen.
- Projekte, Probleme, Status — Sie können angeben, ob bestimmte Projekt-IDs, Problemtypen und Status gecrawlt werden sollen.
- Benutzerkontextfilterung und Zugriffskontrolle —Amazon Kendra durchsucht die Zugriffskontrollliste (ACL) für Ihre Dokumente, sofern Sie über eine ACL für Ihre Dokumente verfügen. Die ACL-Informationen werden verwendet, um Suchergebnisse nach dem Benutzer- oder Gruppenzugriff auf Dokumente zu filtern. Weitere Informationen finden Sie unter Benutzerkontextfilterung.

- Feldzuordnungen — Wählen Sie diese Option, um Ihre Jira-Datenquellenfelder Ihren Indexfeldern zuzuordnen. Amazon Kendra Weitere Informationen finden Sie unter Zuweisen von Datenquellenfeldern.

> **Note**
>
> Das Feld „Hauptteil des Dokuments“ oder das Äquivalent zum Dokumententext für Ihre Dokumente ist erforderlich, damit Sie Ihre Dokumente durchsuchen Amazon Kendra können. Sie müssen den Feldnamen Ihres Dokumenthauptteils in Ihrer Datenquelle dem Namen des Indexfeldes zuordnen`_document_body`. Alle anderen Felder sind optional.

Weitere Informationen

Weitere Informationen zur Integration Amazon Kendra mit Ihrer Jira-Datenquelle finden Sie unter:

- Durchsuchen Sie Ihre Jira-Projekte intelligent mit dem Jira Cloud Connector Amazon Kendra

Microsoft Exchange

Microsoft Exchange ist ein Tool für die Zusammenarbeit in Unternehmen für Messaging, Besprechungen und Filesharing. Wenn Sie ein Microsoft Exchange-Benutzer sind, können Sie Amazon Kendra damit Ihre Microsoft Exchange-Datenquelle indizieren.

Sie können über Amazon Kendra die Amazon Kendra Konsole und die TemplateConfigurationAPI eine Verbindung zu Ihrer Microsoft Exchange-Datenquelle herstellen.

Informationen zur Problembehandlung Ihres Amazon Kendra Microsoft Exchange-Datenquellenconnectors finden Sie unterProblembehandlung bei Datenquellen.

Unterstützte Features

- Feldzuordnungen
- Filterung des Benutzerkontextes
- Einschluss-/Ausschlussfilter
- Vollständige und inkrementelle Inhaltssynchronisierung
- Virtual Private Cloud (VPC)

Voraussetzungen

Bevor Sie Ihre Microsoft Exchange-Datenquelle Amazon Kendra zum Indizieren verwenden können, nehmen Sie diese Änderungen in Ihrem Microsoft Exchange und Ihren AWS Konten vor.

Stellen Sie in Microsoft Exchange sicher, dass Sie über Folgendes verfügen:

- Hat ein Microsoft Exchange-Konto in Office 365 erstellt.
- Haben Sie Ihre Microsoft 365-Mandanten-ID notiert. Sie finden Ihre Mandanten-ID in den Eigenschaften Ihres Azure Active Directory-Portals oder in Ihrer OAuth-Anwendung.
- Sie haben eine OAuth-Anwendung im Azure-Portal erstellt und die Client-ID und das Kundengeheimnis oder die Kundenanmeldedaten notiert. Weitere Informationen finden Sie im Microsoft-Tutorial und im Beispiel für registrierte Apps.

> **Note**
>
> Wenn Sie eine App im Azure-Portal erstellen oder registrieren, stellt die geheime ID den tatsächlichen geheimen Wert dar. Sie müssen den tatsächlichen geheimen Wert sofort bei der Erstellung des Geheimnisses und der App notieren oder speichern. Sie können auf Ihr Geheimnis zugreifen, indem Sie den Namen Ihrer Anwendung im Azure-Portal auswählen und dann zur Menüoption für Zertifikate und Geheimnisse navigieren.
> Sie können auf Ihre Client-ID zugreifen, indem Sie den Namen Ihrer Anwendung im Azure-Portal auswählen und dann zur Übersichtsseite navigieren. Die Anwendungs-ID (Client) ist die Client-ID.

- Die folgenden Berechtigungen für die Connector-Anwendung wurden hinzugefügt:

Microsoft Graph	Office 365 Exchange Online
• Mail.Read (Anwendung) • E-Mail. ReadBasic (Bewerbung) • E-Mail. ReadBasic.Alle (Anwendung) • Calendars.Read (Anwendung) • User.Read.All (Anwendung) • Contacts.Read (Anwendung) • Notes.Read.All (Anwendung)	full_access_as_app (Anwendung)

Microsoft Graph	Office 365 Exchange Online
• Directory.Read.All (Anwendung) • NEUIGKEITEN. AccessAsUser. Alle (delegiert)	

- Aktiviert, dass jedes Dokument in Microsoft Exchange und in anderen Datenquellen, die Sie für denselben Index verwenden möchten, eindeutig ist. Jede Datenquelle, die Sie für einen Index verwenden möchten, darf nicht dasselbe Dokument in allen Datenquellen enthalten. Dokument-IDs gelten für einen Index global und müssen pro Index eindeutig sein.

Stellen Sie sicher AWS-Konto, dass Sie Folgendes in Ihrem haben:

- Hat einen Amazon Kendra Index erstellt und bei Verwendung der API die Index-ID notiert.
- Sie haben eine IAM Rolle für Ihre Datenquelle erstellt und, falls Sie die API verwenden, den ARN der IAM Rolle notiert.

> **Note**
>
> Wenn Sie Ihren Authentifizierungstyp und Ihre Anmeldeinformationen ändern, müssen Sie Ihre IAM Rolle aktualisieren, um auf die richtige AWS Secrets Manager geheime ID zugreifen zu können.

- Ihre Microsoft Exchange-Authentifizierungsdaten AWS Secrets Manager geheim gespeichert und, falls Sie die API verwenden, den ARN des Geheimnisses notiert.

> **Note**
>
> Wir empfehlen Ihnen, Ihre Anmeldeinformationen und Ihr Geheimnis regelmäßig zu aktualisieren oder zu wechseln. Stellen Sie zu Ihrer eigenen Sicherheit nur die Zugriffsebene bereit, die erforderlich ist. Wir raten davon ab, Anmeldeinformationen und geheime Daten für alle Datenquellen und Connector-Versionen 1.0 und 2.0 (sofern zutreffend) wiederzuverwenden.

Wenn Sie noch keine IAM Rolle oder keinen Schlüssel haben, können Sie die Konsole verwenden, um eine neue IAM Rolle und ein neues Secrets Manager Geheimnis zu erstellen, wenn Sie Ihre

Microsoft Exchange-Datenquelle mit verbinden Amazon Kendra. Wenn Sie die API verwenden, müssen Sie den ARN einer vorhandenen IAM Rolle und eines Secrets Manager Geheimnisses sowie eine Index-ID angeben.

Anweisungen zur Verbindung

Um eine Verbindung Amazon Kendra zu Ihrer Microsoft Exchange-Datenquelle herzustellen, müssen Sie die erforderlichen Details zu Ihrer Microsoft Exchange-Datenquelle angeben, damit Sie auf Ihre Daten zugreifen Amazon Kendra können. Wenn Sie Microsoft Exchange noch nicht für konfiguriert haben Amazon Kendra, finden Sie weitere Informationen unterVoraussetzungen.

Console

So stellen Sie eine Verbindung Amazon Kendra zu Microsoft Exchange her

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die Amazon Kendra Konsole.
2. Wählen Sie im linken Navigationsbereich Indizes und dann den Index, den Sie verwenden möchten, aus der Indexliste aus.

   > **Note**
   >
   > Sie können Ihre Einstellungen für die Benutzerzugriffskontrolle unter Indexeinstellungen konfigurieren oder bearbeiten.

3. Wählen Sie auf der Seite Erste Schritte die Option Datenquelle hinzufügen aus.
4. Wählen Sie auf der Seite Datenquelle hinzufügen die Option Microsoft Exchange-Connector und dann Connector hinzufügen aus.
5. Geben Sie auf der Seite „Datenquellendetails angeben“ die folgenden Informationen ein:

   a. Geben Sie im Feld Name und Beschreibung für Datenquellenname einen Namen für Ihre Datenquelle ein. Sie können Bindestriche, aber keine Leerzeichen verwenden.

   b. (Optional) Beschreibung — Geben Sie eine optionale Beschreibung für Ihre Datenquelle ein.

   c. In Standardsprache — Wählen Sie eine Sprache aus, um Ihre Dokumente nach dem Index zu filtern. Sofern Sie nichts anderes angeben, ist die Standardsprache Englisch. Die in den Metadaten des Dokuments angegebene Sprache hat Vorrang vor der ausgewählten Sprache.

d. Unter Tags für Neues Tag hinzufügen — Fügen Sie optionale Tags hinzu, um Ihre Ressourcen zu durchsuchen und zu filtern oder Ihre Kosten nachzuverfolgen. AWS

e. Wählen Sie Weiter aus.

6. Geben Sie auf der Seite Zugriff und Sicherheit definieren die folgenden Informationen ein:

   a. Quelle — Geben Sie Ihre Microsoft 365-Mandanten-ID ein. Sie finden Ihre Mandanten-ID in den Eigenschaften Ihres Azure Active Directory-Portals oder in Ihrer OAuth-Anwendung.

   b. Autorisierung — Aktivieren oder deaktivieren Sie die Informationen der Zugriffskontrollliste (ACL) für Ihre Dokumente, wenn Sie über eine ACL verfügen und diese für die Zugriffskontrolle verwenden möchten. Die ACL gibt an, auf welche Dokumente Benutzer und Gruppen zugreifen können. Die ACL-Informationen werden verwendet, um Suchergebnisse nach dem Benutzer- oder Gruppenzugriff auf Dokumente zu filtern. Weitere Informationen finden Sie unter Benutzerkontextfilterung.

   c. AWS Secrets Manager geheim — Wählen Sie ein vorhandenes Geheimnis aus, oder erstellen Sie ein neues Secrets Manager Geheimnis, um Ihre Microsoft Exchange-Authentifizierungsanmeldeinformationen zu speichern. Wenn Sie ein neues Geheimnis erstellen möchten, wird ein AWS Secrets Manager geheimes Fenster geöffnet.

      i. Geben Sie die folgenden Informationen in das Fenster Create an AWS Secrets Manager Secret ein:

         A. Geheimer Name — Ein Name für Ihr Geheimnis. Das Präfix 'AmazonKendra-Microsoft Exchange

         B. Für Client-ID — Geben Sie die Client-ID ein.

         C. Für Client Secret — Geben Sie die Werte für die Authentifizierungsdaten ein, die Sie in Ihrem Microsoft Exchange-Konto im Azure-Portal erstellt haben.

      ii. Wählen Sie Speichern.

   d. Virtual Private Cloud (VPC) — Sie können wählen, ob Sie eine VPC verwenden möchten. In diesem Fall müssen Sie Subnetze und VPC-Sicherheitsgruppen hinzufügen.

   e. IAM Rolle — Wählen Sie eine bestehende IAM Rolle oder erstellen Sie eine neue IAM Rolle, um auf Ihre Repository-Anmeldeinformationen und Indexinhalte zuzugreifen.

> **Note**
>
> IAM Rollen, die für Indizes verwendet werden, können nicht für Datenquellen verwendet werden. Wenn Sie sich nicht sicher sind, ob eine vorhandene Rolle für einen Index oder eine häufig gestellte Frage verwendet wird, wählen Sie Neue Rolle erstellen, um Fehler zu vermeiden.

f. Wählen Sie Weiter aus.

7. Geben Sie auf der Seite „Synchronisierungseinstellungen konfigurieren“ die folgenden Informationen ein:

   a. Inhalte synchronisieren — Wählen Sie die zu synchronisierenden Inhalte aus.

   b. Zusätzliche Konfiguration — Sie können optional die folgenden Inhalte indizieren, anstatt alle Dokumente zu synchronisieren.

      - Entitätstypen — Wählen Sie die Entitäten aus, die Sie synchronisieren möchten. Sie können zwischen Kalender OneNotesund Kontakten wählen.
      - Kalender-Crawling — Geben Sie das Start- und Enddatum für die Synchronisierung Ihres Kalenders ein.
      - E-Mail einbeziehen — Geben Sie die E-Mail-Adresse von und die E-Mail an die Domain sowie alle Betreffzeilen ein, die Sie in Ihren Index aufnehmen oder ausschließen möchten.
      - Regex für Domains — Fügen Sie Muster hinzu, um bestimmte E-Mail-Domains in Ihren Index aufzunehmen oder daraus auszuschließen.
      - Regex-Muster — Fügen Sie Muster für reguläre Ausdrücke hinzu, um bestimmte Dateien ein- oder auszuschließen. Sie können bis zu 100 Muster hinzufügen.

   c. Synchronisierungsmodus — Wählen Sie aus, wie Sie Ihren Index aktualisieren möchten, wenn sich der Inhalt Ihrer Datenquelle ändert. Wenn Sie Ihre Datenquelle Amazon Kendra zum ersten Mal synchronisieren, werden alle Inhalte standardmäßig gecrawlt und indexiert. Sie müssen eine vollständige Synchronisierung Ihrer Daten durchführen, falls Ihre erste Synchronisierung fehlgeschlagen ist, auch wenn Sie die Option Vollsynchronisierung nicht als Synchronisierungsmodusoption wählen.

      - Vollständige Synchronisierung: Indizieren Sie den gesamten Inhalt neu und ersetzen die vorhandenen Inhalte jedes Mal, wenn Ihre Datenquelle mit Ihrem Index synchronisiert wird.

- Neue, geänderte Synchronisierung: Indizieren Sie jedes Mal, wenn Ihre Datenquelle mit Ihrem Index synchronisiert wird, nur neue und geänderte Inhalte. Amazon Kendra kann den Mechanismus Ihrer Datenquelle verwenden, um Inhaltsänderungen nachzuverfolgen und Inhalte zu indexieren, die sich seit der letzten Synchronisierung geändert haben.
- Neue, geänderte, gelöschte Synchronisierung: Indizieren Sie bei jeder Synchronisierung Ihrer Datenquelle mit Ihrem Index nur neue, geänderte und gelöschte Inhalte. Amazon Kendra kann den Mechanismus Ihrer Datenquelle verwenden, um Inhaltsänderungen nachzuverfolgen und Inhalte zu indexieren, die sich seit der letzten Synchronisierung geändert haben.

8. Geben Sie auf der Seite Feldzuordnungen festlegen die folgenden Informationen ein:

   a. Standard-Datenquellenfelder — Wählen Sie eines der Amazon Kendra generierten Standard-Datenquellenfelder aus, die Sie Ihrem Index zuordnen möchten.

   > **Note**
   >
   > Der Amazon Kendra Microsoft Exchange-Datenquellenconnector unterstützt keine benutzerdefinierten Feldzuordnungen.

   b. Wählen Sie Weiter aus.

9. Überprüfen Sie auf der Seite Überprüfen und erstellen, ob die von Ihnen eingegebenen Informationen korrekt sind, und wählen Sie dann Datenquelle hinzufügen aus. Sie können Ihre Informationen auch auf dieser Seite bearbeiten. Ihre Datenquelle wird auf der Seite Datenquellen angezeigt, nachdem die Datenquelle erfolgreich hinzugefügt wurde.

API

So stellen Sie eine Verbindung Amazon Kendra zu Microsoft Exchange her

Sie müssen mithilfe der TemplateConfigurationAPI eine JSON-Datei des Datenquellenschemas angeben. Sie müssen die folgenden Informationen angeben:

- Datenquelle — Geben Sie den Datenquellentyp wie `MSEXCHANGE` bei der Verwendung des TemplateConfigurationJSON-Schemas an. Geben Sie außerdem die Datenquelle so an`TEMPLATE`, wie Sie die CreateDataSourceAPI aufrufen.

- Mandanten-ID — Sie finden Ihre Mandanten-ID in den Eigenschaften Ihres Azure Active Directory-Portals oder in Ihrer OAuth-Anwendung.
- Synchronisierungsmodus — Geben Sie an, wie Ihr Index aktualisiert Amazon Kendra werden soll, wenn sich der Inhalt Ihrer Datenquelle ändert. Wenn Sie Ihre Datenquelle Amazon Kendra zum ersten Mal synchronisieren, werden alle Inhalte standardmäßig gecrawlt und indexiert. Sie müssen eine vollständige Synchronisierung Ihrer Daten durchführen, falls Ihre erste Synchronisierung fehlgeschlagen ist, auch wenn Sie die Option Vollsynchronisierung nicht als Synchronisierungsmodusoption wählen. Sie können wählen zwischen:
  - `FORCED_FULL_CRAWL`um den gesamten Inhalt neu zu indizieren und vorhandene Inhalte jedes Mal zu ersetzen, wenn Ihre Datenquelle mit Ihrem Index synchronisiert wird.
  - `FULL_CRAWL`um bei jeder Synchronisierung Ihrer Datenquelle mit Ihrem Index nur neue, geänderte und gelöschte Inhalte zu indizieren. Amazon Kendra kann den Mechanismus Ihrer Datenquelle verwenden, um Inhaltsänderungen nachzuverfolgen und Inhalte zu indexieren, die sich seit der letzten Synchronisierung geändert haben.
  - `CHANGE_LOG`um jedes Mal, wenn Ihre Datenquelle mit Ihrem Index synchronisiert wird, nur neue und geänderte Inhalte zu indizieren. Amazon Kendra kann den Mechanismus Ihrer Datenquelle verwenden, um Inhaltsänderungen nachzuverfolgen und Inhalte zu indexieren, die sich seit der letzten Synchronisierung geändert haben.
- Geheimer Amazon-Ressourcenname (ARN) — Geben Sie den Amazon-Ressourcennamen (ARN) eines Secrets Manager Geheimnisses ein, das die Authentifizierungsdaten für Ihr Microsoft Exchange-Konto enthält. Das Geheimnis wird in einer JSON-Struktur mit den folgenden Schlüsseln gespeichert:

```
{
    "clientId": "client ID",
    "clientSecret": "client secret"
}
```

> **Note**
>
> Wir empfehlen Ihnen, Ihre Anmeldeinformationen und Ihr Geheimnis regelmäßig zu aktualisieren oder zu wechseln. Stellen Sie zu Ihrer eigenen Sicherheit nur die Zugriffsebene bereit, die erforderlich ist. Wir raten davon ab, Anmeldeinformationen und geheime Daten für alle Datenquellen und Connector-Versionen 1.0 und 2.0 (sofern zutreffend) wiederzuverwenden.

- IAM role — Geben Sie an`RoleArn`, wann Sie anrufen`CreateDataSource`, um einer IAM Rolle Berechtigungen für den Zugriff auf Ihr Secrets Manager Geheimnis und den Aufruf der erforderlichen öffentlichen APIs für den Microsoft Exchange-Connector und Amazon Kendra zuzuweisen. Weitere Informationen finden Sie unter IAM Rollen für Microsoft Exchange-Datenquellen.

Sie können auch die folgenden optionalen Funktionen hinzufügen:

- Virtual Private Cloud (VPC) — Geben Sie an, `VpcConfiguration` wann Sie anrufen. `CreateDataSource` Weitere Informationen finden Sie unter Konfigurieren von Amazon Kendra für die Verwendung eines Amazon VPC.
- Inklusions- und Ausschlussfilter — Geben Sie an, ob bestimmte Seiten und Ressourcen ein- oder ausgeschlossen werden sollen.

> **Note**
>
> Die meisten Datenquellen verwenden Muster für reguläre Ausdrücke, bei denen es sich um Ein- oder Ausschlussmuster handelt, die als Filter bezeichnet werden. Wenn Sie einen Einschlussfilter angeben, werden nur Inhalte indexiert, die dem Einschlussfilter entsprechen. Jedes Dokument, das nicht dem Einschlussfilter entspricht, wird nicht indexiert. Wenn Sie einen Ein- und Ausschlussfilter angeben, werden Dokumente, die dem Ausschlussfilter entsprechen, nicht indexiert, auch wenn sie dem Einschlussfilter entsprechen.

- Benutzerkontextfilterung und Zugriffskontrolle —Amazon Kendra durchsucht die Zugriffskontrollliste (ACL) für Ihre Dokumente, sofern Sie über eine ACL für Ihre Dokumente verfügen. Die ACL-Informationen werden verwendet, um Suchergebnisse nach dem Benutzer- oder Gruppenzugriff auf Dokumente zu filtern. Weitere Informationen finden Sie unter Benutzerkontextfilterung.
- Feldzuordnungen — Wählen Sie diese Option, um Ihre Microsoft Exchange-Datenquellenfelder Ihren Amazon Kendra Indexfeldern zuzuordnen. Weitere Informationen finden Sie unter Zuweisen von Datenquellenfeldern.

> **Note**
>
> Das Textfeld oder das entsprechende Textfeld für Ihre Dokumente ist erforderlich, um Ihre Dokumente durchsuchen Amazon Kendra zu können. Sie müssen den

Feldnamen Ihres Dokumenthauptteils in Ihrer Datenquelle dem Namen des Indexfeldes zuordnen_document_body. Alle anderen Felder sind optional.

Weitere Informationen

Weitere Informationen zur Integration Amazon Kendra mit Ihrer Microsoft Exchange-Datenquelle finden Sie unter:

- Indizieren Sie Ihre Microsoft Exchange-Inhalte mit dem Exchange-Connector für Amazon Kendra

Microsoft OneDrive

Microsoft OneDrive ist ein Cloud-basierter Speicherdienst, mit dem Sie Ihre Inhalte speichern, teilen und hosten können. Sie können Amazon Kendra es verwenden, um Ihre OneDrive Datenquelle zu indizieren.

Sie können über Amazon Kendra die Amazon Kendra Konsole und die OneDriveConfigurationAPI eine Verbindung zu Ihrer OneDrive Datenquelle herstellen.

Amazon Kendra hat zwei Versionen des OneDrive Connectors. Zu den unterstützten Funktionen jeder Version gehören:

OneDrive Microsoft-Konnektor V1.0//API OneDriveConfiguration

- Feldzuordnungen
- Einschluss-/Ausschlussfilter

OneDrive Microsoft-Konnektor V2.0//API TemplateConfiguration

- Filterung des Benutzerkontextes
- Crawler zur Benutzeridentität
- Einschluss-/Ausschlussfilter
- Vollständige und inkrementelle Inhaltssynchronisierung
- Virtual Private Cloud (VPC)

> **Note**
>
> Die Support für OneDrive Connector OneDriveConfiguration V1.0/API wird voraussichtlich im Juni 2023 eingestellt. Wir empfehlen die Verwendung von OneDrive Connector V2.0 TemplateConfiguration /API.

Informationen zur Fehlerbehebung bei Ihrem Amazon Kendra OneDrive Datenquellen-Connector finden Sie unterProblembehandlung bei Datenquellen.

Themen

- OneDrive Microsoft-Konnektor V1.0
- OneDrive Microsoft-Anschluss V2.0
- Weitere Informationen

OneDrive Microsoft-Konnektor V1.0

Microsoft OneDrive ist ein Cloud-basierter Speicherdienst, mit dem Sie Ihre Inhalte speichern, teilen und hosten können. Sie können Amazon Kendra es verwenden, um Ihre OneDrive Microsoft-Datenquelle zu indizieren.

> **Note**
>
> Die Support für OneDrive Connector V1.0/ Microsft OneDrive API wird voraussichtlich im Juni 2023 eingestellt. Wir empfehlen die Verwendung von OneDrive Connector V2.0 /API. TemplateConfiguration

Informationen zur Fehlerbehebung bei Ihrem Amazon Kendra OneDrive Datenquellen-Connector finden Sie unterProblembehandlung bei Datenquellen.

Themen

- Unterstützte Features
- Voraussetzungen
- Anweisungen zur Verbindung

Unterstützte Features

- Feldzuordnungen
- Einschluss-/Ausschlussfilter

Voraussetzungen

Bevor Sie Ihre OneDrive Datenquelle Amazon Kendra zum Indizieren verwenden können, nehmen Sie diese Änderungen in Ihren OneDrive Konten und Konten vor. AWS

Stellen Sie in Ihrem Azure Active Directory (AD) sicher, dass Sie über Folgendes verfügen:

- Eine Azure Active Directory (AD) -Anwendung erstellt.
- Hat die AD-Anwendungs-ID verwendet, um einen geheimen Schlüssel für die Anwendung auf der AD-Site zu registrieren. Der geheime Schlüssel muss die Anwendungs-ID und einen geheimen Schlüssel enthalten.
- Die AD-Domäne der Organisation wurde kopiert.
- Ihrer AD-Anwendung wurden mit der Option Microsoft Graph die folgenden Anwendungsberechtigungen hinzugefügt:
  - Dateien in allen Websitesammlungen lesen (File.Read.All)
  - Lesen Sie das vollständige Profil aller Benutzer (User.Read.All)
  - Lesen Sie die Verzeichnisdaten (Directory.Read.All)
  - Alle Gruppen lesen (Group.Read.All)
  - Elemente in allen Websitesammlungen lesen (Site.Read.All)
- Die Liste der Benutzer wurde kopiert, deren Dokumente indexiert werden müssen. Sie können wählen, ob Sie eine Liste mit Benutzernamen angeben möchten, oder Sie können die Benutzernamen in einer Datei angeben, die in einer gespeichert ist Amazon S3. Nachdem Sie die Datenquelle erstellt haben, können Sie:
  - Die Benutzerliste ändern.
  - Wechseln Sie von einer Benutzerliste zu einer in einem Amazon S3 Bucket gespeicherten Liste.
  - Ändern Sie den Amazon S3 Bucket-Speicherort einer Benutzerliste. Wenn Sie den Bucket-Speicherort ändern, müssen Sie auch die IAM Rolle für die Datenquelle aktualisieren, damit sie Zugriff auf den Bucket hat.

> **Note**
>
> Wenn Sie die Liste der Benutzernamen in einem Amazon S3 Bucket speichern, muss die IAM Richtlinie für die Datenquelle den Zugriff auf den Bucket und gegebenenfalls den Zugriff auf den Schlüssel ermöglichen, mit dem der Bucket verschlüsselt wurde.

- Aktiviert, dass jedes Dokument in OneDrive und zwischen anderen Datenquellen, die Sie für denselben Index verwenden möchten, einzigartig ist. Jede Datenquelle, die Sie für einen Index verwenden möchten, darf nicht dasselbe Dokument in allen Datenquellen enthalten. Dokument-IDs gelten für einen Index global und müssen pro Index eindeutig sein.

Stellen Sie sicher AWS-Konto, dass Sie Folgendes in Ihrem haben:

- Hat einen Amazon Kendra Index erstellt und bei Verwendung der API die Index-ID notiert.
- Sie haben eine IAM Rolle für Ihre Datenquelle erstellt und, falls Sie die API verwenden, den ARN der IAM Rolle notiert.

> **Note**
>
> Wenn Sie Ihren Authentifizierungstyp und Ihre Anmeldeinformationen ändern, müssen Sie Ihre IAM Rolle aktualisieren, um auf die richtige AWS Secrets Manager geheime ID zugreifen zu können.

- Wir haben Ihre OneDrive Authentifizierungsdaten AWS Secrets Manager geheim gespeichert und, falls Sie die API verwenden, den ARN des Geheimnisses notiert.

> **Note**
>
> Wir empfehlen Ihnen, Ihre Anmeldeinformationen und Ihr Geheimnis regelmäßig zu aktualisieren oder zu wechseln. Stellen Sie zu Ihrer eigenen Sicherheit nur die Zugriffsebene bereit, die erforderlich ist. Wir raten davon ab, Anmeldeinformationen und geheime Daten für alle Datenquellen und Connector-Versionen 1.0 und 2.0 (sofern zutreffend) wiederzuverwenden.

Wenn Sie noch keine IAM Rolle oder keinen Schlüssel haben, können Sie die Konsole verwenden, um eine neue IAM Rolle und ein neues Secrets Manager Geheimnis zu erstellen, wenn Sie Ihre

OneDrive Datenquelle mit verbinden. Amazon Kendra Wenn Sie die API verwenden, müssen Sie den ARN einer vorhandenen IAM Rolle und eines Secrets Manager Geheimnisses sowie eine Index-ID angeben.

Anweisungen zur Verbindung

Um eine Verbindung Amazon Kendra zu Ihrer OneDrive Datenquelle herzustellen, müssen Sie Details zu Ihren OneDrive Anmeldeinformationen angeben, damit Sie auf Ihre Daten zugreifen Amazon Kendra können. Falls Sie das noch nicht konfiguriert haben, Amazon Kendra finden Sie OneDrive weitere Informationen unterVoraussetzungen.

Console

Um eine Verbindung Amazon Kendra herzustellen OneDrive

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die Amazon Kendra Konsole.
2. Wählen Sie im linken Navigationsbereich Indizes und dann den Index, den Sie verwenden möchten, aus der Indexliste aus.

   > **Note**
   >
   > Sie können Ihre Einstellungen für die Benutzerzugriffskontrolle unter Indexeinstellungen konfigurieren oder bearbeiten.

3. Wählen Sie auf der Seite Erste Schritte die Option Datenquelle hinzufügen aus.
4. Wählen Sie auf der Seite Datenquelle hinzufügen die Option OneDrive Connector und dann Connector hinzufügen aus.
5. Geben Sie auf der Seite „Datenquellendetails angeben“ die folgenden Informationen ein:

   a. Geben Sie im Feld Name und Beschreibung für Datenquellenname einen Namen für Ihre Datenquelle ein. Sie können Bindestriche, aber keine Leerzeichen verwenden.

   b. (Optional) Beschreibung — Geben Sie eine optionale Beschreibung für Ihre Datenquelle ein.

   c. In Standardsprache — Wählen Sie eine Sprache aus, um Ihre Dokumente nach dem Index zu filtern. Sofern Sie nichts anderes angeben, ist die Standardsprache Englisch. Die in den Metadaten des Dokuments angegebene Sprache hat Vorrang vor der ausgewählten Sprache.

d. Unter Tags für Neues Tag hinzufügen — Fügen Sie optionale Tags hinzu, um Ihre Ressourcen zu durchsuchen und zu filtern oder Ihre Kosten nachzuverfolgen. AWS

e. Wählen Sie Weiter aus.

6. Geben Sie auf der Seite Zugriff und Sicherheit definieren die folgenden Informationen ein:

   a. OneDrive Mandanten-ID — Geben Sie die OneDrive Mandanten-ID ohne das Protokoll ein.

   b. Art der Authentifizierung — Wählen Sie zwischen Neu und Bestehend.

   c. i. Wenn Sie „Bestehend“ wählen, wählen Sie unter „Geheimnis auswählen“ ein vorhandenes Geheimnis aus.

      ii. Wenn Sie Neu wählen, geben Sie die folgenden Informationen in den Abschnitt Neues AWS Secrets Manager Geheimnis ein:

         A. Geheimer Name — Ein Name für Ihr Geheimnis. Das Präfix 'AmazonKendra-OneDrive -' wird Ihrem geheimen Namen automatisch hinzugefügt.

         B. Für Anwendungs-ID und Anwendungskennwort — Geben Sie die Werte für die Authentifizierungsdaten aus Ihrem OneDrive Konto ein und wählen Sie dann Authentifizierung speichern.

   d. IAM Rolle — Wählen Sie eine bestehende IAM Rolle oder erstellen Sie eine neue IAM Rolle, um auf Ihre Repository-Anmeldeinformationen und Indexinhalte zuzugreifen.

      > **Note**
      >
      > IAM Rollen, die für Indizes verwendet werden, können nicht für Datenquellen verwendet werden. Wenn Sie sich nicht sicher sind, ob eine vorhandene Rolle für einen Index oder eine häufig gestellte Frage verwendet wird, wählen Sie Neue Rolle erstellen, um Fehler zu vermeiden.

   e. Wählen Sie Weiter aus.

7. Geben Sie auf der Seite „Synchronisierungseinstellungen konfigurieren“ die folgenden Informationen ein:

   a. Wählen Sie je nach Anwendungsfall zwischen Listendatei und Namensliste.

      i. Wenn Sie „Datei auflisten“ wählen, geben Sie die folgenden Informationen ein:

         - Standort auswählen — Geben Sie den Pfad zu Ihrem Amazon S3 Bucket ein.

Benutzerlistendatei hinzufügen zu Amazon S3 — Wählen Sie diese Option, um Ihre Benutzerlistendateien zu Ihrem Amazon S3 Bucket hinzuzufügen.

Zuordnungen lokaler Benutzergruppen — Wählen Sie diese Option aus, um Ihre Inhalte mithilfe der lokalen Gruppenzuweisung zu filtern.

ii. Wenn Sie „Namensliste“ wählen, geben Sie die folgenden Informationen ein:

- Benutzername — Geben Sie bis zu 10 Benutzerlaufwerke für die Indizierung ein. Um mehr als 10 Benutzer hinzuzufügen, erstellen Sie eine Datei, die die Namen enthält.

  Weitere hinzufügen — Wählen Sie diese Option, um weitere Benutzer hinzuzufügen.

  Zuordnungen lokaler Benutzergruppen — Wählen Sie diese Option aus, um Ihre Inhalte mithilfe der lokalen Gruppenzuweisung zu filtern.

b. Für zusätzliche Konfigurationen — Fügen Sie Muster für reguläre Ausdrücke hinzu, um bestimmte Dateien ein- oder auszuschließen. Sie können bis zu 100 Muster hinzufügen.

c. Wählen Sie im Zeitplan für die Synchronisierungsausführung für Häufigkeit aus, wie oft mit Ihrer Datenquelle synchronisiert Amazon Kendra werden soll.

d. Wählen Sie Weiter aus.

8. Geben Sie auf der Seite Feldzuordnungen festlegen die folgenden Informationen ein:

   a. Für Standard-Datenquellenfelder und Zusätzliche vorgeschlagene Feldzuordnungen — Wählen Sie eines der Amazon Kendra generierten Standard-Datenquellenfelder aus, die Sie Ihrem Index zuordnen möchten.

   b. Wählen Sie Weiter aus.

9. Überprüfen Sie auf der Seite Überprüfen und erstellen, ob die von Ihnen eingegebenen Informationen korrekt sind, und wählen Sie dann Datenquelle hinzufügen aus. Sie können Ihre Informationen auch auf dieser Seite bearbeiten. Ihre Datenquelle wird auf der Seite Datenquellen angezeigt, nachdem die Datenquelle erfolgreich hinzugefügt wurde.

API

Um eine Verbindung Amazon Kendra herzustellen OneDrive

Mithilfe der OneDriveConfigurationAPI müssen Sie Folgendes angeben:

- Mandanten-ID — Geben Sie die Azure Active Directory-Domäne der Organisation an.
- OneDrive Benutzer — Geben Sie die Liste der Benutzerkonten an, deren Dokumente indexiert werden sollen.
- Geheimer Amazon-Ressourcenname (ARN) — Geben Sie den Amazon-Ressourcennamen (ARN) eines Secrets Manager Geheimnisses ein, das die Authentifizierungsdaten für Ihr OneDrive Konto enthält. Das Geheimnis wird in einer JSON-Struktur mit den folgenden Schlüsseln gespeichert:

```
{
    "username": "OAuth client ID",
    "password": "client secret"
}
```

> **Note**
>
> Wir empfehlen Ihnen, Ihre Anmeldeinformationen und Ihr Geheimnis regelmäßig zu aktualisieren oder zu wechseln. Stellen Sie zu Ihrer eigenen Sicherheit nur die Zugriffsebene bereit, die erforderlich ist. Wir raten davon ab, Anmeldeinformationen und geheime Daten für alle Datenquellen und Connector-Versionen 1.0 und 2.0 (sofern zutreffend) wiederzuverwenden.

- IAM Rolle — Geben Sie an`RoleArn`, wann Sie anrufen`CreateDataSource`, um einer IAM Rolle Berechtigungen für den Zugriff auf Ihr Secrets Manager Geheimnis und für den Aufruf der erforderlichen öffentlichen APIs für den OneDrive Connector und zum Aufrufen der erforderlichen öffentlichen APIs zu erteilen. Amazon Kendra Weitere Informationen finden Sie unter IAM Rollen für OneDrive Datenquellen.

Sie können auch die folgenden optionalen Funktionen hinzufügen:

- Inklusions- und Ausschlussfilter — Geben Sie an, ob bestimmte Dokumente ein- oder ausgeschlossen werden sollen.

> **Note**
>
> Die meisten Datenquellen verwenden Muster für reguläre Ausdrücke, bei denen es sich um Ein- oder Ausschlussmuster handelt, die als Filter bezeichnet werden. Wenn Sie einen Einschlussfilter angeben, werden nur Inhalte indexiert, die dem Einschlussfilter

entsprechen. Jedes Dokument, das nicht dem Einschlussfilter entspricht, wird nicht indexiert. Wenn Sie einen Ein- und Ausschlussfilter angeben, werden Dokumente, die dem Ausschlussfilter entsprechen, nicht indexiert, auch wenn sie dem Einschlussfilter entsprechen.

- Feldzuordnungen — Wählen Sie diese Option, um Ihre OneDrive Datenquellenfelder Ihren Indexfeldern zuzuordnen. Amazon Kendra Weitere Informationen finden Sie unter Zuweisen von Datenquellenfeldern.

> **Note**
>
> Das Textfeld oder das entsprechende Textfeld für Ihre Dokumente ist erforderlich, um Ihre Dokumente durchsuchen Amazon Kendra zu können. Sie müssen den Feldnamen Ihres Dokumenthauptteils in Ihrer Datenquelle dem Namen des Indexfeldes zuordnen `_document_body`. Alle anderen Felder sind optional.

- Benutzerkontextfilterung und ZugriffskontrolleAmazon Kendra — durchsucht die Zugriffskontrollliste (ACL) für Ihre Dokumente, sofern Sie über eine ACL für Ihre Dokumente verfügen. Die ACL-Informationen werden verwendet, um Suchergebnisse nach dem Benutzer- oder Gruppenzugriff auf Dokumente zu filtern. Weitere Informationen finden Sie unter Benutzerkontextfilterung.

OneDrive Microsoft-Anschluss V2.0

Microsoft OneDrive ist ein Cloud-basierter Speicherdienst, mit dem Sie Ihre Inhalte speichern, teilen und hosten können. Sie können Amazon Kendra es verwenden, um Ihre OneDrive Datenquelle zu indizieren.

Sie können über Amazon Kendra die Amazon Kendra Konsole und die OneDriveConfigurationAPI eine Verbindung zu Ihrer OneDrive Datenquelle herstellen.

> **Note**
>
> Die Support für OneDrive Connector V1.0/ OneDriveConfiguration API wird voraussichtlich im Juni 2023 eingestellt. Wir empfehlen die Verwendung von OneDrive Connector V2.0/ TemplateConfiguration API. Version 2.0 bietet zusätzliche ACLs und Identity Crawler-Funktionen.

Informationen zur Fehlerbehebung bei Ihrem Amazon Kendra OneDrive Datenquellen-Connector finden Sie unter. Problembehandlung bei Datenquellen

Themen

- Unterstützte Features
- Voraussetzungen
- Anweisungen zur Verbindung

Unterstützte Features

Amazon Kendra OneDrive Ein Datenquellenconnector unterstützt die folgenden Funktionen:

- Feldzuordnungen
- Filterung des Benutzerkontextes
- Crawler zur Benutzeridentität
- Einschluss-/Ausschlussfilter
- Vollständige und inkrementelle Inhaltssynchronisierung
- Virtual Private Cloud (VPC)

Voraussetzungen

Bevor Sie Ihre OneDrive Datenquelle Amazon Kendra zum Indizieren verwenden können, nehmen Sie diese Änderungen in Ihren Konten OneDrive und AWS Konten vor.

Stellen Sie sicher OneDrive, dass Sie Folgendes haben:

- Ein OneDrive Konto in Office 365 erstellt.
- Haben Sie Ihre Microsoft 365-Mandanten-ID notiert. Sie finden Ihre Mandanten-ID in den Eigenschaften Ihres Azure Active Directory-Portals oder in Ihrer OAuth-Anwendung.
- Sie haben eine OAuth-Anwendung im Azure-Portal erstellt und die Client-ID und das Kundengeheimnis oder die Kundenanmeldedaten notiert. Weitere Informationen finden Sie im Microsoft-Tutorial und im Beispiel für registrierte Apps.

> **Note**
>
> Wenn Sie eine App im Azure-Portal erstellen oder registrieren, stellt die geheime ID den tatsächlichen geheimen Wert dar. Sie müssen den tatsächlichen geheimen Wert sofort bei

der Erstellung des Geheimnisses und der App notieren oder speichern. Sie können auf Ihr Geheimnis zugreifen, indem Sie den Namen Ihrer Anwendung im Azure-Portal auswählen und dann zur Menüoption für Zertifikate und Geheimnisse navigieren.
Sie können auf Ihre Client-ID zugreifen, indem Sie den Namen Ihrer Anwendung im Azure-Portal auswählen und dann zur Übersichtsseite navigieren. Die Anwendungs-ID (Client) ist die Client-ID.

- Hat die AD-Anwendungs-ID verwendet, um einen geheimen Schlüssel für die Anwendung auf der AD-Site zu registrieren. Der geheime Schlüssel muss die Anwendungs-ID und einen geheimen Schlüssel enthalten.
- Die AD-Domäne der Organisation wurde kopiert.
- Ihrer AD-Anwendung wurden die folgenden Berechtigungen für die Microsoft Graph-Option hinzugefügt:
  - Dateien in allen Websitesammlungen lesen (File.Read.All)
  - Lesen Sie die vollständigen Profile aller Benutzer (User.Read.All)
  - Alle Gruppen lesen (Group.Read.All)
  - Alle Notizen lesen (Notes.Read.All)
- Die Liste der Benutzer wurde kopiert, deren Dokumente indexiert werden müssen. Sie können wählen, ob Sie eine Liste mit Benutzernamen angeben möchten, oder Sie können die Benutzernamen in einer Datei angeben, die in einer gespeichert ist Amazon S3. Nachdem Sie die Datenquelle erstellt haben, können Sie:
  - Die Benutzerliste ändern.
  - Wechseln Sie von einer Benutzerliste zu einer in einem Amazon S3 Bucket gespeicherten Liste.
  - Ändern Sie den Amazon S3 Bucket-Speicherort einer Benutzerliste. Wenn Sie den Bucket-Speicherort ändern, müssen Sie auch die IAM Rolle für die Datenquelle aktualisieren, damit sie Zugriff auf den Bucket hat.

> **Note**
>
> Wenn Sie die Liste der Benutzernamen in einem Amazon S3 Bucket speichern, muss die IAM Richtlinie für die Datenquelle den Zugriff auf den Bucket und gegebenenfalls den Zugriff auf den Schlüssel ermöglichen, mit dem der Bucket verschlüsselt wurde.
> Der OneDrive Connector verwendet E-Mail von Kontaktinformationen, die in den OneDrive-Benutzereigenschaften vorhanden sind. Stellen Sie sicher, dass für den

Benutzer, dessen Daten Sie crawlen möchten, das E-Mail-Feld auf der Seite mit den Kontaktinformationen konfiguriert ist, da es für neue Benutzer möglicherweise leer ist.

Stellen Sie sicher, dass Sie in Ihrem AWS Konto Folgendes haben:

- Hat einen Amazon Kendra Index erstellt und bei Verwendung der API die Index-ID notiert.
- Sie haben eine IAM Rolle für Ihre Datenquelle erstellt und, falls Sie die API verwenden, den ARN der IAM Rolle notiert.
- Wir haben Ihre OneDrive Authentifizierungsdaten AWS Secrets Manager geheim gespeichert und, falls Sie die API verwenden, den ARN des Geheimnisses notiert.

Wenn Sie noch keine IAM Rolle oder keinen Schlüssel haben, können Sie die Konsole verwenden, um eine neue IAM Rolle und ein neues Secrets Manager Geheimnis zu erstellen, wenn Sie Ihre OneDrive Datenquelle mit verbinden Amazon Kendra. Wenn Sie die API verwenden, müssen Sie den ARN einer vorhandenen IAM Rolle und eines Secrets Manager Geheimnisses sowie eine Index-ID angeben.

Anweisungen zur Verbindung

Um eine Verbindung Amazon Kendra zu Ihrer OneDrive Datenquelle herzustellen, müssen Sie Details zu Ihren OneDrive Anmeldeinformationen angeben, damit Sie auf Ihre Daten zugreifen Amazon Kendra können. Falls Sie das noch nicht konfiguriert haben Amazon Kendra, finden Sie OneDrive weitere Informationen unterVoraussetzungen.

Console

Um eine Verbindung Amazon Kendra herzustellen OneDrive

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die Amazon Kendra Konsole.
2. Wählen Sie im linken Navigationsbereich Indizes und dann den Index, den Sie verwenden möchten, aus der Indexliste aus.

> **Note**
>
> Sie können Ihre Einstellungen für die Benutzerzugriffskontrolle unter Indexeinstellungen konfigurieren oder bearbeiten.

3. Wählen Sie auf der Seite Erste Schritte die Option Datenquelle hinzufügen aus.
4. Wählen Sie auf der Seite Datenquelle hinzufügen die Option OneDrive Connector und dann Connector hinzufügen aus.
5. Geben Sie auf der Seite „Datenquellendetails angeben“ die folgenden Informationen ein:
    a. Geben Sie im Feld Name und Beschreibung für Datenquellenname einen Namen für Ihre Datenquelle ein. Sie können Bindestriche, aber keine Leerzeichen verwenden.
    b. (Optional) Beschreibung — Geben Sie eine optionale Beschreibung für Ihre Datenquelle ein.
    c. In Standardsprache — Wählen Sie eine Sprache aus, um Ihre Dokumente nach dem Index zu filtern. Sofern Sie nichts anderes angeben, ist die Standardsprache Englisch. Die in den Metadaten des Dokuments angegebene Sprache hat Vorrang vor der ausgewählten Sprache.
    d. Unter Tags für Neues Tag hinzufügen — Fügen Sie optionale Tags hinzu, um Ihre Ressourcen zu durchsuchen und zu filtern oder Ihre Kosten nachzuverfolgen. AWS
    e. Wählen Sie Weiter aus.
6. Geben Sie auf der Seite Zugriff und Sicherheit definieren die folgenden Informationen ein:
    a. OneDrive Mandanten-ID — Geben Sie die OneDrive Mandanten-ID ohne das Protokoll ein.
    b. Autorisierung — Aktivieren oder deaktivieren Sie die Informationen der Zugriffskontrollliste (ACL) für Ihre Dokumente, wenn Sie über eine ACL verfügen und diese für die Zugriffskontrolle verwenden möchten. Die ACL gibt an, auf welche Dokumente Benutzer und Gruppen zugreifen können. Die ACL-Informationen werden verwendet, um Suchergebnisse nach dem Benutzer- oder Gruppenzugriff auf Dokumente zu filtern. Weitere Informationen finden Sie unter Benutzerkontextfilterung.
    c. Bei der Authentifizierung — Wählen Sie zwischen „Neu“ und „Bestehend“.
    d. i. Wenn Sie „Existierend“ wählen, wählen Sie unter „Geheimnis auswählen“ ein vorhandenes Geheimnis aus.
        ii. Wenn Sie Neu wählen, geben Sie die folgenden Informationen in den Abschnitt Neues AWS Secrets Manager Geheimnis ein:
            A. Geheimer Name — Ein Name für Ihr Geheimnis. Das Präfix 'AmazonKendra-OneDrive -' wird Ihrem geheimen Namen automatisch hinzugefügt.

B. Für Client ID und Client Secret — Geben Sie die Client-ID und den geheimen Client-Schlüssel ein und wählen Sie dann Authentifizierung speichern aus.

e. Unter VPC und Sicherheitsgruppe konfigurieren — optional, für Virtual Private Cloud (VPC) — können Sie wählen, ob Sie eine VPC verwenden möchten. In diesem Fall müssen Sie Subnetze und VPC-Sicherheitsgruppen hinzufügen.

f. Identity Crawler — Geben Sie an, ob der Identity Crawler aktiviert Amazon Kendra werden soll. Der Identity Crawler verwendet die Informationen der Zugriffskontrollliste (ACL) für Ihre Dokumente, um Suchergebnisse nach dem Benutzer- oder Gruppenzugriff auf Dokumente zu filtern. Wenn Sie über eine ACL für Ihre Dokumente verfügen und sich dafür entscheiden, Ihre ACL zu verwenden, können Sie auch den Identity Crawler aktivieren, um die Benutzerkontextfilterung von Suchergebnissen zu konfigurieren. Amazon Kendra Andernfalls können alle Dokumente öffentlich durchsucht werden, wenn Identity Crawler ausgeschaltet ist. Wenn Sie die Zugriffskontrolle für Ihre Dokumente verwenden möchten und Identity Crawler ausgeschaltet ist, können Sie alternativ die PutPrincipalMappingAPI verwenden, um Benutzer- und Gruppenzugriffsinformationen für die Benutzerkontextfilterung hochzuladen.

g. IAM Rolle — Wählen Sie eine bestehende IAM Rolle oder erstellen Sie eine neue IAM Rolle, um auf Ihre Repository-Anmeldeinformationen und Indexinhalte zuzugreifen.

> **Note**
>
> IAM Rollen, die für Indizes verwendet werden, können nicht für Datenquellen verwendet werden. Wenn Sie sich nicht sicher sind, ob eine vorhandene Rolle für einen Index oder eine häufig gestellte Frage verwendet wird, wählen Sie Neue Rolle erstellen, um Fehler zu vermeiden.

h. Wählen Sie Weiter aus.

7. Geben Sie auf der Seite „Synchronisierungseinstellungen konfigurieren“ die folgenden Informationen ein:

8. a. Für den Synchronisierungsbereich — Wählen Sie aus, welche OneDrive Benutzerdaten indexiert werden sollen. Sie können maximal 10 Benutzer manuell hinzufügen.

b. Für zusätzliche Konfigurationen — Fügen Sie Muster für reguläre Ausdrücke hinzu, um bestimmte Inhalte ein- oder auszuschließen. Sie können bis zu 100 Muster hinzufügen.

c. Synchronisierungsmodus — Wählen Sie aus, wie Sie Ihren Index aktualisieren möchten, wenn sich der Inhalt Ihrer Datenquelle ändert. Wenn Sie Ihre Datenquelle

Amazon Kendra zum ersten Mal synchronisieren, werden alle Inhalte standardmäßig gecrawlt und indexiert. Sie müssen eine vollständige Synchronisierung Ihrer Daten durchführen, falls Ihre erste Synchronisierung fehlgeschlagen ist, auch wenn Sie die Option Vollsynchronisierung nicht als Synchronisierungsmodusoption wählen.

- Vollständige Synchronisierung: Indizieren Sie den gesamten Inhalt neu und ersetzen die vorhandenen Inhalte jedes Mal, wenn Ihre Datenquelle mit Ihrem Index synchronisiert wird.
- Neue, geänderte Synchronisierung: Indizieren Sie jedes Mal, wenn Ihre Datenquelle mit Ihrem Index synchronisiert wird, nur neue und geänderte Inhalte. Amazon Kendra kann den Mechanismus Ihrer Datenquelle verwenden, um Inhaltsänderungen nachzuverfolgen und Inhalte zu indexieren, die sich seit der letzten Synchronisierung geändert haben.
- Neue, geänderte, gelöschte Synchronisierung: Indizieren Sie bei jeder Synchronisierung Ihrer Datenquelle mit Ihrem Index nur neue, geänderte und gelöschte Inhalte. Amazon Kendra kann den Mechanismus Ihrer Datenquelle verwenden, um Inhaltsänderungen nachzuverfolgen und Inhalte zu indexieren, die sich seit der letzten Synchronisierung geändert haben.

d. Wählen Sie im Zeitplan für die Synchronisierungsausführung unter Frequenz aus, wie oft mit Ihrer Datenquelle synchronisiert Amazon Kendra werden soll.

e. Wählen Sie Weiter aus.

9. Geben Sie auf der Seite Feldzuordnungen festlegen die folgenden Informationen ein:

   a. Für Standard-Datenquellenfelder und Zusätzliche vorgeschlagene Feldzuordnungen — Wählen Sie eines der Amazon Kendra generierten Standard-Datenquellenfelder aus, die Sie Ihrem Index zuordnen möchten.

   b. Wählen Sie Weiter aus.

10. Überprüfen Sie auf der Seite Überprüfen und erstellen, ob die von Ihnen eingegebenen Informationen korrekt sind, und wählen Sie dann Datenquelle hinzufügen aus. Sie können Ihre Informationen auch auf dieser Seite bearbeiten. Ihre Datenquelle wird auf der Seite Datenquellen angezeigt, nachdem die Datenquelle erfolgreich hinzugefügt wurde.

API

Um eine Verbindung Amazon Kendra herzustellen OneDrive

Sie müssen mithilfe der TemplateConfigurationAPI einen JSON-Wert des Datenquellenschemas angeben. Sie müssen die folgenden Informationen angeben:

- Datenquelle — Geben Sie den Datenquellentyp wie `ONEDRIVEV2` bei der Verwendung des TemplateConfigurationJSON-Schemas an. Geben Sie außerdem die Datenquelle so an`TEMPLATE`, wie Sie die CreateDataSourceAPI aufrufen.
- Mandanten-ID — Geben Sie die Microsoft 365-Mandanten-ID an. Sie finden Ihre Mandanten-ID in den Eigenschaften Ihres Azure Active Directory-Portals oder in Ihrer OAuth-Anwendung.
- Synchronisierungsmodus — Geben Sie an, wie Ihr Index aktualisiert Amazon Kendra werden soll, wenn sich der Inhalt Ihrer Datenquelle ändert. Wenn Sie Ihre Datenquelle Amazon Kendra zum ersten Mal synchronisieren, werden alle Inhalte standardmäßig gecrawlt und indexiert. Sie müssen eine vollständige Synchronisierung Ihrer Daten durchführen, falls Ihre erste Synchronisierung fehlgeschlagen ist, auch wenn Sie die Option Vollsynchronisierung nicht als Synchronisierungsmodusoption wählen. Sie können wählen zwischen:
  - `FORCED_FULL_CRAWL`um den gesamten Inhalt neu zu indizieren und vorhandene Inhalte jedes Mal zu ersetzen, wenn Ihre Datenquelle mit Ihrem Index synchronisiert wird.
  - `FULL_CRAWL`um bei jeder Synchronisierung Ihrer Datenquelle mit Ihrem Index nur neue, geänderte und gelöschte Inhalte zu indizieren. Amazon Kendra kann den Mechanismus Ihrer Datenquelle verwenden, um Inhaltsänderungen nachzuverfolgen und Inhalte zu indexieren, die sich seit der letzten Synchronisierung geändert haben.
  - `CHANGE_LOG`um jedes Mal, wenn Ihre Datenquelle mit Ihrem Index synchronisiert wird, nur neue und geänderte Inhalte zu indizieren. Amazon Kendra kann den Mechanismus Ihrer Datenquelle verwenden, um Inhaltsänderungen nachzuverfolgen und Inhalte zu indexieren, die sich seit der letzten Synchronisierung geändert haben.
- Geheimer Amazon-Ressourcenname (ARN) — Geben Sie den Amazon-Ressourcennamen (ARN) eines Secrets Manager Geheimnisses ein, das die Authentifizierungsdaten enthält, die Sie in Ihrem OneDrive Konto erstellt haben.

  Wenn Sie die OAuth 2.0-Authentifizierung verwenden, wird das Geheimnis in einer JSON-Struktur mit den folgenden Schlüsseln gespeichert:

```
{
    "clientId": "client ID",
    "clientSecret": "client secret"
}
```

> **Note**
>
> Wir empfehlen Ihnen, Ihre Anmeldeinformationen und Ihr Geheimnis regelmäßig zu aktualisieren oder zu wechseln. Stellen Sie zu Ihrer eigenen Sicherheit nur die Zugriffsebene bereit, die erforderlich ist. Wir raten davon ab, Anmeldeinformationen und geheime Daten für alle Datenquellen und Connector-Versionen 1.0 und 2.0 (sofern zutreffend) wiederzuverwenden.

- IAM Rolle — Geben Sie an`RoleArn`, wann Sie anrufen`CreateDataSource`, um einer IAM Rolle Berechtigungen für den Zugriff auf Ihr Secrets Manager Geheimnis und für den Aufruf der erforderlichen öffentlichen APIs für den OneDrive Connector und zum Aufrufen der erforderlichen öffentlichen APIs zu erteilen. Amazon Kendra Weitere Informationen finden Sie unter IAM Rollen für OneDrive Datenquellen.

Sie können auch die folgenden optionalen Funktionen hinzufügen:

- Virtual Private Cloud (VPC) — Geben Sie an, `VpcConfiguration` wann Sie anrufen. `CreateDataSource` Weitere Informationen finden Sie unter Konfigurieren von Amazon Kendra für die Verwendung eines Amazon VPC.
- Inklusions- und Ausschlussfilter — Sie können angeben, ob bestimmte Dateien, OneNote Abschnitte und Seiten ein- oder ausgeschlossen werden sollen. OneNote

> **Note**
>
> Die meisten Datenquellen verwenden Muster für reguläre Ausdrücke, bei denen es sich um Ein- oder Ausschlussmuster handelt, die als Filter bezeichnet werden. Wenn Sie einen Einschlussfilter angeben, werden nur Inhalte indexiert, die dem Einschlussfilter entsprechen. Jedes Dokument, das nicht dem Einschlussfilter entspricht, wird nicht indexiert. Wenn Sie einen Ein- und Ausschlussfilter angeben, werden Dokumente, die dem Ausschlussfilter entsprechen, nicht indexiert, auch wenn sie dem Einschlussfilter entsprechen.

- Identity Crawler — Geben Sie an, ob der Identity Crawler aktiviert Amazon Kendra werden soll. Der Identity Crawler verwendet die Informationen der Zugriffskontrollliste (ACL) für Ihre Dokumente, um Suchergebnisse nach dem Benutzer- oder Gruppenzugriff auf Dokumente zu filtern. Wenn Sie über eine ACL für Ihre Dokumente verfügen und sich dafür

entscheiden, Ihre ACL zu verwenden, können Sie auch den Identity Crawler aktivieren, um die Benutzerkontextfilterung von Suchergebnissen zu konfigurieren. Amazon Kendra Andernfalls können alle Dokumente öffentlich durchsucht werden, wenn Identity Crawler ausgeschaltet ist. Wenn Sie die Zugriffskontrolle für Ihre Dokumente verwenden möchten und Identity Crawler ausgeschaltet ist, können Sie alternativ die PutPrincipalMappingAPI verwenden, um Benutzer- und Gruppenzugriffsinformationen für die Benutzerkontextfilterung hochzuladen.

- Feldzuordnungen — Sie können dem Connector nur integrierte oder allgemeine Indexfelder zuordnen. Amazon Kendra OneDrive Die Zuordnung benutzerdefinierter Felder ist für den OneDrive Connector aufgrund von API-Einschränkungen nicht verfügbar. Weitere Informationen finden Sie unter Zuweisen von Datenquellenfeldern.

Eine Liste weiterer wichtiger JSON-Schlüssel, die konfiguriert werden müssen, finden Sie unter OneDrive Microsoft-Vorlagenschema.

Weitere Informationen

Weitere Informationen zur Integration Amazon Kendra mit Ihrer OneDrive Datenquelle finden Sie unter:

- Ankündigung des aktualisierten OneDrive Microsoft-Connectors (V2) für Amazon Kendra.

Microsoft SharePoint

SharePoint ist ein Dienst zur gemeinsamen Erstellung von Websites, mit dem Sie Webinhalte anpassen und Seiten, Websites, Dokumentbibliotheken und Listen erstellen können. Sie können Amazon Kendra es verwenden, um Ihre SharePoint Datenquelle zu indizieren.

Amazon Kendra unterstützt derzeit SharePoint Online und SharePoint Server (Versionen 2013, 2016, 2019 und Subscription Edition).

Sie können entweder über Amazon Kendra die Amazon Kendra Konsole, die API oder die TemplateConfigurationAPI eine Verbindung zu Ihrer SharePoint Datenquelle herstellen. SharePointConfiguration

Amazon Kendra hat zwei Versionen des SharePoint Connectors. Zu den unterstützten Funktionen jeder Version gehören:

SharePoint Konnektor V1.0/ API SharePointConfiguration

- Änderungsprotokoll
- Feldzuordnungen
- Filterung des Benutzerkontextes
- Einschluss-/Ausschlussfilter
- Virtual Private Cloud (VPC)

SharePoint Konnektor V2.0/API TemplateConfiguration

- Feldzuordnungen
- Filterung des Benutzerkontextes
- Crawling der Benutzeridentität
- Einschluss-/Ausschlussfilter
- Vollständige und inkrementelle Inhaltssynchronisierung
- Virtual Private Cloud (VPC)

> **Note**
>
> Die Support für SharePoint Connector SharePointConfiguration V1.0/API wird voraussichtlich 2023 enden. Wir empfehlen, auf SharePoint Connector V2.0/ API zu migrieren oder diesen zu verwenden. TemplateConfiguration

Informationen zur Fehlerbehebung bei Ihrem Amazon Kendra SharePoint Datenquellen-Connector finden Sie unter. Problembehandlung bei Datenquellen

Themen

- SharePoint Konnektor V1.0
- SharePoint Anschluss V2.0

SharePoint Konnektor V1.0

SharePoint ist ein Dienst zur gemeinsamen Erstellung von Websites, mit dem Sie Webinhalte anpassen und Seiten, Websites, Dokumentbibliotheken und Listen erstellen können. Wenn Sie ein SharePoint Benutzer sind, können Amazon Kendra Sie Ihre SharePoint Datenquelle indizieren.

> **Note**
>
> Die Support für SharePoint Connector SharePointConfiguration V1.0/API wird voraussichtlich 2023 enden. Wir empfehlen, auf SharePoint Connector V2.0/ API zu migrieren oder diesen zu verwenden. TemplateConfiguration

Informationen zur Fehlerbehebung bei Ihrem Amazon Kendra SharePoint Datenquellen-Connector finden Sie unter. Problembehandlung bei Datenquellen

Themen

Unterstützte Features

- Änderungsprotokoll
- Feldzuordnungen
- Filterung des Benutzerkontextes
- Einschluss-/Ausschlussfilter
- Virtual Private Cloud (VPC)

Voraussetzungen

Bevor Sie Ihre SharePoint Datenquelle Amazon Kendra zum Indizieren verwenden können, nehmen Sie diese Änderungen in Ihren SharePoint Konten und Konten vor. AWS

Stellen Sie sicher SharePoint, dass Sie Folgendes haben:

- Notiert die URL der SharePoint Websites, die Sie indexieren möchten.
- Für SharePoint Online:
  - Haben Sie Ihre Basisauthentifizierungsdaten notiert, die einen Benutzernamen und ein Passwort mit Administratorberechtigungen für die Website enthalten.

  - Optional: Generierte OAuth 2.0-Anmeldeinformationen, die einen Benutzernamen, ein Passwort, eine Client-ID und einen geheimen Client-Schlüssel enthalten.
  - Deaktivierte Sicherheitsstandards in Ihrem Azure-Portal mithilfe eines Administratorbenutzers. Weitere Informationen zur Verwaltung von Sicherheitsstandardeinstellungen im Azure-Portal finden Sie in der Microsoft-Dokumentation zum Aktivieren/Deaktivieren von Sicherheitsstandards.
- SharePoint Für Server:
  - Notiert Ihren SharePoint Serverdomänennamen (den NetBIOS-Namen in Ihrem Active Directory). Sie verwenden diesen zusammen mit Ihrem Benutzernamen und Passwort für die SharePoint Standardauthentifizierung, um eine Verbindung zum SharePoint Amazon Kendra Server herzustellen.

> **Note**
>
> Wenn Sie SharePoint Server verwenden und Ihre Access Control List (ACL) in das E-Mail-Format konvertieren müssen, um nach Benutzerkontext zu filtern, geben Sie die URL des LDAP-Servers und die LDAP-Suchbasis an. Oder Sie können die Verzeichnisdomänenüberschreibung verwenden. Die URL des LDAP-Servers ist der vollständige Domainname und die Portnummer (z. B. ldap: //example.com:389). Die LDAP-Suchbasis sind die Domänencontroller „example“ und „com“. Mit der Überschreibung der Verzeichnisdomäne können Sie die E-Mail-Domäne verwenden, anstatt die LDAP-Server-URL und die LDAP-Suchbasis zu verwenden. Die E-Mail-Domain für username@example.com lautet beispielsweise „example.com“. Sie können diese Überschreibung verwenden, wenn Sie sich keine Gedanken über die Validierung Ihrer Domain machen und einfach Ihre E-Mail-Domain verwenden möchten.

- Ihrem SharePoint Konto wurden die folgenden Berechtigungen hinzugefügt:

  Für SharePoint Listen

  - Elemente öffnen — Zeigt die Quelle von Dokumenten mit serverseitigen Dateihandlern an.
  - Anwendungsseiten anzeigen — Formulare, Ansichten und Anwendungsseiten anzeigen. Listen auflisten.
  - Elemente anzeigen — Zeigt Elemente in Listen und Dokumente in Dokumentbibliotheken an.
  - Versionen anzeigen — Frühere Versionen eines Listenelements oder Dokuments anzeigen.

  SharePoint Für Websites

  - Verzeichnisse durchsuchen — Listet Dateien und Ordner auf einer Website mithilfe von SharePoint Designer und der Web-DAV-Schnittstelle auf.
  - Benutzerinformationen durchsuchen — Zeigt Informationen über Benutzer der Website an.
  - Berechtigungen auflisten — Zählt die Berechtigungen für die Website, die Liste, den Ordner, das Dokument oder das Listenelement auf.
  - Öffnen — Öffnet eine Website, eine Liste oder einen Ordner, um auf Elemente innerhalb des Containers zuzugreifen.
  - Client-Integrationsfunktionen verwenden — Verwenden Sie SOAP, WebDAV, das Client-Objektmodell oder SharePoint Designer-Schnittstellen, um auf die Website zuzugreifen.
  - Remote-Schnittstellen verwenden — Verwenden Sie Funktionen, die Client-Anwendungen starten.
  - Seiten anzeigen — Seiten auf einer Website anzeigen.
- Vergewissert, dass jedes Dokument in SharePoint und zwischen anderen Datenquellen, die Sie für denselben Index verwenden möchten, einzigartig ist. Jede Datenquelle, die Sie für einen Index verwenden möchten, darf nicht dasselbe Dokument in allen Datenquellen enthalten. Dokument-IDs gelten für einen Index global und müssen pro Index eindeutig sein.

Stellen Sie sicher AWS-Konto, dass Sie Folgendes in Ihrem haben:

- Hat einen Amazon Kendra Index erstellt und bei Verwendung der API die Index-ID notiert.
- Sie haben eine IAM Rolle für Ihre Datenquelle erstellt und, falls Sie die API verwenden, den ARN der IAM Rolle notiert.

> **Note**
>
> Wenn Sie Ihren Authentifizierungstyp und Ihre Anmeldeinformationen ändern, müssen Sie Ihre IAM Rolle aktualisieren, um auf die richtige AWS Secrets Manager geheime ID zugreifen zu können.

- Wir haben Ihre SharePoint Authentifizierungsdaten AWS Secrets Manager geheim gespeichert und, falls Sie die API verwenden, den ARN des Geheimnisses notiert.

> **Note**
>
> Wir empfehlen Ihnen, Ihre Anmeldeinformationen und Ihr Geheimnis regelmäßig zu aktualisieren oder zu wechseln. Stellen Sie zu Ihrer eigenen Sicherheit nur die

Zugriffsebene bereit, die erforderlich ist. Wir raten davon ab, Anmeldeinformationen und geheime Daten für alle Datenquellen und Connector-Versionen 1.0 und 2.0 (sofern zutreffend) wiederzuverwenden.

Wenn Sie noch keine IAM Rolle oder keinen Schlüssel haben, können Sie die Konsole verwenden, um eine neue IAM Rolle und ein neues Secrets Manager Geheimnis zu erstellen, wenn Sie Ihre SharePoint Datenquelle mit verbinden. Amazon Kendra Wenn Sie die API verwenden, müssen Sie den ARN einer vorhandenen IAM Rolle und eines Secrets Manager Geheimnisses sowie eine Index-ID angeben.

Anweisungen zur Verbindung

Um eine Verbindung Amazon Kendra zu Ihrer SharePoint Datenquelle herzustellen, müssen Sie Details zu Ihren SharePoint Anmeldeinformationen angeben, damit Sie auf Ihre Daten zugreifen Amazon Kendra können. Falls Sie das noch nicht konfiguriert haben, Amazon Kendra finden Sie SharePoint weitere Informationen unterVoraussetzungen.

Console

Um eine Verbindung Amazon Kendra herzustellen SharePoint

1. Melden Sie sich bei der AWS Management Console an und öffnen Sie die Amazon Kendra Konsole.
2. Wählen Sie im linken Navigationsbereich Indizes und dann den Index, den Sie verwenden möchten, aus der Indexliste aus.

   > **Note**
   >
   > Sie können Ihre Einstellungen für die Benutzerzugriffskontrolle unter Indexeinstellungen konfigurieren oder bearbeiten.

3. Wählen Sie auf der Seite Erste Schritte die Option Datenquelle hinzufügen aus.
4. Wählen Sie auf der Seite Datenquelle hinzufügen die Option SharePoint Connector v1.0 und dann Datenquelle hinzufügen aus.
5. Geben Sie auf der Seite „Datenquellendetails angeben“ die folgenden Informationen ein:

   a. Geben Sie im Feld Name und Beschreibung für Datenquellenname einen Namen für Ihre Datenquelle ein. Sie können Bindestriche, aber keine Leerzeichen verwenden.

b. (Optional) Beschreibung — Geben Sie eine optionale Beschreibung für Ihre Datenquelle ein.

c. In Standardsprache — Wählen Sie eine Sprache aus, um Ihre Dokumente nach dem Index zu filtern. Sofern Sie nichts anderes angeben, ist die Standardsprache Englisch. Die in den Metadaten des Dokuments angegebene Sprache hat Vorrang vor der ausgewählten Sprache.

d. Unter Tags für Neues Tag hinzufügen — Fügen Sie optionale Tags hinzu, um Ihre Ressourcen zu durchsuchen und zu filtern oder Ihre Kosten nachzuverfolgen. AWS

e. Wählen Sie Weiter aus.

6. Geben Sie auf der Seite Zugriff und Sicherheit definieren die folgenden Informationen ein:

a. Als Hosting-Methode — Wählen Sie zwischen SharePoint Online und SharePointServer.

i. Für SharePointOnline — Geben Sie die Site-URLs ein, die für Ihr SharePoint Repository spezifisch sind.

ii. Für SharePointServer — Wählen Sie Ihre SharePoint Version, geben Sie die für Ihr SharePoint Repository spezifischen Site-URLs und den Amazon S3 Pfad zum Speicherort Ihres SSL-Zertifikats ein.

b. (Nur SharePoint Server) Für Web-Proxy — Geben Sie den Hostnamen und die Portnummer Ihrer internen SharePoint Instanz ein. Die Portnummer sollte ein numerischer Wert zwischen 0 und 65535 sein.

c. Für die Authentifizierung — Wählen Sie je nach Anwendungsfall zwischen den folgenden Optionen:

i. Für SharePoint Online-Nutzung — Wählen Sie zwischen Standardauthentifizierung und OAuth 2.0-Authentifizierung.

ii. Für SharePoint Server — Wählen Sie zwischen Keine, LDAP und Manuell.

d. Für AWS Secrets Manager geheim — Wählen Sie ein vorhandenes Geheimnis oder erstellen Sie ein neues Secrets Manager Geheimnis, um Ihre Authentifizierungsdaten zu speichern. SharePoint Wenn Sie sich dafür entscheiden, ein neues Geheimnis zu erstellen, wird ein AWS Secrets Manager geheimes Fenster geöffnet. Sie müssen einen geheimen Namen eingeben. Das Präfix 'AmazonKendra- SharePoint -' wird automatisch zu Ihrem geheimen Namen hinzugefügt.

e. Geben Sie die folgenden weiteren Informationen in das Fenster Create an AWS Secrets Manager Secret ein:

i. Wählen Sie je nach Anwendungsfall aus den folgenden SharePoint Cloud-Authentifizierungsoptionen:

   A. Standardauthentifizierung — Geben Sie Ihren SharePoint Kontonutzernamen als Benutzername und das SharePoint Kontopasswort als Passwort ein.

   B. OAuth 2.0-Authentifizierung — Geben Sie Ihren SharePoint Kontonutzernamen als Benutzername, das SharePoint Kontopasswort als Passwort, Ihre automatisch generierte eindeutige SharePoint ID als Client-ID und die gemeinsame geheime Zeichenfolge ein, die von beiden verwendet wird, SharePoint und Amazon Kendra als Client-Geheimnis.

ii. Wählen Sie je nach Anwendungsfall aus den folgenden SharePoint Serverauthentifizierungsoptionen:

   A. Keine — Geben Sie Ihren SharePoint Kontonutzernamen als Benutzername, Ihr SharePoint Kontopasswort als Passwort und Ihren Serverdomänennamen ein.

   B. LDAP — *Geben Sie Ihren SharePoint Kontonutzernamen als **Benutzername**, das SharePoint Kontopasswort als **Passwort**, Ihren **LDAP-Serverendpunkt** (einschließlich Protokoll und Portnummer, z. B. ldap: //example.com:389) und Ihre **LDAP-Suchbasis** (z. B. dc=example, dc=com) ein.*

   C. Manuell — Geben Sie Ihren SharePoint Kontonutzernamen als Benutzername, Ihr Kontopasswort als Passwort und Ihre E-Mail-Domain Override (SharePoint E-Mail-Domäne des Verzeichnisbenutzers oder der Gruppe) ein.

iii. Wählen Sie Speichern.

f. Virtual Private Cloud (VPC) — Sie müssen auch Subnetze und VPC-Sicherheitsgruppen hinzufügen.

> **Note**
>
> Sie müssen eine VPC verwenden, wenn Sie SharePoint Server verwenden. Amazon VPC ist für andere SharePoint Versionen optional.

g. IAM Rolle — Wählen Sie eine bestehende IAM Rolle oder erstellen Sie eine neue IAM Rolle, um auf Ihre Repository-Anmeldeinformationen und Indexinhalte zuzugreifen.

> **Note**
>
> IAM Rollen, die für Indizes verwendet werden, können nicht für Datenquellen verwendet werden. Wenn Sie sich nicht sicher sind, ob eine vorhandene Rolle für einen Index oder eine häufig gestellte Frage verwendet wird, wählen Sie Neue Rolle erstellen, um Fehler zu vermeiden.

h. Wählen Sie Weiter aus.

7. Geben Sie auf der Seite „Synchronisierungseinstellungen konfigurieren“ die folgenden Informationen ein:

   a. Änderungsprotokoll verwenden — Wählen Sie diese Option, um Ihren Index zu aktualisieren, anstatt alle Ihre Dateien zu synchronisieren.

   b. Anlagen crawlen — Wählen Sie diese Option, um Anlagen zu crawlen.

   c. Lokale Gruppenzuordnungen verwenden — Wählen Sie diese Option, um sicherzustellen, dass Dokumente ordnungsgemäß gefiltert werden.

   d. Zusätzliche Konfiguration — Fügen Sie Muster für reguläre Ausdrücke hinzu, um bestimmte Dateien ein- oder auszuschließen. Sie können bis zu 100 Muster hinzufügen.

   e. Zeitplan für die Synchronisierungsausführung für die Frequenz — Wie oft Amazon Kendra wird die Synchronisierung mit Ihrer Datenquelle durchgeführt?

   f. Wählen Sie Weiter aus.

8. Geben Sie auf der Seite Feldzuordnungen festlegen die folgenden Informationen ein:

   a. Amazon Kendra Standard-Feldzuordnungen — Wählen Sie eines der Amazon Kendra generierten Standard-Datenquellenfelder aus, die Sie Ihrem Index zuordnen möchten.

   b. Für benutzerdefinierte Feldzuordnungen — Fügen Sie benutzerdefinierte Datenquellenfelder hinzu, um einen Indexfeldnamen für die Zuordnung und den Felddatentyp zu erstellen.

   c. Wählen Sie Weiter aus.

9. Überprüfen Sie auf der Seite Überprüfen und erstellen, ob die von Ihnen eingegebenen Informationen korrekt sind, und wählen Sie dann Datenquelle hinzufügen aus. Sie können Ihre Informationen auch auf dieser Seite bearbeiten. Ihre Datenquelle wird auf der Seite Datenquellen angezeigt, nachdem die Datenquelle erfolgreich hinzugefügt wurde.

API

Um eine Verbindung Amazon Kendra herzustellen SharePoint

Mithilfe der SharePointConfigurationAPI müssen Sie Folgendes angeben:

- SharePointVersion — Geben Sie die SharePoint Version an, die Sie bei der Konfiguration SharePoint verwenden. Dies ist unabhängig davon der Fall, ob Sie SharePoint Server 2013, SharePoint Server 2016, SharePoint Server 2019 oder SharePoint Online verwenden.
- Geheimer Amazon-Ressourcenname (ARN) — Geben Sie den Amazon-Ressourcennamen (ARN) eines Secrets Manager Geheimnisses ein, das die Authentifizierungsdaten enthält, die Sie in Ihrem SharePoint Konto erstellt haben. Das Geheimnis wird in einer JSON-Struktur gespeichert.

  Für die Standardauthentifizierung im SharePoint Internet muss mindestens die folgende JSON-Struktur in Ihrem Secret enthalten sein:

```
{
    "userName": "user name",
    "password": "password"
}
```

  Für die SharePoint Online-OAuth 2.0-Authentifizierung muss die folgende JSON-Struktur mindestens in Ihrem Geheimnis enthalten sein:

```
{
    "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"
}
```

  Für die SharePoint Server-Basisauthentifizierung ist die folgende Mindest-JSON-Struktur in Ihrem Geheimen enthalten:

```
{
    "userName": "user name",
    "password": "password",
    "domain": "server domain name"
```

```
}
```

Für die SharePoint Server-LDAP-Authentifizierung (wenn Sie Ihre Zugriffskontrollliste (ACL) in das E-Mail-Format konvertieren müssen, um nach Benutzerkontext zu filtern, können Sie die LDAP-Server-URL und die LDAP-Suchbasis in Ihr Geheimnis aufnehmen) ist die folgende JSON-Mindeststruktur, die in Ihrem Geheimnis enthalten sein muss:

```
{
    "userName": "user name",
    "password": "password",
    "domain": "server domain name"
    "ldapServerUrl": "ldap://example.com:389",
    "ldapSearchBase": "dc=example,dc=com"
}
```

Für die manuelle SharePoint Serverauthentifizierung muss die folgende JSON-Struktur mindestens in Ihrem Secret enthalten sein:

```
{
    "userName": "user name",
    "password": "password",
    "domain": "server domain name",
    "emailDomainOverride": "example.com"
}
```

> **Note**
>
> Wir empfehlen, dass Sie Ihre Anmeldeinformationen und Ihren geheimen Schlüssel regelmäßig aktualisieren oder austauschen. Stellen Sie zu Ihrer eigenen Sicherheit nur die Zugriffsebene bereit, die erforderlich ist. Wir raten davon ab, Anmeldeinformationen und geheime Daten für alle Datenquellen und Connector-Versionen 1.0 und 2.0 (sofern zutreffend) wiederzuverwenden.

- IAM Rolle — Geben Sie an`RoleArn`, wann Sie anrufen`CreateDataSource`, um einer IAM Rolle Berechtigungen für den Zugriff auf Ihr Secrets Manager Geheimnis und für den Aufruf der erforderlichen öffentlichen APIs für den SharePoint Connector und zum Aufrufen der erforderlichen öffentlichen APIs zu erteilen. Amazon Kendra Weitere Informationen finden Sie unter IAM Rollen für SharePoint Datenquellen.

- Amazon VPC— Wenn Sie SharePoint Server verwenden, geben Sie dies im `VpcConfiguration` Rahmen der Datenquellenkonfiguration an. Siehe Konfiguration Amazon Kendra für die Verwendung einer VPC.

Sie können auch die folgenden optionalen Funktionen hinzufügen:

- Webproxy — Gibt an, ob Sie über einen Webproxy eine Verbindung zu den URLs Ihrer SharePoint Website herstellen möchten. Sie können diese Option nur für SharePoint Server verwenden.
- Listen indizieren — Gibt an, ob Amazon Kendra der Inhalt von Anlagen zu SharePoint Listenelementen indexiert werden soll.
- Änderungsprotokoll — Gibt an, ob der Mechanismus für das Änderungsprotokoll der SharePoint Datenquelle verwendet werden Amazon Kendra soll, um zu ermitteln, ob ein Dokument im Index aktualisiert werden muss.

> **Note**
>
> Verwenden Sie das Änderungsprotokoll, wenn Sie nicht alle Dokumente scannen Amazon Kendra möchten. Wenn Ihr Änderungsprotokoll umfangreich ist, nimmt das Scannen der Dokumente in der SharePoint Datenquelle möglicherweise Amazon Kendra weniger Zeit in Anspruch als das Verarbeiten des Änderungsprotokolls. Wenn Sie Ihre SharePoint Datenquelle zum ersten Mal mit Ihrem Index synchronisieren, werden alle Dokumente gescannt.

- Inklusions- und Ausschlussfilter — Sie können angeben, ob bestimmte Inhalte ein- oder ausgeschlossen werden sollen.

> **Note**
>
> Die meisten Datenquellen verwenden Muster für reguläre Ausdrücke, bei denen es sich um Ein- oder Ausschlussmuster handelt, die als Filter bezeichnet werden. Wenn Sie einen Einschlussfilter angeben, werden nur Inhalte indexiert, die dem Einschlussfilter entsprechen. Jedes Dokument, das nicht dem Einschlussfilter entspricht, wird nicht indexiert. Wenn Sie einen Ein- und Ausschlussfilter angeben, werden Dokumente, die dem Ausschlussfilter entsprechen, nicht indexiert, auch wenn sie dem Einschlussfilter entsprechen.

- Feldzuordnungen — Wählen Sie diese Option, um Ihre SharePoint Datenquellenfelder Ihren Indexfeldern zuzuordnen. Amazon Kendra Weitere Informationen finden Sie unter Zuweisen von Datenquellenfeldern.

  > **Note**
  >
  > Das Textfeld oder das entsprechende Textfeld für Ihre Dokumente ist erforderlich, um Ihre Dokumente durchsuchen Amazon Kendra zu können. Sie müssen den Feldnamen Ihres Dokumenthauptteils in Ihrer Datenquelle dem Namen des Indexfeldes zuordnen `_document_body`. Alle anderen Felder sind optional.

- Benutzerkontextfilterung und ZugriffskontrolleAmazon Kendra — durchsucht die Zugriffskontrollliste (ACL) für Ihre Dokumente, sofern Sie über eine ACL für Ihre Dokumente verfügen. Die ACL-Informationen werden verwendet, um Suchergebnisse nach dem Benutzer- oder Gruppenzugriff auf Dokumente zu filtern. Weitere Informationen finden Sie unter Benutzerkontextfilterung.

Weitere Informationen

Weitere Informationen zur Integration Amazon Kendra mit Ihrer SharePoint Datenquelle finden Sie unter:

- Erste Schritte mit dem Amazon Kendra SharePoint Online-Connector

SharePoint Anschluss V2.0

SharePoint ist ein Dienst zur gemeinsamen Erstellung von Websites, mit dem Sie Webinhalte anpassen und Seiten, Websites, Dokumentbibliotheken und Listen erstellen können. Sie können Amazon Kendra es verwenden, um Ihre SharePoint Datenquelle zu indizieren.

Amazon Kendra unterstützt derzeit SharePoint Online und SharePoint Server (2013, 2016, 2019 und Subscription Edition).

> **Note**
>
> Die Support für SharePoint Connector SharePointConfiguration V1.0/API wird voraussichtlich 2023 enden. Wir empfehlen, auf SharePoint Connector V2.0/ API zu migrieren oder diesen zu verwenden. TemplateConfiguration

Informationen zur Fehlerbehebung bei Ihrem Amazon Kendra SharePoint Datenquellen-Connector finden Sie unter. Problembehandlung bei Datenquellen

Themen

Unterstützte Features

Amazon Kendra SharePoint Ein Datenquellenconnector unterstützt die folgenden Funktionen:

- Feldzuordnungen
- Filterung des Benutzerkontextes
- Crawling der Benutzeridentität
- Muster für Inklusions- und Ausschlüsse
- Vollständige und inkrementelle Inhaltssynchronisierung
- Virtual Private Cloud (VPC)

Voraussetzungen

Bevor Sie Ihre SharePoint Datenquelle Amazon Kendra zum Indizieren verwenden können, nehmen Sie diese Änderungen in Ihren Konten SharePoint und AWS Konten vor.

Stellen Sie unter SharePoint Online sicher, dass Sie über Folgendes verfügen:

- Ihre SharePoint Instanz-URLs wurden kopiert. Das Format für die Host-URL, die Sie eingeben, ist *`https://yourdomain.sharepoint.com/sites/mysite`*. Ihre URL muss mit beginnen `https` und enthaltensharepoint.com.
- Der Domainname Ihrer SharePoint Instanz-URL wurde kopiert.
- Sie haben Ihre grundlegenden Authentifizierungsdaten notiert, die den Benutzernamen und das Passwort mit Administratorberechtigungen für die Verbindung mit SharePoint Online enthalten.
- Die Sicherheitsstandards wurden in Ihrem Azure-Portal mithilfe eines Administratorbenutzers deaktiviert. Weitere Informationen zur Verwaltung von Sicherheitsstandardeinstellungen im

Azure-Portal finden Sie in der Microsoft-Dokumentation zum Aktivieren/Deaktivieren von Sicherheitsstandards.

- Die Multi-Faktor-Authentifizierung (MFA) wurde in Ihrem SharePoint Konto deaktiviert, sodass das Crawlen Ihrer Inhalte nicht blockiert Amazon Kendra wird. SharePoint
- Wenn Sie einen anderen Authentifizierungstyp als die Standardauthentifizierung verwenden: Die Mandanten-ID Ihrer Instanz wurde kopiert. SharePoint Einzelheiten zum Ermitteln Ihrer Mandanten-ID finden Sie unter Finden Sie Ihre Microsoft 365-Mandanten-ID.
- Wenn Sie zur Cloud-Benutzerauthentifizierung mit Microsoft Entra migrieren müssen, lesen Sie die Microsoft-Dokumentation zur Cloud-Authentifizierung.
- Für die OAuth 2.0-Authentifizierung und die OAuth 2.0-Aktualisierungstoken-Authentifizierung: Notieren Sie sich Ihre Basisauthentifizierungsdaten, die den Benutzernamen und das Passwort enthalten, mit denen Sie eine Verbindung zu SharePoint Online herstellen, sowie die Client-ID und das Client-Geheimnis, die nach der Registrierung bei Azure AD generiert wurden. SharePoint
  - Wenn Sie ACL nicht verwenden, wurden die folgenden Berechtigungen hinzugefügt:

Microsoft Graph	SharePoint
• Notes.Read.All (Anwendung) — Alle Notizbücher lesen OneNote • Sites.Read.All (Application) — Lesen Sie Elemente in allen Websitesammlungen	• AllSites.Read (Delegiert) — Liest Elemente in allen Websitesammlungen

> **Note**
>
> Note.Read.All und Sites.Read.All sind nur erforderlich, wenn Sie Dokumente crawlen möchten. OneNote
> Wenn Sie bestimmte Websites crawlen möchten, kann die Berechtigung auf bestimmte Websites und nicht auf alle in der Domäne verfügbaren Websites beschränkt werden. Sie konfigurieren die Berechtigung Sites.Selected (Anwendung). Mit dieser API-Berechtigung müssen Sie die Zugriffsberechtigung für jede Site explizit über die Microsoft Graph-API festlegen. Weitere Informationen finden Sie im Microsoft-Blog unter Sites.Selected permissions.

  - Wenn Sie ACL verwenden, wurden die folgenden Berechtigungen hinzugefügt:

Microsoft Graph	SharePoint
• Group.Member.Read.All (Application) — Alle Gruppenmitgliedschaften lesen • Notes.Read.All (Application) — Alle OneNote Notizbücher lesen • Websites. FullControl.All (delegiert) — Erforderlich, um ACLs der Dokumente abzurufen • Sites.Read.All (Application) — Liest Elemente in allen Websitesammlungen • User.Read.All (Application) — Liest die vollständigen Profile aller Benutzer	• AllSites.Read (Delegiert) — Liest Elemente in allen Websitesammlungen

> **Note**
>
> GroupMember.Read.All und User.Read.All sind nur erforderlich, wenn Identity Crawler aktiviert ist.
> Wenn Sie bestimmte Websites crawlen möchten, kann die Berechtigung auf bestimmte Websites und nicht auf alle in der Domäne verfügbaren Websites beschränkt werden. Sie konfigurieren die Berechtigung Sites.Selected (Anwendung). Mit dieser API-Berechtigung müssen Sie die Zugriffsberechtigung für jede Site explizit über die Microsoft Graph-API festlegen. Weitere Informationen finden Sie im Microsoft-Blog unter Sites.Selected permissions.

- Für Azure AD-Authentifizierung nur für Apps: Privater Schlüssel und Client-ID, die Sie nach der Registrierung bei SharePoint Azure AD generiert haben. Beachten Sie auch das X.509-Zertifikat.
  - Wenn Sie ACL nicht verwenden, wurden die folgenden Berechtigungen hinzugefügt:

SharePoint
• Sites.Read.All (Application) — Erforderlich für den Zugriff auf Elemente und Listen in allen Websitesammlungen

> **Note**
>
> Wenn Sie bestimmte Websites crawlen möchten, kann die Berechtigung auf bestimmte Websites und nicht auf alle in der Domäne verfügbaren Websites beschränkt werden. Sie konfigurieren die Berechtigung Sites.Selected (Anwendung). Mit dieser API-Berechtigung müssen Sie die Zugriffsberechtigung für jede Site explizit über die Microsoft Graph-API festlegen. Weitere Informationen finden Sie im Microsoft-Blog unter Sites.Selected permissions.

- Wenn Sie ACL verwenden, wurden die folgenden Berechtigungen hinzugefügt:

SharePoint
• Websites. FullControl.All (Application) — Erforderlich, um ACLs der Dokumente abzurufen

> **Note**
>
> Wenn Sie bestimmte Websites crawlen möchten, kann die Berechtigung auf bestimmte Websites und nicht auf alle in der Domäne verfügbaren Websites beschränkt werden. Sie konfigurieren die Berechtigung Sites.Selected (Anwendung). Mit dieser API-Berechtigung müssen Sie die Zugriffsberechtigung für jede Site explizit über die Microsoft Graph-API festlegen. Weitere Informationen finden Sie im Microsoft-Blog unter Sites.Selected permissions.

- Für SharePoint reine App-Authentifizierung: Notiert Ihre SharePoint Client-ID und Ihren geheimen Client-Schlüssel, die bei der Erteilung der Berechtigung für SharePoint App Only generiert

wurden, sowie Ihre Client-ID und Ihren geheimen Client-Schlüssel, die bei der Registrierung Ihrer SharePoint App bei Azure AD generiert wurden.

> **Note**
>
> SharePoint Die reine App-Authentifizierung wird für die Version 2013 nicht unterstützt. SharePoint

- (Optional) Wenn Sie OneNote Dokumente crawlen und Identity Crawler verwenden, wurden die folgenden Berechtigungen hinzugefügt:

Microsoft Graph
• GroupMember.Read.All (Application) — Alle Gruppenmitgliedschaften lesen • Notes.Read.All (Anwendung) — Alle Notizbücher lesen OneNote • Sites.Read.All (Application) — Lesen Sie Elemente in allen Websitesammlungen • User.Read.All (Application) — Liest die vollständigen Profile aller Benutzer

> **Note**
>
> Für das Crawlen von Entitäten mithilfe der Standardauthentifizierung und der reinen App-Authentifizierung sind keine API-Berechtigungen erforderlich. SharePoint

Stellen Sie unter SharePoint Server sicher, dass Sie über Folgendes verfügen:

- Ihre SharePoint Instanz-URLs und den Domainnamen Ihrer SharePoint URLs wurden kopiert. Das Format für die Host-URL, die Sie eingeben, ist *`https://yourcompany/sites/mysite`*. Ihre URL muss mit beginnen`https`.

> **Note**
>
> (On-Premise/Server) Amazon Kendra prüft, ob die AWS Secrets Manager darin enthaltenen Endpunktinformationen mit den Endpunktinformationen übereinstimmen, die in den Konfigurationsdetails Ihrer Datenquelle angegeben sind. Dies trägt zum Schutz vor dem Problem des verwirrten Stellvertreters bei, bei dem es sich um ein Sicherheitsproblem handelt, bei dem ein Benutzer nicht berechtigt ist, eine Aktion auszuführen, sondern ihn Amazon Kendra als Proxy verwendet, um auf das konfigurierte Geheimnis zuzugreifen und die Aktion auszuführen. Wenn Sie Ihre Endpunktinformationen später ändern, müssen Sie ein neues Geheimnis erstellen, um diese Informationen zu synchronisieren.

- Die Multi-Faktor-Authentifizierung (MFA) wurde in Ihrem SharePoint Konto deaktiviert, sodass das Crawlen Ihrer Inhalte nicht blockiert Amazon Kendra wird. SharePoint
- Wenn Sie die reine SharePoint App-Authentifizierung für die Zugriffskontrolle verwenden:
  - Die SharePoint Client-ID wurde kopiert, die bei der Registrierung von App Only auf Site-Ebene generiert wurde. Das Client-ID-Format ist ClientId @TenantId. Zum Beispiel *ffa956f3-8f89-44e7-b0e4-49670756342c @888d0b57 -69f1-4fb8-957f-e1f0bedf82fe*.
  - Das SharePoint Client-Geheimnis, das bei der Registrierung von App Only auf Site-Ebene generiert wurde, wurde kopiert.

  Hinweis: Da Client-IDs und Client-Geheimnisse nur für einzelne Sites generiert werden, wenn Sie den SharePoint Server für die Only-App-Authentifizierung registrieren, wird nur eine Site-URL für die SharePoint Only-App-Authentifizierung unterstützt.

> **Note**
>
> SharePoint Die reine App-Authentifizierung wird für die Version SharePoint 2013 nicht unterstützt.

- Wenn Sie eine E-Mail-ID mit benutzerdefinierter Domain für die Zugriffskontrolle verwenden:
  - *Haben Sie den Wert Ihrer benutzerdefinierten E-Mail-Domain notiert – zum Beispiel: "amazon.com“.*
- Wenn Sie eine E-Mail-ID mit Domain aus der IDP-Autorisierung verwenden, haben Sie Folgendes kopiert:

  - LDAP-Serverendpunkt (Endpunkt des LDAP-Servers einschließlich Protokoll und Portnummer). Zum Beispiel: *ldap: //example.com:389*.
  - LDAP-Suchbasis (Suchbasis des LDAP-Benutzers). Zum Beispiel: *CN=Users, DC=SharePoint, DC=com*.
  - LDAP-Benutzername und LDAP-Passwort.
- Entweder konfigurierte NTLM-Authentifizierungsdaten oder konfigurierte Kerberos-Authentifizierungsanmeldeinformationen, die einen Benutzernamen (Kontobenutzername) und ein SharePoint Passwort (Kontokennwort) enthalten. SharePoint

Stellen Sie sicher AWS-Konto, dass Sie Folgendes in Ihrem haben:

- Hat einen Amazon Kendra Index erstellt und bei Verwendung der API die Index-ID notiert.
- Sie haben eine IAM Rolle für Ihre Datenquelle erstellt und, falls Sie die API verwenden, den ARN der IAM Rolle notiert.

> **Note**
>
> Wenn Sie Ihren Authentifizierungstyp und Ihre Anmeldeinformationen ändern, müssen Sie Ihre IAM Rolle aktualisieren, um auf die richtige AWS Secrets Manager geheime ID zugreifen zu können.

- Wir haben Ihre SharePoint Authentifizierungsdaten AWS Secrets Manager geheim gespeichert und, falls Sie die API verwenden, den ARN des Geheimnisses notiert.

> **Note**
>
> Wir empfehlen Ihnen, Ihre Anmeldeinformationen und Ihr Geheimnis regelmäßig zu aktualisieren oder zu wechseln. Stellen Sie zu Ihrer eigenen Sicherheit nur die Zugriffsebene bereit, die erforderlich ist. Wir raten davon ab, Anmeldeinformationen und geheime Daten für alle Datenquellen und Connector-Versionen 1.0 und 2.0 (sofern zutreffend) wiederzuverwenden.

Wenn Sie noch keine IAM Rolle oder keinen Schlüssel haben, können Sie die Konsole verwenden, um eine neue IAM Rolle und ein neues Secrets Manager Geheimnis zu erstellen, wenn Sie Ihre SharePoint Datenquelle mit verbinden. Amazon Kendra Wenn Sie die API verwenden, müssen Sie

den ARN einer vorhandenen IAM Rolle und eines Secrets Manager Geheimnisses sowie eine Index-ID angeben.

Anweisungen zur Verbindung

Amazon Kendra Um eine Verbindung mit Ihrer SharePoint Datenquelle herzustellen, müssen Sie Details zu Ihren SharePoint Anmeldeinformationen angeben, damit Sie auf Ihre Daten zugreifen Amazon Kendra können. Falls Sie das noch nicht konfiguriert haben, Amazon Kendra finden Sie SharePoint weitere Informationen unterVoraussetzungen.

Console: SharePoint Online

Um eine Verbindung Amazon Kendra zu SharePoint Online herzustellen

1. Melden Sie sich bei der AWS Management Console an und öffnen Sie die Amazon Kendra Konsole.
2. Wählen Sie im linken Navigationsbereich Indizes und dann den Index, den Sie verwenden möchten, aus der Indexliste aus.

   > **Note**
   >
   > Sie können Ihre Einstellungen für die Benutzerzugriffskontrolle unter Indexeinstellungen konfigurieren oder bearbeiten.

3. Wählen Sie auf der Seite Erste Schritte die Option Datenquelle hinzufügen aus.
4. Wählen Sie auf der Seite Datenquelle hinzufügen die Option SharePoint Connector V2.0 und dann Datenquelle hinzufügen aus.
5. Geben Sie auf der Seite „Datenquellendetails angeben“ die folgenden Informationen ein:

   a. Geben Sie im Feld Name und Beschreibung für Datenquellenname einen Namen für Ihre Datenquelle ein. Sie können Bindestriche, aber keine Leerzeichen verwenden.

   b. (Optional) Beschreibung — Geben Sie eine optionale Beschreibung für Ihre Datenquelle ein.

   c. In Standardsprache — Wählen Sie eine Sprache aus, um Ihre Dokumente nach dem Index zu filtern. Sofern Sie nichts anderes angeben, ist die Standardsprache Englisch. Die in den Metadaten des Dokuments angegebene Sprache hat Vorrang vor der ausgewählten Sprache.

d. Unter Tags für Neues Tag hinzufügen — Fügen Sie optionale Tags hinzu, um Ihre Ressourcen zu durchsuchen und zu filtern oder Ihre Kosten nachzuverfolgen. AWS

e. Wählen Sie Weiter aus.

6. Geben Sie auf der Seite Zugriff und Sicherheit definieren die folgenden Informationen ein:

a. Wählen Sie im Feld Quelle für Hosting-Methode die Option SharePointOnline aus.

b. Spezifische Site-URLs für Ihr SharePoint Repository — Geben Sie die SharePoint Host-URLs ein. Das Format für die von Ihnen eingegebenen Host-URLs ist *https://yourdomain.sharepoint.com/sites/mysite*. Die URL muss mit dem `https` Protokoll beginnen. Trennen Sie URLs durch eine neue Zeile. Sie können bis zu 100 URLs hinzufügen.

c. Domain — Geben Sie die SharePoint Domain ein. Die Domain in der URL *https://yourdomain.sharepoint.com/sites/mysite* ist beispielsweise *Ihre* Domain.

d. Für die Autorisierung können Sie aus den folgenden ACL-Optionen wählen:

- Benutzerprinzipalname — Die Zugriffskontrolle basiert auf dem Benutzerprinzipalnamen, der aus dem Azure-Portal abgerufen wurde.
- E-Mail — Die Zugriffskontrolle basiert auf E-Mail-IDs, die vom Azure-Portal abgerufen werden.

> **Note**
>
> Wenn Sie keinen Wert angeben, wird E-Mail als Standardwert betrachtet.

e. Wählen Sie für die Authentifizierung je nach Anwendungsfall zwischen Standard-, OAuth 2.0 -, Azure AD-Authentifizierung, SharePoint Nur-App-Authentifizierung und OAuth 2.0-Aktualisierungstoken-Authentifizierung.

i. Wenn Sie die Standardauthentifizierung verwenden, geben Sie die folgenden Informationen ein:

- Für AWS Secrets Manager geheim — Wählen Sie ein vorhandenes Geheimnis aus, oder erstellen Sie ein neues Secrets Manager Geheimnis, um Ihre SharePoint Authentifizierungsdaten zu speichern. Wenn Sie sich dafür entscheiden, ein neues Geheimnis zu erstellen, wird ein AWS Secrets Manager

geheimes Fenster geöffnet. Geben Sie die folgenden Informationen in das Fenster ein:

- Geheimer Name — Ein Name für Ihr Geheimnis. Das Präfix 'AmazonKendra-SharePoint -' wird automatisch zu Ihrem geheimen Namen hinzugefügt.
- Nutzername — Benutzername für Ihr SharePoint Konto.
- Passwort — Passwort für Ihr SharePoint Konto.

ii. Wenn Sie die OAuth 2.0-Authentifizierung verwenden, geben Sie die folgenden Informationen ein:

- Mandanten-ID — Mandanten-ID Ihres Kontos. SharePoint
- AWS Secrets Manager Geheim — Wählen Sie ein vorhandenes Geheimnis aus, oder erstellen Sie ein neues Secrets Manager Geheimnis, um Ihre SharePoint Authentifizierungsdaten zu speichern. Wenn Sie sich dafür entscheiden, ein neues Geheimnis zu erstellen, wird ein AWS Secrets Manager geheimes Fenster geöffnet. Geben Sie die folgenden Informationen in das Fenster ein:
  - Geheimer Name — Ein Name für Ihr Geheimnis. Das Präfix 'AmazonKendra-SharePoint -' wird automatisch zu Ihrem geheimen Namen hinzugefügt.
  - Nutzername — Benutzername für Ihr SharePoint Konto.
  - Passwort — Passwort für Ihr SharePoint Konto.
  - Client-ID — Die Azure AD-Client-ID, die generiert wurde, wenn Sie sich SharePoint in Azure AD registrieren.
  - Geheimer Client-Schlüssel — Der Azure AD-Client-Schlüssel, der generiert wird, wenn Sie sich SharePoint in Azure AD registrieren.

iii. Wenn Sie die Azure AD-Authentifizierung nur für Apps verwenden, geben Sie die folgenden Informationen ein:

- Mandanten-ID — Mandanten-ID Ihres Kontos. SharePoint
- Selbstsigniertes Azure AD-X.509-Zertifikat — Zertifikat zur Authentifizierung des Connectors für Azure AD.
- Als AWS Secrets Manager geheim — Wählen Sie ein vorhandenes Geheimnis aus, oder erstellen Sie ein neues Secrets Manager Geheimnis, um Ihre Authentifizierungsanmeldeinformationen zu speichern. SharePoint Wenn Sie sich dafür entscheiden, ein neues Geheimnis zu erstellen, wird ein AWS Secrets Manager geheimes Fenster geöffnet. Geben Sie die folgenden Informationen in das Fenster ein:

- Geheimer Name — Ein Name für Ihr Geheimnis. Das Präfix 'AmazonKendra-SharePoint -' wird automatisch zu Ihrem geheimen Namen hinzugefügt.
- Client-ID — Die Azure AD-Client-ID, die generiert wird, wenn Sie sich SharePoint in Azure AD registrieren.
- Privater Schlüssel — Ein privater Schlüssel zur Authentifizierung des Connectors für Azure AD.

iv. Wenn Sie die SharePointreine App-Authentifizierung verwenden, geben Sie die folgenden Informationen ein:

- Mandanten-ID — Mandanten-ID Ihres Kontos. SharePoint
- AWS Secrets Manager Geheim — Wählen Sie ein vorhandenes Geheimnis aus, oder erstellen Sie ein neues Secrets Manager Geheimnis, um Ihre SharePoint Authentifizierungsdaten zu speichern. Wenn Sie sich dafür entscheiden, ein neues Geheimnis zu erstellen, wird ein AWS Secrets Manager geheimes Fenster geöffnet. Geben Sie die folgenden Informationen in das Fenster ein:
  - Geheimer Name — Ein Name für Ihr Geheimnis. Das Präfix 'AmazonKendra-SharePoint -' wird automatisch zu Ihrem geheimen Namen hinzugefügt.
  - SharePoint Client-ID — Die SharePoint Client-ID, die Sie bei der Registrierung von App Only auf Mandantenebene generiert haben. *Das ClientID-Format ist clientID@. TenantId Zum Beispiel ffa956f3-8f89-44e7-b0e4-49670756342c @888d0b57 -69f1-4fb8-957f-e1f0bedf82fe.*
  - SharePoint Kundengeheimnis SharePoint — Das Client-Geheimnis, das generiert wird, wenn Sie sich auf Mandantenebene für App Only registrieren.
  - Client-ID — Die Azure AD-Client-ID, die generiert wurde, wenn Sie sich SharePoint in Azure AD registrieren.
  - Geheimer Client-Schlüssel — Der Azure AD-Client-Schlüssel, der generiert wird, wenn Sie SharePoint sich bei Azure AD registrieren.

v. Wenn Sie die OAuth 2.0-Aktualisierungstoken-Authentifizierung verwenden, geben Sie die folgenden Informationen ein:

- Mandanten-ID — Mandanten-ID Ihres Kontos. SharePoint
- AWS Secrets Manager Geheim — Wählen Sie ein vorhandenes Geheimnis aus, oder erstellen Sie ein neues Secrets Manager Geheimnis, um Ihre SharePoint Authentifizierungsdaten zu speichern. Wenn Sie sich dafür entscheiden, ein

neues Geheimnis zu erstellen, wird ein AWS Secrets Manager geheimes Fenster geöffnet. Geben Sie die folgenden Informationen in das Fenster ein:

- Geheimer Name — Ein Name für Ihr Geheimnis. Das Präfix 'AmazonKendra-SharePoint -' wird automatisch zu Ihrem geheimen Namen hinzugefügt.
- Client-ID — Die eindeutige Azure AD-Client-ID, die generiert wird, wenn Sie sich SharePoint in Azure AD registrieren.
- Geheimer Client-Schlüssel — Der Azure AD-Client-Schlüssel, der generiert wird, wenn Sie SharePoint sich bei Azure AD registrieren.
- Aktualisierungstoken — Das Aktualisierungstoken, das für die Verbindung mit Amazon Kendra generiert wurde SharePoint.

f. Identity Crawler — (Nur aktiviert, wenn ACL aktiviert ist) Wählen Sie diese Option, um Amazon Kendra Identity Crawler zu aktivieren, um Identitätsinformationen zu synchronisieren. Wenn Sie Identity Crawler ausschalten möchten, müssen Sie die Hauptinformationen über die API hochladen. PutPrincipalMapping

Sie können sich auch für Folgendes entscheiden:

i. Zuordnung lokaler Gruppen durchforsten — Aktivieren Sie diese Option, um die Zuordnung lokaler Gruppen zu crawlen.

ii. AD-Gruppenzuordnung crawlen — Aktivieren Sie diese Option, um die Azure Active Directory-Gruppenzuordnung zu crawlen.

> **Note**
>
> Das Crawling von AD-Gruppenzuordnungen ist nur für OAuth 2.0, das OAuth 2.0-Aktualisierungstoken und die reine App-Authentifizierung verfügbar. SharePoint

g. (Optional) VPC und Sicherheitsgruppe konfigurieren — Wählen Sie eine VPC aus, die mit Ihrer Instance verwendet werden soll. SharePoint In diesem Fall müssen Sie Subnetze und VPC-Sicherheitsgruppen hinzufügen.

h. IAM Rolle — Wählen Sie eine bestehende IAM Rolle oder erstellen Sie eine neue IAM Rolle, um auf Ihre Repository-Anmeldeinformationen und Indexinhalte zuzugreifen.

> **Note**
>
> IAM Rollen, die für Indizes verwendet werden, können nicht für Datenquellen verwendet werden. Wenn Sie sich nicht sicher sind, ob eine vorhandene Rolle für einen Index oder eine häufig gestellte Frage verwendet wird, wählen Sie Neue Rolle erstellen, um Fehler zu vermeiden.

i. Wählen Sie Weiter aus.

7. Geben Sie auf der Seite „Synchronisierungseinstellungen konfigurieren“ die folgenden Informationen ein:

   a. Wählen Sie unter Synchronisierungsbereich eine der folgenden Optionen aus:

      i. Entitäten auswählen — Wählen Sie die Entitäten aus, die Sie crawlen möchten. Sie können wählen, ob alle Entitäten oder eine beliebige Kombination von Dateien, Anlagen, Link-Seiten, Ereignissen, Kommentaren und Listendaten gecrawlt werden sollen.

      ii. In der zusätzlichen Konfiguration für Entity-Regex-Muster: Fügen Sie reguläre Ausdrucksmuster für Links, Seiten und Ereignisse hinzu, um bestimmte Entitäten einzubeziehen, anstatt alle Ihre Dokumente zu synchronisieren.

      iii. Regex-Muster — Fügen Sie Muster für reguläre Ausdrücke hinzu, um Dateien anhand von Dateipfad, Dateiname, Dateityp, OneNote Abschnittsnamen und OneNote Seitennamen ein- oder auszuschließen, anstatt all Ihre Dokumente zu synchronisieren. Sie können bis zu 100 hinzufügen.

      > **Note**
      >
      > OneNote Crawling ist nur für OAuth 2.0, das OAuth 2.0-Aktualisierungstoken und die App-Only-Authentifizierung verfügbar. SharePoint

   b. Wählen Sie für den Synchronisierungsmodus aus, wie Sie Ihren Index aktualisieren möchten, wenn sich der Inhalt Ihrer Datenquelle ändert. Wenn Sie Ihre Datenquelle Amazon Kendra zum ersten Mal synchronisieren, werden alle Inhalte standardmäßig synchronisiert.

      - Vollständige Synchronisierung — Synchronisiert alle Inhalte unabhängig vom vorherigen Synchronisierungsstatus.

- Synchronisieren neuer oder geänderter Dokumente — Synchronisiert nur neue oder geänderte Dokumente.
- Synchronisieren neuer, geänderter oder gelöschter Dokumente — Synchronisieren Sie nur neue, geänderte und gelöschte Dokumente.

c. Im Zeitplan für die Synchronisierungsausführung, für Häufigkeit — Wie oft Amazon Kendra wird mit Ihrer Datenquelle synchronisiert?

d. Wählen Sie Weiter aus.

8. Geben Sie auf der Seite Feldzuordnungen festlegen die folgenden Informationen ein:

a. Für Event-Seiten, Dateien, Links, Anlagen und Kommentare — Wählen Sie aus den Amazon Kendra generierten Standard-Datenquellenfeldern aus, die Sie Ihrem Index zuordnen möchten.

b. Feld hinzufügen — Um benutzerdefinierte Datenquellenfelder hinzuzufügen, um einen Indexfeldnamen für die Zuordnung und den Felddatentyp zu erstellen.

c. Wählen Sie Weiter aus.

9. Überprüfen Sie auf der Seite Überprüfen und erstellen, ob die von Ihnen eingegebenen Informationen korrekt sind, und wählen Sie dann Datenquelle hinzufügen aus. Sie können Ihre Informationen auch auf dieser Seite bearbeiten. Ihre Datenquelle wird auf der Seite Datenquellen angezeigt, nachdem die Datenquelle erfolgreich hinzugefügt wurde.

Console: SharePoint Server

Um eine Verbindung Amazon Kendra herzustellen SharePoint

1. Melden Sie sich bei der AWS Management Console an und öffnen Sie die Amazon Kendra Konsole.
2. Wählen Sie im linken Navigationsbereich Indizes und dann den Index, den Sie verwenden möchten, aus der Indexliste aus.

> **Note**
>
> Sie können Ihre Einstellungen für die Benutzerzugriffskontrolle unter Indexeinstellungen konfigurieren oder bearbeiten.

3. Wählen Sie auf der Seite Erste Schritte die Option Datenquelle hinzufügen aus.

4. Wählen Sie auf der Seite Datenquelle hinzufügen die Option SharePoint Connector V2.0 und dann Datenquelle hinzufügen aus.
5. Geben Sie auf der Seite „Datenquellendetails angeben“ die folgenden Informationen ein:
   a. Geben Sie im Feld Name und Beschreibung für Datenquellenname einen Namen für Ihre Datenquelle ein. Sie können Bindestriche, aber keine Leerzeichen verwenden.
   b. (Optional) Beschreibung — Geben Sie eine optionale Beschreibung für Ihre Datenquelle ein.
   c. In Standardsprache — Wählen Sie eine Sprache aus, um Ihre Dokumente nach dem Index zu filtern. Sofern Sie nichts anderes angeben, ist die Standardsprache Englisch. Die in den Metadaten des Dokuments angegebene Sprache hat Vorrang vor der ausgewählten Sprache.
   d. Unter Tags für Neues Tag hinzufügen — Fügen Sie optionale Tags hinzu, um Ihre Ressourcen zu durchsuchen und zu filtern oder Ihre Kosten nachzuverfolgen. AWS
   e. Wählen Sie Weiter aus.
6. Geben Sie auf der Seite Zugriff und Sicherheit definieren die folgenden Informationen ein:
   a. Wählen Sie im Feld Quelle für Hosting-Methode die Option SharePointServer aus.
   b. SharePointVersion wählen — Wählen Sie zwischen SharePoint 2013, SharePoint 2016, SharePoint 2019 und SharePoint (Abonnement-Edition).
   c. Spezifische Site-URLs für Ihr SharePoint Repository — Geben Sie die SharePoint Host-URLs ein. Das Format für die von Ihnen eingegebenen Host-URLs ist *`https://yourcompany/sites/mysite`*. Die URL muss mit dem `https` Protokoll beginnen. Trennen Sie URLs durch eine neue Zeile. Sie können bis zu 100 URLs hinzufügen.
   d. Domain — Geben Sie die SharePoint Domain ein. *`Die Domain in der URL https://yourcompany/sites/mysite ist beispielsweise Ihr Unternehmen`*
   e. Speicherort des SSL-Zertifikats — Geben Sie den Amazon S3 Pfad zu Ihrer SSL-Zertifikatsdatei ein.
   f. (Optional) Für Webproxy — Geben Sie den Hostnamen (ohne `https://` das `http://` OR-Protokoll) und die Portnummer ein, die vom Host-URL-Transportprotokoll verwendet wird. Der numerische Wert der Portnummer muss zwischen 0 und 65535 liegen.
   g. Autorisierung — Aktivieren oder deaktivieren Sie die Informationen der Zugriffskontrollliste (ACL) für Ihre Dokumente, wenn Sie über eine ACL verfügen und diese für die Zugriffskontrolle verwenden möchten. Die ACL gibt an, auf welche

Dokumente Benutzer und Gruppen zugreifen können. Die ACL-Informationen werden verwendet, um Suchergebnisse nach dem Benutzer- oder Gruppenzugriff auf Dokumente zu filtern. Weitere Informationen finden Sie unter Benutzerkontextfilterung.

Für SharePoint Server können Sie aus den folgenden ACL-Optionen wählen:

i. E-Mail-ID mit Domain von IDP — Die Zugriffskontrolle basiert auf E-Mail-IDs, die aus E-Mail-Domänen extrahiert wurden, die vom zugrunde liegenden Identity Provider (IDP) abgerufen wurden. Sie geben die IDP-Verbindungsdetails bei der Authentifizierung geheim an. Secrets Manager

ii. E-Mail-ID mit benutzerdefinierter Domain — Die Zugriffskontrolle basiert auf E-Mail-IDs. Sie möchten den E-Mail-Domänenwert angeben. Zum Beispiel "*amazon.com*“. Die E-Mail-Domain wird verwendet, um die E-Mail-ID für die Zugriffskontrolle zu erstellen. Sie müssen Ihre E-Mail-Domain mithilfe von „E-Mail-Domain hinzufügen“ eingeben.

iii. Domain\ User with Domain — Die Zugriffskontrolle wird im Format Domain\ User ID strukturiert. Sie müssen einen gültigen Domänennamen angeben. Zum Beispiel: *„sharepoint2019", um die Zugriffskontrolle* zu erstellen.

h. Wählen Sie für die Authentifizierung je nach SharePoint Anwendungsfall zwischen Nur-App-Authentifizierung, NTLM-Authentifizierung und Kerberos-Authentifizierung.

i. Geben Sie die folgenden Informationen sowohl für die NTLM-Authentifizierung als auch für die Kerberos-Authentifizierung ein:

Für AWS Secrets Manager geheim — Wählen Sie ein vorhandenes Geheimnis aus, oder erstellen Sie ein neues Secrets Manager Geheimnis, um Ihre Authentifizierungsdaten zu speichern. SharePoint Wenn Sie sich dafür entscheiden, ein neues Geheimnis zu erstellen, wird ein AWS Secrets Manager geheimes Fenster geöffnet. Geben Sie die folgenden Informationen in das Fenster ein:

- Geheimer Name — Ein Name für Ihr Geheimnis. Das Präfix 'AmazonKendra-SharePoint -' wird automatisch zu Ihrem geheimen Namen hinzugefügt.
- Nutzername — Benutzername für Ihr SharePoint Konto.
- Passwort — Passwort für Ihr SharePoint Konto.

Wenn Sie eine E-Mail-ID mit einer Domain von IDP verwenden, geben Sie auch Folgendes ein:

- LDAP-Serverendpunkt — Endpunkt des LDAP-Servers, einschließlich Protokoll und Portnummer. Zum Beispiel: *ldap: //example.com:389*.
- LDAP-Suchbasis — Suchbasis des LDAP-Benutzers. Zum Beispiel: *CN=Users, DC=SharePoint, DC=com*.
- LDAP-Benutzername — Ihr LDAP-Benutzername.
- LDAP-Passwort — Ihr LDAP-Passwort.

ii. Geben Sie die folgenden Informationen für SharePoint die reine App-Authentifizierung ein.

Für AWS Secrets Manager geheim — Wählen Sie ein vorhandenes Geheimnis aus, oder erstellen Sie ein neues Secrets Manager Geheimnis, um Ihre SharePoint Authentifizierungsdaten zu speichern. Wenn Sie sich dafür entscheiden, ein neues Geheimnis zu erstellen, wird ein AWS Secrets Manager geheimes Fenster geöffnet. Geben Sie die folgenden Informationen in das Fenster ein:

- Geheimer Name — Ein Name für Ihr Geheimnis. Das Präfix 'AmazonKendra-SharePoint -' wird automatisch zu Ihrem geheimen Namen hinzugefügt.
- Client-ID — Die SharePoint Client-ID, die Sie bei der Registrierung von App Only auf Site-Ebene generiert haben. Das ClientID-Format ist clientID@. TenantId *Zum Beispiel ffa956f3-8f89-44e7-b0e4-49670756342c @888d0b57 -69f1-4fb8-957f-e1f0bedf82fe.*
- SharePoint Client-Geheimnis — SharePoint Das Client-Geheimnis, das generiert wird, wenn Sie sich auf Site-Ebene für App Only registrieren.

  Hinweis: Da Client-IDs und Client-Geheimnisse nur für einzelne Websites generiert werden, wenn Sie die SharePoint Server-Authentifizierung nur für Apps registrieren, wird nur eine Site-URL für die SharePoint Only-App-Authentifizierung unterstützt.

Wenn Sie die E-Mail-ID mit der Domain von IDP verwenden, geben Sie auch Folgendes ein:

- LDAP-Serverendpunkt — Endpunkt des LDAP-Servers, einschließlich Protokoll und Portnummer. Zum Beispiel: *ldap: //example.com:389*.

- LDAP-Suchbasis — Suchbasis des LDAP-Benutzers. Zum Beispiel: *CN=Users, DC=SharePoint, DC=com*.
- LDAP-Benutzername — Ihr LDAP-Benutzername.
- LDAP-Passwort — Ihr LDAP-Passwort.

i. Identity Crawler — Geben Sie an, ob der Identity Crawler aktiviert werden soll. Amazon Kendra Der Identity Crawler verwendet die Informationen der Zugriffskontrollliste (ACL) für Ihre Dokumente, um Suchergebnisse nach dem Benutzer- oder Gruppenzugriff auf Dokumente zu filtern. Wenn Sie über eine ACL für Ihre Dokumente verfügen und Ihre ACL verwenden möchten, können Sie auch den Identity Crawler aktivieren, um die Benutzerkontextfilterung von Suchergebnissen zu konfigurieren. Amazon Kendra Andernfalls können alle Dokumente öffentlich durchsucht werden, wenn Identity Crawler ausgeschaltet ist. Wenn Sie die Zugriffskontrolle für Ihre Dokumente verwenden möchten und Identity Crawler ausgeschaltet ist, können Sie alternativ die PutPrincipalMappingAPI verwenden, um Benutzer- und Gruppenzugriffsinformationen für die Benutzerkontextfilterung hochzuladen.

   i. Zuordnung lokaler Gruppen durchforsten — Aktivieren Sie diese Option, um die Zuordnung lokaler Gruppen zu crawlen.

   ii. (Nur für E-Mail-ID mit Domäne von IDP) AD-Gruppenzuordnung durchforsten — Aktivieren Sie diese Option, um die Active Directory-Zuordnung zu crawlen.

> **Note**
>
> Das Crawling der AD-Gruppenzuweisung ist nur für die App-Authentifizierung verfügbar. SharePoint

j. (Optional) VPC und Sicherheitsgruppe konfigurieren — Wählen Sie eine VPC aus, die mit Ihrer Instance verwendet werden soll. SharePoint In diesem Fall müssen Sie Subnetze und VPC-Sicherheitsgruppen hinzufügen.

k. IAM Rolle — Wählen Sie eine bestehende IAM Rolle oder erstellen Sie eine neue IAM Rolle, um auf Ihre Repository-Anmeldeinformationen und Indexinhalte zuzugreifen.

> **Note**
>
> IAM Rollen, die für Indizes verwendet werden, können nicht für Datenquellen verwendet werden. Wenn Sie sich nicht sicher sind, ob eine vorhandene Rolle für

einen Index oder eine häufig gestellte Frage verwendet wird, wählen Sie Neue Rolle erstellen, um Fehler zu vermeiden.

l. Wählen Sie Weiter aus.

7. Geben Sie auf der Seite „Synchronisierungseinstellungen konfigurieren“ die folgenden Informationen ein:

   a. Wählen Sie unter Synchronisierungsbereich eine der folgenden Optionen aus:

      i. Entitäten auswählen — Wählen Sie die Entitäten aus, die Sie crawlen möchten. Sie können wählen, ob Alle Entitäten oder eine beliebige Kombination aus Dateien, Anlagen, Link-Seiten, Ereignissen und Listendaten gecrawlt werden sollen.

      ii. In der zusätzlichen Konfiguration für Entity-Regex-Muster: Fügen Sie reguläre Ausdrucksmuster für Links, Seiten und Ereignisse hinzu, um bestimmte Entitäten einzubeziehen, anstatt alle Ihre Dokumente zu synchronisieren.

      iii. Regex-Muster — Fügen Sie Muster für reguläre Ausdrücke hinzu, um Dateien nach Dateipfad, Dateiname, Dateityp, OneNoteAbschnittsname und OneNoteSeitenname ein- oder auszuschließen, anstatt all Ihre Dokumente zu synchronisieren. Sie können bis zu 100 hinzufügen.

      > **Note**
      >
      > OneNote Crawling ist nur für die Authentifizierung nur über SharePoint Apps verfügbar.

   b. Synchronisierungsmodus — Wählen Sie aus, wie Sie Ihren Index aktualisieren möchten, wenn sich der Inhalt Ihrer Datenquelle ändert. Wenn Sie Ihre Datenquelle Amazon Kendra zum ersten Mal synchronisieren, werden alle Inhalte standardmäßig gecrawlt und indexiert. Sie müssen eine vollständige Synchronisierung Ihrer Daten durchführen, falls Ihre erste Synchronisierung fehlgeschlagen ist, auch wenn Sie die Option Vollsynchronisierung nicht als Synchronisierungsmodusoption wählen.

      - Vollständige Synchronisierung: Indizieren Sie den gesamten Inhalt neu und ersetzen die vorhandenen Inhalte jedes Mal, wenn Ihre Datenquelle mit Ihrem Index synchronisiert wird.
      - Neue, geänderte Synchronisierung: Indizieren Sie jedes Mal, wenn Ihre Datenquelle mit Ihrem Index synchronisiert wird, nur neue und geänderte Inhalte. Amazon Kendra

kann den Mechanismus Ihrer Datenquelle verwenden, um Inhaltsänderungen nachzuverfolgen und Inhalte zu indexieren, die sich seit der letzten Synchronisierung geändert haben.

- Neue, geänderte, gelöschte Synchronisierung: Indizieren Sie bei jeder Synchronisierung Ihrer Datenquelle mit Ihrem Index nur neue, geänderte und gelöschte Inhalte. Amazon Kendra kann den Mechanismus Ihrer Datenquelle verwenden, um Inhaltsänderungen nachzuverfolgen und Inhalte zu indexieren, die sich seit der letzten Synchronisierung geändert haben.

c. Im Synchronisierungslaufplan für Frequenz — Wie oft Amazon Kendra wird mit Ihrer Datenquelle synchronisiert?

d. Wählen Sie Weiter aus.

8. Geben Sie auf der Seite Feldzuordnungen festlegen die folgenden Informationen ein:

a. Für Event-Seiten, Dateien, Links, Anlagen und Listendaten — Wählen Sie aus den Amazon Kendra generierten Standard-Datenquellenfeldern aus, die Sie Ihrem Index zuordnen möchten.

b. Feld hinzufügen — Um benutzerdefinierte Datenquellenfelder hinzuzufügen, um einen Indexfeldnamen für die Zuordnung und den Felddatentyp zu erstellen.

c. Wählen Sie Weiter aus.

9. Überprüfen Sie auf der Seite Überprüfen und erstellen, ob die von Ihnen eingegebenen Informationen korrekt sind, und wählen Sie dann Datenquelle hinzufügen aus. Sie können Ihre Informationen auch auf dieser Seite bearbeiten. Ihre Datenquelle wird auf der Seite Datenquellen angezeigt, nachdem die Datenquelle erfolgreich hinzugefügt wurde.

API

Um eine Verbindung Amazon Kendra herzustellen SharePoint

Sie müssen mithilfe der TemplateConfigurationAPI ein JSON des Datenquellenschemas angeben. Sie müssen die folgenden Informationen angeben:

- Datenquelle — Geben Sie den Datenquellentyp wie `SHAREPOINTV2` bei der Verwendung des TemplateConfigurationJSON-Schemas an. Geben Sie außerdem die Datenquelle so an`TEMPLATE`, wie Sie die CreateDataSourceAPI aufrufen.
- Repository-Endpunkt-Metadaten — Geben Sie das `tenantID` `domain` `siteUrls` Ende Ihrer SharePoint Instanz an.

- Synchronisierungsmodus — Geben Sie an, wie Ihr Index aktualisiert Amazon Kendra werden soll, wenn sich der Inhalt Ihrer Datenquelle ändert. Wenn Sie Ihre Datenquelle Amazon Kendra zum ersten Mal synchronisieren, werden alle Inhalte standardmäßig gecrawlt und indexiert. Sie müssen eine vollständige Synchronisierung Ihrer Daten durchführen, falls Ihre erste Synchronisierung fehlgeschlagen ist, auch wenn Sie die Option Vollsynchronisierung nicht als Synchronisierungsmodusoption wählen. Sie können wählen zwischen:
  - `FORCED_FULL_CRAWL`um den gesamten Inhalt neu zu indizieren und vorhandene Inhalte jedes Mal zu ersetzen, wenn Ihre Datenquelle mit Ihrem Index synchronisiert wird.
  - `FULL_CRAWL`um bei jeder Synchronisierung Ihrer Datenquelle mit Ihrem Index nur neue, geänderte und gelöschte Inhalte zu indizieren. Amazon Kendra kann den Mechanismus Ihrer Datenquelle verwenden, um Inhaltsänderungen nachzuverfolgen und Inhalte zu indexieren, die sich seit der letzten Synchronisierung geändert haben.
  - `CHANGE_LOG`um jedes Mal, wenn Ihre Datenquelle mit Ihrem Index synchronisiert wird, nur neue und geänderte Inhalte zu indizieren. Amazon Kendra kann den Mechanismus Ihrer Datenquelle verwenden, um Inhaltsänderungen nachzuverfolgen und Inhalte zu indexieren, die sich seit der letzten Synchronisierung geändert haben.
- Identity Crawler — Geben Sie an, ob der Identity Crawler aktiviert Amazon Kendra werden soll. Der Identity Crawler verwendet die Informationen der Zugriffskontrollliste (ACL) für Ihre Dokumente, um Suchergebnisse nach dem Benutzer- oder Gruppenzugriff auf Dokumente zu filtern. Wenn Sie über eine ACL für Ihre Dokumente verfügen und Ihre ACL verwenden möchten, können Sie auch den Identity Crawler aktivieren, um die Benutzerkontextfilterung von Suchergebnissen zu konfigurieren. Amazon Kendra Andernfalls können alle Dokumente öffentlich durchsucht werden, wenn Identity Crawler ausgeschaltet ist. Wenn Sie die Zugriffskontrolle für Ihre Dokumente verwenden möchten und Identity Crawler ausgeschaltet ist, können Sie alternativ die PutPrincipalMappingAPI verwenden, um Benutzer- und Gruppenzugriffsinformationen für die Benutzerkontextfilterung hochzuladen.

  > **Note**
  >
  > Identity Crawler ist nur verfügbar, wenn Sie auf eingestellt `crawlAcl` haben. `true`

- Zusätzliche Eigenschaften des Repositorys — Geben Sie Folgendes an:
  - (Für Azure AD) `s3bucketName` und `s3certificateName` Sie verwenden, um Ihr selbstsigniertes Azure AD-X.509-Zertifikat zu speichern.

- Authentifizierungstyp (`auth_Type`), den Sie verwenden, unabhängig davon `0Auth20Auth2App`,,`0Auth2Certificate`,`Basic`, `0Auth2_RefreshTokenNTLM`, und. `Kerberos`
- Version (`version`), die Sie verwenden, ob `Server` oder`0nline`. Wenn Sie verwenden, können `Server` Sie das on`PremVersion` als`2013`, `20162019`, oder `SubscriptionEdition` weiter spezifizieren.

- Geheimer Amazon-Ressourcenname (ARN) — Geben Sie den Amazon-Ressourcennamen (ARN) eines Secrets Manager Geheimnisses ein, das die Authentifizierungsdaten enthält, die Sie in Ihrem SharePoint Konto erstellt haben.

  Wenn Sie SharePoint Online verwenden, können Sie zwischen Basic-, OAuth 2.0-, Azure AD App-Only- und App-Only-Authentifizierung wählen. SharePoint Im Folgenden sind die Mindest-JSON-Strukturen aufgeführt, die für jede Authentifizierungsoption in Ihrem Geheimnis enthalten sein müssen:

  - Grundlegende Authentifizierung

    ```
    {
        "userName": "SharePoint account user name",
        "password": "SharePoint account password"
    }
    ```

  - OAuth 2.0-Authentifizierung

    ```
    {
        "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"
    }
    ```

  - Azure AD-Authentifizierung nur für Apps

    ```
    {
        "clientId": "client id generated when registering SharePoint with Azure AD",
        "privateKey": "private key to authorize connection with Azure AD"
    }
    ```

  - SharePoint Reine App-Authentifizierung

```
{
    "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"
}
```

- Authentifizierung mit OAuth 2.0-Aktualisierungstoken

```
{
    "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"
}
```

Wenn Sie SharePoint Server verwenden, können Sie zwischen der SharePoint reinen App-Authentifizierung, der NTLM-Authentifizierung und der Kerberos-Authentifizierung wählen. Im Folgenden sind die Mindest-JSON-Strukturen aufgeführt, die für jede Authentifizierungsoption in Ihrem Geheimnis enthalten sein müssen:

- SharePoint Authentifizierung nur über Apps

```
{
    "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 Reine App-Authentifizierung mit Domain aus der IDP-Autorisierung

```
{
    "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"
}
```

- (Nur Server) NTLM- oder Kerberos-Authentifizierung

```
{
    "siteUrlsHash": "Hash representation of SharePoint site URLs",
    "userName": "SharePoint account user name",
    "password": "SharePoint account password"
}
```

- (Nur Server) NTLM- oder Kerberos-Authentifizierung mit Domain aus IDP-Autorisierung

```
{
    "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**
>
> Wir empfehlen, dass Sie Ihre Anmeldeinformationen und Ihr Geheimnis regelmäßig aktualisieren oder austauschen. Stellen Sie zu Ihrer eigenen Sicherheit nur die Zugriffsebene bereit, die erforderlich ist. Wir raten davon ab, Anmeldeinformationen und geheime Daten für alle Datenquellen und Connector-Versionen 1.0 und 2.0 (sofern zutreffend) wiederzuverwenden.

- IAM Rolle — Geben Sie an`RoleArn`, wann Sie anrufen`CreateDataSource`, um einer IAM Rolle Berechtigungen für den Zugriff auf Ihr Secrets Manager Geheimnis und für den Aufruf der erforderlichen öffentlichen APIs für den SharePoint Connector und zum Aufrufen der erforderlichen öffentlichen APIs zu erteilen. Amazon Kendra Weitere Informationen finden Sie unter IAM Rollen für SharePoint Datenquellen.

Sie können auch die folgenden optionalen Funktionen hinzufügen:

- Virtual Private Cloud (VPC) — Geben Sie an, `VpcConfiguration` wann Sie anrufen. `CreateDataSource` Weitere Informationen finden Sie unter Konfigurieren von Amazon Kendra für die Verwendung eines Amazon VPC.
- Inklusions- und Ausschlussfilter — Sie können angeben, ob bestimmte Dateien und andere Inhalte ein- oder ausgeschlossen werden sollen. OneNotes

> **Note**
>
> Die meisten Datenquellen verwenden Muster für reguläre Ausdrücke, bei denen es sich um Ein- oder Ausschlussmuster handelt, die als Filter bezeichnet werden. Wenn Sie einen Einschlussfilter angeben, werden nur Inhalte indexiert, die dem Einschlussfilter entsprechen. Jedes Dokument, das nicht dem Einschlussfilter entspricht, wird nicht indexiert. Wenn Sie einen Ein- und Ausschlussfilter angeben, werden Dokumente, die dem Ausschlussfilter entsprechen, nicht indexiert, auch wenn sie dem Einschlussfilter entsprechen.

- Feldzuordnungen — Wählen Sie diese Option, um Ihre SharePoint Datenquellenfelder Ihren Indexfeldern zuzuordnen. Amazon Kendra Weitere Informationen finden Sie unter Zuweisen von Datenquellenfeldern.

> **Note**
>
> Das Textfeld oder das entsprechende Textfeld für Ihre Dokumente ist erforderlich, um Ihre Dokumente durchsuchen Amazon Kendra zu können. Sie müssen den Feldnamen Ihres Dokumenthauptteils in Ihrer Datenquelle dem Namen des Indexfeldes zuordnen`_document_body`. Alle anderen Felder sind optional.

Eine Liste weiterer wichtiger JSON-Schlüssel, die konfiguriert werden müssen, finden Sie unter SharePoint Microsoft-Vorlagenschema.

Hinweise

- Der Connector unterstützt benutzerdefinierte Feldzuordnungen nur für die Entität Files.

- Für alle SharePoint Serverversionen muss das ACL-Token in Kleinbuchstaben geschrieben werden. Für E-Mail mit Domain von IDP und E-Mail-ID mit benutzerdefinierter Domain-ACL, zum Beispiel: *user@sharepoint2019.com*. Für Domain\ User mit Domain-ACL, zum Beispiel: *sharepoint2013*\ user.
- Der Connector unterstützt den Änderungsprotokollmodus/die Synchronisierung neuer oder geänderter Inhalte für 2013 nicht. SharePoint
- Wenn der Name einer Entität ein % Zeichen enthält, überspringt der Connector diese Dateien aufgrund von API-Einschränkungen.
- OneNote kann nur vom Connector mit einer Mandanten-ID und mit OAuth 2.0, einem OAuth 2.0-Aktualisierungstoken oder einer für Online aktivierten SharePoint App-Only-Authentifizierung gecrawlt werden. SharePoint
- Der Connector durchsucht den ersten Abschnitt eines OneNote Dokuments nur unter Verwendung seines Standardnamens, auch wenn das Dokument umbenannt wurde.
- Der Connector crawlt Links in den Versionen SharePoint 2019, SharePoint Online und Subscription nur, wenn neben Links auch Seiten und Dateien als zu durchsuchende Entitäten ausgewählt wurden.
- Der Connector crawlt Links in den Jahren SharePoint 2013 und SharePoint 2016, wenn Links als Entität für das Crawlen ausgewählt wurde.
- Der Connector durchforstet Listenanhänge und Kommentare nur, wenn List Data auch als Entität für das Crawlen ausgewählt wurde.
- Der Connector durchforstet Ereignisanhänge nur, wenn Ereignisse auch als Entität für das Crawlen ausgewählt wurde.
- In der SharePoint Online-Version wird das ACL-Token in Kleinbuchstaben geschrieben. Wenn der Benutzerprinzipalname im Azure-Portal beispielsweise *MaryMajor@domain .com* lautet, lautet das ACL-Token im SharePoint Connector *marymajor@domain.com*.
- Wenn Sie in Identity Crawler für SharePoint Online und Server verschachtelte Gruppen crawlen möchten, müssen Sie sowohl das lokale Crawling als auch das AD-Gruppen-Crawling aktivieren.
- Wenn Sie SharePoint Online verwenden und der Benutzerprinzipalname in Ihrem Azure-Portal eine Kombination aus Groß- und Kleinschreibung ist, konvertiert die SharePoint API ihn intern in Kleinbuchstaben. Aus diesem Grund legt der Amazon Kendra SharePoint Konnektor ACL in Kleinbuchstaben fest.

Microsoft SQL Server

Microsoft SQL Serverist ein von Microsoft entwickeltes relationales Datenbankmanagementsystem (RDBMS). Wenn Sie ein Microsoft SQL Server Benutzer sind, können Sie es verwenden, um Ihre Microsoft SQL Server Datenquelle Amazon Kendra zu indizieren. Der Amazon Kendra Microsoft SQL Server Datenquellenconnector unterstützt MS SQL Server 2019.

Sie können über Amazon Kendra die Amazon Kendra Konsole und die TemplateConfigurationAPI eine Verbindung zu Ihrer Microsoft SQL Server Datenquelle herstellen.

Informationen zur Fehlerbehebung bei Ihrem Amazon Kendra Microsoft SQL Server Datenquellen-Connector finden Sie unterProblembehandlung bei Datenquellen.

Themen

Unterstützte Features

- Feldzuordnungen
- Filterung des Benutzerkontextes
- Einschluss-/Ausschlussfilter
- Vollständige und inkrementelle Inhaltssynchronisierung
- Virtual Private Cloud (VPC)

Voraussetzungen

Bevor Sie Ihre Microsoft SQL Server Datenquelle Amazon Kendra zum Indizieren verwenden können, nehmen Sie diese Änderungen in Ihren Konten Microsoft SQL Server und AWS Konten vor.

Stellen Sie sicherMicrosoft SQL Server, dass Sie Folgendes haben:

- Haben Sie sich Ihren Datenbank-Benutzernamen und Ihr Passwort notiert.

> **Important**
>
> Es hat sich bewährt, nur lesbare Amazon Kendra Datenbankanmeldeinformationen zur Verfügung zu stellen.

- Die URL, der Port und die Instanz Ihres Datenbank-Hosts wurden kopiert.
- Vergewissert, dass jedes Dokument in Microsoft SQL Server und zwischen anderen Datenquellen, die Sie für denselben Index verwenden möchten, einzigartig ist. Jede Datenquelle, die Sie für einen Index verwenden möchten, darf nicht dasselbe Dokument in allen Datenquellen enthalten. Dokument-IDs gelten für einen Index global und müssen pro Index eindeutig sein.

Stellen Sie sicher AWS-Konto, dass Sie Folgendes in Ihrem haben:

- Hat einen Amazon Kendra Index erstellt und bei Verwendung der API die Index-ID notiert.
- Sie haben eine IAM Rolle für Ihre Datenquelle erstellt und, falls Sie die API verwenden, den ARN der IAM Rolle notiert.

> **Note**
>
> Wenn Sie Ihren Authentifizierungstyp und Ihre Anmeldeinformationen ändern, müssen Sie Ihre IAM Rolle aktualisieren, um auf die richtige AWS Secrets Manager geheime ID zugreifen zu können.

- Wir haben Ihre Microsoft SQL Server Authentifizierungsdaten AWS Secrets Manager geheim gespeichert und, falls Sie die API verwenden, den ARN des Geheimnisses notiert.

> **Note**
>
> Wir empfehlen Ihnen, Ihre Anmeldeinformationen und Ihr Geheimnis regelmäßig zu aktualisieren oder zu wechseln. Stellen Sie zu Ihrer eigenen Sicherheit nur die Zugriffsebene bereit, die erforderlich ist. Wir raten davon ab, Anmeldeinformationen und geheime Daten für alle Datenquellen und Connector-Versionen 1.0 und 2.0 (sofern zutreffend) wiederzuverwenden.

Wenn Sie noch keine IAM Rolle oder keinen Schlüssel haben, können Sie die Konsole verwenden, um eine neue IAM Rolle und ein neues Secrets Manager Geheimnis zu erstellen, wenn Sie Ihre Microsoft SQL Server Datenquelle mit verbinden. Amazon Kendra Wenn Sie die API verwenden, müssen Sie den ARN einer vorhandenen IAM Rolle und eines Secrets Manager Geheimnisses sowie eine Index-ID angeben.

Anweisungen zur Verbindung

Um eine Verbindung Amazon Kendra zu Ihrer Microsoft SQL Server Datenquelle herzustellen, müssen Sie Details zu Ihren Microsoft SQL Server Anmeldeinformationen angeben, damit Sie auf Ihre Daten zugreifen Amazon Kendra können. Falls Sie das noch nicht konfiguriert haben, Amazon Kendra sehen Sie Microsoft SQL Server nachVoraussetzungen.

Console

Um eine Verbindung Amazon Kendra herzustellen Microsoft SQL Server

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die Amazon Kendra Konsole.
2. Wählen Sie im linken Navigationsbereich Indizes und dann den Index, den Sie verwenden möchten, aus der Indexliste aus.

   > **Note**
   >
   > Sie können Ihre Einstellungen für die Benutzerzugriffskontrolle unter Indexeinstellungen konfigurieren oder bearbeiten.

3. Wählen Sie auf der Seite Erste Schritte die Option Datenquelle hinzufügen aus.
4. Wählen Sie auf der Seite Datenquelle hinzufügen die Option Microsoft SQL ServerConnector und dann Connector hinzufügen aus.
5. Geben Sie auf der Seite „Datenquellendetails angeben“ die folgenden Informationen ein:

   a. Geben Sie im Feld Name und Beschreibung für Datenquellenname einen Namen für Ihre Datenquelle ein. Sie können Bindestriche, aber keine Leerzeichen verwenden.

   b. (Optional) Beschreibung — Geben Sie eine optionale Beschreibung für Ihre Datenquelle ein.

   c. In Standardsprache — Wählen Sie eine Sprache aus, um Ihre Dokumente nach dem Index zu filtern. Sofern Sie nichts anderes angeben, ist die Standardsprache Englisch.

Die in den Metadaten des Dokuments angegebene Sprache hat Vorrang vor der ausgewählten Sprache.

d. Unter Tags für Neues Tag hinzufügen — Fügen Sie optionale Tags hinzu, um Ihre Ressourcen zu durchsuchen und zu filtern oder Ihre Kosten nachzuverfolgen. AWS

e. Wählen Sie Weiter aus.

6. Geben Sie auf der Seite Zugriff und Sicherheit definieren die folgenden Informationen ein:

a. Geben Sie im Feld Quelle die folgenden Informationen ein:

b. Host — Geben Sie den Datenbank-Hostnamen ein.

c. Port — Geben Sie den Datenbankport ein.

d. Instanz — Geben Sie die Datenbankinstanz ein.

e. Speicherort für SSL-Zertifikate aktivieren — Geben Sie hier den Amazon S3 Pfad zu Ihrer SSL-Zertifikatsdatei ein.

f. Geben Sie im Feld Authentifizierung die folgenden Informationen ein:

- AWS Secrets Manager geheim — Wählen Sie ein vorhandenes Geheimnis aus, oder erstellen Sie ein neues Secrets Manager Geheimnis, um Ihre Microsoft SQL Server Authentifizierungsdaten zu speichern. Wenn Sie ein neues Geheimnis erstellen möchten, wird ein AWS Secrets Manager geheimes Fenster geöffnet.

  A. Geben Sie die folgenden Informationen in das Fenster Create an AWS Secrets Manager Secret ein:

     I. Geheimer Name — Ein Name für Ihr Geheimnis. Das Präfix 'AmazonKendra- Microsoft SQL Server -' wird Ihrem geheimen Namen automatisch hinzugefügt.

     II. Geben Sie für Datenbankbenutzername und Passwort die Werte der Authentifizierungsdaten ein, die Sie aus Ihrer Datenbank kopiert haben.

  B. Wählen Sie Speichern.

g. Virtual Private Cloud (VPC) — Sie können wählen, ob Sie eine VPC verwenden möchten. In diesem Fall müssen Sie Subnetze und VPC-Sicherheitsgruppen hinzufügen.

h. IAM Rolle — Wählen Sie eine bestehende IAM Rolle oder erstellen Sie eine neue IAM Rolle, um auf Ihre Repository-Anmeldeinformationen und Indexinhalte zuzugreifen.

> **Note**
>
> IAM Rollen, die für Indizes verwendet werden, können nicht für Datenquellen verwendet werden. Wenn Sie sich nicht sicher sind, ob eine vorhandene Rolle für einen Index oder eine häufig gestellte Frage verwendet wird, wählen Sie Neue Rolle erstellen, um Fehler zu vermeiden.

i. Wählen Sie Weiter aus.

7. Geben Sie auf der Seite Synchronisierungseinstellungen konfigurieren die folgenden Informationen ein:

   a. Wählen Sie unter Synchronisierungsbereich eine der folgenden Optionen aus:

   - SQL-Abfrage — Geben Sie SQL-Abfrageanweisungen wie SELECT- und JOIN-Operationen ein. SQL-Abfragen müssen weniger als 32 KB groß sein. Amazon Kendra durchsucht den gesamten Datenbankinhalt, der Ihrer Abfrage entspricht.

     > **Note**
     >
     > Wenn ein Tabellenname Sonderzeichen (nicht alphanumerisch) enthält, müssen Sie den Tabellennamen in eckige Klammern setzen. *`Wählen Sie beispielsweise * aus [] my-database-table`*

   - Primärschlüsselspalte — Geben Sie den Primärschlüssel für die Datenbanktabelle an. Dies identifiziert eine Tabelle in Ihrer Datenbank.
   - Titelspalte — Geben Sie den Namen der Titelspalte des Dokuments in Ihrer Datenbanktabelle an.
   - Hauptspalte — Geben Sie den Namen der Hauptspalte des Dokuments in Ihrer Datenbanktabelle an.

   b. Wählen Sie unter Zusätzliche Konfiguration — optional aus den folgenden Optionen, um bestimmte Inhalte zu synchronisieren, anstatt alle Dateien zu synchronisieren:

   - Spalten zur Erkennung von Änderungen — Geben Sie die Namen der Spalten ein, anhand derer Inhaltsänderungen erkannt Amazon Kendra werden sollen. Amazon Kendra indexiert den Inhalt neu, wenn sich eine dieser Spalten ändert.

- Spalte mit Benutzer-IDs — Geben Sie den Namen der Spalte ein, die Benutzer-IDs enthält, um Zugriff auf Inhalte zu erhalten.
- Spalte „Gruppen“ — Geben Sie den Namen der Spalte ein, die Gruppen enthält, denen der Zugriff auf Inhalte gewährt werden soll.
- Spalte Quell-URLs — Geben Sie den Namen der Spalte ein, die Quell-URLs enthält, die indexiert werden sollen.
- Spalte mit Zeitstempeln — Geben Sie den Namen der Spalte ein, die Zeitstempel enthält. Amazon Kendra verwendet Zeitstempelinformationen, um Änderungen an Ihren Inhalten zu erkennen und nur geänderte Inhalte zu synchronisieren.
- Spalte „Zeitzonen“ — Geben Sie den Namen der Spalte ein, die Zeitzonen für den Inhalt enthält, der gecrawlt werden soll.
- Zeitstempelformat — Geben Sie den Namen der Spalte ein, die Zeitstempelformate enthält, anhand derer Inhaltsänderungen erkannt und Ihre Inhalte erneut synchronisiert werden sollen.

c. Synchronisierungsmodus — Wählen Sie aus, wie Sie Ihren Index aktualisieren möchten, wenn sich der Inhalt Ihrer Datenquelle ändert. Wenn Sie Ihre Datenquelle Amazon Kendra zum ersten Mal synchronisieren, werden alle Inhalte standardmäßig gecrawlt und indexiert. Sie müssen eine vollständige Synchronisierung Ihrer Daten durchführen, falls Ihre erste Synchronisierung fehlgeschlagen ist, auch wenn Sie die Option Vollsynchronisierung nicht als Synchronisierungsmodusoption wählen.

   - Vollständige Synchronisierung: Indizieren Sie alle Inhalte neu und ersetzen vorhandene Inhalte jedes Mal, wenn Ihre Datenquelle mit Ihrem Index synchronisiert wird.
   - Neue, geänderte Synchronisierung: Indizieren Sie bei jeder Synchronisierung Ihrer Datenquelle mit Ihrem Index nur neue und geänderte Inhalte. Amazon Kendra kann den Mechanismus Ihrer Datenquelle verwenden, um Inhaltsänderungen nachzuverfolgen und Inhalte zu indexieren, die sich seit der letzten Synchronisierung geändert haben.
   - Neue, geänderte, gelöschte Synchronisierung: Indizieren Sie bei jeder Synchronisierung Ihrer Datenquelle mit Ihrem Index nur neue, geänderte und gelöschte Inhalte. Amazon Kendra kann den Mechanismus Ihrer Datenquelle verwenden, um Inhaltsänderungen nachzuverfolgen und Inhalte zu indexieren, die sich seit der letzten Synchronisierung geändert haben.

d. Im Synchronisierungslaufplan für Frequenz — Wie oft Amazon Kendra wird mit Ihrer Datenquelle synchronisiert?

e. Wählen Sie Weiter aus.

8. Geben Sie auf der Seite Feldzuordnungen festlegen die folgenden Informationen ein:

a. Wählen Sie aus den generierten Standard-Datenquellenfeldern — Dokument-IDs, Dokumenttitel und Quell-URLs — aus, die Sie dem Index zuordnen möchten. Amazon Kendra

b. Feld hinzufügen — Um benutzerdefinierte Datenquellenfelder hinzuzufügen, um einen Indexfeldnamen für die Zuordnung und den Felddatentyp zu erstellen.

c. Wählen Sie Weiter aus.

9. Überprüfen Sie auf der Seite Überprüfen und erstellen, ob die von Ihnen eingegebenen Informationen korrekt sind, und wählen Sie dann Datenquelle hinzufügen aus. Sie können Ihre Informationen auch auf dieser Seite bearbeiten. Ihre Datenquelle wird auf der Seite Datenquellen angezeigt, nachdem die Datenquelle erfolgreich hinzugefügt wurde.

API

Um eine Verbindung Amazon Kendra herzustellen Microsoft SQL Server

Mithilfe der TemplateConfigurationAPI müssen Sie Folgendes angeben:

- Datenquelle — Geben Sie den Datenquellentyp wie `JDBC` bei der Verwendung des TemplateConfigurationJSON-Schemas an. Geben Sie außerdem die Datenquelle so an`TEMPLATE`, wie Sie die CreateDataSourceAPI aufrufen.
- Datenbanktyp — Sie müssen den Datenbanktyp als `sqlserver` angeben.
- SQL-Abfrage — Geben Sie SQL-Abfrageanweisungen wie SELECT- und JOIN-Operationen an. SQL-Abfragen müssen weniger als 32 KB groß sein. Amazon Kendra durchsucht den gesamten Datenbankinhalt, der Ihrer Abfrage entspricht.

> **Note**
>
> Wenn ein Tabellenname Sonderzeichen (nicht alphanumerisch) enthält, müssen Sie den Tabellennamen in eckige Klammern setzen. *`Wählen Sie beispielsweise * aus [] my-database-table`*

- Synchronisierungsmodus — Geben Sie an, wie Ihr Index aktualisiert Amazon Kendra werden soll, wenn sich der Inhalt Ihrer Datenquelle ändert. Wenn Sie Ihre Datenquelle Amazon Kendra zum ersten Mal synchronisieren, werden alle Inhalte standardmäßig gecrawlt und indexiert. Sie müssen eine vollständige Synchronisierung Ihrer Daten durchführen, falls Ihre erste Synchronisierung fehlgeschlagen ist, auch wenn Sie die Option Vollsynchronisierung nicht als Synchronisierungsmodusoption wählen. Sie können wählen zwischen:
  - `FORCED_FULL_CRAWL`um den gesamten Inhalt neu zu indizieren und vorhandene Inhalte jedes Mal zu ersetzen, wenn Ihre Datenquelle mit Ihrem Index synchronisiert wird.
  - `FULL_CRAWL`um bei jeder Synchronisierung Ihrer Datenquelle mit Ihrem Index nur neue, geänderte und gelöschte Inhalte zu indizieren. Amazon Kendra kann den Mechanismus Ihrer Datenquelle verwenden, um Inhaltsänderungen nachzuverfolgen und Inhalte zu indexieren, die sich seit der letzten Synchronisierung geändert haben.
  - `CHANGE_LOG`um bei jeder Synchronisierung Ihrer Datenquelle mit Ihrem Index nur neue und geänderte Inhalte zu indizieren. Amazon Kendra kann den Mechanismus Ihrer Datenquelle verwenden, um Inhaltsänderungen nachzuverfolgen und Inhalte zu indexieren, die sich seit der letzten Synchronisierung geändert haben.
- Geheimer Amazon-Ressourcenname (ARN) — Geben Sie den Amazon-Ressourcennamen (ARN) eines Secrets Manager Geheimnisses ein, das die Authentifizierungsdaten enthält, die Sie in Ihrem Microsoft SQL Server Konto erstellt haben. Das Geheimnis wird in einer JSON-Struktur mit den folgenden Schlüsseln gespeichert:

```
{
    "user name": "database user name",
    "password": "password"
}
```

> **Note**
>
> Wir empfehlen Ihnen, Ihre Anmeldeinformationen und Ihr Geheimnis regelmäßig zu aktualisieren oder zu wechseln. Stellen Sie zu Ihrer eigenen Sicherheit nur die Zugriffsebene bereit, die erforderlich ist. Wir raten davon ab, Anmeldeinformationen und geheime Daten für alle Datenquellen und Connector-Versionen 1.0 und 2.0 (sofern zutreffend) wiederzuverwenden.

- IAM Rolle — Geben Sie an`RoleArn`, wann Sie anrufen`CreateDataSource`, um einer IAM Rolle Berechtigungen für den Zugriff auf Ihr Secrets Manager Geheimnis und für den Aufruf der

erforderlichen öffentlichen APIs für den Microsoft SQL Server Connector und zum Aufrufen der erforderlichen öffentlichen APIs zu erteilen. Amazon Kendra Weitere Informationen finden Sie unter IAM Rollen für Microsoft SQL Server Datenquellen.

Sie können auch die folgenden optionalen Funktionen hinzufügen:

- Virtual Private Cloud (VPC) — Geben Sie an, `VpcConfiguration` wann Sie anrufen. `CreateDataSource` Weitere Informationen finden Sie unter Konfigurieren von Amazon Kendra für die Verwendung eines Amazon VPC.
- Inklusions- und Ausschlussfilter — Sie können mithilfe von Benutzer-IDs, Gruppen, Quell-URLs, Zeitstempeln und Zeitzonen angeben, ob bestimmte Inhalte eingeschlossen werden sollen.
- Benutzerkontextfilterung und Zugriffskontrolle —Amazon Kendra durchsucht die Zugriffskontrollliste (ACL) für Ihre Dokumente, sofern Sie über eine ACL für Ihre Dokumente verfügen. Die ACL-Informationen werden verwendet, um Suchergebnisse nach dem Benutzer- oder Gruppenzugriff auf Dokumente zu filtern. Weitere Informationen finden Sie unter Benutzerkontextfilterung.
- Feldzuordnungen — Wählen Sie diese Option, um Ihre Microsoft SQL Server Datenquellenfelder Ihren Indexfeldern zuzuordnen. Amazon Kendra Weitere Informationen finden Sie unter Zuweisen von Datenquellenfeldern.

> **Note**
>
> Das Textfeld oder das entsprechende Textfeld für Ihre Dokumente ist erforderlich, um Ihre Dokumente durchsuchen Amazon Kendra zu können. Sie müssen den Feldnamen Ihres Dokumenthauptteils in Ihrer Datenquelle dem Namen des Indexfeldes zuordnen`_document_body`. Alle anderen Felder sind optional.

Eine Liste weiterer wichtiger JSON-Schlüssel, die konfiguriert werden müssen, finden Sie unterMicrosoft SQL Server-Vorlagenschema.

Hinweise

- Gelöschte Datenbankzeilen werden nicht nachverfolgt, wenn nach Amazon Kendra aktualisierten Inhalten gesucht wird.

- Die Größe von Feldnamen und Werten in einer Zeile Ihrer Datenbank darf 400 KB nicht überschreiten.
- Wenn Ihre Datenbankdatenquelle eine große Datenmenge enthält und Sie nicht möchten Amazon Kendra , dass Ihr gesamter Datenbankinhalt nach der ersten Synchronisierung indexiert wird, können Sie wählen, ob nur neue, geänderte oder gelöschte Dokumente synchronisiert werden sollen.
- Es hat sich bewährt, nur lesbare Amazon Kendra Datenbankanmeldeinformationen zur Verfügung zu stellen.
- Es hat sich bewährt, das Hinzufügen von Tabellen mit sensiblen Daten oder personenbezogenen Daten (PII) zu vermeiden.

Microsoft Teams

Microsoft Teams ist ein Tool für die Zusammenarbeit in Unternehmen für Messaging, Besprechungen und Filesharing. Wenn Sie ein Microsoft Teams-Benutzer sind, können Sie Amazon Kendra damit Ihre Microsoft Teams-Datenquelle indizieren.

Sie können über Amazon Kendra die Amazon Kendra Konsole und die TemplateConfigurationAPI eine Verbindung zu Ihrer Microsoft Teams-Datenquelle herstellen.

Informationen zur Problembehandlung Ihres Amazon Kendra Microsoft Teams-Datenquellenconnectors finden Sie unterProblembehandlung bei Datenquellen.

Themen

- Unterstützte Features
- Voraussetzungen
- Anweisungen zur Verbindung
- Weitere Informationen

Unterstützte Features

- Feldzuordnungen
- Filterung des Benutzerkontextes
- Crawling der Benutzeridentität
- Einschluss-/Ausschlussfilter

- Vollständige und inkrementelle Inhaltssynchronisierung
- Virtual Private Cloud (VPC)

Voraussetzungen

Bevor Sie Ihre Microsoft Teams-Datenquelle Amazon Kendra zum Indizieren verwenden können, nehmen Sie diese Änderungen in Ihren Microsoft Teams und AWS Konten vor.

Stellen Sie in Microsoft Teams sicher, dass Sie über Folgendes verfügen:

- Hat ein Microsoft Teams-Konto in Office 365 erstellt.
- Haben Sie Ihre Microsoft 365-Mandanten-ID notiert. Sie finden Ihre Mandanten-ID in den Eigenschaften Ihres Azure Active Directory-Portals oder in Ihrer OAuth-Anwendung.
- Sie haben eine OAuth-Anwendung im Azure-Portal erstellt und die Client-ID und das Client-Geheimnis oder die Kundenanmeldedaten notiert. Weitere Informationen finden Sie im Microsoft-Tutorial und im Beispiel für registrierte Apps.

  > **Note**
  >
  > Wenn Sie eine App im Azure-Portal erstellen oder registrieren, stellt die geheime ID den tatsächlichen geheimen Wert dar. Sie müssen den tatsächlichen geheimen Wert sofort bei der Erstellung des Geheimnisses und der App notieren oder speichern. Sie können auf Ihr Geheimnis zugreifen, indem Sie den Namen Ihrer Anwendung im Azure-Portal auswählen und dann zur Menüoption für Zertifikate und Geheimnisse navigieren.
  > Sie können auf Ihre Client-ID zugreifen, indem Sie den Namen Ihrer Anwendung im Azure-Portal auswählen und dann zur Übersichtsseite navigieren. Die Anwendungs-ID (Client) ist die Client-ID.

- Die erforderlichen Berechtigungen wurden hinzugefügt. Sie können wählen, ob Sie alle Berechtigungen hinzufügen möchten, oder Sie können den Umfang einschränken, indem Sie weniger Berechtigungen auswählen, je nachdem, welche Entitäten Sie crawlen möchten. In der folgenden Tabelle sind die Berechtigungen auf Anwendungsebene nach der entsprechenden Entität aufgeführt:

Entität	Erforderliche Berechtigungen für die Datensynchronisierung	Erforderliche Berechtigungen für Identity Sync
Beitrag auf dem Kanal	• ChannelMessage.Lesen.Alles • Gruppe.Lesen.Alle • Benutzer.Lesen • Benutzer.Lesen.Alle	TeamMember.Lesen.Alle
Anschluss an den Kanal	• ChannelMessage.Lesen.Alles • Gruppe.Lesen.Alle • Benutzer.Lesen • Benutzer.Lesen.Alle	TeamMember.Lesen.Alle
Kanal-Wiki	• Gruppe.Read.All • Benutzer.Lesen • Benutzer.Lesen.Alle	TeamMember.Lesen.Alle
Chat-Nachricht	• Chatten. Lesen. Alles • ChatMessage. Lesen.Alles • ChatMember.Lesen.Alles • Benutzer.Lesen • Benutzer.Lesen.Alle • Gruppe.Lesen.Alle	TeamMember.Lesen.Alle
Besprechung, Chat	• Chatten. Lesen. Alles • ChatMessage.Lesen • ChatMember.Lesen.Alles • Benutzer.Lesen • Benutzer.Lesen.Alle • Gruppe.Lesen.Alle	TeamMember.Lesen.Alle

Entität	Erforderliche Berechtigungen für die Datensynchronisierung	Erforderliche Berechtigungen für Identity Sync
Chat-Anhang	• Chatten. Lesen. Alles • ChatMessage.Lesen • ChatMember.Lesen.Alles • Benutzer.Lesen • Benutzer.Lesen.Alle • Gruppe.Lesen.Alle	TeamMember.Lesen.Alle
Besprechungsdatei	• Chatten. Lesen. Alles • ChatMessage. Lesen.Alles • ChatMember.Lesen.Alles • Benutzer.Lesen • Benutzer.Lesen.Alle • Gruppe.Lesen.Alle • Dateien.Lesen.Alle	TeamMember.Lesen.Alle
Besprechungskalender	• Chatten. Lesen. Alles • ChatMessage. Lesen.Alles • ChatMember.Lesen.Alles • Benutzer.Lesen • Benutzer.Lesen.Alle • Gruppe.Lesen.Alle • Dateien.Lesen.Alle	TeamMember.Lesen.Alle
Notizen zur Besprechung	• Benutzer.Lesen • Benutzer.Lesen.Alle • Gruppe.Lesen.Alle • Dateien.Lesen.Alle	TeamMember.Lesen.Alle

- Aktiviert, dass jedes Dokument in Microsoft Teams und in anderen Datenquellen, die Sie für denselben Index verwenden möchten, einzigartig ist. Jede Datenquelle, die Sie für einen Index

verwenden möchten, darf nicht dasselbe Dokument in allen Datenquellen enthalten. Dokument-IDs gelten für einen Index global und müssen pro Index eindeutig sein.

Stellen Sie sicher AWS-Konto, dass Sie Folgendes in Ihrem haben:

- Hat einen Amazon Kendra Index erstellt und bei Verwendung der API die Index-ID notiert.
- Sie haben eine IAM Rolle für Ihre Datenquelle erstellt und, falls Sie die API verwenden, den ARN der IAM Rolle notiert.

> **Note**
>
> Wenn Sie Ihren Authentifizierungstyp und Ihre Anmeldeinformationen ändern, müssen Sie Ihre IAM Rolle aktualisieren, um auf die richtige AWS Secrets Manager geheime ID zugreifen zu können.

- Haben Ihre Microsoft Teams-Authentifizierungsdaten AWS Secrets Manager geheim gespeichert und, falls Sie die API verwenden, den ARN des Geheimnisses notiert.

> **Note**
>
> Wir empfehlen Ihnen, Ihre Anmeldeinformationen und Ihr Geheimnis regelmäßig zu aktualisieren oder zu wechseln. Stellen Sie zu Ihrer eigenen Sicherheit nur die Zugriffsebene bereit, die erforderlich ist. Wir raten davon ab, Anmeldeinformationen und geheime Daten für alle Datenquellen und Connector-Versionen 1.0 und 2.0 (sofern zutreffend) wiederzuverwenden.

Wenn Sie noch keine IAM Rolle oder keinen Schlüssel haben, können Sie die Konsole verwenden, um eine neue IAM Rolle und ein neues Secrets Manager Geheimnis zu erstellen, wenn Sie Ihre Microsoft Teams-Datenquelle mit verbinden Amazon Kendra. Wenn Sie die API verwenden, müssen Sie den ARN einer vorhandenen IAM Rolle und eines Secrets Manager Geheimnisses sowie eine Index-ID angeben.

Anweisungen zur Verbindung

Um eine Verbindung Amazon Kendra zu Ihrer Microsoft Teams-Datenquelle herzustellen, müssen Sie die erforderlichen Details zu Ihrer Microsoft Teams-Datenquelle angeben, damit Sie auf Ihre Daten

zugreifen Amazon Kendra können. Wenn Sie Microsoft Teams für noch nicht konfiguriert haben Amazon Kendra, finden Sie weitere Informationen unterVoraussetzungen.

Console

So stellen Sie eine Verbindung Amazon Kendra zu Microsoft Teams her

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die Amazon Kendra Konsole.
2. Wählen Sie im linken Navigationsbereich Indizes und dann den Index, den Sie verwenden möchten, aus der Indexliste aus.

   > **Note**
   >
   > Sie können Ihre Einstellungen für die Benutzerzugriffskontrolle unter Indexeinstellungen konfigurieren oder bearbeiten.

3. Wählen Sie auf der Seite Erste Schritte die Option Datenquelle hinzufügen aus.
4. Wählen Sie auf der Seite Datenquelle hinzufügen die Option Microsoft Teams-Connector und dann Connector hinzufügen aus.
5. Geben Sie auf der Seite „Datenquellendetails angeben“ die folgenden Informationen ein:

   a. Geben Sie im Feld Name und Beschreibung für Datenquellenname einen Namen für Ihre Datenquelle ein. Sie können Bindestriche, aber keine Leerzeichen verwenden.

   b. (Optional) Beschreibung — Geben Sie eine optionale Beschreibung für Ihre Datenquelle ein.

   c. In Standardsprache — Wählen Sie eine Sprache aus, um Ihre Dokumente nach dem Index zu filtern. Sofern Sie nichts anderes angeben, ist die Standardsprache Englisch. Die in den Metadaten des Dokuments angegebene Sprache hat Vorrang vor der ausgewählten Sprache.

   d. Unter Tags für Neues Tag hinzufügen — Fügen Sie optionale Tags hinzu, um Ihre Ressourcen zu durchsuchen und zu filtern oder Ihre Kosten nachzuverfolgen. AWS

   e. Wählen Sie Weiter aus.

6. Geben Sie auf der Seite Zugriff und Sicherheit definieren die folgenden Informationen ein:

a. Quelle — Geben Sie Ihre Microsoft 365-Mandanten-ID ein. Sie finden Ihre Mandanten-ID in den Eigenschaften Ihres Azure Active Directory-Portals oder in Ihrer OAuth-Anwendung.

b. AWS Secrets Manager geheim — Wählen Sie ein vorhandenes Geheimnis aus, oder erstellen Sie ein neues Secrets Manager Geheimnis, um Ihre Microsoft Teams-Authentifizierungsdaten zu speichern. Wenn Sie ein neues Geheimnis erstellen möchten, wird ein AWS Secrets Manager geheimes Fenster geöffnet.

   i. Geben Sie die folgenden Informationen in das Fenster Create an AWS Secrets Manager Secret ein:

      A. Geheimer Name — Ein Name für Ihr Geheimnis. Das Präfix 'AmazonKendra-Microsoft Teams-' wird Ihrem geheimen Namen automatisch hinzugefügt.

      B. Für Client ID und Client Secret: Geben Sie die Werte für die Authentifizierungsdaten ein, die Sie in Ihrem Microsoft Teams-Konto im Azure-Portal generiert haben.

   ii. Wählen Sie Speichern.

c. Zahlungsmodell — Sie können ein Lizenz- und Zahlungsmodell für Ihr Microsoft Teams-Konto wählen. Modell A-Zahlungsmodelle sind auf Lizenz- und Zahlungsmodelle beschränkt, für die Sicherheitsbestimmungen eingehalten werden müssen. Die Zahlungsmodelle des Modells B eignen sich für Lizenz- und Zahlungsmodelle, für die keine Einhaltung von Sicherheitsvorschriften erforderlich ist.

d. Virtual Private Cloud (VPC) — Sie können wählen, ob Sie eine VPC verwenden möchten. In diesem Fall müssen Sie Subnetze und VPC-Sicherheitsgruppen hinzufügen.

e. Identity Crawler — Geben Sie an, ob der Identity Crawler aktiviert Amazon Kendra werden soll. Der Identity Crawler verwendet die Informationen der Zugriffskontrollliste (ACL) für Ihre Dokumente, um Suchergebnisse nach dem Benutzer- oder Gruppenzugriff auf Dokumente zu filtern. Wenn Sie über eine ACL für Ihre Dokumente verfügen und Ihre ACL verwenden möchten, können Sie auch den Identity Crawler aktivieren, um die Benutzerkontextfilterung der Suchergebnisse zu konfigurieren. Amazon Kendra Andernfalls können alle Dokumente öffentlich durchsucht werden, wenn Identity Crawler ausgeschaltet ist. Wenn Sie die Zugriffskontrolle für Ihre Dokumente verwenden möchten und Identity Crawler ausgeschaltet ist, können Sie alternativ die PutPrincipalMappingAPI verwenden, um Benutzer- und Gruppenzugriffsinformationen für die Benutzerkontextfilterung hochzuladen.

f. IAM Rolle — Wählen Sie eine bestehende IAM Rolle oder erstellen Sie eine neue IAM Rolle, um auf Ihre Repository-Anmeldeinformationen und Indexinhalte zuzugreifen.

> **Note**
>
> IAM Rollen, die für Indizes verwendet werden, können nicht für Datenquellen verwendet werden. Wenn Sie sich nicht sicher sind, ob eine vorhandene Rolle für einen Index oder eine häufig gestellte Frage verwendet wird, wählen Sie Neue Rolle erstellen, um Fehler zu vermeiden.

g. Wählen Sie Weiter aus.

7. Geben Sie auf der Seite „Synchronisierungseinstellungen konfigurieren“ die folgenden Informationen ein:

   a. Inhalte synchronisieren — Wählen Sie die zu synchronisierenden Inhalte aus.

   b. Zusätzliche Konfiguration — Sie können diese Einstellungen optional verwenden, um bestimmte Inhalte zu indizieren, anstatt alle Dokumente zu synchronisieren.

   c. Synchronisierungsmodus — Wählen Sie aus, wie Sie Ihren Index aktualisieren möchten, wenn sich der Inhalt Ihrer Datenquelle ändert. Wenn Sie Ihre Datenquelle Amazon Kendra zum ersten Mal synchronisieren, werden alle Inhalte standardmäßig gecrawlt und indexiert. Sie müssen eine vollständige Synchronisierung Ihrer Daten durchführen, falls Ihre erste Synchronisierung fehlgeschlagen ist, auch wenn Sie die Option Vollsynchronisierung nicht als Synchronisierungsmodusoption wählen.

      - Vollständige Synchronisierung: Indizieren Sie den gesamten Inhalt neu und ersetzen die vorhandenen Inhalte jedes Mal, wenn Ihre Datenquelle mit Ihrem Index synchronisiert wird.
      - Neue, geänderte Synchronisierung: Indizieren Sie jedes Mal, wenn Ihre Datenquelle mit Ihrem Index synchronisiert wird, nur neue und geänderte Inhalte. Amazon Kendra kann den Mechanismus Ihrer Datenquelle verwenden, um Inhaltsänderungen nachzuverfolgen und Inhalte zu indexieren, die sich seit der letzten Synchronisierung geändert haben.
      - Neue, geänderte, gelöschte Synchronisierung: Indizieren Sie bei jeder Synchronisierung Ihrer Datenquelle mit Ihrem Index nur neue, geänderte und gelöschte Inhalte. Amazon Kendra kann den Mechanismus Ihrer Datenquelle

verwenden, um Inhaltsänderungen nachzuverfolgen und Inhalte zu indexieren, die sich seit der letzten Synchronisierung geändert haben.

8. Geben Sie auf der Seite Feldzuordnungen festlegen die folgenden Informationen ein:

   a. Standard-Datenquellenfelder — Wählen Sie eines der Amazon Kendra generierten Standard-Datenquellenfelder aus, die Sie Ihrem Index zuordnen möchten.

   b. Feld hinzufügen — Um benutzerdefinierte Datenquellenfelder hinzuzufügen, um einen Indexfeldnamen für die Zuordnung und den Felddatentyp zu erstellen.

   c. Wählen Sie Weiter aus.

9. Überprüfen Sie auf der Seite Überprüfen und erstellen, ob die von Ihnen eingegebenen Informationen korrekt sind, und wählen Sie dann Datenquelle hinzufügen aus. Sie können Ihre Informationen auch auf dieser Seite bearbeiten. Ihre Datenquelle wird auf der Seite Datenquellen angezeigt, nachdem die Datenquelle erfolgreich hinzugefügt wurde.

API

So stellen Sie eine Verbindung Amazon Kendra zu Microsoft Teams her

Sie müssen mithilfe der TemplateConfigurationAPI eine JSON-Datei des Datenquellenschemas angeben. Sie müssen die folgenden Informationen angeben:

- Datenquelle — Geben Sie den Datenquellentyp wie `MSTEAMS` bei der Verwendung des TemplateConfigurationJSON-Schemas an. Geben Sie außerdem die Datenquelle so an`TEMPLATE`, wie Sie die CreateDataSourceAPI aufrufen.
- Mandanten-ID — Sie finden Ihre Mandanten-ID in den Eigenschaften Ihres Azure Active Directory-Portals oder in Ihrer OAuth-Anwendung.
- Synchronisierungsmodus — Geben Sie an, wie Ihr Index aktualisiert Amazon Kendra werden soll, wenn sich der Inhalt Ihrer Datenquelle ändert. Wenn Sie Ihre Datenquelle Amazon Kendra zum ersten Mal synchronisieren, werden alle Inhalte standardmäßig gecrawlt und indexiert. Sie müssen eine vollständige Synchronisierung Ihrer Daten durchführen, falls Ihre erste Synchronisierung fehlgeschlagen ist, auch wenn Sie die Option Vollsynchronisierung nicht als Synchronisierungsmodusoption wählen. Sie können wählen zwischen:
  - `FORCED_FULL_CRAWL`um den gesamten Inhalt neu zu indizieren und vorhandene Inhalte jedes Mal zu ersetzen, wenn Ihre Datenquelle mit Ihrem Index synchronisiert wird.
  - `FULL_CRAWL`um bei jeder Synchronisierung Ihrer Datenquelle mit Ihrem Index nur neue, geänderte und gelöschte Inhalte zu indizieren. Amazon Kendra kann den Mechanismus Ihrer

Datenquelle verwenden, um Inhaltsänderungen nachzuverfolgen und Inhalte zu indexieren, die sich seit der letzten Synchronisierung geändert haben.

- `CHANGE_LOG`um jedes Mal, wenn Ihre Datenquelle mit Ihrem Index synchronisiert wird, nur neue und geänderte Inhalte zu indizieren. Amazon Kendra kann den Mechanismus Ihrer Datenquelle verwenden, um Inhaltsänderungen nachzuverfolgen und Inhalte zu indexieren, die sich seit der letzten Synchronisierung geändert haben.

- Geheimer Amazon-Ressourcenname (ARN) — Geben Sie den Amazon-Ressourcennamen (ARN) eines Secrets Manager Geheimnisses ein, das die Authentifizierungsdaten für Ihr Microsoft Teams-Konto enthält. Das Geheimnis wird in einer JSON-Struktur mit den folgenden Schlüsseln gespeichert:

```
{
    "clientId": "client ID",
    "clientSecret": "client secret"
}
```

> **Note**
>
> Wir empfehlen Ihnen, Ihre Anmeldeinformationen und Ihr Geheimnis regelmäßig zu aktualisieren oder zu wechseln. Stellen Sie zu Ihrer eigenen Sicherheit nur die Zugriffsebene bereit, die erforderlich ist. Wir raten davon ab, Anmeldeinformationen und geheime Daten für alle Datenquellen und Connector-Versionen 1.0 und 2.0 (sofern zutreffend) wiederzuverwenden.

- IAM role — Geben Sie an`RoleArn`, wann Sie anrufen`CreateDataSource`, um einer IAM Rolle Berechtigungen für den Zugriff auf Ihr Secrets Manager Geheimnis und den Aufruf der erforderlichen öffentlichen APIs für den Microsoft Teams-Connector und Amazon Kendra zuzuweisen. Weitere Informationen finden Sie unter IAM Rollen für Microsoft Teams-Datenquellen.

Sie können auch die folgenden optionalen Funktionen hinzufügen:

- Virtual Private Cloud (VPC) — Geben Sie an, `VpcConfiguration` wann Sie anrufen. `CreateDataSource` Weitere Informationen finden Sie unter Konfigurieren von Amazon Kendra für die Verwendung eines Amazon VPC.

- Inklusions- und Ausschlussfilter — Geben Sie an, ob bestimmte Inhalte in Microsoft Teams ein- oder ausgeschlossen werden sollen. Sie können Teamnamen, Kanalnamen, Dateinamen und Dateitypen, Benutzer-E-Mails, OneNote Abschnitte und OneNote Seiten ein- oder ausschließen. Du kannst auch angeben, ob Chat-Nachrichten und -Anlagen, Kanalbeiträge und -anhänge, Kanal-Wikis, Kalenderinhalte, Besprechungs-Chats sowie Dateien und Notizen indexiert werden sollen.

  > **Note**
  >
  > Die meisten Datenquellen verwenden Muster für reguläre Ausdrücke, bei denen es sich um Ein- oder Ausschlussmuster handelt, die als Filter bezeichnet werden. Wenn Sie einen Einschlussfilter angeben, werden nur Inhalte indexiert, die dem Einschlussfilter entsprechen. Jedes Dokument, das nicht dem Einschlussfilter entspricht, wird nicht indexiert. Wenn Sie einen Ein- und Ausschlussfilter angeben, werden Dokumente, die dem Ausschlussfilter entsprechen, nicht indexiert, auch wenn sie dem Einschlussfilter entsprechen.

- Identity Crawler — Geben Sie an, ob der Identity Crawler aktiviert Amazon Kendra werden soll. Der Identity Crawler verwendet die Informationen der Zugriffskontrollliste (ACL) für Ihre Dokumente, um Suchergebnisse nach dem Benutzer- oder Gruppenzugriff auf Dokumente zu filtern. Wenn Sie über eine ACL für Ihre Dokumente verfügen und Ihre ACL verwenden möchten, können Sie auch den Identity Crawler aktivieren, um die Benutzerkontextfilterung der Suchergebnisse zu konfigurieren. Amazon Kendra Andernfalls können alle Dokumente öffentlich durchsucht werden, wenn Identity Crawler ausgeschaltet ist. Wenn Sie die Zugriffskontrolle für Ihre Dokumente verwenden möchten und Identity Crawler ausgeschaltet ist, können Sie alternativ die PutPrincipalMappingAPI verwenden, um Benutzer- und Gruppenzugriffsinformationen für die Benutzerkontextfilterung hochzuladen.
- Feldzuordnungen — Wählen Sie diese Option, um Ihre Microsoft Teams-Datenquellenfelder Ihren Amazon Kendra Indexfeldern zuzuordnen. Weitere Informationen finden Sie unter Zuweisen von Datenquellenfeldern.

  > **Note**
  >
  > Das Textfeld oder das entsprechende Textfeld für Ihre Dokumente ist erforderlich, um Ihre Dokumente durchsuchen Amazon Kendra zu können. Sie müssen den

Feldnamen Ihres Dokumenthauptteils in Ihrer Datenquelle dem Namen des Indexfeldes zuordnen_document_body. Alle anderen Felder sind optional.

Eine Liste weiterer wichtiger JSON-Schlüssel, die konfiguriert werden müssen, finden Sie unterMicrosoft Teams-Vorlagenschema.

Weitere Informationen

Weitere Informationen zur Integration Amazon Kendra mit Ihrer Microsoft Teams-Datenquelle finden Sie unter:

- Durchsuchen Sie die Microsoft Teams-Datenquelle Ihres Unternehmens intelligent mit dem Amazon Kendra Connector für Microsoft Teams

Microsoft Yammer

Microsoft Yammer ist ein Tool für die Zusammenarbeit in Unternehmen für Messaging, Besprechungen und Filesharing. Wenn Sie ein Microsoft Yammer-Benutzer sind, können Sie Amazon Kendra damit Ihre Microsoft Yammer-Datenquelle indizieren.

Sie können über Amazon Kendra die Amazon Kendra Konsole und die TemplateConfigurationAPI eine Verbindung zu Ihrer Microsoft Yammer-Datenquelle herstellen.

Informationen zur Problembehandlung Ihres Amazon Kendra Microsoft Yammer-Datenquellenconnectors finden Sie unterProblembehandlung bei Datenquellen.

Unterstützte Features

- Feldzuordnungen
- Einschluss-/Ausschlussfilter
- Vollständige und inkrementelle Inhaltssynchronisierung
- Virtual Private Cloud (VPC)

Voraussetzungen

Bevor Sie Ihre Microsoft Yammer-Datenquelle Amazon Kendra zum Indizieren verwenden können, nehmen Sie diese Änderungen in Ihrem Microsoft Yammer und AWS Ihren Konten vor.

Stellen Sie in Microsoft Yammer sicher, dass Sie über Folgendes verfügen:

- Es wurde ein Microsoft Yammer-Administratorkonto in Office 365 erstellt.
- Haben Ihren Microsoft Yammer-Benutzernamen und Ihr Passwort notiert.
- Haben Sie Ihre Microsoft 365-Mandanten-ID notiert. Sie finden Ihre Mandanten-ID in den Eigenschaften Ihres Azure Active Directory-Portals oder in Ihrer OAuth-Anwendung.
- Sie haben eine OAuth-Anwendung im Azure-Portal erstellt und die Client-ID und das Client-Geheimnis oder die Kundenanmeldedaten notiert. Weitere Informationen finden Sie im Microsoft-Tutorial und im Beispiel für registrierte Apps.

  > **Note**
  >
  > Wenn Sie eine App im Azure-Portal erstellen oder registrieren, stellt die geheime ID den tatsächlichen geheimen Wert dar. Sie müssen den tatsächlichen geheimen Wert sofort bei der Erstellung des Geheimnisses und der App notieren oder speichern. Sie können auf Ihr Geheimnis zugreifen, indem Sie den Namen Ihrer Anwendung im Azure-Portal auswählen und dann zur Menüoption für Zertifikate und Geheimnisse navigieren.
  > Sie können auf Ihre Client-ID zugreifen, indem Sie den Namen Ihrer Anwendung im Azure-Portal auswählen und dann zur Übersichtsseite navigieren. Die Anwendungs-ID (Client) ist die Client-ID.

- Aktiviert, dass jedes Dokument in Microsoft Yammer und in anderen Datenquellen, die Sie für denselben Index verwenden möchten, eindeutig ist. Jede Datenquelle, die Sie für einen Index verwenden möchten, darf nicht dasselbe Dokument in allen Datenquellen enthalten. Dokument-IDs gelten für einen Index global und müssen pro Index eindeutig sein.

Stellen Sie sicher AWS-Konto, dass Sie Folgendes in Ihrem haben:

- Hat einen Amazon Kendra Index erstellt und bei Verwendung der API die Index-ID notiert.
- Sie haben eine IAM Rolle für Ihre Datenquelle erstellt und, falls Sie die API verwenden, den ARN der IAM Rolle notiert.

> **Note**
>
> Wenn Sie Ihren Authentifizierungstyp und Ihre Anmeldeinformationen ändern, müssen Sie Ihre IAM Rolle aktualisieren, um auf die richtige AWS Secrets Manager geheime ID zugreifen zu können.

- Ihre Microsoft Yammer-Authentifizierungsanmeldedaten AWS Secrets Manager geheim gespeichert und, falls Sie die API verwenden, den ARN des Geheimnisses notiert.

> **Note**
>
> Wir empfehlen Ihnen, Ihre Anmeldeinformationen und Ihr Geheimnis regelmäßig zu aktualisieren oder zu wechseln. Stellen Sie zu Ihrer eigenen Sicherheit nur die Zugriffsebene bereit, die erforderlich ist. Wir raten davon ab, Anmeldeinformationen und geheime Daten für alle Datenquellen und Connector-Versionen 1.0 und 2.0 (sofern zutreffend) wiederzuverwenden.

Wenn Sie noch keine IAM Rolle oder keinen Schlüssel haben, können Sie die Konsole verwenden, um eine neue IAM Rolle und ein neues Secrets Manager Geheimnis zu erstellen, wenn Sie Ihre Microsoft Yammer-Datenquelle mit verbinden. Amazon Kendra Wenn Sie die API verwenden, müssen Sie den ARN einer vorhandenen IAM Rolle und eines Secrets Manager Geheimnisses sowie eine Index-ID angeben.

Anweisungen zur Verbindung

Um eine Verbindung Amazon Kendra zu Ihrer Microsoft Yammer-Datenquelle herzustellen, müssen Sie die erforderlichen Details zu Ihrer Microsoft Yammer-Datenquelle angeben, damit Sie auf Ihre Daten zugreifen Amazon Kendra können. Wenn Sie Microsoft Yammer für noch nicht konfiguriert haben Amazon Kendra, finden Sie weitere Informationen unterVoraussetzungen.

Console

So stellen Sie eine Verbindung Amazon Kendra zu Microsoft Yammer her

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die Amazon Kendra Konsole.

2. Wählen Sie im linken Navigationsbereich Indizes und dann den Index, den Sie verwenden möchten, aus der Indexliste aus.

> **Note**
>
> Sie können Ihre Einstellungen für die Benutzerzugriffskontrolle unter Indexeinstellungen konfigurieren oder bearbeiten.

3. Wählen Sie auf der Seite Erste Schritte die Option Datenquelle hinzufügen aus.
4. Wählen Sie auf der Seite Datenquelle hinzufügen die Option Microsoft Yammer-Connector und dann Connector hinzufügen aus.
5. Geben Sie auf der Seite „Datenquellendetails angeben“ die folgenden Informationen ein:

   a. Geben Sie im Feld Name und Beschreibung für Datenquellenname einen Namen für Ihre Datenquelle ein. Sie können Bindestriche, aber keine Leerzeichen verwenden.

   b. (Optional) Beschreibung — Geben Sie eine optionale Beschreibung für Ihre Datenquelle ein.

   c. In Standardsprache — Wählen Sie eine Sprache aus, um Ihre Dokumente nach dem Index zu filtern. Sofern Sie nichts anderes angeben, ist die Standardsprache Englisch. Die in den Metadaten des Dokuments angegebene Sprache hat Vorrang vor der ausgewählten Sprache.

   d. Unter Tags für Neues Tag hinzufügen — Fügen Sie optionale Tags hinzu, um Ihre Ressourcen zu durchsuchen und zu filtern oder Ihre Kosten nachzuverfolgen. AWS

   e. Wählen Sie Weiter aus.
6. Geben Sie auf der Seite Zugriff und Sicherheit definieren die folgenden Informationen ein:

   a. Quelle — Verwenden Sie Ihre Microsoft Yammer-URL.

   b. AWS Secrets Manager geheim — Wählen Sie ein vorhandenes Geheimnis aus, oder erstellen Sie ein neues Secrets Manager Geheimnis, um Ihre Microsoft Yammer-Authentifizierungsanmeldeinformationen zu speichern. Wenn Sie ein neues Geheimnis erstellen möchten, wird ein AWS Secrets Manager geheimes Fenster geöffnet.

      i. Geben Sie die folgenden Informationen in das Fenster Create an AWS Secrets Manager Secret ein:

         A. Geheimer Name — Ein Name für Ihr Geheimnis. Das Präfix 'AmazonKendra-Microsoft Yammer-' wird Ihrem geheimen Namen automatisch hinzugefügt.

B. Für Username, Password — Geben Sie Ihren Microsoft Yammer-Benutzernamen und Ihr Passwort ein.

C. Für Client ID, Client secret — Geben Sie die Werte für die Authentifizierungsdaten ein, die Sie mit Ihrem Microsoft Yammer-Konto im Azure-Portal generiert haben.

ii. Wählen Sie Speichern.

c. Virtual Private Cloud (VPC) — Sie können wählen, ob Sie eine VPC verwenden möchten. In diesem Fall müssen Sie Subnetze und VPC-Sicherheitsgruppen hinzufügen.

d. Identity Crawler — Geben Sie an, ob der Identity Crawler aktiviert Amazon Kendra werden soll. Der Identity Crawler verwendet die Informationen der Zugriffskontrollliste (ACL) für Ihre Dokumente, um Suchergebnisse nach dem Benutzer- oder Gruppenzugriff auf Dokumente zu filtern. Wenn Sie über eine ACL für Ihre Dokumente verfügen und Ihre ACL verwenden möchten, können Sie auch den Identity Crawler aktivieren, um die Benutzerkontextfilterung von Suchergebnissen zu konfigurieren. Amazon Kendra Andernfalls können alle Dokumente öffentlich durchsucht werden, wenn Identity Crawler ausgeschaltet ist. Wenn Sie die Zugriffskontrolle für Ihre Dokumente verwenden möchten und Identity Crawler ausgeschaltet ist, können Sie alternativ die PutPrincipalMappingAPI verwenden, um Benutzer- und Gruppenzugriffsinformationen für die Benutzerkontextfilterung hochzuladen.

e. IAM Rolle — Wählen Sie eine bestehende IAM Rolle oder erstellen Sie eine neue IAM Rolle, um auf Ihre Repository-Anmeldeinformationen und Indexinhalte zuzugreifen.

> **Note**
>
> IAM Rollen, die für Indizes verwendet werden, können nicht für Datenquellen verwendet werden. Wenn Sie sich nicht sicher sind, ob eine vorhandene Rolle für einen Index oder eine häufig gestellte Frage verwendet wird, wählen Sie Neue Rolle erstellen, um Fehler zu vermeiden.

f. Wählen Sie Weiter aus.

7. Geben Sie auf der Seite „Synchronisierungseinstellungen konfigurieren“ die folgenden Informationen ein:

a. Seit dem Datum — Geben Sie das Datum an, an dem mit dem Crawlen Ihrer Daten in Microsoft Yammer begonnen werden soll.

b. Inhalte synchronisieren — Wählen Sie den Inhaltstyp aus, den Sie indexieren möchten. Zum Beispiel öffentliche Nachrichten, private Nachrichten und Anlagen.

c. Zusätzliche Konfiguration — Sie können diese Optionen optional verwenden, um bestimmte Inhalte zu indizieren, anstatt alle Dokumente zu synchronisieren. Sie können beispielsweise bestimmte Community-Namen indizieren und Muster mit regulären Ausdrücken verwenden, um bestimmte Dateien ein- oder auszuschließen.

d. Synchronisierungsmodus — Wählen Sie aus, wie Sie Ihren Index aktualisieren möchten, wenn sich der Inhalt Ihrer Datenquelle ändert. Wenn Sie Ihre Datenquelle Amazon Kendra zum ersten Mal synchronisieren, werden alle Inhalte standardmäßig gecrawlt und indexiert. Sie müssen eine vollständige Synchronisierung Ihrer Daten durchführen, falls Ihre erste Synchronisierung fehlgeschlagen ist, auch wenn Sie die Option Vollsynchronisierung nicht als Synchronisierungsmodusoption wählen.

   - Vollständige Synchronisierung: Indizieren Sie den gesamten Inhalt neu und ersetzen die vorhandenen Inhalte jedes Mal, wenn Ihre Datenquelle mit Ihrem Index synchronisiert wird.
   - Neue, geänderte Synchronisierung: Indizieren Sie jedes Mal, wenn Ihre Datenquelle mit Ihrem Index synchronisiert wird, nur neue und geänderte Inhalte. Amazon Kendra kann den Mechanismus Ihrer Datenquelle verwenden, um Inhaltsänderungen nachzuverfolgen und Inhalte zu indexieren, die sich seit der letzten Synchronisierung geändert haben.
   - Neue, geänderte, gelöschte Synchronisierung: Indizieren Sie bei jeder Synchronisierung Ihrer Datenquelle mit Ihrem Index nur neue, geänderte und gelöschte Inhalte. Amazon Kendra kann den Mechanismus Ihrer Datenquelle verwenden, um Inhaltsänderungen nachzuverfolgen und Inhalte zu indexieren, die sich seit der letzten Synchronisierung geändert haben.

8. Geben Sie auf der Seite Feldzuordnungen festlegen die folgenden Informationen ein:

   a. Standard-Datenquellenfelder — Wählen Sie eines der Amazon Kendra generierten Standard-Datenquellenfelder aus, die Sie Ihrem Index zuordnen möchten.

   b. Feld hinzufügen — Um benutzerdefinierte Datenquellenfelder hinzuzufügen, um einen Indexfeldnamen für die Zuordnung und den Felddatentyp zu erstellen.

   c. Wählen Sie Weiter aus.

9. Überprüfen Sie auf der Seite Überprüfen und erstellen, ob die von Ihnen eingegebenen Informationen korrekt sind, und wählen Sie dann Datenquelle hinzufügen aus. Sie können

Ihre Informationen auch auf dieser Seite bearbeiten. Ihre Datenquelle wird auf der Seite Datenquellen angezeigt, nachdem die Datenquelle erfolgreich hinzugefügt wurde.

API

So stellen Sie eine Verbindung Amazon Kendra zu Microsoft Yammer her

Sie müssen mithilfe der TemplateConfigurationAPI eine JSON-Datei des Datenquellenschemas angeben. Sie müssen die folgenden Informationen angeben:

- Datenquelle — Geben Sie den Datenquellentyp wie `YAMMER` bei der Verwendung des TemplateConfigurationJSON-Schemas an. Geben Sie außerdem die Datenquelle so an`TEMPLATE`, wie Sie die CreateDataSourceAPI aufrufen.
- Synchronisierungsmodus — Geben Sie an, wie Ihr Index aktualisiert Amazon Kendra werden soll, wenn sich der Inhalt Ihrer Datenquelle ändert. Wenn Sie Ihre Datenquelle Amazon Kendra zum ersten Mal synchronisieren, werden alle Inhalte standardmäßig gecrawlt und indexiert. Sie müssen eine vollständige Synchronisierung Ihrer Daten durchführen, falls Ihre erste Synchronisierung fehlgeschlagen ist, auch wenn Sie die Option Vollsynchronisierung nicht als Synchronisierungsmodusoption wählen. Sie können wählen zwischen:
  - `FORCED_FULL_CRAWL`um den gesamten Inhalt neu zu indizieren und vorhandene Inhalte jedes Mal zu ersetzen, wenn Ihre Datenquelle mit Ihrem Index synchronisiert wird.
  - `FULL_CRAWL`um bei jeder Synchronisierung Ihrer Datenquelle mit Ihrem Index nur neue, geänderte und gelöschte Inhalte zu indizieren. Amazon Kendra kann den Mechanismus Ihrer Datenquelle verwenden, um Inhaltsänderungen nachzuverfolgen und Inhalte zu indexieren, die sich seit der letzten Synchronisierung geändert haben.
  - `CHANGE_LOG`um jedes Mal, wenn Ihre Datenquelle mit Ihrem Index synchronisiert wird, nur neue und geänderte Inhalte zu indizieren. Amazon Kendra kann den Mechanismus Ihrer Datenquelle verwenden, um Inhaltsänderungen nachzuverfolgen und Inhalte zu indexieren, die sich seit der letzten Synchronisierung geändert haben.
- Geheimer Amazon-Ressourcenname (ARN) — Geben Sie den Amazon-Ressourcennamen (ARN) eines Secrets Manager Geheimnisses ein, das die Authentifizierungsdaten für Ihr Microsoft Yammer-Konto enthält. Das Geheimnis wird in einer JSON-Struktur mit den folgenden Schlüsseln gespeichert:

```
{
    "username": "user name",
    "password": "password",
```

```
    "clientId": "client ID",
    "clientSecret": "client secret"
}
```

> **Note**
>
> Wir empfehlen Ihnen, Ihre Anmeldeinformationen und Ihr Geheimnis regelmäßig zu aktualisieren oder zu wechseln. Stellen Sie zu Ihrer eigenen Sicherheit nur die Zugriffsebene bereit, die erforderlich ist. Wir raten davon ab, Anmeldeinformationen und geheime Daten für alle Datenquellen und Connector-Versionen 1.0 und 2.0 (sofern zutreffend) wiederzuverwenden.

- IAM role — Geben Sie an`RoleArn`, wann Sie aufrufen`CreateDataSource`, um einer IAM Rolle Berechtigungen für den Zugriff auf Ihr Secrets Manager Geheimnis und den Aufruf der erforderlichen öffentlichen APIs für den Microsoft Yammer-Connector und zuzuweisen. Amazon Kendra Weitere Informationen finden Sie unter IAM Rollen für Microsoft Yammer-Datenquellen.

Sie können auch die folgenden optionalen Funktionen hinzufügen:

- Virtual Private Cloud (VPC) — Geben Sie an, `VpcConfiguration` wann Sie anrufen. `CreateDataSource` Weitere Informationen finden Sie unter Konfigurieren von Amazon Kendra für die Verwendung eines Amazon VPC.
- Inklusions- und Ausschlussfilter — Geben Sie an, ob bestimmte Inhalte ein- oder ausgeschlossen werden sollen.

> **Note**
>
> Die meisten Datenquellen verwenden Muster mit regulären Ausdrücken, bei denen es sich um Ein- oder Ausschlussmuster handelt, die als Filter bezeichnet werden. Wenn Sie einen Einschlussfilter angeben, werden nur Inhalte indexiert, die dem Einschlussfilter entsprechen. Jedes Dokument, das nicht dem Einschlussfilter entspricht, wird nicht indexiert. Wenn Sie einen Ein- und Ausschlussfilter angeben, werden Dokumente, die dem Ausschlussfilter entsprechen, nicht indexiert, auch wenn sie dem Einschlussfilter entsprechen.

- Identity Crawler — Geben Sie an, ob der Identity Crawler aktiviert Amazon Kendra werden soll. Der Identity Crawler verwendet die Informationen der Zugriffskontrollliste (ACL) für Ihre

Dokumente, um Suchergebnisse nach dem Benutzer- oder Gruppenzugriff auf Dokumente zu filtern. Wenn Sie über eine ACL für Ihre Dokumente verfügen und Ihre ACL verwenden möchten, können Sie auch den Identity Crawler aktivieren, um die Benutzerkontextfilterung von Suchergebnissen zu konfigurieren. Amazon Kendra Andernfalls können alle Dokumente öffentlich durchsucht werden, wenn Identity Crawler ausgeschaltet ist. Wenn Sie die Zugriffskontrolle für Ihre Dokumente verwenden möchten und Identity Crawler ausgeschaltet ist, können Sie alternativ die PutPrincipalMappingAPI verwenden, um Benutzer- und Gruppenzugriffsinformationen für die Benutzerkontextfilterung hochzuladen.

- Feldzuordnungen — Wählen Sie diese Option, um Ihre Microsoft Yammer-Datenquellenfelder Ihren Indexfeldern zuzuordnen. Amazon Kendra Weitere Informationen finden Sie unter Zuweisen von Datenquellenfeldern.

> **Note**
>
> Das Textfeld oder das entsprechende Textfeld für Ihre Dokumente ist erforderlich, um Ihre Dokumente durchsuchen Amazon Kendra zu können. Sie müssen den Feldnamen Ihres Dokumenthauptteils in Ihrer Datenquelle dem Namen des Indexfeldes zuordnen`_document_body`. Alle anderen Felder sind optional.

Weitere Informationen

Weitere Informationen zur Integration Amazon Kendra mit Ihrer Microsoft Yammer-Datenquelle finden Sie unter:

- Ankündigung des Yammer-Connectors für Amazon Kendra

MySQL

MySQList ein relationales Open-Source-Datenbankverwaltungssystem. Wenn Sie ein MySQL Benutzer sind, können Sie Amazon Kendra damit Ihre MySQL Datenquelle indizieren. Der Amazon Kendra MySQL Datenquellenconnector unterstützt MySQL 8.0. 21.

Sie können über Amazon Kendra die Amazon Kendra Konsole und die TemplateConfigurationAPI eine Verbindung zu Ihrer MySQL Datenquelle herstellen.

Informationen zur Fehlerbehebung bei Ihrem Amazon Kendra MySQL Datenquellen-Connector finden Sie unterProblembehandlung bei Datenquellen.

Themen

Unterstützte Features

- Feldzuordnungen
- Filterung des Benutzerkontextes
- Einschluss-/Ausschlussfilter
- Vollständige und inkrementelle Inhaltssynchronisierung
- Virtual Private Cloud (VPC)

Voraussetzungen

Bevor Sie Ihre MySQL Datenquelle Amazon Kendra zum Indizieren verwenden können, nehmen Sie diese Änderungen in Ihren Konten MySQL und AWS Konten vor.

Stellen Sie sicherMySQL, dass Sie Folgendes haben:

- Notiert Ihren Datenbank-Benutzernamen und Ihr Passwort.

> **Important**
>
> Es hat sich bewährt, nur lesbare Amazon Kendra Datenbankanmeldeinformationen zur Verfügung zu stellen.

- Die URL, der Port und die Instanz Ihres Datenbank-Hosts wurden kopiert.
- Vergewissert, dass jedes Dokument in MySQL und zwischen anderen Datenquellen, die Sie für denselben Index verwenden möchten, einzigartig ist. Jede Datenquelle, die Sie für einen Index verwenden möchten, darf nicht dasselbe Dokument in allen Datenquellen enthalten. Dokument-IDs gelten für einen Index global und müssen pro Index eindeutig sein.

Stellen Sie sicher AWS-Konto, dass Sie Folgendes in Ihrem haben:

- Hat einen Amazon Kendra Index erstellt und bei Verwendung der API die Index-ID notiert.
- Sie haben eine IAM Rolle für Ihre Datenquelle erstellt und, falls Sie die API verwenden, den ARN der IAM Rolle notiert.

> **Note**
>
> Wenn Sie Ihren Authentifizierungstyp und Ihre Anmeldeinformationen ändern, müssen Sie Ihre IAM Rolle aktualisieren, um auf die richtige AWS Secrets Manager geheime ID zugreifen zu können.

- Wir haben Ihre MySQL Authentifizierungsdaten AWS Secrets Manager geheim gespeichert und, falls Sie die API verwenden, den ARN des Geheimnisses notiert.

> **Note**
>
> Wir empfehlen Ihnen, Ihre Anmeldeinformationen und Ihr Geheimnis regelmäßig zu aktualisieren oder zu wechseln. Stellen Sie zu Ihrer eigenen Sicherheit nur die Zugriffsebene bereit, die erforderlich ist. Wir raten davon ab, Anmeldeinformationen und geheime Daten für alle Datenquellen und Connector-Versionen 1.0 und 2.0 (sofern zutreffend) wiederzuverwenden.

Wenn Sie noch keine IAM Rolle oder keinen Schlüssel haben, können Sie die Konsole verwenden, um eine neue IAM Rolle und ein neues Secrets Manager Geheimnis zu erstellen, wenn Sie Ihre MySQL Datenquelle mit verbinden. Amazon Kendra Wenn Sie die API verwenden, müssen Sie den ARN einer vorhandenen IAM Rolle und eines Secrets Manager Geheimnisses sowie eine Index-ID angeben.

Anweisungen zur Verbindung

Um eine Verbindung Amazon Kendra zu Ihrer MySQL Datenquelle herzustellen, müssen Sie Details zu Ihren MySQL Anmeldeinformationen angeben, damit Sie auf Ihre Daten zugreifen Amazon Kendra können. Falls Sie das noch nicht konfiguriert haben, Amazon Kendra finden Sie MySQL weitere Informationen unterVoraussetzungen.

Console

Um eine Verbindung Amazon Kendra herzustellen MySQL

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die Amazon Kendra Konsole.
2. Wählen Sie im linken Navigationsbereich Indizes und dann den Index, den Sie verwenden möchten, aus der Indexliste aus.

> **Note**
>
> Sie können Ihre Einstellungen für die Benutzerzugriffskontrolle unter Indexeinstellungen konfigurieren oder bearbeiten.

3. Wählen Sie auf der Seite Erste Schritte die Option Datenquelle hinzufügen aus.
4. Wählen Sie auf der Seite Datenquelle hinzufügen die Option MySQLConnector und dann Connector hinzufügen aus.
5. Geben Sie auf der Seite „Datenquellendetails angeben“ die folgenden Informationen ein:
   a. Geben Sie im Feld Name und Beschreibung für Datenquellenname einen Namen für Ihre Datenquelle ein. Sie können Bindestriche, aber keine Leerzeichen verwenden.
   b. (Optional) Beschreibung — Geben Sie eine optionale Beschreibung für Ihre Datenquelle ein.
   c. In Standardsprache — Wählen Sie eine Sprache aus, um Ihre Dokumente nach dem Index zu filtern. Sofern Sie nichts anderes angeben, ist die Standardsprache Englisch. Die in den Metadaten des Dokuments angegebene Sprache hat Vorrang vor der ausgewählten Sprache.
   d. Unter Tags für Neues Tag hinzufügen — Fügen Sie optionale Tags hinzu, um Ihre Ressourcen zu durchsuchen und zu filtern oder Ihre Kosten nachzuverfolgen. AWS
   e. Wählen Sie Weiter aus.
6. Geben Sie auf der Seite Zugriff und Sicherheit definieren die folgenden Informationen ein:
   a. Geben Sie im Feld Quelle die folgenden Informationen ein:
   b. Host — Geben Sie den Datenbank-Hostnamen ein.
   c. Port — Geben Sie den Datenbankport ein.
   d. Instanz — Geben Sie die Datenbankinstanz ein.
   e. Speicherort für SSL-Zertifikate aktivieren — Geben Sie hier den Amazon S3 Pfad zu Ihrer SSL-Zertifikatsdatei ein.
   f. Geben Sie im Feld Authentifizierung die folgenden Informationen ein:

- AWS Secrets Manager geheim — Wählen Sie ein vorhandenes Geheimnis aus, oder erstellen Sie ein neues Secrets Manager Geheimnis, um Ihre MySQL Authentifizierungsdaten zu speichern. Wenn Sie sich dafür entscheiden, ein neues Geheimnis zu erstellen, wird ein AWS Secrets Manager geheimes Fenster geöffnet.

  A. Geben Sie die folgenden Informationen in das Fenster Create an AWS Secrets Manager Secret ein:

     I. Geheimer Name — Ein Name für Ihr Geheimnis. Das Präfix 'AmazonKendra- MySQL -' wird Ihrem geheimen Namen automatisch hinzugefügt.

     II. Für Datenbankbenutzername und Passwort — Geben Sie die Werte der Authentifizierungsdaten ein, die Sie aus Ihrer Datenbank kopiert haben.

  B. Wählen Sie Speichern.

g. Virtual Private Cloud (VPC) — Sie können wählen, ob Sie eine VPC verwenden möchten. In diesem Fall müssen Sie Subnetze und VPC-Sicherheitsgruppen hinzufügen.

h. IAM Rolle — Wählen Sie eine bestehende IAM Rolle oder erstellen Sie eine neue IAM Rolle, um auf Ihre Repository-Anmeldeinformationen und Indexinhalte zuzugreifen.

> **Note**
>
> IAM Rollen, die für Indizes verwendet werden, können nicht für Datenquellen verwendet werden. Wenn Sie sich nicht sicher sind, ob eine vorhandene Rolle für einen Index oder eine häufig gestellte Frage verwendet wird, wählen Sie Neue Rolle erstellen, um Fehler zu vermeiden.

i. Wählen Sie Weiter aus.

7. Geben Sie auf der Seite „Synchronisierungseinstellungen konfigurieren“ die folgenden Informationen ein:

   a. Wählen Sie unter Synchronisierungsbereich eine der folgenden Optionen aus:

   - SQL-Abfrage — Geben Sie SQL-Abfrageanweisungen wie SELECT- und JOIN-Operationen ein. SQL-Abfragen müssen weniger als 32 KB groß sein. Amazon Kendra durchsucht den gesamten Datenbankinhalt, der Ihrer Abfrage entspricht.

- Primärschlüsselspalte — Geben Sie den Primärschlüssel für die Datenbanktabelle an. Dies identifiziert eine Tabelle in Ihrer Datenbank.
- Titelspalte — Geben Sie den Namen der Titelspalte des Dokuments in Ihrer Datenbanktabelle an.
- Hauptspalte — Geben Sie den Namen der Hauptspalte des Dokuments in Ihrer Datenbanktabelle an.

b. Wählen Sie unter Zusätzliche Konfiguration — optional aus den folgenden Optionen, um bestimmte Inhalte zu synchronisieren, anstatt alle Dateien zu synchronisieren:

- Spalten zur Erkennung von Änderungen — Geben Sie die Namen der Spalten ein, anhand derer Inhaltsänderungen erkannt Amazon Kendra werden sollen. Amazon Kendra indexiert den Inhalt neu, wenn sich eine dieser Spalten ändert.
- Spalte mit Benutzer-IDs — Geben Sie den Namen der Spalte ein, die Benutzer-IDs enthält, um Zugriff auf Inhalte zu erhalten.
- Spalte „Gruppen“ — Geben Sie den Namen der Spalte ein, die Gruppen enthält, denen der Zugriff auf Inhalte gewährt werden soll.
- Spalte Quell-URLs — Geben Sie den Namen der Spalte ein, die Quell-URLs enthält, die indexiert werden sollen.
- Spalte mit Zeitstempeln — Geben Sie den Namen der Spalte ein, die Zeitstempel enthält. Amazon Kendra verwendet Zeitstempelinformationen, um Änderungen an Ihren Inhalten zu erkennen und nur geänderte Inhalte zu synchronisieren.
- Spalte „Zeitzonen“ — Geben Sie den Namen der Spalte ein, die Zeitzonen für den Inhalt enthält, der gecrawlt werden soll.
- Zeitstempelformat — Geben Sie den Namen der Spalte ein, die Zeitstempelformate enthält, anhand derer Inhaltsänderungen erkannt und Ihre Inhalte erneut synchronisiert werden sollen.

c. Synchronisierungsmodus — Wählen Sie aus, wie Sie Ihren Index aktualisieren möchten, wenn sich der Inhalt Ihrer Datenquelle ändert. Wenn Sie Ihre Datenquelle Amazon Kendra zum ersten Mal synchronisieren, werden alle Inhalte standardmäßig gecrawlt und indexiert. Sie müssen eine vollständige Synchronisierung Ihrer Daten durchführen, falls Ihre erste Synchronisierung fehlgeschlagen ist, auch wenn Sie die Option Vollsynchronisierung nicht als Synchronisierungsmodusoption wählen.

- Vollständige Synchronisierung: Indizieren Sie den gesamten Inhalt neu und ersetzen die vorhandenen Inhalte jedes Mal, wenn Ihre Datenquelle mit Ihrem Index synchronisiert wird.
- Neue, geänderte Synchronisierung: Indizieren Sie jedes Mal, wenn Ihre Datenquelle mit Ihrem Index synchronisiert wird, nur neue und geänderte Inhalte. Amazon Kendra kann den Mechanismus Ihrer Datenquelle verwenden, um Inhaltsänderungen nachzuverfolgen und Inhalte zu indexieren, die sich seit der letzten Synchronisierung geändert haben.
- Neue, geänderte, gelöschte Synchronisierung: Indizieren Sie bei jeder Synchronisierung Ihrer Datenquelle mit Ihrem Index nur neue, geänderte und gelöschte Inhalte. Amazon Kendra kann den Mechanismus Ihrer Datenquelle verwenden, um Inhaltsänderungen nachzuverfolgen und Inhalte zu indexieren, die sich seit der letzten Synchronisierung geändert haben.

d. Im Synchronisierungslaufplan für Frequenz — Wie oft Amazon Kendra wird mit Ihrer Datenquelle synchronisiert?

e. Wählen Sie Weiter aus.

8. Geben Sie auf der Seite Feldzuordnungen festlegen die folgenden Informationen ein:

   a. Wählen Sie aus den generierten Standard-Datenquellenfeldern — Dokument-IDs, Dokumenttitel und Quell-URLs — aus, die Sie dem Index zuordnen möchten. Amazon Kendra

   b. Feld hinzufügen — Um benutzerdefinierte Datenquellenfelder hinzuzufügen, um einen Indexfeldnamen für die Zuordnung und den Felddatentyp zu erstellen.

   c. Wählen Sie Weiter aus.

9. Überprüfen Sie auf der Seite Überprüfen und erstellen, ob die von Ihnen eingegebenen Informationen korrekt sind, und wählen Sie dann Datenquelle hinzufügen aus. Sie können Ihre Informationen auch auf dieser Seite bearbeiten. Ihre Datenquelle wird auf der Seite Datenquellen angezeigt, nachdem die Datenquelle erfolgreich hinzugefügt wurde.

API

Um eine Verbindung Amazon Kendra herzustellen MySQL

Mithilfe der TemplateConfigurationAPI müssen Sie Folgendes angeben:

- Datenquelle — Geben Sie den Datenquellentyp wie `JDBC` bei der Verwendung des TemplateConfigurationJSON-Schemas an. Geben Sie außerdem die Datenquelle so an`TEMPLATE`, wie Sie die CreateDataSourceAPI aufrufen.
- Datenbanktyp — Sie müssen den Datenbanktyp als `mySql` angeben.
- SQL-Abfrage — Geben Sie SQL-Abfrageanweisungen wie SELECT- und JOIN-Operationen an. SQL-Abfragen müssen weniger als 32 KB groß sein. Amazon Kendra durchsucht den gesamten Datenbankinhalt, der Ihrer Abfrage entspricht.
- Synchronisierungsmodus — Geben Sie an, wie Ihr Index aktualisiert Amazon Kendra werden soll, wenn sich der Inhalt Ihrer Datenquelle ändert. Wenn Sie Ihre Datenquelle Amazon Kendra zum ersten Mal synchronisieren, werden alle Inhalte standardmäßig gecrawlt und indexiert. Sie müssen eine vollständige Synchronisierung Ihrer Daten durchführen, falls Ihre erste Synchronisierung fehlgeschlagen ist, auch wenn Sie die Option Vollsynchronisierung nicht als Synchronisierungsmodusoption wählen. Sie können wählen zwischen:
  - `FORCED_FULL_CRAWL`um den gesamten Inhalt neu zu indizieren und vorhandene Inhalte jedes Mal zu ersetzen, wenn Ihre Datenquelle mit Ihrem Index synchronisiert wird.
  - `FULL_CRAWL`um bei jeder Synchronisierung Ihrer Datenquelle mit Ihrem Index nur neue, geänderte und gelöschte Inhalte zu indizieren. Amazon Kendra kann den Mechanismus Ihrer Datenquelle verwenden, um Inhaltsänderungen nachzuverfolgen und Inhalte zu indexieren, die sich seit der letzten Synchronisierung geändert haben.
  - `CHANGE_LOG`um jedes Mal, wenn Ihre Datenquelle mit Ihrem Index synchronisiert wird, nur neue und geänderte Inhalte zu indizieren. Amazon Kendra kann den Mechanismus Ihrer Datenquelle verwenden, um Inhaltsänderungen nachzuverfolgen und Inhalte zu indexieren, die sich seit der letzten Synchronisierung geändert haben.
- Geheimer Amazon-Ressourcenname (ARN) — Geben Sie den Amazon-Ressourcennamen (ARN) eines Secrets Manager Geheimnisses ein, das die Authentifizierungsdaten enthält, die Sie in Ihrem MySQL Konto erstellt haben. Das Geheimnis wird in einer JSON-Struktur mit den folgenden Schlüsseln gespeichert:

```
{
    "user name": "database user name",
    "password": "password"
}
```

> **Note**
>
> Wir empfehlen Ihnen, Ihre Anmeldeinformationen und Ihr Geheimnis regelmäßig zu aktualisieren oder zu wechseln. Stellen Sie zu Ihrer eigenen Sicherheit nur die Zugriffsebene bereit, die erforderlich ist. Wir raten davon ab, Anmeldeinformationen und geheime Daten für alle Datenquellen und Connector-Versionen 1.0 und 2.0 (sofern zutreffend) wiederzuverwenden.

- IAM Rolle — Geben Sie an`RoleArn`, wann Sie anrufen`CreateDataSource`, um einer IAM Rolle Berechtigungen für den Zugriff auf Ihr Secrets Manager Geheimnis und den Aufruf der erforderlichen öffentlichen APIs für den MySQL Connector und zum Aufrufen der erforderlichen öffentlichen APIs zu erteilen. Amazon Kendra Weitere Informationen finden Sie unter IAM Rollen für MySQL Datenquellen.

Sie können auch die folgenden optionalen Funktionen hinzufügen:

- Virtual Private Cloud (VPC) — Geben Sie an, `VpcConfiguration` wann Sie anrufen. `CreateDataSource` Weitere Informationen finden Sie unter Konfigurieren von Amazon Kendra für die Verwendung eines Amazon VPC.
- Inklusions- und Ausschlussfilter — Sie können mithilfe von Benutzer-IDs, Gruppen, Quell-URLs, Zeitstempeln und Zeitzonen angeben, ob bestimmte Inhalte eingeschlossen werden sollen.
- Benutzerkontextfilterung und Zugriffskontrolle —Amazon Kendra durchsucht die Zugriffskontrollliste (ACL) für Ihre Dokumente, sofern Sie über eine ACL für Ihre Dokumente verfügen. Die ACL-Informationen werden verwendet, um Suchergebnisse nach dem Benutzer- oder Gruppenzugriff auf Dokumente zu filtern. Weitere Informationen finden Sie unter Benutzerkontextfilterung.
- Feldzuordnungen — Wählen Sie diese Option, um Ihre MySQL Datenquellenfelder Ihren Indexfeldern zuzuordnen. Amazon Kendra Weitere Informationen finden Sie unter Zuweisen von Datenquellenfeldern.

> **Note**
>
> Das Textfeld oder das entsprechende Textfeld für Ihre Dokumente ist erforderlich, um Ihre Dokumente durchsuchen Amazon Kendra zu können. Sie müssen den

Feldnamen Ihres Dokumenthauptteils in Ihrer Datenquelle dem Namen des Indexfeldes zuordnen_document_body. Alle anderen Felder sind optional.

Hinweise

- Gelöschte Datenbankzeilen werden nicht nachverfolgt, wenn nach Amazon Kendra aktualisiertem Inhalt gesucht wird.
- Die Größe von Feldnamen und Werten in einer Zeile Ihrer Datenbank darf 400 KB nicht überschreiten.
- Wenn Ihre Datenbankdatenquelle eine große Datenmenge enthält und Sie nicht Ihren gesamten Datenbankinhalt nach der ersten Synchronisierung indizieren möchten Amazon Kendra , können Sie wählen, ob nur neue, geänderte oder gelöschte Dokumente synchronisiert werden sollen.
- Es hat sich bewährt, nur lesbare Amazon Kendra Datenbankanmeldeinformationen zur Verfügung zu stellen.
- Es hat sich bewährt, das Hinzufügen von Tabellen mit sensiblen Daten oder personenbezogenen Daten (PII) zu vermeiden.

Oracle Database

Oracle Databaseist ein Datenbankverwaltungssystem. Wenn Sie ein Oracle Database Benutzer sind, können Sie Amazon Kendra damit Ihre Oracle Database Datenquelle indizieren. Der Amazon Kendra Oracle Database Datenquellen-Connector unterstützt Oracle Database 18c, 19c und 21c.

Sie können über Amazon Kendra die Amazon Kendra Konsole und die API eine Verbindung zu Ihrer Oracle Database Datenquelle herstellen. TemplateConfiguration

Informationen zur Fehlerbehebung bei Ihrem Amazon Kendra Oracle Database Datenquellen-Connector finden Sie unterProblembehandlung bei Datenquellen.

Themen

- Unterstützte Features
- Voraussetzungen
- Anweisungen zur Verbindung
- Hinweise

Unterstützte Features

- Feldzuordnungen
- Filterung des Benutzerkontextes
- Einschluss-/Ausschlussfilter
- Vollständige und inkrementelle Inhaltssynchronisierung
- Virtual Private Cloud (VPC)

Voraussetzungen

Bevor Sie Ihre Oracle Database Datenquelle Amazon Kendra zum Indizieren verwenden können, nehmen Sie diese Änderungen in Ihren Konten Oracle Database und AWS Konten vor.

Stellen Sie sicherOracle Database, dass Sie Folgendes haben:

- Haben Sie sich Ihren Datenbank-Benutzernamen und Ihr Passwort notiert.

> **Important**
>
> Es hat sich bewährt, nur lesbare Amazon Kendra Datenbankanmeldeinformationen zur Verfügung zu stellen.

- Die URL, der Port und die Instanz Ihres Datenbank-Hosts wurden kopiert.
- Vergewissert, dass jedes Dokument in Oracle Database und zwischen anderen Datenquellen, die Sie für denselben Index verwenden möchten, einzigartig ist. Jede Datenquelle, die Sie für einen Index verwenden möchten, darf nicht dasselbe Dokument in allen Datenquellen enthalten. Dokument-IDs gelten für einen Index global und müssen pro Index eindeutig sein.

Stellen Sie sicher AWS-Konto, dass Sie Folgendes in Ihrem haben:

- Hat einen Amazon Kendra Index erstellt und bei Verwendung der API die Index-ID notiert.
- Sie haben eine IAM Rolle für Ihre Datenquelle erstellt und, falls Sie die API verwenden, den ARN der IAM Rolle notiert.

> **Note**
>
> Wenn Sie Ihren Authentifizierungstyp und Ihre Anmeldeinformationen ändern, müssen Sie Ihre IAM Rolle aktualisieren, um auf die richtige AWS Secrets Manager geheime ID zugreifen zu können.

- Wir haben Ihre Oracle Database Authentifizierungsdaten AWS Secrets Manager geheim gespeichert und, falls Sie die API verwenden, den ARN des Geheimnisses notiert.

> **Note**
>
> Wir empfehlen Ihnen, Ihre Anmeldeinformationen und Ihr Geheimnis regelmäßig zu aktualisieren oder zu wechseln. Stellen Sie zu Ihrer eigenen Sicherheit nur die Zugriffsebene bereit, die erforderlich ist. Wir raten davon ab, Anmeldeinformationen und geheime Daten für alle Datenquellen und Connector-Versionen 1.0 und 2.0 (sofern zutreffend) wiederzuverwenden.

Wenn Sie noch keine IAM Rolle oder keinen Schlüssel haben, können Sie die Konsole verwenden, um eine neue IAM Rolle und ein neues Secrets Manager Geheimnis zu erstellen, wenn Sie Ihre Oracle Database Datenquelle mit verbinden. Amazon Kendra Wenn Sie die API verwenden, müssen Sie den ARN einer vorhandenen IAM Rolle und eines Secrets Manager Geheimnisses sowie eine Index-ID angeben.

Anweisungen zur Verbindung

Um eine Verbindung Amazon Kendra zu Ihrer Oracle Database Datenquelle herzustellen, müssen Sie Details zu Ihren Oracle Database Anmeldeinformationen angeben, damit Sie auf Ihre Daten zugreifen Amazon Kendra können. Falls Sie das noch nicht konfiguriert haben, Amazon Kendra finden Sie Oracle Database weitere Informationen unterVoraussetzungen.

Console

Um eine Verbindung Amazon Kendra herzustellen Oracle Database

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die Amazon Kendra Konsole.

2. Wählen Sie im linken Navigationsbereich Indizes und dann den Index, den Sie verwenden möchten, aus der Indexliste aus.

> **Note**
>
> Sie können Ihre Einstellungen für die Benutzerzugriffskontrolle unter Indexeinstellungen konfigurieren oder bearbeiten.

3. Wählen Sie auf der Seite Erste Schritte die Option Datenquelle hinzufügen aus.
4. Wählen Sie auf der Seite Datenquelle hinzufügen die Option Oracle DatabaseConnector und dann Connector hinzufügen aus.
5. Geben Sie auf der Seite „Datenquellendetails angeben“ die folgenden Informationen ein:

   a. Geben Sie im Feld Name und Beschreibung für Datenquellenname einen Namen für Ihre Datenquelle ein. Sie können Bindestriche, aber keine Leerzeichen verwenden.

   b. (Optional) Beschreibung — Geben Sie eine optionale Beschreibung für Ihre Datenquelle ein.

   c. In Standardsprache — Wählen Sie eine Sprache aus, um Ihre Dokumente nach dem Index zu filtern. Sofern Sie nichts anderes angeben, ist die Standardsprache Englisch. Die in den Metadaten des Dokuments angegebene Sprache hat Vorrang vor der ausgewählten Sprache.

   d. Unter Tags für Neues Tag hinzufügen — Fügen Sie optionale Tags hinzu, um Ihre Ressourcen zu durchsuchen und zu filtern oder Ihre Kosten nachzuverfolgen. AWS

   e. Wählen Sie Weiter aus.
6. Geben Sie auf der Seite Zugriff und Sicherheit definieren die folgenden Informationen ein:

   a. Geben Sie im Feld Quelle die folgenden Informationen ein:

   b. Host — Geben Sie den Datenbank-Hostnamen ein.

   c. Port — Geben Sie den Datenbankport ein.

   d. Instanz — Geben Sie die Datenbankinstanz ein.

   e. Speicherort des SSL-Zertifikats aktivieren — Geben Sie hier den Amazon S3 Pfad zu Ihrer SSL-Zertifikatsdatei ein.

   f. Geben Sie im Feld Authentifizierung die folgenden Informationen ein:

      - AWS Secrets Manager geheim — Wählen Sie ein vorhandenes Geheimnis aus, oder erstellen Sie ein neues Secrets Manager Geheimnis, um Ihre Oracle Database

Authentifizierungsdaten zu speichern. Wenn Sie ein neues Geheimnis erstellen möchten, wird ein AWS Secrets Manager geheimes Fenster geöffnet.

A. Geben Sie die folgenden Informationen in das Fenster Create an AWS Secrets Manager Secret ein:

I. Geheimer Name — Ein Name für Ihr Geheimnis. Das Präfix 'AmazonKendra- Oracle Database -' wird automatisch zu Ihrem geheimen Namen hinzugefügt.

II. Für Datenbankbenutzername und Passwort — Geben Sie die Werte der Authentifizierungsdaten ein, die Sie aus Ihrer Datenbank kopiert haben.

B. Wählen Sie Speichern.

g. Virtual Private Cloud (VPC) — Sie können wählen, ob Sie eine VPC verwenden möchten. In diesem Fall müssen Sie Subnetze und VPC-Sicherheitsgruppen hinzufügen.

h. IAM Rolle — Wählen Sie eine bestehende IAM Rolle oder erstellen Sie eine neue IAM Rolle, um auf Ihre Repository-Anmeldeinformationen und Indexinhalte zuzugreifen.

> **Note**
>
> IAM Rollen, die für Indizes verwendet werden, können nicht für Datenquellen verwendet werden. Wenn Sie sich nicht sicher sind, ob eine vorhandene Rolle für einen Index oder eine häufig gestellte Frage verwendet wird, wählen Sie Neue Rolle erstellen, um Fehler zu vermeiden.

i. Wählen Sie Weiter aus.

7. Geben Sie auf der Seite „Synchronisierungseinstellungen konfigurieren“ die folgenden Informationen ein:

a. Wählen Sie unter Synchronisierungsbereich eine der folgenden Optionen aus:

- SQL-Abfrage — Geben Sie SQL-Abfrageanweisungen wie SELECT- und JOIN-Operationen ein. SQL-Abfragen müssen weniger als 32 KB groß sein. Amazon Kendra durchsucht den gesamten Datenbankinhalt, der Ihrer Abfrage entspricht.
- Primärschlüsselspalte — Geben Sie den Primärschlüssel für die Datenbanktabelle an. Dadurch wird eine Tabelle in Ihrer Datenbank identifiziert.
- Titelspalte — Geben Sie den Namen der Titelspalte des Dokuments in Ihrer Datenbanktabelle an.

- Hauptspalte — Geben Sie den Namen der Hauptspalte des Dokuments in Ihrer Datenbanktabelle an.

b. Wählen Sie unter Zusätzliche Konfiguration — optional aus den folgenden Optionen, um bestimmte Inhalte zu synchronisieren, anstatt alle Dateien zu synchronisieren:

- Spalten zur Erkennung von Änderungen — Geben Sie die Namen der Spalten ein, anhand derer Inhaltsänderungen erkannt Amazon Kendra werden sollen. Amazon Kendra indexiert den Inhalt neu, wenn sich eine dieser Spalten ändert.
- Spalte mit Benutzer-IDs — Geben Sie den Namen der Spalte ein, die Benutzer-IDs enthält, um Zugriff auf Inhalte zu erhalten.
- Spalte „Gruppen“ — Geben Sie den Namen der Spalte ein, die Gruppen enthält, denen der Zugriff auf Inhalte gewährt werden soll.
- Spalte Quell-URLs — Geben Sie den Namen der Spalte ein, die Quell-URLs enthält, die indexiert werden sollen.
- Spalte mit Zeitstempeln — Geben Sie den Namen der Spalte ein, die Zeitstempel enthält. Amazon Kendra verwendet Zeitstempelinformationen, um Änderungen an Ihren Inhalten zu erkennen und nur geänderte Inhalte zu synchronisieren.
- Spalte „Zeitzonen“ — Geben Sie den Namen der Spalte ein, die Zeitzonen für den Inhalt enthält, der gecrawlt werden soll.
- Zeitstempelformat — Geben Sie den Namen der Spalte ein, die Zeitstempelformate enthält, anhand derer Inhaltsänderungen erkannt und Ihre Inhalte erneut synchronisiert werden sollen.

c. Synchronisierungsmodus — Wählen Sie aus, wie Sie Ihren Index aktualisieren möchten, wenn sich der Inhalt Ihrer Datenquelle ändert. Wenn Sie Ihre Datenquelle Amazon Kendra zum ersten Mal synchronisieren, werden alle Inhalte standardmäßig gecrawlt und indexiert. Sie müssen eine vollständige Synchronisierung Ihrer Daten durchführen, falls Ihre erste Synchronisierung fehlgeschlagen ist, auch wenn Sie die Option Vollsynchronisierung nicht als Synchronisierungsmodusoption wählen.

- Vollständige Synchronisierung: Indizieren Sie den gesamten Inhalt neu und ersetzen die vorhandenen Inhalte jedes Mal, wenn Ihre Datenquelle mit Ihrem Index synchronisiert wird.
- Neue, geänderte Synchronisierung: Indizieren Sie jedes Mal, wenn Ihre Datenquelle mit Ihrem Index synchronisiert wird, nur neue und geänderte Inhalte. Amazon Kendra kann den Mechanismus Ihrer Datenquelle verwenden, um Inhaltsänderungen

nachzuverfolgen und Inhalte zu indexieren, die sich seit der letzten Synchronisierung geändert haben.

- Neue, geänderte, gelöschte Synchronisierung: Indizieren Sie bei jeder Synchronisierung Ihrer Datenquelle mit Ihrem Index nur neue, geänderte und gelöschte Inhalte. Amazon Kendra kann den Mechanismus Ihrer Datenquelle verwenden, um Inhaltsänderungen nachzuverfolgen und Inhalte zu indexieren, die sich seit der letzten Synchronisierung geändert haben.

d. Im Synchronisierungslaufplan für Frequenz — Wie oft Amazon Kendra wird mit Ihrer Datenquelle synchronisiert?

e. Wählen Sie Weiter aus.

8. Geben Sie auf der Seite Feldzuordnungen festlegen die folgenden Informationen ein:

a. Wählen Sie aus den generierten Standard-Datenquellenfeldern — Dokument-IDs, Dokumenttitel und Quell-URLs — aus, die Sie dem Index zuordnen möchten. Amazon Kendra

b. Feld hinzufügen — Um benutzerdefinierte Datenquellenfelder hinzuzufügen, um einen Indexfeldnamen für die Zuordnung und den Felddatentyp zu erstellen.

c. Wählen Sie Weiter aus.

9. Überprüfen Sie auf der Seite Überprüfen und erstellen, ob die von Ihnen eingegebenen Informationen korrekt sind, und wählen Sie dann Datenquelle hinzufügen aus. Sie können Ihre Informationen auch auf dieser Seite bearbeiten. Ihre Datenquelle wird auf der Seite Datenquellen angezeigt, nachdem die Datenquelle erfolgreich hinzugefügt wurde.

API

Um eine Verbindung Amazon Kendra herzustellen Oracle Database

Mithilfe der TemplateConfigurationAPI müssen Sie Folgendes angeben:

- Datenquelle — Geben Sie den Datenquellentyp wie `JDBC` bei der Verwendung des TemplateConfigurationJSON-Schemas an. Geben Sie außerdem die Datenquelle so an`TEMPLATE`, wie Sie die CreateDataSourceAPI aufrufen.
- Datenbanktyp — Sie müssen den Datenbanktyp als `oracle` angeben.
- SQL-Abfrage — Geben Sie SQL-Abfrageanweisungen wie SELECT- und JOIN-Operationen an. SQL-Abfragen müssen weniger als 32 KB groß sein. Amazon Kendra durchsucht den gesamten Datenbankinhalt, der Ihrer Abfrage entspricht.

- Synchronisierungsmodus — Geben Sie an, wie Ihr Index aktualisiert Amazon Kendra werden soll, wenn sich der Inhalt Ihrer Datenquelle ändert. Wenn Sie Ihre Datenquelle Amazon Kendra zum ersten Mal synchronisieren, werden alle Inhalte standardmäßig gecrawlt und indexiert. Sie müssen eine vollständige Synchronisierung Ihrer Daten durchführen, falls Ihre erste Synchronisierung fehlgeschlagen ist, auch wenn Sie die Option Vollsynchronisierung nicht als Synchronisierungsmodusoption wählen. Sie können wählen zwischen:
  - `FORCED_FULL_CRAWL`um den gesamten Inhalt neu zu indizieren und vorhandene Inhalte jedes Mal zu ersetzen, wenn Ihre Datenquelle mit Ihrem Index synchronisiert wird.
  - `FULL_CRAWL`um bei jeder Synchronisierung Ihrer Datenquelle mit Ihrem Index nur neue, geänderte und gelöschte Inhalte zu indizieren. Amazon Kendra kann den Mechanismus Ihrer Datenquelle verwenden, um Inhaltsänderungen nachzuverfolgen und Inhalte zu indexieren, die sich seit der letzten Synchronisierung geändert haben.
  - `CHANGE_LOG`um jedes Mal, wenn Ihre Datenquelle mit Ihrem Index synchronisiert wird, nur neue und geänderte Inhalte zu indizieren. Amazon Kendra kann den Mechanismus Ihrer Datenquelle verwenden, um Inhaltsänderungen nachzuverfolgen und Inhalte zu indexieren, die sich seit der letzten Synchronisierung geändert haben.
- Geheimer Amazon-Ressourcenname (ARN) — Geben Sie den Amazon-Ressourcennamen (ARN) eines Secrets Manager Geheimnisses ein, das die Authentifizierungsdaten enthält, die Sie in Ihrem Oracle Database Konto erstellt haben. Das Geheimnis wird in einer JSON-Struktur mit den folgenden Schlüsseln gespeichert:

```
{
    "user name": "database user name",
    "password": "password"
}
```

> **Note**
>
> Wir empfehlen Ihnen, Ihre Anmeldeinformationen und Ihr Geheimnis regelmäßig zu aktualisieren oder zu wechseln. Stellen Sie zu Ihrer eigenen Sicherheit nur die Zugriffsebene bereit, die erforderlich ist. Wir raten davon ab, Anmeldeinformationen und geheime Daten für alle Datenquellen und Connector-Versionen 1.0 und 2.0 (sofern zutreffend) wiederzuverwenden.

- IAM Rolle — Geben Sie an`RoleArn`, wann Sie anrufen`CreateDataSource`, um einer IAM Rolle Berechtigungen für den Zugriff auf Ihr Secrets Manager Geheimnis und für den Aufruf

der erforderlichen öffentlichen APIs für den Oracle Database Connector und zum Aufrufen der erforderlichen öffentlichen APIs zu erteilen. Amazon Kendra Weitere Informationen finden Sie unter IAM Rollen für Oracle Database Datenquellen.

Sie können auch die folgenden optionalen Funktionen hinzufügen:

- Virtual Private Cloud (VPC) — Geben Sie an, `VpcConfiguration` wann Sie anrufen. `CreateDataSource` Weitere Informationen finden Sie unter Konfigurieren von Amazon Kendra für die Verwendung eines Amazon VPC.
- Inklusions- und Ausschlussfilter — Sie können mithilfe von Benutzer-IDs, Gruppen, Quell-URLs, Zeitstempeln und Zeitzonen angeben, ob bestimmte Inhalte eingeschlossen werden sollen.
- Benutzerkontextfilterung und Zugriffskontrolle —Amazon Kendra durchsucht die Zugriffskontrollliste (ACL) für Ihre Dokumente, sofern Sie über eine ACL für Ihre Dokumente verfügen. Die ACL-Informationen werden verwendet, um Suchergebnisse nach dem Benutzer- oder Gruppenzugriff auf Dokumente zu filtern. Weitere Informationen finden Sie unter Benutzerkontextfilterung.
- Feldzuordnungen — Wählen Sie diese Option, um Ihre Oracle Database Datenquellenfelder Ihren Indexfeldern zuzuordnen. Amazon Kendra Weitere Informationen finden Sie unter Zuweisen von Datenquellenfeldern.

> **Note**
>
> Das Textfeld oder das entsprechende Textfeld für Ihre Dokumente ist erforderlich, um Ihre Dokumente durchsuchen Amazon Kendra zu können. Sie müssen den Feldnamen Ihres Dokumenthauptteils in Ihrer Datenquelle dem Namen des Indexfeldes zuordnen`_document_body`. Alle anderen Felder sind optional.

Eine Liste weiterer wichtiger JSON-Schlüssel, die konfiguriert werden müssen, finden Sie unterOracle-Datenbank-Vorlagenschema.

Hinweise

- Gelöschte Datenbankzeilen werden nicht nachverfolgt, wenn nach Amazon Kendra aktualisiertem Inhalt gesucht wird.

- Die Größe von Feldnamen und Werten in einer Zeile Ihrer Datenbank darf 400 KB nicht überschreiten.
- Wenn Ihre Datenbankdatenquelle eine große Datenmenge enthält und Sie nicht möchten Amazon Kendra , dass Ihr gesamter Datenbankinhalt nach der ersten Synchronisierung indexiert wird, können Sie wählen, ob nur neue, geänderte oder gelöschte Dokumente synchronisiert werden sollen.
- Es hat sich bewährt, nur lesbare Amazon Kendra Datenbankanmeldeinformationen zur Verfügung zu stellen.
- Es hat sich bewährt, das Hinzufügen von Tabellen mit sensiblen Daten oder personenbezogenen Daten (PII) zu vermeiden.

PostgreSQL

PostgreSQLList ein Open-Source-Datenbankverwaltungssystem. Wenn Sie ein PostgreSQL Benutzer sind, können Sie es verwenden, Amazon Kendra um Ihre PostgreSQL Datenquelle zu indizieren. Der Amazon Kendra PostgreSQL Datenquellenconnector unterstützt PostgreSQL 9.6.

Sie können über Amazon Kendra die Amazon Kendra Konsole und die API eine Verbindung zu Ihrer PostgreSQL Datenquelle herstellen. TemplateConfiguration

Informationen zur Fehlerbehebung bei Ihrem Amazon Kendra PostgreSQL Datenquellen-Connector finden Sie unterProblembehandlung bei Datenquellen.

Themen

- Unterstützte Features
- Voraussetzungen
- Anweisungen zur Verbindung
- Hinweise

Unterstützte Features

- Feldzuordnungen
- Filterung des Benutzerkontextes
- Einschluss-/Ausschlussfilter
- Vollständige und inkrementelle Inhaltssynchronisierung

- Virtual Private Cloud (VPC)

Voraussetzungen

Bevor Sie Ihre PostgreSQL Datenquelle Amazon Kendra zum Indizieren verwenden können, nehmen Sie diese Änderungen in Ihren Konten PostgreSQL und AWS Konten vor.

Stellen Sie sicherPostgreSQL, dass Sie Folgendes haben:

- Haben Sie sich Ihren Datenbank-Benutzernamen und Ihr Passwort notiert.

> **Important**
>
> Es hat sich bewährt, nur lesbare Amazon Kendra Datenbankanmeldeinformationen zur Verfügung zu stellen.

- Die URL, der Port und die Instanz Ihres Datenbank-Hosts wurden kopiert.
- Vergewissert, dass jedes Dokument in PostgreSQL und zwischen anderen Datenquellen, die Sie für denselben Index verwenden möchten, einzigartig ist. Jede Datenquelle, die Sie für einen Index verwenden möchten, darf nicht dasselbe Dokument in allen Datenquellen enthalten. Dokument-IDs gelten für einen Index global und müssen pro Index eindeutig sein.

Stellen Sie sicher AWS-Konto, dass Sie Folgendes in Ihrem haben:

- Hat einen Amazon Kendra Index erstellt und bei Verwendung der API die Index-ID notiert.
- Sie haben eine IAM Rolle für Ihre Datenquelle erstellt und, falls Sie die API verwenden, den ARN der IAM Rolle notiert.

> **Note**
>
> Wenn Sie Ihren Authentifizierungstyp und Ihre Anmeldeinformationen ändern, müssen Sie Ihre IAM Rolle aktualisieren, um auf die richtige AWS Secrets Manager geheime ID zugreifen zu können.

- Wir haben Ihre PostgreSQL Authentifizierungsdaten AWS Secrets Manager geheim gespeichert und, falls Sie die API verwenden, den ARN des Geheimnisses notiert.

> **Note**
>
> Wir empfehlen Ihnen, Ihre Anmeldeinformationen und Ihr Geheimnis regelmäßig zu aktualisieren oder zu wechseln. Stellen Sie zu Ihrer eigenen Sicherheit nur die Zugriffsebene bereit, die erforderlich ist. Wir raten davon ab, Anmeldeinformationen und geheime Daten für alle Datenquellen und Connector-Versionen 1.0 und 2.0 (sofern zutreffend) wiederzuverwenden.

Wenn Sie noch keine IAM Rolle oder keinen Schlüssel haben, können Sie die Konsole verwenden, um eine neue IAM Rolle und ein neues Secrets Manager Geheimnis zu erstellen, wenn Sie Ihre PostgreSQL Datenquelle mit verbinden. Amazon Kendra Wenn Sie die API verwenden, müssen Sie den ARN einer vorhandenen IAM Rolle und eines Secrets Manager Geheimnisses sowie eine Index-ID angeben.

Anweisungen zur Verbindung

Um eine Verbindung Amazon Kendra zu Ihrer PostgreSQL Datenquelle herzustellen, müssen Sie Details zu Ihren PostgreSQL Anmeldeinformationen angeben, damit Sie auf Ihre Daten zugreifen Amazon Kendra können. Falls Sie das noch nicht konfiguriert haben, Amazon Kendra finden Sie PostgreSQL weitere Informationen unterVoraussetzungen.

Console

Um eine Verbindung Amazon Kendra herzustellen PostgreSQL

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die Amazon Kendra Konsole.
2. Wählen Sie im linken Navigationsbereich Indizes und dann den Index, den Sie verwenden möchten, aus der Indexliste aus.

   > **Note**
   >
   > Sie können Ihre Einstellungen für die Benutzerzugriffskontrolle unter Indexeinstellungen konfigurieren oder bearbeiten.

3. Wählen Sie auf der Seite Erste Schritte die Option Datenquelle hinzufügen aus.

4. Wählen Sie auf der Seite Datenquelle hinzufügen die Option PostgreSQLConnector und dann Connector hinzufügen aus.
5. Geben Sie auf der Seite „Datenquellendetails angeben“ die folgenden Informationen ein:
    a. Geben Sie im Feld Name und Beschreibung für Datenquellenname einen Namen für Ihre Datenquelle ein. Sie können Bindestriche, aber keine Leerzeichen verwenden.
    b. (Optional) Beschreibung — Geben Sie eine optionale Beschreibung für Ihre Datenquelle ein.
    c. In Standardsprache — Wählen Sie eine Sprache aus, um Ihre Dokumente nach dem Index zu filtern. Sofern Sie nichts anderes angeben, ist die Standardsprache Englisch. Die in den Metadaten des Dokuments angegebene Sprache hat Vorrang vor der ausgewählten Sprache.
    d. Unter Tags für Neues Tag hinzufügen — Fügen Sie optionale Tags hinzu, um Ihre Ressourcen zu durchsuchen und zu filtern oder Ihre Kosten nachzuverfolgen. AWS
    e. Wählen Sie Weiter aus.
6. Geben Sie auf der Seite Zugriff und Sicherheit definieren die folgenden Informationen ein:
    a. Geben Sie im Feld Quelle die folgenden Informationen ein:
    b. Host — Geben Sie den Datenbank-Hostnamen ein.
    c. Port — Geben Sie den Datenbankport ein.
    d. Instanz — Geben Sie die Datenbankinstanz ein.
    e. Speicherort des SSL-Zertifikats aktivieren — Geben Sie hier den Amazon S3 Pfad zu Ihrer SSL-Zertifikatsdatei ein.
    f. Geben Sie im Feld Authentifizierung die folgenden Informationen ein:
        - AWS Secrets Manager geheim — Wählen Sie ein vorhandenes Geheimnis aus, oder erstellen Sie ein neues Secrets Manager Geheimnis, um Ihre PostgreSQL Authentifizierungsdaten zu speichern. Wenn Sie ein neues Geheimnis erstellen möchten, wird ein AWS Secrets Manager geheimes Fenster geöffnet.
            A. Geben Sie die folgenden Informationen in das Fenster Create an AWS Secrets Manager Secret ein:
                I. Geheimer Name — Ein Name für Ihr Geheimnis. Das Präfix 'AmazonKendra- PostgreSQL -' wird automatisch zu Ihrem geheimen Namen hinzugefügt.

II. Für Datenbankbenutzername und Passwort — Geben Sie die Werte der Authentifizierungsdaten ein, die Sie aus Ihrer Datenbank kopiert haben.

B. Wählen Sie Speichern.

g. Virtual Private Cloud (VPC) — Sie können wählen, ob Sie eine VPC verwenden möchten. In diesem Fall müssen Sie Subnetze und VPC-Sicherheitsgruppen hinzufügen.

h. IAM Rolle — Wählen Sie eine bestehende IAM Rolle oder erstellen Sie eine neue IAM Rolle, um auf Ihre Repository-Anmeldeinformationen und Indexinhalte zuzugreifen.

> **Note**
>
> IAM Rollen, die für Indizes verwendet werden, können nicht für Datenquellen verwendet werden. Wenn Sie sich nicht sicher sind, ob eine vorhandene Rolle für einen Index oder eine häufig gestellte Frage verwendet wird, wählen Sie Neue Rolle erstellen, um Fehler zu vermeiden.

i. Wählen Sie Weiter aus.

7. Geben Sie auf der Seite „Synchronisierungseinstellungen konfigurieren“ die folgenden Informationen ein:

a. Wählen Sie unter Synchronisierungsbereich eine der folgenden Optionen aus:

- SQL-Abfrage — Geben Sie SQL-Abfrageanweisungen wie SELECT- und JOIN-Operationen ein. SQL-Abfragen müssen weniger als 32 KB groß sein. Amazon Kendra durchsucht den gesamten Datenbankinhalt, der Ihrer Abfrage entspricht.
- Primärschlüsselspalte — Geben Sie den Primärschlüssel für die Datenbanktabelle an. Dadurch wird eine Tabelle in Ihrer Datenbank identifiziert.
- Titelspalte — Geben Sie den Namen der Titelspalte des Dokuments in Ihrer Datenbanktabelle an.
- Hauptspalte — Geben Sie den Namen der Hauptspalte des Dokuments in Ihrer Datenbanktabelle an.

b. Wählen Sie unter Zusätzliche Konfiguration — optional aus den folgenden Optionen, um bestimmte Inhalte zu synchronisieren, anstatt alle Dateien zu synchronisieren:

- Spalten zur Erkennung von Änderungen — Geben Sie die Namen der Spalten ein, anhand derer Inhaltsänderungen erkannt Amazon Kendra werden sollen. Amazon Kendra indexiert den Inhalt neu, wenn sich eine dieser Spalten ändert.

- Spalte mit Benutzer-IDs — Geben Sie den Namen der Spalte ein, die Benutzer-IDs enthält, um Zugriff auf Inhalte zu erhalten.
- Spalte „Gruppen“ — Geben Sie den Namen der Spalte ein, die Gruppen enthält, denen der Zugriff auf Inhalte gewährt werden soll.
- Spalte Quell-URLs — Geben Sie den Namen der Spalte ein, die Quell-URLs enthält, die indexiert werden sollen.
- Spalte mit Zeitstempeln — Geben Sie den Namen der Spalte ein, die Zeitstempel enthält. Amazon Kendra verwendet Zeitstempelinformationen, um Änderungen an Ihren Inhalten zu erkennen und nur geänderte Inhalte zu synchronisieren.
- Spalte „Zeitzonen“ — Geben Sie den Namen der Spalte ein, die Zeitzonen für den Inhalt enthält, der gecrawlt werden soll.
- Zeitstempelformat — Geben Sie den Namen der Spalte ein, die Zeitstempelformate enthält, anhand derer Inhaltsänderungen erkannt und Ihre Inhalte erneut synchronisiert werden sollen.

c. Synchronisierungsmodus — Wählen Sie aus, wie Sie Ihren Index aktualisieren möchten, wenn sich der Inhalt Ihrer Datenquelle ändert. Wenn Sie Ihre Datenquelle Amazon Kendra zum ersten Mal synchronisieren, werden alle Inhalte standardmäßig gecrawlt und indexiert. Sie müssen eine vollständige Synchronisierung Ihrer Daten durchführen, falls Ihre erste Synchronisierung fehlgeschlagen ist, auch wenn Sie die Option Vollsynchronisierung nicht als Synchronisierungsmodusoption wählen.

   - Vollständige Synchronisierung: Indizieren Sie den gesamten Inhalt neu und ersetzen die vorhandenen Inhalte jedes Mal, wenn Ihre Datenquelle mit Ihrem Index synchronisiert wird.
   - Neue, geänderte Synchronisierung: Indizieren Sie jedes Mal, wenn Ihre Datenquelle mit Ihrem Index synchronisiert wird, nur neue und geänderte Inhalte. Amazon Kendra kann den Mechanismus Ihrer Datenquelle verwenden, um Inhaltsänderungen nachzuverfolgen und Inhalte zu indexieren, die sich seit der letzten Synchronisierung geändert haben.
   - Neue, geänderte, gelöschte Synchronisierung: Indizieren Sie bei jeder Synchronisierung Ihrer Datenquelle mit Ihrem Index nur neue, geänderte und gelöschte Inhalte. Amazon Kendra kann den Mechanismus Ihrer Datenquelle verwenden, um Inhaltsänderungen nachzuverfolgen und Inhalte zu indexieren, die sich seit der letzten Synchronisierung geändert haben.

d. Im Synchronisierungslaufplan für Frequenz — Wie oft Amazon Kendra wird mit Ihrer Datenquelle synchronisiert?

e. Wählen Sie Weiter aus.

8. Geben Sie auf der Seite Feldzuordnungen festlegen die folgenden Informationen ein:

a. Wählen Sie aus den generierten Standard-Datenquellenfeldern — Dokument-IDs, Dokumenttitel und Quell-URLs — aus, die Sie dem Index zuordnen möchten. Amazon Kendra

b. Feld hinzufügen — Um benutzerdefinierte Datenquellenfelder hinzuzufügen, um einen Indexfeldnamen für die Zuordnung und den Felddatentyp zu erstellen.

c. Wählen Sie Weiter aus.

9. Überprüfen Sie auf der Seite Überprüfen und erstellen, ob die von Ihnen eingegebenen Informationen korrekt sind, und wählen Sie dann Datenquelle hinzufügen aus. Sie können Ihre Informationen auch auf dieser Seite bearbeiten. Ihre Datenquelle wird auf der Seite Datenquellen angezeigt, nachdem die Datenquelle erfolgreich hinzugefügt wurde.

API

Um eine Verbindung Amazon Kendra herzustellen PostgreSQL

Mithilfe der TemplateConfigurationAPI müssen Sie Folgendes angeben:

- Datenquelle — Geben Sie den Datenquellentyp wie `JDBC` bei der Verwendung des TemplateConfigurationJSON-Schemas an. Geben Sie außerdem die Datenquelle so an`TEMPLATE`, wie Sie die CreateDataSourceAPI aufrufen.
- Datenbanktyp — Sie müssen den Datenbanktyp als `postgresql` angeben.
- SQL-Abfrage — Geben Sie SQL-Abfrageanweisungen wie SELECT- und JOIN-Operationen an. SQL-Abfragen müssen weniger als 32 KB groß sein. Amazon Kendra durchsucht den gesamten Datenbankinhalt, der Ihrer Abfrage entspricht.
- Synchronisierungsmodus — Geben Sie an, wie Ihr Index aktualisiert Amazon Kendra werden soll, wenn sich der Inhalt Ihrer Datenquelle ändert. Wenn Sie Ihre Datenquelle Amazon Kendra zum ersten Mal synchronisieren, werden alle Inhalte standardmäßig gecrawlt und indexiert. Sie müssen eine vollständige Synchronisierung Ihrer Daten durchführen, falls Ihre erste Synchronisierung fehlgeschlagen ist, auch wenn Sie die Option Vollsynchronisierung nicht als Synchronisierungsmodusoption wählen. Sie können wählen zwischen:

  - `FORCED_FULL_CRAWL`um den gesamten Inhalt neu zu indizieren und vorhandene Inhalte jedes Mal zu ersetzen, wenn Ihre Datenquelle mit Ihrem Index synchronisiert wird.
  - `FULL_CRAWL`um bei jeder Synchronisierung Ihrer Datenquelle mit Ihrem Index nur neue, geänderte und gelöschte Inhalte zu indizieren. Amazon Kendra kann den Mechanismus Ihrer Datenquelle verwenden, um Inhaltsänderungen nachzuverfolgen und Inhalte zu indexieren, die sich seit der letzten Synchronisierung geändert haben.
  - `CHANGE_LOG`um jedes Mal, wenn Ihre Datenquelle mit Ihrem Index synchronisiert wird, nur neue und geänderte Inhalte zu indizieren. Amazon Kendra kann den Mechanismus Ihrer Datenquelle verwenden, um Inhaltsänderungen nachzuverfolgen und Inhalte zu indexieren, die sich seit der letzten Synchronisierung geändert haben.
- Geheimer Amazon-Ressourcenname (ARN) — Geben Sie den Amazon-Ressourcennamen (ARN) eines Secrets Manager Geheimnisses ein, das die Authentifizierungsdaten enthält, die Sie in Ihrem PostgreSQL Konto erstellt haben. Das Geheimnis wird in einer JSON-Struktur mit den folgenden Schlüsseln gespeichert:

```
{
    "user name": "database user name",
    "password": "password"
}
```

> **Note**
>
> Wir empfehlen Ihnen, Ihre Anmeldeinformationen und Ihr Geheimnis regelmäßig zu aktualisieren oder zu wechseln. Stellen Sie zu Ihrer eigenen Sicherheit nur die Zugriffsebene bereit, die erforderlich ist. Wir raten davon ab, Anmeldeinformationen und geheime Daten für alle Datenquellen und Connector-Versionen 1.0 und 2.0 (sofern zutreffend) wiederzuverwenden.

- IAM Rolle — Geben Sie an`RoleArn`, wann Sie anrufen`CreateDataSource`, um einer IAM Rolle Berechtigungen für den Zugriff auf Ihr Secrets Manager Geheimnis und für den Aufruf der erforderlichen öffentlichen APIs für den PostgreSQL Connector und zum Aufrufen der erforderlichen öffentlichen APIs zu erteilen. Amazon Kendra Weitere Informationen finden Sie unter IAM Rollen für PostgreSQL Datenquellen.

Sie können auch die folgenden optionalen Funktionen hinzufügen:

- Virtual Private Cloud (VPC) — Geben Sie an, `VpcConfiguration` wann Sie anrufen. `CreateDataSource` Weitere Informationen finden Sie unter Konfigurieren von Amazon Kendra für die Verwendung eines Amazon VPC.
- Inklusions- und Ausschlussfilter — Sie können mithilfe von Benutzer-IDs, Gruppen, Quell-URLs, Zeitstempeln und Zeitzonen angeben, ob bestimmte Inhalte eingeschlossen werden sollen.
- Benutzerkontextfilterung und Zugriffskontrolle —Amazon Kendra durchsucht die Zugriffskontrollliste (ACL) für Ihre Dokumente, sofern Sie über eine ACL für Ihre Dokumente verfügen. Die ACL-Informationen werden verwendet, um Suchergebnisse nach dem Benutzer- oder Gruppenzugriff auf Dokumente zu filtern. Weitere Informationen finden Sie unter Benutzerkontextfilterung.
- Feldzuordnungen — Wählen Sie diese Option, um Ihre PostgreSQL Datenquellenfelder Ihren Indexfeldern zuzuordnen. Amazon Kendra Weitere Informationen finden Sie unter Zuweisen von Datenquellenfeldern.

> **Note**
>
> Das Textfeld oder das entsprechende Textfeld für Ihre Dokumente ist erforderlich, um Ihre Dokumente durchsuchen Amazon Kendra zu können. Sie müssen den Feldnamen Ihres Dokumenthauptteils in Ihrer Datenquelle dem Namen des Indexfeldes zuordnen`_document_body`. Alle anderen Felder sind optional.

Eine Liste weiterer wichtiger JSON-Schlüssel, die konfiguriert werden müssen, finden Sie unterPostgreSQL-Vorlagenschema.

Hinweise

- Gelöschte Datenbankzeilen werden nicht nachverfolgt, wenn nach Amazon Kendra aktualisiertem Inhalt gesucht wird.
- Die Größe von Feldnamen und Werten in einer Zeile Ihrer Datenbank darf 400 KB nicht überschreiten.
- Wenn Ihre Datenbankdatenquelle eine große Datenmenge enthält und Sie nicht möchten Amazon Kendra , dass Ihr gesamter Datenbankinhalt nach der ersten Synchronisierung indexiert wird, können Sie wählen, ob nur neue, geänderte oder gelöschte Dokumente synchronisiert werden sollen.

- Es hat sich bewährt, nur lesbare Amazon Kendra Datenbankanmeldeinformationen zur Verfügung zu stellen.
- Es hat sich bewährt, das Hinzufügen von Tabellen mit sensiblen Daten oder personenbezogenen Daten (PII) zu vermeiden.

Quip

Quip ist eine kollaborative Produktivitätssoftware, die Funktionen zur Erstellung von Dokumenten in Echtzeit bietet. Sie können sie verwenden Amazon Kendra , um Ihre Quip-Ordner, Dateien, Dateikommentare, Chatrooms und Anlagen zu indizieren.

Sie können über Amazon Kendra die Amazon Kendra Konsole und die API eine Verbindung zu Ihrer Quip-Datenquelle herstellen. QuipConfiguration

Informationen zur Fehlerbehebung bei Ihrem Amazon Kendra Quip-Datenquellen-Connector finden Sie unter. Problembehandlung bei Datenquellen

Themen

Unterstützte Features

Amazon Kendra Der Quip-Datenquellenconnector unterstützt die folgenden Funktionen:

- Feldzuordnungen
- Filterung des Benutzerkontextes
- Einschluss-/Ausschlussfilter
- Virtual Private Cloud (VPC)

Voraussetzungen

Bevor Sie Ihre Quip-Datenquelle Amazon Kendra zum Indizieren verwenden können, nehmen Sie diese Änderungen in Ihrem Quip und Ihren Konten vor. AWS

Stellen Sie in Quip sicher, dass Sie über Folgendes verfügen:

- Ein Quip-Konto mit Administratorrechten.
- Es wurden Quip-Authentifizierungsdaten erstellt, die ein persönliches Zugriffstoken enthalten. Weitere Informationen finden Sie in der Quip-Dokumentation zur Authentifizierung.
- Ihre Quip-Site-Domain wurde kopiert. Zum Beispiel *`https://quip-company.quipdomain.com/browse`*, wobei *`quipdomain die Domain`* ist.
- Vergewissert, dass jedes Dokument in Quip und in anderen Datenquellen, die Sie für denselben Index verwenden möchten, einzigartig ist. Jede Datenquelle, die Sie für einen Index verwenden möchten, darf nicht dasselbe Dokument in allen Datenquellen enthalten. Dokument-IDs gelten für einen Index global und müssen pro Index eindeutig sein.

Stellen Sie sicher AWS-Konto, dass Sie Folgendes in Ihrem haben:

- Hat einen Amazon Kendra Index erstellt und bei Verwendung der API die Index-ID notiert.
- Sie haben eine IAM Rolle für Ihre Datenquelle erstellt und, falls Sie die API verwenden, den ARN der IAM Rolle notiert.

> **Note**
>
> Wenn Sie Ihren Authentifizierungstyp und Ihre Anmeldeinformationen ändern, müssen Sie Ihre IAM Rolle aktualisieren, um auf die richtige AWS Secrets Manager geheime ID zugreifen zu können.

- Wir haben Ihre Quip-Authentifizierungsdaten AWS Secrets Manager geheim gespeichert und, falls Sie die API verwenden, den ARN des Geheimnisses notiert.

> **Note**
>
> Wir empfehlen Ihnen, Ihre Anmeldeinformationen und Ihr Geheimnis regelmäßig zu aktualisieren oder zu wechseln. Stellen Sie zu Ihrer eigenen Sicherheit nur die Zugriffsebene bereit, die erforderlich ist. Wir raten davon ab, Anmeldeinformationen und geheime Daten für alle Datenquellen und Connector-Versionen 1.0 und 2.0 (sofern zutreffend) wiederzuverwenden.

Wenn Sie noch keine IAM Rolle oder keinen Schlüssel haben, können Sie die Konsole verwenden, um eine neue IAM Rolle und ein neues Secrets Manager Geheimnis zu erstellen, wenn Sie Ihre Quip-Datenquelle mit verbinden. Amazon Kendra Wenn Sie die API verwenden, müssen Sie den ARN einer vorhandenen IAM Rolle und eines Secrets Manager Geheimnisses sowie eine Index-ID angeben.

Anweisungen zur Verbindung

Um eine Verbindung Amazon Kendra zu Ihrer Quip-Datenquelle herzustellen, müssen Sie die erforderlichen Details zu Ihrer Quip-Datenquelle angeben, damit Sie auf Ihre Daten zugreifen Amazon Kendra können. Wenn Sie Quip für Amazon Kendra noch nicht konfiguriert haben, finden Sie weitere Informationen unter. Voraussetzungen

Console

So stellen Sie eine Verbindung Amazon Kendra zu Quip her

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die Amazon Kendra Konsole.
2. Wählen Sie im linken Navigationsbereich Indizes und dann den Index, den Sie verwenden möchten, aus der Indexliste aus.

   > **Note**
   >
   > Sie können Ihre Einstellungen für die Benutzerzugriffskontrolle unter Indexeinstellungen konfigurieren oder bearbeiten.

3. Wählen Sie auf der Seite Erste Schritte die Option Datenquelle hinzufügen aus.
4. Wählen Sie auf der Seite Datenquelle hinzufügen die Option Quip-Connector und dann Connector hinzufügen aus.
5. Geben Sie auf der Seite „Datenquellendetails angeben“ die folgenden Informationen ein:

   a. Geben Sie im Feld Name und Beschreibung für Datenquellenname einen Namen für Ihre Datenquelle ein. Sie können Bindestriche, aber keine Leerzeichen verwenden.

   b. (Optional) Beschreibung — Geben Sie eine optionale Beschreibung für Ihre Datenquelle ein.

   c. In Standardsprache — Wählen Sie eine Sprache aus, um Ihre Dokumente nach dem Index zu filtern. Sofern Sie nichts anderes angeben, ist die Standardsprache Englisch.

Die in den Metadaten des Dokuments angegebene Sprache hat Vorrang vor der ausgewählten Sprache.

d. Unter Tags für Neues Tag hinzufügen — Fügen Sie optionale Tags hinzu, um Ihre Ressourcen zu durchsuchen und zu filtern oder Ihre Kosten nachzuverfolgen. AWS

e. Wählen Sie Weiter aus.

6. Geben Sie auf der Seite Zugriff und Sicherheit definieren die folgenden Informationen ein:

a. Quip-Domainname — Geben Sie den Quip ein, den Sie aus Ihrem Quip-Konto kopiert haben.

b. AWS Secrets Manager geheim — Wählen Sie ein vorhandenes Geheimnis oder erstellen Sie ein neues Secrets Manager Geheimnis, um Ihre Quip-Authentifizierungsdaten zu speichern. Wenn Sie sich dafür entscheiden, ein neues Geheimnis zu erstellen, wird ein AWS Secrets Manager geheimes Fenster geöffnet.

i. Geben Sie die folgenden Informationen in das Fenster Create an AWS Secrets Manager Secret ein:

A. Geheimer Name — Ein Name für Ihr Geheimnis. Das Präfix 'AmazonKendra-Quip-' wird Ihrem geheimen Namen automatisch hinzugefügt.

B. Quip-Token — Geben Sie das persönliche Quip-Zugriffstoken ein, das Sie in Ihrem Quip-Konto erstellt haben.

ii. Wählen Sie Speichern.

c. Virtual Private Cloud (VPC) — Sie können wählen, ob Sie eine VPC verwenden möchten. In diesem Fall müssen Sie Subnetze und VPC-Sicherheitsgruppen hinzufügen.

d. IAM Rolle — Wählen Sie eine bestehende IAM Rolle oder erstellen Sie eine neue IAM Rolle, um auf Ihre Repository-Anmeldeinformationen und Indexinhalte zuzugreifen.

> **Note**
>
> IAM Rollen, die für Indizes verwendet werden, können nicht für Datenquellen verwendet werden. Wenn Sie sich nicht sicher sind, ob eine vorhandene Rolle für einen Index oder eine häufig gestellte Frage verwendet wird, wählen Sie Neue Rolle erstellen, um Fehler zu vermeiden.

e. Wählen Sie Weiter aus.

7. Geben Sie auf der Seite „Synchronisierungseinstellungen konfigurieren“ die folgenden Informationen ein:

   a. Quip-Ordner-IDs zum Crawlen hinzufügen — Die Quip-Ordner-IDs, die Sie crawlen möchten.

   > **Note**
   >
   > Um einen Stammordner einschließlich aller darin enthaltenen Unterordner und Dokumente zu crawlen, geben Sie die Stammordner-ID ein. Um bestimmte Unterordner zu crawlen, fügen Sie die spezifischen Unterordner-IDs hinzu.

   b. Zusätzliche Konfiguration (Inhaltstypen) — Geben Sie die Inhaltstypen ein, die Sie crawlen möchten.

   c. Regex-Muster — Reguläre Ausdrucksmuster zum Ein- oder Ausschließen bestimmter Dateien. Sie können bis zu 100 Muster hinzufügen.

   d. Wählen Sie im Synchronisierungslaufplan für Frequenz aus, wie oft Amazon Kendra mit Ihrer Datenquelle synchronisiert.

   e. Wählen Sie Weiter aus.

8. Geben Sie auf der Seite Feldzuordnungen festlegen die folgenden Informationen ein:

   a. Wählen Sie aus den generierten Standard-Datenquellenfeldern aus, die Sie dem Index zuordnen möchten Amazon Kendra .

   b. Feld hinzufügen — Um benutzerdefinierte Datenquellenfelder hinzuzufügen, um einen Indexfeldnamen für die Zuordnung und den Felddatentyp zu erstellen.

   c. Wählen Sie Weiter aus.

9. Überprüfen Sie auf der Seite Überprüfen und erstellen, ob die von Ihnen eingegebenen Informationen korrekt sind, und wählen Sie dann Datenquelle hinzufügen aus. Sie können Ihre Informationen auch auf dieser Seite bearbeiten. Ihre Datenquelle wird auf der Seite Datenquellen angezeigt, nachdem die Datenquelle erfolgreich hinzugefügt wurde.

API

Um eine Verbindung Amazon Kendra zu Quip herzustellen

Mithilfe der QuipConfiguration API müssen Sie Folgendes angeben:

- Quip-Site-Domain — Zum Beispiel *`https://quip-company.quipdomain.com/browse`*, wobei *`quipdomain die Domain`* ist.
- Geheimer Amazon-Ressourcenname (ARN) — Geben Sie den Amazon-Ressourcennamen (ARN) eines Secrets Manager Geheimnisses ein, das die Authentifizierungsdaten für Ihr Quip-Konto enthält. Das Geheimnis wird in einer JSON-Struktur mit den folgenden Schlüsseln gespeichert:

```
{
    "accessToken": "token"
}
```

> **Note**
>
> Wir empfehlen Ihnen, Ihre Anmeldeinformationen und Ihr Geheimnis regelmäßig zu aktualisieren oder zu wechseln. Stellen Sie zu Ihrer eigenen Sicherheit nur die Zugriffsebene bereit, die erforderlich ist. Wir raten davon ab, Anmeldeinformationen und geheime Daten für alle Datenquellen und Connector-Versionen 1.0 und 2.0 (sofern zutreffend) wiederzuverwenden.

- IAM Rolle — Geben Sie an`RoleArn`, wann Sie anrufen`CreateDataSource`, um einer IAM Rolle Berechtigungen für den Zugriff auf Ihr Secrets Manager Geheimnis und den Aufruf der erforderlichen öffentlichen APIs für den Quip-Connector und zum Aufrufen der erforderlichen öffentlichen APIs zu erteilen. Amazon Kendra Weitere Informationen finden Sie unter IAM Rollen für Quip-Datenquellen.

Sie können auch die folgenden optionalen Funktionen hinzufügen:

- Virtual Private Cloud (VPC) — Geben Sie dies `VpcConfiguration` als Teil der Datenquellenkonfiguration an. Siehe Konfiguration Amazon Kendra für die Verwendung einer VPC.
- Inklusions- und Ausschlussfilter — Geben Sie an, ob bestimmte Dateien ein- oder ausgeschlossen werden sollen.

> **Note**
>
> Die meisten Datenquellen verwenden Muster mit regulären Ausdrücken, bei denen es sich um Ein- oder Ausschlussmuster handelt, die als Filter bezeichnet werden.

Wenn Sie einen Einschlussfilter angeben, werden nur Inhalte indexiert, die dem Einschlussfilter entsprechen. Jedes Dokument, das nicht dem Einschlussfilter entspricht, wird nicht indexiert. Wenn Sie einen Ein- und Ausschlussfilter angeben, werden Dokumente, die dem Ausschlussfilter entsprechen, nicht indexiert, auch wenn sie dem Einschlussfilter entsprechen.

- Ordner — Geben Sie die Quip-Ordner und Unterordner an, die Sie indizieren möchten

> **Note**
>
> Um einen Stammordner einschließlich aller darin enthaltenen Unterordner und Dokumente zu crawlen, geben Sie die Stammordner-ID ein. Um bestimmte Unterordner zu crawlen, fügen Sie die spezifischen Unterordner-IDs hinzu.

- Anlagen, Chatrooms, Dateikommentare — Wählen Sie aus, ob das Crawlen von Anhängen, Chatroom-Inhalten und Dateikommentaren eingeschlossen werden soll.
- Feldzuordnungen — Wählen Sie diese Option, um Ihre Quip-Datenquellenfelder Ihren Indexfeldern zuzuordnen. Amazon Kendra Weitere Informationen finden Sie unter Zuweisen von Datenquellenfeldern.

> **Note**
>
> Das Textfeld oder das entsprechende Textfeld für Ihre Dokumente ist erforderlich, um Ihre Dokumente durchsuchen Amazon Kendra zu können. Sie müssen den Feldnamen Ihres Dokumenthauptteils in Ihrer Datenquelle dem Namen des Indexfeldes zuordnen`_document_body`. Alle anderen Felder sind optional.

- Benutzerkontextfilterung und ZugriffskontrolleAmazon Kendra — durchsucht die Zugriffskontrollliste (ACL) für Ihre Dokumente, sofern Sie über eine ACL für Ihre Dokumente verfügen. Die ACL-Informationen werden verwendet, um Suchergebnisse nach dem Benutzer- oder Gruppenzugriff auf Dokumente zu filtern. Weitere Informationen finden Sie unter Benutzerkontextfilterung.

Weitere Informationen

Weitere Informationen zur Integration Amazon Kendra mit Ihrer Quip-Datenquelle finden Sie unter:

- Suchen Sie mithilfe der intelligenten Suche mithilfe des Quip-Konnektors nach Wissen in Quip-Dokumenten für Amazon Kendra

Salesforce

Salesforce ist ein Tool für das Kundenbeziehungsmanagement (CRM) zur Verwaltung von Support-, Vertriebs- und Marketingteams. Sie können Amazon Kendra damit Ihre Salesforce-Standardobjekte und sogar benutzerdefinierte Objekte indizieren.

Sie können entweder über Amazon Kendra die Amazon Kendra Konsole, die API oder die TemplateConfigurationAPI eine Verbindung zu Ihrer Salesforce-Datenquelle herstellen. SalesforceConfiguration

Amazon Kendra hat zwei Versionen des Salesforce-Connectors. Zu den unterstützten Funktionen jeder Version gehören:

Salesforce-Konnektor V1.0//API SalesforceConfiguration

- Feldzuordnungen
- Filterung des Benutzerkontextes
- Einschluss-/Ausschlussfilter

Salesforce-Konnektor V2.0//API TemplateConfiguration

- Feldzuordnungen
- Filterung des Benutzerkontextes
- Crawling der Benutzeridentität
- Einschluss-/Ausschlussfilter
- Vollständige und inkrementelle Inhaltssynchronisierung
- Crawlen von Entitätsanhängen
- Virtual Private Cloud (VPC)

> **Note**
>
> Die Support für Salesforce Connector SalesforceConfiguration V1.0/API wird voraussichtlich 2023 enden. Wir empfehlen, zu Salesforce Connector V2.0/ API zu migrieren oder diese zu verwenden. TemplateConfiguration

Informationen zur Fehlerbehebung bei Ihrem Amazon Kendra Salesforce-Datenquellen-Connector finden Sie unter. Problembehandlung bei Datenquellen

Themen

Salesforce-Konnektor V1.0

Salesforce ist ein Tool für das Kundenbeziehungsmanagement (CRM) zur Verwaltung von Support-, Vertriebs- und Marketingteams. Sie können Amazon Kendra damit Ihre Salesforce-Standardobjekte und sogar benutzerdefinierte Objekte indizieren.

> **Important**
>
> Amazon Kendra verwendet die Salesforce-API-Version 48. Die Salesforce-API begrenzt die Anzahl der Anfragen, die Sie pro Tag stellen können. Wenn Salesforce diese Anfragen überschreitet, versucht es erneut, bis es fortfahren kann.

> **Note**
>
> Die Support für Salesforce Connector SalesforceConfiguration V1.0/API wird voraussichtlich 2023 enden. Wir empfehlen, zu Salesforce Connector V2.0/ API zu migrieren oder diese zu verwenden. TemplateConfiguration

Informationen zur Fehlerbehebung bei Ihrem Amazon Kendra Salesforce-Datenquellen-Connector finden Sie unter. Problembehandlung bei Datenquellen

Themen

Unterstützte Features

Amazon Kendra Der Salesforce-Datenquellen-Connector unterstützt die folgenden Funktionen:

- Feldzuordnungen
- Filterung des Benutzerkontextes
- Einschluss-/Ausschlussfilter

Voraussetzungen

Bevor Sie Ihre Salesforce-Datenquelle Amazon Kendra zum Indizieren verwenden können, nehmen Sie diese Änderungen in Ihrem Salesforce und Ihren Accounts vor. AWS

Stellen Sie in Salesforce sicher, dass Sie über Folgendes verfügen:

- Sie haben ein Salesforce-Konto erstellt und den Benutzernamen und das Passwort notiert, die Sie für die Verbindung mit Salesforce verwenden.
- Sie haben ein Salesforce Connected App-Konto mit aktiviertem OAuth erstellt und den Verbraucherschlüssel (Client-ID) und das Verbrauchergeheimnis (Kundengeheimnis) kopiert, die Ihrer Salesforce Connected-Anwendung zugewiesen sind. Weitere Informationen finden Sie in der Salesforce-Dokumentation zu Connected Apps.
- Das Salesforce-Sicherheitstoken wurde kopiert, das dem Konto zugeordnet ist, das für die Verbindung mit Salesforce verwendet wurde.
- Die URL der Salesforce-Instanz, die Sie indexieren möchten, wurde kopiert. In der Regel ist dies *`https://.salesforce.com/.`* <company> Auf dem Server muss eine mit Salesforce verbundene Anwendung ausgeführt werden.
- Ihrem Salesforce-Server wurden Anmeldeinformationen für einen Benutzer mit Lesezugriff auf Salesforce hinzugefügt, indem Sie das ReadOnly Profil geklont und anschließend die Berechtigungen „Alle Daten anzeigen“ und „Artikel verwalten“ hinzugefügt haben. Diese Anmeldeinformationen identifizieren den Benutzer, der die Verbindung herstellt, und die verbundene Salesforce-Anwendung, Amazon Kendra mit der eine Verbindung hergestellt wird.

- Aktiviert, dass jedes Dokument in Salesforce und in anderen Datenquellen, die Sie für denselben Index verwenden möchten, einzigartig ist. Jede Datenquelle, die Sie für einen Index verwenden möchten, darf nicht dasselbe Dokument in allen Datenquellen enthalten. Dokument-IDs gelten für einen Index global und müssen pro Index eindeutig sein.

Stellen Sie sicher AWS-Konto, dass Sie Folgendes in Ihrem haben:

- Hat einen Amazon Kendra Index erstellt und bei Verwendung der API die Index-ID notiert.
- Sie haben eine IAM Rolle für Ihre Datenquelle erstellt und, falls Sie die API verwenden, den ARN der IAM Rolle notiert.

> **Note**
>
> Wenn Sie Ihren Authentifizierungstyp und Ihre Anmeldeinformationen ändern, müssen Sie Ihre IAM Rolle aktualisieren, um auf die richtige AWS Secrets Manager geheime ID zugreifen zu können.

- Sie haben Ihre Salesforce-Authentifizierungsdaten AWS Secrets Manager geheim gespeichert und, falls Sie die API verwenden, den ARN des Geheimnisses notiert.

> **Note**
>
> Wir empfehlen Ihnen, Ihre Anmeldeinformationen und Ihr Geheimnis regelmäßig zu aktualisieren oder zu wechseln. Stellen Sie zu Ihrer eigenen Sicherheit nur die Zugriffsebene bereit, die erforderlich ist. Wir raten davon ab, Anmeldeinformationen und geheime Daten für alle Datenquellen und Connector-Versionen 1.0 und 2.0 (sofern zutreffend) wiederzuverwenden.

Wenn Sie noch keine IAM Rolle oder keinen Schlüssel haben, können Sie die Konsole verwenden, um eine neue IAM Rolle und ein neues Secrets Manager Geheimnis zu erstellen, wenn Sie Ihre Salesforce-Datenquelle mit verbinden. Amazon Kendra Wenn Sie die API verwenden, müssen Sie den ARN einer vorhandenen IAM Rolle und eines Secrets Manager Geheimnisses sowie eine Index-ID angeben.

Anweisungen zur Verbindung

Um eine Verbindung Amazon Kendra zu Ihrer Salesforce-Datenquelle herzustellen, müssen Sie die erforderlichen Details zu Ihrer Salesforce-Datenquelle angeben, damit Sie auf Ihre Daten zugreifen Amazon Kendra können. Falls Sie Salesforce noch nicht konfiguriert haben, Amazon Kendra sehen Sie nachVoraussetzungen.

Console

Um eine Verbindung Amazon Kendra zu Salesforce herzustellen

1. Melden Sie sich bei der AWS Management Console an und öffnen Sie die Amazon Kendra Konsole.
2. Wählen Sie im linken Navigationsbereich Indizes und dann den Index, den Sie verwenden möchten, aus der Indexliste aus.

   > **Note**
   >
   > Sie können Ihre Einstellungen für die Benutzerzugriffskontrolle unter Indexeinstellungen konfigurieren oder bearbeiten.

3. Wählen Sie auf der Seite Erste Schritte die Option Datenquelle hinzufügen aus.
4. Wählen Sie auf der Seite Datenquelle hinzufügen die Option Salesforce Connector V1.0 und dann Connector hinzufügen aus.
5. Geben Sie auf der Seite „Datenquellendetails angeben“ die folgenden Informationen ein:

   a. Datenquellenname — Geben Sie einen Namen für Ihre Datenquelle ein. Sie können Bindestriche, aber keine Leerzeichen verwenden.

   b. (Optional) Beschreibung — Geben Sie eine optionale Beschreibung für Ihre Datenquelle ein.

   c. Standardsprache — Eine Sprache, um Ihre Dokumente nach dem Index zu filtern. Sofern Sie nichts anderes angeben, ist die Standardsprache Englisch. Die in den Metadaten angegebene Sprache hat Vorrang vor der ausgewählten Sprache.

   d. Neues Tag hinzufügen — Stichwörter, mit denen du deine Ressourcen durchsuchen und filtern oder deine gemeinsamen Kosten verfolgen kannst.

   e. Wählen Sie Weiter aus.

6. Geben Sie auf der Seite „Zugriff und Sicherheit definieren“ die folgenden Informationen ein:

a. Salesforce-URL — Geben Sie die Instanz-URL für die Salesforce-Site ein, die Sie indexieren möchten.

b. Wählen Sie unter Authentifizierungstyp zwischen „Bestehend“ und „Neu“, um Ihre Salesforce-Authentifizierungsdaten zu speichern. Wenn Sie ein neues Geheimnis erstellen möchten, wird ein AWS Secrets Manager geheimes Fenster geöffnet.

- Geben Sie die folgenden Informationen in das Fenster Create an AWS Secrets Manager Secret ein:

A. Geheimer Name — Ein Name für Ihr Geheimnis. Das Präfix 'AmazonKendra-Salesforce-' wird Ihrem geheimen Namen automatisch hinzugefügt.

B. Geben Sie für Benutzername, Passwort, Sicherheitstoken, Verbraucherschlüssel, Verbrauchergeheimnis und Authentifizierungs-URL die Werte für die Authentifizierungsdaten ein, die Sie in Ihrem Salesforce-Konto erstellt haben.

C. Wählen Sie Authentifizierung speichern aus.

c. IAM Rolle — Wählen Sie eine bestehende IAM Rolle oder erstellen Sie eine neue IAM Rolle, um auf Ihre Repository-Anmeldeinformationen und Indexinhalte zuzugreifen.

> **Note**
>
> IAM Rollen, die für Indizes verwendet werden, können nicht für Datenquellen verwendet werden. Wenn Sie sich nicht sicher sind, ob eine vorhandene Rolle für einen Index oder eine häufig gestellte Frage verwendet wird, wählen Sie Neue Rolle erstellen, um Fehler zu vermeiden.

d. Wählen Sie Weiter aus.

7. Geben Sie auf der Seite „Synchronisierungseinstellungen konfigurieren“ die folgenden Informationen ein:

a. Für Crawl-Anlagen — Wählen Sie diese Option, um alle angehängten Objekte, Artikel und Feeds zu crawlen.

b. Wählen Sie für Standardobjekte, Knowledge-Artikel und Chatter-Feeds die Salesforce-Entitäten oder Inhaltstypen aus, die Sie crawlen möchten.

> **Note**
>
> Sie müssen Konfigurationsinformationen für die Indizierung mindestens eines der Standardobjekte, Wissensartikel oder Chatter-Feeds angeben. Wenn Sie Knowledge-Artikel crawlen möchten, müssen Sie die Typen von Wissensartikeln, die indexiert werden sollen, den Namen der Artikel angeben und angeben, ob die Standardfelder aller Wissensartikel oder nur die Felder eines benutzerdefinierten Artikeltyps indexiert werden sollen. Wenn Sie benutzerdefinierte Artikel indizieren möchten, müssen Sie den internen Namen des Artikeltyps angeben. Sie können bis zu 10 Artikeltypen angeben.

c. Häufigkeit — Wie oft Amazon Kendra wird mit Ihrer Datenquelle synchronisiert.

d. Wählen Sie Weiter aus.

8. Geben Sie auf der Seite Feldzuordnungen festlegen die folgenden Informationen ein:

a. Für den Artikel Standardwissen, Standardobjektanhänge und Zusätzliche vorgeschlagene Feldzuordnungen — Wählen Sie eines der Amazon Kendra generierten Standard-Datenquellenfelder aus, die Sie Ihrem Index zuordnen möchten.

> **Note**
>
> Eine Indexzuordnung zu `_document_body` ist erforderlich. Sie können die Zuordnung zwischen dem `Salesforce ID` Feld und dem Amazon Kendra `_document_id` Feld nicht ändern.

b. Feld hinzufügen — Um benutzerdefinierte Datenquellenfelder hinzuzufügen, um einen Indexfeldnamen für die Zuordnung und den Felddatentyp zu erstellen.

c. Wählen Sie Weiter aus.

9. Überprüfen Sie auf der Seite Überprüfen und erstellen, ob die von Ihnen eingegebenen Informationen korrekt sind, und wählen Sie dann Datenquelle hinzufügen aus. Sie können Ihre Informationen auch auf dieser Seite bearbeiten. Ihre Datenquelle wird auf der Seite Datenquellen angezeigt, nachdem die Datenquelle erfolgreich hinzugefügt wurde.

API

Um eine Verbindung Amazon Kendra zu Salesforce herzustellen

Sie müssen die folgende SalesforceConfigurationAPI angeben:

- Server-URL — Die Instanz-URL für die Salesforce-Site, die Sie indizieren möchten.
- Geheimer Amazon-Ressourcenname (ARN) — Geben Sie den Amazon-Ressourcennamen (ARN) eines Secrets Manager Geheimnisses ein, das die Authentifizierungsdaten für Ihr Salesforce-Konto enthält. Das Geheimnis wird in einer JSON-Struktur mit den folgenden Schlüsseln gespeichert:

```
{
    "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**
>
> Wir empfehlen Ihnen, Ihre Anmeldeinformationen und Ihr Geheimnis regelmäßig zu aktualisieren oder zu wechseln. Stellen Sie zu Ihrer eigenen Sicherheit nur die Zugriffsebene bereit, die erforderlich ist. Wir raten davon ab, Anmeldeinformationen und geheime Daten für alle Datenquellen und Connector-Versionen 1.0 und 2.0 (sofern zutreffend) wiederzuverwenden.

- IAM Rolle — Geben Sie an`RoleArn`, wann Sie anrufen`CreateDataSource`, um einer IAM Rolle Berechtigungen für den Zugriff auf Ihr Secrets Manager Geheimnis und den Aufruf der erforderlichen öffentlichen APIs für den Salesforce-Connector und zu erteilen. Amazon Kendra Weitere Informationen finden Sie unter IAM Rollen für Salesforce-Datenquellen.
- Sie müssen Konfigurationsinformationen für die Indizierung mindestens eines der Standardobjekte, Wissensartikel oder Chatter-Feeds bereitstellen.

- Standardobjekte — Wenn Sie Standardobjekte crawlen möchten, müssen Sie den Namen des Standardobjekts und den Namen des Felds in der Standardobjekttabelle angeben, das den Dokumentinhalt enthält.
- Knowledge-Artikel — Wenn Sie Knowledge-Artikel crawlen möchten, müssen Sie die Typen der zu indizierenden Wissensartikel, den Status der zu indizierenden Wissensartikel und angeben, ob die Standardfelder aller Wissensartikel oder nur die Felder eines benutzerdefinierten Artikeltyps indexiert werden sollen.
- Chatter-Feeds — Wenn Sie Chatter-Feeds crawlen möchten, müssen Sie den Namen der Spalte in der FeedItem Salesforce-Tabelle angeben, die den zu indizierenden Inhalt enthält.

Sie können auch die folgenden optionalen Funktionen hinzufügen:

- Inklusions- und Ausschlussfilter — Geben Sie an, ob bestimmte Dateianhänge ein- oder ausgeschlossen werden sollen.

  > **Note**
  >
  > Die meisten Datenquellen verwenden Muster für reguläre Ausdrücke, bei denen es sich um Ein- oder Ausschlussmuster handelt, die als Filter bezeichnet werden. Wenn Sie einen Einschlussfilter angeben, werden nur Inhalte indexiert, die dem Einschlussfilter entsprechen. Jedes Dokument, das nicht dem Einschlussfilter entspricht, wird nicht indexiert. Wenn Sie einen Ein- und Ausschlussfilter angeben, werden Dokumente, die dem Ausschlussfilter entsprechen, nicht indexiert, auch wenn sie dem Einschlussfilter entsprechen.

- Feldzuordnungen — Ordnen Sie Ihre Salesforce-Datenquellenfelder Ihren Indexfeldern zu. Amazon Kendra Weitere Informationen finden Sie unter Zuweisen von Datenquellenfeldern.

  > **Note**
  >
  > Das Textfeld oder das entsprechende Textfeld für Ihre Dokumente ist erforderlich, um Ihre Dokumente durchsuchen Amazon Kendra zu können. Sie müssen den Feldnamen Ihres Dokumenthauptteils in Ihrer Datenquelle dem Namen des Indexfeldes zuordnen`_document_body`. Alle anderen Felder sind optional.

- Benutzerkontextfilterung und ZugriffskontrolleAmazon Kendra — durchsucht die Zugriffskontrollliste (ACL) für Ihre Dokumente, sofern Sie über eine ACL für Ihre Dokumente

verfügen. Die ACL-Informationen werden verwendet, um Suchergebnisse nach dem Benutzer- oder Gruppenzugriff auf Dokumente zu filtern. Weitere Informationen finden Sie unter Benutzerkontextfilterung.

Salesforce-Konnektor V2.0

Salesforce ist ein Tool für das Kundenbeziehungsmanagement (CRM) zur Verwaltung von Support-, Vertriebs- und Marketingteams. Sie können Amazon Kendra damit Ihre Salesforce-Standardobjekte und sogar benutzerdefinierte Objekte indizieren.

Der Amazon Kendra Salesforce-Datenquellen-Connector unterstützt die folgenden Salesforce-Editionen: Developer Edition und Enterprise Edition.

> **Note**
>
> Die Support für Salesforce Connector SalesforceConfiguration V1.0/API wird voraussichtlich 2023 enden. Wir empfehlen, zu Salesforce Connector V2.0/ API zu migrieren oder diese zu verwenden. TemplateConfiguration

Informationen zur Fehlerbehebung bei Ihrem Amazon Kendra Salesforce-Datenquellen-Connector finden Sie unter. Problembehandlung bei Datenquellen

Themen

- Unterstützte Features
- Voraussetzungen
- Anweisungen zur Verbindung
- Weitere Informationen

Unterstützte Features

Amazon Kendra Der Salesforce-Datenquellen-Connector unterstützt die folgenden Funktionen:

- Feldzuordnungen
- Filterung des Benutzerkontextes
- Crawling der Benutzeridentität

- Einschluss-/Ausschlussfilter
- Vollständige und inkrementelle Inhaltssynchronisierung
- Crawlen von Entitätsanhängen
- Virtual Private Cloud (VPC)

Voraussetzungen

Bevor Sie Ihre Salesforce-Datenquelle Amazon Kendra zum Indizieren verwenden können, nehmen Sie diese Änderungen in Ihrem Salesforce und Ihren AWS Accounts vor.

Stellen Sie in Salesforce sicher, dass Sie über Folgendes verfügen:

- Sie haben ein Salesforce-Administratorkonto erstellt und sich den Benutzernamen und das Passwort notiert, die Sie für die Verbindung mit Salesforce verwenden.
- Das Salesforce-Sicherheitstoken wurde kopiert, das dem Konto zugeordnet ist, das für die Verbindung mit Salesforce verwendet wurde.
- Sie haben ein Salesforce Connected App-Konto mit aktiviertem OAuth erstellt und den Verbraucherschlüssel (Client-ID) und das Verbrauchergeheimnis (Kundengeheimnis) kopiert, die Ihrer Salesforce Connected-Anwendung zugewiesen sind. Weitere Informationen finden Sie in der Salesforce-Dokumentation zu Connected Apps.
- Die URL der Salesforce-Instanz, die Sie indizieren möchten, wurde kopiert. In der Regel ist dies *https://.salesforce.com/.* <company> Auf dem Server muss eine mit Salesforce verbundene Anwendung ausgeführt werden.
- Ihrem Salesforce-Server wurden Anmeldeinformationen für einen Benutzer mit Lesezugriff auf Salesforce hinzugefügt, indem Sie das ReadOnly Profil geklont und anschließend die Berechtigungen „Alle Daten anzeigen“ und „Artikel verwalten“ hinzugefügt haben. Diese Anmeldeinformationen identifizieren den Benutzer, der die Verbindung herstellt, und die verbundene Salesforce-Anwendung, Amazon Kendra mit der eine Verbindung hergestellt wird.
- Aktiviert, dass jedes Dokument in Salesforce und in anderen Datenquellen, die Sie für denselben Index verwenden möchten, einzigartig ist. Jede Datenquelle, die Sie für einen Index verwenden möchten, darf nicht dasselbe Dokument in allen Datenquellen enthalten. Dokument-IDs gelten für einen Index global und müssen pro Index eindeutig sein.

Stellen Sie sicher AWS-Konto, dass Sie Folgendes in Ihrem haben:

- Hat einen Amazon Kendra Index erstellt und bei Verwendung der API die Index-ID notiert.

- Sie haben eine IAM Rolle für Ihre Datenquelle erstellt und, falls Sie die API verwenden, den ARN der IAM Rolle notiert.

> **Note**
>
> Wenn Sie Ihren Authentifizierungstyp und Ihre Anmeldeinformationen ändern, müssen Sie Ihre IAM Rolle aktualisieren, um auf die richtige AWS Secrets Manager geheime ID zugreifen zu können.

- Sie haben Ihre Salesforce-Authentifizierungsdaten AWS Secrets Manager geheim gespeichert und, falls Sie die API verwenden, den ARN des Geheimnisses notiert.

> **Note**
>
> Wir empfehlen Ihnen, Ihre Anmeldeinformationen und Ihr Geheimnis regelmäßig zu aktualisieren oder zu wechseln. Stellen Sie zu Ihrer eigenen Sicherheit nur die Zugriffsebene bereit, die erforderlich ist. Wir raten davon ab, Anmeldeinformationen und geheime Daten für alle Datenquellen und Connector-Versionen 1.0 und 2.0 (sofern zutreffend) wiederzuverwenden.

Wenn Sie noch keine IAM Rolle oder keinen Schlüssel haben, können Sie die Konsole verwenden, um eine neue IAM Rolle und ein neues Secrets Manager Geheimnis zu erstellen, wenn Sie Ihre Salesforce-Datenquelle mit verbinden. Amazon Kendra Wenn Sie die API verwenden, müssen Sie den ARN einer vorhandenen IAM Rolle und eines Secrets Manager Geheimnisses sowie eine Index-ID angeben.

Anweisungen zur Verbindung

Um eine Verbindung Amazon Kendra zu Ihrer Salesforce-Datenquelle herzustellen, müssen Sie die erforderlichen Details zu Ihrer Salesforce-Datenquelle angeben, damit Sie auf Ihre Daten zugreifen Amazon Kendra können. Falls Sie Salesforce noch nicht konfiguriert haben, Amazon Kendra sehen Sie nachVoraussetzungen.

Console

So stellen Sie eine Verbindung Amazon Kendra zu Salesforce her:

1. Melden Sie sich bei der AWS Management Console an und öffnen Sie die Amazon Kendra Konsole.
2. Wählen Sie im linken Navigationsbereich Indizes und dann den Index, den Sie verwenden möchten, aus der Indexliste aus.

> **Note**
>
> Sie können Ihre Einstellungen für die Benutzerzugriffskontrolle unter Indexeinstellungen konfigurieren oder bearbeiten.

3. Wählen Sie auf der Seite Erste Schritte die Option Datenquelle hinzufügen aus.
4. Wählen Sie auf der Seite Datenquelle hinzufügen die Option Salesforce Connector V2.0 und dann Connector hinzufügen aus.
5. Geben Sie auf der Seite „Datenquellendetails angeben“ die folgenden Informationen ein:
   a. Datenquellenname — Geben Sie einen Namen für Ihre Datenquelle ein. Sie können Bindestriche, aber keine Leerzeichen verwenden.
   b. (Optional) Beschreibung — Geben Sie eine optionale Beschreibung für Ihre Datenquelle ein.
   c. Standardsprache — Eine Sprache, um Ihre Dokumente nach dem Index zu filtern. Sofern Sie nichts anderes angeben, ist die Standardsprache Englisch. Die in den Metadaten angegebene Sprache hat Vorrang vor der ausgewählten Sprache.
   d. Wählen Sie Weiter aus.
6. Geben Sie auf der Seite Zugriff und Sicherheit definieren die folgenden Informationen ein:
   a. Salesforce-URL — Geben Sie die Instanz-URL für die Salesforce-Site ein, die Sie indexieren möchten.
   b. Autorisierung — Aktivieren oder deaktivieren Sie die Informationen der Zugriffskontrollliste (ACL) für Ihre Dokumente, wenn Sie über eine ACL verfügen und diese für die Zugriffskontrolle verwenden möchten. Die ACL gibt an, auf welche Dokumente Benutzer und Gruppen zugreifen können. Die ACL-Informationen werden verwendet, um Suchergebnisse nach dem Benutzer- oder Gruppenzugriff auf Dokumente zu filtern. Weitere Informationen finden Sie unter Benutzerkontextfilterung.
   c. Geben Sie ein vorhandenes Geheimnis ein, oder wenn Sie ein neues Geheimnis erstellen, wird ein AWS Secrets Manager geheimes Fenster geöffnet.

- Authentifizierung — Geben Sie die folgenden Informationen in das Fenster AWS Secrets Manager Geheimes Konto erstellen ein:

  A. Geheimer Name — Ein Name für Ihr Geheimnis. Das Präfix 'AmazonKendra-Salesforce-' wird Ihrem geheimen Namen automatisch hinzugefügt.

  B. Geben Sie für Benutzername, Passwort, Sicherheitstoken, Verbraucherschlüssel, Verbrauchergeheimnis und Authentifizierungs-URL die Werte für die Authentifizierungsdaten ein, die Sie generiert und von Ihrem Salesforce-Konto heruntergeladen haben.

  C. Wählen Sie Authentifizierung speichern aus.

d. Virtual Private Cloud (VPC) — Sie können wählen, ob Sie eine VPC verwenden möchten. In diesem Fall müssen Sie Subnetze und VPC-Sicherheitsgruppen hinzufügen.

e. Identity Crawler — Geben Sie an, ob der Identity Crawler aktiviert Amazon Kendra werden soll. Der Identity Crawler verwendet die Informationen der Zugriffskontrollliste (ACL) für Ihre Dokumente, um Suchergebnisse nach dem Benutzer- oder Gruppenzugriff auf Dokumente zu filtern. Wenn Sie über eine ACL für Ihre Dokumente verfügen und Ihre ACL verwenden möchten, können Sie auch den Identity Crawler aktivieren, um die Benutzerkontextfilterung der Suchergebnisse zu konfigurieren. Amazon Kendra Andernfalls können alle Dokumente öffentlich durchsucht werden, wenn Identity Crawler ausgeschaltet ist. Wenn Sie die Zugriffskontrolle für Ihre Dokumente verwenden möchten und Identity Crawler ausgeschaltet ist, können Sie alternativ die PutPrincipalMappingAPI verwenden, um Benutzer- und Gruppenzugriffsinformationen für die Benutzerkontextfilterung hochzuladen.

f. IAM Rolle — Wählen Sie eine bestehende IAM Rolle oder erstellen Sie eine neue IAM Rolle, um auf Ihre Repository-Anmeldeinformationen und Indexinhalte zuzugreifen.

> **Note**
>
> IAM Rollen, die für Indizes verwendet werden, können nicht für Datenquellen verwendet werden. Wenn Sie sich nicht sicher sind, ob eine vorhandene Rolle für einen Index oder eine häufig gestellte Frage verwendet wird, wählen Sie Neue Rolle erstellen, um Fehler zu vermeiden.

g. Wählen Sie Weiter aus.

7. Geben Sie auf der Seite „Synchronisierungseinstellungen konfigurieren“ die folgenden Informationen ein:

   a. Für Crawl-Anlagen — Wählen Sie diese Option, um alle angehängten Salesforce-Objekte zu crawlen.

   b. Für Standardobjekte, Standardobjekte mit Anlagen und Standardobjekte ohne Anlage und Knowledge-Artikel: Wählen Sie Salesforce-Entitäten oder Inhaltstypen aus, die Sie crawlen möchten.

   c. Sie müssen Konfigurationsinformationen für die Indizierung mindestens eines der Standardobjekte, Wissensartikel oder Chatter-Feeds angeben. Wenn Sie Knowledge-Artikel crawlen möchten, müssen Sie die Typen von Wissensartikeln angeben, die indexiert werden sollen. Sie können zwischen veröffentlichten, archivierten, Entwürfen und Anhängen wählen.

      Regex-Filter — Geben Sie ein Regex-Muster an, um bestimmte Katalogelemente einzubeziehen.

8. Für zusätzliche Konfigurationen:

   - ACL-Informationen Alle Zugriffskontrolllisten sind standardmäßig enthalten. Wenn Sie die Auswahl einer Zugriffskontrollliste aufheben, werden alle Dateien in dieser Kategorie öffentlich zugänglich gemacht.
   - Regex-Muster — Fügen Sie Muster für reguläre Ausdrücke hinzu, um bestimmte Dateien ein- oder auszuschließen. Sie können bis zu 100 Muster hinzufügen.

   Synchronisierungsmodus — Wählen Sie aus, wie Sie Ihren Index aktualisieren möchten, wenn sich der Inhalt Ihrer Datenquelle ändert. Wenn Sie Ihre Datenquelle Amazon Kendra zum ersten Mal synchronisieren, werden alle Inhalte standardmäßig gecrawlt und indexiert. Sie müssen eine vollständige Synchronisierung Ihrer Daten durchführen, falls Ihre erste Synchronisierung fehlgeschlagen ist, auch wenn Sie die Option Vollsynchronisierung nicht als Synchronisierungsmodusoption wählen.

   - Vollständige Synchronisierung: Indizieren Sie den gesamten Inhalt neu und ersetzen die vorhandenen Inhalte jedes Mal, wenn Ihre Datenquelle mit Ihrem Index synchronisiert wird.
   - Neue, geänderte Synchronisierung: Indizieren Sie jedes Mal, wenn Ihre Datenquelle mit Ihrem Index synchronisiert wird, nur neue und geänderte Inhalte. Amazon Kendra kann den

Mechanismus Ihrer Datenquelle verwenden, um Inhaltsänderungen nachzuverfolgen und Inhalte zu indexieren, die sich seit der letzten Synchronisierung geändert haben.

- Neue, geänderte, gelöschte Synchronisierung: Indizieren Sie bei jeder Synchronisierung Ihrer Datenquelle mit Ihrem Index nur neue, geänderte und gelöschte Inhalte. Amazon Kendra kann den Mechanismus Ihrer Datenquelle verwenden, um Inhaltsänderungen nachzuverfolgen und Inhalte zu indexieren, die sich seit der letzten Synchronisierung geändert haben.

9. Wählen Sie Weiter aus.
10. Geben Sie auf der Seite Feldzuordnungen festlegen die folgenden Informationen ein:

    a. Für den Artikel Standardwissen, Standardobjektanhänge und Zusätzliche vorgeschlagene Feldzuordnungen — Wählen Sie eines der Amazon Kendra generierten Standard-Datenquellenfelder aus, die Sie Ihrem Index zuordnen möchten.

    > **Note**
    >
    > Eine Indexzuordnung zu `_document_body` ist erforderlich. Sie können die Zuordnung zwischen dem `Salesforce ID` Feld und dem Amazon Kendra `_document_id` Feld nicht ändern. Sie können jedes Salesforce-Feld dem Dokumenttitel oder dem Dokumenttext zuordnen. Die reservierten/standardmäßigen Indexfelder von Amazon Kendra.

    b. Feld hinzufügen — Um benutzerdefinierte Datenquellenfelder hinzuzufügen, um einen Indexfeldnamen für die Zuordnung und den Felddatentyp zu erstellen.

    c. Wählen Sie Weiter aus.

11. Überprüfen Sie auf der Seite Überprüfen und erstellen, ob die von Ihnen eingegebenen Informationen korrekt sind, und wählen Sie dann Datenquelle hinzufügen aus. Sie können Ihre Informationen auch auf dieser Seite bearbeiten. Ihre Datenquelle wird auf der Seite Datenquellen angezeigt, nachdem die Datenquelle erfolgreich hinzugefügt wurde.

API

Um eine Verbindung Amazon Kendra zu Salesforce herzustellen

Sie müssen mithilfe der TemplateConfigurationAPI ein JSON des Datenquellenschemas angeben. Sie müssen die folgenden Informationen angeben:

- Datenquelle — Geben Sie den Datenquellentyp wie `SALESFORCEV2` bei der Verwendung des TemplateConfigurationJSON-Schemas an. Geben Sie außerdem die Datenquelle so an`TEMPLATE`, wie Sie die CreateDataSourceAPI aufrufen.
- Host-URL — Geben Sie die Host-URL der Salesforce-Instanz an.
- Synchronisierungsmodus — Geben Sie an, wie Ihr Index aktualisiert Amazon Kendra werden soll, wenn sich der Inhalt Ihrer Datenquelle ändert. Wenn Sie Ihre Datenquelle Amazon Kendra zum ersten Mal synchronisieren, werden alle Inhalte standardmäßig gecrawlt und indexiert. Sie müssen eine vollständige Synchronisierung Ihrer Daten durchführen, falls Ihre erste Synchronisierung fehlgeschlagen ist, auch wenn Sie die Option Vollsynchronisierung nicht als Synchronisierungsmodusoption wählen. Sie können wählen zwischen:
  - `FORCED_FULL_CRAWL`um den gesamten Inhalt neu zu indizieren und vorhandene Inhalte jedes Mal zu ersetzen, wenn Ihre Datenquelle mit Ihrem Index synchronisiert wird.
  - `FULL_CRAWL`um bei jeder Synchronisierung Ihrer Datenquelle mit Ihrem Index nur neue, geänderte und gelöschte Inhalte zu indizieren. Amazon Kendra kann den Mechanismus Ihrer Datenquelle verwenden, um Inhaltsänderungen nachzuverfolgen und Inhalte zu indexieren, die sich seit der letzten Synchronisierung geändert haben.
  - `CHANGE_LOG`um jedes Mal, wenn Ihre Datenquelle mit Ihrem Index synchronisiert wird, nur neue und geänderte Inhalte zu indizieren. Amazon Kendra kann den Mechanismus Ihrer Datenquelle verwenden, um Inhaltsänderungen nachzuverfolgen und Inhalte zu indexieren, die sich seit der letzten Synchronisierung geändert haben.
- Geheimer Amazon-Ressourcenname (ARN) — Geben Sie den Amazon-Ressourcennamen (ARN) eines Secrets Manager Geheimnisses ein, das die Authentifizierungsdaten für Ihr Salesforce-Konto enthält. Das Geheimnis wird in einer JSON-Struktur mit den folgenden Schlüsseln gespeichert:

```
{
    "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**
>
> Wir empfehlen Ihnen, Ihre Anmeldeinformationen und Ihr Geheimnis regelmäßig zu aktualisieren oder zu wechseln. Stellen Sie zu Ihrer eigenen Sicherheit nur die Zugriffsebene bereit, die erforderlich ist. Wir raten davon ab, Anmeldeinformationen und geheime Daten für alle Datenquellen und Connector-Versionen 1.0 und 2.0 (sofern zutreffend) wiederzuverwenden.

- IAM Rolle — Geben Sie an`RoleArn`, wann Sie anrufen`CreateDataSource`, um einer IAM Rolle Berechtigungen für den Zugriff auf Ihr Secrets Manager Geheimnis und den Aufruf der erforderlichen öffentlichen APIs für den Salesforce-Connector und zu erteilen. Amazon Kendra Weitere Informationen finden Sie unter IAM Rollen für Salesforce-Datenquellen.

Sie können auch die folgenden optionalen Funktionen hinzufügen:

- Virtual Private Cloud (VPC) — Geben Sie an, `VpcConfiguration` wann Sie anrufen. `CreateDataSource` Weitere Informationen finden Sie unter Konfigurieren von Amazon Kendra für die Verwendung eines Amazon VPC.
- Inklusions- und Ausschlussfilter — Sie können angeben, ob bestimmte Dokumente, Konten, Kampagnen, Kundenvorgänge, Kontakte, Leads, Opportunities, Lösungen, Aufgaben, Gruppen, Chatter und benutzerdefinierte Entitätsdateien ein- oder ausgeschlossen werden sollen.

  > **Note**
  >
  > Die meisten Datenquellen verwenden Muster mit regulären Ausdrücken. Dabei handelt es sich um Ein- oder Ausschlussmuster, die als Filter bezeichnet werden. Wenn Sie einen Einschlussfilter angeben, werden nur Inhalte indexiert, die dem Einschlussfilter entsprechen. Jedes Dokument, das nicht dem Einschlussfilter entspricht, wird nicht indexiert. Wenn Sie einen Ein- und Ausschlussfilter angeben, werden Dokumente, die dem Ausschlussfilter entsprechen, nicht indexiert, auch wenn sie dem Einschlussfilter entsprechen.

- Identity Crawler — Geben Sie an, ob der Identity Crawler aktiviert Amazon Kendra werden soll. Der Identity Crawler verwendet die Informationen der Zugriffskontrollliste (ACL) für Ihre Dokumente, um Suchergebnisse nach dem Benutzer- oder Gruppenzugriff auf Dokumente

zu filtern. Wenn Sie über eine ACL für Ihre Dokumente verfügen und Ihre ACL verwenden möchten, können Sie auch den Identity Crawler aktivieren, um die Benutzerkontextfilterung der Suchergebnisse zu konfigurieren. Amazon Kendra Andernfalls können alle Dokumente öffentlich durchsucht werden, wenn Identity Crawler ausgeschaltet ist. Wenn Sie die Zugriffskontrolle für Ihre Dokumente verwenden möchten und Identity Crawler ausgeschaltet ist, können Sie alternativ die PutPrincipalMappingAPI verwenden, um Benutzer- und Gruppenzugriffsinformationen für die Benutzerkontextfilterung hochzuladen.

- Feldzuordnungen — Wählen Sie, ob Sie Ihre Salesforce-Datenquellenfelder Ihren Indexfeldern zuordnen möchten. Amazon Kendra Weitere Informationen finden Sie unter Zuweisen von Datenquellenfeldern.

  > **Note**
  >
  > Das Textfeld oder das entsprechende Textfeld für Ihre Dokumente ist erforderlich, um Ihre Dokumente durchsuchen Amazon Kendra zu können. Sie müssen den Feldnamen Ihres Dokumenthauptteils in Ihrer Datenquelle dem Namen des Indexfeldes zuordnen`_document_body`. Alle anderen Felder sind optional.

Eine Liste weiterer wichtiger JSON-Schlüssel, die konfiguriert werden müssen, finden Sie unterSalesforce-Vorlagenschema.

Weitere Informationen

Weitere Informationen zur Integration Amazon Kendra mit Ihrer Salesforce-Datenquelle finden Sie unter:

- Ankündigung des aktualisierten Salesforce-Connectors (V2) für Amazon Kendra

ServiceNow

ServiceNow bietet ein cloudbasiertes Servicemanagementsystem zur Erstellung und Verwaltung von Workflows auf Organisationsebene, z. B. für IT-Services, Ticketsysteme und Support. Sie können Amazon Kendra es verwenden, um Ihre ServiceNow Kataloge, Wissensartikel, Vorfälle und deren Anlagen zu indizieren.

Sie können entweder über Amazon Kendra die Amazon Kendra Konsole, die API oder die TemplateConfigurationAPI eine Verbindung zu Ihrer ServiceNow Datenquelle herstellen. ServiceNowConfiguration

Amazon Kendra hat zwei Versionen des ServiceNow Connectors. Zu den unterstützten Funktionen jeder Version gehören:

ServiceNow Konnektor V1.0//API ServiceNowConfiguration

- Feldzuordnungen
- ServiceNow Instanzversionen: London, Andere
- Muster von Inklusionen/Ausschlüssen: Servicekataloge, Wissensartikel, Anlagen

ServiceNow Konnektor V2.0/API TemplateConfiguration

- Feldzuordnungen
- Filterung des Benutzerkontextes
- Einschluss-/Ausschlussfilter
- Vollständige und inkrementelle Inhaltssynchronisierung
- ServiceNow Instanzversionen: Rom, Sandiego, Tokio, Andere
- Virtual Private Cloud (VPC)

> **Note**
>
> Die Support für ServiceNow Connector ServiceNowConfiguration V1.0/API wird voraussichtlich 2023 enden. Wir empfehlen, zu ServiceNow Connector V2.0/ API zu migrieren oder diesen zu verwenden. TemplateConfiguration

Informationen zur Fehlerbehebung bei Ihrem Amazon Kendra ServiceNow Datenquellen-Connector finden Sie unter. Problembehandlung bei Datenquellen

Themen

- ServiceNow Konnektor V1.0
- ServiceNow Anschluss V2.0
- Angeben von Dokumenten, die mit einer Abfrage indexiert werden sollen

ServiceNow Konnektor V1.0

ServiceNow bietet ein cloudbasiertes Servicemanagementsystem zur Erstellung und Verwaltung von Workflows auf Organisationsebene, z. B. für IT-Services, Ticketsysteme und Support. Sie können Amazon Kendra es verwenden, um Ihre ServiceNow Kataloge, Wissensartikel und deren Anlagen zu indizieren.

> **Note**
>
> Die Support für ServiceNow Connector ServiceNowConfiguration V1.0/API wird voraussichtlich 2023 enden. Wir empfehlen, zu ServiceNow Connector V2.0/ API zu migrieren oder diesen zu verwenden. TemplateConfiguration

Informationen zur Fehlerbehebung bei Ihrem Amazon Kendra ServiceNow Datenquellen-Connector finden Sie unter. Problembehandlung bei Datenquellen

Themen

Unterstützte Features

Amazon Kendra ServiceNow Ein Datenquellenconnector unterstützt die folgenden Funktionen:

- ServiceNow Instanzversionen: London, Andere
- Muster von Inklusionen/Ausschlüssen: Servicekataloge, Wissensartikel und deren Anlagen

Voraussetzungen

Bevor Sie Ihre ServiceNow Datenquelle Amazon Kendra zum Indizieren verwenden können, müssen Sie diese Änderungen in Ihren Konten und Konten vornehmen. ServiceNow AWS

Stellen Sie sicher ServiceNow, dass Sie Folgendes haben:

- Sie haben ein ServiceNow Administratorkonto erstellt und eine ServiceNow Instanz erstellt.
- Der Host Ihrer ServiceNow Instanz-URL wurde kopiert. Wenn die URL der Instanz beispielsweise *https://your-domain.service-now.com* lautet, lautet das Format für die Host-URL, die Sie eingeben, *your-domain.service-now.com*.
- Haben Sie Ihre Basisauthentifizierungsdaten notiert, die einen Benutzernamen und ein Passwort enthalten, um eine Verbindung zu Ihrer Instance herzustellen Amazon Kendra . ServiceNow
- Optional: Es wurde ein OAuth 2.0-Anmeldeinformationstoken konfiguriert, mit dem ein Benutzername, ein Passwort, eine Client-ID Amazon Kendra und ein Client-Geheimnis identifiziert und generiert werden können. Der Benutzername und das Passwort müssen den Zugriff auf die ServiceNow Wissensdatenbank und den Servicekatalog ermöglichen. Weitere Informationen finden Sie in der ServiceNow Dokumentation zur OAuth 2.0-Authentifizierung.
- Die folgenden Berechtigungen wurden hinzugefügt:
  - kb_category
  - kb_Wissen
  - kb_knowledge base
  - kb_uc_kann_mtom nicht_lesen
  - kb_uc_can_read_mtom
  - sc_catalog
  - sc_category
  - sc_cat_item
  - sys_attachment
  - sys_anhang_doc
  - sys_user_role
- Vergewissert, dass jedes Dokument in ServiceNow und zwischen anderen Datenquellen, die Sie für denselben Index verwenden möchten, einzigartig ist. Jede Datenquelle, die Sie für einen Index verwenden möchten, darf nicht dasselbe Dokument in allen Datenquellen enthalten. Dokument-IDs gelten für einen Index global und müssen pro Index eindeutig sein.

Stellen Sie sicher AWS-Konto, dass Sie Folgendes in Ihrem haben:

- Hat einen Amazon Kendra Index erstellt und bei Verwendung der API die Index-ID notiert.
- Sie haben eine IAM Rolle für Ihre Datenquelle erstellt und, falls Sie die API verwenden, den ARN der IAM Rolle notiert.

> **Note**
>
> Wenn Sie Ihren Authentifizierungstyp und Ihre Anmeldeinformationen ändern, müssen Sie Ihre IAM Rolle aktualisieren, um auf die richtige AWS Secrets Manager geheime ID zugreifen zu können.

- Wir haben Ihre ServiceNow Authentifizierungsdaten AWS Secrets Manager geheim gespeichert und, falls Sie die API verwenden, den ARN des Geheimnisses notiert.

> **Note**
>
> Wir empfehlen Ihnen, Ihre Anmeldeinformationen und Ihr Geheimnis regelmäßig zu aktualisieren oder zu wechseln. Stellen Sie zu Ihrer eigenen Sicherheit nur die erforderliche Zugriffsebene bereit. Wir raten davon ab, Anmeldeinformationen und geheime Daten für alle Datenquellen und Connector-Versionen 1.0 und 2.0 (sofern zutreffend) wiederzuverwenden.

Wenn Sie noch keine IAM Rolle oder keinen Schlüssel haben, können Sie die Konsole verwenden, um eine neue IAM Rolle und ein neues Secrets Manager Geheimnis zu erstellen, wenn Sie Ihre ServiceNow Datenquelle mit verbinden. Amazon Kendra Wenn Sie die API verwenden, müssen Sie den ARN einer vorhandenen IAM Rolle und eines Secrets Manager Geheimnisses sowie eine Index-ID angeben.

Anweisungen zur Verbindung

Amazon Kendra Um eine Verbindung mit Ihrer ServiceNow Datenquelle herzustellen, müssen Sie die erforderlichen Details zu Ihrer ServiceNow Datenquelle angeben, damit Sie auf Ihre Daten zugreifen Amazon Kendra können. Falls Sie das noch nicht konfiguriert ServiceNow haben, Amazon Kendra sieheVoraussetzungen.

Console

Um eine Verbindung Amazon Kendra herzustellen ServiceNow

1. Melden Sie sich bei der AWS Management Console an und öffnen Sie die Amazon Kendra Konsole.

2. Wählen Sie im linken Navigationsbereich Indizes und dann den Index, den Sie verwenden möchten, aus der Indexliste aus.

> **Note**
>
> Sie können Ihre Einstellungen für die Benutzerzugriffskontrolle unter Indexeinstellungen konfigurieren oder bearbeiten.

3. Wählen Sie auf der Seite Erste Schritte die Option Datenquelle hinzufügen aus.
4. Wählen Sie auf der Seite Datenquelle hinzufügen die Option ServiceNowConnector V1.0 und dann Datenquelle hinzufügen aus.
5. Geben Sie auf der Seite „Datenquellendetails angeben“ die folgenden Informationen ein:

   a. Geben Sie im Feld Name und Beschreibung für Datenquellenname einen Namen für Ihre Datenquelle ein. Sie können Bindestriche, aber keine Leerzeichen verwenden.

   b. (Optional) Beschreibung — Geben Sie eine optionale Beschreibung für Ihre Datenquelle ein.

   c. In Standardsprache — Wählen Sie eine Sprache aus, um Ihre Dokumente nach dem Index zu filtern. Sofern Sie nichts anderes angeben, ist die Standardsprache Englisch. Die in den Metadaten des Dokuments angegebene Sprache hat Vorrang vor der ausgewählten Sprache.

   d. Unter Tags für Neues Tag hinzufügen — Fügen Sie optionale Tags hinzu, um Ihre Ressourcen zu durchsuchen und zu filtern oder Ihre Kosten nachzuverfolgen. AWS

   e. Wählen Sie Weiter aus.

6. Geben Sie auf der Seite Zugriff und Sicherheit definieren die folgenden Informationen ein:

   a. ServiceNow host — Geben Sie die ServiceNow Host-URL ein.

   b. ServiceNow Version — Wählen Sie Ihre ServiceNow Version aus.

   c. Wählen Sie je nach Anwendungsfall zwischen Standardauthentifizierung und OAuth 2.0-Authentifizierung.

   d. AWS Secrets Manager geheim — Wählen Sie ein vorhandenes Geheimnis oder erstellen Sie ein neues Secrets Manager Geheimnis, um Ihre ServiceNow Authentifizierungsdaten zu speichern. Wenn Sie ein neues Geheimnis erstellen möchten, wird ein AWS Secrets Manager geheimes Fenster geöffnet.

i. Geheimer Name — Ein Name für Ihr Geheimnis. Das Präfix 'AmazonKendra-ServiceNow -' wird Ihrem geheimen Namen automatisch hinzugefügt.

ii. Wenn Sie die Standardauthentifizierung verwenden — Geben Sie den geheimen Namen, den Benutzernamen und das Passwort für Ihr Konto ein. ServiceNow

Wenn Sie die OAuth2-Authentifizierung verwenden, geben Sie den geheimen Namen, den Benutzernamen, das Passwort, die Client-ID und das geheime Client-Geheimnis ein, die Sie in Ihrem Konto erstellt haben. ServiceNow

iii. Wählen Sie Speichern und Geheimnis hinzufügen.

e. IAM Rolle — Wählen Sie eine bestehende IAM Rolle oder erstellen Sie eine neue IAM Rolle, um auf Ihre Repository-Anmeldeinformationen und Indexinhalte zuzugreifen.

> **Note**
>
> IAM Rollen, die für Indizes verwendet werden, können nicht für Datenquellen verwendet werden. Wenn Sie sich nicht sicher sind, ob eine vorhandene Rolle für einen Index oder eine häufig gestellte Frage verwendet wird, wählen Sie Neue Rolle erstellen, um Fehler zu vermeiden.

f. Wählen Sie Weiter aus.

7. Geben Sie auf der Seite Synchronisierungseinstellungen konfigurieren die folgenden Informationen ein:

a. Wissensartikel einbeziehen — Wählen Sie diese Option, um Wissensartikel zu indizieren.

b. Art der Wissensartikel — Wählen Sie je nach Anwendungsfall zwischen Nur öffentliche Artikel einbeziehen und Artikel anhand einer ServiceNow Filterabfrage einbeziehen. Wenn Sie Artikel basierend auf einer ServiceNow Filterabfrage einbeziehen auswählen, müssen Sie eine aus Ihrem ServiceNow Konto kopierte Filterabfrage eingeben.

c. Anlagen zu Wissensartikeln einbeziehen — Wählen Sie diese Option, um Anlagen zu Wissensartikeln zu indizieren. Sie können auch bestimmte Dateitypen für die Indizierung auswählen.

d. Katalogelemente einbeziehen — Wählen Sie diese Option, um Katalogelemente zu indizieren.

e. Anlagen zu Katalogelementen einbeziehen — Wählen Sie diese Option, um die Anhänge von Katalogelementen zu indizieren. Sie können auch bestimmte Dateitypen für die Indizierung auswählen.

f. Häufigkeit — Wie oft Amazon Kendra wird mit Ihrer Datenquelle synchronisiert?

g. Wählen Sie Weiter aus.

8. Geben Sie auf der Seite Feldzuordnungen festlegen die folgenden Informationen ein:

a. Knowledge-Artikel und Servicekatalog — Wählen Sie aus den Amazon Kendra generierten Standard-Datenquellenfeldern und weiteren vorgeschlagenen Feldzuordnungen aus, die Sie Ihrem Index zuordnen möchten.

b. Feld hinzufügen — Um benutzerdefinierte Datenquellenfelder hinzuzufügen, um einen Indexfeldnamen für die Zuordnung und den Felddatentyp zu erstellen.

c. Wählen Sie Weiter aus.

9. Überprüfen Sie auf der Seite Überprüfen und erstellen, ob die von Ihnen eingegebenen Informationen korrekt sind, und wählen Sie dann Datenquelle hinzufügen aus. Sie können Ihre Informationen auch auf dieser Seite bearbeiten. Ihre Datenquelle wird auf der Seite Datenquellen angezeigt, nachdem die Datenquelle erfolgreich hinzugefügt wurde.

API

Um eine Verbindung Amazon Kendra herzustellen ServiceNow

Mithilfe der ServiceNowConfiguration API müssen Sie Folgendes angeben:

- Datenquellen-URL — Geben Sie die ServiceNow URL an. Der Host-Endpunkt sollte wie folgt aussehen: *your-domain.service-now.com*.
- Hostinstanz der Datenquelle — Geben Sie die Version der ServiceNow Host-Instanz entweder als oder an. `LONDON OTHERS`
- Geheimer Amazon-Ressourcenname (ARN) — Geben Sie den Amazon-Ressourcennamen (ARN) eines Secrets Manager Geheimnisses ein, das die Authentifizierungsdaten enthält, die Sie in Ihrem ServiceNow Konto erstellt haben.

  Wenn Sie die Standardauthentifizierung verwenden, wird das Geheimnis in einer JSON-Struktur mit den folgenden Schlüsseln gespeichert:

```
{
```

```
    "username": "user name",
    "password": "password"
}
```

Wenn Sie die OAuth2-Authentifizierung verwenden, wird das Geheimnis in einer JSON-Struktur mit den folgenden Schlüsseln gespeichert:

```
{
    "username": "user name",
    "password": "password",
    "clientId": "client id",
    "clientSecret": "client secret"
}
```

> **Note**
>
> Wir empfehlen Ihnen, Ihre Anmeldeinformationen und Ihr Geheimnis regelmäßig zu aktualisieren oder zu wechseln. Stellen Sie zu Ihrer eigenen Sicherheit nur die erforderliche Zugriffsebene bereit. Wir raten davon ab, Anmeldeinformationen und geheime Daten für alle Datenquellen und Connector-Versionen 1.0 und 2.0 (sofern zutreffend) wiederzuverwenden.

- IAM Rolle — Geben Sie an`RoleArn`, wann Sie anrufen`CreateDataSource`, um einer IAM Rolle Berechtigungen für den Zugriff auf Ihr Secrets Manager Geheimnis und für den Aufruf der erforderlichen öffentlichen APIs für den ServiceNow Connector und zum Aufrufen der erforderlichen öffentlichen APIs zu erteilen. Amazon Kendra Weitere Informationen finden Sie unter IAM Rollen für ServiceNow Datenquellen.

Sie können auch die folgenden optionalen Funktionen hinzufügen:

- Feldzuordnungen — Wählen Sie diese Option, um Ihre ServiceNow Datenquellenfelder Ihren Indexfeldern zuzuordnen. Amazon Kendra Weitere Informationen finden Sie unter Zuweisen von Datenquellenfeldern.

> **Note**
>
> Das Textfeld oder das entsprechende Textfeld für Ihre Dokumente ist erforderlich, um Ihre Dokumente durchsuchen Amazon Kendra zu können. Sie müssen den

Feldnamen Ihres Dokumenthauptteils in Ihrer Datenquelle dem Namen des Indexfeldes zuordnen_document_body. Alle anderen Felder sind optional.

- Inklusions- und Ausschlussfilter — Geben Sie an, ob bestimmte Dateianhänge von Katalogen und Wissensartikeln ein- oder ausgeschlossen werden sollen.

> **Note**
>
> Die meisten Datenquellen verwenden Muster für reguläre Ausdrücke, bei denen es sich um Ein- oder Ausschlussmuster handelt, die als Filter bezeichnet werden. Wenn Sie einen Einschlussfilter angeben, werden nur Inhalte indexiert, die dem Einschlussfilter entsprechen. Jedes Dokument, das nicht dem Einschlussfilter entspricht, wird nicht indexiert. Wenn Sie einen Ein- und Ausschlussfilter angeben, werden Dokumente, die dem Ausschlussfilter entsprechen, nicht indexiert, auch wenn sie dem Einschlussfilter entsprechen.

- Indizierungsparameter — Sie können auch angeben, ob Sie:
  - Indexieren Sie Wissensartikel und Servicekataloge oder beides. Wenn Sie Wissensartikel und Servicekatalogelemente indizieren möchten, müssen Sie den Namen des Felds angeben, das dem ServiceNow Inhaltsfeld des Indexdokuments im Amazon Kendra Index zugeordnet ist.
  - Indizieren Sie Anlagen zu Wissensartikeln und Katalogelementen.
  - Verwenden Sie eine ServiceNow Abfrage, die Dokumente aus einer oder mehreren Wissensdatenbanken auswählt. Die Wissensdatenbanken können öffentlich oder privat sein. Weitere Informationen finden Sie unter Angeben von Dokumenten für die Indexierung mit einer Abfrage.

Weitere Informationen

Weitere Informationen zur Integration Amazon Kendra mit Ihrer ServiceNow Datenquelle finden Sie unter:

- Erste Schritte mit dem Amazon Kendra ServiceNow Online Connector

ServiceNow Anschluss V2.0

ServiceNow bietet ein cloudbasiertes Servicemanagementsystem zur Erstellung und Verwaltung von Workflows auf Organisationsebene, z. B. für IT-Services, Ticketsysteme und Support. Sie können Amazon Kendra es verwenden, um Ihre ServiceNow Kataloge, Wissensartikel, Vorfälle und deren Anlagen zu indizieren.

Informationen zur Problembehandlung Ihres Amazon Kendra ServiceNow Datenquellen-Connectors finden Sie unterProblembehandlung bei Datenquellen.

Themen

Unterstützte Features

Amazon Kendra ServiceNow Ein Datenquellenconnector unterstützt die folgenden Funktionen:

- Feldzuordnungen
- Filterung des Benutzerkontextes
- Einschluss-/Ausschlussfilter
- Vollständige und inkrementelle Inhaltssynchronisierung
- ServiceNow Instanzversionen: Rom, Sandiego, Tokio, Andere
- Virtual Private Cloud (VPC)

Voraussetzungen

Bevor Sie Ihre ServiceNow Datenquelle Amazon Kendra zum Indizieren verwenden können, nehmen Sie diese Änderungen in Ihren AWS Konten ServiceNow und Konten vor.

Stellen Sie sicher ServiceNow, dass Sie Folgendes haben:

- Sie haben eine Personal- oder Enterprise Developer-Instanz erstellt und verfügen über eine ServiceNow Instanz mit Administratorrolle.

- Der Host Ihrer ServiceNow Instanz-URL wurde kopiert. Das Format für die Host-URL, die Sie eingeben, ist *your-domain.service-now.com*. Sie benötigen Ihre ServiceNow Instanz-URL, um eine Verbindung herzustellen. Amazon Kendra
- Haben Sie sich Ihre grundlegenden Authentifizierungsdaten mit einem Benutzernamen und einem Passwort notiert, um eine Verbindung Amazon Kendra zu Ihrer ServiceNow Instance herstellen zu können.
- Optional: Konfigurierte OAuth 2.0-Client-Anmeldeinformationen, die Amazon Kendra anhand eines Benutzernamens, eines Kennworts und einer generierten Client-ID sowie eines geheimen Client-Schlüssels identifiziert werden können. Weitere Informationen finden Sie in der ServiceNow Dokumentation zur OAuth 2.0-Authentifizierung.
- Vergewissert, dass jedes Dokument in ServiceNow und zwischen anderen Datenquellen, die Sie für denselben Index verwenden möchten, einzigartig ist. Jede Datenquelle, die Sie für einen Index verwenden möchten, darf nicht dasselbe Dokument in allen Datenquellen enthalten. Dokument-IDs gelten für einen Index global und müssen pro Index eindeutig sein.

Stellen Sie sicher AWS-Konto, dass Sie Folgendes in Ihrem haben:

- Hat einen Amazon Kendra Index erstellt und bei Verwendung der API die Index-ID notiert.
- Sie haben eine IAM Rolle für Ihre Datenquelle erstellt und, falls Sie die API verwenden, den ARN der IAM Rolle notiert.

> **Note**
>
> Wenn Sie Ihren Authentifizierungstyp und Ihre Anmeldeinformationen ändern, müssen Sie Ihre IAM Rolle aktualisieren, um auf die richtige AWS Secrets Manager geheime ID zugreifen zu können.

- Wir haben Ihre ServiceNow Authentifizierungsdaten AWS Secrets Manager geheim gespeichert und, falls Sie die API verwenden, den ARN des Geheimnisses notiert.

> **Note**
>
> Wir empfehlen Ihnen, Ihre Anmeldeinformationen und Ihr Geheimnis regelmäßig zu aktualisieren oder zu wechseln. Stellen Sie zu Ihrer eigenen Sicherheit nur die erforderliche Zugriffsebene bereit. Wir raten davon ab, Anmeldeinformationen und geheime

Daten für alle Datenquellen und Connector-Versionen 1.0 und 2.0 (sofern zutreffend) wiederzuverwenden.

Wenn Sie noch keine IAM Rolle oder keinen Schlüssel haben, können Sie die Konsole verwenden, um eine neue IAM Rolle und ein neues Secrets Manager Geheimnis zu erstellen, wenn Sie Ihre ServiceNow Datenquelle mit verbinden. Amazon Kendra Wenn Sie die API verwenden, müssen Sie den ARN einer vorhandenen IAM Rolle und eines Secrets Manager Geheimnisses sowie eine Index-ID angeben.

Anweisungen zur Verbindung

Amazon Kendra Um eine Verbindung mit Ihrer ServiceNow Datenquelle herzustellen, müssen Sie die erforderlichen Details zu Ihrer ServiceNow Datenquelle angeben, damit Sie auf Ihre Daten zugreifen Amazon Kendra können. Falls Sie das noch nicht konfiguriert ServiceNow haben, Amazon Kendra sieheVoraussetzungen.

Console

Um eine Verbindung Amazon Kendra herzustellen ServiceNow

1. Melden Sie sich bei der AWS Management Console an und öffnen Sie die Amazon Kendra Konsole.
2. Wählen Sie im linken Navigationsbereich Indizes und dann den Index, den Sie verwenden möchten, aus der Indexliste aus.

   > **Note**
   >
   > Sie können Ihre Einstellungen für die Benutzerzugriffskontrolle unter Indexeinstellungen konfigurieren oder bearbeiten.

3. Wählen Sie auf der Seite Erste Schritte die Option Datenquelle hinzufügen aus.
4. Wählen Sie auf der Seite Datenquelle hinzufügen die Option ServiceNowConnector V2.0 und dann Datenquelle hinzufügen aus.
5. Geben Sie auf der Seite „Datenquellendetails angeben“ die folgenden Informationen ein:

   a. Geben Sie im Feld Name und Beschreibung für Datenquellenname einen Namen für Ihre Datenquelle ein. Sie können Bindestriche, aber keine Leerzeichen verwenden.

b. (Optional) Beschreibung — Geben Sie eine optionale Beschreibung für Ihre Datenquelle ein.

c. In Standardsprache — Wählen Sie eine Sprache aus, um Ihre Dokumente nach dem Index zu filtern. Sofern Sie nichts anderes angeben, ist die Standardsprache Englisch. Die in den Metadaten des Dokuments angegebene Sprache hat Vorrang vor der ausgewählten Sprache.

d. Unter Tags für Neues Tag hinzufügen — Fügen Sie optionale Tags hinzu, um Ihre Ressourcen zu durchsuchen und zu filtern oder Ihre Kosten nachzuverfolgen. AWS

e. Wählen Sie Weiter aus.

6. Geben Sie auf der Seite Zugriff und Sicherheit definieren die folgenden Informationen ein:

a. ServiceNow host — Geben Sie die ServiceNow Host-URL ein. Das Format für die Host-URL, die Sie eingeben, ist *your-domain.service-now.com*.

b. ServiceNow Version — Wählen Sie Ihre Instanzversion aus. ServiceNow Sie können zwischen Rom, Sandiego, Tokio oder anderen wählen.

c. Autorisierung — Aktivieren oder deaktivieren Sie die Informationen der Zugriffskontrollliste (ACL) für Ihre Dokumente, wenn Sie über eine ACL verfügen und diese für die Zugriffskontrolle verwenden möchten. Die ACL gibt an, auf welche Dokumente Benutzer und Gruppen zugreifen können. Die ACL-Informationen werden verwendet, um Suchergebnisse nach dem Benutzer- oder Gruppenzugriff auf Dokumente zu filtern. Weitere Informationen finden Sie unter Benutzerkontextfilterung.

d. Authentifizierung — Wählen Sie zwischen Standardauthentifizierung und OAuth 2.0-Authentifizierung.

e. AWS Secrets Manager geheim — Wählen Sie ein vorhandenes Geheimnis oder erstellen Sie ein neues Secrets Manager Geheimnis, um Ihre Authentifizierungsdaten zu speichern. ServiceNow Wenn Sie ein neues Geheimnis erstellen möchten, wird ein AWS Secrets Manager geheimes Fenster geöffnet. Geben Sie die folgenden Informationen in das Fenster ein:

i. Geheimer Name — Ein Name für Ihr Geheimnis. Das Präfix 'AmazonKendra-ServiceNow -' wird Ihrem geheimen Namen automatisch hinzugefügt.

ii. Wenn Sie die Standardauthentifizierung verwenden — Geben Sie den geheimen Namen, den Benutzernamen und das Passwort für Ihr Konto ein. ServiceNow

Wenn Sie die OAuth2.0-Authentifizierung verwenden, geben Sie den geheimen Namen, den Benutzernamen, das Passwort, die Client-ID und das geheime Client-Geheimnis ein, die Sie in Ihrem Konto erstellt haben. ServiceNow

iii. Wählen Sie Speichern und Geheimnis hinzufügen.

f. Virtual Private Cloud (VPC) — Sie können wählen, ob Sie eine VPC verwenden möchten. In diesem Fall müssen Sie Subnetze und VPC-Sicherheitsgruppen hinzufügen.

g. Identity Crawler — Geben Sie an, ob der Identity Crawler aktiviert Amazon Kendra werden soll. Der Identity Crawler verwendet die Informationen der Zugriffskontrollliste (ACL) für Ihre Dokumente, um Suchergebnisse nach dem Benutzer- oder Gruppenzugriff auf Dokumente zu filtern. Wenn Sie über eine ACL für Ihre Dokumente verfügen und sich dafür entscheiden, Ihre ACL zu verwenden, können Sie auch den Identity Crawler aktivieren, um die Benutzerkontextfilterung von Suchergebnissen zu konfigurieren. Amazon Kendra Andernfalls können alle Dokumente öffentlich durchsucht werden, wenn Identity Crawler ausgeschaltet ist. Wenn Sie die Zugriffskontrolle für Ihre Dokumente verwenden möchten und Identity Crawler ausgeschaltet ist, können Sie alternativ die PutPrincipalMappingAPI verwenden, um Benutzer- und Gruppenzugriffsinformationen für die Benutzerkontextfilterung hochzuladen.

h. IAM Rolle — Wählen Sie eine bestehende IAM Rolle oder erstellen Sie eine neue IAM Rolle, um auf Ihre Repository-Anmeldeinformationen und Indexinhalte zuzugreifen.

> **Note**
>
> IAM Rollen, die für Indizes verwendet werden, können nicht für Datenquellen verwendet werden. Wenn Sie sich nicht sicher sind, ob eine vorhandene Rolle für einen Index oder eine häufig gestellte Frage verwendet wird, wählen Sie Neue Rolle erstellen, um Fehler zu vermeiden.

i. Wählen Sie Weiter aus.

7. Geben Sie auf der Seite Synchronisierungseinstellungen konfigurieren die folgenden Informationen ein:

   a. Wählen Sie für Knowledge-Artikel aus den folgenden Optionen:

   - Knowledge-Artikel — Wählen Sie diese Option, um Wissensartikel zu indizieren.
   - Anlagen zu Wissensartikeln — Wählen Sie diese Option, um die Anhänge von Wissensartikeln zu indizieren.

- Art der Wissensartikel — Wählen Sie je nach Anwendungsfall zwischen Nur öffentliche Artikel und Knowledge-Artikel basierend auf einer ServiceNow Filterabfrage. Wenn Sie Artikel basierend auf einer ServiceNow Filterabfrage einbeziehen auswählen, müssen Sie eine aus Ihrem ServiceNow Konto kopierte Filterabfrage eingeben. *Zu den Beispielfilterabfragen gehören: workflow_state=draft^EQ, kb_knowledge_base=dfc19531bf2021003f07e2c1ac0739ab^textISNOTEMPTY^EQ, article_type=text^active=true^EQ.*

  > **Important**
  >
  > Wenn Sie nur öffentliche Artikel crawlen möchten, werden nur Wissensartikel gecrawlt, denen eine öffentliche Zugriffsrolle zugewiesen wurde. Amazon Kendra ServiceNow

- Artikel basierend auf dem Kurzbeschreibungsfilter einbeziehen — Geben Sie Muster für reguläre Ausdrücke an, um bestimmte Artikel ein- oder auszuschließen.

b. Für Servicekatalogelemente:

- Servicekatalogelemente — Wählen Sie diese Option, um Servicekatalogelemente zu indizieren.
- Anlagen von Servicekatalogelementen — Wählen Sie diese Option, um die Anhänge von Servicekatalogelementen zu indizieren.
- Aktive Servicekatalogelemente — Wählen Sie diese Option, um aktive Servicekatalogelemente zu indizieren.
- Inaktive Servicekatalogelemente — Wählen Sie diese Option, um inaktive Servicekatalogelemente zu indizieren.
- Filterabfrage — Wählen Sie aus, ob Servicekatalogelemente auf der Grundlage eines in Ihrer ServiceNow Instanz definierten Filters aufgenommen werden sollen. *Zu den Filterabfragen gehören beispielsweise: short_descriptionLIKEAccess^category=2809952237b1300054b6a3549dbe5dd4nameSTARTSWITHService^active=true^EQ.*
- Servicekatalogelemente basierend auf dem Kurzbeschreibungsfilter einbeziehen — Geben Sie ein Regex-Muster an, um bestimmte Katalogelemente einzubeziehen.

c. Für Vorfälle:

- Vorfälle — Wählen Sie diese Option, um Dienstvorfälle zu indizieren.

- Vorfallsanhänge — Wählen Sie diese Option, um Vorfallanhänge zu indizieren.
- Aktive Vorfälle — Wählen Sie diese Option, um aktive Vorfälle zu indizieren.
- Inaktive Vorfälle — Wählen Sie diese Option, um inaktive Vorfälle zu indizieren.
- Aktiver Vorfalltyp — Wählen Sie je nach Anwendungsfall zwischen Alle Incidents, Open Incidents, Offen — nicht zugewiesene Incidents und Behobene Incidents.
- Filterabfrage — Wählen Sie aus, ob Vorfälle auf der Grundlage eines in Ihrer Instanz definierten Filters eingeschlossen werden sollen. ServiceNow *Zu den Filterabfragen gehören beispielsweise: short_descriptionLikeTest^urgency=3^state=1^EQ, Priority=2^Software^EQ.*
- Vorfälle auf der Grundlage des Kurzbeschreibungsfilters einbeziehen — Geben Sie ein Regex-Muster an, um bestimmte Vorfälle einzubeziehen.

d. Für zusätzliche Konfigurationen:

- ACL-Informationen — Zugriffskontrolllisten für die von Ihnen ausgewählten Entitäten sind standardmäßig enthalten. Wenn Sie die Auswahl einer Zugriffskontrollliste aufheben, werden alle Dateien in dieser Kategorie öffentlich zugänglich gemacht. ACL-Optionen werden für nicht ausgewählte Entitäten automatisch deaktiviert. Für öffentliche Artikel wird ACL nicht angewendet.
- Für Maximale Dateigröße — Geben Sie die Dateigrößenbeschränkung in MB an, die Amazon Kendra crawlt. Amazon Kendra crawlt nur die Dateien innerhalb der von Ihnen definierten Größenbeschränkung. Die Standarddateigröße ist 50 MB. Die maximale Dateigröße sollte größer als 0 MB und kleiner oder gleich 50 MB sein.
- Regex-Muster für Anlagen — Fügen Sie Muster für reguläre Ausdrücke hinzu, um bestimmte angehängte Dateien von Katalogen, Wissensartikeln und Vorfällen ein- oder auszuschließen. Sie können bis zu 100 Muster hinzufügen.

e. Synchronisierungsmodus — Wählen Sie aus, wie Sie Ihren Index aktualisieren möchten, wenn sich der Inhalt Ihrer Datenquelle ändert. Wenn Sie Ihre Datenquelle Amazon Kendra zum ersten Mal synchronisieren, werden alle Inhalte standardmäßig gecrawlt und indexiert. Sie müssen eine vollständige Synchronisierung Ihrer Daten durchführen, falls Ihre erste Synchronisierung fehlgeschlagen ist, auch wenn Sie die Option Vollsynchronisierung nicht als Synchronisierungsmodusoption wählen.

- Vollständige Synchronisierung: Indizieren Sie den gesamten Inhalt neu und ersetzen die vorhandenen Inhalte jedes Mal, wenn Ihre Datenquelle mit Ihrem Index synchronisiert wird.
- Neue, geänderte, gelöschte Synchronisierung: Indizieren Sie bei jeder Synchronisierung Ihrer Datenquelle mit Ihrem Index nur neue, geänderte und gelöschte Inhalte. Amazon Kendra kann den Mechanismus Ihrer Datenquelle verwenden, um Inhaltsänderungen nachzuverfolgen und Inhalte zu indexieren, die sich seit der letzten Synchronisierung geändert haben.

f. Im Synchronisierungslaufplan für Frequenz — Wie oft Amazon Kendra wird mit Ihrer Datenquelle synchronisiert?

g. Wählen Sie Weiter aus.

8. Geben Sie auf der Seite Feldzuordnungen festlegen die folgenden Informationen ein:

   a. Knowledge-Artikel, Servicekatalog, Anlagen und Vorfälle — Wählen Sie aus den Amazon Kendra generierten Standard-Datenquellenfeldern aus, die Sie Ihrem Index zuordnen möchten.

   b. Feld hinzufügen — Um benutzerdefinierte Datenquellenfelder hinzuzufügen, um einen Indexfeldnamen für die Zuordnung und den Felddatentyp zu erstellen.

   c. Wählen Sie Weiter aus.

9. Überprüfen Sie auf der Seite Überprüfen und erstellen, ob die von Ihnen eingegebenen Informationen korrekt sind, und wählen Sie dann Datenquelle hinzufügen aus. Sie können Ihre Informationen auch auf dieser Seite bearbeiten. Ihre Datenquelle wird auf der Seite Datenquellen angezeigt, nachdem die Datenquelle erfolgreich hinzugefügt wurde.

API

Um eine Verbindung Amazon Kendra herzustellen ServiceNow

Sie müssen mithilfe der TemplateConfigurationAPI ein JSON des Datenquellenschemas angeben. Sie müssen die folgenden Informationen angeben:

- Datenquelle — Geben Sie den Datenquellentyp wie `SERVICENOWV2` bei der Verwendung des TemplateConfigurationJSON-Schemas an. Geben Sie außerdem die Datenquelle so an`TEMPLATE`, wie Sie die CreateDataSourceAPI aufrufen.

- Host-URL — Geben Sie die Version der ServiceNow Host-Instanz an. Zum Beispiel *your-domain.service-now.com*.
- Authentifizierungstyp — Geben Sie den Authentifizierungstyp an, den Sie verwenden, unabhängig davon, ob oder für Ihre Instanz. `basicAuth` `0Auth2` ServiceNow
- ServiceNow Instanzversion — Geben Sie die ServiceNow Instanz an, die Sie verwenden, ob`Tokyo`, `SandiegoRome`, oder. `Others`
- Synchronisierungsmodus — Geben Sie an, wie Ihr Index aktualisiert Amazon Kendra werden soll, wenn sich der Inhalt Ihrer Datenquelle ändert. Wenn Sie Ihre Datenquelle Amazon Kendra zum ersten Mal synchronisieren, werden alle Inhalte standardmäßig gecrawlt und indexiert. Sie müssen eine vollständige Synchronisierung Ihrer Daten durchführen, falls Ihre erste Synchronisierung fehlgeschlagen ist, auch wenn Sie die Option Vollsynchronisierung nicht als Synchronisierungsmodusoption wählen. Sie können wählen zwischen:
  - `FORCED_FULL_CRAWL`um den gesamten Inhalt neu zu indizieren und vorhandene Inhalte jedes Mal zu ersetzen, wenn Ihre Datenquelle mit Ihrem Index synchronisiert wird.
  - `FULL_CRAWL`um bei jeder Synchronisierung Ihrer Datenquelle mit Ihrem Index nur neue, geänderte und gelöschte Inhalte zu indizieren. Amazon Kendra kann den Mechanismus Ihrer Datenquelle verwenden, um Inhaltsänderungen nachzuverfolgen und Inhalte zu indexieren, die sich seit der letzten Synchronisierung geändert haben.
- Geheimer Amazon-Ressourcenname (ARN) — Geben Sie den Amazon-Ressourcennamen (ARN) eines Secrets Manager Geheimnisses ein, das die Authentifizierungsdaten enthält, die Sie in Ihrem ServiceNow Konto erstellt haben.

  Wenn Sie die Standardauthentifizierung verwenden, wird das Geheimnis in einer JSON-Struktur mit den folgenden Schlüsseln gespeichert:

```
{
    "username": "user name",
    "password": "password"
}
```

> **Note**
>
> Wir empfehlen Ihnen, Ihre Anmeldeinformationen und Ihr Geheimnis regelmäßig zu aktualisieren oder zu wechseln. Stellen Sie zu Ihrer eigenen Sicherheit nur die erforderliche Zugriffsebene bereit. Wir raten davon ab, Anmeldeinformationen und

geheime Daten für alle Datenquellen und Connector-Versionen 1.0 und 2.0 (sofern zutreffend) wiederzuverwenden.

- Wenn Sie OAuth2-Client-Anmeldeinformationen verwenden, wird das Geheimnis in einer JSON-Struktur mit den folgenden Schlüsseln gespeichert:

```
{
    "username": "user name",
    "password": "password",
    "clientId": "client id",
    "clientSecret": "client secret"
}
```

- IAM role — Geben Sie an`RoleArn`, wann Sie aufrufen`CreateDataSource`, um einer IAM Rolle Berechtigungen für den Zugriff auf Ihr Secrets Manager Geheimnis und den Aufruf der erforderlichen öffentlichen APIs für den ServiceNow Connector und zu erteilen. Amazon Kendra Weitere Informationen finden Sie unter IAM Rollen für ServiceNow Datenquellen.

Sie können auch die folgenden optionalen Funktionen hinzufügen:

- Virtual Private Cloud (VPC) — Geben Sie an, `VpcConfiguration` wann Sie anrufen. `CreateDataSource` Weitere Informationen finden Sie unter Konfigurieren von Amazon Kendra für die Verwendung eines Amazon VPC.
- Inklusions- und Ausschlussfilter — Sie können anhand der Dateinamen und Dateitypen von Wissensartikeln, Servicekatalogen und Vorfällen angeben, ob bestimmte angehängte Dateien ein- oder ausgeschlossen werden sollen.

> **Note**
>
> Die meisten Datenquellen verwenden Muster für reguläre Ausdrücke. Dabei handelt es sich um Ein- oder Ausschlussmuster, die als Filter bezeichnet werden. Wenn Sie einen Einschlussfilter angeben, werden nur Inhalte indexiert, die dem Einschlussfilter entsprechen. Jedes Dokument, das nicht dem Einschlussfilter entspricht, wird nicht indexiert. Wenn Sie einen Ein- und Ausschlussfilter angeben, werden Dokumente, die dem Ausschlussfilter entsprechen, nicht indexiert, auch wenn sie dem Einschlussfilter entsprechen.

- Bestimmte zu indizierende Dokumente — Sie können eine ServiceNow Abfrage verwenden, um die gewünschten Dokumente aus einer oder mehreren Wissensdatenbanken, einschließlich privater Wissensdatenbanken, anzugeben. Der Zugriff auf die Wissensdatenbanken wird durch den Benutzer bestimmt, den Sie für die Verbindung mit der ServiceNow Instanz verwenden. Weitere Informationen finden Sie unter Angeben von Dokumenten für die Indexierung mit einer Abfrage.
- Indizierungsparameter — Sie können auch angeben, ob Sie:
  - Indexieren Sie Wissensartikel, Servicekataloge und Vorfälle oder alle diese. Wenn Sie Wissensartikel, Servicekatalogelemente und Vorfälle indizieren möchten, müssen Sie den Namen des ServiceNow Felds angeben, das dem Inhaltsfeld des Indexdokuments im Amazon Kendra Index zugeordnet ist.
  - Indexieren Sie Anlagen zu Wissensartikeln, Servicekatalogeinträgen und Vorfällen.
  - Fügen Sie Wissensartikel, Servicekatalogelemente und Vorfälle auf der Grundlage des `short description` Filtermusters hinzu.
  - Wählen Sie aus, ob aktive und inaktive Servicekatalogelemente und Vorfälle gefiltert werden sollen.
  - Wählen Sie, ob Vorfälle nach Art des Vorfalls gefiltert werden sollen.
  - Wählen Sie aus, für welche Entitäten die ACL gecrawlt werden soll.
  - Sie können eine ServiceNow Abfrage verwenden, um die gewünschten Dokumente aus einer oder mehreren Wissensdatenbanken, einschließlich privater Wissensdatenbanken, anzugeben. Der Zugriff auf die Wissensdatenbanken wird durch den Benutzer bestimmt, den Sie für die Verbindung mit der ServiceNow Instanz verwenden. Weitere Informationen finden Sie unter Angeben von Dokumenten für die Indexierung mit einer Abfrage.
- Identity Crawler — Geben Sie an, ob der Identity Crawler aktiviert Amazon Kendra werden soll. Der Identity Crawler verwendet die Informationen der Zugriffskontrollliste (ACL) für Ihre Dokumente, um Suchergebnisse nach dem Benutzer- oder Gruppenzugriff auf Dokumente zu filtern. Wenn Sie über eine ACL für Ihre Dokumente verfügen und sich dafür entscheiden, Ihre ACL zu verwenden, können Sie auch den Identity Crawler aktivieren, um die Benutzerkontextfilterung von Suchergebnissen zu konfigurieren. Amazon Kendra Andernfalls können alle Dokumente öffentlich durchsucht werden, wenn Identity Crawler ausgeschaltet ist. Wenn Sie die Zugriffskontrolle für Ihre Dokumente verwenden möchten und Identity Crawler ausgeschaltet ist, können Sie alternativ die PutPrincipalMappingAPI verwenden, um Benutzer- und Gruppenzugriffsinformationen für die Benutzerkontextfilterung hochzuladen.

- Feldzuordnungen — Wählen Sie diese Option, um Ihre ServiceNow Datenquellenfelder Ihren Indexfeldern zuzuordnen. Amazon Kendra Weitere Informationen finden Sie unter Zuweisen von Datenquellenfeldern.

  > **Note**
  >
  > Das Textfeld oder das entsprechende Textfeld für Ihre Dokumente ist erforderlich, um Ihre Dokumente durchsuchen Amazon Kendra zu können. Sie müssen den Feldnamen Ihres Dokumenthauptteils in Ihrer Datenquelle dem Namen des Indexfeldes zuordnen`_document_body`. Alle anderen Felder sind optional.

Eine Liste weiterer wichtiger JSON-Schlüssel, die konfiguriert werden müssen, finden Sie unterServiceNow Vorlagenschema.

Weitere Informationen

Weitere Informationen zur Integration Amazon Kendra mit Ihrer ServiceNow Datenquelle finden Sie unter:

- Erste Schritte mit der Amazon Kendra Ankündigung des aktualisierten ServiceNow Connectors (V2) für Amazon Kendra

Angeben von Dokumenten, die mit einer Abfrage indexiert werden sollen

Sie können eine ServiceNow Abfrage verwenden, um die Dokumente anzugeben, die Sie in einen Amazon Kendra Index aufnehmen möchten. Wenn Sie eine Abfrage verwenden, können Sie mehrere Wissensdatenbanken angeben, einschließlich privater Wissensdatenbanken. Der Zugriff auf die Wissensdatenbanken wird durch den Benutzer bestimmt, den Sie für die Verbindung mit der ServiceNow Instanz verwenden.

Um eine Abfrage zu erstellen, verwenden Sie den ServiceNow Query Builder. Sie können den Builder verwenden, um die Abfrage zu erstellen und zu testen, ob die Abfrage die richtige Liste von Dokumenten zurückgibt.

Um eine Abfrage mit der ServiceNow Konsole zu erstellen

1. Loggen Sie sich in die ServiceNow Konsole ein.

2. Wählen Sie im linken Menü „Wissen“, dann „Artikel“ und anschließend „Alle“.
3. Wählen Sie oben auf der Seite das Filtersymbol aus.
4. Verwenden Sie den Query Builder, um die Abfrage zu erstellen.
5. Wenn die Abfrage abgeschlossen ist, klicken Sie mit der rechten Maustaste auf die Abfrage und wählen Sie Abfrage kopieren, um die Abfrage aus dem Abfrage-Generator zu kopieren. Speichern Sie diese Abfrage, um sie in zu verwenden Amazon Kendra.

Achten Sie darauf, dass Sie beim Kopieren der Abfrage keinen Abfrageparameter ändern. Wenn einer der Abfrageparameter nicht erkannt wird, ServiceNow behandelt den Parameter als leer und verwendet ihn nicht zum Filtern der Ergebnisse.

Slack

Slack ist eine Kommunikations-App für Unternehmen, mit der Benutzer Nachrichten und Anhänge über verschiedene öffentliche und private Kanäle senden können. Du kannst Amazon Kendra damit deine öffentlichen und privaten Slack-Kanäle, Bot- und Archivierungsnachrichten, Dateien und Anhänge, Direkt- und Gruppennachrichten indizieren. Du kannst auch bestimmte Inhalte zum Filtern auswählen.

> **Note**
>
> Amazon Kendra unterstützt jetzt einen aktualisierten Slack-Connector.
> Die Konsole wurde automatisch für dich aktualisiert. Alle neuen Konnektoren, die Sie in der Konsole erstellen, verwenden die aktualisierte Architektur. Wenn Sie die API verwenden, müssen Sie jetzt das TemplateConfigurationObjekt anstelle des `SlackConfiguration` Objekts verwenden, um Ihren Connector zu konfigurieren.
> Konnektoren, die mit der älteren Konsolen- und API-Architektur konfiguriert wurden, funktionieren weiterhin wie konfiguriert. Sie können sie jedoch nicht bearbeiten oder aktualisieren. Wenn Sie Ihre Connectorkonfiguration bearbeiten oder aktualisieren möchten, müssen Sie einen neuen Connector erstellen.

> Wir empfehlen, Ihren Connector-Workflow auf die aktualisierte Version zu migrieren. Die Support für Konnektoren, die mit der älteren Architektur konfiguriert wurden, soll bis Juni 2024 eingestellt werden.

Du kannst über Amazon Kendra die Amazon Kendra Konsole oder die TemplateConfigurationAPI eine Verbindung zu deiner Slack-Datenquelle herstellen.

Informationen zur Fehlerbehebung bei deinem Amazon Kendra Slack-Datenquellen-Connector findest du unter. Problembehandlung bei Datenquellen

Themen

Unterstützte Features

Amazon Kendra Der Datenquellen-Connector von Slack unterstützt die folgenden Funktionen:

- Feldzuordnungen
- Filterung des Benutzerkontextes
- Crawling der Benutzeridentität
- Einschluss-/Ausschlussfilter
- Vollständige und inkrementelle Inhaltssynchronisierung
- Virtual Private Cloud (VPC)

Voraussetzungen

Bevor du deine Slack-Datenquelle Amazon Kendra zum Indizieren verwenden kannst, nimm diese Änderungen in deinem Slack und deinen Accounts vor. AWS

Stelle in Slack sicher, dass du:

- Du hast ein Slack-Bot-Benutzer-OAuth-Token oder ein Slack-Benutzer-OAuth-Token erstellt. Du kannst eines der beiden Tokens wählen, um eine Verbindung zu deiner Slack-Datenquelle

herzustellen Amazon Kendra . Weitere Informationen findest du in der Slack-Dokumentation zu Zugriffstoken.

> **Note**
>
> Wenn du das Bot-Token als Teil deiner Slack-Zugangsdaten verwendest, kannst du Direktnachrichten und Gruppennachrichten nicht indizieren und du musst das Bot-Token zu dem Channel hinzufügen, den du indexieren möchtest.

- Du hast dir deine Slack-Workspace-Team-ID aus der URL deiner Slack-Workspace-Hauptseite notiert. *Zum Beispiel https://app.slack.com/client/T0123456789/...* wobei *T0123456789* die Team-ID ist.
- Die folgenden Oauth-Bereiche/Berechtigungen wurden hinzugefügt:

Geltungsbereich des Benutzer-Tokens	Geltungsbereich des Bot-Tokens
• Kanäle: Geschichte • Kanäle:lesen • Emoji: lesen • Dateien:lesen • Gruppen:Verlauf • Gruppen:lesen • Ich bin: Geschichte • Ich: lese • mpim: Geschichte • mpim:lesen • team:lesen • users.profil:lesen • Benutzer:lesen • Benutzer:read.email	• Kanäle:Verlauf • Kanäle:verwalten • Kanäle:lesen • conversations.connect:verwalten • conversations.connect:lesen • Dateien:lesen • Gruppen:Verlauf • Gruppen:lesen • Ich bin: Geschichte • Ich: lese • mpim: Geschichte • mpim:lesen • Reaktionen:lesen • team:lesen • Benutzergruppen: lesen • users.profil:lesen • Benutzer:lesen

Geltungsbereich des Benutzer-Tokens	Geltungsbereich des Bot-Tokens
	• Benutzer:read.email

- Aktiviert, dass jedes Dokument in Slack und in anderen Datenquellen, die du für denselben Index verwenden möchtest, einzigartig ist. Jede Datenquelle, die du für einen Index verwenden möchtest, darf nicht dasselbe Dokument in allen Datenquellen enthalten. Dokument-IDs gelten für einen Index global und müssen pro Index eindeutig sein.

Stellen Sie sicher AWS-Konto, dass Sie Folgendes in Ihrem haben:

- Hat einen Amazon Kendra Index erstellt und bei Verwendung der API die Index-ID notiert.
- Sie haben eine IAM Rolle für Ihre Datenquelle erstellt und, falls Sie die API verwenden, den ARN der IAM Rolle notiert.

> **Note**
>
> Wenn Sie Ihren Authentifizierungstyp und Ihre Anmeldeinformationen ändern, müssen Sie Ihre IAM Rolle aktualisieren, um auf die richtige AWS Secrets Manager geheime ID zugreifen zu können.

- Du hast deine Slack-Authentifizierungsdaten AWS Secrets Manager geheim gespeichert und, falls du die API verwendest, den ARN des Geheimnisses notiert.

> **Note**
>
> Wir empfehlen dir, deine Zugangsdaten und dein Geheimnis regelmäßig zu aktualisieren oder zu wechseln. Stellen Sie zu Ihrer eigenen Sicherheit nur die Zugriffsebene bereit, die erforderlich ist. Wir raten davon ab, Anmeldeinformationen und geheime Daten für alle Datenquellen und Connector-Versionen 1.0 und 2.0 (sofern zutreffend) wiederzuverwenden.

Wenn du noch keine IAM Rolle oder keinen Schlüssel hast, kannst du die Konsole verwenden, um eine neue IAM Rolle und ein neues Secrets Manager Geheimnis zu erstellen, wenn du deine Slack-Datenquelle mit verbindest. Amazon Kendra Wenn Sie die API verwenden, müssen Sie den ARN einer vorhandenen IAM Rolle und eines Secrets Manager Geheimnisses sowie eine Index-ID angeben.

Anweisungen zur Verbindung

Um eine Verbindung Amazon Kendra zu deiner Slack-Datenquelle herzustellen, musst du die erforderlichen Details zu deiner Slack-Datenquelle angeben, damit du auf deine Daten zugreifen Amazon Kendra kannst. Falls du Slack noch nicht für Amazon Kendra konfiguriert hast, findest du weitere Informationen unter. Voraussetzungen

Console

Um eine Verbindung zu Amazon Kendra Slack herzustellen

1. Melde dich bei der an AWS Management Console und öffne die Amazon Kendra Konsole.
2. Wählen Sie im linken Navigationsbereich Indizes und dann den Index, den Sie verwenden möchten, aus der Indexliste aus.

   > **Note**
   >
   > Sie können Ihre Einstellungen für die Benutzerzugriffskontrolle unter Indexeinstellungen konfigurieren oder bearbeiten.

3. Wählen Sie auf der Seite Erste Schritte die Option Datenquelle hinzufügen aus.
4. Wähle auf der Seite Datenquelle hinzufügen die Option Slack-Konnektor und dann Konnektor hinzufügen aus.
5. Gib auf der Seite „Datenquellendetails angeben“ die folgenden Informationen ein:

   a. Geben Sie im Feld Name und Beschreibung für Datenquellenname einen Namen für Ihre Datenquelle ein. Sie können Bindestriche, aber keine Leerzeichen verwenden.

   b. (Optional) Beschreibung — Geben Sie eine optionale Beschreibung für Ihre Datenquelle ein.

   c. In Standardsprache — Wählen Sie eine Sprache aus, um Ihre Dokumente nach dem Index zu filtern. Sofern Sie nichts anderes angeben, ist die Standardsprache Englisch. Die in den Metadaten des Dokuments angegebene Sprache hat Vorrang vor der ausgewählten Sprache.

   d. Unter Tags für Neues Tag hinzufügen — Fügen Sie optionale Tags hinzu, um Ihre Ressourcen zu durchsuchen und zu filtern oder Ihre Kosten nachzuverfolgen. AWS

   e. Wählen Sie Weiter aus.

6. Geben Sie auf der Seite Zugriff und Sicherheit definieren die folgenden Informationen ein:

a. Im Feld Quelle für Slack-Workspace-Team-ID — Die Team-ID deines Slack-Workspace.

b. AWS Secrets Manager geheim — Wähle ein vorhandenes Geheimnis oder erstelle ein neues Secrets Manager Geheimnis, um deine Slack-Authentifizierungsdaten zu speichern. Wenn du dich dafür entscheidest, ein neues Geheimnis zu erstellen, öffnet sich ein AWS Secrets Manager geheimes Fenster.

   i. Geben Sie die folgenden Informationen in das Fenster Create an AWS Secrets Manager Secret ein:

      A. Geheimer Name — Ein Name für Ihr Geheimnis. Das Präfix 'AmazonKendra-Slack-' wird deinem geheimen Namen automatisch hinzugefügt.

      B. Für Slack-Token — Gib die Werte für die Authentifizierungsdaten ein, die du in deinem Slack-Account erstellt hast.

   ii. Wählen Sie Speichern.

c. Virtual Private Cloud (VPC) — Sie können wählen, ob Sie eine VPC verwenden möchten. In diesem Fall müssen Sie Subnetze und VPC-Sicherheitsgruppen hinzufügen.

d. Identity Crawler — Geben Sie an, ob der Identity Crawler aktiviert Amazon Kendra werden soll. Der Identity Crawler verwendet die Informationen der Zugriffskontrollliste (ACL) für Ihre Dokumente, um Suchergebnisse nach dem Benutzer- oder Gruppenzugriff auf Dokumente zu filtern. Wenn Sie über eine ACL für Ihre Dokumente verfügen und Ihre ACL verwenden möchten, können Sie auch den Identity Crawler aktivieren, um die Benutzerkontextfilterung von Suchergebnissen zu konfigurieren. Amazon Kendra Andernfalls können alle Dokumente öffentlich durchsucht werden, wenn Identity Crawler ausgeschaltet ist. Wenn Sie die Zugriffskontrolle für Ihre Dokumente verwenden möchten und Identity Crawler ausgeschaltet ist, können Sie alternativ die PutPrincipalMappingAPI verwenden, um Benutzer- und Gruppenzugriffsinformationen für die Benutzerkontextfilterung hochzuladen.

e. IAM Rolle — Wählen Sie eine bestehende IAM Rolle oder erstellen Sie eine neue IAM Rolle, um auf Ihre Repository-Anmeldeinformationen und Indexinhalte zuzugreifen.

> **Note**
>
> IAM Rollen, die für Indizes verwendet werden, können nicht für Datenquellen verwendet werden. Wenn Sie sich nicht sicher sind, ob eine vorhandene Rolle für

einen Index oder eine häufig gestellte Frage verwendet wird, wählen Sie Neue Rolle erstellen, um Fehler zu vermeiden.

f. Wählen Sie Weiter aus.

7. Geben Sie auf der Seite „Synchronisierungseinstellungen konfigurieren“ die folgenden Informationen ein:

a. Wählen Sie den Inhaltstyp aus, der gecrawlt werden soll — Die Slack-Entitäten oder Inhaltstypen, die Sie crawlen möchten. Du kannst zwischen „Alle Channels“, „Öffentliche Channels“, „Private Channels“, „Gruppennachrichten“ und „Private Nachrichten“ wählen.

b. Startdatum des Crawls auswählen — Gib das Datum ein, ab dem deine Amazon Kendra Slack-Inhalte gecrawlt werden sollen.

c. Gib für „Zusätzliche Konfiguration — optional“ die folgenden Informationen ein:

- (Optional) Kanal-ID/Name — Wenn du dich dafür entschieden hast, Inhalte von Kanälen zu synchronisieren, kannst du Inhalte von bestimmten Kanälen zur Synchronisierung hinzufügen, indem du Kanal-IDs und Kanalnamen angibst.
- Nachrichten — Wähle aus, ob Bot-Nachrichten, archivierte Nachrichten oder sowohl Bot-Nachrichten als auch archivierte Nachrichten aufgenommen werden sollen.

> **Note**
>
> Wenn du dich dafür entscheidest, Filter sowohl für die Kanal-ID als auch für den Kanalnamen zu konfigurieren, priorisiert der Amazon Kendra Slack-Connector Kanal-IDs gegenüber Kanalnamen.
> Wenn du dich dafür entscheidest, Filter entweder für die Kanal-ID oder den Kanalnamen zu konfigurieren, ignoriert der Amazon Kendra Slack-Connector private Nachrichten und Gruppennachrichten, selbst wenn du dich dafür entschieden hast, private Nachrichten und Gruppennachrichten im Bereich Sync zu crawlen.

- Regex-Muster — Reguläre Ausdrucksmuster zum Ein- oder Ausschließen bestimmter Dateien. Sie können bis zu 100 Muster hinzufügen. Beispiele für Regex-Muster sind:
  - Dateityp — .pdf, .docx
  - Dateiname — Hallo*.txt,. TestFile *

d. Synchronisierungsmodus — Wählen Sie aus, wie Sie Ihren Index aktualisieren möchten, wenn sich der Inhalt Ihrer Datenquelle ändert. Wenn Sie Ihre Datenquelle Amazon Kendra zum ersten Mal synchronisieren, werden alle Inhalte standardmäßig gecrawlt und indexiert. Sie müssen eine vollständige Synchronisierung Ihrer Daten durchführen, falls Ihre erste Synchronisierung fehlgeschlagen ist, auch wenn Sie die Option Vollsynchronisierung nicht als Synchronisierungsmodusoption wählen.

   - Vollständige Synchronisierung: Indizieren Sie den gesamten Inhalt neu und ersetzen die vorhandenen Inhalte jedes Mal, wenn Ihre Datenquelle mit Ihrem Index synchronisiert wird.
   - Neue, geänderte, gelöschte Synchronisierung: Indizieren Sie bei jeder Synchronisierung Ihrer Datenquelle mit Ihrem Index nur neue, geänderte und gelöschte Inhalte. Amazon Kendra kann den Mechanismus Ihrer Datenquelle verwenden, um Inhaltsänderungen nachzuverfolgen und Inhalte zu indexieren, die sich seit der letzten Synchronisierung geändert haben.

e. Im Synchronisierungslaufplan für Frequenz — Wie oft Amazon Kendra wird mit Ihrer Datenquelle synchronisiert?

f. Wählen Sie Weiter aus.

8. Geben Sie auf der Seite Feldzuordnungen festlegen die folgenden Informationen ein:

   a. Für Feldzuordnungen in Slack — Wählen Sie aus den Amazon Kendra generierten Standard-Datenquellenfeldern aus, die Sie Ihrem Index zuordnen möchten.

   b. Feld hinzufügen — Um benutzerdefinierte Datenquellenfelder hinzuzufügen, um einen Indexfeldnamen für die Zuordnung und den Felddatentyp zu erstellen.

   c. Wählen Sie Weiter aus.

9. Überprüfen Sie auf der Seite Überprüfen und erstellen, ob die von Ihnen eingegebenen Informationen korrekt sind, und wählen Sie dann Datenquelle hinzufügen aus. Sie können Ihre Informationen auch auf dieser Seite bearbeiten. Ihre Datenquelle wird auf der Seite Datenquellen angezeigt, nachdem die Datenquelle erfolgreich hinzugefügt wurde.

API

Um eine Verbindung Amazon Kendra zu Slack herzustellen

Du musst mithilfe der TemplateConfigurationAPI ein JSON des Datenquellenschemas angeben. Sie müssen die folgenden Informationen angeben:

- Datenquelle — Geben Sie den Datenquellentyp wie `SLACK` bei der Verwendung des TemplateConfigurationJSON-Schemas an. Geben Sie außerdem die Datenquelle so an`TEMPLATE`, wie Sie die CreateDataSourceAPI aufrufen.
- Team-ID des Slack-Workspace — Die Slack-Team-ID, die du von der URL deiner Slack-Hauptseite kopiert hast.
- Seit dem Datum — Das Datum, an dem mit dem Crawlen deiner Daten aus deinem Slack-Workspace-Team begonnen werden soll. Das Datum muss diesem Format folgen:. yyyy-mm-dd
- Synchronisierungsmodus — Geben Sie an, wie Ihr Index aktualisiert Amazon Kendra werden soll, wenn sich der Inhalt Ihrer Datenquelle ändert. Wenn Sie Ihre Datenquelle Amazon Kendra zum ersten Mal synchronisieren, werden alle Inhalte standardmäßig gecrawlt und indexiert. Sie müssen eine vollständige Synchronisierung Ihrer Daten durchführen, falls Ihre erste Synchronisierung fehlgeschlagen ist, auch wenn Sie die Option Vollsynchronisierung nicht als Synchronisierungsmodusoption wählen. Sie können wählen zwischen:
  - `FORCED_FULL_CRAWL`um den gesamten Inhalt neu zu indizieren und vorhandene Inhalte jedes Mal zu ersetzen, wenn Ihre Datenquelle mit Ihrem Index synchronisiert wird.
  - `FULL_CRAWL`um bei jeder Synchronisierung Ihrer Datenquelle mit Ihrem Index nur neue, geänderte und gelöschte Inhalte zu indizieren. Amazon Kendra kann den Mechanismus Ihrer Datenquelle verwenden, um Inhaltsänderungen nachzuverfolgen und Inhalte zu indexieren, die sich seit der letzten Synchronisierung geändert haben.
  - `CHANGE_LOG`um jedes Mal, wenn Ihre Datenquelle mit Ihrem Index synchronisiert wird, nur neue und geänderte Inhalte zu indizieren. Amazon Kendra kann den Mechanismus Ihrer Datenquelle verwenden, um Inhaltsänderungen nachzuverfolgen und Inhalte zu indexieren, die sich seit der letzten Synchronisierung geändert haben.
- Identity Crawler — Geben Sie an, ob der Identity Crawler aktiviert Amazon Kendra werden soll. Der Identity Crawler verwendet die Informationen der Zugriffskontrollliste (ACL) für Ihre Dokumente, um Suchergebnisse nach dem Benutzer- oder Gruppenzugriff auf Dokumente zu filtern. Wenn Sie über eine ACL für Ihre Dokumente verfügen und Ihre ACL verwenden möchten, können Sie auch den Identity Crawler aktivieren, um die Benutzerkontextfilterung von Suchergebnissen zu konfigurieren. Amazon Kendra Andernfalls können alle Dokumente öffentlich durchsucht werden, wenn Identity Crawler ausgeschaltet ist. Wenn Sie die Zugriffskontrolle für Ihre Dokumente verwenden möchten und Identity Crawler ausgeschaltet ist, können Sie alternativ die PutPrincipalMappingAPI verwenden, um Benutzer- und Gruppenzugriffsinformationen für die Benutzerkontextfilterung hochzuladen.

- Geheimer Amazon-Ressourcenname (ARN) — Gib den Amazon-Ressourcennamen (ARN) eines Secrets Manager Geheimnisses an, das die Authentifizierungsdaten für dein Slack-Konto enthält. Das Geheimnis wird in einer JSON-Struktur mit den folgenden Schlüsseln gespeichert:

```
{
    "slackToken": "token"
}
```

> **Note**
>
> Wir empfehlen Ihnen, Ihre Anmeldeinformationen und Ihr Geheimnis regelmäßig zu aktualisieren oder zu wechseln. Stellen Sie zu Ihrer eigenen Sicherheit nur die Zugriffsebene bereit, die erforderlich ist. Wir raten davon ab, Anmeldeinformationen und geheime Daten für alle Datenquellen und Connector-Versionen 1.0 und 2.0 (sofern zutreffend) wiederzuverwenden.

- IAM role — Gib an`RoleArn`, wann du anrufst`CreateDataSource`, um einer IAM Rolle Berechtigungen für den Zugriff auf dein Secrets Manager Geheimnis und den Aufruf der erforderlichen öffentlichen APIs für den Slack-Connector und zu erteilen. Amazon Kendra Weitere Informationen findest du unter IAM Rollen für Slack-Datenquellen.

Du kannst auch die folgenden optionalen Funktionen hinzufügen:

- Virtual Private Cloud (VPC) — Geben Sie an, `VpcConfiguration` wann Sie anrufen. `CreateDataSource` Weitere Informationen finden Sie unter Konfigurieren von Amazon Kendra für die Verwendung eines Amazon VPC.
- Spezifische Kanäle — Filtern Sie nach öffentlichen oder privaten Kanälen und geben Sie bestimmte Kanäle anhand ihrer ID an.
- Arten von Kanälen und Nachrichten — Gibt an, ob deine öffentlichen und privaten Kanäle, deine Gruppen- und Direktnachrichten sowie dein Bot und deine archivierten Nachrichten indexiert werden Amazon Kendra sollen. Wenn du ein Bot-Token als Teil deiner Slack-Authentifizierungsdaten verwendest, musst du das Bot-Token dem Kanal hinzufügen, den du indexieren möchtest. Du kannst Direktnachrichten und Gruppennachrichten nicht mit einem Bot-Token indizieren.

- Rückblick — Du kannst einen `lookBack` Parameter so konfigurieren, dass der Slack-Connector aktualisierte oder gelöschte Inhalte bis zu einer bestimmten Anzahl von Stunden vor deiner letzten Connector-Synchronisierung crawlt.
- Inklusions- und Ausschlussfilter — Gib an, ob bestimmte Slack-Inhalte ein- oder ausgeschlossen werden sollen. Wenn du ein Bot-Token als Teil deiner Slack-Authentifizierungsdaten verwendest, musst du das Bot-Token zu dem Channel hinzufügen, den du indexieren möchtest. Du kannst Direktnachrichten und Gruppennachrichten nicht mit einem Bot-Token indizieren.

  > **Note**
  >
  > Die meisten Datenquellen verwenden Muster für reguläre Ausdrücke, bei denen es sich um Ein- oder Ausschlussmuster handelt, die als Filter bezeichnet werden. Wenn Sie einen Einschlussfilter angeben, werden nur Inhalte indexiert, die dem Einschlussfilter entsprechen. Jedes Dokument, das nicht dem Einschlussfilter entspricht, wird nicht indexiert. Wenn Sie einen Ein- und Ausschlussfilter angeben, werden Dokumente, die dem Ausschlussfilter entsprechen, nicht indexiert, auch wenn sie dem Einschlussfilter entsprechen.

- Feldzuordnungen — Wähle, ob du deine Slack-Datenquellenfelder deinen Indexfeldern zuordnen möchtest. Amazon Kendra Weitere Informationen finden Sie unter Zuweisen von Datenquellenfeldern.

  > **Note**
  >
  > Das Textfeld oder das entsprechende Textfeld für deine Dokumente ist erforderlich, um deine Dokumente durchsuchen Amazon Kendra zu können. Sie müssen den Feldnamen Ihres Dokumenthauptteils in Ihrer Datenquelle dem Namen des Indexfeldes zuordnen`_document_body`. Alle anderen Felder sind optional.

Eine Liste weiterer wichtiger JSON-Schlüssel, die konfiguriert werden müssen, finden Sie unter SlackVorlagenschema.

Weitere Informationen

Weitere Informationen zur Integration Amazon Kendra mit deiner Slack-Datenquelle findest du unter:

- Entdecke das Wissen in Slack-Workspaces mit intelligenter Suche mithilfe des Slack-Connectors Amazon Kendra

Zendesk

Zendesk ist ein Kundenbeziehungsmanagementsystem, das Unternehmen dabei unterstützt, Interaktionen mit dem Kundensupport zu automatisieren und zu verbessern. Sie können es verwenden, Amazon Kendra um Ihre Zendesk-Supporttickets, Ticketkommentare, Ticketanhänge, Help-Center-Artikel, Artikelkommentare, Anlagen zu Artikelkommentaren, Leitfadenthemen, Community-Posts und Kommentare zu Community-Posts zu indexieren.

Sie können nach dem Namen der Organisation filtern, wenn Sie Tickets indizieren möchten, die sich nur innerhalb einer bestimmten Organisation befinden. Sie können auch ein Crawldatum festlegen, an dem Sie mit dem Crawlen von Daten aus Zendesk beginnen möchten.

Sie können über Amazon Kendra die Amazon Kendra Konsole und die API eine Verbindung zu Ihrer Zendesk-Datenquelle herstellen. TemplateConfiguration

Informationen zur Fehlerbehebung bei Ihrem Amazon Kendra Zendesk-Datenquellen-Connector finden Sie unter. Problembehandlung bei Datenquellen

Themen

- Unterstützte Features
- Voraussetzungen
- Anweisungen zur Verbindung
- Weitere Informationen

Unterstützte Features

Amazon Kendra Der Zendesk-Datenquellen-Connector unterstützt die folgenden Funktionen:

- Änderungsprotokoll
- Zuordnung von Feldern
- Filterung des Benutzerkontextes
- Einschluss-/Ausschlussfilter
- Virtual Private Cloud (VPC)

Voraussetzungen

Bevor Sie Ihre Zendesk-Datenquelle indizieren können Amazon Kendra , nehmen Sie diese Änderungen in Ihrem Zendesk und Ihren Konten vor. AWS

Stellen Sie in Zendesk sicher, dass Sie über Folgendes verfügen:

- Sie haben ein Administratorkonto für die Zendesk Suite (Professional/Enterprise) erstellt.
- Ich habe Ihre Zendesk-Host-URL notiert. Zum Beispiel *https://{sub-domain (https://{host/)}.zendesk.com/*.

> **Note**
>
> (On-Premise/Server) Amazon Kendra überprüft, ob die in AWS Secrets Manager der Datei enthaltenen Endpunktinformationen mit den Endpunktinformationen übereinstimmen, die in den Konfigurationsdetails Ihrer Datenquelle angegeben sind. Dies trägt zum Schutz vor dem Problem des verwirrten Stellvertreters bei, bei dem es sich um ein Sicherheitsproblem handelt, bei dem ein Benutzer nicht berechtigt ist, eine Aktion auszuführen, sondern ihn Amazon Kendra als Proxy verwendet, um auf das konfigurierte Geheimnis zuzugreifen und die Aktion auszuführen. Wenn Sie Ihre Endpunktinformationen später ändern, müssen Sie ein neues Geheimnis erstellen, um diese Informationen zu synchronisieren.

- Es wurde ein OAuth 2.0-Anmeldeinformationstoken generiert, das eine Client-ID, einen geheimen Clientschlüssel, einen Benutzernamen und ein Passwort enthält. Weitere Informationen finden Sie in der Zendesk-Dokumentation zur Generierung von OAuth 2.0-Token.
- Der folgende OAuth 2.0-Bereich wurde hinzugefügt:
  - read
- Optional: Es wurde ein SSL-Zertifikat installiert, um eine Verbindung herzustellen Amazon Kendra .
- Aktiviert, dass jedes Dokument in Zendesk und in anderen Datenquellen, die Sie für denselben Index verwenden möchten, einzigartig ist. Jede Datenquelle, die Sie für einen Index verwenden möchten, darf nicht dasselbe Dokument in allen Datenquellen enthalten. Dokument-IDs gelten für einen Index global und müssen pro Index eindeutig sein.

Stellen Sie sicher AWS-Konto, dass Sie Folgendes in Ihrem haben:

- Hat einen Amazon Kendra Index erstellt und bei Verwendung der API die Index-ID notiert.

- Sie haben eine IAM Rolle für Ihre Datenquelle erstellt und, falls Sie die API verwenden, den ARN der IAM Rolle notiert.

> **Note**
>
> Wenn Sie Ihren Authentifizierungstyp und Ihre Anmeldeinformationen ändern, müssen Sie Ihre IAM Rolle aktualisieren, um auf die richtige AWS Secrets Manager geheime ID zugreifen zu können.

- Sie haben Ihre Zendesk-Authentifizierungsdaten AWS Secrets Manager geheim gespeichert und, falls Sie die API verwenden, den ARN des Geheimnisses notiert.

> **Note**
>
> Wir empfehlen Ihnen, Ihre Anmeldeinformationen und Ihr Geheimnis regelmäßig zu aktualisieren oder zu wechseln. Stellen Sie zu Ihrer eigenen Sicherheit nur die Zugriffsebene bereit, die erforderlich ist. Wir raten davon ab, Anmeldeinformationen und geheime Daten für alle Datenquellen und Connector-Versionen 1.0 und 2.0 (sofern zutreffend) wiederzuverwenden.

Wenn Sie noch keine IAM Rolle oder keinen Schlüssel haben, können Sie die Konsole verwenden, um eine neue IAM Rolle und ein neues Secrets Manager Geheimnis zu erstellen, wenn Sie Ihre Zendesk-Datenquelle mit verbinden. Amazon Kendra Wenn Sie die API verwenden, müssen Sie den ARN einer vorhandenen IAM Rolle und eines Secrets Manager Geheimnisses sowie eine Index-ID angeben.

Anweisungen zur Verbindung

Um eine Verbindung Amazon Kendra zu Ihrer Zendesk-Datenquelle herzustellen, müssen Sie die erforderlichen Details zu Ihrer Zendesk-Datenquelle angeben, damit Sie auf Ihre Daten zugreifen Amazon Kendra können. Wenn Sie Zendesk noch nicht für Amazon Kendra konfiguriert haben, finden Sie weitere Informationen unter. Voraussetzungen

Console

So stellen Sie eine Verbindung Amazon Kendra zu Zendesk her

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die Amazon Kendra Konsole.
2. Wählen Sie im linken Navigationsbereich Indizes und dann den Index, den Sie verwenden möchten, aus der Indexliste aus.

> **Note**
>
> Sie können Ihre Einstellungen für die Benutzerzugriffskontrolle unter Indexeinstellungen konfigurieren oder bearbeiten.

3. Wählen Sie auf der Seite Erste Schritte die Option Datenquelle hinzufügen aus.
4. Wählen Sie auf der Seite Datenquelle hinzufügen die Option Zendesk-Connector und dann Connector hinzufügen aus.
5. Geben Sie auf der Seite „Datenquellendetails angeben“ die folgenden Informationen ein:
   a. Geben Sie im Feld Name und Beschreibung für Datenquellenname einen Namen für Ihre Datenquelle ein. Sie können Bindestriche, aber keine Leerzeichen verwenden.
   b. (Optional) Beschreibung — Geben Sie eine optionale Beschreibung für Ihre Datenquelle ein.
   c. In Standardsprache — Wählen Sie eine Sprache aus, um Ihre Dokumente nach dem Index zu filtern. Sofern Sie nichts anderes angeben, ist die Standardsprache Englisch. Die in den Metadaten des Dokuments angegebene Sprache hat Vorrang vor der ausgewählten Sprache.
   d. Unter Tags für Neues Tag hinzufügen — Fügen Sie optionale Tags hinzu, um Ihre Ressourcen zu durchsuchen und zu filtern oder Ihre Kosten nachzuverfolgen. AWS
   e. Wählen Sie Weiter aus.
6. Geben Sie auf der Seite Zugriff und Sicherheit definieren die folgenden Informationen ein:
   a. Zendesk-URL — Geben Sie Ihre Zendesk-URL ein.
   b. AWS Secrets Manager geheim — Wählen Sie ein vorhandenes Geheimnis oder erstellen Sie ein neues Secrets Manager Geheimnis, um Ihre Zendesk-Authentifizierungsdaten zu speichern. Wenn Sie ein neues Geheimnis erstellen möchten, wird ein AWS Secrets Manager geheimes Fenster geöffnet.
      i. Geben Sie die folgenden Informationen in das Fenster Create an AWS Secrets Manager Secret ein:

A. Geheimer Name — Ein Name für Ihr Geheimnis. Das Präfix 'AmazonKendra-Zendesk' wird Ihrem geheimen Namen automatisch hinzugefügt.

B. Für Kunden-ID, Kundengeheimnis, Benutzername und Passwort — Geben Sie die Werte für die Authentifizierungsdaten ein, die Sie in Ihrem Zendesk-Konto erstellt haben.

ii. Wählen Sie Speichern.

c. Virtual Private Cloud (VPC) — Sie können wählen, ob Sie eine VPC verwenden möchten. In diesem Fall müssen Sie Subnetze und VPC-Sicherheitsgruppen hinzufügen.

d. IAM Rolle — Wählen Sie eine bestehende IAM Rolle oder erstellen Sie eine neue IAM Rolle, um auf Ihre Repository-Anmeldeinformationen und Indexinhalte zuzugreifen.

> **Note**
>
> IAM Rollen, die für Indizes verwendet werden, können nicht für Datenquellen verwendet werden. Wenn Sie sich nicht sicher sind, ob eine vorhandene Rolle für einen Index oder eine häufig gestellte Frage verwendet wird, wählen Sie Neue Rolle erstellen, um Fehler zu vermeiden.

e. Wählen Sie Weiter aus.

7. Geben Sie auf der Seite „Synchronisierungseinstellungen konfigurieren“ die folgenden Informationen ein:

a. Wählen Sie Entitäten oder Inhaltstypen aus — Die Zendesk-Entitäten oder Inhaltstypen, die Sie crawlen möchten.

b. Änderungsprotokoll — Wählen Sie diese Option, um Ihren Index nur mit neuen und geänderten Inhalten zu aktualisieren, anstatt alle Ihre Dateien zu synchronisieren.

c. Name der Organisation — Geben Sie die Namen der Zendesk-Organisation ein, um Ihre Synchronisierung zu filtern.

d. Startdatum der Synchronisierung — Das Datum, ab dem Sie Ihre Inhalte indexieren möchten.

e. Regex-Muster — Reguläre Ausdrucksmuster zum Ein- oder Ausschließen bestimmter Dateien. Sie können bis zu 100 Muster hinzufügen.

f. Zeitplan für Synchronisierungsläufe für Häufigkeit — Wählen Sie aus, wie oft Amazon Kendra die Synchronisierung mit Ihrer Datenquelle erfolgen soll.

g. Wählen Sie Weiter aus.

8. Geben Sie auf der Seite Feldzuordnungen festlegen die folgenden Informationen ein:

   a. Für Tickets, Ticketkommentar, Ticketkommentar-Anlage, Artikel, Artikelkommentar, Anlage zu Artikelkommentaren, Community-Thema, Community-Beitrag, Community-Kommentar — Wählen Sie aus den Amazon Kendra generierten Standard-Datenquellenfeldern, die Sie Ihrem Index zuordnen möchten.

   b. Feld hinzufügen — Um benutzerdefinierte Datenquellenfelder hinzuzufügen, um einen Indexfeldnamen für die Zuordnung und den Felddatentyp zu erstellen.

   c. Wählen Sie Weiter aus.

9. Überprüfen Sie auf der Seite Überprüfen und erstellen, ob die von Ihnen eingegebenen Informationen korrekt sind, und wählen Sie dann Datenquelle hinzufügen aus. Sie können Ihre Informationen auch auf dieser Seite bearbeiten. Ihre Datenquelle wird auf der Seite Datenquellen angezeigt, nachdem die Datenquelle erfolgreich hinzugefügt wurde.

API

Um eine Verbindung Amazon Kendra zu Zendesk herzustellen

Sie müssen mithilfe der TemplateConfigurationAPI ein JSON des Datenquellenschemas angeben. Sie müssen die folgenden Informationen angeben:

- Datenquelle — Geben Sie den Datenquellentyp wie `ZENDESK` bei der Verwendung des TemplateConfigurationJSON-Schemas an. Geben Sie außerdem die Datenquelle so an`TEMPLATE`, wie Sie die CreateDataSourceAPI aufrufen.
- Host-URL — Geben Sie Ihre Zendesk-Host-URL als Teil der Verbindungskonfiguration oder der Repository-Endpunktdetails an. *Zum Beispiel https://yoursubdomain.zendesk.com.*
- Änderungsprotokoll — Gibt an, ob der Änderungsprotokollmechanismus der Zendesk-Datenquelle verwendet werden Amazon Kendra soll, um festzustellen, ob ein Dokument im Index aktualisiert werden muss.

> **Note**
>
> Verwenden Sie das Änderungsprotokoll, wenn Sie nicht alle Dokumente scannen Amazon Kendra möchten. Wenn Ihr Änderungsprotokoll umfangreich ist, dauert das Scannen der Dokumente in der Zendesk-Datenquelle möglicherweise Amazon Kendra weniger Zeit als das Verarbeiten des Änderungsprotokolls. Wenn Sie Ihre Zendesk-

Datenquelle zum ersten Mal mit Ihrem Index synchronisieren, werden alle Dokumente gescannt.

- Geheimer Amazon-Ressourcenname (ARN) — Geben Sie den Amazon-Ressourcennamen (ARN) eines Secrets Manager Geheimnisses ein, das die Authentifizierungsdaten für Ihr Zendesk-Konto enthält. Das Geheimnis wird in einer JSON-Struktur mit den folgenden Schlüsseln gespeichert:

```
{
    "hostUrl": "https://yoursubdomain.zendesk.com",
    "clientId": "client ID",
    "clientSecret": "Zendesk client secret",
    "userName": "Zendesk user name",
    "password": "Zendesk password"
}
```

> **Note**
>
> Wir empfehlen Ihnen, Ihre Anmeldeinformationen und Ihr Geheimnis regelmäßig zu aktualisieren oder zu wechseln. Stellen Sie zu Ihrer eigenen Sicherheit nur die Zugriffsebene bereit, die erforderlich ist. Wir raten davon ab, Anmeldeinformationen und geheime Daten für alle Datenquellen und Connector-Versionen 1.0 und 2.0 (sofern zutreffend) wiederzuverwenden.

- IAM Rolle — Geben Sie an`RoleArn`, wann Sie anrufen`CreateDataSource`, um einer IAM Rolle Berechtigungen für den Zugriff auf Ihr Secrets Manager Geheimnis und für den Aufruf der erforderlichen öffentlichen APIs für den Zendesk-Connector und zum Aufrufen der erforderlichen öffentlichen APIs zu erteilen. Amazon Kendra Weitere Informationen finden Sie unter IAM Rollen für Zendesk-Datenquellen.

Sie können auch die folgenden optionalen Funktionen hinzufügen:

- Virtual Private Cloud (VPC) — Geben Sie an, `VpcConfiguration` wann Sie anrufen. `CreateDataSource` Weitere Informationen finden Sie unter Konfigurieren von Amazon Kendra für die Verwendung eines Amazon VPC.
- Inklusions- und Ausschlussfilter — Geben Sie an, ob Folgendes ein- oder ausgeschlossen werden soll:

- Supporttickets, Ticketkommentare und/oder Ticketkommentaranhänge
- Help-Center-Artikel, Artikelanhänge und Artikelkommentare
- Leitfäden für Community-Themen, Beiträge oder Kommentare

> **Note**
>
> Die meisten Datenquellen verwenden Muster für reguläre Ausdrücke, bei denen es sich um Ein- oder Ausschlussmuster handelt, die als Filter bezeichnet werden. Wenn Sie einen Einschlussfilter angeben, werden nur Inhalte indexiert, die dem Einschlussfilter entsprechen. Jedes Dokument, das nicht dem Einschlussfilter entspricht, wird nicht indexiert. Wenn Sie einen Ein- und Ausschlussfilter angeben, werden Dokumente, die dem Ausschlussfilter entsprechen, nicht indexiert, auch wenn sie dem Einschlussfilter entsprechen.

- Benutzerkontextfilterung und Zugriffskontrolle —Amazon Kendra durchsucht die Zugriffskontrollliste (ACL) für Ihre Dokumente, sofern Sie über eine ACL für Ihre Dokumente verfügen. Die ACL-Informationen werden verwendet, um Suchergebnisse nach dem Benutzer- oder Gruppenzugriff auf Dokumente zu filtern. Weitere Informationen finden Sie unter Benutzerkontextfilterung.
- Feldzuordnungen — Wählen Sie diese Option, um Ihre Zendesk-Datenquellenfelder Ihren Indexfeldern zuzuordnen. Amazon Kendra Weitere Informationen finden Sie unter Zuweisen von Datenquellenfeldern.

> **Note**
>
> Das Textfeld oder das entsprechende Textfeld für Ihre Dokumente ist erforderlich, um Ihre Dokumente durchsuchen Amazon Kendra zu können. Sie müssen den Feldnamen Ihres Dokumenthauptteils in Ihrer Datenquelle dem Namen des Indexfeldes zuordnen`_document_body`. Alle anderen Felder sind optional.

Eine Liste weiterer wichtiger JSON-Schlüssel, die konfiguriert werden müssen, finden Sie unterZendesk-Vorlagenschema.

Weitere Informationen

Weitere Informationen zur Integration Amazon Kendra mit Ihrer Zendesk-Datenquelle finden Sie unter:

- Entdecken Sie mit Amazon Kendra der intelligenten Suche Erkenntnisse von Zendesk

Zuordnen von Datenquellenfeldern

Amazon Kendra -Datenquellen-Konnektoren können Dokument- oder Inhaltsfelder aus Ihrer Datenquelle Feldern in Ihrem Amazon Kendra Index zuordnen. Standardmäßig ist jeder Konnektor so konzipiert, dass er bestimmte Datenquellenfelder crawlt. Standarddatenquellenfelder und ihre Eigenschaften können nicht geändert oder angepasst werden. In der Amazon Kendra Konsole sind Standardfelder und Standardfeldeigenschaften, die nicht bearbeitet werden können, ausgegraut.

Amazon Kendra Mit -Konnektoren können Sie auch benutzerdefinierte Dokument- oder Inhaltsfelder aus Ihrer Datenquelle benutzerdefinierten Feldern in Ihrem Index zuordnen. Wenn Sie beispielsweise ein Feld in Ihrer Datenquelle namens „dept“ haben, das Abteilungsinformationen für ein Dokument enthält, können Sie es einem Indexfeld namens „Department“ zuordnen. Auf diese Weise können Sie das Feld beim Abfragen von Dokumenten verwenden.

Sie können auch Amazon Kendra reservierte oder allgemeine Felder wie zuordnen`_created_at`. Wenn Ihre Datenquelle über ein Feld namens „creation_date“ verfügt, können Sie dieses dem entsprechenden Amazon Kendra reservierten Feld namens zuordnen`_created_at`. Weitere Informationen zu Amazon Kendra reservierten Feldern finden Sie unter Dokumentattribute oder Felder .

Sie können Felder für die meisten Datenquellen zuordnen. Sie können Feldzuordnungen für die folgenden Datenquellen erstellen:

- Adobe Experience Manager
- Alfresien
- Aurora (MySQL)
- Aurora (PostgreSQL)
- Amazon FSx (Windows)
- Amazon FSx (NetApp ONTAP)
- Amazon RDS/Aurora

- Amazon RDS (Microsoft SQL Server)
- Amazon RDS (MySQL)
- Amazon RDS (Oracle)
- Amazon RDS (PostgreSQL)
- Amazon Kendra Web-Crawler
- Amazon WorkDocs
- Box (Kasten)
- Confluence
- Dropbox
- Drupal
- GitHub
- Google Workspace-Laufwerke
- Gmail
- IBM DB2
- Jira
- Microsoft Exchange
- Microsoft OneDrive
- Microsoft SharePoint
- Microsoft Teams
- Microsoft SQL Server
- Microsoft Yammer
- MySQL
- Oracle Database
- PostgreSQL
- Warteschlange
- Salesforce
- ServiceNow
- Slack
- Zendesk

Wenn Sie Ihre Dokumente in einem S3-Bucket oder einer S3-Datenquelle speichern, geben Sie Ihre Felder mithilfe einer JSON-Metadatendatei an. Weitere Informationen finden Sie unter S3-Datenquellen-Konnektor.

Die Zuordnung Ihrer Datenquellenfelder zu einem Indexfeld ist ein dreistufiger Prozess:

1. Erstellen Sie einen Index. Weitere Informationen finden Sie unter Erstellen eines Index.
2. Aktualisieren Sie den Index, um Felder hinzuzufügen.
3. Erstellen Sie eine Datenquelle und schließen Sie Feldzuordnungen ein, um reservierte Felder und alle benutzerdefinierten Felder Amazon Kendra Indexfeldern zuzuordnen.

Um den Index zum Hinzufügen benutzerdefinierter Felder zu aktualisieren, verwenden Sie die Konsole, um die Datenquellenfeldzuordnungen zu bearbeiten und ein benutzerdefiniertes Feld hinzuzufügen oder die UpdateIndex API zu verwenden. Sie können Ihrem Index insgesamt 500 benutzerdefinierte Felder hinzufügen.

Wenn bei Datenbankdatenquellen der Name der Datenbankspalte mit dem Namen eines reservierten Felds übereinstimmt, werden das Feld und die Spalte automatisch zugeordnet.

Mit der UpdateIndex API fügen Sie reservierte und benutzerdefinierte Felder mit hinzu`DocumentMetadataConfigurationUpdates`.

Im folgenden JSON-Beispiel wird verwendet`DocumentMetadataConfigurationUpdates`, um dem Index ein Feld namens „Abteilung“ hinzuzufügen.

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

Wenn Sie das Feld erstellen, haben Sie die Möglichkeit festzulegen, wie das Feld für die Suche verwendet wird. Sie können aus den folgenden Optionen auswählen:

- Anzeigbar – Bestimmt, ob das Feld in der Abfrageantwort zurückgegeben wird. Der Standardwert ist `true`.
- Facetable – Zeigt an, dass das Feld zum Erstellen von Facetten verwendet werden kann. Der Standardwert ist `false`.

- Durchsuchbar – Bestimmt, ob das Feld bei der Suche verwendet wird. Die Standardeinstellung bei Zeichenfolgenfeldern ist `true` und bei Zahlen- und Datumsfeldern `false`.
- Sortierbar – Zeigt an, dass das Feld verwendet werden kann, um die Antwort aus einer Abfrage zu sortieren. Kann nur für Datums-, Zahlen- und Zeichenfolgenfelder festgelegt werden. Kann nicht für Zeichenfolgenlistenfelder festgelegt werden.

Im folgenden JSON-Beispiel wird verwendet`DocumentMetadataConfigurationUpdates`, um dem Index ein Feld mit dem Namen „Abteilung“ hinzuzufügen und es als Facetable zu markieren.

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

Verwenden von Amazon Kendra reservierten oder gemeinsamen Dokumentfeldern

Mit der UpdateIndex API können Sie reservierte oder allgemeine Felder erstellen, indem Sie den Amazon Kendra reservierten Indexfeldnamen verwenden `DocumentMetadataConfigurationUpdates` und angeben, der Ihrem entsprechenden Dokumentattribut/Feldnamen zugeordnet werden soll. Sie können auch benutzerdefinierte Felder erstellen. Wenn Sie einen Datenquellen-Konnektor verwenden, enthalten die meisten Feldzuordnungen, die Ihre Datenquellendokumentfelder Amazon Kendra Indexfeldern zuordnen. Wenn Sie die Konsole verwenden, aktualisieren Sie Felder, indem Sie Ihre Datenquelle auswählen, die Bearbeitungsaktion auswählen und dann neben dem Abschnitt Feldzuordnungen zur Konfiguration der Datenquelle fortfahren.

Sie können das -`Search`Objekt so konfigurieren, dass ein Feld entweder als anzeigbar, facettbar, durchsuchbar und sortierbar festgelegt wird. Sie können das -`Relevance`Objekt so konfigurieren, dass die Rangfolge, die Boost-Dauer oder der Zeitraum eines Feldes festgelegt werden, die auf Boosting-, Aktualitäts-, Wichtigkeitswert- und Wichtigkeitswerte angewendet werden, die bestimmten Feldwerten zugeordnet sind. Wenn Sie die Konsole verwenden, können Sie die Sucheinstellungen für ein Feld festlegen, indem Sie die Facettenoption im Navigationsmenü auswählen. Um die

Relevanzoptimierung festzulegen, wählen Sie die Option aus, um Ihren Index im Navigationsmenü zu durchsuchen, geben Sie eine Abfrage ein und verwenden Sie die Seitenbereichsoptionen, um die Suchrelevanz zu optimieren. Sie können den Feldtyp nicht mehr ändern, nachdem Sie das Feld erstellt haben.

Amazon Kendra verfügt über die folgenden reservierten oder allgemeinen Dokumentfelder, die Sie verwenden können:

- `_authors`– Eine Liste mit einem oder mehreren Autoren, die für den Inhalt des Dokuments verantwortlich sind.
- `_category`– Eine Kategorie, die ein Dokument in einer bestimmten Gruppe ablegt.
- `_created_at`– Das Datum und die Uhrzeit im ISO 8601-Format, zu der das Dokument erstellt wurde. Beispiel: 2012-03-25T12:30:10+01:00 ist das ISO-8601-Datums-/Uhrzeitformat für den 25. März 2012 um 12:30 Uhr (plus 10 Sekunden) in mitteleuropäischer Zeit (CET).
- `_data_source_id`– Die Kennung der Datenquelle, die das Dokument enthält.
- `_document_body`– Der Inhalt des Dokuments.
- `_document_id`– Eine eindeutige Kennung für das Dokument.
- `_document_title`– Der Titel des Dokuments.
- `_excerpt_page_number`– Die Seitennummer in einer PDF-Datei, in der der Dokumentauszug angezeigt wird. Wenn Ihr Index vor dem 8. September 2020 erstellt wurde, müssen Sie Ihre Dokumente neu indizieren, bevor Sie dieses Attribut verwenden können.
- `_faq_id`– Wenn es sich um ein Frage-Antwort-Dokument (FAQ) handelt, eine eindeutige Kennung für die häufig gestellten Fragen.
- `_file_type`– Der Dateityp des Dokuments, z. B. PDF oder Dokument.
- `_last_updated_at`– Das Datum und die Uhrzeit im ISO 8601-Format, zu der das Dokument zuletzt aktualisiert wurde. Beispiel: 2012-03-25T12:30:10+01:00 ist das ISO-8601-Datums-/Uhrzeitformat für den 25. März 2012 um 12:30 Uhr (plus 10 Sekunden) in mitteleuropäischer Zeit (CET).
- `_source_uri`– Die URI, in der das Dokument verfügbar ist. Zum Beispiel die URI des Dokuments auf einer Unternehmenswebsite.
- `_version`– Eine Kennung für die spezifische Version eines Dokuments.
- `_view_count`– Gibt an, wie oft das Dokument angezeigt wurde.
- `_language_code` (Zeichenfolge) – Der Code für eine Sprache, die für das Dokument gilt. Dies ist standardmäßig Englisch, wenn Sie keine Sprache angeben. Weitere Informationen zu unterstützten

Sprachen, einschließlich ihrer Codes, finden Sie unter Hinzufügen von Dokumenten in anderen Sprachen als Englisch.

Bei benutzerdefinierten Feldern erstellen Sie diese Felder mit `DocumentMetadataConfigurationUpdates` mit mit der `UpdateIndex` -API, genau wie beim Erstellen eines reservierten oder allgemeinen Felds. Sie müssen den entsprechenden Datentyp für Ihr benutzerdefiniertes Feld festlegen. Wenn Sie die Konsole verwenden, aktualisieren Sie Felder, indem Sie Ihre Datenquelle auswählen, die Bearbeitungsaktion auswählen und dann neben dem Abschnitt Feldzuordnungen zur Konfiguration der Datenquelle fortfahren. Einige Datenquellen unterstützen das Hinzufügen neuer Felder oder benutzerdefinierter Felder nicht. Sie können den Feldtyp nicht mehr ändern, nachdem Sie das Feld erstellt haben.

Die folgenden Typen können Sie für benutzerdefinierte Felder festlegen:

- Datum
- Zahl
- String
- Zeichenfolgenliste

Wenn Sie dem Index mithilfe der BatchPutDocument API Dokumente hinzugefügt haben, `Attributes` listet die Felder/Attribute Ihrer Dokumente auf und Sie erstellen Felder mithilfe des -`DocumentAttribute`Objekts.

Für Dokumente, die aus einer Amazon S3 -Datenquelle indiziert wurden, erstellen Sie Felder mit einer JSON-Metadatendatei, die die Feldinformationen enthält.

Wenn Sie eine unterstützte Datenbank als Datenquelle verwenden, können Sie Ihre Felder mit der Feldzuordnungsoption konfigurieren.

Hinzufügen von Dokumenten in anderen Sprachen als Englisch

Sie können Dokumente in mehreren Sprachen indizieren. Wenn Sie keine Sprache angeben, Amazon Kendra indiziert Dokumente standardmäßig in englischer Sprache. Sie fügen den Sprachcode für ein Dokument in die Dokumentmetadaten als Feld ein. Weitere Informationen zum `_language_code` Feld für ein Dokument finden Sie unter Feldzuordnungen und Benutzerdefinierte Attribute.

Sie können den Sprachcode für alle Ihre Dokumente in Ihrer Datenquelle angeben, wenn Sie aufrufenCreateDataSource. Wenn für ein Dokument kein Sprachcode in einem Metadatenfeld angegeben ist, wird das Dokument mit dem Sprachcode indiziert, der für alle Dokumente auf Datenquellenebene angegeben ist. In der Konsole können Sie Dokumente in einer unterstützten Sprache nur auf Datenquellenebene indizieren. Gehen Sie zu Datenquellen, dann zur Seite Datenquellendetails angeben und wählen Sie eine Sprache aus der Dropdown-Liste Sprache aus.

Sie können Dokumente auch in einer unterstützten Sprache suchen oder abfragen. Weitere Informationen finden Sie unter Suchen in Sprachen.

Die folgenden Sprachen und ihre Codes werden unterstützt (Englisch oder `en` wird standardmäßig unterstützt, wenn Sie keine Sprache angeben). Diese Tabelle enthält Sprachen, die bei vollständiger semantischer Suche Amazon Kendra unterstützt, sowie Sprachen, die nur einen einfachen Schlüsselwortabgleich unterstützen. Sprachen, die eine vollständige semantische Suche unterstützen, sind in der folgenden Tabelle mit einem Sternchen gekennzeichnet und sind fett gedruckt. Englisch (Standardsprache) wird auch bei vollständiger semantischer Suche unterstützt.

Sprachname	Sprachcode
Arabisch	`ar`
Armenisch	`hy`
Baskisch	`eu`
Bengalisch	`bn`
Bulgarisch	`bg`
Katalanisch	`ca`
Chinesisch – vereinfacht und traditionell*	`zh`
Tschechisch	`cs`
Dänisch	`da`
Niederländisch	`nl`
Finnisch	`fi`

Sprachname	Sprachcode
Französisch – enthält Französisch (Kanada)*	fr
Galizisch	gl
Deutsch*	de
Griechisch	el
Hindi	hi
Ungarisch	hu
Indonesisch	id
Trichter	ga
Italienisch	it
Japanisch*	ja
Koreanisch*	ko
Lettisch	lv
Litauisch	lt
Norwegisch	no
Persisch	fa
Portugiesisch	pt
Portugiesisch (Brasilien)*	pt-BR
Rumänisch	ro
Russisch	ru
Sorani	ckb

Sprachname	Sprachcode
Spanisch – umfasst Spanisch (Mexiko)*	`es`
Schwedisch	`sv`
Türkisch	`tr`

*Semantische Suche wird für die Sprache unterstützt.

Für Sprachen, die die semantische Suche unterstützen, werden die folgenden Funktionen unterstützt.

- Dokumentrelevanz über den einfachen Schlüsselwortabgleich hinaus.
- Häufig FAQs über den einfachen Schlüsselwortabgleich hinaus.
- Extrahieren von Antworten aus Dokumenten basierend auf dem Leseverstehen Amazon Kendravon .
- Konfidenz-Buckets (sehr hoch, hoch, mittel und niedrig) der Suchergebnisse.

Für Sprachen, die die semantische Suche nicht unterstützen, wird ein einfacher Schlüsselwortabgleich für die Dokumentrelevanz und häufig FAQs unterstützt.

Synonyme (einschließlich benutzerdefinierter Synonyme), inkrementelles Lernen und Feedback sowie Abfragevorschläge werden nur für Englisch (Standardsprache) unterstützt.

Konfigurieren von Amazon Kendra für die Verwendung eines Amazon VPC

Amazon Kendra kann eine Verbindung zu einer Virtual Private Cloud (VPC) herstellen, die Sie mit erstellt haben, Amazon Virtual Private Cloud um Inhalte zu indizieren, die in Datenquellen gespeichert sind, die in Ihrer privaten Cloud ausgeführt werden. Wenn Sie einen Datenquellen-Connector erstellen, können Sie Sicherheitsgruppen- und Subnetz-IDs für das Subnetz angeben, das Ihre Datenquelle enthält. Mit diesen Informationen Amazon Kendra erstellt eine Elastic Network-Schnittstelle, die für die sichere Kommunikation mit Ihrer Datenquelle innerhalb Ihrer VPC verwendet wird.

Um einen Amazon Kendra Datenquellen-Connector mit einzurichten Amazon VPC, können Sie entweder die - AWS Management Console oder die CreateDataSource-API-Operation verwenden.

Wenn Sie die Konsole verwenden, verbinden Sie während des Konnektor-Konfigurationsprozesses eine VPC.

> **Note**
>
> Die Amazon VPC Funktion ist beim Einrichten eines Amazon Kendra Datenquellen-Connectors optional. Wenn Ihre Datenquelle über das öffentliche Internet zugänglich ist, müssen Sie die Amazon VPC Funktion nicht aktivieren. Nicht alle Amazon Kendra Datenquellen-Connectors unterstützen Amazon VPC.

Wenn Ihre Datenquelle nicht auf ausgeführt wird Amazon VPC und nicht über das öffentliche Internet zugänglich ist, verbinden Sie Ihre Datenquelle zunächst über ein Virtual Private Network (VPN) mit Ihrer VPC. Anschließend können Sie Ihre Datenquelle mit verbinden, Amazon Kendra indem Sie eine Kombination aus Amazon VPC und verwenden AWS Virtual Private Network. Weitere Informationen zum Einrichten eines VPN finden Sie in der AWS VPN -Dokumentation.

Themen

- Konfigurieren der Amazon VPC Unterstützung für Amazon Kendra Konnektoren
- Einrichten einer - Amazon Kendra Datenquelle für die Verbindung mit Amazon VPC
- Herstellen einer Verbindung mit einer Datenbank in einer VPC
- Fehlerbehebung bei VPC-Verbindungsproblemen

Konfigurieren der Amazon VPC Unterstützung für Amazon Kendra Konnektoren

Führen Sie die folgenden Schritte aus, um Amazon VPC für die Verwendung mit Ihren Amazon Kendra Konnektoren zu konfigurieren.

Schritte

- Schritt 1. Erstellen von Amazon VPC Subnetzen für Amazon Kendra
- Schritt 2. Erstellen von Amazon VPC Sicherheitsgruppen für Amazon Kendra
- Schritt 3. Konfigurieren Ihrer externen Datenquelle und Amazon VPC

Schritt 1. Erstellen von Amazon VPC Subnetzen für Amazon Kendra

Erstellen oder wählen Sie ein vorhandenes Amazon VPC Subnetz aus, Amazon Kendra das für den Zugriff auf Ihre Datenquelle verwenden kann. Die vorbereiteten Subnetze müssen sich in einer der folgenden Availability Zones AWS-Regionen und befinden:

- USA West (Oregon)/us-west-2 –usw2-az1, usw2-az2, usw2-az3
- USA Ost (Nord-Virginia)/us-east-1 – use1-az1, use1-az2, use1-az4
- USA Ost (Ohio)/us-east-2 – use2-az1, use2-az2, use2-az3
- Asien-Pazifik (Tokio)/ap-northeast-1 – ane1-az1, apne1-az2, apne1-az4
- Asien-Pazifik (Mumbai)/ap-south-1 –aps1-az1, aps1-az2, aps1-az3
- Asien-Pazifik (Singapur)/ap-southeast-1 –apse1-az1, apse1-az2, apse1-az3
- Asien-Pazifik (Sydney)/ap-southeast-2 –apse2-az1, apse2-az2, apse2-az3
- Kanada (Zentral)/ca-central-1—cac1-az1, cac1-az2, cac1-az4
- Europa (Irland)/eu-west-1 – euw1-az1, uew1-az2, euw1-az3
- Europa (London)/eu-west-2 –usw2-az1, usw2-az2, usw2-az3

Ihre Datenquelle muss von den Subnetzen aus zugänglich sein, die Sie dem Amazon Kendra Konnektor zur Verfügung gestellt haben.

Weitere Informationen zum Konfigurieren von Amazon VPC Subnetzen finden Sie unter Subnetze für Ihr Amazon VPC im Amazon-VPC-Benutzerhandbuch.

Wenn die Verbindung zwischen zwei oder mehr Subnetzen weiterleiten Amazon Kendra muss, können Sie mehrere Subnetze vorbereiten. Beispielsweise hat das Subnetz, das Ihre Datenquelle enthält, keine IP-Adressen mehr. In diesem Fall können Sie ein zusätzliches Subnetz Amazon Kendra bereitstellen, das über genügend IP-Adressen verfügt und mit dem ersten Subnetz verbunden ist. Wenn Sie mehrere Subnetze auflisten, müssen die Subnetze miteinander kommunizieren können.

Schritt 2. Erstellen von Amazon VPC Sicherheitsgruppen für Amazon Kendra

Um Ihren Amazon Kendra Datenquellen-Connector mit zu verbinden Amazon VPC, müssen Sie eine oder mehrere Sicherheitsgruppen aus Ihrer VPC vorbereiten, die Sie zuweisen möchten Amazon Kendra. Die Sicherheitsgruppen werden der von erstellten Elastic-Network-Schnittstelle zugeordnet Amazon Kendra. Diese Netzwerkschnittstelle steuert den ein- und ausgehenden Datenverkehr zu und von Amazon Kendra beim Zugriff auf die Amazon VPC Subnetze.

Stellen Sie sicher, dass die Regeln für ausgehenden Datenverkehr Ihrer Sicherheitsgruppe dem Datenverkehr von Amazon Kendra Datenquellen-Connectors den Zugriff auf die Subnetze und die Datenquelle erlauben, mit der Sie synchronisieren möchten. Sie können beispielsweise einen -MySQLKonnektor verwenden, um aus einer MySQL Datenbank zu synchronisieren. Wenn Sie den Standardport verwenden, müssen die Sicherheitsgruppen den Zugriff Amazon Kendra auf Port 3306 auf dem Host zulassen, auf dem die Datenbank ausgeführt wird.

Wir empfehlen Ihnen, eine Standardsicherheitsgruppe mit den folgenden Werten Amazon Kendra zu konfigurieren, die verwenden soll:

- Regeln für eingehenden Datenverkehr – Wenn Sie dies leer lassen, wird der gesamte eingehende Datenverkehr blockiert.
- Regeln für ausgehenden Datenverkehr – Fügen Sie eine Regel hinzu, um den gesamten ausgehenden Datenverkehr zuzulassen, damit die Anforderungen zur Synchronisierung von Ihrer Datenquelle aus initiieren Amazon Kendra kann.
  - IP-Version – IPv4
  - Typ – Gesamter Datenverkehr
  - Protokoll – Der gesamte Datenverkehr
  - Portbereich – Alle
  - Ziel – 0.0.0.0/0

Weitere Informationen zum Konfigurieren von Amazon VPC Sicherheitsgruppen finden Sie unter Sicherheitsgruppenregeln im Amazon-VPC-Benutzerhandbuch.

Schritt 3. Konfigurieren Ihrer externen Datenquelle und Amazon VPC

Stellen Sie sicher, dass Ihre externe Datenquelle über die richtigen Berechtigungskonfigurationen und Netzwerkeinstellungen für verfügt Amazon Kendra , um darauf zuzugreifen. Detaillierte Anweisungen zur Konfiguration Ihrer Datenquellen finden Sie im Abschnitt Voraussetzungen jeder Konnektor-Seite.

Überprüfen Sie außerdem Ihre Amazon VPC Einstellungen und stellen Sie sicher, dass Ihre externe Datenquelle über das Subnetz erreichbar ist, das Sie zuweisen werden Amazon Kendra. Dazu empfehlen wir Ihnen, eine Amazon EC2 Instance im selben Subnetz mit denselben Sicherheitsgruppen zu erstellen und den Zugriff auf Ihre Datenquelle von dieser Amazon EC2 Instance aus zu testen. Weitere Informationen finden Sie unter Fehlerbehebung bei Amazon VPC Verbindungen.

Einrichten einer - Amazon Kendra Datenquelle für die Verbindung mit Amazon VPC

Wenn Sie eine neue Datenquelle in hinzufügen Amazon Kendra, können Sie die Amazon VPC Funktion verwenden, wenn der ausgewählte Datenquellen-Konnektor diese Funktion unterstützt.

Sie können eine neue Amazon Kendra Datenquelle mit Amazon VPC aktivierter einrichten, indem Sie die AWS Management Console oder die Amazon Kendra -API verwenden. Verwenden Sie insbesondere die CreateDataSource -API-Operation und dann den -`VpcConfiguration`Parameter, um die folgenden Informationen bereitzustellen:

- `SubnetIds` – Eine Liste von Kennungen von Amazon VPC Subnetzen
- `SecurityGroupIds` – Eine Liste von IDs von Amazon VPC Sicherheitsgruppen

Wenn Sie die Konsole verwenden, geben Sie die erforderlichen Amazon VPC Informationen während der Konnektor-Konfiguration an. Um die Konsole zum Aktivieren der Amazon-VPC-Funktion für einen Konnektor zu verwenden, wählen Sie zunächst eine Amazon-VPC aus. Anschließend geben Sie Kennungen aller Amazon-VPC-Subnetze und Kennungen aller Amazon-VPC-Sicherheitsgruppen an. Sie können die Amazon-VPC-Subnetze und Amazon-VPC-Sicherheitsgruppen auswählen, die Sie unter Konfigurieren von Amazon VPC erstellt haben, oder vorhandene verwenden.

Themen

- Anzeigen von Amazon VPC Kennungen
- Überprüfen Ihrer IAM Datenquellenrolle

Anzeigen von Amazon VPC Kennungen

Die Kennungen für Subnetze und Sicherheitsgruppen sind in der - Amazon VPC Konsole konfiguriert. Gehen Sie wie folgt vor, um die Kennungen anzuzeigen.

So zeigen Sie Subnetz-IDs an

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Subnetze aus.
3. Wählen Sie in der Liste Subnetze das Subnetz aus, das Ihren Datenbankserver enthält.

4. Notieren Sie sich auf der Registerkarte Details die ID im Feld Subnetz-ID.

So zeigen Sie Sicherheitsgruppen-IDs an

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Sicherheitsgruppen aus.
3. Wählen Sie in der Liste der Sicherheitsgruppen die Gruppe aus, für die Sie die Kennung verwenden möchten.
4. Notieren Sie sich auf der Registerkarte Details die ID im Feld Sicherheitsgruppen-ID.

Überprüfen Ihrer IAM Datenquellenrolle

Stellen Sie sicher, dass Ihre Datenquellen-Connector- AWS Identity and Access Management IAM)Rolle Berechtigungen für den Zugriff auf Ihr enthält Amazon VPC.

Wenn Sie die Konsole verwenden, um eine neue Rolle für Ihre IAM Rolle zu erstellen, fügt Amazon Kendra automatisch die richtigen Berechtigungen zu Ihrer IAM Rolle in Ihrem Namen hinzu. Wenn Sie die -API oder eine vorhandene IAM Rolle verwenden, überprüfen Sie, ob Ihre Rolle Berechtigungen für den Zugriff auf enthält Amazon VPC. Informationen zum Überprüfen, ob Sie über die richtigen Berechtigungen verfügen, finden Sie unter IAM Rollen für VPC .

Sie können eine vorhandene Datenquelle ändern, um ein anderes Amazon VPC Subnetz zu verwenden. Überprüfen Sie jedoch die IAM Rolle Ihrer Datenquelle und ändern Sie sie bei Bedarf so, dass sie der Änderung entspricht, damit der Amazon Kendra Datenquellen-Konnektor ordnungsgemäß funktioniert.

Herstellen einer Verbindung mit einer Datenbank in einer VPC

Das folgende Beispiel zeigt, wie Sie eine MySQL Datenbank verbinden, die in einer Virtual Private Cloud (VPC) ausgeführt wird. Im Beispiel wird davon ausgegangen, dass Sie mit Ihrer Standard-VPC beginnen und eine MySQL Datenbank erstellen müssen. Wenn Sie bereits über eine VPC verfügen, stellen Sie sicher, dass diese wie gezeigt konfiguriert ist. Wenn Sie eine MySQL Datenbank haben, können Sie diese verwenden, anstatt eine neue zu erstellen.

Schritte

- Schritt 1: Konfigurieren einer VPC

- Schritt 2: Erstellen und Konfigurieren von Sicherheitsgruppen
- Schritt 3: Erstellen einer Datenbank
- Schritt 4: Erstellen eines Datenquellen-Connectors

Schritt 1: Konfigurieren einer VPC

Konfigurieren Sie Ihre VPC so, dass Sie über ein privates Subnetz und eine Sicherheitsgruppe für verfügen, Amazon Kendra um auf eine MySQL Datenbank zuzugreifen, die im Subnetz ausgeführt wird. Die in der VPC-Konfiguration bereitgestellten Subnetze müssen sich in der Region USA West (Oregon), der Region USA Ost (Nord-Virginia) oder der Region Europa (Irland) befinden.

So konfigurieren Sie eine VPC mit Amazon VPC

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Routing-Tabellen und dann Routing-Tabelle erstellen aus.
3. Geben Sie in das Feld Name ein**`Private subnet route table`**. Wählen Sie in der Dropdownliste VPC Ihre VPC aus und wählen Sie dann Routing-Tabelle erstellen aus. Wählen Sie Close aus, um zur Liste der Routing-Tabellen zurückzukehren.
4. Wählen Sie im Navigationsbereich NAT-Gateways und dann NAT-Gateway erstellen aus.
5. Wählen Sie in der Dropdownliste Subnet zdas Subnetz aus, das das öffentliche Subnetz ist. Notieren Sie sich die Subnetz-ID.
6. Wenn Sie keine Elastic IP-Adresse haben, wählen Sie Create New EIP , wählen Sie Create a NAT Gateway und dann Close aus.
7. Wählen Sie im Navigationsbereich Routing-Tabellen aus.
8. Wählen Sie in der Liste der Routing-Tabellen die Routing-Tabelle für private Subnetze aus, die Sie in Schritt 3 erstellt haben. Wählen Sie unter Aktionen die Option Routen bearbeiten aus.
9. Wählen Sie Route hinzufügen aus. Geben Sie als Ziel ein, **`0.0.0.0/0`** um den gesamten ausgehenden Datenverkehr zum Internet zuzulassen. Wählen Sie für Ziel NAT Gateway und dann das Gateway aus, das Sie in Schritt 4 erstellt haben. Wählen Sie Änderungen speichern und dann Schließen aus.
10. Wählen Sie unter Aktionen die Option Subnetzzuordnungen bearbeiten aus.
11. Wählen Sie die Subnetze aus, die privat sein sollen. Wählen Sie nicht das Subnetz mit dem NAT-Gateway aus, das Sie zuvor notiert haben. Wählen Sie Zuordnungen speichern, wenn Sie fertig sind.

Schritt 2: Erstellen und Konfigurieren von Sicherheitsgruppen

Konfigurieren Sie als Nächstes Sicherheitsgruppen für Ihre Datenbank.

So erstellen und konfigurieren Sie Sicherheitsgruppen

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Notieren Sie sich in der Beschreibung Ihrer VPC das IPv4 CIDR.
3. Wählen Sie im Navigationsbereich Sicherheitsgruppen und dann Sicherheitsgruppe erstellen aus.
4. Geben Sie für Security group name (Name der Sicherheitsgruppe) **`DataSourceInboundSecurityGroup`** ein. Geben Sie eine Beschreibung ein und wählen Sie dann Ihre VPC aus der Liste aus. Wählen Sie Sicherheitsgruppe erstellen und dann Schließen aus.
5. Wählen Sie die Registerkarte Inbound rules (Regeln für eingehenden Datenverkehr) aus.
6. Wählen Sie Regeln für eingehenden Datenverkehr bearbeiten und dann Regel hinzufügen aus.
7. Geben Sie für eine Datenbank die Portnummer für den Portbereich ein. Für MySQL ist es beispielsweise **`3306`**, und für HTTPS ist es **`443`**. Geben Sie für die Quelle das Classless Inter-Domain Routing (CIDR) Ihrer VPC ein. Wählen Sie Regeln speichern und dann Schließen aus.

Die Sicherheitsgruppe ermöglicht es jedem innerhalb der VPC, eine Verbindung zur Datenbank herzustellen, und erlaubt ausgehende Verbindungen zum Internet.

Schritt 3: Erstellen einer Datenbank

Erstellen Sie eine Datenbank für Ihre Dokumente, oder Sie können Ihre vorhandene Datenbank verwenden.

Anweisungen zum Erstellen einer MySQL Datenbank finden Sie unter MySQL.

Schritt 4: Erstellen eines Datenquellen-Connectors

Nachdem Sie Ihre VPC konfiguriert und Ihre Datenbank erstellt haben, können Sie einen Datenquellen-Connector für die Datenbank erstellen. Informationen zu Datenbank-Connectors, die Amazon Kendra unterstützt, finden Sie unter Unterstützte Connectors.

Stellen Sie für Ihre Datenbank sicher, dass Sie Ihre VPC, die privaten Subnetze, die Sie in Ihrer VPC erstellt haben, und die Sicherheitsgruppe konfigurieren, die Sie in Ihrer VPC erstellt haben.

Fehlerbehebung bei VPC-Verbindungsproblemen

Wenn Probleme mit Ihrer Virtual Private Cloud (VPC)-Verbindung auftreten, überprüfen Sie, ob Ihre IAM Berechtigungen, Sicherheitsgruppeneinstellungen und die Routing-Tabellen des Subnetzes korrekt konfiguriert sind.

Eine mögliche Ursache für eine fehlgeschlagene Datenquellen-Konnektor-Synchronisierung ist, dass die Datenquelle möglicherweise nicht über das Subnetz erreichbar ist, das Sie zugewiesen haben Amazon Kendra. Um dieses Problem zu beheben, empfehlen wir Ihnen, eine Amazon EC2 Instance mit denselben Amazon VPC Einstellungen zu erstellen. Versuchen Sie dann, von dieser Instance aus Amazon EC2 mit REST-API-Aufrufen oder anderen Methoden (basierend auf dem spezifischen Typ Ihrer Datenquelle) auf die Datenquelle zuzugreifen.

Wenn Sie von der von Ihnen Amazon EC2 erstellten Instance aus erfolgreich auf die Datenquelle zugreifen, bedeutet dies, dass Ihre Datenquelle von diesem Subnetz aus erreichbar ist. Daher steht Ihr Synchronisierungsproblem nicht im Zusammenhang damit, dass auf Ihre Datenquelle nicht von zugegriffen werden kann Amazon VPC.

Wenn Sie nicht von Ihrer VPC-Konfiguration aus auf Ihre Amazon EC2 Instance zugreifen und sie mit der von Ihnen Amazon EC2 erstellten Instance validieren können, müssen Sie weitere Fehler beheben. Wenn Sie beispielsweise einen Amazon S3 Konnektor haben, dessen Synchronisierung mit Fehlern bei Verbindungsproblemen fehlgeschlagen ist, können Sie eine Amazon EC2 Instance mit derselben Amazon VPC Konfiguration einrichten, die Sie Ihrem Amazon S3 Konnektor zugewiesen haben. Verwenden Sie dann diese Amazon EC2-Instance, um zu testen, ob Ihr korrekt eingerichtet Amazon VPC wurde.

Im Folgenden finden Sie ein Beispiel für die Einrichtung einer Amazon EC2 Instance zur Fehlerbehebung bei Ihrer Amazon VPC Verbindung mit einer Amazon S3 -Datenquelle.

Themen

Schritt 1: Starten einer Amazon EC2 Instance

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie Starten einer Instance aus.
3. Wählen Sie Netzwerkeinstellungen und dann Bearbeiten und gehen Sie dann wie folgt vor:

   a. Wählen Sie dieselbe VPC und dasselbe Subnet zaus, das Sie zugewiesen haben Amazon Kendra.

   b. Wählen Sie für Firewall (Sicherheitsgruppen) die Option Vorhandene Sicherheitsgruppe auswählen aus. Wählen Sie dann die Sicherheitsgruppe aus, die Sie zugewiesen haben Amazon Kendra.

   > **Note**
   >
   > Die Sicherheitsgruppe sollte ausgehenden Datenverkehr zu zulassen Amazon S3.

   c. Legen Sie die Option Öffentliche IP automatisch zuweisen auf Deaktivieren fest.

   d. Gehen Sie unter Erweiterte Details wie folgt vor:

   - Wählen Sie für IAM-Instance-Profil die Option Neues IAM-Profil erstellen aus, um ein IAM Instance-Profil zu erstellen und an Ihre Instance anzufügen. Stellen Sie sicher, dass das Profil über Berechtigungen für den Zugriff auf verfügt Amazon S3. Weitere Informationen finden Sie unter Wie kann ich meiner Amazon EC2 Instance Zugriff auf einen - Amazon S3 Bucket gewähren? in AWS re:Post.
   - Behalten Sie alle anderen Einstellungen als Standard bei.

   e. Überprüfen und starten Sie die Amazon EC2 Instance.

Schritt 2: Herstellen einer Verbindung mit Amazon EC2 der Instance

Nachdem Ihre Amazon EC2 Instance ausgeführt wurde, rufen Sie Ihre Instance-Detailseite auf und stellen Sie eine Verbindung zu Ihrer Instance her. Führen Sie dazu die Schritte unter Herstellen einer Verbindung mit Ihren Instances aus, ohne dass eine öffentliche IPv4-Adresse mit EC2-Instance-Connect-Endpunkt erforderlich ist im Amazon EC2 Benutzerhandbuch für Linux-Instances.

Schritt 3: Testen Amazon S3 des Zugriffs

Nachdem Sie eine Verbindung zu Ihrem Amazon EC2 Instance-Terminal hergestellt haben, führen Sie einen - AWS CLI Befehl aus, um die Verbindung von diesem privaten Subnetz zu Ihrem Amazon S3 Bucket zu testen.

Um den Amazon S3 Zugriff zu testen, geben Sie den folgenden AWS CLI Befehl in ein AWS CLI: `aws s3 ls`

Nachdem der AWS CLI Befehl ausgeführt wurde, überprüfen Sie Folgendes:

- Wenn Sie die erforderlichen IAM Berechtigungen korrekt eingerichtet haben und Ihre Amazon S3 Einrichtung korrekt ist, sollten Sie eine Liste Ihrer Amazon S3 Buckets sehen.
- Wenn Sie Berechtigungsfehler wie sehen`Access Denied`, ist Ihre yourVPC-Konfiguration wahrscheinlich korrekt, aber mit Ihren IAM Berechtigungen oder Ihrer Amazon S3 Bucket-Richtlinie stimmt etwas nicht.

Wenn der Befehl eine Zeitüberschreitung aufweist, ist es wahrscheinlich, dass Ihre Verbindung eine Zeitüberschreitung aufweist, da Ihre VPC-Einrichtung falsch ist und die Amazon EC2-Instance nicht von Ihrem Subnetz aus auf Amazon S3 zugreifen kann. Konfigurieren Sie Ihre VPC neu und versuchen Sie es erneut.

Löschen eines Indexes, einer Datenquelle oder eines stapelweise hochgeladenen Dokuments

In diesem Abschnitt erfahren Sie, wie Sie einen Index, ein Datenquellenspeicher mit Dokumenten in Ihrem Index oder Dokumente in Ihrem Index löschen, die Sie stapelweise hochgeladen haben.

Themen

Löschen eines Indexes

Sie können einen Index löschenAmazon Kendra, wenn Sie ihn nicht mehr verwenden. Löschen Sie beispielsweise einen Index, wenn:

- Sie verwenden den Index nicht mehr und möchten die Gebühren für Ihr AWS Konto reduzieren. Für einen Amazon Kendra Index fallen Gebühren an, während er läuft, unabhängig davon, ob Sie Abfragen für den Index stellen oder nicht.
- Sie möchten den Index für eine andere Ausgabe von Amazon Kendra neu konfigurieren. Löschen Sie den vorhandenen Index und erstellen Sie dann einen neuen mit der anderen Ausgabe.
- Sie haben die maximale Anzahl von Indizes in Ihrem Konto erreicht und möchten Ihr Kontingent nicht überschreiten. Löschen Sie einen vorhandenen Index und fügen Sie einen neuen hinzu. Informationen zur maximalen Anzahl von Indizes, die Sie erstellen können, finden Sie unter Kontingente.

Um einen Index zu löschen, verwenden Sie die KonsoleAWS Command Line Interface, das AWS CloudFormation Skript oder die `DeleteIndex` API. Beim Löschen eines Indexes werden der Index und alle zugehörigen Datenquellen und Dokumentdaten entfernt. Durch das Löschen eines Indexes werden die Originaldokumente nicht aus Ihrem Speicher entfernt.

Das Löschen eines Indexes ist ein asynchroner Vorgang. Wenn Sie mit dem Löschen eines Index beginnen, ändert sich der Indexstatus in`DELETING`. Es bleibt so lange im `DELETING` Status, bis alle Informationen zum Index entfernt wurden. Sobald der Index gelöscht wurde, erscheint er nicht mehr

in den Ergebnissen eines ListIndicesAPI-Aufrufs. Wenn Sie die DescribeIndexAPI mit der Kennung des gelöschten Indexes aufrufen, erhalten Sie eine `ResourceNotFound` Ausnahme.

Um einen Index zu löschen (Konsole)

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die Amazon Kendra Konsole unter https://console.aws.amazon.com/kendra/.
2. Wählen Sie im Navigationsbereich Indizes und dann den Index aus, den Sie löschen möchten.
3. Wählen Sie Löschen, um den ausgewählten Index zu löschen.

Um einen Index zu löschen (CLI)

- Geben Sie in der AWS CLI den folgenden Befehl ein. Der Befehl ist für Linux und macOS formatiert. Wenn Sie Windows verwenden, ersetzen Sie das Unix-Zeilenfortsetzungszeichen (\) durch ein Caret (^).

```
aws kendra delete-index \
   --id index-id
```

Löschen einer Datenquelle

Sie löschen eine Datenquelle, wenn Sie die in der Datenquelle enthaltenen Informationen aus Ihrem Amazon Kendra Index entfernen möchten. Löschen Sie beispielsweise eine Datenquelle, wenn:

- Eine Datenquelle ist falsch konfiguriert. Löschen Sie die Datenquelle, warten Sie, bis die Datenquelle mit dem Löschen fertig ist, und erstellen Sie sie dann erneut.
- Sie haben Dokumente von einer Datenquelle in eine andere migriert. Löschen Sie die ursprüngliche Datenquelle und erstellen Sie sie am neuen Speicherort neu.
- Sie haben das Limit an Datenquellen für einen Index erreicht. Löschen Sie eine der vorhandenen Datenquellen und fügen Sie eine neue hinzu. Weitere Informationen zur Anzahl der Datenquellen, die Sie erstellen können, finden Sie unterKontingente.

Um eine Datenquelle zu löschen, verwenden Sie die Konsole, die AWS Command Line Interface (AWS CLI), die `DeleteDataSource` API oder ein AWS CloudFormation Skript. Durch das Löschen einer Datenquelle werden alle Informationen über die Datenquelle aus dem Index

entfernt. Wenn Sie nur die Synchronisierung der Datenquelle beenden möchten, ändern Sie den Synchronisierungszeitplan für die Datenquelle auf „Bei Bedarf ausführen“.

Das Löschen einer Datenquelle ist ein asynchroner Vorgang. Wenn Sie mit dem Löschen einer Datenquelle beginnen, ändert sich der Datenquellenstatus in`DELETING`. Es bleibt im `DELETING` Status, bis die Informationen zur Datenquelle entfernt werden. Nachdem die Datenquelle gelöscht wurde, erscheint sie nicht mehr in den Ergebnissen eines ListDataSourcesAPI-Aufrufs. Wenn Sie die DescribeDataSourceAPI mit dem Identifier der gelöschten Datenquelle aufrufen, erhalten Sie eine `ResourceNotFound` Ausnahme.

> **Note**
>
> Das Löschen einer gesamten Datenquelle oder die erneute Synchronisierung Ihres Indexes nach dem Löschen bestimmter Dokumente aus einer Datenquelle kann je nach Anzahl der Dokumente, die Sie löschen möchten, bis zu einer Stunde oder länger dauern.

So löschen Sie eine Datenquelle (Konsole)

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die Amazon Kendra Konsole unter https://console.aws.amazon.com/kendra/.
2. Wählen Sie im Navigationsbereich Indizes und dann den Index aus, der die zu löschende Datenquelle enthält.
3. Klicken Sie im Navigationsbereich auf Data sources (Datenquellen).
4. Wählen Sie die zu entfernende Datenquelle aus.
5. Wählen Sie Löschen, um die Datenquelle zu löschen.

So löschen Sie eine Datenquelle (CLI)

- Geben Sie in der AWS Command Line Interface den folgenden Befehl ein. Der Befehl ist für Linux und macOS formatiert. Wenn Sie Windows verwenden, ersetzen Sie das Unix-Zeilenfortsetzungszeichen (\) durch ein Caret (^).

```
aws kendra delete-data-source \
   --id data-source-id \
   --index-id index-id
```

Wenn Sie eine Datenquelle löschen, werden alle gespeicherten Informationen über die Datenquelle Amazon Kendra entfernt. Amazon Kendraentfernt alle im Index gespeicherten Dokumentdaten sowie alle mit der Datenquelle verknüpften Laufverläufe und Metriken. Durch das Löschen einer Datenquelle werden die Originaldokumente nicht aus Ihrem Speicher entfernt.

Dokumente in der Datenquelle können in der Anzahl der Dokumente enthalten sein, die von der `DescribeIndex` API zurückgegeben wird, wenn eine Datenquelle Amazon Kendra gelöscht wird. Dokumente aus der Datenquelle werden möglicherweise in den Suchergebnissen angezeigt, während die Datenquelle Amazon Kendra gelöscht wird.

Amazon Kendragibt die Ressourcen für eine Datenquelle frei, sobald Sie die `DeleteDataSource` API aufrufen oder die Datenquelle in der Konsole löschen. Wenn Sie die Datenquelle löschen, um die Anzahl der Datenquellen unter Ihr Limit zu reduzieren, können Sie sofort eine neue Datenquelle erstellen.

Wenn Sie eine Datenquelle löschen und dann eine weitere Datenquelle für die Dokumentdaten erstellen, warten Sie, bis die erste Datenquelle gelöscht ist, bevor Sie die neue Datenquelle synchronisieren.

Sie können eine Datenquelle löschen, mit Amazon Kendra der gerade synchronisiert wird. Die Synchronisierung wird beendet und die Datenquelle wird entfernt. Wenn Sie versuchen, eine Synchronisierung zu starten, während die Datenquelle gelöscht wird, erhalten Sie eine `ConflictException` Ausnahme.

Sie können eine Datenquelle nicht löschen, wenn sich der zugehörige Index im `DELETING` Status befindet. Wenn Sie einen Index löschen, werden alle Datenquellen für den Index gelöscht. Sie können mit dem Löschen eines Index beginnen, solange sich eine Datenquelle für diesen Index im `DELETING` Status befindet.

Wenn Sie zwei Datenquellen haben, die auf dieselben Dokumente verweisen, z. B. zwei Datenquellen, die auf denselben Amazon S3 Bucket verweisen, sind Dokumente im Index möglicherweise inkonsistent, wenn eine der Datenquellen gelöscht wird. Wenn zwei Datenquellen auf dieselben Dokumente verweisen, wird nur eine Kopie der Dokumentdaten im Index gespeichert. Durch das Entfernen einer Datenquelle werden die Indexdaten für die Dokumente entfernt. Die andere Datenquelle weiß nicht, dass die Dokumente entfernt wurden, und indexiert die Dokumente daher bei der nächsten Synchronisierung Amazon Kendra nicht korrekt. Wenn Sie zwei Datenquellen haben, die auf denselben Speicherort des Dokuments verweisen, sollten Sie beide Datenquellen löschen und dann eine neu erstellen.

Löschen von stapelweise hochgeladenen Dokumenten

Mithilfe der BatchDeleteDocumentAPI können Sie Dokumente direkt aus einem Index löschen. Sie können Dokumente nicht direkt über die Konsole löschen. Wenn Sie die Konsole verwenden, können Sie entweder bestimmte Dokumente aus Ihrem Datenquellen-Repository löschen und erneut mit Ihrem Index synchronisieren oder den gesamten Datenquellenconnector löschen.

Das Löschen von Dokumenten aus einem Index mithilfe von `BatchDeleteDocument` ist ein asynchroner Vorgang. Nachdem Sie die `BatchDeleteDocument` API aufgerufen haben, verwenden Sie die BatchGetDocumentStatusAPI, um den Fortschritt beim Löschen Ihrer Dokumente zu überwachen. Wenn ein Dokument aus dem Index gelöscht wird, wird `NOT_FOUND` der Status Amazon Kendra zurückgegeben.

> **Note**
>
> Das Löschen von Dokumenten aus einem Index mithilfe von `BatchDeleteDocument` kann je nach Anzahl der Dokumente, die Sie löschen möchten, bis zu einer Stunde oder länger dauern.

So löschen Sie stapelweise hochgeladene Dokumente aus einem Index (CLI)

- Geben Sie in der AWS Command Line Interface den folgenden Befehl ein. Der Befehl ist für Linux und macOS formatiert. Wenn Sie Windows verwenden, ersetzen Sie das Unix-Zeilenfortsetzungszeichen (\) durch ein Caret (^).

```
aws kendra batch-delete-document \
   --index-id index-id \
   --document-id-list 'doc-id-1' 'doc-id-2'
```

Bereichern Sie Ihre Dokumente während der Aufnahme

Sie können Ihre Inhalts- und Dokumentmetadatenfelder oder -Attribute während des Erfassungsprozesses des Dokuments ändern. Mit Amazon Kendra der Funktion zur benutzerdefinierten Dokumentanreicherung können Sie Dokumentattribute und Inhalte erstellen, ändern oder löschen, wenn Sie Ihre Dokumente in aufnehmen. Amazon Kendra Das bedeutet, dass Sie Ihre Daten nach Bedarf bearbeiten und aufnehmen können.

Mit dieser Funktion haben Sie die Kontrolle darüber, wie Ihre Dokumente behandelt und aufgenommen Amazon Kendra werden. Sie können beispielsweise persönlich identifizierbare Informationen in den Metadaten des Dokuments entfernen, während Sie Ihre Dokumente in das Dokument aufnehmen. Amazon Kendra

Sie können diese Funktion auch verwenden, indem Sie eine Lambda-Funktion aufrufen, AWS Lambda um die optische Zeichenerkennung (OCR) für Bilder, die Übersetzung von Text und andere Aufgaben zur Vorbereitung der Daten für die Suche oder Analyse auszuführen. Sie können beispielsweise eine Funktion aufrufen, um OCR auf Bildern auszuführen. Die Funktion könnte Text aus Bildern interpretieren und jedes Bild als Textdokument behandeln. Ein Unternehmen, das Kundenumfragen per Post erhält und diese Umfragen als Bilder speichert, könnte diese Bilder als Textdokumente aufnehmen. Amazon Kendra Das Unternehmen kann dann in nach wertvollen Informationen zu Kundenumfragen suchenAmazon Kendra.

Sie können grundlegende Operationen verwenden, um sie als erste Analyse Ihrer Daten anzuwenden, und dann eine Lambda-Funktion verwenden, um komplexere Operationen auf Ihre Daten anzuwenden. Sie könnten beispielsweise eine einfache Operation verwenden, um einfach alle Werte im Metadatenfeld 'Customer_ID' des Dokuments zu entfernen und dann eine Lambda-Funktion anzuwenden, um Text aus Bildern des Texts in den Dokumenten zu extrahieren.

So funktioniert Custom Document Enrichment

Der Gesamtprozess von Custom Document Enrichment sieht wie folgt aus:

1. Sie konfigurieren Custom Document Enrichment, wenn Sie Ihre Datenquelle erstellen oder aktualisieren oder Ihre Dokumente direkt in Amazon Kendra indexieren.
2. Amazon Kendrawendet Inline-Konfigurationen oder grundlegende Logik an, um Ihre Daten zu ändern. Weitere Informationen finden Sie unter the section called “Grundlegende Operationen zum Ändern von Metadaten”.

3. Wenn Sie sich dafür entscheiden, die erweiterte Datenmanipulation zu konfigurieren, Amazon Kendra können Sie dies auf Ihre ursprünglichen Rohdokumente oder auf die strukturierten, analysierten Dokumente anwenden. Weitere Informationen finden Sie unter the section called “Lambda-Funktionen: Metadaten oder Inhalte extrahieren und ändern”.
4. Ihre geänderten Dokumente werden aufgenommen. Amazon Kendra

Wenn Ihre Konfiguration zu irgendeinem Zeitpunkt dieses Vorgangs nicht gültig ist, wird Amazon Kendra ein Fehler ausgelöst.

Wenn Sie BatchPutDocumentAPIs aufrufen CreateDataSourceUpdateDataSource, oder geben Sie Ihre Custom Document Enrichment-Konfiguration an. Wenn Sie anrufen`BatchPutDocument`, müssen Sie Custom Document Enrichment bei jeder Anfrage konfigurieren. Wenn Sie die Konsole verwenden, wählen Sie Ihren Index und dann Document Enrichments aus, um Custom Document Enrichment zu konfigurieren.

Wenn Sie Document Enrichments in der Konsole verwenden, können Sie wählen, ob Sie nur grundlegende Operationen oder nur Lambda-Funktionen oder beides konfigurieren möchten, wie Sie es mit der API tun können. Sie können in den Konsolenschritten Weiter auswählen, um keine grundlegenden Operationen und nur Lambda-Funktionen zu konfigurieren, einschließlich der Frage, ob diese auf die Originaldaten (vor der Extraktion) oder auf strukturierte Daten (nach der Extraktion) angewendet werden sollen. Sie können Ihre Konfigurationen nur speichern, indem Sie alle Schritte in der Konsole ausführen. Ihre Dokumentkonfigurationen werden nicht gespeichert, wenn Sie nicht alle Schritte abgeschlossen haben.

Grundlegende Operationen zum Ändern von Metadaten

Sie können Ihre Dokumentfelder und Inhalte mithilfe grundlegender Logik manipulieren. Dazu gehören das Entfernen von Werten in einem Feld, das Ändern von Werten in einem Feld mithilfe einer Bedingung oder das Erstellen eines Felds. Rufen Sie für fortgeschrittene Manipulationen, die über das hinausgehen, was Sie mit grundlegender Logik manipulieren können, eine Lambda-Funktion auf. Weitere Informationen finden Sie unter the section called “Lambda-Funktionen: Metadaten oder Inhalte extrahieren und ändern”.

Um grundlegende Logik anzuwenden, geben Sie das Zielfeld an, das Sie mithilfe des DocumentAttributeTargetObjekts manipulieren möchten. Sie geben den Attributschlüssel an. Der Schlüssel „Abteilung“ ist beispielsweise ein Feld oder Attribut, das alle Abteilungsnamen enthält, die den Dokumenten zugeordnet sind. Sie können auch einen Wert angeben, der im Zielfeld verwendet

werden soll, wenn eine bestimmte Bedingung erfüllt ist. Sie legen die Bedingung mithilfe des DocumentAttributeConditionObjekts fest. Wenn das Feld 'source_URI' beispielsweise 'financial' in seinem URI-Wert enthält, füllen Sie das Zielfeld 'Department' vorab mit dem Zielwert 'Finanzen' für das Dokument aus. Sie können auch die Werte des Zieldokumentattributs löschen.

Um die grundlegende Logik mithilfe der Konsole anzuwenden, wählen Sie Ihren Index und dann im Navigationsmenü die Option Document Enrichments aus. Gehen Sie zu Grundfunktionen konfigurieren, um grundlegende Manipulationen an Ihren Dokumentfeldern und Inhalten vorzunehmen.

Im Folgenden finden Sie ein Beispiel für die Verwendung einer einfachen Logik zum Entfernen aller Kundenidentifikationsnummern aus dem Dokumentfeld mit dem Namen 'Customer_ID'.

Beispiel 1: Entfernen der mit den Dokumenten verknüpften Kundenidentifikationsnummern

Daten vor der grundlegenden Manipulation.

Dokument-ID	Haupttext_Text	Kunden_ID
1	Lorem Ipsum.	CID1234
2	Lorem Ipsum.	CID1235
3	Lorem Ipsum.	CID1236

Daten nach erfolgter grundlegender Manipulation.

Dokument-ID	Haupttext_Text	Kunden_ID
1	Lorem Ipsum.	
2	Lorem Ipsum.	
3	Lorem Ipsum.	

Im Folgenden finden Sie ein Beispiel für die Verwendung grundlegender Logik, um ein Feld mit dem Namen „Abteilung“ zu erstellen und dieses Feld anhand der Informationen aus dem Feld „source_URI“ mit den Abteilungsnamen vorzufüllen. Dabei wird die Bedingung verwendet, dass,

wenn das Feld 'source_URI' in seinem URI-Wert 'financial' enthält, das Zielfeld 'Department' mit dem Zielwert 'Finanzen' für das Dokument vorab ausgefüllt wird.

Beispiel 2: Erstellen Sie das Feld „Abteilung“ und füllen Sie es mithilfe einer Bedingung mit den Abteilungsnamen aus, die den Dokumenten zugeordnet sind.

Daten vor der grundlegenden Manipulation.

Dokument-ID	Haupttext_Text	Quelle_URI
1	Lorem Ipsum.	finanziell/1
2	Lorem Ipsum.	finanziell/2
3	Lorem Ipsum.	finanziell/3

Daten nach erfolgter grundlegender Manipulation.

Dokument-ID	Haupttext_Text	Quelle_URI	Abteilung
1	Lorem Ipsum.	finanziell/1	Finanzen
2	Lorem Ipsum.	finanziell/2	Finanzen
3	Lorem Ipsum.	finanziell/3	Finanzen

> **Note**
>
> Amazon Kendrakann kein Zieldokumentfeld erstellen, wenn es nicht bereits als Indexfeld erstellt wurde. Nachdem Sie Ihr Indexfeld erstellt haben, können Sie mithilfe von`DocumentAttributeTarget`. Amazon Kendraordnet dann Ihr neu erstelltes Dokumentmetadatenfeld Ihrem Indexfeld zu.

Der folgende Code ist ein Beispiel für die Konfiguration der grundlegenden Datenmanipulation, um die mit den Dokumenten verknüpften Kundenidentifikationsnummern zu entfernen.

Console

So konfigurieren Sie die grundlegende Datenmanipulation zum Entfernen von Kundenidentifikationsnummern

1. Wählen Sie im linken Navigationsbereich unter Indizes die Option Dokumentanreicherungen und dann Dokumentanreicherung hinzufügen aus.
2. Wählen Sie auf der Seite „Grundlegende Operationen konfigurieren“ aus der Dropdown-Liste Ihre Datenquelle aus, für die Sie die Dokumentfelder und den Inhalt ändern möchten. Wählen Sie dann aus der Dropdown-Liste den Dokumentfeldnamen 'Customer_ID', wählen Sie aus der Dropdown-Liste den Indexfeldnamen 'Customer_ID' und wählen Sie aus der Dropdown-Liste die Zielaktion Löschen aus. Wählen Sie dann Basisoperation hinzufügen aus.

CLI

So konfigurieren Sie die grundlegende Datenmanipulation zum Entfernen von Kundenidentifikationsnummern

```
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

So konfigurieren Sie die grundlegende Datenmanipulation zum Entfernen von Kundenidentifikationsnummern

```
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

So konfigurieren Sie die grundlegende Datenmanipulation zum Entfernen von Kundenidentifikationsnummern

```
package com.amazonaws.kendra;

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

public class CreateDataSourceWithCustomizationsExample {

    public static void main(String[] args) throws InterruptedException {
        System.out.println("Create a data source with customizations");

        String dataSourceName = "data-source-name";
        String indexId = "index-id";
        String dataSourceRoleArn = "arn:aws:iam::account-id:role/role-name";
        String s3BucketName = "S3-bucket-name"

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

        CreateDataSourceRequest createDataSourceRequest = CreateDataSourceRequest
            .builder()
            .name(dataSourceName)
            .description(experienceDescription)
            .roleArn(experienceRoleArn)
            .type(DataSourceType.S3)
            .configuration(
```

```
                DataSourceConfiguration
                    .builder()
                    .s3Configuration(
                        S3DataSourceConfiguration
                            .builder()
                            .bucketName(s3BucketName)
                            .build()
                    ).build()
            )
            .customDocumentEnrichmentConfiguration(
                CustomDocumentEnrichmentConfiguration
                    .builder()
                    .inlineConfigurations(Arrays.asList(
                        InlineCustomDocumentEnrichmentConfiguration
                            .builder()
                            .target(
                                DocumentAttributeTarget
                                    .builder()
                                    .targetDocumentAttributeKey("Customer_ID")
                                    .targetDocumentAttributeValueDeletion(true)
                                    .build())
                            .build()
                    )).build();

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

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

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

            DataSourceStatus status = describeDataSourceResponse.status();
```

```
            System.out.println(String.format("Creating data source. Status: %s",
status));
            TimeUnit.SECONDS.sleep(60);
            if (status != DataSourceStatus.CREATING) {
                break;
            }
        }

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

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

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

            TimeUnit.SECONDS.sleep(60);
            if (job.status() != DataSourceSyncJobStatus.SYNCING) {
                break;
            }

        }
```

```
        System.out.println("Data source creation with customizations is complete");
    }
}
```

Lambda-Funktionen: Metadaten oder Inhalte extrahieren und ändern

Sie können Ihre Dokumentfelder und Inhalte mithilfe von Lambda-Funktionen bearbeiten. Dies ist nützlich, wenn Sie über die grundlegende Logik hinausgehen und erweiterte Datenmanipulationen anwenden möchten. Verwenden Sie beispielsweise die optische Zeichenerkennung (OCR), die Text aus Bildern interpretiert und jedes Bild als Textdokument behandelt. Oder Sie rufen das aktuelle Datum und die Uhrzeit in einer bestimmten Zeitzone ab und fügen das Datum und die Uhrzeit ein, wenn ein leerer Wert für ein Datumsfeld vorhanden ist.

Sie können zuerst grundlegende Logik anwenden und dann eine Lambda-Funktion verwenden, um Ihre Daten weiter zu manipulieren, oder umgekehrt. Sie können sich auch dafür entscheiden, nur eine Lambda-Funktion anzuwenden.

Amazon Kendrakann eine Lambda-Funktion aufrufen, um erweiterte Datenmanipulationen während des Erfassungsprozesses als Teil Ihres durchzuführen. CustomDocumentEnrichmentConfiguration Sie geben eine Rolle an, die die Berechtigung beinhaltet, die Lambda-Funktion auszuführen und auf Ihren Amazon S3 Bucket zuzugreifen, um die Ausgabe Ihrer Datenmanipulationen zu speichern — IAM siehe Zugriffsrollen.

Amazon Kendrakann eine Lambda-Funktion auf Ihre ursprünglichen Rohdokumente oder auf die strukturierten, analysierten Dokumente anwenden. Sie können eine Lambda-Funktion konfigurieren, die Ihre Original- oder Rohdaten verwendet und Ihre Datenmanipulationen mithilfe von. PreExtractionHookConfiguration Sie können auch eine Lambda-Funktion konfigurieren, die Ihre strukturierten Dokumente verwendet und Ihre Datenmanipulationen mithilfe von. PostExtractionHookConfiguration Amazon Kendraextrahiert die Metadaten und den Text des Dokuments, um Ihre Dokumente zu strukturieren. Ihre Lambda-Funktionen müssen den obligatorischen Anfrage- und Antwortstrukturen folgen. Weitere Informationen finden Sie unter the section called “Datenverträge für Lambda-Funktionen”.

Um eine Lambda-Funktion in der Konsole zu konfigurieren, wählen Sie Ihren Index und dann im Navigationsmenü die Option Document Enrichments aus. Gehen Sie zu Lambda-Funktionen konfigurieren, um eine Lambda-Funktion zu konfigurieren.

Sie können nur eine Lambda-Funktion für `PreExtractionHookConfiguration` und nur eine Lambda-Funktion für konfigurieren. `PostExtractionHookConfiguration` Ihre Lambda-Funktion kann jedoch andere Funktionen aufrufen, die sie benötigt. Sie können beide und/oder `PreExtractionHookConfiguration` eines davon konfigurieren. `PostExtractionHookConfiguration` Ihre Lambda-Funktion für `PreExtractionHookConfiguration` darf eine Laufzeit von 5 Minuten nicht überschreiten und Ihre Lambda-Funktion für `PostExtractionHookConfiguration` darf eine Laufzeit von 1 Minute nicht überschreiten. Die Konfiguration von Custom Document Enrichment dauert natürlich länger, bis Ihre Dokumente aufgenommen werden, Amazon Kendra als wenn Sie dies nicht konfigurieren würden.

Sie können so konfigurierenAmazon Kendra, dass eine Lambda-Funktion nur aufgerufen wird, wenn eine Bedingung erfüllt ist. Sie können beispielsweise eine Bedingung angeben, nach der bei leeren Datums- und Uhrzeitwerten eine Funktion aufgerufen werden Amazon Kendra soll, die die aktuelle Uhrzeit einfügt.

Im Folgenden finden Sie ein Beispiel für die Verwendung einer Lambda-Funktion zur Ausführung von OCR, um Text aus Bildern zu interpretieren und diesen Text in einem Feld namens 'Document_Image_Text' zu speichern.

Beispiel 1: Extrahieren von Text aus Bildern zur Erstellung von Textdokumenten

Daten, bevor die erweiterte Manipulation angewendet wurde.

Dokument-ID	Dokument_Bild
1	image_1.png
2	image_2.png
3	image_3.png

Daten nach Anwendung erweiterter Manipulationen.

Dokument-ID	Dokument_Bild	Dokument_Bild_Text
1	image_1.png	Antwort auf die Umfrage per Post

Dokument-ID	Dokument_Bild	Dokument_Bild_Text
2	image_2.png	Antwort auf die Umfrage per Post
3	image_3.png	Antwort auf die Umfrage per Post

Im Folgenden finden Sie ein Beispiel für die Verwendung einer Lambda-Funktion zum Einfügen der aktuellen Datums- und Uhrzeitangabe für leere Datumswerte. Dabei wird die Bedingung verwendet, dass, wenn ein Datumsfeldwert 'Null' ist, dieser durch das aktuelle Datum und Uhrzeit ersetzt wird.

Beispiel 2: Ersetzen leerer Werte im Feld Last_Updated durch das aktuelle Datum und Uhrzeit.

Daten, bevor die erweiterte Manipulation angewendet wurde.

Dokument-ID	Haupttext_Text	Zuletzt aktualisiert
1	Lorem Ipsum.	1. Januar 2020
2	Lorem Ipsum.	
3	Lorem Ipsum.	1. Juli 2020

Daten nach Anwendung erweiterter Manipulationen.

Dokument-ID	Haupttext_Text	Zuletzt aktualisiert
1	Lorem Ipsum.	1. Januar 2020
2	Lorem Ipsum.	1. Dezember 2021
3	Lorem Ipsum.	1. Juli 2020

Der folgende Code ist ein Beispiel für die Konfiguration einer Lambda-Funktion für die erweiterte Datenmanipulation an den rohen Originaldaten.

Console

Um eine Lambda-Funktion für erweiterte Datenmanipulationen an den rohen Originaldaten zu konfigurieren

1. Wählen Sie im linken Navigationsbereich unter Indizes die Option Dokumentanreicherungen und dann Dokumentanreicherung hinzufügen aus.
2. Wählen Sie auf der Seite Lambda-Funktionen konfigurieren im Abschnitt Lambda for Pre-Extraction aus den Dropdownlisten Ihren Lambda-Funktions-ARN und Ihren Bucket aus. Amazon S3 Fügen Sie Ihre IAM Zugriffsrolle hinzu, indem Sie in der Dropdown-Liste die Option zum Erstellen einer neuen Rolle auswählen. Dadurch werden die erforderlichen Amazon Kendra Berechtigungen für die Erstellung der Dokumentanreicherung erstellt.

CLI

Um eine Lambda-Funktion für erweiterte Datenmanipulationen an den rohen Originaldaten zu konfigurieren

```
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

Um eine Lambda-Funktion für erweiterte Datenmanipulationen an den rohen Originaldaten zu konfigurieren

```
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

Um eine Lambda-Funktion für erweiterte Datenmanipulationen an den rohen Originaldaten zu konfigurieren

```
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");
    }
}
```

Datenverträge für Lambda-Funktionen

Ihre Lambda-Funktionen für erweiterte Datenmanipulation interagieren mit Amazon Kendra Datenverträgen. Die Verträge sind die verbindlichen Anfrage- und Antwortstrukturen Ihrer Lambda-Funktionen. Wenn Ihre Lambda-Funktionen diesen Strukturen nicht folgen, wird ein Amazon Kendra Fehler ausgegeben.

Ihre Lambda-Funktion für `PreExtractionHookConfiguration` sollte die folgende Anforderungsstruktur erwarten:

```
{
    "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>
}
```

Die `metadata` Struktur, die die `CustomDocumentAttribute` Struktur einschließt, sieht wie folgt aus:

```
{
    "attributes": [<CustomDocumentAttribute<]
}

CustomDocumentAttribute
{
    "name": <str>,
    "value": <CustomDocumentAttributeValue>
}

CustomDocumentAttributeValue
```

```
{
    "stringValue": <str>,
    "integerValue": <int>,
    "longValue": <long>,
    "stringListValue": list<str>,
    "dateValue": <str>
}
```

Ihre Lambda-Funktion für `PreExtractionHookConfiguration` muss der folgenden Antwortstruktur entsprechen:

```
{
    "version": <str>,
    "dataBlobStringEncodedInBase64": <str>, //In the case of a data blob
    "s3ObjectKey": <str>, //In the case of an S3 bucket
    "metadataUpdates": [<CustomDocumentAttribute>]
}
```

Ihre Lambda-Funktion für `PostExtractionHookConfiguration` sollte die folgende Anforderungsstruktur erwarten:

```
{
    "version": <str>,
    "s3Bucket": <str>,
    "s3ObjectKey": <str>,
    "metadata": <Metadata>
}
```

Ihre Lambda-Funktion für `PostExtractionHookConfiguration` muss der folgenden Antwortstruktur entsprechen:

```
PostExtractionHookConfiguration Lambda Response
{
    "version": <str>,
    "s3ObjectKey": <str>,
    "metadataUpdates": [<CustomDocumentAttribute>]
}
```

Ihr geändertes Dokument wird in Ihren Amazon S3 Bucket hochgeladen. Das geänderte Dokument muss dem angegebenen Format entsprechenthe section called “Strukturiertes Dokumentenformat”.

Strukturiertes Dokumentenformat

Amazon Kendralädt Ihr strukturiertes Dokument in den angegebenen Amazon S3 Bucket hoch. Das strukturierte Dokument folgt diesem Format:

```
Kendra document

{
   "textContent": <TextContent>
}

TextContent
{
  "documentBodyText": <str>
}
```

Beispiel für eine Lambda-Funktion, die Datenverträge einhält

Der folgende Python-Code ist ein Beispiel für eine Lambda-Funktion, die erweiterte Manipulationen der Metadatenfelder `_authors` und des `_document_title` Hauptinhalts auf die Rohdokumente oder Originaldokumente anwendet.

Im Fall, dass sich der Körperinhalt in einem Amazon S3 Eimer befindet

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

Im Fall, dass sich der Textinhalt in einem Datenblob befindet

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

Der folgende Python-Code ist ein Beispiel für eine Lambda-Funktion, die eine erweiterte Manipulation der Metadatenfelder `_authors` und des `_document_title` Textinhalts auf die strukturierten oder analysierten Dokumente anwendet.

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

Einen Index durchsuchen

Um einen Amazon Kendra Index zu durchsuchen, verwenden Sie die Query API. Die `Query` API gibt Informationen zu den indizierten Dokumenten zurück, die Sie in Ihrer Anwendung verwenden. In diesem Abschnitt erfahren Sie, wie Sie eine Abfrage stellen, Filter durchführen und die Antwort interpretieren, die Sie von der `Query` API erhalten.

Verwenden Sie AMAZON, um nach Dokumenten zu suchen Amazon Lex, die Sie mit Amazon Kendra for indexiert haben. KendraSearchIntent. Ein Beispiel für die Konfiguration Amazon Kendra mit Amazon Lex finden Sie unter Einen FAQ-Bot für einen Amazon Kendra Index erstellen.

Themen

Einen Index abfragen

Wenn Sie Ihren Index durchsuchen, Amazon Kendra verwendet alle Informationen, die Sie zu Ihren Dokumenten angegeben haben, um die Dokumente zu ermitteln, die für die eingegebenen Suchbegriffe am relevantesten sind. Dabei werden unter anderem folgende Punkte Amazon Kendra berücksichtigt:

- Der Text oder der Hauptteil des Dokuments.
- Der Titel des Dokuments.

- Benutzerdefinierte Textfelder, die Sie als durchsuchbar markiert haben.
- Das von Ihnen angegebene Datumsfeld sollte verwendet werden, um die „Aktualität“ eines Dokuments zu bestimmen.
- Jedes andere Feld, das relevante Informationen liefern könnte.

Amazon Kendra kann die Antwort auch anhand von Feld-/Attributfiltern filtern, die Sie möglicherweise für die Suche festgelegt haben. Wenn Sie beispielsweise über ein benutzerdefiniertes Feld mit dem Namen „Abteilung“ verfügen, können Sie die Antwort so filtern, dass nur Dokumente aus einer Abteilung mit dem Namen „Rechtsabteilung“ zurückgegeben werden. Weitere Informationen finden Sie unter Benutzerdefinierte Felder oder Attribute.

Die zurückgegebenen Suchergebnisse sind nach der Relevanz sortiert, die für jedes Dokument Amazon Kendra maßgeblich ist. Die Ergebnisse sind paginiert, sodass Sie Ihrem Benutzer jeweils eine Seite anzeigen können.

Verwenden Sie AMAZON, um nach Dokumenten zu suchen, die Sie mit Amazon Kendra for Amazon Lex indexiert haben. KendraSearchIntent. Ein Beispiel für die Konfiguration Amazon Kendra mit Amazon Lex finden Sie unter Einen FAQ-Bot für einen Amazon Kendra Index erstellen.

Das folgende Beispiel zeigt, wie ein Index durchsucht wird. Amazon Kendra bestimmt den Typ des Suchergebnisses (Antwort, Dokument, Frage-Antwort), der für die Abfrage am besten geeignet ist. Sie können nicht so konfigurieren Amazon Kendra , dass eine bestimmte Art von Suchantwort (Antwort, Dokument, Frage-Antwort) auf eine Abfrage zurückgegeben wird.

Informationen zu den Abfrageantworten finden Sie unter. Antworten und Antworttypen abfragen

Voraussetzungen

Bevor Sie mit der Query API einen Index abfragen:

- Richten Sie die erforderlichen Berechtigungen für einen Index ein und stellen Sie eine Verbindung zu Ihrer Datenquelle her oder laden Sie Ihre Dokumente stapelweise hoch. Weitere Informationen finden Sie unter IAM Rollen. Sie verwenden den Amazon-Ressourcennamen der Rolle, wenn Sie die API aufrufen, um einen Index- und Datenquellen-Connector oder einen Batch-Upload von Dokumenten zu erstellen.
- Richten Sie entweder AWS Command Line Interface das SDK ein oder rufen Sie die Amazon Kendra Konsole auf. Weitere Informationen finden Sie unter Einrichten von Amazon Kendra.

- Erstellen Sie einen Index und stellen Sie eine Verbindung zu einer Datenquelle mit Dokumenten her oder laden Sie Dokumente stapelweise hoch. Weitere Informationen finden Sie unter Erstellen eines Indexes und Erstellen eines Datenquellenconnectors.

Einen Index durchsuchen (Konsole)

Sie können die Amazon Kendra Konsole verwenden, um Ihren Index zu suchen und zu testen. Sie können Abfragen stellen und die Ergebnisse sehen.

Um einen Index mit der Konsole zu durchsuchen

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die Amazon Kendra Konsole unter http://console.aws.amazon.com/kendra/.
2. Wählen Sie im Navigationsbereich Indizes aus.
3. Wählen Sie Ihren Index aus.
4. Wählen Sie im Navigationsmenü die Option, um Ihren Index zu durchsuchen.
5. Geben Sie eine Abfrage in das Textfeld ein und drücken Sie dann die Eingabetaste.
6. Amazon Kendra gibt die Ergebnisse der Suche zurück.

Sie können die Abfrage-ID für die Suche auch abrufen, indem Sie auf das Glühbirnensymbol in der Seitenleiste klicken.

Einen Index durchsuchen (SDK)

Um einen Index mit Python oder Java zu durchsuchen

- Im folgenden Beispiel wird ein Index durchsucht. Ändern Sie den Wert von `query` in Ihre Suchabfrage `index_id` und/oder in `indexId` den Indexbezeichner des Indexes, den Sie durchsuchen möchten.

  Sie können die Abfrage-ID für die Suche auch als Teil der Antwortelemente abrufen, wenn Sie die Abfrage-API aufrufen.

  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");
       }
   }
```

```
}
```

Einen Index durchsuchen (Postman)

Sie können Postman verwenden, um Ihren Amazon Kendra Index abzufragen und zu testen.

Um einen Index mit Postman zu durchsuchen

1. Erstellen Sie eine neue Sammlung in Postman und legen Sie den Anforderungstyp auf POST fest.
2. Geben Sie die Endpunkt-URL ein. Zum Beispiel https://kendra. .amazonaws.com<region>.
3. Wählen Sie die Registerkarte Autorisierung und geben Sie die folgenden Informationen ein.
   - Typ — Wählen Sie die AWS Signatur aus.
   - AccessKey— Geben Sie den Zugriffsschlüssel ein, der beim Erstellen eines IAM Benutzers generiert wurde.
   - SecretKey— Geben Sie den geheimen Schlüssel ein, der beim Erstellen eines IAM Benutzers generiert wurde.
   - AWS Region — Geben Sie die Region Ihres Indexes ein. Zum Beispiel us-west-2.
   - Dienstname — Geben Sie Kendra ein. Dabei wird zwischen Groß- und Kleinschreibung unterschieden, also muss es sich um Kleinbuchstaben handeln.

   > **Warning**
   >
   > Wenn Sie den falschen Dienstnamen eingeben oder keine Kleinbuchstaben verwenden, wird ein Fehler ausgegeben, sobald Sie Senden auswählen, um die Anfrage zu senden: „Die Anmeldeinformationen sollten auf den richtigen Dienst 'Kendra' beschränkt sein.“
   > Sie müssen außerdem überprüfen, ob Sie den richtigen Zugriffs- und Geheimschlüssel eingegeben haben.

4. Wählen Sie die Registerkarte Header und geben Sie die folgenden Schlüssel- und Wertinformationen ein.
   - Schlüssel: X-Amz-Target

     Wert: com.amazonaws.kendra. AWSKendraFrontendService. Abfrage

- Schlüssel: Content-Encoding

  Wert: amz-1.0

5. Wählen Sie die Registerkarte Körper und gehen Sie wie folgt vor.

   - Wählen Sie den rohen JSON-Typ für den Hauptteil der Anfrage.
   - Geben Sie eine JSON-Datei ein, die Ihre Index-ID und Ihren Abfragetext enthält.

```
{
    "IndexId": "index-id",
    "QueryText": "enter a query here"
}
```

> **Warning**
>
> Wenn Ihr JSON nicht den richtigen Einzug verwendet, wird ein Fehler ausgegeben: ""SerializationException. Überprüfe die Einrückung in deinem JSON.

6. Wählen Sie Senden (in der Nähe oben rechts) aus.

Suche mit erweiterter Abfragesyntax

Mithilfe erweiterter Abfragesyntax oder Operatoren können Sie Abfragen erstellen, die spezifischer sind als Abfragen mit einfachen Schlüsselwörtern oder Abfragen in natürlicher Sprache. Dazu gehören Bereiche, Boolesche Werte, Platzhalter und mehr. Durch die Verwendung von Operatoren können Sie Ihrer Abfrage mehr Kontext geben und die Suchergebnisse weiter verfeinern.

Amazon Kendra unterstützt die folgenden Operatoren.

- Boolean: Logik zur Einschränkung oder Erweiterung der Suche. `amazon AND sports`Beschränkt die Suche beispielsweise darauf, nur nach Dokumenten zu suchen, die beide Begriffe enthalten.
- Klammern: Liest verschachtelte Abfrageausdrücke in der Reihenfolge ihrer Rangfolge. Liest beispielsweise vorher. `(amazon AND sports) NOT rainforest` `(amazon AND sports) NOT rainforest`
- Bereiche: Datums- oder numerische Bereichswerte. Bereiche können inklusiv, exklusiv oder unbegrenzt sein. Sie können beispielsweise nach Dokumenten suchen, die zuletzt zwischen dem 1. Januar 2020 und dem 31. Dezember 2020 aktualisiert wurden, einschließlich dieser Daten.

- Felder: Verwendet ein bestimmtes Feld, um die Suche einzuschränken. Sie können beispielsweise nach Dokumenten suchen, bei denen das Wort „Vereinigte Staaten“ im Feld „Standort“ steht.
- Platzhalter: Entsprechen teilweise einer Textfolge. `Cloud*`Könnte zum Beispiel übereinstimmen CloudFormation. Amazon Kendra unterstützt derzeit nur Platzhalter am Ende.
- Exakte Anführungszeichen: Entspricht genau einer Textfolge. Zum Beispiel Dokumente, die enthalten`"Amazon Kendra" "pricing"`.

Sie können eine Kombination aus jedem der oben genannten Operatoren verwenden.

Beachten Sie, dass eine übermäßige Verwendung von Operatoren oder hochkomplexe Abfragen die Abfragelatenz beeinträchtigen können. Platzhalter gehören zu den teuersten Operatoren, was die Latenz angeht. Als allgemeine Regel gilt: Je mehr Begriffe und Operatoren Sie verwenden, desto größer sind die potenziellen Auswirkungen auf die Latenz. Andere Faktoren, die sich auf die Latenz auswirken, sind die durchschnittliche Größe der indexierten Dokumente, die Größe Ihres Indexes, jegliche Filterung von Suchergebnissen und die Gesamtauslastung Ihres Amazon Kendra Index.

Boolesch

Mithilfe der booleschen Operatoren`AND`,, können Sie Wörter kombinieren oder ausschließen. `OR NOT`

Im Folgenden finden Sie Beispiele für die Verwendung boolescher Operatoren.

`amazon AND sports`

Gibt Suchergebnisse zurück, die sowohl die Begriffe „Amazon“ als auch „Sport“ im Text enthalten, z. B. Amazon Prime Video Sports oder andere ähnliche Inhalte.

`sports OR recreation`

Gibt Suchergebnisse zurück, die die Begriffe „Sport“ oder „Freizeit“ oder beides im Text enthalten.

`amazon NOT rainforest`

Gibt Suchergebnisse zurück, die den Begriff „Amazon“, aber nicht den Begriff „Regenwald“ im Text enthalten. Dies dient dazu, nach Dokumenten über das Unternehmen Amazon zu suchen, nicht über den Amazonas-Regenwald.

Klammern

Sie können verschachtelte Wörter in der Reihenfolge ihrer Rangfolge abfragen, indem Sie Klammern verwenden. Die Klammern geben an, Amazon Kendra wie eine Abfrage gelesen werden soll.

Im Folgenden finden Sie Beispiele für die Verwendung von Klammeroperatoren.

`(amazon AND sports) NOT rainforest`

Gibt Dokumente zurück, die sowohl die Begriffe „Amazon“ als auch „Sport“ im Text enthalten, nicht jedoch den Begriff „Regenwald“. Dies dient der Suche nach Amazon Prime-Videosportarten oder ähnlichen Inhalten, nicht nach Abenteuersportarten im Amazonas-Regenwald. Die Klammern weisen darauf hin, dass dies vorher gelesen werden `amazon AND sports` sollte. `NOT rainforest` Die Abfrage sollte nicht als gelesen werden. `amazon AND (sports NOT rainforest)`

`(amazon AND (sports OR recreation)) NOT rainforest`

Gibt Dokumente zurück, die die Begriffe „Sport“ oder „Freizeit“ oder beides sowie den Begriff „Amazon“ enthalten. Der Begriff „Regenwald“ ist jedoch nicht enthalten. Dies dient dazu, Amazon Prime Video nach Sport oder Freizeit zu durchsuchen, nicht nach Abenteuersportarten im Amazonas-Regenwald. Die Klammern weisen darauf hin, dass dieser Begriff gelesen werden `sports OR recreation` sollte, bevor er mit dem zuvor gelesenen Wort „Amazon“ kombiniert wird. `NOT rainforest` Die Abfrage sollte nicht als gelesen werden. `amazon AND (sports OR (recreation NOT rainforest))`

Bereiche

Sie können einen Wertebereich verwenden, um die Suchergebnisse zu filtern. Sie geben ein Attribut und die Bereichswerte an. Dies kann ein Datum oder ein numerischer Typ sein.

Datumsbereiche müssen die folgenden Formate haben:

- Epoch
- YYYY
- YYYY-MM
- JJJJ-MM-tt
- JJJJ-MM-tt nicht

Sie können auch angeben, ob die unteren und höheren Werte des Bereichs ein- oder ausgeschlossen werden sollen.

Im Folgenden finden Sie Beispiele für die Verwendung von Bereichsoperatoren.

`_processed_date:>2019-12-31 AND _processed_date:<2021-01-01`

Gibt Dokumente zurück, die im Jahr 2020 verarbeitet wurden — also vor dem 31. Dezember 2019 und weniger als dem 1. Januar 2021.

`_processed_date:>=2020-01-01 AND _processed_date:<=2020-12-31`

Gibt Dokumente zurück, die im Jahr 2020 bearbeitet wurden — also größer oder gleich dem 1. Januar 2020 und weniger als oder gleich dem 31. Dezember 2020.

`_document_likes:<1`

Gibt Dokumente zurück, die keine „Gefällt mir“ -Angaben oder kein Benutzerfeedback haben — weniger als 1 „Gefällt mir“.

Sie können angeben, ob ein Bereich so behandelt werden soll, dass er die angegebenen Bereichswerte einschließt oder ausschließt.

Inklusiv

`_last_updated_at:[2020-01-01 TO 2020-12-31]`

Gibt Dokumente zurück, die zuletzt im Jahr 2020 aktualisiert wurden — einschließlich der Tage 1. Dezember 2020 und 31. Dezember 2020.

Exklusiv

`_last_updated_at:{2019-12-31 TO 2021-01-01}`

Gibt Dokumente zurück, die zuletzt im Jahr 2020 aktualisiert wurden — ausgenommen sind die Tage 31. Dezember 2019 und 1. Januar 2021.

< and **>**Verwenden Sie für unbegrenzte Bereiche, die weder inklusiv noch exklusiv sind, einfach die Operatoren. Beispiel: `_last_updated_at:>2019-12-31 AND _last_updated_at:<2021-01-01`

Felder

Sie können Ihre Suche so einschränken, dass nur Dokumente zurückgegeben werden, die einem Wert in einem bestimmten Feld entsprechen. Das Feld kann einen beliebigen Typ haben.

Im Folgenden finden Sie Beispiele für die Verwendung von Kontextoperatoren auf Feldebene.

`status:"Incomplete" AND financial_year:2021`

Gibt Dokumente für das Geschäftsjahr 2021 mit dem Status „unvollständig“ zurück.

`(sports OR recreation) AND country:"United States" AND level:"professional"`

Gibt Dokumente zurück, in denen es um Profisport oder Freizeit in den Vereinigten Staaten geht.

Platzhalter

Sie können Ihre Suche erweitern, um Varianten von Wörtern und Ausdrücken zu berücksichtigen, indem Sie den Platzhalteroperator verwenden. Dies ist nützlich, wenn Sie nach Namensvarianten suchen. Amazon Kendra unterstützt derzeit nur nachfolgende Platzhalter. Die Anzahl der Präfixzeichen für einen Platzhalter am Ende muss größer als zwei sein.

Im Folgenden finden Sie Beispiele für die Verwendung von Platzhalteroperatoren.

`Cloud*`

Gibt Dokumente zurück, die Varianten wie CloudFormation und CloudWatch enthalten.

`kendra*aws`

Gibt Dokumente zurück, die Varianten wie kendra.amazonaws enthalten.

`kendra*aws*`

Gibt Dokumente zurück, die Varianten wie kendra.amazonaws.com enthalten

Genaue Zitate

Sie können Anführungszeichen verwenden, um nach einer exakten Übereinstimmung mit einem Text zu suchen.

Im Folgenden finden Sie Beispiele für die Verwendung von Anführungszeichen.

`"Amazon Kendra" "pricing"`

Gibt Dokumente zurück, die sowohl den Ausdruck " als auch den Begriff Amazon Kendra'Preisgestaltung' enthalten. Dokumente müssen sowohl " als auch Amazon Kendra'Preis' enthalten, damit die Ergebnisse zurückgegeben werden.

`"Amazon Kendra" "pricing" cost`

Gibt Dokumente zurück, die sowohl den Ausdruck 'Amazon Kendra' als auch den Begriff 'Preisgestaltung' und optional den Begriff 'Kosten' enthalten. Dokumente müssen sowohl „Amazon Kendra“ als auch „Preisgestaltung“ enthalten, damit die Ergebnisse zurückgegeben werden, müssen aber nicht unbedingt „Kosten“ enthalten.

Ungültige Abfragesyntax

Amazon Kendra gibt eine Warnung aus, wenn es Probleme mit Ihrer Abfragesyntax gibt oder Ihre Abfrage derzeit nicht unterstützt wird von Amazon Kendra. Weitere Informationen finden Sie in der API-Dokumentation für Abfragewarnungen.

Die folgenden Abfragen sind Beispiele für eine ungültige Abfragesyntax.

`_last_updated_at:<2021-12-32`

Ungültiges Datum. Tag 32 existiert nicht im gregorianischen Kalender, der von verwendet wird. Amazon Kendra

`_view_count:ten`

Ungültiger numerischer Wert. Zahlen müssen verwendet werden, um numerische Werte darzustellen.

`nonExistentField:123`

Ungültige Feldsuche. Das Feld muss vorhanden sein, um die Feldsuche verwenden zu können.

`Product:[A TO D]`

Ungültiger Bereich. Numerische Werte oder Datumsangaben müssen für Bereiche verwendet werden.

`OR Hello`

Ungültiger boolescher Wert. Operatoren müssen zusammen mit Begriffen verwendet und zwischen Begriffen platziert werden.

In Sprachen suchen

Sie können nach Dokumenten in einer unterstützten Sprache suchen. Sie übergeben den Sprachcode in, AttributeFilterum gefilterte Dokumente in der von Ihnen ausgewählten Sprache zurückzugeben. Sie können die Abfrage in einer unterstützten Sprache eingeben.

Wenn Sie keine Sprache angeben, werden Dokumente standardmäßig auf Englisch Amazon Kendra abgefragt. Weitere Informationen zu den unterstützten Sprachen, einschließlich ihrer Codes, finden Sie unter Dokumente in anderen Sprachen als Englisch hinzufügen.

Um in der Konsole nach Dokumenten in einer unterstützten Sprache zu suchen, wählen Sie Ihren Index und dann im Navigationsmenü die Option zum Durchsuchen Ihres Index aus. Wählen Sie die

Sprache aus, in der Sie Dokumente zurückgeben möchten, indem Sie die Sucheinstellungen und dann eine Sprache aus der Dropdownliste Sprache auswählen.

Die folgenden Beispiele zeigen, wie Sie auf Spanisch nach Dokumenten suchen.

Um in der Konsole nach einem Index auf Spanisch zu suchen

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die Amazon Kendra Konsole unter http://console.aws.amazon.com/kendra/.
2. Wählen Sie im Navigationsmenü Indizes und wählen Sie Ihren Index aus.
3. Wählen Sie im Navigationsmenü die Option, um Ihren Index zu durchsuchen.
4. Wählen Sie in den Sucheinstellungen das Drop-down-Menü Sprachen aus und wählen Sie Spanisch aus.
5. Geben Sie eine Abfrage in das Textfeld ein und drücken Sie dann die Eingabetaste.
6. Amazon Kendra gibt die Ergebnisse der Suche auf Spanisch zurück.

Um einen Index auf Spanisch mit der CLI, Python oder Java zu durchsuchen

- Im folgenden Beispiel wird ein Index auf Spanisch durchsucht. Ändern Sie `searchString` den Wert in Ihrer Suchabfrage und den Wert in `indexID` den Bezeichner des Indexes, den Sie durchsuchen möchten. Der Sprachcode für Spanisch lautet`es`. Sie können dies durch Ihren eigenen Sprachcode ersetzen.

  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");
        }
    }
}
```

Passagen werden abgerufen

Sie können die RetrieveAPI als Retriever für Retrieval Augmented Generation (RAG) -Systeme verwenden.

RAG-Systeme verwenden generative künstliche Intelligenz, um Anwendungen zur Beantwortung von Fragen zu erstellen. RAG-Systeme bestehen aus einem Retriever und großen Sprachmodellen (LLM). Bei einer Anfrage identifiziert der Retriever die relevantesten Textblöcke aus einem Korpus von Dokumenten und leitet sie an das LLM weiter, um die nützlichste Antwort zu erhalten. Anschließend analysiert das LLM die relevanten Textblöcke oder Passagen und generiert eine umfassende Antwort auf die Anfrage.

Die `Retrieve` API betrachtet Textblöcke oder Auszüge, die als Passagen bezeichnet werden, und gibt die wichtigsten Passagen zurück, die für die Abfrage am relevantesten sind.

Wie die QueryAPI sucht auch die `Retrieve` API mithilfe der semantischen Suche nach relevanten Informationen. Die semantische Suche berücksichtigt den Kontext der Suchabfrage sowie alle verfügbaren Informationen aus den indizierten Dokumenten. Standardmäßig gibt die `Query` API jedoch nur Auszüge von bis zu 100 Stichwörtern zurück. Mit der `Retrieve` API können Sie längere Passagen mit bis zu 200 Token-Wörtern und bis zu 100 semantisch relevanten Passagen abrufen.

Dies schließt keine Antworten vom Typ Frage-Antwort oder häufig gestellte Fragen aus Ihrem Index ein. Bei den Passagen handelt es sich um Textauszüge, die semantisch aus mehreren Dokumenten und mehreren Teilen desselben Dokuments extrahiert werden können. Wenn Ihre Dokumente im Extremfall mithilfe der `Retrieve` API keine Passagen enthalten, können Sie alternativ die `Query` API und ihre Antworttypen verwenden.

Sie können mit der `Retrieve` API auch Folgendes tun:

- Überschreiben Sie das Boosting auf Indexebene
- Filtern Sie auf der Grundlage von Dokumentfeldern oder Attributen
- Filtern Sie basierend auf dem Benutzer- oder Gruppenzugriff auf Dokumente
- Sehen Sie sich den Bereich mit dem Konfidenzwert für ein abgerufenes Passageergebnis an. Das Konfidenzfeld bietet eine relative Rangfolge, die angibt, wie sicher Amazon Kendra es ist, dass die Antwort für die Abfrage relevant ist.

> **Note**
>
> Buckets mit Konfidenzwerten sind derzeit nur für Englisch verfügbar.

Sie können der Antwort auch bestimmte Felder hinzufügen, die möglicherweise nützliche Zusatzinformationen enthalten.

Die `Retrieve` API unterstützt derzeit nicht alle von der `Query` API unterstützten Funktionen. Die folgenden Funktionen werden nicht unterstützt: Abfragen mit erweiterter Abfragesyntax, vorgeschlagene Rechtschreibkorrekturen für Abfragen, Facettierung, Abfragevorschläge zur automatischen Vervollständigung von Suchanfragen und inkrementelles Lernen. Beachten Sie, dass nicht alle Funktionen für die API gelten. `Retrieve` Alle future Versionen der `Retrieve` API werden in diesem Handbuch dokumentiert.

Die `Retrieve` API teilt sich die Anzahl der Abfragekapazitätseinheiten, die Sie für Ihren Index festgelegt haben. Weitere Informationen darüber, was in einer einzelnen Kapazitätseinheit enthalten ist, und zur Standard-Basiskapazität für einen Index finden Sie unter Kapazität anpassen.

> **Note**
>
> Sie können keine Kapazität hinzufügen, wenn Sie die Amazon Kendra Developer Edition verwenden. Sie können Kapazität nur hinzufügen, wenn Sie die Amazon Kendra Enterprise

Edition verwenden. Weitere Informationen darüber, was in der Developer Edition und der Enterprise Edition enthalten ist, finden Sie unter Amazon Kendra Editionen.

Im Folgenden finden Sie ein Beispiel für die Verwendung der `Retrieve` API, um die 100 relevantesten Passagen aus Dokumenten in einem Index für die Abfrage abzurufen "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");
        }
    }
}
```

Einen Index durchsuchen

Sie können Dokumente nach ihren Attributen oder Facetten durchsuchen, ohne eine Suchabfrage eingeben zu müssen. Amazon Kendra Index Browse kann Ihren Benutzern helfen, Dokumente zu finden, indem sie einen Index frei durchsuchen, ohne eine bestimmte Abfrage im Hinterkopf zu haben. Dies hilft Ihren Benutzern auch dabei, einen Index als Ausgangspunkt für ihre Suche umfassend zu durchsuchen.

Die Indexsuche kann nur für die Suche nach einem Dokumentattribut oder einer Facette mit einem Sortiertyp verwendet werden. Mit der Indexsuche können Sie nicht einen gesamten Index durchsuchen. Wenn der Abfragetext fehlt, werden Sie Amazon Kendra nach einem Dokumentattributfilter oder einer Facette und einem Sortiertyp gefragt.

Um das Durchsuchen von Indizes mithilfe der Abfrage-API zu ermöglichen, müssen Sie AttributeFilteroder Facet und angeben. SortingConfiguration Um das Durchsuchen von Indizes in der Konsole zu ermöglichen, wählen Sie im Navigationsmenü unter Indizes Ihren Index aus und wählen Sie dann die Option, Ihren Index zu durchsuchen. Drücken Sie im Suchfeld zweimal die Eingabetaste. Wählen Sie die Dropdownliste Suchergebnisse filtern aus, um einen Filter auszuwählen, und wählen Sie die Dropdownliste Sortieren aus, um einen Sortierungstyp auszuwählen.

Im Folgenden finden Sie ein Beispiel für das Durchsuchen eines Indexes nach Dokumenten in der Sprache Spanisch in absteigender Reihenfolge des Erstellungsdatums des Dokuments.

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");
        }
    }
}
```

Mit Suchergebnissen

Sie können bestimmte Dokumente in den Suchergebnissen angeben, wenn Ihre Benutzer bestimmte Abfragen stellen. Dies trägt dazu bei, dass die Ergebnisse für Ihre Benutzer sichtbarer und prominenter werden. Ausgewählte Ergebnisse werden von der üblichen Ergebnisliste getrennt und oben auf der Suchseite angezeigt. Sie können damit experimentieren, verschiedene Dokumente für verschiedene Suchanfragen zu präsentieren, oder sicherstellen, dass bestimmte Dokumente die Sichtbarkeit erhalten, die sie verdienen.

Sie ordnen bestimmte Abfragen bestimmten Dokumenten zu, damit sie in den Ergebnissen angezeigt werden. Wenn eine Abfrage eine exakte Übereinstimmung enthält, werden ein oder mehrere spezifische Dokumente in den Suchergebnissen aufgeführt.

Sie können beispielsweise festlegen, dass, wenn Ihre Benutzer die Abfrage „Neue Produkte 2023“ stellen, dann die Dokumente mit den Titeln „Was ist neu“ und „In Kürze verfügbar“ auswählen, die oben auf der Suchergebnisseite angezeigt werden sollen. Dadurch wird sichergestellt, dass diese Dokumente zu neuen Produkten die Aufmerksamkeit erhalten, die sie verdienen.

Amazon Kendra dupliziert keine Suchergebnisse, wenn ein Ergebnis bereits ausgewählt wurde, das oben auf der Suchergebnisseite angezeigt werden soll. Ein hervorgehobenes Ergebnis wird nicht erneut als erstes Ergebnis eingestuft, wenn es bereits vor allen anderen Ergebnissen angezeigt wird.

Um bestimmte Ergebnisse anzuzeigen, müssen Sie eine exakte Übereinstimmung mit einer Volltextabfrage angeben, nicht eine teilweise Übereinstimmung mit einer Abfrage, bei der ein Schlüsselwort oder eine Wortgruppe verwendet wird, die in einer Abfrage enthalten ist. Wenn Sie beispielsweise nur die Abfrage „Kendra“ in einer Ergebnismenge angeben, sind Abfragen wie „Wie ordnet Kendra Ergebnisse semantisch ein?“ rendert die ausgewählten Ergebnisse nicht. Ausgewählte

Ergebnisse sind für spezifische Abfragen konzipiert und nicht für Abfragen, deren Umfang zu umfangreich ist. Amazon Kendra verarbeitet auf natürliche Weise Abfragen vom Typ Schlüsselwort, um die nützlichsten Dokumente in den Suchergebnissen zu ordnen und so zu vermeiden, dass Ergebnisse, die auf einfachen Schlüsselwörtern basieren, übermäßig dargestellt werden.

Wenn es bestimmte Abfragen gibt, die Ihre Benutzer häufig verwenden, können Sie diese Abfragen für besonders beliebte Ergebnisse spezifizieren. Wenn Sie sich beispielsweise mithilfe von Amazon Kendra Analytics Ihre häufigsten Suchanfragen ansehen und dabei bestimmte Abfragen finden, z. B. „Wie ordnet Kendra Ergebnisse semantisch ein?“ und „Semantische Kendra-Suche“ werden häufig verwendet, dann kann es nützlich sein, diese Abfragen zu spezifizieren, um das Dokument mit dem Titel „Suche 101“ anzuzeigen.Amazon Kendra

Amazon Kendra behandelt Abfragen nach ausgewählten Ergebnissen ohne Berücksichtigung der Groß- und Kleinschreibung. Amazon Kendra wandelt eine Abfrage in Kleinbuchstaben um und ersetzt nachfolgende Leerzeichen durch ein einzelnes Leerzeichen. Amazon Kendra entspricht allen anderen Zeichen so, wie sie sind, wenn Sie Ihre Abfragen für herausragende Ergebnisse angeben.

Sie erstellen eine Reihe von ausgewählten Ergebnissen, die Sie mithilfe der CreateFeaturedResultsSetAPI bestimmten Abfragen zuordnen. Wenn Sie die Konsole verwenden, wählen Sie Ihren Index aus und wählen dann im Navigationsmenü die Option Ausgewählte Ergebnisse aus, um einen Satz mit ausgewählten Ergebnissen zu erstellen. Sie können bis zu 50 Gruppen von ausgewählten Ergebnissen pro Index, bis zu vier Dokumente, die pro Satz vorgestellt werden sollen, und bis zu 49 Abfragetexte pro Satz von ausgewählten Ergebnissen erstellen. Sie können eine Erhöhung dieser Limits beantragen, indem Sie sich an den Support wenden.

Sie können dasselbe Dokument aus mehreren Gruppen von ausgewählten Ergebnissen auswählen. Sie dürfen jedoch nicht denselben Abfragetext mit exakt übereinstimmender Übereinstimmung in mehreren Sätzen verwenden. Die Abfragen, die Sie für hervorgehobene Ergebnisse angeben, müssen pro ausgewähltem Ergebnissatz für jeden Index eindeutig sein.

Sie können die Reihenfolge der Dokumente festlegen, wenn Sie bis zu vier ausgewählte Dokumente auswählen. Wenn Sie die API verwenden, entspricht die Reihenfolge, in der Sie die ausgewählten Dokumente auflisten, der in den ausgewählten Ergebnissen angezeigten Reihenfolge. Wenn Sie die Konsole verwenden, können Sie die Reihenfolge der Dokumente einfach per Drag-and-Drop verschieben, wenn Sie Dokumente auswählen, die in den Ergebnissen angezeigt werden sollen.

Die Zugriffskontrolle, bei der bestimmte Benutzer und Gruppen Zugriff auf bestimmte Dokumente haben und andere nicht, wird bei der Konfiguration von ausgewählten Ergebnissen weiterhin berücksichtigt. Das gilt auch für die Filterung von Benutzerkontexten. Beispielsweise gehört Benutzer

A zur Unternehmensgruppe „Praktikanten“, die nicht auf Dokumente zu Unternehmensgeheimnissen zugreifen sollte. Wenn Benutzer A eine Abfrage eingibt, die ein Dokument mit einem Unternehmensgeheimnis enthält, sieht Benutzer A dieses Dokument nicht in seinen Ergebnissen. Das gilt auch für alle anderen Ergebnisse auf der Suchergebnisseite. Sie können Tags auch verwenden, um den Zugriff auf einen Ergebnissatz mit ausgewählten Ergebnissen zu steuern. Dabei handelt es sich um eine Amazon Kendra Ressource, für die Sie den Zugriff kontrollieren.

Im Folgenden finden Sie ein Beispiel für die Erstellung einer Reihe von ausgewählten Ergebnissen mit den Abfragen „Neue Produkte 2023" und „Neue Produkte verfügbar“, die den Dokumenten mit den Titeln „Was ist neu“ (doc-id-1) und „Demnächst“ (doc-id-2) zugeordnet sind.

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.")
```

Tabellarische Suche nach HTML

Amazon Kendra Die tabellarische Suchfunktion kann Antworten aus Tabellen suchen und extrahieren, die in HTML-Dokumente eingebettet sind. Wenn Sie Ihren Index durchsuchen, Amazon Kendra fügt sie einen Auszug aus einer Tabelle hinzu, sofern dieser für die Abfrage relevant ist, und liefert nützliche Informationen.

Amazon Kendra durchsucht alle Informationen im Haupttext eines Dokuments, einschließlich nützlicher Informationen in Tabellen. Ein Index enthält beispielsweise Geschäftsberichte mit Tabellen zu Betriebskosten, Einnahmen und anderen Finanzinformationen. Für die Abfrage „Wie hoch sind die jährlichen Betriebskosten von 2020-2022?“ , Amazon Kendra kann einen Auszug aus einer Tabelle zurückgeben, die die relevanten Tabellenspalten „Operationen (Millionen USD)“ und „Geschäftsjahr“ sowie Tabellenzeilen mit Einkommenswerten für 2020, 2021 und 2022 enthält. Der Tabellenauszug

ist zusammen mit dem Dokumenttitel, einem Link zum vollständigen Dokument und allen anderen Dokumentfeldern, die Sie einbeziehen möchten, im Ergebnis enthalten.

Tabellenauszüge können in den Suchergebnissen angezeigt werden, unabhängig davon, ob sich die Informationen in einer Zelle einer Tabelle oder in mehreren Zellen befinden. Amazon Kendra Kann beispielsweise einen Tabellenauszug anzeigen, der auf jede dieser Arten von Abfragen zugeschnitten ist:

- „Kreditkarte mit dem höchsten Zinssatz im Jahr 2020"
- „Kreditkarte mit dem höchsten Zinssatz von 2020-2022"
- „Top 3 Kreditkarten mit dem höchsten Zinssatz in den Jahren 2020-2022"
- „Kreditkarten mit Zinssätzen von weniger als 10%“
- „alle verfügbaren zinsgünstigen Kreditkarten“

Amazon Kendra hebt die Tabellenzelle oder -zellen hervor, die für die Abfrage am relevantesten sind. Die relevantesten Zellen mit den entsprechenden Zeilen, Spalten und Spaltennamen werden im Suchergebnis angezeigt. Der Tabellenauszug zeigt bis zu fünf Spalten und drei Zeilen an, je nachdem, wie viele Tabellenzellen für die Abfrage relevant sind und wie viele Spalten in der Originaltabelle verfügbar sind. Die oberste relevanteste Zelle wird im Tabellenauszug zusammen mit den nächstrelevantesten Zellen angezeigt.

Die Antwort enthält den Konfidenzbereich (`MEDIUM`,`HIGH`,`VERY_HIGH`), der zeigt, wie relevant die Tabellenantwort für die Abfrage ist. Wenn ein Tabellenzellenwert vertraulich ist`VERY_HIGH`, wird er zur „häufigsten Antwort“ und hervorgehoben. Vertrauliche Tabellenzellenwerte werden `HIGH` hervorgehoben. Bei vertraulichen Tabellenzellenwerten werden sie nicht hervorgehoben. `MEDIUM` Die Gesamtsicherheit für die Tabellenantwort wird in der Antwort zurückgegeben. Wenn eine Tabelle beispielsweise hauptsächlich Tabellenzellen mit `HIGH` Konfidenz enthält, dann ist die Gesamtkonfidenz, die in der Antwort für die Tabellenantwort zurückgegeben wird, `HIGH` Konfidenz.

Standardmäßig wird Tabellen kein höheres Maß an Wichtigkeit oder Gewicht beigemessen als anderen Komponenten eines Dokuments. Wenn innerhalb eines Dokuments eine Tabelle für eine Abfrage nur geringfügig relevant ist, es aber einen Absatz mit hoher Relevanz gibt, wird ein Auszug aus dem Absatz Amazon Kendra zurückgegeben. In den Suchergebnissen wird der Inhalt angezeigt, der die bestmögliche Antwort und die nützlichsten Informationen bietet, und zwar im selben Dokument oder in anderen Dokumenten. Wenn die Konfidenz für eine Tabelle unter `MEDIUM` das Konfidenzniveau fällt, wird der Tabellenauszug in der Antwort nicht zurückgegeben.

Um die tabellarische Suche für einen vorhandenen Index zu verwenden, müssen Sie Ihren Inhalt neu indizieren.

Amazon Kendra Die tabellarische Suche unterstützt Synonyme (einschließlich benutzerdefinierter Synonyme). Amazon Kendra unterstützt nur englische Dokumente mit HTML-Tabellen, die sich innerhalb des Tabellen-Tags befinden.

Das folgende Beispiel zeigt einen Tabellenauszug, der im Abfrageergebnis enthalten ist. Ein JSON-Beispiel mit Abfrageantworten, einschließlich Tabellenauszügen, finden Sie unter Abfrageantworten und Typen.

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");
        }
    }
}
```

Vorschläge für Abfragen

Amazon Kendra Abfragevorschläge können Ihren Benutzern helfen, ihre Suchanfragen schneller einzugeben, und sie bei der Suche unterstützen.

Amazon Kendra schlägt Anfragen vor, die für Ihre Benutzer relevant sind, und zwar auf der Grundlage einer der folgenden Kriterien:

- Beliebte Abfragen im Abfrageverlauf oder im Abfrageprotokoll
- Der Inhalt von Feldern/Attributen des Dokuments

Sie können Ihre Präferenz für die Verwendung des Abfrageverlaufs oder der Dokumentfelder festlegen, indem Sie entweder auf `QUERY` oder setzen `SuggestionTypes` `DOCUMENT_ATTRIBUTES` und dann aufrufen. GetQuerySuggestions Amazon Kendra Verwendet standardmäßig den Abfrageverlauf als Grundlage für Vorschläge. Wenn sowohl der Abfrageverlauf als auch die Dokumentfelder beim Aufrufen aktiviert sind UpdateQuerySuggestionsConfigund Sie Ihre `SuggestionTypes` Präferenz für die Verwendung von Dokumentfeldern nicht festgelegt haben, wird der Abfrageverlauf Amazon Kendra verwendet.

Wenn Sie die Konsole verwenden, können Sie Abfragevorschläge entweder auf dem Abfrageverlauf oder auf Dokumentfeldern basieren. Sie wählen zuerst Ihren Index aus und wählen dann im Navigationsmenü unter Erweiterungen die Option Abfragevorschläge aus. Wählen Sie dann Abfragevorschläge konfigurieren aus. Nachdem Sie Abfragevorschläge konfiguriert haben, werden Sie zu einer Suchkonsole weitergeleitet, in der Sie entweder die Felder Abfrageverlauf oder Dokument im rechten Bereich auswählen und eine Suchabfrage in die Suchleiste eingeben können.

Standardmäßig werden Abfragevorschläge, die den Abfrageverlauf und die Dokumentfelder verwenden, beide ohne zusätzliche Kosten aktiviert. Sie können diese Art von Abfragevorschlägen jederzeit mithilfe der `UpdateQuerySuggestionsConfig` API deaktivieren. Um Abfragevorschläge zu deaktivieren, die auf dem Abfrageverlauf basieren, stellen Sie `DISABLED` beim Aufrufen `Mode` auf ein`UpdateQuerySuggestionsConfig`. Um auf Dokumentfeldern basierende Abfragevorschläge `AttributeSuggestionsMode` zu deaktivieren, stellen Sie `INACTIVE` in der Konfiguration der Dokumentfelder auf ein und rufen Sie dann auf`UpdateQuerySuggestionsConfig>`. Wenn Sie die Konsole verwenden, können Sie Abfragevorschläge in den Einstellungen für Abfragevorschläge deaktivieren.

Bei Abfragevorschlägen wird nicht zwischen Groß- und Kleinschreibung unterschieden. Amazon Kendra wandelt das Abfragepräfix und die vorgeschlagene Abfrage in Kleinbuchstaben um, ignoriert alle einfachen und doppelten Anführungszeichen und ersetzt mehrere Leerzeichen durch ein einzelnes Leerzeichen. Amazon Kendra entspricht allen anderen Sonderzeichen, wie sie sind. Amazon Kendra zeigt keine Vorschläge an, wenn ein Benutzer weniger als zwei Zeichen oder mehr als 60 Zeichen eingibt.

Themen

Fragen Sie Vorschläge mithilfe des Abfrageverlaufs ab

Themen

Sie können wählen, ob Sie Abfragen vorschlagen möchten, die für Ihre Benutzer relevant sind, und zwar auf der Grundlage häufig verwendeter Abfragen im Abfrageverlauf oder im Abfrageprotokoll. Amazon Kendra verwendet alle Abfragen, nach denen Ihre Benutzer suchen, und lernt aus diesen Abfragen, um Ihren Benutzern Vorschläge zu unterbreiten. Amazon Kendra schlägt Benutzern beliebte Abfragen vor, wenn sie mit der Eingabe ihrer Anfrage beginnen. Amazon Kendra schlägt eine Abfrage vor, wenn das Präfix oder die ersten Zeichen der Abfrage mit dem übereinstimmen, was der Benutzer als Abfrage eingibt.

Ein Benutzer beginnt beispielsweise mit der Eingabe der Abfrage „bevorstehende Ereignisse“. Amazon Kendra hat aus dem Abfrageverlauf erfahren, dass viele Benutzer viele Male nach „bevorstehende Ereignisse 2050“ gesucht haben. Der Benutzer sieht, dass „bevorstehende Ereignisse 2050“ direkt unter seiner Suchleiste angezeigt werden, wodurch seine Suchabfrage automatisch vervollständigt wird. Der Benutzer wählt diesen Abfragevorschlag aus und das Dokument „Neue Ereignisse: Was passiert in 2050“ wird in den Suchergebnissen angezeigt.

Sie können angeben, wie geeignete Abfragen Amazon Kendra ausgewählt werden, um Ihren Benutzern vorzuschlagen. Sie können beispielsweise angeben, dass ein Abfragevorschlag von mindestens 10 eindeutigen Benutzern (Standard ist drei) durchsucht worden sein muss, dass er innerhalb der letzten 30 Tage durchsucht wurde und dass er keine Wörter oder Ausdrücke aus Ihrer Sperrliste enthält. Amazon Kendra erfordert, dass eine Abfrage mindestens ein Suchergebnis hat und mindestens ein Wort mit mehr als vier Zeichen enthält.

Einstellungen für die Auswahl von Abfragen für Vorschläge

Sie können die folgenden Einstellungen für die Auswahl von Abfragen für Vorschläge mithilfe der UpdateQuerySuggestionsConfigAPI konfigurieren:

- Modus — Abfragevorschläge, die den Abfrageverlauf verwenden, sind entweder `ENABLED` oder`LEARN_ONLY`. Amazon Kendra aktiviert standardmäßig Abfragevorschläge. `LEARN_ONLY`deaktiviert Abfragevorschläge. Ist diese Option deaktiviert, lernt Amazon Kendra weiterhin Vorschläge, unterbreitet Benutzern jedoch keine Abfragevorschläge.
- Zeitfenster für die Abfrageprotokollierung — Gibt an, wie aktuell Ihre Abfragen in Ihrem Zeitfenster für die Abfrageprotokollierung sind. Das Zeitfenster ist ein ganzzahliger Wert für die Anzahl der Tage vom aktuellen Tag bis zu den vergangenen Tagen.
- Abfragen ohne Benutzerinformationen — Wählen Sie diese Option aus, `TRUE` um alle Abfragen einzubeziehen, oder legen Sie fest, `FALSE` dass nur Abfragen mit Benutzerinformationen eingeschlossen werden. Sie können diese Einstellung verwenden, wenn Ihre Suchanwendung Benutzerinformationen wie die Benutzer-ID enthält, wenn ein Benutzer eine Abfrage ausgibt. Standardmäßig filtert diese Einstellung keine Abfragen heraus, wenn den Abfragen keine spezifischen Benutzerinformationen zugeordnet sind. Sie können diese Einstellung jedoch verwenden, um nur Vorschläge zu unterbreiten, die auf Abfragen basieren, die Benutzerinformationen enthalten.
- Eindeutige Benutzer — Die Mindestanzahl an eindeutigen Benutzern, die eine Abfrage durchsuchen müssen, um sie Ihren Benutzern vorschlagen zu können. Diese Zahl ist eine Ganzzahl.
- Anzahl der Abfragen — Eine Abfrage muss mindestens so oft durchsucht werden, dass sie Ihren Benutzern vorgeschlagen werden kann. Diese Zahl ist eine Ganzzahl.

Diese Einstellungen wirken sich darauf aus, wie Abfragen als beliebte Abfragen ausgewählt werden, um sie Ihren Benutzern vorzuschlagen. Wie Sie Ihre Einstellungen anpassen, hängt von Ihren spezifischen Bedürfnissen ab, zum Beispiel:

- Wenn Ihre Benutzer in der Regel durchschnittlich einmal pro Monat suchen, können Sie die Anzahl der Tage im Zeitfenster für das Abfrageprotokoll auf 30 Tage festlegen. Mit dieser Einstellung erfassen Sie die meisten der letzten Abfragen Ihrer Benutzer, bevor sie im Zeitfenster veraltet sind.
- Wenn nur eine geringe Anzahl Ihrer Abfragen Benutzerinformationen enthält und Sie keine Abfragen vorschlagen möchten, die auf einer kleinen Stichprobengröße basieren, können Sie Abfragen so einrichten, dass sie alle Benutzer einbeziehen.

- Wenn Sie beliebte Abfragen so definieren, dass sie von mindestens 10 eindeutigen Benutzern und mindestens 100 Mal durchsucht werden, legen Sie die eindeutigen Benutzer auf 10 und die Anzahl der Abfragen auf 100 fest.

> **Warning**
>
> Ihre Änderungen an den Einstellungen werden möglicherweise nicht sofort wirksam. Sie können die Änderungen an den Einstellungen mithilfe der DescribeQuerySuggestionsConfigAPI verfolgen. Die Zeit, bis Ihre aktualisierten Einstellungen wirksam werden, hängt von den von Ihnen vorgenommenen Aktualisierungen und der Anzahl der Suchanfragen in Ihrem Index ab. Amazon Kendra aktualisiert die Vorschläge automatisch alle 24 Stunden, nachdem Sie eine Einstellung geändert oder eine Sperrliste angewendet haben.

CLI

Um Abfragevorschläge abzurufen

```
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
```

Um Abfragevorschläge zu aktualisieren

Um beispielsweise das Zeitfenster für das Abfrageprotokoll und die Mindestanzahl der Suchvorgänge für eine Abfrage zu ändern, gehen Sie wie folgt vor:

```
aws kendra update-query-suggestions-config \
 --index-id index-id \
 --query-log-look-back-window-in-days 30 \
 --minimum-query-count 100
```

Python

Um Abfragevorschläge abzurufen

```
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.")
```

Um Abfragevorschläge zu aktualisieren

Um beispielsweise das Zeitfenster für das Abfrageprotokoll und die Mindestanzahl der Suchvorgänge für eine Abfrage zu ändern, gehen Sie wie folgt vor:

```
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.")
```

Vorschläge löschen und gleichzeitig den Abfrageverlauf beibehalten

Sie können Abfragevorschläge mithilfe der ClearQuerySuggestionsAPI löschen. Durch das Löschen von Vorschlägen werden nur vorhandene Abfragevorschläge gelöscht, nicht die Abfragen im Abfrageverlauf. Wenn Sie Vorschläge löschen, Amazon Kendra lernt es neue Vorschläge auf der Grundlage neuer Abfragen, die dem Abfrageprotokoll seit dem Löschen der Vorschläge hinzugefügt wurden.

CLI

Um Abfragevorschläge zu löschen

```
aws  kendra clear-query-suggestions \
 --index-id index-id
```

Python

Um Abfragevorschläge zu löschen

```
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.")
```

Keine Vorschläge verfügbar

Wenn Sie keine Vorschläge für eine Anfrage sehen, kann das einen der folgenden Gründe haben:

- Ihr Index enthält nicht genügend Abfragen, aus denen Amazon Kendra Sie lernen könnten.
- Ihre Einstellungen für Abfragevorschläge sind zu streng, was dazu führt, dass die meisten Abfragen aus den Vorschlägen herausgefiltert werden.
- Sie haben vor Kurzem Vorschläge gelöscht und benötigen Amazon Kendra immer noch Zeit, bis sich neue Abfragen angesammelt haben, um neue Vorschläge zu sammeln.

Sie können Ihre aktuellen Einstellungen mithilfe der DescribeQuerySuggestionsConfigAPI überprüfen.

Fragen Sie Vorschläge mithilfe von Dokumentfeldern ab

Themen

- Einstellungen für die Auswahl von Feldern für Vorschläge
- Benutzersteuerung in Dokumentfeldern

Sie können wählen, ob Sie anhand des Inhalts von Dokumentfeldern Abfragen vorschlagen möchten, die für Ihre Benutzer relevant sind. Anstatt den Abfrageverlauf zu verwenden, um andere beliebte relevante Abfragen vorzuschlagen, können Sie Informationen verwenden, die in einem Dokumentfeld enthalten sind und für die automatische Vervollständigung der Abfrage nützlich sind. Amazon Kendra sucht in Feldern, die auf eingestellt sind, nach `Suggestable` relevantem Inhalt, der eng mit der Anfrage Ihres Benutzers übereinstimmt. Schlägt Ihrem Benutzer diesen Inhalt dann Amazon Kendra vor, wenn er mit der Eingabe seiner Anfrage beginnt.

Wenn Sie beispielsweise das Titelfeld angeben, auf dem Vorschläge basieren sollen, und ein Benutzer beginnt, die Abfrage „Wie Amazon Ken... Amazon Kendra 'könnte der relevanteste Titel „Wie funktioniert“ vorgeschlagen werden, um die Suche automatisch zu vervollständigen. Der Nutzer sieht „So Amazon Kendra funktioniert“ direkt unter seiner Suchleiste und vervollständigt seine

Suchabfrage automatisch. Der Benutzer wählt diesen Abfragevorschlag aus und das Dokument „So Amazon Kendra funktioniert“ wird in den Suchergebnissen angezeigt.

Sie können den Inhalt eines beliebigen Dokumentfeldes `String` und `StringList` -typs verwenden, um eine Abfrage vorzuschlagen, indem Sie das Feld `Suggestable` als Teil Ihrer Feldkonfiguration für Abfragevorschläge auf festlegen. Sie können auch eine Blockliste verwenden, sodass vorgeschlagene Dokumentfelder, die bestimmte Wörter oder Ausdrücke enthalten, Ihren Benutzern nicht angezeigt werden. Sie können eine Blockliste verwenden. Die Sperrliste gilt unabhängig davon, ob Sie Abfragevorschläge so einrichten, dass sie den Abfrageverlauf oder die Dokumentfelder verwenden.

Einstellungen für die Auswahl von Feldern für Vorschläge

Sie können die folgenden Einstellungen für die Auswahl von Dokumentfeldern für Vorschläge konfigurieren, indem Sie die UpdateQuerySuggestionsConfigAPI verwenden AttributeSuggestionsConfigund aufrufen, um die Einstellungen auf Indexebene zu aktualisieren:

- Modus für Feld-/Attributvorschläge — Abfragevorschläge, die Dokumentfelder verwenden, sind entweder oder. `ACTIVE` `INACTIVE` Amazon Kendra aktiviert standardmäßig Abfragevorschläge.
- Suggestible Felder/Attribute — Die Feldnamen oder Feldschlüssel, auf denen Vorschläge basieren sollen. Diese Felder müssen als Teil der `TRUE` Feldkonfiguration auf für `Suggestable` gesetzt werden. Sie können die Feldkonfiguration auf Abfrageebene überschreiben und gleichzeitig die Konfiguration auf Indexebene beibehalten. Verwenden Sie die GetQuerySuggestionsAPI, um Änderungen `AttributeSuggestionConfig` auf Abfrageebene vorzunehmen. Diese Konfiguration auf Abfrageebene kann nützlich sein, um schnell mit der Verwendung verschiedener Dokumentfelder zu experimentieren, ohne die Konfiguration auf Indexebene aktualisieren zu müssen.
- Zusätzliche Felder/Attribute — Die zusätzlichen Felder, die Sie in die Antwort auf einen Abfragevorschlag aufnehmen möchten. Diese Felder werden verwendet, um zusätzliche Informationen in der Antwort bereitzustellen, sie werden jedoch nicht als Grundlage für Vorschläge verwendet.

> **Warning**
>
> Ihre Änderungen an den Einstellungen werden möglicherweise nicht sofort wirksam. Sie können die Änderungen an den Einstellungen mithilfe der DescribeQuerySuggestionsConfigAPI verfolgen. Die Zeit, bis Ihre aktualisierten Einstellungen

wirksam werden, hängt von den Aktualisierungen ab, die Sie vornehmen. Amazon Kendra aktualisiert die Vorschläge automatisch alle 24 Stunden, nachdem Sie eine Einstellung geändert oder eine Sperrliste angewendet haben.

CLI

Um Abfragevorschläge abzurufen und die Konfiguration der Dokumentfelder auf Abfrageebene zu überschreiben, anstatt die Konfiguration auf Indexebene ändern zu müssen.

```
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
```

Um Abfragevorschläge zu aktualisieren

Um beispielsweise die Konfiguration der Dokumentfelder auf Indexebene zu ändern:

```
aws kendra update-query-suggestions-config \
 --index-id index-id \
 --attribute-suggestions-config '{"SuggestableConfigList": '[{"SuggestableConfig":
 "_document_title", "Suggestable": true}]', "AttributeSuggestionsMode": "ACTIVE"}'
```

Python

Um Abfragevorschläge abzurufen und die Konfiguration der Dokumentfelder auf Abfrageebene zu überschreiben, anstatt die Konfiguration auf Indexebene ändern zu müssen.

```
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.")
```

Um Abfragevorschläge zu aktualisieren

Um beispielsweise die Konfiguration der Dokumentfelder auf Indexebene zu ändern:

```
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.")
```

Benutzersteuerung in Dokumentfeldern

Sie können die Benutzerkontextfilterung auf die Dokumentfelder anwenden, auf denen Sie Abfragevorschläge basieren möchten. Dadurch werden Dokumentfeldinformationen basierend auf dem Benutzer- oder Gruppenzugriff auf Dokumente gefiltert. Beispielsweise durchsucht ein Praktikant das Unternehmensportal und hat keinen Zugriff auf ein streng geheimes Unternehmensdokument. Aus diesem Grund werden dem Praktikanten keine Suchanfragen angezeigt, die auf dem Titel des streng geheimen Dokuments oder einem anderen Eingabefeld basieren.

Sie können Ihre Dokumente mit einer Zugriffskontrollliste (ACL) indexieren, in der festgelegt wird, welchen Benutzern und Gruppen Zugriff auf welche Dokumente gewährt wird. Anschließend können Sie die Benutzerkontextfilterung auf Ihre Dokumentenfelder anwenden, um Abfragevorschläge zu erhalten. Die Benutzerkontextfilterung, die derzeit für Ihren Index festgelegt ist, ist dieselbe Benutzerkontextfilterung, die auf Ihre Konfiguration der Dokumentfelder für Abfragevorschläge angewendet wurde. Die Benutzerkontextfilterung ist Teil der Konfiguration Ihrer Dokumentfelder. Sie verwenden den AttributeSuggestionsGetConfigund -Aufruf GetQuerySuggestions.

Sperren Sie bestimmte Abfragen oder dokumentieren Sie Feldinhalte aus Vorschlägen

Eine Blockliste Amazon Kendra verhindert, dass Ihren Benutzern bestimmte Abfragen vorgeschlagen werden. Eine Blockliste ist eine Liste von Wörtern oder Ausdrücken, die Sie von Abfragevorschlägen ausschließen möchten. Amazon Kendra schließt Abfragen aus, die eine exakte Übereinstimmung mit den Wörtern oder Ausdrücken in der Blockliste enthalten.

Sie können eine Sperrliste verwenden, um sich vor anstößigen Wörtern oder Ausdrücken zu schützen, die häufig in Ihrem Abfrageverlauf oder in Dokumentfeldern vorkommen und die als Vorschläge ausgewählt werden Amazon Kendra könnten. Eine Sperrliste kann auch Amazon Kendra verhindern, dass Abfragen vorgeschlagen werden, die Informationen enthalten, die noch nicht veröffentlicht oder angekündigt werden können. Beispielsweise fragen Ihre Benutzer häufig nach einer bevorstehenden Veröffentlichung eines potenziellen neuen Produkts. Sie möchten das Produkt jedoch nicht vorschlagen, da Sie noch nicht bereit sind, es zu veröffentlichen. Sie können Anfragen, die den Produktnamen und Produktinformationen enthalten, aus Vorschlägen ausschließen.

Mithilfe der API können Sie eine Sperrliste für Abfragen erstellen. CreateQuerySuggestionsBlockList Sie fügen jedes Blockwort oder jede Wortgruppe in eine separate Zeile in einer Textdatei ein. Anschließend laden Sie die Textdatei in Ihren Amazon S3 S3-Bucket hoch und geben den Pfad oder

Speicherort der Datei an Amazon S3. Amazon Kendra unterstützt derzeit nur die Erstellung einer Blockliste.

Sie können die Textdatei mit Ihren blockierten Wörtern und Ausdrücken in Ihrem Amazon S3 Bucket ersetzen. Verwenden Sie die UpdateQuerySuggestionsBlockListAPI Amazon Kendra, um die Blockliste zu aktualisieren.

Verwenden Sie die DescribeQuerySuggestionsBlockListAPI, um den Status Ihrer Blockliste abzurufen. `DescribeQuerySuggestionsBlockList`kann Ihnen auch andere nützliche Informationen zur Verfügung stellen, z. B. die folgenden:

- Wann wurde Ihre Sperrliste zuletzt aktualisiert
- Wie viele Wörter oder Ausdrücke befinden sich in Ihrer aktuellen Blockliste
- Hilfreiche Fehlermeldungen beim Erstellen einer Blockliste

Sie können die ListQuerySuggestionsBlockListsAPI auch verwenden, um eine Liste mit Zusammenfassungen von Blocklisten für einen Index abzurufen.

Verwenden Sie die DeleteQuerySuggestionsBlockListAPI, um Ihre Blockliste zu löschen.

Ihre Aktualisierungen der Blockliste werden möglicherweise nicht sofort wirksam. Sie können Aktualisierungen mithilfe der `DescribeQuerySuggestionsBlockList` API verfolgen.

CLI

Um eine Blockliste zu erstellen

```
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
```

Um eine Blockliste zu aktualisieren

```
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
```

Um eine Blockliste zu löschen

```
aws kendra delete-query-suggestions-block-list \
 --index-id index-id \
 --id block-list-id
```

Python

Um eine Blockliste zu erstellen

```
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.")
```

Um eine Blockliste zu aktualisieren

```
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.")
```

Um eine Blockliste zu löschen

```
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.")
```

Rechtschreibprüfung abfragen

Amazon Kendra Die Rechtschreibprüfung schlägt Rechtschreibkorrekturen für eine Abfrage vor. Auf diese Weise können Sie die Anzahl der Suchergebnisse auf ein Minimum reduzieren und relevante Ergebnisse zurückgeben. Ihre Benutzer erhalten möglicherweise keine Suchergebnisse bei falsch geschriebenen Abfragen ohne übereinstimmende Ergebnisse oder ohne zurückgegebene Dokumente. Oder Ihre Benutzer erhalten möglicherweise irrelevante Suchergebnisse aufgrund falsch geschriebener Abfragen.

Die Rechtschreibprüfung ist so konzipiert, dass sie anhand der Wörter, die in Ihren indizierten Dokumenten vorkommen, Korrekturen für falsch geschriebene Wörter vorschlägt und darauf basiert, wie genau ein korrigiertes Wort mit einem falsch geschriebenen Wort übereinstimmt. Wenn

beispielsweise das Wort „Kontoauszüge“ in Ihren indexierten Dokumenten vorkommt, könnte dies dem falsch geschriebenen Wort „Kontoauszüge“ in der Abfrage „Jahresabschlüsse“ sehr ähnlich sein.

Die Rechtschreibprüfung gibt die beabsichtigten oder korrigierten Wörter zurück, die falsch geschriebene Wörter im ursprünglichen Abfragetext ersetzen. Zum Beispiel könnte „Kendre-Suche bereitstellen“ „Kendra-Suche bereitstellen“ zurückgeben. Sie können auch Offset-Positionen verwenden, die in der API bereitgestellt werden, um die zurückgegebenen korrigierten Wörter in einer Abfrage in Ihrer Frontend-Anwendung hervorzuheben oder kursiv zu formatieren. In der Konsole sind die korrigierten Wörter standardmäßig hervorgehoben oder kursiv gedruckt. Zum Beispiel „Kendra Search bereitstellen“.

Bei unternehmensspezifischen oder speziellen Begriffen, die in Ihren indizierten Dokumenten vorkommen, interpretiert Spell Checker diese Begriffe nicht als Rechtschreibfehler in der Abfrage. Beispielsweise wird „Amazon Macie“ nicht in „Amazon Mace“ geändert.

Wörter mit Bindestrich wie „Jahresende“ behandelt die Rechtschreibprüfung als einzelne Wörter und schlägt Korrekturen für diese Wörter vor. Die vorgeschlagene Korrektur für „Jahresende“ könnte beispielsweise „Jahresende“ lauten.

Für Antworttypen `DOCUMENT` und `QUESTION_ANSWER` Abfragen schlägt die Rechtschreibprüfung anhand von Wörtern im Hauptteil des Dokuments Korrekturen für falsch geschriebene Wörter vor. Der Hauptteil des Dokuments ist zuverlässiger als der Titel, wenn es darum geht, Korrekturen vorzuschlagen, die den falsch geschriebenen Wörtern sehr nahe kommen. Bei Antworten auf `ANSWER` Abfragen schlägt die Rechtschreibprüfung Korrekturen vor, die auf Wörtern im Standarddokument für Fragen und Antworten in Ihrem Index basieren.

Sie können die Rechtschreibprüfung mithilfe des SpellCorrectionConfigurationObjekts aktivieren. Sie haben auf eingestelltIncludeQuerySpellCheckSuggestions. `TRUE` Die Rechtschreibprüfung ist in der Konsole standardmäßig aktiviert. Sie ist standardmäßig in die Konsole integriert.

Die Rechtschreibprüfung kann auch Rechtschreibkorrekturen für Abfragen in mehreren Sprachen vorschlagen, nicht nur in Englisch. Eine Liste der Sprachen, die von Spell Checker unterstützt werden, finden Sie unter Amazon Kendra Unterstützte Sprachen.

Verwenden der Abfrage-Rechtschreibprüfung mit Standardgrenzwerten

Die Rechtschreibprüfung ist mit bestimmten Standardeinstellungen oder Grenzwerten konzipiert. Im Folgenden finden Sie eine Liste der aktuellen Grenzwerte, die gelten, wenn Sie Vorschläge zur Rechtschreibkorrektur aktivieren.

- Vorgeschlagene Rechtschreibkorrekturen können nicht für Wörter zurückgegeben werden, die weniger als drei Zeichen oder mehr als 30 Zeichen lang sind. Wenn Sie mehr als 30 Zeichen oder weniger als drei Zeichen zulassen möchten, wenden Sie sich an den Support.
- Vorgeschlagene Rechtschreibkorrekturen können Vorschläge, die auf der Benutzerzugriffskontrolle oder Ihrer Zugriffskontrollliste für die Benutzerkontextfilterung basieren, nicht einschränken. Rechtschreibkorrekturen basieren auf allen Wörtern in Ihren indizierten Dokumenten, unabhängig davon, ob die Wörter auf bestimmte Benutzer beschränkt sind oder nicht. Wenn Sie vermeiden möchten, dass bestimmte Wörter in den vorgeschlagenen Rechtschreibkorrekturen für Abfragen vorkommen, sollten Sie diese Option nicht aktivieren`SpellCorrectionConfiguration`.
- Vorgeschlagene Rechtschreibkorrekturen können für Wörter, die Zahlen enthalten, nicht zurückgegeben werden. Zum Beispiel „how 2 not br8k ubun2“.
- Vorgeschlagene Rechtschreibkorrekturen dürfen keine Wörter verwenden, die nicht in Ihren indizierten Dokumenten vorkommen.
- Bei den vorgeschlagenen Rechtschreibkorrekturen dürfen keine Wörter verwendet werden, die in Ihren indexierten Dokumenten weniger als 0,01 Prozent vorkommen. Um den Schwellenwert von 0,01% zu ändern, wenden Sie sich an den Support.

Filterung und Facettensuche

Sie können die Suchergebnisse oder die Antwort der Query API verbessern, indem Sie Filter verwenden. Filter beschränken die Anzahl der Dokumente in der Antwort auf Dokumente, die direkt auf die Abfrage zutreffen. Um facettierte Suchvorschläge zu erstellen, verwenden Sie die boolesche Logik, um bestimmte Dokumentattribute oder Dokumente, die bestimmten Kriterien nicht entsprechen, aus der Antwort herauszufiltern. Sie können Facetten mithilfe des `Facets` Parameters in der API angeben. `Query`

Verwenden Sie AMAZON, um nach Dokumenten zu suchen, die Sie mit Amazon Kendra for Amazon Lex indexiert haben. KendraSearchIntent. Ein Beispiel für die Konfiguration Amazon Kendra mit Amazon Lex finden Sie unter Einen FAQ-Bot für einen Amazon Kendra Index erstellen. Sie können auch einen Filter für die Antwort bereitstellen, indem Sie AttributeFilter Dies ist der Abfragefilter in JSON bei der Konfiguration`AMAZON.KendraSearchIntent`. Um bei der Konfiguration einer Suchabsicht in der Konsole einen Attributfilter bereitzustellen, rufen Sie den Intent-Editor auf und wählen Sie Amazon Kendra Query aus, um einen Abfragefilter in JSON bereitzustellen. Weitere Informationen zu `AMAZON.KendraSearchIntent` finden Sie im Amazon Lex Dokumentationsleitfaden.

Facets

Facetten sind bereichsbezogene Ansichten einer Reihe von Suchergebnissen. Sie können beispielsweise Suchergebnisse für Städte auf der ganzen Welt bereitstellen, in denen Dokumente nach einer bestimmten Stadt gefiltert werden, der sie zugeordnet sind. Oder Sie können Facetten erstellen, um Ergebnisse eines bestimmten Autors anzuzeigen.

Sie können ein Dokumentattribut oder ein Metadatenfeld, das einem Dokument zugeordnet ist, als Facette verwenden, sodass Ihre Benutzer innerhalb dieser Facette nach Kategorien oder Werten suchen können. Sie können auch verschachtelte Facetten in den Suchergebnissen anzeigen, sodass Ihre Benutzer nicht nur nach einer Kategorie oder einem Feld, sondern auch nach einer Unterkategorie oder einem Unterfeld suchen können.

Das folgende Beispiel zeigt, wie Facetteninformationen für das benutzerdefinierte Attribut „Stadt“ abgerufen werden.

```
response=kendra.query(
        QueryText = query,
        IndexId = index,
        Facets = [
            {
                "DocumentAttributeKey" : "City"
            }
        ]
        )
```

Sie können verschachtelte Facetten verwenden, um die Suche weiter einzugrenzen. Beispielsweise enthält das Dokumentattribut oder die Facette „Stadt“ einen Wert namens „Seattle“. Darüber hinaus enthält das Dokumentattribut oder die Facette "CityRegion" die Werte „North“ und „South“ für Dokumente, die „Seattle“ zugewiesen sind. Sie können verschachtelte Facetten mit ihrer Anzahl in den Suchergebnissen anzeigen, sodass Dokumente nicht nur nach Stadt, sondern auch nach einer Region innerhalb einer Stadt durchsucht werden können.

Beachten Sie, dass verschachtelte Facetten die Abfragelatenz beeinflussen können. Als allgemeine Regel gilt: Je mehr verschachtelte Facetten Sie verwenden, desto größer ist die potenzielle Auswirkung auf die Latenz. Andere Faktoren, die sich auf die Latenz auswirken, sind die durchschnittliche Größe der indizierten Dokumente, die Größe Ihres Indexes, hochkomplexe Abfragen und die Gesamtauslastung Ihres Index. Amazon Kendra

Das folgende Beispiel zeigt, wie Facetteninformationen für das benutzerdefinierte Attribut "CityRegion" als verschachtelte Facette innerhalb von „City“ abgerufen werden.

```
response=kendra.query(
        QueryText = query,
        IndexId = index,
        Facets = [
            {
                "DocumentAttributeKey" : "City",
                "Facets": [
                    {
                        "DocumentAttributeKey" : "CityRegion"
                    }
                ]
            }
        ]
        )
```

Facetteninformationen, wie z. B. die Anzahl der Dokumente, werden im Antwort-Array zurückgegeben. `FacetResults` Sie verwenden den Inhalt, um facettierte Suchvorschläge in Ihrer Anwendung anzuzeigen. Wenn das Dokumentattribut „Stadt“ beispielsweise die Stadt enthält, für die eine Suche gelten könnte, verwenden Sie diese Informationen, um eine Liste von Suchanfragen nach Städten anzuzeigen. Benutzer können eine Stadt auswählen, um ihre Suchergebnisse zu filtern. Um die facettierte Suche durchzuführen, rufen Sie die Query API auf und verwenden Sie das gewählte Dokumentattribut, um die Ergebnisse zu filtern.

Sie können bis zu 10 Facettenwerte pro Facette für eine Abfrage und nur eine verschachtelte Facette innerhalb einer Facette anzeigen. Wenn Sie diese Limits erhöhen möchten, wenden Sie sich an den Support. Wenn Sie die Anzahl der Facettenwerte pro Facette auf weniger als 10 beschränken möchten, können Sie dies im `Facet` Objekt angeben.

Die folgende JSON-Beispielantwort zeigt Facetten, die auf das Dokumentattribut „City“ beschränkt sind. Die Antwort beinhaltet die Anzahl der Dokumente für den Facettenwert.

```
{
    'FacetResults': [
        {
            'DocumentAttributeKey': 'City',
            'DocumentAttributeValueCountPairs': [
                {
                    'Count': 3,
```

```
                    'DocumentAttributeValue': {
                        'StringValue': 'Dubai'
                    }
                },
                {
                    'Count': 3,
                    'DocumentAttributeValue': {
                        'StringValue': 'Seattle'
                    }
                },
                {
                    'Count': 1,
                    'DocumentAttributeValue': {
                        'StringValue': 'Paris'
                    }
                }
            ]
        }
    ]
```

Sie können auch Facetteninformationen für eine verschachtelte Facette anzeigen, z. B. eine Region innerhalb einer Stadt, um die Suchergebnisse weiter zu filtern.

Die folgende JSON-Beispielantwort zeigt Facetten, die auf das Dokumentattribut "CityRegion" beschränkt sind, als verschachtelte Facette innerhalb von „City“. Die Antwort beinhaltet die Anzahl der Dokumente für die verschachtelten Facettenwerte.

```
{
    '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'
                                    }
                                }
                             ]
                        }
                    ]
                }
        }
    ]
}
```

Wenn Sie ein Zeichenkettenlistenfeld verwenden, um Facetten zu erstellen, basieren die zurückgegebenen Facettenergebnisse auf dem Inhalt der Zeichenfolgenliste. Wenn Sie beispielsweise ein Zeichenkettenlistenfeld haben, das zwei Elemente enthält, eines mit der Liste „Dackel“, „Wursthund“ und eines mit dem Wert „Husky“, erhalten Sie drei Facetten. `FacetResults`

Weitere Informationen finden Sie unter Antworten und Antworttypen abfragen.

Verwenden von Dokumentattributen zum Filtern von Suchergebnissen

`Query`Gibt standardmäßig alle Suchergebnisse zurück. Um Antworten zu filtern, können Sie logische Operationen an den Dokumentattributen ausführen. Wenn Sie beispielsweise nur Dokumente für eine bestimmte Stadt benötigen, können Sie nach den benutzerdefinierten Dokumentattributen „Stadt“ und „Bundesland“ filtern. Verwenden Sie AttributeFilter, um eine boolesche Operation für die von Ihnen angegebenen Filter zu erstellen.

Die meisten Attribute können verwendet werden, um Antworten für alle Antworttypen zu filtern. Das `_excerpt_page_number` Attribut gilt jedoch nur für `ANSWER` Antworttypen, wenn Antworten gefiltert werden.

Das folgende Beispiel zeigt, wie eine logische UND-Operation ausgeführt wird, indem nach einer bestimmten Stadt, Seattle, und einem Bundesstaat, Washington, gefiltert wird.

```
response=kendra.query(
```

```
        QueryText = query,
        IndexId = index,
        AttributeFilter = {'AndAllFilters':
            [
                {"EqualsTo": {"Key": "City","Value": {"StringValue": "Seattle"}}},
                {"EqualsTo": {"Key": "State","Value": {"StringValue": "Washington"}}}
            ]
            }
        )
```

Das folgende Beispiel zeigt, wie eine logische OR-Operation ausgeführt wird, wenn einer der `SourceURI` Schlüssel `FileformatAuthor`, oder den angegebenen Werten entspricht.

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

Verwenden Sie für `StringList` Felder die `ContainsAll` Attributfilter `ContainsAny` oder, um Dokumente mit der angegebenen Zeichenfolge zurückzugeben. Das folgende Beispiel zeigt, wie alle Dokumente zurückgegeben werden, deren `Locations` benutzerdefiniertes Attribut die Werte „Seattle“ oder „Portland“ enthält.

```
response=kendra.query(
        QueryText = query,
        IndexId = index,
        AttributeFilter = {
                "ContainsAny": { "Key": "Locations", "Value": { "StringListValue":
 [ "Seattle", "Portland"] }}
            }
        )
```

Filterung der Attribute der einzelnen Dokumente in den Suchergebnissen

Amazon Kendra gibt Dokumentattribute für jedes Dokument in den Suchergebnissen zurück. Sie können bestimmte Dokumentattribute filtern, die Sie als Teil der Suchergebnisse in die Antwort aufnehmen möchten. Standardmäßig werden alle einem Dokument zugewiesenen Dokumentattribute in der Antwort zurückgegeben.

Im folgenden Beispiel sind nur die `_author` Dokumentattribute `_source_uri` und in der Antwort für ein Dokument enthalten.

```
response=kendra.query(
        QueryText = query,
        IndexId = index,
        RequestedDocumentAttributes = ["_source_uri", "_author"]
        )
```

Nach Benutzerkontext filtern

Sie können die Suchergebnisse eines Benutzers nach dem Zugriff des Benutzers oder seiner Gruppe auf Dokumente filtern. Sie können ein Benutzertoken, eine Benutzer-ID oder ein Benutzerattribut verwenden, um Dokumente zu filtern. Amazon Kendra kann Benutzer auch ihren Gruppen zuordnen. Sie können wählen, ob Sie es AWS IAM Identity Center als Ihren Identitätsspeicher/Ihre Identitätsquelle verwenden möchten.

Die Benutzerkontextfilterung ist eine Art personalisierte Suche mit dem Vorteil, den Zugriff auf Dokumente zu kontrollieren. Beispielsweise sollten nicht alle Teams, die das Unternehmensportal nach Informationen durchsuchen, auf streng geheime Unternehmensdokumente zugreifen, und diese Dokumente sind auch nicht für alle Benutzer relevant. Nur bestimmte Benutzer oder Gruppen von Teams, denen Zugriff auf streng geheime Dokumente gewährt wurde, sollten diese Dokumente in ihren Suchergebnissen sehen.

Wenn ein Dokument indexiert wird Amazon Kendra, wird für die meisten Dokumente eine entsprechende Zugriffskontrollliste (ACL) aufgenommen. Die ACL gibt an, welche Benutzer- und Gruppennamen der Zugriff auf das Dokument erlaubt oder verweigert wird. Dokumente ohne ACL sind öffentliche Dokumente.

Amazon Kendra kann für die meisten Datenquellen die Benutzer- oder Gruppeninformationen extrahieren, die jedem Dokument zugeordnet sind. Ein Dokument in Quip kann beispielsweise eine Liste mit ausgewählten Benutzern enthalten, denen Zugriff auf das Dokument gewährt wird. Wenn

Sie einen S3-Bucket als Datenquelle verwenden, stellen Sie eine JSON-Datei für Ihre ACL bereit und fügen den S3-Pfad zu dieser Datei als Teil der Datenquellenkonfiguration hinzu. Wenn Sie Dokumente direkt zu einem Index hinzufügen, geben Sie die ACL im Principal-Objekt als Teil des Dokumentobjekts in der BatchPutDocumentAPI an.

Sie können die CreateAccessControlConfigurationAPI verwenden, um Ihre bestehende Zugriffskontrolle auf Dokumentebene neu zu konfigurieren, ohne alle Ihre Dokumente erneut indizieren zu müssen. Ihr Index enthält beispielsweise streng geheime Unternehmensdokumente, auf die nur bestimmte Mitarbeiter oder Benutzer zugreifen sollten. Einer dieser Benutzer verlässt das Unternehmen oder wechselt zu einem Team, das für den Zugriff auf streng geheime Dokumente gesperrt werden sollte. Der Benutzer hat weiterhin Zugriff auf streng geheime Dokumente, da er Zugriff hatte, als Ihre Dokumente zuvor indexiert wurden. Sie können eine spezielle Konfiguration der Zugriffskontrolle für den Benutzer erstellen, dem der Zugriff verweigert wurde. Sie können die Konfiguration der Zugriffskontrolle später aktualisieren, um den Zugriff zu ermöglichen, falls der Benutzer in das Unternehmen zurückkehrt und wieder dem „streng geheimen“ Team beitritt. Sie können die Zugriffskontrolle für Ihre Dokumente neu konfigurieren, wenn sich die Umstände ändern.

Um Ihre Zugriffskontrollkonfiguration auf bestimmte Dokumente anzuwenden, rufen Sie die BatchPutDocumentAPI mit dem im Dokument `AccessControlConfigurationId` enthaltenen Objekt auf. Wenn Sie einen S3-Bucket als Datenquelle verwenden, aktualisieren Sie den `.metadata.json` mit der `AccessControlConfigurationId` und synchronisieren Ihre Datenquelle. Amazon Kendra unterstützt derzeit nur die Konfiguration der Zugriffskontrolle für S3-Datenquellen und Dokumente, die mithilfe der `BatchPutDocument` API indexiert wurden.

Filterung nach Benutzertoken

Wenn Sie einen Index abfragen, können Sie ein Benutzertoken verwenden, um Suchergebnisse nach dem Benutzer- oder Gruppenzugriff auf Dokumente zu filtern. Wenn Sie eine Abfrage ausgeben, wird das Token Amazon Kendra extrahiert und validiert, die Benutzer- und Gruppeninformationen abgerufen und überprüft und die Abfrage ausgeführt. Alle Dokumente, auf die der Benutzer Zugriff hat, einschließlich öffentlicher Dokumente, werden zurückgegeben. Weitere Informationen finden Sie unter Tokenbasierte Benutzerzugriffskontrolle.

Sie geben das Benutzertoken im UserContextObjekt an und übergeben es in der Abfrage-API.

Im Folgenden wird gezeigt, wie ein Benutzertoken eingefügt wird.

```
response = kendra.query(
    QueryText = query,
    IndexId = index,
```

```
    UserToken = {
        Token = "token"
    })
```

Sie können Benutzer Gruppen zuordnen. Wenn Sie die Benutzerkontextfilterung verwenden, ist es nicht erforderlich, bei der Ausgabe der Abfrage alle Gruppen einzubeziehen, denen ein Benutzer angehört. Mit der PutPrincipalMappingAPI können Sie Benutzer ihren Gruppen zuordnen. Wenn Sie die `PutPrincipalMapping` API nicht verwenden möchten, müssen Sie den Benutzernamen und alle Gruppen angeben, zu denen der Benutzer gehört, wenn Sie eine Anfrage stellen. Mithilfe des Objekts können Sie auch Zugriffsebenen von Gruppen und Benutzern in Ihrer IAM Identity Center-Identitätsquelle abrufen. UserGroupResolutionConfiguration

Nach Benutzer-ID und Gruppe filtern

Wenn Sie einen Index abfragen, können Sie anhand der Benutzer-ID und der Gruppe die Suchergebnisse nach dem Benutzer- oder Gruppenzugriff auf Dokumente filtern. Wenn Sie eine Abfrage ausgeben, werden die Benutzer- und Gruppeninformationen Amazon Kendra überprüft und die Abfrage ausgeführt. Alle für die Abfrage relevanten Dokumente, auf die der Benutzer Zugriff hat, einschließlich öffentlicher Dokumente, werden zurückgegeben.

Sie können Suchergebnisse auch nach Datenquellen filtern, auf die Benutzer und Gruppen Zugriff haben. Die Angabe einer Datenquelle ist nützlich, wenn eine Gruppe an mehrere Datenquellen gebunden ist, Sie aber möchten, dass die Gruppe nur auf Dokumente einer bestimmten Datenquelle zugreift. Beispielsweise sind die Gruppen „Forschung“, „Technik“ und „Vertrieb und Marketing“ alle an die Dokumente des Unternehmens gebunden, die in den Datenquellen Confluence und Salesforce gespeichert sind. Das Team „Vertrieb und Marketing“ benötigt jedoch nur Zugriff auf kundenbezogene Dokumente, die in Salesforce gespeichert sind. Wenn Vertriebs- und Marketingbenutzer also nach kundenbezogenen Dokumenten suchen, können sie Dokumente von Salesforce in ihren Ergebnissen sehen. Benutzer, die nicht in Vertrieb und Marketing arbeiten, sehen in ihren Suchergebnissen keine Salesforce-Dokumente.

Sie geben die Benutzer-, Gruppen- und Datenquelleninformationen im UserContextObjekt an und übergeben diese an die Query-API. Die Benutzer-ID und die Liste der Gruppen und Datenquellen sollten mit dem Namen übereinstimmen, den Sie im Principal-Objekt angeben, um den Benutzer, die Gruppen und Datenquellen zu identifizieren. Mit dem `Principal` Objekt können Sie einen Benutzer, eine Gruppe oder eine Datenquelle entweder einer Zulassungsliste oder einer Verweigerungsliste für den Zugriff auf ein Dokument hinzufügen.

Sie müssen eine der folgenden Angaben machen:

- Benutzer- und Gruppeninformationen sowie (optionale) Informationen zu Datenquellen.
- Nur die Benutzerinformationen, wenn Sie Ihre Benutzer mithilfe der PutPrincipalMappingAPI Gruppen und Datenquellen zuordnen. Mithilfe des Objekts können Sie auch Zugriffsebenen von Gruppen und Benutzern in Ihrer IAM Identity Center-Identitätsquelle abrufen. UserGroupResolutionConfiguration

Wenn diese Informationen nicht in der Abfrage enthalten sind, werden alle Dokumente Amazon Kendra zurückgegeben. Wenn Sie diese Informationen angeben, werden nur Dokumente mit übereinstimmenden Benutzer-IDs, Gruppen und Datenquellen zurückgegeben.

Im Folgenden wird gezeigt, wie Benutzer-ID, Gruppen und Datenquellen eingeschlossen werden.

```
response = kendra.query(
    QueryText = query,
    IndexId = index,
    UserId = {
        UserId = "user1"
    },
    Groups = {
        Groups = ["Sales and Marketing"]
    },
    DataSourceGroups = {
        DataSourceGroups = [{"DataSourceId" : "SalesforceCustomerDocsGroup", "GroupId":
 "Sales and Marketing"}]
    })
```

Nach Benutzerattribut filtern

Wenn Sie einen Index abfragen, können Sie integrierte Attribute verwenden `_user_id` und `_group_id` Suchergebnisse nach dem Benutzer- und Gruppenzugriff auf Dokumente filtern. Sie können bis zu 100 Gruppen-IDs einrichten. Wenn Sie eine Abfrage ausgeben, werden die Benutzer- und Gruppeninformationen Amazon Kendra überprüft und die Abfrage ausgeführt. Alle für die Abfrage relevanten Dokumente, auf die der Benutzer Zugriff hat, einschließlich öffentlicher Dokumente, werden zurückgegeben.

Sie geben die Benutzer- und Gruppenattribute im AttributeFilterObjekt an und übergeben diese an die Abfrage-API.

Das folgende Beispiel zeigt eine Anfrage, bei der die Abfrageantwort anhand der Benutzer-ID und der Gruppen „HR“ und „IT“, zu denen der Benutzer gehört, gefiltert wird. Die Abfrage gibt jedes Dokument

zurück, das den Benutzer oder die Gruppen „HR“ oder „IT“ in der Zulassungsliste enthält. Wenn der Benutzer oder eine der Gruppen auf der Sperrliste für ein Dokument steht, wird das Dokument nicht zurückgegeben.

```
response = kendra.query(
        QueryText = query,
        IndexId = index,
        AttributeFilter = {
            "OrAllFilters": [
                {
                    "EqualsTo": {
                        "Key": "_user_id",
                        "Value": {
                            "StringValue": "user1"
                        }
                     }
                },
                {
                    "EqualsTo": {
                        "Key": "_group_ids",
                        "Value": {
                            "StringListValue": ["HR", "IT"]
                        }
                    }
                }
            ]
        }
        )
```

Sie können auch angeben, auf welche Datenquelle eine Gruppe im `Principal` Objekt zugreifen kann.

> **Note**
>
> Die Benutzerkontextfilterung ist keine Authentifizierungs- oder Autorisierungssteuerung für Ihre Inhalte. Es führt keine Benutzerauthentifizierung für den Benutzer und die Gruppen durch, die an die `Query` API gesendet wurden. Es liegt an Ihrer Anwendung, sicherzustellen, dass die an die `Query` API gesendeten Benutzer- und Gruppeninformationen authentifiziert und autorisiert sind.

Für jede Datenquelle gibt es eine Implementierung der Benutzerkontextfilterung. Im folgenden Abschnitt werden die einzelnen Implementierungen beschrieben.

Themen

Filterung des Benutzerkontextes für Dokumente, die direkt zu einem Index hinzugefügt wurden

Wenn Sie Dokumente mithilfe der BatchPutDocumentAPI direkt zu einem Index hinzufügen, Amazon Kendra werden Benutzer- und Gruppeninformationen aus dem `AccessControlList` Feld des Dokuments abgerufen. Sie stellen eine Zugriffskontrollliste (ACL) für Ihre Dokumente bereit, und die ACL wird zusammen mit Ihren Dokumenten aufgenommen.

Sie geben die ACL im Principal-Objekt als Teil des Document-Objekts in der `BatchPutDocument` API an. Sie geben die folgenden Informationen an:

- Der Zugriff, den der Benutzer oder die Gruppe haben sollte. Sie können `ALLOW` oder sagen`DENY`.
- Die Art der Entität. Du kannst sagen `USER` oder`GROUP`.
- Der Name des Benutzers oder der Gruppe.

Sie können dem `AccessControlList` Feld bis zu 200 Einträge hinzufügen.

Filterung des Benutzerkontextes für häufig gestellte Fragen

Wenn Sie einem Index eine häufig gestellte Frage hinzufügen, werden Benutzer- und Gruppeninformationen aus dem `AccessControlList` Objekt/Feld der FAQ-JSON-Datei Amazon Kendra abgerufen. Sie können auch eine FAQ-CSV-Datei mit benutzerdefinierten Feldern oder Attributen für die Zugriffskontrolle verwenden.

Sie geben die folgenden Informationen an:

- Der Zugriff, den der Benutzer oder die Gruppe haben sollte. Sie können `ALLOW` oder sagen`DENY`.
- Die Art der Entität. Du kannst sagen `USER` oder`GROUP`.
- Der Name des Benutzers oder der Gruppe.

Weitere Informationen finden Sie in den FAQ-Dateien.

Filterung des Benutzerkontextes für Datenquellen

Amazon Kendra durchsucht auch Informationen über Benutzer- und Gruppenzugriffskontrolllisten (ACL) von unterstützten Datenquellen-Connectors. Dies ist nützlich für die Benutzerkontextfilterung, bei der Suchergebnisse nach dem Benutzer- oder Gruppenzugriff auf Dokumente gefiltert werden.

Themen

- Benutzerkontextfilterung für SharePoint Microsoft-Datenquellen
- Benutzerkontextfilterung für Microsoft SQL Server-Datenquellen
- Benutzerkontextfilterung für Microsoft Teams-Datenquellen
- Benutzerkontextfilterung für Microsoft Yammer-Datenquellen
- Benutzerkontextfilterung für MySQL-Datenquellen
- Filterung des Benutzerkontextes für Oracle-Datenbankdatenquellen
- Benutzerkontextfilterung für PostgreSQL-Datenquellen
- Filterung des Benutzerkontextes für Quip-Datenquellen
- Filterung des Benutzerkontextes für Salesforce-Datenquellen
- Filterung des Benutzerkontextes für ServiceNow Datenquellen
- Filterung des Benutzerkontextes für Slack-Datenquellen
- Filterung des Benutzerkontextes für Zendesk-Datenquellen

Filterung des Benutzerkontextes für Adobe Experience Manager-Datenquellen

Wenn Sie eine Adobe Experience Manager-Datenquelle verwenden, Amazon Kendra ruft die Benutzer- und Gruppeninformationen aus der Adobe Experience Manager-Instanz ab.

Die Gruppen- und Benutzer-IDs werden wie folgt zugeordnet:

- `_group_ids`— Gruppen-IDs existieren in Adobe Experience Manager-Inhalten, für die es festgelegte Zugriffsberechtigungen gibt. Sie werden anhand der Namen der Gruppen in Adobe Experience Manager zugeordnet.
- `_user_id`— Benutzer-IDs existieren in Adobe Experience Manager-Inhalten, für die es festgelegte Zugriffsberechtigungen gibt. Sie werden anhand der Benutzer-E-Mails den IDs in Adobe Experience Manager zugeordnet.

Sie können dem `AccessControlList` Feld bis zu 200 Einträge hinzufügen.

Filterung des Benutzerkontextes für Alfresco-Datenquellen

Wenn Sie eine Alfresco-Datenquelle verwenden, werden die Benutzer- und Gruppeninformationen aus der Alfresco-Instanz Amazon Kendra abgerufen.

Die Gruppen- und Benutzer-IDs werden wie folgt zugeordnet:

- `_group_ids`— Gruppen-IDs existieren in Alfresco für Dateien, für die Zugriffsberechtigungen festgelegt sind. Sie werden anhand der Systemnamen der Gruppen (nicht anhand der Anzeigenamen) in Alfresco zugeordnet.
- `_user_id`— Benutzer-IDs existieren in Alfresco für Dateien, für die Zugriffsberechtigungen festgelegt sind. Sie werden anhand der Benutzer-E-Mails den IDs in Alfresco zugeordnet.

Sie können dem Feld bis zu 200 Einträge hinzufügen. `AccessControlList`

Benutzerkontextfilterung für Aurora (MySQL-) Datenquellen

Wenn Sie eine Aurora (MySQL-) Datenquelle verwenden, Amazon Kendra ruft Benutzer- und Gruppeninformationen aus einer Spalte in der Quelltabelle ab. Sie geben diese Spalte in der Konsole an oder verwenden das TemplateConfigurationObjekt als Teil der CreateDataSourceAPI.

Eine Aurora (MySQL-) Datenbankdatenquelle hat die folgenden Einschränkungen:

- Sie können nur eine Zulassungsliste für eine Datenbankdatenquelle angeben. Sie können keine Sperrliste angeben.
- Sie können nur Gruppen angeben. Sie können keine einzelnen Benutzer für die Zulassungsliste angeben.
- Die Datenbankspalte sollte eine Zeichenfolge sein, die eine durch Semikolons getrennte Liste von Gruppen enthält.

Benutzerkontextfilterung für Aurora (PostgreSQL-) Datenquellen

Wenn Sie eine Aurora (PostgreSQL-) Datenquelle verwenden, Amazon Kendra ruft Benutzer- und Gruppeninformationen aus einer Spalte in der Quelltabelle ab. Sie geben diese Spalte in der Konsole an oder verwenden das TemplateConfigurationObjekt als Teil der CreateDataSourceAPI.

Eine Aurora (PostgreSQL-) Datenbankdatenquelle hat die folgenden Einschränkungen:

- Sie können nur eine Zulassungsliste für eine Datenbankdatenquelle angeben. Sie können keine Sperrliste angeben.
- Sie können nur Gruppen angeben. Sie können keine einzelnen Benutzer für die Zulassungsliste angeben.
- Die Datenbankspalte sollte eine Zeichenfolge sein, die eine durch Semikolons getrennte Liste von Gruppen enthält.

Filterung des Benutzerkontextes für Datenquellen Amazon FSx

Wenn Sie eine Amazon FSx Datenquelle verwenden, Amazon Kendra werden Benutzer- und Gruppeninformationen aus dem Verzeichnisdienst der Amazon FSx Instanz abgerufen.

Die Amazon FSx Gruppen- und Benutzer-IDs werden wie folgt zugeordnet:

- `_group_ids`— Gruppen-IDs existieren in Amazon FSx Dateien, für die Zugriffsberechtigungen festgelegt sind. Sie werden anhand der Systemgruppennamen im Verzeichnisdienst von zugeordnet. Amazon FSx
- `_user_id`— Benutzer-IDs sind in Amazon FSx allen Dateien vorhanden, für die Zugriffsberechtigungen festgelegt wurden. Sie werden anhand der Systembenutzernamen im Verzeichnisdienst von zugeordnet. Amazon FSx

Sie können dem `AccessControlList` Feld bis zu 200 Einträge hinzufügen.

Filterung des Benutzerkontextes für Datenbankdatenquellen

Wenn Sie eine Datenbankdatenquelle verwenden, z. B. Amazon Aurora PostgreSQL Benutzer Amazon Kendra - und Gruppeninformationen aus einer Spalte in der Quelltabelle abrufen. Sie geben diese Spalte im AclConfigurationObjekt als Teil des DatabaseConfigurationObjekts in der CreateDataSourceAPI an.

Eine Datenbankdatenquelle hat die folgenden Einschränkungen:

- Sie können nur eine Zulassungsliste für eine Datenbankdatenquelle angeben. Sie können keine Sperrliste angeben.
- Sie können nur Gruppen angeben. Sie können keine einzelnen Benutzer für die Zulassungsliste angeben.
- Die Datenbankspalte sollte eine Zeichenfolge sein, die eine durch Semikolons getrennte Liste von Gruppen enthält.

Benutzerkontextfilterung für Amazon RDS (Microsoft SQL Server) -Datenquellen

Wenn Sie eine Amazon RDS (Microsoft SQL Server-) Datenquelle verwenden, Amazon Kendra ruft Benutzer- und Gruppeninformationen aus einer Spalte in der Quelltabelle ab. Sie geben diese Spalte in der Konsole an oder verwenden das TemplateConfigurationObjekt als Teil der CreateDataSourceAPI.

Eine Datenbankdatenquelle Amazon RDS (Microsoft SQL Server) hat die folgenden Einschränkungen:

- Sie können nur eine Zulassungsliste für eine Datenbankdatenquelle angeben. Sie können keine Sperrliste angeben.
- Sie können nur Gruppen angeben. Sie können keine einzelnen Benutzer für die Zulassungsliste angeben.
- Die Datenbankspalte sollte eine Zeichenfolge sein, die eine durch Semikolons getrennte Liste von Gruppen enthält.

Benutzerkontextfilterung für Amazon RDS (MySQL-) Datenquellen

Wenn Sie eine Amazon RDS (MySQL-) Datenquelle verwenden, Amazon Kendra ruft Benutzer- und Gruppeninformationen aus einer Spalte in der Quelltabelle ab. Sie geben diese Spalte in der Konsole an oder verwenden das TemplateConfigurationObjekt als Teil der CreateDataSourceAPI.

Eine Amazon RDS (MySQL-) Datenbankdatenquelle hat die folgenden Einschränkungen:

- Sie können nur eine Zulassungsliste für eine Datenbankdatenquelle angeben. Sie können keine Sperrliste angeben.
- Sie können nur Gruppen angeben. Sie können keine einzelnen Benutzer für die Zulassungsliste angeben.
- Die Datenbankspalte sollte eine Zeichenfolge sein, die eine durch Semikolons getrennte Liste von Gruppen enthält.

Filterung des Benutzerkontextes für Amazon RDS (Oracle-) Datenquellen

Wenn Sie eine Amazon RDS (Oracle-) Datenquelle verwenden, Amazon Kendra ruft Benutzer- und Gruppeninformationen aus einer Spalte in der Quelltabelle ab. Sie geben diese Spalte in der Konsole an oder verwenden das TemplateConfigurationObjekt als Teil der CreateDataSourceAPI.

Eine Amazon RDS (Oracle-) Datenbankdatenquelle hat die folgenden Einschränkungen:

- Sie können nur eine Zulassungsliste für eine Datenbankdatenquelle angeben. Sie können keine Sperrliste angeben.
- Sie können nur Gruppen angeben. Sie können keine einzelnen Benutzer für die Zulassungsliste angeben.

- Die Datenbankspalte sollte eine Zeichenfolge sein, die eine durch Semikolons getrennte Liste von Gruppen enthält.

Benutzerkontextfilterung für Amazon RDS (PostgreSQL-) Datenquellen

Wenn Sie eine Amazon RDS (PostgreSQL-) Datenquelle verwenden, Amazon Kendra ruft Benutzer- und Gruppeninformationen aus einer Spalte in der Quelltabelle ab. Sie geben diese Spalte in der Konsole an oder verwenden das TemplateConfigurationObjekt als Teil der CreateDataSourceAPI.

Eine Amazon RDS (PostgreSQL-) Datenbankdatenquelle hat die folgenden Einschränkungen:

- Sie können nur eine Zulassungsliste für eine Datenbankdatenquelle angeben. Sie können keine Sperrliste angeben.
- Sie können nur Gruppen angeben. Sie können keine einzelnen Benutzer für die Zulassungsliste angeben.
- Die Datenbankspalte sollte eine Zeichenfolge sein, die eine durch Semikolons getrennte Liste von Gruppen enthält.

Filterung des Benutzerkontextes für Datenquellen Amazon S3

Sie fügen einem Dokument in einer Amazon S3 Datenquelle Benutzerkontextfilter hinzu, indem Sie eine dem Dokument zugeordnete Metadatendatei verwenden. Sie fügen die Informationen dem `AccessControlList` Feld im JSON-Dokument hinzu. Weitere Informationen zum Hinzufügen von Metadaten zu Dokumenten, die aus einer Amazon S3 Datenquelle indexiert wurden, finden Sie unter S3-Dokumentmetadaten.

Sie geben drei Informationen an:

- Der Zugriff, den die Entität haben sollte. Du kannst sagen `ALLOW` oder`DENY`.
- Die Art der Entität. Du kannst sagen `USER` oder`GROUP`.
- Der Name der Entität.

Sie können dem `AccessControlList` Feld bis zu 200 Einträge hinzufügen.

Filterung des Benutzerkontextes für Amazon WorkDocs Datenquellen

Wenn Sie eine Amazon WorkDocs Datenquelle verwenden, Amazon Kendra ruft Benutzer- und Gruppeninformationen aus der Amazon WorkDocs Instanz ab.

Die Amazon WorkDocs Gruppen- und Benutzer-IDs werden wie folgt zugeordnet:

- `_group_ids`— Gruppen-IDs existieren in Amazon WorkDocs Dateien, für die Zugriffsberechtigungen festgelegt sind. Sie werden anhand der Namen der Gruppen in zugeordnet. Amazon WorkDocs
- `_user_id`— Benutzer-IDs sind in Amazon WorkDocs allen Dateien vorhanden, für die Zugriffsberechtigungen festgelegt wurden. Sie werden anhand der Benutzernamen in zugeordnet. Amazon WorkDocs

Sie können dem `AccessControlList` Feld bis zu 200 Einträge hinzufügen.

Filterung des Benutzerkontextes für Box-Datenquellen

Wenn Sie eine Box-Datenquelle verwenden, Amazon Kendra werden Benutzer- und Gruppeninformationen aus der Box-Instanz abgerufen.

Die Box-Gruppen- und Benutzer-IDs werden wie folgt zugeordnet:

- `_group_ids`— Gruppen-IDs sind in Box für Dateien vorhanden, für die Zugriffsberechtigungen festgelegt wurden. Sie werden anhand der Namen der Gruppen in Box zugeordnet.
- `_user_id`— Benutzer-IDs sind in Box für Dateien vorhanden, für die Zugriffsberechtigungen festgelegt wurden. Sie werden anhand der Benutzer-E-Mails den Benutzer-IDs in Box zugeordnet.

Sie können dem `AccessControlList` Feld bis zu 200 Einträge hinzufügen.

Filterung des Benutzerkontextes für Confluence-Datenquellen

Wenn Sie eine Confluence-Datenquelle verwenden, werden Benutzer- und Gruppeninformationen aus der Confluence-Instanz Amazon Kendra abgerufen.

Sie konfigurieren den Benutzer- und Gruppenzugriff auf Spaces auf der Seite mit den Space-Berechtigungen. Für Seiten und Blogs verwenden Sie die Seite mit Einschränkungen. Weitere Informationen zu Speicherberechtigungen finden Sie unter Übersicht über Speicherberechtigungen auf der Confluence-Support-Website. Weitere Informationen zu Seiten- und Blogeinschränkungen findest du unter Seiteneinschränkungen auf der Confluence-Support-Website.

Die Gruppen- und Benutzernamen von Confluence sind wie folgt zugeordnet:

- `_group_ids`— Gruppennamen sind in Bereichen, Seiten und Blogs vorhanden, für die Einschränkungen gelten. Sie werden dem Namen der Gruppe in Confluence zugeordnet. Gruppennamen werden immer in Kleinbuchstaben geschrieben.

- `_user_id`— Benutzernamen sind in dem Bereich, der Seite oder dem Blog vorhanden, für den Einschränkungen gelten. Sie werden abhängig vom Typ der Confluence-Instanz, die Sie verwenden, zugeordnet.

  Für Confluence Connector v1.0

  - Server — Das `_user_id` ist der Benutzername. Der Benutzername wird immer in Kleinbuchstaben geschrieben.
  - Cloud — Das `_user_id` ist die Konto-ID des Benutzers.

  Für Confluence Connector v2.0

  - Server — Das `_user_id` ist der Benutzername. Der Benutzername wird immer in Kleinbuchstaben geschrieben.
  - Cloud — Das `_user_id` ist die E-Mail-ID des Benutzers.

  > **Important**
  >
  > Damit die Benutzerkontextfilterung für Ihren Confluence-Connector korrekt funktioniert, müssen Sie sicherstellen, dass die Sichtbarkeit eines Benutzers, dem Zugriff auf eine Confluence-Seite gewährt wurde, auf Jeder gesetzt ist. Weitere Informationen findest du in der Atlassian-Dokumentation für Entwickler unter Sichtbarkeit deiner E-Mails einrichten.

Du kannst dem Feld bis zu 200 Einträge hinzufügen. `AccessControlList`

Filterung des Benutzerkontextes für Dropbox-Datenquellen

Wenn Sie eine Dropbox-Datenquelle verwenden, Amazon Kendra ruft die Benutzer- und Gruppeninformationen aus der Dropbox-Instanz ab.

Die Gruppen- und Benutzer-IDs werden wie folgt zugeordnet:

- `_group_ids`— Gruppen-IDs existieren in Dropbox für Dateien, für die Zugriffsberechtigungen festgelegt sind. Sie werden den Namen der Gruppen in Dropbox zugeordnet.

- `_user_id`— In Dropbox gibt es Benutzer-IDs für Dateien, für die Zugriffsberechtigungen festgelegt sind. Sie werden anhand der Benutzer-E-Mails den IDs in Dropbox zugeordnet.

Sie können dem `AccessControlList` Feld bis zu 200 Einträge hinzufügen.

Filterung des Benutzerkontextes für Drupal-Datenquellen

Wenn Sie eine Drupal-Datenquelle verwenden, Amazon Kendra ruft die Benutzer- und Gruppeninformationen aus der Drupal-Instanz ab.

Die Gruppen- und Benutzer-IDs werden wie folgt zugeordnet:

- `_group_ids`— Gruppen-IDs existieren in Drupal für Dateien, für die Zugriffsberechtigungen festgelegt sind. Sie werden anhand der Namen der Gruppen in Drupal zugeordnet.
- `_user_id`— Benutzer-IDs existieren in Drupal für Dateien, für die Zugriffsberechtigungen festgelegt sind. Sie werden anhand der Benutzer-E-Mails den IDs in Drupal zugeordnet.

Sie können dem Feld bis zu 200 Einträge hinzufügen. `AccessControlList`

Filterung des Benutzerkontextes für GitHub Datenquellen

Wenn Sie eine GitHub Datenquelle verwenden, Amazon Kendra ruft Benutzerinformationen aus der GitHub Instanz ab.

Die GitHub Benutzer-IDs werden wie folgt zugeordnet:

- `_user_id`— Benutzer-IDs existieren in GitHub allen Dateien, für die Zugriffsberechtigungen festgelegt sind. Sie werden den Benutzer-E-Mails als IDs in zugeordnet. GitHub

Sie können dem `AccessControlList` Feld bis zu 200 Einträge hinzufügen.

Filterung des Benutzerkontextes für Gmail-Datenquellen

Wenn Sie eine Gmail-Datenquelle verwenden, Amazon Kendra werden die Benutzerinformationen aus der Gmail-Instanz abgerufen.

Die Benutzer-IDs werden wie folgt zugeordnet:

- `_user_id`— Benutzer-IDs existieren in Gmail für Dateien, für die Zugriffsberechtigungen festgelegt sind. Sie werden anhand der Benutzer-E-Mails den IDs in Gmail zugeordnet.

Sie können dem `AccessControlList` Feld bis zu 200 Einträge hinzufügen.

Filterung des Benutzerkontextes für Google Drive-Datenquellen

Eine Google Workspace Drive-Datenquelle gibt Nutzer- und Gruppeninformationen für Google Drive-Nutzer und -Gruppen zurück. Gruppen- und Domänenmitgliedschaft werden dem `_group_ids` Indexfeld zugeordnet. Der Google Drive-Nutzername ist dem `_user_id` Feld zugeordnet.

Wenn Sie eine oder mehrere Benutzer-E-Mail-Adressen in der `Query` API angeben, werden nur Dokumente zurückgegeben, die mit diesen E-Mail-Adressen geteilt wurden. Der folgende `AttributeFilter` Parameter gibt nur Dokumente zurück, die mit "martha@example.com" geteilt wurden.

```
"AttributeFilter": {
                "EqualsTo":{
                   "Key": "_user_id",
                   "Value": {
                       "StringValue": "martha@example.com"
                   }
               }
          }
```

Wenn Sie in der Abfrage eine oder mehrere Gruppen-E-Mail-Adressen angeben, werden nur Dokumente zurückgegeben, die für die Gruppen freigegeben wurden. Der folgende `AttributeFilter` Parameter gibt nur Dokumente zurück, die mit der Gruppe "hr@example.com" geteilt wurden.

```
"AttributeFilter": {
                "EqualsTo":{
                   "Key": "_group_ids",
                   "Value": {
                       "StringListValue": ["hr@example.com"]
                   }
               }
          }
```

Wenn Sie die Domäne in der Abfrage angeben, werden alle Dokumente zurückgegeben, die für die Domäne freigegeben wurden. Der folgende `AttributeFilter` Parameter gibt Dokumente zurück, die mit der Domäne „example.com“ gemeinsam genutzt werden.

```
"AttributeFilter": {
```

```
            "EqualsTo":{
               "Key": "_group_ids",
               "Value": {
                   "StringListValue": ["example.com"]
               }
            }
        }
```

Sie können dem `AccessControlList` Feld bis zu 200 Einträge hinzufügen.

Filterung des Benutzerkontextes für IBM DB2-Datenquellen

Wenn Sie eine IBM DB2-Datenquelle verwenden, werden Benutzer- und Gruppeninformationen aus einer Spalte in der Quelltabelle Amazon Kendra abgerufen. Sie geben diese Spalte in der Konsole an oder verwenden das TemplateConfigurationObjekt als Teil der CreateDataSourceAPI.

Eine IBM DB2-Datenbankdatenquelle hat die folgenden Einschränkungen:

- Sie können nur eine Zulassungsliste für eine Datenbankdatenquelle angeben. Sie können keine Sperrliste angeben.
- Sie können nur Gruppen angeben. Sie können keine einzelnen Benutzer für die Zulassungsliste angeben.
- Die Datenbankspalte sollte eine Zeichenfolge sein, die eine durch Semikolons getrennte Liste von Gruppen enthält.

Filterung des Benutzerkontextes für Jira-Datenquellen

Wenn Sie eine Jira-Datenquelle verwenden, werden Benutzer- und Gruppeninformationen aus der Jira-Instanz Amazon Kendra abgerufen.

Die Jira-Benutzer-IDs werden wie folgt zugeordnet:

- `_user_id`— Benutzer-IDs existieren in Jira für Dateien, für die Zugriffsberechtigungen festgelegt sind. Sie werden anhand der Benutzer-E-Mails den Benutzer-IDs in Jira zugeordnet.

Sie können dem Feld bis zu 200 Einträge hinzufügen. `AccessControlList`

Benutzerkontextfilterung für Microsoft Exchange-Datenquellen

Wenn Sie eine Microsoft Exchange-Datenquelle verwenden, Amazon Kendra ruft die Benutzerinformationen aus der Microsoft Exchange-Instanz ab.

Die Microsoft Exchange-Benutzer-IDs sind wie folgt zugeordnet:

- `_user_id`— In Microsoft Exchange-Berechtigungen gibt es Benutzer-IDs, mit denen Benutzer auf bestimmte Inhalte zugreifen können. Sie werden anhand der Benutzernamen als IDs in Microsoft Exchange zugeordnet.

Sie können dem `AccessControlList` Feld bis zu 200 Einträge hinzufügen.

Benutzerkontextfilterung für OneDrive Microsoft-Datenquellen

Amazon Kendra ruft Benutzer- und Gruppeninformationen von Microsoft ab OneDrive , wenn es die Dokumente auf der Site indexiert. Die Benutzer- und Gruppeninformationen stammen von der zugrunde liegenden SharePoint Microsoft-Website, die hostet OneDrive.

Wenn Sie einen OneDrive Benutzer oder eine Gruppe zum Filtern von Suchergebnissen verwenden, berechnen Sie die ID wie folgt:

1. Ermitteln Sie den Namen der Site. Beispiel: `https://host.onmicrosoft.com/sites/siteName.`
2. Nehmen Sie den MD5-Hash des Site-Namens. z. B. `430a6b90503eef95c89295c8999c7981`.
3. Erstellen Sie die Benutzer-E-Mail oder Gruppen-ID, indem Sie den MD5-Hash mit einem senkrechten Balken (|) und der ID verketten. Wenn ein Gruppenname beispielsweise "localGroupName„lautet, wäre die Gruppen-ID:

   ```
   "430a6b90503eef95c89295c8999c7981 | localGroupName"
   ```

   > **Note**
   >
   > Fügen Sie vor und nach dem senkrechten Balken ein Leerzeichen ein. Der vertikale Balken wird verwendet, um sich `localGroupName` mit seinem MD5-Hash zu identifizieren.

Für den Benutzernamen "someone@host.onmicrosoft.com" würde die Benutzer-ID wie folgt lauten:

```
"430a6b90503eef95c89295c8999c7981 | someone@host.onmicrosoft.com"
```

Senden Sie die Benutzer- oder Gruppen-ID Amazon Kendra als `_group_id` Attribut `_user_id` oder, wenn Sie die Abfrage-API aufrufen. Der AWS CLI Befehl, der eine Gruppe zum Filtern der Suchergebnisse verwendet, sieht beispielsweise so aus:

```
aws kendra  query \
                --index-id index ID
                --query-text "query text"
                --attribute-filter '{
                   "EqualsTo":{
                     "Key": "_group_id",
                     "Value": {"StringValue": "430a6b90503eef95c89295c8999c7981 |
 localGroupName"}
                  }}'
```

Sie können dem `AccessControlList` Feld bis zu 200 Einträge hinzufügen.

Benutzerkontextfilterung für Microsoft OneDrive v2.0-Datenquellen

Eine Microsoft OneDrive v2.0-Datenquelle gibt Abschnitts- und Seiteninformationen aus ACL-Entitäten (OneDrive Access Control List) zurück. Amazon Kendra verwendet die OneDrive Mandantendomäne, um eine Verbindung mit der OneDrive Instanz herzustellen, und kann dann Suchergebnisse auf der Grundlage des Benutzer- oder Gruppenzugriffs auf Abschnitte und Dateinamen filtern.

Für Standardobjekte `_group_id` werden die `_user_id` und wie folgt verwendet:

- `_user_id`— Ihre OneDrive Microsoft-Benutzer-E-Mail-ID ist dem `_user_id` Feld zugeordnet.
- `_group_id`— Ihre OneDrive Microsoft-Gruppen-E-Mail ist dem `_group_id` Feld zugeordnet.

Sie können dem `AccessControlList` Feld bis zu 200 Einträge hinzufügen.

Benutzerkontextfilterung für SharePoint Microsoft-Datenquellen

Amazon Kendra ruft Benutzer- und Gruppeninformationen von Microsoft ab, SharePoint wenn es die Site-Dokumente indexiert. Um Suchergebnisse nach Benutzer- oder Gruppenzugriffen zu filtern, geben Sie Benutzer- und Gruppeninformationen an, wenn Sie die `Query` API aufrufen.

Verwenden Sie die E-Mail-Adresse des Benutzers, um nach einem Benutzernamen zu filtern. Zum Beispiel johnstiles@example.com.

Wenn Sie eine SharePoint Gruppe zum Filtern von Suchergebnissen verwenden, berechnen Sie die Gruppen-ID wie folgt:

Für lokale Gruppen

1. Holen Sie sich den Namen der Site. Beispiel: `https://host.onmicrosoft.com/sites/siteName.`
2. Nimm den SHA256-Hash des Seitennamens. z. B. `430a6b90503eef95c89295c8999c7981`.
3. Erstellen Sie die Gruppen-ID, indem Sie den SHA256-Hash mit einem senkrechten Balken (|) und dem Gruppennamen verketten. Wenn der Gruppenname beispielsweise "localGroupName„lautet, wäre die Gruppen-ID:

   `"430a6b90503eef95c89295c8999c7981 | localGroupName"`

   > **Note**
   >
   > Fügen Sie vor und nach dem senkrechten Balken ein Leerzeichen ein. Der vertikale Balken wird verwendet, um sich `localGroupName` mit seinem SHA256-Hash zu identifizieren.

Senden Sie die Gruppen-ID Amazon Kendra als `_group_id` Attribut an, wenn Sie die Abfrage-API aufrufen. Der AWS CLI Befehl sieht zum Beispiel so aus:

```
aws kendra  query \
                --index-id index ID
                --query-text "query text"
                --attribute-filter '{
                   "EqualsTo":{
                     "Key": "_group_id",
```

```
                    "Value": {"StringValue": "430a6b90503eef95c89295c8999c7981 |
localGroupName"}
                }}'
```

Für AD-Gruppen

1. Verwenden Sie die AD-Gruppen-ID für die Konfiguration der Filterung von Suchergebnissen.

Senden Sie die Gruppen-ID Amazon Kendra als `_group_id` Attribut an, wenn Sie die Abfrage-API aufrufen. Der AWS CLI Befehl sieht zum Beispiel so aus:

```
aws kendra  query \
               --index-id index ID
               --query-text "query text"
               --attribute-filter '{
                  "EqualsTo":{
                    "Key": "_group_id",
                    "Value": {"StringValue": "AD group"}
                  }}'
```

Sie können dem `AccessControlList` Feld bis zu 200 Einträge hinzufügen.

Benutzerkontextfilterung für Microsoft SQL Server-Datenquellen

Wenn Sie eine Microsoft SQL Server-Datenquelle verwenden, Amazon Kendra ruft Benutzer- und Gruppeninformationen aus einer Spalte in der Quelltabelle ab. Sie geben diese Spalte in der Konsole an oder verwenden das TemplateConfigurationObjekt als Teil der CreateDataSourceAPI.

Eine Microsoft SQL Server-Datenbankdatenquelle hat die folgenden Einschränkungen:

- Sie können nur eine Zulassungsliste für eine Datenbankdatenquelle angeben. Sie können keine Sperrliste angeben.
- Sie können nur Gruppen angeben. Sie können keine einzelnen Benutzer für die Zulassungsliste angeben.
- Die Datenbankspalte sollte eine Zeichenfolge sein, die eine durch Semikolons getrennte Liste von Gruppen enthält.

Benutzerkontextfilterung für Microsoft Teams-Datenquellen

Amazon Kendra ruft Benutzerinformationen von Microsoft Teams ab, wenn es die Dokumente indexiert. Die Benutzerinformationen stammen aus der zugrunde liegenden Microsoft Teams-Instanz.

Sie können dem `AccessControlList` Feld bis zu 200 Einträge hinzufügen.

Benutzerkontextfilterung für Microsoft Yammer-Datenquellen

Amazon Kendra ruft Benutzerinformationen von Microsoft Yammer ab, wenn es die Dokumente indexiert. Die Benutzer- und Gruppeninformationen stammen aus der zugrunde liegenden Microsoft Yammer-Instanz.

Die Microsoft Yammer-Benutzer-IDs werden wie folgt zugeordnet:

- `_email_id`— Die dem `_user_id` Feld zugeordnete Microsoft-E-Mail-ID.

Sie können dem `AccessControlList` Feld bis zu 200 Einträge hinzufügen.

Benutzerkontextfilterung für MySQL-Datenquellen

Wenn Sie eine MySQL-Datenquelle verwenden, Amazon Kendra ruft Benutzer- und Gruppeninformationen aus einer Spalte in der Quelltabelle ab. Sie geben diese Spalte in der Konsole an oder verwenden das TemplateConfigurationObjekt als Teil der CreateDataSourceAPI.

Eine MySQL-Datenbankdatenquelle hat die folgenden Einschränkungen:

- Sie können nur eine Zulassungsliste für eine Datenbankdatenquelle angeben. Sie können keine Sperrliste angeben.
- Sie können nur Gruppen angeben. Sie können keine einzelnen Benutzer für die Zulassungsliste angeben.
- Die Datenbankspalte sollte eine Zeichenfolge sein, die eine durch Semikolons getrennte Liste von Gruppen enthält.

Filterung des Benutzerkontextes für Oracle-Datenbankdatenquellen

Wenn Sie eine Oracle Database-Datenquelle verwenden, Amazon Kendra ruft Benutzer- und Gruppeninformationen aus einer Spalte in der Quelltabelle ab. Sie geben diese Spalte in der Konsole an oder verwenden das TemplateConfigurationObjekt als Teil der CreateDataSourceAPI.

Eine Oracle Database-Datenbankdatenquelle hat die folgenden Einschränkungen:

- Sie können nur eine Zulassungsliste für eine Datenbank-Datenquelle angeben. Sie können keine Sperrliste angeben.
- Sie können nur Gruppen angeben. Sie können keine einzelnen Benutzer für die Zulassungsliste angeben.
- Die Datenbankspalte sollte eine Zeichenfolge sein, die eine durch Semikolons getrennte Liste von Gruppen enthält.

Benutzerkontextfilterung für PostgreSQL-Datenquellen

Wenn Sie eine PostgreSQL-Datenquelle verwenden, Amazon Kendra ruft Benutzer- und Gruppeninformationen aus einer Spalte in der Quelltabelle ab. Sie geben diese Spalte in der Konsole an oder verwenden das TemplateConfigurationObjekt als Teil der CreateDataSourceAPI.

Eine PostgreSQL-Datenbankdatenquelle hat die folgenden Einschränkungen:

- Sie können nur eine Zulassungsliste für eine Datenbankdatenquelle angeben. Sie können keine Sperrliste angeben.
- Sie können nur Gruppen angeben. Sie können keine einzelnen Benutzer für die Zulassungsliste angeben.
- Die Datenbankspalte sollte eine Zeichenfolge sein, die eine durch Semikolons getrennte Liste von Gruppen enthält.

Filterung des Benutzerkontextes für Quip-Datenquellen

Wenn Sie eine Quip-Datenquelle verwenden, Amazon Kendra ruft die Benutzerinformationen aus der Quip-Instanz ab.

Die Quip-Benutzer-IDs werden wie folgt zugeordnet:

- `_user_id`— Benutzer-IDs existieren in Quip für Dateien, für die Zugriffsberechtigungen festgelegt sind. Sie werden anhand der Benutzer-E-Mails den IDs in Quip zugeordnet.

Sie können dem Feld bis zu 200 Einträge hinzufügen. `AccessControlList`

Filterung des Benutzerkontextes für Salesforce-Datenquellen

Eine Salesforce-Datenquelle gibt Benutzer- und Gruppeninformationen aus Entitäten der Salesforce-Zugriffskontrollliste (ACL) zurück. Sie können die Benutzerkontextfilterung auf Salesforce-Standardobjekte und Chatter-Feeds anwenden. Die Benutzerkontextfilterung ist für Salesforce-Wissensartikel nicht verfügbar.

Für Standardobjekte `_group_ids` werden die `_user_id` und wie folgt verwendet:

- `_user_id`— Der Benutzername des Salesforce-Benutzers.
- `_group_ids`—
  - Name des Salesforce-Benutzers `Profile`
  - Name des Salesforce `Group`
  - Name des Salesforce `UserRole`
  - Name des Salesforce `PermissionSet`

Für Chatter-Feeds `_group_ids` werden die `_user_id` und wie folgt verwendet:

- `_user_id`— Der Benutzername des Salesforce-Benutzers. Nur verfügbar, wenn der Artikel im Feed des Benutzers veröffentlicht wurde.
- `_group_ids`— Gruppen-IDs werden wie folgt verwendet. Nur verfügbar, wenn das Feedelement in einer Chatter- oder Kollaborationsgruppe gepostet wurde.
  - Der Name der Chatter- oder Kollaborationsgruppe.
  - Wenn die Gruppe öffentlich ist,`PUBLIC:ALL`.

Sie können dem `AccessControlList` Feld bis zu 200 Einträge hinzufügen.

Filterung des Benutzerkontextes für ServiceNow Datenquellen

Die Benutzerkontextfilterung für ServiceNow wird nur für die TemplateConfiguration API und ServiceNow Connector v2.0 unterstützt. ServiceNowConfigurationAPI und ServiceNow Connector v1.0. unterstützen keine Benutzerkontextfilterung.

Wenn Sie eine ServiceNow Datenquelle verwenden, Amazon Kendra ruft die Benutzer- und Gruppeninformationen aus der ServiceNow Instanz ab.

Die Gruppen- und Benutzer-IDs werden wie folgt zugeordnet:

- `_group_ids`— Gruppen-IDs existieren in ServiceNow Dateien, für die Zugriffsberechtigungen festgelegt sind. Sie werden anhand der Rollennamen von `sys_ids` in zugeordnet. ServiceNow
- `_user_id`— Benutzer-IDs sind in ServiceNow allen Dateien vorhanden, für die Zugriffsberechtigungen festgelegt wurden. Sie werden den Benutzer-E-Mails als IDs in zugeordnet. ServiceNow

Sie können dem `AccessControlList` Feld bis zu 200 Einträge hinzufügen.

Filterung des Benutzerkontextes für Slack-Datenquellen

Wenn du eine Slack-Datenquelle verwendest, werden die Benutzerinformationen aus der Slack-Instanz Amazon Kendra abgerufen.

Die Slack-Benutzer-IDs werden wie folgt zugeordnet:

- `_user_id`— Benutzer-IDs existieren in Slack in Nachrichten und Channels, für die es festgelegte Zugriffsberechtigungen gibt. Sie werden anhand der Benutzer-E-Mails den IDs in Slack zugeordnet.

Du kannst dem Feld bis zu 200 Einträge hinzufügen. `AccessControlList`

Filterung des Benutzerkontextes für Zendesk-Datenquellen

Wenn Sie eine Zendesk-Datenquelle verwenden, Amazon Kendra ruft die Benutzer- und Gruppeninformationen aus der Zendesk-Instanz ab.

Die Gruppen- und Benutzer-IDs werden wie folgt zugeordnet:

- `_group_ids`— Gruppen-IDs existieren in Zendesk-Tickets und Beiträgen, für die es festgelegte Zugriffsberechtigungen gibt. Sie werden anhand der Namen der Gruppen in Zendesk zugeordnet.
- `_user_id`— Gruppen-IDs existieren in Zendesk-Tickets und Beiträgen, für die es festgelegte Zugriffsberechtigungen gibt. Sie werden anhand der Benutzer-E-Mails den IDs in Zendesk zugeordnet.

Sie können dem Feld bis zu 200 Einträge hinzufügen. `AccessControlList`

Antworten und Antworttypen abfragen

Amazon Kendra unterstützt verschiedene Abfrageantworten und Antworttypen.

Antworten abfragen

Ein Aufruf der Query API gibt Informationen über die Ergebnisse einer Suche zurück. Die Ergebnisse befinden sich in einem Array von QueryResultItemObjekten (`ResultItems`). Jedes `QueryResultItem` enthält eine Zusammenfassung des Ergebnisses. Mit dem Abfrageergebnis verknüpfte Dokumentattribute sind enthalten.

Zusammenfassende Informationen

Die zusammenfassenden Informationen variieren je nach Art des Ergebnisses. In jedem Fall enthält es Dokumenttext, der dem Suchbegriff entspricht. Es enthält auch Hervorhebungsinformationen, mit denen Sie den Suchtext in der Ausgabe Ihrer Anwendung hervorheben können. Wenn der Suchbegriff beispielsweise wie hoch ist die Space Needle? , die zusammenfassenden Informationen beinhalten die Textposition für die Wörter Höhe und Space Needle. Informationen zu Antworttypen finden Sie unterAntworten und Antworttypen abfragen.

Attribute des Dokuments

Jedes Ergebnis enthält Dokumentattribute für das Dokument, das einer Abfrage entspricht. Einige der Attribute sind vordefiniert, z. B. `DocumentId``DocumentTitle`, und`DocumentUri`. Andere sind benutzerdefinierte Attribute, die Sie definieren. Sie können Dokumentattribute verwenden, um die Antwort von der `Query` API zu filtern. Beispielsweise möchten Sie möglicherweise nur die Dokumente verwenden, die von einem bestimmten Autor oder einer bestimmten Version eines Dokuments verfasst wurden. Weitere Informationen finden Sie unter Filterung und Facettensuche. Sie geben Dokumentattribute an, wenn Sie Dokumente zu einem Index hinzufügen. Weitere Informationen finden Sie unter Benutzerdefinierte Felder oder Attribute.

Im Folgenden finden Sie einen JSON-Beispielcode für ein Abfrageergebnis. Notieren Sie sich die Dokumentattribute in `DocumentAttributes` und`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
}
```

Arten von Antworten

Amazon Kendra gibt drei Arten von Abfrageantworten zurück.

- Antwort (beinhaltet Tabellenantwort)
- Dokument
- Frage und Antwort

Der Typ der Antwort wird im `Type` Antwortfeld des QueryResultItemObjekts zurückgegeben.

Antwort

Amazon Kendra hat eine oder mehrere Antworten auf Fragen in der Antwort erkannt. Ein Faktoid ist die Antwort auf eine „Wer“, „Was“, „Wann“ oder „Wo“ -Frage wie „Wo ist das nächstgelegene Servicecenter?“ Amazon Kendra gibt Text im Index zurück, der der Abfrage am besten entspricht. Der Text befindet sich im `AnswerText` Feld und enthält hervorgehobene Informationen für den Suchbegriff im Antworttext. `AnswerText`enthält den vollständigen Dokumentauszug mit hervorgehobenem Text und `DocumentExcerpt` den gekürzten (290 Zeichen) Dokumentauszug mit hervorgehobenem Text.

Amazon Kendra gibt nur eine Antwort pro Dokument zurück, und das ist die Antwort mit der höchsten Zuverlässigkeit. Um mehrere Antworten aus einem Dokument zurückzugeben, müssen Sie das Dokument in mehrere Dokumente aufteilen.

```
{
    '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'
}
```

Dokument

Amazon Kendra gibt Dokumente mit Rangfolge für diejenigen zurück, die dem Suchbegriff entsprechen. Die Rangfolge basiert auf dem Vertrauen, Amazon Kendra das Sie in die Richtigkeit des Suchergebnisses haben. Informationen über das passende Dokument werden in der zurückgegeben QueryResultItem. Es enthält den Titel des Dokuments. Der Auszug enthält hervorgehobene Informationen für den Suchtext und den Abschnitt mit dem passenden Text im Dokument. Der URI für übereinstimmende Dokumente befindet sich im `SourceURI` Dokumentattribut. Das folgende JSON-Beispiel zeigt die Dokumentzusammenfassung für ein passendes Dokument.

```
{
```

```
    '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'
}
```

Frage und Antwort

Eine Antwort mit Frage und Antwort wird zurückgegeben, wenn eine Frage mit einer der häufig gestellten Fragen in Ihrem Index Amazon Kendra übereinstimmt. Die Antwort enthält die passende Frage und Antwort in dem QueryResultItemFeld. Sie enthält auch Informationen zur Hervorhebung

von Abfragebegriffen, die in der Abfragezeichenfolge erkannt wurden. Die folgende JSON-Datei zeigt eine Frage und eine Antwort. Beachten Sie, dass die Antwort den Fragetext enthält.

```
{
    '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?'
    }
}
```

Informationen zum Hinzufügen von Frage- und Antworttext zu einem Index finden Sie unter Häufig gestellte Fragen erstellen.

Antworten optimieren und sortieren

Sie können die Auswirkung eines Felds oder Attributs auf die Suchrelevanz mithilfe der Relevanzoptimierung ändern. Sie können die Suchergebnisse auch nach einem bestimmten Attribut oder Feld sortieren.

Themen

- Antworten optimieren
- Antworten sortieren

Antworten optimieren

Sie können die Auswirkung eines Felds oder Attributs auf die Suchrelevanz mithilfe der Relevanzoptimierung ändern. Um die Relevanzoptimierung schnell zu testen, verwenden Sie die Abfrage-API, um Optimierungskonfigurationen in der Abfrage zu übergeben. Anschließend können Sie die verschiedenen Suchergebnisse sehen, die Sie aus verschiedenen Konfigurationen erhalten. Die Optimierung der Relevanz auf Abfrageebene wird in der Konsole nicht unterstützt. Sie können Felder oder Attribute des Typs auch nur `StringList` auf Indexebene optimieren. Weitere Informationen finden Sie unter Suchrelevanz optimieren.

Standardmäßig werden Abfrageantworten nach dem Relevanzwert sortiert, der für jedes Ergebnis in der Antwort Amazon Kendra ausschlaggebend ist.

Sie können die Ergebnisse für jedes integrierte oder benutzerdefinierte Attribut/Feld der folgenden Typen optimieren:

- Datumswert
- Langer Wert
- Zeichenfolge_Wert

Sie können Attribute des folgenden Typs nicht sortieren:

- Werte in der Zeichenkettenliste

Ordnen und optimieren Sie die Dokumentergebnisse (AWS SDK)

Setzen Sie den `Searchable` Parameter auf true, um die Konfiguration der Dokumentmetadaten zu verbessern.

Um ein Attribut in einer Abfrage zu optimieren, legen Sie den `DocumentRelevanceOverrideConfigurations` `Query` API-Parameter fest und geben Sie den Namen des zu optimierenden Attributs an.

Das folgende JSON-Beispiel zeigt ein `DocumentRelevanceOverrideConfigurations` Objekt, das die Optimierung für das Attribut „department“ im Index überschreibt.

```
"DocumentRelevanceOverrideConfigurations" : [
    "Name": "department",
    "Relevance": {
        "Importance": 1,
        "ValueImportanceMap": {
            "IT": 3,
            "HR": 7
        }
    }
]
```

Antworten sortieren

Amazon Kendra verwendet das Sortierattribut oder das Sortierfeld als Teil der Kriterien für die von der Abfrage zurückgegebenen Dokumente. Beispielsweise enthalten die Ergebnisse, die von einer nach „_created_at“ sortierten Abfrage zurückgegeben werden, möglicherweise nicht dieselben Ergebnisse wie eine nach „_version“ sortierte Abfrage.

Standardmäßig werden Abfrageantworten nach dem Relevanzwert sortiert, der für jedes Ergebnis in der Antwort Amazon Kendra ausschlaggebend ist. Um die Sortierreihenfolge zu ändern, machen Sie ein Dokumentattribut sortierbar und konfigurieren Sie es dann so, dass dieses Attribut Amazon Kendra zum Sortieren von Antworten verwendet wird.

Sie können Ergebnisse nach allen integrierten oder benutzerdefinierten Attributen/Feldern der folgenden Typen sortieren:

- Datumswert
- Langer Wert

- Zeichenfolge_Wert

Sie können Attribute des folgenden Typs nicht sortieren:

- Werte in der Zeichenkettenliste

Sie können in jeder Abfrage nach einem oder mehreren Dokumentattributen sortieren. Abfragen geben 100 Ergebnisse zurück. Wenn weniger als 100 Dokumente mit festgelegtem Sortierattribut vorhanden sind, werden Dokumente ohne Wert für das Sortierattribut am Ende der Ergebnisse zurückgegeben, sortiert nach Relevanz für die Abfrage.

Um Dokumentergebnisse zu sortieren (AWS SDK)

1. Um die UpdateIndexAPI zu verwenden, um ein Attribut sortierbar zu machen, setzen Sie den `Sortable` Parameter auf`true`. Das folgende JSON-Beispiel verwendet`DocumentMetadataConfigurationUpdates`, um dem Index ein Attribut namens „Department“ hinzuzufügen und es sortierbar zu machen.

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

2. Um ein sortierbares Attribut in einer Abfrage zu verwenden, legen Sie den `SortingConfiguration` Parameter der Abfrage-API fest. Geben Sie den Namen des zu sortierenden Attributs an und ob die Antwort in aufsteigender oder absteigender Reihenfolge sortiert werden soll.

   Das folgende JSON-Beispiel zeigt den `SortingConfiguration` Parameter, mit dem Sie die Ergebnisse einer Abfrage in aufsteigender Reihenfolge nach dem Attribut „Department“ sortieren.

```
   "SortingConfiguration": {
      "DocumentAttributeKey": "Department",
      "SortOrder": "ASC"
```

```
    }
```

3. Um mehr als ein sortierbares Attribut in einer Abfrage zu verwenden, legen Sie den `SortingConfigurations` Parameter der Abfrage-API fest. Sie können bis zu 3 Felder einrichten, nach denen die Ergebnisse sortiert Amazon Kendra werden sollen. Sie können auch angeben, ob die Ergebnisse in aufsteigender oder absteigender Reihenfolge sortiert werden sollen. Das Kontingent für Sortierfelder kann erhöht werden.

   Wenn Sie keine Sortierkonfiguration angeben, werden die Ergebnisse nach der Relevanz sortiert, die für das Ergebnis Amazon Kendra ausschlaggebend ist. Bei Gleichstand bei der Sortierung der Ergebnisse werden die Ergebnisse nach Relevanz sortiert.

   Das folgende JSON-Beispiel zeigt den `SortingConfigurations` Parameter, mit dem Sie die Ergebnisse einer Abfrage nach den Attributen „Name“ und „Preis“ in aufsteigender Reihenfolge sortieren.

```
"CollapseConfiguration" : {
    "DocumentAttributeKey": "Name",
    "SortingConfigurations": [
        {
            "DocumentAttributeKey": "Price",
            "SortOrder": "ASC"
        }
    ],
    "MissingAttributeKeyStrategy": "IGNORE"
}
```

Um Dokumentergebnisse zu sortieren (Konsole)

> **Note**
>
> Die Sortierung mit mehreren Attributen wird derzeit von der AWS Management Console nicht unterstützt.

1. Um ein Attribut in der Konsole sortierbar zu machen, wählen Sie in der Attributdefinition Sortierbar aus. Sie können ein Attribut sortierbar machen, wenn Sie das Attribut erstellen, oder Sie können es später ändern.

2. Um eine Abfrageantwort in der Konsole zu sortieren, wählen Sie im Menü Sortieren das Attribut aus, nach dem die Antwort sortiert werden soll. In der Liste werden nur Attribute angezeigt, die bei der Konfiguration der Datenquelle als sortierbar markiert wurden.

Abfrageergebnisse reduzieren/erweitern

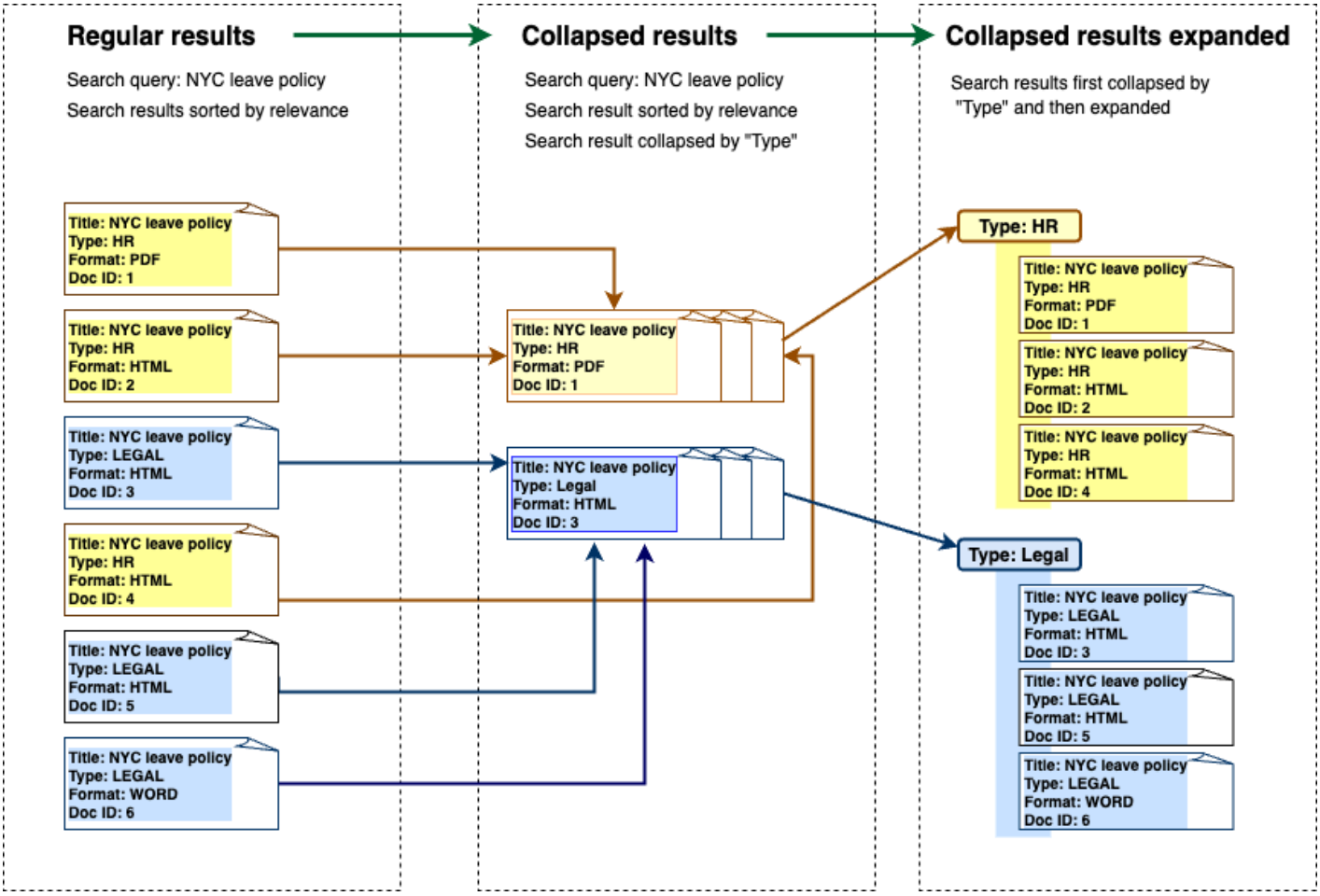
Wenn Sie eine Verbindung Amazon Kendra zu Ihren Daten herstellen, durchsucht es die Metadatenattribute von Dokumenten wie `_document_title_created_at`, und und `_document_id` verwendet diese Attribute oder Felder, um erweiterte Suchfunktionen während der Abfrage bereitzustellen.

Amazon Kendra Mit der Funktion „Abfrageergebnisse reduzieren und erweitern“ können Sie Suchergebnisse anhand eines gemeinsamen Dokumentattributs gruppieren und sie — entweder reduziert oder teilweise erweitert — unter einem bestimmten Hauptdokument anzeigen.

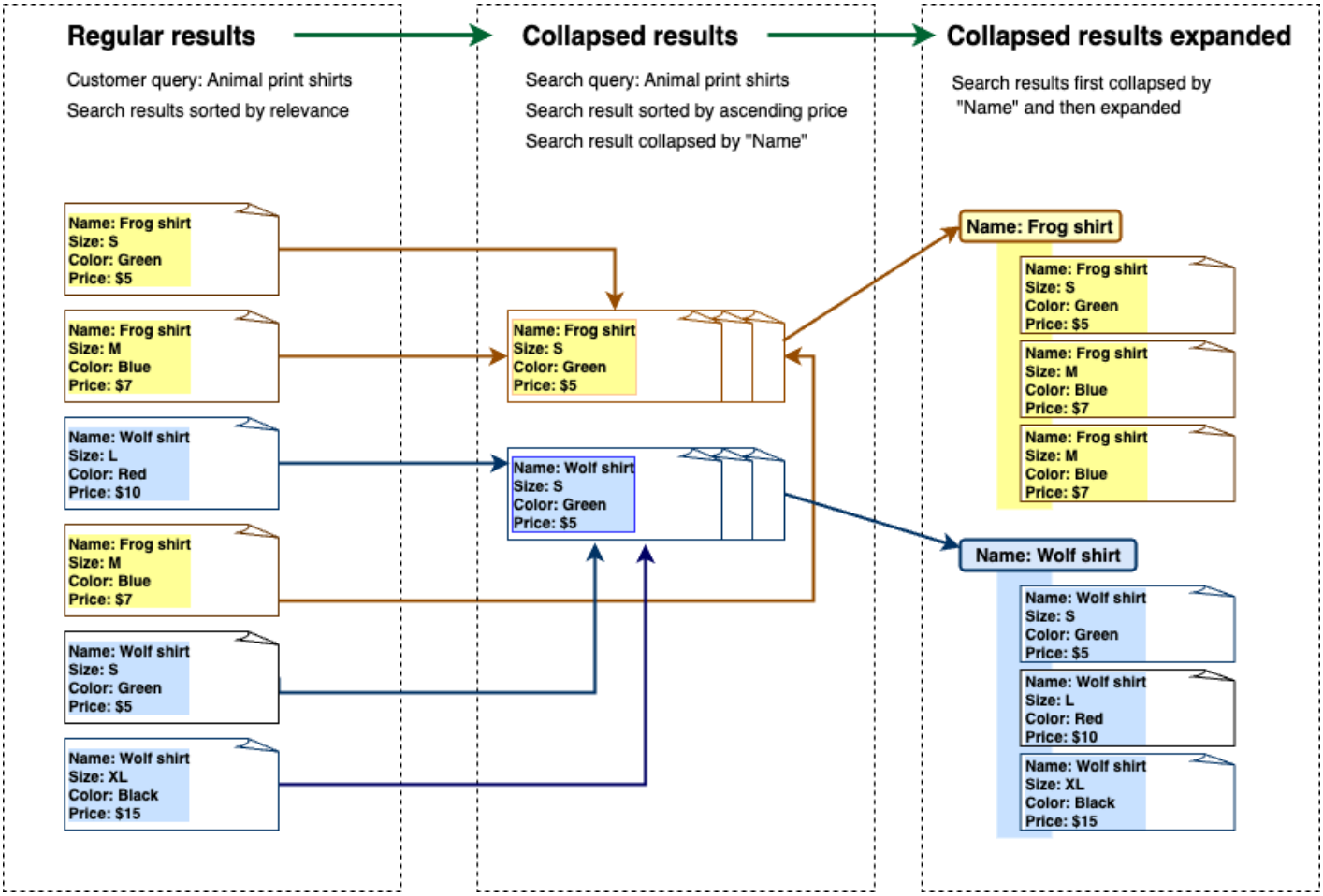
> **Note**
>
> Die Funktion zum Reduzieren und Erweitern von Abfrageergebnissen ist derzeit nur über die API verfügbar.Amazon Kendra

Dies ist in den folgenden Suchsituationen nützlich:

- In Dokumenten in Ihrem Index gibt es mehrere Versionen von Inhalten. Wenn Ihr Endbenutzer den Index abfragt, möchten Sie, dass ihm die relevanteste Version des Dokuments angezeigt wird, wobei Duplikate ausgeblendet/reduziert sind. Wenn Ihr Index beispielsweise mehrere Versionen eines Dokuments mit dem Namen „NYC Leave Policy“ enthält, können Sie festlegen, dass die Dokumente für die spezifischen Gruppen „HR“ und „Legal“ mithilfe des Attributs/Felds „Type“ ausgeblendet werden.



- Ihr Index enthält mehrere Dokumente mit eindeutigen Informationen zu einer Art von Artikel oder Objekt, z. B. zu einem Produktinventar. Um Artikelinformationen bequem zu erfassen und zu sortieren, möchten Sie, dass Endbenutzer auf alle Dokumente, die mit einem Artikel oder Objekt verknüpft sind, als ein Suchergebnis zugreifen können. Im Beispiel unten werden bei einer Kundensuche nach „Hemden mit Animal-Print“ Ergebnisse angezeigt, die nach Namen gruppiert und nach aufsteigender Preisreihenfolge sortiert sind.



Ergebnisse werden zusammengeklappt

Um ähnliche oder verwandte Dokumente zu gruppieren, müssen Sie das Attribut angeben, nach dem die Anzeige reduziert werden soll (Sie können beispielsweise Dokumente zusammenklappen/gruppieren). `_category` Rufen Sie dazu die Abfrage-API auf und verwenden Sie das Objekt, um das CollapseConfigurationObjekt zu spezifizieren, auf das reduziert `DocumentAttributeKey` werden soll. Das `DocumentAttributeKey` steuert, bei welchen Feldern die Suchergebnisse ausgeblendet werden. Zu den unterstützten Attributschlüsselfeldern gehören `String` und`Number`. `String list`und `Date` type werden nicht unterstützt.

Ein Hauptdokument mithilfe der Sortierreihenfolge auswählen

Um das Hauptdokument so zu konfigurieren, dass es für eine reduzierte Gruppe angezeigt wird, verwenden Sie den `SortingConfigurations` Parameter unter CollapseConfiguration. Um beispielsweise die neueste Version eines Dokuments abzurufen, würden Sie jede reduzierte Gruppe nach sortieren`_version`. Sie können bis zu 3 Attribute/Felder angeben, nach denen sortiert werden

soll, und für jedes Attribut/Feld eine Sortierreihenfolge angeben. `SortingConfigurations` Sie können eine Erhöhung des Kontingents für die Anzahl der Sortierattribute beantragen.

Amazon Kendra Sortiert Abfrageantworten standardmäßig nach der Relevanzbewertung, die für jedes Ergebnis in der Antwort ermittelt wird. Um die Standardsortierreihenfolge zu ändern, machen Sie die Dokumentattribute sortierbar und konfigurieren Sie dann, dass diese Attribute Amazon Kendra zum Sortieren von Antworten verwendet werden. Weitere Informationen finden Sie unter Antworten sortieren.

Schlüsselstrategie für das Dokument fehlt

Wenn Ihr Dokument keinen Wert für das Attribut „Ausblenden“ hat, Amazon Kendra bietet es drei Anpassungsoptionen:

- Wählen Sie `COLLAPSE` alle Dokumente mit Nullwerten oder fehlenden Werten in einer Gruppe aus. Dies ist die Standardkonfiguration.
- Wählen Sie `IGNORE` Dokumente mit Nullwerten oder fehlenden Werten aus. Ignorierte Dokumente werden nicht in den Abfrageergebnissen angezeigt.
- Ordnen Sie `EXPAND` jedes Dokument mit einem Nullwert oder einem fehlenden Wert in eine eigene Gruppe zu.

Erweiterung der Ergebnisse

Mithilfe des `Expand` Parameters im CollapseConfigurationObjekt können Sie wählen, ob zusammengeklappte Suchergebnisgruppen erweitert werden sollen. Bei erweiterten Ergebnissen wird dieselbe Sortierreihenfolge beibehalten, die bei der Auswahl des Hauptdokuments für die Gruppe verwendet wurde.

Um die Anzahl der zusammengeklappten Suchergebnisgruppen zu konfigurieren, die erweitert werden sollen, verwenden Sie den `MaxResultItemstoExpand` Parameter im ExpandConfigurationObjekt. Wenn Sie diesen Wert beispielsweise auf 10 setzen, verfügen nur die ersten 10 von 100 Ergebnisgruppen über die Erweiterungsfunktion.

Verwenden Sie den `MaxExpandResultsPerItem` Parameter, um die Anzahl der erweiterten Ergebnisse zu konfigurieren, die pro reduziertem Hauptdokument angezeigt werden sollen. Wenn Sie diesen Wert beispielsweise auf 3 setzen, werden maximal 3 Ergebnisse pro reduzierter Gruppe angezeigt.

Interaktionen mit anderen Amazon Kendra Funktionen

- Das Reduzieren und Erweitern von Ergebnissen hat keine Auswirkungen auf die Anzahl der Facetten und wirkt sich auch nicht auf die Gesamtzahl der angezeigten Ergebnisse aus.
- Amazon Kendra Ausgewählte Suchergebnisse werden auch dann nicht ausgeblendet, wenn sie denselben Feldwert wie das von Ihnen konfigurierte Ausblendfeld haben.
- Das Reduzieren und Erweitern von Ergebnissen gilt nur für Ergebnisse des Typs`DOCUMENT`.

Relevanz der Optimierungssuche

Amazon Kendra -Abfragen erzeugen Suchergebnisse, die nach ihrer Relevanz geordnet sind. Die durchsuchbaren Felder oder Attribute im Index tragen alle zu dieser Rangfolge bei.

Sie können die Auswirkungen eines Felds oder Attributs auf die Suchrelevanz durch Relevanzoptimierung ändern. Die Relevanz der Optimierungssuche kann entweder manuell auf Indexebene, bei der Sie die Optimierungskonfigurationen für Ihren Index festlegen, oder auf Abfrageebene erfolgen, indem Sie die auf Indexebene festgelegten Konfigurationen überschreiben.

Wenn Sie die Relevanzoptimierung verwenden, erhält ein Ergebnis einen Schub in der Antwort, wenn die Abfrage Begriffe enthält, die dem Feld oder Attribut entsprechen. Sie geben auch an, wie viel Schub das Dokument erhält, wenn eine Übereinstimmung vorliegt. Die Relevanzoptimierung führt Amazon Kendra nicht dazu, dass ein Dokument in die Abfrageantwort aufgenommen wird. Es ist nur einer der Faktoren, die Amazon Kendra verwendet, um die Relevanz eines Dokuments zu bestimmen.

Sie können bestimmte Felder oder Attribute in Ihrem Index steigern, um bestimmten Antworten mehr Bedeutung zuzuweisen. Zum Beispiel, wenn jemand nach „Wann ist re:Invent?“ sucht Sie könnten die Relevanz der Dokumentenaktualität im `_last_update_at` Feld erhöhen. Oder Sie könnten in einem Index von Forschungsberichten eine bestimmte Datenquelle im Feld „Quelle“ steigern.

Sie können Dokumente auch auf der Grundlage von Stimmen erhöhen oder die Anzahl anzeigen, die in Foren und anderen Support-Wissensdatenbanken üblich ist. Sie können Boosts kombinieren, um beispielsweise Dokumente zu verbessern, die sowohl häufiger als auch aktueller angesehen werden.

Sie legen den Schub fest, den ein Dokument erhält, indem Sie den -`Importance`Parameter verwenden. Je höher der `Importance`, desto mehr erhöht das Feld oder Attribut die Relevanz eines Dokuments. Wenn Sie Ihren Index oder Ihre Optimierung auf Abfrageebene optimieren, erhöhen Sie den Wert des `Importance` Parameters in kleinen Schritten, bis Sie den gewünschten Effekt erhalten. Um festzustellen, ob Sie die Suchergebnisse verbessern, führen Sie die Suche durch und vergleichen Sie die Ergebnisse mit früheren Abfragen.

Sie können Datums-, Zahlen- oder Zeichenfolgenattribute angeben, um einen Index oder eine Optimierung auf Abfrageebene vorzunehmen. Sie können Felder oder Attribute des Typs `StringList` nur auf Indexebene optimieren. Jedes Feld oder Attribut hat spezifische Kriterien dafür, wann es ein Ergebnis verbessert.

- Datumsfelder oder Attribute – Es gibt drei spezifische Kriterien für `Duration`Datumsfelder, `Freshness` und `RankOrder`.
  - `Duration` legt den Zeitraum fest, für den der Boost gilt. Wenn Sie beispielsweise den Zeitraum auf 86 400 Sekunden (d. h. einen Tag) festlegen, beginnt der Schub nach einem Tag zu verringern. Je höher die Wichtigkeit, desto schneller nimmt der Schubeffekt ab.
  - `Freshness` bestimmt, wie aktuell ein Dokument ist, wenn es auf ein Feld oder Attribut angewendet wird. Wenn Sie entweder `Freshness` auf das Feld für das Erstellungsdatum oder das Datum der letzten Aktualisierung anwenden, wird ein kürzlich erstelltes oder zuletzt aktualisiertes Dokument als „aktualisierter“ als ein älteres Dokument betrachtet. Wenn beispielsweise Dokument 1 am 14. November und Dokument 2 am 5. November erstellt wurde, ist Dokument 1 „aktualer“ als Dokument 2. Und wenn Dokument 1 am 14. November zuletzt aktualisiert wurde und Dokument 2 am 20. November zuletzt aktualisiert wurde, ist Dokument 2 „neuer“ als Dokument 1. Je neuer das Dokument, desto mehr wird dieser Schub angewendet. Sie können nur ein `Freshness` Feld in Ihrem Index haben.
  - `RankOrder` wendet den Schub entweder in aufsteigender oder absteigender Reihenfolge an. Wenn Sie angeben`ASCENDING`, haben spätere Daten Vorrang vor . Wenn Sie angeben`DESCENDING`, haben frühere Daten Vorrang.
- Zahlenfelder oder Attribute – Für Zahlenfelder oder Attribute können Sie die Rangfolge angeben, die bei der Bestimmung der Relevanz des Felds oder Attributs verwenden Amazon Kendra soll. Wenn Sie angeben`ASCENDING`, haben höhere Zahlen Vorrang. Wenn Sie angeben`DESCENDING`, haben niedrigere Zahlen Vorrang.
- Zeichenfolgenfelder oder Attribute – Bei Zeichenfolgenfeldern oder Attributen können Sie Kategorien eines Felds erstellen, um jeder Kategorie einen anderen Schub zu geben. Wenn Sie beispielsweise ein Feld oder Attribut namens „Abteilung“ steigern, können Sie Dokumenten von „Personal“ einen anderen Schub verleihen als Dokumenten von „Recht“. Sie können ein Feld oder Attribut des Typs erhöhen`String`. Sie können `StringList` Felder nur auf Indexebene erhöhen.

Relevanzoptimierung auf Indexebene

Sie optimieren die Relevanz eines Felds oder Attributs auf Indexebene, indem Sie entweder die Konsole verwenden, um die Optimierung in den Indexdetails oder die UpdateIndex API festzulegen.

Im folgenden Beispiel wird das `_last_updated_at` Feld als `Freshness` Feld für ein Dokument festgelegt.

```
"DocumentMetadataConfigurationUpdates" : [
```

```
    {
        "Name": "_last_updated_at",
        "Type": "DATE_VALUE",
        "Relevance": {
            "Freshness": TRUE,
            "Importance": 2
        }
    }
]
```

Das folgende Beispiel wendet unterschiedliche Bedeutung auf die verschiedenen Kategorien im Feld „Abteilung“ an.

```
"DocumentMetadataConfigurationUpdates" : [
    {
        "Name": "department",
        "Type": "STRING_VALUE",
        "Relevance": {
            "Importance": 2,
            "ValueImportanceMap": {
                "HR": 3,
                "Legal": 1
            }
        }
    }
]
```

Relevanzoptimierung auf Abfrageebene

Sie optimieren die Relevanz eines Felds oder Attributs auf Abfrageebene mithilfe der Abfrage-API.

Die Relevanzoptimierung auf Abfrageebene wird in der Konsole nicht unterstützt.

Die Optimierung auf Abfrageebene kann den Prozess der Testrelevanzoptimierung beschleunigen, da Sie die Optimierungskonfigurationen im Index für jeden Test nicht manuell aktualisieren müssen. Sie können die Relevanz eines Dokuments anpassen, indem Sie Optimierungskonfigurationen in der Abfrage übergeben. Dann können Sie die verschiedenen Ergebnisse sehen, die Sie aus verschiedenen Konfigurationen erhalten. Eine Konfiguration, die in der Abfrage übergeben wird, überschreibt die Konfiguration, die auf Indexebene festgelegt ist.

Das folgende Beispiel überschreibt die Bedeutung, die auf das Feld „Abteilung“ und jede Abteilungskategorie angewendet wird, die auf Indexebene festgelegt ist, wie im obigen Beispiel gezeigt. Wenn ein Benutzer seine Suchabfrage eingibt, hat das Feld „Abteilung“ ein gewisses Maß an Bedeutung und die Rechtsabteilung hat mehr Bedeutung als die Personalabteilung.

```
"DocumentRelevanceOverrideConfigurations" : [
    {
        "Name": "department",
        "Type": "STRING_VALUE",
        "Relevance": {
            "Importance": 2,
            "ValueImportanceMap": {
                "HR": 2,
                "Legal": 8
            }
        }
    }
]
```

Gewinnen von Erkenntnissen mit Suchanalysen

Sie können Amazon Kendra Suchanalysen verwenden, um Erkenntnisse darüber zu gewinnen, wie Ihre Suchanwendung Ihren Benutzern erfolgreich oder erfolglos hilft, Informationen zu finden.

Amazon Kendra Analyse bietet einen Snapshot darüber, wie Ihre Benutzer mit Ihrer Suchanwendung interagieren und wie effektiv Ihre Suchanwendungskonfiguration ist. Sie können die Metrikdaten mithilfe der GetSnapshots -API oder durch Auswahl von Analytics im Navigationsbereich der -Konsole anzeigen.

Sie können die von generierten Daten `GetSnapshots` in Ihrem eigenen benutzerdefinierten Dashboard rendern. Oder Sie können das in der Konsole bereitgestellte Metrik-Dashboard verwenden, das visuelle Diagramme enthält. Mit einem visuellen Dashboard können Sie nach Trends oder Mustern im Benutzerverhalten im Laufe der Zeit suchen oder Probleme mit Ihrer Suchanwendungskonfiguration aufdecken. Beispielsweise könnte ein Liniendiagramm, das eine konsistente Anzahl von Abfragen pro Tag und einen konstanten Anstieg zeigt, auf eine erhöhte Akzeptanz und Nutzung hinweisen. Andererseits kann ein plötzlicher Rückgang darauf hindeuten, dass ein Problem vorliegt, das untersucht werden muss.

Sie können die Metriken verwenden, um Verbindungen zwischen verschiedenen Datenpunkten herzustellen, um Probleme damit zu lösen, wie Ihre Benutzer Informationen abfragen oder Geschäftsmöglichkeiten entdecken. Zum Beispiel das Dokument „Wie funktioniert KI?“ ist das am häufigsten auf Dokument in den Suchergebnissen geklickte und die am häufigsten durchsuchte Abfrage ist „Wie funktioniert Machine Learning?“. Dies informiert Sie über die bevorzugten Begriffe und die Sprache, die Ihre Benutzer verwenden. Sie können diese Begriffe in Ihre Dokumente integrieren oder benutzerdefinierte Synonyme für diese Begriffe verwenden, um Ihre Dokumente für Ihre Benutzer besser durchsuchbar zu machen.

Metriken für die Suche

Es gibt 10 Metriken, um die Leistung Ihrer Suchanwendung zu analysieren oder nach welchen Informationen Ihre Benutzer suchen. Um die Metrikdaten abzurufen, geben Sie den Zeichenfolgennamen der Metrikdaten an, die Sie abrufen möchten, wenn Sie aufrufen`GetSnapshots`.

Sie müssen auch ein Zeitintervall oder Zeitfenster angeben, um die Metrikdaten anzuzeigen. Das Zeitintervall verwendet die Zeitzone Ihres Index. Sie können Daten in den folgenden Zeitfenstern anzeigen:

- `THIS_WEEK`: Die aktuelle Woche, beginnend am Sonntag und endend am Tag vor dem aktuellen Datum.
- `ONE_WEEK_AGO`: Die Vorwoche, beginnend am Sonntag und endend am folgenden Samstag.
- `TWO_WEEKS_AGO`: Die Woche vor der vorherigen Woche, beginnend am Sonntag und endend am folgenden Samstag.
- `THIS_MONTH`: Der aktuelle Monat, beginnend am ersten Tag des Monats und endend an dem Tag vor dem aktuellen Datum.
- `ONE_MONTH_AGO`: Der Vormonat, beginnend am ersten Tag des Monats und endend am letzten Tag des Monats.
- `TWO_MONTHS_AGO`: Der Monat vor dem Vormonat, beginnend am ersten Tag des Monats und endend am letzten Tag des Monats.

In der Konsole sind die unterstützten Zeitfenster Diese Woche, Vorherige Woche, Dieser Monat, Vorheriger Monat .

Click-Through-Rate

Der Anteil der Abfragen, die zu einem Durchklicken auf ein Dokument in den Suchergebnissen führen. Dies hilft Ihnen zu verstehen, ob Ihre Suchanwendungskonfiguration Ihren Benutzern hilft, Informationen zu ihren Abfragen zu finden. Bei Abfragen, die sofortige Antworten zurückgeben, müssen Benutzer möglicherweise nicht auf ein Dokument klicken, um weitere Informationen zu erhalten. Weitere Informationen finden Sie unter the section called “Sofortige Antwortrate”. Sie müssen anrufen, SubmitFeedback um sicherzustellen, dass Click-Through-Feedback gesammelt wird.

Um Daten mit Click-Through-Rate mithilfe der `GetSnapshots` API abzurufen, geben Sie `metricType` als an`AGG_QUERY_DOC_METRICS`. Sie können diese Metrik auch in der Konsole anzeigen, indem Sie im Navigationsbereich Analyse auswählen.

Null-Klickrate

Der Anteil der Abfragen, die zu keinem Klick in den Suchergebnissen führen. Auf diese Weise können Sie Lücken in Ihren Inhalten verstehen und irrelevante Suchergebnisse liefern. Bei Abfragen, die sofortige Antworten zurückgeben, müssen Benutzer möglicherweise nicht auf ein Dokument klicken, um weitere Informationen zu erhalten. Weitere Informationen finden Sie unter the section called

“Sofortige Antwortrate”. Außerdem können Ihre Sucheinstellungen, wie z. B. Tuning-Konfigurationen, Auswirkungen darauf haben, wie Dokumente in den Suchergebnissen zurückgegeben werden.

Um Daten mit Null-Klickrate über die `GetSnapshots` API abzurufen, geben Sie `metricType` als an`AGG_QUERY_DOC_METRICS`. Sie können diese Metrik auch in der Konsole anzeigen, indem Sie im Navigationsbereich Analyse auswählen.

Rate der Null-Suchergebnisse

Der Anteil der Abfragen, die zu keinen Suchergebnissen führen. Auf diese Weise können Sie Lücken in Ihren Inhalten verstehen und keine relevanten Suchergebnisse liefern.

Um Daten mit einer Rate von Null-Suchergebnissen mithilfe der `GetSnapshots` API abzurufen, geben Sie `metricType` als an`AGG_QUERY_DOC_METRICS`. Sie können diese Metrik auch in der Konsole anzeigen, indem Sie im Navigationsbereich Analyse auswählen.

Sofortige Antwortrate

Der Anteil der Abfragen mit sofortiger Antwort oder zurückgegebenen häufig gestellten Fragen. Dies hilft Ihnen, die Rolle sofortiger Antworten bei der Bereitstellung von Informationen zu verstehen.

Um Daten mit sofortiger Antwortrate mithilfe der `GetSnapshots` API abzurufen, geben Sie `metricType` als an`AGG_QUERY_DOC_METRICS`. Sie können diese Metrik auch in der Konsole anzeigen, indem Sie im Navigationsbereich Analyse auswählen.

Top-Abfragen

Die 100 häufigsten Abfragen, die von Ihren Benutzern durchsucht werden. Dies hilft Ihnen zu verstehen, welche Abfragen beliebt sind und an welcher Art von Informationen Ihre Benutzer am meisten interessiert sind.

Zu den Metriken gehören die Anzahl der Durchsuchungen der Abfrage, der Anteil der Click-Throughs an ein Dokument, der Anteil der Click-Throughs an einem Dokument, die durchschnittliche Klicktiefe in den Suchergebnissen für die Abfrage, der Anteil der sofortigen Antworten auf die Abfrage und die durchschnittliche Zuverlässigkeit für die ersten 10 Suchergebnisse für eine Abfrage.

Um Daten zu Top`GetSnapshots`-Abfragen mithilfe der API abzurufen, geben Sie `metricType` als an`QUERIES_BY_COUNT`. Sie können diese Metrik auch in der Konsole anzeigen, indem Sie im Navigationsbereich der Konsole Analyse und dann Top-Abfragen unter Abfragelisten auswählen.

Top-Abfragen ohne Klicks

Die 100 häufigsten Abfragen, die zu keinem Klick in den Suchergebnissen führen. Auf diese Weise können Sie alle Lücken in Ihren Inhalten verstehen, bei denen für einige Abfragen relevante Dokumente fehlen oder Ihre Suchanwendungskonfiguration irrelevante Suchergebnisse zurückgibt. Bei Abfragen, die sofortige Antworten zurückgeben, müssen Benutzer möglicherweise nicht auf ein Dokument klicken, um weitere Informationen zu erhalten. Weitere Informationen finden Sie unter the section called “Sofortige Antwortrate”.

Metriken umfassen die Häufigkeit, mit der die Abfrage zu Nullklicks führt, den Anteil der Nullklicks für die Abfrage, den Anteil der sofortigen Antworten für die Abfrage und die durchschnittliche Zuverlässigkeit für die ersten 10 Suchergebnisse für eine Abfrage.

Um Daten zu Top-Abfragen ohne Klicks über die `GetSnapshots` API abzurufen, geben Sie `metricType` als an`QUERIES_BY_ZERO_CLICK_RATE`. Sie können diese Metrik auch in der Konsole anzeigen, indem Sie im Navigationsbereich der Konsole Analyse und dann Top-Zero-Click-Abfragen unter Abfragelisten auswählen.

Top-Abfragen ohne Suchergebnisse

Die 100 häufigsten Abfragen, die zu keinen Suchergebnissen führen. Auf diese Weise können Sie alle Lücken in Ihren Inhalten verstehen, bei denen es keine Dokumente gibt, die für einige Abfragen relevant sind. Oder Ihre Benutzer fragen möglicherweise mit speziellen Begriffen ab, die möglicherweise zu keinen Suchergebnissen führen, sodass Sie benutzerdefinierte Synonyme erstellen müssen, um dies zu verarbeiten.

Metriken umfassen die Häufigkeit, mit der die Abfrage zu null Suchergebnissen führt, den Anteil der Nullsuchergebnisse für die Abfrage und den Anteil der Abfragesuche im Vergleich zu allen Abfragen.

Um Daten zu Top-Abfragen ohne Suchergebnisse mithilfe der `GetSnapshots` API abzurufen, geben Sie `metricType` als an`QUERIES_BY_ZERO_RESULT_RATE`. Sie können diese Metrik auch in der Konsole anzeigen, indem Sie im Navigationsbereich der Konsole Analyse und dann Top-Null-Ergebnisabfragen unter Abfragelisten auswählen.

Oben auf Dokumente geklickt

Die 100 am häufigsten auf Dokumente in den Suchergebnissen geklickt. Dies hilft Ihnen zu verstehen, welche Dokumente oder Suchergebnisse für Ihre Benutzer am relevantesten sind, wenn sie Informationen abfragen.

Zu den Metriken gehören die Häufigkeit, mit der das Dokument angeklickt wird, die Anzahl der Likes, die ein Dokument von Ihren Benutzern erhält (Daumen nach oben), die Anzahl der Unlikes, die ein Dokument von Ihren Benutzern erhält (Daumen nach unten).

Um Daten abzurufen, auf die Dokumente mit der -`GetSnapshots`API oben geklickt wurden, geben Sie `metricType` als an`DOCS_BY_CLICK_COUNT`. Sie können diese Metrik auch in der Konsole anzeigen, indem Sie im Navigationsbereich der Konsole Analyse und dann am häufigsten angeklickte Dokumente unter Abfragelisten auswählen.

Gesamtzahl der Abfragen

Die Gesamtzahl der von Ihren Benutzern durchsuchten Abfragen. Dies hilft Ihnen zu verstehen, wie engagiert Ihre Benutzer mit Ihrer Suchanwendung sind.

Um Daten zu Gesamtabfragen mithilfe der `GetSnapshots` API abzurufen, geben Sie `metricType` als an`AGG_QUERY_DOC_METRICS`. Sie können diese Metrik auch in der Konsole anzeigen, indem Sie im Navigationsbereich Analyse auswählen.

Gesamtzahl der Dokumente

Die Gesamtzahl der Dokumente in Ihrem Index. Auf diese Weise können Sie die Größe Ihres Index mit der Gesamtzahl der Abfragen vergleichen, um zu überprüfen, ob für das Abfragevolumen eine angemessene Anzahl von Dokumenten vorhanden ist.

Um Daten zu den gesamten Dokumenten mithilfe der `GetSnapshots` API abzurufen, geben Sie `metricType` als an`AGG_QUERY_DOC_METRICS`. Sie können diese Metrik auch in der Konsole anzeigen, indem Sie im Navigationsbereich Analyse auswählen.

Beispiel für das Abrufen von Metrikdaten

Der folgende Code ist ein Beispiel für das Abrufen von Daten zu den Top-Abfragen für den Vormonat.

Console

So rufen Sie Top-Abfragen für den Vormonat ab

1. Wählen Sie im linken Navigationsbereich unter Indizes Ihren Index und dann Analyse aus.
2. Wählen Sie auf der Seite Analyse die Schaltfläche Diese Woche aus, um das Zeitfenster für den Abruf der Daten in den Vormonat zu ändern.

3. Wählen Sie auf der Seite Analytics unter Abfragelisten die Option Top-Abfragen aus.

CLI

So rufen Sie Top-Abfragen für den Vormonat ab

```
aws kendra get-snapshots \
--index-id index-id \
--interval "ONE_MONTH_AGO" \
--metric-type "QUERIES_BY_COUNT"
```

Python

So rufen Sie die häufigsten Abfragen für den Vormonat ab

```
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

So rufen Sie die häufigsten Abfragen für den Vormonat ab

```
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()))
```

Von Metriken bis hin zu verwertbaren Erkenntnissen

Verwertbare Erkenntnisse sind aussagekräftige Informationen, die aus Rohdaten extrahiert werden und als Grundlage für Ihre Aktionen oder Entscheidungen verwendet werden. Um aus den Metriken Bedeutung zu extrahieren und sie zur Förderung verwertbarer Erkenntnisse zu verwenden, ist es wichtig, die Metriken nicht nur isoliert zu betrachten, sondern auch Verbindungen zwischen den Metriken herzustellen.

Die oberste Abfrage ohne Klicks ist beispielsweise „ Welche Regionen sind derzeit verfügbar?“. Es hat jedoch auch eine Instant-Antwortrate von 100 Prozent. Dies deutet darauf hin, dass Ihre Benutzer die Antwort auf diese Frage erhalten, ohne auf ein Suchergebnis oder Dokument klicken zu müssen, das Informationen zu verfügbaren Regionen enthält. Wenn Sie sich nur Nullklicks angesehen haben, würden Sie nicht die gesamte Geschichte ansehen und möglicherweise die falschen Schlussfolgerungen über den Erfolg Ihrer Suchanwendungskonfiguration bei der Verarbeitung dieser Abfrage ziehen.

Ein weiteres Beispiel für einen verwertbaren Einblick ist die Entdeckung einer Geschäftsmöglichkeit. Unternehmen suchen häufig nach Möglichkeiten, ihre Kunden zu vergrößern, indem sie Suchmetriken analysieren. Die am häufigsten auf das Dokument geklickte Region ist „Verfügbare

Regionen“. Darüber hinaus beziehen sich die meisten der am häufigsten durchsuchten Abfragen auf Fragen zur Produktverfügbarkeit in der Region Jungfernische Region, mit 100 Prozent Instant-Antwortraten und einer hohen Click-Through-Rate für weitere Informationen zu verfügbaren Regionen als Teil der Antwort. Dies deutet darauf hin, dass in dieser Region Interesse und Nachfrage für Ihr Produkt oder Ihren Service bestehen.

Visualisieren und Melden von Suchanalysen

Es gibt fünf Metriken, die Trenddaten enthalten, mit denen Sie Trends oder Muster im Laufe der Zeit visualisieren und suchen können. Wenn Sie die Konsole verwenden, werden Diagramme der Trendsdaten bereitgestellt. Wenn Sie die APIs verwenden, können Sie die Trenddaten abrufen, um Ihre eigenen Diagramme oder Visualisierungen zu erstellen. Die meisten Diagramme in der Konsole stellen die täglichen Datenpunkte über das von Ihnen gewählte Zeitfenster dar.

Die Konsole bietet ein Dashboard mit den Metriken, in dem Sie ein Diagramm und eine Top-Liste auswählen können, die Sie anzeigen möchten. Sie können die auf Ihrem Dashboard angezeigten Metriken im CSV-Format exportieren, indem Sie auf der Analytics-Startseite Export ierenauswählen. Sie können diese Berichte in Ihre Geschäftsdokumente oder Präsentation aufnehmen.

Sie können die folgenden Metriken visualisieren:

Diagramm der Gesamtzahl der Abfragen

Ein Liniendiagramm der Anzahl der pro Tag ausgegebenen Abfragen. Das Diagramm hilft Ihnen, Muster im täglichen Benutzerinteraktionen zu visualisieren. Einige Beispiele sind eine stetige Zunahme oder Abnahme der Benutzerinteraktion oder ein drastischer Rückgang auf 0 Abfragen aufgrund eines Absturzs Ihrer Suchanwendung oder von Problemen mit Ihrer Website.

Wenn Sie die API verwenden, können Sie diese Daten abrufen, indem Sie angeben`TREND_QUERY_DOC_METRICS`. Sie können die Daten verwenden, um Ihre eigenen Diagramme zu erstellen, oder die in der Konsole bereitgestellten Diagramme verwenden.

Click-Through-Ratendiagramm

Ein Liniendiagramm der Proportionen der Click-Throughs pro Tag. Das Diagramm hilft Ihnen, Muster in der täglichen Click-Through-Rate zu visualisieren. Einige Beispiele sind eine stetige Zunahme oder Abnahme der Click-Through-Rate oder eine Abnahme der sofortigen Antworten, die möglicherweise eine Zunahme des Click-Throughs beeinflussen.

Wenn Sie die API verwenden, können Sie diese Daten abrufen, indem Sie angeben`TREND_QUERY_DOC_METRICS`. Sie können die Daten verwenden, um Ihre eigenen Diagramme zu erstellen, oder die in der Konsole bereitgestellten Diagramme verwenden.

Null-Klickratendiagramm

Ein Liniendiagramm des Anteils von Nullklicks pro Tag. Das Diagramm hilft Ihnen, Muster in der täglichen Null-Klickrate zu visualisieren. Einige Beispiele sind eine stetige Erhöhung oder Verringerung der Null-Klickrate oder eine Erhöhung der sofortigen Antworten, die möglicherweise eine Erhöhung der Null-Klick-Werte beeinflussen.

Wenn Sie die API verwenden, können Sie diese Daten abrufen, indem Sie angeben`TREND_QUERY_DOC_METRICS`. Sie können die Daten verwenden, um Ihre eigenen Diagramme zu erstellen, oder die in der Konsole bereitgestellten Diagramme verwenden.

Ratendiagramm für Nullsuchergebnisse

Ein Liniendiagramm des Anteils an Null-Suchergebnissen pro Tag. Das Diagramm hilft Ihnen dabei, Muster in der täglichen Nullsuchergebnisrate zu visualisieren. Einige Beispiele sind eine stetige Zunahme oder Abnahme der Rate der Null-Suchergebnisse oder eine starke Abnahme der Anzahl der Dokumente in Ihrem Index, die möglicherweise eine Zunahme der Null-Suchergebnisse beeinflussen.

Wenn Sie die API verwenden, können Sie diese Daten abrufen, indem Sie angeben`TREND_QUERY_DOC_METRICS`. Sie können die Daten verwenden, um Ihre eigenen Diagramme zu erstellen, oder die in der Konsole bereitgestellten Diagramme verwenden.

Diagramm mit sofortiger Antwortrate

Ein Liniendiagramm des Anteils der Abfragen mit sofortiger Antwort oder zurückgegebenen häufig gestellten Fragen. Das Diagramm hilft Ihnen, Muster in der täglichen Instant-Antwortrate zu visualisieren. Einige Beispiele sind eine stetige Zunahme oder Abnahme von Abfragen vom Typ Frage-Antwort oder eine Abnahme von Click-Throughs, die möglicherweise eine Zunahme sofortiger Antworten beeinflussen.

Wenn Sie die API verwenden, können Sie diese Daten abrufen, indem Sie angeben`TREND_QUERY_DOC_METRICS`. Sie können die Daten verwenden, um Ihre eigenen Diagramme zu erstellen, oder die in der Konsole bereitgestellten Diagramme verwenden.

Feedback für inkrementelles Lernen einreichen

Amazon Kendra verwendet inkrementelles Lernen, um die Suchergebnisse zu verbessern. Durch inkrementelles Lernen werden anhand von Rückmeldungen aus Abfragen die Ranking-Algorithmen verbessert und die Suchergebnisse für eine höhere Genauigkeit optimiert.

Nehmen wir zum Beispiel an, dass Ihre Benutzer nach dem Begriff „Leistungen im Gesundheitswesen“ suchen. Wenn Benutzer durchweg das zweite Ergebnis aus der Liste wählen, wird dieses Ergebnis im Laufe Amazon Kendra der Zeit auf den ersten Platz angehoben. Der Boost nimmt mit der Zeit ab. Wenn Benutzer also aufhören, ein Ergebnis auszuwählen, wird es Amazon Kendra irgendwann entfernt und stattdessen ein anderes, beliebteres Ergebnis angezeigt. Auf diese Weise Amazon Kendra können Ergebnisse anhand von Relevanz, Alter und Inhalt priorisiert werden.

Inkrementelles Lernen ist für alle Indizes und für alle unterstützten Dokumenttypen aktiviert.

Amazon Kendra beginnt mit dem Lernen, sobald Sie Feedback geben. Es kann jedoch mehr als 24 Stunden dauern, bis die Ergebnisse des Feedbacks sichtbar sind. Amazon Kendra bietet drei Methoden, mit denen Sie Feedback einreichen können: die AWS Konsole, eine JavaScript Bibliothek, die Sie in Ihre Suchergebnisseite aufnehmen können, und eine API, die Sie verwenden können.

Amazon Kendra akzeptiert zwei Arten von Benutzerfeedback:

- Klicks — Informationen darüber, welche Abfrageergebnisse der Benutzer ausgewählt hat. Das Feedback umfasst die Ergebnis-ID und den Unix-Zeitstempel des Datums und der Uhrzeit der Auswahl des Suchergebnisses.

  Um Klick-Feedback zu senden, muss Ihre Anwendung Klickinformationen aus den Aktivitäten Ihrer Benutzer sammeln und diese Informationen dann an Amazon Kendra senden. Sie können Klickinformationen mit der Konsole, der JavaScript Bibliothek und der Amazon Kendra API sammeln.
- Relevanz — Informationen über die Relevanz eines Suchergebnisses, die der Benutzer in der Regel bereitstellt. Das Feedback enthält die Ergebnis-ID und einen Relevanzindikator (`RELEVANT`oder`NOT_RELEVANT`). Der Benutzer bestimmt die Relevanzinformationen.

  Um Feedback zur Relevanz zu senden, muss Ihre Anwendung einen Feedback-Mechanismus bieten, der es dem Benutzer ermöglicht, die entsprechende Relevanz für ein Abfrageergebnis auszuwählen und diese Informationen dann an zu senden Amazon Kendra. Sie können Relevanzinformationen nur mit der Konsole und der Amazon Kendra API sammeln.

Feedback wird verwendet, solange der Index aktiv ist. Feedback wirkt sich nur auf den Index aus, an den es übermittelt wurde. Es kann nicht indexübergreifend oder für verschiedene Konten verwendet werden.

Sie sollten zusätzlichen Benutzerkontext angeben, wenn Sie Ihren Amazon Kendra Index abfragen. Wenn Sie Benutzerkontext angeben, kann Amazon Kendra es feststellen, ob das Feedback von einem einzelnen Benutzer oder von mehreren Benutzern gegeben wurde, und die Suchergebnisse entsprechend anpassen.

Wenn Sie den Benutzerkontext angeben, wird das Feedback für die Anfrage dem spezifischen Benutzer zugeordnet, der im Kontext angegeben wurde. Wenn Sie keinen Benutzerkontext angeben, können Sie eine Besucher-ID angeben, die zum Gruppieren und Aggregieren von Abfragen verwendet wird.

Wenn Sie keinen Benutzerkontext oder keine Besucher-ID angeben, ist das Feedback anonym und wird mit anderem anonymen Feedback zusammengefasst.

Der folgende Code zeigt, wie Sie den Benutzerkontext als Token oder die Besucher-ID einbeziehen können.

```
response = kendra.query(
    QueryText = query,
    IndexId = index,
    UserToken = {
        Token = "token"
    })

    OR

    response = kendra.query(
    QueryText = query,
    IndexId = index,
    VisitorId = "visitor-id")
```

Für Webanwendungen können Sie Cookies, Standorte oder Browserbenutzer verwenden, um für jeden Benutzer eine Besucher-ID zu generieren.

Bei Suchanfragen, dem größten Volumen an Anfragen, bietet die Bereitstellung von Click-Through-Feedback genügend Informationen, um die Gesamtgenauigkeit zu verbessern. Bei Einzelanfragen, also solchen, die selten sind, sollten Fachexperten relevantes und nicht relevantes Feedback geben, um die Genauigkeit dieser Anfragen zu verbessern.

Zusätzlich zur Konsole können Sie eine von zwei Methoden verwenden: eine JavaScript Bibliothek oder die SubmitFeedbackAPI. Sie sollten nur eine Methode verwenden, um Feedback zu sammeln. Um optimale Ergebnisse zu erzielen, sollten Sie innerhalb von 24 Stunden nach der Anfrage Feedback einreichen.

Themen

Verwenden Sie die Amazon Kendra JavaScript Bibliothek, um Feedback einzureichen

Amazon Kendra bietet eine JavaScript Bibliothek, mit der Sie Klick-Feedback zu Ihrer Suchergebnisseite hinzufügen können. Um die Bibliothek zu verwenden, fügen Sie ein Skript-Tag in Ihren Client-Code ein, das das Suchergebnis anzeigt, und fügen dann Informationen zu den einzelnen Dokumentlinks in Ihrer Ergebnisliste hinzu. Wenn ein Benutzer einen Link zum Anzeigen eines Dokuments auswählt, werden Klickinformationen an gesendet Amazon Kendra.

Die Bibliothek funktioniert mit Browsern, die JavaScript Version ES6/ES2015 unterstützen.

Schritt 1: Fügen Sie ein Script-Tag in Ihre Suchanwendung ein Amazon Kendra

Fügen Sie in Ihrem Client-Code, der die Amazon Kendra Suchergebnisse rendert, ein <script>Tag ein und fügen Sie einen Verweis auf die JavaScript Bibliothek hinzu:

```
<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>
```

Das Skript lädt die JavaScript Bibliothek asynchron von einem Amazon Kendra gehosteten CDN herunter und initialisiert eine globale Variable namens`kendraFeedback`, mit der Sie optionale Parameter festlegen können.

Ersetzen Sie die *`Download-URL der Bibliothek`* und den *`Feedback-Endpunkt`* durch eine Kennung aus der folgenden Tabelle, die auf der Region basiert, in der Ihr Index gehostet wird. Amazon Kendra

Region	URL herunterladen	Feedback-Endpunkt
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

Region	URL herunterladen	Feedback-Endpunkt
ap-southeast-1	https://d1vvuam7g4taoe.cloudfront.net/ksf-v1	https://9je5uw7t5l.execute-api.ap-southeast-1.amazonaws.com/prod/submit
ap-southeast-2	https://dopqntoe6z0ce.cloudfront.net/ksf-v1.js	https://oovf4nvjj7.execute-api.ap-southeast-2.amazonaws.com/prod/submit
ap-south-1	https://d1ts9ouelsmk3g.cloudfront.net/ksf-v1.js	https://k1abnmd43b.execute-api.ap-south-1.amazonaws.com/prod/submit
ap-northeast-1	https://d3w0ybsa293kb4.cloudfront.net/ksf-v1.js	https://wg7rz0uzjh.execute-api.ap-northeast-1.amazonaws.com/prod/submit
eu-west-2	https://d1tsrujswld1d1.cloudfront.net/ksf-v1.js	https://qi7mct3x7f.execute-api.eu-west-2.amazonaws.com/prod/submit

Wenn sich Ihr Index beispielsweise in USA Ost (Nord-Virginia) befindet, lautet die *Download-URL für die Bibliothek* `https://d2zm0lpns956f8.cloudfront.net/ksf-v1.js` und der *Feedback-Endpunkt*`https://ujxwp5s92h.execute-api.us-east-1.amazonaws.com/prod/submit`.

Es gibt zwei optionale Einstellungen, die Sie für die Amazon Kendra JavaScript Bibliothek vornehmen können:

- `disableCookies`— Amazon Kendra Setzt standardmäßig ein Cookie, das den Benutzer eindeutig identifiziert. Stellen Sie dies auf ein`true`, um das Cookie zu deaktivieren.

  ```
  kendraFeedback('disableCookie', 'true | false');
  ```

  `searchDivClassName`— Überprüft standardmäßig alle Links auf Ihrer Suchergebnisseite auf Klicks. Amazon Kendra Stellen Sie dies auf einen `<div>` Klassennamen ein, um nur Links in der angegebenen Klasse zu überwachen.

```
kendraFeedback('searchDivClassName', 'class name');
```

Schritt 2: Fügen Sie das Feedback-Token zu den Suchergebnissen hinzu

Fügen Sie auf Ihrer Ergebnisseite ein HTML-Attribut hinzu, das dem Anchor-Tag oder dem unmittelbar übergeordneten Div-Tag zugeordnet ist und einen Link zu dem Dokument aus der Abfrageantwort enthält. `data-kendra-token` Beispielsweise:

```
<a href="document location" data-kendra-token="feedback token value"></a>
OR
<div data-url="document location" data-kendra-token="feedback token value"></div>
```

Eine Abfrageantwort enthält ein Token im `feedbackToken` Feld. Das Token identifiziert die Antwort eindeutig, wenn der Benutzer sie auswählt. Weisen Sie dem `data-kendra-token` Attribut den Wert des Tokens zu. Die Amazon Kendra JavaScript Bibliothek sucht nach diesem Token, wenn der Benutzer das Ergebnis auswählt, und sendet es als Feedback an einen Amazon Kendra Endpunkt.

Die Amazon Kendra JavaScript Bibliothek übermittelt nur das Feedback-Token und andere Metadaten wie den Zeitpunkt, zu dem das Ergebnis ausgewählt wurde, und eine eindeutige Besucher-ID.

Schritt 3: Testen Sie das Feedback-Skript

Gehen Sie wie folgt vor, um sicherzustellen, dass die JavaScript Bibliothek korrekt konfiguriert ist und Feedback an den richtigen Endpunkt gesendet wird. In diesem Beispiel wird der Chrome-Browser verwendet.

1. Öffnen Sie die Tools für Webentwickler im Browser. Öffnen Sie in Chrome das Chrome-Menü in der oberen rechten Ecke des Browsers, wählen Sie Weitere Tools und dann Entwicklertools.
2. Stellen Sie sicher, dass auf der Registerkarte „Konsole“ keine Fehler im Zusammenhang mit der Amazon Kendra JavaScript Bibliothek vorliegen.
3. Führen Sie eine Suche durch und wählen Sie ein beliebiges Ergebnis aus. Auf der Registerkarte Netzwerk der Entwicklertools. Sie sollten eine an den Feedback-Endpunkt gesendete Anfrage, das Token für das Ergebnis und den Status 200 OK sehen.

Verwenden Sie die Amazon Kendra API, um Feedback einzureichen

Um die Amazon Kendra API zum Senden von Rückmeldungen zu Anfragen zu verwenden, verwenden Sie die SubmitFeedbackAPI. Um die Abfrage zu identifizieren, geben Sie die Index-ID des Indexes an, auf den sich die Abfrage bezieht, und die Abfrage-ID, die in der Antwort von der Abfrage-API zurückgegeben wurde.

Das folgende Beispiel zeigt, wie Sie mithilfe der Amazon Kendra API Feedback zu Klicks und Relevanz einreichen können. Über die `RelevanceFeedbackItems` Arrays `ClickFeedbackItems` und können Sie mehrere Feedback-Sets einreichen. In diesem Beispiel werden ein einziger Klick und ein einzelnes Relevanz-Feedback-Element gesendet. Für die Übermittlung des Feedbacks wird die aktuelle Uhrzeit verwendet.

Um Feedback für eine Suche einzureichen (SDK)AWS

1. Sie können den folgenden Beispielcode mit den erforderlichen Werten verwenden:

   a. `index id`— Die ID des Indexes, für den sich die Abfrage bezieht.

   b. `query id`— Die Abfrage, zu der Sie Feedback geben möchten.

   c. `result id`— Die ID des Abfrageergebnisses, zu dem Sie Feedback geben möchten. Die Abfrageantwort enthält die Ergebnis-ID.

   d. `relevance value`— Entweder `RELEVANT` (das Abfrageergebnis ist relevant) oder `NOT_RELEVANT` (das Abfrageergebnis ist nicht relevant).

   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. Führen Sie den Code aus. Nachdem das Feedback übermittelt wurde, zeigt der Code eine Meldung an.

Hinzufügen von benutzerdefinierten Synonymen zu einem Index

Um benutzerdefinierte Synonyme zu einem Index hinzuzufügen, geben Sie sie in einer Thesaurusdatei an. Sie können geschäftsspezifische oder spezielle Begriffe in Amazon Kendra die Verwendung von Synonymen einbeziehen. Generische englische Synonyme, wie z. B.`leader, head`, sind in eine Thesaurusdatei integriert Amazon Kendra und sollten nicht in einer Thesaurusdatei enthalten sein. Dies gilt auch für generische Synonyme, die Bindestriche verwenden. Amazon Kendra unterstützt Synonyme für alle Antworttypen, einschließlich `DOCUMENT` Antworttypen und/oder Antworttypen. `QUESTION_ANSWER` `ANSWER` Amazon Kendra unterstützt derzeit nicht das Hinzufügen von Synonymen, die als Stoppwörter gekennzeichnet sind. Dies soll in einer future Version enthalten sein.

Amazon Kendra stellt Korrelationen zwischen Synonymen her. Wenn Sie beispielsweise das Synonympaar verwendenDynamo, `Amazon DynamoDB`, Amazon Kendra korreliert Dynamo mit. Amazon DynamoDB Die Abfrage „Was ist Dynamo?“ gibt dann ein Dokument wie „Was ist Amazon DynamoDB?“ zurück. Bei Synonymen Amazon Kendra kann die Korrelation leichter erkannt werden.

Die Thesaurus-Datei ist eine Textdatei, die in einem Amazon S3 Bucket gespeichert ist. Siehe Einen Thesaurus zu einem Index hinzufügen.

Die Thesaurus-Datei verwendet das Solr-Synonymformat. Amazon Kendra hat eine Obergrenze für die Anzahl der Thesauri pro Index. Siehe Kontingente.

Synonyme können in den folgenden Szenarien nützlich sein:

- Fachbegriffe, bei denen es sich nicht um traditionelle Synonyme in englischer Sprache handelt, wie `NLP, Natural Language Processing` z.
- Eigennamen mit komplexen semantischen Assoziationen. Dies sind Substantive, die die breite Öffentlichkeit wahrscheinlich nicht verstehen wird, beispielsweise beim maschinellen Lernen. `cost, loss, model performance`
- Verschiedene Formen von Produktnamen, zum BeispielElastic `Compute Cloud, EC2`.
- Domainspezifische oder geschäftsspezifische Begriffe wie Produktnamen. z. B. `Route53, DNS`.

Verwenden Sie in den folgenden Szenarien keine Synonyme:

- Generische Synonyme in englischer Sprache wie`leader, head`. Diese Synonyme sind nicht domänenspezifisch, und die Verwendung von Synonymen in diesen Szenarien kann unbeabsichtigte Auswirkungen haben.
- Tippfehler wie. `teh => the`
- Morphologische Varianten wie die Pluralformen und Possessiven von Substantiven, die Vergleichs- und Superlativform von Adjektiven sowie die Vergangenheitsform, das Partizip und die progressive Form von Verben. Ein Beispiel für komparative und superlative Adjektive ist. `good, better, best`
- Unigram (einzelnes Wort) Stoppwörter wie. `WHO` Unigram-Stoppwörter sind im Thesaurus nicht zulässig und werden von der Suche ausgeschlossen. Wird beispielsweise abgelehnt. `WHO => World Health Organization` Sie können `W.H.O.` jedoch einen synonymen Begriff verwenden, und Sie können Stoppwörter als Teil eines Synonyms mit mehreren Wörtern verwenden. Zum Beispiel ist das nicht erlaubt, `of` wird aber akzeptiert. `United States of America`

Mit benutzerdefinierten Synonymen können Sie Ihr Verständnis Ihrer unternehmensspezifischen Terminologie auf einfache Weise verbessern Amazon Kendra, indem Sie Ihre Abfragen auf Ihre unternehmensspezifischen Synonyme ausweiten. Auch wenn Synonyme die Suchgenauigkeit verbessern können, ist es wichtig zu verstehen, wie sich Synonyme auf die Latenz auswirken, damit Sie Ihre Suche entsprechend optimieren können.

Eine allgemeine Regel für Synonyme lautet: Je mehr Begriffe in Ihrer Abfrage mit Synonymen abgeglichen und erweitert werden, desto größer ist die potenzielle Auswirkung auf die Latenz. Andere Faktoren, die sich auf die Latenz auswirken, sind die durchschnittliche Größe der indexierten Dokumente, die Größe Ihres Indexes, jegliche Filterung der Suchergebnisse und die Gesamtauslastung Ihres Amazon Kendra Index. Abfragen, die mit keinem Synonym übereinstimmen, sind nicht betroffen.

Eine allgemeine Richtlinie dazu, wie sich Synonyme auf die Latenz auswirken:

Anwendungsfall	Erhöhung der Latenz*
Typische Abfragen in natürlicher Sprache oder nach Schlüsselwörtern mit jeweils 3 bis 5 Wörtern	Weniger als 15 Prozent
Ein Suchbegriff wird zu 3 Synonymen erweitert	

Anwendungsfall	Erhöhung der Latenz*
Index von etwa 500.000 Dokumenten (durchschnittlich 10,48 KB extrahierter Text pro Dokument) oder 30.000 FAQ/Fragenpaaren	

* Die Leistung hängt von Ihrer spezifischen Verwendung von Synonymen und Konfigurationen in Ihrem Index ab. Es empfiehlt sich, die Suchleistung zu testen, um genauere Benchmarks für Ihren speziellen Anwendungsfall zu erhalten.

Wenn Ihr Thesaurus groß ist, ein hohes Term-Expansionsverhältnis aufweist und Ihre Latenzzunahme nicht innerhalb akzeptabler Grenzen liegt, können Sie eine oder beide der folgenden Möglichkeiten ausprobieren:

- Kürzen Sie Ihren Thesaurus, um das Expansionsverhältnis (Anzahl der Synonyme pro Begriff) zu verringern.
- Reduzieren Sie die Gesamtabdeckung der Begriffe (Anzahl der Zeilen in Ihrem Thesaurus).

Alternativ können Sie die Bereitstellungskapazität (virtuelle Speichereinheiten) erhöhen, um den Anstieg der Latenz auszugleichen.

Themen

Eine Thesaurusdatei erstellen

Eine Amazon Kendra Thesaurus-Datei ist eine UTF-8-kodierte Datei, die eine Liste von Synonymen im Solr-Synonymlistenformat enthält. Die Thesaurus-Datei muss weniger als 5 MB groß sein.

Es gibt zwei Möglichkeiten, Synonymzuordnungen anzugeben:

- Bidirektionale Synonyme werden als kommagetrennte Liste von Begriffen angegeben. Wenn Ihr Benutzer einen der Begriffe abfragt, werden alle Begriffe in der Liste für die Suche nach Dokumenten verwendet, einschließlich des ursprünglich abgefragten Begriffs.
- Unidirektionale Synonyme werden als Begriffe angegeben, die durch das Symbol „**=>**“ voneinander getrennt werden, um Begriffe ihren Synonymen zuzuordnen. Wenn Ihr Benutzer einen Begriff links neben dem Symbol „**=>**“ abfragt, wird er einem Begriff auf der rechten Seite zugeordnet, um nach Dokumenten zu suchen, die das Synonym verwenden. Es wird nicht umgekehrt zugeordnet, sodass es unidirektional ist.

Bei den Synonymen selbst wird Groß- und Kleinschreibung beachtet, bei den Begriffen, denen sie zugeordnet werden, wird jedoch nicht zwischen Groß- und Kleinschreibung unterschieden. `ML => Machine Learning`Das heißt, wenn Ihr Benutzer „ML“ oder „ml“ abfragt oder eine andere Groß- und Kleinschreibung verwendet, wird dies „Machine Learning“ zugeordnet. Wenn Sie dies umgekehrt abbilden würden`Machine Learning => ML`, dann würden „Machine Learning“ oder „Machine Learning“ oder ein anderer Fall „ML“ zugeordnet.

Ein Synonym sucht nicht nach einer exakten Übereinstimmung bei Sonderzeichen. Wenn Sie beispielsweise nach "" dead-letter-queue suchen, Amazon Kendra können Dokumente zurückgegeben werden, die dem Begriff „Warteschlange für tote Briefe“ entsprechen (kein Bindestrich). Wenn Ihre Dokumente Bindestriche enthalten, z. B. "dead-letter-queue„, Amazon Kendra verarbeitet die Dokumente während der Suche, um Bindestriche zu entfernen. Nach allgemeinen englischen Synonymbegriffen, die in eine Thesaurusdatei integriert sind Amazon Kendra und nicht in einer Thesaurusdatei enthalten sein sollten, Amazon Kendra können Sie sowohl nach der Version mit Bindestrich als auch nach der Version ohne Bindestrich suchen. Wenn Sie beispielsweise nach „Drittanbieter“ und „Drittanbieter“ suchen, werden Dokumente Amazon Kendra zurückgegeben, die einer der beiden Versionen dieser Begriffe entsprechen.

Bei Synonymen, die Stoppwörter oder häufig verwendete Wörter enthalten, werden Dokumente Amazon Kendra zurückgegeben, die Begriffen, einschließlich Stoppwörtern, entsprechen. Sie können beispielsweise eine Synonymregel erstellen, um „Onboarding“ und „Onboarding“ zuzuordnen. Sie können Stoppwörter nicht allein für Synonyme verwenden. Wenn Sie beispielsweise nach „on“ suchen, Amazon Kendra können nicht alle Dokumente zurückgegeben werden, die „on“ enthalten.

Einige Synonymregeln werden ignoriert. `a => b`Ist zum Beispiel eine Regel, `a => a` wird aber ignoriert und zählt nicht als Regel.

Die Anzahl der Begriffe ist die Anzahl der eindeutigen Begriffe in der Theaurus-Datei. Die folgende Beispieldatei enthält Begriffe`AWS CodeStar`,`ML`,`Machine Learning`, `autoscaling group`ASG, und mehr.

Es gibt eine maximale Anzahl von Synonymregeln pro Thesaurus und eine maximale Anzahl von Synonymen pro Begriff. Weitere Informationen finden Sie unter Kontingente für Amazon Kendra.

Das folgende Beispiel zeigt eine Thesaurusdatei mit Synonymregeln. Jede Zeile enthält eine einzelne Synonymregel. Leerzeilen und Kommentare werden ignoriert.

```
# 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.
```

Einen Thesaurus zu einem Index hinzufügen

Die folgenden Verfahren zeigen, wie Sie einem Index eine Thesaurusdatei mit Synonymen hinzufügen. Es kann bis zu 30 Minuten dauern, bis die Auswirkungen Ihrer aktualisierten Thesaurusdatei sichtbar werden. Weitere Informationen zur Thesaurus-Datei finden Sie unter. Eine Thesaurusdatei erstellen

Console

So fügen Sie einen Thesaurus hinzu

1. Wählen Sie im linken Navigationsbereich unter dem Index, dem Sie eine Liste von Synonymen hinzufügen möchten, Ihrem Thesaurus, Synonyme aus.
2. Wählen Sie auf der Synonymseite die Option Thesaurus hinzufügen aus.
3. Geben Sie Ihrem Thesaurus unter Thesaurus definieren einen Namen und optional eine Beschreibung.
4. Geben Sie in den Thesaurus-Einstellungen den Amazon S3 Pfad zu Ihrer Thesaurusdatei an. Die Datei muss kleiner als 5 MB sein.
5. Wählen Sie für IAM-Rolle eine Rolle aus, oder wählen Sie Neue Rolle erstellen und geben Sie einen Rollennamen an, um eine neue Rolle zu erstellen. Amazon Kendra verwendet diese Rolle, um in Ihrem Namen auf die Amazon S3 Ressource zuzugreifen. Die IAM-Rolle hat das Präfix "AmazonKendra-“.
6. Wählen Sie Speichern, um die Konfiguration zu speichern und den Thesaurus hinzuzufügen. Sobald der Thesaurus aufgenommen wurde, ist er aktiv und Synonyme werden in den Ergebnissen hervorgehoben. Es kann bis zu 30 Minuten dauern, bis die Auswirkungen Ihrer Thesaurus-Datei sichtbar werden.

CLI

Um einem Index mit dem einen Thesarus hinzuzufügen, rufen Sie folgenden Befehl auf 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
```

Rufen Sie an`list-thesauri`, um eine Liste von Thesauren zu sehen:

```
aws kendra list-thesauri \
--index-id index-id
```

Einzelheiten zu einem Thesaurus erhalten Sie unter: `describe-thesaurus`

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

Es kann bis zu 30 Minuten dauern, bis Sie die Auswirkungen Ihrer Thesaurus-Datei sehen.

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.");
  }
}
```

Einen Thesaurus aktualisieren

Sie können die Konfiguration eines Thesaurus ändern, nachdem er erstellt wurde. Sie können Details wie den Namen des Thesaurus und die IAM-Informationen ändern. Sie können auch den Speicherort des Amazon S3 S3-Pfads der Thesaurusdatei ändern. Wenn Sie den Pfad zur Thesaurusdatei ändern, wird der vorhandene Thesaurus Amazon Kendra durch den Thesaurus ersetzt, der im aktualisierten Pfad angegeben ist.

Es kann bis zu 30 Minuten dauern, bis die Auswirkungen Ihrer aktualisierten Thesaurusdatei sichtbar werden.

> **Note**
>
> Wenn die Thesaurusdatei Überprüfungs- oder Syntaxfehler enthält, wird die zuvor hochgeladene Thesaurusdatei beibehalten.

Die folgenden Verfahren zeigen, wie Sie Thesaurusdetails ändern können.

Console

Um Thesaurusdetails zu ändern

1. Wählen Sie im linken Navigationsbereich unter dem Index, den Sie ändern möchten, die Option Synonyme aus.
2. Wählen Sie auf der Synonym-Seite den Thesaurus aus, den Sie ändern möchten, und klicken Sie dann auf Bearbeiten.
3. Aktualisieren Sie auf der Seite Thesaurus aktualisieren die Thesaurusdetails.
4. (Optional) Wählen Sie Thesaurusdateipfad ändern und geben Sie dann einen Amazon S3 Pfad zur neuen Thesaurusdatei an. Ihre bestehende Thesaurusdatei wird durch die von Ihnen angegebene Datei ersetzt. Wenn Sie den Pfad nicht ändern, wird der Thesaurus aus dem vorhandenen Pfad Amazon Kendra neu geladen.

   Wenn Sie Aktuelle Thesaurusdatei beibehalten auswählen, wird die Thesaurusdatei Amazon Kendra nicht erneut geladen.
5. Wählen Sie Speichern, um die Konfiguration zu speichern.

Sie können den Thesaurus auch aus dem vorhandenen Thesaurus-Pfad neu laden.

Um einen Thesaurus aus einem vorhandenen Pfad neu zu laden

1. Wählen Sie im linken Navigationsbereich unter dem Index, den Sie ändern möchten, die Option Synonyme aus.
2. Wählen Sie auf der Synonym-Seite den Thesaurus aus, den Sie neu laden möchten, und klicken Sie dann auf Aktualisieren.
3. Bestätigen Sie auf der Seite Thesaurusdatei neu laden, dass Sie die Thesaurusdatei aktualisieren möchten.

CLI

Um einen Thesaurus zu aktualisieren, rufen Sie: `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.");
  }
}
```

Einen Thesaurus löschen

Die folgenden Verfahren zeigen, wie Sie einen Thesaurus löschen.

Console

1. Wählen Sie im linken Navigationsbereich unter dem Index, den Sie ändern möchten, die Option Synonyme aus.
2. Wählen Sie auf der Synonym-Seite den Thesaurus aus, den Sie löschen möchten.
3. Wählen Sie auf der Thesaurus-Detailseite die Option Löschen aus und bestätigen Sie dann den Löschvorgang.

CLI

Um einen Thesarus aus einem Index mit dem zu löschen AWS CLI, rufen Sie: `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);
  }
}
```

Höhepunkte in den Suchergebnissen

Die Synonymhervorhebung ist standardmäßig aktiviert. Highlight-Informationen sind in den Amazon Kendra SDK- und CLI-Abfrageergebnissen enthalten. Wenn Sie mit dem Amazon Kendra SDK oder der CLI interagieren, bestimmen Sie, wie die Ergebnisse angezeigt werden.

Synonymhervorhebungen haben den Markierungstyp. `THESAURUS_SYNONYM` Weitere Informationen zu Highlights finden Sie im Highlight-Objekt.

Tutorial: Aufbau einer mit Metadaten angereicherten, intelligenten Suchlösung mit Amazon Kendra

Dieses Tutorial zeigt Ihnen, wie Sie mithilfe von Amazon Kendra, Amazon Comprehend, Amazon Simple Storage Service (S3) und eine mit Metadaten angereicherte, auf natürlicher Sprache basierende, intelligente Suchlösung für Ihre Unternehmensdaten erstellen. AWS CloudShell

Amazon Kendra ist ein intelligenter Suchdienst, der einen Suchindex für Ihre unstrukturierten Datenrepositorien in natürlicher Sprache erstellen kann. Um es Ihren Kunden zu erleichtern, relevante Antworten zu finden und zu filtern, können Sie Amazon Comprehend verwenden, um Metadaten aus Ihren Daten zu extrahieren und sie in Ihren Amazon Kendra-Suchindex aufzunehmen.

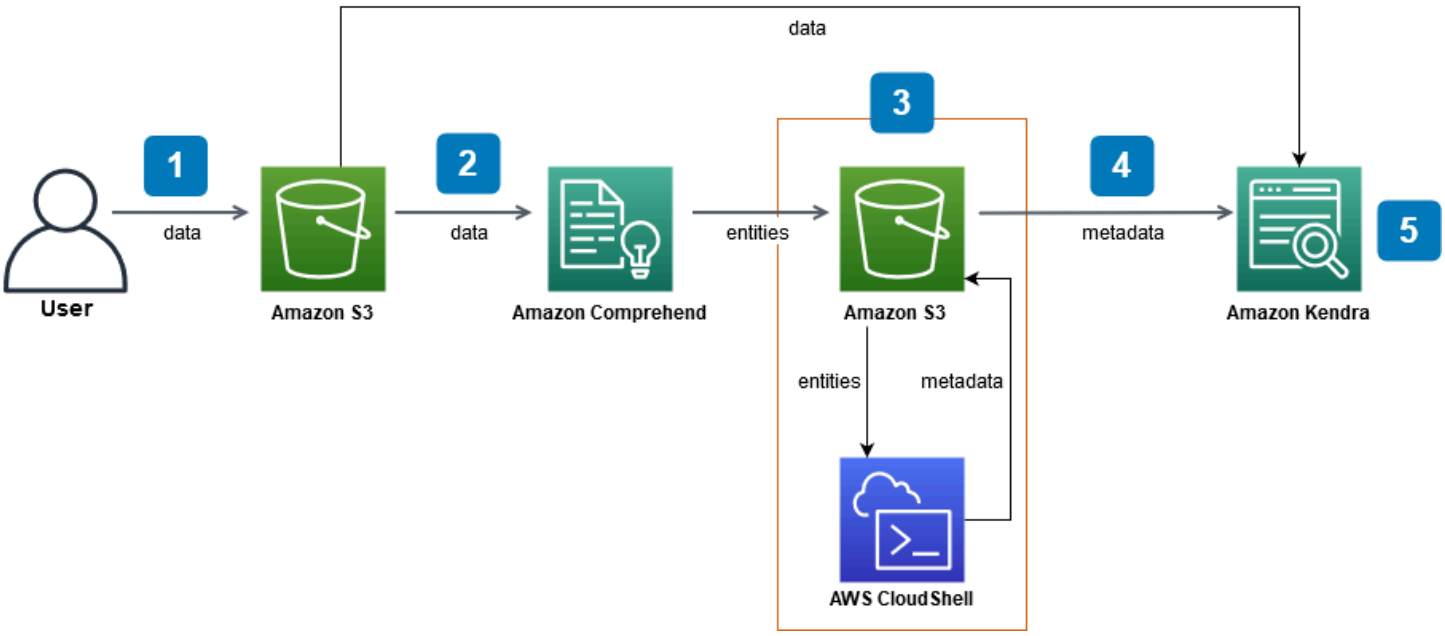
Amazon Comprehend ist ein Service zur Verarbeitung natürlicher Sprache (Natural Language Processing, NLP), der Entitäten identifizieren kann. Entitäten sind Verweise auf Personen, Orte, Orte, Organisationen und Objekte in Ihren Daten.

In diesem Tutorial wird ein Beispieldatensatz mit Nachrichtenartikeln verwendet, um Entitäten zu extrahieren, sie in Metadaten umzuwandeln und sie in Ihren Amazon Kendra-Index aufzunehmen, um Suchen durchzuführen. Mit den hinzugefügten Metadaten können Sie Ihre Suchergebnisse anhand einer beliebigen Teilmenge dieser Entitäten filtern und die Suchgenauigkeit verbessern. In diesem Tutorial erfahren Sie, wie Sie eine Suchlösung für Ihre Unternehmensdaten ohne spezielle Kenntnisse im Bereich maschinelles Lernen erstellen.

Dieses Tutorial zeigt Ihnen, wie Sie Ihre Suchlösung mithilfe der folgenden Schritte erstellen:

1. Speichern eines Beispieldatensatzes mit Nachrichtenartikeln in Amazon S3.
2. Verwenden Sie Amazon Comprehend, um Entitäten aus Ihren Daten zu extrahieren.
3. Ausführen eines Python-3-Skripts zur Konvertierung der Entitäten in das Amazon Kendra-Index-Metadatenformat und Speichern dieser Metadaten in S3.
4. Erstellen eines Amazon Kendra-Suchindex und Erfassung der Daten und Metadaten.
5. Den Suchindex abfragen.

Das folgende Diagramm zeigt den Arbeitsablauf:



Geschätzte Zeit bis zum Abschluss dieses Tutorials: 1 Stunde

Geschätzte Kosten: Für einige der Aktionen in diesem Tutorial fallen Gebühren von Ihrem AWS Konto an. Weitere Informationen zu den Kosten der einzelnen Services finden Sie auf den Preisseiten für Amazon S3, Amazon Comprehend und Amazon AWS CloudShellKendra.

Themen

Voraussetzungen

Um dieses Tutorial abzuschließen, benötigen Sie die folgenden Ressourcen:

- Ein AWS-Konto. Wenn Sie kein AWS Konto haben, folgen Sie den Schritten unter Amazon Kendra einrichten, um Ihr AWS Konto einzurichten.

- Ein Entwicklungscomputer, auf dem Windows, macOS oder Linux ausgeführt wird, um auf die AWS Managementkonsole zuzugreifen. Weitere Informationen finden Sie unter Konfiguration der AWS Management Console.
- Ein AWS Identity and Access Management(IAM-) Benutzer. Informationen zum Einrichten eines IAM-Benutzers und einer IAM-Gruppe für Ihr Konto finden Sie im Abschnitt Erste Schritte im IAM-Benutzerhandbuch.

  Wenn Sie die verwendenAWS Command Line Interface, müssen Sie Ihrem IAM-Benutzer außerdem die folgende Richtlinie zuordnen, um ihm die grundlegenden Berechtigungen zu gewähren, die für die Durchführung dieses Tutorials erforderlich sind.

  Weitere Informationen finden Sie unter Erstellen von IAM-Richtlinien und Hinzufügen und Entfernen von IAM-Identitätsberechtigungen.
- Die Liste der AWS regionalen Dienste. Um die Latenz zu reduzieren, sollten Sie die AWS Region wählen, die Ihrem geografischen Standort am nächsten liegt und die sowohl von Amazon Comprehend als auch von Amazon Kendra unterstützt wird.
- (Fakultativ) Ein AWS Key Management Service. In diesem Tutorial wird zwar keine Verschlüsselung verwendet, Sie sollten jedoch die bewährten Verschlüsselungsmethoden für Ihren speziellen Anwendungsfall verwenden.
- (Optional) Eine Amazon Virtual Private Cloud. In diesem Tutorial wird zwar keine VPC verwendet, Sie sollten jedoch die bewährten VPC-Methoden verwenden, um die Datensicherheit für Ihren speziellen Anwendungsfall zu gewährleisten.

Schritt 1: Dokumente zu Amazon S3 hinzufügen

Bevor Sie einen Amazon Comprehend-Entitätsanalysejob für Ihren Datensatz ausführen, erstellen Sie einen Amazon S3-Bucket, um die Daten, Metadaten und die Analyseausgabe der Amazon Comprehend-Entitäten zu hosten.

Themen

- Herunterladen des Beispieldatensatzes
- Erstellung eines Amazon S3-Buckets
- Erstellen von Daten- und Metadatenordnern in Ihrem S3-Bucket
- Upload der Eingabedaten

Herunterladen des Beispieldatensatzes

Bevor Amazon Comprehend einen Entitätsanalyse-Job für Ihre Daten ausführen kann, müssen Sie den Datensatz herunterladen, extrahieren und in einen S3-Bucket hochladen.

Um den Datensatz herunterzuladen und zu extrahieren (Konsole)

1. Laden Sie den Ordner tutorial-dataset.zip auf Ihr Gerät herunter.
2. Extrahieren `tutorial-dataset` Sie den Ordner, um auf den `data` Ordner zuzugreifen.

Zum Herunterladen und Extrahieren des Datensatzes (Terminal)

1. Um das herunterzuladen`tutorial-dataset`, führen Sie den folgenden Befehl in einem Terminalfenster aus:

   Linux

   ```
   curl -o path/tutorial-dataset.zip https://docs.aws.amazon.com/kendra/latest/dg/
   samples/tutorial-dataset.zip
   ```

   Wobei gilt:

   - *path/* ist der lokale Dateipfad zu dem Ort, an dem Sie den Zip-Ordner speichern möchten.

   macOS

   ```
   curl -o path/tutorial-dataset.zip https://docs.aws.amazon.com/kendra/latest/dg/
   samples/tutorial-dataset.zip
   ```

   Wobei gilt:

   - *path/* ist der lokale Dateipfad zu dem Ort, an dem Sie den Zip-Ordner speichern möchten.

   Windows

   ```
   curl -o path/tutorial-dataset.zip https://docs.aws.amazon.com/kendra/latest/dg/
   samples/tutorial-dataset.zip
   ```

Wobei gilt:

- *path/* ist der lokale Dateipfad zu dem Ort, an dem Sie den Zip-Ordner speichern möchten.

2. Um die Daten aus dem Zip-Ordner zu extrahieren, führen Sie den folgenden Befehl im Terminalfenster aus:

   Linux

   ```
   unzip path/tutorial-dataset.zip -d path/
   ```

   Wobei gilt:

   - *path/* ist der lokale Dateipfad zu Ihrem gespeicherten Zip-Ordner.

   macOS

   ```
   unzip path/tutorial-dataset.zip -d path/
   ```

   Wobei gilt:

   - *path/* ist der lokale Dateipfad zu Ihrem gespeicherten Zip-Ordner.

   Windows

   ```
   tar -xf path/tutorial-dataset.zip -C path/
   ```

   Wobei gilt:

   - *path/* ist der lokale Dateipfad zu Ihrem gespeicherten Zip-Ordner.

Am Ende dieses Schritts sollten Sie die extrahierten Dateien in einem dekomprimierten Ordner namens `tutorial-dataset` haben. Dieser Ordner enthält eine `README` Datei mit einer Apache 2.0-Open-Source-Zuordnung und einen Ordner mit dem Namen, der den Datensatz für dieses Tutorial `data` enthält. Der Datensatz besteht aus 100 Dateien mit `.story` Erweiterungen.

Erstellung eines Amazon S3-Buckets

Nachdem Sie den Beispieldatenordner heruntergeladen und extrahiert haben, speichern Sie ihn in einem Amazon S3-Bucket.

> **Important**
>
> Der Name eines Amazon S3-Buckets muss für alle von eindeutig seinAWS.

So erstellen Sie einen S3-Bucket (Konsole)

1. Melden Sie sich bei der AWS Management Console an und öffnen Sie die Amazon-S3-Konsole unter https://console.aws.amazon.com/s3/.
2. Wählen Sie unter Buckets die Option Create bucket aus.
3. Geben Sie für Bucket name einen eindeutigen Namen ein.
4. Wählen Sie unter Region die AWS Region aus, in der Sie den Bucket erstellen möchten.

   > **Note**
   >
   > Sie müssen eine Region auswählen, die sowohl Amazon Comprehend als auch Amazon Kendra unterstützt. Sie können die Region eines Buckets nicht ändern, nachdem Sie ihn erstellt haben.

5. Behalten Sie die Standardeinstellungen für Block Public Access für diesen Bucket, Bucket Versioning und Tags bei.
6. Wählen Sie für Standardverschlüsselung die Option Deaktivieren.
7. Behalten Sie die Standardeinstellungen für die erweiterten Einstellungen bei.
8. Überprüfen Sie Ihre Bucket-Konfiguration und wählen Sie dann Create Bucket aus.

Um einen S3-Bucket zu erstellen (AWS CLI)

1. Um einen S3-Bucket zu erstellen, verwenden Sie den Befehl create-bucket in der: AWS CLI

   Linux

   ```
   aws s3api create-bucket \
   ```

```
        --bucket DOC-EXAMPLE-BUCKET \
        --region aws-region \
        --create-bucket-configuration LocationConstraint=aws-region
```

Wobei gilt:

- *DOC-EXAMPLE-BUCKET ist Ihr Bucket-Name*,
- *aws-region* ist die Region, in der Sie Ihren Bucket erstellen möchten.

macOS

```
aws s3api create-bucket \
        --bucket DOC-EXAMPLE-BUCKET \
        --region aws-region \
        --create-bucket-configuration LocationConstraint=aws-region
```

Wobei gilt:

- *DOC-EXAMPLE-BUCKET ist Ihr Bucket-Name*,
- *aws-region* ist die Region, in der Sie Ihren Bucket erstellen möchten.

Windows

```
aws s3api create-bucket ^
        --bucket DOC-EXAMPLE-BUCKET ^
        --region aws-region ^
        --create-bucket-configuration LocationConstraint=aws-region
```

Wobei gilt:

- *DOC-EXAMPLE-BUCKET ist Ihr Bucket-Name*,
- *aws-region* ist die Region, in der Sie Ihren Bucket erstellen möchten.

> **Note**
>
> Sie müssen eine Region auswählen, die sowohl Amazon Comprehend als auch Amazon Kendra unterstützt. Sie können die Region eines Buckets nicht ändern, nachdem Sie ihn erstellt haben.

2. Um sicherzustellen, dass Ihr Bucket erfolgreich erstellt wurde, verwenden Sie den Befehl list:

   Linux

   ```
   aws s3 ls
   ```

   macOS

   ```
   aws s3 ls
   ```

   Windows

   ```
   aws s3 ls
   ```

Erstellen von Daten- und Metadatenordnern in Ihrem S3-Bucket

Nachdem Sie Ihren S3-Bucket erstellt haben, erstellen Sie darin Daten- und Metadatenordner.

So erstellen Sie Ordner in Ihrem S3-Bucket (Konsole)

1. Öffnen Sie die Amazon-S3-Konsole unter https://console.aws.amazon.com/s3/.
2. Klicken Sie unter Buckets in der Liste der Buckets auf den Namen Ihres Buckets.
3. Wählen Sie auf der Registerkarte Objekte die Option Ordner erstellen aus.
4. Geben Sie als neuen Ordnernamen ein**`data`**.
5. Wählen Sie für die Verschlüsselungseinstellungen Deaktivieren.
6. Wählen Sie Create folder.
7. Wiederholen Sie die Schritte 3 bis 6, um einen weiteren Ordner zum Speichern der Amazon Kendra-Metadaten zu erstellen, und geben Sie dem in Schritt 4 **`metadata`** erstellten Ordner einen Namen.

So erstellen Sie Ordner in Ihrem S3-Bucket (AWS CLI)

1. Um den `data` Ordner in Ihrem S3-Bucket zu erstellen, verwenden Sie den Befehl put-object in der: AWS CLI

   Linux

   ```
   aws s3api put-object \
           --bucket DOC-EXAMPLE-BUCKET \
           --key data/
   ```

   Wobei gilt:

   - *DOC-EXAMPLE-BUCKET ist Ihr Bucket-Name*.

   macOS

   ```
   aws s3api put-object \
           --bucket DOC-EXAMPLE-BUCKET \
           --key data/
   ```

   Wobei gilt:

   - *DOC-EXAMPLE-BUCKET ist Ihr Bucket-Name*.

   Windows

   ```
   aws s3api put-object ^
           --bucket DOC-EXAMPLE-BUCKET ^
           --key data/
   ```

   Wobei gilt:

   - *DOC-EXAMPLE-BUCKET ist Ihr Bucket-Name*.

2. Um den `metadata` Ordner in Ihrem S3-Bucket zu erstellen, verwenden Sie den Befehl put-object in der: AWS CLI

Linux

```
aws s3api put-object \
        --bucket DOC-EXAMPLE-BUCKET \
        --key metadata/
```

Wobei gilt:

- *DOC-EXAMPLE-BUCKET ist Ihr Bucket-Name*.

macOS

```
aws s3api put-object \
        --bucket DOC-EXAMPLE-BUCKET \
        --key metadata/
```

Wobei gilt:

- *DOC-EXAMPLE-BUCKET ist Ihr Bucket-Name*.

Windows

```
aws s3api put-object ^
        --bucket DOC-EXAMPLE-BUCKET ^
        --key metadata/
```

Wobei gilt:

- *DOC-EXAMPLE-BUCKET ist Ihr Bucket-Name*.

3. Um sicherzustellen, dass Ihre Ordner erfolgreich erstellt wurden, überprüfen Sie den Inhalt Ihres Buckets mit dem Befehl list:

Linux

```
aws s3 ls s3://DOC-EXAMPLE-BUCKET/
```

Wobei gilt:

- *DOC-EXAMPLE-BUCKET ist Ihr Bucket-Name*.

macOS

```
aws s3 ls s3://DOC-EXAMPLE-BUCKET/
```

Wobei gilt:

- *DOC-EXAMPLE-BUCKET ist Ihr Bucket-Name*.

Windows

```
aws s3 ls s3://DOC-EXAMPLE-BUCKET/
```

Wobei gilt:

- *DOC-EXAMPLE-BUCKET ist Ihr Bucket-Name*.

Upload der Eingabedaten

Nachdem Sie Ihre Daten- und Metadatenordner erstellt haben, laden Sie den Beispieldatensatz in den `data` Ordner hoch.

Um den Beispieldatensatz in den Datenordner hochzuladen (Konsole)

1. Öffnen Sie die Amazon-S3-Konsole unter https://console.aws.amazon.com/s3/.
2. Klicken Sie in Buckets in der Liste der Buckets auf den Namen Ihres Buckets und dann auf. `data`
3. Wählen Sie Hochladen und dann Dateien hinzufügen.
4. Navigieren Sie im Dialogfeld zu dem `data` Ordner innerhalb des `tutorial-dataset` Ordners auf Ihrem lokalen Gerät, wählen Sie alle Dateien aus und wählen Sie dann Öffnen.
5. Behalten Sie die Standardeinstellungen für Ziel, Berechtigungen und Eigenschaften bei.
6. Klicken Sie auf Upload.

Um den Beispieldatensatz in den Datenordner hochzuladen (AWS CLI)

1. Um die Beispieldaten in den `data` Ordner hochzuladen, verwenden Sie den Befehl copy in derAWS CLI:

   Linux

   ```
   aws s3 cp path/tutorial-dataset/data s3://DOC-EXAMPLE-BUCKET/data/ --recursive
   ```

   Wobei gilt:

   - *path/* ist der Dateipfad zu dem `tutorial-dataset` Ordner auf Ihrem Gerät,
   - *DOC-EXAMPLE-BUCKET ist Ihr Bucket-Name*.

   macOS

   ```
   aws s3 cp path/tutorial-dataset/data s3://DOC-EXAMPLE-BUCKET/data/ --recursive
   ```

   Wobei gilt:

   - *path/* ist der Dateipfad zu dem `tutorial-dataset` Ordner auf Ihrem Gerät,
   - *DOC-EXAMPLE-BUCKET ist Ihr Bucket-Name*.

   Windows

   ```
   aws s3 cp path/tutorial-dataset/data s3://DOC-EXAMPLE-BUCKET/data/ --recursive
   ```

   Wobei gilt:

   - *path/* ist der Dateipfad zu dem `tutorial-dataset` Ordner auf Ihrem Gerät,
   - *DOC-EXAMPLE-BUCKET ist Ihr Bucket-Name*.

2. Um sicherzustellen, dass Ihre Datensatzdateien erfolgreich in Ihren `data` Ordner hochgeladen wurden, verwenden Sie den Befehl list in derAWS CLI:

   Linux

   ```
   aws s3 ls s3://DOC-EXAMPLE-BUCKET/data/
   ```

Wobei gilt:

- *DOC-EXAMPLE-BUCKET* ist der Name Ihres S3-Buckets.

macOS

```
aws s3 ls s3://DOC-EXAMPLE-BUCKET/data/
```

Wobei gilt:

- *DOC-EXAMPLE-BUCKET* ist der Name Ihres S3-Buckets.

Windows

```
aws s3 ls s3://DOC-EXAMPLE-BUCKET/data/
```

Wobei gilt:

- *DOC-EXAMPLE-BUCKET* ist der Name Ihres S3-Buckets.

Am Ende dieses Schritts haben Sie einen S3-Bucket, in dem Ihr Datensatz im `data` Ordner gespeichert ist, und einen leeren `metadata` Ordner, in dem Ihre Amazon Kendra-Metadaten gespeichert werden.

Schritt 2: Ausführen eines Entitätsanalyse-Jobs auf Amazon Comprehend

Nachdem Sie den Beispieldatensatz in Ihrem S3-Bucket gespeichert haben, führen Sie einen Amazon Comprehend-Entitätsanalysejob aus, um Entitäten aus Ihren Dokumenten zu extrahieren. Diese Entitäten bilden benutzerdefinierte Amazon Kendra-Attribute und helfen Ihnen dabei, Suchergebnisse in Ihrem Index zu filtern. Weitere Informationen finden Sie unter Entitäten erkennen.

Themen

- Ausführen eines Amazon Comprehend Entities Analyse-Jobs

Ausführen eines Amazon Comprehend Entities Analyse-Jobs

Um Entitäten aus Ihrem Datensatz zu extrahieren, führen Sie einen Amazon Comprehend-Entitätsanalysejob aus.

Wenn Sie in diesem Schritt die AWS CLI verwenden, erstellen Sie zunächst eine AWS IAM-Rolle und -Richtlinie für Amazon Comprehend, hängen sie an und führen dann einen Entitätsanalyse-Job aus. Um einen Entitätsanalyse-Job für Ihre Beispieldaten auszuführen, benötigt Amazon Comprehend:

- eine AWS Identity and Access Management (IAM-) Rolle, die sie als vertrauenswürdige Entität anerkennt
- eine an die AWS IAM-Rolle angehängte IAM-Richtlinie, die ihr Berechtigungen für den Zugriff auf Ihren S3-Bucket erteilt

Weitere Informationen finden Sie unter So arbeitet Amazon Comprehend mit IAM und identitätsbasierte Richtlinien für Amazon Comprehend.

Um einen Amazon Comprehend Entities Analyse-Job auszuführen (Konsole)

1. Öffnen Sie die Amazon Comprehend-Konsole unter https://console.aws.amazon.com/comprehend/.

   > **Important**
   >
   > Stellen Sie sicher, dass Sie sich in derselben Region befinden, in der Sie Ihren Amazon S3-Bucket erstellt haben. Wenn Sie sich in einer anderen Region befinden, wählen Sie in der AWS Regionsauswahl in der oberen Navigationsleiste die Region aus, in der Sie Ihren S3-Bucket erstellt haben.

2. Wählen Sie Amazon Comprehend starten.
3. Wählen Sie im linken Navigationsbereich Analyseaufträge aus.
4. Wählen Sie Create job (Auftrag erstellen) aus.
5. Gehen Sie im Abschnitt Jobeinstellungen wie folgt vor:

   a. Geben Sie unter Name **`data-entities-analysis`** ein.

   b. Wählen Sie als Analysetyp Entitäten aus.

   c. Wählen Sie für Sprache die Option Englisch aus.

   d. Lassen Sie die Jobverschlüsselung deaktiviert.

6. Gehen Sie im Abschnitt Eingabedaten wie folgt vor:

   a. Wählen Sie als Datenquelle Meine Dokumente aus.

   b. Wählen Sie für den S3-Standort die Option S3 durchsuchen aus.

   c. Klicken Sie unter Ressourcen auswählen in der Liste der Buckets auf den Namen Ihres Buckets.

   d. Wählen Sie für Objekte das Optionsfeld für `data` und wählen Sie Auswählen.

   e. Wählen Sie als Eingabeformat Die Option Ein Dokument pro Datei aus.

7. Gehen Sie im Abschnitt Ausgabedaten wie folgt vor:

   a. Wählen Sie für den S3-Standort die Option S3 durchsuchen aus und wählen Sie dann das Optionsfeld für Ihren Bucket aus der Liste der Buckets aus und klicken Sie auf Auswählen.

   b. Lassen Sie die Verschlüsselung ausgeschaltet.

8. Gehen Sie im Abschnitt Zugriffsberechtigungen wie folgt vor:

   a. Wählen Sie für IAM-Rolle die Option Create an IAM-Rolle aus.

   b. Wählen Sie für Zugriffsberechtigungen die Option Eingabe- und Ausgabe-S3-Buckets aus.

   c. Geben **`comprehend-role`** Sie als Namenssuffix ein. Diese Rolle bietet Zugriff auf Ihren Amazon S3-Bucket.

9. Behalten Sie die Standard-VPC-Einstellungen bei.

10. Wählen Sie Create job (Auftrag erstellen) aus.

Um einen Amazon Comprehend Entities Analyse-Job auszuführen () AWS CLI

1. Gehen Sie wie folgt vor, um eine IAM-Rolle für Amazon Comprehend zu erstellen und anzuhängen, die diese Rolle als vertrauenswürdige Entität anerkennt:

   a. Speichern Sie die folgende Vertrauensrichtlinie als JSON-Datei, die `comprehend-trust-policy.json` in einem Texteditor auf Ihrem lokalen Gerät aufgerufen wird.

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

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

b. Verwenden Sie den Befehl create-role, um eine IAM-Rolle mit dem Namen zu erstellen `comprehend-role` und Ihre gespeicherte `comprehend-trust-policy.json` Datei daran anzuhängen:

Linux

```
aws iam create-role \
          --role-name comprehend-role \
          --assume-role-policy-document file://path/comprehend-trust-
policy.json
```

Wobei gilt:

- *path/* ist der Dateipfad zu `comprehend-trust-policy.json` Ihrem lokalen Gerät.

macOS

```
aws iam create-role \
          --role-name comprehend-role \
          --assume-role-policy-document file://path/comprehend-trust-
policy.json
```

Wobei gilt:

- *path/* ist der Dateipfad zu `comprehend-trust-policy.json` Ihrem lokalen Gerät.

Windows

```
aws iam create-role ^
          --role-name comprehend-role ^
          --assume-role-policy-document file://path/comprehend-trust-
policy.json
```

Wobei gilt:

- *path/* ist der Dateipfad zu `comprehend-trust-policy.json` Ihrem lokalen Gerät.

c. Kopieren Sie den Amazon Resource Name (ARN) in Ihren Texteditor und speichern Sie ihn lokal unter`comprehend-role-arn`.

> **Note**
>
> Der ARN hat ein ähnliches Format wie *arn:aws:iam: :123456789012:role/comprehend-role*. Sie benötigen den ARN, unter dem Sie gespeichert haben`comprehend-role-arn`, um den Amazon Comprehend-Analysejob auszuführen.

2. Gehen Sie wie folgt vor, um eine IAM-Richtlinie zu erstellen und an Ihre IAM-Rolle anzuhängen, die ihr Berechtigungen für den Zugriff auf Ihren S3-Bucket gewährt:

a. Speichern Sie die folgende Vertrauensrichtlinie als JSON-Datei, die `comprehend-S3-access-policy.json` in einem Texteditor auf Ihrem lokalen Gerät aufgerufen wird.

```
{
    "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. Verwenden Sie den Befehl create-policy, `comprehend-S3-access-policy` um eine IAM-Richtlinie für den Zugriff auf Ihren S3-Bucket zu erstellen:

Linux

```
aws iam create-policy \
          --policy-name comprehend-S3-access-policy \
          --policy-document file://path/comprehend-S3-access-policy.json
```

Wobei gilt:

- *path/* ist der Dateipfad zu `comprehend-S3-access-policy.json` Ihrem lokalen Gerät.

macOS

```
aws iam create-policy \
          --policy-name comprehend-S3-access-policy \
          --policy-document file://path/comprehend-S3-access-policy.json
```

Wobei gilt:

- *path/* ist der Dateipfad zu `comprehend-S3-access-policy.json` Ihrem lokalen Gerät.

Windows

```
aws iam create-policy ^
```

```
        --policy-name comprehend-S3-access-policy ^
        --policy-document file://path/comprehend-S3-access-policy.json
```

Wobei gilt:

- *path/* ist der Dateipfad zu `comprehend-S3-access-policy.json` Ihrem lokalen Gerät.

c. Kopieren Sie den Amazon Resource Name (ARN) in Ihren Texteditor und speichern Sie ihn lokal unter`comprehend-S3-access-arn`.

> **Note**
>
> Der ARN hat ein ähnliches Format wie *arn:aws:iam: :123456789012:role/Comprehend-S3-Access-Policy*. Sie benötigen den ARN, unter dem Sie gespeichert haben`comprehend-S3-access-arn`, um ihn an `comprehend-S3-access-policy` Ihre IAM-Rolle anzuhängen.

d. Um das `comprehend-S3-access-policy` an Ihre IAM-Rolle anzuhängen, verwenden Sie den attach-role-policyfolgenden Befehl:

Linux

```
aws iam attach-role-policy \
        --policy-arn policy-arn \
        --role-name comprehend-role
```

Wobei gilt:

- *policy-arn* ist der ARN, unter dem Sie gespeichert haben. `comprehend-S3-access-arn`

macOS

```
aws iam attach-role-policy \
        --policy-arn policy-arn \
        --role-name comprehend-role
```

Wobei gilt:

- *policy-arn* ist der ARN, unter dem Sie gespeichert haben. comprehend-S3-access-arn

Windows

```
aws iam attach-role-policy ^
          --policy-arn policy-arn ^
          --role-name comprehend-role
```

Wobei gilt:

- *policy-arn* ist der ARN, unter dem Sie gespeichert haben. comprehend-S3-access-arn

3. Verwenden Sie den folgenden Befehl, um einen Amazon Comprehend Entities Analyse-Job auszuführen: start-entities-detection-job

Linux

```
aws comprehend start-entities-detection-job \
        --input-data-config S3Uri=s3://DOC-EXAMPLE-BUCKET/
data/,InputFormat=ONE_DOC_PER_FILE \
        --output-data-config S3Uri=s3://DOC-EXAMPLE-BUCKET/ \
        --data-access-role-arn role-arn \
        --job-name data-entities-analysis \
        --language-code en \
        --region aws-region
```

Wobei gilt:

- *DOC-EXAMPLE-BUCKET* ist der Name Ihres S3-Buckets,
- *role-arn* ist der ARN, unter dem Sie gespeichert haben, comprehend-role-arn
- *aws-region* ist Ihre AWS Region.

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
```

Wobei gilt:

- *DOC-EXAMPLE-BUCKET* ist der Name Ihres S3-Buckets,
- *role-arn* ist der ARN, unter dem Sie gespeichert haben, `comprehend-role-arn`
- *aws-region* ist Ihre AWS Region.

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
```

Wobei gilt:

- *DOC-EXAMPLE-BUCKET* ist der Name Ihres S3-Buckets,
- *role-arn* ist der ARN, unter dem Sie gespeichert haben, `comprehend-role-arn`
- *aws-region* ist Ihre AWS Region.

4. Kopieren Sie die `JobId` Entitätsanalyse und speichern Sie sie in einem Texteditor unter`comprehend-job-id`. Das `JobId` hilft Ihnen, den Status Ihres Entitätsanalyse-Jobs zu verfolgen.
5. Verwenden Sie den describe-entities-detection-jobfolgenden Befehl, um den Fortschritt Ihres Entitätsanalyse-Jobs zu verfolgen:

   Linux

```
aws comprehend describe-entities-detection-job \
        --job-id entities-job-id \
```

```
        --region aws-region
```

Wobei gilt:

- *entities-job-id*ist dein gerettetcomprehend-job-id,
- *aws-region* ist Ihre AWS Region.

macOS

```
aws comprehend describe-entities-detection-job \
        --job-id entities-job-id \
        --region aws-region
```

Wobei gilt:

- *entities-job-id*ist dein gerettetcomprehend-job-id,
- *aws-region* ist Ihre AWS Region.

Windows

```
aws comprehend describe-entities-detection-job ^
        --job-id entities-job-id ^
        --region aws-region
```

Wobei gilt:

- *entities-job-id*ist dein gerettetcomprehend-job-id,
- *aws-region* ist Ihre AWS Region.

Es kann mehrere Minuten dauern, `JobStatus` bis der Wechsel zu erfolgt`COMPLETED`.

Am Ende dieses Schritts speichert Amazon Comprehend die Ergebnisse der Entitätsanalyse als gezippte `output.tar.gz` Datei in einem `output` Ordner innerhalb eines automatisch generierten Ordners in Ihrem S3-Bucket. Vergewissern Sie sich, dass der Status Ihres Analyseauftrags abgeschlossen ist, bevor Sie mit dem nächsten Schritt fortfahren.

Schritt 3: Formatieren der Analyseausgabe der Entitäten als Amazon Kendra-Metadaten

Um die von Amazon Comprehend extrahierten Entitäten in das für einen Amazon Kendra-Index erforderliche Metadatenformat zu konvertieren, führen Sie ein Python-3-Skript aus. Die Ergebnisse der Konvertierung werden in dem `metadata` Ordner in Ihrem Amazon S3-Bucket gespeichert.

Weitere Informationen zum Format und zur Struktur von Amazon Kendra-Metadaten finden Sie unter Metadaten von S3-Dokumenten.

Themen

Herunterladen und Extrahieren der Amazon Comprehend-Ausgabe

Um die Ausgabe der Amazon Comprehend-Entitätsanalyse zu formatieren, müssen Sie zuerst das Amazon `output.tar.gz` Comprehend-Entitätsanalysearchiv herunterladen und die Entitätsanalysedatei extrahieren.

Um die Ausgabedatei herunterzuladen und zu extrahieren (Konsole)

1. Navigieren Sie im Navigationsbereich der Amazon Comprehend-Konsole zu Analysis Jobs.
2. Wählen Sie Ihren Job zur Entitätsanalyse`data-entities-analysis`.
3. Wählen Sie unter Ausgabe den Link aus, der neben dem Speicherort der Ausgabedaten angezeigt wird. Dadurch werden Sie zum `output.tar.gz` Archiv in Ihrem S3-Bucket weitergeleitet.
4. Wählen Sie auf der Registerkarte Übersicht die Option Herunterladen aus.

> **Tip**
>
> Die Ausgabe aller Amazon Comprehend-Analyseaufträge hat denselben Namen. Wenn Sie Ihr Archiv umbenennen, können Sie es leichter verfolgen.

5. Dekomprimieren und extrahieren Sie die heruntergeladene Amazon Comprehend-Datei auf Ihr Gerät.

Um die Ausgabedatei herunterzuladen und zu extrahieren (AWS CLI)

1. Verwenden Sie den folgenden Befehl, um auf den Namen des automatisch generierten Ordners von Amazon Comprehend in Ihrem S3-Bucket zuzugreifen, der die Ergebnisse des Entitätsanalyse-Jobs enthält: describe-entities-detection-job

   Linux

   ```
   aws comprehend describe-entities-detection-job \
             --job-id entities-job-id \
             --region aws-region
   ```

   Wobei gilt:

   - *entities-job-id*ist dein gerettet `comprehend-job-id` the section called “Schritt 2: Entitäten erkennen” vor
   - *aws-region* ist Ihre AWS Region.

   macOS

   ```
   aws comprehend describe-entities-detection-job \
             --job-id entities-job-id \
             --region aws-region
   ```

   Wobei gilt:

   - *entities-job-id*ist dein gerettet `comprehend-job-id` the section called “Schritt 2: Entitäten erkennen” vor
   - *aws-region* ist Ihre AWS Region.

   Windows

   ```
   aws comprehend describe-entities-detection-job ^
             --job-id entities-job-id ^
   ```

```
    --region aws-region
```

Wobei gilt:

- *entities-job-id*ist dein gerettet `comprehend-job-id` the section called “Schritt 2: Entitäten erkennen” vor
- *aws-region* ist Ihre AWS Region.

2. Kopieren Sie den `S3Uri` Wert aus dem `OutputDataConfig` Objekt in der Stellenbeschreibung Ihrer Entity und speichern Sie ihn wie `comprehend-S3uri` in einem Texteditor.

> **Note**
>
> Der `S3Uri` Wert hat ein ähnliches Format wie *s3://DOC-EXAMPLE-BUCKET /...* / output/output.tar.gz.

3. Verwenden Sie den Befehl copy, um das Ausgabearchiv der Entitäten herunterzuladen:

Linux

```
aws s3 cp s3://DOC-EXAMPLE-BUCKET/.../output/output.tar.gz path/output.tar.gz
```

Wobei gilt:

- *s3://DOC-BEISPIEL-BUCKET /...* /output/output.tar.gz ist der `S3Uri` Wert, unter dem Sie gespeichert habencomprehend-S3uri,
- *path/* ist das lokale Verzeichnis, in dem Sie die Ausgabe speichern möchten.

macOS

```
aws s3 cp s3://DOC-EXAMPLE-BUCKET/.../output/output.tar.gz path/output.tar.gz
```

Wobei gilt:

- *s3://DOC-BEISPIEL-BUCKET /...* /output/output.tar.gz ist der `S3Uri` Wert, unter dem Sie gespeichert habencomprehend-S3uri,
- *path/* ist das lokale Verzeichnis, in dem Sie die Ausgabe speichern möchten.

Windows

```
aws s3 cp s3://DOC-EXAMPLE-BUCKET/.../output/output.tar.gz path/output.tar.gz
```

Wobei gilt:

- *s3://DOC-BEISPIEL-BUCKET /...* /output/output.tar.gz ist der `S3Uri` Wert, unter dem Sie gespeichert habe`comprehend-S3uri`,
- *path/* ist das lokale Verzeichnis, in dem Sie die Ausgabe speichern möchten.

4. Um die Entitätsausgabe zu extrahieren, führen Sie den folgenden Befehl in einem Terminalfenster aus:

Linux

```
tar -xf path/output.tar.gz -C path/
```

Wobei gilt:

- *path/* ist der Dateipfad zum heruntergeladenen `output.tar.gz` Archiv auf Ihrem lokalen Gerät.

macOS

```
tar -xf path/output.tar.gz -C path/
```

Wobei gilt:

- *path/* ist der Dateipfad zum heruntergeladenen `output.tar.gz` Archiv auf Ihrem lokalen Gerät.

Windows

```
tar -xf path/output.tar.gz -C path/
```

Wobei gilt:

- *path/* ist der Dateipfad zum heruntergeladenen `output.tar.gz` Archiv auf Ihrem lokalen Gerät.

Am Ende dieses Schritts sollte auf Ihrem Gerät eine Datei `output` mit einer Liste der von Amazon Comprehend identifizierten Entitäten aufgerufen werden.

Upload der Ausgabe in den S3-Bucket

Nachdem Sie die Analysedatei für Amazon Comprehend Entities heruntergeladen und extrahiert haben, laden Sie die extrahierte `output` Datei in Ihren Amazon S3-Bucket hoch.

Um die extrahierte Amazon Comprehend-Ausgabedatei hochzuladen (Konsole)

1. Öffnen Sie die Amazon-S3-Konsole unter https://console.aws.amazon.com/s3/.
2. Klicken Sie in Buckets auf den Namen Ihres Buckets und wählen Sie dann Upload.
3. Wählen Sie unter Dateien und Ordner die Option Dateien hinzufügen aus.
4. Navigieren Sie im Dialogfeld zu Ihrer extrahierten `output` Datei auf Ihrem Gerät, wählen Sie sie aus und wählen Sie Öffnen.
5. Behalten Sie die Standardeinstellungen für Ziel, Berechtigungen und Eigenschaften bei.
6. Klicken Sie auf Upload.

Um die extrahierte Amazon Comprehend-Ausgabedatei hochzuladen () AWS CLI

1. Verwenden Sie den Befehl copy, um die extrahierte `output` Datei in Ihren Bucket hochzuladen:

   Linux

   ```
   aws s3 cp path/output s3://DOC-EXAMPLE-BUCKET/output
   ```

   Wobei gilt:

   - *path/* ist der lokale Dateipfad zu Ihrer entpackten Datei, `output`
   - *DOC-EXAMPLE-BUCKET* ist der Name Ihres S3-Buckets.

macOS

```
aws s3 cp path/output s3://DOC-EXAMPLE-BUCKET/output
```

Wobei gilt:

- *path/* ist der lokale Dateipfad zu Ihrer entpackten Datei, `output`
- *DOC-EXAMPLE-BUCKET* ist der Name Ihres S3-Buckets.

Windows

```
aws s3 cp path/output s3://DOC-EXAMPLE-BUCKET/output
```

Wobei gilt:

- *path/* ist der lokale Dateipfad zu Ihrer entpackten Datei, `output`
- *DOC-EXAMPLE-BUCKET* ist der Name Ihres S3-Buckets.

2. Um sicherzustellen, dass die `output` Datei erfolgreich in Ihren S3-Bucket hochgeladen wurde, überprüfen Sie ihren Inhalt mit dem Befehl list:

Linux

```
aws s3 ls s3://DOC-EXAMPLE-BUCKET/
```

Wobei gilt:

- *DOC-EXAMPLE-BUCKET* ist der Name Ihres S3-Buckets.

macOS

```
aws s3 ls s3://DOC-EXAMPLE-BUCKET/
```

Wobei gilt:

- *DOC-EXAMPLE-BUCKET* ist der Name Ihres S3-Buckets.

Windows

```
aws s3 ls s3://DOC-EXAMPLE-BUCKET/
```

Wobei gilt:

- *DOC-EXAMPLE-BUCKET* ist der Name Ihres S3-Buckets.

Konvertierung der Ausgabe in das Amazon Kendra-Metadatenformat

Um die Amazon Comprehend-Ausgabe in Amazon Kendra-Metadaten zu konvertieren, führen Sie ein Python-3-Skript aus. Wenn Sie die Konsole verwenden, verwenden Sie AWS CloudShell für diesen Schritt.

Um das Python-3-Skript auszuführen (Konsole)

1. Laden Sie die komprimierte Datei converter.py.zip auf Ihr Gerät herunter.
2. Extrahieren Sie die Python-3-Datei`converter.py`.
3. Melden Sie sich bei der AWSManagement Console an und stellen Sie sicher, dass Ihre AWS Region auf dieselbe Region eingestellt ist wie Ihr S3-Bucket und Ihr Amazon Comprehend-Analysejob.
4. Wählen Sie das AWS CloudShellSymbol oder geben Sie das Suchfeld AWSCloudShellin der oberen Navigationsleiste ein, um eine Umgebung zu starten.

   > **Note**
   >
   > Wenn AWS CloudShell zum ersten Mal in einem neuen Browser-Fenster gestartet wird, erscheint ein Begrüßungsfenster und listet die wichtigsten Funktionen auf. Die Shell ist bereit für die Interaktion, nachdem Sie dieses Fenster geschlossen haben und die Befehlszeile angezeigt wird.

5. Nachdem das Terminal vorbereitet ist, wählen Sie im Navigationsbereich Aktionen und dann im Menü die Option Datei hochladen.
6. Wählen Sie in dem sich öffnenden Dialogfeld Datei auswählen und wählen Sie dann die heruntergeladene Python 3-Datei `converter.py` von Ihrem Gerät aus. Klicken Sie auf Upload.
7. Geben Sie in der AWS CloudShell Umgebung den folgenden Befehl ein:

```
python3 converter.py
```

8. Wenn Sie von der Shell-Schnittstelle aufgefordert werden, den Namen Ihres S3-Buckets einzugeben, geben Sie den Namen Ihres S3-Buckets ein und drücken Sie die Eingabetaste.
9. Wenn Sie von der Shell-Oberfläche aufgefordert werden, den vollständigen Dateipfad zu Ihrer Comprehend-Ausgabedatei einzugeben, geben Sie die Eingabetaste ein und drücken Sie die Eingabetaste. **`output`**
10. Wenn Sie von der Shell-Oberfläche aufgefordert werden, den vollständigen Dateipfad zu Ihrem Metadatenordner einzugeben, geben Sie die Eingabetaste ein **`metadata/`** und drücken Sie die Eingabetaste.

> **Important**
>
> Damit die Metadaten korrekt formatiert werden, müssen die Eingabewerte in den Schritten 8 bis 10 exakt sein.

Um das Python-3-Skript auszuführen (AWS CLI)

1. Führen Sie den folgenden Befehl in einem Terminalfenster aus`converter.py`, um die Python-3-Datei herunterzuladen:

   Linux

   ```
   curl -o path/converter.py.zip https://docs.aws.amazon.com/kendra/latest/dg/
   samples/converter.py.zip
   ```

   Wobei gilt:

   - *`path/`* ist der Dateipfad zu dem Ort, an dem Sie die komprimierte Datei speichern möchten.

   macOS

   ```
   curl -o path/converter.py.zip https://docs.aws.amazon.com/kendra/latest/dg/
   samples/converter.py.zip
   ```

Wobei gilt:

- *path/* ist der Dateipfad zu dem Ort, an dem Sie die komprimierte Datei speichern möchten.

Windows

```
curl -o path/converter.py.zip https://docs.aws.amazon.com/kendra/latest/dg/
samples/converter.py.zip
```

Wobei gilt:

- *path/* ist der Dateipfad zu dem Ort, an dem Sie die komprimierte Datei speichern möchten.

2. Um die Python-3-Datei zu extrahieren, führen Sie den folgenden Befehl im Terminalfenster aus:

Linux

```
unzip path/converter.py.zip -d path/
```

Wobei gilt:

- *path/* ist der Dateipfad zu Ihrem gespeicherten. `converter.py.zip`

macOS

```
unzip path/converter.py.zip -d path/
```

Wobei gilt:

- *path/* ist der Dateipfad zu Ihrem gespeicherten. `converter.py.zip`

Windows

```
tar -xf path/converter.py.zip -C path/
```

Wobei gilt:

- *path/* ist der Dateipfad zu Ihrem gespeicherten. `converter.py.zip`

3. Stellen Sie sicher, dass Boto3 auf Ihrem Gerät installiert ist, indem Sie den folgenden Befehl ausführen.

   Linux

   ```
   pip3 show boto3
   ```

   macOS

   ```
   pip3 show boto3
   ```

   Windows

   ```
   pip3 show boto3
   ```

   > **Note**
   >
   > Wenn Sie Boto3 nicht installiert haben, starten Sie es, `pip3 install boto3` um es zu installieren.

4. Führen Sie den folgenden Befehl aus, um das Python-3-Skript zur Konvertierung der `output` Datei auszuführen.

   Linux

   ```
   python path/converter.py
   ```

   Wobei gilt:

   - *path/* ist der Dateipfad zu Ihrem gespeicherten. `converter.py.zip`

   macOS

   ```
   python path/converter.py
   ```

Wobei gilt:

- *path/* ist der Dateipfad zu Ihrem gespeicherten. `converter.py.zip`

Windows

```
python path/converter.py
```

Wobei gilt:

- *path/* ist der Dateipfad zu Ihrem gespeicherten. `converter.py.zip`

5. Wenn Sie AWS CLI dazu aufgefordert werden`Enter the name of your S3 bucket`, geben Sie den Namen Ihres S3-Buckets ein und drücken Sie die Eingabetaste.
6. Wenn Sie AWS CLI dazu aufgefordert werden`Enter the full filepath to your Comprehend output file`, geben Sie die Eingabetaste ein **`output`** und drücken Sie die Eingabetaste.
7. Wenn Sie AWS CLI dazu aufgefordert werden`Enter the full filepath to your metadata folder`, geben Sie die Eingabetaste ein **`metadata/`** und drücken Sie die Eingabetaste.

> **Important**
>
> Damit die Metadaten korrekt formatiert werden, müssen die Eingabewerte in den Schritten 5 bis 7 exakt sein.

Am Ende dieses Schritts werden die formatierten Metadaten in dem `metadata` Ordner in Ihrem S3-Bucket abgelegt.

Ihren Amazon S3-Bucket aufräumen

Da der Amazon Kendra-Index alle in einem Bucket gespeicherten Dateien synchronisiert, empfehlen wir Ihnen, Ihren Amazon S3-Bucket zu bereinigen, um redundante Suchergebnisse zu vermeiden.

So bereinigen Sie Ihren Amazon S3-Bucket (Konsole)

1. Öffnen Sie die Amazon-S3-Konsole unter https://console.aws.amazon.com/s3/.

2. Wählen Sie unter Buckets Ihren Bucket und dann den Ausgabeordner für die Amazon Comprehend-Entitätsanalyse, die Amazon `.temp` Comprehend-Entitätsanalysedatei und die extrahierte Amazon Comprehend-Datei aus. `output`
3. Wählen Sie auf der Registerkarte Übersicht die Option Löschen aus.
4. Wählen Sie unter Objekte löschen die Option Objekte dauerhaft löschen? und geben Sie **`permanently delete`** in das Texteingabefeld ein.
5. Wählen Sie Delete objects (Objekte löschen).

So bereinigen Sie Ihren Amazon S3-Bucket (AWS CLI)

1. Um alle Dateien und Ordner in Ihrem S3-Bucket außer den `metadata` Ordnern `data` und zu löschen, verwenden Sie den Befehl remove in derAWS CLI:

   Linux

   ```
   aws s3 rm s3://DOC-EXAMPLE-BUCKET/ --recursive --exclude "data/*" --exclude
    "metadata/*"
   ```

   Wobei gilt:

   - *DOC-EXAMPLE-BUCKET* ist der Name Ihres S3-Buckets.

   macOS

   ```
   aws s3 rm s3://DOC-EXAMPLE-BUCKET/ --recursive --exclude "data/*" --exclude
    "metadata/*"
   ```

   Wobei gilt:

   - *DOC-EXAMPLE-BUCKET* ist der Name Ihres S3-Buckets.

   Windows

   ```
   aws s3 rm s3://DOC-EXAMPLE-BUCKET/ --recursive --exclude "data/*" --exclude
    "metadata/*"
   ```

   Wobei gilt:

- *DOC-EXAMPLE-BUCKET* ist der Name Ihres S3-Buckets.

2. Um sicherzustellen, dass die Objekte erfolgreich aus Ihrem S3-Bucket gelöscht wurden, überprüfen Sie den Inhalt mit dem Befehl list:

   Linux

   ```
   aws s3 ls s3://DOC-EXAMPLE-BUCKET/
   ```

   Wobei gilt:

   - *DOC-EXAMPLE-BUCKET* ist der Name Ihres S3-Buckets.

   macOS

   ```
   aws s3 ls s3://DOC-EXAMPLE-BUCKET/
   ```

   Wobei gilt:

   - *DOC-EXAMPLE-BUCKET* ist der Name Ihres S3-Buckets.

   Windows

   ```
   aws s3 ls s3://DOC-EXAMPLE-BUCKET/
   ```

   Wobei gilt:

   - *DOC-EXAMPLE-BUCKET* ist der Name Ihres S3-Buckets.

Am Ende dieses Schritts haben Sie die Analyseausgabe der Amazon Comprehend-Entitäten in Amazon Kendra-Metadaten konvertiert. Sie sind jetzt bereit, einen Amazon Kendra-Index zu erstellen.

Schritt 4: Erstellen eines Amazon Kendra-Index und Erfassung der Metadaten

Um Ihre intelligente Suchlösung zu implementieren, erstellen Sie einen Amazon Kendra-Index und nehmen Ihre S3-Daten und Metadaten in diesen Index auf.

Bevor Sie Ihrem Amazon Kendra-Index Metadaten hinzufügen, erstellen Sie benutzerdefinierte Indexfelder, die benutzerdefinierten Dokumentattributen entsprechen, die wiederum den Amazon Comprehend-Entitätstypen entsprechen. Amazon Kendra verwendet die Indexfelder und benutzerdefinierten Dokumentattribute, die Sie erstellen, um Ihre Dokumente zu suchen und zu filtern.

Weitere Informationen finden Sie unter Index und Erstellen benutzerdefinierter Dokumentattribute.

Themen

Einen Amazon Kendra-Index erstellen

Um Ihre Quelldokumente abzufragen, erstellen Sie einen Amazon Kendra-Index.

Wenn Sie AWS CLI in diesem Schritt die verwenden, erstellen Sie eine AWS IAM-Rolle und -Richtlinie, die Amazon Kendra den Zugriff auf Ihre CloudWatch Protokolle ermöglichen, und hängen sie an, bevor Sie einen Index erstellen. Weitere Informationen finden Sie unter Voraussetzungen.

So erstellen Sie einen Amazon Kendra-Index (Konsole)

1. Öffnen Sie die Amazon Kendra-Konsole unter https://console.aws.amazon.com/kendra/.

> **Important**
>
> Stellen Sie sicher, dass Sie sich in derselben Region befinden, in der Sie Ihren Amazon Comprehend Entities Analyse-Job und Ihren Amazon S3-Bucket erstellt haben. Wenn Sie sich in einer anderen Region befinden, wählen Sie in der AWS Regionsauswahl in

der oberen Navigationsleiste die Region aus, in der Sie Ihren Amazon S3-Bucket erstellt haben.

2. Wählen Sie Index erstellen aus.
3. Gehen Sie wie folgt vor, um Indexdetails auf der Seite „Indexdetails angeben“ zu erhalten:
   a. Geben Sie für Indexname **`kendra-index`** ein.
   b. Lassen Sie das Feld Beschreibung leer.
   c. Wählen Sie für IAM Role (IAM-Rolle) die Option Create a New Role (Neue Rolle erstellen) aus. Diese Rolle bietet Zugriff auf Ihren Amazon S3-Bucket.
   d. Geben Sie für Rollenname den Namen **`kendra-role`** ein. Die IAM-Rolle wird das Präfix `AmazonKendra-` haben.
   e. Behalten Sie die Standardeinstellungen für Verschlüsselung und Tags bei und wählen Sie Weiter.
4. Wählen Sie für die Zugriffskontrolleinstellungen auf der Seite Benutzerzugriffskontrolle konfigurieren die Option Nein und dann Weiter.
5. Wählen Sie für Provisioning-Editionen auf der Seite mit den Bereitstellungsdetails die Option Developer Edition und dann Create aus.

Um einen Amazon Kendra-Index zu erstellen () AWS CLI

1. Gehen Sie wie folgt vor, um eine IAM-Rolle für Amazon Kendra zu erstellen und anzuhängen, die Amazon Kendra als vertrauenswürdige Entität anerkennt:
   a. Speichern Sie die folgende Vertrauensrichtlinie als JSON-Datei, die `kendra-trust-policy.json` in einem Texteditor auf Ihrem lokalen Gerät aufgerufen wird.

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

b. Verwenden Sie den Befehl create-role, um eine IAM-Rolle mit dem Namen zu erstellen `kendra-role` und Ihre gespeicherte `kendra-trust-policy.json` Datei daran anzuhängen:

Linux

```
aws iam create-role \
          --role-name kendra-role \
          --assume-role-policy-document file://path/kendra-trust-policy.json
```

Wobei gilt:

- *path/* ist der Dateipfad zu `kendra-trust-policy.json` Ihrem lokalen Gerät.

macOS

```
aws iam create-role \
          --role-name kendra-role \
          --assume-role-policy-document file://path/kendra-trust-policy.json
```

Wobei gilt:

- *path/* ist der Dateipfad zu `kendra-trust-policy.json` Ihrem lokalen Gerät.

Windows

```
aws iam create-role ^
          --role-name kendra-role ^
          --assume-role-policy-document file://path/kendra-trust-policy.json
```

Wobei gilt:

- *path/* ist der Dateipfad zu `kendra-trust-policy.json` Ihrem lokalen Gerät.

c. Kopieren Sie den Amazon Resource Name (ARN) in Ihren Texteditor und speichern Sie ihn lokal unter`kendra-role-arn`.

> **Note**
>
> Der ARN hat ein ähnliches Format wie *arn:aws:iam: :123456789012:role/kendra-role*. Sie benötigen den ARN, unter dem Sie gespeichert haben`kendra-role-arn`, um Amazon Kendra-Jobs auszuführen.

2. Bevor Sie einen Index erstellen, müssen Sie Ihre Erlaubnis `kendra-role` zum Schreiben in CloudWatch Logs erteilen. Führen Sie dazu die folgenden Schritte aus:

   a. Speichern Sie die folgende Vertrauensrichtlinie als JSON-Datei, die `kendra-cloudwatch-policy.json` in einem Texteditor auf Ihrem lokalen Gerät aufgerufen wird.

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

Ersetzen Sie *aws-region* durch Ihre AWS Region und *aws-account-id*durch Ihre 12-stellige AWS Konto-ID.

b. Verwenden Sie den Befehl create-policy, um eine IAM-Richtlinie für den Zugriff auf CloudWatch Protokolle zu erstellen:

Linux

```
aws iam create-policy \
          --policy-name kendra-cloudwatch-policy \
          --policy-document file://path/kendra-cloudwatch-policy.json
```

Wobei gilt:

- *path/* ist der Dateipfad zu `kendra-cloudwatch-policy.json` Ihrem lokalen Gerät.

macOS

```
aws iam create-policy \
          --policy-name kendra-cloudwatch-policy \
          --policy-document file://path/kendra-cloudwatch-policy.json
```

Wobei gilt:

- *path/* ist der Dateipfad zu `kendra-cloudwatch-policy.json` Ihrem lokalen Gerät.

Windows

```
aws iam create-policy ^
          --policy-name kendra-cloudwatch-policy ^
```

```
        --policy-document file://path/kendra-cloudwatch-policy.json
```

Wobei gilt:

- *path/* ist der Dateipfad zu `kendra-cloudwatch-policy.json` Ihrem lokalen Gerät.

c. Kopieren Sie den Amazon Resource Name (ARN) in Ihren Texteditor und speichern Sie ihn lokal unter`kendra-cloudwatch-arn`.

> **Note**
>
> Der ARN hat ein ähnliches Format wie *arn:aws:iam: :123456789012:role/*. kendra-cloudwatch-policy Sie benötigen den ARN, unter dem Sie gespeichert haben`kendra-cloudwatch-arn`, um ihn an `kendra-cloudwatch-policy` Ihre IAM-Rolle anzuhängen.

d. Um das `kendra-cloudwatch-policy` an Ihre IAM-Rolle anzuhängen, verwenden Sie den attach-role-policyfolgenden Befehl:

Linux

```
aws iam attach-role-policy \
        --policy-arn policy-arn \
        --role-name kendra-role
```

Wobei gilt:

- *policy-arn* ist deine Rettung. `kendra-cloudwatch-arn`

macOS

```
aws iam attach-role-policy \
        --policy-arn policy-arn \
        --role-name kendra-role
```

Wobei gilt:

- *policy-arn* ist deine Rettung. `kendra-cloudwatch-arn`

Windows

```
aws iam attach-role-policy ^
          --policy-arn policy-arn ^
          --role-name kendra-role
```

Wobei gilt:

- *policy-arn* ist deine Rettung. `kendra-cloudwatch-arn`

3. Verwenden Sie den Befehl create-index, um einen Index zu erstellen:

Linux

```
aws kendra create-index \
        --name kendra-index \
        --edition DEVELOPER_EDITION \
        --role-arn role-arn \
        --region aws-region
```

Wobei gilt:

- *role-arn* ist dein Geretteter, `kendra-role-arn`
- *aws-region* ist Ihre AWS Region.

macOS

```
aws kendra create-index \
        --name kendra-index \
        --edition DEVELOPER_EDITION \
        --role-arn role-arn \
        --region aws-region
```

Wobei gilt:

- *role-arn* ist dein Geretteter, `kendra-role-arn`
- *aws-region* ist Ihre AWS Region.

Windows

```
aws kendra create-index ^
        --name kendra-index ^
        --edition DEVELOPER_EDITION ^
        --role-arn role-arn ^
        --region aws-region
```

Wobei gilt:

- *role-arn* ist dein Geretteter, `kendra-role-arn`
- *aws-region* ist Ihre AWS Region.

4. Kopieren Sie den Index `Id` und speichern Sie ihn in einem Texteditor unter`kendra-index-id`. Das `Id` hilft Ihnen, den Status Ihrer Indexerstellung zu verfolgen.
5. Um den Fortschritt Ihres Auftrags zur Indexerstellung zu verfolgen, verwenden Sie den Befehl describe-index:

Linux

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

Wobei gilt:

- *kendra-index-id*ist dein gerettet`kendra-index-id`,
- *aws-region* ist Ihre AWS Region.

macOS

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

Wobei gilt:

- *kendra-index-id*ist dein gerettet`kendra-index-id`,

- *aws-region* ist Ihre AWS Region.

Windows

```
aws kendra describe-index ^
        --id kendra-index-id ^
        --region aws-region
```

Wobei gilt:

- *kendra-index-id*ist dein gerettetkendra-index-id,
- *aws-region* ist Ihre AWS Region.

Die Indexerstellung dauert im Durchschnitt 15 Minuten, kann aber auch länger dauern. Wenn der Status des Index aktiv ist, ist Ihr Index einsatzbereit. Während Ihr Index erstellt wird, können Sie mit dem nächsten Schritt beginnen.

Wenn Sie AWS CLI in diesem Schritt die verwenden, erstellen Sie eine IAM-Richtlinie und hängen sie an Ihre Amazon Kendra IAM-Rolle an, die Ihren Indexberechtigungen für den Zugriff auf Ihren S3-Bucket erteilt.

Aktualisierung der IAM-Rolle für den Amazon S3-Zugriff

Während der Indexerstellung aktualisieren Sie Ihre Amazon Kendra IAM-Rolle, damit der von Ihnen erstellte Index Daten aus Ihrem Amazon S3-Bucket lesen kann. Weitere Informationen finden Sie unter IAM-Zugriffsrollen für Amazon Kendra.

So aktualisieren Sie Ihre IAM-Rolle (Konsole)

1. Öffnen Sie die IAM-Konsole unter https://console.aws.amazon.com/iam/.
2. Wählen Sie im linken Navigationsbereich Rollen aus und geben Sie **kendra-role** in das Suchfeld über dem Rollennamen ein.
3. Klicken Sie in den vorgeschlagenen Optionen aufkendra-role.
4. Wählen Sie unter Zusammenfassung die Option Richtlinien anhängen aus.
5. Geben Sie unter Berechtigungen anhängen im Suchfeld das Kontrollkästchen neben der ReadOnlyAccessAmazonS3-Richtlinie ein **S3** und wählen Sie es aus den vorgeschlagenen Optionen aus.

6. Wählen Sie Attach policy (Richtlinie anfügen) aus. Auf der Übersichtsseite sehen Sie nun zwei Richtlinien, die der IAM-Rolle zugeordnet sind.
7. Kehren Sie zur Amazon Kendra-Konsole unter https://console.aws.amazon.com/kendra/ zurück und warten Sie, bis sich der Status Ihres Index von Creating zu Active ändert, bevor Sie mit dem nächsten Schritt fortfahren.

Um Ihre IAM-Rolle zu aktualisieren () AWS CLI

1. Speichern Sie den folgenden Text in einer JSON-Datei, die `kendra-S3-access-policy.json` in einem Texteditor auf Ihrem lokalen Gerät aufgerufen wird.

```
{
   "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"
```

```
            ]
        }
    ]
}
```

Ersetzen Sie *DOC-EXAMPLE-BUCKET* durch Ihren S3-Bucket-Namen, *aws-Region durch Ihre AWS Region*, durch Ihre 12-stellige AWS Konto-ID und *aws-account-id*durch Ihre gespeicherten. *kendra-index-id*kendra-index-id

2. Verwenden Sie den Befehl create-policy, um eine IAM-Richtlinie für den Zugriff auf Ihren S3-Bucket zu erstellen:

   Linux

   ```
   aws iam create-policy \
            --policy-name kendra-S3-access-policy \
            --policy-document file://path/kendra-S3-access-policy.json
   ```

   Wobei gilt:

   - *path/* ist der Dateipfad zu kendra-S3-access-policy.json Ihrem lokalen Gerät.

   macOS

   ```
   aws iam create-policy \
            --policy-name kendra-S3-access-policy \
            --policy-document file://path/kendra-S3-access-policy.json
   ```

   Wobei gilt:

   - *path/* ist der Dateipfad zu kendra-S3-access-policy.json Ihrem lokalen Gerät.

   Windows

   ```
   aws iam create-policy ^
            --policy-name kendra-S3-access-policy ^
            --policy-document file://path/kendra-S3-access-policy.json
   ```

   Wobei gilt:

- *path/* ist der Dateipfad zu `kendra-S3-access-policy.json` Ihrem lokalen Gerät.

3. Kopieren Sie den Amazon Resource Name (ARN) in Ihren Texteditor und speichern Sie ihn lokal unter`kendra-S3-access-arn`.

> **Note**
>
> Der ARN hat ein ähnliches Format wie *arn:aws:iam: :123456789012:role/kendra-s3-Access-Policy*. Sie benötigen den ARN, unter dem Sie gespeichert haben`kendra-S3-access-arn`, um ihn an `kendra-S3-access-policy` Ihre IAM-Rolle anzuhängen.

4. `kendra-S3-access-policy`Um die an Ihre Amazon Kendra IAM-Rolle anzuhängen, verwenden Sie den attach-role-policyfolgenden Befehl:

Linux

```
aws iam attach-role-policy \
          --policy-arn policy-arn \
          --role-name kendra-role
```

Wobei gilt:

- *policy-arn* ist deine Rettung. `kendra-S3-access-arn`

macOS

```
aws iam attach-role-policy \
          --policy-arn policy-arn \
          --role-name kendra-role
```

Wobei gilt:

- *policy-arn* ist deine Rettung. `kendra-S3-access-arn`

Windows

```
aws iam attach-role-policy ^
```

```
        --policy-arn policy-arn ^
        --role-name kendra-role
```

Wobei gilt:

- *policy-arn* ist deine Rettung. `kendra-S3-access-arn`

Erstellen benutzerdefinierter Suchindexfelder für Amazon Kendra

Um Amazon Kendra darauf vorzubereiten, Ihre Metadaten als benutzerdefinierte Dokumentattribute zu erkennen, erstellen Sie benutzerdefinierte Felder, die den Amazon Comprehend-Entitätstypen entsprechen. Sie geben die folgenden neun Amazon Comprehend-Entitätstypen als benutzerdefinierte Felder ein:

- GEWERBLICHES_ARTIKEL
- DATUM
- EREIGNIS
- LOCATION
- ORGANISATION
- OTHER
- PERSON
- MENGE
- TITLE

> **Important**
>
> Falsch geschriebene Entitätstypen werden vom Index nicht erkannt.

So erstellen Sie benutzerdefinierte Felder für Ihren Amazon Kendra-Index (Konsole)

1. Öffnen Sie die Amazon Kendra-Konsole unter https://console.aws.amazon.com/kendra/.
2. Klicken Sie in der Liste der Indizes auf. `kendra-index`
3. Wählen Sie im linken Navigationsbereich unter Datenverwaltung die Option Facettendefinition aus.

4. Wählen Sie im Menü Indexfelder die Option Feld hinzufügen aus.
5. Gehen Sie im Dialogfeld Indexfeld hinzufügen wie folgt vor:
   a. Geben Sie im Feld Feldname den Wert ein**`COMMERCIAL_ITEM`**.
   b. Wählen Sie unter Datentyp die Option Zeichenfolgenliste aus.
   c. Wählen Sie unter Verwendungstypen die Optionen Facetable, Durchsuchbar und Anzeigebar aus und wählen Sie dann Hinzufügen aus.
   d. Wiederholen Sie die Schritte a bis c für jeden Amazon Comprehend-Entitätstyp: COMMERCIAL_ITEM, DATE, EVENT, LOCATION, ORGANIZATION, OTHER, PERSON, QUANTITY, TITLE.

Die Konsole zeigt Meldungen über das erfolgreiche Hinzufügen von Feldern an. Sie können sie schließen, bevor Sie mit dem nächsten Schritt fortfahren.

So erstellen Sie benutzerdefinierte Felder für Ihren Amazon Kendra-Index () AWS CLI

1. Speichern Sie den folgenden Text als JSON-Datei, die `custom-attributes.json` in einem Texteditor auf Ihrem lokalen Gerät aufgerufen wird.

```
[
   {
       "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. Verwenden Sie den Befehl update-index, um benutzerdefinierte Felder in Ihrem Index zu erstellen:

   Linux

   ```
   aws kendra update-index \
           --id kendra-index-id \
           --document-metadata-configuration-updates file://path/custom-
   attributes.json \
           --region aws-region
   ```

   Wobei gilt:

   - *kendra-index-id*ist dein gerettetkendra-index-id,
   - *path/* ist der Dateipfad zu custom-attributes.json auf Ihrem lokalen Gerät,
   - *aws-region* ist Ihre AWS Region.

   macOS

   ```
   aws kendra update-index \
           --id kendra-index-id \
   ```

```
        --document-metadata-configuration-updates file://path/custom-
attributes.json \
        --region aws-region
```

Wobei gilt:

- *kendra-index-id*ist dein gerettetkendra-index-id,
- *path/* ist der Dateipfad zu custom-attributes.json auf Ihrem lokalen Gerät,
- *aws-region* ist Ihre AWS Region.

Windows

```
aws kendra update-index ^
        --id kendra-index-id ^
        --document-metadata-configuration-updates file://path/custom-
attributes.json ^
        --region aws-region
```

Wobei gilt:

- *kendra-index-id*ist dein gerettetkendra-index-id,
- *path/* ist der Dateipfad zu custom-attributes.json auf Ihrem lokalen Gerät,
- *aws-region* ist Ihre AWS Region.

3. Um zu überprüfen, ob die benutzerdefinierten Attribute zu Ihrem Index hinzugefügt wurden, verwenden Sie den Befehl describe-index:

   Linux

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

   Wobei gilt:

   - *kendra-index-id*ist dein gerettetkendra-index-id,
   - *aws-region* ist Ihre AWS Region.

macOS

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

Wobei gilt:

- *kendra-index-id*ist dein gerettetkendra-index-id,
- *aws-region* ist Ihre AWS Region.

Windows

```
aws kendra describe-index ^
        --id kendra-index-id ^
        --region aws-region
```

Wobei gilt:

- *kendra-index-id*ist dein gerettetkendra-index-id,
- *aws-region* ist Ihre AWS Region.

Hinzufügen des Amazon S3-Buckets als Datenquelle für den Index

Bevor Sie Ihren Index synchronisieren können, müssen Sie Ihre S3-Datenquelle damit verbinden.

So verbinden Sie einen S3-Bucket mit Ihrem Amazon Kendra-Index (Konsole)

1. Öffnen Sie die Amazon Kendra-Konsole unter https://console.aws.amazon.com/kendra/.
2. Klicken Sie in der Liste der Indizes auf. kendra-index
3. Wählen Sie im linken Navigationsmenü unter Datenverwaltung die Option Datenquellen aus.
4. Navigieren Sie im Abschnitt Datenquellen-Connectortyp auswählen zu Amazon S3 und wählen Sie Connector hinzufügen aus.
5. Gehen Sie auf der Seite „Datenquellendetails angeben“ wie folgt vor:

a. Geben Sie unter Name und Beschreibung den Wert Datenquellenname ein**`S3-data-source`**.

b. Lassen Sie den Abschnitt Beschreibung leer.

c. Behalten Sie die Standardeinstellungen für Tags bei.

d. Wählen Sie Weiter.

6. Gehen Sie auf der Seite Synchronisierungseinstellungen konfigurieren im Abschnitt Synchronisierungsbereich wie folgt vor:

a. Wählen Sie unter Geben Sie den Speicherort der Datenquelle ein die Option S3 durchsuchen aus.

b. Wählen Sie unter Ressourcen auswählen Ihren S3-Bucket aus und klicken Sie dann auf Auswählen.

c. Wählen Sie unter Speicherort des Präfixordners für Metadatendateien die Option S3 durchsuchen aus.

d. Klicken Sie unter Ressourcen auswählen in der Liste der Buckets auf den Namen Ihres Buckets.

e. Wählen Sie für Objekte das Optionsfeld für `metadata` und wählen Sie Auswählen. Das Standortfeld sollte jetzt lauten`metadata/`.

f. Behalten Sie die Standardeinstellungen für Speicherort der Zugriffskontrollliste, Entschlüsselungsschlüssel auswählen und Zusätzliche Konfiguration bei.

7. Wählen Sie für die IAM-Rolle auf der Seite „Synchronisierungseinstellungen konfigurieren“ die Option`kendra-role`.

8. Wählen Sie auf der Seite „Synchronisierungseinstellungen konfigurieren“ unter „Ausführungsplan synchronisieren“ für Frequenz die Option „Bei Bedarf ausführen“ und dann „Weiter“.

9. Überprüfen Sie auf der Seite Überprüfen und erstellen Ihre Auswahl für die Datenquellendetails und wählen Sie Datenquelle hinzufügen aus.

So verbinden Sie einen S3-Bucket mit Ihrem Amazon Kendra-Index () AWS CLI

1. Speichern Sie den folgenden Text als JSON-Datei, die `S3-data-connector.json` in einem Texteditor auf Ihrem lokalen Gerät aufgerufen wird.

```
{
   "S3Configuration":{
```

```
      "BucketName":"DOC-EXAMPLE-BUCKET",
      "DocumentsMetadataConfiguration":{
         "S3Prefix":"metadata"
      }
   }
}
```

Ersetzen Sie *DOC-EXAMPLE-BUCKET* durch den Namen Ihres S3-Buckets.

2. Verwenden Sie den create-data-sourceBefehl, um Ihren S3-Bucket mit Ihrem Index zu verbinden:

   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
   ```

   Wobei gilt:

   - *kendra-index-id*ist dein gerettetkendra-index-id,
   - *path/* ist der Dateipfad zu S3-data-connector.json auf Ihrem lokalen Gerät,
   - *role-arn* ist dein Geretteter, kendra-role-arn
   - *aws-region* ist Ihre AWS Region.

   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
   ```

   Wobei gilt:

- *kendra-index-id*ist dein gerettetkendra-index-id,
- *path/* ist der Dateipfad zu S3-data-connector.json auf Ihrem lokalen Gerät,
- *role-arn* ist dein Geretteter, kendra-role-arn
- *aws-region* ist Ihre AWS Region.

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
```

Wobei gilt:

- *kendra-index-id*ist dein gerettetkendra-index-id,
- *path/* ist der Dateipfad zu S3-data-connector.json auf Ihrem lokalen Gerät,
- *role-arn* ist dein Geretteter, kendra-role-arn
- *aws-region* ist Ihre AWS Region.

3. Kopieren Sie den Connector Id und speichern Sie ihn in einem Texteditor unterS3-connector-id. Das Id hilft Ihnen, den Status des Datenverbindungsprozesses zu verfolgen.
4. Um sicherzustellen, dass Ihre S3-Datenquelle erfolgreich verbunden wurde, verwenden Sie den describe-data-sourcefolgenden Befehl:

   Linux

   ```
   aws kendra describe-data-source \
           --id S3-connector-id \
           --index-id kendra-index-id \
           --region aws-region
   ```

   Wobei gilt:

   - *s3-Connector-ID ist deine gespeichert*, S3-connector-id

- *kendra-index-id*ist dein gerettetkendra-index-id,
- *aws-region* ist Ihre AWS Region.

macOS

```
aws kendra describe-data-source \
        --id S3-connector-id \
        --index-id kendra-index-id \
        --region aws-region
```

Wobei gilt:

- *s3-Connector-ID ist deine gespeichert*, S3-connector-id
- *kendra-index-id*ist dein gerettetkendra-index-id,
- *aws-region* ist Ihre AWS Region.

Windows

```
aws kendra describe-data-source ^
        --id S3-connector-id ^
        --index-id kendra-index-id ^
        --region aws-region
```

Wobei gilt:

- *s3-Connector-ID ist deine gespeichert*, S3-connector-id
- *kendra-index-id*ist dein gerettetkendra-index-id,
- *aws-region* ist Ihre AWS Region.

Am Ende dieses Schritts ist Ihre Amazon S3-Datenquelle mit dem Index verbunden.

Synchronisieren des Amazon Kendra-Index

Nachdem die Amazon S3-Datenquelle hinzugefügt wurde, synchronisieren Sie jetzt Ihren Amazon Kendra-Index damit.

So synchronisieren Sie Ihren Amazon Kendra-Index (Konsole)

1. Öffnen Sie die Amazon Kendra-Konsole unter https://console.aws.amazon.com/kendra/.
2. Klicken Sie in der Liste der Indizes auf. `kendra-index`
3. Wählen Sie im linken Navigationsmenü Datenquellen aus.
4. Wählen Sie unter Datenquellen die Option aus`S3-data-source`.
5. Wählen Sie in der oberen Navigationsleiste die Option Jetzt synchronisieren aus.

So synchronisieren Sie Ihren Amazon Kendra-Index () AWS CLI

1. Verwenden Sie den Befehl start-data-source-sync-job, um Ihren Index zu synchronisieren:

   Linux

   ```
   aws kendra start-data-source-sync-job \
           --id S3-connector-id \
           --index-id kendra-index-id \
           --region aws-region
   ```

   Wobei gilt:

   - *s3-Connector-ID ist deine gespeichert*, `S3-connector-id`
   - *kendra-index-id*ist dein gerettet`kendra-index-id`,
   - *aws-region* ist Ihre AWS Region.

   macOS

   ```
   aws kendra start-data-source-sync-job \
           --id S3-connector-id \
           --index-id kendra-index-id \
           --region aws-region
   ```

   Wobei gilt:

   - *s3-Connector-ID ist deine gespeichert*, `S3-connector-id`
   - *kendra-index-id*ist dein gerettet`kendra-index-id`,
   - *aws-region* ist Ihre AWS Region.

Windows

```
aws kendra start-data-source-sync-job ^
        --id S3-connector-id ^
        --index-id kendra-index-id ^
        --region aws-region
```

Wobei gilt:

- *s3-Connector-ID ist deine gespeichert*, S3-connector-id
- *kendra-index-id*ist dein gerettetkendra-index-id,
- *aws-region* ist Ihre AWS Region.

2. Um den Status der Indexsynchronisierung zu überprüfen, verwenden Sie den Befehl 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
```

Wobei gilt:

- *s3-Connector-ID ist deine gespeichert*, S3-connector-id
- *kendra-index-id*ist dein gerettetkendra-index-id,
- *aws-region* ist Ihre AWS Region.

macOS

```
aws kendra list-data-source-sync-jobs \
        --id S3-connector-id \
        --index-id kendra-index-id \
        --region aws-region
```

Wobei gilt:

- *s3-Connector-ID ist deine gespeichert*, S3-connector-id
- *kendra-index-id*ist dein gerettetkendra-index-id,
- *aws-region* ist Ihre AWS Region.

Windows

```
aws kendra list-data-source-sync-jobs ^
        --id S3-connector-id ^
        --index-id kendra-index-id ^
        --region aws-region
```

Wobei gilt:

- *s3-Connector-ID ist deine gespeichert*, S3-connector-id
- *kendra-index-id*ist dein gerettetkendra-index-id,
- *aws-region* ist Ihre AWS Region.

Am Ende dieses Schritts haben Sie einen durchsuchbaren und filterbaren Amazon Kendra-Index für Ihren Datensatz erstellt.

Schritt 5: Abfragen des Amazon Kendra-Index

Ihr Amazon Kendra-Index ist jetzt bereit für Abfragen in natürlicher Sprache. Wenn Sie Ihren Index durchsuchen, verwendet Amazon Kendra alle von Ihnen bereitgestellten Daten und Metadaten, um die genauesten Antworten auf Ihre Suchanfrage zurückzugeben.

Es gibt drei Arten von Anfragen, die Amazon Kendra beantworten kann:

- Faktoid-Abfragen („wer“, „was“, „wann“ oder „wo“ -Fragen)
- Beschreibende Abfragen („Wie“ -Fragen)
- Stichwortsuche (Fragen, deren Absicht und Umfang nicht klar sind)

Themen

- Ihren Amazon Kendra-Index abfragen
- Filtern Ihrer Suchergebnisse

Ihren Amazon Kendra-Index abfragen

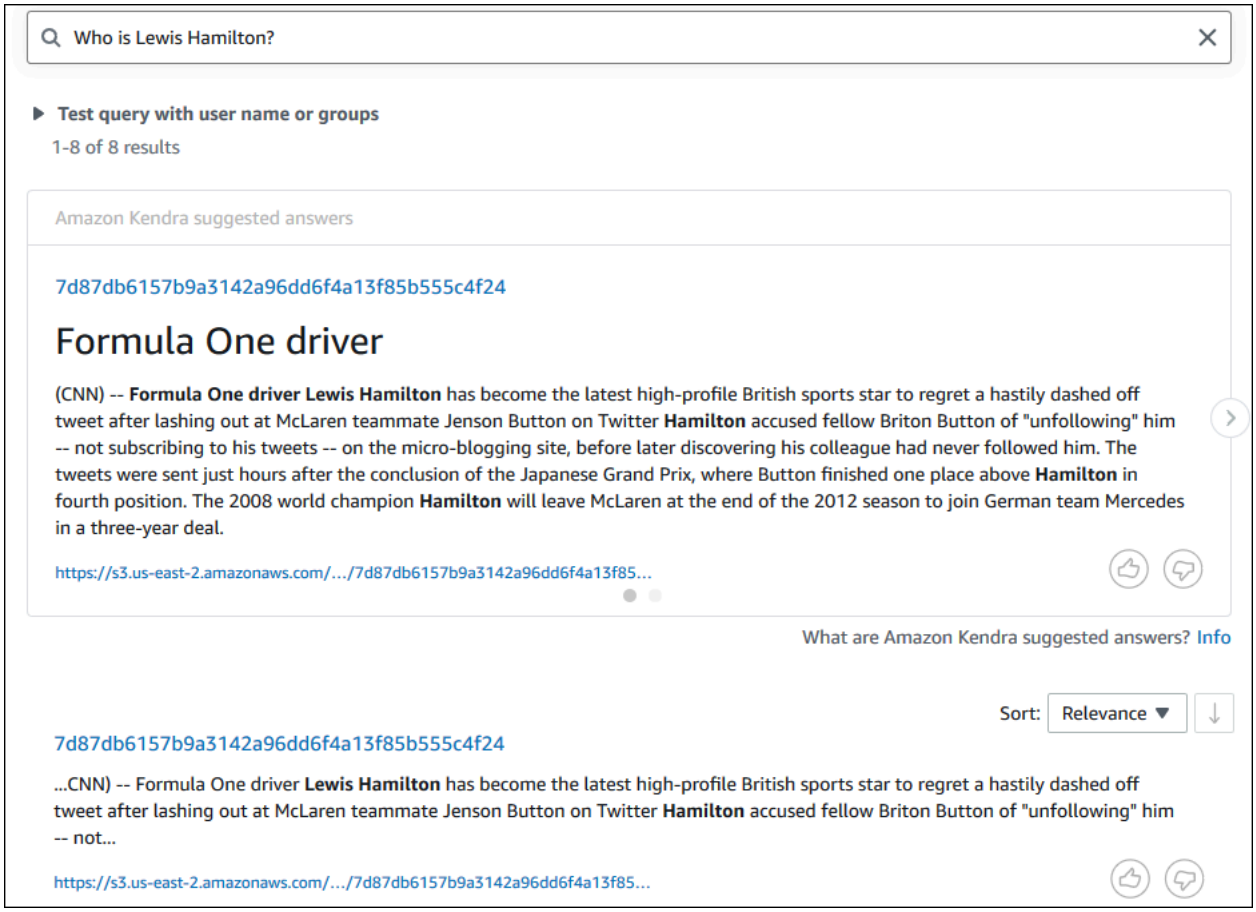
Sie können Ihren Amazon Kendra-Index mithilfe von Fragen abfragen, die den drei Arten von Abfragen entsprechen, die Amazon Kendra unterstützt. Weitere Informationen finden Sie unter Abfragen.

Die Beispielfragen in diesem Abschnitt wurden auf der Grundlage des Beispieldatensatzes ausgewählt.

Um Ihren Amazon Kendra-Index abzufragen (Konsole)

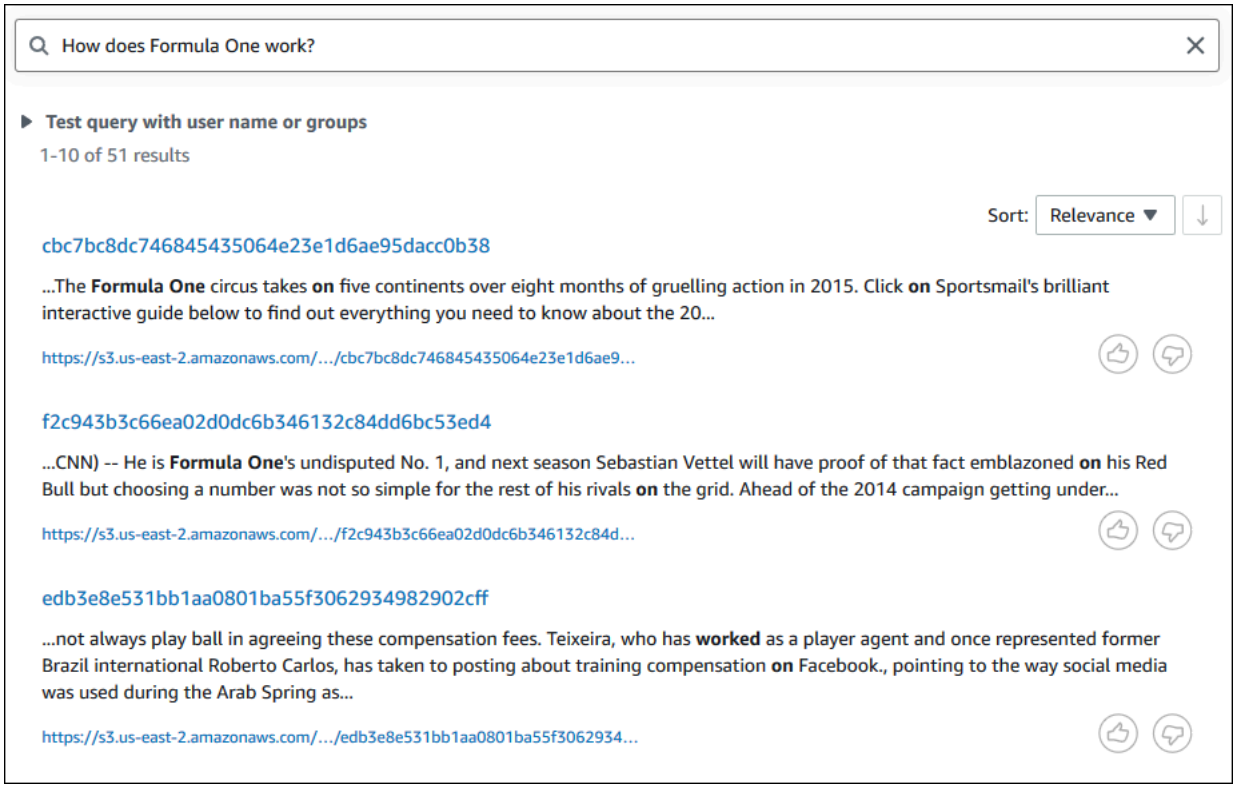
1. Öffnen Sie die Amazon Kendra-Konsole unter https://console.aws.amazon.com/kendra/.
2. Klicken Sie in der Liste der Indizes auf. `kendra-index`
3. Wählen Sie im linken Navigationsmenü die Option, um Ihren Index zu durchsuchen.
4. Um eine Faktoid-Beispielabfrage auszuführen, geben Sie den Text **`Who is Lewis Hamilton?`** in das Suchfeld ein und drücken Sie die Eingabetaste.

   Das erste zurückgegebene Ergebnis ist die von Amazon Kendra vorgeschlagene Antwort zusammen mit der Datendatei, die die Antwort enthält. Die restlichen Ergebnisse bilden den Satz empfohlener Dokumente.



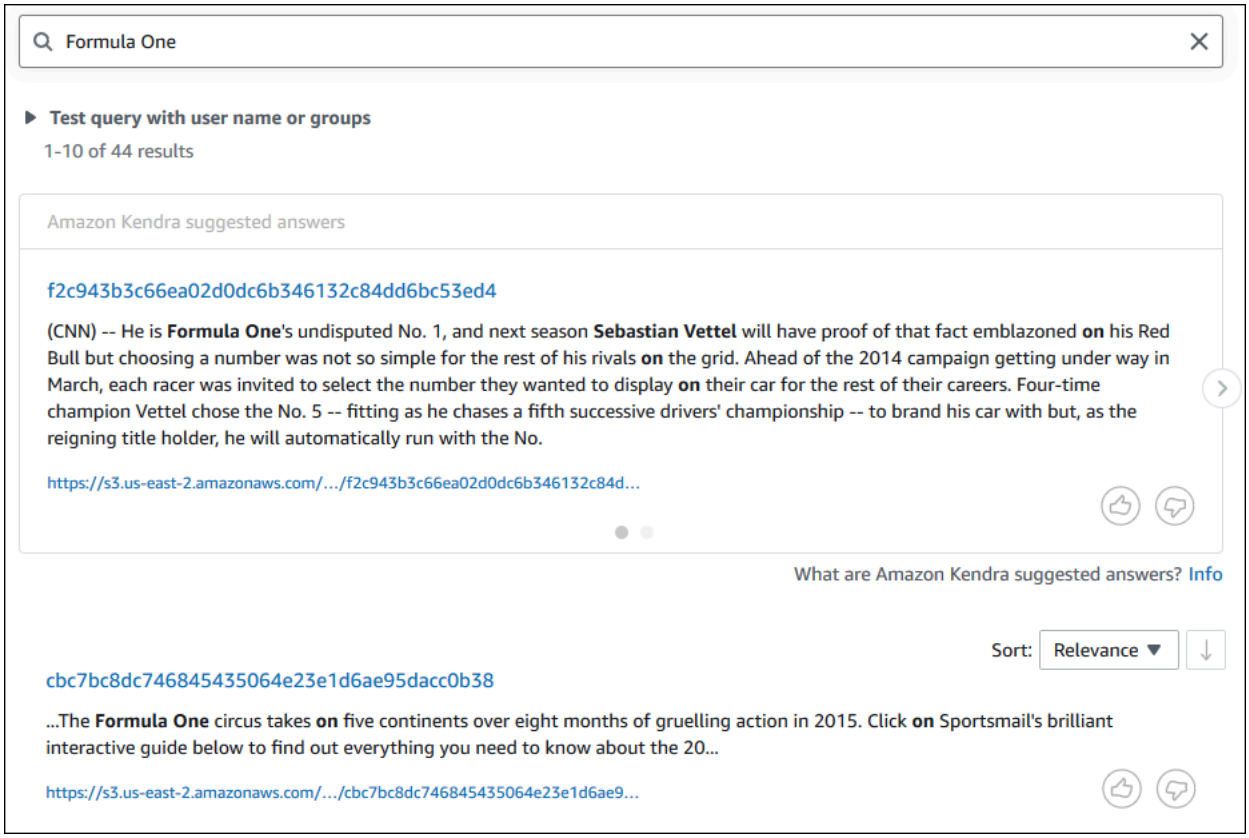
5. Um eine beschreibende Abfrage auszuführen, geben Sie sie **`How does Formula One work?`** in das Suchfeld ein und drücken Sie die Eingabetaste.

   Sie sehen ein weiteres Ergebnis, das von der Amazon Kendra-Konsole zurückgegeben wird. Dieses Mal ist der entsprechende Ausdruck hervorgehoben.



6. Um eine Stichwortsuche durchzuführen, geben Sie **`Formula One`** das Suchfeld ein und drücken Sie die Eingabetaste.

   Sie sehen ein weiteres Ergebnis, das von der Amazon Kendra-Konsole zurückgegeben wird, gefolgt von den Ergebnissen für alle anderen Erwähnungen der Phrase im Datensatz.



Um Ihren Amazon Kendra-Index abzufragen () AWS CLI

1. Verwenden Sie den Befehl query, um eine Beispiel für eine Factoid-Abfrage auszuführen:

   Linux

   ```
   aws kendra query \
           --index-id kendra-index-id \
           --query-text "Who is Lewis Hamilton?" \
           --region aws-region
   ```

   Wobei gilt:

   - *kendra-index-id*ist dein gerettetkendra-index-id,
   - *aws-region* ist Ihre AWS Region.

macOS

```
aws kendra query \
        --index-id kendra-index-id \
        --query-text "Who is Lewis Hamilton?" \
        --region aws-region
```

Wobei gilt:

- *kendra-index-id*ist dein gerettetkendra-index-id,
- *aws-region* ist Ihre AWS Region.

Windows

```
aws kendra query ^
        --index-id kendra-index-id ^
        --query-text "Who is Lewis Hamilton?" ^
        --region aws-region
```

Wobei gilt:

- *kendra-index-id*ist dein gerettetkendra-index-id,
- *aws-region* ist Ihre AWS Region.

Der AWS CLI zeigt die Ergebnisse Ihrer Abfrage an.

2. Verwenden Sie den Befehl query, um eine beispielhafte beschreibende Abfrage auszuführen:

Linux

```
aws kendra query \
        --index-id kendra-index-id \
        --query-text "How does Formula One work?" \
        --region aws-region
```

Wobei gilt:

- *kendra-index-id*ist dein gerettetkendra-index-id,

- *aws-region* ist Ihre AWS Region.

macOS

```
aws kendra query \
        --index-id kendra-index-id \
        --query-text "How does Formula One work?" \
        --region aws-region
```

Wobei gilt:

- *kendra-index-id*ist dein gerettetkendra-index-id,
- *aws-region* ist Ihre AWS Region.

Windows

```
aws kendra query ^
        --index-id kendra-index-id ^
        --query-text "How does Formula One work?" ^
        --region aws-region
```

Wobei gilt:

- *kendra-index-id*ist dein gerettetkendra-index-id,
- *aws-region* ist Ihre AWS Region.

Der AWS CLI zeigt die Ergebnisse Ihrer Abfrage an.

3. Verwenden Sie den Befehl query, um eine Beispielsuche nach Schlüsselwörtern auszuführen:

Linux

```
aws kendra query \
        --index-id kendra-index-id \
        --query-text "Formula One" \
        --region aws-region
```

Wobei gilt:

- *kendra-index-id*ist dein gerettetkendra-index-id,
- *aws-region* ist Ihre AWS Region.

macOS

```
aws kendra query \
        --index-id kendra-index-id \
        --query-text "Formula One" \
        --region aws-region
```

Wobei gilt:

- *kendra-index-id*ist dein gerettetkendra-index-id,
- *aws-region* ist Ihre AWS Region.

Windows

```
aws kendra query ^
        --index-id kendra-index-id ^
        --query-text "Formula One" ^
        --region aws-region
```

Wobei gilt:

- *kendra-index-id*ist dein gerettetkendra-index-id,
- *aws-region* ist Ihre AWS Region.

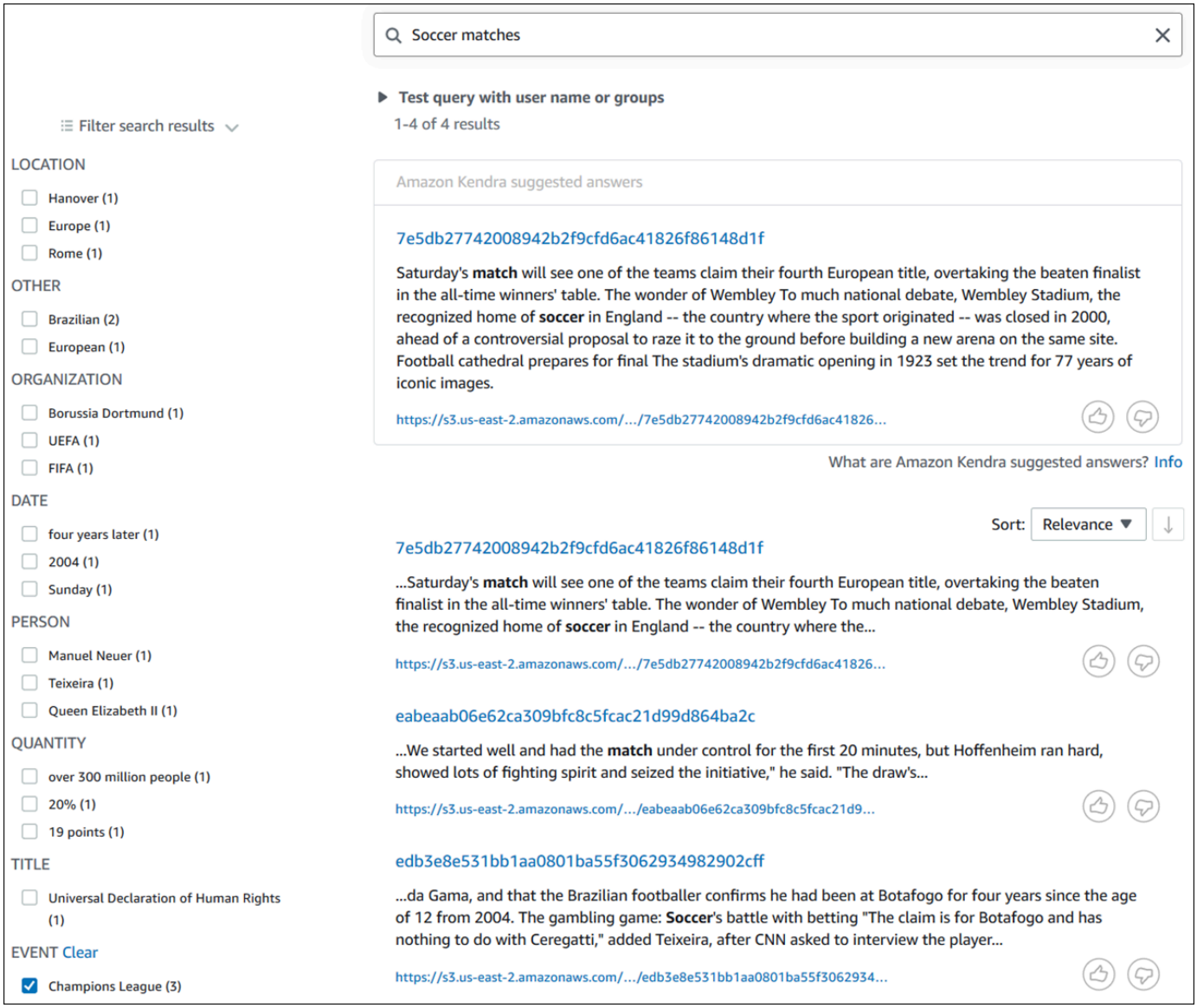
Der AWS CLI zeigt die zurückgegebenen Antworten auf Ihre Anfrage an.

Filtern Ihrer Suchergebnisse

Sie können Ihre Suchergebnisse mithilfe benutzerdefinierter Dokumentattribute in der Amazon Kendra-Konsole filtern und sortieren. Weitere Informationen darüber, wie Amazon Kendra Abfragen verarbeitet, finden Sie unter Filtern von Abfragen.

So filtern Sie Ihre Suchergebnisse (Konsole)

1. Öffnen Sie die Amazon Kendra-Konsole unter https://console.aws.amazon.com/kendra/.
2. Klicken Sie in der Liste der Indizes auf. `kendra-index`
3. Wählen Sie im linken Navigationsmenü die Option, um Ihren Index zu durchsuchen.
4. Geben Sie **`Soccer matches`** in das Suchfeld eine Abfrage ein und drücken Sie die Eingabetaste.
5. Wählen Sie im linken Navigationsmenü die Option Suchergebnisse filtern aus, um eine Liste von Facetten anzuzeigen, mit denen Sie Ihre Suche filtern können.
6. Markieren Sie das Kontrollkästchen für „Champions League“ unter der Unterüberschrift EVENT, um Ihre Suchergebnisse nur nach den Ergebnissen gefiltert zu sehen, die „Champions League“ enthalten.



Um Ihre Suchergebnisse zu filtern (AWS CLI)

1. Verwenden Sie den Befehl query, um die Entitäten eines bestimmten Typs (z. B.EVENT) zu sehen, die für eine Suche verfügbar sind:

   Linux

```
aws kendra query \
        --index-id kendra-index-id \
        --query-text "Soccer matches" \
        --facets '[{"DocumentAttributeKey":"EVENT"}]' \
        --region aws-region
```

Wobei gilt:

- *kendra-index-id*ist dein gerettetkendra-index-id,
- *aws-region* ist Ihre AWS Region.

macOS

```
aws kendra query \
        --index-id kendra-index-id \
        --query-text "Soccer matches" \
        --facets '[{"DocumentAttributeKey":"EVENT"}]' \
        --region aws-region
```

Wobei gilt:

- *kendra-index-id*ist dein gerettetkendra-index-id,
- *aws-region* ist Ihre AWS Region.

Windows

```
aws kendra query ^
        --index-id kendra-index-id ^
        --query-text "Soccer matches" ^
        --facets '[{"DocumentAttributeKey":"EVENT"}]' ^
        --region aws-region
```

Wobei gilt:

- *kendra-index-id*ist dein gerettetkendra-index-id,
- *aws-region* ist Ihre AWS Region.

Der AWS CLI zeigt die Suchergebnisse an. Um eine Liste der Facetten des Typs zu erhaltenEVENT, navigieren Sie zum Abschnitt "FacetResults" der AWS CLI Ausgabe, um eine Liste der filterbaren Facetten mit ihrer Anzahl zu sehen. Eine der Facetten ist beispielsweise die „Champions League“.

> **Note**
>
> Stattdessen können Sie jedes der Indexfelder auswählen`EVENT`, in denen Sie the section called “Einen Amazon Kendra-Index erstellen” für den `DocumentAttributeKey` Wert erstellt haben.

2. Um dieselbe Suche auszuführen, aber nur nach den Ergebnissen zu filtern, die „Champions League“ enthalten, verwenden Sie den Abfragebefehl:

   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
   ```

   Wobei gilt:

   - *`kendra-index-id`*ist dein gerettet`kendra-index-id`,
   - *`aws-region`* ist Ihre AWS Region.

   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
   ```

   Wobei gilt:

   - *`kendra-index-id`*ist dein gerettet`kendra-index-id`,
   - *`aws-region`* ist Ihre AWS Region.

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
```

Wobei gilt:

- *kendra-index-id*ist dein gerettetkendra-index-id,
- *aws-region* ist Ihre AWS Region.

Der AWS CLI zeigt die gefilterten Suchergebnisse an.

Schritt 6: Aufräumen

Deine Dateien bereinigen

Um nach Abschluss dieses Tutorials keine Gebühren mehr auf Ihrem AWS Konto anzustellen, können Sie die folgenden Schritte ausführen:

1. Löschen Sie Ihren Amazon S3-Bucket

   Informationen zum Löschen eines Buckets finden Sie unter Löschen eines Buckets.
2. Löschen Sie Ihren Amazon Kendra-Index

   Informationen zum Löschen eines Amazon Kendra-Index finden Sie unter Löschen eines Indexes.
3. Löschen **converter.py**
   - Für Konsole: Gehe zu und vergewissere dich AWS CloudShell, dass die Region auf deine AWS Region eingestellt ist. Nachdem die Bash-Shell geladen wurde, geben Sie den folgenden Befehl in die Umgebung ein und drücken Sie die Eingabetaste.

     ```
     rm converter.py
     ```

- FürAWS CLI: Führen Sie den folgenden Befehl in einem Terminalfenster aus.

  Linux

  ```
  rm file/converter.py
  ```

  Wobei gilt:

  - *file/* ist der Dateipfad zu `converter.py` Ihrem lokalen Gerät.

  macOS

  ```
  rm file/converter.py
  ```

  Wobei gilt:

  - *file/* ist der Dateipfad zu `converter.py` Ihrem lokalen Gerät.

  Windows

  ```
  rm file/converter.py
  ```

  Wobei gilt:

  - *file/* ist der Dateipfad zu `converter.py` Ihrem lokalen Gerät.

Weitere Informationen

Um mehr über die Integration von Amazon Kendra in Ihren Workflow zu erfahren, können Sie sich die folgenden Blogposts ansehen:

- Tagging von Inhaltsmetadaten für eine erweiterte Suche
- Erstellen Sie eine intelligente Suchlösung mit automatisierter Inhaltsanreicherung

Weitere Informationen zu Amazon Comprehend finden Sie im Amazon Comprehend Developer Guide.

Überwachung und Protokollierung für Amazon Kendra

Themen

Überwachen Sie Ihren Index (Konsole)

Verwenden Sie die Amazon Kendra-Konsole, um den Status von Indizes und Datenquellen zu überwachen. Sie können diese Informationen verwenden, um die Größe und den Speicherbedarf Ihres Indexes zu verfolgen und den Fortschritt und Erfolg der Synchronisation zwischen Ihrem Index und den Datenquellen zu überwachen.

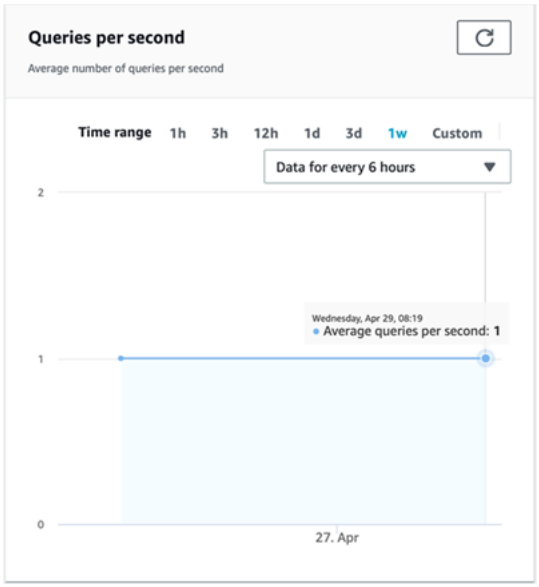
Um Indexmetriken anzuzeigen (Konsole)

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die Amazon Kendra-Konsole unter https://console.aws.amazon.com/kendra/home.
2. Wählen Sie aus der Liste der Indizes den Index aus, den Sie anzeigen möchten.
3. Scrollen Sie auf dem Bildschirm, um die Indexmetriken zu sehen.

Sie können die folgenden Kennzahlen zu Ihrem Index sehen.

- Anzahl der Dokumente — Die Gesamtzahl der indizierten Dokumente. Dazu gehören alle Dokumente aus allen Datenquellen. Verwenden Sie diese Metrik, um zu ermitteln, ob Sie mehr oder weniger Speichereinheiten für Ihren Index kaufen müssen.

- Abfragen pro Sekunde — Die Anzahl der Indexabfragen, die jede Sekunde angefordert werden. Verwenden Sie diese Metrik, um festzustellen, ob Sie mehr oder weniger Abfrageeinheiten für Ihren Index kaufen müssen.



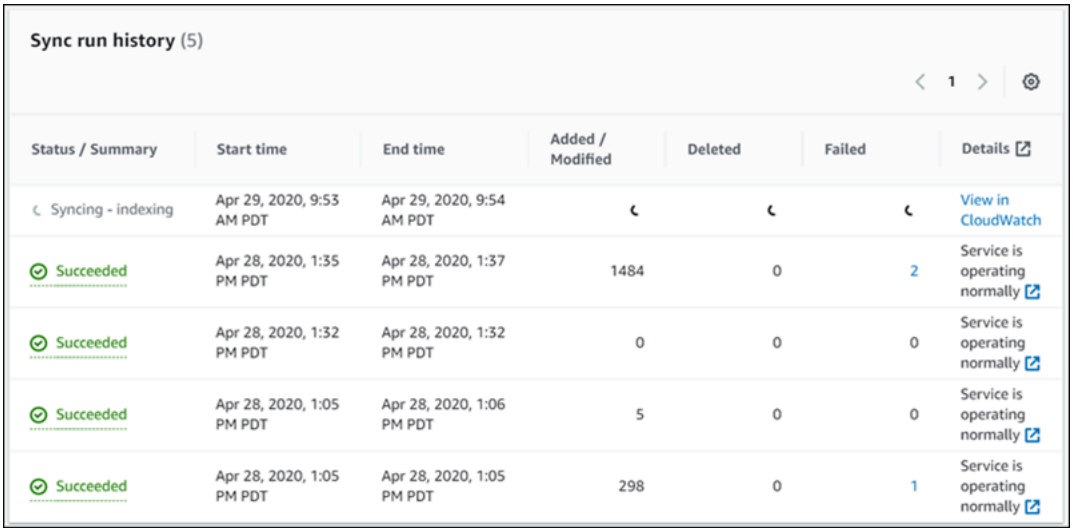
Verwenden Sie die Amazon Kendra-Konsole, um den Fortschritt und den Erfolg der Synchronisation zwischen Ihrem Index und einer Datenquelle zu überwachen. Verwenden Sie diese Informationen, um den Zustand Ihrer Datenquelle zu ermitteln.

Um Synchronisierungsmetriken anzuzeigen (Konsole)

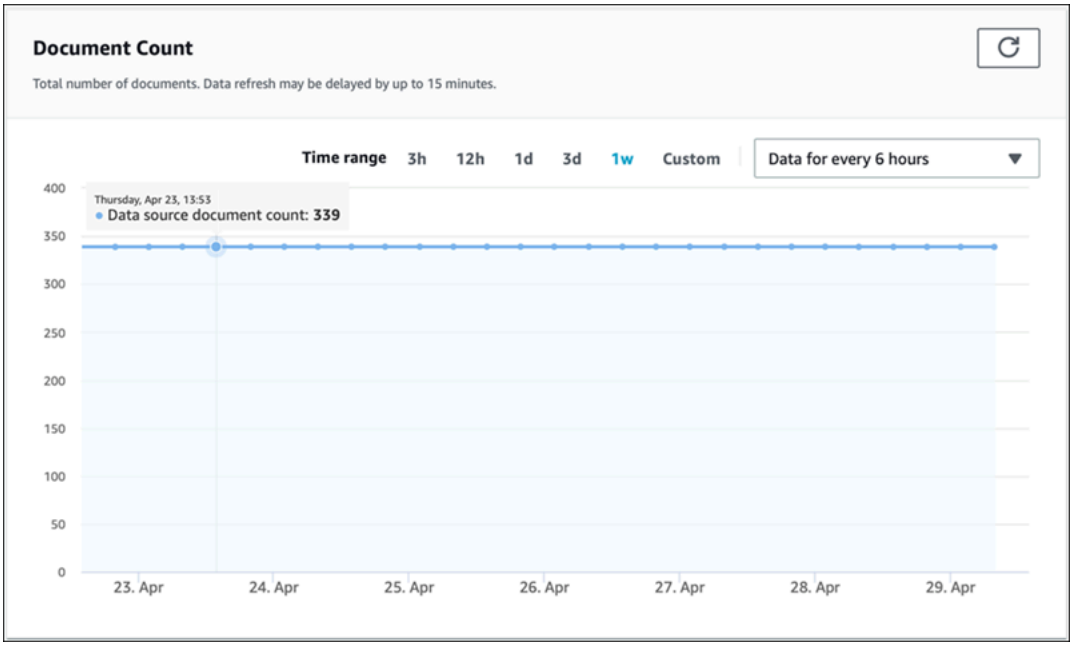
1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die Amazon Kendra-Konsole unter https://console.aws.amazon.com/kendra/home.
2. Wählen Sie aus der Liste der Indizes den Index aus, für den Synchronisierungsmetriken angezeigt werden sollen.
3. Wählen Sie im linken Menü Datenquellen aus.
4. Wählen Sie aus der Liste der Datenquellen die anzuzeigende Datenquelle aus.
5. Scrollen Sie auf dem Bildschirm, um die Sync-Run-Metriken zu sehen.

Sie können die folgenden Informationen sehen.

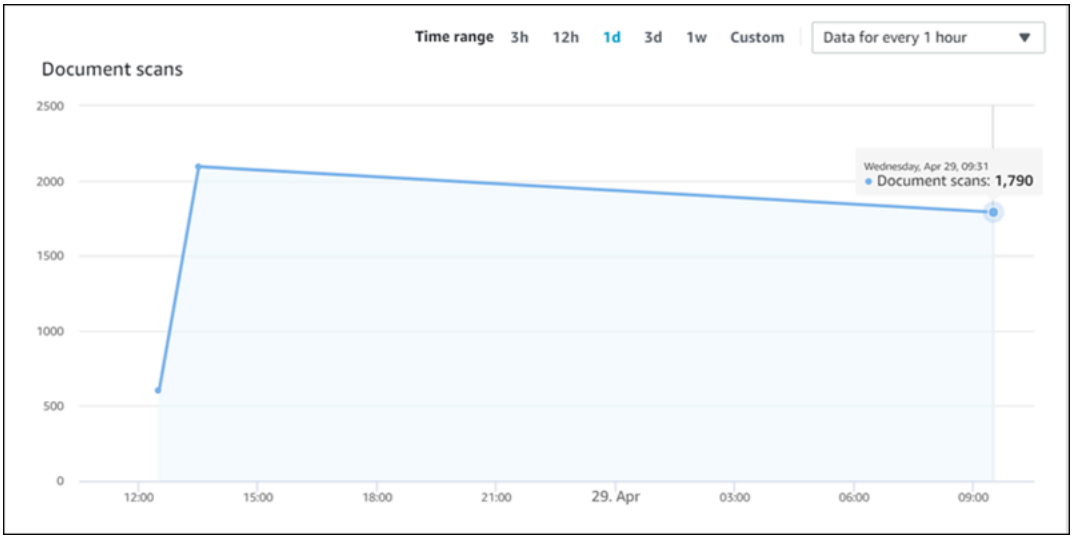
- Verlauf der Synchronisierungsläufe — Statistiken über den Synchronisierungslauf, einschließlich der Start- und Endzeit, der Anzahl der hinzugefügten, gelöschten und fehlgeschlagenen Dokumente. Wenn der Synchronisierungslauf fehlschlägt, gibt es einen Link zu CloudWatch Protokollen mit weiteren Informationen. Wählen Sie das Einstellungssymbol oben links, um die Spalten zu ändern, die im Verlauf angezeigt werden. Verwenden Sie diese Informationen, um den allgemeinen Zustand Ihrer Datenquelle zu ermitteln.



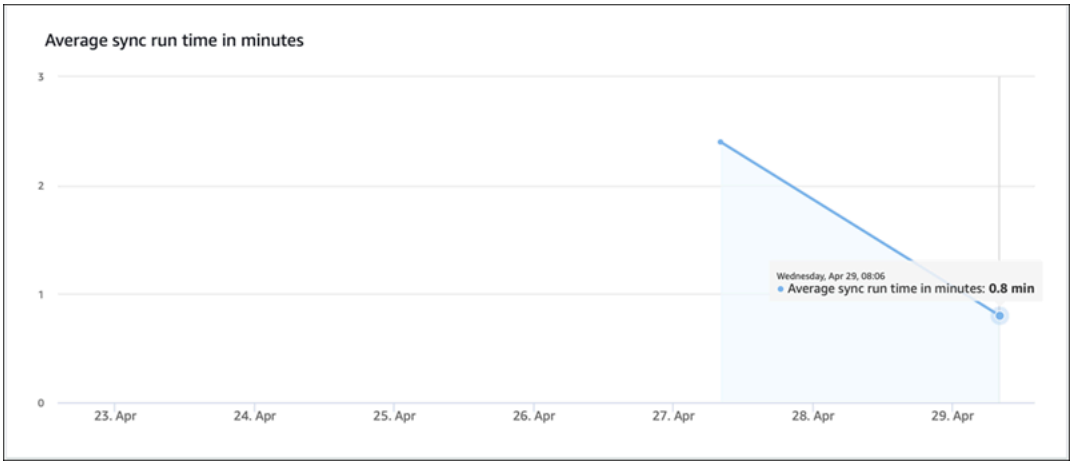
- Anzahl Dokumente — Die Gesamtzahl der Dokumente, die aus dieser Datenquelle indexiert wurden. Dies ist die Summe aller Dokumente, die der Datenquelle hinzugefügt wurden, abzüglich der Summe aller aus der Datenquelle gelöschten Dokumente. Verwenden Sie diese Informationen, um zu ermitteln, wie viele Dokumente aus dieser Datenquelle im Index enthalten sind.



- Dokumentenscans — Die Gesamtzahl der Dokumente, die während des Synchronisierungslaufs gescannt wurden. Dazu gehören alle Dokumente in der Datenquelle, einschließlich der hinzugefügten, aktualisierten, gelöschten oder unveränderten Dokumente. Verwenden Sie diese Informationen, um festzustellen, ob Amazon Kendra alle Dokumente in der Datenquelle scannt. Die Anzahl der gescannten Dokumente wirkt sich auf den für den Service in Rechnung gestellten Betrag aus.



- Durchschnittliche Synchronisierungslaufzeit in Minuten — Die durchschnittliche Zeit, die benötigt wird, bis ein Synchronisierungslauf abgeschlossen ist. Die Zeit, die für die Synchronisierung einer Datenquelle benötigt wird, wirkt sich auf den für den Dienst in Rechnung gestellten Betrag aus.



Protokollieren von Amazon-Kendra-API-Aufrufen mitAWS CloudTrailaufzeichnen

Amazon Kendra ist integriert inAWS CloudTrail, ein Dienst, der eine Aufzeichnung der Aktionen, die von einem Benutzer, eine Rolle oder einAWSService in Amazon Kendra. CloudTrail erfasst alle API-Aufrufe von Amazon Kendra als Ereignisse, einschließlich der Aufrufe von der Amazon Kendra Console und Codeaufrufen an die Amazon Kendra APIs. Wenn Sie einen Trail erstellen, können Sie die kontinuierliche Bereitstellung von aktivieren CloudTrail Ereignisse in ein Amazon S3 S3-Bucket, einschließlich Ereignisse für Amazon Kendra. Wenn du keinen Trail konfigurierst, kannst du die neuesten Ereignisse trotzdem in der CloudTrail Konsole inHistlieren. Verwendung der gesammelten Informationen von CloudTrail, können Sie die Anfrage, die an Amazon Kendra gesendet wird, die IP-Adresse, von der aus die Anfrage gesendet wird, wer die Anfrage gestellt hat, wann sie gestellt wurde und weitere Informationen.

Für weitere Informationen über CloudTrail, einschließlich der Konfiguration und Aktivierung, finden Sie in derAWS CloudTrailBenutzerleitfaden.

Amazon-Kendra-Informationen in CloudTrail

CloudTrail ist auf Ihrem aktiviertAWSKonto, wenn Sie das Konto erstellen. Wenn eine Aktivität in Amazon Kendra auftritt, wird diese Aktivität in einem CloudTrail Ereignis zusammen mit anderenAWSServiceveranstalten in der CloudTrail Histlieren. Sie können die neusten Ereignisse in Ihr AWS-Konto herunterladen und dort suchen und anzeigen. Weitere Informationen finden Sie unter Anzeigen von Ereignissen mit dem CloudTrail -API-Ereignisverlauf.

Für eine fortlaufende Aufzeichnung der Ereignisse in IhremAWSein Konto, einschließlich Veranstaltungen für Amazon Kendra, ein Amazon Kendra erstellen. EINWanderwegist eine Konfiguration, die es ermöglicht CloudTrail um Ereignisse als Protokolldateien an ein bestimmtes S3-Bucket zu liefern. Wenn Sie ein Trail in der Konsole anlegen, gilt dieser für alle AWS-Regionen. Der Trail protokolliert Ereignisse aus allen Regionen in der AWS-Partition und stellt die Protokolldateien für den von Ihnen angegebenen S3 Bucket bereit. Darüber hinaus können Sie andere konfigurierenAWSDienste zur weiteren Analyse und Bearbeitung der in CloudTrail Logs. Weitere Informationen finden Sie unter:

- Übersicht zum Erstellen eines Trails
- CloudTrail Von unterstützte Services und Integrationen
- Konfigurieren von Amazon SNS-Benachrichtigungen für CloudTrail
- Empfangen CloudTrail Protokollieren von Kendra-AufrufenundEmpfangen CloudTrail Protokollieren von Kendten

CloudTrail protokolliert alle Amazon Kendra Kendra-Aktionen, die dokumentiert sind inAPI-Referenz. Zum Beispiel Aufrufen an`CreateIndex`,`CreateDataSource`, und`Query`Operationen generieren Einträge in CloudTrail Protokolllieren.

Jeder Ereignis- oder Protokolleintrag enthält Informationen zu dem Benutzer, der die Anforderung generiert hat. Weitere Informationen finden Sie unter CloudTrail userIdentity-Element.

Beispiel: Amazon Kendra Kendra-Protokolldateieinträge

EINWanderwegist eine Konfiguration, die die Übermittlung von Ereignissen als Protokolldateien an ein bestimmtes S3-Bucket ermöglicht. CloudTrail Protokolldateien enthalten einen oder mehrere Protokolleinträge. EinVeranstaltungstellt eine einzelne Anfrage aus einer beliebigen Quelle dar und enthält Informationen über die angeforderte Aktion, das Datum und die Uhrzeit der Aktion, Anforderungsparameter usw. CloudTrail Bei Protokolldateien handelt es sich um keine geordnete Stack-Trace der öffentlichen API-Aufrufe, sodass sie nicht in einer bestimmten Reihenfolge angezeigt werden.

Aufrufe an die`Query`Operation erstellt den folgenden Eintrag.

```
        {
            "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"
        },
```

Protokollieren von Amazon Kendra Intelligent Ranking API-Aufrufen mitAWS CloudTrailaufzeichnen

Amazon Kendra Intelligent Ranking ist integriert inAWS CloudTrail, ein Dienst, der eine Aufzeichnung der Aktionen, die von einem Benutzer, eine Rolle oder einAWSService im Amazon Kendra Intelligent Ranking. CloudTrail erfasst alle API-Aufrufe von Amazon Kendra Intelligent Ranking als Ereignisse, einschließlich Codeaufrufen an die Amazon Kendra Intelligent Ranking APIs. Wenn Sie einen Trail erstellen, können Sie die kontinuierliche Bereitstellung von aktivieren CloudTrail Ereignisse in ein Amazon S3 S3-Bucket, einschließlich Ereignisse für Amazon Kendra Intelligent Ranking. Wenn du keinen Trail konfigurierst, kannst du die neuesten Ereignisse trotzdem in der CloudTrail Konsole inHistlieren. Verwendung der gesammelten Informationen von CloudTrail, können Sie die Anfrage, die an Amazon Kendra Intelligent Ranking gesendet wird, die IP-Adresse, von der aus die Anfrage gesendet wird, wer die Anfrage gestellt hat, wann sie gestellt wird und weitere Details ermitteln.

Für weitere Informationen über CloudTrail, einschließlich der Konfiguration und Aktivierung, finden Sie in derAWS CloudTrailBenutzerleitfaden.

Amazon Kendra Intelligent Rankinginformationen in CloudTrail

CloudTrail ist auf Ihrem aktiviertAWSKonto, wenn Sie das Konto erstellen. Wenn eine Aktivität in Amazon Kendra Intelligent Ranking auftritt, wird diese Aktivität in einem CloudTrailEreignis zusammen mit anderenAWSServiceveranstalten in der CloudTrail Histlieren. Sie können die neusten Ereignisse in Ihr AWS-Konto herunterladen und dort suchen und anzeigen. Weitere Informationen finden Sie unterAnzeigen von Ereignissen mit CloudTrail Verlauf der Ereignisse.

Für eine fortlaufende Aufzeichnung der Ereignisse in IhremAWSein Konto, einschließlich der Ereignisse für Amazon Kendra Intelligent Ranking, eine Spur erstellen. EINWanderwegist eine Konfiguration, die es ermöglicht CloudTrail um Ereignisse als Protokolldateien an ein bestimmtes S3-Bucket zu liefern. Wenn Sie ein Trail in der Konsole anlegen, gilt dieser für alle AWS-Regionen. Der Trail protokolliert Ereignisse aus allen Regionen in der AWS-Partition und stellt die Protokolldateien für den von Ihnen angegebenen S3 Bucket bereit. Darüber hinaus können Sie andere konfigurierenAWSDienste zur weiteren Analyse und Bearbeitung der in CloudTrail Logs. Weitere Informationen finden Sie unter:

- Übersicht zum Erstellen eines Trails
- CloudTrail Von unterstützte Services und Integrationen
- Konfigurieren von Amazon SNS-Benachrichtigungen für CloudTrail

- Empfangen CloudTrail Protokollieren von Kendra-AufrufenundEmpfangen CloudTrail Protokollieren von Kendten

CloudTrail protokolliert alle Amazon Kendra Intelligent Ranking-Aktionen, die dokumentiert sind inAPI-Referenz. Zum Beispiel Aufrufen an`CreateRescoreExecutionPlan`Generieren Sie Einträge in der CloudTrail Protokolllieren.

Jeder Ereignis- oder Protokolleintrag enthält Informationen zu dem Benutzer, der die Anforderung generiert hat. Weitere Informationen finden Sie unter CloudTrail userIdentity-Element.

Beispiel: Amazon Kendra Intelligent Rankinging-Protokolldateieinträge

EINWanderwegist eine Konfiguration, die die Übermittlung von Ereignissen als Protokolldateien an ein bestimmtes S3-Bucket ermöglicht. CloudTrail Protokolldateien enthalten einen oder mehrere Protokolleinträge. EinVeranstaltungstellt eine einzelne Anfrage aus einer beliebigen Quelle dar und enthält Informationen über die angeforderte Aktion, das Datum und die Uhrzeit der Aktion, Anforderungsparameter usw. CloudTrail Bei Protokolldateien handelt es sich um keine geordnete Stack-Trace der öffentlichen API-Aufrufe, sodass sie nicht in einer bestimmten Reihenfolge angezeigt werden.

Aufrufe an die`CreateRescoreExecutionPlan`Operation erstellt den folgenden Eintrag.

```
{
            "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"
        }
    }
```

Überwachung von Amazon Kendra mit Amazon CloudWatch

Verwenden Sie Amazon, um den Zustand Ihrer Indizes zu verfolgen CloudWatch. Mit CloudWatch, können Sie Metriken für die Dokumentensynchronisierung für Ihren Index abrufen. Sie können auch einrichten CloudWatch Alarme, um benachrichtigt zu werden, wenn eine oder mehrere Metriken einen von Ihnen definierten Schwellenwert überschreiten. Sie können beispielsweise die Anzahl der Dokumente überwachen, die zur Indexierung eingereicht wurden, oder die Anzahl der Dokumente, die nicht indexiert werden konnten.

Sie müssen die entsprechenden CloudWatch Berechtigungen zur Überwachung von Amazon Kendra mit CloudWatch. Weitere Informationen finden Sie unterAuthentifizierung und Zugriffskontrolle für Amazon CloudWatchin derAmazon CloudWatchBenutzerleitfaden.

Anzeigen von Amazon-Kendra-Aufrufen

Anzeigen von Amazon-Kendra-Aufrufen mit CloudWatch Konsole.

Um Kendten zu sehen (CloudWatch Konsole)

1. Melden Sie sich beiAWS Management Consoleund öffne CloudWatch Konsole beihttps://console.aws.amazon.com/cloudwatch/.
2. WähleMetriken, wählenAlle Metrikenund dann wähleKendra.
3. Wählen Sie die Dimension, den Namen einer Metrik und schließlich Add to graph (Dem Diagramm hinzufügen) aus.
4. Wählen Sie einen Wert für den Datumsbereich aus. Die Anzahl der Kennzahlen für den ausgewählten Zeitraum wird im Diagramm angezeigt.

Erstellen eines Alarms

EIN CloudWatch Bei einem Alarm wird eine einzelne Metrik über einen bestimmten Zeitraum überwacht und eine oder mehrere Aktionen ausgeführt: eine Benachrichtigung wird an ein Amazon Simple Notification Service (Amazon SNS) -Thema oder eine Auto Scaling-Richtlinie gesendet wird. Bei den Aktionen oder Aktionen handelt es sich um den Wert der Metrik im Verhältnis zu einem bestimmten Schwellenwert über eine von Ihnen angegebene Anzahl von Zeiträumen. CloudWatch kann Ihnen auch eine Amazon SNS Benachrichtigung senden, wenn sich der Alarmstatus ändert.

CloudWatch Bei Alarmen werden nur Aktionen ausgelöst, wenn sich der Status ändert und für den von Ihnen angegebenen Zeitraum bestehen bleibt.

So legen Sie einen Alarm fest

1. Melden Sie sich beiAWS Management Consoleund öffne CloudWatch Konsole beihttps://console.aws.amazon.com/cloudwatch/.
2. WähleAlarmeund dann wähleErstellen Sie einen Alarm.
3. Wählen Sie eine Metrik aus. Wählen Sie eineKendraMetrik für Ihren Index und Ihre Datenquelle. Stellen Sie die Uhrzeit auch als festgelegte Anzahl von Stunden, Tagen, Wochen oder als benutzerdefinierte Anzahl ein.

4. Wählen Sie Ihre Statistik aus. Zum BeispielDurchschnittlich. Wählen Sie auch den Zeitraum für die Alarmauslösung als festgelegte Anzahl von Minuten, Stunden, pro Tag oder als benutzerdefinierte Zeitspanne.
5. Wählen Sie den Schwellenwert für die Auslösung des Alarms aus, ob Sie einen statischen Wert oder ein Band verwenden möchten, und wählen Sie die Bedingung, die für den Schwellenwert erfüllt sein muss.
6. Wählen Sie den Alarmstatus für den Auslöser, ob die Metrik Ihren festgelegten Schwellenwert überschreiten muss, oder einen anderen Status. Wählen Sie aus, an wen oder welche E-Mail die Alarmbenachrichtigung gesendet werden soll.
7. Wenn Sie mit dem Alarm zufrieden sind, wählen SieErstellen Sie einen Alarm.

> **Note**
>
> Sie müssen einen Namen für CloudWatch Allieren.

CloudWatch Metriken für Jobs zur Indexsynchronisierung

In der folgenden Tabelle werden die Amazon Kendra-Metriken für Datenquellensynchronisierungsjobs beschrieben.

Wenn Sie die API oder CLI verwenden, müssen Sie Folgendes angeben`Namespace`als 'AWS/Kendra' zusätzlich zu`MetricName`Ihrer Wahl bei der VerwendungGetMetricStatisticsAPI.

Metrik	Beschreibung
`DocumentsCrawled`	Die Anzahl der Dokumente, die der Synchroni sierungsauftrag während der Ausführung gescannt oder entdeckt hat. Dimensionen: • IndexId • DataSourceId Einheit: Anzahl

Metrik	Beschreibung
DocumentsSubmittedForIndexing	Die Anzahl der Dokumente, die der Synchronisierungsauftrag an den Index übermittelt hat. Dimensionen: • IndexId • DataSourceId Einheit: Anzahl
DocumentsSubmittedForIndexingFailed	Die Anzahl der Dokumente, bei denen die Indizierung fehlgeschlagen ist. Überprüfen Sie den Inhalt des CloudWatch Einzelheiten finden Sie im Protokoll für den Synchronisationsjob. Dimensionen: • IndexId • DataSourceId Einheit: Anzahl
DocumentsSubmittedForDeletion	Die Anzahl der Dokumente, die im Rahmen des Synchronisierungsauftrags aus dem Index entfernt werden sollten. Dimensionen: • IndexId • DataSourceId Einheit: Anzahl

Metrik	Beschreibung
`DocumentsSubmittedForDeletionFailed`	Die Anzahl der Dokumente, die nicht gelöscht werden konnten. Überprüfen Sie den Inhalt des CloudWatch Einzelheiten finden Sie im Protokoll für den Synchronisationsjob. Dimensionen: • IndexId • DataSourceId Einheit: Anzahl

Metlieren für Amazon-Kendra-Datenquellen

In der folgenden Tabelle werden die Amazon Kendra-Metriken für Datenquellensynchronisierungsjobs beschrieben. Mit einem Sternchen (*) markierte Metriken werden nur für Amazon S3 S3-Datenquellen verwendet.

Wenn Sie die API oder CLI verwenden, müssen Sie Folgendes angeben`Namespace`als 'AWS/Kendra' zusätzlich zu`MetricName`Ihrer Wahl bei der VerwendungGetMetricStatisticsAPI.

Metrik	Beschreibung
`DocumentsSkippedNoChange *`	Die Anzahl der untersuchten Dokumente, bei denen festgestellt wurde, dass sie sich nicht geändert haben, sodass sie nicht zur Indexierung eingereicht wurden. Dimensionen: • IndexId • DataSourceId Einheit: Anzahl

Metrik	Beschreibung
`DocumentsSkippedInvalidMetadata *`	Die Anzahl der Dokumente, die übersprungen wurden, weil ein Problem mit der zugehörigen Metadatendatei aufgetreten ist. Überprüfen Sie den Inhalt des CloudWatch Einzelheiten finden Sie im Protokoll des Synchronisierungslaufs. Dimensionen: • IndexId • DataSourceId Einheit: Anzahl
`DocumentsCrawled`	Die Anzahl der untersuchten Dokumentdateien. Dimensionen: • IndexId • DataSourceId Einheit: Anzahl
`DocumentsSubmittedForDeletion`	Die Anzahl der untersuchten Dokumente, die aus der Datenquelle gelöscht und zur Löschung eingereicht wurden. Dimensionen: • IndexId • DataSourceId Einheit: Anzahl

Metrik	Beschreibung
`DocumentsSubmittedForDeletionFailed`	Die Anzahl der Dokumente, die aus einer Datenquelle nicht gelöscht werden konnten. Dimensionen: • IndexId • DataSourceId Einheit: Anzahl
`DocumentsSubmittedForIndexing`	Die Anzahl der Dokumente, die geprüft und zur Indexierung eingereicht wurden. Dimensionen: • IndexId • DataSourceId Einheit: Anzahl
`DocumentsSubmittedForIndexingFailed`	Die Anzahl der zur Indexierung eingereichten Dokumente, die nicht indexiert werden konnten. Dimensionen: • IndexId • DataSourceId Einheit: Anzahl

Metriken für indizierte Dokumente

In der folgenden Tabelle werden die Amazon Kendra Kendra-Metriken für indizierte Dokumente beschrieben. Für Dokumente, die mit dem indexiert wurdenBatchPutDocumentOperation, nur der`IndexId`Dimension wird unterstützt.

Wenn Sie die API oder CLI verwenden, müssen Sie Folgendes angeben`Namespace`als 'AWS/Kendra' zusätzlich zu`MetricName`Ihrer Wahl bei der VerwendungGetMetricStatisticsAPI.

Metrik	Beschreibung
`DocumentsIndexed`	Die Anzahl der indexierten Dokumente. Dimensionen: • IndexId • DataSourceId Einheit: Anzahl
`DocumentsFailedToIndex`	Die Anzahl der Dokumente, die nicht indexiert werden konnten. Überprüfen Sie den Inhalt des CloudWatch Protokollieren Sie für Details. Dimensionen: • IndexId • DataSourceId Einheit: Anzahl
`IndexQueryCount`	Die Anzahl der Indexabfragen pro Minute. Dimensionen: • IndexId Einheit: Anzahl

Überwachung von Amazon Kendra mit Amazon CloudWatch Logs

Amazon-Kendra-verwendet Amazon-Kendra- CloudWatch Protokolle, die Ihnen einen Einblick in den Betrieb Ihrer Datenquellen geben. Amazon Kendra protokolliert Prozessdetails für die Dokumente,

während sie indexiert werden. Es protokolliert Fehler aus Ihrer Datenquelle, die während der Indexierung Ihrer Dokumente auftreten. Sie verwenden CloudWatch Protokolle zur Überwachung, Speicherung und zum Zugriff auf die Protokolldateien.

CloudWatch Logs speichert Protokollereignisse in einem Protokollstream, der Teil einer Protokollgruppe ist. Amazon Kendra verwendet diese Funktionen wie folgt:

- Protokollgruppen — Amazon Kendra speichert alle Ihre Protokollstreams in einer einzigen Protokollgruppe für jeden Index. Amazon Kendra erstellt die Protokollgruppe, wenn der Index erstellt wird. Die Protokollgruppen-ID beginnt immer mit „aws/kendra/“.
- Protokollstream — Amazon Kendra erstellt einen neuen Datenquellen-Protokollstream in der Protokollgruppe für jeden Indexsynchronisierungsauftrag, den Sie ausführen. Es erstellt auch einen neuen Dokument-Log-Stream, wenn ein Stream ungefähr 500 Einträge erreicht.
- Protokolleinträge — Amazon Kendra erstellt bei der Indizierung von Dokumenten einen Protokolleintrag im Protokollstream. Jeder Eintrag enthält Informationen über die Verarbeitung des Dokuments oder über aufgetretene Fehler.

Für weitere Informationen zur Verwendung von CloudWatch Protokolle finden Sie unterWas ist Amazon-Kendra-Protokollierenin derAmazon Cloud Watch Logs-Benutzerhandbuch.

Amazon Kendra erstellt zwei Arten von Protokollstreams:

- Datenquellen-Log-Streams
- Protokollieren von Dokumlieren

Datenquellen-Log-Streams

Datenquellen-Logstreams veröffentlichen Einträge zu Ihren Indexsynchronisierungsjobs. Jeder Synchronisierungsauftrag erstellt einen neuen Protokollstream, der zum Veröffentlichen von Einträgen verwendet wird. Der Protokollstream-Name ist:

```
data source id/YYYY-MM-DD-HH/data source sync job ID
```

Für jeden ausgeführten Synchronisationsauftrag wird ein neuer Protokollstream erstellt.

Es gibt drei Arten von Protokollnachrichten, die in einem Datenquellen-Protokollstream veröffentlicht werden:

- Eine Protokollnachricht für ein Dokument, das nicht zur Indizierung gesendet werden konnte. Im Folgenden finden Sie ein Beispiel für diese Nachricht für ein Dokument in einer S3-Datenquelle:

```
{
    "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."
}
```

- Eine Protokollnachricht für ein Dokument, das nicht zum Löschen gesendet werden konnte. Im Folgenden ein Beispiel für diese Nachricht:

```
{
    "DocumentId": "document ID",
    "Message": "Failed to delete document via BatchDeleteDocument.",
    "ErrorCode": "InvalidRequest",
    "ErrorMessage": "Document can't be deleted because it doesn't exist."
}
```

- Eine Protokollmeldung, wenn eine ungültige Metadatendatei für ein Dokument in einem Amazon S3 S3-Bucket gefunden wird. Im Folgenden finden Sie ein Beispiel für diese Nachricht.

```
{
    "Message": "Found invalid metadata
 file bucket/prefix/filename.extension.metadata.json."
}
```

- Für SharePoint und Datenbank-Konnektoren, Amazon Kendra schreibt nur dann Nachrichten in den Protokollstream, wenn ein Dokument nicht indexiert werden kann. Im Folgenden finden Sie ein Beispiel für eine Fehlermeldung, die Amazon Kendra protokolliert.

```
{
    "DocumentID": "document ID",
    "IndexID": "index ID",
    "SourceURI": "",
    "CrawlStatus": "FAILED",
    "ErrorCode": "403",
    "ErrorMessage": "Access Denied",
    "DataSourceErrorCode": "403"
```

```
}
```

Protokollieren von Dokumlieren

Amazon Kendra protokolliert Informationen über die Verarbeitung von Dokumenten, während sie indexiert werden. Es protokolliert eine Reihe von Nachrichten für Dokumente, die in einer Amazon S3 S3-Datenquelle gespeichert sind. Es protokolliert Fehler nur für Dokumente, die in einem Microsoft gespeichert sind SharePoint oder eine Datenbankdatenquelle.

Wenn die Dokumente dem Index hinzugefügt wurden, indemBatchPutDocumentOperation, der Protokollstream wird wie folgt benannt:

```
YYYY-MM-DD-HH/UUID
```

Wenn die Dokumente mithilfe einer Datenquelle zum Index hinzugefügt wurden, wird der Protokollstream wie folgt benannt:

```
dataSourceId/YYYY-MM-DD-HH/UUID
```

Jeder Protokollstream enthält bis zu 500 Nachrichten.

Wenn die Indizierung eines Dokuments fehlschlägt, wird diese Meldung in den Protokollstream ausgegeben:

```
{
    "DocumentId": "document ID",
    "IndexName": "index name",
    "IndexId": "index ID"
    "SourceURI": "source URI"
    "IndexingStatus": "DocumentFailedToIndex",
    "ErrorCode": "400 | 500",
    "ErrorMessage": "message"
}
```

Sicherheit in Amazon Kendra

Cloud-Sicherheit hat AWS höchste Priorität. Als AWS Kunde profitieren Sie von einer Rechenzentrums- und Netzwerkarchitektur, die darauf ausgelegt sind, die Anforderungen der sicherheitssensibelsten Unternehmen zu erfüllen.

Sicherheit ist eine gemeinsame Verantwortung von Ihnen AWS und Ihnen. Das Modell der geteilten Verantwortung beschreibt dies als Sicherheit der Cloud selbst und Sicherheit in der Cloud:

- Sicherheit der Cloud —AWS ist verantwortlich für den Schutz der Infrastruktur, die AWS Dienste in der AWS Cloud ausführt. AWS bietet Ihnen auch Dienste, die Sie sicher nutzen können. Externe Prüfer testen und verifizieren regelmäßig die Wirksamkeit unserer Sicherheitsmaßnahmen im Rahmen der AWS . Weitere Informationen zu den Compliance-Programmen, die für Amazon Kendra gelten, finden Sie unter AWS Services in Scope by Compliance Program AWS .
- Sicherheit in der Cloud — Ihre Verantwortung richtet sich nach dem AWS Service, den Sie nutzen. Sie sind auch für andere Faktoren verantwortlich, etwa für die Vertraulichkeit Ihrer Daten, für die Anforderungen Ihres Unternehmens und für die geltenden Gesetze und Vorschriften.

Diese Dokumentation hilft Ihnen zu verstehen, wie Sie das Modell der gemeinsamen Verantwortung bei der Verwendung von Amazon Kendra anwenden können. In den folgenden Themen erfahren Sie, wie Sie Amazon Kendra konfigurieren, um Ihre Sicherheits- und Compliance-Ziele zu erreichen. Sie lernen auch, wie Sie andere AWS Dienste nutzen können, die Ihnen helfen, Ihre Amazon Kendra Kendra-Ressourcen zu überwachen und zu sichern.

Themen

- Konfiguration und Schwachstellenanalyse in AWS Identity and Access Management

Datenschutz bei Amazon Kendra

Das AWS Modell der gilt für den Datenschutz in Amazon Kendra. Wie in diesem Modell beschrieben, AWS ist verantwortlich für den Schutz der globalen Infrastruktur, auf der AWS Cloud alle Systeme laufen. Sie sind dafür verantwortlich, die Kontrolle über Ihre in dieser Infrastruktur gehosteten Inhalte zu behalten. Sie sind auch für die Sicherheitskonfiguration und die Verwaltungsaufgaben für die von Ihnen verwendeten AWS-Services verantwortlich. Weitere Informationen zum Datenschutz finden Sie unter Häufig gestellte Fragen zum Datenschutz. Informationen zum Datenschutz in Europa finden Sie im Blog-Beitrag AWS -Modell der geteilten Verantwortung und in der DSGVO im AWS -Sicherheitsblog.

Aus Datenschutzgründen empfehlen wir, dass Sie AWS-Konto Anmeldeinformationen schützen und einzelne Benutzer mit AWS IAM Identity Center oder AWS Identity and Access Management (IAM) einrichten. So erhält jeder Benutzer nur die Berechtigungen, die zum Durchführen seiner Aufgaben erforderlich sind. Außerdem empfehlen wir, die Daten mit folgenden Methoden schützen:

- Verwenden Sie für jedes Konto die Multi-Faktor-Authentifizierung (MFA).
- Verwenden Sie SSL/TLS, um mit Ressourcen zu kommunizieren. AWS Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Richten Sie die API und die Protokollierung von Benutzeraktivitäten mit ein. AWS CloudTrail
- Verwenden Sie AWS Verschlüsselungslösungen zusammen mit allen darin enthaltenen Standardsicherheitskontrollen AWS-Services.
- Verwenden Sie erweiterte verwaltete Sicherheitsservices wie Amazon Macie, die dabei helfen, in Amazon S3 gespeicherte persönliche Daten zu erkennen und zu schützen.
- Wenn Sie für den Zugriff AWS über eine Befehlszeilenschnittstelle oder eine API FIPS 140-2-validierte kryptografische Module benötigen, verwenden Sie einen FIPS-Endpunkt. Weitere Informationen über verfügbare FIPS-Endpunkte finden Sie unter Federal Information Processing Standard (FIPS) 140-2.

Wir empfehlen dringend, in Freitextfeldern, z. B. im Feld Name, keine vertraulichen oder sensiblen Informationen wie die E-Mail-Adressen Ihrer Kunden einzugeben. Dies gilt auch, wenn Sie mit Amazon Kendra oder anderen AWS-Services über die Konsole AWS CLI, API oder AWS SDKs arbeiten. Alle Daten, die Sie in Tags oder Freitextfelder eingeben, die für Namen verwendet werden,

können für Abrechnungs- oder Diagnoseprotokolle verwendet werden. Wenn Sie eine URL für einen externen Server bereitstellen, empfehlen wir dringend, keine Anmeldeinformationen zur Validierung Ihrer Anforderung an den betreffenden Server in die URL einzuschließen.

Verschlüsselung im Ruhezustand

Amazon Kendra verschlüsselt Ihre Daten im Ruhezustand mit einem Verschlüsselungsschlüssel Ihrer Wahl. Sie können eine der folgenden Optionen auswählen:

- Ein AWS eigener KMS-Schlüssel AWS . Wenn Sie keinen Verschlüsselungsschlüssel angeben, werden Ihre Daten standardmäßig mit diesem Schlüssel verschlüsselt.
- Ein AWS verwalteter KMS-Schlüssel in Ihrem Konto. Dieser Schlüssel wird in Ihrem Namen von Amazon Kendra erstellt, verwaltet und verwendet. Der Schlüsselname lautet`aws/kendra`.
- Ein vom Kunden verwalteter Schlüssel. Sie können den ARN eines Verschlüsselungsschlüssels angeben, den Sie in Ihrem Konto erstellt haben. Wenn Sie einen vom Kunden verwalteten KMS-Schlüssel verwenden, müssen Sie dem Schlüssel eine Schlüsselrichtlinie zuweisen, die Amazon Kendra die Verwendung des Schlüssels ermöglicht. Wählen Sie einen vom Kunden verwalteten KMS-Schlüssel mit symmetrischer Verschlüsselung aus. Amazon Kendra unterstützt keine asymmetrischen KMS-Schlüssel. Weitere Informationen finden Sie unter Schlüsselverwaltung.

Verschlüsselung während der Übertragung

Amazon Kendra verwendet das HTTPS-Protokoll, um mit Ihrer Client-Anwendung zu kommunizieren. Es verwendet HTTPS und AWS Signaturen, um im Namen Ihrer Anwendung mit anderen Diensten zu kommunizieren. Wenn Sie eine VPC verwenden, können Sie AWS PrivateLink damit eine private Verbindung zwischen Ihrer VPC und Amazon Kendra herstellen.

Schlüsselverwaltung

Amazon Kendra verschlüsselt den Inhalt Ihres Indexes mit einem von drei Schlüsseltypen. Sie können eine der folgenden Optionen auswählen:

- Ein eigener AWS KMS. AWS Dies ist die Standardeinstellung.
- Ein AWS-verwalteter KMS-Schlüssel. Dieser Schlüssel wird in Ihrem Konto erstellt und in Ihrem Namen von Amazon Kendra verwaltet und verwendet.
- Ein vom Kunden verwalteter KMS-Schlüssel. Sie können den Schlüssel erstellen, wenn Sie einen Amazon Kendra Kendra-Index oder eine Datenquelle erstellen, oder Sie können den

Schlüssel mithilfe der AWS KMS Konsole erstellen. Wählen Sie einen vom Kunden verwalteten KMS-Schlüssel mit symmetrischer Verschlüsselung aus. Amazon Kendra unterstützt keine asymmetrischen KMS-Schlüssel. Weitere Informationen finden Sie unter Verwenden von symmetrischen und asymmetrischen Schlüsseln im Entwicklerhandbuch für AWS Key Management Service.

Amazon Kendra Amazon Kendra Intelligentes Ranking und Schnittstelle für VPC-Endpunkte ()AWS PrivateLink

Sie können eine private Verbindung zwischen Ihrer VPC und Amazon Kendra herstellen, indem Sie einen VPC-Schnittstellen-Endpunkt erstellen. Schnittstellenendpunkte werden von einer Technologie unterstützt AWS PrivateLink, mit der Sie privat auf Amazon Kendra Kendra-APIs zugreifen können, ohne ein Internet-Gateway, ein NAT-Gerät, eine VPN-Verbindung oder eine AWS Direct Connect-Verbindung zu benötigen. Instances in Ihrer VPC benötigen keine öffentlichen IP-Adressen, um mit Amazon Kendra APIs zu kommunizieren. Der Verkehr zwischen Ihrer VPC und Amazon Kendra verlässt das Amazon-Netzwerk nicht.

Jeder Schnittstellenendpunkt wird durch eine oder mehrere Elastic-Network-Schnittstellen in Ihren Subnetzen dargestellt.

Überlegungen zu Amazon Kendra und Amazon Kendra Intelligent Ranking VPC-Endpunkten

Bevor Sie einen VPC-Schnittstellen-Endpunkt für Amazon Kendra oder Amazon Kendra Intelligent Ranking einrichten, stellen Sie sicher, dass Sie die Voraussetzungen im Amazon VPC-Benutzerhandbuch lesen.

Amazon Kendra und Amazon Kendra Intelligent Ranking unterstützen Aufrufe aller API-Aktionen von Ihrer VPC aus.

Erstellen eines Schnittstellen-VPC-Endpunkts für Amazon Kendra und Amazon Kendra Intelligent Ranking

Sie können einen VPC-Endpunkt für den Amazon Kendra- oder Amazon Kendra Intelligent Ranking-Service entweder mit der Amazon VPC-Konsole oder mit () erstellen. AWS Command Line Interface AWS CLI

Erstellen Sie einen VPC-Endpunkt für Amazon Kendra mit dem folgenden Servicenamen:

- com.amazonaws.*region*.kendra

Erstellen Sie einen VPC-Endpunkt für Amazon Kendra Intelligent Ranking mit dem folgenden Servicenamen:

- aws.api.*region*.kendra-ranking

Nachdem Sie einen VPC-Endpunkt erstellt haben, können Sie den folgenden AWS CLI Beispielbefehl verwenden, der den `endpoint-url` Parameter verwendet, um einen Schnittstellenendpunkt zur Amazon Kendra API anzugeben:

```
aws kendra list-indices --endpoint-url https://VPC endpoint
```

VPC-Endpunkt ist der DNS-Name, der bei der Erstellung des Schnittstellenendpunkts generiert wird. Dieser Name umfasst die VPC-Endpunkt-ID und den Amazon Kendra-Servicenamen, der die Region einschließt. z. B. `vpce-1234-abcdef.kendra.us-west-2.vpce.amazonaws.com`.

Wenn Sie privates DNS für den Endpunkt aktivieren, können Sie API-Anfragen an Amazon Kendra stellen, indem Sie den Standard-DNS-Namen für die Region verwenden. z. B. `kendra.us-east-1.amazonaws.com`.

Weitere Informationen finden Sie unter Erstellung eines Schnittstellenendpunkts im Benutzerhandbuch für Amazon VPC.

Erstellen einer VPC-Endpunktrichtlinie für Amazon Kendra und Amazon Kendra Intelligent Ranking

Sie können Ihrem VPC-Endpunkt eine Endpunktrichtlinie hinzufügen, die den Zugriff auf Amazon Kendra oder Amazon Kendra Intelligent Ranking steuert.

Die Richtlinie für Amazon Kendra oder Amazon Kendra Intelligent Ranking spezifiziert die folgenden Informationen:

- Der Haupt-/autorisierte Benutzer, der Aktionen ausführen kann.
- Aktionen, die ausgeführt werden können
- Die Ressourcen, für die Aktionen ausgeführt werden können.

Beispiel: VPC-Endpunktrichtlinie für Amazon Kendra Kendra-Aktionen

Im Folgenden finden Sie ein Beispiel für eine Endpunktrichtlinie für Amazon Kendra. Wenn diese Richtlinie an einen Endpunkt angehängt ist, gewährt sie allen Prinzipalen/autorisierten Benutzern auf allen Ressourcen Zugriff auf alle verfügbaren Amazon Kendra Kendra-Aktionen.

```
{
   "Statement":[
      {
         "Principal":"*",
         "Effect":"Allow",
         "Action":[
            "kendra:*"
         ],
         "Resource":"*"
      }
   ]
}
```

Beispiel: VPC-Endpunktrichtlinie für Amazon Kendra Intelligent Ranking-Aktionen

Im Folgenden finden Sie ein Beispiel für eine Endpunktrichtlinie für Amazon Kendra Intelligent Ranking. Wenn diese Richtlinie an einen Endpunkt angehängt ist, gewährt sie allen Prinzipalen/autorisierten Benutzern auf allen Ressourcen Zugriff auf alle verfügbaren Amazon Kendra Intelligent Ranking-Aktionen.

```
{
   "Statement":[
      {
         "Principal":"*",
         "Effect":"Allow",
         "Action":[
            "kendra-ranking:*"
         ],
         "Resource":"*"
      }
   ]
}
```

Weitere Informationen finden Sie unter Steuern des Zugriffs auf VPC-Endpunkte mithilfe von Endpunktrichtlinien im Amazon VPC-Benutzerhandbuch.

Identitäts- und Zugriffsmanagement für Amazon Kendra

AWS Identity and Access Management (IAM) hilft einem Administrator AWS-Service , den Zugriff auf Ressourcen sicher zu kontrollieren. AWS IAM-Administratoren kontrollieren, wer authentifiziert (angemeldet) und autorisiert werden kann (über Berechtigungen verfügt), um Amazon Kendra Kendra-Ressourcen zu verwenden. IAM ist ein Programm AWS-Service , das Sie ohne zusätzliche Kosten nutzen können.

Themen

Zielgruppe

Wie Sie AWS Identity and Access Management (IAM) verwenden, hängt von der Arbeit ab, die Sie in Amazon Kendra ausführen.

Servicebenutzer — Wenn Sie den Amazon Kendra Kendra-Service für Ihre Arbeit verwenden, stellt Ihnen Ihr Administrator die Anmeldeinformationen und Berechtigungen zur Verfügung, die Sie benötigen. Da Sie für Ihre Arbeit mehr Funktionen von Amazon Kendra verwenden, benötigen Sie möglicherweise zusätzliche Berechtigungen. Wenn Sie die Fuktionsweise der Zugriffskontrolle nachvollziehen, wissen Sie bereits, welche Berechtigungen Sie von Ihrem Administrator anzufordern müssen. Wenn Sie auf eine Funktion in Amazon Kendra nicht zugreifen können, finden Sie weitere Informationen unterFehlerbehebung bei Amazon Kendra Identity and Access.

Service-Administrator — Wenn Sie in Ihrem Unternehmen für die Amazon Kendra-Ressourcen verantwortlich sind, haben Sie wahrscheinlich vollen Zugriff auf Amazon Kendra. Es ist Ihre Aufgabe, zu bestimmen, auf welche Funktionen und Ressourcen von Amazon Kendra Ihre Servicebenutzer zugreifen sollen. Sie müssen dann Anträge an Ihren IAM-Administrator stellen, um die Berechtigungen Ihrer Servicenutzer zu ändern. Lesen Sie die Informationen auf dieser Seite, um

die Grundkonzepte von IAM nachzuvollziehen. Weitere Informationen darüber, wie Ihr Unternehmen IAM mit Amazon Kendra verwenden kann, finden Sie unter. So arbeitet Amazon Kendra mit IAM

IAM-Administrator — Wenn Sie ein IAM-Administrator sind, möchten Sie vielleicht mehr darüber erfahren, wie Sie Richtlinien schreiben können, um den Zugriff auf Amazon Kendra zu verwalten. Beispiele für identitätsbasierte Amazon Kendra-Richtlinien, die Sie in IAM verwenden können, finden Sie unter. Beispiele für identitätsbasierte Richtlinien in Amazon Kendra

Authentifizierung mit Identitäten

Authentifizierung ist die Art und Weise, wie Sie sich AWS mit Ihren Identitätsdaten anmelden. Sie müssen als IAM-Benutzer authentifiziert (angemeldet AWS) sein oder eine IAM-Rolle annehmen. Root-Benutzer des AWS-Kontos

Sie können sich AWS als föderierte Identität anmelden, indem Sie Anmeldeinformationen verwenden, die über eine Identitätsquelle bereitgestellt wurden. AWS IAM Identity Center (IAM Identity Center) -Benutzer, die Single Sign-On-Authentifizierung Ihres Unternehmens und Ihre Google- oder Facebook-Anmeldeinformationen sind Beispiele für föderierte Identitäten. Wenn Sie sich als Verbundidentität anmelden, hat der Administrator vorher mithilfe von IAM-Rollen einen Identitätsverbund eingerichtet. Wenn Sie über den Verbund darauf zugreifen AWS , übernehmen Sie indirekt eine Rolle.

Je nachdem, welcher Benutzertyp Sie sind, können Sie sich beim AWS Management Console oder beim AWS Zugangsportal anmelden. Weitere Informationen zur Anmeldung finden Sie AWS unter So melden Sie sich bei Ihrem an AWS-Konto im AWS-Anmeldung Benutzerhandbuch.

Wenn Sie AWS programmgesteuert darauf zugreifen, AWS stellt es ein Software Development Kit (SDK) und eine Befehlszeilenschnittstelle (CLI) bereit, um Ihre Anfragen mithilfe Ihrer Anmeldeinformationen kryptografisch zu signieren. Wenn Sie keine AWS Tools verwenden, müssen Sie Anfragen selbst signieren. Weitere Informationen zur Verwendung der empfohlenen Methode, um Anfragen selbst zu signieren, finden Sie im IAM-Benutzerhandbuch unter AWS API-Anfragen signieren.

Unabhängig von der verwendeten Authentifizierungsmethode müssen Sie möglicherweise zusätzliche Sicherheitsinformationen angeben. AWS Empfiehlt beispielsweise, die Multi-Faktor-Authentifizierung (MFA) zu verwenden, um die Sicherheit Ihres Kontos zu erhöhen. Weitere Informationen finden Sie unter Multi-Faktor-Authentifizierung im AWS IAM Identity Center - Benutzerhandbuch und Verwenden der Multi-Faktor-Authentifizierung (MFA) in AWS im IAM-Benutzerhandbuch.

AWS-Konto Root-Benutzer

Wenn Sie einen erstellen AWS-Konto, beginnen Sie mit einer Anmeldeidentität, die vollständigen Zugriff auf alle AWS-Services Ressourcen im Konto hat. Diese Identität wird als AWS-Konto Root-Benutzer bezeichnet. Sie können darauf zugreifen, indem Sie sich mit der E-Mail-Adresse und dem Passwort anmelden, mit denen Sie das Konto erstellt haben. Wir raten ausdrücklich davon ab, den Root-Benutzer für Alltagsaufgaben zu verwenden. Schützen Sie Ihre Root-Benutzer-Anmeldeinformationen und verwenden Sie diese, um die Aufgaben auszuführen, die nur der Root-Benutzer ausführen kann. Eine vollständige Liste der Aufgaben, für die Sie sich als Root-Benutzer anmelden müssen, finden Sie unter Aufgaben, die Root-Benutzer-Anmeldeinformationen erfordern im IAM-Benutzerhandbuch.

IAM-Benutzer und -Gruppen

Ein IAM-Benutzer ist eine Identität innerhalb von Ihnen AWS-Konto , die über spezifische Berechtigungen für eine einzelne Person oder Anwendung verfügt. Wenn möglich, empfehlen wir, temporäre Anmeldeinformationen zu verwenden, anstatt IAM-Benutzer zu erstellen, die langfristige Anmeldeinformationen wie Passwörter und Zugriffsschlüssel haben. Bei speziellen Anwendungsfällen, die langfristige Anmeldeinformationen mit IAM-Benutzern erfordern, empfehlen wir jedoch, die Zugriffsschlüssel zu rotieren. Weitere Informationen finden Sie unter Regelmäßiges Rotieren von Zugriffsschlüsseln für Anwendungsfälle, die langfristige Anmeldeinformationen erfordern im IAM-Benutzerhandbuch.

Eine IAM-Gruppe ist eine Identität, die eine Sammlung von IAM-Benutzern angibt. Sie können sich nicht als Gruppe anmelden. Mithilfe von Gruppen können Sie Berechtigungen für mehrere Benutzer gleichzeitig angeben. Gruppen vereinfachen die Verwaltung von Berechtigungen, wenn es zahlreiche Benutzer gibt. Sie könnten beispielsweise einer Gruppe mit dem Namen IAMAdmins Berechtigungen zum Verwalten von IAM-Ressourcen erteilen.

Benutzer unterscheiden sich von Rollen. Ein Benutzer ist einer einzigen Person oder Anwendung eindeutig zugeordnet. Eine Rolle kann von allen Personen angenommen werden, die sie benötigen. Benutzer besitzen dauerhafte Anmeldeinformationen. Rollen stellen temporäre Anmeldeinformationen bereit. Weitere Informationen finden Sie unter Erstellen eines IAM-Benutzers (anstatt einer Rolle) im IAM-Benutzerhandbuch.

IAM-Rollen

Eine IAM-Rolle ist eine Identität innerhalb Ihres Unternehmens AWS-Konto , die über bestimmte Berechtigungen verfügt. Sie ist einem IAM-Benutzer vergleichbar, ist aber nicht mit einer bestimmten

Person verknüpft. Sie können vorübergehend eine IAM-Rolle in der übernehmen, AWS Management Console indem Sie die Rollen wechseln. Sie können eine Rolle übernehmen, indem Sie eine AWS CLI oder AWS API-Operation aufrufen oder eine benutzerdefinierte URL verwenden. Weitere Informationen zu Methoden für die Verwendung von Rollen finden Sie unter Verwenden von IAM-Rollen im IAM-Benutzerhandbuch.

IAM-Rollen mit temporären Anmeldeinformationen sind in folgenden Situationen hilfreich:

- Verbundbenutzerzugriff – Um einer Verbundidentität Berechtigungen zuzuweisen, erstellen Sie eine Rolle und definieren Berechtigungen für die Rolle. Wird eine Verbundidentität authentifiziert, so wird die Identität der Rolle zugeordnet und erhält die von der Rolle definierten Berechtigungen. Informationen zu Rollen für den Verbund finden Sie unter Erstellen von Rollen für externe Identitätsanbieter im IAM-Benutzerhandbuch. Wenn Sie IAM Identity Center verwenden, konfigurieren Sie einen Berechtigungssatz. Wenn Sie steuern möchten, worauf Ihre Identitäten nach der Authentifizierung zugreifen können, korreliert IAM Identity Center den Berechtigungssatz mit einer Rolle in IAM. Informationen zu Berechtigungssätzen finden Sie unter Berechtigungssätze im AWS IAM Identity Center -Benutzerhandbuch.
- Temporäre IAM-Benutzerberechtigungen – Ein IAM-Benutzer oder eine -Rolle kann eine IAM-Rolle übernehmen, um vorübergehend andere Berechtigungen für eine bestimmte Aufgabe zu erhalten.
- Kontoübergreifender Zugriff – Sie können eine IAM-Rolle verwenden, um einem vertrauenswürdigen Prinzipal in einem anderen Konto den Zugriff auf Ressourcen in Ihrem Konto zu ermöglichen. Rollen stellen die primäre Möglichkeit dar, um kontoübergreifendem Zugriff zu gewähren. Bei einigen können Sie AWS-Services jedoch eine Richtlinie direkt an eine Ressource anhängen (anstatt eine Rolle als Proxy zu verwenden). Informationen zu den Unterschieden zwischen Rollen und ressourcenbasierten Richtlinien für den kontoübergreifenden Zugriff finden Sie unter So unterscheiden sich IAM-Rollen von ressourcenbasierten Richtlinien im IAM-Benutzerhandbuch.
- Serviceübergreifender Zugriff — Einige AWS-Services verwenden Funktionen in anderen AWS-Services. Wenn Sie beispielsweise einen Aufruf in einem Service tätigen, führt dieser Service häufig Anwendungen in Amazon-EC2 aus oder speichert Objekte in Amazon-S3. Ein Dienst kann dies mit den Berechtigungen des aufrufenden Prinzipals mit einer Servicerolle oder mit einer serviceverknüpften Rolle tun.
  - Forward Access Sessions (FAS) — Wenn Sie einen IAM-Benutzer oder eine IAM-Rolle verwenden, um Aktionen auszuführen AWS, gelten Sie als Principal. Bei einigen Diensten könnte es Aktionen geben, die dann eine andere Aktion in einem anderen Service initiieren. FAS verwendet die Berechtigungen des Prinzipals, der einen aufruft AWS-Service, in Kombination

mit der Anfrage, Anfragen an AWS-Service nachgelagerte Dienste zu stellen. FAS-Anfragen werden nur gestellt, wenn ein Dienst eine Anfrage erhält, für deren Abschluss Interaktionen mit anderen AWS-Services oder Ressourcen erforderlich sind. In diesem Fall müssen Sie über Berechtigungen zum Ausführen beider Aktionen verfügen. Einzelheiten zu den Richtlinien für FAS-Anfragen finden Sie unter Zugriffssitzungen weiterleiten.

- Servicerolle – Eine Servicerolle ist eine IAM-Rolle, die ein Service übernimmt, um Aktionen in Ihrem Namen auszuführen. Ein IAM-Administrator kann eine Servicerolle innerhalb von IAM erstellen, ändern und löschen. Weitere Informationen finden Sie unter Erstellen einer Rolle zum Delegieren von Berechtigungen an einen AWS-Service im IAM-Benutzerhandbuch.
- Dienstbezogene Rolle — Eine dienstbezogene Rolle ist eine Art von Servicerolle, die mit einer verknüpft ist. AWS-Service Der Service kann die Rolle übernehmen, um eine Aktion in Ihrem Namen auszuführen. Servicebezogene Rollen erscheinen in Ihrem Dienst AWS-Konto und gehören dem Dienst. Ein IAM-Administrator kann die Berechtigungen für Service-verknüpfte Rollen anzeigen, aber nicht bearbeiten.

- Auf Amazon EC2 ausgeführte Anwendungen — Sie können eine IAM-Rolle verwenden, um temporäre Anmeldeinformationen für Anwendungen zu verwalten, die auf einer EC2-Instance ausgeführt werden und API-Anfragen stellen AWS CLI . AWS Das ist eher zu empfehlen, als Zugriffsschlüssel innerhalb der EC2-Instance zu speichern. Um einer EC2-Instance eine AWS Rolle zuzuweisen und sie allen ihren Anwendungen zur Verfügung zu stellen, erstellen Sie ein Instance-Profil, das an die Instance angehängt ist. Ein Instance-Profil enthält die Rolle und ermöglicht, dass Programme, die in der EC2-Instance ausgeführt werden, temporäre Anmeldeinformationen erhalten. Weitere Informationen finden Sie unter Verwenden einer IAM-Rolle zum Erteilen von Berechtigungen für Anwendungen, die auf Amazon-EC2-Instances ausgeführt werden im IAM-Benutzerhandbuch.

Informationen dazu, wann Sie IAM-Rollen oder IAM-Benutzer verwenden sollten, finden Sie unter Erstellen einer IAM-Rolle (anstatt eines Benutzers) im IAM-Benutzerhandbuch.

Verwalten des Zugriffs mit Richtlinien

Sie kontrollieren den Zugriff, AWS indem Sie Richtlinien erstellen und diese an AWS Identitäten oder Ressourcen anhängen. Eine Richtlinie ist ein Objekt, AWS das, wenn es einer Identität oder Ressource zugeordnet ist, deren Berechtigungen definiert. AWS wertet diese Richtlinien aus, wenn ein Prinzipal (Benutzer, Root-Benutzer oder Rollensitzung) eine Anfrage stellt. Berechtigungen in den Richtlinien bestimmen, ob die Anforderung zugelassen oder abgelehnt wird. Die meisten Richtlinien werden AWS als JSON-Dokumente gespeichert. Weitere Informationen zu Struktur und

Inhalten von JSON-Richtliniendokumenten finden Sie unter Übersicht über JSON-Richtlinien im IAM-Benutzerhandbuch.

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer auf was Zugriff hat. Das bedeutet, welcher Prinzipal kann Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen.

Standardmäßig haben Benutzer, Gruppen und Rollen keine Berechtigungen. Ein IAM-Administrator muss IAM-Richtlinien erstellen, die Benutzern die Berechtigung erteilen, Aktionen für die Ressourcen auszuführen, die sie benötigen. Der Administrator kann dann die IAM-Richtlinien zu Rollen hinzufügen, und Benutzer können die Rollen annehmen.

IAM-Richtlinien definieren Berechtigungen für eine Aktion unabhängig von der Methode, die Sie zur Ausführung der Aktion verwenden. Angenommen, es gibt eine Richtlinie, die Berechtigungen für die `iam:GetRole`-Aktion erteilt. Ein Benutzer mit dieser Richtlinie kann Rolleninformationen von der AWS Management Console AWS CLI, der oder der AWS API abrufen.

Identitätsbasierte Richtlinien

Identitätsbasierte Richtlinien sind JSON-Berechtigungsrichtliniendokumente, die Sie einer Identität anfügen können, wie z. B. IAM-Benutzern, -Benutzergruppen oder -Rollen. Diese Richtlinien steuern, welche Aktionen die Benutzer und Rollen für welche Ressourcen und unter welchen Bedingungen ausführen können. Informationen zum Erstellen identitätsbasierter Richtlinien finden Sie unter Erstellen von IAM-Richtlinien im IAM-Benutzerhandbuch.

Identitätsbasierte Richtlinien können weiter als Inline-Richtlinien oder verwaltete Richtlinien kategorisiert werden. Inline-Richtlinien sind direkt in einen einzelnen Benutzer, eine einzelne Gruppe oder eine einzelne Rolle eingebettet. Verwaltete Richtlinien sind eigenständige Richtlinien, die Sie mehreren Benutzern, Gruppen und Rollen in Ihrem System zuordnen können AWS-Konto. Zu den verwalteten Richtlinien gehören AWS verwaltete Richtlinien und vom Kunden verwaltete Richtlinien. Informationen dazu, wie Sie zwischen einer verwalteten Richtlinie und einer eingebundenen Richtlinie wählen, finden Sie unter Auswahl zwischen verwalteten und eingebundenen Richtlinien im IAM-Benutzerhandbuch.

Ressourcenbasierte Richtlinien

Ressourcenbasierte Richtlinien sind JSON-Richtliniendokumente, die Sie an eine Ressource anfügen. Beispiele für ressourcenbasierte Richtlinien sind IAM-Rollen-Vertrauensrichtlinien und Amazon-S3-Bucket-Richtlinien. In Services, die ressourcenbasierte Richtlinien unterstützen, können Service-Administratoren sie verwenden, um den Zugriff auf eine bestimmte Ressource zu steuern.

Für die Ressource, an welche die Richtlinie angehängt ist, legt die Richtlinie fest, welche Aktionen ein bestimmter Prinzipal unter welchen Bedingungen für diese Ressource ausführen kann. Sie müssen in einer ressourcenbasierten Richtlinie einen Prinzipal angeben. Zu den Prinzipalen können Konten, Benutzer, Rollen, Verbundbenutzer oder gehören. AWS-Services

Ressourcenbasierte Richtlinien sind Richtlinien innerhalb dieses Diensts. Sie können AWS verwaltete Richtlinien von IAM nicht in einer ressourcenbasierten Richtlinie verwenden.

Zugriffssteuerungslisten (ACLs)

Zugriffssteuerungslisten (ACLs) steuern, welche Prinzipale (Kontomitglieder, Benutzer oder Rollen) auf eine Ressource zugreifen können. ACLs sind ähnlich wie ressourcenbasierte Richtlinien, verwenden jedoch nicht das JSON-Richtliniendokumentformat.

Amazon S3 und Amazon VPC sind Beispiele für Services, die ACLs unterstützen. AWS WAF Weitere Informationen“ zu ACLs finden Sie unter Zugriffskontrollliste (ACL) – Übersicht (Access Control List) im Amazon-Simple-Storage-Service-Entwicklerhandbuch.

Weitere Richtlinientypen

AWS unterstützt zusätzliche, weniger verbreitete Richtlinientypen. Diese Richtlinientypen können die maximalen Berechtigungen festlegen, die Ihnen von den häufiger verwendeten Richtlinientypen erteilt werden können.

- Berechtigungsgrenzen – Eine Berechtigungsgrenze ist ein erweitertes Feature, mit der Sie die maximalen Berechtigungen festlegen können, die eine identitätsbasierte Richtlinie einer IAM-Entität (IAM-Benutzer oder -Rolle) erteilen kann. Sie können eine Berechtigungsgrenze für eine Entität festlegen. Die daraus resultierenden Berechtigungen sind der Schnittpunkt der identitätsbasierten Richtlinien einer Entität und ihrer Berechtigungsgrenzen. Ressourcenbasierte Richtlinien, die den Benutzer oder die Rolle im Feld `Principal` angeben, werden nicht durch Berechtigungsgrenzen eingeschränkt. Eine explizite Zugriffsverweigerung in einer dieser Richtlinien setzt eine Zugriffserlaubnis außer Kraft. Weitere Informationen über Berechtigungsgrenzen finden Sie unter Berechtigungsgrenzen für IAM-Entitäten im IAM-Benutzerhandbuch.
- Service Control Policies (SCPs) — SCPs sind JSON-Richtlinien, die die maximalen Berechtigungen für eine Organisation oder Organisationseinheit (OU) in festlegen. AWS Organizations AWS Organizations ist ein Dienst zur Gruppierung und zentralen Verwaltung mehrerer Objekte AWS-Konten , die Ihrem Unternehmen gehören. Wenn Sie innerhalb einer Organisation alle Features aktivieren, können Sie Service-Kontrollrichtlinien (SCPs) auf alle oder einzelne Ihrer Konten anwenden. Das SCP schränkt die Berechtigungen für Entitäten in

Mitgliedskonten ein, einschließlich der einzelnen Entitäten. Root-Benutzer des AWS-Kontos Weitere Informationen zu Organizations und SCPs finden Sie unter Funktionsweise von SCPs im AWS Organizations -Benutzerhandbuch.

- Sitzungsrichtlinien – Sitzungsrichtlinien sind erweiterte Richtlinien, die Sie als Parameter übergeben, wenn Sie eine temporäre Sitzung für eine Rolle oder einen verbundenen Benutzer programmgesteuert erstellen. Die resultierenden Sitzungsberechtigungen sind eine Schnittmenge der auf der Identität des Benutzers oder der Rolle basierenden Richtlinien und der Sitzungsrichtlinien. Berechtigungen können auch aus einer ressourcenbasierten Richtlinie stammen. Eine explizite Zugriffsverweigerung in einer dieser Richtlinien setzt eine Zugriffserlaubnis außer Kraft. Weitere Informationen finden Sie unter Sitzungsrichtlinien im IAM-Benutzerhandbuch.

Mehrere Richtlinientypen

Wenn mehrere auf eine Anforderung mehrere Richtlinientypen angewendet werden können, sind die entsprechenden Berechtigungen komplizierter. Informationen darüber, wie AWS bestimmt wird, ob eine Anfrage zulässig ist, wenn mehrere Richtlinientypen betroffen sind, finden Sie im IAM-Benutzerhandbuch unter Bewertungslogik für Richtlinien.

So arbeitet Amazon Kendra mit IAM

Bevor Sie IAM verwenden, um den Zugriff auf Amazon Kendra zu verwalten, sollten Sie wissen, welche IAM-Funktionen für Amazon Kendra verfügbar sind. Einen allgemeinen Überblick darüber, wie Amazon Kendra und andere AWS Services mit IAM zusammenarbeiten, finden Sie unter AWS Services That Work with IAM im IAM-Benutzerhandbuch.

Themen

- Identitätsbasierte Richtlinien von Amazon Kendra
- Ressourcenbasierte Richtlinien von Amazon Kendra
- Zugriffssteuerungslisten (ACLs)
- Autorisierung basierend auf Amazon Kendra Kendra-Tags
- Amazon Kendra IAM-Rollen

Identitätsbasierte Richtlinien von Amazon Kendra

Mit identitätsbasierten IAM-Richtlinien können Sie angeben, welche Aktionen und Ressourcen zugelassen oder abgelehnt werden. Darüber hinaus können Sie die Bedingungen festlegen, unter

denen Aktionen zugelassen oder abgelehnt werden. Amazon Kendra unterstützt bestimmte Aktionen, Ressourcen und Bedingungsschlüssel. Informationen zu sämtlichen Elementen, die Sie in einer JSON-Richtlinie verwenden, finden Sie in der IAM-Referenz für JSON-Richtlinienelemente im IAM-Benutzerhandbuch.

Aktionen

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer Zugriff auf was hat. Das heißt, welcher Prinzipal kann Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen.

Das Element `Action` einer JSON-Richtlinie beschreibt die Aktionen, mit denen Sie den Zugriff in einer Richtlinie zulassen oder verweigern können. Richtlinienaktionen haben normalerweise denselben Namen wie der zugehörige AWS API-Vorgang. Es gibt einige Ausnahmen, z. B. Aktionen, die nur mit Genehmigung durchgeführt werden können und für die es keine passende API-Operation gibt. Es gibt auch einige Operationen, die mehrere Aktionen in einer Richtlinie erfordern. Diese zusätzlichen Aktionen werden als abhängige Aktionen bezeichnet.

Schließen Sie Aktionen in eine Richtlinie ein, um Berechtigungen zur Durchführung der zugeordneten Operation zu erteilen.

Richtlinienaktionen in Amazon Kendra verwenden das folgende Präfix vor der Aktion:`kendra:`. Um beispielsweise jemandem die Erlaubnis zu erteilen, Amazon Kendra Kendra-Indizes mit der ListIndicesAPI-Operation aufzulisten, nehmen Sie die `kendra:ListIndices` Aktion in seine Richtlinie auf. Richtlinienanweisungen müssen entweder ein – `Action`oder ein `NotAction`-Element enthalten. Amazon Kendra definiert eigene Aktionen, die Aufgaben beschreiben, die Sie mit diesem Service ausführen können.

Um mehrere Aktionen in einer einzigen Anweisung anzugeben, trennen Sie sie wie folgt durch Kommata:

```
"Action": [
      "kendra:action1",
      "kendra:action2"
```

Sie können auch Platzhalter verwenden, um mehrere Aktionen anzugeben. Beispielsweise können Sie alle Aktionen festlegen, die mit dem Wort `Describe` beginnen, einschließlich der folgenden Aktion:

```
"Action": "kendra:Describe*"
```

Eine Liste der Amazon Kendra-Aktionen finden Sie unter Von Amazon Kendra definierte Aktionen im IAM-Benutzerhandbuch.

Ressourcen

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer Zugriff auf was hat. Das bedeutet die Festlegung, welcher Prinzipal Aktionen für welche Ressourcen unter welchen Bedingungen ausführen kann.

Das JSON-Richtlinienelement `Resource` gibt die Objekte an, auf welche die Aktion angewendet wird. Anweisungen müssen entweder ein – `Resource`oder ein `NotResource`-Element enthalten. Als bewährte Methode geben Sie eine Ressource mit dem zugehörigen Amazon-Ressourcennamen (ARN) an. Sie können dies für Aktionen tun, die einen bestimmten Ressourcentyp unterstützen, der als Berechtigungen auf Ressourcenebene bezeichnet wird.

Verwenden Sie für Aktionen, die keine Berechtigungen auf Ressourcenebene unterstützen, z. B. Auflistungsoperationen, einen Platzhalter (*), um anzugeben, dass die Anweisung für alle Ressourcen gilt.

```
"Resource": "*"
```

Die Amazon Kendra Kendra-Indexressource hat den folgenden ARN:

```
arn:${Partition}:kendra:${Region}:${Account}:index/${IndexId}
```

Weitere Informationen zum Format von ARNs finden Sie unter Amazon Resource Names (ARNs) und AWS Service Namespaces.

Um beispielsweise einen Index in Ihrer Anweisung anzugeben, verwenden Sie die GUID des Indexes im folgenden ARN:

```
"Resource": "arn:aws:kendra:${Region}:${Account}:index/${GUID}"
```

Um alle Indizes anzugeben, die zu einem bestimmten Konto gehören, verwenden Sie den Platzhalter (*):

```
"Resource": "arn:aws:${Region}:${Account}:index/*"
```

Einige Amazon Kendra Kendra-Aktionen, z. B. zum Erstellen von Ressourcen, können nicht für eine bestimmte Ressource ausgeführt werden. In diesen Fällen müssen Sie den Platzhalter (*) verwenden.

```
"Resource": "*"
```

Eine Liste der Amazon Kendra-Ressourcentypen und ihrer ARNs finden Sie unter Von Amazon Kendra definierte Ressourcen im IAM-Benutzerhandbuch. Informationen darüber, mit welchen Aktionen Sie den ARN jeder Ressource angeben können, finden Sie unter Von Amazon Kendra definierte Aktionen.

Bedingungsschlüssel

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer Zugriff auf was hat. Das heißt, welcher Prinzipal kann Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen.

Das Element `Condition` (oder `Condition` block) ermöglicht Ihnen die Angabe der Bedingungen, unter denen eine Anweisung wirksam ist. Das Element `Condition` ist optional. Sie können bedingte Ausdrücke erstellen, die Bedingungsoperatoren verwenden, z. B. ist gleich oder kleiner als, damit die Bedingung in der Richtlinie mit Werten in der Anforderung übereinstimmt.

Wenn Sie mehrere `Condition`-Elemente in einer Anweisung oder mehrere Schlüssel in einem einzelnen `Condition`-Element angeben, wertet AWS diese mittels einer logischen `AND`-Operation aus. Wenn Sie mehrere Werte für einen einzelnen Bedingungsschlüssel angeben, AWS wertet die Bedingung mithilfe einer logischen `OR` Operation aus. Alle Bedingungen müssen erfüllt werden, bevor die Berechtigungen der Anweisung gewährt werden.

Sie können auch Platzhaltervariablen verwenden, wenn Sie Bedingungen angeben. Beispielsweise können Sie einem IAM-Benutzer die Berechtigung für den Zugriff auf eine Ressource nur dann gewähren, wenn sie mit dessen IAM-Benutzernamen gekennzeichnet ist. Weitere Informationen finden Sie unter IAM-Richtlinienelemente: Variablen und Tags im IAM-Benutzerhandbuch.

AWS unterstützt globale Bedingungsschlüssel und dienstspezifische Bedingungsschlüssel. Eine Übersicht aller AWS globalen Bedingungsschlüssel finden Sie unter Kontextschlüssel für AWS globale Bedingungen im IAM-Benutzerhandbuch.

Amazon Kendra stellt keine dienstspezifischen Bedingungsschlüssel bereit, unterstützt jedoch die Verwendung einiger globaler Bedingungsschlüssel. Eine Übersicht aller AWS globalen

Bedingungsschlüssel finden Sie unter AWS Globale Bedingungskontextschlüssel im IAM-Benutzerhandbuch.

Beispiele

Beispiele für identitätsbasierte Richtlinien von Amazon Kendra finden Sie unter. Beispiele für identitätsbasierte Richtlinien in Amazon Kendra

Ressourcenbasierte Richtlinien von Amazon Kendra

Amazon Kendra unterstützt keine ressourcenbasierten Richtlinien.

Zugriffssteuerungslisten (ACLs)

Amazon Kendra unterstützt keine Zugriffskontrolllisten (ACLs) für den Zugriff auf AWS Dienste und Ressourcen.

Autorisierung basierend auf Amazon Kendra Kendra-Tags

Sie können Tags mit bestimmten Arten von Amazon Kendra Kendra-Ressourcen verknüpfen, um den Zugriff auf diese Ressourcen zu autorisieren. Um den Zugriff anhand von Tags zu steuern, geben Sie Tag-Informationen im Bedingungselement einer Richtlinie an`aws:RequestTag/`*`key-name`*, indem Sie die `aws:TagKeys` Bedingungstasten oder verwenden.

In der folgenden Tabelle sind die Aktionen, die entsprechenden Ressourcentypen und Bedingungsschlüssel für die Tag-basierte Zugriffskontrolle aufgeführt. Jede Aktion wird basierend auf den Tags autorisiert, die dem entsprechenden Ressourcentyp zugeordnet sind.

Aktion	Ressourcentyp	Bedingungsschlüssel
CreateDataSource		`aws:RequestTag` , `aws:TagKeys`
CreateFaq		`aws:RequestTag` , `aws:TagKeys`
CreateIndex		`aws:RequestTag` , `aws:TagKeys`

Aktion	Ressourcentyp	Bedingungsschlüssel
API_ ListTagsForResource	Datenquelle, Häufig gestellte Fragen, Index	
TagResource	Datenquelle, Häufig gestellte Fragen, Index	`aws:RequestTag` , `aws:TagKeys`
UntagResource	Datenquelle, Häufig gestellte Fragen, Index	`aws:TagKeys`

Informationen zum Taggen von Amazon Kendra Kendra-Ressourcen finden Sie unter. Tags Ein Beispiel für eine identitätsbasierte Richtlinie, die den Zugriff auf eine Ressource anhand von Ressourcen-Tags einschränkt, finden Sie unter. Beispiel für eine tagbasierte Richtlinie Weitere Informationen zur Verwendung von Tags zur Beschränkung des Zugriffs auf Ressourcen finden Sie unter Steuern des Zugriffs mithilfe von Tags im IAM-Benutzerhandbuch.

Amazon Kendra IAM-Rollen

Eine IAM-Rolle ist eine Entität innerhalb Ihres AWS Kontos, die über bestimmte Berechtigungen verfügt.

Temporäre Anmeldeinformationen mit Amazon Kendra verwenden

Sie können temporäre Anmeldeinformationen verwenden, um sich über einen Verbund anzumelden, eine IAM-Rolle anzunehmen oder eine kontenübergreifende Rolle anzunehmen. Sie erhalten temporäre Sicherheitsanmeldedaten, indem Sie AWS STS API-Operationen wie AssumeRoleoder GetFederationTokenaufrufen.

Amazon Kendra unterstützt die Verwendung temporärer Anmeldeinformationen.

Servicerollen

Dieses Feature ermöglicht einem Service das Annehmen einer Servicerolle in Ihrem Namen. Diese Rolle gewährt dem Service Zugriff auf Ressourcen in anderen Diensten, um eine Aktion in Ihrem Namen auszuführen. Servicerollen werden in Ihrem IAM-Konto angezeigt und gehören zum Konto. Dies bedeutet, dass ein IAM-Administrator die Berechtigungen für diese Rolle ändern kann. Dies kann jedoch die Funktionalität des Dienstes beeinträchtigen.

Amazon Kendra unterstützt Servicerollen.

Auswahl einer IAM-Rolle in Amazon Kendra

Wenn Sie einen Index erstellen, den `BatchPutDocument` Vorgang aufrufen, eine Datenquelle erstellen oder eine häufig gestellte Frage erstellen, müssen Sie eine Zugriffsrolle angeben, die Amazon Resource Name (ARN) Amazon Kendra um in Ihrem Namen auf die erforderlichen Ressourcen zuzugreifen. Wenn Sie zuvor eine Rolle erstellt haben, bietet Ihnen die Amazon Kendra Kendra-Konsole eine Liste von Rollen, aus denen Sie wählen können. Es ist wichtig, eine Rolle auszuwählen, die den Zugriff auf die Ressourcen ermöglicht, die Sie benötigen. Weitere Informationen finden Sie unter IAM -Zugriffsrollen für Amazon Kendra.

Beispiele für identitätsbasierte Richtlinien in Amazon Kendra

Standardmäßig sind Benutzer und Rollen nicht berechtigt, Amazon Kendra Kendra-Ressourcen zu erstellen oder zu ändern. Sie können auch keine Aufgaben mit der AWS Management Console AWS CLI, oder AWS API ausführen. Ein IAM-Administrator muss IAM-Richtlinien erstellen, die Benutzern und Rollen die Berechtigung zum Ausführen bestimmter API-Operationen für die angegebenen Ressourcen gewähren, die diese benötigen. Der Administrator muss diese Richtlinien anschließend den -Benutzern oder -Gruppen anfügen, die diese Berechtigungen benötigen.

Informationen dazu, wie Sie unter Verwendung dieser beispielhaften JSON-Richtliniendokumente eine identitätsbasierte IAM-Richtlinie erstellen, finden Sie unter Erstellen von Richtlinien auf der JSON-Registerkarte im IAM-Benutzerhandbuch.

Themen

- Bewährte Methoden für Richtlinien
- AWS Verwaltete (vordefinierte) Richtlinien für Amazon Kendra
- Gewähren der Berechtigung zur Anzeige der eigenen Berechtigungen für Benutzer
- Zugreifen auf einen Amazon Kendra Kendra-Index
- Beispiel für eine tagbasierte Richtlinie

Bewährte Methoden für Richtlinien

Identitätsbasierte Richtlinien legen fest, ob jemand Amazon Kendra Kendra-Ressourcen in Ihrem Konto erstellen, darauf zugreifen oder diese löschen kann. Dies kann zusätzliche Kosten für Ihr verursachen AWS-Konto. Befolgen Sie beim Erstellen oder Bearbeiten identitätsbasierter Richtlinien die folgenden Anleitungen und Empfehlungen:

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten — Verwenden Sie die AWS verwalteten Richtlinien, die Berechtigungen für viele gängige Anwendungsfälle gewähren, um Ihren Benutzern und Workloads zunächst Berechtigungen zu gewähren. Sie sind in Ihrem verfügbar. AWS-Konto Wir empfehlen Ihnen, die Berechtigungen weiter zu reduzieren, indem Sie vom AWS Kunden verwaltete Richtlinien definieren, die speziell auf Ihre Anwendungsfälle zugeschnitten sind. Weitere Informationen finden Sie unter AWS -verwaltete Richtlinien oder AWS -verwaltete Richtlinien für Auftrags-Funktionen im IAM-Benutzerhandbuch.
- Anwendung von Berechtigungen mit den geringsten Rechten – Wenn Sie mit IAM-Richtlinien Berechtigungen festlegen, gewähren Sie nur die Berechtigungen, die für die Durchführung einer Aufgabe erforderlich sind. Sie tun dies, indem Sie die Aktionen definieren, die für bestimmte Ressourcen unter bestimmten Bedingungen durchgeführt werden können, auch bekannt als die geringsten Berechtigungen. Weitere Informationen zur Verwendung von IAM zum Anwenden von Berechtigungen finden Sie unter Richtlinien und Berechtigungen in IAM im IAM-Benutzerhandbuch.
- Verwenden von Bedingungen in IAM-Richtlinien zur weiteren Einschränkung des Zugriffs – Sie können Ihren Richtlinien eine Bedingung hinzufügen, um den Zugriff auf Aktionen und Ressourcen zu beschränken. Sie können beispielsweise eine Richtlinienbedingung schreiben, um festzulegen, dass alle Anforderungen mithilfe von SSL gesendet werden müssen. Sie können auch Bedingungen verwenden, um Zugriff auf Serviceaktionen zu gewähren, wenn diese für einen bestimmten Zweck verwendet werden AWS-Service, z. AWS CloudFormation B. Weitere Informationen finden Sie unter IAM-JSON-Richtlinienelemente: Bedingung im IAM-Benutzerhandbuch.
- Verwenden von IAM Access Analyzer zur Validierung Ihrer IAM-Richtlinien, um sichere und funktionale Berechtigungen zu gewährleisten – IAM Access Analyzer validiert neue und vorhandene Richtlinien, damit die Richtlinien der IAM-Richtliniensprache (JSON) und den bewährten IAM-Methoden entsprechen. IAM Access Analyzer stellt mehr als 100 Richtlinienprüfungen und umsetzbare Empfehlungen zur Verfügung, damit Sie sichere und funktionale Richtlinien erstellen können. Weitere Informationen finden Sie unter Richtlinienvalidierung zum IAM Access Analyzer im IAM-Benutzerhandbuch.
- Multi-Faktor-Authentifizierung (MFA) erforderlich — Wenn Sie ein Szenario haben, das IAM-Benutzer oder einen Root-Benutzer in Ihrem System erfordert AWS-Konto, aktivieren Sie MFA für zusätzliche Sicherheit. Um MFA beim Aufrufen von API-Vorgängen anzufordern, fügen Sie Ihren Richtlinien MFA-Bedingungen hinzu. Weitere Informationen finden Sie unter Konfigurieren eines MFA-geschützten API-Zugriffs im IAM-Benutzerhandbuch.

Weitere Informationen zu bewährten Methoden in IAM finden Sie unter Bewährte Methoden für die Sicherheit in IAM im IAM-Benutzerhandbuch.

AWS Verwaltete (vordefinierte) Richtlinien für Amazon Kendra

AWS adressiert viele gängige Anwendungsfälle durch die Bereitstellung eigenständiger IAM-Richtlinien, die von erstellt und verwaltet werden. AWS Diese Richtlinien werden als AWS verwaltete Richtlinien bezeichnet. AWS Mit verwalteten Richtlinien können Sie Benutzern, Gruppen und Rollen einfacher Berechtigungen zuweisen, als wenn Sie die Richtlinien selbst schreiben müssten. Weitere Informationen finden Sie unter Hinzufügen von Berechtigungen zu einem Benutzer im IAM-Benutzerhandbuch.

Die folgenden AWS verwalteten Richtlinien, die Sie Gruppen und Rollen in Ihrem Konto zuordnen können, sind spezifisch für Amazon Kendra:

- AmazonKendraReadOnly— Gewährt schreibgeschützten Zugriff auf Amazon Kendra Kendra-Ressourcen.
- AmazonKendraFullAccess— Gewährt vollen Zugriff zum Erstellen, Lesen, Aktualisieren, Löschen, Markieren und Ausführen aller Amazon Kendra Kendra-Ressourcen.

Für die Konsole muss Ihre Rolle außerdem über die `s3:ListBucket` Berechtigungen`iam:CreateRole`, `iam:CreatePolicy`und `iam:AttachRolePolicy`, verfügen.

> **Note**
>
> Sie können diese Berechtigungen überprüfen, indem Sie sich bei der IAM-Konsole anmelden und nach bestimmten Richtlinien suchen.

Sie können auch Ihre eigenen benutzerdefinierten Richtlinien erstellen, um Berechtigungen für Amazon Kendra API-Aktionen zuzulassen. Die benutzerdefinierten Richtlinien können Sie dann den IAM-Rollen oder -Gruppen zuweisen, die diese Berechtigungen benötigen. Beispiele für IAM-Richtlinien für Amazon Kendra finden Sie unter. Beispiele für identitätsbasierte Richtlinien in Amazon Kendra

Gewähren der Berechtigung zur Anzeige der eigenen Berechtigungen für Benutzer

In diesem Beispiel wird gezeigt, wie Sie eine Richtlinie erstellen, die IAM-Benutzern die Berechtigung zum Anzeigen der eingebundenen Richtlinien und verwalteten Richtlinien gewährt, die ihrer

Benutzeridentität angefügt sind. Diese Richtlinie umfasst Berechtigungen zum Ausführen dieser Aktion auf der Konsole oder programmgesteuert mithilfe der API oder. 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": "*"
        }
    ]
}
```

Zugreifen auf einen Amazon Kendra Kendra-Index

In diesem Beispiel möchten Sie einem Benutzer in Ihrem AWS Konto Zugriff gewähren, um einen Index abzufragen.

```
{
```

```
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "QueryIndex",
            "Effect": "Allow",
            "Action": [
                "kendra:Query"
            ],
            "Resource": "arn:aws:kendra:${Region}:${Account}:index/${Index ID}"
        }
    ]
}
```

Beispiel für eine tagbasierte Richtlinie

Tag-basierte Richtlinien sind JSON-Richtliniendokumente, die die Aktionen spezifizieren, die ein Principal für markierte Ressourcen ausführen kann.

Beispiel: Verwenden Sie ein Tag, um auf eine Ressource zuzugreifen

Diese Beispielrichtlinie gewährt einem Benutzer oder einer Rolle in Ihrem AWS Konto die Erlaubnis, den `Query` Vorgang mit jeder Ressource zu verwenden, die mit dem Schlüssel **`department`** und dem Wert gekennzeichnet ist**`finance`**.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "kendra:Query"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/department": "finance"
                }
            }
        }
   ]
}
```

Beispiel: Verwenden Sie ein Tag, um Amazon Kendra Kendra-Operationen zu aktivieren

Diese Beispielrichtlinie gewährt einem Benutzer oder einer Rolle in Ihrem AWS Konto die Erlaubnis, jeden Amazon Kendra Kendra-Vorgang zu verwenden, mit Ausnahme von `TagResource` Vorgängen mit Ressourcen, die mit dem Schlüssel **`department`** und dem Wert **`finance`** gekennzeichnet sind.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "kendra:*",
            "Resource": "*"
        },
        {
            "Effect": "Deny",
            "Action": [
                "kendra:TagResource"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/department": "finance"
                }
            }
        }
    ]
}
```

Beispiel: Verwenden Sie ein Tag, um den Zugriff auf einen Vorgang einzuschränken

Diese Beispielrichtlinie schränkt den Zugriff eines Benutzers oder einer Rolle in Ihrem AWS Konto auf die Nutzung des `CreateIndex` Vorgangs ein, es sei denn, der Benutzer gibt das **`department`** Tag an und es hat die zulässigen Werte **`finance`** und**`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 verwaltete Richtlinien für Amazon Kendra

Um Benutzern, Gruppen und Rollen Berechtigungen hinzuzufügen, ist es einfacher, AWS verwaltete Richtlinien zu verwenden, als Richtlinien selbst zu schreiben. Es erfordert Zeit und Fachwissen, um von Kunden verwaltete IAM-Richtlinien zu erstellen, die Ihrem Team nur die benötigten Berechtigungen bieten. Um schnell loszulegen, können Sie unsere AWS verwalteten Richtlinien verwenden. Diese Richtlinien decken allgemeine Anwendungsfälle ab und sind in Ihrem AWS Konto verfügbar. Weitere Informationen zu AWS verwalteten Richtlinien finden Sie unter AWS Verwaltete Richtlinien im IAM-Benutzerhandbuch.

AWS Dienste verwalten und aktualisieren AWS verwaltete Richtlinien. Sie können die Berechtigungen in AWS verwalteten Richtlinien nicht ändern. Services fügen einer von AWS verwalteten Richtlinien gelegentlich zusätzliche Berechtigungen hinzu, um neue Features zu unterstützen. Diese Art von Update betrifft alle Identitäten (Benutzer, Gruppen und Rollen), an welche

die Richtlinie angehängt ist. Services aktualisieren eine von AWS verwaltete Richtlinie am ehesten, ein neues Feature gestartet wird oder neue Vorgänge verfügbar werden. Dienste entfernen keine Berechtigungen aus einer AWS verwalteten Richtlinie, sodass durch Richtlinienaktualisierungen Ihre bestehenden Berechtigungen nicht beeinträchtigt werden.

AWS Unterstützt außerdem verwaltete Richtlinien für Jobfunktionen, die sich über mehrere Dienste erstrecken. Die ReadOnlyAccess AWS verwaltete Richtlinie bietet beispielsweise schreibgeschützten Zugriff auf alle AWS Dienste und Ressourcen. Wenn ein Dienst eine neue Funktion startet, werden nur Leseberechtigungen für neue Operationen und Ressourcen AWS hinzugefügt. Eine Liste und Beschreibungen der Richtlinien für Auftragsfunktionen finden Sie in Verwaltete AWS -Richtlinien für Auftragsfunktionen im IAM-Leitfaden.

AWS verwaltete Richtlinie: AmazonKendraReadOnly

Gewährt schreibgeschützten Zugriff auf Amazon Kendra Kendra-Ressourcen. Diese Richtlinie umfasst die folgenden Berechtigungen.

- `kendra`— Ermöglicht Benutzern das Ausführen von Aktionen, bei denen entweder eine Liste von Elementen oder Details zu einem Artikel zurückgegeben wird. Dazu gehören API-Operationen, die mit`Describe`,`List`,`Query`, `BatchGetDocumentStatus``GetQuerySuggestions`, oder beginnen`GetSnapshots`.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "kendra:Describe*",
                "kendra:List*",
                "kendra:Query",
                "kendra:BatchGetDocumentStatus",
                "kendra:GetQuerySuggestions",
                "kendra:GetSnapshots"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
```

```
}
```

AWS verwaltete Richtlinie: AmazonKendraFullAccess

Gewährt vollen Zugriff zum Erstellen, Lesen, Aktualisieren, Löschen, Markieren und Ausführen aller Amazon Kendra Kendra-Ressourcen. Diese Richtlinie umfasst die folgenden Berechtigungen.

- `kendra`— Ermöglicht Prinzipalen Lese- und Schreibzugriff auf alle Aktionen in Amazon Kendra.
- `s3`— Ermöglicht Prinzipalen das Abrufen von Amazon S3 S3-Bucket-Standorten und List-Buckets.
- `iam`— Ermöglicht es Prinzipalen, Rollen zu übergeben und aufzulisten.
- `kms`— Ermöglicht Prinzipalen, Schlüssel und Aliase zu beschreiben und aufzulisten AWS KMS .
- `secretsmanager`— Ermöglicht Prinzipalen das Erstellen, Beschreiben und Auflisten von Geheimnissen.
- `ec2`— Ermöglicht Prinzipalen die Beschreibung von Sicherheitsgruppen, VCPs (Virtual Private Cloud) und Subnetzen.
- `cloudwatch`— Ermöglicht Prinzipalen, Cloud Watch-Metriken einzusehen.

```
{
    "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 aktualisiert AWS verwaltete Richtlinien

Sehen Sie sich Details zu Aktualisierungen der AWS verwalteten Richtlinien für Amazon Kendra an, seit dieser Service begonnen hat, diese Änderungen zu verfolgen. Abonnieren Sie den RSS-Feed auf der Amazon Kendra Document-Verlaufsseite, um automatische Benachrichtigungen über Änderungen an dieser Seite zu erhalten.

Änderung	Beschreibung	Datum
AmazonKendraReadOnly—Genehmigung zum Support GetSnapshots hinzufügen, APIs BatchGetDocumentStatus	Amazon Kendra hat neue APIs hinzugefügt `GetSnapshots` und `BatchGetDocumentStatus` . `GetSnapshots` stellt Daten bereit, die zeigen, wie Ihre Benutzer mit Ihrer Suchanwendung interagieren. `BatchGetDocumentStatus` überwacht den Fortschritt der Indizierung Ihrer Dokumente.	3. Januar 2022
AmazonKendraReadOnly—Genehmigung zur Unterstützung des Vorgangs hinzufügen GetQuerySuggestions	Amazon Kendra hat eine neue API hinzugefügt `GetQuerySuggestions` , mit der Sie Abfragevorschläge für beliebte Suchanfragen abrufen	27. Mai 2021

Änderung	Beschreibung	Datum
	können, um Ihre Benutzer bei der Suche zu unterstüt zen. Wenn Benutzer ihre Suchabfrage eingeben, hilft die vorgeschlagene Abfrage dabei, ihre Suche automatisch zu vervollständigen.	
Amazon Kendra hat begonnen, Änderungen zu verfolgen	Amazon Kendra hat damit begonnen, Änderungen an seinen AWS verwalteten Richtlinien nachzuverfolgen.	27. Mai 2021

Fehlerbehebung bei Amazon Kendra Identity and Access

Verwenden Sie die folgenden Informationen, um häufig auftretende Probleme zu diagnostizieren und zu beheben, die bei der Arbeit mit Amazon Kendra und IAM auftreten können.

Themen

- Ich bin nicht berechtigt, eine Aktion in Amazon Kendra durchzuführen
- Ich bin nicht berechtigt, iam auszuführen: PassRole
- Ich bin Administrator und möchte anderen den Zugriff auf Amazon Kendra ermöglichen
- Ich möchte Personen außerhalb meines AWS Kontos den Zugriff auf meine Amazon Kendra Kendra-Ressourcen ermöglichen

Ich bin nicht berechtigt, eine Aktion in Amazon Kendra durchzuführen

Wenn Ihnen AWS Management Console mitgeteilt wird, dass Sie nicht berechtigt sind, eine Aktion durchzuführen, müssen Sie sich an Ihren Administrator wenden, um Unterstützung zu erhalten. Ihr Administrator hat Ihnen Ihre Anmeldeinformationen zur Verfügung gestellt.

Der folgende Beispielfehler tritt auf, wenn der `mateojackson` Benutzer versucht, die Konsole zu verwenden, um Details zu einem Index anzuzeigen, aber nicht über die `kendra:DescribeIndex` entsprechenden Berechtigungen verfügt.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 kendra:DescribeIndex on resource: index ARN
```

In diesem Fall bittet Mateo seinen Administrator um die Aktualisierung seiner Richtlinien, um unter Verwendung der Aktion `index` auf die Ressource `kendra:DescribeIndex` zugreifen zu können.

Ich bin nicht berechtigt, iam auszuführen: PassRole

Wenn Sie eine Fehlermeldung erhalten, dass Sie nicht berechtigt sind, die `iam:PassRole` Aktion durchzuführen, müssen Ihre Richtlinien aktualisiert werden, damit Sie eine Rolle an Amazon Kendra übergeben können.

Einige AWS-Services ermöglichen es Ihnen, eine bestehende Rolle an diesen Service zu übergeben, anstatt eine neue Servicerolle oder eine dienstbezogene Rolle zu erstellen. Hierzu benötigen Sie Berechtigungen für die Übergabe der Rolle an den Dienst.

Der folgende Beispielfehler tritt auf, wenn ein IAM-Benutzer mit dem Namen `marymajor` versucht, die Konsole zu verwenden, um eine Aktion in Amazon Kendra auszuführen. Die Aktion erfordert jedoch, dass der Service über Berechtigungen verfügt, die durch eine Servicerolle gewährt werden. Mary besitzt keine Berechtigungen für die Übergabe der Rolle an den Dienst.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

In diesem Fall müssen die Richtlinien von Mary aktualisiert werden, um die Aktion `iam:PassRole` ausführen zu können.

Wenn Sie Hilfe benötigen, wenden Sie sich an Ihren AWS Administrator. Ihr Administrator hat Ihnen Ihre Anmeldeinformationen zur Verfügung gestellt.

Ich bin Administrator und möchte anderen den Zugriff auf Amazon Kendra ermöglichen

Um anderen den Zugriff auf Amazon Kendra zu ermöglichen, müssen Sie eine IAM-Entität (Benutzer oder Rolle) für die Person oder Anwendung erstellen, die Zugriff benötigt. Sie werden die Anmeldeinformationen für diese Einrichtung verwenden, um auf AWS zuzugreifen. Anschließend müssen Sie der Entität eine Richtlinie beifügen, die ihr die richtigen Berechtigungen in Amazon Kendra gewährt.

Informationen zum Einstieg finden Sie unter Erstellen Ihrer ersten delegierten IAM-Benutzer und -Gruppen im IAM-Benutzerhandbuch.

Ich möchte Personen außerhalb meines AWS Kontos den Zugriff auf meine Amazon Kendra Kendra-Ressourcen ermöglichen

Sie können eine Rolle erstellen, die Benutzer in anderen Konten oder Personen außerhalb Ihrer Organisation für den Zugriff auf Ihre Ressourcen verwenden können. Sie können festlegen, wem die Übernahme der Rolle anvertraut wird. Im Fall von Diensten, die ressourcenbasierte Richtlinien oder Zugriffskontrolllisten (Access Control Lists, ACLs) verwenden, können Sie diese Richtlinien verwenden, um Personen Zugriff auf Ihre Ressourcen zu gewähren.

Weitere Informationen dazu finden Sie hier:

- Informationen darüber, ob Amazon Kendra diese Funktionen unterstützt, finden Sie unterSo arbeitet Amazon Kendra mit IAM.
- Informationen dazu, wie Sie Zugriff auf Ihre Ressourcen gewähren können, AWS-Konten die Ihnen gehören, finden Sie im IAM-Benutzerhandbuch unter Gewähren des Zugriffs auf einen IAM-Benutzer in einem anderen AWS-Konto , den Sie besitzen.
- Informationen dazu, wie Sie Dritten Zugriff auf Ihre Ressourcen gewähren können AWS-Konten, finden Sie AWS-Konten im IAM-Benutzerhandbuch unter Gewähren des Zugriffs für Dritte.
- Informationen dazu, wie Sie über einen Identitätsverbund Zugriff gewähren, finden Sie unter Gewähren von Zugriff für extern authentifizierte Benutzer (Identitätsverbund) im IAM-Benutzerhandbuch.
- Informationen zum Unterschied zwischen der Verwendung von Rollen und ressourcenbasierten Richtlinien für den kontoübergreifenden Zugriff finden Sie unter So unterscheiden sich IAM-Rollen von ressourcenbasierten Richtlinien im IAM-Benutzerhandbuch.

Bewährte Methoden für die Gewährleistung der Sicherheit

Amazon Kendra bietet eine Reihe von Sicherheitsfunktionen, die Sie bei der Entwicklung und Implementierung Ihrer eigenen Sicherheitsrichtlinien berücksichtigen sollten. Die folgenden bewährten Methoden stellen allgemeine Richtlinien und keine vollständige Sicherheitslösung dar. Da diese bewährten Methoden für Ihre Umgebung möglicherweise nicht angemessen oder ausreichend sind, sollten Sie sie als hilfreiche Überlegungen und nicht als bindend ansehen.

Anwendung des Prinzips der geringsten Privilegien

Amazon Kendra bietet eine detaillierte Zugriffsrichtlinie für Anwendungen, die Rollen verwenden IAM . Wir empfehlen, den Rollen nur die für den Job erforderlichen Mindestberechtigungen zu

gewähren, z. B. für Ihre Bewerbung und den Zugriff auf das Protokollziel. Wir empfehlen außerdem, die Aufträge regelmäßig und bei jeder Änderung an Ihrer Bewerbung auf Berechtigungen zu überprüfen.

Rollenbasierte Zugriffskontrolle (RBAC) Berechtigungen

Administratoren sollten die Berechtigungen für die rollenbasierte Zugriffskontrolle (RBAC) für Amazon Kendra Kendra-Anwendungen strikt kontrollieren.

Protokollierung und Überwachung in Amazon Kendra

Die Überwachung ist ein wichtiger Bestandteil der Aufrechterhaltung der Zuverlässigkeit, Verfügbarkeit und Leistung Ihrer Amazon Kendra Kendra-Anwendungen. Um Amazon Kendra API-Aufrufe zu überwachen, können Sie verwenden AWS CloudTrail. Verwenden Sie Amazon CloudWatch Logs, um den Status Ihrer Jobs zu überwachen.

- Amazon CloudWatch Alarms — Mithilfe von CloudWatch Alarmen beobachten Sie eine einzelne Metrik über einen von Ihnen angegebenen Zeitraum. Wenn die Metrik eine Richtlinie überschreitet. CloudWatch Alarme lösen keine Aktionen aus, wenn sich eine Metrik in einem bestimmten Status befindet. Der Status muss sich stattdessen geändert haben und für eine festgelegte Anzahl an Zeiträumen aufrechterhalten worden sein. Weitere Informationen finden Sie unter Überwachung von Amazon Kendra mit Amazon CloudWatch.
- AWS CloudTrail Protokolle — CloudTrail bietet eine Aufzeichnung der Aktionen, die von einem Benutzer, einer Rolle oder einem AWS Service in Amazon Kendra oder Amazon Kendra Intelligent Ranking ausgeführt wurden. Anhand der von gesammelten Informationen können Sie die Anfrage CloudTrail, die an Amazon Kendra gestellt wurde, die IP-Adresse, von der aus die Anfrage gestellt wurde, wer die Anfrage gestellt hat, wann sie gestellt wurde, und weitere Details ermitteln. Weitere Informationen finden Sie unter Protokollieren von Amazon-Kendra-API-Aufrufen mitAWS CloudTrailaufzeichnen und Protokollieren von Amazon Kendra Intelligent Ranking API-Aufrufen mitAWS CloudTrailaufzeichnen.

Konformitätsvalidierung für Amazon Kendra

Externe Prüfer bewerten die Sicherheit und Konformität von Amazon Kendra im Rahmen mehrerer Compliance-Programme von Amazon Kendra. Amazon Kendra erfüllt die folgenden Anforderungen:

- Health Insurance Portability and Accountability Act (HIPAA)

- System- und Organisationskontrollen (SOC) 2
- Programm für registrierte Prüfer im Bereich Informationssicherheit (IRAP)
- Das Federal Risk and Authorization Management Program (FedRAMP) ist in den Regionen Ost/West der USA moderat
- Das Federal Risk and Authorization Management Program (FedRAMP) ist in der AWS-Region GovCloud (USA West) hoch im Kurs

Eine Liste der AWS Services im Rahmen bestimmter Compliance-Programme finden Sie unter AWS Services im Umfang nach Compliance-Programmen AWS Compliance-Programmen. Allgemeine Informationen finden Sie unter AWS Compliance-Programme AWS .

Sie können Prüfberichte von Drittanbietern unter herunterladen AWS Artifact. Weitere Informationen finden Sie unter Berichte in AWS Artifact herunterladen Berichte in AWS Artifact .

Ihre Compliance-Verantwortung bei der Nutzung von Amazon Kendra hängt von der Sensibilität Ihrer Daten, den Compliance-Zielen Ihres Unternehmens und den geltenden Gesetzen und Vorschriften ab. AWS bietet die folgenden Ressourcen zur Unterstützung bei der Einhaltung von Vorschriften:

- Schnellstartanleitungen zu Sicherheit und Compliance Schnellstartanleitungen zu — In diesen Bereitstellungshandbüchern werden architektonische Überlegungen erörtert und Schritte für die Implementierung von sicherheits- und Compliance-orientierten Basisumgebungen beschrieben. AWS
- Whitepaper „Architecting for HIPAA Security and Compliance“ — In diesem Whitepaper wird beschrieben, wie Unternehmen HIPAA-konforme Anwendungen entwickeln können. AWS
- AWS Ressourcen AWS zur Einhaltung
- Evaluierung von Ressourcen anhand von Regeln im AWS Config Entwicklerhandbuch — Der AWS Config Service bewertet, wie gut Ihre Ressourcenkonfigurationen den internen Praktiken, Branchenrichtlinien und Vorschriften entsprechen.
- AWS Security Hub—Dieser AWS Service bietet einen umfassenden Überblick über Ihren Sicherheitsstatus und hilft Ihnen AWS , die Einhaltung der Sicherheitsstandards und Best Practices der Branche zu überprüfen.

Resilienz bei Amazon Kendra

Die AWS globale Infrastruktur basiert auf AWS Regionen und Availability Zones. AWS Regionen bieten mehrere physisch getrennte und isolierte Availability Zones, die über Netzwerke mit niedriger

Latenz, hohem Durchsatz und hoher Redundanz miteinander verbunden sind. Mithilfe von Availability Zones können Sie Anwendungen und Datenbanken erstellen und ausführen, die automatisch Failover zwischen Zonen ausführen, ohne dass es zu Unterbrechungen kommt. Availability Zones sind besser verfügbar, fehlertoleranter und skalierbarer als herkömmliche Infrastrukturen mit einem oder mehreren Rechenzentren.

Weitere Informationen zu AWS Regionen und Availability Zones finden Sie unter AWS Globale Infrastruktur.

Mit AWS seiner globalen Infrastruktur ist Amazon Kendra Enterprise Edition fehlertolerant, skalierbar und hochverfügbar. Ein Rollback zu früheren Versionen eines Indexes wird derzeit nicht unterstützt. Sie können jedoch Teile Ihres Indexes aktualisieren oder neu erstellen, indem Sie bestehende Datenquellen löschen und wieder zu Ihrem Index hinzufügen.

Infrastruktursicherheit in Amazon Kendra

Als verwalteter Service ist Amazon Kendra durch AWS globale Netzwerksicherheit geschützt. Informationen zu AWS Sicherheitsdiensten und zum AWS Schutz der Infrastruktur finden Sie unter AWS Cloud-Sicherheit. Informationen zum Entwerfen Ihrer AWS Umgebung unter Verwendung der bewährten Methoden für die Infrastruktursicherheit finden Sie unter Infrastructure Protection in Security Pillar AWS Well-Architected Framework.

Sie verwenden AWS veröffentlichte API-Aufrufe, um über das Netzwerk auf Amazon Kendra zuzugreifen. Kunden müssen Folgendes unterstützen:

- Transport Layer Security (TLS). Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Verschlüsselungs-Suiten mit Perfect Forward Secrecy (PFS) wie DHE (Ephemeral Diffie-Hellman) oder ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). Die meisten modernen Systeme wie Java 7 und höher unterstützen diese Modi.

Außerdem müssen Anforderungen mit einer Zugriffsschlüssel-ID und einem geheimen Zugriffsschlüssel signiert sein, der einem IAM-Prinzipal zugeordnet ist. Alternativ können Sie mit AWS Security Token Service (AWS STS) temporäre Sicherheitsanmeldeinformationen erstellen, um die Anforderungen zu signieren.

Konfiguration und Schwachstellenanalyse in AWS Identity and Access Management

AWS kümmert sich um grundlegende Sicherheitsaufgaben wie das Patchen von Gastbetriebssystemen (OS) und Datenbanken, die Firewall-Konfiguration und die Notfallwiederherstellung. Diese Verfahren wurden von qualifizierten Dritten überprüft und zertifiziert. Weitere Informationen finden Sie in den folgenden Ressourcen:

- Modell der übergreifenden Verantwortlichkeit
- AWS: Überblick über Sicherheitsprozesse (Whitepaper)

Die folgenden Ressourcen befassen sich auch mit der Konfiguration und Schwachstellenanalyse in AWS Identity and Access Management (IAM):

- Überprüfung der Einhaltung der Vorschriften für AWS Identity and Access Management
- Bewährte Sicherheitsmethoden und Anwendungsfälle in AWS Identity and Access Management.

Kontingente für Amazon Kendra

Unterstützte -Regionen

Eine Liste der AWS Regionen, in denen Amazon Kendra es verfügbar ist, finden Sie unter Amazon Kendra Regionen und Endpunkte in der Amazon Web Services General Reference.

Kontingente

Servicekontingenten, auch Limits genannt, sind die maximale Anzahl von Serviceressourcen für Ihr AWS Konto. Weitere Informationen finden Sie unter Amazon Kendra Service Quotas in der Allgemeinen AWS -Referenz.

Indexkontingente

Beschreibung	Standard	Edition	Einstellbar
Maximale Anzahl von Indizes pro Konto	10	Entwickler, Unternehmen	Ja
Menge des für einen Index extrahier ten Texts in einer einzigen Einheit (Entwickler). Sie können keine zusätzlichen Einheiten zum Extrahieren von Text für die Developer Edition hinzufügen.	3 GB	Developer	Nein
Menge des für einen Index extrahier ten Texts in einer einzigen Einheit (Enterprise). Sie	30 GB	Enterprise	Ja

Beschreibung	Standard	Edition	Einstellbar
können bis zu 100 zusätzliche Einheiten zum Extrahieren von Text für die Enterprise Edition hinzufügen oder sich einfach an den Support wenden.			

Datenquellen-Connector-Kontingente

Beschreibung	Standard	Edition	Einstellbar
Maximale Anzahl von Datenquellenconnectors pro Index (Entwickler)	5	Developer	Nein
Maximale Anzahl von Datenquellen-Connectors pro Index (Enterprise)	50	Enterprise	Ja
Maximale Größe eines einzelnen Dokuments oder einer Rohdatei bei Verwendung eines Datenquellen-Connectors	50 MB	Entwickler, Unternehmen	Ja
Maximale Anzahl von S3-Präfixen in der Konfigurationsdatei der Zugriffskontrollliste,	100	Entwickler, Unternehmen	Nein

Beschreibung	Standard	Edition	Einstellbar
die im Amazon S3 Datenquellenconnector enthalten ist			
Maximale Größe der Konfigurationsdatei für die Zugriffskontrollliste, die im Amazon S3 Datenquellenconnector enthalten ist	50 MB	Entwickler, Unternehmen	Ja

Häufig gestellte Fragen zu Kontin

Beschreibung	Standard	Edition	Einstellbar
Maximale Anzahl von FAQs pro Index	30	Entwickler, Unternehmen	Ja
Maximale Größe von 1 FAQ	5 MB	Entwickler, Unternehmen	Ja
Maximale Anzahl von Ergebnissen, die für häufig gestellte Fragen zurückgegeben wurden	4	Entwickler, Unternehmen	Ja
Die maximal zulässige Anzahl von Zeichen für eine FAQ-Frage	300	Entwickler, Unternehmen	Nein
Maximale Anzahl von Zeichen in einer FAQ-Antwort	2000	Entwickler, Unternehmen	Nein

Thesaurus-Quoten

Beschreibung	Standard	Edition	Einstellbar
Maximale Anzahl von Thesauri pro Index	1	Entwickler, Unternehmen	Nein
Maximale Größe einer Thesaurus-Datei	5 MB	Entwickler, Unternehmen	Ja
Maximale Anzahl von Synonymregeln pro Thesaurus	10.000	Entwickler, Unternehmen	Ja
Maximale Anzahl von Synonymen pro Begriff in allen Thesauri in einem Index	10	Entwickler, Unternehmen	Nein

Amazon Kendra erleben Sie Kontingente

Beschreibung	Standard	Edition	Einstellbar
Maximale Anzahl von Amazon Kendra Erlebnissen pro Index	50	Entwickler, Unternehmen	Ja

Quoten für Abfragen und Suchergebnisse

Beschreibung	Standard	Edition	Einstellbar
Anzahl der Abfragen pro Sekunde für einen Index in einer	0,05	Developer	Nein

Beschreibung	Standard	Edition	Einstellbar
einzigen Einheit (Entwickler). Sie können keine zusätzlichen Einheiten für Abfragen für die Developer Edition hinzufügen.			
Anzahl der Abfragen pro Sekunde für einen Index in einer einzelnen Einheit (Enterprise). Sie können bis zu 100 zusätzliche Einheiten für Anfragen zur Enterprise Edition hinzufügen oder sich einfach an den Support wenden.	0.1	Enterprise	Ja
Maximale Anzahl von Zeichen pro Abfragetext	1000	Entwickler, Unternehmen	Ja
Maximale Anzahl von Suchergebnissen pro Abfrage. Die Standardeinstellung ist 100. Um mehr als 100 Ergebnisse zu erhalten, wenden Sie sich einfach an den Support.	100	Entwickler, Unternehmen	Ja

Beschreibung	Standard	Edition	Einstellbar
Maximale Anzahl von Suchergebnissen pro Seite	100	Entwickler, Unternehmen	Ja
Maximale Anzahl von Tokenwörtern pro Abfragetext vor der Kürzung. Die Standardeinstellung ist 30. Um mehr als 30 Wörter zuzulassen, wenden Sie sich einfach an den Support.	30	Entwickler, Unternehmen	Ja
Maximale Größe der Benutzergruppenliste pro Abfrageattribut	10	Entwickler, Unternehmen	Ja
Maximale Größe der Zeichenfolgenliste pro Abfrageattribut	10	Entwickler, Unternehmen	Ja

Quoten für Vorschläge abfragen

Beschreibung	Standard	Edition	Einstellbar
Maximale Anzahl der pro GetQuerySuggestionsAnruf zurückgegebenen Abfragevorschläge	10	Entwickler, Unternehmen	Ja
Maximale Anzahl von Feldern/Attributen für	10	Entwickler, Unternehmen	Ja

Beschreibung	Standard	Edition	Einstellbar
Abfragevorschläge pro Anruf GetQuerySuggestions			
Maximale Anzahl zusätzlicher Felder/Attribute für Abfragevorschläge pro Anruf GetQuerySuggestions	5	Entwickler, Unternehmen	Ja
Maximale Anzahl von Blocklisten pro Index	1	Entwickler, Unternehmen	Nein
Maximale Größe einer Blocklisten-Textdatei	2 MB	Entwickler, Unternehmen	Ja
Maximale Anzahl von Elementen (Wörtern oder Ausdrücken) in einer Sperrliste	20 000	Entwickler, Unternehmen	Ja
Maximale Anzahl von Rechtschreibkorrektur-Abfragevorschlägen, die bei einem `Query` API-Aufruf zurückgegeben werden.	1	Entwickler, Unternehmen	Ja

Kontingente für Dokumente

Beschreibung	Standard	Edition	Einstellbar
Menge an Text, der für einen Index	3 GB	Developer	Nein

Beschreibung	Standard	Edition	Einstellbar
in einer einzigen Einheit extrahiert wurde (Entwickler). Sie können keine zusätzlichen Einheiten zum Extrahieren von Text für die Developer Edition hinzufügen.			
Menge des für einen Index extrahier ten Texts in einer einzigen Einheit (Enterprise). Sie können bis zu 100 zusätzliche Einheiten zum Extrahieren von Text für die Enterpris e Edition hinzufügen oder sich einfach an den Support wenden.	30 GB	Enterprise	Ja
Maximale Größe eines einzelnen Dokuments oder einer Rohdatei bei Verwendung eines Datenquellen-Conne ctors	50 MB	Entwickler, Unternehmen	Ja

Beschreibung	Standard	Edition	Einstellbar
Maximale Größe eines einzelnen Dokuments oder einer Rohdatei bei Verwendung der `BatchPutDocument` API	5 MB	Entwickler, Unternehmen	Ja
Maximale Textmenge, die aus einem einzelnen Dokument extrahiert wurde	5 MB	Entwickler, Unternehmen	Nein
Maximale Anzahl von benutzerdefinierten Feldern/Attributen pro Index	500	Entwickler, Unternehmen	Nein

Kontingente für ausgewählte Suchergebnisse

Beschreibung	Standard	Edition	Einstellbar
Maximale Anzahl von ausgewählten Dokumenten pro ausgewähltem Ergebnissatz	4	Enterprise	Ja
Maximale Anzahl von Abfragetexten pro ausgewähltem Ergebnissatz	49	Enterprise	Nein
Maximale Anzahl von Zeichen pro Abfragete	1000	Enterprise	Ja

Beschreibung	Standard	Edition	Einstellbar
xt in einem ausgewähl ten Ergebnissatz			
Maximale Anzahl von ausgewählten Ergebnissätzen pro Index	50	Enterprise	Ja

Kontingente für Suchergebnisse neu bewerten/neu einordnen

Beschreibung	Standard	Edition	Einstellbar
Maximale Anzahl von `Rescore` Anfragen pro Sekunde für einen Rescore-A usführungsplan oder eine einzelne Kapazitätseinheit. Sie können bis zu 1000 zusätzliche Einheiten hinzufügen.	0.01	Enterprise	Nein
Maximale Anzahl von Rescore-Ausführung splänen pro Konto.	50	Enterprise	Ja
Maximale Anzahl von Tokens `Title` für ein Dokument in einer `Rescore` Anfrage.	100	Enterprise	Nein
Maximale Anzahl von Tokens `Body` für ein	200	Enterprise	Nein

Beschreibung	Standard	Edition	Einstellbar
Dokument in einer `Rescore` Anfrage.			
Maximale Anzahl von Dokumenten in einer `Rescore` Anfrage.	25	Enterprise	Nein
Maximale Anzahl von Dokumenten pro Gruppe in einer `Rescore` Anfrage.	3	Enterprise	Nein

Weitere Informationen zu Amazon Kendra Service Quotas und zur Beantragung einer Kontingenterhöhung finden Sie unter Servicekontingente.

Fehlerbehebung

Dieser Abschnitt kann Ihnen helfen, häufig auftretende Probleme zu lösen, auf die Sie bei der Arbeit mit Problemen stoßen könnten Amazon Kendra.

Themen

Problembehandlung bei Datenquellen

Dieser Abschnitt kann Ihnen helfen, häufig auftretende Probleme bei der Konfiguration und Verwendung von Amazon Kendra Datenquellenconnectors zu lösen.

Meine Dokumente wurden nicht indexiert

Wenn Sie Ihren Amazon Kendra Index mit einer Datenquelle synchronisieren, können Probleme auftreten, die verhindern, dass die Dokumente indexiert werden. Die Indizierung erfolgt in zwei Schritten. Zunächst wird in der Datenquelle nach neuen und aktualisierten Dokumenten gesucht, die indexiert werden sollen, und nach Dokumenten, die aus dem Index entfernt werden sollen. Zweitens wird auf Dokumentebene auf jedes Dokument zugegriffen und es wird indexiert.

In jedem dieser Schritte kann ein Fehler auftreten. Fehler auf Datenquellenebene werden in der Konsole im Abschnitt Synchronisierungslaufverlauf der Datenquellendetailseite gemeldet. Der Status des Synchronisierungsauftrags kann „Erfolgreich“, „Unvollständig“ oder „Fehlgeschlagen“ lauten. Sie können auch die Anzahl der Dokumente sehen, die während des Jobs indexiert und gelöscht wurden. Wenn der Status Fehlgeschlagen lautet, wird in der Spalte Details eine Meldung angezeigt.

Fehler auf Dokumentebene werden in gemeldet Amazon CloudWatch Logs. Sie können die Fehler in der CloudWatch Konsole sehen.

Informationen zum Generieren eines Statusberichts zur Dokumentensynchronisierung finden Sie unter Ich möchte einen Synchronisierungsstatusbericht für meine Dokumente erstellen.

Mein Synchronisierungsauftrag ist fehlgeschlagen

Ein Synchronisationsjob schlägt normalerweise fehl, wenn ein Konfigurationsfehler im Index oder in der Datenquelle vorliegt. In der Konsole finden Sie die Fehlermeldung im Abschnitt Synchronisierungslaufverlauf der Datenquellendetails in der Spalte Details. Fehler auf Dokumentebene werden unter gemeldet Amazon CloudWatch Logs. Die Fehlermeldung gibt Auskunft darüber, was schief gelaufen ist. Das Problem besteht normalerweise darin, dass der Index oder die Datenquelle nicht über die richtigen IAM Berechtigungen verfügt. Die Fehlermeldung beschreibt die fehlenden Berechtigungen. Hier sind einige der Fehlermeldungen, die Sie erhalten können:

```
Failed to create log group for job. Please make sure that the IAM role
provided has sufficient permissions.
```

Wenn Ihre Indexrolle keine Nutzungsberechtigung hat CloudWatch, kann die Datenquelle kein CloudWatch Protokoll erstellen. Wenn Sie diesen Fehler erhalten, müssen Sie der Indexrolle CloudWatch Berechtigungen hinzufügen.

```
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.
```

Wenn Sie eine Amazon S3 Datenquelle verwenden, Amazon Kendra müssen Sie berechtigt sein, auf den Bucket zuzugreifen, der die Dokumente enthält. Sie müssen der IAM Datenquellenrolle die Berechtigung Amazon Kendra zum Lesen des Buckets hinzufügen.

```
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 benötigt die Erlaubnis, die Index- und IAM Datenquellenrollen zu übernehmen. Sie müssen den Rollen, die für die `sts:AssumeRole` Aktion berechtigt sind, eine Vertrauensrichtlinie hinzufügen.

Die IAM Richtlinien, die eine Datenquelle indizieren Amazon Kendra müssen, finden Sie unter IAM Rollen.

Informationen zum Generieren eines Statusberichts zur Dokumentensynchronisierung finden Sie unter Ich möchte einen Synchronisierungsstatusbericht für meine Dokumente erstellen.

Mein Synchronisierungsauftrag ist unvollständig

Jobs sind in der Regel unvollständig, wenn sie den Prozess auf Datenquellenebene abgeschlossen haben, während des Prozesses auf Dokumentebene jedoch einige Fehler auftreten. Wenn ein Job unvollständig ist, wurden einige Dokumente möglicherweise nicht erfolgreich indexiert. Bei einer Amazon S3 Datenquelle wird ein unvollständiger Job in der Regel durch folgende Ursachen verursacht:

- Die Metadaten für ein oder mehrere Dokumente waren ungültig.
- Wenn Dokumente zur Indexierung eingereicht wurden, aber mindestens ein Dokument nicht eingereicht wurde.
- Wenn Dokumente zum Löschen aus dem Index eingereicht wurden, aber mindestens ein Dokument nicht eingereicht wurde.

Um Fehler bei einer unvollständigen Synchronisation zu beheben, schauen Sie sich zunächst Ihre CloudWatch Logs an.

1. Wählen Sie in der Detailspalte die Option Details anzeigen in aus CloudWatch.
2. Sehen Sie sich die Fehlermeldungen an, um herauszufinden, warum das Dokument nicht erfolgreich war.

Informationen zum Generieren eines Statusberichts zur Dokumentensynchronisierung finden Sie unter Ich möchte einen Synchronisierungsstatusbericht für meine Dokumente erstellen.

Mein Synchronisierungsauftrag war erfolgreich, aber es gibt keine indizierten Dokumente

Gelegentlich wird ein ausgeführter Indexsynchronisierungsauftrag als Erfolgreich markiert, aber es wurden keine neuen oder aktualisierten Dokumente zu dem erwarteten Zeitpunkt indexiert. Mögliche Gründe sind:

- Überprüfen Sie die CloudWatch `DocumentsSubmittedForIndexingFailed` Metrik, um festzustellen, ob Dokumente nicht synchronisiert werden konnten. Einzelheiten finden Sie in Ihren CloudWatch Protokollen.

- Für eine Amazon S3 Datenquelle haben Sie möglicherweise Amazon Kendra den falschen Bucket-Namen oder das falsche Präfix angegeben. Stellen Sie sicher, dass der Bucket, der verwendet Amazon Kendra wird, derjenige ist, der die zu indizierenden Dokumente enthält.
- Wenn Sie ein Dokument erneut indizieren, das in einem früheren Job nicht indexiert werden konnte, Amazon Kendra wird es nur indexiert, wenn Sie das Dokument oder die zugehörige Metadatendatei geändert haben.

Informationen zum Generieren eines Statusberichts zur Dokumentensynchronisierung finden Sie unter Ich möchte einen Synchronisierungsstatusbericht für meine Dokumente erstellen.

Beim Synchronisieren meiner Datenquelle treten Probleme mit dem Dateiformat auf

Wenn Sie beim Hinzufügen von Dateien zu Ihrer Datenquelle oder beim Synchronisieren Ihrer Datenquelle auf Probleme mit dem Dateiformat stoßen, stellen Sie sicher, dass Ihre Dokumenttypen unterstützt werden Amazon Kendra . Eine Liste der von unterstützten Dokumenttypen Amazon Kendra finden Sie unter Dokumenttypen oder Formate.

Wenn Sie die `BatchPutDocument` API mit Nur-Text-Dateien verwenden, geben Sie `PLAIN_TEXT` als Inhaltstyp an.

Ich möchte einen Synchronisierungsverlaufsbericht für meine Dokumente erstellen

Wenn Sie Ihren Amazon Kendra Datenquellen-Connector synchronisieren, Amazon Kendra kann er Synchronisierungsstatusberichte für jedes Dokument in Ihrer Datenquelle generieren und in einen Amazon S3 Bucket kopieren. Während dieses Vorgangs werden Ihre Daten mithilfe von AWS KMS Schlüsseln verschlüsselt und können nur von Ihnen eingesehen werden. Der Status des gemeldeten Dokuments kann einer der folgenden sein: Fehlgeschlagen, Abgeschlossen oder Erfolgreich mit Fehlern.

Bevor Sie Synchronisierungsstatusberichte erstellen können, müssen Sie Folgendes tun:

- Fügen Sie Ihrer Amazon S3 Zugriffsrichtlinie den folgenden Amazon Kendra Dienstprinzipal hinzu

```
{
    “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/*”
        }
    ]
}
```

- Erstellen Sie einen Amazon S3 Bucket mit Zugriffsberechtigungen für Amazon Kendra

Wenn Sie die Konsole verwenden, um einen Synchronisierungsstatusbericht zu generieren, aktivieren Sie auf der Seite mit den Datenquellendetails die Option zum Generieren des Synchronisierungsverlaufs. Geben Sie dann den Amazon S3 Bucket-Speicherort ein und wählen Sie aus den verfügbaren Konfigurationsoptionen. Berichte werden bei der nächsten Synchronisierung generiert, nachdem Sie die Option Bericht generieren aktiviert haben.

Wenn Sie den Amazon S3 Bucket löschen, verlieren Sie Ihre Protokolldaten und müssen einen neuen Bucket einrichten, um neue Synchronisierungsberichte zu speichern.

Das Generieren des Status von Synchronisierungsberichten wird derzeit nur für den Amazon S3 Connector unterstützt.

Wie viel Zeit nimmt das Synchronisieren einer Datenquelle in Anspruch?

Wenn Dokumente nicht aktualisiert werden, erhöht sich die Synchronisierungszeit für einen Amazon Kendra Index linear proportional zur Anzahl der Dokumente. Beispielsweise würde die Synchronisierung von 1.000 Dokumenten ohne Aktualisierungen etwa fünf Minuten dauern, und bei 2.000 Dokumenten ohne Aktualisierungen etwa 10 Minuten. Wenn die Dokumente aktualisiert werden, erhöht sich die Synchronisierungszeit je nach Anzahl der aktualisierten Dokumente.

Wie hoch sind die Gebühren für die Synchronisierung einer Datenquelle?

Wenn Sie Ihren Index synchronisieren, dauert das Aufwärmen und Aktivieren zwei Minuten Amazon EC2 , um die erforderlichen Verbindungen herzustellen. Während dieses Vorgangs werden Ihnen keine Gebühren berechnet. Ihr Nutzungszähler beginnt erst, nachdem der Synchronisierungsjob

gestartet wurde. Weitere Informationen zur Amazon Kendra Preisgestaltung finden Sie unter Amazon Kendra Preise.

Ich erhalte einen Amazon EC2 Autorisierungsfehler

Wenn während einer Synchronisierung für eine Virtual Private Cloud (VPC) -Datenquelle ein Fehler bei einem Amazon EC2 nicht autorisierten Vorgang auftritt, fehlen Ihrer IAM VPC-Rolle wahrscheinlich die erforderlichen Berechtigungen. Bitte überprüfen Sie, ob die IAM Rolle, die Sie für Ihre Datenquelle verwenden, über die entsprechenden Berechtigungen verfügt. Weitere Informationen finden Sie unter IAM Rolle „Virtuelle private Cloud“.

Ich kann keine Suchindexlinks verwenden, um meine Amazon S3 Objekte zu öffnen

Ihr Amazon Kendra Index kann nur auf Dateien zugreifen, für die ihm eine Amazon S3 Datenquelle Zugriffsberechtigungen erteilt. Beispielsweise Amazon Kendra können die Amazon S3 Berechtigungen, die festlegen, ob ein Objekt öffentlich oder verschlüsselt sein soll, nicht geändert werden. Amazon Kendra verfügt auch nicht über die Standardberechtigungen, um einen signierten Link für Amazon S3 Objekte zu erstellen oder zurückzugeben. Wenn Sie signierte Verknüpfungen für Amazon S3 Objekte in einem Amazon Kendra Index aktivieren möchten, haben Sie zwei Möglichkeiten:

- Sie können Ihre Indexabfrageergebnisse mit dem Quell-URI-Objekt signieren, bevor Sie das Ergebnis an die Suchseite zurückgeben. Eine step-by-step exemplarische Vorgehensweise für diesen Vorgang finden Sie unter Freigeben von Objekten mithilfe vorsignierter URLs.
- Sie können die Quell-URI der Amazon S3 Objektmetadaten überschreiben und Ihren Service über ein CloudFront Content Delivery Network (CDN) verfügbar machen, das mit einem Bucket verbunden ist. Amazon S3 Sie können auch einen API Gateway Proxy-Endpunkt verwenden, der eine vorsignierte URL zurückgibt und zu dieser weiterleitet.

Ich erhalte eine Fehlermeldung AccessDenied bei Verwendung der SSL-Zertifikatsdatei

Wenn Sie bei der Verwendung eines SSL-Zertifikats mit Ihrer Datenquelle die Fehlermeldung „Zugriff verweigert“ erhalten, stellen Sie sicher, dass Ihre IAM Rolle berechtigt ist, auf die SSL-Zertifikatsdatei am angegebenen Speicherort zuzugreifen. Wenn das Zertifikat mit einem AWS KMS

Schlüssel verschlüsselt ist, sollte Ihre IAM Rolle auch die Berechtigung haben, es mithilfe des AWS KMS Schlüssels zu entschlüsseln. Weitere Informationen finden Sie unter Authentifizierung und Zugriffskontrolle für AWS KMS.

Ich erhalte einen Autorisierungsfehler, wenn ich eine SharePoint Datenquelle verwende

Wenn Sie beim Synchronisieren Ihres Indexes mit einer SharePoint Datenquelle einen Autorisierungsfehler erhalten, vergewissern Sie sich, dass Ihnen eine Site-Administrator-Rolle zugewiesen wurde. SharePoint

Mein Index crawlt keine Dokumente aus meiner Confluence-Datenquelle

Wenn dein Amazon Kendra Index während des Synchronisierungsvorgangs keine Dokumente aus deiner Confluence-Datenquelle crawlt, vergewissere dich, dass du Teil der Administratorgruppen in Confluence bist.

Problembehandlung bei Suchergebnissen in Dokumenten

Dieser Abschnitt kann Ihnen helfen, Probleme in Ihren Amazon Kendra Suchergebnissen zu beheben.

Meine Suchergebnisse sind für meine Suchanfrage nicht relevant

Wenn Ihre Suchergebnisse irrelevant erscheinen, kann das folgende Gründe haben:

- `LOW`Zuverlässige Ergebnisse sind in den Ergebnissen enthalten. Sie können Ergebnisse mit `LOW` Sicherheit herausfiltern, indem Sie das `ScoreAttributes` Feld QueryResultItems verwenden, um alle Ergebnisse mit einem Wert von auszuschließen`LOW`. Amazon Kendra weist jedem Ergebnis einen Konfidenzwert von entweder `VERY_HIGH`HIGH, `MEDIUM` und `LOW` zu. Diese Werte geben das Maß an Sicherheit an, mit dem ein Ergebnis für eine Abfrage relevant ist. Außerdem werden unabhängig von den Konfidenzbereichen drei Arten von Ergebnissen in der folgenden Reihenfolge Amazon Kendra zurückgegeben: `ANSWER` (Auszug mit der vorgeschlagenen Antwort), (Häufig gestellte Fragen) und `QUESTION_ANSWER` `DOCUMENT` (Auszug aus dem Dokument). Daher ist es möglich, dass ein `LOW` `QUESTION_ANSWER` Konfidenzergebnis über einem `VERY_HIGH` Konfidenzergebnis positioniert wird. `DOCUMENT` Es stimmt jedoch nicht immer, dass `LOW` Vertrauen ein besseres Ergebnis `QUESTION_ANSWER` ist als `VERY_HIGH` Konfidenz`DOCUMENT`.

- Bestimmte Metadatenfelder oder Attribute werden auf einen sehr hohen Wert angehoben, was sich auf die Rangfolge der Ergebnisse auswirkt. Amazon Kendra durchsucht Ihren Index anhand mehrerer Parameter wie Dokumenttitel, Text, Datum und benutzerdefinierten Textfeldern oder Attributen. Sie können mit verschiedenen Boosting-Werten experimentieren, um bei allen Abfragen die besten Ergebnisse zu erzielen. Sie können auch die dynamische Relevanzoptimierung auf Abfrageebene verwenden, um für jede Abfrage unterschiedliche Boosting-Werte zu verwenden.
- Ihre Benutzer verwenden spezielle Begriffe, wenn sie Informationen abfragen, und es gibt keine benutzerdefinierten Synonyme für Ihren Index, um diese Fachbegriffe zu behandeln. Weitere Informationen darüber, wie und wann Synonyme verwendet werden sollten, finden Sie unter Hinzufügen von benutzerdefinierten Synonymen zu einem Index.

Warum sehe ich nur 100 Ergebnisse?

Amazon Kendra gibt die Gesamtzahl der relevanten Dokumente zurück. Die 100 besten werden standardmäßig pro Abfrage zurückgegeben. Die Ergebnisse sind paginiert. Sie können verwenden`PageNumber`, um auf verschiedene Seiten zuzugreifen.

Sie können so konfigurieren Amazon Kendra , dass bis zu 1.000 Dokumente oder Suchergebnisse pro Abfrage mit bis zu 100 Ergebnissen pro Seite zurückgegeben werden. Um mehr als 100 Ergebnisse zurückzugeben, können Sie dies anfordern, indem Sie sich an den Quotas-Support wenden. Eine Erhöhung der Anzahl der Suchergebnisse könnte sich auf die Latenz auswirken.

Warum fehlen Dokumente, die ich erwarte?

Amazon Kendra unterstützt Zugriffskontrolllisten (ACLs), die auf Benutzern und Gruppen basieren. Amazon Kendra nimmt ACL-Richtlinien über Konnektoren auf. Wenn ein Index keine ACL konfiguriert, werden nur Dokumente angezeigt, die dem Attributfilter für Benutzer und Gruppe entsprechen. Wenn ein Benutzer- oder Gruppenattributfilter bereitgestellt wird, werden Dokumente ohne ACL nicht angezeigt.

Wenn Sie die tokenbasierte Zugriffskontrolle verwenden, werden Dokumente ohne ACL-Richtlinie und Dokumente, die dem Benutzer und den Gruppen entsprechen, angezeigt.

Warum sehe ich Dokumente, für die eine ACL-Richtlinie gilt?

Wenn ein Index keine Zugriffskontrollrichtlinie konfiguriert, können Benutzer und Gruppen über den Filter bereitgestellt werden. Wenn kein Benutzer- und Gruppenfilter angewendet wird, werden alle zugehörigen Dokumente zurückgegeben. Jede ACL-Richtlinie wird ignoriert.

Fehlerbehebung bei allgemeinen Problemen

Amazon Kendra verwendet CloudWatch Metriken und Protokolle, um Einblicke in die Synchronisation Ihrer Datenquellen zu erhalten. Anhand der Metriken und Protokolle können Sie feststellen, was bei einem Synchronisierungslauf schief gelaufen ist und wie Sie das Problem beheben können.

Beginnen Sie bei der allgemeinen Problembehandlung mit Ihren CloudWatch Metriken.

- Überprüfen Sie anhand der `DocumentsCrawled` Metrik, wie viele Dokumente Ihre Datenquelle überprüft hat. Wenn die Anzahl bei einem Amazon S3 Bucket geringer ist als erwartet, überprüfen Sie, ob Ihre Datenquelle auf den richtigen Bucket verweist.
- Überprüfen Sie anhand der `DocumentsSkippedNoChange` Metrik, wie viele Dokumente übersprungen wurden, da sie sich seit der letzten Synchronisation nicht geändert haben. Wenn die Zahl nicht Ihren Erwartungen entspricht, überprüfen Sie, ob Ihr Repository korrekt aktualisiert wurde.
- Prüfen Sie anhand der `DocumentsSkippedInvalidMetadata` Metrik, wie viele Dokumente ungültige Metadaten enthielten. Sehen Sie in Ihren CloudWatch Protokollen nach, welche spezifischen Fehler aufgetreten sind.
- Anhand der `DocumentsSubmittedForIndexingFailed` Metrik können Sie feststellen, wie viele Dokumente von der Datenquelle an den Index gesendet wurden, aber nicht indexiert werden konnten. Wenn Sie beispielsweise ein Metadatenattribut in einer Amazon S3 Datenquelle verwenden, die nicht als benutzerdefiniertes Indexfeld definiert wurde, wird das Dokument nicht indexiert. Sehen Sie in Ihren CloudWatch Protokollen nach, welche spezifischen Fehler aufgetreten sind.
- Anhand der `DocumentsSubmittedForDeletionFailed` Metrik können Sie feststellen, wie viele Dokumente, die die Datenquelle aus dem Index zu entfernen versuchte, nicht aus dem Index gelöscht werden konnten. Sehen Sie in Ihren CloudWatch Protokollen nach, welche spezifischen Fehler aufgetreten sind.

Sie können sich die CloudWatch Protokolle für einen bestimmten Synchronisierungslauf ansehen, um Einzelheiten zu den Fehlern zu erhalten, die während des Synchronisierungslaufs aufgetreten sind. Weitere Hinweise zu CloudWatch Protokollen mit Amazon Kendra finden Sie unter CloudWatch Logs.

Amazon KendraIntelligentes Ranking

Amazon KendraIntelligent Ranking verwendet Amazon Kendra semantische Suchfunktionen, um die Ergebnisse eines Suchdienstes intelligent neu zu bewerten.

Themen

Amazon Kendra Intelligentes Ranking für Selbstverwalter OpenSearch

Sie können die semantischen Suchfunktionen nutzen, um die Suchergebnisse Amazon Kendra des selbstverwalteten Open-Source-Suchdienstes OpenSearch, der auf der Apache 2.0-Lizenz basiert, zu verbessern. Das Amazon Kendra Intelligent Ranking-Plugin ordnet die Ergebnisse semantisch neu an mithilfe OpenSearch von. Amazon Kendra Dazu wird die Bedeutung und der Kontext einer Suchabfrage anhand bestimmter Felder, wie z. B. des Hauptteils oder des Titels des Dokuments, aus den OpenSearch Standard-Suchergebnissen verstanden.

Nehmen wir zum Beispiel diese Abfrage: „Haupt-Keynote-Adresse“. Da „Adresse“ mehrere Bedeutungen hat, Amazon Kendra kann die Bedeutung hinter der Anfrage abgeleitet werden, sodass relevante Informationen zurückgegeben werden, die der beabsichtigten Bedeutung entsprechen. In diesem Zusammenhang handelt es sich um eine Grundsatzrede auf einer Konferenz. Ein einfacherer Suchdienst berücksichtigt die Absicht möglicherweise nicht und könnte beispielsweise Ergebnisse für eine Straßenadresse an der Main Street zurückgeben.

Das Intelligent Ranking-Plugin für OpenSearch ist für die OpenSearch (selbstverwaltete) Version 2.4.0 und höher verfügbar. Sie können das Plugin mithilfe eines Schnellstart-Bash-Skripts installieren, um ein neues Docker-Image OpenSearch mit dem mitgelieferten Intelligent Ranking-Plugin zu erstellen. Sehen Sie Einrichtung des intelligenten Such-Plugins — dies ist ein Beispiel für ein Setup, mit dem Sie schnell loslegen können.

So funktioniert das intelligente Such-Plugin

Der Gesamtprozess des Intelligent Ranking-Plugins für OpenSearch (selbst verwaltet) sieht wie folgt aus:

1. Ein OpenSearch Benutzer gibt eine Abfrage aus und OpenSearch gibt eine Antwort auf die Anfrage oder eine Liste von Dokumenten, die für die Abfrage relevant sind.
2. Das Intelligent Ranking-Plugin verwendet die Antwort auf die Anfrage und extrahiert Informationen aus den Dokumenten.
3. Das Intelligent Ranking-Plugin ruft die Rescore-API von Amazon Kendra Intelligent Ranking auf.
4. Die `Rescore` API verwendet die extrahierten Informationen aus den Dokumenten und ordnet die Suchergebnisse semantisch neu.
5. Die `Rescore` API sendet die neu eingestuften Suchergebnisse zurück an das Plugin. Das Plugin ordnet die Suchergebnisse in der OpenSearch Suchantwort neu an, um das neue semantische Ranking widerzuspiegeln.

Das Intelligent Ranking-Plugin ordnet die Ergebnisse anhand der Felder „Hauptteil“ und „Titel“ neu an. Diese Plugin-Felder können Feldern in Ihrem OpenSearch Index zugeordnet werden, die der Definition des Hauptteils und des Titels eines Dokuments am ehesten entsprechen. Wenn Ihr Index beispielsweise Kapitel eines Buches mit Feldern wie „chapter_heading“ und „chapter_contents“ enthält, können Sie erstere dem „Titel“ und letztere dem „Hauptteil“ zuordnen, um die besten Ergebnisse zu erzielen.

Einrichtung des intelligenten Such-Plugins

Im Folgenden wird beschrieben, wie Sie das Intelligent Ranking-Plugin schnell einrichten OpenSearch (selbst verwalten) können.

Einrichtung OpenSearch (selbst verwaltet) mit dem Intelligent Ranking-Plugin (schnelle Einrichtung)

Wenn Sie bereits ein Docker-Image verwendenopensearch:2.4.0, können Sie dieses Dockerfile verwenden, um mit dem Intelligent Ranking-Plugin ein neues Image von OpenSearch 2.4.0 zu erstellen. Sie fügen einen Container für das neue Bild in Ihre docker-compose.yml-Datei oder opensearch.yml-Datei ein. Sie geben auch Ihre generierte Rescore-Ausführungsplan-ID bei der Erstellung eines Rescore-Ausführungsplans zusammen mit Ihren Regions- und Endpunktinformationen an — siehe Schritt 2 zur Erstellung eines Rescore-Ausführungsplans.

Wenn Sie zuvor eine Version des `opensearch` Docker-Images heruntergeladen haben, die älter als 2.4.0 ist, müssen Sie das Docker-Image `opensearch:2.4.0` oder eine neuere Version verwenden und ein neues Image mit dem mitgelieferten Intelligent Ranking-Plugin erstellen.

1. Laden Sie Docker Desktop für Ihr Betriebssystem herunter und installieren Sie es. Docker Desktop umfasst Docker Compose und Docker Engine. Es wird empfohlen, dass Sie überprüfen, ob Ihr Computer die in den Docker-Installationsdetails genannten Systemanforderungen erfüllt.

   Sie können Ihre Anforderungen an die Speichernutzung auch in den Einstellungen Ihres Docker-Desktops erhöhen. Sie sind für die Nutzungsanforderungen von Docker außerhalb der frei verfügbaren Nutzungsbeschränkungen für Docker-Dienste verantwortlich. Siehe Docker-Abonnements.

   Überprüfen Sie, ob der Docker Desktop-Status „läuft“ lautet.

2. Stellen Sie Amazon Kendra Intelligent Ranking und Ihre Kapazitätsanforderungen bereit. Sobald Sie Amazon Kendra Intelligent Ranking bereitgestellt haben, wird Ihnen eine stündliche Abrechnung auf der Grundlage Ihrer festgelegten Kapazitätseinheiten berechnet. Weitere Informationen zum kostenlosen Kontingent und zu den Preisen finden Sie hier.

   Sie verwenden die CreateRescoreExecutionPlanAPI zur Bereitstellung von`Rescore API`. Wenn Sie nicht mehr Kapazitätseinheiten als die Standardkapazität für eine Einheit benötigen, fügen Sie keine weiteren Einheiten hinzu und geben Sie nur einen Namen für Ihren Rescore-Ausführungsplan an. Sie können Ihre Kapazitätsanforderungen auch mithilfe der UpdateRescoreExecutionPlanAPI aktualisieren. Weitere Informationen finden Sie unter Semantisches Ranking der Ergebnisse eines Suchdienstes.

   Optional können Sie mit Schritt 3 fortfahren, um einen standardmäßigen Rescore-Ausführungsplan zu erstellen, wenn Sie das Schnellstart-Bash-Skript ausführen.

   Notieren Sie sich für Schritt 4 die in der Antwort enthaltene Rescore-Ausführungsplan-ID.

   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. Laden Sie das Schnellstart-Bash-Skript von GitHub für Ihre Version von herunter, OpenSearch indem Sie den Versionszweig aus dem Drop-down-Menü für den Hauptzweig auswählen.

   Dieses Skript verwendet Docker-Images für OpenSearch und OpenSearch Dashboards, die Ihre Version verwenden, die Sie im GitHub Repository für das Skript ausgewählt haben. Es lädt eine ZIP-Datei für das Intelligent Ranking-Plugin herunter und generiert ein, `Dockerfile` um ein neues Docker-Image zu erstellen OpenSearch , das das Plugin enthält. Außerdem wird eine docker-compose.yml-Datei erstellt, die Container für das Intelligent Ranking-Plugin und OpenSearch Dashboards enthält. OpenSearch Das Skript fügt Ihre Rescore-Ausführungsplan-ID, Regionsinformationen und Endpunkt (verwendet die Region) zur Datei docker-compose.yml hinzu. Das Skript wird dann ausgeführt, `docker-compose up` um die Container für OpenSearch inklusive Intelligent Ranking und Dashboards zu starten. OpenSearch Führen `docker-compose stop` Sie den Befehl aus, um die Container zu stoppen, ohne sie zu entfernen. Führen Sie den Befehl aus, um die Container zu entfernen`docker-compose down`.

4. Öffnen Sie Ihr Terminal und führen Sie im Verzeichnis des Bash-Skripts den folgenden Befehl aus.

   ```
   bash search_processing_kendra_quickstart.sh -p <execution-plan-id> -r <region>
   ```

   Wenn Sie diesen Befehl ausführen, geben Sie die Rescore-Ausführungsplan-ID, die Sie in Schritt 2 bei der Bereitstellung von Amazon Kendra Intelligent Ranking notiert haben, zusammen mit Ihren Regionsinformationen an. Optional können Sie Amazon Kendra Intelligent Ranking stattdessen mithilfe der `--create-execution-plan` Option bereitstellen. Dadurch wird ein Rescore-Ausführungsplan mit einem Standardnamen und einer Standardkapazität erstellt.

   Um Ihren Index nicht zu verlieren, wenn der standardmäßige temporäre Container entfernt wird, können Sie Ihren Index über alle Ausführungen hinweg beibehalten lassen, indem Sie den Namen des Datenvolumes mithilfe der Option angeben. `--volume-name` Wenn Sie zuvor einen Index erstellt haben, können Sie das Volume in Ihrer Datei docker-compose.yml oder

opensearch.yml angeben. Um Ihre Volumes intakt zu lassen, führen Sie das Programm nicht aus. `docker-compose down -v`

Das Schnellstart-Bash-Skript konfiguriert Ihre AWS Anmeldeinformationen im OpenSearch Keystore, um eine Verbindung zu Intelligent Ranking herzustellen. Amazon Kendra Um Ihre AWS Anmeldeinformationen für das Skript bereitzustellen, verwenden Sie die `--profile` Option, um das Profil anzugeben. AWS Wenn die `--profile` Option nicht angegeben ist, versucht das Schnellstart-Bash-Skript, AWS Anmeldeinformationen (Zugriffs-/Geheimschlüssel, optionales Sitzungstoken) aus Umgebungsvariablen und dann aus dem Standardprofil zu lesen. AWS Wenn die `--profile` Option nicht angegeben ist und keine Anmeldeinformationen gefunden werden, leitet das Skript keine Anmeldeinformationen an den Keystore weiter. OpenSearch Wenn im OpenSearch Keystore keine Anmeldeinformationen angegeben sind, überprüft das Plugin trotzdem die Anmeldeinformationen in der Standard-Credential-Provider-Kette, einschließlich Amazon ECS Container-Anmeldeinformationen oder Instanzprofil-Anmeldeinformationen, die über den Metadatendienst bereitgestellt werden. Amazon EC2

Stellen Sie sicher, dass Sie eine IAM Rolle mit den erforderlichen Berechtigungen erstellt haben, um Intelligent Ranking aufzurufen Amazon Kendra . Im Folgenden finden Sie ein Beispiel für eine IAM Richtlinie zur Erteilung der Erlaubnis zur Verwendung der `Rescore` API für einen bestimmten Rescore-Ausführungsplan:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "kendra-ranking:Rescore",
            "Resource": "arn:aws:kendra-ranking:${Region}:${Account}:rescore-
execution-plan/${RescoreExecutionPlanId}"
        }
    ]
}
```

Beispiel für docker-compose.yml

Ein Beispiel für eine docker-compose.yml-Datei, die 2.4.0 oder höher mit dem Intelligent Ranking-Plugin und Dashboards OpenSearch 2.4.0 oder höher verwendet. 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
```

Beispiel für ein Dockerfile und das Erstellen eines Images

Ein Beispiel `Dockerfile` für die Verwendung von OpenSearch 2.4.0 oder höher mit dem Intelligent Ranking-Plugin.

```
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
```

Erstellen eines Docker-Images für OpenSearch mit dem Intelligent Ranking-Plugin.

```
docker build --tag=<Docker image tag name of OpenSearch with Intelligent Ranking
 plugin>
```

Interaktion mit dem intelligenten Such-Plugin

Sobald Sie das Intelligent Ranking-Plugin eingerichtet OpenSearch (selbst verwaltet) haben, können Sie mithilfe von Curl-Befehlen oder OpenSearch Client-Bibliotheken mit dem Plugin interagieren. Die Standardanmeldedaten für den Zugriff OpenSearch mit dem Intelligent Ranking-Plugin sind der Benutzername „admin“ und das Passwort „admin“.

So wenden Sie die Plugin-Einstellungen für Intelligent Ranking auf einen Index an 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)
```

Sie müssen den Namen des Haupttextfeldes angeben, das Sie für die Rangfolge verwenden möchten, z. B. den Hauptteil eines Dokuments oder ein Feld mit dem Dokumentinhalt. Sie können auch andere Textfelder wie den Dokumenttitel oder die Dokumentzusammenfassung einbeziehen.

Jetzt können Sie jede beliebige Abfrage stellen und die Ergebnisse werden mit dem Intelligent Ranking-Plugin eingestuft.

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)
```

Um die Plugin-Einstellungen für Intelligent Ranking für einen OpenSearch Index zu entfernen:

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)
```

Um das Intelligent Ranking-Plugin mit einer bestimmten Abfrage oder mit bestimmten Text- und Titelfeldern zu testen:

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)
```

OpenSearch Ergebnisse mit Amazon Kendra Ergebnissen vergleichen

Sie können side-by-side OpenSearch (selbst verwaltete) Rangfolge mit Ergebnissen mit neu eingestuften Ergebnissen vergleichen. Amazon Kendra OpenSearch Die Dashboard-Version 2.4.0 und höher bietet side-by-side Ergebnisse, sodass Sie die Rangfolge von Dokumenten mit der OpenSearch Rangfolge von Amazon Kendra Dokumenten für eine Suchabfrage vergleichen können.

Bevor Sie OpenSearch Rangergebnisse mit Ergebnissen vergleichen können, die Amazon Kendra neu eingestuft wurden, stellen Sie sicher, dass Ihre OpenSearch Dashboards von einem OpenSearch Server mit dem Intelligent Ranking-Plugin unterstützt werden. Sie können dies mit Docker und einem Schnellstart-Bash-Skript einrichten. Siehe Einrichtung des intelligenten Such-Plugins.

Im Folgenden wird beschrieben, wie Sie Ergebnisse in OpenSearch OpenSearch Dashboards vergleichen und Amazon Kendra suchen. Weitere Informationen finden Sie in der OpenSearchDokumentation.

Suchergebnisse in OpenSearch Dashboards vergleichen

1. Öffnen Sie http://localhost:5601 und melden Sie sich bei OpenSearch Dashboards an. Die Standardanmeldedaten sind der Benutzername „admin“ und das Passwort „admin“.
2. Wählen Sie in den OpenSearch Plugins im Navigationsmenü die Option Suchrelevanz aus.
3. Geben Sie den Suchtext in die Suchleiste ein.
4. Wählen Sie Ihren Index für Abfrage 1 aus und geben Sie eine Abfrage in die OpenSearch Query DSL ein. Sie können die `%SearchText%` Variable verwenden, um auf den Suchtext zu verweisen, den Sie in die Suchleiste eingegeben haben. Ein Beispiel für diese Abfrage finden Sie in der OpenSearch Dokumentation. Die für diese Abfrage zurückgegebenen Ergebnisse sind die OpenSearch Ergebnisse ohne Verwendung des Intelligent Ranking-Plug-ins.
5. Wählen Sie denselben Index für Abfrage 2 aus und geben Sie dieselbe Abfrage in die OpenSearch Query-DSL ein. Geben Sie außerdem die Erweiterung mit an `kendra_intelligent_ranking` und geben Sie die obligatorische Erweiterung an, `body_field` nach der die Rangfolge erfolgen soll. Sie können auch das Titelfeld angeben, aber das Textfeld ist ein Pflichtfeld. Ein Beispiel für diese Abfrage finden Sie in der OpenSearch Dokumentation. Bei den für diese Abfrage zurückgegebenen Ergebnissen handelt es sich um Ergebnisse, die mit dem Intelligent Ranking-Plugin Amazon Kendra neu eingestuft wurden. Das Plugin bewertet bis zu 25 Ergebnisse.
6. Wählen Sie Suchen, um die Ergebnisse zurückzugeben und zu vergleichen.

Semantisches Ranking der Ergebnisse eines Suchdienstes

Amazon Kendra Intelligent Ranking nutzt Amazon Kendra die semantischen Suchfunktionen, um die Ergebnisse eines Suchdienstes neu zu ordnen. Dabei werden der Kontext der Suchabfrage sowie alle verfügbaren Informationen aus den Dokumenten des Suchdienstes berücksichtigt. Amazon Kendra Intelligentes Ranking kann den einfachen Keyword-Abgleich verbessern.

Die CreateRescoreExecutionPlanAPI erstellt eine Amazon Kendra Intelligent Ranking-Ressource, die für die Bereitstellung der Rescore-API verwendet wird. Die `Rescore` API ordnet Suchergebnisse eines Suchdienstes wie OpenSearch (selbst verwaltet) neu ein.

Wenn Sie aufrufen`CreateRescoreExecutionPlan`, legen Sie die benötigten Kapazitätseinheiten fest, um die Ergebnisse eines Suchdienstes neu einzuordnen. Wenn Sie nicht mehr Kapazitätseinheiten als den Standard für einzelne Einheiten benötigen, ändern Sie den Standard nicht. Geben Sie nur einen Namen für Ihren Rescore-Ausführungsplan an. Sie können bis zu 1000 zusätzliche Einheiten einrichten. Informationen darüber, was in einer einzelnen Kapazitätseinheit enthalten ist, finden Sie unter Kapazität anpassen. Sobald Sie Amazon Kendra Intelligent Ranking bereitgestellt haben, wird Ihnen eine stündliche Abrechnung auf der Grundlage Ihrer festgelegten Kapazitätseinheiten berechnet. Weitere Informationen zum kostenlosen Kontingent und zu den Preisen finden Sie hier.

Eine Rescore-Ausführungsplan-ID wird generiert und in der Antwort zurückgegeben, wenn Sie anrufen`CreateRescoreExecutionPlan`. Die `Rescore` API verwendet die Rescore-Ausführungsplan-ID, um die Ergebnisse eines Suchdienstes anhand der von Ihnen festgelegten Kapazität neu zu ordnen. Sie nehmen die Rescore-Ausführungsplan-ID in die Konfigurationsdateien Ihres Suchdienstes auf. Wenn Sie beispielsweise OpenSearch (selbst verwaltet) verwenden, fügen Sie die Rescore-Ausführungsplan-ID in Ihre Datei docker-compose.yml oder opensearch.yml ein — siehe Ergebnisse intelligent ordnen (Self-Service). OpenSearch

Ein Amazon-Ressourcenname (ARN) wird auch in der Antwort generiert, wenn Sie anrufen`CreateRescoreExecutionPlan`. Sie können diesen ARN verwenden, um eine Berechtigungsrichtlinie in AWS Identity and Access Management (IAM) zu erstellen, um den Benutzerzugriff auf einen bestimmten ARN für einen bestimmten Rescore-Ausführungsplan einzuschränken. Ein Beispiel für eine IAM Richtlinie zur Erteilung der Erlaubnis zur Verwendung der `Rescore` API für einen bestimmten Rescore-Ausführungsplan finden Sie unter Amazon Kendra Intelligentes Ranking für selbstverwaltete Systeme. OpenSearch

Im Folgenden finden Sie ein Beispiel für die Erstellung eines Rescore-Ausführungsplans mit Kapazitätseinheiten, die auf 1 gesetzt sind.

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.");
  }
}
```

Im Folgenden finden Sie ein Beispiel für die Aktualisierung eines Rescore-Ausführungsplans, sodass die Kapazitätseinheiten auf 2 festgelegt werden.

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.");
  }
}
```

Im Folgenden finden Sie ein Beispiel für die Verwendung der `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());
  }
}
```

Dokumentverlauf für Amazon Kendra

- Letzte Aktualisierung der Dokumentation: 27. Februar 2024

In der folgenden Tabelle werden wichtige Änderungen in jeder Version von beschrieben Amazon Kendra. Um Benachrichtigungen über Aktualisierungen dieser Dokumentation zu erhalten, können Sie den RSS-Feed abonnieren.

Änderung	Beschreibung	Datum
Neues Feature	Amazon Kendra unterstützt jetzt eine aktualisierte Version des GitHub Datenquellen-Connectors. Weitere Informationen finden Sie unter GitHub.	27. Februar 2024
Neues Feature	Amazon Kendra unterstützt jetzt eine aktualisierte Version des Amazon FSx Datenquellen-Konnektors. Weitere Informationen finden Sie unter Amazon FSx (Windows) und Amazon FSx (NetApp ONTAP).	8. Februar 2024
Neues Feature	Amazon Kendra unterstützt jetzt eine aktualisierte Version des Slack-Datenquellen-Konnektors. Weitere Informationen finden Sie unter Slack.	11. Januar 2024
Neues Feature	Amazon Kendra unterstützt jetzt das Ein- und Erweitern Ihrer Suchergebnisse. Weitere Informationen finden Sie unter	19. Oktober 2023

	Eingrenzen/Erweitern von Suchergebnissen.	
Neues Feature	Amazon Kendra unterstützt jetzt einen Aurora (MySQL)-Datenquellen-Konnektor. Weitere Informationen finden Sie unter Aurora (MySQL).	28. September 2023
Neues Feature	Amazon Kendra unterstützt jetzt einen Aurora (PostgreSQL)-Datenquellen-Konnektor. Weitere Informationen finden Sie unter Aurora (PostgreSQL).	28. September 2023
Neues Feature	Amazon Kendra unterstützt jetzt einen Amazon RDS (MySQL)-Datenquellen-Konnektor. Weitere Informationen finden Sie unter Amazon RDS (MySQL).	28. September 2023
Neues Feature	Amazon Kendra unterstützt jetzt einen Amazon RDS (Microsoft SQL Server)-Datenquellen-Connector. Weitere Informationen finden Sie unter Amazon RDS (Microsoft SQL Server).	28. September 2023
Neues Feature	Amazon Kendra unterstützt jetzt einen Amazon RDS (Oracle)-Datenquellen-Konnektor. Weitere Informationen finden Sie unter Amazon RDS (Oracle).	28. September 2023

Neues Feature	Amazon Kendra unterstützt jetzt einen Amazon RDS (PostgreSQL)-Datenquellen-Konnektor. Weitere Informationen finden Sie unter Amazon RDS (PostgreSQL).	28. September 2023
Neues Feature	Amazon Kendra unterstützt jetzt einen IBM DB2-Datenquellen-Connector. Weitere Informationen finden Sie unter IBM DB2.	28. September 2023
Neues Feature	Amazon Kendra unterstützt jetzt einen Microsoft SQL Server-Datenquellen-Connector. Weitere Informationen finden Sie unter Microsoft SQL Server.	28. September 2023
Neues Feature	Amazon Kendra unterstützt jetzt einen MySQL-Datenquellen-Konnektor. Weitere Informationen finden Sie unter MySQL.	28. September 2023
Neues Feature	Amazon Kendra unterstützt jetzt einen Oracle Database-Datenquellen-Connector. Weitere Informationen finden Sie unter Oracle Database .	28. September 2023
Neues Feature	Amazon Kendra unterstützt jetzt einen PostgreSQL-Datenquellen-Konnektor. Weitere Informationen finden Sie unter PostgreSQL .	28. September 2023

Neues Feature	Amazon Kendra bietet jetzt einen Datenquellen-Konnektor für Drupal. Weitere Informationen finden Sie unter Drupal.	6. September 2023
Neues Feature	Rufen Sie semantisch relevante Passionen mit der Amazon Kendra Retrieve API for Retrieval Augmented Generation (RAG)-Systeme ab.	22. Juni 2023
Neues Feature	Amazon Kendra unterstützt jetzt eine aktualisierte Version des Amazon Kendra Web-Crawler-Datenquellen-Konnektors. Weitere Informationen finden Sie unter Amazon Kendra Web Crawler v2.0.	21. Juni 2023
Regionale Erweiterung	Amazon Kendra ist jetzt in Europa (London) (eu-west-2) verfügbar.	5. Juni 2023
Neues Feature	Amazon Kendra unterstützt jetzt eine aktualisierte Version des Alfresco-Datenquellen-Connectors. Weitere Informationen finden Sie unter Alfresco.	16. Mai 2023
Neues Feature	Amazon Kendra bietet jetzt einen Datenquellen-Konnektor für Adobe Experience Manager. Weitere Informationen finden Sie unter Adobe Experience Manager.	11. Mai 2023

Neues Feature	Amazon Kendra unterstützt jetzt die Konfiguration von Dokumentfeldern/Attributen, wenn Sie aufrufen GetQuerySuggestions. Sie können jetzt Abfragevorschläge auf dem Inhalt von Dokumentfeldern basieren. Weitere Informationen finden Sie unter Abfragevorschläge.	2. Mai 2023
Neues Feature	Amazon Kendra bietet jetzt einen Datenquellen-Connector für Gmail. Weitere Informationen finden Sie unter Gmail.	13. April 2023
Neues Feature	Amazon Kendra unterstützt jetzt eine aktualisierte Version des Microsoft OneDrive-Datenquellen-Konnektors. Weitere Informationen finden Sie unter Microsoft OneDrive v2.0.	03. April 2023
Neues Feature	Verbessern Sie die Sichtbarkeit neuer Dokumente oder stufen Sie bestimmte Dokumente hoch, wenn Ihre Benutzer bestimmte Abfragen mit Featured results eingeben.	30. März 2023
Neues Feature	Amazon Kendra unterstützt jetzt einen aktualisierten Datenquellen-Connector für Microsoft SharePoint. Weitere Informationen finden Sie unter Microsoft SharePoint.	2. März 2023

Neues Feature	Amazon Kendra unterstützt jetzt eine aktualisierte Version des Confluence-Datenquellen-Konnektors. Weitere Informationen finden Sie unter Confluence.	1. März 2023
Regionale Erweiterung	Amazon Kendra ist jetzt in Asien-Pazifik (Tokio) (ap-northeast-1) verfügbar.	07. Februar 2023
Neues Feature	Amazon Kendra bietet jetzt einen Datenquellen-Connector für Microsoft Exchange. Weitere Informationen finden Sie unter Microsoft Exchange.	12. Januar 2023
Neues Feature	Amazon Kendra bietet jetzt einen Datenquellen-Connector für Microsoft Yammer. Weitere Informationen finden Sie unter Microsoft Yammer.	12. Januar 2023
Neues Feature	Amazon Kendra unterstützt jetzt die Indizierung von RTF-, XML-, XSLT-, MS_EXCEL-, CSV-, JSON- und MD-Dokumenttypen. Weitere Informationen finden Sie unter Dokumenttypen.	11. Januar 2023
Neues Feature	Amazon Kendra unterstützt jetzt eine aktualisierte Version des Amazon S3 Datenquellen-Connectors. Weitere Informationen finden Sie unter Amazon S3.	10. Januar 2023

Neues Feature	OpenSearch (selbstverwaltete) Suchergebnisse können mit Amazon Kendra Intelligent Ranking semantisch eingestuft werden.	9. Januar 2023
Neues Feature	Amazon Kendra bietet jetzt einen Datenquellen-Connector für Microsoft Teams. Weitere Informationen finden Sie unter Microsoft Teams.	5. Januar 2023
Neues Feature	Amazon Kendra verfügt über einen aktualisierten Datenquellen-Connector für Google Drive. Weitere Informationen finden Sie unter Google Drive.	5. Januar 2023
Neues Feature	Amazon Kendra verfügt über einen aktualisierten Datenquellen-Connector für ServiceNow. Weitere Informationen finden Sie unter ServiceNow.	21. Dezember 2022
Neues Feature	Amazon Kendra verfügt über einen aktualisierten Datenquellen-Connector für Salesforce. Weitere Informationen finden Sie unter Salesforce.	21. Dezember 2022
Regionale Erweiterung	Amazon Kendra ist jetzt in Asien-Pazifik (Mumbai) (ap-south-1) verfügbar.	14. Dezember 2022

Neues Feature	Amazon KendraDie tabellarische Suchfunktion von kann Antworten aus Tabellen durchsuchen und extrahieren, die in HTML-Dokumenten eingebettet sind.	27. November 2022
Neues Feature	Amazon Kendra unterstützt die semantische Suche nach einem ausgewählten Satz von Sprachen.	27. November 2022
Neues Feature	Amazon Kendra bietet jetzt einen Datenquellen-Konnektor für Dropbox. Weitere Informationen finden Sie unter Dropbox.	27. September 2022
Neues Feature	Amazon Kendra bietet jetzt einen Datenquellen-Connector für Zendesk. Weitere Informationen finden Sie unter Zendesk.	17. August 2022
Neues Feature	Die Zugriffskontrolle auf Dokumentebene kann jetzt neu konfiguriert werden, nachdem Sie Ihre Dokumente indiziert haben. Weitere Informationen finden Sie unter Konfiguration der Zugriffskontrolle .	14. Juli 2022
Neues Feature	Amazon Kendra bietet jetzt einen Datenquellen-Connector für Alfresco. Weitere Informationen finden Sie unter Alfresco.	30. Juni 2022

Neues Feature	Amazon Kendra bietet jetzt einen Datenquellen-Connector für GitHub. Weitere Informationen finden Sie unter GitHub.	2. Juni 2022
Neues Feature	Amazon Kendra bietet jetzt einen Datenquellen-Connector für JSpeed. Weitere Informationen finden Sie unter Jira.	12. Mai 2022
Neues Feature	Verschachtelte Facetten innerhalb einer Facette können in den Suchergebnissen angezeigt werden. Weitere Informationen finden Sie unter Facets.	5. Mai 2022
Neues Feature	Amazon Kendra bietet jetzt einen Datenquellen-Connector für Quip. Weitere Informationen finden Sie unter Warteschlange.	19. April 2022
Neues Feature	Amazon Kendra bietet jetzt einen Datenquellen-Konnektor für Box. Weitere Informationen finden Sie unter Feld .	6. April 2022
Neues Feature	Amazon Kendra bietet jetzt einen Datenquellen-Konnektor für Slack. Weitere Informationen finden Sie unter Slack.	14. März 2022
Neues Feature	Amazon Kendra bietet jetzt einen Datenquellen-Connector für Amazon FSx. Weitere Informationen finden Sie unter Amazon FSx.	8. Februar 2022

AWS Von verwaltete Richtlinienaktualisierungen – Neue Richtlinien	Amazon Kendra hat neue AWS verwaltete Richtlinien hinzugefügt. Weitere Informationen finden Sie unter AWS Verwaltete Richtlinien für Amazon Kendra.	3. Januar 2022
Neues Feature	Amazon Kendra Die - Suchanwendung kann mit wenigen Klicks bereitgestellt werden, ohne dass ein Frontend-Code erforderlich ist. Weitere Informationen finden Sie unter Bereitstellen einer Suchanwendung ohne Code .	1. Dezember 2021
Neues Feature	Dokumentmetadaten und -inhalte können während der Dokumentenerfassung erweitert werden. Weitere Informationen finden Sie unter Anpassen der Metadaten von Dokumenten während des Erfassungsprozesses.	1. Dezember 2021
Neues Feature	Amazon Kendra bietet Suchanalysen, um nützliche Einblicke in Ihre Suchanwendung zu erhalten. Weitere Informationen finden Sie unter Gewinnen von Erkenntnissen mit Suchanalysen.	1. Dezember 2021
Regionale Erweiterung	Amazon Kendra ist jetzt in AWS GovCloud (USA-West) (us-gov-west-1) verfügbar.	13. Oktober 2021

Neues Feature	Amazon Kendra kann jetzt Dokumente in mehreren Sprachen indizieren und Suchergebnisse nach Sprache filtern. Siehe Hinzufügen von Dokumenten in anderen Sprachen als Englisch und Suchen in Sprachen .	7. Oktober 2021
Neues Feature	Amazon Kendra ist jetzt in Identity-Center-Verzeichnis integriert, um Zugriffsebenen von Gruppen und Benutzern für die Benutzerkontextfil terung abzurufen. Siehe Benutzergruppenkonfiguration für IAM Identity Center .	6. Oktober 2021
Neues Tutorial	Amazon Kendra bietet jetzt ein Tutorial, das Sie durch die Erstellung einer mit Metadaten erweiterten Suchlösung führt. Weitere Informationen finden Sie unter Erstellen einer intelligenter Suchlösung.	13. August 2021
Neues Feature	Amazon Kendra bietet jetzt einen Datenquellen-Conne ctor für Amazon WorkDocs. Weitere Informationen finden Sie unter Amazon WorkDocs.	20. Juli 2021

Neues Feature	Amazon Kendra bietet jetzt einen Web-Crawler zum Crawlen und Indizieren von Webseiten. Weitere Informationen finden Sie unter Web-Crawler.	17. Juni 2021
Regionale Erweiterung	Amazon Kendra ist jetzt in Kanada (Zentral) (ca-central-1) verfügbar.	16. Juni 2021
Regionale Erweiterung	Amazon Kendra ist jetzt in USA Ost (Ohio) (us-east-2) verfügbar.	7. Juni 2021
Neues Feature	Amazon Kendra unterstützt jetzt Abfragevorschläge, bei denen Benutzern beliebte Abfragen vorgeschlagen werden, die für ihre Suche relevant sind. Weitere Informationen finden Sie unter Vorschläge für beliebte Suchabfragen.	27. Mai 2021
AWS Von verwaltete Richtlinienaktualisierungen – Neue Richtlinien	Amazon Kendra hat neue AWS verwaltete Richtlinien hinzugefügt. Weitere Informationen finden Sie unter AWS Verwaltete Richtlinien für Amazon Kendra.	27. Mai 2021
Regionale Erweiterung	Amazon Kendra ist jetzt in Asien-Pazifik (Singapur) (ap-southeast-1) verfügbar.	5. Mai 2021

Neues Feature	Amazon Kendra unterstützt jetzt die Optimierung der Suchrelevanz in der Abfrage, indem die auf Indexebene festgelegten Optimierungskonfigurationen überschrieben werden. Weitere Informationen finden Sie unter Optimieren der Suchrelevanz und Optimieren von Antworten.	20. April 2021
Neues Feature	Amazon Kendra unterstützt jetzt die OAuth-2.0-Authentifizierung und die Verwendung von ServiceNow Abfragen, um Dokumente für die Indizierung auszuwählen. Weitere Informationen finden Sie unter ServiceNow.	01. April 2021
Neues Feature	Amazon Kendra unterstützt jetzt inkrementelles Lernen für häufig gestellte Fragen. Weitere Informationen finden Sie unter Senden von Feedback für inkrementelles Lernen.	17. Februar 2021
Neues Feature	Amazon Kendra unterstützt jetzt Indexsynonyme. Weitere Informationen finden Sie unter Hinzufügen von Synonymen zu einem Index.	10. Dezember 2020

Neues Feature	Amazon Kendra bietet jetzt einen Datenbank-Connector für Google Workspace Drive. Weitere Informationen finden Sie unter Verwenden einer Google Workspace Drive-Datenquelle.	08. Dezember 2020
Neues Feature	Amazon Kendra bietet jetzt eine JavaScript Bibliothek, die es Ihnen erleichtert, Abfrage-Feedback an zu übermitte ln Amazon Kendra. Weitere Informationen finden Sie unter Senden von Feedback.	08. Dezember 2020
Neues Feature	Amazon Kendra unterstützt jetzt die tokenbasierte Benutzerzugriffskontrolle. Weitere Informationen finden Sie unter Steuern des Zugriffs auf Dokumente in einem Index .	5. November 2020
Neues Feature	Der Amazon Kendra Confluence-Datenquellen-Konnektor funktioniert jetzt mit der Confluence-Cloud. Weitere Informationen finden Sie unter Verwenden einer Confluence-Datenquelle.	5. November 2020
Regionale Erweiterung	Amazon Kendra ist jetzt in Asien-Pazifik (Sydney) (ap-southeast-2) verfügbar.	2. November 2020

Neues Feature	Amazon Kendra bietet jetzt einen Datenquellen-Connector für Confluence-Server. Weitere Informationen finden Sie unter Verwenden einer Confluence-Datenquelle.	26. Oktober 2020
Neues Feature	Amazon Kendra stellt jetzt eine Datenquelle bereit, mit der Sie Statistiken für Ihre benutzerdefinierten Connectors generieren können. Weitere Informationen finden Sie unter Verwenden einer benutzerdefinierten Datenquelle.	21. Oktober 2020
Neues Feature	Amazon Kendra unterstützt jetzt benutzerdefinierte Attribute für häufig gestellte Fragen. Weitere Informationen finden Sie unter Hinzufügen von Fragen und Antworten.	17. September 2020
Neues Feature	Amazon Kendra gibt jetzt Konfidenzwerte für Abfrageergebnisse zurück. Weitere Informationen finden Sie unter QueryResultItem.	15. September 2020
Neues Feature	AWS CloudFormation unterstützt jetzt Amazon Kendra. Weitere Informationen finden Sie in der Amazon Kendra Ressourcentypreferenz - AWS CloudFormation.	10. September 2020

Neues Feature	Amazon Kendra fügt Unterstützung für hinzu AWS PrivateLink. Weitere Informationen finden Sie unter Amazon Kendra und Schnittstellen-VPC-Endpunkte (AWS PrivateLink).	7. Juli 2020
Neues Handbuch	Dies ist die erste Version des Amazon Kendra -Entwicklerhandbuchs.	11. Mai 2020

API-Referenz

Die API-Referenzdokumentation ist jetzt ein separater Leitfaden.

AWS-Glossar

Die neueste AWS-Terminologie finden Sie im AWS-Glossar in der AWS-Glossar-Referenz.

Die vorliegende Übersetzung wurde maschinell erstellt. Im Falle eines Konflikts oder eines Widerspruchs zwischen dieser übersetzten Fassung und der englischen Fassung (einschließlich infolge von Verzögerungen bei der Übersetzung) ist die englische Fassung maßgeblich.