Informatica®

Informatica® Mass Ingestion
April 2024

コネクタと接続

Informatica Mass Ingestion コネクタと接続
April 2024

発行日: 2024-05-20

目次

序文

『*一括取り込みコネクタと接続*』では、各タイプの取り込みタスクのソースとターゲットにアクセスするためにダウンロードする必要のあるコネクタのタイプを確認できます。また、取り込みタスクで使用される接続を定義するときに設定するプロパティについても説明します。コネクタをダウンロードし、Administrator で接続を定義します。

Informatica のリソース

Informatica は、Informatica Network やその他のオンラインポータルを通じてさまざまな製品リソースを提供しています。リソースを使用して Informatica 製品とソリューションを最大限に活用し、その他の Informatica ユーザーや各分野の専門家から知見を得ることができます。

Informatica マニュアル

Informatica マニュアルポータルでは、最新および最近の製品リリースに関するドキュメントの膨大なライブラリを参照できます。マニュアルポータルを利用するには、https://docs.informatica.com にアクセスしてください。

製品マニュアルに関する質問、コメント、ご意見については、Informatica マニュアルチーム（infa_documentation@informatica.com）までご連絡ください。

Informatica Intelligent Cloud Services Web サイト

Informatica Intelligent Cloud Services Web サイト（http://www.informatica.com/cloud）にアクセスできます。このサイトには、Informatica Cloud 統合サービスに関する情報が含まれます。

Informatica Intelligent Cloud Services コミュニティ

Informatica Intelligent Cloud Services コミュニティを使用して、技術的な問題について議論し、解決します。また、技術的なヒント、マニュアルの更新情報、FAQ（よくある質問）への答えを得ることもできます。

次の Informatica Intelligent Cloud Services コミュニティにアクセスします。

https://network.informatica.com/community/informatica-network/products/cloud-integration

開発者は、次の Cloud 開発者コミュニティで詳細情報を確認したり、ヒントを共有したりできます。

https://network.informatica.com/community/informatica-network/products/cloud-integration/cloud-developers

Informatica Intelligent Cloud Services マーケットプレース

Informatica マーケットプレイスにアクセスすると、データ統合コネクタ、テンプレート、およびマップレットを試用したり購入したりできます。

https://marketplace.informatica.com/

データ統合のコネクタのドキュメント

データ統合のコネクタのドキュメントには、マニュアルポータルからアクセスできます。マニュアルポータルを利用するには、https://docs.informatica.com にアクセスしてください。

Informatica ナレッジベース

Informatica ナレッジベースを使用して、ハウツー記事、ベストプラクティス、よくある質問に対する回答など、製品リソースを見つけることができます。

ナレッジベースを検索するには、https://search.informatica.com にアクセスしてください。ナレッジベースに関する質問、コメント、ご意見の連絡先は、Informatica ナレッジベースチーム（KB_Feedback@informatica.com）です。

Informatica Intelligent Cloud Services Trust Center

Informatica Intelligent Cloud Services Trust Center は、Informatica のセキュリティポリシーおよびリアルタイムでのシステムの可用性について情報を提供します。

Trust Center（https://www.informatica.com/trust-center.html）にアクセスします。

Informatica Intelligent Cloud Services Trust Center にサブスクライブして、アップグレード、メンテナンス、およびインシデントの通知を受信します。Informatica Intelligent Cloud Services Status ページには、すべての Informatica Cloud 製品の実稼働ステータスが表示されます。メンテナンスの更新はすべてこのページに送信され、停止中は最新の情報が表示されます。更新と停止の通知がされるようにするには、Informatica Intelligent Cloud Services の 1 つのコンポーネントまたはすべてのコンポーネントについて更新の受信をサブスクライブします。すべてのコンポーネントにサブスクライブするのが、更新を逃さないようにするための最良の方法です。

サブスクライブするには、Informatica Intelligent Cloud Services Status ページで **[サブスクライブして更新]** をクリックします。電子メール、SMS テキストメッセージ、Webhook、RSS フィード、またはこの 4 つの任意に組み合わせとして送信される通知を受信するという選択ができます。

Informatica グローバルカスタマサポート

グローバルサポートセンターには、Informatica Network または電話でお問い合わせください。

Informatica Network でオンラインサポートリソースを検索するには、Informatica Intelligent Cloud Services のヘルプメニューで **[サポートにお問い合わせください]** をクリックして、**Cloud Support** ページに移動します。**Cloud Support** ページには、システムステータス情報とコミュニティディスカッションが記載されています。追加のリソースを検索する場合や電子メールで Informatica グローバルカスタマサポートに問い合わせる場合は、Informatica Network にログインし、**[サポートが必要な場合]** をクリックしてください。

Informatica グローバルカスタマサポートの電話番号は、Informatica の Web サイト https://www.informatica.com/services-and-training/support-services/contact-us.html に掲載されています。

第 1 章

コネクタと接続

接続は、クラウドとオンプレミスのアプリケーション、プラットフォーム、データベース、およびフラットファイルのデータへのアクセスを提供します。接続を定義する前に、ソースタイプまたはターゲットタイプのコネクタが Informatica Intelligent Cloud Services にインストールされていることを確認してください。

ソースタイプまたはターゲットタイプに複数のコネクタが使用できる場合は、取り込みタイプがサポートするコネクタを入手してください。一部のコネクタはプレインストールされています。プリインストールされていないコネクタが必要な場合は、管理者の **[アドオンコネクタ]** ページからダウンロードできます。

第 2 章

一括取り込みコネクタ

取り込みタスクで使用するソースとターゲットの接続を作成するには、正しいコネクタが必要です。

接続を定義する前に、組織の管理者は、組織が使用するソースコネクタとターゲットコネクタがインストールされていることを確認する必要があります。また、ランタイム環境でコネクタを有効にする必要があります。

コネクタと接続の詳細については、管理者ヘルプの「ライセンス」、「ランタイム環境」、および「接続」を参照してください。

一括取り込みアプリケーションコネクタ

アプリケーション取り込みタスクの接続を定義する前に、ソースタイプおよびターゲットタイプのコネクタが Informatica Intelligent Cloud Services で使用できることを確認してください。

次の表に、一括取り込みアプリケーションがソースまたはターゲットに接続するために必要なコネクタのリストを示します。

ソースタイプまたはターゲットタイプ	コネクタ	用途
Amazon Aurora PostgreSQL	PostgreSQL	初期ロード、増分ロード、および初期ロードと増分ロードの組み合わせ操作のターゲット Salesforce ソースにのみ適用
Adobe Analytics	Adobe Analytics Mass Ingestion	初期ロード、増分ロード、および初期ロードと増分ロードの組み合わせ操作のソース
Amazon Redshift	Amazon Redshift V2	初期ロード、増分ロード、および初期ロードと増分ロードの組み合わせ操作のターゲット
Amazon S3	Amazon S3 V2	初期ロード、増分ロード、および初期ロードと増分ロードの組み合わせ操作のターゲット
Apache Kafka	Kafka	増分ロード操作のターゲット
Databricks Delta	Databricks Delta	初期ロード、増分ロード、および初期ロードと増分ロードの組み合わせ操作のターゲット

ソースタイプまたはターゲットタイプ	コネクタ	用途
Google Analytics	Google Analytics Mass Ingestion	初期ロード、増分ロード、および初期ロードと増分ロードの組み合わせ操作のソース
Google BigQuery	Google BigQuery V2	初期ロード、増分ロード、および初期ロードと増分ロードの組み合わせ操作のターゲット
Google Cloud Storage	Google Cloud Storage V2	初期ロード、増分ロード、および初期ロードと増分ロードの組み合わせ操作のターゲット
Marketo	Marketo V3	初期ロード、増分ロード、および初期ロードと増分ロードの組み合わせ操作のソース **注:** Apache Kafka ターゲットは増分ロードのみをサポートします。
Microsoft Azure Data Lake Storage Gen2	Microsoft Azure Data Lake Storage Gen2	初期ロード、増分ロード、および初期ロードと増分ロードの組み合わせ操作のターゲット
Microsoft Azure Synapse Analytics[1]	Microsoft Azure Synapse Analytics Database Ingestion	初期ロード、増分ロード、および初期ロードと増分ロードの組み合わせ操作のターゲット
Microsoft Azure SQL Database	SQL Server	初期ロードのターゲット。Salesforce ソースにのみ適用。
Microsoft Fabric OneLake	Microsoft Fabric OneLake	初期ロード操作のターゲット
Microsoft Dynamics 365	Microsoft Dynamics 365 Mass Ingestion	初期ロード、増分ロード、および初期ロードと増分ロードの組み合わせ操作のソース
NetSuite	NetSuite Mass Ingestion	初期ロード、増分ロード、および初期ロードと増分ロードの組み合わせ操作のソース
Oracle Fusion Cloud Applications	Oracle Fusion Cloud Mass Ingestion	- REST: 初期ロード、増分ロード、および初期ロードと増分ロードの組み合わせ操作のソース - BICC: 初期ロード、増分ロード、および初期ロードと増分ロードの組み合わせ操作のソース
Salesforce	Salesforce Mass Ingestion	初期ロード、増分ロード、および初期ロードと増分ロードの組み合わせ操作のソース
Salesforce Marketing Cloud	Salesforce Marketing Cloud	初期ロード操作のソース
SAP ECC	- SAP Mass Ingestion - SAP ODP Extractor	- SAP Mass Ingestion: 初期ロード、増分ロード、および初期ロードと増分ロードの組み合わせ操作のソース - SAP ODP Extractor: 初期ロード、増分ロード、および初期ロードと増分ロードの組み合わせ操作のソース

ソースタイプまたはターゲットタイプ	コネクタ	用途
SAP S/4HANA	SAP ODP Extractor	初期ロード、増分ロード、および初期ロードと増分ロードの組み合わせ操作のソース
ServiceNow	ServiceNow Mass Ingestion	初期ロード、増分ロード、および初期ロードと増分ロードの組み合わせ操作のソース
Snowflake	Snowflake Data Cloud	初期ロード、増分ロード、および初期ロードと増分ロードの組み合わせ操作のターゲット
Workday	Workday Mass Ingestion	- SOAP: 初期ロード、増分ロード、および初期ロードと増分ロードの組み合わせ操作のソース **注:** Apache Kafka ターゲットは増分ロードのみをサポートします。 - RaaS: 初期ロードのソース
Zendesk	Zendesk Mass Ingestion	初期ロード、増分ロード、および初期ロードと増分ロードの組み合わせ操作のソース
1. Microsoft Azure Synapse Analytics ターゲットの場合、一括取り込みアプリケーションは Microsoft Azure SQL Data Lake Storage Gen2 を使用してステージングファイルを格納します。Microsoft Azure Synapse Analytics ターゲットの接続を構成する前に、Microsoft Azure SQL Data Lake Storage Gen2 がインストールされていることを確認してください。		

一括取り込みデータベースコネクタ

データベース統合タスクの接続の定義を開始する前に、ソースタイプおよびターゲットタイプのコネクタが Informatica Intelligent Cloud Services で使用できることを確認してください。

次の表に、一括取り込みデータベースでデータベース統合タスクで設定できるソースまたはターゲットに接続するために必要とされるコネクタのリストを示します。

ソースタイプまたはターゲットタイプ	コネクタ	用途
Amazon Redshift	Amazon Redshift V2	初期ロード、増分ロード、および初期ロードと増分ロードのジョブのターゲット
Amazon S3	Amazon S3 V2	初期ロードおよび増分ロードのジョブのターゲット
Databricks Delta	Databricks Delta	初期ロード、増分ロード、および初期ロードと増分ロードのジョブのターゲット
Db2 for i	Db2 for i Database Ingestion	初期ロード、増分ロード、および初期ロードと増分ロードのジョブのソース

ソースタイプまたはターゲットタイプ	コネクタ	用途
Db2 for Linux, UNIX, and Windows	Db2 for LUW Database Ingestion	初期ロードジョブのソース
DB2 for z/OS	Db2 for zOS Database Ingestion	初期ロードおよび増分ロードのジョブのソース
フラットファイル	コネクタは必要ありません	初期ロードジョブのターゲット
Google BigQuery	Google BigQuery V2	初期ロード、増分ロード、および初期ロードと増分ロードのジョブのターゲット
Google Cloud Storage	Google Cloud Storage V2	初期ロードおよび増分ロードのジョブのターゲット
Kafka（Apache Kafka、Confluent Kafka、Amazon Managed Streaming for Apache Kafka、Kafka 対応 Azure Event Hubs を含む）	Kafka	増分ロードジョブのターゲット
Microsoft Azure Data Lake Storage Gen2	Microsoft Azure Data Lake Storage Gen2	初期ロードおよび増分ロードのジョブのターゲット
Microsoft SQL Server（オンプレミスの SQL Server、RDS for SQL Server、Azure SQL Database、Azure SQL Managed Instance を含む）	SQL Server	初期ロード、増分ロード、および初期ロードと増分ロードの組み合わせジョブのソース Azure SQL Database ソースの場合、増分ロードジョブと組み合わせロードジョブには、**[クエリベース]** または **[CDC テーブル]** のキャプチャメソッドを使用する必要があります。 初期ロード、増分ロード、および初期ロードと増分ロードのジョブのターゲット。
Microsoft Azure Synapse Analytics[1]	Microsoft Azure Synapse Analytics Database Ingestion	初期ロード、増分ロード、および初期ロードと増分ロードのジョブのターゲット
Microsoft Fabric OneLake	Microsoft Fabric OneLake	初期ロードジョブのターゲット
MongoDB	MongoDB Mass Ingestion	初期ロードおよび増分ロードのジョブのソース
MySQL（RDS for MySQL を含む）	MySQL	初期ロードおよび増分ロードのジョブのソース。初期ロードジョブのみの RDS for MySQL。
Netezza	Netezza	初期ロードジョブのソース
Oracle（RDS for Oracle を含む）	Oracle Database Ingestion	初期ロード、増分ロード、および初期ロードと増分ロードのジョブのソース 初期ロード、増分ロード、および初期ロードと増分ロードのジョブのターゲット
Oracle Cloud Infrastructure（OCI）Object Storage	Oracle Cloud Object Storage	初期ロード、増分ロード、および初期ロードと増分ロードのジョブのターゲット

ソースタイプまたはターゲットタイプ	コネクタ	用途
PostgreSQL（オンプレミスの PostgreSQL を含む）、Amazon Aurora PostgreSQL、Azure Database for PostgreSQL - Flexible Server、RDS for PostgreSQL、および Cloud SQL for PostgreSQL	PostgreSQL	初期ロード、増分ロード、および初期ロードと増分ロードのジョブのソース 初期ロード、増分ロード、および初期ロードと増分ロードの組み合わせジョブのターゲット（Amazon Aurora PostgreSQL のみ）
SAP HANA（オンプレミスの SAP HANA と SAP HANA Cloud を含む）	SAP HANA Database Ingestion	初期ロードおよび増分ロードのジョブのソース
Snowflake	Snowflake Data Cloud	初期ロード、増分ロード、および初期ロードと増分ロードのジョブのターゲット
Teradata Data Warehouse Appliance	Teradata	初期ロードジョブのソース
1. Microsoft Azure Synapse Analytics ターゲットタイプの場合、一括取り込みデータベースは Microsoft Azure SQL Data Lake Storage Gen2 を使用してステージングファイルを格納します。Microsoft Azure SQL Data Lake StorageGen2 がインストールされていることを確認してください。		

モックコネクタ

一括取り込みデータベースは、一部のソースおよびターゲットのモック、サンプル、接続をサポートします。モック接続を使用して、データベースへの実際の接続を作成せずに、初期ロードデータベース取り込みタスクを作成する方法を確認します。

モックコネクタは実際のデータベースに接続しません。代わりに、ソースモックコネクタはサンプルデータを含むフラットファイルを使用します。ターゲットモックコネクタは、処理されたソースデータに関する情報を一括取り込みデータベースユーザーインタフェースに報告しますが、ターゲットにはデータを書き込みません。

MockConnector ライセンスがある場合、サンプル接続は一括取り込みデータベースのソース接続リストとターゲット接続リストに表示されます。

次の表に、一括取り込みデータベースのソースとターゲットに使用できるモック接続を示します。

接続名	ソースまたはターゲット
Sample Oracle Connection	ソース
Sample SQL Server Connection	ソース
Sample S3 Connection	ターゲット
Sample ADLS Gen2 Connection	ターゲット

注: ソースデータベースとターゲットデータベースの両方にサンプル接続を使用する必要があります。たとえば、ソースには使用でき、ターゲットには使用できない場合など一方だけにサンプル接続を使用することはできません。

ソースデータ

サンプル接続のソースデータは、次のディレクトリの CVS ファイルに保存されています。

Secure_Agent_installation/downloads/package-MockConnector.*version*/package/sampleData/source/*database_type*/

各ファイルは単一のテーブルを表します。モックテーブル名がファイル名と一致します。ファイルの最初の行はカラムヘッダーを決定し、後続の行には行データが含まれます。

一括取り込みファイルコネクタ

ファイル取り込みタスクの接続を定義する前に、一括取り込みファイルでソースタイプとターゲットタイプに対して必要となるコネクタのライセンスがあることを確認してください。

次の表に、ファイル取り込みタスクがソースタイプとターゲットタイプに基づいてサポートするコネクタを示します。

ソース名またはターゲット名	コネクタ	ソースタイプまたはターゲットタイプ
ローカルフォルダ	コネクタは必要ありません	ソースとターゲット
Advanced FTP	Advanced FTP V2（アドオン）	ソースとターゲット
Advanced FTPS	Advanced FTPS V2（アドオン）	ソースとターゲット
Advanced SFTP	Advanced SFTP V2（アドオン）	ソースとターゲット
Amazon S3	Amazon S3 V2（アドオン）	ソースとターゲット
Amazon Redshift	Amazon Redshift V2（アドオン）	ターゲット
Cloud 統合ハブ	Cloud 統合ハブ（アドオン）	ソースとターゲット **注**: ソースとターゲットの両方に Cloud 統合ハブを使用して、ファイル取り込みタスクを設定することはできません。
Databricks Delta	Databricks Delta（アドオン）	ソースとターゲット
Google BigQuery	Google BigQuery V2（アドオン）	ターゲット
Google Cloud Storage	Google Cloud Storage V2（アドオン）	ソースとターゲット
Hadoop Files	Hadoop Files V2（アドオン）	ソースとターゲット
Microsoft Azure Blob Storage	Microsoft Azure Blob Storage V3（アドオン）	ソースとターゲット

ソース名またはターゲット名	コネクタ	ソースタイプまたはターゲットタイプ
Microsoft Azure Data Lake Store	Microsoft Azure Data Lake Store Gen2（アドオン）	ソースとターゲット
Microsoft Azure Data Lake Store	Microsoft Azure Data Lake Store V3（アドオン）	ソースとターゲット
Microsoft Azure Synapse SQL	Microsoft Azure Synapse SQL（アドオン）	ターゲット
Microsoft Fabric OneLake	Microsoft Fabric OneLake（アドオン）	ソースとターゲット
Snowflake	Snowflake クラウドデータウェアハウス V2（アドオン）	ターゲット

一括取り込みストリーミングコネクタ

ストリーミング統合タスクの接続を定義する前に、ソースタイプとターゲットタイプに必要なコネクタのライセンスがあることを確認してください。

次の表に、ストリーミング統合タスクがソースタイプとターゲットタイプに基づいてサポートするコネクタを示します。

ソース名またはターゲット名。	コネクタ	ソースタイプまたはターゲットタイプ
Amazon Kinesis Data Firehose	Amazon Kinesis（アドオン）	ターゲット
Amazon Kinesis Data Streams	Amazon Kinesis（アドオン）	ソースとターゲット
Amazon Managed Streaming for Apache Kafka（Amazon MSK）	Kafka（アドオン）	ソースとターゲット
Amazon S3	Amazon S3 V2（アドオン）	ターゲット
AMQP	AMQP（アドオン）	ソース
Apache Kafka	Kafka（アドオン）	ソースとターゲット
Azure Event Hubs Kafka	Kafka（アドオン）	ソース
Confluent Kafka	Kafka（アドオン）	ソースとターゲット
Databricks Delta	Databricks Delta（アドオン）	ターゲット

ソース名またはターゲット名。	コネクタ	ソースタイプまたはターゲットタイプ
フラットファイル	コネクタは必要ありません	ソースとターゲット
Google BigQuery V2	Google BigQuery V2（アドオン）	ターゲット
Google Cloud Storage	Google Cloud Storage V2（アドオン）	ターゲット
Google PubSub	Google PubSub（アドオン）	ソースとターゲット
JDBC V2	JDBC V2（アドオン）	ターゲット
JMS	JMS（アドオン）	ソース
Microsoft Azure Data Lake Storage	Azure Data Lake Store Gen2（アドオン）	ターゲット
Microsoft Azure Event Hub	Azure Event Hubs（アドオン）	ターゲット
MQTT	MQTT（アドオン）	ソース
OPC UA	OPCUA（アドオン）	ソース
REST V2	REST V2（アドオン）	ソース

注: ストリーミング統合タスクのインポート中に、読み取り接続タイプと書き込み接続タイプの両方が、**［インポートの確認］**ページのドロップダウンリストに表示されます。一括取り込みストリーミングでサポートされていないコネクタへの接続も確認できます。

第 3 章

一括取り込み接続プロパティ

接続は、クラウドとオンプレミスのアプリケーション、プラットフォーム、データベース、およびフラットファイルのデータへのアクセスを提供します。接続定義には、ソースまたはターゲットの場所、ランタイム環境、および接続タイプに固有のその他のプロパティが含まれます。

接続を作成する前に、ソースとターゲットに適したコネクタを Informatica Intelligent Cloud Services で利用できることを確認してください。サポートされているコネクタは、取り込みタスクのタイプによって異なります。

接続を作成したり、既存の接続を検索したりするには、管理者サービスを使用します。

接続プロパティを設定すると、この接続が組織内で利用可能になります。

接続の設定

管理者の［**接続**］のページでソース接続またはターゲット接続を設定します。

1. 管理者で［**接続**］を選択します。
2. ［**接続**］ページで、［**新しい接続**］をクリックします。
3. 次の接続の詳細を設定します。

プロパティ	説明
接続名	接続の名前。 各接続名は組織内で一意である必要があります。接続名には、英数字、スペース、および次の特殊文字を含めることができます。_ .+ - 最大長は 100 文字です。接続名では大文字と小文字は区別されません。
説明	接続の説明。
タイプ	Amazon S3 などの接続のタイプ。

接続タイプを選択すると、そのタイプに固有の追加のプロパティが表示されます。

4. 接続固有のプロパティを設定します。

   たとえば、Amazon S3 接続を設定している場合は、Amazon S3 接続プロパティを入力します。各接続プロパティの説明については、ヘルプアイコンをクリックしてください。
5. 接続をテストするには、［**テスト接続**］をクリックします。

テストの結果はページの上部に表示されます。

接続に失敗した場合は、データベース管理者に連絡するか、設定を再確認して、選択したランタイム環境のステータスが［稼働中］であることを確認してください。

6. **［保存］**をクリックして接続を保存します。

Adobe Analytics Mass Ingestion 接続のプロパティ

Adobe Analytics Mass Ingestion 接続をセットアップする際には、接続プロパティを設定する必要があります。

Adobe Analytics は、JSON Web Token（JWT）を使用して Adobe Analytics Mass Ingestion 接続を認証します。Adobe Analytics Mass Ingestion 接続を使用するには、Adobe Developer Console でサービスアカウント統合を作成してから、接続プロパティでサービス統合の詳細を指定する必要があります。Adobe Developer Console でサービスアカウント統合を作成する方法の詳細については、「Adobe documentation」を参照してください。

次の表に、Adobe Analytics Mass Ingestion 接続の接続プロパティを示します。

接続プロパティ	説明
接続名	接続の名前。この名前は、組織内で一意にする必要があります。接続名には、英数字、スペース、および次の特殊文字を含めることができます。_ .+ - 名前の先頭または末尾のスペースはトリミングされ、名前の一部として保存されません。最大長は 100 文字です。接続名では大文字と小文字は区別されません。
説明	接続の説明（オプション）。最大長は 255 文字です。
タイプ	接続のタイプ。【Adobe Analytics Mass Ingestion】接続タイプを選択します。
ランタイム環境	取り込みタスクを実行するランタイム環境の名前。 ランタイム環境として Secure Agent を指定する必要があります。 **注**: Hosted Agent やサーバーレスランタイム環境でアプリケーション取り込みタスクを実行することはできません。
クライアント ID	Adobe Developer Console で作成したサービスアカウントのクライアント ID。
クライアントシークレット	Adobe Developer Console で作成したサービスアカウントのクライアントシークレット。
テクニカルアカウント ID	サービスアカウントのテクニカルアカウント ID。
組織 ID	サービスアカウントの組織 ID。
秘密鍵	サービスアカウント統合を作成するときに生成される秘密鍵。JWT を生成するには、秘密鍵が必要です。

接続プロパティ	説明
IMS ホスト	Adobe Identity Management System（IMS）のベース URL。 デフォルト値は以下のようになります。 `ims-na1.adobelogin.com`
IMS 交換	IMS の交換 URL。接続は、JWT を使用して交換 URL に POST リクエストを行うことで、Adobe からアクセストークンを取得します。 デフォルト値は以下のようになります。 `https://ims-na1.adobelogin.com/ims/exchange/jwt`

Advanced FTP V2 接続のプロパティ

Advanced FTP V2 接続をセットアップするには、接続プロパティを設定する必要があります。

次の表に、Advanced FTP V2 接続のプロパティを示します。

接続プロパティ	説明
接続名	接続の名前。この名前では、大文字と小文字が区別されず、ドメイン内で一意にする必要があります。このプロパティは、接続を作成した後に変更できます。名前は 128 文字以内で指定し、空白および次の特殊文字は使用できません。~ ` ! $ % ^ & * ( ) - + = { [}] | \ : ; " ' < , > . ? /
説明	オプション。接続の説明。説明は、4,000 文字を超えることはできません。
タイプ	[Advanced FTP V2] 接続タイプを選択します。
ランタイム環境	タスクを実行するランタイム環境の名前。Secure Agent を指定します。
ホスト	FTP サーバーのホスト名または IP アドレス。
ポート	FTP サーバーへの接続に使用するためのポート番号。空白のままにすると、デフォルトのポート番号 21 が使用されます。
ユーザー名	FTP サーバーに接続するためのユーザー名。
パスワード	FTP サーバーに接続するためのパスワード。
フォルダパス	FTP サーバーへの接続後に使用するディレクトリ。

接続プロパティ	説明
パッシブモードを使用	接続が**パッシブ**または**アクティブ**のどちらのモードを使用しているかを示します。**パッシブ**モードを使用するには［**はい**］を指定します。**アクティブ**モードを使用するには［**いいえ**］を指定します。 デフォルト値は［**はい**］です。 パッシブモードでは、サーバーは接続クライアント上のポートに接続する必要はなく、ファイアウォールに優しいモードです。サーバーへの接続に問題がある場合は、このオプションで［**はい**］を選択して、モードをパッシブに変更することができます。パッシブモードでは、FTP サーバーによっては、データを転送するために、ポートの可用性に基づいて接続に高いポート範囲が必要になる場合があります。 アクティブモードでは、サーバーはデータ転送を実行するために接続クライアント上のポートに接続しようとします。
データ接続の開始ポート	データ接続に使用する開始ポート番号。
データ接続の終了ポート	データ接続に使用する終了ポート番号。
タイムアウト	サーバーへの接続を試行するときに待機する秒数。指定した時間内に接続を確立できない場合、タイムアウトになります。空白のままにすると、デフォルト値の 120 秒が使用されます。
接続の再試行	接続を確立できない場合に FTP 接続の再試行のために接続する回数。この設定は、最初の接続と接続の切断による再接続の試行の両方に使用されます。空白のままにすると、再試行は行われません。
接続再試行の間隔	接続の再試行ごとに待機する秒数。 **注**: 例えば、再試行ごとに 5 秒間空けて最大 10 回接続しようとする場合は、**接続の再試行回数**に 10 を指定し、**接続再試行**の間隔に 5 を指定します。
制御エンコーディング	空白のままにすると、接続では ISO 標準 ISO-8859-1 が使用されます。サーバーでサポートされている場合は、UTF-8 などの他のエンコーディングを指定すると、国際文字をサポートできます。
リストパーサー	サーバー接続に使用するリストパーサー。フィールドが空白のままの場合、Advanced FTP V2 コネクタは MLSD パーサーを使用しようとします。MLSD パーサーがサーバーでサポートされていない場合は、UNIX パーサーが使用されます。ディレクトリのリストに問題が発生した場合は、別のリストパーサーを選択します。
日付形式	この日付形式は、サーバーが選択したリストパーサーのデフォルト値と異なる日付を返す場合に適用されます。別の日付形式（d MMM yyyy など）が必要な場合は、このフィールドで日付形式を指定します。すべてのリストパーサーが日付形式の設定をサポートしているわけではありません。日付形式設定をサポートしていないリストパーサーは、ユーザーが指定した値を無視します。
最近の日付形式	各ファイルの最終更新日を解析する場合に使用する日付形式を指定します。最近の日付形式は UNIX ベースのシステムで適用され、1 年未満のエントリに表示されます。特定の日付形式（d MMM HH: mm など）が必要な場合は、このフィールドでそのパターンを指定します。すべてのリストパーサーが最近の日付形式設定をサポートしているわけではありません。最近の日付形式設定をサポートしていないリストパーサーは、ユーザーが指定した値を無視します。

接続プロパティ	説明
帯域幅	ファイル転送に使用されるネットワークリソースの最大量を制御します。この値は、ファイルのアップロードとダウンロードに適用されます。デフォルトは 0 です。0 は帯域幅が制限されていないことを示します。
帯域幅単位	ファイル転送に使用されるネットワーク帯域幅の単位。以下のいずれかの単位を選択することができます。 - キロバイト/秒（KBps） - メガバイト/秒（MBps）

注: Advanced FTP V2 コネクタは、NTLM プロキシ認証をサポートしていません。

Advanced FTPS V2 接続のプロパティ

Advanced FTPS V2 接続をセットアップするには、接続プロパティを設定する必要があります。

以下の表に、Advanced FTPS V2 接続のプロパティを示します。

接続プロパティ	説明
接続名	接続の名前。この名前では、大文字と小文字が区別されず、ドメイン内で一意にする必要があります。このプロパティは、接続を作成した後に変更できます。名前は 128 文字以内で指定し、空白および次の特殊文字は使用できません。~ ` ! $ % ^ & * ( ) - + = { [}] | \ : ; " ' < , > . ? /
説明	オプション。接続の説明。説明は、4,000 文字を超えることはできません。
タイプ	[Advanced FTPS V2] 接続タイプを選択します。
ランタイム環境	タスクを実行する Secure Agent が含まれるランタイム環境の名前。
ホスト	サーバーのホスト名または IP アドレス。
ポート	サーバーへの接続に使用するためのポート番号。空白のままにすると、デフォルトのポート番号は 21 になります。
ユーザー名	FTPS サーバーに接続するためのユーザー名。
パスワード	FTPS サーバーに接続するためのパスワード。
フォルダパス	サーバーへの接続後に使用するディレクトリ。

接続プロパティ	説明
パッシブモードを使用	接続が**パッシブ**または**アクティブ**のどちらのモードを使用しているかを示します。**パッシブ**モードを使用するには**［はい］**を指定します。**アクティブ**モードを使用するには**［いいえ］**を指定します。 デフォルト値は**［はい］**です。 パッシブモードでは、サーバーは接続クライアント上のポートに接続する必要はなく、ファイアウォールに優しいモードです。サーバーへの接続に問題がある場合は、このオプションで**［はい］**を選択して、モードをパッシブに変更することができます。パッシブモードでは、FTPS サーバーによっては、データを転送するために、ポートの可用性に基づいて接続に高いポート範囲が必要になる場合があります。 アクティブモードでは、サーバーはデータ転送を実行するために接続クライアント上のポートに接続しようとします。
データ接続の開始ポート	データ接続に使用する開始ポート番号。
データ接続の終了ポート	データ接続に使用する終了ポート番号。
タイムアウト	サーバーへの接続を試行するときに待機する秒数。指定した時間内に接続を確立できない場合、タイムアウトになります。空白のままにすると、デフォルト値の 120 秒が使用されます。
接続の再試行	接続を確立できない場合に Advanced FTP V2 接続の再試行のために接続する回数。この設定は、最初の接続と接続の切断による再接続の試行の両方に使用されます。空白のままにすると、再試行は行われません。
接続再試行の間隔	接続の再試行ごとに待機する秒数。 **注**: 例えば、再試行ごとに 5 秒間空けて最大 10 回接続しようとする場合は、**接続の再試行回数**に 10 を指定し、**接続再試行**の間隔に 5 を指定します。
制御エンコーディング	空白のままにすると、接続では ISO 標準 ISO-8859-1 が使用されます。サーバーでサポートされている場合は、UTF-8 のような他のエンコーディングを指定すると、国際文字をサポートできます。
信頼済みサーバー	FTPS サーバーが信頼済みサーバーであるかどうかを指定します。Advanced FTP V2 コネクタは、信頼済みサーバーのみをサポートします。
リストパーサー	サーバー接続に使用するリストパーサー。フィールドが空白のままの場合、Advanced FTP V2 コネクタは MLSD パーサーを使用しようとします。サーバーが MLSD パーサーをサポートしていない場合、コネクタは UNIX パーサーを使用します。ディレクトリのリストに問題が発生した場合は、別のリストパーサーを選択します。
日付形式	この日付形式は、サーバーが選択したリストパーサーのデフォルト値と異なる日付を返す場合に適用されます。別の日付形式（d MMM yyyy など）が必要な場合は、このフィールドで日付形式を指定します。すべてのリストパーサーが日付形式の設定をサポートしているわけではありません。日付形式設定をサポートしていないリストパーサーは、ユーザーが指定した値を無視します。
最近の日付形式	各ファイルの最終更新日を解析する場合に使用する日付形式を指定します。最近の日付形式は UNIX ベースのシステムで適用され、1 年未満のエントリに表示されます。特定の日付形式（d MMM HH: mm など）が必要な場合は、このフィールドでそのパターンを指定します。すべてのリストパーサーが最近の日付形式設定をサポートしているわけではありません。最近の日付形式設定をサポートしていないリストパーサーは、ユーザーが指定した値を無視します。

接続プロパティ	説明
接続タイプ	接続タイプが IMPLICIT_SSL または EXPLICIT_SSL のどちらであるかを指定します。 - IMPLICIT_SSL。接続は自動的に SSL 接続として開始されます。 - EXPLICIT_SSL。FTPS サーバーでの初期認証後、選択したセキュリティプロトコルに応じて、接続は SSL または TLS で暗号化されます。 デフォルトは IMPLICIT_SSL です。
セキュリティプロトコル	EXPLICIT_SSL 接続に SSL または TLS のどちらが使用されるかを指定します。 デフォルトは SSL です。
キーストアファイル	キーストアファイルのパスおよびファイル名。キーストアファイルには、FTPS サーバーを認証するための証明書が含まれます。
キーストアのパスワード	信頼済みサーバーの証明書ストアにアクセスするために必要なキーストアファイルのパスワード。
キーエイリアス	個別のキーのエイリアス。
キーストアタイプ	キーストアのタイプが Java KeyStore（JKS）または Public Key Cryptology Standard（PKCS12）のどちらであるかを指定します。 デフォルトは JKS です。
帯域幅	ファイル転送に使用されるネットワークリソースの最大量を制御します。この値は、ファイルのアップロードとダウンロードに適用されます。デフォルトは 0 です。0 は帯域幅が制限されていないことを示します。
帯域幅単位	ファイル転送に使用されるネットワーク帯域幅の単位。以下のいずれかの単位を選択することができます。 - キロバイト/秒（KBps） - メガバイト/秒（MBps）

注: Advanced FTPS V2 コネクタは、NTLM プロキシ認証をサポートしていません。

Advanced SFTP V2 接続のプロパティ

Advanced SFTP V2 接続をセットアップするには、接続プロパティを設定する必要があります。

以下の表に、Advanced SFTP V2 接続のプロパティを示します。

接続プロパティ	説明
接続名	接続の名前。この名前では、大文字と小文字が区別されず、ドメイン内で一意にする必要があります。このプロパティは、接続を作成した後に変更できます。名前は 128 文字以内で指定し、空白および次の特殊文字は使用できません。~ ` ! $ % ^ & * ( ) - + = { [}] | \ : ; " ' < , > . ? /
説明	オプション。接続の説明。説明は、4,000 文字を超えることはできません。
タイプ	【Advanced SFTP V2】接続タイプを選択します。
ランタイム環境	タスクを実行する Secure Agent が含まれるランタイム環境の名前。
ホスト	サーバーのホスト名または IP アドレス。
ポート	サーバーへの接続に使用するポート番号。デフォルトは 21 です。
ユーザー名	SFTP サーバーに接続するためのユーザー名。
パスワード	SFTP サーバーに接続するためのパスワード。
フォルダパス	サーバーへの接続後に使用するディレクトリ。
タイムアウト	サーバーへの接続を試行するときに待機する秒数。指定した時間内に接続を確立できない場合、タイムアウトになります。空白のままにすると、デフォルト値の 120 秒が使用されます。
接続の再試行	接続を確立できない場合に SFTP 接続の再試行のために接続する回数。この設定は、最初の接続と接続の切断による再接続の試行の両方に使用されます。空白のままにすると、再試行は行われません。
接続再試行の間隔	接続の再試行ごとに待機する秒数。 例えば、再試行ごとに 5 秒間空けて最大 10 回接続しようとする場合は、接続の再試行回数に 10 を指定し、接続再試行の間隔に 5 を指定します。
プライベートキーファイル	SSH プライベートキーファイルの名前と、ファイルが保存されている場所へのパス。 ファイルパスが、Secure Agent をホストするマシン上にあることを確認します。 例: `C:/SSH/my_keys/key.ppk`
プライベートキーパスフレーズ	SSH プライベートキーを暗号化するためのパスフレーズを指定します。
曲線キーアルゴリズムの使用	曲線などの追加のキー交換アルゴリズム、および-hmac-sha2-512 や-hmac-sha2-256 などのキー付きハッシュアルゴリズムを有効にします。

接続プロパティ	説明
帯域幅	ファイル転送に使用されるネットワークリソースの最大量を制御します。この値は、ファイルのアップロードとダウンロードに適用されます。デフォルトは 0 です。0 は帯域幅が制限されていないことを示します。
帯域幅単位	ファイル転送に使用されるネットワーク帯域幅の単位。以下のいずれかの単位を選択することができます。 - キロバイト/秒（KBps） - メガバイト/秒（MBps）
ファイル統合プロキシサーバーの使用	コネクタは、ファイル統合プロキシサーバー経由で SFTP サーバーに接続します。 次の前提条件が満たされていることを確認してください。 - このオプションを使用するには、ファイル統合サービスのライセンスが必要です。 - ファイルサーバーでプロキシサーバーを定義する必要があります。 - ファイル統合サービスプロキシがない場合は、proxy.ini ファイル経由でエージェントプロキシを使用する必要があります。
プロキシサーバーのホスト名	送信ファイル統合サービスプロキシサーバーのホスト名または IP アドレス。
プロキシサーバーのポート	送信ファイル統合サービスプロキシサーバーのポート番号。

注: Advanced SFTP V2 コネクタは、NTLM プロキシ認証をサポートしていません。

Amazon Kinesis 接続のプロパティ

Amazon Kinesis 接続はメッセージング接続です。Amazon Kinesis Data Streams または Amazon Kinesis Data Firehose にターゲットとしてアクセスするには、Amazon Kinesis 接続を使用します。

Amazon Kinesis Firehose 接続のプロパティ

Amazon Kinesis Firehose 接続をセットアップする際には、接続プロパティを設定する必要があります。

次の表に、Amazon Kinesis Firehose 接続のプロパティを示します。

プロパティ	説明
接続名	接続の名前。 この名前では、大文字と小文字が区別されず、ドメイン内で一意にする必要があります。このプロパティは、接続を作成した後に変更できます。名前は 128 文字以内で指定し、空白および以下の特殊文字は使用できません。 ~ ` ! $ % ^ & * ( ) - + = { [}] | \ : ; " ' < , > . ? /
説明	オプション。接続を識別するために使用できる説明。 説明は、4,000 文字を超える事は出来ません。

プロパティ	説明
タイプ	Amazon Kinesis 接続タイプ。 Amazon Kinesis 接続タイプが見つからない場合は、**［アドオンコネクタ］**ページに移動し、コネクタを有効にしてください。
ランタイム環境	タスクを実行するランタイム環境の名前。
サービス	使用する Kinesis サービスのタイプ。［Kinesis Firehose］を選択します。
AWS アクセスキー ID	Amazon AWS ユーザーアカウントのアクセスキー ID。
AWS シークレットアクセスキー	Amazon AWS ユーザーアカウントのシークレットアクセスキー。
リージョン	サービスのエンドポイントを利用できるリージョン。次の値から選択する事ができます。 - us-east-2。米国東部（オハイオ）リージョンを示します。 - us-east-1。米国東部（バージニア北部）リージョンを示します。 - us-west-1。米国西部（北カリフォルニア）リージョンを示します。 - us-west-2。米国西部（オレゴン）リージョンを示します。 - ap-northeast-1。アジアパシフィック（東京）リージョンを示します。 - ap-northeast-2。アジアパシフィック（ソウル）リージョンを示します。 - ap-northeast-3。アジアパシフィック（大阪: ローカル）リージョンを示します。 - ap-south-1。アジアパシフィック（ムンバイ）リージョンを示します。 - ap-southeast-1。アジアパシフィック（シンガポール）リージョンを示します。 - ap-southeast-2。アジアパシフィック（シドニー）リージョンを示します。 - ca-central-1。カナダ（中部）リージョンを示します。 - cn-north-1。中国（北京）リージョンを示します。 - cn-northwest-1。中国（寧夏）リージョンを示します。 - eu-central-1。欧州（フランクフルト）リージョンを示します。 - eu-west-1。欧州（アイルランド）リージョンを示します。 - eu-west-2。欧州（ロンドン）リージョンを示します。 - eu-west-3。欧州（パリ）リージョンを示します。 - sa-east-1。南米（サンパウロ）リージョンを示します。 - us-gov-west-1.AWS GovCloud（US-West）リージョンを示します。 - us-gov-east-1.AWS GovCloud（US-East）リージョンを示します。 ストリーミング取り込みタスクは、ap-northeast-3 リージョンをサポートしていません。
接続タイムアウト（ミリ秒）	オプション。一括取り込みサービスが Kinesis Firehose への接続の確立を待機してタイムアウトになるまでの時間（ミリ秒）。 デフォルトは 10,000 ミリ秒です。
AWS 認証情報プロファイル名	認証情報ファイル内で定義された AWS 認証情報プロファイル。 マッピングは実行時のプロファイル名を使用して AWS 認証情報にアクセスします。AWS 認証情報プロファイル名を指定しない場合、接続を作成するときに指定したアクセスキー ID とシークレットアクセスキーを使用します。
IAM ロールの ARN	IAM ユーザーのロールを指定する Amazon リソースネーム。アカウント間の IAM ロール認証に適用されます。
外部 ID	IAM ロールの外部 ID は、IAM ロールを引き受けることができるユーザーを指定するために、IAM ロールの信頼ポリシーで使用できる追加の制限です。アカウント間の IAM ロール認証に適用されます。

Amazon Kinesis Streams 接続のプロパティ

Amazon Kinesis Streams 接続をセットアップする際には、接続プロパティを設定する必要があります。

次の表に、Amazon Kinesis Streams 接続のプロパティを示します。

プロパティ	説明
接続名	接続の名前。 この名前では、大文字と小文字が区別されず、ドメイン内で一意にする必要があります。このプロパティは、接続を作成した後に変更できます。名前は 128 文字以内で指定し、空白および以下の特殊文字は使用できません。 ~ ` ! $ % ^ & * ( ) - + = { [}] | \ : ; " ' < , > . ? /
説明	オプション。接続を識別するために使用できる説明。 説明は、4,000 文字を超える事は出来ません。
タイプ	Amazon Kinesis 接続タイプ。 Amazon Kinesis 接続タイプが見つからない場合は、**［アドオンコネクタ］**ページに移動し、コネクタをインストールしてください。
ランタイム環境	タスクを実行するランタイム環境の名前。
サービス	使用する Kinesis サービスのタイプ。［Kinesis Streams］を選択します。
AWS アクセスキー ID	Amazon AWS ユーザーアカウントのアクセスキー ID。
AWS シークレットアクセスキー	Amazon AWS ユーザーアカウントのシークレットアクセスキー。
リージョン	サービスのエンドポイントを利用できるリージョン。次の値から選択する事ができます。 - us-east-2。米国東部（オハイオ）リージョンを示します。 - us-east-1。米国東部（バージニア北部）リージョンを示します。 - us-west-1。米国西部（北カリフォルニア）リージョンを示します。 - us-west-2。米国西部（オレゴン）リージョンを示します。 - ap-northeast-1。アジアパシフィック（東京）リージョンを示します。 - ap-northeast-2。アジアパシフィック（ソウル）リージョンを示します。 - ap-northeast-3。アジアパシフィック（大阪: ローカル）リージョンを示します。 - ap-south-1。アジアパシフィック（ムンバイ）リージョンを示します。 - ap-southeast-1。アジアパシフィック（シンガポール）リージョンを示します。 - ap-southeast-2。アジアパシフィック（シドニー）リージョンを示します。 - ca-central-1。カナダ（中部）リージョンを示します。 - cn-north-1。中国（北京）リージョンを示します。 - cn-northwest-1。中国（寧夏）リージョンを示します。 - eu-central-1。欧州（フランクフルト）リージョンを示します。 - eu-west-1。欧州（アイルランド）リージョンを示します。 - eu-west-2。欧州（ロンドン）リージョンを示します。 - eu-west-3。欧州（パリ）リージョンを示します。 - sa-east-1。南米（サンパウロ）リージョンを示します。 - us-gov-west-1.AWS GovCloud（US-West）リージョンを示します。 - us-gov-east-1.AWS GovCloud（US-East）リージョンを示します。 ストリーミング取り込みタスクは、ap-northeast-3 リージョンをサポートしていません。

プロパティ	説明
接続タイムアウト（ミリ秒）	オプション。一括取り込みが Kinesis Streams への接続の確立を待機してタイムアウトになるまでの時間（ミリ秒）。 デフォルトは 10,000 ミリ秒です。
AWS 認証情報プロファイル名	認証情報ファイル内で定義された AWS 認証情報プロファイル。 マッピングは実行時のプロファイル名を使用して AWS 認証情報にアクセスします。AWS 認証情報プロファイル名を指定しない場合、接続を作成するときに指定したアクセスキー ID とシークレットアクセスキーを使用します。
IAM ロールの ARN	IAM ユーザーのロールを指定する Amazon リソースネーム。アカウント間の IAM ロール認証に適用されます。
外部 ID	IAM ロールの外部 ID は、IAM ロールを引き受けることができるユーザーを指定するために、IAM ロールの信頼ポリシーで使用できる追加の制限です。アカウント間の IAM ロール認証に適用されます。

AWS 認証情報プロファイル

AWS 認証情報プロファイルは、認証情報ファイルで定義できます。各認証情報プロファイルは、シークレットアクセスキーとアクセスキー ID で構成されています。

ユーザーは AWS 認証情報プロファイル名を使用して、実行時に、Amazon Kinesis Streams をソースとターゲット、Amazon Kinesis Firehose をターゲットとする Amazon Kinesis 接続を作成したときに指定した AWS 認証情報とは異なる AWS 認証情報を使用できます。

アクセスキー ID やシークレットアクセスキーなど、ユーザーの AWS 認証情報を作成します。ユーザーは、AWS 認証情報プロファイルなどの Amazon Kinesis 接続を作成するときに認証タイプを選択できます。デフォルトの認証タイプは AWS 認証情報プロファイルです。

AWS のユーザーのアクセスキー ID とシークレットアクセスキーを生成します。

Amazon Redshift V2 接続のプロパティ

Amazon Redshift との間でデータの読み取りまたは書き込みを行うための Amazon Redshift V2 接続を作成します。

認証の準備

Amazon Redshift V2 接続で**デフォルト**認証および **AssumeRole 認証タイプによる Redshift IAM** 認証を設定し、Amazon Redshift に接続できます。さらに、S3 リソースにアクセスするには、S3 ステージングの前提条件を満たす必要があります。必要に応じて、Amazon Redshift に接続するための暗号化を設定することもできます。

注: アプリケーション取り込みタスクとデータベース統合タスクは、EC2 インスタンスを使用してロールを引き受けない限り、AssumeRole による Redshift IAM 認証をサポートしません。

認証、ステージング、および暗号化の前提条件の概要については、次の各セクションを参照してください。

認証の前提条件

開始する前に、Amazon Redshift に登録されたユーザーアカウントが必要です。

次の表に示すように、設定する認証タイプに応じて、AWS コンソールで Amazon Redshift アカウントから最低限必要な詳細を取得します。

デフォルト認証	**引き受けロールによる Redshift IAM 認証**
- JDBC URL - ユーザー名 - パスワード	- JDBC URL - ユーザー名 - データベース名 - クラスタ識別子 - Redshift IAM ロール ARN*
*Redshift IAM ロール ARN を使用するには、必要な信頼ポリシーを使用して Redshift IAM ロール ARN を設定し、Amazon Redshift にアクセスするための一時的なセキュリティ資格情報を生成します。 詳細については、「Amazon Redshift の引き受けロールの設定」 (ページ 31)を参照してください。	

ステージングの前提条件

Amazon S3 でステージングを有効にし、データの読み取りまたは書き込み時に S3 リソースにアクセスするには、Amazon Redshift V2 接続でステージングプロパティを設定する必要があります。

次の表は、デフォルト認証と、AssumeRole 認証による Redshift IAM 認証の両方について接続で設定できるステージングオプションと、S3 ステージングに必要な詳細を取得するために実行する必要があるタスクをまとめたものです。

S3 ステージングオプション	**タスク**
S3 ステージングにアクセスするために S3 IAM ロールを引き受ける IAM ユーザーの一時的な資格情報を生成します。	**AWS の設定** IAM ユーザーが S3 IAM ロールを引き受け、一時的な資格情報を生成できるようにします。 手順については、次の参考資料を参照してください。 - 「Amazon S3 ステージングに AssumeRole を使用した一時的なセキュリティ資格情報の生成」 (ページ 35)。 - Using an assume role for Amazon S3 resources を参照してください。 **Redshift V2 接続設定** - S3 IAM **ロール** ARN の値を入力します。 - **[S3 アクセスキー** ID] と **[S3 シークレットアクセスキー]** の値を入力します。
S3 ステージングにアクセスするために S3 IAM ロールを引き受ける EC2 インスタンスの一時的なセキュリティ資格情報を生成します。	**AWS の設定** S3 IAM ロールを引き受けて S3 ステージング用の一時的な資格情報を生成するように EC2 インスタンスを定義します。 詳細については、「EC2 に AssumeRole を使用した一時的なセキュリティ資格情報の生成」 (ページ 37)を参照してください。 **Redshift V2 接続設定** 次の最小限必要なプロパティを設定します。 - **[ロールの引き受けに** EC2 **ロールを使用]** を有効にします。 - S3 IAM **ロール** ARN の値を入力します。

S3 ステージングオプション	タスク
S3 バケットへのアクセス権を持つ IAM ユーザーの S3 アクセスキーとシークレットアクセスキーを生成します。	AWS **の設定** 資格情報を生成するには、次のタスクを実行します。 1. 「最小限の Amazon IAM ポリシーの作成」 (ページ 30)。 2. IAM ユーザーを作成し、そのユーザーにポリシーを割り当てて、AWS コンソールで S3 アクセスキー ID と S3 シークレットアクセスキーを生成します。 IAM ユーザーの作成方法とキーの生成方法の詳細については、AWS のマニュアルを参照してください。 Redshift V2 **接続設定** [S3 **アクセスキー** ID] と [S3 **シークレットアクセスキー**] の値を入力します。
IAM 認証の設定	AWS **の設定** EC2 インスタンスがあり、キーを指定したり、IAM ロール ARN を使用したりしない場合は、S3 バケットにアクセスできる EC2 に最小限のポリシーを割り当てます。 詳細については、「IAM 認証の設定」 (ページ 31)を参照してください。 Redshift V2 **接続設定** この場合、接続でステージングプロパティを有効にしたり指定したりする必要はありません。

暗号化の前提条件

ステージング時のデフォルト認証と AssumeRole による Redshift IAM 認証にクライアントサイド暗号化とサーバーサイド暗号化を設定するには、「暗号化を有効にする」 (ページ 37)を参照してください。

最小限の Amazon IAM ポリシーの作成

Amazon S3 でデータをステージングするには、S3 リソースにアクセスするために最低限必要な権限を持つ IAM ポリシーを作成する必要があります。

ポリシーを IAM ユーザーにアタッチし、S3 リソースにアクセスするための S3 アクセスキー ID と S3 シークレットアクセスキーを生成できます。または、EC2 インスタンスがある場合は、EC2 インスタンスにステージング用の S3 バケットにアクセスするための最小限のポリシーを割り当てることもできます。

ポリシーには、次の最低限必要な権限を設定する必要があります。

- PutObject
- GetObject
- DeleteObject
- ListBucket

次のサンプル Amazon IAM ポリシーを使用できます。

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

```
            "Resource": [
                "arn:aws:s3:::<bucket_name>/*",
                "arn:aws:s3:::<bucket_name>"
            ]
        }
    ]
}
```

注: ［テスト接続］はユーザーに割り当てられた IAM ポリシーを検証しません。したがって、ユーザーに割り当てられたポリシーが有効であることを確認してください。

IAM 認証の設定

AWS Identity and Access Management（IAM）認証を設定して、EC2 ロールおよび Redshift ロールに最小限の Amazon IAM ポリシーを作成します。

手順については、次の How-To ライブラリの記事を参照してください: Configuring AWS IAM Authentication

Amazon Redshift の引き受けロールの設定

Redshift IAM ロール ARN を使用するには、必要な信頼ポリシーを使用して Redshift IAM ロール ARN を設定し、Amazon Redshift にアクセスするための一時的なセキュリティ資格情報を生成します。

次のいずれかのオプションを使用して、一時的なセキュリティ資格情報を生成できます。

AWS **の設定**	**接続の詳細**
オプション 1: IAM ユーザーを有効にするように AssumeRole を設定します。	IAM ユーザーに AssumeRole を使用するには、以下の IAM ユーザーの詳細を指定します。 - Redshift アクセスキー ID - Redshift シークレットアクセスキー - Redshift IAM ロール ARN
オプション 2: EC2 インスタンスを定義して、Redshift IAM ロールを引き受けます。	Amazon EC2 の AssumeRole を使用するには、次のようにします。 - ［Redshift IAM **ロール** ARN］値を指定します。 - **［ロールの引き受けに** EC2 **ロールを使用］**チェックボックスをオンにします。

アプリケーション取り込みタスクとデータベース取り込みタスクでは、オプション 2 を使用して、EC2 ロールが Redshift IAM ロールを引き受けるようにします。

AssumeRole の設定の詳細については、次の How-To ライブラリの記事を参照してください:
Configure AssumeRole authentication for Amazon Redshift V2 Connector

要件に基づいて一時的なセキュリティ資格情報を生成します。

Amazon Redshift の一時的なセキュリティ資格情報ポリシーの生成

一時的なセキュリティ資格情報を使用して Amazon Redshift に接続するには、IAM ユーザーと IAM ロールの両方にポリシーが必要です。

次のセクションに、IAM ユーザーと IAM ロールに必要なポリシーを示します。

IAM **ユーザー**

IAM ユーザーは、同じ AWS アカウントまたは異なる AWS アカウントで一時的なセキュリティ資格情報を使用するために、sts:AssumeRole ポリシーを持っている必要があります。IAM ユーザーの資格情報は、接続プロパティで Redshift アクセスキーと Redshift 秘密鍵を入力するために使用されます。

次のサンプルポリシーでは、IAM ユーザーに AWS アカウントで一時的なセキュリティ資格情報を使用することを許可しています。

```
{
"Version":"2012-10-17",
"Statement":
   { "Effect":"Allow",
"Action":"sts:AssumeRole",
"Resource":"arn:aws:iam::<ACCOUNT-HYPHENS>:role/<REDSHIFT-IAM-ROLE-NAME>"
   }
}
```

Redshift IAM **ロールの信頼ポリシー**

Redshift IAM ロールポリシーは、［Redshift IAM ロール ARN］で指定されたロールに関係します。IAM ユーザーが一時的なセキュリティ資格情報を使用して Redshift にアクセスできるようにするには、IAM ロールに信頼ポリシーがアタッチされている必要があります。

次のポリシーは、サンプルの信頼ポリシーです。

```
{
"Version":"2012-10-17",
"Statement":[
         {
         "Effect":"Allow",
         "Principal":{ "AWS":"arn:aws:iam::AWS-account-ID:<IAM-USER>" },
         "Action":"sts:AssumeRole"
          }
        ]
       }
}
```

例えば、ロールまたはユーザーを次の形式で指定できます。

```
{
"Version": "2012-10-17",
"Statement": [
    {
"Effect": "Allow",
"Principal": {
"AWS": "arn:aws:iam::<AWS-account>:role/<name-of-the-role>"
    },
       "Action": "sts:AssumeRole"
    }
 ]
}


{
"Version": "2012-10-17",
"Statement": [
    {
"Effect": "Allow",
"Principal": {
"AWS": " arn:aws:iam::<AWS-account>:user/<name-of-the-user>"
    },
       "Action": "sts:AssumeRole"
    }
 ]
}
```

Redshift IAM **ロールの最小限のアクセス許可ポリシー**

次のポリシーは、Redshift IAM ロールに必要なアクセス許可を示しています。これは、既存の Amazon Redshift ユーザーを使用して Redshift データベースに接続するために IAM ユーザーが引き受けます。

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

```
"Effect": "Allow",
"Action": [
          "redshift:GetClusterCredentials",

          "redshift:DescribeClusters"
            ],

"Resource": [
          "arn:aws:redshift:<REGION>:<ACCOUNT-ID>:dbuser:<Cluster_Identifier>/<USER_NAME>",

          "arn:aws:redshift:<REGION>:<ACCOUNT-ID>:dbname:<Cluster_Identifier>/<DATABASE_NAME>"

            ]

}
}
]
}
}
```

次のポリシーは、Redshift IAM ロールにアタッチする必要があるアクセス許可を示しています。これは、[DBUser の自動作成] チェックボックスで新規作成されたユーザーが Redshift データベースに接続するために、IAM ユーザーが引き受けます。

```
{

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

"Statement": [

{

"Effect": "Allow",

"Action": [
          "redshift:GetClusterCredentials",

          "redshift:DescribeClusters",

          "redshift:CreateClusterUser",

          "redshift:JoinGroup"
            ],

"Resource": [
          "arn:aws:redshift:<REGION>:<ACCOUNT-ID>:dbuser:<Cluster_Identifier>/<USER_NAME>",

          "arn:aws:redshift:<REGION>:<ACCOUNT-ID>:dbname:<Cluster_Identifier>/<DATABASE_NAME>",

          "arn:aws:redshift:<REGION>:<ACCOUNT-ID>:dbgroup:<Cluster_Identifier>/<GROUP_NAME>"
            ]
}

}

]

}
```

EC2 に AssumeRole を使用した一時的なセキュリティ資格情報の生成

Amazon EC2 ロールに AssumeRole を使用した一時的なセキュリティ資格情報を使用すると、同じ AWS アカウントまたは異なる AWS アカウントから Amazon Redshift に接続することができます。

Amazon EC2 ロールにより、Redshift アクセスキーと Redshift シークレットキーを必要とせずに、同じ AWS アカウントまたは異なる AWS アカウントから別の IAM ロールを引き受けることができます。

AssumeRole for EC2 を使用して一時的なセキュリティ資格情報を使用する場合は、次の前提条件を考慮してください。

- AssumeRole for EC2 を使用して一時的なセキュリティ資格情報を使用するには、Amazon EC2 などの AWS サービスに Secure Agent をインストールします。
- AWS EC2 サービスにアタッチされた EC2 ロールは、Amazon Redshift へのアクセス権を持っていてはいけませんが、別の IAM ロールを引き受ける権限が必要です。
- EC2 ロールが引き受ける必要のある IAM ロールには、アクセス許可ポリシーと信頼ポリシーがアタッチされている必要があります。

［Redshift IAM ロール ARN］接続プロパティで指定した IAM ロールを引き受けるように EC2 ロールを設定するには、接続プロパティの **［ロールの引き受けに EC2 ロールを使用］**チェックボックスをオンにします。

EC2 **サービスロールの信頼ポリシー**

以下は、EC2 インスタンスにアタッチされた EC2 ロールの信頼関係で定義されている信頼ポリシーの例です。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "ec2.amazonaws.com"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

EC2 のロールを引き受ける場合の Redshift IAM ロールの信頼ポリシーの例を以下に示します。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "redshift.amazonaws.com"
            },
            "Action": "sts:AssumeRole"
        },
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::<Account-ID:role>/ec2_role_attached_to_ec2_instance"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

EC2 インスタンスにアタッチする必要がある権限ポリシーは、IAM ユーザーに対して定義されたポリシーと同じです。

Amazon S3 ステージングの引き受けロールの設定

S3 ステージングの AssumeRole 認証を設定するには、AWS コンソールで IAM ユーザーと IAM ロールに最小限の権限ポリシーと信頼ポリシーをアタッチする必要があります。

IAM ユーザーは、AssumeRole を使用して、Amazon S3 リソースに一時的にアクセスできます。Amazon S3 リソースの引き受けロールの使用方法の詳細については、次の How-To ライブラリの記事も参照してください: Using an assume role for Amazon S3 resources

Amazon S3 ステージング用の AssumeRole を使用して一時的なセキュリティ資格情報を生成すると、Amazon S3 ステージングバケットにアクセスできます。EC2 インスタンスが IAM ロールを引き受けて S3 ステージングバケットに安全にアクセスできるようにする場合は、AssumeRole for EC2 インスタンスを使用して生成された一時的なセキュリティ資格情報を使用します。

注: 一時的なセキュリティ資格情報を生成する場合は、AWS アカウントのルートユーザー資格情報を使用しないでください。一時的なセキュリティ資格情報を生成するには、IAM ユーザーの資格情報を使用する必要があります。

要件に基づいて一時的なセキュリティ資格情報を生成します。

Amazon S3 ステージングに AssumeRole を使用した一時的なセキュリティ資格情報の生成

AssumeRole を使用した一時的なセキュリティ資格情報を使用すると、同じ AWS アカウントまたは異なる AWS アカウントから Amazon S3 ステージングバケットにアクセスできます。

sts:AssumeRole 権限が割り当てられており、AWS アカウント内に一時的なセキュリティ資格情報を使用するための信頼関係が構築されていることを確認します。信頼関係は、ロールを作成するときに、IAM ロールの信頼ポリシーで定義します。IAM ロールにより、IAM ユーザーを信頼されたエンティティとして追加し、IAM ユーザーに一時的なセキュリティ資格情報の使用と AWS アカウントへのアクセスを許可します。信頼関係を構築する方法の詳細については、AWS のマニュアルを参照してください。

信頼された IAM ユーザーが一時的なセキュリティ資格情報を要求すると、AWS Security Token Service（AWS STS）によって、指定した期間有効な一時的なセキュリティ資格情報が動的に生成され、信頼された IAM ユーザーにその資格情報が提供されます。一時的なセキュリティ資格情報は、アクセスキー ID、シークレットアクセスキー、シークレットトークンで構成されます。

動的に生成された一時的なセキュリティ資格情報を使用するには、Amazon Redshift V2 接続を作成するときに［**S3 IAM ロール ARN**］接続プロパティの値を入力します。IAM ロール ARN では、AWS リソースが一意に識別されます。次に、［**一時的な資格情報の期間**］詳細ソースプロパティおよびターゲットプロパティで、一時的なセキュリティ資格情報を使用できる期間を秒単位で指定します。

外部 ID

Amazon S3 バケットが IAM ユーザーまたは EC2 インスタンスとは別の AWS アカウントにある場合に、Amazon S3 バケットへのより安全なアクセスを確立するための外部 ID を指定できます。

注: アプリケーション取り込みタスクとデータベース統合タスクでは、外部 ID の使用はサポートされていません。

必要に応じて、AWS Security Token Service（STS）への AssumeRole 要求で外部 ID を指定できます。

外部 ID は文字列である必要があります。次のサンプルは、引き継がれた IAM ロールの信頼ポリシー内の外部 ID 条件を示しています。

```
"Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::AWS_Account_ID : user/user_name"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "sts:ExternalId": "dummy_external_id"
        }
      }
    }
  ]
```

一時的なセキュリティ資格情報のポリシー

一時的なセキュリティ資格情報を使用して Amazon S3 ステージングバケットにアクセスするには、IAM ユーザーと IAM ロールにポリシーが必要です。

次のセクションに、IAM ユーザーと IAM ロールに必要なポリシーを示します。

IAM **ユーザー**

IAM ユーザーは、同じ AWS アカウントまたは異なる AWS アカウントで一時的なセキュリティ資格情報を使用するために、sts:AssumeRole ポリシーを持っている必要があります。

次のサンプルポリシーでは、IAM ユーザーに AWS アカウントで一時的なセキュリティ資格情報を使用することを許可しています。

```
{
"Version":"2012-10-17",
"Statement":
        { "Effect":"Allow", "Action":"sts:AssumeRole",
          "Resource":"arn:aws:iam::<ACCOUNT-HYPHENS>:role/<ROLE-NAME>" }
}
```

次のサンプルポリシーでは、中国地域の IAM ユーザーに AWS アカウントで一時的なセキュリティ資格情報を使用することを許可しています。

```
{
"Version":"2012-10-17",
"Statement":
        {
        "Effect":"Allow", "Action":"sts:AssumeRole",
        "Resource":"arn:aws-cn:iam::<ACCOUNT-HYPHENS>:role/<ROLE-NAME>"
       }
}
```

IAM **ロール**

IAM ロールには、IAM ユーザーに対して一時的なセキュリティ資格情報を使用した Amazon S3 バケットへのアクセスを許可するために、sts:AssumeRole ポリシーと IAM ロールにアタッチされた信頼ポリシーが必要です。このポリシーは、IAM ユーザーがアクセスできる Amazon S3 バケットと、IAM ユーザーが実行できるアクションを指定します。信頼ポリシーは、Amazon S3 バケットにアクセスできる AWS アカウントの IAM ユーザーを指定します。

次のポリシーは、サンプルの信頼ポリシーです。

```
{
"Version":"2012-10-17",
"Statement":[
         {
         "Effect":"Allow",
         "Principal":{ "AWS":"arn:aws:iam::AWS-account-ID:<ROLE-NAME" },
         "Action":"sts:AssumeRole"
          }
        ]
       }
}
```

KMS に対する一時的なセキュリティ資格情報

AWS Key Management Service（AWS KMS）で管理されたカスタママスタキーを使用する一時的なセキュリティ資格情報を使用し、KMS を使用した暗号化を有効にするには、KMS ポリシーを作成する必要があります。

次の操作を実行すると、一時的なセキュリティ資格情報を使用し、KMS を使用した暗号化を有効にすることができます。

- GenerateDataKey
- DescribeKey

- 暗号化
- 復号化
- ReEncrypt

次のサンプルポリシーを使用できます。

```
{
"Version":"2012-10-17",
"Statement":[
{ "Effect":"Allow",
"Action":
[ "kms:GenerateDataKey", "kms:DescribeKey", "kms:Encrypt", "kms:Decrypt", "kms:ReEncrypt*" ],
"Resource": ["arn:aws:kms:region:account:key/<KMS_key>"]
    }
  ]
   }
```

KMS を設定し、中国地域の Amazon S3 エンドポイントにアクセスする場合は、次のサンプルポリシーを使用します。

```
{
"Version":"2012-10-17",
"Statement":[
{ "Effect":"Allow",
"Action":[ "kms:GenerateDataKey", "kms:DescribeKey", "kms:Encrypt", "kms:Decrypt", "kms:ReEncrypt*" ],
"Resource": ["arn:aws-cn:kms:region:account:key/<KMS_key>"]
    }
  ]
   }
```

EC2 に AssumeRole を使用した一時的なセキュリティ資格情報の生成

Amazon EC2 ロールに AssumeRole を使用した一時的なセキュリティ資格情報を使用すると、同じ AWS アカウントまたは異なる AWS アカウントから Amazon S3 ステージングバケットにアクセスできます。

Amazon EC2 ロールにより、永続的なアクセスキーとシークレットキーを必要とせずに、同じ AWS アカウントまたは異なる AWS アカウントから別の IAM ロールを引き受けることができます。Amazon EC2 ロールにより、別のリージョンから別の IAM ロールを引き受けることもできます。

AssumeRole for EC2 を使用した一時的なセキュリティ資格情報を使用する場合は、次の前提条件を考慮してください。

- AssumeRole for EC2 を使用して一時的なセキュリティ認証情報を使用するには、Amazon EC2 などの AWS サービスに Secure Agent をインストールします。
- AWS EC2 サービスにアタッチされた EC2 ロールは、Amazon S3 へのアクセス権を持っていてはいけませんが、別の IAM ロールを引き受ける権限が必要です。
- EC2 ロールが引き受ける必要のある IAM ロールには、アクセス許可ポリシーと信頼ポリシーがアタッチされている必要があります。

［IAM ロール ARN］接続プロパティで指定した IAM ロールを引き受けるように EC2 ロールを設定するには、接続プロパティの**［ロールの引き受けに EC2 ロールを使用］**チェックボックスをオンにします。

暗号化を有効にする

Amazon S3 でデータをステージングするために、Amazon Redshift V2 接続でクライアントサイド暗号化とサーバーサイド暗号化を有効にすることができます。
Amazon Redshift V2 接続で設定する暗号化のタイプに応じた前提条件を満たします。

クライアントサイド暗号化

クライアントサイド暗号化には、Base64 形式の 256 ビット AES 暗号化キーが必要です。暗号化キーは、サードパーティ製ツールを使用して生成できます。

Amazon Redshift V2 接続を作成するときに、**[マスタ対称キー]** フィールドにキー値を指定します。

サーバーサイド暗号化

サーバーサイド暗号化を有効にするには、AWS Key Management Service（AWS KMS）で管理される顧客マスタキーを作成します。

Amazon S3 ステージングバケットが存在するリージョンの顧客マスタキー ID を生成します。顧客マスタキーの生成の詳細については、AWS のドキュメントを参照してください。

カスタママスタキーを使用した暗号化を有効にするには、最小限の KMS ポリシーを作成する必要があります。Amazon Redshift V2 接続を作成するときに、顧客マスタキー ID を指定できます。

注: マスタ対称キーを使用したサーバーサイド暗号化と、顧客マスタキーを使用したクライアントサイド暗号化を設定することはできません。

AWS KMS を使用するための最小限のポリシーの作成

AWS Key Management Service（AWS KMS）で管理された顧客マスタキーを使用し、KMS を使用した暗号化を有効にするには、KMS ポリシーを作成する必要があります。

KMS を使用した暗号化を有効にするには、次の操作を実行します。

- GenerateDataKey
- DescribeKey
- 暗号化
- 復号化
- ReEncrypt

サンプルポリシー:

```
{
"Version":"2012-10-17",
"Statement":[
{ "Effect":"Allow",
"Action":
[ "kms:GenerateDataKey", "kms:DescribeKey", "kms:Encrypt", "kms:Decrypt", "kms:ReEncrypt*" ],
"Resource": ["arn:aws:kms:region:account:key/<KMS_key>"]
    }
  ]
   }
```

KMS を設定し、中国地域の Amazon S3 エンドポイントにアクセスする場合は、次のサンプルポリシーを使用します。

```
{
"Version":"2012-10-17",
"Statement":[
{ "Effect":"Allow",
"Action":[ "kms:GenerateDataKey", "kms:DescribeKey", "kms:Encrypt", "kms:Decrypt", "kms:ReEncrypt*" ],
"Resource": ["arn:aws-cn:kms:region:account:key/<KMS_key>"]
    }
  ]
   }
```

Amazon Redshift への接続

Amazon Redshift に接続するように Amazon Redshift V2 接続プロパティを設定してみましょう。

始める前に

接続を設定する前に、「認証の準備」 (ページ 28)を参照して認証要件を確認してください。

接続の詳細

次の表に、基本接続プロパティを示します。

プロパティ	説明
接続名	接続の名前。各接続名は組織内で一意である必要があります。接続名には、英数字、スペース、および次の特殊文字を含めることができます。_.+ -。最大長は 255 文字です。
説明	接続の説明。最大長は 4000 文字です。
タイプ	Amazon Redshift V2
ランタイム環境	タスクを実行するランタイム環境の名前。 ホステッドエージェントまたはサーバーレスランタイム環境では、アプリケーション取り込みタスク、データベース取り込みタスク、ファイル取り込みタスク、またはストリーミング取り込みタスクを実行することはできません。

認証タイプ

Amazon Redshift にアクセスするために、デフォルトの認証タイプおよび Redshift IAM AssumeRole 認証タイプを設定できます。
注: アプリケーション取り込みタスクとデータベース取り込みタスクは、EC2 インスタンスを使用しない Redshift IAM AssumeRole 認証をサポートしていません。

必要な認証方法を選択し、認証固有のパラメータを設定します。

デフォルト認証

次の表に、デフォルト認証の基本接続プロパティを示します。

プロパティ	説明
JDBC URL	Amazon Redshift クラスタに接続するための JDBC URL。 JDBC URL は、Amazon AWS Redshift クラスタ設定ページから取得できます。 JDBC URL は次の形式で入力します。 `jdbc:redshift://<cluster_endpoint>:<port_number>/<database_name>`ここで、エンドポイントには Redshift クラスタ名とリージョンが含まれます。 例: `jdbc:redshift://infa-rs-cluster.abc.us-west-2.redshift.amazonaws.com:5439/rsdb` この例では、 - infa-rs-qa-cluster は Redshift クラスタの名前です。 - us-west-2.redshift.amazonaws.com は Redshift クラスタエンドポイントであり、米国西部（オレゴン）リージョンです。 - 5439 は Redshift クラスタのポート番号です。 - rsdb は、接続先の Redshift クラスタ内の特定のデータベースインスタンスです。
ユーザー名	Amazon Redshift クラスタ内のデータベースインスタンスのユーザー名。

プロパティ	説明
パスワード	Amazon Redshift データベースユーザーのパスワード。
ロールの引き受けに EC2 ロールを使用	S3 IAM ロールを引き受ける EC2 インスタンスが S3 リソースにアクセスし、一時的なセキュリティ資格情報を使用してデータをステージングできるようにします。 EC2 ロールには、S3 IAM ロールを引き受ける権限がアタッチされたポリシーが必要です。S3 IAM ロールと EC2 インスタンスは、同じ AWS アカウントでも異なる AWS アカウントでもかまいません。 このチェックボックスを選択すると、EC2 ロールが［S3 IAM ロール ARN］オプションで指定された S3 IAM ロールを引き受けて、ステージングデータ用の S3 リソースにアクセスできるようになります。 このプロパティは、アプリケーション取り込みタスクおよびデータベース取り込みタスクには適用されません。デフォルトでは、このチェックボックスは選択されていません。 詳細については、「EC2 に AssumeRole を使用した一時的なセキュリティ資格情報の生成」 (ページ 37)を参照してください。
S3 IAM ロール ARN	Amazon S3 にデータをステージングする目的で動的に生成された一時的なセキュリティ資格情報を使用するために IAM ユーザーまたは EC2 に引き受けられた IAM ロールの Amazon Resource Number（ARN）。 このプロパティは、EC2 インスタンス、または S3 IAM ロールを引き受ける IAM ユーザーを使用して S3 ステージングバケットにアクセスするための一時的なセキュリティ資格情報を生成する場合に適用されます。 一時的なセキュリティ資格情報を使用して Amazon S3 ステージングバケットにアクセスするための S3 IAM ロール名を指定します。 S3 IAM ロールの ARN の取得方法の詳細については、AWS documentation を参照してください。 **注**: ロールベースの認証を利用するアプリケーション取り込みタスクまたはデータベース取り込みタスクの接続を使用するが、AWS クラスタのデフォルトロールではない場合は、［IAM ロール ARN］を指定します。デフォルトロールを使用する場合、このフィールドは空白のままにします。

詳細設定

次の表に、デフォルト認証の詳細接続プロパティを示します。

プロパティ	説明
S3 アクセスキー ID	Amazon S3 ステージングバケットにアクセスするための IAM ユーザーのアクセスキー。 S3 ステージングに次の方法を使用する場合は、アクセスキー ID を入力します。 - IAM ユーザーが S3 ステージングにアクセスできる場合。 - S3 IAM ロールを引き受ける IAM ユーザーが一時的なセキュリティ資格情報を使用して S3 にアクセスする場合。 IAM 認証または EC2 の引き受けロールを使用して S3 にアクセスする場合は、S3 アクセスキー ID を入力する必要はありません。 **注**: キーベースの認証を利用するアプリケーション取り込みタスクまたはデータベース取り込みタスクの接続を使用する場合は、アクセスキーの値を指定します。
S3 シークレットアクセスキー	Amazon S3 ステージングバケットにアクセスするためのシークレットアクセスキー。 秘密鍵はアクセスキーに関連付けられており、アカウントを一意に識別します。 S3 ステージングに次の方法を使用する場合は、シークレットアクセスキー値を入力します。 - IAM ユーザーが S3 ステージングにアクセスできる場合。 - S3 IAM ロールを引き受ける IAM ユーザーが一時的なセキュリティ資格情報を使用して S3 にアクセスする場合。 IAM 認証または EC2 の引き受けロールを使用して S3 にアクセスする場合は、S3 シークレットアクセスキーを入力する必要はありません。 **注**: キーベースの認証を利用するアプリケーション取り込みタスクまたはデータベース取り込みタスクの接続を使用する場合は、アクセスキーの値を指定します。
S3 VPC エンドポイントタイプ	Amazon S3 用の Amazon Virtual Private Cloud エンドポイントのタイプ。 VPC エンドポイントを使用して、Amazon S3 とのプライベート通信を有効にすることができます。 次のいずれかのオプションを選択します。 - デフォルト。VPC エンドポイントを使用しない場合に選択します。 - インタフェースエンドポイント。サブネットの IP アドレス範囲内のプライベート IP アドレスを持つインタフェースエンドポイントを介して Amazon S3 とのプライベート通信を確立する場合に選択します。これは、AWS のサービス宛てのトラフィックのエントリポイントとして機能します。
Amazon S3 のエンドポイント DNS 名	Amazon S3 インタフェースエンドポイントの DNS 名。 DNS 名のアスタリスク記号を bucket キーワードで置き換えます。 DNS 名は以下の形式で入力します。 `bucket.<インタフェースエンドポイントの DNS 名>` 例: `bucket.vpce-s3.us-west-2.vpce.amazonaws.com`
外部 ID	IAM ロールに関連付けられた外部 ID。 Amazon S3 バケットへのより安全なアクセスを提供する場合は、外部 ID を指定できます。Amazon S3 ステージングバケットと IAM ロールは、同じ AWS アカウントでも異なる AWS アカウントでもかまいません。 必要に応じて、引き受けた IAM ロールの信頼ポリシーの外部 ID 条件を使用して、AWS Security Token Service（STS）への AssumeRole 要求で外部 ID を指定することもできます。 外部 ID の使用方法の詳細については、 External ID when granting access to your AWS resources を参照してください。 このプロパティは、アプリケーション取り込みタスクおよびデータベース取り込みタスクには適用されません。

プロパティ	説明
クラスタリージョン	Redshift クラスタが存在する AWS クラスタリージョン。 ［JDBC URL］フィールドプロパティで指定されているものとは異なるクラスタリージョンのカスタム JDBC URL を指定する場合は、リストからクラスタリージョンを選択します。［JDBC URL］フィールドプロパティで指定されているクラスタリージョン名を引き続き使用するには、このプロパティでクラスタリージョンとして**［なし］**を選択します。 AWS SDK によってサポートされるクラスタリージョンとの間でのみ、データの読み取りと書き込みを行うことができます。 次のいずれかのクラスタリージョンを選択します。 なし アジアパシフィック（ムンバイ） アジアパシフィック（ソウル） アジアパシフィック（シンガポール） アジアパシフィック（シドニー） アジアパシフィック（東京） アジアパシフィック（香港） AWS GovCloud(米国) AWS GovCloud （米国東部） カナダ（中部） 中国（北京） 中国（寧夏） 欧州（アイルランド） 欧州（フランクフルト） 欧州(パリ) 欧州(ストックホルム) 南米（サンパウロ） 中東(バーレーン) 米国東部（バージニア北部） 米国東部（オハイオ） 米国西部（北カリフォルニア） 米国西部（オレゴン） デフォルトは**［なし］**です。 **注**: リージョン値は、アプリケーション取り込みタスクとデータベース取り込みタスクに必要です。
マスタ対称キー	Amazon S3 でステージングするためにデータを送信する前にクライアントサイド暗号化でデータを暗号化できる、Base64 形式の 256 ビット AES 暗号化キー。 詳細については、「「暗号化を有効にする」 (ページ 37)」を参照してください。 このプロパティは、アプリケーション取り込みタスクおよびデータベース取り込みタスクには適用されません。
顧客マスタキー ID	AWS Key Management Service（AWS KMS）によって生成されたカスタママスタキー ID、または Amazon S3 でデータをステージングする際にクロスアカウントアクセスするためのカスタムキーの ARN。カスタママスタキーは、データが Amazon S3 に保存される前にコピー先で暗号化するためのものです。 顧客が生成した顧客マスタキー ID、またはデフォルトの顧客マスタキー ID を入力できます。 このプロパティは、アプリケーション取り込みタスクおよびデータベース取り込みタスクには適用されません。

AssumeRole による Redshift の IAM 認証。

Redshift AssumeRole 認証を使用すると、ユーザーは IAM ロールを引き受けるか、必要な信頼ポリシーで設定された EC2 ロールを定義して、Amazon Redshift にアクセスするための一時的なセキュリティ資格情報を生成できます。

注: アプリケーション取り込みタスクとデータベース取り込みタスクでは、EC2 ロールを使用する必要があります。

次の表に、Redshift IAM AssumeRole 認証の基本接続プロパティを示します。

プロパティ	説明
JDBC URL	Amazon Redshift クラスタに接続するための JDBC URL。 JDBC URL は、Amazon AWS Redshift クラスタ設定ページから取得できます。 JDBC URL は次の形式で入力します。 `jdbc:redshift://<cluster_endpoint>:<port_number>/<database_name>`ここで、エンドポイントには Redshift クラスタ名とリージョンが含まれます。 例: `jdbc:redshift://infa-rs-cluster.abc.us-west-2.redshift.amazonaws.com:5439/rsdb` この例では、 - infa-rs-qa-cluster は Redshift クラスタの名前です。 - us-west-2.redshift.amazonaws.com は Redshift クラスタエンドポイントであり、米国西部（オレゴン）リージョンです。 - 5439 は Redshift クラスタのポート番号です。 - rsdb は、接続先の Redshift クラスタ内の特定のデータベースインスタンスです。
ユーザー名	Amazon Redshift クラスタ内のデータベースインスタンスのユーザー名。
クラスタ識別子	Amazon Redshift をホストするクラスタの一意の識別子。 Amazon Redshift クラスタ名を指定します。
データベース名	アクセスするテーブルが保存されている Amazon Redshift データベースの名前。
Redshift IAM ロール ARN	Amazon Redshift にアクセスする目的で動的に生成された一時的なセキュリティ資格情報を使用するために EC2 によって引き受けられた IAM ロールの Amazon Resource Number (ARN)。 Amazon Redshift クラスタにアクセスするための Redshift IAM ロール ARN を入力します。

プロパティ	説明
ロールの引き受けに EC2 ロールを使用	EC2 ロールが IAM ロールを引き受けて、Redshift に接続するか、一時的なセキュリティ資格情報を使用してデータをステージングできるようにします。 **EC2 ロールを使用して IAM 認証で Redshift に接続する** チェックボックスを選択すると、[Redshift IAM **ロール** ARN] フィールドで指定された Redshift IAM ロールを引き受ける EC2 ロールが Amazon Redshift にアクセスできるようになります。 EC2 ロールには、同じアカウントまたは異なるアカウントから Redshift IAM ロールを引き受けるための権限がアタッチされたポリシーが必要です。 **S3 リソースにアクセスしてデータをステージングする** このチェックボックスをオンにすると、EC2 ロールが [S3 IAM **ロール** ARN] フィールドで指定された S3 IAM ロールを引き受け、S3 ステージングバケットにアクセスするための一時的なセキュリティ資格情報を動的に生成できるようになります。 EC2 ロールには、同じ AWS アカウントまたは異なる AWS アカウントから S3 IAM ロールを引き受けるための権限がアタッチされたポリシーが必要です。
S3 IAM ロール ARN	Amazon S3 にデータをステージングする目的で動的に生成された一時的なセキュリティ資格情報を使用するために IAM ユーザーまたは EC2 に引き受けられた S3 IAM ロールの Amazon Resource Number（ARN）。 このプロパティは、EC2 インスタンス、または S3 IAM ロールを引き受ける IAM ユーザーを使用して S3 ステージングバケットにアクセスするための一時的なセキュリティ資格情報を生成する場合に適用されます。 一時的なセキュリティ資格情報を使用して Amazon S3 ステージングバケットにアクセスするための S3 IAM ロール名を指定します。 IAM ロールの ARN の取得方法の詳細については、AWS documentation を参照してください。 **注**: ロールベースの認証を利用するアプリケーション取り込みタスクまたはデータベース取り込みタスクの接続を使用するが、AWS クラスタのデフォルトロールではない場合は、[IAM ロール ARN] を指定します。デフォルトロールを使用する場合、このフィールドは空白のままにします。

詳細設定

次の表に、Redshift IAM AssumeRole 認証の詳細接続プロパティを示します。

プロパティ	説明
Redshift アクセスキー ID	Redshift IAM AssumeRole ARN を引き受ける権限を持つ IAM ユーザーのアクセスキー。 このプロパティは、EC2 ロールを使用した Amazon Redshift AssumeRole 認証には適用されません。
Redshift シークレットアクセスキー	Redshift IAM AssumeRole ARN を引き受ける権限を持つ IAM ユーザーのシークレットアクセスキー。 このプロパティは、EC2 ロールを使用した Amazon Redshift AssumeRole 認証には適用されません。

プロパティ	説明
データベースグループ	この接続プロパティで［DBUser **の自動作成**］オプションを選択した場合にデータベースユーザーを追加するデータベースグループの名前。 このデータベースグループに追加したユーザーは、指定されたグループ特権を継承します。 データベースグループ名を指定しない場合、ユーザーはパブリックグループに追加され、関連する特権を継承します。 また、複数のデータベースグループをカンマで区切って入力し、指定した各データベースグループにユーザーを追加することもできます。
有効期限	Amazon Redshift データベースユーザーのパスワードの有効期限。 900 秒から 3600 秒の間の値を指定します。 デフォルトは 900 です。
DBUser の自動作成	実行時に新しい Amazon Redshift データベースユーザーの作成を選択します。 エージェントは、**［ユーザー名］**フィールドで指定したユーザーをデータベースグループに追加します。追加されたユーザーは、データベースグループに割り当てられた特権を引き受けます。 デフォルトでは無効になっています。
S3 アクセスキー ID	Amazon S3 ステージングバケットにアクセスするための IAM ユーザーのアクセスキー。 S3 ステージングに次の方法を使用する場合は、アクセスキー ID を入力します。 - IAM ユーザーが S3 ステージングにアクセスできる場合。 - S3 IAM ロールを引き受ける IAM ユーザーが一時的なセキュリティ資格情報を使用して S3 にアクセスする場合。 IAM 認証または EC2 の引き受けロールを使用して S3 にアクセスする場合は、S3 アクセスキー ID を入力する必要はありません。 **注**: キーベースの認証を利用するアプリケーション取り込みタスクまたはデータベース取り込みタスクの接続を使用する場合は、アクセスキーの値を指定します。
S3 シークレットアクセスキー	Amazon S3 ステージングバケットにアクセスするためのシークレットアクセスキー。 秘密鍵はアクセスキーに関連付けられており、アカウントを一意に識別します。 S3 ステージングに次の方法を使用する場合は、シークレットアクセスキー値を入力します。 - IAM ユーザーが S3 ステージングにアクセスできる場合。 - S3 IAM ロールを引き受ける IAM ユーザーが一時的なセキュリティ資格情報を使用して S3 にアクセスする場合。 IAM 認証または EC2 の引き受けロールを使用して S3 にアクセスする場合は、S3 シークレットアクセスキーを入力する必要はありません。 **注**: キーベースの認証を利用するアプリケーション取り込みタスクまたはデータベース取り込みタスクの接続を使用する場合は、アクセスキーの値を指定します。
S3 VPC エンドポイントタイプ	Amazon S3 用の Amazon Virtual Private Cloud エンドポイントのタイプ。 VPC エンドポイントを使用して、Amazon S3 とのプライベート通信を有効にすることができます。 次のいずれかのオプションを選択します。 - デフォルト。VPC エンドポイントを使用しない場合に選択します。 - インタフェースエンドポイント。サブネットの IP アドレス範囲内のプライベート IP アドレスを持つインタフェースエンドポイントを介して Amazon S3 とのプライベート通信を確立する場合に選択します。これは、AWS のサービス宛てのトラフィックのエントリポイントとして機能します。

プロパティ	説明
Amazon S3 のエンドポイント DNS 名	Amazon S3 インタフェースエンドポイントの DNS 名。 DNS 名のアスタリスク記号を bucket キーワードで置き換えます。 DNS 名は以下の形式で入力します。 `bucket.<インタフェースエンドポイントの DNS 名>` 例: `bucket.vpce-s3.us-west-2.vpce.amazonaws.com`
外部 ID	IAM ロールに関連付けられた外部 ID。 Amazon S3 ステージングバケットが同じ AWS アカウントまたは異なる AWS アカウントにあり、Amazon S3 バケットへのより安全なアクセスを提供する場合に、外部 ID を指定できます。 必要に応じて、引き受けた IAM ロールの信頼ポリシーの外部 ID 条件を使用して、AWS Security Token Service（STS）への AssumeRole 要求で外部 ID を指定することもできます。 外部 ID の使用方法の詳細については、 External ID when granting access to your AWS resources を参照してください。 このプロパティは、アプリケーション取り込みタスクおよびデータベース取り込みタスクには適用されません。

プロパティ	説明
クラスタリージョン	Redshift クラスタが存在する AWS の地理的なリージョン。 ［JDBC URL］フィールドプロパティで指定されているものとは異なるクラスタリージョンのカスタム JDBC URL を指定する場合は、リストからクラスタリージョンを選択します。［JDBC URL］フィールドプロパティで指定されているクラスタリージョン名を引き続き使用するには、このプロパティでクラスタリージョンとして**［なし］**を選択します。 AWS SDK によってサポートされるクラスタリージョンとの間でのみ、データの読み取りと書き込みを行うことができます。 次のいずれかのクラスタリージョンを選択します。 なし アジアパシフィック（ムンバイ） アジアパシフィック（ソウル） アジアパシフィック（シンガポール） アジアパシフィック（シドニー） アジアパシフィック（東京） アジアパシフィック（香港） AWS GovCloud（米国） AWS GovCloud （米国東部） カナダ（中部） 中国（北京） 中国（寧夏） 欧州（アイルランド） 欧州（フランクフルト） EU（パリ） EU（ストックホルム） 南米（サンパウロ） 中東（バーレーン） 米国東部（バージニア北部） 米国東部（オハイオ） 米国西部（北カリフォルニア） 米国西部（オレゴン） デフォルトは**［なし］**です。 **注**: リージョン値は、アプリケーション取り込みタスクとデータベース取り込みタスクに必要です。

プロパティ	説明
マスタ対称キー	Amazon S3 でステージングするためにデータを送信する前にクライアントサイド暗号化でデータを暗号化できる、Base64 形式の 256 ビット AES 暗号化キー。 詳細については、「「暗号化を有効にする」 (ページ 37)」を参照してください。 このプロパティは、アプリケーション取り込みタスクおよびデータベース取り込みタスクには適用されません。
顧客マスタキー ID	AWS Key Management Service（AWS KMS）によって生成されたカスタママスタキー ID、または Amazon S3 でデータをステージングする際にクロスアカウントアクセスするためのカスタムキーの ARN。カスタママスタキーは、データが Amazon S3 に保存される前にコピー先で暗号化するためのものです。 顧客が生成した顧客マスタキー ID、またはデフォルトの顧客マスタキー ID を入力できます。 サーバーサイド暗号化の設定方法の詳細については、「暗号化を有効にする」 (ページ 37)を参照してください。 このプロパティは、アプリケーション取り込みタスクおよびデータベース取り込みタスクには適用されません。

プロキシサーバーの設定

組織で送信プロキシサーバーを使用してインターネットに接続する場合、Secure Agent は、そのプロキシサーバー経由で Informatica Intelligent Cloud Services に接続します。

Windows および Linux でプロキシサーバーを使用するように Secure Agent を設定できます。認証されていないプロキシサーバーのみを使用できます。

Secure Agent のプロキシの設定を行うには、次のいずれかの方法を使用します。

- Windows の場合は Secure Agent Manager を使用し、Linux の場合はシェルコマンドを使用して Secure Agent を設定します。

  手順については、データ統合のヘルプの『基本操作』にある、トピックまたは「Windows でのプロキシ設定」または「Linux でのプロキシ設定」を参照してください。
- Secure Agent のプロパティで、DTM の JVM オプションを設定します。手順については、ナレッジベースの記事「Proxy server settings」を参照してください。

注: HTTP プロキシと SOCKS プロキシの両方を有効にすると、デフォルトでは SOCKS プロキシが使用されます。SOCKS プロキシの代わりに HTTP プロキシを使用する場合は、システムプロパティで **[DisableSocksProxy]** プロパティの値を true に設定します。

Amazon Redshift とのプライベート通信

トラフィックを公共のインターネットに公開しないようにする場合は、AWS コンソールでゲートウェイエンドポイントを設定することで、Amazon Redshift とのプライベート通信を有効にすることができます。

Amazon Redshift とのプライベート接続を確立するには、Secure Agent が AWS Virtual Private Cloud（VPC）のサブネットの一部であることを確認します。ゲートウェイエンドポイントを作成し、Amazon S3 データを Amazon Redshift にステージングできます。

Amazon Redshift に接続するためのプライベート通信を設定するには、次のタスクを実行する必要があります。

- クラスタサブネットグループを作成します。
- Redshift 管理の VPC エンドポイントを作成します。

- ゲートウェイエンドポイントを設定します。

これにより、Amazon Redshift V2 接続プロパティでゲートウェイエンドポイントを指定できるようになります。

詳細については、
「Configuring private communication with Amazon Redshift using the Amazon Redshift V2 Connector」を参照してください。

Amazon S3 V2 接続プロパティ

Amazon S3 V2 接続をセットアップする際には、接続プロパティを設定します。

次の表に、Amazon S3 V2 接続プロパティを示します。

プロパティ	説明
接続名	接続の名前。 各接続名は組織内で一意である必要があります。接続名には、英数字、スペース、および次の特殊文字を含めることができます。_ .+ -, 最大長は 255 文字です。
説明	接続の説明。最大長は 4000 文字です。
タイプ	Amazon S3 V2 接続タイプ。
ランタイム環境	タスクを実行するランタイム環境の名前。 Hosted Agent またはサーバーレスランタイム環境でアプリケーション取り込みタスクまたはデータベース取り込みタスクを実行することはできません。
アクセスキー	Amazon S3 バケットにアクセスするためのアクセスキー。 次の認証方法に基づいてアクセスキー値を入力します。 - 基本認証。実際のアクセスキー値を入力します。 - IAM 認証。アクセスキー値は入力しないでください。 - ロールの引き受けを使用した一時的なセキュリティ資格情報。Amazon S3 バケットへのアクセス権限なしで、IAM ユーザーのシークレットアクセスキーを入力します。 - EC2 用のロールの引き受け。アクセスキー値は入力しないでください。 - 資格情報プロファイルファイルの認証。アクセスキー値は入力しないでください。 - 統合ユーザーシングルサインオン。シークレットアクセスキー値は入力しないでください。

プロパティ	説明
秘密鍵	Amazon S3 バケットにアクセスするためのシークレットアクセスキー。秘密鍵はアクセスキーに関連付けられており、アカウントを一意に識別します。 次の認証方法に基づいてシークレットアクセスキー値を入力します。 - 基本認証。実際のアクセスシークレット値を入力します。 - IAM 認証。アクセスシークレット値は入力しないでください。 - ロールの引き受けを使用した一時的なセキュリティ資格情報。Amazon S3 バケットへのアクセス権限なしで、IAM ユーザーのアクセスシークレットを入力します。 - EC2 用のロールの引き受け。アクセスキー値は入力しないでください。 - 資格情報プロファイルファイルの認証。アクセスシークレット値は入力しないでください。 - 統合ユーザーシングルサインオン。アクセスシークレット値は入力しないでください。
IAM ロール ARN	動的に生成された一時的なセキュリティ資格情報を使用するためにユーザーに引き継がれた AWS Identity and Access Management（IAM）ロールの Amazon リソース名（ARN）。 一時的なセキュリティ資格情報を使用して AWS リソースにアクセスする場合はこのプロパティの値を入力します。 このプロパティは、アプリケーションの取り込みタスクには適用されません。 **注**: エージェントによる Amazon S3 バケットへのアクセスを有効にする IAM ロールを削除して接続を作成してもテスト接続は成功します。 IAM ロールの ARN の取得方法の詳細については、AWS のマニュアルを参照してください。
外部 ID	Amazon S3 バケットが別の AWS アカウントにある場合に、Amazon S3 バケットへのより安全なアクセスを提供します。
ロールの引き受けに EC2 ロールを使用	EC2 ロールが、[IAM ロール ARN] オプションで指定された別の IAM ロールを引き受けることができるようにします。 **注**: EC2 ロールには、同じアカウントまたは異なるアカウントから IAM ロールを引き受けるためのアクセス許可がアタッチされたポリシーが必要です。 デフォルトでは、[ロールの引き受けに EC2 ロールを使用] チェックボックスは選択されていません。 **注**: ストリーミング取り込みタスクでこのプロパティを有効にする場合は、[IAM ロール ARN] プロパティの値を入力します。
フォルダパス	Amazon S3 オブジェクトへのバケット名または完全なフォルダパス。 アプリケーション取り込みタスクとデータベース取り込みタスク以外のタスクでは、フォルダパスの末尾にスラッシュを使用しないでください。例: <バケット名>/<フォルダ名> アプリケーション取り込みタスクとデータベース取り込みタスクの場合は、末尾にスラッシュを追加します。例: <bucket name>/<my folder name>/
マスタ対称キー	クライアントサイド暗号化を使用する場合の、Base64 形式で示す 256 ビットの AES 暗号化キー。暗号化キーは、サードパーティ製ツールを使用して生成できます。 アプリケーション取り込みタスク、データベース取り込みタスク、またはストリーミング取り込みタスクには適用されません。

プロパティ	説明
顧客マスタキー ID	AWS Key Management Service（AWS KMS）によって生成された顧客マスタキー ID またはエイリアス名、またはアカウント間アクセス用のカスタムキーの Amazon リソース名（ARN）。 Amazon S3 バケットが存在するリージョンの顧客マスタキーを生成する必要があります。 次のマスタキーを指定できます。 - 顧客が生成した顧客マスタキー。クライアントサイドまたはサーバーサイドの暗号化を有効にします。 - デフォルトの顧客マスタキー。クライアントサイドまたはサーバーサイドの暗号化を有効にします。アカウントの管理者ユーザーのみがデフォルトの顧客マスタキー ID を使用してクライアントサイド暗号化を有効にできます。 アプリケーション取り込みタスク、データベース取り込みタスク、またはストリーミング取り込みタスクには適用されません。
S3 アカウントタイプ	Amazon S3 アカウントのタイプ。 次のオプションから選択します。 - Amazon S3 ストレージ。Amazon S3 サービスを使用できるようにします。 - S3 互換ストレージ。Scality RING や MinIO などのサードパーティのストレージプロバイダのエンドポイントを使用できるようにします。 デフォルトは Amazon S3 ストレージです。
REST エンドポイント	S3 互換ストレージに必要な S3 ストレージエンドポイント。 S3 ストレージエンドポイントを HTTP または HTTPS 形式で入力します。 例えば、http://s3.isv.scality.com と指定します。

プロパティ	説明
リージョン名	アクセス先のバケットの AWS リージョン。 次のいずれかのリージョンを選択します。 - アフリカ(ケープタウン) - アジアパシフィック（ムンバイ） - アシスパシフィック（ジャカルタ） - アジアパシフィック（大阪） - アジアパシフィック（ソウル） - アジアパシフィック（シンガポール） - アジアパシフィック（シドニー） - アジアパシフィック（東京） - アジアパシフィック（香港） - AWS GovCloud（米国） - AWS GovCloud（米国東部） - カナダ（中部） - 中国（北京） - 中国（寧夏） - 欧州（アイルランド） - 欧州（フランクフルト） - 欧州（ロンドン） - 欧州（ミラノ） - EU（パリ） - EU（ストックホルム） - 南米（サンパウロ） - 中東（バーレーン） - 中東（UAE） - 米国東部（バージニア北部） - 米国東部（オハイオ） - 米国 ISO 東部 - 米国 ISOB 東部（オハイオ） - 米国 ISO 西部 - 米国西部（北カリフォルニア） - 米国西部（オレゴン） デフォルトは［米国東部（バージニア北部)］です。
統合 SSO IdP	AWS アカウントで使用する、統合ユーザーシングルサインオンの SAML 2.0 対応 ID プロバイダ。 Amazon S3 V2 コネクタは、ADFS 3.0 ID プロバイダのみをサポートします。統合ユーザーシングルサインオンを使用しない場合は、**［なし］**を選択します。 **注**: 統合ユーザーシングルサインオンは、アプリケーション取り込みタスク、データベース取り込みタスク、およびストリーミング取り込みタスクには適用されません。
その他の認証タイプ	次のいずれかの認証タイプを選択します。 - なし - 認証情報プロファイルファイルの認証 アクセスキーと秘密鍵を含む認証情報ファイルから Amazon S3 認証情報にアクセスするには、［資格情報プロファイルファイルの認証］オプションを選択します。 資格情報プロファイルファイルのパスとプロファイル名を入力して、Amazon S3 との接続を確立します。 資格情報プロファイルファイルの認証を設定する際に、永続的な IAM 資格情報または一時的なセッショントークンを使用できます。 デフォルトは［なし］です。

プロパティ	説明
資格情報プロファイルのファイルパス	資格情報プロファイルファイルのパスを指定します。 資格情報プロファイルのパスを入力しない場合、Secure Agent はホームディレクトリの次のデフォルトの場所にある資格情報プロファイルファイルを使用します。 ~/.aws/credentials **注**: 一括取り込みデータベースは、**［資格情報プロファイルファイルのパス］**および**［プロファイル名］**の接続プロパティでは認証されていません。一括取り込みデータベースは、認証情報プロファイルファイルを含む DefaultAWSCredentialsProviderChain クラスによって実装されるデフォルトの認証情報プロバイダチェーンを使用して AWS 認証情報を検索します。
プロファイル名	資格情報の取得に使用される資格情報プロファイルファイル内のプロファイルの名前。 プロファイル名を入力しない場合、資格情報プロファイルファイルのデフォルトプロファイルの資格情報が使用されます。
S3 VPC エンドポイントタイプ	Amazon S3 の VPC エンドポイントタイプ。 VPC エンドポイントを選択することで、Amazon S3 とのプライベート通信を有効にできます。 次の VPC エンドポイントタイプのいずれかを選択します。 - なし - ゲートウェイエンドポイント - インタフェースエンドポイント デフォルトは［なし］です。 アプリケーション取り込みタスクまたはデータベース取り込みタスクには適用されません。
Amazon S3 のエンドポイント DNS 名	Amazon S3 インタフェースエンドポイントの DNS 名。 DNS 名は以下の形式で入力します。 bucket.<インタフェースエンドポイントの DNS 名> アプリケーション取り込みタスクまたはデータベース取り込みタスクには適用されません。
STS VPC エンドポイントタイプ	S3 VPC インタフェースエンドポイントを選択する場合に適用されます。 AWS STS の VPC エンドポイントタイプ。 **［IAM ロール** ARN］または**［フェデレーション** SSO IDp］を選択した場合は、STS VPC エンドポイントを設定します。 アプリケーション取り込みタスク、ストリーミング取り込みタスク、またはデータベース取り込みタスクには適用されません。
AWS STS サービスのエンドポイント DNS 名	AWS STS インタフェースエンドポイントの DNS 名。 アプリケーション取り込みタスクまたはデータベース取り込みタスクには適用されません。

プロパティ	説明
KMS VPC エンドポイントタイプ	インタフェースエンドポイントを選択する場合に適用されます。 AWS KMS の VPC エンドポイントタイプ。 アプリケーション取り込みタスクまたはデータベース取り込みタスクには適用されません。
AWS KMS サービスのエンドポイント DNS 名	AWS KMS インタフェースエンドポイントの DNS 名。 アプリケーション取り込みタスクまたはデータベース取り込みタスクには適用されません。

統合ユーザーシングルサインオン接続のプロパティ

［統合 SSO IdP］で［ADFS 3.0］を選択した場合は、次のプロパティを設定します。

プロパティ	説明
統合ユーザー名	ID プロバイダ経由で AWS アカウントにアクセスする統合ユーザーのユーザー名。
統合ユーザーパスワード	ID プロバイダ経由で AWS アカウントにアクセスする統合ユーザーのパスワード。
IdP SSO URL	AWS に使用する ID プロバイダのシングルサインオン URL。 ストリーミング取り込みタスクには適用されません。
SAML ID プロバイダ ARN	ID プロバイダを信頼できるプロバイダとして登録するために AWS 管理者が作成した、SAML ID プロバイダの ARN。
ロール ARN	統合ユーザーに引き継がれた IAM ロールの ARN。

認証情報プロファイルファイルの認証

アクセスキーと秘密鍵を含む認証情報プロファイルファイルを介して、Amazon S3 との接続を確立するために必要な認証情報を指定できます。一時的なセキュリティ認証情報を使用する場合、認証情報プロファイルファイルには、アクセスキー、秘密鍵、およびセッショントークンが含まれます。

認証情報プロファイルファイルによる認証を使用する場合は、セッショントークンで永続的な IAM 認証情報または一時的なセキュリティ認証情報を使用できます。

認証情報プロファイルファイルのパスを指定しない場合は、デフォルトの認証情報ファイルのパスが使用されます。プロファイル名を指定しない場合、認証情報は認証情報ファイルのデフォルトプロファイルから使用されます。

認証情報プロファイルファイルについては、次のルールを考慮してください。

- 資格情報ファイルは、Secure Agent をインストールしたマシンと同じマシン上にある必要があります。
- 資格情報プロファイルファイル名は、.credentials で終わる必要があります。
- 資格情報プロファイルのパスを指定しない場合、Secure Agent はホームディレクトリの次のデフォルトの場所にある資格情報プロファイルファイルを使用します。
  ~/.aws/credentials

  注: Windows では、環境変数%UserProfile%を使用してホームディレクトリを参照できます。Unix 系のシステムでは、環境変数$HOME を使用できます。

サンプルの認証情報プロファイルファイル:

```
[default]

aws_access_key_id = 1233333

aws_secret_access_key = abcabcabc


[test-profile]

aws_access_key_id = 1233333

aws_secret_access_key = abcabcabc

aws_session_token = jahaheieomdrtflmlioerp
```

aws_access_key_id と aws_secret_access_key により、ユーザーを認証するための認証情報の一部として使用される AWS アクセスキーと秘密鍵を指定します。

aws_session_token により、ユーザーを認証するための認証情報の一部として使用される AWS セッショントークンを指定します。セッショントークンは、一時的なセキュリティ認証情報を指定する場合にのみ必要です。

Amazon S3 とのプライベート通信

Amazon S3 とのプライベート通信は、AWS コンソールと Amazon S3 V2 接続で、ゲートウェイエンドポイントまたはインタフェースエンドポイントを設定することで有効にできます。

トラフィックをパブリックインターネットに公開せずに Amazon S3 とのプライベート通信を確立するように Amazon S3 V2 コネクタを設定できます。Amazon S3 にアクセスするには、Secure Agent が AWS Virtual Private Cloud（VPC）のサブネットの一部であることを確認します。AWS S3 VPC エンドポイントを使用すると、サブネットをインターネットゲートウェイに接続せずに、S3 要求を Amazon S3 サービスにルーティングできます。インタフェースエンドポイントまたはゲートウェイエンドポイントを作成できます。

詳細については、
「Configuring private communication with Amazon S3 using the Amazon S3 V2 Connector」を参照してください。

AMQP 接続プロパティ

AMQP 接続をセットアップする場合は、接続プロパティを設定する必要があります。

次の表に、AMQP 接続のプロパティを示します。

プロパティ	説明
接続名	接続の名前。 この名前では、大文字と小文字が区別されず、ドメイン内で一意にする必要があります。このプロパティは、接続を作成した後に変更できます。名前は 128 文字以内で指定し、空白および以下の特殊文字は使用できません。 ~ ` ! $ % ^ & * ( ) - + = { [}] | \ : ; " ' < , > . ? /
説明	オプション。接続を識別するために使用できる説明。 説明は、4,000 文字を超えることはできません。

プロパティ	説明
タイプ	AMQP 接続タイプ。 接続タイプが見つからない場合は、**［アドオンコネクタ］**ページに移動し、コネクタをインストールしてください。
ランタイム環境	タスクを実行するランタイム環境の名前。
ホスト名	AMQP ブローカーのネットワークアドレス。
ポート	基盤となる TCP 接続が確立される AMQP ブローカーのポート番号。 デフォルトは 5672 です。
仮想ホスト	AMQP システムを識別する仮想ホスト名。 セキュリティを強化するために仮想ホスト名を使用します。
ユーザー名	AMQP ブローカーのユーザー名。
パスワード	AMQP ブローカーのパスワード。
SSL の使用	安全な送信のために SSL を使用するには、このオプションを有効にします。 SSL 認証を有効にする場合は、ストリーミング取り込みタスクで AMQP 接続を使用するためのキーストアとトラストストアの詳細を必ず指定してください。
キーストアファイル名	セキュアな通信に必要なキーと証明書が含まれます。
キーストアのパスワード	キーストアファイル名のパスワード。
キーストアのタイプ	使用するキーストアのタイプ。 キーストアタイプによって、キーストア情報のストレージとデータ形式、およびキーストア内のプライベートキーを保護するために使用されるアルゴリズムを定義します。 次のいずれかのタイプを使用してください: - JKS。プライベートキーと証明書を格納します。 - PKCS12。プライベートキー、秘密鍵、および証明書を格納します。
トラストストアファイル名	トラストストアファイルの名前。
トラストストアのパスワード	トラストストアファイルのパスワード。
トラストストアのタイプ	使用するトラストストアのタイプ。 次のいずれかのタイプを使用してください: - JKS - PKCS12

プロパティ	説明
TLS プロトコル	使用するトランスポートプロトコル。 次のいずれかのタイプを使用してください: - SSL - SSLv2Hello - SSLv3 - TLS - TLSv1 - TLSv1.1 - TLSv1.2
クライアント認証	保護された AMQP ブローカーに接続する際のクライアント認証ポリシー。 SSL コンテキストを定義して有効にする場合は、次のいずれかのプロパティ値を使用します。 - WANT - REQUIRED - NONE

Cloud 統合ハブ接続プロパティ

Cloud 統合ハブ接続は、組織に Cloud 統合ハブがプロビジョニングされている場合にのみ表示できます。この接続は編集、変更、または削除しないでください。**[サブスクリプションフローに中間ステージングを使用しない]** および **[プライベートパブリケーションリポジトリに JDBC を使用する]** プロパティ以外の接続プロパティは変更しないでください。

次の表に、Cloud 統合ハブ接続の接続プロパティを示します。

接続プロパティ	説明	編集可能
接続名	接続の名前。大文字と小文字は区別されず、ドメイン内で一意である必要があります。 名前は 128 文字以内で指定し、空白および以下の特殊文字は使用できません。 ~ ` ! $ % ^ & * ( ) - + = { [}] | \ : ; " ' < , > . ? /	編集しないでください。
説明	オプション。接続の説明。説明は、4,000 文字を超えることはできません。	○
タイプ	Cloud **統合ハブ**接続タイプ。	編集しないでください。

接続プロパティ	説明	編集可能
シークレット Vault を有効にする	接続用のパブリケーションリポジトリパスワードを、組織に設定されたランタイム環境のシークレットマネージャに保存します。 このプロパティは、組織にシークレットマネージャが設定されている場合にのみ表示されます。 シークレットマネージャの資格情報を使用するには、このオプションを選択します。このオプションを有効にしない場合、資格情報は組織の設定に応じてリポジトリまたはローカル Secure Agent に保存されます。 シークレットマネージャの設定および使用方法については、Administrator ヘルプの「シークレットマネージャの設定」を参照してください。	編集しないでください。
ランタイム環境	タスクを実行するランタイム環境の名前。	編集しないでください。
サブスクリプションフローに中間ステージングを使用しない	中間ステージングへの書き込みを無効にします。中間ステージングに書き込みたくない場合は、このプロパティを有効にします。データ統合タスクは Cloud 統合ハブからデータを読み取り、ターゲットの場所にデータを直接書き込みます。中間ステージングへの書き込みを無効にすると、システムパフォーマンスに影響を与える可能性があります。	○
プライベートパブリケーションリポジトリに JDBC を使用する	プライベートパブリケーションリポジトリのゼロダウンタイムを設定する場合。このプロパティを有効にすると、プライベートパブリケーションリポジトリ上のデータに中断なくアクセスできるようになります。データ統合タスクをトリガするパブリケーションおよびサブスクリプションのゼロダウンタイムを有効にできます。 ホストされたパブリケーションリポジトリでは、Cloud 統合ハブはすべてのパブリケーションおよびサブスクリプションタイプに対してデフォルトでゼロダウンタイムを適用します。	○

Databricks Delta 接続のプロパティ

Databricks Delta との間でデータの安全な読み取りまたは書き込みを行うための Databricks Delta 接続を作成します。

ステージングの前提条件

接続を作成する前に、SQL ウェアハウスまたは Databricks クラスタに接続するステージング環境を設定するために、特定の前提条件タスクを実行する必要があります。

SQL ウェアハウス

デプロイされた環境に基づいて、SQL ウェアハウス用の AWS または Azure ステージング環境を設定します。また、Azure および AWS ステージングを使用するには、SQL ウェアハウスの Spark パラメータを設定する必要があります。

AWS ステージングの設定

SQL ウェアハウスに AWS ステージングを使用するように IAM AssumeRole 認証を設定します。

AWS ステージング用の Spark パラメータの設定

Databricks SQL 管理コンソールで、**［SQL ウェアハウスの設定］ > ［データセキュリティ］**に移動し、**［データアクセス設定］**で AWS の Spark パラメータを設定します。

次の Spark 構成パラメータを追加し、SQL ウェアハウスを再起動します。

- `spark.hadoop.fs.s3a.access.key <S3 アクセスキーの値>`
- `spark.hadoop.fs.s3a.secret.key <S3 シークレットキーの値>`
- `smile.hadoop.fs.s3a.endpoint <S3 ステージングバケットエンドポイントの値>`

例えば、S3 ステージングバケットウェアハウスの値は *s3.ap-south-1.amazonaws.com* のようになります。

設定したアクセスキーとシークレットキーで、Databricks Delta テーブルのデータを保存する S3 バケットにアクセスできることを確認します。

Azure ステージングの設定

Microsoft Azure Data Lake Storage Gen2 を使用してファイルをステージングする前に、次のタスクを実行します。

- Microsoft Azure Data Lake Storage Gen2 で使用するストレージアカウントを作成し、Azure ポータルで**［階層名前空間］**を有効にします。
  ロールベースのアクセス制御を使用して、ユーザーがストレージアカウントのリソースにアクセスすることを許可できます。ユーザーに Contributor ロールまたは Reader ロールを割り当てます。Contributor ロールにはストレージアカウント内のすべてのリソースを管理できる完全なアクセス権限が付与されますが、ロールの割り当ては許可されません。［Reader］ロールにはストレージアカウント内のすべてのリソースの閲覧権限が付与されますが、リソースの変更は許可されません。

  注: ロールの割り当てを追加または削除するには、［Owner］ロールなどの書き込みおよび削除権限が必要です。
- Azure Active Directory にアプリケーションを登録して、Microsoft Azure Data LakeStorage Gen2 アカウントにアクセスするユーザーを認証します。
  ロールベースのアクセス制御を使用してアプリケーションを許可できます。アプリケーションに Storage Blob Data Contributor ロールまたは Storage Blob Data Reader ロールを割り当てます。Storage Blob Data Contributor ロールを割り当てた場合は、ストレージアカウント内の Azure Storage コンテナと Blob の読み取り、書き込み、および削除を行うことができます。Storage Blob Data Reader ロールを割り当てた場合は、ストレージアカウント内の Azure Storage コンテナと Blob の読み取りおよび一覧表示のみを行うことができます。
- Microsoft Azure Data Lake Storage Gen2 でのサービス間認証用に Azure Active Directory Web アプリケーションを作成します。

  注: コネクタを使用してアプリケーションで作成されたフォルダまたはファイルにアクセスするためのスーパーユーザー特権があることを確認します。
- 複合ファイルの読み取りを行うには、タイプ DTM の JVM オプションを設定して、Secure Agent のシステム構成の詳細で-Xms および-Xmx 値を増やし、Java ヒープ領域不足のエラーを回避します。推奨される-Xms 値は 512MB、-Xmx 値は 1024MB です。

Azure ステージング用の Spark パラメータの設定

Databricks SQL 管理コンソールで、**［SQL ウェアハウスの設定］ > ［データセキュリティ］**に移動し、**［データアクセス設定］**で Azure の Spark パラメータを設定します。

次の Spark 構成パラメータを追加し、SQL ウェアハウスを再起動します。

- spark.hadoop.fs.azure.account.oauth2.client.id.<storage-account-name>.dfs.core.windows.net <value>
- spark.hadoop.fs.azure.account.auth.type.<storage-account-name>.dfs.core.windows.net OAuth
- spark.hadoop.fs.azure.account.oauth2.client.secret.<storage-account-name>.dfs.core.windows.net <Value>
- spark.hadoop.fs.azure.account.oauth.provider.type.<storage-account-name>.dfs.core.windows.net org.apache.hadoop.fs.azurebfs.oauth2.ClientCredsTokenProvider
- spark.hadoop.fs.azure.account.oauth2.client.endpoint.<storage-account-name>.dfs.core.windows.net https://login.microsoftonline.com/<テナント ID>/oauth2/token

設定したクライアント ID とクライアントシークレットで、Databricks Delta テーブルのデータを保存するファイルシステムにアクセスできることを確認します。

Databricks クラスタ

クラスタがデプロイされている場所に基づいて Azure および AWS ステージングを使用するように、Databricks クラスタの Spark パラメータを設定します。

また、Databricks クラスタでの実行時および設計時の処理に対して Secure Agent プロパティを有効にする必要があります。

Spark 設定

Databricks クラスタに接続する前に、AWS と Azure で Spark パラメータを設定する必要があります。

AWS での設定

Databricks クラスタに次の Spark 構成パラメータを追加し、クラスタを再起動します。

- spark.hadoop.fs.s3a.access.key <値>
- spark.hadoop.fs.s3a.secret.key <value>
- spark.hadoop.fs.s3a.endpoint <value>

構成したアクセスキーとシークレットキーで、Databricks Delta テーブルのデータを保存するバケットにアクセスできることを確認します。

Azure での設定

Databricks クラスタに次の Spark 構成パラメータを追加し、クラスタを再起動します。

- fs.azure.account.oauth2.client.id.<storage-account-name>.dfs.core.windows.net <value>
- fs.azure.account.auth.type.<storage-account-name>.dfs.core.windows.net <value>
- fs.azure.account.oauth2.client.secret.<storage-account-name>.dfs.core.windows.net <Value>
- fs.azure.account.oauth.provider.type.<storage-account-name>.dfs.core.windows.net org.apache.hadoop.fs.azurebfs.oauth2.ClientCredsTokenProvider
- fs.azure.account.oauth2.client.endpoint.<storage-account-name>.dfs.core.windows.net https://login.microsoftonline.com/<テナント ID>/oauth2/token

設定したクライアント ID とクライアントシークレットで、Databricks Delta テーブルのデータを保存するファイルシステムにアクセスできることを確認します。

Databricks Delta への接続

Databricks Delta に接続するように Databricks Delta 接続プロパティを設定してみましょう。

始める前に

開始する前に、Databricks Delta アカウントから情報を取得する必要があります。

次のビデオは、必要な情報を取得する方法を示しています。

また、接続で SQL エンドポイントまたは Databricks クラスタを使用するように AWS または Azure ステージング環境を設定する必要があります。

Azure または AWS 環境のステージングの前提条件については、「「 SQL ウェアハウス」 (ページ 58)」または「「Databricks クラスタ」 (ページ 60)」を確認してください。

接続の詳細

次の表に、基本接続プロパティを示します。

プロパティ	説明
接続名	接続の名前。 各接続名は組織内で一意である必要があります。接続名には、英数字、スペース、および次の特殊文字を含めることができます。_ .+ -, 最大長は 255 文字です。
説明	接続の説明。最大長は 4000 文字です。
タイプ	Databricks Delta
ランタイム環境	タスクを実行するランタイム環境の名前。 ホステッドエージェントまたはサーバーレスランタイム環境で、アプリケーション取り込みタスク、データベース取り込みタスク、またはストリーミング取り込みタスクを実行することはできません。
SQL ウェアハウス JDBC URL	Databricks SQL ウェアハウスの JDBC 接続 URL。 Databricks SQL ウェアハウスに接続するために必要です。Databricks クラスタには適用されません。 SQL ウェアハウス JDBC URL を取得するには、Databricks コンソールに移動し、［JDBC URL］メニューから JDBC ドライババージョンを選択します。 アプリケーション取り込みタスクとデータベース取り込みタスクでは、JDBC URL バージョン 2.6.25 **以降**または 2.6.22 **以前**を使用できます。URL は次のように、プレフィックス jdbc:databricks://で始まる必要があります。 `jdbc:databricks://<Databricks ホスト>:443/default;transportMode=http;ssl=1;AuthMech=3;httpPath=/sql/1.0/endpoints/<SQL エンドポイントのクラスタ ID>;` Secure Agent で必要な環境変数を設定してください。また、詳細接続設定で正しい**［JDBC ドライバクラス名］**を指定します。 **注**: データベース名は［データベース名］接続プロパティで指定します。JDBC URL でデータベース名を指定した場合、そのデータベース名は考慮されません。［SQL ウェアハウス JDBC URL］プロパティを設定した場合、［Databricks ホスト］、［組織 ID］、および［クラスタ ID］のプロパティは考慮されません。

プロパティ	説明
Databricks トークン	Databricks にアクセスするためのパーソナルアクセストークン。 SQL ウェアハウスと Databricks クラスタの場合は必須です。
カタログ名	Unity Catalog を使用する場合は、メタストア内の既存のカタログの名前。 SQL ウェアハウスの場合はオプションです。Databricks クラスタには適用されません。 SQL ウェアハウス JDBC URL の末尾にカタログ名を指定することもできます。 **注**: カタログ名に特殊文字を含めることはできません。 Unity Catalog の詳細については、Databricks Delta のドキュメントを参照してください。

詳細設定

次の表に、詳細接続のプロパティを示します。

プロパティ	説明
データベース	Databricks Delta で接続するデータベース名。 SQL ウェアハウスと Databricks クラスタの場合はオプションです。 データ統合では、データベース名を指定しない場合、ワークスペース内の使用可能なすべてのデータベースが一覧表示されます。ここで指定した値は、[SQL **ウェアハウス** JDBC URL] 接続プロパティで指定したデータベース名よりも優先されます。
JDBC ドライバクラス名	JDBC ドライバクラスの名前。 SQL ウェアハウスと Databricks クラスタの場合はオプションです。 JDBC URL バージョン 2.6.22 以前の場合は、ドライバクラス名を `com.simba.spark.jdbc.Driver` として指定します。 JDBC URL バージョン 2.6.25 以降の場合は、ドライバクラス名を `com.databricks.client.jdbc.Driver` として指定します。
ステージング環境	Databricks クラスタがデプロイされるクラウドプロバイダ。 SQL ウェアハウスと Databricks クラスタの場合は必須です。 次のいずれかのオプションを選択します。 - AWS - Azure - 個人用ステージングの場所 デフォルトは個人用ステージングの場所です。 Azure または AWS ステージング環境の代わりに個人用ステージングの場所をステージング環境として選択し、マッピングやタスク用にデータをローカルにステージングすることができます。 一括取り込みで使用する接続に［個人用ステージングの場所］を選択した場合、アプリケーション取り込みジョブまたはデータベース取り込みジョブの Parquet データファイルをローカルの個人用ストレージの場所にステージングできます。データ保持期間は 7 日間です。また、［データベースホスト］の値も指定する必要があります。Unity Catalog を使用する場合は、個人用ストレージの場所が自動的にプロビジョニングされます。 個人用ステージングの場所は、Databricks クラスタには適用されません。 Databricks Delta アンマネージドテーブルで個人用ステージングの場所を使用することはできません。 **注**: 接続を確立した後にクラスタを切り替えることはできません。

プロパティ	説明
Databricks ホスト	Databricks アカウントが属するエンドポイントのホスト名。 Databricks クラスタの場合は必須です。SQL ウェアハウスには適用されません。 Databricks ホストは、JDBC URL から取得できます。この URL は、Databricks Delta 汎用クラスタの JDBC または ODBC の［詳細オプション］で確認できます。 次の例に、JDBC URL の Databicks ホストを示します。 jdbc:spark://<Databricks Host>:443/default;transportMode=http;ssl=1;httpPath=sql/protocolv1/o/<Org Id>/<Cluster ID>;AuthMech=3;UID=token;PWD=<personal-access-token> Databricks ホスト、組織 Id、およびクラスタ ID の PWD の値は常に<personal-access-token>です。
クラスタ ID	クラスタの ID。 Databricks クラスタの場合は必須です。SQL ウェアハウスには適用されません。 クラスタ ID は、JDBC URL から取得できます。この URL は、Databricks Delta 汎用クラスタの JDBC または ODBC の［詳細オプション］で確認できます 次の例に、JDBC URL のクラスタ ID を示します。 jdbc:spark://<Databricks Host>:443/default;transportMode=http;ssl=1;httpPath=sql/protocolv1/o/<Org Id>/<Cluster ID>;AuthMech=3;UID=token;PWD=<personal-access-token>
組織 ID	Databricks のワークスペースの一意の組織 ID。 Databricks クラスタの場合は必須です。SQL ウェアハウスには適用されません。 組織 ID は、JDBC URL から取得できます。この URL は、Databricks Delta 汎用クラスタの JDBC または ODBC の［詳細オプション］で確認できます 次の例に、JDBC URL の組織 ID を示します。 jdbc:spark://<Databricks Host>:443/ default;transportMode=http; ssl=1;httpPath=sql/protocolv1/o/<Organization ID>/ <Cluster ID>;AuthMech=3;UID=token; PWD=<personal-access-token>
最小ワーカー数	Spark ジョブに使用される最小のワーカーノードの数。最小値は 1 です。 Databricks クラスタの場合は必須です。SQL ウェアハウスには適用されません。
最大ワーカー数	Spark ジョブに使用される最大のワーカーノードの数。自動スケーリングを行わない場合は、最大ワーカー数を最小ワーカー数と同じ値に設定するか、最大ワーカー数を設定しないでください。 Databricks クラスタの場合はオプションです。SQL ウェアハウスには適用されません。
DB ランタイムバージョン	Databricks クラスタに接続してマッピングを処理するときに生成する Databricks クラスタのバージョン。 Databricks クラスタの場合は必須です。SQL ウェアハウスには適用されません。 Databricks ランタイムバージョン 9.1 LTS または 13.3 LTS を選択します。
ワーカーノードタイプ	Spark ジョブの実行に使用されるワーカーノードインスタンスタイプ。 Databricks クラスタの場合は必須です。SQL ウェアハウスには適用されません。 例えば、AWS のワーカーノードタイプは i3.2xlarge にすることができます。Azure のワーカーノードタイプは Standard_DS3_v2 にすることができます。

プロパティ	説明
ドライバノードタイプ	Spark ワーカーからデータを収集するために使用されるドライバノードインスタンスタイプ。 Databricks クラスタの場合はオプションです。SQL ウェアハウスには適用されません。 例えば、AWS のドライバノードタイプは i3.2xlarge にすることができます。Azure のドライバノードタイプは Standard_DS3_v2 にすることができます。 ドライバノードタイプを指定しない場合、Databricks はワーカーノードタイプのフィールドで指定した値を使用します。
インスタンスプール ID	Spark クラスタに使用されるインスタンスプール ID。 Databricks クラスタの場合はオプションです。SQL ウェアハウスには適用されません。 マッピングを実行するためにインスタンスプール ID を指定すると、次の接続プロパティは無視されます。 - ドライバノードタイプ - EBS ボリューム数 - EBS ボリュームタイプ - EBS ボリュームサイズ - Elastic Disk を有効にする - ワーカーノードタイプ - ゾーン ID
エラスティックディスク	クラスタによる追加のディスク容量の取得を有効にします。 Databricks クラスタの場合はオプションです。SQL ウェアハウスには適用されません。 Spark ワーカーのディスク容量が不足している場合は、このオプションを有効にします。
Spark 設定	データローダータスクや一括取り込みタスクには適用されません。
Spark 環境変数	データローダータスクや一括取り込みタスクには適用されません。

AWS ステージング環境

次の表に、AWS ステージング環境のプロパティを示します。

プロパティ	説明
S3 アクセスキー	Amazon S3 バケットにアクセスするためのキー。
S3 シークレットキー	Amazon S3 バケットにアクセスするためのシークレットキー。
S3 データバケット	Databricks Delta データを格納するための既存のバケット。
S3 ステージングバケット	ステージングファイルを保存するための既存のバケット。

プロパティ	説明
S3 認証モード	Amazon S3 にアクセスするための認証モード。 次のいずれかの認証モードを選択します。 - 永続的な IAM 資格情報。S3 アクセスキーと S3 シークレットキーを使用して Databricks Delta に接続します。 - IAM Assume RoleIAM 認証に AssumeRole を使用して Databricks Delta に接続します。Databricks クラスタには適用されません。
IAM ロール ARN	動的に生成された一時的なセキュリティ資格情報を使用するためにユーザーに引き継がれた IAM ロールの Amazon Resource Number（ARN）。 一時的なセキュリティ資格情報を使用して Amazon S3 ステージングバケットにアクセスする場合はこのプロパティの値を設定します。 IAM ロールの ARN の取得方法の詳細については、*AWS のマニュアル*を参照してください。
ロールの引き受けに EC2 ロールを使用	オプション。EC2 ロールが IAM ロール ARN オプションで指定された別の IAM ロールを引き受けることができるようにするには、このチェックボックスをオンにします。 EC2 ロールには、同じ AWS アカウントまたは異なる AWS アカウントから IAM ロールを引き受けるためのアクセス許可がアタッチされたポリシーが必要です。
S3 リージョン名	アクセスするバケットが存在する AWS クラスタリージョンです。 ［JDBC URL］接続プロパティで指定したカスタム JDBC URL にクラスタリージョン名が含まれていない場合にクラスタリージョンを選択します。
S3 サービスリージョナルエンドポイント	S3 データバケットと S3 ステージングバケットに、リージョン固有の S3 リージョナルエンドポイントを介してアクセスする必要がある場合の S3 リージョナルエンドポイント。 Databricks クラスタには適用されません。 デフォルトは `s3.amazonaws.com` です。
ゾーン ID	Databricks ジョブクラスタのゾーン ID。 Databricks クラスタの場合はオプションです。SQL ウェアハウスには適用されません。 実行時に、特定のゾーンで Databricks ジョブクラスタを作成する場合にのみ適用されます。 例: us-west-2a。 **注**: ゾーンは、Databricks アカウントが存在する場所と同じリージョンにある必要があります。
EBS ボリュームタイプ	クラスタで起動される EBS ボリュームのタイプ。 Databricks クラスタの場合はオプションです。SQL ウェアハウスには適用されません。
EBS ボリューム数	インスタンスごとに起動される EBS ボリュームの数。最大 10 までのボリュームを選択できます。 Databricks クラスタの場合はオプションです。SQL ウェアハウスには適用されません。 **注**: Databricks Delta 接続では、インスタンスストアなしでノードタイプに少なくとも 1 つの EBS ボリュームを指定してください。そうしないと、クラスタの作成は失敗します。
EBS ボリュームサイズ	インスタンスに対して起動される単一の EBS ボリュームのサイズ（GiB 単位）。 Databricks クラスタの場合はオプションです。SQL ウェアハウスには適用されません。

Azure ステージング環境

次の表に、Azure ステージング環境のプロパティを示します。

プロパティ	説明
ADLS ストレージアカウント名	Microsoft Azure Data Lake Storage アカウントの名前。
ADLS クライアント ID	Active Directory で OAuth 認証を完了するためのアプリケーションの ID。
ADLS クライアントシークレット	Active Directory で OAuth 認証を完了するためのクライアントシークレットキー。
ADLS テナント ID	データの書き込みに使用する Microsoft Azure Data Lake Storage ディレクトリの ID。
ADLS エンドポイント	クライアント ID とクライアントシークレットに基づく認証が完了する OAuth 2.0 トークンエンドポイント。
ADLS ファイルシステム名	Databricks Delta データを格納するための既存のファイルシステムの名前。
ADLS ステージングファイルシステム名	ステージングデータを格納するための既存のファイルシステムの名前。

JDBC URL パラメータ

Databricks Delta 接続の追加の JDBC URL パラメータフィールドを利用して、Databricks Delta への接続に必要な追加パラメータをカスタマイズおよび設定できます。
Databricks Delta 接続では、次のプロパティを追加の JDBC URL パラメータとして設定できます。

- Unity カタログ情報を Databricks Delta に渡すには、SQL ウェアハウスクラスタ ID の後に次の形式でカタログ名を指定します。
  `jdbc:spark://<Databricks ホスト>:443/default;transportMode=http;ssl=1;AuthMech=3;httpPath=/sql/1.0/endpoints/<SQL エンドポイントのクラスタ ID>;`**`ConnCatalog=<catalog_name>;`**
- プロキシサーバーを使用して Databricks Delta に接続するには、次のパラメータを入力します。
  `jdbc: spark://<Databricks ホスト>:443/default;transportMode=http;ssl=1;AuthMech=3;httpPath=/sql/1.0/warehouses/219fe3013963cdce;`**`UseProxy=<Proxy=true>;ProxyHost=<プロキシホストの IP アドレス>;ProxyPort=<プロキシサーバーのポート番号>;ProxyAuth=<Auth_true>;`**

  注: 一括取り込みでは、プロキシサーバーを使用した Databricks Delta への接続はサポートされていません。
- SSL 対応の Databricks Delta に接続するには、JDBC URL に次の形式で値を指定します。
  `jdbc:spark://<Databricks Host>:443/default;transportMode=http;`**`ssl=1`**`;AuthMech=3;httpPath=/sql/1.0/endpoints/<SQL endpoint cluster ID>;`

個人用ステージングの場所についてのルールおよびガイドライン

ステージング環境として個人用ステージングの場所を選択すると、データは最初に Java の一時的な場所にステージングされ、次に Unity カタログの個人用ステージングの場所にコピーされます。タスクが正常に実行された後に、ステージングされたファイルはどちらも削除されます。
ただし、データを別のディレクトリにステージングするには、Administrator サービスのシステム構成設定の JVM オプションで DTM プロパティ `-Djava.io.tmpdir=/my/dir/path` を設定します。

別のディレクトリでのデータステージングを有効にするには、読み取りおよび書き込み権限と、ディレクトリにデータをステージングするための十分なディスク領域が必要です。。

ステージング用の Databricks Delta 接続プロパティで個人用ステージングの場所を指定する場合は、次のルールとガイドラインを考慮してください。

- SQL ウェアハウス JDBC URL では、Unity 対応カタログのみを指定できます。
- 設定されたすべてのマッピングは、SQL ELT の最適化なしで実行されます。
- データはフォルダ stage://tmp/<user_name>にステージングされます。ここで、<user_name>は接続で提供される Databricks トークンから選択され、AWS および Azure のルートの場所にある個人用ステージング場所への読み取りおよび書き込みアクセス権が必要です。

Db2 for i Database Ingestion 接続のプロパティ

Db2 for i Database Ingestion 接続の定義時に、接続プロパティを設定する必要があります。この接続タイプは、一括取り込みサービスで設定したデータベース取り込みタスクで使用できます。

以下の表に、接続のプロパティを示します。

プロパティ	説明
接続名	接続の名前。この名前は、組織内で一意にする必要があります。接続名には、英数字、スペース、および次の特殊文字を含めることができます。_ .+ - 名前の先頭または末尾のスペースはトリミングされ、名前の一部として保存されません。最大長は 100 文字です。接続名では大文字と小文字は区別されません。
説明	接続の説明（オプション）。最大長は 255 文字です。
タイプ	接続のタイプ。タイプが Db2 for i Database Ingestion であることを確認してください。
ランタイム環境	データベース統合タスクを実行するランタイム環境の名前。ランタイム環境は、管理者で定義します。
ユーザー名	Db2 for i インスタンスへの接続に使用するユーザー名。
パスワード	Db2 for i インスタンスへの接続に使用するパスワード。
ホスト	データベースサーバをホストするマシンの名前。
ポート	データベースサーバーへの接続時に使用するネットワークポート番号。
場所名	アクセスする Db2 for i ロケーションの名前。システム管理者は、WRKRDBDIRE コマンドを使用して、Db2 ロケーションの名前を判別できます。出力で*LOCAL としてリストされているデータベースの名前を見つけ、その値をこのプロパティの値として使用します。
JDBC ドライバ	JDBC ドライバのタイプ。 次のいずれかのオプションを選択します。 - Data Direct - JTOpen デフォルトは Data Direct です。
ビットデータのコードページ	一括取り込みデータベースがビットデータとして保存された文字データを読み取るために使用するコードページ。この値は、java.io API および java.lang API の正規名である必要があります。詳細については、Oracle Java のマニュアルで、サポートされているエンコーディングを参照してください。FOR BIT DATA ソースカラムがある場合は、このプロパティを指定します。

プロパティ	説明
詳細接続プロパティ	Db2 for i ソースへの接続に使用される JDBC ドライバの詳細プロパティ。*property=value* エントリを複数指定する場合は、セミコロン（;）で区切ります。 DataDirect JDBC ドライバ接続プロパティについては、Progress DataDirect documentation を参照してください。例えば、ConnectionRetryCount プロパティを設定して、ドライバがプライマリデータベースサーバーへの接続を再試行する回数を制御できます。 JTOpen JDBC ドライバ接続プロパティについては、IBM Toolbox for Java JDBC properties を参照してください。
暗号化方法	JTOpen JDBC ドライバのデータ暗号化方式。 次のいずれかのオプションを選択します。 - 暗号化なし - SSL デフォルトは［暗号化なし］です。 SSL を選択する場合は、次のいずれかの場所にある Informatica Cloud Secure Agent JRE cacerts キーストアに必要な証明書を追加する必要があります。 Linux の場合: *Secure Agent Directory*\jdk\jre\lib\security\cacerts Windows の場合: *Secure Agent Directory*\apps\jdk*LatestVersion*\jre

Db2 for LUW Database Ingestion 接続のプロパティ

Db2 for LUW Database Ingestion 接続を定義する場合は、接続プロパティを設定する必要があります。この接続タイプは、一括取り込みサービスで設定したデータベース取り込みタスクで使用できます。

以下の表に、接続のプロパティを示します。

プロパティ	説明
接続名	接続の名前。この名前は、組織内で一意にする必要があります。接続名には、英数字、スペース、および次の特殊文字を含めることができます。_ .+ - 名前の先頭または末尾のスペースはトリミングされ、名前の一部として保存されません。最大長は 100 文字です。接続名では大文字と小文字は区別されません。
説明	接続の説明（オプション）。最大長は 255 文字です。
タイプ	接続のタイプ。タイプが Db2 for LUW Database Ingestion であることを確認してください。
ランタイム環境	データベース統合タスクを実行するランタイム環境の名前。ランタイム環境は、管理者で定義します。
ユーザー名	Db2 for LUW インスタンスへの接続に使用するユーザー名。
パスワード	Db2 for LUW インスタンスへの接続に使用するパスワード。

プロパティ	説明
ホスト	データベースサーバをホストするマシンの名前。
ポート	データベースサーバーへの接続時に使用するネットワークポート番号。
データベース名	アクセスする Db2 for LUW ロケーションの名前。
詳細接続プロパティ	Db2 for LUW ソースへの接続に使用される Progress DataDirect JDBC DB2 ドライバの詳細プロパティ。*property=value* エントリを複数指定する場合は、セミコロン（;）で区切ります。 このフィールドに入力できるドライバのプロパティについては、connection properties にある Progress DataDirect のドキュメントで説明されています。例えば、EncryptionMethod プロパティを設定して、ドライバとデータベースサーバー間のネットワークを介してデータを送信するときにデータを暗号化および復号するかどうかを制御できます。

Db2 for zOS Database Ingestion 接続のプロパティ

Db2 for zOS Database Ingestion 接続を定義する場合は、接続プロパティを設定する必要があります。この接続タイプは、一括取り込みサービスで設定したデータベース取り込みタスクで使用できます。

以下の表に、接続のプロパティを示します。

プロパティ	説明
接続名	接続の名前。この名前は、組織内で一意にする必要があります。接続名には、英数字、スペース、および次の特殊文字を含めることができます。_ .+ - 名前の先頭または末尾のスペースはトリミングされ、名前の一部として保存されません。最大長は 100 文字です。接続名では大文字と小文字は区別されません。
説明	接続の説明（オプション）。最大長は 255 文字です。
タイプ	接続のタイプ。タイプが Db2 for zOS Database Ingestion であることを確認してください。
ランタイム環境	データベース統合タスクを実行するランタイム環境の名前。ランタイム環境は、管理者で定義します。
ユーザー名	Db2 for zOS インスタンスへの接続に使用するユーザー名。
パスワード	Db2 for zOS インスタンスへの接続に使用するパスワード。
ホスト	データベースサーバをホストするマシンの名前。
ポート	データベースサーバーへの接続時に使用するネットワークポート番号。
場所名	アクセスする Db2 for zOS ロケーションの名前。Db2 for z/OS の場合、システム管理者は、コマンド DISPLAYDDF を使用して Db2 ロケーションの名前を判別できます。

プロパティ	説明
ビットデータのコードページ	一括取り込みデータベースがビットデータとして保存された文字データを読み取るために使用するコードページ。この値は、java.io API および java.lang API の正規名である必要があります。詳細については、Oracle Java のマニュアルで、サポートされているエンコーディングを参照してください。FOR BIT DATA ソースカラムがある場合は、このプロパティを指定します。
CDC ストアドプロシージャスキーマ	増分変更データキャプチャ処理の場合に、Db2 ログから変更データを収集するために必要な z/OS ストアドプロシージャスキーマの名前。この値は、z/OS でストアドプロシージャをセットアップするときにカスタマイズした#STPINST データセットで指定されています。デフォルト値は指定されていません。
CDC ストアドプロシージャ名	増分変更データキャプチャ処理の場合に、Db2 ログから変更データを収集するために必要な z/OS ストアドプロシージャの名前。この値は、z/OS でストアドプロシージャをセットアップするときにカスタマイズした#STPINST データセットで指定されています。デフォルト値は INFALOG です。
詳細接続プロパティ	Db2 for z/OS ソースへの接続に使用される Progress DataDirect JDBC DB2 ドライバの詳細プロパティ。*property=value* エントリを複数指定する場合は、セミコロン（;）で区切ります。 このフィールドに入力できるドライバのプロパティについては、https://docs.progress.com/bundle/datadirect-connect-jdbc-51/page/Connection-Properties_10.html にある Progress DataDirect のドキュメントで説明されています。例えば、ConnectionRetryCount プロパティを設定して、ドライバがプライマリデータベースサーバーへの接続を再試行する回数を制御できます。

フラットファイル接続のプロパティ

フラットファイルソース接続に割り当てる必要があるプロパティを定義します。

次の表に、フラットファイル接続のプロパティを示します。

接続プロパティ	説明
接続名	接続の名前。この名前は、組織内で一意にする必要があります。接続名には、英数字、スペース、および次の特殊文字を含めることができます。_ .+ - 名前の先頭または末尾のスペースはトリミングされ、名前の一部として保存されません。最大長は 100 文字です。接続名では大文字と小文字は区別されません。
説明	接続の説明（オプション）。最大長は 255 文字です。
タイプ	接続のタイプ。**[フラットファイル]** 接続タイプを選択します。
ランタイム環境	フラットファイルへのアクセスに使用する Secure Agent が含まれるランタイム環境。 **注:** NTT 上で実行される Secure Agent を含むランタイム環境を選択しないでください。フラットファイル接続では、NTT 上で実行される Secure Agent を使用できません。

接続プロパティ	説明
ディレクトリ	フラットファイルの保存先ディレクトリ。選択されたランタイム環境内のすべての Secure Agent によってアクセス可能である必要があります。 完全ディレクトリを入力するか、**[参照]** をクリックして目的のディレクトリを特定し選択します。 接続を使用する場合、ディレクトリまたはそのサブディレクトリのいずれかに含まれているファイルを選択します。 最大長は 100 文字です。ディレクトリ名には、英数字、スペース、および次の特殊文字を含めることができます。 / \ : _ ~ ディレクトリは、この接続タイプのサービス URL です。 **注**: Windows では、**[ディレクトリの参照]** ダイアログボックスにマッピング済みドライブは表示されません。Windows エクスプローラで［マイネットワーク］を参照してディレクトリを検索し、アドレスバーからその場所をコピーするか、ディレクトリ名を\\<server_name>\<directory_path>の形式で入力できます。ネットワークディレクトリが表示されない場合は、Secure Agent サービスのログインを設定します。この機能は、新しいバージョンの Windows では使用できない場合があります。 フラットファイルの名前を含めないでください。ファイル名はタスクを作成するときに指定します。
［参照］ボタン	フラットファイルの保存先ディレクトリを特定および選択するために使用します。
日付形式	フラットファイルの日付フィールドの日付形式。デフォルトの日付形式は次のとおりです。 MM/dd/yyyy HH:mm:ss

接続プロパティ	説明
コードページ	フラットファイルをホストしているシステムのコードページ。次のいずれかのコードページを選択します。 - MS Windows Latin 1。ISO 8859-1 Western European データの場合に選択します - UTF-8。Unicode データの場合に選択します - Unicode の UTF-32 エンコード（ビッグエンディアン） - Unicode の UTF-32 エンコード（ロウワーエンディアン） - Shift-JIS。ダブルバイト文字データの場合に選択します。 - ISO 8859-15 Latin 9（Western European） - ISO 8859-2 Eastern European - ISO 8859-3 Southeast European - ISO 8859-5 Cyrillic - ISO 8859-9 Latin 5（Turkish） - IBM EBCDIC International Latin-1 - Japanese EUC (with \ <-> Yen mapping - IBM EBCDIC Japanese - IBM EBCDIC Japanese CP939 - PC Japanese SJIS-78 syntax (IBM-942) - PC Japanese SJIS-90 (IBM-943) - MS Windows Traditional Chinese, superset of Big 5 - Taiwan Big-5 (w/o euro update) - Chinese EUC - ISO 8859-8 Hebrew - PC Hebrew (old) - PC Hebrew (w/o euro update) - EBCDIC Hebrew (updated with new sheqel, control characters) - IBM EBCDIC US English IBM037 - Unicode の UTF-32 エンコード（ロウワーエンディアン） - ISO 8859-1 Western European - IBM EBCDIC French - ISO 8859-10 Latin 6（Nordic）* - EBCDIC Finland, Sweden - MOS-DOS Thai, superset of TIS 620 - 7-bit ASCII - EBCDIC Finland, Sweden (w/ euro update) - MS-DOS Windows Latin 2 (Central Europe) - Japanese EBCDIC-Kana Fujitsu 詳細マッピングでは、クラウドストレージ接続のフラットファイルオブジェクトは UTF-8 エンコードを使用する必要があります。 ファイルに UTF-16 エンコードの補助文字が含まれている場合、タスクは失敗します。 **注**: Shift-JIS コードページと UTF データオブジェクトでフラットファイル接続を使用する場合は、必ず Unicode を完全にサポートするフォントをインストールしてください。
* データプレビューでは、類似した ISO 8859-4 Scandinavian/Baltic コードページが使用されますが、ランタイム処理では ISO 8859-10 Latin 6 (Nordic)が使用されるため、データプレビューとランタイムエンコーディングは一致しません。	

Google Analytics Mass Ingestion 接続のプロパティ

Google Analytics Mass Ingestion 接続をセットアップする際には、接続プロパティを設定する必要があります。

次の表に、Google Analytics Mass Ingestion 接続の接続プロパティを示します。

接続プロパティ	説明
接続名	接続の名前。この名前は、組織内で一意にする必要があります。接続名には、英数字、スペース、および次の特殊文字を含めることができます。_ .+ - 名前の先頭または末尾のスペースはトリミングされ、名前の一部として保存されません。最大長は 100 文字です。接続名では大文字と小文字は区別されません。
説明	接続の説明（オプション）。最大長は 255 文字です。
タイプ	接続のタイプ。【Google Analytics Mass Ingestion】接続タイプを選択します。
ランタイム環境	取り込みタスクを実行するランタイム環境の名前。 ランタイム環境として Secure Agent を指定する必要があります。 **注**: Hosted Agent やサーバーレスランタイム環境でアプリケーション取り込みタスクを実行することはできません。
サービスアカウント ID	サービスアカウントの作成後にダウンロードする JSON ファイル内にある client_email 値。
サービスアカウントキー	サービスアカウントの作成後にダウンロードする JSON ファイル内にある private_key 値。

Google BigQuery V2 接続のプロパティ

Google BigQuery V2 接続を作成する際には、接続プロパティを設定します。

次の表に、Google BigQuery V2 接続プロパティを示します。

プロパティ	説明
接続名	接続の名前。 各接続名は組織内で一意である必要があります。接続名には、英数字、スペース、および次の特殊文字を含めることができます。_ .+ -, 最大長は 255 文字です。
説明	接続の説明。最大長は 4000 文字です。
タイプ	Google BigQuery V2 接続タイプ。
ランタイム環境	タスクを実行するランタイム環境の名前。 Hosted Agent やサーバーレスランタイム環境でデータベース取り込みタスクを実行することはできません。

プロパティ	説明
サービスアカウントの電子メール	サービスアカウントの作成後にダウンロードする JSON ファイル内にある client_email 値。
サービスアカウントキー	サービスアカウントの作成後にダウンロードする JSON ファイル内にある private_key 値。
プロジェクト ID	サービスアカウントの作成後にダウンロードする JSON ファイル内にある project_id 値。 同じサービスアカウントを使用して複数のプロジェクトを作成した場合、接続先のデータセットが含まれるプロジェクトの ID を入力します。
ストレージパス	データを一時的に格納するためにエージェントがローカルステージファイルを作成する、Google Cloud Storage 内のパス。 大量のデータを読み書きするタスクに適用されます。このプロパティは、ステージングモードでデータを読み取る場合、またはバルクモードでデータを書き込む場合に使用します。 バケット名、またはバケット名とフォルダ名のいずれかを入力できます。 次のいずれかの形式を使用します。 - gs://<bucket_name> - gs://<bucket_name>/<folder_name>
接続モード	Google BigQuery との間でのデータの読み書きに使用するモード。 次のいずれかの接続モードを選択します。 - 簡易。レコードデータ型フィールド内の各フィールドを、マッピング内の個別のフィールドとしてフラット化します。 - 混合。レコードデータ型のフィールドを含む Google BigQuery テーブル内のすべての最上位のフィールドを表示します。Google BigQuery V2 コネクタは、最上位のレコードデータ型のフィールドを、マッピング内の文字列データ型の単一のフィールドとして表示します。 - 複合。Google BigQuery テーブル内のすべての列を、マッピング内の文字列データ型の単一のフィールドとして表示します。 デフォルトは［簡易］です。
スキーマ定義のファイルパス	Secure Agent が Google BigQuery テーブルのサンプルスキーマと一緒に JSON ファイルを作成する、Secure Agent マシン上のディレクトリ。JSON ファイル名は、Google BigQuery テーブル名と同じです。 または、Secure Agent が、Google BigQuery テーブルのサンプルスキーマと一緒に JSON ファイルを作成する必要がある場所の Google Cloud Storage 内のストレージパスを指定します。JSON ファイルは、Google Cloud Storage 内の指定したパスからローカルマシンにダウンロードできます。 複合接続モードを次のシナリオで設定する場合、スキーマ定義ファイルが必要です。 - リレーショナルソースからのデータの読み取りと、Google BigQuery ターゲットへのデータの書き込みのために、マッピング内に階層ビルダトランスフォーメーションを追加する場合。 - Google BigQuery ソースからのデータの読み取りと、リレーショナルターゲットへのデータの書き込みのために、マッピング内に階層パーサートランスフォーメーションを追加する場合。
従来の SQL をカスタムクエリに使用	このオプションは、カスタムクエリを定義するための従来の SQL を使用する場合に選択します。このオプションを選択しない場合、カスタムクエリの定義に標準 SQL を使用する必要があります。 **注**: 混合モードまたは複合モードで Google BigQuery V2 接続を設定する場合は適用されません。

プロパティ	説明
カスタムクエリのデータセット名	カスタムクエリを定義する際は、Google BigQuery データセットを指定する必要があります。
リージョン ID	アクセスする Google BigQuery データセットが存在する地域名。 **注**: 指定された地域に存在するバケット名またはバケット名とフォルダ名を **［ストレージパス］** プロパティで指定する必要があります。 Google BigQuery でサポートされる地域の詳細については、Dataset locations を参照してください。
ステージングデータセット	データをステージングするためのステージングテーブルを作成する Google BigQuery データセット名。ソースまたはターゲットデータセットとは異なる Google BigQuery データセットを定義できます。
オプションのプロパティの指定	特定のソースおよびターゲット機能を設定するための、Google BigQuery V2 接続のカスタムプロパティのカンマ区切りのキーと値のペア。 指定できるカスタムプロパティのリストの詳細については、次の Informatica Knowledge Base の記事を参照してください: https://kb.informatica.com/faq/7/Pages/26/632722.aspx

注: 接続プロパティで有効な資格情報を指定していることを確認してください。接続プロパティで誤った資格情報を指定しても、テスト接続は成功します。

Google Cloud Storage V2

Google Cloud Storage V2 接続を作成する際には、接続プロパティを設定します。

次の表に、Google Cloud Storage 接続のプロパティを示します。

プロパティ	説明
接続名	接続の名前。 各接続名は組織内で一意である必要があります。接続名には、英数字、スペース、および次の特殊文字を含めることができます。_ .+ -, 最大長は 255 文字です。
説明	接続の説明。最大長は 4000 文字です。
タイプ	Google Cloud Storage V2 接続タイプ。
ランタイム環境	タスクを実行するランタイム環境の名前。 Hosted Agent またはサーバーレスランタイム環境でデータベース取り込みタスクまたはストリーミング取り込みタスクを実行することはできません。
サービスアカウント ID	サービスアカウントの作成後にダウンロードする JSON ファイル内にある client_email 値。
サービスアカウントキー	サービスアカウントの作成後にダウンロードする JSON ファイル内にある private_key 値。

プロパティ	説明
プロジェクト ID	サービスアカウントの作成後にダウンロードする JSON ファイル内にある project_id 値。 同じサービスアカウントを使用して複数のプロジェクトを作成した場合、接続先のバケットが含まれるプロジェクトの ID を入力します。
プライベートキー ID	サービスアカウントの作成後にダウンロードする JSON ファイル内にある private_key_id 値。 このプロパティは、データベースの取り込みタスクまたはストリーミングの取り込みタスクにのみ適用されます。
クライアント ID	サービスアカウントの作成後にダウンロードする JSON ファイル内にある client_id 値。 このプロパティは、データベースの取り込みタスクまたはストリーミングの取り込みタスクにのみ適用されます。
バケット名	接続する Google Cloud Storage のバケット名です。 ソースオブジェクトを選択すると、Package Explorer に、指定した Google Cloud Storage バケットで使用可能なファイルとフォルダが一覧表示されます。 バケット名を指定しない場合は、Package Explorer からバケットを選択して、ソースを選択できます。

Windows でのプロキシ設定

組織で送信プロキシサーバーを使用してインターネットに接続する場合、Secure Agent は、そのプロキシサーバーを使用して Informatica Intelligent Cloud Services に接続します。
Windows マシンで Secure Agent のプロキシサーバーを設定するには、Secure Agent Manager を使用するか、Secure Agent の JVM オプションを使用する必要があります。

制限: これらのステップは、一括取り込みデータベースでは機能しません。

プロキシ設定については、ネットワーク管理者にお問い合わせください。

1. **［開始］** > **［すべてのプログラム］** > **［Informatica Cloud Secure Agent］** > **［Informatica Cloud Secure Agent］**をクリックして、Secure Agent Manager を起動します。
   Secure Agent Manager に **Secure Agent** のステータスが表示されます。
2. ［Secure Agent Manager］ページで **［プロキシ］**をクリックします。
3. **［プロキシサーバーを使用］**をクリックして、プロキシサーバーの設定を入力します。
4. 次のプロキシサーバーの詳細を設定します。

フィールド	説明
プロキシホスト	Secure Agent が使用する送信プロキシサーバーのホスト名。
プロキシポート	送信プロキシサーバーのポート番号。
ユーザー名	送信プロキシサーバーに接続するユーザー名。
パスワード	送信プロキシサーバーに接続するためのパスワード。

5. **［OK］**をクリックします。
6. Informatica Intelligent Cloud Services にログインします。
7. ［管理］を開いて **［ランタイム環境］**を選択します。

8. プロキシサーバーを設定する Secure Agent を選択します。
9. ページの右上隅にある **[編集]** をクリックします。
10. **[システム構成の詳細]** セクションで、CMI Streaming Agent Service の **[タイプ]** に **[エージェント]** を選択します。
11. プロキシサーバーを使用するには、任意の **JVMOption** フィールドに次のパラメータを追加して、それぞれに適切な値を指定します。

パラメータ	説明
-Dproxy.host=	送信 HTTPS プロキシサーバーのホスト名。
-Dproxy.port=	送信 HTTPS プロキシサーバーのポート番号。
-Dproxy.user=	HTTPS プロキシサーバーのユーザー名。
-Dproxy.password=	HTTPS プロキシサーバーのパスワード。

注: パラメータと単一引用符で囲まれたパラメータの値を指定する必要があります。

以下に例を示します。

```
JVMOption1='-Dproxy.host=INPQ8583WI29'
JVMOption2='-Dproxy.port=8081'
JVMOption3='-Dproxy.user=adminuser'
JVMOption4='-Dproxy.password=password'
```

注: **[システム構成の詳細]** セクションで設定できる **JVMOption** フィールドは 5 つだけです。残りのパラメータを設定するには、**[カスタム構成の詳細]** セクションで **JVMOption** フィールドを追加する必要があります。**[カスタム構成の詳細]** セクションで、CMI Streaming Agent Service の **[タイプ]** に **[エージェント]** を選択し、**JVMOption** フィールドを追加して、残りのパラメータとその適切な値を指定します。

12. **[保存]** をクリックします。

    Secure Agent が再起動して設定が適用されます。

    注: プロキシサーバーを設定した場合でも、セッションログにはプロキシサーバーの詳細は記録されません。

Linux でのプロキシ設定

組織で送信プロキシサーバーを使用してインターネットに接続する場合、Secure Agent は、そのプロキシサーバー経由で Informatica Intelligent Cloud Services に接続します。
Secure Agent に定義されているプロキシサーバーの設定は、コマンドラインから更新できます。Linux マシンで Secure Agent のプロキシサーバー設定を行うには、 `proxy.ini` ファイルを更新し、Secure Agent の JVM オプションを設定する必要があります。

制限: これらのステップは、一括取り込みデータベースでは機能しません。

プロキシ設定については、ネットワーク管理者にお問い合わせください。

1. 次のディレクトリに移動します。

   `<Secure Agent のインストールディレクトリ>/apps/agentcore/conf`

2. proxy.ini ファイルを更新するには、次のパラメータを追加し、各パラメータに適切な値を指定します。

```
InfaAgent.ProxyHost=<proxy_server_hostname>
           InfaAgent.ProxyPort=<proxy_server_port>
           InfaAgent.ProxyUser=<user_name>
           InfaAgent.ProxyPassword=<password>
           InfaAgent.ProxyPasswordEncrypted=false
```

以下に例を示します。

```
InfaAgent.ProxyHost=INW2PFOMT01V
           InfaAgent.ProxyPort=808
           InfaAgent.ProxyUser=user06
           InfaAgent.ProxyPassword=user06
           InfaAgent.ProxyPasswordEncrypted=false
```

3. Informatica Intelligent Cloud Services にログインします。
4. ［管理］を開いて **［ランタイム環境］** を選択します。
5. プロキシサーバーを設定する Secure Agent を選択します。
6. ページの右上隅にある **［編集］** をクリックします。
7. **［システム構成の詳細］** セクションで、CMI Streaming Agent Service の **［タイプ］** に **［エージェント］** を選択します。
8. プロキシサーバーを使用するには、任意の **JVMOption** フィールドに次のパラメータを追加して、それぞれに適切な値を指定します。

パラメータ	説明
-Dproxy.host=	送信 HTTPS プロキシサーバーのホスト名。
-Dproxy.port=	送信 HTTPS プロキシサーバーのポート番号。
-Dproxy.user=	HTTPS プロキシサーバーのユーザー名。
-Dproxy.password=	HTTPS プロキシサーバーのパスワード。

注: パラメータと単一引用符で囲まれたパラメータの値を指定する必要があります。

以下に例を示します。

```
JVMOption1='-Dproxy.host=INPQ8583WI29'

JVMOption2='-Dproxy.port=8081'

JVMOption3='-Dproxy.user=adminuser'

JVMOption4='-Dproxy.password=password'
```

注: ［システム構成の詳細］ セクションで設定できる **JVMOption** フィールドは 5 つだけです。残りのパラメータを設定するには、**［カスタム構成の詳細］** セクションで **JVMOption** フィールドを追加する必要があります。**［カスタム構成の詳細］** セクションで、CMI Streaming Agent Service の **［タイプ］** に **［エージェント］** を選択し、**JVMOption** フィールドを追加して、残りのパラメータとその適切な値を指定します。

9. **［保存］** をクリックします。

Secure Agent が再起動して設定が適用されます。

注: プロキシサーバーを設定した場合でも、セッションログにはプロキシサーバーの詳細は記録されません。

Google PubSub - 一括取り込みストリーミング接続のプロパティ

Google PubSub 一括取り込みストリーミング接続を定義するときは、接続プロパティを設定する必要があります。この接続タイプは、一括取り込みサービスで設定するストリーミング統合タスクで使用できます。

次の表に、Google PubSub 接続のプロパティを示します。

プロパティ	説明
接続名	接続の名前。この名前では、大文字と小文字が区別されず、ドメイン内で一意にする必要があります。このプロパティは、接続を作成した後に変更できます。名前は 128 文字以内で指定し、空白および以下の特殊文字は使用できません。~ ` ! $ % ^ & * ( ) - + = { [}] | \ : ; " ' < , > . ? /
説明	オプション。接続を識別するために使用する説明。 説明は 4000 文字以下にする必要があります。
タイプ	Google PubSub 接続タイプ。
ランタイム環境	タスクを実行するランタイム環境の名前。
クライアントの電子メール	サービスアカウントの作成後にダウンロードする JSON ファイル内にある client_email 値。
クライアント ID	サービスアカウントの作成後にダウンロードする JSON ファイル内にある client_id 値。
プライベートキー ID	サービスアカウントの作成後にダウンロードする JSON ファイル内にある private_key_id 値。
秘密鍵	サービスアカウントの作成後にダウンロードする JSON ファイル内にある private_key 値。
プロジェクト ID	サービスアカウントの作成後にダウンロードする JSON ファイル内にある project_id 値。

注: ［クライアント ID］と**［プライベートキー ID］**に間違った値を入力した場合でも、Google PubSub コネクタのテスト接続が失敗することはありません。

Hadoop Files V2 接続のプロパティ

Hadoop Files V2 接続を設定する場合は、接続プロパティを設定する必要があります。

次の表に、Hadoop Files V2 接続のプロパティを示します。

接続プロパティ	説明
接続名	Hadoop Files V2 接続の名前。
説明	接続の説明。説明は、765 文字を超えることはできません。

接続プロパティ	説明
タイプ	接続タイプ。[Hadoop Files V2] を選択します。
ランタイム環境	タスクを実行するランタイム環境の名前。
ユーザー名	HDFS からデータを読み取るため必要。データの読み書きのために、単一ノードの HDFS の場所へのアクセス権限を持つユーザーの名前を入力します。
NameNode の URI	HDFS にアクセスするための URI。 Cloudera、Amazon EMR、Hortonworks ディストリビューションでは、以下の形式を使用して名前ノード URI を指定します。 hdfs://<namenode>:<port>/ ここで、 - <namenode>は、名前ノードのホスト名または IP アドレスです。 - <port>は、名前ノードがリモートプロシージャコール（RPC）をリスンするポートです。 Hadoop クラスタに接続するには、ネームノードポート fs.defaultFS を指定します。 Hadoop クラスタが高可用性用に設定されている場合、core-site.xml ファイルの fs.defaultFS 値をコピーし、/を追加して名前ノード URI を指定する必要があります。 例として、次のスニペットにサンプル core-site.xml ファイルの fs.defaultFS 値を示します。 <property> <name>fs.defaultFS</name> <value>hdfs://nameservice1</value> <source>core-site.xml</source> </property> 上のスニペットで、fs.defaultFS 値は次のとおりです。 hdfs://nameservice1 対応する名前ノード URI は次のとおりです。 hdfs://nameservice1/ **注**: 名前ノード URI またはローカルパスのいずれかを指定します。ローカルファイルシステムパスとの間でデータを読み書きする場合、名前ノード URI は指定しません。
ローカルパス	データを読み書きするためのローカルファイルシステムパス。ローカルパスを指定するには、次の条件を参照します。 - 名前ノード URI を指定する場合、ローカルパスに NA を入力する必要があります。ローカルパスに NA が含まれていない場合、名前ノード URI は機能しません。 - 名前ノード URI およびローカルパスを指定する場合、ノーカルパスが優先されます。その接続は、すべてのタスクを実行するためにローカルパスを使用します。 - ローカルパスを空欄にした場合、エージェントはその接続内でルートディレクトリ（/）を設定します。その接続は、すべてのタスクを実行するためにローカルパスを使用します。 - ファイルまたはディレクトリがローカルシステム内にある場合は、ファイルまたはディレクトリの完全修飾パスを入力します。 例えば、/user/testdir はローカルシステム内のディレクトリの場所を指定します。 [ローカルパス] のデフォルト値は [NA] です。
構成ファイルのパス	Hadoop 構成ファイルを格納するディレクトリ。 **注**: core-site.xml、hdfs-site.xml、および hive-site.xml を Hadoop クラスタからコピーし、Linux Box のフォルダに追加します。
キータブファイル	マシンを認証するための暗号化キーと Kerberos プリンシパルが格納されたファイル。

接続プロパティ	説明
プリンシパル名	スーパーユーザー特権に割り当てられたユーザーは、管理者特権を持つユーザーが行うことができるすべてのタスクを実行することができます。
偽装ユーザー名	Kerberos 認証を使用する Hadoop クラスタ内でマッピングを実行する、または Kerberos 認証を使用するソースおよびターゲットに接続するために、異なるユーザーを有効にできます。マッピングの実行またはビッグデータのソースおよびターゲットへの接続のために、異なるユーザーを有効にするには、ユーザーの偽装を設定する必要があります。

注: リモートファイルに対して読み取りまたは書き込みを行う場合、**［ネームノード URI］**フィールドと **［構成ファイルパス］**フィールドは必須です。ローカルファイルに対して読み取りまたは書き込みを行う場合、必要なのは **［ローカルパス］**フィールドのみです。

JDBC V2 接続のプロパティ

JDBC V2 接続をセットアップする際には、接続プロパティを設定します。

次の表に、JDBC V2 接続のプロパティを示します。

プロパティ	説明
接続名	接続の名前。
説明	接続の説明。
タイプ	接続タイプ。 リストから JDBC V2 を選択します。
ランタイム環境	タスクを実行するランタイム環境の名前。 Secure Agent を選択します。
ユーザー名	データベースに接続するためのユーザー名。
パスワード	データベースユーザー名のパスワード。
スキーマ名	オプション。スキーマ名です。 スキーマ名を指定しない場合は、データベース内で使用できるすべてのスキーマがリストされます。 Oracle のパブリックシノニムに対して読み取りまたは書き込みを行うには、「PUBLIC」と入力します。
JDBC ドライバクラス名	JDBC ドライバクラスの名前。 Aurora PostgreSQL に接続するには、次のドライバクラス名を指定します: org.postgresql.Driver 特定のデータベースで使用するドライバクラスの詳細については、対応するサードパーティベンダ提供のドキュメントを参照してください。

プロパティ	説明
接続文字列	データベースへの接続に使用する接続文字列。 以下の形式を使用して、接続文字列を指定します: jdbc:<subprotocol>:<subname> 例えば、Aurora PostgreSQL データベースタイプの接続文字列は、jdbc:postgresql://<host>:<port>[/dbname]です。。 特定のドライバで使用する接続文字列の詳細については、対応するサードパーティベンダ提供のマニュアルを参照してください。
追加セキュリティプロパティ	セッションログに表示しない、接続文字列の機密データをマスクします。 接続文字列のうち、マスクする部分を指定します。 接続を作成する際、このフィールドに入力した文字列が、**[接続文字列]** フィールドに指定した文字列に追加されます。
データベースタイプ	接続するデータベースタイプを入力します。 以下のいずれかのデータベースタイプを選択できます。 - PostgreSQL。Amazon Web Services または Microsoft Azure 環境でホストされている Aurora PostgreSQL データベースに接続します。 - Azure SQL データベース。Microsoft Azure 環境でホストされている Azure SQL データベースに接続します。 - その他。タイプ 4 の JDBC ドライバをサポートする任意のデータベースに接続します。 デフォルトは［その他］です。
自動コミットを有効化 [1]	ドライバが、SQL 文の実行時にデータベースにデータを自動的にコミットする接続をサポートするかどうかを指定します。 無効にすると、JDBC ドライバで自動コミットモードが有効になっている場合でも、ドライバはデータを自動的にコミットする接続をサポートしません。 デフォルトでは無効になっています。
大文字と小文字が混在する識別子をサポート	データベースが大文字と小文字を区別する識別子をサポートするかどうか指定します。 有効にした場合、Secure Agent は、すべての識別子を［SQL 識別子文字］プロパティに対して選択された文字で囲みます。 デフォルトでは無効になっています。
SQL 識別子文字	データベースが、SQL クエリで区切り識別子を囲むのに使用する文字のタイプ。使用できる文字は、データベースタイプによって異なります。 データベースで通常識別子が使用される場合、［なし］を選択します。Secure Agent で SQL クエリを生成するときは、区切り文字で識別子を囲みません。 データベースで区切り識別子が使用される場合、文字を選択します。Secure Agent で SQL クエリを生成するときは、この文字で区切り識別子を囲みます。

[1] 詳細モードのマッピングには適用されません。

JMS 接続のプロパティ

JMS 接続をセットアップする際には、接続プロパティを設定する必要があります。

次の表に、JMS 接続の接続プロパティを示します。

プロパティ	説明
接続名	接続の名前。 この名前では、大文字と小文字が区別されず、ドメイン内で一意にする必要があります。このプロパティは、接続を作成した後に変更できます。名前は 128 文字以内で指定し、空白および以下の特殊文字は使用できません。 ~ ` ! $ % ^ & * ( ) - + = { [}] | \ : ; " ' < , > . ? /
説明	オプション。接続を識別するために使用できる説明。 説明は、4,000 文字を超える事は出来ません。
タイプ	JMS 接続タイプ。 接続タイプが見つからない場合は、**[アドオンコネクタ]** ページに移動し、コネクタをインストールしてください。
ランタイム環境	タスクを実行するランタイム環境の名前。
接続 URL	JNDI 命名プロバイダの URL。 例えば、IBM MQ では.bindings ファイルが含まれるディレクトリの場所です。
JNDI ユーザー名	オプション。JNDI コンテキストファクトリに接続するためのユーザー名。
JNDI パスワード	オプション。JNDI コンテキストファクトリに接続するために使用するユーザーアカウントのパスワード。
JNDI コンテキストファクトリ	JNDI サービスへの接続のための JMS プロバイダ固有の初期 JNDI コンテキストファクトリの実装。この値は、初期コンテキストファクトリの完全修飾クラス名です。 例えば、ActiveMQ の初期コンテキストファクトリのクラス名は、 `org.apache.activemq.jndi.ActiveMQInitialContextFactory` です。 詳細については、JMS プロバイダのドキュメントを参照してください。
JNDI パッケージプレフィックス	URL コンテキストファクトリのロード時に使用するパッケージプレフィックスのコロン区切りのリスト。これらは、URL ファクトリクラスを作成するファクトリクラス名のパッケージプレフィックスです。 値の詳細については、JMS プロバイダのドキュメントを参照してください。
JMS 接続ファクトリ	JNDI サーバー内のオブジェクト名です。これにより JMS クライアントは JMS 接続を作成できます。 例えば、`jms/QCF` または `jmsSalesSystem` です。
JMS Connection ユーザー名	オプション。JMS 接続ファクトリに接続するためのユーザー名。
JMS Connection パスワード	オプション。JMS 接続ファクトリに接続するために使用するユーザーアカウントのパスワード。

注: 外部 JMS JAR ファイルを次の場所にコピーしてください。

<Secure_Agent_home>/ext/connectors/thirdparty/infa.jms

外部 JMS JAR ファイルをコピーした後、Secure Agent を再起動します。

Kafka 接続のプロパティ

Kafka 接続をセットアップする際には、接続プロパティを設定する必要があります。

次の表に、Kafka 接続のプロパティを示します。

プロパティ	説明
接続名	接続の名前。 名前では大文字小文字を区別しません。ドメイン内で一意である必要があります。このプロパティは、接続を作成した後に変更できます。名前は 128 文字以内で指定し、空白および以下の特殊文字は使用できません。 ~ ` ! $ % ^ & * ( ) - + = { [}] | \ : ; " ' < , > . ? /
説明	オプション。接続を識別するために使用する説明。 説明は、4,000 文字を超えることはできません。
タイプ	Kafka 接続タイプ。 接続タイプが見つからない場合は、管理者で **[アドオンコネクタ]** ページに移動し、コネクタをインストールしてください。
ランタイム環境	タスクを実行するランタイム環境の名前。
Kafka Broker リスト	Kafka Broker のカンマ区切りリスト。 Kafka Broker を一覧表示するには、次の形式を使用します。 *<HostName>:<PortNumber>* **注:** SSL を介して Kafka Broker に接続する場合は、ホスト名に完全修飾ドメイン名を指定する必要があります。それ以外の場合、テスト接続は SSL ハンドシェイクエラーで失敗します。
再試行タイムアウト	オプション。Secure Agent がデータの読み取りまたは書き込みのために Kafka Broker への再接続を試行した後の秒数。 デフォルトは 180 秒です。 このプロパティは、一括取り込みデータベースでは使用されません。**[追加接続プロパティ]** で同等の Kafka プロパティを指定できます。
Kafka Broker のバージョン	Kafka メッセージブローカーのバージョン。有効な値は Apache 0.10.1.1 以上のみです。 ストリーミング取り込みタスクのオプション。

プロパティ	説明
追加接続プロパティ	オプション。Kafka プロデューサまたはコンシューマの追加設定プロパティのカンマ区切りリスト。 ストリーミング取り込みタスクの場合で、<Security Protocol>を SASL_PLAINTEXT または SASL_SSL に設定する場合は、<kerberos name>プロパティを設定してください。 データベース取り込みタスクでセキュリティプロトコルとプロパティを指定する場合は、**[追加セキュリティプロパティ]** プロパティではなく、ここで指定します。例: security.protocol=SSL,ssl.truststore.location=/opt/kafka/config/kafka.truststore.jks,ssl.truststore.password=<trustore_password>
スキーマレジストリの URL	Kafka の Avro ソースとターゲットにアクセスするための Confluent スキーマレジストリサービスの場所とポート。 スキーマレジストリの URL を一覧表示するには、次の形式を使用します。 <https>://<*HostName or IP*>:<*PortNumber*> または <http>://<*HostName or IP*>:<*PortNumber*> スキーマレジストリの URL の例: https://kafkarnd.informatica.com:8082 または http://10.65.146.181:8084 メタデータを格納するために Confluent スキーマレジストリを使用する Avro 形式で Kafka トピックをインポートする場合にのみ適用されます。 このプロパティは、一括取り込みデータベースでは使用されません。**[追加接続プロパティ]** で同等の Kafka プロパティを指定できます。
SSL モード	必須。接続に使用する暗号化タイプを決定します。 次の SSL モードからモードを選択できます。 - 利用不可状態。Kafka ブローカとの暗号化されていない接続を確立します。 - 一方向。トラストストアファイルおよびトラストストアパスワードを使用して Kafka ブローカとの暗号化された接続を確立します。 - 双方向。トラストストアファイル、トラストストアパスワード、キーストアファイル、およびキーストアパスワードを使用して、Kafka ブローカへの暗号化された接続を確立します。 このプロパティは、一括取り込みデータベースでは使用されません。**[追加接続プロパティ]** で同等の Kafka プロパティを指定できます。
SSL トラストストアファイルパス	一方向または双方向 SSL モードを使用するときは必須です。 Kafka ブローカに接続するための SSL 証明書を格納する SSL トラストストアファイルの絶対パスとファイル名。
SSL トラストストアパスワード	一方向または双方向 SSL モードを使用するときは必須です。 SSL トラストストアのパスワード。
SSL キーストアファイルパス	双方向 SSL モードを使用するときは必須です。 Kafka ブローカに接続するためのプライベートキーと証明書を格納する SSL キーストアファイルの絶対パスとファイル名。

プロパティ	説明
SSL キーストアパスワード	双方向 SSL モードを使用するときは必須です。 SSL キーストアのパスワード。
追加セキュリティプロパティ	オプション。安全な方法で Kafka ブローカに接続するための、追加の設定プロパティのカンマ区切りリスト。 **［追加接続プロパティ］**と**［追加セキュリティプロパティ］**で同じプロパティに 2 つの異なる値を指定すると、**［追加セキュリティプロパティ］**の値が**［追加接続プロパティ］**の値をオーバーライドします。 このプロパティは、一括取り込みデータベースでは使用されません。セキュリティプロトコルとプロパティは、**［追加接続プロパティ］**で指定できます。

スキーマレジストリのセキュリティ設定プロパティ

［スキーマレジストリの URL］接続プロパティを設定する際は、スキーマレジストリのセキュリティ設定プロパティを設定できます。一方向 SSL、双方向 SSL、および基本認証を設定して、安全な方法で Confluent スキーマレジストリに接続できます。

次の表に、Confluent スキーマレジストリを使用する場合の、Kafka 接続のセキュリティプロパティを示します。

プロパティ	説明
SSL モードスキーマレジストリ[1]	必須。接続に使用する暗号化タイプを決定します。 次の SSL モードからモードを選択できます。 - 利用不可状態。暗号化されていない、Confluent スキーマへの接続を確立します。 - 一方向。トラストストアファイルおよびトラストストアパスワードを使用して、Confluent スキーマレジストリへの暗号化された接続を確立します。 - 双方向。トラストストアファイル、トラストストアパスワード、キーストアファイル、およびキーストアパスワードを使用して、Confluent スキーマレジストリへの暗号化された接続を確立します。 このプロパティは、一括取り込みデータベースでは使用されません。**［追加接続プロパティ］**で同等の Kafka プロパティを指定できます。
SSL TrustStore ファイルパススキーマレジストリ[1]	一方向または双方向 SSL モードを使用するときは必須です。 Confluent スキーマレジストリに接続するための SSL 証明書を格納する SSL トラストストアファイルの絶対パスとファイル名。
SSL TrustStore パスワードスキーマレジストリ[1]	一方向または双方向 SSL モードを使用するときは必須です。 SSL トラストストアのパスワード。
SSL KeyStore ファイルパススキーマレジストリ[1]	双方向 SSL モードを使用するときは必須です。 Confluent スキーマレジストリに接続するためのプライベートキーと証明書を格納する SSL キーストアファイルの絶対パスとファイル名。

プロパティ	説明
SSL KeyStore パスワードスキーマレジストリ[1]	双方向 SSL モードを使用するときは必須です。 SSL キーストアのパスワード。
追加のセキュリティプロパティスキーマレジストリ	オプション。安全な方法で Confluent スキーマレジストリに接続するための、追加のセキュリティプロパティのカンマ区切りリスト。 例えば、Confluent スキーマレジストリとの安全な通信を確立するための基本認証を設定する場合は、次の値を指定します。 basic.auth.credentials.source=USER_INFO,basic.auth.user.info=<username>:<password> **［追加接続プロパティ］**と**［追加のセキュリティプロパティスキーマレジストリ］**で同じプロパティに 2 つの異なる値を指定した場合は、**［追加のセキュリティプロパティスキーマレジストリ］**の値が**［追加接続プロパティ］**の値より優先されます。 このプロパティは、一括取り込みデータベースでは使用されません。

[1] マッピングには適用されません。

Kerberised Kafka クラスタからのデータの読み取りまたは書き込みのための krb5.conf ファイルの設定

Kerberised Kafka クラスタに対する読み取りまたは書き込みを行うには、デフォルトのレルム、KDC、および Kafka の詳細ソースプロパティまたは詳細ターゲットプロパティを設定します。

必要な Kerberos 構成ファイルを Secure Agent マシンに配置し、Kafka 接続で必要な JAAS 設定を指定することで、Kafka クライアントの Kerberos 認証を設定できます。JAAS 設定により、Kafka ブローカが Kafka クライアントを認証するために使用する必要があるキータブとプリンシパルの詳細を定義します。

注: このトピックは一括取り込みアプリケーションと一括取り込みデータベースには適用されません。一括取り込みアプリケーションと一括取り込みデータベースでは、この機能はまだサポートされていません。

Kerberised Kafka クラスタからの読み取りまたは Kerberised Kafka クラスタへの書き込みを行う前に、次のタスクを実行します。

1. Kerberised Kafka クラスタに krb5.conf ファイルがあることをを確認してください。
2. デフォルトのレルムと KDC を設定します。デフォルトの/etc/krb5.conf ファイルが設定されていないか、設定を変更する場合は、/etc/krb5.conf ファイルに次の行を追加します。

```
[libdefaults]
default_realm = <REALM NAME>
dns_lookup_realm = false
dns_lookup_kdc = false
ticket_lifetime = 24h
renew_lifetime = 7d
forwardable = true

[realms]
<REALM NAME> = {
kdc = <Location where KDC is installed>
admin_server = <Location where KDC is installed>
                                }
 [domain_realm]
.<domain name or hostname> = <KERBEROS DOMAIN NAME>
<domain name or hostname> = <KERBEROS DOMAIN NAME>
```

3. 実行時に java.security.auth.login.config ファイルを使用して静的 JAAS 設定ファイルを JVM に渡すには、次のタスクを実行します。

   a. JAAS 設定ファイルがあることを確認してください。

      JAAS 設定の作成および Kafka クライアントのキータブの設定については、https://kafka.apache.org/0101/documentation/#security の Apache Kafka のドキュメントを参照してください。

      たとえば、JAAS 設定ファイルには、次の設定行を含めることができます。

      ```
      //Kafka Client Authentication. Used for client to kafka broker connection
      KafkaClient {
      com.sun.security.auth.module.Krb5LoginModule required
      doNotPrompt=true
      useKeyTab=true
      storeKey=true
      keyTab="<path to Kafka keytab  file>/<Kafka keytab file name>"
      principal="<principal name>"
      client=true
      };
      ```

   b. JAAS 設定ファイルとキータブファイルをすべての Secure Agent の同じ場所に配置します。

      ランタイム環境のすべての Secure Agent がアクセスできる場所にファイルを配置することをお勧めします。たとえば、/etc または/temp です。

   c. 以下のプロパティを設定します。

      Kafka **接続**

      追加接続プロパティを Kafka 接続で設定し、次の形式で値を指定します。

      ```
      security.protocol=SASL_PLAINTEXT,sasl.kerberos.service.name=kafka,sasl.mechanism=GSSAPI
      ```

      ソース

      詳細ソースプロパティの**［コンシューマ設定プロパティ］**を設定して、Kafka 接続の**［追加接続プロパティ］**で指定した値をオーバーライドします。次の形式で値を指定します。

      ```
      security.protocol=SASL_PLAINTEXT,sasl.kerberos.service.name=kafka,sasl.mechanism=GSSAPI
      ```

      ターゲット

      詳細ターゲットプロパティの**［プロデューサ設定プロパティ］**を設定して、Kafka 接続の**［追加接続プロパティ］**で指定した値をオーバーライドします。次の形式で値を指定します。

      ```
      security.protocol=SASL_PLAINTEXT,sasl.kerberos.service.name=kafka,sasl.mechanism=GSSAPI
      ```

4. JAAS 設定を sasl.jaas.config 設定プロパティに埋め込むには、次のプロパティを設定します。

   Kafka **接続**

   追加接続プロパティを Kafka 接続で設定し、次の形式で値を指定します。

   ```
   security.protocol=SASL_PLAINTEXT,sasl.kerberos.service.name=kafka,sasl.mechanism=GSSAPI,
   sasl.jaas.config=com.sun.security.auth.module.Krb5LoginModule required useKeyTab=true
   storeKey=true doNotPrompt=true serviceName="<service_name>" keyTab="<location of keytab file>"
   client=true principal="<principal_name>";
   ```

   ソース

   詳細ソースプロパティの**［コンシューマ設定プロパティ］**を設定して、Kafka 接続の**［Kerberos 接続プロパティ］**で指定した値をオーバーライドします。次の形式で値を指定します。

   ```
   security.protocol=SASL_PLAINTEXT,sasl.kerberos.service.name=kafka,sasl.mechanism=GSSAPI,
   sasl.jaas.config=com.sun.security.auth.module.Krb5LoginModule required useKeyTab=true
   storeKey=true doNotPrompt=true serviceName="<service_name>" keyTab="<location of keytab file>"
   client=true principal="<principal_name>";
   ```

ターゲット

詳細ターゲットプロパティの［**プロデューサ設定プロパティ**］を設定して、Kafka 接続の［**Kerberos 接続プロパティ**］で指定した値をオーバーライドします。次の形式で値を指定します。

```
security.protocol=SASL_PLAINTEXT,sasl.kerberos.service.name=kafka,sasl.mechanism=GSSAPI,
sasl.jaas.config=com.sun.security.auth.module.Krb5LoginModule required useKeyTab=true
storeKey=true doNotPrompt=true serviceName="<service_name>" keyTab="<location of keytab file>"
client=true principal="<principal_name>";
```

Kafka クラスタの SASL PLAIN 認証の設定

Kafka 接続では、Kafka ブローカーの PLAIN セキュリティを Kafka ブローカーに接続するように設定できます。SASL PLAIN 認証を使用して Kafka ブローカーからデータを読み取ったり、Kafka ブローカーにデータを書き込んだりするには、Kafka 接続プロパティを設定します。Kafka 接続で定義されたプロパティをオーバーライドするには、詳細ソースプロパティまたは詳細ターゲットプロパティを設定できます。

Kafka ブローカーが Kafka プロデューサおよび Kafka コンシューマを認証できるように、SASL PLAIN 認証を設定できます。Kafka は、Java Authentication and Authorization Service（JAAS）を SASL PLAIN 認証に使用します。SASL PLAIN 認証を有効にするには、SASL メカニズムを PLAIN として指定する必要があります。また、Kafka ブローカーが認証に使用する必要がある書式設定済みの JAAS 設定を指定する必要があります。JAAS 設定により、Kafka ブローカーが Kafka クライアントを認証するために使用する必要があるユーザー名とパスワードを定義します。

注: このトピックは一括取り込みアプリケーションと一括取り込みデータベースには適用されません。一括取り込みアプリケーションと一括取り込みデータベースでは、この機能はまだサポートされていません。

以下のプロパティを設定します。

Kafka **接続**

［**追加接続プロパティ**］または［**追加セキュリティプロパティ**］プロパティを Kafka 接続で設定し、次の形式で値を指定します。

```
security.protocol=SASL_SSL,sasl.mechanism=PLAIN,sasl.jaas.config=org.apache.kafka.common.security.plain.Pl
ainLoginModule required username=<username> password=<password>
```

［**セキュリティ設定セクション**］で、［**一方向**］を **SSL モード**として指定し、SSL トラストストアファイルパスと SSL トラストストアパスワードを指定します。

ソース

詳細ソースプロパティの［**コンシューマ設定プロパティ**］プロパティを設定して、Kafka 接続の［**追加接続プロパティ**］プロパティで指定した値をオーバーライドします。次の形式で値を指定します。

```
security.protocol=SASL_SSL,sasl.mechanism=PLAIN,sasl.jaas.config=org.apache.kafka.common.security.plain.Pl
ainLoginModule required username=<username> password=<password>
```

ターゲット

詳細ターゲットプロパティの［**プロデューサ設定プロパティ**］プロパティを設定して、Kafka 接続の［**追加接続プロパティ**］プロパティで指定した値をオーバーライドします。次の形式で値を指定します。

```
security.protocol=SASL_SSL,sasl.mechanism=PLAIN,sasl.jaas.config=org.apache.kafka.common.security.plain.Pl
ainLoginModule required username=<username> password=<password>
```

Azure Event Hub Kafka ブローカーの SASL PLAIN 認証の設定

Kafka 接続では、Kafka ブローカーの PLAIN セキュリティを Azure Event Hub Kafka ブローカーに接続するように設定できます。Azure Event Hub Kakfa ブローカーに接続する場合、パスワードは、Event Hub 名前空間の完全修飾ドメイン名（FQDN）、共有アクセスキー名、および Azure Event Hub Kakfa ブローカーへの接続に必要な共有アクセスキーを含むエンドポイント URL を定義します。SSL モードを一方向として設定し、SSL トラストストアファイルパス用にファイルシステム上の信頼されたルート証明書へのパスを指定します。

Azure Event Hub Kafka ブローカーに接続するには、上記のプロパティのいずれかを設定し、次の形式で値を指定します。

```
security.protocol=SASL_SSL,sasl.mechanism=PLAIN,sasl.kerberos.service.name=Kafka,sasl.jaas.config=org.apache.ka
fka.common.security.plain.PlainLoginModule required username="$ConnectionString" password="Endpoint=sb://
<FQDN>/;SharedAccessKeyName=<key name>;SharedAccessKey=<shared access key>=";
```

Cloud Confluent Kafka クラスタの SASL_SSL 認証の設定

Kafka 接続では、Kafka ブローカーへの接続時に SSL セキュリティを暗号化と認証のために設定できます。SASL_SSL 認証を使用して Confluent Kafka ブローカーに対してデータを読み書きするには、Kafka 接続プロパティを設定します。Kafka 接続で定義されたプロパティをオーバーライドするには、詳細ソースプロパティまたは詳細ターゲットプロパティを設定できます。

注: このトピックは一括取り込みアプリケーションと一括取り込みデータベースには適用されません。一括取り込みアプリケーションと一括取り込みデータベースでは、この機能はまだサポートされていません。

以下のプロパティを設定します。

プロパティ	値
追加接続プロパティ	security.protocol=SASL_SSL,sasl.kerberos.service.name=kafka,ssl.endpoint.identification.algorithm=https,sasl.mechanism=P required username=<> password=<>
SSL モード	一方向

プロパティ	値
SSL トラストストアファイルパス	エージェント JDK の cacert ファイルを使用します。 例: /root/staging/infaagent/jdk/jre/lib/security/cacerts
SSL トラストストアパスワード	SSL トラストストアのパスワード。

Amazon Managed Streaming for Apache Kafka への接続

Kafka 接続では、Amazon Managed Streaming for Apache Kafka ブローカに接続するように PLAINTEXT または TLS 暗号化を設定できます。Amazon Managed Streaming for Apache Kafka ブローカに対してデータの読み取りと書き込みを行うには、Kafka 接続プロパティを設定します。

Kafka 接続の **[Kafka ブローカリスト]** プロパティを設定し、接続先の Kafka ブローカのカンマ区切りリストを次の形式で指定します。

<HostName>:<PortNumber>

TLS 暗号化を設定して、Kafka ブローカを Kafka プロデューサと Kafka コンシューマに安全に接続できるようにします。Amazon Managed Streaming for Apache Kafka ブローカの TLS 暗号化を設定するには、以下のプロパティを設定します。

財産	値
追加接続プロパティ	security.protocol=SSL
SSL モード	一方向または双方向。

財産	値
SSL トラストストアファイルパス	一方向または双方向 SSL モードを使用するときは必須です。 SSL トラストストアファイルの絶対パスおよびファイル名。
SSL トラストストアパスワード	一方向または双方向 SSL モードを使用するときは必須です。 SSL トラストストアのパスワード。
SSL キーストアファイルパス	双方向 SSL モードを使用するときは必須です。 Kafka ブローカーが Kafka クラスタ証明書に対して検証するプライベートキーと証明書を含む SSL キーストアファイルの絶対パスとファイル名。
SSL キーストアパスワード	双方向 SSL モードを使用するときは必須です。 SSL キーストアのパスワード。

詳細クラスタで実行されるマッピングを実行し、Amazon Managed Streaming for Apache Kafka ブローカに接続する場合は、Salted Challenge Response Authentication Mechanism（SCRAM）による SASL_SSL 認証を使用して Kafka ブローカを設定します。SASL_SSL 認証を使用して Amazon Managed Streaming for Apache Kafka ブローカに対してデータの読み取りと書き込みを行うには、以下のプロパティを設定します。

財産	値
追加接続プロパティ	security.protocol=SASL_SSL,sasl.mechanism=SCRAM-SHA-512,sasl.jaas.config=org.apache.kafka.common.security.scram.ScramLoginModule required username="<username>" password="<password>";
SSL モード	一方向または双方向。
SSL トラストストアファイルパス	一方向または双方向 SSL モードを使用するときは必須です。 SSL トラストストアファイルの絶対パスおよびファイル名。
SSL トラストストアパスワード	一方向または双方向 SSL モードを使用するときは必須です。 SSL トラストストアのパスワード。
SSL キーストアファイルパス	双方向 SSL モードを使用するときは必須です。 Kafka ブローカーが Kafka クラスタ証明書に対して検証するプライベートキーと証明書を含む SSL キーストアファイルの絶対パスとファイル名。
SSL キーストアパスワード	双方向 SSL モードを使用するときは必須です。 SSL キーストアのパスワード。

Marketo V3 接続のプロパティ

Marketo V3 接続をセットアップする際には、接続プロパティを設定します。

次の表に、Marketo V3 接続のプロパティを示します。

プロパティ	説明
接続名	接続の名前。 各接続名は組織内で一意である必要があります。接続名には、英数字、スペース、および次の特殊文字を含めることができます。_ .+ -, 最大長は 255 文字です。
説明	接続の説明。最大長は 4000 文字です。
タイプ	Marketo V3 接続タイプ。
ランタイム環境	タスクを実行するランタイム環境の名前。
client_ID	有効なアクセストークンを生成するために必要なカスタムサービスのクライアント ID。
client_secret	有効なアクセストークンを生成するために必要な Marketo カスタムサービスのクライアントシークレット。
grant_type	Marketo では、client_credentials 許可タイプのみサポートしています。
REST API URL	URL の形式は次のとおりです: https://<Marketo Rest API Server のホスト名>。 REST API URL については Marketo 管理者にお問い合わせください。
プロキシのバイパス	**注**: このプロパティは、アプリケーション取り込みタスク用に設定された接続には適用されません。

Microsoft Azure Blob Storage V3 接続のプロパティ

Microsoft Azure Blob Storage V3 接続をセットアップするときは、接続プロパティを設定します。

次の表に、Microsoft Azure Blob Storage V3 接続のプロパティを示します。

プロパティ	説明
接続名	接続の名前。 各接続名は組織内で一意である必要があります。接続名には、英数字、スペース、および次の特殊文字を含めることができます。_ .+ -, 最大長は 255 文字です。
説明	接続の説明。最大長は 4000 文字です。
タイプ	Microsoft Azure Blob Storage V3 接続タイプ。

プロパティ	説明
ランタイム環境	タスクを実行するランタイム環境の名前。 Secure Agent、Hosted Agent、またはサーバーレスランタイム環境を指定します。
アカウント名	Microsoft Azure Blob Storage アカウント名。
認証タイプ	Microsoft Azure Blob Storage アカウントの認証タイプ。 次のいずれかのオプションを選択します。 - 共有キー認証。アカウントキーを使用して Microsoft Azure Blob Storage に接続します。 - 共有アクセス署名。SAS トークンを使用して Microsoft Azure Blob Storage に接続します。SAS トークンを使用して、アカウントキーを共有せずに、特定の時間範囲でストレージアカウントまたはコンテナのリソースへのアクセス許可を付与します。 **注:** このオプションがコンテナレベルにあり、別のコンテナを使用している場合、ファイル取り込みタスクは失敗します。
アカウントキー	共有キー認証に適用されます。 Microsoft Azure Blob Storage アカウントのアカウントキー。
SAS トークン	共有アクセス署名に適用されます。 Azure Portal で生成された共有アクセス署名トークン。
コンテナ名	Microsoft Azure Blob Storage コンテナ名。
エンドポイントサフィックス	Microsoft Azure エンドポイントのタイプ。 次のいずれかのオプションを選択します。 - core.windows.net。Azure エンドポイントに接続します。 - core.usgovcloudapi.net。Azure Government エンドポイントに接続します。 - core.chinacloudapi.cn。該当なし。 デフォルトは core.windows.net です

Microsoft Azure Data Lake Storage Gen2 接続のプロパティ

Microsoft Azure Data Lake Storage Gen2 接続をセットアップするときは、接続プロパティを設定します。

以下の表に、Microsoft Azure Data Lake Storage Gen2 接続のプロパティを示します。

プロパティ	説明
接続名	接続の名前。 各接続名は組織内で一意である必要があります。接続名には、英数字、スペース、および次の特殊文字を含めることができます。_ .+ -, 最大長は 255 文字です。
説明	接続の説明。最大長は 4000 文字です。
タイプ	Microsoft Azure Data Lake Storage Gen2 接続タイプ。

プロパティ	説明
ランタイム環境	タスクを実行するランタイム環境の名前。 Hosted Agent またはサーバーレスランタイム環境でデータベース取り込みまたはストリーミング取り込みタスクを実行することはできません。
アカウント名	Microsoft Azure Data Lake Storage Gen2 のアカウント名またはサービス名。
認証タイプ	Microsoft Azure Data Lake Storage Gen2 アカウントにアクセスするための認証タイプ。 次のいずれかのオプションを選択します。 - サービスプリンシパル認証。クライアント ID、クライアントシークレット、およびテナント ID を使用して Microsoft Azure Data Lake Storage Gen2 に接続します。 - 共有キー認証。アカウントキーを使用して、Microsoft Azure Data Lake Storage Gen2 に接続します。 - マネージド ID 認証。Azure のアプリケーションに割り当てられた ID を使用して認証し、Microsoft Azure Data Lake Storage Gen2 の Azure リソースにアクセスする場合に選択します。 **注**: 一括取り込みストリーミングは、共有キー認証またはマネージド ID 認証をサポートしていません。
クライアント ID	サービスプリンシパル認証とマネージド ID 認証に適用されます。 アプリケーションのクライアント ID。 サービスプリンシパル認証を使用するには、Azure アクティブディレクトリに登録されているアプリケーションのアプリケーション ID またはクライアント ID を指定します。 マネージド ID 認証を使用するには、ユーザー割り当てマネージド ID のクライアント ID を指定します。権限がシステム割り当てマネージド ID によって提供される場合は、フィールドを空のままにします。システム割り当て ID がなく、ユーザー割り当てマネージド ID が 1 つだけある場合も、フィールドを空のままにしておくことをお勧めします。
クライアントシークレット	サービスプリンシパル認証に適用されます。 Azure Active Directory で OAuth 認証を完了するためのクライアントシークレットキー。
テナント ID	サービスプリンシパル認証に適用されます。 Azure Active Directory のディレクトリ ID。
アカウントキー	共有キー認証に適用されます。 Microsoft Azure Data Lake Storage Gen2 アカウントのアカウントキー。
ファイルシステム名	Microsoft Azure Data Lake Storage Gen2 アカウントのファイルシステムの名前。

プロパティ	説明
ディレクトリパス	ファイルシステム名を使用していない既存のディレクトリのパス。 以下のいずれかの構文を選択できます。 - / (ルートディレクトリの場合)。 - /dir1 - dir1/dir2 デフォルトのディレクトリはありません。
Adls Gen2 エンドポイント	Microsoft Azure エンドポイントのタイプ。 次のいずれかのエンドポイントを選択します。 - core.windows.net。Azure エンドポイントに接続します。 - core.usgovcloudapi.net。米国政府の Microsoft Azure Data Lake Storage Gen2 エンドポイントに接続します。 - core.chinacloudapi.cn。中国地域の Microsoft Azure Data Lake Storage Gen2 エンドポイントに接続します。 デフォルトは core.windows.net です

Microsoft Azure Event Hub 接続のプロパティ

Azure Event Hub 接続をセットアップする際には、接続プロパティを設定する必要があります。

次の表に、Azure Event Hub 接続のプロパティを示します。

プロパティ	説明
接続名	接続の名前。 名前では大文字小文字を区別しません。ドメイン内で一意である必要があります。このプロパティは、接続を作成した後に変更できます。名前は 128 文字以内で指定し、空白および以下の特殊文字は使用できません。 ~ ` ! $ % ^ & * ( ) - + = { [}] | \ : ; " ' < , > . ? /
説明	オプション。接続を識別するために使用する説明。 説明は、4,000 文字を超えることはできません。
タイプ	Azure Event Hub 接続のタイプ。 接続タイプが見つからない場合は、管理者で **[アドオンコネクタ]** ページに移動し、コネクタをインストールしてください。
ランタイム環境	タスクを実行するランタイム環境の名前。
テナント ID	データが属するテナントの ID。 この ID は、Azure Active Directory のディレクトリ ID です。
サブスクリプション ID	Azure サブスクリプションの ID。
リソースグループ名	Event Hub 名前空間に関連付けられた Azure リソースグループの名前。
クライアントアプリケーション ID	Azure Active Directory に作成されているアプリケーションの ID。

プロパティ	説明
クライアント秘密鍵	アプリケーション用に生成された秘密鍵。
Event Hub 名前空間	リソースグループ名に関連付けられた Event Hub 名前空間の名前。
共有アクセスポリシー名	オプション。Event Hub 名前空間共有アクセスポリシーの名前 このポリシーは、この接続に関連付けられたすべてのデータオブジェクトに適用される必要があります。 Event Hub から読み取るには、リスン権限が必要です。Event Hub に書き込むには、ポリシーに送信権限が必要です。
共有アクセスポリシーのプライマリキー	オプション。Event Hub 名前空間共有アクセスポリシーのプライマリキー。

Microsoft Azure Synapse Analytics Database Ingestion 接続のプロパティ

Microsoft Azure Synapse Analytics Database Ingestion 接続を定義するときは、接続プロパティを設定する必要があります。この接続タイプは、一括取り込みサービスで設定したアプリケーション取り込みタスクまたはデータベース取り込みタスクで使用できます。

注: 一部のプロパティは、Microsoft Azure Data Lake Storage Gen2 用です。一括取り込みアプリケーションおよび一括取り込みデータベースは、Microsoft Azure Data Lake Storage Gen2 を使用して、データを Microsoft Azure Synapse Analytics ターゲットテーブルに送信する前にファイルにステージングします。

以下の表に、接続のプロパティを示します。

プロパティ	説明
接続名	接続の名前。この名前は、組織内で一意にする必要があります。接続名には、英数字、スペース、および次の特殊文字を含めることができます。_ .+ - 名前の先頭または末尾のスペースはトリミングされ、名前の一部として保存されません。最大長は 100 文字です。接続名では大文字と小文字は区別されません。
説明	接続の説明（オプション）。最大長は 255 文字です。
タイプ	接続のタイプ。タイプが Microsoft Azure Synapse Analytics - データベース取り込み用であることを確認してください。
ランタイム環境	アプリケーション取り込みタスクおよびデータベース統合タスクを実行するランタイム環境の名前。ランタイム環境は、管理者で定義します。 **注:** Hosted Agent またはサーバーレスランタイム環境では、アプリケーション取り込みタスクとデータベース取り込みタスクを実行できません。

プロパティ	説明

Azure Synapse Analytics JDBC URL	Microsoft Azure Synapse Analytics（以前の SQL Data Warehouse）の JDBC 接続文字列。
	Microsoft SQL Server 認証の接続文字列の例:
	`jdbc:sqlserver://server.database.windows.net:1433;database=database`
	Azure Active Directory（AAD）認証の接続文字列の例:
	`jdbc:sqlserver://server.database.windows.net:1433;database=database;encrypt=true;trustServerCertificate=false;hostNameInCertificate=*.database.windows.net;loginTimeout=30;Authentication=ActiveDirectoryPassword;`
	注: デフォルトの認証タイプは、Microsoft SQL Server 認証です。

Azure Synapse Analytics JDBC ユーザー名	Microsoft Azure Synapse Analytics アカウントに接続するために使用するユーザー名。AAD 認証の AAD ユーザー名を指定します。
Azure Synapse Analytics JDBC パスワード	Microsoft Azure Synapse Analytics アカウントに接続するために使用するパスワード。
Azure Synapse Analytics スキーマ名	Microsoft Azure Synapse Analytics ターゲット内のスキーマの名前。
ADLS Gen2 アカウント名	Microsoft Azure Data Lake Storage Gen2 アカウントの名前。
クライアント ID	Active Directory で OAuth 認証を完了するためのクライアントアプリケーションの ID。
クライアントシークレット	Active Directory で OAuth 認証を完了するためのクライアント秘密鍵。
ディレクトリ	一括取り込みアプリケーションおよび一括取り込みデータベースがデータをファイルにステージングするために使用する Microsoft Azure Data Lake Storage Gen2 ディレクトリ。デフォルトはルートディレクトリです。
ファイルシステム名	Microsoft Azure Data Lake Storage Gen2 アカウントの既存のファイルシステムの名前。
テナント ID	Azure Active Directory のディレクトリ ID。

Microsoft Azure Synapse SQL 接続のプロパティ

Microsoft Azure Synapse SQL 接続をセットアップするときは、接続プロパティを設定します。

次の表に、Microsoft Azure Synapse SQL 接続のプロパティを示します。

プロパティ	説明
接続名	接続の名前。 各接続名は組織内で一意である必要があります。接続名には、英数字、スペース、および次の特殊文字を含めることができます。_ .+ -, 最大長は 255 文字です。
説明	接続の説明。最大長は 4000 文字です。
タイプ	Microsoft Azure Synapse SQL 接続タイプ。
ランタイム環境	タスクを実行するランタイム環境の名前。 Secure Agent、Hosted Agent、またはサーバーレスランタイム環境を選択します。

Azure DW JDBC URL	Microsoft Azure Synapse SQL JDBC 接続文字列。
	Microsoft SQL Server 認証の場合は、接続文字列を次の形式で入力します。
	`jdbc:sqlserver://<Server>.database.windows.net:1433;database=<Database>`
	Azure Active Directory（AAD）認証の場合は、接続文字列を次の形式で入力します。
	`jdbc:sqlserver://<Server>.database.windows.net:1433;database=<Database>;encrypt=true;trustServerCertificate=false;hostNameInCertificate=*.database.windows.net;loginTimeout=30;Authentication=ActiveDirectoryPassword;`
	マネージド ID 認証の場合は、接続文字列を次の形式で入力します。
	`jdbc:sqlserver://<サーバー>.database.windows.net:1433;database=<データーベース>;Authentication=ActiveDirectoryMsi;`
	デフォルト値は、Microsoft SQL Server 認証です。

Azure DW JDBC ユーザー名	Microsoft Azure Synapse SQL アカウントに接続するためのユーザー名。AAD 認証の AAD ユーザー名を指定します。
Azure DW JDBC パスワード	Microsoft Azure Synapse SQL アカウントに接続するためのパスワード。AAD 認証の場合は、AAD ユーザーのパスワードを指定します。
Azure DW スキーマ名	Microsoft Azure Synapse SQL 内のスキーマの名前。
Azure DW クライアント ID	マネージド ID 認証でユーザー割り当てマネージド ID を使用して Microsoft Azure Synapse SQL に接続する場合は必須です。 ユーザー割り当てマネージド ID のクライアント ID。 マネージド ID がシステム割り当てである場合は、フィールドを空のままにします。

プロパティ	説明
Azure Storage のタイプ	ファイルをステージングする Azure ストレージのタイプ。 次のいずれかのストレージタイプを選択します。 - Azure BlobMicrosoft Azure Blob Storage を使用してファイルをステージングします。 - ADLS Gen2Microsoft Azure Data Lake Storage Gen2 を使用してファイルをステージングします。 デフォルトは Azure Blob です。
認証タイプ	ファイルをステージングする Azure ストレージに接続するための認証タイプ。 次のいずれかのオプションを選択します。 - 共有キー認証。アカウント名とアカウントキーを使用して、Microsoft Azure Blob Storage または Microsoft Azure Data Lake Storage Gen2 に接続します。 - サービスプリンシパル認証。Microsoft Azure Data Lake Storage Gen2 に適用されます。クライアント ID、クライアントシークレット、およびテナント ID を使用して Microsoft Azure Data Lake Storage Gen2 に接続します。サービスプリンシパル認証を使用するには、Azure Active Directory にアプリケーションを登録し、クライアントシークレットを生成してから、Storage Blob Contributor ロールをアプリケーションに割り当てる必要があります。 - マネージド ID 認証。Microsoft Azure Data Lake Storage Gen2 に適用されます。Azure のアプリケーションに割り当てられた ID を使用して認証し、Microsoft Azure Data Lake Storage Gen2 の Azure リソースにアクセスする場合に選択します。 ファイル取り込みタスクで、ターゲットとしてマネージド ID 認証タイプの Microsoft Azure Synapse SQL を選択した場合は、ソースとして Microsoft Azure Data Lake Storage Gen2 を選択する必要があります。
Azure Blob アカウント名	Microsoft Azure Blob Storage の共有キー認証に適用されます。 ファイルをステージングする Microsoft Azure Blob Storage アカウントの名前。
Azure Blob アカウントキー	Microsoft Azure Blob Storage の共有キー認証に適用されます。 ファイルをステージングするための Microsoft Azure Blob Storage アクセスキー。
コンテナ名	Microsoft Azure Blob Storage に適用されます。 Azure Blob Storage アカウントのコンテナの名前。
ADLS Gen2 ストレージアカウント名	Microsoft Azure Data Lake Storage Gen2 の共有キー認証とサービスプリンシパル認証に適用されます。 ファイルをステージングするための Microsoft Azure Data Lake Storage Gen2 ストレージアカウントの名前。
ADLS Gen2 アカウントキー	Microsoft Azure Data Lake Storage Gen2 の共有キー認証に適用されます。 ファイルをステージングするための Microsoft Azure Data Lake Storage Gen2 アクセスキー。
クライアント ID	Microsoft Azure Data Lake Storage Gen2 のサービスプリンシパル認証とマネージド ID 認証に適用されます。 アプリケーションのクライアント ID。 サービスプリンシパル認証を使用するには、Azure Active Directory に登録されているアプリケーションのアプリケーション ID またはクライアント ID を入力します。 マネージド ID 認証を使用するには、ユーザー割り当てマネージド ID のクライアント ID を入力します。マネージド ID がシステム割り当てである場合は、フィールドを空のままにします。

プロパティ	説明
クライアントシークレット	Microsoft Azure Data Lake Storage Gen2 のサービスプリンシパル認証に適用されます。 アプリケーションのクライアントシークレット。
テナント ID	Microsoft Azure Data Lake Storage Gen2 のサービスプリンシパル認証に適用されます。 アプリケーションのディレクトリ ID またはテナント ID。
ファイルシステム名	Microsoft Azure Data Lake Storage Gen2 に適用されます。 Microsoft Azure Data Lake Storage Gen2 アカウントのファイルシステムの名前。
Blob エンドポイント	Microsoft Azure エンドポイントのタイプ。 次のいずれかのエンドポイントを選択します。 - core.windows.net。Azure エンドポイントに接続します。 - core.usgovcloudapi.net。米国政府の Microsoft Azure Synapse SQL エンドポイントに接続します。 - core.chinacloudapi.cn。中国地域の Microsoft Azure Synapse SQL エンドポイントに接続します。 デフォルトは core.windows.net です
VNet ルール	仮想ネットワーク（VNet）にある Microsoft Azure Synapse SQL エンドポイントへの接続を有効にします。 サーバーレスランタイム環境を使用している場合、仮想ネットワーク内にある Microsoft Azure Synapse SQL エンドポイントに接続することはできません。

Microsoft Dynamics 365 Mass Ingestion 接続のプロパティ

Microsoft Dynamics 365 Mass Ingestion 接続をセットアップする際には、接続プロパティを設定する必要があります。

Microsoft Dynamics 365 Mass Ingestion の接続には、Microsoft Dynamics 365 データにアクセスするために、Azure Active Directory（Azure AD）に登録されているネイティブアプリケーションが必要です。接続を設定する前に、Azure AD にアプリケーションを登録して、接続が Microsoft Dynamics 365 データにアクセスできるようにする必要があります。Azure AD にアプリケーションを登録する方法の詳細については、Microsoft documentation を参照してください。

Microsoft Dynamics 365 Mass Ingestion 接続のプロパティは、接続に指定した認証方法によって異なります。接続を作成する際に、次の認証方法のいずれかを選択できます。

- **OAuth 2.0 ユーザー名パスワードフロー**: Microsoft Dynamics 365 アカウントのログイン資格情報と、Azure AD に登録されているアプリケーションのクライアント ID を使用して、接続を認証します。
- **OAuth 2.0 クライアントシークレットフロー**: Azure AD に登録されているアプリケーションのクライアント ID とクライアントシークレットを使用して、接続を認証します。
- **OAuth 2.0 JWT ベアラーフロー**: X509 公開鍵基盤（PKI）証明書と JSON Web Token（JWT）を使用して接続を認証します。クライアントシークレットや Microsoft Dynamics 365 アカウントのログイン資格情報などの機密情報を共有せずに、Microsoft Dynamics 365 への安全なアクセスを取得するには、この認証方法を使用します。

OAuth 2.0 ユーザー名パスワードフロー認証の接続プロパティ

次の表に、OAuth 2.0 ユーザー名パスワードフロー認証を使用して設定された Microsoft Dynamics 365 Mass Ingestion 接続の接続プロパティを示します。

接続プロパティ	説明
接続名	接続の名前。この名前は、組織内で一意にする必要があります。接続名には、英数字、スペース、および次の特殊文字を含めることができます。_ .+ - 名前の先頭または末尾のスペースはトリミングされ、名前の一部として保存されません。最大長は 100 文字です。接続名では大文字と小文字は区別されません。
説明	接続の説明（オプション）。最大長は 255 文字です。
タイプ	接続のタイプ。【Microsoft Dynamics 365 Mass Ingestion】接続タイプを選択します。
ランタイム環境	取り込みタスクを実行するランタイム環境の名前。 ランタイム環境として Secure Agent を指定する必要があります。 **注:** Hosted Agent やサーバーレスランタイム環境でアプリケーション取り込みタスクを実行することはできません。
ユーザー名	Microsoft Dynamics 365 アカウントのユーザー名。
パスワード	Microsoft Dynamics 365 アカウントのパスワード。
クライアント ID	Azure AD に登録されているアプリケーションのクライアント ID。
リソース URL	Microsoft Dynamics 365 組織の URL。 次の形式でリソース URL を入力する必要があります。 `https://<Microsoft_Dynamics_365_org_name>.api.crm8.dynamics.com`
OAuth トークン URL	Microsoft Dynamics 365 組織の OAuth 2.0 トークンエンドポイント。Azure AD に登録されているアプリケーションは、アクセストークン要求をこのエンドポイントに送信します。 このフィールドには、次の値を入力する必要があります。 `https://login.windows.net/common/oauth2/token`

注: OAuth 2.0 ユーザー名パスワードフロー認証方法の詳細については、Microsoft Dynamics 365 のドキュメントを参照してください。

OAuth 2.0 クライアントシークレットフロー認証の接続プロパティ

次の表に、OAuth 2.0 クライアントシークレットフロー認証を使用して設定された Microsoft Dynamics 365 Mass Ingestion 接続の接続プロパティを示します。

接続プロパティ	説明
接続名	接続の名前。この名前は、組織内で一意にする必要があります。接続名には、英数字、スペース、および次の特殊文字を含めることができます。_ .+ - 名前の先頭または末尾のスペースはトリミングされ、名前の一部として保存されません。最大長は 100 文字です。接続名では大文字と小文字は区別されません。
説明	接続の説明（オプション）。最大長は 255 文字です。
タイプ	接続のタイプ。Oracle Database Ingestion 接続の場合、タイプは［Microsoft Dynamics 365 Mass Ingestion］でなければなりません。
ランタイム環境	取り込みタスクを実行するランタイム環境の名前。 ランタイム環境として Secure Agent を指定する必要があります。 **注:** Hosted Agent やサーバーレスランタイム環境でアプリケーション取り込みタスクを実行することはできません。
クライアント ID	Azure AD に登録されているアプリケーションのクライアント ID。
クライアントシークレット	Azure AD に登録されているアプリケーションのクライアントシークレット。
リソース URL	Microsoft Dynamics 365 組織の URL。 次の形式でリソース URL を入力する必要があります。 `https://<Microsoft_Dynamics_365_org_name>.api.crm8.dynamics.com`
OAuth トークン URL	Microsoft Dynamics 365 組織の OAuth 2.0 トークンエンドポイント。Azure AD に登録されているアプリケーションは、アクセストークン要求をこのエンドポイントに送信します。 このフィールドには、次の値を入力する必要があります。 `https://login.microsoftonline.com/<tentant_id>/oauth2/token`

注: OAuth 2.0 クライアントシークレットフロー認証方法の詳細については、Microsoft Dynamics 365 のドキュメントを参照してください。

OAuth 2.0 JWT ベアラーフロー認証の接続プロパティ

次の表に、OAuth 2.0 JWT ベアラーフロー認証を使用して設定された Microsoft Dynamics 365 Mass Ingestion 接続の接続プロパティを示します。

接続プロパティ	説明
接続名	接続の名前。この名前は、組織内で一意にする必要があります。接続名には、英数字、スペース、および次の特殊文字を含めることができます。_ .+ - 名前の先頭または末尾のスペースはトリミングされ、名前の一部として保存されません。最大長は 100 文字です。接続名では大文字と小文字は区別されません。
説明	接続の説明（オプション）。最大長は 255 文字です。

接続プロパティ	説明
タイプ	接続のタイプ。Oracle Database Ingestion 接続の場合、タイプは［Microsoft Dynamics 365 Mass Ingestion］でなければなりません。
ランタイム環境	取り込みタスクを実行するランタイム環境の名前。 ランタイム環境として Secure Agent を指定する必要があります。 **注**: Hosted Agent やサーバーレスランタイム環境でアプリケーション取り込みタスクを実行することはできません。
クライアント ID	Azure AD に登録されているアプリケーションのクライアント ID。
証明書の署名	X509 証明書の SHA-1 フィンガープリントを表す 16 進値をエンコードする Base64URL 文字列。
キーストアのパス	JSON Web Token（JWT）を検証して Microsoft Dynamics 365 との安全な接続を確立するために必要な X509 証明書を含むキーストアファイルへの絶対パス。 キーストアファイルは Java KeyStore （JKS）形式である必要があります。
キーストアのパスワード	キーストアファイルのパスワード。
プライベートキーのエイリアス	JWT の署名に使用されるプライベートキーのエイリアス名。
プライベートキーのパスワード	プライベートキーのパスワード。
JWT のオーディエンス	Azure AD に登録されているアプリケーションが検証のために JWT を送信する宛先となる、Microsoft Dynamics 365 リソースサーバーの URL。 次の形式でアドレスを入力する必要があります。 `https://login.microsoftonline.com/<tentant_id>/oauth2/token`
リソース URL	Microsoft Dynamics 365 組織の URL。 次の形式でリソース URL を入力する必要があります。 `https://<Microsoft_Dynamics_365_org_name>.api.crm8.dynamics.com`
OAuth トークン URL	Microsoft Dynamics 365 組織の OAuth 2.0 トークンエンドポイント。Azure AD に登録されているアプリケーションは、アクセストークン要求をこのエンドポイントに送信します。 このフィールドには、次の値を入力する必要があります。 `https://login.microsoftonline.com/<tentant_id>/oauth2/token`

注: OAuth 2.0 クライアントシークレットフロー認証方法の詳細については、Microsoft Dynamics 365 のドキュメントを参照してください。

Microsoft SQL Server 接続のプロパティ

Microsoft SQL Server 接続をセットアップするときは、接続プロパティを設定します。

以下の表に、Microsoft SQL Server 接続のプロパティを示します。

プロパティ	説明
接続名	接続の名前。 各接続名は組織内で一意である必要があります。接続名には、英数字、スペース、および次の特殊文字を含めることができます。_ .+ -, 最大長は 255 文字です。
説明	接続の説明。最大長は 4000 文字です。
タイプ	接続タイプ。 リストから SQL Server を選択します。
ランタイム環境	タスクを実行するランタイム環境の名前。 Hosted Agent やサーバーレスランタイム環境でデータベース取り込みタスクを実行することはできません。
SQL Server のバージョン	Microsoft SQL Server データベースのバージョン。

プロパティ	説明
認証モード	Microsoft SQL Server にアクセスするための認証方法。 次のいずれかの方法を選択します。 - SQL Server 認証 Microsoft SQL Server へのアクセス時に、Microsoft SQL Server のユーザー名とパスワードを使用します。 - Windows 認証（非推奨）。Microsoft SQL Server にアクセスするには、Microsoft Windows 認証を使用します。このオプションは、Microsoft Windows を使用してデータ統合にアクセスでする際に使用できます。 このオプションを選択する場合、Microsoft SQL Server にアクセスするために資格情報を入力する必要はなく、Secure Agent サービスを開始するユーザーアカウントが、Microsoft SQL Server データベースで使用可能になっていることを確認します。 **注**: Windows 認証は、Linux でホストされる Microsoft SQL Server 2017 バージョンでは使用できません。サーバーレスランタイム環境を使用している場合、Windows 認証を設定することはできません。 - Active Directory パスワード。Microsoft Azure SQL Database で認証を行い、このデータベースにアクセスするための Azure Active Directory のユーザー名とパスワードを使用します。 - Windows 認証 v2。この認証方法を使用して、Linux または Windows マシンでホストされているエージェントを使用してデータ統合または一括取り込みから Microsoft SQL Server にアクセスします。 Linux でこのオプションを選択する場合は、ドメイン名と Microsoft Windows 資格情報を入力して Microsoft SQL Server にアクセスします。 Windows でこのオプションを選択すると、エージェントは接続で指定されたユーザー資格情報のみを使用して接続をテストします。実行時に、エージェントは Secure Agent サービスを開始したユーザーの資格情報を使用します。Secure Agent サービスを開始するユーザーアカウントが、Microsoft SQL Server データベースで使用可能になっていることを確認します。 - Kerberos。Kerberos 認証を使用して Microsoft SQL Server に接続します。 Windows でこのオプションを選択する場合は、Secure Agent サービスを開始するユーザーアカウントが、Microsoft SQL Server データベースで使用可能になっていることを確認します。Microsoft SQL Server にアクセスする際に資格情報を入力する必要はありません。
ドメイン	Windows 認証 v2 に適用されます。 Windows ユーザーのドメイン名。
ユーザー名	データベースログインに使用するユーザー名。ユーザー名にセミコロンを含めることはできません。 Microsoft Azure SQL Database に接続するには、次の形式でユーザー名を指定します: `username@host` Windows で Windows 認証 v2 を使用する場合、ユーザー名は次のように使用されます。 - 設計時に、エージェントはここで指定したユーザー名を使用して接続をテストします。 - 実行時に、Microsoft SQL Server ドライバは、このフィールドで指定されたユーザー名を無視し、Secure Agent サービスを開始したユーザーの資格情報を使用します。 Linux で Windows 認証 v2 を使用する場合、ここで指定したユーザー名は、設計時と実行時の両方で使用されます。 **注**: Windows 認証モードを使用して Microsoft SQL Server にアクセスする場合、このプロパティは適用されません。

プロパティ	説明
パスワード	データベースログインに使用するパスワード。パスワードにセミコロンを含めることはできません。 Windows で Windows 認証 v2 を使用する場合、パスワードは次のように使用されます。 - 設計時に、エージェントはここで指定したパスワードを使用して接続をテストします。 - 実行時に、Microsoft SQL Server ドライバは、このフィールドで指定されたパスワードを無視し、Secure Agent サービスを開始したユーザーの資格情報を使用します。 Linux で Windows 認証 v2 を使用する場合、ここで指定したパスワードは、設計時と実行時の両方で使用されます。 **注**: Windows 認証モードを使用して Microsoft SQL Server にアクセスする場合、このプロパティは適用されません。
ホスト	データベースサーバーをホストするマシンの名前。 Microsoft Azure SQL Database に接続するには、完全修飾ホスト名を指定します。 例えば、`vmjcmwxsfboheng.westus.cloudapp.azure.com` のように指定します。。
ポート	データベースサーバーに接続するときに使用するネットワークポート番号。 デフォルトは 1433 です。
インスタンス名	Microsoft SQL Server データベースのインスタンス名。
データベース名	Microsoft SQL Server ターゲット接続のデータベース名。 データベースで大文字と小文字が区別される場合は、データベース名の大文字と小文字も区別されます。最大長は 100 文字です。 データベース名には英数字とアンダースコアのみを使用できます。
スキーマ	ターゲット接続に使用するスキーマ。
コードページ	データベースサーバーのコードページ。
暗号化方法	Secure Agent が、ドライバとデータベースサーバーとの間で送信されるデータの暗号化に使用する方法。暗号化方法を使用して、Microsoft Azure SQL Database に接続できます。 デフォルトは［なし］です。
暗号プロトコルバージョン	SSL 暗号化を有効にしたときに使用される暗号プロトコル。
サーバー証明書の検証	True に設定すると、Secure Agent が、データベースサーバーによって送信された証明書を検証します。 HostNameInCertificate パラメータを指定すると、Secure Agent は証明書内のホスト名も検証します。 False に設定すると、Secure Agent は、データベースサーバーによって送信された証明書を検証しません。
トラストストア	トラストストアファイルの場所と名前。トラストストアファイルには、ドライバが SSL サーバー認証に使用する認証局（CA）の一覧が含まれています。
信頼ストアのパスワード	トラストストアファイルの内容にアクセスするためのパスワード。

プロパティ	説明
証明書内のホスト名	セキュアデータベースをホストするマシンのホスト名。ホスト名を指定すると、Secure Agent は、SSL 証明書内のホスト名との接続に含まれているホスト名を検証します。
メタデータの詳細接続プロパティ	JDBC ドライバがメタデータを取得するための追加プロパティ。 複数のプロパティを指定する場合は、各キーと値のペアをセミコロンで区切ります。 例: `LoginTimeout=100` **注**: デフォルトの接続タイムアウトは 270 秒です。このプロパティを追加して、設計時の接続タイムアウトを設定します。
ランタイムの詳細接続プロパティ	ODBC ドライバがマッピングを実行するための追加のプロパティ。 複数のプロパティを指定する場合は、各キーと値のペアをセミコロンで区切ります。 例: `LoginTimeout=100` **注**: デフォルトの接続タイムアウトは 270 秒です。このプロパティを追加して、実行時の接続タイムアウトを設定します。

Microsoft Fabric OneLake 接続のプロパティ

Microsoft Fabric OneLake 接続をセットアップする際に、接続プロパティを設定します。

次の表に、Microsoft Fabric OneLake 接続のプロパティを示します。

プロパティ	説明
接続名	接続の名前。 各接続名は組織内で一意である必要があります。接続名には、英数字、スペース、および次の特殊文字を含めることができます。_ .+ -, 最大長は 255 文字です。
説明	接続の説明。最大長は 4000 文字です。
タイプ	Microsoft Fabric OneLake 接続タイプ。
ランタイム環境	タスクを実行するランタイム環境の名前。 Secure Agent を選択します。
ワークスペース名	Microsoft Fabric OneLake のワークスペースの名前。
レイクハウスのパス	ワークスペースに存在するレイクハウスのパスまたは名前。 パスは、次のいずれかの方法で指定できます。 - ワークスペース内のファイルにアクセスするには、*ルートディレクトリ（/）*を使用します。 - レイクハウスに存在するファイルにアクセスするには、*lakehouse name/Files* を使用します。

プロパティ	説明
認証タイプ	Microsoft Fabric OneLake にアクセスするための認証タイプ。 サービスプリンシパル認証は、クライアント ID、クライアントシークレット、およびテナント ID を使用して Microsoft Fabric OneLake に接続します。
クライアント ID	Azure Active Directory に登録されているアプリケーションのアプリケーション ID またはクライアント ID。
クライアントシークレット	Azure Active Directory に登録されているアプリケーションのクライアントシークレット。
テナント ID	アプリケーションを作成した Azure Active Directory インスタンスの ID。
Microsoft Fabric OneLake エンドポイント	接続先の Microsoft Fabric OneLake エンドポイントのタイプ。 デフォルトは［fabric.microsoft.com］です。

MongoDB Mass Ingestion 接続のプロパティ

MongoDB Mass Ingestion 接続をセットアップする際には、接続プロパティを設定する必要があります。

次の表に、MongoDB Mass Ingestion 接続のプロパティを示します。

接続プロパティ	説明
接続名	接続の名前。この名前では、大文字と小文字が区別されず、ドメイン内で一意にする必要があります。このプロパティは、接続を作成した後に変更できます。名前は 255 文字以内で指定し、空白および以下の特殊文字は使用できません。 ~ ` ! $ % ^ & * ( ) - + = { [}] | \ : ; " ' < , > . ? /
説明	オプション。接続の説明。説明は、4,000 文字を超えることはできません。
タイプ	接続タイプ。［MongoDB Mass Ingestion］を選択する必要があります。
ランタイム環境	タスクを実行するランタイム環境の名前。
ホストとポート	SRV レコード、または *host_name:port* ペアのカンマ区切りのリスト。 **注**: MongoDB レプリカセットモードを使用している場合は、回復機能用として複数のホスト名を入力できます。1 つのホストが使用できない場合は、指定した別のホストが使用されます。
SRV	**［ホストとポート］**プロパティで SRV レコードを指定した場合は、このチェックボックスをオンにします。
ユーザー名	データベースにログインするためのユーザー名。
パスワード	指定したデータベースユーザーのパスワード。

接続プロパティ	説明
認証データベース	指定ユーザーに関連付けられている認証データベースの名前。
レプリカセット名	ソースデータのレプリカを含む MongoDB サーバーで構成されているレプリカセットの名前。このフィールドは、MongoDB レプリカセットモードを使用している場合に関連します。
追加接続プロパティ	使用する 1 つ以上の追加の MongoDB 接続文字列オプション。キーと値のペアとしてプロパティを指定します。複数のプロパティを指定する場合は、アンパサンド記号（&）で区切ります。接続プロパティでは大文字小文字が区別されます。 例: `authSource=admin&replicaSet=rsprimary` MongoDB 接続文字列オプションの詳細については、以下を参照してください: https://www.mongodb.com/docs/v5.2/reference/connection-string/#connection-string-options

MQTT 接続のプロパティ

MQ Telemetry Transport（MQTT）接続をセットアップする際には、接続プロパティを設定する必要があります。

次の表に、MQTT 接続のプロパティを示します。

プロパティ	説明
接続名	接続の名前。 この名前では、大文字と小文字が区別されず、ドメイン内で一意にする必要があります。このプロパティは、接続を作成した後に変更できます。名前は 128 文字以内で指定し、空白および以下の特殊文字は使用できません。 ~ ` ! $ % ^ & * ( ) - + = { [}] | \ : ; " ' < , > . ? /
説明	オプション。接続を識別するために使用できる説明。 説明は、4,000 文字を超えることはできません。
タイプ	MQTT 接続タイプ。 接続タイプが見つからない場合は、**［アドオンコネクタ］**ページに移動し、コネクタをインストールしてください。
ランタイム環境	タスクを実行するランタイム環境の名前。
ブローカー URl	MQTT ブローカーの接続 URL。指定した場合、この値は、URL の主要部分で指定された URL を上書きします。 サンプル URL: `tcp://<IP Address>:<port>`

プロパティ	説明
クライアント ID	MQTT クライアントのクライアント識別子。 この値を空白のままにした場合、MQTT サーバーは一意の値を割り当てます。 このプロパティ値は、特定の MQTT サーバーに接続する MQTT クライアントごとに一意である必要があります。クライアント ID を変更せずにプロジェクトを共有した場合、切断や更新漏れといった接続の問題が発生する可能性があります。
ユーザー名	ブローカーへの接続時に使用するユーザー名。
パスワード	ブローカーへの接続時に使用するパスワード。
接続タイムアウト	MQTT サーバーへの接続が確立されるのをクライアントが待機する最大時間間隔。 デフォルトタイムアウトは 30 秒です。 値を 0 にするとタイムアウト処理は無効になります。つまり、クライアントはネットワーク接続が正常に確立されるか失敗するまで待機します。
SSL の使用	安全な送信のために SSL を使用するには、このオプションを有効にします。 SSL 認証を有効にする場合は、ストリーミング取り込みタスクで MQTT 接続を使用するためのキーストアとトラストストアの詳細を必ず指定してください。
キーストアファイル名	セキュアな通信に必要なキーと証明書が含まれます。
キーストアのパスワード	キーストアファイル名のパスワード。
キーストアのタイプ	使用するキーストアのタイプ。 キーストアタイプによって、キーストア情報のストレージとデータ形式、およびキーストア内のプライベートキーを保護するために使用されるアルゴリズムを定義します。 次のいずれかのタイプを使用してください: - JKS。プライベートキーと証明書を格納します。 - PKCS12。プライベートキー、秘密鍵、証明書を格納します。
トラストストアのファイル名	トラストストアファイルのファイル名。
トラストストアのパスワード	トラストストアファイル名のパスワード。
トラストストアのタイプ	使用するトラストストアのタイプ。 次のいずれかのタイプを使用してください: - JKS - PKCS12
TLS プロトコル	使用するトランスポートプロトコル。 次のいずれかのタイプを使用してください: - SSL - SSLv3 - TLS - TLSv1 - TLSv1.1 - TLSv1.2

MySQL 接続のプロパティ

MySQL 接続をセットアップする際には、接続プロパティを設定します。

次の表に、MySQL 接続のプロパティを示します。

プロパティ	説明
接続名	接続の名前。 各接続名は組織内で一意である必要があります。接続名には、英数字、スペース、および次の特殊文字を含めることができます。_ .+ -, 最大長は 255 文字です。
説明	接続の説明。最大長は 4000 文字です。
タイプ	接続タイプ。 リストから MySQL を選択します。
ランタイム環境	タスクを実行するランタイム環境の名前。 **注**: Hosted Agent やサーバーレスランタイム環境でデータベース取り込みタスクを実行することはできません。
ユーザー名	データベースログインに使用するユーザー名。ユーザー名にセミコロンを含めることはできません。
パスワード	データベースログインに使用するパスワード。パスワードにセミコロンを含めることはできません。
ホスト	データベースサーバーをホストするマシンの名前。
ポート	データベースサーバーに接続するときに使用するネットワークポート番号。 デフォルトは 3306 です。
データベース名	接続する MySQL データベースの名前。 **注**: データベース名は大文字と小文字が区別されます。 最大長は 64 文字です。データベース名には英数字とアンダースコアのみを使用してください。
コードページ	データベースサーバーのコードページ。

メタデータの詳細接続プロパティ	JDBC ドライバがメタデータを取得するための追加プロパティ。プロパティを次の形式で入力します。
	`<parameter name>=<parameter value>`
	複数のプロパティを入力する場合は、キーと値のペアをそれぞれセミコロンで区切ります。
	例えば、次のプロパティを入力して、接続をテストする際の接続タイムアウトを設定します。
	`connectTimeout=<value_in_miliseconds>`
	注: デフォルトの接続タイムアウトは 270000 ミリ秒です。

ランタイムの詳細接続プロパティ	ODBC ドライバが取り込みジョブを実行するための追加のプロパティ。 複数のプロパティを指定する場合は、各キーと値のペアをセミコロンで区切ります。

Netezza 接続のプロパティ

Netezza 接続をセットアップする際には、接続プロパティを設定する必要があります。

以下の表に、Netezza 接続のプロパティを示します。

接続プロパティ	説明
接続名	接続の名前。 各接続名は組織内で一意である必要があります。接続名には、英数字、スペース、および次の特殊文字を含めることができます。_ .+ -, 最大長は 255 文字です。
説明	接続の説明。最大長は 4000 文字です。
タイプ	Netezza。
ランタイム環境	タスクを実行するランタイム環境の名前。 Secure Agent を指定します。
データベース	Netezza データベースの名前。
スキーマ名	Netezza ソースまたはターゲットに使用されるスキーマ。 スキーマ名は大文字と小文字が区別されます。
サーバ名	Netezza データベースホスト名。
ポート	データベースサーバーに接続するときに使用するネットワークポート番号。 デフォルトは 1521 です。
ドライバ	Netezza データベースへの接続に使用される Netezza ODBC ドライバ名、NetezzaSQL。
ランタイム追加接続設定	データを取得するために必要な追加のランタイム属性。 例: `securityLevel=preferredUnSecured;caCertFile =`
メタデータ追加接続設定	メタデータを取得するために、JDBC ドライバのオプションのプロパティに設定する値。
ユーザー名	データベースへのアクセスに必要な読み取りおよび書き込みデータベース権限を持つデータベースユーザー名。
パスワード	上記データベースユーザー名のパスワード。

NetSuite Mass Ingestion 接続のプロパティ

NetSuite Mass Ingestion 接続をセットアップする際には、接続プロパティを設定する必要があります。

注: 接続プロパティを設定する前に、SuiteAnalytics Connect JDBC ドライバをインストールし、NQjc.jar ファイルを次のディレクトリにコピーします。 `<Secure_Agent>\ext\connectors\thirdparty\informatica.netsuiteami`

SuiteAnalytics Connect JDBC ドライバのインストールの詳細については、「SuiteAnalytics Connect documentation」を参照してください。

次の表に、NetSuite Mass Ingestion 接続の接続プロパティを示します。

接続プロパティ	説明
接続名	接続の名前。この名前は、組織内で一意にする必要があります。接続名には、英数字、スペース、および次の特殊文字を含めることができます。_ .+ - 名前の先頭または末尾のスペースはトリミングされ、名前の一部として保存されません。最大長は 100 文字です。接続名では大文字と小文字は区別されません。
説明	接続の説明（オプション）。最大長は 255 文字です。
タイプ	接続のタイプ。[Netsuite Mass Ingestion] 接続タイプを選択します。
ランタイム環境	取り込みタスクを実行するランタイム環境の名前。 ランタイム環境として Secure Agent を指定する必要があります。 **注:** Hosted Agent やサーバーレスランタイム環境でアプリケーション取り込みタスクを実行することはできません。
電子メール ID	NetSuite アカウントのユーザー名。ユーザー名は、電子メールアドレスです。
パスワード	NetSuite アカウントのパスワード。
サービスホスト	SuiteAnalytics Connect サービスホストの名前。 このフィールドの値は、NetSuite の［SuiteAnalytics Connect **ドライバのダウンロード**］ページの **［構成］** セクションにある **［サービスホスト］** フィールドで指定した値と一致している必要があります。［SuiteAnalytics Connect **ドライバのダウンロード**］ページにアクセスするには、NetSuite にログインし、［設定］ポートレットの［SuiteAnalytics 接続のセットアップ］リンクをクリックします。
サービスポート	SuiteAnalytics Connect サーバーがリッスンしている TCP/IP ポート。デフォルトは 1708 です。
サービスデータソース	NetSuite データへのアクセスに使用するデータソース。以下のいずれかのデータソースを選択できます。 - NetSuite.com - NetSuite2.com デフォルトは NetSuite2.com です。 **注:** - 2022 年 8 月のリリースより前に設定された接続では、このフィールドのデフォルト値は NetSuite.com です。 - NetSuite2.com データソースを使用するには、NetSuite ユーザーアカウントに特定のロールと権限を設定する必要があります。NetSuite2.com データソースへのアクセスに必要なロールと権限の詳細については、「NetSuite documentation」を参照してください。
アカウント ID	NetSuite アカウント ID。 アカウント ID を検索するには、NetSuite にログインして、[Setup] > [Integration] > [Web Services Preferences] に移動します。 [Setup] メニューが使用できない場合は、[Support] > [Go to Suite Answers] > [Contact support by phone] に移動します。ページにアカウント ID が表示されます。

接続プロパティ	説明
ロール ID	NetSuite アカウントに関連付けられているロール ID。
追加接続プロパティ	NetSuite サービスデータソースへの接続に使用される SuiteAnalytics Connect Driver の追加プロパティ。<property>=<value>という形式でプロパティを指定します。複数のプロパティを指定する場合は、各プロパティと値のペアをセミコロン（;）で区切ります。 このフィールドでは、次の接続プロパティを指定できます。 - ValidateServerCertificate: SuiteAnalytics Connect サーバーから送信された証明書をドライバが検証するかどうかを指定します。SSL サーバー認証中に、SuiteAnalytics Connect サーバーは、信頼された認証機関（CA）によって発行された証明書を送信します。通常、必要な CA は Java トラストストアに含まれていますが、TrustStore プロパティを使用して指定することもできます。ValidateServerCertificate プロパティの有効な値は true と false です。 - TrustStore: サーバー認証に使用されるセキュリティ証明書を含んだ有効なトラストストアへのパスが含まれています。ValidateServerCertificate プロパティが false に設定されている場合、TrustStore プロパティは無視されます。 **注**: 追加接続プロパティの詳細については、「NetSuite documentation」を参照してください。

OPC UA 接続のプロパティ

OPC UA 接続をセットアップする際には、接続のプロパティを設定する必要があります。

以下の表に、OPC UA 接続のプロパティを示します。

プロパティ	説明
接続名	接続の名前。 この名前では、大文字と小文字が区別されず、ドメイン内で一意にする必要があります。このプロパティは、接続を作成した後に変更できます。名前は 128 文字以内で指定し、空白および以下の特殊文字は使用できません。~ ` ! $ % ^ & * ( ) - + = { [}] | \ : ; " ' < , > . ? /
説明	オプション。接続の説明。 説明は、4,000 文字を超えることはできません。
タイプ	OPC UA 接続タイプ。
ランタイム環境	タスクを実行するランタイム環境の名前。
エンドポイント URL	OPC UA サーバーに接続するための一意の URL。 エンドポイント URL は、サーバーの特定のインスタンスとセキュリティポリシータイプを特定します。有効なエンドポイント URL は、エンドポイントタイプ（opc.tcp）、エンドポイントホスト名（IP アドレス、URL、または DSN）、およびエンドポイントポート番号で構成されます。 例: `opc.tcp://opcuaserver.com:48010`

プロパティ	説明
セキュリティポリシー	OPC UA サーバーに接続するために使用されるセキュリティポリシー。 セキュリティポリシーパラメータは、OPC UA サーバーがサポートするセキュリティアルゴリズムを指定します。 次のいずれかのセキュリティポリシーを選択することができます。 - なし。セキュリティは提供されていません。 - Basic128Rsa15 - Basic256 - Basic256Sha256 - Aes128_Sha256_RsaOaep - Aes256_Sha256_RsaPss **注**: OPC Foundation は、OPC UA 仕様バージョン 1.04 の時点でセキュリティポリシー Basic128Rsa15 および Basic256 を非推奨にしました。これらのポリシーによって提供される暗号化は、安全性が低くなります。これらのセキュリティポリシーは、下位互換性を提供するためにのみ使用してください。
セキュリティモード	OPC UA サーバーに接続するために使用されるセキュリティモード。 セキュリティモードは、セキュリティポリシーが［なし］に設定されていない場合にのみ有効です。次のいずれかのセキュリティポリシーを選択することができます。 - 署名。暗号化されていないデータを転送しますが、データの整合性を検証できるデジタル署名を使用します。 - SignAndEncrypt。署名および暗号化されたデータを転送します。
アプリケーション URI	オプション。OPC UA アプリケーションが OPC UA サーバーに接続するために使用できる一意の識別子。 一意の ID は次の形式で入力します。 `urn:aaa:bbb` 例: `urn:nifi:opcua` 一意の識別子は、OPC UA クライアント証明書のサブジェクト代替名の URI と一致する必要があります。
クライアントキーストアの場所	オプション。OPC UA サーバーのプライベートキーと証明書を含むキーストアファイルの絶対パスおよびファイル名。 このパスは次の形式で入力します。 `/root/opcua/client.jks` キーストアにはプライベートキーと証明書のキーペアエントリが 1 つだけ含まれている必要があります。複数のキーペアが存在する場合は、最初のエントリが使用されます。
クライアントキーストアパスワード	オプション。クライアントキーストアのパスワード。
サーバー認証が必要	オプション。クライアント証明書のサーバー認証、サーバー証明書のクライアント認証、またはその両方が必要な場合は有効にします。
トラストストアの場所	オプション。信頼済みの証明書を含むトラストストアファイルの絶対パス。 このパスは次の形式で入力します。 `/root/opcua/trust.jks`
トラストストアパスワード	トラストストアファイルのパスワード。

プロパティ	説明
認証ポリシー	接続を確立するために必要な認証設定。 以下のいずれかの認証ポリシーを選択することができます。 - Anon. 匿名認証。匿名トークンは、ユーザー認証を必要としないサーバーに関連付けられています。 - UserName。ユーザー名とパスワードトークンは、Windows などのパスワードベースのシステムを使用しているサーバーに関連付けられています。
ユーザ名	認証ポリシーに UserName を選択した場合に、OPC UA サーバーにアクセスするためのユーザー名。
パスワード	認証ポリシーに UserName を選択した場合に、OPC UA サーバーにアクセスするためのパスワード。

Oracle Cloud Object Storage 接続プロパティ

データベース取り込みタスクの Oracle Cloud Object Storage 接続を定義するときは、接続プロパティを設定する必要があります。

次の表に、Oracle Cloud Object Storage 接続プロパティを示します。

プロパティ	説明
接続名	接続の名前。 この名前は、組織内で一意にする必要があります。接続名には、英数字、スペース、および次の特殊文字を含めることができます: _ . + - , 最大長は 255 文字です。
説明	接続の説明（オプション）。最大長は 4000 文字です。
タイプ	接続のタイプ。Oracle Cloud Object Storage Database Ingestion 接続の場合、タイプは Oracle Cloud Object Storage であることが必要です。
ランタイム環境	データベース取り込みタスクを実行するランタイム環境の名前。ランタイム環境は、Administrator で定義します。
認証タイプ	ファイルをステージングする Oracle Cloud Object Storage に接続するために使用する認証タイプ。 次のいずれかのオプションを選択します。 - 簡易認証。API キーベース認証。 - ConfigFile 認証。ID 資格情報の詳細は、構成ファイルを通じて提供されます。
ユーザー	認証タイプとして簡易認証を選択した場合は、キーペアを追加するユーザーの Oracle Cloud Identifier（OCID）を指定します。
フィンガープリント	認証タイプとして簡易認証を選択した場合は、パブリックキーのフィンガープリントを指定します。
テナンシー	認証タイプとして簡易認証を選択した場合は、テナンシーの Oracle Cloud Identifier（OCID）（OCI アカウントのグローバルで一意の名前）を指定します。

プロパティ	説明
PrivateKey ファイルの場所	認証タイプとして簡易認証を選択した場合は、Secure Agent マシン上のプライベートキーファイルの場所を.PEM 形式で指定します。
構成ファイルの場所	認証タイプとして ConfigFile 認証を選択した場合は、Secure Agent マシン上の構成ファイルの場所を指定します。 絶対パスを入力します。 値を入力しない場合は、<システムのデフォルトの場所>/.oci/config を使用して構成ファイルが取得されます。
プロファイル名	認証タイプとして ConfigFile 認証を選択した場合は、使用する構成ファイル内のプロファイルの名前を指定します。 デフォルトは DEFAULT です。
バケット名	Oracle Cloud Storage バケット名。 バケットには、オブジェクトとファイルが含まれます。
フォルダパス	指定した Oracle Cloud Storage バケットにあるフォルダへのパス。 次はその例です: bucket/Dir_1/Dir_2/FileName.txt。ここで、Dir_1/Dir_2 はフォルダパスです。
リージョン	バケットがある Oracle Cloud Object Storage リージョン。

Oracle Database Ingestion 接続のプロパティ

データベース統合タスクの Oracle Database Ingestion 接続を定義するときは、接続プロパティを設定する必要があります。

以下の表に、接続のプロパティを示します。

プロパティ	説明
接続名	接続の名前。この名前は、組織内で一意にする必要があります。接続名には、英数字、スペース、および次の特殊文字を含めることができます。_ .+ - 名前の先頭または末尾のスペースはトリミングされ、名前の一部として保存されません。最大長は 100 文字です。接続名では大文字と小文字は区別されません。
説明	接続の説明（オプション）。最大長は 255 文字です。
タイプ	接続のタイプ。Oracle Database Ingestion 接続の場合、タイプは【Oracle Database Ingestion】でなければなりません。
ランタイム環境	データベース統合タスクを実行するランタイム環境の名前。ランタイム環境は、管理者で定義します。

プロパティ	説明
ユーザー名	Oracle データベースログインに使用するユーザー名。ユーザー名にセミコロンを含めることはできません。
パスワード	Oracle データベースログインに使用するパスワード。パスワードにセミコロンを含めることはできません。
ホスト	データベースサーバーのホスト名。
ポート	データベースサーバーに接続するときに使用するネットワークポート番号。デフォルトは 1521 です。
サービス名	Oracle データベースを一意に識別するサービス名またはシステム ID（SID）。Oracle データベースに接続するための SID を;SID=<ORACLE_SID>の形式で指定します。先頭のセミコロン（;）も含めてください。
スキーマ	Oracle 接続に使用されるスキーマ。
コードページ	データベースサーバーのコードページ。データベース統合タスクでは、UTF-8 コードページを使用します。デフォルトは UTF-8 です。
暗号化方法	初期ロードジョブの場合、Secure Agent と Oracle データベースサーバー間でやり取りされるデータを暗号化するかどうかを決定します。 次のオプションがあります。 - SSL。データ暗号化に SSL を使用してセキュアな接続を確立します。Oracle データベースサーバーが SSL を設定できない場合、接続は失敗します。 - **暗号化なし**。SSL を使用せずに接続を確立します。データは暗号化されません。 デフォルトは［暗号化なし］です。
暗号プロトコルバージョン	暗号化方法として SSL を選択した場合は、暗号化接続で使用する、サーバーでサポートされている 1 つの暗号化プロトコルまたは暗号化プロトコルのリストを指定する必要があります。次のオプションがあります。 - SSLv2 - SSLv3 - TLSv1.2 デフォルトは TLSV1.2 です。
サーバー証明書の検証	暗号化方法として SSL を選択した場合、Secure Agent が Oracle データベースサーバーから送信されたサーバー証明書を検証するかどうかを制御します。 - True。サーバー証明書を検証します。 - False。サーバー証明書を検証しません。 デフォルトは False です。 **［証明書内のホスト名］**プロパティを指定すると、Secure Agent は証明書内のホスト名も検証します。

プロパティ	説明
トラストストア	暗号化方法として SSL を選択し、サーバー証明書の検証を有効にした場合は、クライアントが SSL 認証のために信頼する認証局（CA）のリストを含むトラストストアファイルのパスと名前を指定します。
トラストストアのパスワード	暗号化方法として SSL を選択し、サーバー証明書の検証を有効にした場合は、トラストストアファイルのコンテンツにアクセスするためのパスワードを指定します。
証明書内のホスト名	暗号化方法として SSL を選択し、サーバー証明書の検証を有効にした場合は、セキュリティを強化するために、Oracle データベースをホストするマシンのホスト名を指定します。Secure Agent は、SSL 証明書のホスト名との接続に含まれるホスト名を検証します。
キーストア	暗号化方法として SSL を選択し、Oracle データベースサーバーでクライアント認証が有効になっている場合は、キーストアファイルのパスと名前を指定します。キーストアファイルには、クライアントが、Oracle サーバーの証明書要求に応答して送信する証明書が含まれます。
キーストアのパスワード	暗号化方法として SSL を選択し、Oracle データベースサーバーでクライアント認証が有効になっている場合は、キーストアファイルのパスワードを指定します。
キーパスワード	暗号化方法として SSL を選択し、Oracle データベースサーバーでクライアント認証が有効になっている場合は、キーストアファイルのキーのパスワードを指定します。キーのパスワードがキーストアファイルと異なる場合は、このプロパティを使用します。
データベース接続文字列	OCI が Oracle への接続に使用する TNS 名、Oracle Net のキーワードと値のペア、または SQL 接続文字列 URL。
TDE ウォレットディレクトリ	Oracle 透過的データ暗号化（TDE）に使用される Oracle ウォレットファイルを含むディレクトリへのパス。このプロパティ値は、TDE 暗号化テーブルスペースから変更データをキャプチャし、次のいずれかの条件が当てはまる場合にのみ指定してください。 - Oracle ウォレットはデータベースで使用できません。 - Oracle データベースは、Oracle REDO ログから離れたサーバーで実行されています。 - ウォレットディレクトリがデータベースホストのデフォルトの場所にないか、ウォレット名が ewallet.p12 のデフォルト名ではありません。 - ウォレットディレクトリは、Secure Agent ホストでは使用できません。

プロパティ	説明
TDE ウォレットパスワード	Oracle TDE ウォレットにアクセスしてマスターキーを取得するために必要な、クリアテキストのパスワード。Oracle ソースデータベースの TDE 暗号化テーブルスペースから変更データを取得する必要がある場合は、このプロパティ値が必要です。
代替ディレクトリ	Oracle サーバー上の REDO ログのサーバーパスプレフィックスの代替となるローカルパスプレフィックス。この代替ローカルパスは、ログリーダーが Oracle サーバーとは別のシステムで実行されていて、別のマッピングを使用して REDO ログファイルにアクセスする場合に必要になります。このプロパティは次の状況で使用します。 - REDO ログは共有ディスクに存在します。 - REDO ログは、Oracle システムとは別のシステムにコピーされています。 - アーカイブ REDO ログには、別の NFS マウントを使用してアクセスします。 Oracle Automatic Storage Management（ASM）を使用して REDO ログを管理する場合は、この文を使用しないでください。 次の形式で 1 つまたは複数の置換を定義できます。 *server_path_prefix*,*local_path_prefix*;*server_path_prefix*,*local_path_prefix*;... **注**: このプロパティは、Oracle ターゲットには適用されません。
リーダーアクティブログマスク	Oracle データベースで REDO ログの多重化を使用しているときに、ログリーダーがアクティブな REDO ログを選択するために使用するマスク。ログリーダーは、アクティブ REDO ロググループ内のメンバ名とマスクを比較して、読み取るログを決定します。マスクでは、アスタリスク（*）ワイルドカードを使用して、0 個以上の文字を表すことができます。 マスクの最大長は 128 文字です。大文字小文字は Linux と UNIX システムでは区別されますが、Windows システムでは区別されません。 **注**: このプロパティは、Oracle ターゲットには適用されません。
リーダーアーカイブ保存先 1	アーカイブ REDO ログごとに複数のコピーを書き込むよう Oracle が設定されているときに、ログリーダーがアーカイブログを読み取るプライマリのログ保存先。Oracle LOG_ARCHIVE_DEST_*n* 初期化パラメータの *n* 値に対応する数値を入力します。ここで *n* は、1〜10 の値です。 [リーダーアーカイブ保存先 1] および [リーダーアーカイブ保存先 2] プロパティのいずれか一方のみを設定した場合、ログリーダーはそのプロパティ設定を使用します。どちらのプロパティも指定しない場合、アーカイブログクエリはログ保存先でフィルタされません。 **注**: このプロパティは、Oracle ターゲットには適用されません。

プロパティ	説明
リーダーアーカイブ保存先 2	プライマリ保存先が利用できないとき、またはプライマリ保存先にあるログが読み取れないとき、ログリーダーがアーカイブログを読み取るセカンダリのログ保存先。例えば、ログが破損または削除されている場合です。Oracle LOG_ARCHIVE_DEST_*n* 初期化パラメータの *n* 値に対応する数値を入力します。ここで *n* は、1～10 の値です。この値は通常、1 より大きい数値です。 **注**: このプロパティは、Oracle ターゲットには適用されません。
リーダー ASM 接続文字列	Oracle ASM 環境で、ソースデータベースのアクティブ REDO ログとアーカイブ REDO ログのストレージを管理する ASM インスタンスへの接続のためにログリーダーで使用される、TNS で定義された Oracle 接続文字列です。 **注**: このプロパティは、Oracle ターゲットには適用されません。
リーダー ASM ユーザー名	Oracle ASM 環境で、ソースデータベースのアクティブ REDO ログとアーカイブ REDO ログのストレージを管理する ASM インスタンスへの接続のためにログリーダーで使用される、Oracle ユーザー ID です。このユーザー ID には SYSDBA 権限または SYSASM 権限が必要です。SYSASM 権限を使用するには、**[SYSASM としてリーダー ASM 接続]** プロパティを「Y」に設定します。 **注**: このプロパティは、Oracle ターゲットには適用されません。
リーダー ASM パスワード	Oracle ASM 環境で、**[リーダー ASM ユーザー名]** パラメータに指定されているユーザーのクリアテキストのパスワード。ログリーダーは、このパスワードと ASM ユーザー名を使用して、ソースデータベースのアクティブ REDO ログとアーカイブ REDO ログのストレージを管理する ASM インスタンスに接続します。 **注**: このプロパティは、Oracle ターゲットには適用されません。
SYSASM としてリーダー ASM 接続	Oracle 11*g* ASM 以降を使用していて、ログリーダーが ASM インスタンスに接続するために SYSASM 権限を持つユーザー ID を使用する場合は、このチェックボックスをオンにします。また、**[リーダー ASM ユーザー名]** プロパティで SYSASM 権限を持つユーザー ID を指定します。SYSDBA 権限を持つユーザー ID を使用するには、このチェックボックスをオフにします。デフォルトでは、このチェックボックスはオフです。 **注**: このプロパティは、Oracle ターゲットには適用されません。

プロパティ	説明

リーダーモード	ログリーダーが読み取る Oracle REDO ログのソースとタイプを指定します。有効なオプションは以下のとおりです。
	- ACTIVE。アクティブおよびアーカイブ REDO ログを Oracle オンラインシステムから読み取ります。オプションで、**[リーダーアクティブログマスク]** プロパティを使用してアクティブ REDO ログをフィルタしたり、**[リーダーアーカイブ保存先 1]** および **[リーダーアーカイブ保存先 2]** プロパティを使用してアーカイブログの読み取り元となるアーカイブログ保存先を制限したりすることができます。
	- ARCHIVEONLY。アーカイブ REDO ログのみを読み取ります。オプションで、**[リーダーアーカイブ保存先 1]** および **[リーダーアーカイブ保存先 2]** プロパティを使用して、アーカイブログの読み取り元となるアーカイブログ保存先を制限できます。
	- ARCHIVECOPY。代替ファイルシステムにコピーされたアーカイブ REDO ログを読み取ります。初期ロードジョブと増分ロードジョブの組み合わせの場合は、Informatica グローバルカスタマサポートの指示に従って、ソースカスタムプロパティ pwx.cdcreader.oracle.reader.additional を、dir パラメータと file パラメータを指定して設定する必要もあります。
	このオプションは次の状況で使用できます。
	  - Oracle のアーカイブ REDO ログに直接アクセスするための権限がない。
	  - アーカイブ REDO ログが ASM に書き込まれているが、ASM にアクセスできない。
	  - データベースサーバーのアーカイブログ保持ポリシーによって、アーカイブログが十分長期間保持されない。
	このオプションを使用する場合、**[リーダーアーカイブ保存先 1]** および **[リーダーアーカイブ保存先 2]** プロパティは無視されます。
	デフォルトは ACTIVE です。
	注: このプロパティは、Oracle ターゲットには適用されません。

リーダースタンバイログマスク	Oracle 物理スタンバイデータベースで REDO ログの多重化を使用しているときに、ログリーダーがデータベースの REDO ログを選択するために使用するマスク。ログリーダーは、REDO ロググループ内のメンバ名とマスクを比較して、読み取るログを決定します。マスクでは、アスタリスク（*）ワイルドカードを使用して、0 個以上の文字を表すことができます。 マスクの最大長は 128 文字です。大文字小文字は Linux と UNIX システムでは区別されますが、Windows システムでは区別されません。 **注**: このプロパティは、Oracle ターゲットには適用されません。

プロパティ	説明
スタンバイ接続文字列	データベースが読み取り専用アクセスで開かれていない場合の変更のキャプチャ用に、ログリーダーがOracle 物理スタンバイデータベースへ接続するために使用する、TNS で定義された Oracle 接続文字列。 **注**: このプロパティは、Oracle ターゲットには適用されません。
スタンバイユーザー名	変更のキャプチャ用に、ログリーダーが Oracle 物理スタンバイデータベースへ接続するために使用するユーザー ID。このユーザー ID には SYSDBA 権限が必要です。 **注**: このプロパティは、Oracle ターゲットには適用されません。
スタンバイパスワード	変更のキャプチャ用に、ログリーダーが Oracle 物理スタンバイデータベースへ接続するために使用するパスワード。 **注**: このプロパティは、Oracle ターゲットには適用されません。
RAC メンバ	Oracle Real Application Cluster（RAC）内で、追跡可能なアクティブ REDO ログスレッド（*メンバ*）の最大数。RAC 環境でプライマリデータベースをサポートする Data Guard 物理スタンバイデータベースの場合、この値はプライマリデータベースのアクティブなスレッドの数です。 有効な値は 1〜100 です。デフォルトは 0 で、適切なログスレッド数が自動的に決定されます。この値がお使いの環境で適切でない場合は、このプロパティを 0 より大きい値に設定してください。 **注**: このプロパティは、Oracle ターゲットには適用されません。
BFILE アクセス	次の状況では、このチェックボックスをオンにします。 - BFILE アクセスを使用して、ローカル Oracle サーバーファイルシステム上の物理ディレクトリの REDO ログにアクセスする。BFILE アクセスは、Oracle ディレクトリオブジェクトを使用して、ファイルシステムの REDO ログにリモートアクセスします。この方法は、ASM や NFS マウントなどの他のログアクセス方法に代わるものです。 - Amazon Relational Database Service（RDS）for Oracle ソースがある。この場合、このオプションを使用すると、RDS にデプロイされたクラウドベースのデータベースインスタンスの REDO ログにアクセスできます。 デフォルトでは、このチェックボックスはオフです。 **注**: このプロパティは、Oracle ターゲットには適用されません。

Oracle Fusion Cloud Mass Ingestion 接続のプロパティ

Oracle Fusion Cloud Mass Ingestion 接続をセットアップする際には、接続プロパティを設定する必要があります。

注: Oracle Fusion Cloud Mass Ingestion 接続は、Oracle Fusion Cloud Applications スイートの Enterprise Resource Planning（ERP）モジュール、Human Capital Management（HCM）モジュール、および Oracle Supply Chain and Manufacturing（SCM）モジュールのデータのみにアクセスできます。

次の表に、Oracle Fusion Cloud Mass Ingestion 接続の接続プロパティを示します。

接続プロパティ	説明
接続名	接続の名前。この名前は、組織内で一意にする必要があります。接続名には、英数字、スペース、および次の特殊文字を含めることができます。_ .+ - 名前の先頭または末尾のスペースはトリミングされ、名前の一部として保存されません。最大長は 100 文字です。接続名では大文字と小文字は区別されません。
説明	接続の説明（オプション）。最大長は 255 文字です。
タイプ	接続のタイプ。[Oracle Fusion Cloud Mass Ingestion] 接続タイプを選択します。
ランタイム環境	取り込みタスクを実行するランタイム環境の名前。 ランタイム環境として Secure Agent を指定する必要があります。 **注**: Hosted Agent やサーバーレスランタイム環境でアプリケーション取り込みタスクを実行することはできません。
認証	接続の認証方法。 デフォルトでは、接続は基本認証方式を使用します。
ユーザー名	Oracle Cloud アカウントのユーザー名。
パスワード	Oracle Cloud アカウントのパスワード。
サーバーの URL	アクセス先の Oracle Cloud サービスの URL。
API バージョン	接続に使用する Oracle Cloud REST API のバージョン。 BICC レプリケーションアプローチの場合はオプションです。

PostgreSQL 接続のプロパティ

PostgreSQL 接続をセットアップする際には、接続プロパティを設定します。

次の表に、PostgreSQL 接続のプロパティを示します。

プロパティ	説明
接続名	接続の名前。 各接続名は組織内で一意である必要があります。接続名には、英数字、スペース、および次の特殊文字を含めることができます。_ .+ -, 最大長は 255 文字です。
説明	接続の説明。最大長は 4000 文字です。
タイプ	接続タイプ。 リストから PostgreSQL を選択します。
ランタイム環境	タスクを実行するランタイム環境の名前。 Hosted Agent やサーバーレスランタイム環境でデータベース取り込みタスクを実行することはできません。
ホスト名	接続先の PostgreSQL サーバーのホスト名。
ポート	接続先の PostgreSQL サーバーのポート番号。 デフォルトは 5432 です。
スキーマ	スキーマ名です。 スキーマ名を指定しない場合、データ統合でソースオブジェクトをインポートするときに、データベース内で使用できるすべてのスキーマが一覧表示されます。
データベース	PostgreSQL データベース名。
ユーザー名	PostgreSQL データベースにアクセスするためのユーザー名。
パスワード	PostgreSQL データベースユーザー名のパスワード。
暗号化方法	Secure Agent と PostgreSQL データベースサーバー間でやり取りされるデータを暗号化するかどうかを決定します。 次のいずれかの暗号化方法を選択します。 - noEncryption。SSL を使用せずに接続を確立します。データは暗号化されません。 - SSL。SSL を使用して接続を確立します。データは SSL を使用して暗号化されます。PostgreSQL データベースサーバーが SSL を設定できない場合、接続は失敗します。 - requestSSL。SSL を使用して接続の確立を試みます。PostgreSQL データベースサーバーが SSL を設定できない場合、Secure Agent が暗号化されていない接続を確立します。 デフォルトは noEncryption です。
サーバー証明書の検証	暗号化方式として［SSL］または［requestSSL］を選択した場合に適用されます。 ［サーバー証明書の検証］オプションを選択した場合は、Secure Agent で、PostgreSQL データベースサーバーから送信されたサーバー証明書が検証されます。［証明書内のホスト名］プロパティを指定すると、Secure Agent では証明書内のホスト名も検証されます。

プロパティ	説明
TrustStore	暗号化方法として SSL または requestSSL を選択し、［サーバー証明書の検証］オプションを選択した場合に適用。 トラストストアファイルのパスおよび名前で、PostgreSQL クライアントが信頼する認証局（CA）のリストが含まれます。
トラストストアのパスワード	暗号化方法として SSL または requestSSL を選択し、［サーバー証明書の検証］オプションを選択した場合に適用。 SSL 証明書を含むトラストストアファイルにアクセスするためのパスワード。
証明書内のホスト名	暗号化方法として SSL または requestSSL を選択し、［サーバー証明書の検証］オプションを選択した場合にオプションで適用。 追加のセキュリティを提供するためのホスト名。Secure Agent は、SSL 証明書のホスト名との接続に含まれるホスト名を検証します。
キーストア	暗号化方法として SSL を選択し、PostgreSQL データベースサーバーでクライアント認証を有効にしている場合に適用。 キーストアのパスおよびファイル名。キーストアファイルには、PostgreSQL クライアントが、PostgreSQL サーバーの証明書要求に応答して送信する証明書が含まれます。
キーストアのパスワード	暗号化方法として SSL を選択し、PostgreSQL データベースサーバーでクライアント認証を有効にしている場合に適用。 通信を安全に行うために必要なキーストアファイルのパスワード。
キーパスワード	暗号化方法として SSL を選択し、PostgreSQL データベースサーバーでクライアント認証を有効にしている場合に適用。 キーストアファイルに含まれる個別のキーに、キーストアファイルとは別のパスワードが設定されている場合に必要になります。
追加接続プロパティ	使用する追加接続パラメータ。 接続パラメータは、キー値のペアをセミコロンで区切って指定します。
暗号プロトコルバージョン	暗号化方式として［SSL］または［requestSSL］を選択した場合は必須です。 暗号化された接続で使用する暗号化プロトコルまたは暗号化プロトコルのリスト。 次のいずれかのプロトコルを選択できます。 - SSLv3 - TLSv1_2 デフォルトは TLSv1_2 です。

REST V2 接続のプロパティ

REST V2 接続をセットアップする際には、接続プロパティを設定する必要があります。

次の表に、標準認証タイプ接続の REST V2 接続プロパティを示します。

接続プロパティ	説明
接続名	接続の名前。 各接続名は組織内で一意である必要があります。接続名には、英数字、スペース、および次の特殊文字を含めることができます。_ .+ -, 最大長は 255 文字です。
説明	接続の説明。最大長は 4000 文字です。
タイプ	REST V2 接続タイプ。
ランタイム環境	タスクを実行するランタイム環境の名前。 Secure Agent、Hosted Agent、またはサーバーレスランタイム環境を選択します。 Hosted Agent やサーバーレスランタイム環境でストリーミング取り込みタスクを実行することはできません。
認証	REST V2 コネクタが REST エンドポイントに接続するために使用する必要のある認証方法。 **［標準］**を選択します。
認証タイプ	標準認証を選択した場合に使用できる認証タイプ。 以下のいずれかの認証タイプを選択できます。 - 基本 - ダイジェスト - OAuth - なし デフォルトは **［なし］**です。
認証ユーザー ID	［基本］認証を選択したときに Web サービスアプリケーションにログインするためのユーザー名。 ダイジェスト認証は適用されません。
認証パスワード	基本認証を選択したときにユーザー名に関連付けられたパスワード。 ダイジェスト認証は適用されません。
OAuth コンシューマキー	Web サービスアプリケーションに関連付けられるクライアントキー。 認証タイプが［OAuth］の場合にのみ必要です。
OAuth コンシューマシークレット	Web サービスアプリケーションに接続するためのクライアントパスワード。 認証タイプが［OAuth］の場合にのみ必要です。
OAuth トークン	Web サービスアプリケーションに接続するためのアクセストークン。 認証タイプが［OAuth］の場合にのみ必要です。
OAuth トークンシークレット	OAuth トークンに関連付けられるパスワード。 認証タイプが［OAuth］の場合にのみ必要です。

接続プロパティ	説明
Swagger ファイルパス	Swagger ファイルまたは OpenAPI ファイルのパス。 次のいずれかのファイルパスを指定できます。 - ファイル名を含む絶対パス - ホストされている URL Swagger ファイルまたは OpenAPI ファイルの絶対パスを指定する場合、ファイルは Secure Agent マシン上に存在する必要があります。 ホストされた URL は、それ以上の認証とリダイレクトを要求せずにファイルのコンテンツを返す必要があります。 例えば、Swagger ファイルのパスは次のようになります。 `C:\swagger\sampleSwagger.json` ユーザーにはフォルダとファイルの読み取り権限が必要です。
トラストストアファイルパス	REST API との一方向または双方向の安全な接続を確立するための TLS 証明書を含むトラストストアファイルの絶対パス。各 Secure Agent マシンで使用可能なディレクトリパスを指定します。 トラストストアファイル名とパスワードを JVM オプションとして設定することもできますし、証明書を次のディレクトリにインポートすることもできます。 `<Secure Agent のインストールディレクトリ>\jre\lib\security\cacerts` サーバーレスランタイム環境の場合、サーバーレスエージェントディレクトリでトラストストアファイルパスを指定します。 例: `/home/cldagnt/SystemAgent/serverless/configurations/ssl_store/<cert_name>.jks`
トラストストアのパスワード	SSL 証明書を含むトラストストアファイルのパスワード。 トラストストアのパスワードを JVM オプションとして設定することもできます。
キーストアファイルパス	REST API との双方向の安全な接続を確立するために必要なキーと証明書を含むキーストアファイルの絶対パス。各 Secure Agent マシンで使用可能なディレクトリパスを指定します。 キーストアファイル名と格納場所を JVM オプションとして設定することもできます。また、証明書を任意のディレクトリにインポートすることもできます。 サーバーレスランタイム環境の場合、サーバーレスエージェントディレクトリでキーストアファイルパスを指定します。 例: `/home/cldagnt/SystemAgent/serverless/configurations/ssl_store/<cert_name>.jks`
キーストアのパスワード	通信を安全に行うために必要なキーストアファイルのパスワード。 キーストアのパスワードを JVM オプションとして設定することもできます。
プロキシタイプ	プロキシのタイプ。以下のいずれかのオプションを選択することができます。 - プロキシなし。エージェントレベルまたは接続プロパティで設定されたプロキシサーバーをバイパスします。 - プラットフォームプロキシ。エージェントで設定されたプロキシを考慮します。 - カスタムプロキシ。接続プロパティで設定されたプロキシを考慮します。

接続プロパティ	説明
プロキシ設定	プロキシを設定するために必要な形式。 次の形式を使用してプロキシを設定できます: <ホスト>:<ポート> 認証されたプロキシサーバーを設定することはできません。
詳細フィールド	エージェントが REST エンドポイントに接続するときに使用する引数を入力します。 次の引数をセミコロン（;）で区切って指定できます。 - ConnectionTimeout。REST エンドポイントからの応答を取得するための待機時間（ミリ秒）。接続タイムアウトを過ぎると、接続は終了します。デフォルトはエンドポイント API で定義されているタイムアウトです。 **注**: REST V2 接続タイムアウトとエンドポイント API タイムアウトの両方が定義されている場合、接続は定義されている最短のタイムアウトで終了します。 - connectiondelaytime。REST エンドポイントに要求を送信するための遅延時間（ミリ秒）。デフォルトは 10000 です。 - retryattempts。応答で 400 および 500 シリーズのエラーコードが返された場合に接続が試行された回数。デフォルトは 3 です。再試行を無効にするには 0 を指定します。 - qualifiedSchema。選択したスキーマが修飾されているかどうかを指定します。デフォルトは false です。 例: `connectiondelaytime:10000;retryattempts:5` **注**: ストリーミング統合タスクでは、ConnectionTimeout および retryattempts のみが適用されます。

表 1. **［**OAuth 2.0 - **クライアント資格情報］認証の場合**

接続プロパティ	説明
アクセストークン URL	アプリケーションで設定されているアクセストークン URL。
クライアント ID	アプリケーションのクライアント ID。
クライアントシークレット	アプリケーションのクライアントシークレット。
スコープ	API エンドポイントでカスタムスコープが定義されている場合に、アクセス制御を指定します。スコープ属性をスペースで区切って入力します。例: `root_readonly root_readwrite manage_app_users`
アクセストークンパラメータ	アクセストークン URL で使用する追加パラメータ。パラメータは JSON 形式で定義する必要があります。 例: `[{"Name":"resource","Value":"https://<serverName>"}]`
クライアント認証	認証のためにクライアント ID およびクライアントシークレットを送信するオプションを、要求本文または要求ヘッダーのいずれかから選択します。 デフォルトは、**［本文でクライアント資格情報を送信する］**です。
アクセストークンの生成	上のフィールドで指定された情報に基づいて、アクセストークンを生成します。

接続プロパティ	説明
アクセストークン	アクセストークンの値を入力するか、**[アクセストークンの生成]** をクリックして、アクセストークンの値を指定します。 プロキシサーバーを介してアクセストークンの生成呼び出しを渡すには、Secure Agent レベルで認証されていないプロキシサーバーを設定する必要があります。REST V2 接続レベルのプロキシ設定は、アクセストークンの生成呼び出しには適用されません。
Swagger ファイルパス	Swagger ファイルまたは OpenAPI ファイルのパス。 次のいずれかのファイルパスを指定できます。 - ファイル名を含む絶対パス - ホストされている URL Swagger ファイルまたは OpenAPI ファイルの絶対パスを指定する場合、ファイルは Secure Agent マシン上に存在する必要があります。 ホストされた URL は、それ以上の認証とリダイレクトを要求せずにファイルのコンテンツを返す必要があります。 例えば、Swagger ファイルのパスは次のようになります。 `C:\swagger\sampleSwagger.json` ユーザーにはフォルダとファイルの読み取り権限が必要です。 **注**: ストリーミング統合タスクでは、Swagger ファイルパスとして Swagger 仕様ファイルのホストされた URL のみを使用できます。
トラストストアファイルパス	REST API との一方向または双方向の安全な接続を確立するための TLS 証明書を含むトラストストアファイルの絶対パス。各 Secure Agent マシンで使用可能なディレクトリパスを指定します。 トラストストアファイル名とパスワードを JVM オプションとして設定することもできますし、証明書を次のディレクトリにインポートすることもできます。 `<Secure Agent のインストールディレクトリ>\jre\lib\security\cacerts` サーバーレスランタイム環境の場合、サーバーレスエージェントディレクトリでトラストストアファイルパスを指定します。 例: `/home/cldagnt/SystemAgent/serverless/configurations/ssl_store/<cert_name>.jks`
トラストストアのパスワード	SSL 証明書を含むトラストストアファイルのパスワード。 トラストストアのパスワードを JVM オプションとして設定することもできます。
キーストアファイルパス	REST API との双方向の安全な接続を確立するために必要なキーと証明書を含むキーストアファイルの絶対パス。各 Secure Agent マシンで使用可能なディレクトリパスを指定します。 キーストアファイル名と格納場所を JVM オプションとして設定することもできます。また、証明書を任意のディレクトリにインポートすることもできます。 サーバーレスランタイム環境の場合、サーバーレスエージェントディレクトリでキーストアファイルパスを指定します。 例: `/home/cldagnt/SystemAgent/serverless/configurations/ssl_store/<cert_name>.jks`
キーストアのパスワード	通信を安全に行うために必要なキーストアファイルのパスワードです。 キーストアのパスワードを JVM オプションとして設定することもできます。
プロキシタイプ	プロキシのタイプ。 以下のいずれかのオプションを選択することができます。 - プロキシなし: エージェントレベルまたは接続レベルで設定されたプロキシサーバーをバイパスします。 - プラットフォームプロキシ: エージェントで設定されたプロキシを考慮します。 - カスタムプロキシ: 接続プロパティで設定されたプロキシを考慮します。

接続プロパティ	説明
プロキシ構成	プロキシを設定するために必要な形式。 次の形式を使用してプロキシを設定できます: <ホスト>:<ポート> 認証されたプロキシサーバーを設定することはできません。
詳細フィールド	エージェントが REST エンドポイントに接続するときに使用する引数を入力します。 次の引数をセミコロン（;）で区切って指定できます。 - ConnectionTimeout。REST エンドポイントからの応答を取得するための待機時間（ミリ秒）。接続タイムアウトを過ぎると、接続は終了します。デフォルトはエンドポイント API で定義されているタイムアウトです。 **注**: REST V2 接続タイムアウトとエンドポイント API タイムアウトの両方が定義されている場合、接続は定義されている最短のタイムアウトで終了します。 - connectiondelaytime。REST エンドポイントに要求を送信するための遅延時間（ミリ秒）。デフォルトは 10000 です。 - retryattempts。応答で 400 および 500 シリーズのエラーコードが返された場合に接続が試行された回数。デフォルトは 3 です。再試行を無効にするには 0 を指定します。 - qualifiedSchema。選択したスキーマが修飾されているかどうかを指定します。デフォルトは false です。 例: `connectiondelaytime:10000;retryattempts:5` **注**: ストリーミング統合タスクでは、ConnectionTimeout および retryattempts のみが適用されます。

表 2. ［OAuth 2.0 - 認証コード］認証の場合

接続プロパティ	説明
認証トークン URL	アプリケーションで設定されている認証サーバー URL。
アクセストークン URL	アプリケーションで設定されているアクセストークン URL。
クライアント ID	アプリケーションのクライアント ID。
クライアントシークレット	アプリケーションのクライアントシークレット。
スコープ	API エンドポイントでカスタムスコープが定義されている場合に、アクセス制御を指定します。スコープ属性をスペースで区切って入力します。 例: `root_readonly root_readwrite manage_app_users`
アクセストークンパラメータ	アクセストークン URL で使用する追加パラメータ。パラメータは JSON 形式で定義する必要があります。 例: `[{"Name":"resource","Value":"https://<serverName>"}]`

接続プロパティ	説明
認証コードパラメータ	認証トークン URL で使用する追加パラメータ。パラメータは JSON 形式で定義する必要があります。 例: `[{"Name":"max_age","Value":60},{"Name":"state","Value":"test"}]`
クライアント認証	認証のためにクライアント ID およびクライアントシークレットを送信するオプションを、要求本文または要求ヘッダーのいずれかから選択します。 デフォルトは、**[本文でクライアント資格情報を送信する]** です。
アクセストークンの生成	上のフィールドで指定された情報に基づいて、アクセストークンを生成し、トークンをリフレッシュします。
アクセストークン	アクセストークンの値を入力するか、**[アクセストークンの生成]** をクリックして、アクセストークンの値を指定します。 プロキシサーバーを介してアクセストークンの生成呼び出しを渡すには、Secure Agent レベルで認証されていないプロキシサーバーを設定する必要があります。REST V2 接続レベルのプロキシ設定は、アクセストークンの生成呼び出しには適用されません。
更新トークン	リフレッシュトークンの値を入力するか、**[アクセストークンの生成]** をクリックして、リフレッシュトークンの値を指定します。アクセストークンが有効でないか、有効期限切れの場合、Secure Agent は、リフレッシュトークンを使用して新しいアクセストークンを取得します。 リフレッシュトークンが期限切れの場合は、有効なリフレッシュトークンを指定するか、**[アクセストークンの生成]** をクリックして新しいリフレッシュトークンを生成します。
Swagger ファイルパス	Swagger ファイルまたは OpenAPI ファイルのパス。 次のいずれかのファイルパスを指定できます。 - ファイル名を含む絶対パス - ホストされている URL Swagger ファイルまたは OpenAPI ファイルの絶対パスを指定する場合、ファイルは Secure Agent マシン上に存在する必要があります。 ホストされた URL は、それ以上の認証とリダイレクトを要求せずにファイルのコンテンツを返す必要があります。 例えば、Swagger ファイルのパスは次のようになります。 `C:\swagger\sampleSwagger.json` ユーザーにはフォルダとファイルの読み取り権限が必要です。 **注**: ストリーミング統合タスクでは、Swagger ファイルパスとして Swagger 仕様ファイルのホストされた URL のみを使用できます。
トラストストアファイルパス	REST API との一方向または双方向の安全な接続を確立するための TLS 証明書を含むトラストストアファイルの絶対パス。各 Secure Agent マシンで使用可能なディレクトリパスを指定します。 トラストストアファイル名とパスワードを JVM オプションとして設定することもできますし、証明書を次のディレクトリにインポートすることもできます。 `<Secure Agent のインストールディレクトリ>\jre\lib\security\cacerts` サーバーレスランタイム環境の場合、サーバーレスエージェントディレクトリでトラストストアファイルパスを指定します。 例: `/home/cldagnt/SystemAgent/serverless/configurations/ssl_store/<cert_name>.jks`
トラストストアのパスワード	SSL 証明書を含むトラストストアファイルのパスワード。 トラストストアのパスワードを JVM オプションとして設定することもできます。

接続プロパティ	説明
キーストアファイルパス	REST API との双方向の安全な接続を確立するために必要なキーと証明書を含むキーストアファイルの絶対パス。各 Secure Agent マシンで使用可能なディレクトリパスを指定します。 キーストアファイル名と格納場所を JVM オプションとして設定することもできます。また、証明書を任意のディレクトリにインポートすることもできます。 サーバーレスランタイム環境の場合、サーバーレスエージェントディレクトリでキーストアファイルパスを指定します。 例: /home/cldagnt/SystemAgent/serverless/configurations/ssl_store/<cert_name>.jks
キーストアのパスワード	通信を安全に行うために必要なキーストアファイルのパスワードです。 キーストアのパスワードを JVM オプションとして設定することもできます。
プロキシタイプ	プロキシのタイプ。以下のいずれかのオプションを選択することができます。 - プロキシなし: エージェントレベルまたは接続レベルで設定されたプロキシサーバーをバイパスします。 - プラットフォームプロキシ: エージェントで設定されたプロキシを考慮します。 - カスタムプロキシ: 接続プロパティで設定されたプロキシを考慮します。
プロキシ構成	プロキシを設定するために必要な形式。 次の形式を使用してプロキシを設定できます: <ホスト>:<ポート> 認証されたプロキシサーバーを設定することはできません。
詳細フィールド	エージェントが REST エンドポイントに接続するときに使用する引数を入力します。 次の引数をセミコロン（;）で区切って指定できます。 - ConnectionTimeout。REST エンドポイントからの応答を取得するための待機時間（ミリ秒）。接続タイムアウトを過ぎると、接続は終了します。デフォルトはエンドポイント API で定義されているタイムアウトです。 **注**: REST V2 接続タイムアウトとエンドポイント API タイムアウトの両方が定義されている場合、接続は定義されている最短のタイムアウトで終了します。 - connectiondelaytime。REST エンドポイントに要求を送信するための遅延時間（ミリ秒）。デフォルトは 10000 です。 - retryattempts。応答で 400 および 500 シリーズのエラーコードが返された場合に接続が試行された回数。デフォルトは 3 です。再試行を無効にするには 0 を指定します。 - qualifiedSchema。選択したスキーマが修飾されているかどうかを指定します。デフォルトは false です。 例: connectiondelaytime:10000;retryattempts:5 **注**: ストリーミング統合タスクでは、ConnectionTimeout および retryattempts のみが適用されます。

表 3. ［JWT ベアラートークン］認証の場合

接続プロパティ	説明

JWT ヘッダー	JSON 形式の JWT ヘッダー。
	サンプル:
	{
	"alg":"RS256",
	"kid":"xxyyzz"
	}

接続プロパティ	説明
	HS256 および RS256 アルゴリズムを設定できます。

JWT ペイロード	JSON 形式の JWT ペイロード。
	サンプル:
	{
	"iss":"abc",
	"sub":"678",
	"aud":"https://api.box.com/oauth2/token",
	"box_sub_type":"enterprise",
	"exp":"120",
	"jti":"3ee9364e"
	}
	exp として表される有効期限は、秒単位の相対時間です。有効期限は、トークン発行者の時間（iat）から UTC 形式で計算されます。
	ペイロードに iat が定義されており、有効期限に達すると、マッピングとアクセストークンの生成が失敗します。新しいアクセストークンを生成するには、ペイロードに有効な iat を指定する必要があります。
	iat がペイロードで定義されていない場合、有効期限は現在のタイムスタンプから計算されます。
	有効期限を文字列値として渡すには、値を二重引用符で囲みます。例:
	"exp":"120",
	有効期限を整数値として渡すには、値を二重引用符で囲まないでください。
	例:
	"exp":120,

認証サーバー	アプリケーションで設定されているアクセストークン URL。
認証の詳細プロパティ	アクセストークン URL で使用する追加パラメータ。パラメータは JSON 形式で定義する必要があります。 例: [\{"Name":"client_id","Value":"abc"},\ {"Name":"client_secret","Value":"abc"}]

接続プロパティ	説明
トラストストアファイルパス	REST API との一方向または双方向の安全な接続を確立するための TLS 証明書を含むトラストストアファイルの絶対パス。各 Secure Agent マシンで使用可能なディレクトリパスを指定します。 トラストストアファイル名とパスワードを JVM オプションとして設定することもできますし、証明書を次のディレクトリにインポートすることもできます。 <Secure Agent のインストールディレクトリ>\jre\lib\security\cacerts サーバーレスランタイム環境の場合、サーバーレスエージェントディレクトリでトラストストアファイルパスを指定します。 例: /home/cldagnt/SystemAgent/serverless/configurations/ssl_store/<cert_name>.jks
トラストストアのパスワード	SSL 証明書を含むトラストストアファイルのパスワード。 トラストストアのパスワードを JVM オプションとして設定することもできます。
キーストアファイルパス	必須。REST API との双方向の安全な接続を確立するために必要なキーと証明書を含むキーストアファイルの絶対パス。各 Secure Agent マシンで使用可能なディレクトリパスを指定します。 キーストアファイル名と格納場所を JVM オプションとして設定することもできます。また、証明書を任意のディレクトリにインポートすることもできます。 サーバーレスランタイム環境の場合、サーバーレスエージェントディレクトリでキーストアファイルパスを指定します。 例: /home/cldagnt/SystemAgent/serverless/configurations/ssl_store/<cert_name>.jks
キーストアのパスワード	必須。通信を安全に行うために必要なキーストアファイルのパスワードです。 キーストアのパスワードを JVM オプションとして設定することもできます。
プライベートキーのエイリアス	必須。JWT ペイロードの署名に使用されるプライベートキーのエイリアス名。
プライベートキーのパスワード	必須。通信を安全に行うために必要なキーストアファイルのパスワード。プライベートキーのパスワードは、キーストアのパスワードと同じでなければなりません。

接続プロパティ	説明
アクセストークン	アクセストークンの値を入力するか、**[アクセストークンの生成]** をクリックして、アクセストークンの値を指定します。 プロキシサーバーを介してアクセストークンの生成呼び出しを渡すには、Secure Agent レベルで認証されていないプロキシサーバーを設定する必要があります。REST V2 接続レベルのプロキシ設定は、アクセストークンの生成呼び出しには適用されません。
Swagger ファイルパス	Swagger ファイルまたは OpenAPI ファイルのパス。 次のいずれかのファイルパスを指定できます。 - ファイル名を含む絶対パス - ホストされている URL Swagger ファイルまたは OpenAPI ファイルの絶対パスを指定する場合、ファイルは Secure Agent マシン上に存在する必要があります。 ホストされた URL は、それ以上の認証とリダイレクトを要求せずにファイルのコンテンツを返す必要があります。 例えば、Swagger ファイルのパスは次のようになります。 `C:\swagger\sampleSwagger.json` ユーザーにはフォルダとファイルの読み取り権限が必要です。 **注**: ストリーミング統合タスクでは、Swagger ファイルパスとして Swagger 仕様ファイルのホストされた URL のみを使用できます。
プロキシタイプ	プロキシのタイプ。以下のいずれかのオプションを選択することができます。 - プロキシなし。エージェントレベルまたは接続プロパティで設定されたプロキシサーバーをバイパスします。 - プラットフォームプロキシ。エージェントで設定されたプロキシを考慮します。 - カスタムプロキシ。接続プロパティで設定されたプロキシを考慮します。

接続プロパティ	説明
プロキシ構成	プロキシを設定するために必要な形式。 次の形式を使用してプロキシを設定できます: <ホスト>:<ポート> 認証されたプロキシサーバーを設定することはできません。
詳細フィールド	エージェントが REST エンドポイントに接続するときに使用する引数を入力します。 次の引数をセミコロン（;）で区切って指定できます。 - ConnectionTimeout。REST エンドポイントからの応答を取得するための待機時間（ミリ秒）。接続タイムアウトを過ぎると、接続は終了します。デフォルトはエンドポイント API で定義されているタイムアウトです。 **注**: REST V2 接続タイムアウトとエンドポイント API タイムアウトの両方が定義されている場合、接続は定義されている最短のタイムアウトで終了します。 - connectiondelaytime。REST エンドポイントに要求を送信するための遅延時間（ミリ秒）。デフォルトは 10000 です。 - retryattempts。応答で 400 および 500 シリーズのエラーコードが返された場合に接続が試行された回数。デフォルトは 3 です。再試行を無効にするには 0 を指定します。 - qualifiedSchema。選択したスキーマが修飾されているかどうかを指定します。デフォルトは false です。 例: `connectiondelaytime:10000;retryattempts:5` **注**: ストリーミング統合タスクでは、ConnectionTimeout および retryattempts のみが適用されます。

Salesforce Marketing Cloud 接続のプロパティ

Salesforce Marketing Cloud 接続をセットアップする際には、接続プロパティを設定します。

次の表に、Salesforce Marketing Cloud 接続のプロパティを示します。

プロパティ	説明
接続名	接続の名前。 各接続名は組織内で一意である必要があります。接続名には、英数字、スペース、および次の特殊文字を含めることができます。_ .+ -, 最大長は 255 文字です。
説明	接続の説明。最大長は 4000 文字です。

プロパティ	説明
タイプ	Salesforce Marketing Cloud 接続タイプ。
ランタイム環境	タスクを実行するランタイム環境の名前。 Hosted Agent やサーバーレスランタイム環境でアプリケーション取り込みタスクを実行することはできません。
Salesforce Marketing Cloud の URL	エージェントが Salesforce Marketing Cloud WSDL への接続に使用する URL。
ユーザー名	基本認証に適用されます。Salesforce Marketing Cloud アカウントのユーザー名。 **注:** このプロパティは、アプリケーション取り込みタスク用に設定された接続には適用されません。
パスワード	基本認証に適用されます。Salesforce Marketing Cloud アカウントのパスワード。 **注:** このプロパティは、アプリケーション取り込みタスク用に設定された接続には適用されません。
クライアント ID	有効なアクセストークンを生成するために必要な Salesforce Marketing Cloud のクライアント ID。
クライアントシークレット	有効なアクセストークンを生成するために必要な Salesforce Marketing Cloud のクライアントシークレット。
プロキシサーバーを使用	プロキシを経由して Salesforce Marketing Cloud に接続します。 **注:** このプロパティは、アプリケーション取り込みタスク用に設定された接続には適用されません。
ロギングの有効化	タスクのロギングを有効にします。 ロギングを有効にすると、ログ詳細のセッションログを表示できます。 **注:** このプロパティは、アプリケーション取り込みタスク用に設定された接続には適用されません。
UTC オフセット	UTC オフセットの接続プロパティを使用して、UTC オフセットタイムゾーンの Salesforce Marketing Cloud との間でデータの読み書きを行います。 **注:** このプロパティは、アプリケーション取り込みタスク用に設定された接続には適用されません。
バッチサイズ	エージェントがバッチでターゲットに書き込む行数。 データを挿入または更新し、コンタクトキーを指定するときに、指定したコンタクト ID に関連付けられているデータが、1 つのバッチで Salesforce Marketing Cloud に挿入または更新されます。Salesforce Marketing Cloud にデータを更新/挿入する場合は、コンタクトキーを指定しないようにします。 **注:** このプロパティは、アプリケーション取り込みタスク用に設定された接続には適用されません。
複数の BU の有効化	Salesforce Marketing Cloud 接続を使用して、すべてのビジネスユニットのデータにアクセスします。 Salesforce Marketing Cloud アカウントに複数のビジネスユニットがある場合は、このオプションを選択します。 **注:** このプロパティは、アプリケーション取り込みタスク用に設定された接続には適用されません。

Salesforce Mass Ingestion 接続のプロパティ

Salesforce Mass Ingestion 接続をセットアップする際には、接続プロパティを設定する必要があります。

Salesforce Mass Ingestion の接続は、接続されたアプリケーションを使用して Salesforce データにアクセスします。接続を設定する前に、Salesforce の接続アプリケーションを設定して、接続が Salesforce データにアクセスできるようにする必要があります。
注: 接続アプリケーションの設定の詳細については、ナレッジベース記事「000172095」を参照してください。

Salesforce Mass Ingestion 接続のプロパティは、接続に指定した認証方法によって異なります。接続を作成する際に、次の認証方法のいずれかを選択できます。

- **OAuth 2.0 ユーザー名パスワードフロー**: Salesforce アカウントのログイン資格情報と、Salesforce が接続されたアプリケーション用に生成するコンシューマキーとコンシューマシークレットを使用して、接続を認証します。
- **OAuth 2.0 JWT ベアラーフロー**: Salesforce アカウントのユーザー名、プライベートキーのエイリアス、プライベートキーのパスワード、および Salesforce が接続アプリケーション用に生成するコンシューマキーを使用して、接続を認証します。Informatica では、この認証方法を使用することをお勧めします。この方法では、コンシューマシークレットや Salesforce アカウントのパスワードなどの機密情報を共有せずに Salesforce への安全なアクセスが提供されるためです。

OAuth 2.0 ユーザー名パスワードフロー認証の接続プロパティ

次の表に、OAuth 2.0 ユーザー名パスワードフロー認証を使用して設定された Salesforce Mass Ingestion 接続の接続プロパティを示します。

接続プロパティ	説明
接続名	接続の名前。この名前は、組織内で一意にする必要があります。接続名には、英数字、スペース、および次の特殊文字を含めることができます。_ .+ - 名前の先頭または末尾のスペースはトリミングされ、名前の一部として保存されません。最大長は 100 文字です。接続名では大文字と小文字は区別されません。
説明	接続の説明（オプション）。最大長は 255 文字です。
タイプ	接続のタイプ。Oracle Database Ingestion 接続の場合、タイプは［Salesforce Mass Ingestion］でなければなりません。
ランタイム環境	取り込みタスクを実行するランタイム環境の名前。 ランタイム環境として Secure Agent を指定する必要があります。 **注**: Hosted Agent やサーバーレスランタイム環境でアプリケーション取り込みタスクを実行することはできません。
ユーザー名	Salesforce アカウントのユーザー名。
パスワード	Salesforce アカウントのパスワード。
セキュリティトークン	Salesforce アカウントに関連付けられたセキュリティトークン。 接続されたアプリケーションに IP 制限が指定されていない場合は、セキュリティトークンを指定せずに接続を設定できます。ただし、接続されたアプリケーションに IP 制限が適用されている場合、および Salesforce 組織に指定された、信頼できる IP 範囲で Secure Agent が実行されていない場合は、セキュリティトークンを指定する必要があります。 **注**: セキュリティトークンがない場合は、Salesforce でセキュリティトークンをリセットします。セキュリティトークンのリセットの詳細については、Salesforce documentation を参照してください。

接続プロパティ	説明
コンシューマキー	接続アプリケーションに対して OAuth 2.0 認証を有効にしたときに Salesforce が生成するコンシューマキー。
コンシューマシークレット	接続されたアプリに対して OAuth 2.0 認証を有効にしたときに Salesforce が生成するコンシューマシークレット。
API バージョン	ソースデータへのアクセスに使用する Salesforce API のバージョン。 デフォルトは 51.0 です。 **注**: 51.0 より古いバージョンは使用できません。

OAuth トークン URL	Salesforce 組織の OAuth 2.0 トークンエンドポイント。接続アプリケーションは、このエンドポイントにアクセストークン要求を送信します。
	デフォルト値は次のとおりです。
	`https://login.salesforce.com/services/oauth2/token`
	このデフォルト URL は、すべての Salesforce インスタンスに使用されます。
	または、インスタンス固有の URL を入力できます。
	`https://<instance domain URL>/services/oauth2/token`
	インスタンス固有の URL を使用すると、Salesforce ホストサーバーへのより直接的で高速な接続を確立できます。共通のデフォルトエンドポイントの負荷が高く、共通のデフォルトエンドポイントの使用時に取り込みジョブが認証エラーで失敗する場合は、代わりにこの代替 URL を使用してください。

注: OAuth 2.0 ユーザー名パスワードフロー認証方法の詳細については、Salesforce のドキュメントを参照してください。

OAuth 2.0 JWT ベアラーフロー認証の接続プロパティ

次の表に、OAuth 2.0 JWT ベアラーフロー認証を使用して設定された Salesforce Mass Ingestion 接続の接続プロパティを示します。

接続プロパティ	説明
接続名	接続の名前。この名前は、組織内で一意にする必要があります。接続名には、英数字、スペース、および次の特殊文字を含めることができます。_ .+ - 名前の先頭または末尾のスペースはトリミングされ、名前の一部として保存されません。最大長は 100 文字です。接続名では大文字と小文字は区別されません。
説明	接続の説明（オプション）。最大長は 255 文字です。
タイプ	接続のタイプ。Oracle Database Ingestion 接続の場合、タイプは［Salesforce Mass Ingestion］でなければなりません。
ランタイム環境	取り込みタスクを実行するランタイム環境の名前。 ランタイム環境として Secure Agent を指定する必要があります。 **注**: Hosted Agent やサーバーレスランタイム環境でアプリケーション取り込みタスクを実行することはできません。
ユーザー名	Salesforce アカウントのユーザー名。
コンシューマキー	接続アプリケーションに対して OAuth 2.0 認証を有効にしたときに Salesforce が生成するコンシューマキー。

接続プロパティ	説明
キーストアのパス	JSON Web Token（JWT）を検証し、Salesforce との安全な接続を確立するために必要な X509 証明書を含むキーストアファイルへの絶対パス。 キーストアファイルは Java KeyStore （JKS）形式である必要があります。
キーストアのパスワード	キーストアファイルのパスワード。
プライベートキーのエイリアス	JWT の署名に使用されるプライベートキーのエイリアス名。
プライベートキーのパスワード	プライベートキーのパスワード。
API バージョン	ソースデータへのアクセスに使用する Salesforce API のバージョン。 デフォルトは 51.0 です。 **注**: 51.0 より古いバージョンは使用できません。

OAuth トークン URL	Salesforce 組織の OAuth 2.0 トークンエンドポイント。接続アプリケーションは、このエンドポイントにアクセストークン要求を送信します。
	デフォルト値は次のとおりです。
	`https://login.salesforce.com/services/oauth2/token`
	このデフォルト URL は、すべての Salesforce インスタンスに使用されます。
	または、インスタンス固有の URL を入力できます。
	`https://<instance domain URL>/services/oauth2/token`
	インスタンス固有の URL を使用すると、Salesforce ホストサーバーへのより直接的で高速な接続を確立できます。共通のデフォルトエンドポイントの負荷が高く、共通のデフォルトエンドポイントの使用時に取り込みジョブが認証エラーで失敗する場合は、代わりにこの代替 URL を使用してください。

注: OAuth 2.0 JWT ベアラーフロー認証方法の詳細については、Salesforce のドキュメントを参照してください。

SAP HANA Database Ingestion 接続のプロパティ

データベース統合タスクの SAP HANA 接続をセットアップする際には、接続プロパティを設定する必要があります。

以下の表に、SAP HANA 接続のプロパティを示します。

接続プロパティ	説明
接続名	接続の名前。この名前は、組織内で一意にする必要があります。接続名には、英数字、スペース、および次の特殊文字を含めることができます。_ .+ - 名前の先頭または末尾のスペースはトリミングされ、名前の一部として保存されません。最大長は 100 文字です。接続名では大文字と小文字は区別されません。
説明	接続の説明（オプション）。最大長は 255 文字です。
タイプ	接続タイプとして【SAP HANA Database Ingestion】を選択します。
ランタイム環境	データベース統合タスクを実行するランタイム環境の名前。ランタイム環境は、管理者で定義します。
ユーザー名	SAP HANA インスタンスへの接続に使用するユーザー名。
パスワード	SAP HANA インスタンスへの接続に使用するパスワード。
ホスト	SAP HANA データベースサーバーをホストするマシンの名前。
ポート	接続先の SAP HANA サーバーのポート番号。デフォルトは 30015 です。
データベース名	SAP HANA ソースデータベース名。
詳細接続プロパティ	SAP HANA ソースへの接続に使用される SAP HANA JDBC ドライバのオプションの詳細プロパティ。*property=value* エントリを複数指定する場合は、アンパサンド（&）で区切ります。このフィールドに入力できる JDBC 接続プロパティについては、SAP の JDBC Connection Properties のドキュメントを参照してください。例: encrypt=true。
キャプチャタイプ	次のいずれかのオプションを選択して、データベース取り込み増分ロードジョブが SAP HANA データベースから変更データをキャプチャするために使用するキャプチャメソッドを指定します。 - **トリガベース。**AFTER DELETE、AFTER INSERT、AFTER UPDATE トリガを使用して、スキーマ内の SAP HANA ソーステーブルから変更データをキャプチャします。トリガは、各ソーステーブルの DML 変更の操作前イメージと操作後イメージを取得し、変更のエントリを PKLOG テーブルとシャドー_CDC テーブルに書き込みます。このメソッドは、元のキャプチャメソッドです。 - **ログベース（プレビュー）。**SAP HANA データベースログから変更データをキャプチャします。このメソッドは、プレビューモードでのみ使用できます。プレビュー機能は評価を目的としてサポートされていますが、保証対象外で、本番環境または本番環境にプッシュする予定の環境には対応していません。詳細については、Informatica グローバルカスタマサポートにお問い合わせください。

接続プロパティ	説明
ログのクリア	増分ロードの場合は必須です。PKLOG テーブルエントリとシャドー_CDC テーブルエントリがパージされるまでの時間間隔（日数）。パージは、増分ロードジョブの実行中にのみ行われます。 データベース取り込みジョブの有効な値は 0 から 366 です。この範囲の正の値を指定すると、増分ジョブの実行中に自動ハウスキーピングが実行されます。デフォルトは 14 です。 値 0 は、テーブルエントリがパージされないことを意味します。手動でハウスキーピングを行う場合は、0 を入力して社内プロセスを使用してください。 負の数または数値以外の値を含め、0 から 366 の範囲外の値があると、接続を使用するデータベース取り込みジョブが次のエラーで失敗します。 `LogClear contains a non numeric number. Caused by: LogClear contains a non numeric number.`
トリガプレフィックス	トリガベースのキャプチャタイプを使用する場合、DML 変更の操作前と操作後のイメージを取得するために CDC スクリプトが各ソーステーブルに対して生成する AFTER DELETE、AFTER INSERT、および AFTER UPDATE トリガの名前にプレフィックスを追加できます。最大 16 文字のプレフィックス値を入力します。トリガ名のプレフィックスの後にアンダースコア（_）が続きます（例: TX_SAP_DEMO_TABLE_DBMI_USER_t_d）。プレフィックスを使用して、サイトのトリガ命名規則に準拠できます。
キャッシュタイプ	[ログベース（プレビュー）] キャプチャタイプを選択した場合は、キャッシュタイプとして【Hana】または【Oracle】を選択します。
キャッシュホスト	[ログベース（プレビュー）] キャプチャタイプを選択した場合は、キャッシュデータベースをホストするマシンのホスト名を入力します。
キャッシュポート	[ログベース（プレビュー）] キャプチャタイプを選択した場合は、キャッシュデータベースサーバーのポート番号を入力します。
キャッシュユーザー名	[ログベース（プレビュー）] キャプチャタイプを選択した場合は、キャッシュデータベースへの接続に使用するユーザー名を入力します。
キャッシュパスワード	[ログベース（プレビュー）] キャプチャタイプを選択した場合は、キャッシュデータベースへの接続に使用するパスワードを入力します。
キャッシュデータベース/サービス名	[ログベース（プレビュー）] キャプチャタイプを選択した場合は、選択したキャッシュタイプに応じて、Hana キャッシュデータベース名または Oracle キャッシュサービス名を入力します。
キャッシュ追加接続プロパティ	[ログベース（プレビュー）] キャプチャタイプを選択した場合は、オプションのキャッシュ接続プロパティのリストを入力できます。Hana キャッシュを使用する場合は、アンパサンド（&）区切り記号を使用します。Oracle キャッシュを使用する場合は、セミコロン（;）区切り記号を使用します。 例: Hana: `latency=0&communicationtimeout=0` Oracle: `EncryptionMethod=SSL;CryptoProtocolVersion=TLSv1.1`

接続プロパティ	説明
キャッシュセキュリティ接続プロパティ	[ログベース（プレビュー）] キャプチャタイプを選択した場合は、キャッシュ接続のオプションのセキュリティプロパティのリストを入力できます。Hana キャッシュを使用する場合は、アンパサンド（&）区切り記号を使用します。Oracle キャッシュを使用する場合は、セミコロン（;）区切り記号を使用します。 例: Hana: `encrypt=true&validateCertificate=false` Oracle: `KeyStorePassword=xyz;TrustStorePassword=xy`
サーバーログのパス	[ログベース（プレビュー）] キャプチャタイプを選択した場合は、SAP HANA DB サーバーのログパスを入力します。
クライアントログのパス	[ログベース（プレビュー）] キャプチャタイプを選択した場合は、Secure Agent マシンのマウントパスとソースデータベースのログの場所のマッピングを入力します。
クライアントアーカイブログのパス	[ログベース（プレビュー）] キャプチャタイプを選択した場合は、Secure Agent マシンのマウントパスとソースデータベースのアーカイブログの場所のマッピングを入力します。

注: 接続をテストしてテストが失敗した場合は、SAP HANA JDBC ドライバファイル ngdbc.jar が*<Secure Agent installation directory>*/ext/connectors/thirdparty/informatica.hanami にインストールされていることを確認してください。

SAP 一括取り込み接続のプロパティ

SAP 一括取り込み接続を設定する際には、接続プロパティを設定する必要があります。

次の表に、SAP 一括取り込み接続の接続プロパティを示します。

接続プロパティ	説明
接続名	接続の名前。この名前は、組織内で一意にする必要があります。接続名には、英数字、スペース、および次の特殊文字を含めることができます。 _ .+ - 名前の先頭または末尾のスペースはトリミングされ、名前の一部として保存されません。最大長は 100 文字です。接続名では大文字と小文字は区別されません。
説明	接続の説明（オプション）。最大長は 255 文字です。
タイプ	接続のタイプ。Oracle Database Ingestion 接続の場合、タイプは［SAP Mass Ingestion］でなければなりません。
ランタイム環境	取り込みタスクを実行するランタイム環境の名前。 ランタイム環境として Secure Agent を指定する必要があります。 **注**: Hosted Agent やサーバーレスランタイム環境でアプリケーション取り込みタスクを実行することはできません。

接続プロパティ	説明
ユーザー名	SAP インスタンスのユーザー名。
パスワード	SAP インスタンスのパスワード。
言語コード	SAP 言語に対応する言語コード。
システム番号	SAP サーバーのシステム番号。
クライアント番号	SAP サーバーのクライアント番号。
ポート範囲	Netty サーバーを実行する HTTP ポート範囲。
接続タイプ	ABAP アプリケーションサーバーにアクセスするための接続タイプ。次のオプションがあります。 - **直接接続**: サーバーホストを使用して単一の ABAP アプリケーションサーバーにアクセスします。 - **負荷分散接続**: メッセージサーバーを介して ABAP アプリケーションサーバーのグループにアクセスします。
アプリケーションサーバー	SAP アプリケーションサーバーホストの名前。 **注**: このフィールドは、**［直接接続］**タイプの場合にのみ表示されます。
メッセージサーバー	SAP メッセージサーバーの IP アドレスまたは名前。 **注**: このフィールドは、**［負荷分散接続］**タイプの場合にのみ表示されます。
SAP ログオングループ	アクセスする SAP システムに属するサーバーのグループ名。 **注**: このフィールドは、**［負荷分散接続］**タイプの場合にのみ表示されます。
SAP システム ID	アクセスする SAP システムの ID。 **注**: このフィールドは、**［負荷分散接続］**タイプの場合にのみ表示されます。
メッセージサーバーポート	SAP メッセージサーバーがリッスンしているポート番号。 **注**: このフィールドは、**［負荷分散接続］**タイプの場合にのみ表示されます。
データベース	基盤データベースの名前。 次のいずれかのオプションを選択します。 - Oracle - SAP HANA（S/4 トリガベース）
Oracle データベースの場合	
データベースユーザー名	データベースインスタンスのユーザー名。
データベースパスワード	データベースインスタンスのパスワード。
ホスト	データベースサーバーのホスト名。
ポート	データベースサーバーに接続するときに使用するネットワークポート番号。デフォルトは 1521 です。

接続プロパティ	説明
サービス名	Oracle データベースを一意に識別するサービス名またはシステム ID (SID)。Oracle データベースに接続するための SID を次の形式で指定します。SID:<ORACLE_SID>
コードページ	データベースサーバーのコードページ。アプリケーション取り込みタスクでは、UTF-8 コードページを使用します。デフォルトは UTF-8 です。
暗号化方法	初期ロードジョブの場合、Secure Agent と Oracle データベースサーバーとの間で交換するデータを暗号化するかどうかを決定します。: 次のいずれかのオプションを選択します。 - SSL。データ暗号化に SSL を使用してセキュアな接続を確立します。Oracle データベースサーバーが SSL を設定できない場合、接続は失敗します。 - **暗号化なし**。SSL を使用せずに接続を確立します。データは暗号化されません。 デフォルトは **[暗号化なし]** です。
暗号プロトコルバージョン	暗号化方法として SSL を選択した場合、暗号化された接続を使用するためにサーバーでサポートされている暗号プロトコルを 1 つ指定するか、複数のリストで指定する必要があります。を参照してください。 次のいずれかのオプションを選択します。 - SSLv2 - SSLv3 - TLSv1.2 デフォルトは [TLSv1.2] です。
サーバー証明書の検証	暗号化方法として SSL を選択した場合、このオプションは、Secure Agent が Oracle データベースサーバーから送信されたサーバー証明書を検証するかどうかを制御します。 次のいずれかのオプションを選択します。 - True。サーバー証明書を検証します。 - False。サーバー証明書を検証しません。 デフォルトは False です。 **[証明書内のホスト名]** プロパティを指定すると、Secure Agent は証明書内のホスト名も検証します。
トラストストア	暗号化方法として SSL を選択し、サーバー証明書の検証を有効にした場合は、クライアントが SSL 認証で信頼する認証局(CA)のリストが含まれているトラストストアファイルのパスと名前を指定します。
トラストストアパスワード	暗号化方法として SSL を選択し、サーバー証明書の検証を有効にした場合は、トラストストアファイルの内容にアクセスするためのパスワードを指定します。
証明書内のホスト名	暗号化方法として SSL を選択し、サーバー証明書の検証を有効にした場合は、セキュリティを強化するために、Oracle データベースをホストするマシンのホスト名を指定します。Secure Agent は、SSL 証明書のホスト名との接続に含まれるホスト名を検証します。
キーストア	暗号化方法として SSL を選択し、Oracle データベースサーバーでクライアント認証が有効になっている場合は、キーストアファイルのパスと名前を指定します。キーストアファイルには、クライアントが、Oracle サーバーの証明書要求に応答して送信する証明書が含まれます。

接続プロパティ	説明
キーストアのパスワード	暗号化方法として SSL を選択し、Oracle データベースサーバーでクライアント認証が有効になっている場合は、キーストアファイルのパスワードを指定します。
キーパスワード	暗号化方法として SSL を選択し、Oracle データベースサーバーでクライアント認証が有効になっている場合は、キーストアファイルのキーのパスワードを指定します。このプロパティは、キーのパスワードがキーストアファイルとは異なる場合に使用してください。
データベース接続文字列	アプリケーション取り込みタスクが Oracle データベースへの接続に使用する、TNS で定義された Oracle 接続文字列。
TDE ウォレットディレクトリ	Oracle 透過的データ暗号化（TDE）に使用される Oracle ウォレットファイルを含むディレクトリへのパス。このプロパティ値は、TDE 暗号化テーブルスペースから変更データをキャプチャする場合、かつ、次のいずれかの条件が当てはまる場合にのみ指定してください。 - Oracle ウォレットはデータベースで使用できません。 - Oracle データベースは、Oracle REDO ログから離れたサーバーで実行されています。 - ウォレットディレクトリがデータベースホストのデフォルトの場所にないか、ウォレット名が ewallet.p12 のデフォルト名ではありません。 - ウォレットディレクトリは、Secure Agent ホストでは使用できません。
TDE ウォレットパスワード	Oracle TDE ウォレットにアクセスしてマスターキーを取得するために必要な、クリアテキストのパスワード。Oracle ソースデータベースの TDE 暗号化テーブルスペースから変更データを取得する必要がある場合は、このプロパティ値が必要です。
代替ディレクトリ	Oracle サーバー上の REDO ログのサーバーパスプレフィックスを置き換えるローカルパスプレフィックス。ログリーダーが Oracle サーバー以外のシステムで実行され、別のマッピングを使用して REDO ログファイルにアクセスする場合、置き換え先のローカルパスは必須です。 このプロパティは次の状況で使用します。 - REDO ログは共有ディスクに存在します。 - REDO ログは、Oracle システムとは別のシステムにコピーされています。 - アーカイブ REDO ログには、別の NFS マウントを使用してアクセスします。 **注**: Oracle Automatic Storage Management（ASM）を使用して REDO ログを管理する場合は、このプロパティを使用しないでください。 1 つ以上の代替パスを定義できます。次の形式を使用します。 *server_path_prefix*,*local_path_prefix*;*server_path_prefix*,*local_path_prefix*;...
リーダーアクティブログマスク	Oracle データベースで REDO ログの多重化を使用しているときに、ログリーダーがアクティブな REDO ログを選択するために使用するマスク。ログリーダーは、アクティブ REDO ロググループ内のメンバ名とマスクを比較して、読み取るログを決定します。マスクでは、アスタリスク（*）ワイルドカードを使用して、0 個以上の文字を表すことができます。 マスクの最大長は 128 文字です。大文字小文字は Linux と UNIX システムでは区別されますが、Windows システムでは区別されません。

接続プロパティ	説明
リーダーアーカイブ保存先 1	アーカイブ REDO ログごとに複数のコピーを書き込むよう Oracle が設定されているときに、ログリーダーがアーカイブログを読み取るプライマリのログ保存先。Oracle LOG_ARCHIVE_DEST_*n* 初期化パラメータの *n* 値に対応する数値を入力します。ここで *n* は、1〜10 の値です。 [リーダーアーカイブ保存先 1] および [リーダーアーカイブ保存先 2] プロパティのいずれか一方のみを設定した場合、ログリーダーはそのプロパティ設定を使用します。どちらのプロパティも指定しない場合、アーカイブログクエリはログ保存先でフィルタされません。
リーダーアーカイブ保存先 2	プライマリ保存先が利用できないとき、またはプライマリ保存先にあるログが読み取れないとき、ログリーダーがアーカイブログを読み取るセカンダリのログ保存先。例えば、ログが破損または削除されている場合です。Oracle LOG_ARCHIVE_DEST_*n* 初期化パラメータの *n* 値に対応する数値を入力します。ここで *n* は、1〜10 の値です。この値は通常、1 より大きい数値です。
リーダー ASM 接続文字列	Oracle ASM 環境で、ソースデータベースのアクティブ REDO ログとアーカイブ REDO ログのストレージを管理する ASM インスタンスへの接続のためにログリーダーで使用される、TNS で定義された Oracle 接続文字列です。
リーダー ASM ユーザー名	Oracle ASM 環境で、ソースデータベースのアクティブ REDO ログとアーカイブ REDO ログのストレージを管理する ASM インスタンスへの接続のためにログリーダーで使用される、Oracle ユーザー ID です。このユーザー ID には SYSDBA 権限または SYSASM 権限が必要です。SYSASM 権限を使用するには、**[SYSASM としてリーダー ASM 接続]** プロパティを「Y」に設定します。
リーダー ASM パスワード	Oracle ASM 環境で、**[リーダー ASM ユーザー名]** プロパティに指定されているユーザーのクリアテキストのパスワード。ログリーダーは、このパスワードと ASM ユーザー名を使用して、ソースデータベースのアクティブ REDO ログとアーカイブ REDO ログのストレージを管理する ASM インスタンスに接続します。
SYSASM としてリーダー ASM 接続	Oracle 11*g* ASM 以降を使用していて、ログリーダーが ASM インスタンスに接続するために SYSASM 権限を持つユーザー ID を使用する場合は、このチェックボックスをオンにします。また、**[リーダー ASM ユーザー名]** プロパティで SYSASM 権限を持つユーザー ID を指定します。SYSDBA 権限を持つユーザー ID を使用するには、このチェックボックスをオフにします。デフォルトでは、このチェックボックスはオフです。

接続プロパティ	説明

リーダーモード	ログリーダーが読み取る Oracle REDO ログのソースとタイプを示します。
	次のいずれかのオプションを選択します。
	- ACTIVE。アクティブおよびアーカイブ REDO ログを Oracle オンラインシステムから読み取ります。オプションで、**［リーダーアクティブログマスク］**プロパティを使用してアクティブ REDO ログをフィルタしたり、**［リーダーアーカイブ保存先 1］**および**［リーダーアーカイブ保存先 2］**プロパティを使用してアーカイブログの読み取り元となるアーカイブログ保存先を制限したりすることができます。
	- ARCHIVEONLY。アーカイブ REDO ログのみを読み取ります。オプションで、**［リーダーアーカイブ保存先 1］**および**［リーダーアーカイブ保存先 2］**プロパティを使用して、アーカイブログの読み取り元となるアーカイブログ保存先を制限できます。
	- ARCHIVECOPY。代替ファイルシステムにコピーされたアーカイブ REDO ログを読み取ります。このオプションは次の状況で使用します。
	  - Oracle のアーカイブ REDO ログに直接アクセスするための権限がない。
	  - アーカイブ REDO ログが ASM に書き込まれているが、ASM にアクセスできない。
	  - データベースサーバーのアーカイブログ保持ポリシーによって、アーカイブログが十分長期間保持されない。
	  このオプションを使用する場合、**［リーダーアーカイブ保存先 1］**および**［リーダーアーカイブ保存先 2］**プロパティは無視されます。
	デフォルトは ACTIVE です。

リーダースタンバイログマスク	Oracle 物理スタンバイデータベースで REDO ログの多重化を使用しているときに、ログリーダーがデータベースの REDO ログを選択するために使用するマスク。ログリーダーは、REDO ロググループ内のメンバ名とマスクを比較して、読み取るログを決定します。マスクでは、アスタリスク（*）ワイルドカードを使用して、0 個以上の文字を表すことができます。 マスクの最大長は 128 文字です。大文字小文字は Linux と UNIX システムでは区別されますが、Windows システムでは区別されません。
スタンバイ接続文字列	データベースが読み取り専用アクセスで開かれていない場合の変更のキャプチャ用に、ログリーダーが Oracle 物理スタンバイデータベースへ接続するために使用する、TNS で定義された Oracle 接続文字列。
スタンバイユーザー名	変更のキャプチャ用に、ログリーダーが Oracle 物理スタンバイデータベースへ接続するために使用するユーザー ID。このユーザー ID には SYSDBA 権限が必要です。
スタンバイパスワード	変更のキャプチャ用に、ログリーダーが Oracle 物理スタンバイデータベースへ接続するために使用するパスワード。
RAC メンバ	Oracle Real Application Cluster（RAC）内で、追跡可能なアクティブ REDO ログスレッド（*メンバ*）の最大数。RAC 環境でプライマリデータベースをサポートする Data Guard 物理スタンバイデータベースの場合、この値はプライマリデータベースのアクティブなスレッドの数です。 有効な値は 1〜100 です。デフォルトは 0 で、適切なログスレッド数が自動的に決定されます。この値がお使いの環境で適切でない場合は、このプロパティを 0 より大きい値に設定してください。

接続プロパティ	説明
BFILE アクセス	次の状況では、このチェックボックスをオンにします。 - BFILE アクセスを使用して、ローカル Oracle サーバーファイルシステム上の物理ディレクトリの REDO ログにアクセスする。BFILE アクセスは、Oracle ディレクトリオブジェクトを使用して、ファイルシステムの REDO ログにリモートアクセスします。この方法は、ASM や NFS マウントなどの他のログアクセス方法に代わるものです。 - Amazon Relational Database Service（RDS）for Oracle ソースがある。この場合、このオプションを使用すると、RDS にデプロイされたクラウドベースのデータベースインスタンスの REDO ログにアクセスできます。 デフォルトでは、このチェックボックスはオフです。
SAP HANA（S/4 トリガベース）データベースの場合	
ユーザー名	SAP HANA インスタンスへの接続に使用するユーザー名。
パスワード	SAP HANA インスタンスに接続するためのパスワード。
ホスト	SAP HANA データベースサーバーをホストするマシンの名前。
ポート	接続先の SAP HANA サーバーのポート番号。デフォルトは 30015 です。
データベース名	SAP HANA ソースデータベース名。
詳細接続プロパティ	SAP HANA ソースへの接続に使用される SAP HANA JDBC ドライバの詳細プロパティ。*property=value* エントリを複数指定する場合は、アンパサンド（&）で区切ります。このフィールドに入力できる JDBC 接続プロパティについては、SAP の JDBC Connection Properties のドキュメントを参照してください。例: encrypt=true。
ログのクリア	増分ロードの場合は必須です。PKLOG テーブルエントリとシャドー _CDC テーブルエントリがパージされるまでの時間間隔（日数）。パージは、増分ロードジョブの実行中にのみ行われます。 データベース取り込みジョブの有効な値は 0 から 366 です。この範囲の正の値を指定すると、増分ジョブの実行中に自動ハウスキーピングが実行されます。デフォルトは 14 です。 値 0 は、テーブルエントリがパージされないことを意味します。手動でハウスキーピングを行う場合は、0 を入力して社内プロセスを使用してください。 負の数または数値以外の値を含め、0 から 366 の範囲外の値があると、接続を使用するデータベース取り込みジョブが次のエラーで失敗します。 `LogClear contains a non numeric number. Caused by: LogClear contains a non numeric number.`
トリガプレフィックス	トリガベースのキャプチャメソッドを使用する場合、DML 変更の操作前と操作後のイメージを取得するために CDC スクリプトが各ソーステーブルに対して生成する AFTER DELETE、AFTER INSERT、および AFTER UPDATE トリガの名前にプレフィックスを追加できます。最大 16 文字の任意のプレフィックス値を入力します。トリガ名のプレフィックスの後にアンダースコア（_）が続きます（例: TX_SAP_DEMO_TABLE_DBMI_USER_t_d）。プレフィックスを使用して、サイトのトリガ命名規則に準拠できます。

SAP ODP Extractor 接続のプロパティ

[SAP ODP Extractor] 接続をセットアップする際には、接続プロパティを設定します。

次の表に、SAP ODP Extractor の接続プロパティを示します。

プロパティ	説明
接続名	接続の名前。 各接続名は組織内で一意である必要があります。接続名には、英数字、スペース、および次の特殊文字を含めることができます。_ .+ -, 最大長は 255 文字です。
説明	接続の説明。最大長は 4000 文字です。
タイプ	SAP ODP Extractor
ランタイム環境	SAP S/4HANA または SAP ECC にアクセスするためのタスクを実行するランタイム環境の名前。

SAP サーバー接続タイプ	使用する SAP サーバー接続タイプ。
	次のオプションから選択します。
	- **アプリケーションサーバー接続**。SAP ユーザー名とパスワードを使用して SAP アプリケーションサーバーに接続します。
	- **アプリケーションサーバー SNC 接続**。次のセキュアなネットワーク接続を使用して SAP アプリケーションサーバーに接続します:
	  - X.509 証明書を使用。SAP ユーザー名やパスワードを明示的に指定する必要はありません。X.509 証明書ファイルのパスを指定する必要があります。
	  - X.509 証明書なし。SAP ユーザー名を指定する必要があります。
	- **負荷分散サーバー接続**。実行時の負荷が最小である SAP アプリケーションサーバーに接続します。
	- **負荷分散サーバー SNC 接続**。実行時の負荷が最小である SNC を使用して SAP アプリケーションサーバーに接続します。
	注: SNC 接続を使用する前に、SAP サーバーと Secure Agent が実行されているマシンで SNC が設定されていることを確認する必要があります。

次の表に、接続タイプとして **[アプリケーションサーバー接続]** を選択した場合に設定する必要のあるプロパティを示します。

接続プロパティ	説明
SAP クライアント番号	SAP サーバーのクライアント番号。
SAP 言語	SAP 言語に対応する言語コード
SAP アプリケーションサーバー	SAP アプリケーションサーバーのホスト名。
SAP システム番号	接続する SAP サーバーのシステム番号。
SAP ユーザー名	適切なユーザー権限が付与された SAP ユーザー名。
SAP パスワード	SAP パスワード。

接続プロパティ	説明
サブスクライバ名	Secure Agent を SAP システムの一意のサブスクライバとして定義する名前。SAP はこの名前を使用して、ODP からのデルタ読み取りを行う場合に一意の Operational Delta Queue（ODQ）を定義します。

追加パラメータ	Secure Agent が SAP システムに接続するために使用する追加の SAP パラメータ。
	たとえば、SAP JCo および SAP CPIC トレースを生成するには、次のプロパティを指定します。
	`jco.client.trace="1";`
	`jco.client.cpic_trace="3";`
	実行時に、JCo および CPIC トレースファイルが次の場所に生成されます。
	`<Informatica Secure Agent installation directory>\apps\Data_Integration_Server\<DIS version>\ICS\main\bin\rdtm`
	設計時に、CPIC トレースは次の場所にある tomcat.out ファイルに生成されます。
	`<Informatica Secure Agent installation directory>\apps\Data_Integration_Server\<DIS version>tomcat.out`

差分フィールドを表示	ODP ソース上のデータ変更の原因となった操作モードをマッピングに表示するかどうかを指定します。 有効にすると、マッピングによって、Operational Delta Queue（ODQ）で有効になっている ODP ソースの**［フィールド］**タブに ODQ_CHANGEMODE および ODQ_ENTITYCNTR フィールドが生成されます。 デフォルトでは無効になっています。

次の表に、接続タイプとして**［負荷分散サーバー接続］**を選択した場合に設定する必要のあるプロパティを示します。

接続プロパティ	説明
SAP クライアント番号	SAP サーバーのクライアント番号。
SAP 言語	SAP 言語に対応する言語コード
SAP メッセージサーバー	SAP メッセージサーバのホスト名。
SAP システム ID	SAP メッセージサーバーのシステム ID。
SAP グループ	ログイングループ名（例: PUBLIC）。
SAP ユーザー名	適切なユーザー権限が付与された SAP ユーザー名。
SAP パスワード	SAP パスワード。
サブスクライバ名	Secure Agent を SAP システムの一意のサブスクライバとして定義する名前。 SAP はこの名前を使用して、ODP からのデルタ読み取りを行う場合に一意の Operational Delta Queue（ODQ）を定義します。

接続プロパティ	説明

追加パラメータ	Secure Agent が SAP システムに接続するために使用する追加の SAP パラメータ。
	たとえば、SAP JCo および SAP CPIC トレースを生成するには、次のプロパティを指定します。
	`jco.client.trace="1";`
	`jco.client.cpic_trace="3";`
	実行時に、JCo および CPIC トレースファイルが次の場所に生成されます。
	`<Informatica Secure Agent installation directory>\apps\Data_Integration_Server\<DIS version>\ICS\main\bin\rdtm`
	設計時に、CPIC トレースは次の場所にある tomcat.out ファイルに生成されます。
	`<Informatica Secure Agent installation directory>\apps\Data_Integration_Server\<DIS version>tomcat.out`

差分フィールドを表示	ODP ソース上のデータ変更の原因となった操作モードをマッピングに表示するかどうかを指定します。 有効にすると、マッピングによって、Operational Delta Queue（ODQ）で有効になっている ODP ソースの**［フィールド］**タブに ODQ_CHANGEMODE および ODQ_ENTITYCNTR フィールドが生成されます。 デフォルトでは無効になっています。

次の表に、接続タイプとして**［アプリケーションサーバー SNC 接続］**を選択した場合に設定する必要のあるプロパティを示します。

接続プロパティ	説明
SAP クライアント番号	SAP サーバーのクライアント番号。
SAP 言語	SAP 言語に対応する言語コード
SAP アプリケーションサーバー	SAP アプリケーションサーバーのホスト名。
SAP システム番号	接続する SAP サーバーのシステム番号。
SNC マイネーム	オプション。Informatica クライアントのパーソナルセキュリティ環境（PSE）または証明書名。 デフォルトの長さは 256 です。
SNC パートナー名	Informatica クライアントの PSE または証明書名。 デフォルトの長さは 256 です。
SNC 保護品質（QoP）	SAP PSE または証明書名を指定します。 以下のオプションから選択できます。 - 1 - 認証のみを適用。 - 2 - 整合性保護（認証）を適用。 - 3 - プライバシー保護（整合性と認証）を適用。 - 8 - デフォルトの保護を適用。 - 9 - 最大限の保護を適用。 デフォルトは、*［3 - プライバシー保護（整合性と認証）を適用］*です。

接続プロパティ	説明
SAP 暗号ライブラリパス	暗号ライブラリへのパス。 Windows の場合は sapcrypto.dll を、Linux の場合は libsapcrypto.so を指定します。
X509 証明書を使用	保護の品質を指定します。X509 証明書ベースの SNC 接続を使用することを選択します。
X509 証明書のパスまたは SAP ユーザー名	X509 証明書ファイルへのパス。 X509 証明書を使用することを選択した場合は、.crt という拡張子を持つ X509 証明書ファイルへのパスを指定します。SAP ユーザー名やパスワードを指定する必要はありません。 X509 証明書を使用しない場合は、SAP サーバーで SNC が設定されている SAP ユーザー名を指定します。
サブスクライバ名	Informatica Secure Agent を SAP システムの一意のサブスクライバとして定義する名前。 SAP は、Secure Agent が ODP からデルタデータを読み取る際に、この名前を使用して一意の Operational Delta Queue（ODQ）を定義します。

追加パラメータ	Secure Agent が SAP システムに接続するために使用する追加の SAP パラメータ。
	たとえば、SAP JCo および SAP CPIC トレースを生成するには、次のプロパティを指定します。
	`jco.client.trace="1";`
	`jco.client.cpic_trace="3";`
	実行時に、JCo および CPIC トレースファイルが次の場所に生成されます。
	`<Informatica Secure Agent installation directory>\apps\Data_Integration_Server\<DIS version>\ICS\main\bin\rdtm`
	設計時に、CPIC トレースは次の場所にある tomcat.out ファイルに生成されます。
	`<Informatica Secure Agent installation directory>\apps\Data_Integration_Server\<DIS version>tomcat.out`

差分フィールドを表示	ODP ソース上のデータ変更の原因となった操作モードをマッピングに表示するかどうかを指定します。 有効にすると、マッピングによって、Operational Delta Queue（ODQ）で有効になっている ODP ソースの **［フィールド］** タブに ODQ_CHANGEMODE および ODQ_ENTITYCNTR フィールドが生成されます。 デフォルトでは無効になっています。

次の表に、接続タイプとして **［負荷分散サーバー SNC 接続］** を選択した場合に設定する必要のあるプロパティを示します。

接続プロパティ	説明
SAP クライアント番号	SAP サーバーのクライアント番号。
SAP 言語	SAP 言語に対応する言語コード
SAP メッセージサーバー	SAP メッセージサーバのホスト名。
SAP システム ID	SAP メッセージサーバーのシステム ID。

接続プロパティ	説明
SAP グループ	ログイングループ名（例: PUBLIC）。
SNC マイネーム	オプション。Secure Agent マシンで生成された Informatica クライアントの PSE または証明書名。 デフォルトの長さは 256 です。
SNC パートナー名	SAP サーバーで生成された Informatica クライアントの PSE または証明書名。 デフォルトの長さは 256 です。
SNC 保護品質（QoP）	SAP PSE または証明書名を指定します。 以下のオプションから選択できます。 - 1 - 認証のみを適用。 - 2 - 整合性保護（認証）を適用。 - 3 - プライバシー保護（整合性と認証）を適用。 - 8 - デフォルトの保護を適用。 - 9 - 最大限の保護を適用。 デフォルトは、*[3 - プライバシー保護（整合性と認証）を適用]* です。
SAP 暗号ライブラリパス	暗号ライブラリへのパス。 Windows の場合は `sapcrypto.dll` を、Linux の場合は `libsapcrypto.so` を指定します。
X509 証明書を使用	保護の品質を指定します。X509 証明書ベースの SNC 接続を使用することを選択します。
X509 証明書のパスまたは SAP ユーザー名	X509 証明書ファイルへのパス。 X509 証明書を使用することを選択した場合は、.crt という拡張子を持つ X509 証明書ファイルへのパスを指定します。SAP ユーザー名やパスワードを指定する必要はありません。 X509 証明書を使用しない場合は、SAP サーバーで SNC が設定されている SAP ユーザー名を指定します。
サブスクライバ名	Informatica Secure Agent を SAP システムの一意のサブスクライバとして定義する名前。 SAP は、Secure Agent が ODP からデルタデータを読み取る際に、この名前を使用して一意の Operational Delta Queue（ODQ）を定義します。

接続プロパティ	説明

追加パラメータ	Secure Agent が SAP システムに接続するために使用する追加の SAP パラメータ。
	たとえば、SAP JCo および SAP CPIC トレースを生成するには、次のプロパティを指定します。
	`jco.client.trace="1";`
	`jco.client.cpic_trace="3";`
	実行時に、JCo および CPIC トレースファイルが次の場所に生成されます。
	`<Informatica Secure Agent installation directory>\apps\Data_Integration_Server\<DIS version>\ICS\main\bin\rdtm`
	設計時に、CPIC トレースは次の場所にある tomcat.out ファイルに生成されます。
	`<Informatica Secure Agent installation directory>\apps\Data_Integration_Server\<DIS version>tomcat.out`

差分フィールドを表示	ODP ソース上のデータ変更の原因となった操作モードをマッピングに表示するかどうかを指定します。 有効にすると、マッピングによって、Operational Delta Queue（ODQ）で有効になっている ODP ソースの **［フィールド］** タブに ODQ_CHANGEMODE および ODQ_ENTITYCNTR フィールドが生成されます。 デフォルトでは無効になっています。

ServiceNow Mass Ingestion 接続のプロパティ

ServiceNow Mass Ingestion 接続をセットアップする際には、接続プロパティを設定する必要があります。

ServiceNow Mass Ingestion 接続のプロパティは、接続に指定した認証方法によって異なります。接続を作成する際に、次の認証方法のいずれかを選択できます。

- **OAuth 2.0**: ServiceNow で接続用に作成された OAuth API エンドポイントの詳細を使用して、接続を認証します。この方法を使用するには、ServiceNow で OAuth API エンドポイントを作成してから、接続プロパティで API エンドポイントのクライアント ID とクライアントシークレットを指定する必要があります。ServiceNow で OAuth API エンドポイントを作成する方法の詳細については、「ServiceNow documentation」を参照してください。
- **基本**: ServiceNow アカウントのログイン資格情報を検証することにより、接続を認証します。

OAuth 2.0 認証の接続プロパティ

次の表に、OAuth 2.0 認証を使用して設定された ServiceNow Mass Ingestion 接続の接続プロパティを示します。

接続プロパティ	説明
接続名	接続の名前。この名前は、組織内で一意にする必要があります。接続名には、英数字、スペース、および次の特殊文字を含めることができます。_ .+ - 名前の先頭または末尾のスペースはトリミングされ、名前の一部として保存されません。最大長は 100 文字です。接続名では大文字と小文字は区別されません。
説明	接続の説明（オプション）。最大長は 255 文字です。

接続プロパティ	説明
タイプ	接続のタイプ。Oracle Database Ingestion 接続の場合、タイプは【ServiceNow Mass Ingestion】でなければなりません。
ランタイム環境	取り込みタスクを実行するランタイム環境の名前。 ランタイム環境として Secure Agent を指定する必要があります。 **注**: Hosted Agent やサーバーレスランタイム環境でアプリケーション取り込みタスクを実行することはできません。
ユーザー名	ServiceNow アカウントのユーザー名。
パスワード	ServiceNow アカウントのパスワード。
クライアントシークレット	ServiceNow の接続用に作成された API エンドポイントのクライアントシークレット。
クライアント ID	ServiceNow の接続用に作成された API エンドポイントのクライアント ID。
ベース URI	ServiceNow インスタンスの URL。 次の形式でベース URI を入力する必要があります。 `https://{your_servicenow_instance}.service-now.com/`
OAuth トークン URL	ServiceNow インスタンスの OAuth トークンエンドポイント。接続に関連付けられた API クライアントは、アクセストークン要求をこのエンドポイントに送信します。

基本認証の接続プロパティ

次の表に、基本認証を使用して設定された ServiceNow Mass Ingestion 接続の接続プロパティを示します。

接続プロパティ	説明
接続名	接続の名前。この名前は、組織内で一意にする必要があります。接続名には、英数字、スペース、および次の特殊文字を含めることができます。_ .+ - 名前の先頭または末尾のスペースはトリミングされ、名前の一部として保存されません。最大長は 100 文字です。接続名では大文字と小文字は区別されません。
説明	接続の説明（オプション）。最大長は 255 文字です。
タイプ	接続のタイプ。Oracle Database Ingestion 接続の場合、タイプは【ServiceNow Mass Ingestion】でなければなりません。
ランタイム環境	取り込みタスクを実行するランタイム環境の名前。 ランタイム環境として Secure Agent を指定する必要があります。 **注**: Hosted Agent やサーバーレスランタイム環境でアプリケーション取り込みタスクを実行することはできません。
ユーザー名	ServiceNow アカウントのユーザー名。

接続プロパティ	説明
パスワード	ServiceNow アカウントのパスワード。
ベース URI	ServiceNow インスタンスの URL。 次の形式でベース URI を入力する必要があります。 `https://{your_servicenow_instance}.service-now.com/`

Snowflake Data Cloud 接続のプロパティ

Snowflake Data Cloud 接続をセットアップする際には、接続プロパティを設定します。

Snowflake には次の認証方法を使用して接続できます。

- 標準。Snowflake アカウントのユーザー名とパスワードの資格情報を使用して、Snowflake に接続します。

  注: アプリケーション取り込みタスクの場合、標準認証方法のみを使用できます。
- 認証コード。認証コード付与タイプの OAuth 2.0 プロトコルを使用して、Snowflake に接続します。認証コードを使用すると、ログイン資格情報を共有または保存せずに Snowflake への承認済みアクセスが可能になります。
- KeyPair。プライベートキーファイルとプライベートキーファイルパスワード、および既存の Snowflake アカウントのユーザー名を使用して Snowflake に接続します。
- クライアント資格情報。クライアント資格情報付与タイプの OAuth 2.0 プロトコルを使用して、Snowflake に接続します。一括取り込みアプリケーションタスクおよび一括取り込みデータベースタスクには適用されません。

[接続] ページで Snowflake Data Cloud 接続を作成します。その後、Snowflake からのデータの読み取りまたは Snowflake へのデータの書き込み時にこの接続を使用できます。

標準認証

Snowflake Data Cloud 接続をセットアップする際には、接続プロパティを設定します。

次の表に、標準認証モードの Snowflake Data Cloud 接続プロパティを示します。

プロパティ	説明
接続名	接続の名前。 各接続名は組織内で一意である必要があります。接続名には、英数字、スペース、および次の特殊文字を含めることができます。_ .+ -, 最大長は 255 文字です。
説明	接続の説明。最大長は 4000 文字です。
タイプ	Snowflake Data Cloud 接続タイプ。

プロパティ	説明
ランタイム環境	タスクを実行するランタイム環境の名前。 Hosted Agent またはサーバーレスランタイム環境では、アプリケーション取り込みタスクとデータベース取り込みタスクを実行できません。
認証	コネクタが Snowflake へのログインに使用する必要のある認証方法。 **［標準］**を選択します。 デフォルトは**［標準］**です。
ユーザー名	Snowflake アカウントに接続するためのユーザー名。
パスワード	Snowflake アカウントに接続するためのパスワード。
アカウント	Snowflake アカウントの名前。 例えば、Snowflake の URL が https://<123abc>.us-east-2.aws.snowflakecomputing.com/console/login#/の場合、アカウント名は URL の最初のセグメント（snowflakecomputing.com より前）です。ここでは、123abc.us-east-2.aws がアカウント名です。 Snowsight の URL を使用する場合、例えば https://app.snowflake.com/us-east-2.aws/<123abc>/dashboard では、アカウント名は 123abc.us-east-2.aws です。 **注**: アカウント名にアンダースコアが含まれていないことを確認します。エイリアス名を使用するには、Snowflake カスタマーサポートにお問い合わせください。
ウェアハウス	Snowflake ウェアハウス名。
ロール	ユーザーに割り当てられた Snowflake ロール。

追加の JDBC URL パラメータ	追加の JDBC 接続パラメータ。
	以下の形式で、1 つ以上の JDBC 接続パラメータを入力します。
	`<param1>=<value>&<param2>=<value>&<param3>=<value>....`
	例えば、Snowflake に接続するときにデータベースとスキーマの値を渡します。
	`db=mydb&schema=public`
	重要: パラメータを追加するときは、等号（=）の前後にスペースを入れないでください。

OAuth 2.0 認証コードの認証

次の表に、OAuth 2.0 - AuthorizationCode タイプの接続の Snowflake Data Cloud 接続プロパティを示します。

プロパティ	説明
接続名	接続の名前。 各接続名は組織内で一意である必要があります。接続名には、英数字、スペース、および次の特殊文字を含めることができます。_ .+ -, 最大長は 255 文字です。
説明	接続の説明。最大長は 4000 文字です。
タイプ	Snowflake Data Cloud 接続タイプ。
ランタイム環境	タスクを実行するランタイム環境の名前。 Hosted Agent またはサーバーレスランタイム環境では、アプリケーション取り込みタスクとデータベース取り込みタスクを実行できません。
認証	Snowflake Data Cloud Connector が Snowflake へのログインに使用する必要がある認証方法。 [AuthorizationCode] を選択します。
アカウント	Snowflake アカウントの名前。 例えば、Snowflake の URL が https://<123abc>.us-east-2.aws.snowflakecomputing.com/console/login#/の場合、アカウント名は URL の最初のセグメント（snowflakecomputing.com より前）です。ここでは、123abc.us-east-2.aws がアカウント名です。 Snowsight の URL を使用する場合、例えば https://app.snowflake.com/us-east-2.aws/<123abc>/dashboard では、アカウント名は 123abc.us-east-2.aws です。 **注**: アカウント名にアンダースコアが含まれていないことを確認します。エイリアス名を使用するには、Snowflake カスタマーサポートにお問い合わせください。
ウェアハウス	Snowflake ウェアハウス名。

追加の JDBC URL パラメータ	追加の JDBC 接続パラメータ。
	以下の形式で、1 つ以上の JDBC 接続パラメータを入力します。
	`<param1>=<value>&<param2>=<value>&<param3>=<value>....`
	例えば、Snowflake に接続するときにデータベースとスキーマの値を渡します。
	`db=mydb&schema=public`
	重要: パラメータを追加するときは、等号（=）の前後にスペースを入れないでください。

認証 URL	ユーザー要求を承認するために使用する Snowflake サーバーのエンドポイント。 認証 URL は、https://<アカウント名>.snowflakecomputing.com/oauth/authorize です。この<アカウント名>には、Snowflake が提供するアカウントの完全な名前を指定します。 例: https://<abc>.snowflakecomputing.com/oauth/authorize **注**: アカウント名にアンダースコアが含まれている場合は、エイリアス名を使用します。 また、仮想プライベートクラウドネットワークで認証サーバーをサポートする認証コード付与タイプを使用することもできます。

プロパティ	説明
アクセストークン URL	アクセストークンの認証コードを交換するために使用する Snowflake アクセストークンのエンドポイント。 アクセストークンの URL は、https://<アカウント名>.snowflakecomputing.com/oauth/token-request です。この<アカウント名>には、Snowflake が提供するアカウントの完全な名前を指定します。 例: https://<abc>.snowflakecomputing.com/oauth/token-request **注**: アカウント名にアンダースコアが含まれている場合は、エイリアス名を使用します。
クライアント ID	Snowflake で OAuth タイプのセキュリティ統合を作成するときに生成されるアプリケーションのクライアント ID。 詳細については、Snowflake のドキュメントを参照してください。 一括取り込みアプリケーションタスクおよび一括取り込みデータベースタスクでは使用されません。
クライアントシークレット	クライアント ID に対して生成されたクライアントシークレット。 一括取り込みアプリケーションタスクおよび一括取り込みデータベースタスクでは使用されません。
スコープ	API エンドポイントでカスタムスコープが定義されている場合に、アクセス制御を決定します。 スペース区切りのスコープ属性を入力します。 例えば、デフォルトのユーザーロールの値を上書きするスコープとして、session:role:CQA_GCP を指定します。この値は、Security Integration で割り当てたロールの 1 つである必要があります。 一括取り込みアプリケーションタスクおよび一括取り込みデータベースタスクでは使用されません。
アクセストークンパラメータ	アクセストークン URL で使用する追加パラメータ。 パラメータを JSON 形式で定義します。 例えば、次のようなパラメータを定義します。 [{"Name":"code_verifier","Value":"5PMddu6Zcg6Tc4sbg"}] 一括取り込みアプリケーションタスクおよび一括取り込みデータベースタスクでは使用されません。
認証コードパラメータ	認証トークン URL で使用する追加パラメータ。 パラメータを JSON 形式で定義します。 例えば、次のようなパラメータを定義します。 [{"Name":"code_challenge","Value":"Ikr-vv52th0UeVRi4"}, {"Name":"code_challenge_method","Value":"S256"}] 一括取り込みアプリケーションタスクおよび一括取り込みデータベースタスクでは使用されません。
アクセストークン	アクセストークンの値。 取り込まれたアクセストークンの値を入力するか、**[トークンの生成]** をクリックして、アクセストークンの値を取り込みます。

プロパティ	説明
トークンの生成	指定した OAuth 属性に基づいてアクセストークンと更新トークンを生成します。
リフレッシュトークン	リフレッシュトークンの値。 取り込まれたリフレッシュトークンの値を入力するか、**[トークンの生成]** をクリックして、リフレッシュトークンの値を取り込みます。アクセストークンが有効でないか、有効期限切れの場合、エージェントは、リフレッシュトークンを使用して新しいアクセストークンを取得します。 **注**: リフレッシュトークンが期限切れの場合は、有効なリフレッシュトークンを指定するか、**[トークンの生成]** をクリックして新しいリフレッシュトークンを再生成します。 一括取り込みアプリケーションタスクおよび一括取り込みデータベースタスクでは使用されません。

キーペア認証

次の表に、KeyPair 認証タイプの接続の Snowflake Data Cloud 接続プロパティを示します。

接続プロパティ	説明
接続名	接続の名前。 各接続名は組織内で一意である必要があります。接続名には、英数字、スペース、および次の特殊文字を含めることができます。_ .+ -, 最大長は 255 文字です。
説明	接続の説明。最大長は 4000 文字です。
タイプ	Snowflake Data Cloud 接続タイプ。
ランタイム環境	タスクを実行するランタイム環境の名前。 Hosted Agent またはサーバーレスランタイム環境では、アプリケーション取り込みタスクとデータベース取り込みタスクを実行できません。
認証	Snowflake にログインするための認証方法。 [KeyPair] を選択します。
ユーザ名	Snowflake アカウントに接続するためのユーザー名。
アカウント	Snowflake アカウントの名前。 例えば、Snowflake の URL が https://<123abc>.us-east-2.aws.snowflakecomputing.com/console/login#/の場合、アカウント名は URL の最初のセグメント（snowflakecomputing.com より前）です。ここでは、123abc.us-east-2.aws がアカウント名です。 Snowsight の URL を使用する場合、例えば https://app.snowflake.com/us-east-2.aws/<123abc>/dashboard では、アカウント名は 123abc.us-east-2.aws です。 **注**: アカウント名にアンダースコアが含まれていないことを確認します。エイリアス名を使用するには、Snowflake カスタマーサポートにお問い合わせください。
ウェアハウス	Snowflake ウェアハウス名。

接続プロパティ	説明
追加の JDBC URL パラメータ	追加の JDBC 接続パラメータ。 以下の形式で、1 つ以上の JDBC 接続パラメータを入力します。 <param1>=<value>&<param2>=<value>&<param3>=<value>.... 例えば、Snowflake に接続するときにデータベースとスキーマの値を渡します。 db=mydb&schema=public **重要**: パラメータを追加するときは、等号（=）の前後にスペースを入れないでください。
プライベートキーファイル	プライベートキーファイル名を含む、Secure Agent が Snowflake にアクセスするのに使用するプライベートキーファイルへのパス。 例えば、次のパスとキーファイル名を指定します。 - Windows の場合: C:\Users\path_to_key_file\rsa_key.p8 - Linux の場合: /export/home/user/path_to_key_file/rsa_key.p8 **注**: キーストアが FIPS 認証されていることを確認します。
プライベートキーのパスワード	プライベートキーファイルのパスワード。

JDBC URL パラメータの設定

選択した認証タイプを問わず、Snowflake Data Cloud 接続プロパティの **[追加の JDBC URL パラメータ]** フィールドで、JDBC URL パラメータを設定できます。

一括取り込みタスクでは、次のパラメータのみが使用されます。

- 必須。Snowflake テーブルのインポート中に指定したデータベースのみを表示するには、次の形式でデータベース名を入力します。

  db=<database_name>
- オプション。オブジェクト ID 内の二重引用符を無視し、大文字と小文字を区別しないものとしてすべてのテーブルを処理するには、次のパラメータを入力します。

  QUOTED_IDENTIFIERS_IGNORE_CASE=true

  このプロパティが true に設定されている場合、Snowflake はオブジェクト ID の二重引用符を無視し、すべてのテーブルを大文字と小文字を区別しないものとして処理します。

Snowflake にアクセスするためのプライベートリンク

Azure Private Link エンドポイントを使用して Snowflake にアクセスできます。Snowflake Data Cloud 接続の作成時に、Snowflake プライベートリンクアカウント名を指定します。

Azure Private Link の設定によって、Snowflake への接続が Azure 内部ネットワークを使用して確立され、パブリックインターネットを介して行われないようにします。

プライベート Azure ネットワーク経由で Snowflake アカウントに接続するには、「Azure Private Link and Snowflake」を参照してください。

Teradata 接続のプロパティ

Teradata 接続をセットアップする際には、接続プロパティを設定する必要があります。

次の表に、Teradata 接続のプロパティを示します。

接続プロパティ	説明
接続名	接続の名前。
説明	接続の説明。
タイプ	Teradata
ランタイム環境	タスクを実行するランタイム環境の名前。 Teradata コネクタには Hosted Agent を使用できません。
TDPID	Teradata データベースマシンの名前、または IP アドレス。
固執度	Teradata データベース上で最大数の操作が実行されている場合に、Teradata PT API が継続してログオンを試行する時間（単位: 時間）。 正の整数を指定します。デフォルト値は 4 です。
データベース名	Teradata データベース名。 データベース名を入力しない場合、Teradata PT API はデフォルトのログインデータベース名を使用します。
コードページ	Teradata データベースに関連付けられているコードページ。 次のいずれかのコードページを選択します。 - MS Windows Latin 1。ISO 8859-1 Western European データの場合に選択します。 - UTF-8。Unicode および Unicode 以外のデータの場合に選択します。 Teradata ソースからデータの抽出を行うタスクを実行する場合、Teradata PT API 接続のコードページはその Teradata ソースのコードページと同じである必要があります。
最大セッション数	Teradata PT API が Teradata データベースとの間で確立するセッションの最大数。 ゼロ以外の正の整数を指定します。デフォルト値は 4 です。
最小セッション数	Teradata PT API ジョブを継続するために必要な Teradata PT API セッションの最大数。 1 から［最大セッション数］の値までの正の整数を指定します。 デフォルトは 1 です。
スリープ	Teradata データベース上で最大数の操作が実行されている場合に、Teradata PT API がログオンを再試行する前に待機する時間（分単位）。 ゼロ以外の正の整数を指定します。デフォルト値は 6 です。
データの暗号化	SQL の要求、応答およびデータの完全なセキュリティ暗号化を有効にします。 デフォルトでは無効になっています。

接続プロパティ	説明
ブロックサイズ	最大ブロックサイズ（バイト単位）。 Teradata PT API は、このプロパティを使用して、エクスポートオペレータを介してソースからデータブロックサイズを読み取ります。 Teradata Database バージョン 16.20 以降の場合、最大値は 16775168 バイトです。 Teradata Database のバージョンが 16.20 より前の場合、Teradata はブロックサイズを 16775168 バイトから最大許容値に縮小します。ブロックサイズ 16775168 は、スプールモードでは使用できません。詳細については、Teradata のログを参照し、同じバージョンの Teradata ドキュメントを確認してください。
認証タイプ	ユーザーを認証する方法。 次のいずれかの認証タイプを選択します。 - ネイティブ。接続で指定した Teradata データベースに対してユーザー名およびパスワードを認証します。 - LDAP。外部 LDAP のディレクトリサービスに対してユーザークレデンシャルを認証します。 - KRB5。Kerberos を使用して Teradata データベースを認証します。 デフォルトはネイティブです。
Kerberos アーティファクトディレクトリ	krb5.conf および IICSTPT.keytab という名前の Kerberos 構成ファイルを含むディレクトリ。 認証タイプとして KRB5 を選択した場合に適用されます。
メタデータの詳細接続プロパティ	メタデータを取得するために、JDBC ドライバのオプションのプロパティを設定する値。 例: tmode=ANSI
メタデータの資格の有効化	テーブル名またはカラム名として使用されている予約語を、Teradata 接続が Teradata データベースから読み取れるようにするために選択するオプション。 デフォルトでは、［メタデータの資格の有効化］チェックボックスは選択されておらず、Secure Agent は Teradata から予約語を読み取りません。
ユーザー名	データベースへのアクセスに必要な読み取りおよび書き込みデータベース権限を持つデータベースユーザー名。 認証タイプとして KRB5 を選択した場合、Kerberos ユーザー名を指定する必要があります。
パスワード	上記データベースユーザー名のパスワード。 認証タイプとして KRB5 を選択した場合、Kerberos ユーザーパスワードを指定する必要はありません。

Workday Mass Ingestion 接続のプロパティ

Workday Mass Ingestion 接続をセットアップする際には、接続プロパティを設定する必要があります。

Workday Mass Ingestion 接続のプロパティは、接続に指定した認証方法によって異なります。接続を作成する際に、次の認証方法のいずれかを選択できます。

- **基本**: Workday アカウントのログイン資格情報を検証することにより、接続を認証します。

- **OAuth 2.0 更新トークンフロー**: Workday に登録されているアプリケーションを使用して接続を認証します。この方法を使用するには、Workday でアプリケーションを登録してから、接続プロパティでそのアプリケーションのクライアント ID とクライアントシークレットを指定する必要があります。Workday にアプリケーションを登録する方法の詳細については、「Workday documentation」を参照してください。

基本認証の接続プロパティ

次の表に、基本認証を使用して設定された Workday Mass Ingestion 接続の接続プロパティを示します。

接続プロパティ	説明
接続名	接続の名前。この名前は、組織内で一意にする必要があります。接続名には、英数字、スペース、および次の特殊文字を含めることができます。_ .+ - 名前の先頭または末尾のスペースはトリミングされ、名前の一部として保存されません。最大長は 100 文字です。接続名では大文字と小文字は区別されません。
説明	接続の説明（オプション）。最大長は 255 文字です。
タイプ	接続のタイプ。Oracle Database Ingestion 接続の場合、タイプは【Workday Mass Ingestion】でなければなりません。
ランタイム環境	取り込みタスクを実行するランタイム環境の名前。 ランタイム環境として Secure Agent を指定する必要があります。 **注**: Hosted Agent やサーバーレスランタイム環境でアプリケーション取り込みタスクを実行することはできません。
ドメイン名	アクセスするリソースを含む Workday ドメインの名前。
テナント名	アクセスする Workday テナントの識別子。
バージョン	オプション。接続が Workday データを取得するために使用する必要があるエンドポイントの Web サービス記述言語（WSDL）バージョン。Web サービスでサポートされる操作のリストは、このフィールドで指定した WSDL バージョンによって異なります。 **注**: Workday Mass Ingestion 接続は、WSDL v37.0 に含まれていないサービスからデータを読み取らない可能性があるため、WSDL v37.0 を使用することをお勧めします。 WSDL バージョンの詳細については、「Workday Web Services (WWS) documentation」を参照してください。
ユーザー名	Workday アカウントのユーザー名。
パスワード	Workday アカウントのパスワード。

注: 基本認証方式で接続を設定してから接続をテストすると、指定した接続プロパティ値が正しくない場合でも、テストは常に成功します。したがって、接続を保存する前に、接続プロパティに正しい値を指定していることを確認してください。

OAuth 2.0 更新トークンフロー認証の接続プロパティ

次の表に、OAuth 2.0 更新トークンフロー認証を使用して設定された Workday Mass Ingestion 接続の接続プロパティを示します。

接続プロパティ	説明
接続名	接続の名前。この名前は、組織内で一意にする必要があります。接続名には、英数字、スペース、および次の特殊文字を含めることができます。_ .+ - 名前の先頭または末尾のスペースはトリミングされ、名前の一部として保存されません。最大長は 100 文字です。接続名では大文字と小文字は区別されません。
説明	接続の説明（オプション）。最大長は 255 文字です。
タイプ	接続のタイプ。Oracle Database Ingestion 接続の場合、タイプは【Workday Mass Ingestion】でなければなりません。
ランタイム環境	取り込みタスクを実行するランタイム環境の名前。 ランタイム環境として Secure Agent を指定する必要があります。 **注:** Hosted Agent やサーバーレスランタイム環境でアプリケーション取り込みタスクを実行することはできません。
ドメイン名	アクセスするリソースを含む Workday ドメインの名前。
テナント名	アクセスする Workday テナントの識別子。
バージョン	オプション。接続が Workday データを取得するために使用する必要があるエンドポイントの Web サービス記述言語（WSDL）バージョン。Web サービスでサポートされる操作のリストは、このフィールドで指定した WSDL バージョンによって異なります。 **注:** Workday Mass Ingestion 接続は、WSDL v37.0 に含まれていないサービスからデータを読み取らない可能性があるため、WSDL v37.0 を使用することをお勧めします。 WSDL バージョンの詳細については、「Workday Web Services (WWS) documentation」を参照してください。
ユーザー名	オプション。Workday アカウントのユーザー名。
クライアント ID	Workday に登録されているアプリケーションのクライアント ID。
クライアントシークレット	Workday に登録されているアプリケーションのプライベートキー。
更新トークン	Workday が登録済みアプリケーション用に生成するトークン文字列を更新します。
トークンエンドポイント	Workday インスタンスの OAuth トークンエンドポイント。登録されているアプリケーションは、このエンドポイントにアクセストークン要求を送信します。

Zendesk Mass Ingestion 接続のプロパティ

Zendesk Mass Ingestion 接続をセットアップする際には、接続プロパティを設定する必要があります。

Zendesk Mass Ingestion 接続のプロパティは、接続に指定した認証方法によって異なります。接続を作成する際に、次の認証方法のいずれかを選択できます。

- **基本**: Zendesk アカウントに関連付けられているログイン資格情報とサブドメインを使用して接続を認証します。基本認証方式では、データソースに接続する際に暗号化されたアクセストークンを使用しないため、Zendesk データにすばやく簡単にアクセスできます。

  注: 基本認証方式は、Zendesk アカウントが 2 要素認証で設定されていない場合にのみ使用できます。アカウントが 2 要素認証で設定されている場合は、接続に OAuth 2.0 認証方式を使用する必要があります。
- **OAuth 2.0**: Zendesk に登録されているアプリケーションと、Zendesk アカウントに関連付けられているログイン資格情報およびサブドメインを使用して、接続を認証します。この方法を使用するには、Zendesk でアプリケーションを登録してから、接続プロパティでそのアプリケーションのクライアント ID とクライアントシークレットを指定する必要があります。Zendesk にアプリケーションを登録する方法の詳細については、「Zendesk documentation」を参照してください。

基本認証の接続プロパティ

次の表に、基本認証を使用して設定された Zendesk Mass Ingestion 接続の接続プロパティを示します。

接続プロパティ	説明
接続名	接続の名前。この名前は、組織内で一意にする必要があります。接続名には、英数字、スペース、および次の特殊文字を含めることができます。_ .+ - 名前の先頭または末尾のスペースはトリミングされ、名前の一部として保存されません。最大長は 100 文字です。接続名では大文字と小文字は区別されません。
説明	接続の説明（オプション）。最大長は 255 文字です。
タイプ	接続のタイプ。Oracle Database Ingestion 接続の場合、タイプは【Zendesk Mass Ingestion】でなければなりません。
ランタイム環境	取り込みタスクを実行するランタイム環境の名前。 ランタイム環境として Secure Agent を指定する必要があります。 **注**: Hosted Agent やサーバーレスランタイム環境でアプリケーション取り込みタスクを実行することはできません。
電子メール ID	Zendesk アカウントのユーザー名。ユーザー名は、電子メールアドレスです。
パスワード	Zendesk アカウントのパスワード。
サブドメイン	アクセス先の Zendesk ヘルプセンターの URL。

注: 基本認証方法の詳細については、Zendesk のドキュメントを参照してください。

OAuth 2.0 認証の接続プロパティ

次の表に、OAuth 2.0 認証を使用して設定された Zendesk Mass Ingestion 接続の接続プロパティを示します。

接続プロパティ	説明
接続名	接続の名前。この名前は、組織内で一意にする必要があります。接続名には、英数字、スペース、および次の特殊文字を含めることができます。_ .+ - 名前の先頭または末尾のスペースはトリミングされ、名前の一部として保存されません。最大長は 100 文字です。接続名では大文字と小文字は区別されません。
説明	接続の説明（オプション）。最大長は 255 文字です。
タイプ	接続のタイプ。Oracle Database Ingestion 接続の場合、タイプは［Zendesk Mass Ingestion］でなければなりません。
ランタイム環境	取り込みタスクを実行するランタイム環境の名前。 ランタイム環境として Secure Agent を指定する必要があります。 **注**: Hosted Agent やサーバーレスランタイム環境でアプリケーション取り込みタスクを実行することはできません。
電子メール ID	Zendesk アカウントのユーザー名。ユーザー名は、電子メールアドレスです。
パスワード	Zendesk アカウントのパスワード。
サブドメイン	接続でアクセスする Zendesk ヘルプセンターの URL。
クライアント ID	Zendesk に登録されているアプリケーションのクライアント ID。
クライアントシークレット	Zendesk に登録されているアプリケーションのクライアントシークレット。
許可タイプ	接続で使用される OAuth 2.0 グラントタイプ。 デフォルトでは、Zendesk Mass Ingestion 接続は、パスワードグラントタイプを使用してユーザー名とパスワードをアクセストークンと交換するように設定されています。

注: OAuth 2.0 認証方法の詳細については、Zendesk のドキュメントを参照してください。

索引