Informatica®

Informatica® Intelligent Cloud Services
October 2022

接続

Informatica Intelligent Cloud Services 接続
October 2022

発行日: 2022-12-01

目次

序文

『*Informatica Intelligent Cloud Services℠接続*』では、Informatica Intelligent Cloud Services とクラウドおよび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、フラットファイルの間で接続を設定する方法を学習します。Informatica Intelligent Cloud Services で使用できるすべてのコネクタの接続プロパティについては、『*Informatica Intelligent Cloud Services 接続*』を参照してください。

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/

データ統合コネクタのドキュメント

データ統合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。

登録するには、https://status.informatica.com/に移動し、**[更新を購読登録]** をクリックします。その後、電子メール、SMS テキストメッセージ、Webhook、RSS フィードとして、またはこの 4 つを任意に組み合わせて送信された通知を受信することを選択ができます。

Informatica グローバルカスタマサポート

電話またはオンラインでカスタマサポートセンターに連絡できます。

オンラインサポートについては、Informatica Intelligent Cloud Services の **[サポート要求の送信]** をクリックしてください。またオンラインサポートを使用して問題を記録することもできます。オンラインサポートを利用するには、ログインが必要です。https://network.informatica.com/welcome でログイン要求できます。

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。タスクに含まれるソース、ルックアップオブジェクト、およびターゲットの場所を指定します。

コネクタを使用すると接続を作成できます。Informatica Intelligent Cloud Services にインストールされているコネクタの接続を作成できます。多くのコネクタはプレインストールされています。ただし、Informatica または Informatica パートナーによって作成されたアドオンコネクタをインストールすることによって、プレインストールされていないコネクタを使用することもできます。

アドオンコネクタ

アドオンコネクタは、Informatica Intelligent Cloud Services にはデフォルトでインストールされていない接続タイプの接続性を提供します。

アドオンコネクタをインストールすると、このコネクタは組織およびすべてのサブ組織で接続タイプとして利用可能になります。ユーザーはこのタイプの接続を作成し、タスクで使用できます。一部のコネクタは使用前に設定する必要があります。

組織にサブ組織が含まれる場合は、親組織にアドオンコネクタをインストールします。サブ組織にアドオンコネクタをインストールすることはできません。サブ組織が親組織で利用可能なコネクタを使用しない場合、サブ組織のコネクタライセンスを無効にします。

個々のコネクタについては、適切なコネクタのヘルプを参照してください。

まだ利用できないコネクタに対する要望がある場合、またはコネクタの構築についての情報が必要な場合は、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。

アドオンコネクタのインストール

Informatica Intelligent Cloud Services のアドオンコネクタの無料トライアル版をインストールしたり、Informatica からコネクタを購入したりできます。アドオンコネクタをインストールすると、このコネクタは組織およびすべてのサブ組織で接続タイプとして利用可能になります。

注: サブ組織で使用するアドオンコネクタをインストールする場合は、このコネクタを親組織にインストールします。アドオンコネクタはサブ組織にインストールできません。

1. 管理者で **[アドオンコネクタ]** を選択します。
2. 次のいずれかの手順に従います。

- Informatica Intelligent Cloud Services の無料トライアル版を起動すには、コネクタの **[無料トライアル]** をクリックし、無料トライアル版の起動を確認します。
- 有効期限の切れた無料トライアル版のコネクタのライセンスを購入するには、**[お問い合わせ]** をクリックします。

  Informatica の担当者から連絡があります。

コネクタをインストールすると、**[アドオンコネクタ]** ページに［使用可能なコネクタ］メッセージが表示され、接続タイプが組織およびサブ組織で使用できるようになります。接続タイプでは、「Teradata (Informatica Cloud)」など、命名規則に<コネクタ名> （<パブリッシャ名>）が使用されます。

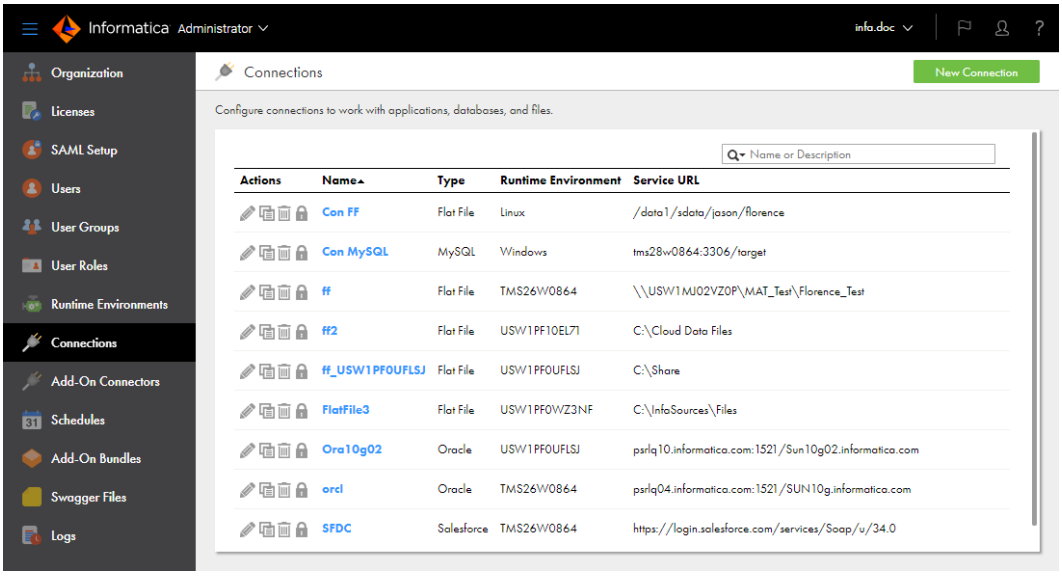
第 2 章

接続設定

接続を設定すると、この接続が組織内で利用可能になります。サブ組織を使用していて、複数のサブ組織で接続を利用可能にするには、各サブ組織でこの接続を作成します。

[接続] ページで接続を設定します。**[接続]** ページには、組織で設定されているすべての接続のリストが表示されます。このページで、接続を作成出来ます。名前または説明、名前のみ、または説明のみで既存の接続を検索することも出来ます。

次の図は、**[接続]** ページを示しています。



ほとんどの接続タイプで接続を設定する場合は、接続のランタイム環境を指定します。ランタイム環境には実行中のエージェントを含める必要があります。その他の接続タイプの場合は、タスクの設定時にランライム環境を指定します。

データベースに対する接続を設定出来ます。データベースに対するソース接続を作成する際には、データベースのテーブル、エイリアス、またはビューに対する接続を作成します。データベースに対するターゲット接続を作成する際には、データベーステーブルに対する接続を作成します。

マッピングまたはタスクでソースとターゲットの接続を設定する場合は、コードページが同じであることを確認します。タスクのソースシステムとターゲットシステムが異なるコードページを使用している場合、Informatica Intelligent Cloud Services はターゲットに予期しないデータをロードする可能性があります。

保存したクエリまたはタスクで接続が使用されていない限り、作成した接続を削除出来ます。

接続の設定

マッピングまたはタスクを設定する場合は、管理者またはウィザードの［**接続**］ページで接続を設定できます。

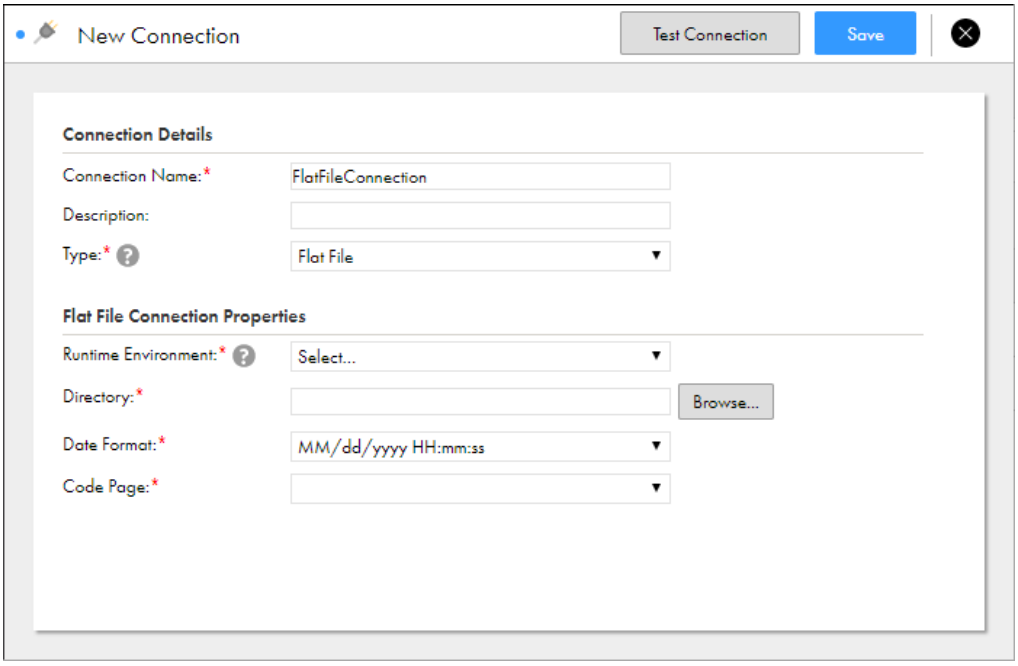
1. 次のいずれかの手順に従います。
   - 管理者で［**接続**］を選択します。
   - データ統合のマッピングまたはタスクで、ソース、ターゲット、またはルックアップオブジェクトを開きます。
2. ［**新しい接続**］をクリックします。
3. 次の接続の詳細を設定します。

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。 最大長は 255 文字です。
タイプ	Salesforce や Oracle などの接続のタイプ。

4. 接続固有のプロパティを設定します。

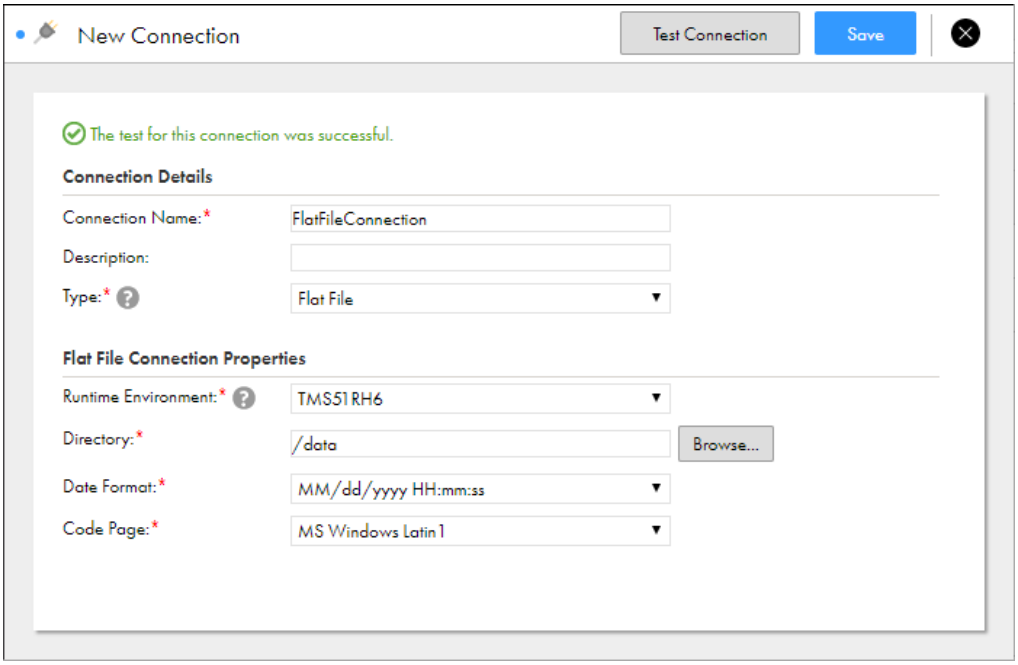
   例えば、フラットファイル接続を設定する場合は、接続で使用するランタイム環境、ファイルの保存先ディレクトリ、ファイルの日付フィールドの日付形式、ファイルをホストするシステムのコードページを入力します。

   次の画像は、フラットファイル接続のプロパティを示しています。



5. 接続をテストするには、**［テスト接続］**をクリックします。

   次の画像に示すとおり、テスト結果がページに表示されます。



   データベース接続に失敗する場合は、データベース管理者にお問い合わせください。

6. **［保存］**をクリックして接続を保存します。

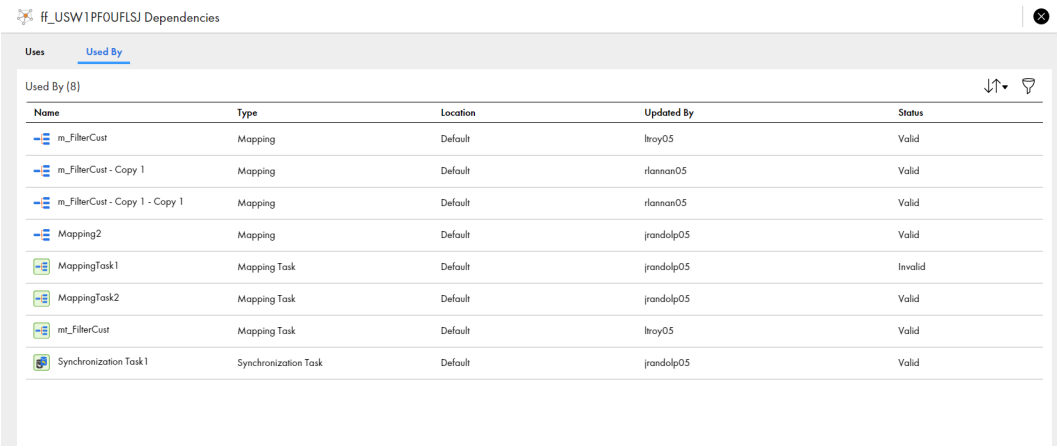
接続依存関係の表示

接続のオブジェクトの依存関係を表示できます。接続のオブジェクトの依存関係を表示すると、接続に使用されるランタイム環境と接続を使用するサービスごとのアセットのリストが管理者に表示されます。

接続のオブジェクトの依存関係を表示するには、［接続］ページで**［依存関係の表示］**アイコンをクリックします。

デフォルトでは［使用］タブが表示された**［依存関係］**ページが開きます。接続を使用するアセットを確認するには、［次により使用］タブを選択します。

次の図は、接続の［次により使用］タブのアセット依存関係を示しています。



ページに表示されるオブジェクトをソートするには、ソートアイコンをクリックしてソート基準とするプロパティのカラム名を選択します。

［依存関係］ページに表示されるオブジェクトをフィルタ処理するには、**［フィルタ］**アイコンをクリックします。フィルタを使用して特定のオブジェクトを見つけます。フィルタを適用するには、**［フィールドの追加］**をクリックし、フィルタ対象のプロパティを選択し、プロパティ値を入力します。複数のフィルタを指定できます。例えば「MyMapping」というマッピングを見つけるには、［タイプ］フィルタを追加してマッピングを指定します。次に［名前］フィルタを追加して「MyMapping」を入力します。

第 3 章

接続プロパティ

接続を設定する際には、接続の接続プロパティを指定します。接続プロパティによって、データソースに接続するためのエージェントが有効になります。

Informatica Intelligent Cloud Services にインストールされているコネクタの接続を作成出来ます。

Adabas CDC 接続のプロパティ

Adabas CDC 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、Adabas CDC 接続のプロパティを示します。

プロパティ	説明
接続名	Adabas CDC 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	Adabas CDC 接続の説明。最大長は 4000 文字です。
タイプ	接続タイプ。Adabas CDC の場合、タイプは【Adabas CDC】である必要があります。
ランタイム環境	マッピングタスクの実行に使用する Secure Agent が含まれるランタイム環境の名前。
リスナの場所	Adabas 変更データのための PWX CDC リーダー要求を処理する PowerExchange リスナがあり、PowerExchange ロッガー（Linux、UNIX、Windows 用）を実行するシステムのホスト名または IP アドレス。リスナのポート番号も含めます。次の形式で値を入力します。 *host_name* は、ホスト名または IP アドレスにできます。 *host_name*:*port_number* 以下に例を示します。 ADACDC1A:1467
ユーザー名	PowerExchange リスナセキュリティが有効化されているときに、PowerExchange リスナにアクセスするために使用できるユーザー名。詳細については、『PowerExchange リファレンスマニュアル』の「SECURITY 文」を参照してください。

プロパティ	説明
パスワード	**［ユーザー名］**プロパティで指定されるユーザー名と関連付けられたパスワード。
コレクション名	Adabas ソーステーブルのキャプチャ登録が含まれる登録グループの**［データベースインスタンス］**フィールド内に指定される Adabas インスタンス。この値は、接続の使用時に、PWX CDC メタデータアダプタがインポートする抽出マップメタデータをフィルタするために使用されます。
CAPI 接続名	PowerExchange DBMOVER コンフィギュレーションファイル内に定義される CAPX CAPI_CONNECTION 文の名前。この文には、PWX CDC リーダーが PowerExchange ロッガー（Linux、UNIX、Windows 用）ログファイルからの変更データを抽出するために使用するパラメータが含まれます。PWX CDC リーダーにこのプロパティ値が必要であり、DBMOVER コンフィギュレーションファイル内に定義される任意のデフォルトの CAPI_CONNECTION 文を無視します。
接続リトライ期限	初期接続の試行の失敗後、PWX CDC リーダーが PowerExchange リスナへの再接続を試行する秒数。接続が再試行時間中に確立できない場合、マッピングタスクに失敗します。デフォルト値は 0 であり、接続の再試行は無効になります。
圧縮	変更データをネットワーク経由で PWX CDC リーダーに送信する前に、PowerExchange リスナがデータを圧縮するかどうかを制御します。データを圧縮するには、このプロパティを選択します。デフォルトでは、このプロパティは選択されていません。
暗号化	変更データをネットワーク経由で PWX CDC リーダーに送信する前に、PowerExchange リスナがデータを暗号化するかどうかを制御します。また、使用する暗号化の種類も指定します。次のいずれかのオプションを選択します。 - **なし**。暗号化は使用しません。 - AES 128 **ビット**。128 ビットの暗号化キーを使用します。 - AES 192 **ビット**。192 ビットの暗号化キーを使用します。 - AES 256 **ビット**。256 暗号化キーを使用します。 デフォルトは**［なし］**です。
ペーシングサイズ	後続データ用に次の PWX CDC リーダー要求を待機する一時停止までに、ソースシステムが PowerExchange リスナに渡す行数またはキロバイト単位でのデータ量。この値を減らすと、セッションのパフォーマンスが向上します。パフォーマンスを最大にするには、0 を使用します。 デフォルトである最小値は 0 です。
ペーシング単位	**［ペーシングサイズ］**プロパティと一緒に使用する単位の種類。 **［行］**または**［キロバイト］**のいずれかを選択します。
マップの場所	抽出マップがあるシステムのホスト名または IP アドレス。ポート番号も含めます。 この値は、PowerExchange リスナが、抽出マップからリモートにある PowerExchange ロッガー（Linux、UNIX、Windows 用）マシン上で実行されている場合に必要です。リスナは、変更データ抽出要求を処理するために、抽出マップへのアクセスを必要とします。 次の形式で値を入力します。*host_name* は、ホスト名または IP アドレスにできます。 *host_name*:*port_number* 以下に例を示します。 ADACDC01:25100 **注**: 接続をテストして抽出マップメタデータをインポートするための**［マップの場所］**の値は、**［リスナの場所］**の値よりも優先されます。

プロパティ	説明
マップの場所のユーザー	**[マップの場所]** プロパティ内に指定された場所の PowerExchange リスナにアクセスできるユーザー名。
マップの場所のパスワード	**[マップの場所のユーザー]** プロパティで指定されるユーザー名と関連付けられたパスワード。
イベントテーブル	ユーザー定義イベントに基づく変更データ抽出を停止するためにイベントテーブルを作成した場合、イベントテーブルの PowerExchange 抽出マップの名前を入力します。イベントテーブルは、CDC ソースシステム上の Adabas テーブルである必要があります。
低値をスペースに置き換える	文字データ内の NULL をスペースに置き換えるかどうかを制御します。文字データ内の NULL を置き換えるには、このプロパティを選択します。デフォルトでは、このプロパティが選択されています。
カスタムプロパティ	PowerExchange のデフォルト設定よりも優先するために指定できるカスタムプロパティ。セミコロン（;）を区切り文字として使用することで、複数のプロパティを入力できます。通常は、Informatica グローバルカスタマサポートの指示の下でのみ、カスタムプロパティを設定します。 **注**: これらのプロパティは、PowerCenter の PowerExchange Client for PowerCenter（PWXPC）Adabas CDC 接続の **[PWX オーバーライド]** オプションと同じです。

Adabas 接続のプロパティ

Adabas 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、Adabas 接続のプロパティを示します。

プロパティ	説明
接続名	Adabas 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	Adabas 接続の説明。最大長は 4000 文字です。
タイプ	接続タイプ。Adabas の場合、タイプは [Adabas] である必要があります。
ランタイム環境	マッピングタスクの実行に使用する Secure Agent が含まれるランタイム環境の名前。

プロパティ	説明
リスナの場所	Adabas の要求を処理する PowerExchange リスナを実行するシステムのホスト名または IP アドレス。リスナのポート番号も含めます。次の形式で値を入力します。*host_name* は、ホスト名または IP アドレスにできます。 *host_name*:*port_number* 以下に例を示します。 ADALSNR:14673
ユーザー名	PowerExchange リスナセキュリティが有効化されているときに、PowerExchange リスナにアクセスするために使用できるユーザー名。詳細については、『PowerExchange リファレンスマニュアル』の「SECURITY 文」を参照してください。
パスワード	**[ユーザー名]** プロパティで指定されるユーザー名と関連付けられたパスワード。
スキーマ名	データマップのスキーマ名。
コードページ	ソースデータベースからデータを抽出するために、データ統合サービスの Secure Agent が使用するコードページ。
オフロード処理	オフロード処理を使用するかどうかを制御します。オフロード処理は、バルクデータ処理をソースシステムからターゲットシステムに転送します。次のオプションがあります。 - **自動**。オフロード処理を使用するかどうかが Cloud データ統合によって決定されます。 - **事後フィルタ**。データのフィルタリングなど、バルクデータ処理をターゲットにオフロードします。 - **事前フィルタ**。処理はターゲットにオフロードされますが、データは引き続きソースシステム上でフィルタリングされます。 - **いいえ**。オフロード処理を無効化します。 デフォルトは［いいえ］です。
オフロードスレッド	Cloud データ統合がバルクデータを処理するために使用するスレッドの数。 最適なパフォーマンスを得るには、この値が、Secure Agent が実行されているマシンに搭載済み、またはこのマシンで使用可能なプロセッサ数より大きくならないようにします。 有効な値は 1～64 です。 デフォルトは 0 です。マルチスレッド処理は無効になります。 すべての接続タイプがオフロードスレッドをサポートしているわけではありません。これらのうち、いずれかの接続の **[オフロードスレッド]** 接続属性がゼロ以外の値に設定されている場合は、スレッドなしで処理が続行されます。
配列サイズ	Adabas データセットおよびシーケンシャルファイルの場合は、パーティション化されたセッションまたはマルチスレッドセッションで使用されるストレージ配列のサイズ（単位はレコード数）。 パーティション化されたセッションの場合、この配列サイズはパーティション間で共有されます。マルチスレッドセッションの場合、各スレッドでこの配列サイズが使用されます。 有効な値は 1～5000 です。デフォルトは 25 です。 特に **[書き込みモード]** 属性で[**書き込み確認オン**]が指定されている場合、パーティション化されたセッションを調整するために配列サイズを増やします。

プロパティ	説明
低値をスペースに置き換える	文字データ内の NULL をスペースに置き換えるかどうかを制御します。文字データ内の NULL を置き換えるには、このプロパティを選択します。デフォルトでは、このプロパティが選択されています。
接続リトライ期限	初期接続の試行の失敗後、PowerExchange Bulk Reader が PowerExchange リスナへの再接続を試行する秒数。接続が再試行時間中に確立できない場合、マッピングタスクに失敗します。デフォルト値は 0 であり、接続の再試行は無効になります。
カスタムプロパティ	PowerExchange のデフォルト設定よりも優先するために指定できるカスタムプロパティ。セミコロン（;）を区切り文字として使用することで、複数のプロパティを入力できます。通常は、Informatica グローバルカスタマサポートの指示の下でのみ、カスタムプロパティを設定します。 **注**: これらのプロパティは、PowerCenter の PowerExchange Client for PowerCenter（PWXPC）Adabas 接続の［PWX **オーバーライド**］オプションと同じです。
書き込みモード	次のオプションがあります。 - **書き込み確認オン**。PowerExchange リスナにデータを送信し、成功/失敗の応答を待ってから、以降のデータを送信します。このモードではデータをバッファしないで、PowerExchange リスナにデータを同期的に送信します。 - **書き込み確認オフ**。データをバッファして PowerExchange リスナにデータを非同期的に送信します。このモードでは、成功または失敗応答を待機しません。 デフォルト値は［**書き込み確認オン**］です。

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
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。

接続プロパティ	説明
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。
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`

Adobe Experience Platform 接続のプロパティ

Adobe Experience Platform 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。

サービス統合を生成すると、アクセストークンを生成するために必要な組織固有のプロパティを取得できます。

統合用のアクセストークンを取得するには、まず、クライアント資格情報をカプセル化する JSON Web Token（JWT）を作成する必要があります。各 API セッションについて、Adobe IMS からアクセストークン用の JWT を交換できます。このトークンによって統合が認識され、設定したサービスへのアクセス権が付与されます。

以下の表に、Adobe Experience Platform に接続するたびに JWT をトークン生成するために必要な Adobe Experience Platform 接続のプロパティを示します。

プロパティ	説明
環境	Adobe Experience Platform 環境。Prod を選択します。
秘密鍵パス	Secure Agent マシンのプライベートキーのパス。 プライベートキーのパスをドライブ名なしで入力します。 例えば、プライベートキーのファイルが C ドライブのパス `C:\a_IOD\Files\AdobeExperiencePlatform\key.der` にある場合、プライベートキーのパスは以下のようになります。 `file:///a_IOD/Files/AdobeExperiencePlatform/key.der`
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 Adobe Experience Platform 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 Adobe Experience Platform のクライアント秘密鍵。
アカウント ID	Adobe Experience Platform のアカウント ID。

プロパティ	説明
IMS 組織	Adobe Identity Management System（IMS）組織の ID。
サンドボックス名	オプション。接続する Adobe Experience Platform サンドボックスアカウントの名前。

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。
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。

接続プロパティ	説明
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。

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。
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。

接続プロパティ	説明
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。

接続プロパティ	説明
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。

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	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。

接続プロパティ	説明
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。
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。
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。 **注**: - 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。

Amazon Athena 接続のプロパティ

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

次の表に、Amazon Athena の接続プロパティを示します。

接続プロパティ	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 または Hosted Agent を指定します。
認証タイプ	Amazon Athena に接続するための認証メカニズム。**[永続的な IAM 認証情報]** を選択します。
アクセスキー	オプション。Amazon Athena に接続するためのアクセスキー。

接続プロパティ	説明
秘密鍵	オプション。Amazon Athena に接続するためのシークレットキー。

JDBC URL	Amazon Athena 接続の URL。
	JDBC URL は次の形式で入力します。
	`jdbc:awsathena://AwsRegion=<region_name>;S3OutputLocation=<S3_Output_Location>;`
	ページネーションを使用して、Amazon Athena クエリの結果を取得できます。ページネーションを使用するには、プロパティに `UseResultsetStreaming=0` を設定します。
	このプロパティは次の形式で入力します。
	`jdbc:awsathena://AwsRegion=<region_name>;S3OutputLocation=<S3_Output_Location>;UseResultsetStreaming=0;`
	また、ストリーミングを使用してパフォーマンスを向上させて、Amazon Athena クエリ結果をより高速に取得することもできます。ストリーミングを使用する場合は、ポート 444 が開いていることを確認してください。
	デフォルトでは、ストリーミングが有効になっています。

顧客マスタキー ID	オプション。AWS Key Management Service（AWS KMS）によって生成された顧客マスタキー ID、またはアカウント間アクセス用のカスタムキーの Amazon リソースネーム（ARN）を指定します。 Amazon S3 バケットが存在するリージョンの顧客マスタキー ID を生成する必要があります。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 を指定できます。

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。
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。

プロパティ	説明
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
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

Amazon Aurora 接続のプロパティ

Amazon Aurora 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 Aurora 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	Amazon Aurora 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。
ホスト	Amazon Aurora サーバーのホスト名。 例: `xyzcloud-cluster.cluster-cj8irztl1mku.us-west-2.rds.amazonaws.com`。
ポート	Amazon Aurora ディレクトリサーバーのポート番号。
データベース名	Amazon Aurora データベースの名前。
コードページ	接続に定義されているデータベースサーバーのコードページ。 次のいずれかのコードページを選択します。 - MS Windows Latin 1 - UTF-8 - Shift-JIS - 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
メタデータの詳細接続プロパティ	JDBC ドライバがソースからメタデータを取得するための追加プロパティ。 以下に例を示します。`connectTimeout=180000` メタデータの詳細接続プロパティの詳細については、MariaDB Connector for JDBC を参照してください。。
ランタイムの詳細接続プロパティ	ODBC ドライバがランタイムに必要とする追加プロパティ。 例: `charset=sjis;readtimeout=180` ランタイムの詳細接続プロパティの詳細については、MariaDB Connector for ODBC を参照してください。
ユーザー名	Amazon Aurora アカウントのユーザー名。
パスワード	Amazon Aurora アカウントのパスワード。

Amazon DynamoDB V2 接続のプロパティ

Amazon DynamoDB 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、Amazon DynamoDB 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。 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	DynamoDB 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 またはサーバーレスランタイム環境を指定します。
アクセスキー	Amazon DynamoDB にアクセスするためのアクセスキー。 IAM ユーザーのロールを引き受けるときにアクセスキーを入力することもできます。
秘密鍵	Amazon DynamoDB にアクセスするための秘密鍵。この値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。 IAM ユーザーのロールを引き受けるときに秘密鍵を入力することもできます。
リージョン名	アクセスする Amazon DynamoDB の AWS リージョン。
ロールの引き受け	IAM エンティティによるロールの引き受けを有効にします。
ロール ARN の引き受け	一時的なセキュリティ資格情報を生成するための、IAM ユーザーが引き受けた IAM ロールの ARN。
外部 ID	一時的なセキュリティ資格情報を生成するための外部 ID。

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。
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。

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。
認証タイプ	認証のタイプ。 次のいずれかの値を選択します。 - AWS 認証情報プロファイル - クロスアカウント IAM ロール デフォルトは AWS 認証情報プロファイルです。 クロスアカウント IAM ロールは、ストリーミング取り込みタスクには適用されません。
AWS 資格情報プロファイル名前	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。 AWS 認証情報プロファイルの認証タイプを使用する場合は必須です。 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 ロール認証タイプを使用する場合は必須です。 ストリーミング取り込みタスクには適用されません。
外部 ID	IAM ロールの外部 ID は、IAM ロールを引き受ける事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 ロール認証タイプを使用する場合および外部 ID が AWS アカウントによって定義されている場合は必須です。 ストリーミング取り込みタスクには適用されません。

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。

プロパティ	説明
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。
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。
認証タイプ	認証のタイプ。 次のいずれかの値を選択します。 - AWS 資格情報プロファイル。 - クロスアカウント IAM ロール デフォルトは AWS 資格情報プロファイルです。 クロスアカウント IAM ロールは、ストリーミング取り込みタスクには適用されません。
AWS 資格情報プロファイル名前	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。 AWS 認証情報プロファイルの認証タイプを使用する場合は必須です。 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。

プロパティ	説明
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 ロール認証タイプを使用する場合は必須です。 ストリーミング取り込みタスクには適用されません。
外部 ID	IAM ロールの外部 ID は、IAM ロールを引き受ける事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 ロール認証タイプを使用する場合および外部 ID が AWS アカウントによって定義されている場合は必須です。 ストリーミング取り込みタスクには適用されません。

Amazon Redshift 接続のプロパティ

Amazon Redshift 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 Redshift 接続プロパティを示します。

接続プロパティ	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。
ユーザー名	Amazon Redshift アカウントのユーザー名。
パスワード	Amazon Redshift アカウントのパスワード。
スキーマ	Amazon Redshift スキーマ名。 デフォルトは public です。
AWS アクセスキー ID	オプション。Amazon S3 バケットアクセスキー ID。 EC2 システムにインストールされた Secure Agent でタスクを実行するには、アクセスキー ID を空欄にする必要がある場合があります。 EC2 システムにインストールされたのでない Secure Agent でタスクを実行するには、アクセスキー ID を指定する必要があります。
AWS シークレットアクセスキー	オプション。Amazon S3 バケットシークレットアクセスキー ID。 EC2 システムにインストールされた Secure Agent でタスクを実行するには、シークレットアクセスキーを空欄にする必要がある場合があります。 EC2 システムにインストールされたのでない Secure Agent でタスクを実行するには、シークレットアクセスキーを指定する必要があります。
マスタ対称キー	オプション。Amazon S3 暗号化キー。 256 ビット AES 暗号化キーを Base64 形式で指定します。
顧客マスタキー ID	オプション。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を指定します。Amazon S3 バケットが存在するリージョンの顧客マスタキー ID を生成する必要があります。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 を指定できます。

接続プロパティ	説明
JDBC URL	Amazon Redshift 接続 URL。
Varchar 用のマルチバイトをサポートするために必要なバイト数	［ターゲットの作成］に適用されます。ソーステーブルの Varchar 精度を参照して、ソース精度の 1x/2x/3x/4x 倍のターゲットテーブルを作成し、ターゲットテーブルにマルチバイト文字が正常に書き込めるようにします。 **注:** Varchar 精度が、最大である 65535 を超えている場合、ターゲットテーブルは作成できません。

注: 接続をテストすると、Secure Agent が Redshift 接続を検証します。AWS アクセスキーと AWS 秘密鍵の検証には、Amazon S3 バケット名が高度なソースおよびターゲットのプロパティ内に指定されている必要があります。そのため、Secure Agent は、同期またはマッピングタスクの実行時に、AWS アクセスキーと AWS 秘密鍵を検証します。

Amazon Redshift V2 接続のプロパティ

Amazon Redshift 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 Redshift 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 Redshift 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 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。 **注:** Hosted Agent は、詳細クラスタで実行されるマッピングには適用されません。
ユーザー名	Amazon Redshift アカウントのユーザー名。
パスワード	Amazon Redshift アカウントのパスワード。

プロパティ	説明
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 ステージングバケットへのアクセス権なしで、IAM ユーザーの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。 **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。
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。 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 ステージングバケットへのアクセス権なしで、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。アクセスシークレット値は入力しないでください。 **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。
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。 **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。
外部 ID	Amazon S3 ステージングバケットが別の 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確立するための外部 ID。 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。
ロールの引き受けに EC2 ロールを使用	オプション。チェックボックスを選択すると、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。 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す。
マスタ対称キー [1]	クライアントサイド暗号化を有効にする場合の、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。
JDBC URL	Amazon Redshift V2 接続の URL。 JDBC URL は次の形式で入力します。 `jdbc:redshift://<amazon_redshift_host>:<port_number>/<database_name>`

プロパティ	説明
クラスタリージョン	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。 **[クラスタリージョン]** と [JDBC URL] の両方の接続プロパティでクラスタリージョンを選択した場合、[JDBC URL] 接続プロパティで指定したクラスタリージョンは無視されます。 [JDBC URL] 接続プロパティで指定したクラスタリージョン名を使用するには、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に対してのみ、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。
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、またはアカウント間アクセス用のカスタムキーの ARN。 Amazon S3 ステージングバケットが存在するリージョンのカスタママスタキー ID を生成する必要があります。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。 詳細モードでマッピングを実行すると、同じリージョンに対してクロスアカウント KMS キーを使用できます。 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。

[1] 詳細モードのマッピングには適用されません。

Amazon S3 接続のプロパティ

Amazon S3 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 S3 接続のプロパティを示します。

接続プロパティ	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。
アクセスキー	Amazon アカウントリソースへのアクセスに使用するアクセスキー ID。AWS Identity and Access Management（IAM）認証を使用しない場合は必須です。 **注**: 接続を作成する前に有効な AWS 資格情報を所有していることを確認してください。
秘密鍵	Amazon アカウントリソースへのアクセス時に使用するシークレットアクセスキー。 この値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。アクセスキー ID を指定する場合は、この値を指定する必要があります。AWS Identity and Access Management（IAM）認証を使用しない場合は必須です。
フォルダパス	Amazon S3 オブジェクトへの完全なパス。バケット名と任意のフォルダ名が含まれている必要があります。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>
マスタ対称キー	オプション。クライアントサイド暗号化を有効にする場合に、256 ビットの AES 暗号化キーを Base64 形式で指定します。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。 この値を指定する場合は、**［スケジュール］**ページの詳細ターゲットプロパティで、暗号化タイプとしてクライアントサイド暗号化を指定してください。

接続プロパティ	説明
コードページ	Amazon S3 ソースと互換性のあるコードページ。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。 - 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。
リージョン名	Amazon S3 バケットが使用可能で、顧客マスタキー ID を生成したリージョンの名前を指定します。次のいずれかのリージョンを選択します。 - アジアパシフィック（東京） - 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） - AWS GovCloud - 中国（北京） - 欧州（アイルランド） - 欧州（フランクフルト） - 南米（サンパウロ） - 米国東部（バージニア北部） - 米国西部（北カリフォルニア） - 米国西部（オレゴン） - 米国東部（オハイオ） - カナダ（中部） - アジアパシフィック（ムンバイ） Amazon S3 コネクタが使用する AWS SDK によってサポートされるリージョンに対してのみ、データの読み取り/書き込みを行うことができます。

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。

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選択します。 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 [1]。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 [1]。シークレットアクセスキー値は入力しないでください。
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 [1]。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 [1]。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。

プロパティ	説明
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。 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>
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。
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）。 **注**: 詳細モードのマッピングでは、クロスアカウントアクセスは使用できません。 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。 - アジアパシフィック（ムンバイ） - アジアパシフィック（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） - EU（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） - 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。 **注**: 中東（バーレーン）およびアフリカ（ケープタウン）地域は、詳細モードでのマッピングには適用されません。
統合 SSO IdP[1]	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、詳細モードのマッピングには適用されません。 **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 [1]	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 [1]	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 [1]	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 [1]	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。 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。
Amazon S3 のエンドポイント DNS 名 [1]	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>` 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。
STS VPC エンドポイントタイプ [1]	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。 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。
AWS STS サービスのエンドポイント DNS 名 [1]	AWS STS インタフェースエンドポイントの DNS 名。 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。
KMS VPC エンドポイントタイプ [1]	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。 **［顧客マスタキー** ID］を選択した場合は、KMS VPC エンドポイントを設定します。 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。

プロパティ	説明
AWS KMS サービスのエンドポイント DNS 名 [1]	AWS KMS インタフェースエンドポイントの DNS 名。 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。
[1] マッピングにのみ適用されます。	

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。

Anaplan V2 接続のプロパティ

Anaplan 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、Anaplan 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	Anaplan V2 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。
説明	Anaplan V2 接続の説明。
タイプ	接続タイプ。Anaplan V2 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。
認証タイプ	［基本認証］または［証明書認証］を選択します。

接続プロパティ	説明
ユーザー名	Anaplan にログインするユーザー名。例: firstname.lastname@anaplan.com。 **注**: このフィールドを空白のままにしないでください。証明書ベースの認証を使用して接続を確立する場合でも、このフィールドにはランダムな値または文字列を入力する必要があります。
パスワード	[ユーザー名] プロパティで指定されるユーザー名と関連付けられたパスワード。
証明書パスの場所	Anaplan 認証証明書へのパス。証明書パスの場所が必要になるのは、Anaplan によって発行された証明書を使用する接続を設定し、API バージョン 1.3 を使用する場合のみです。 すなわち、証明書パスの場所が必要になるのは、認証タイプが証明書認証、メジャーバージョンが 1、およびマイナーバージョンが 3 の場合のみです。
ワークスペース ID	ワークスペースの名前または ID。 ID を取得するには、Anaplan モデルを開き、URL から selectedWorkspaceId=の後の値をコピーします。
モデル ID	モデルの名前または ID。 ID を取得するには、Anaplan モデルを開き、URL から selectedModelId=の後の値をコピーします。
API ベース URL	API ベース URL を入力します。例: https://api.anaplan.com
認証 URL	取得した認証を生成するために必要な認証サービスの URL を指定します。 例: https://auth.anaplan.com
API メジャーバージョン	Anaplan API バージョンには、メジャーバージョンとマイナーバージョンの 2 つの部分があります。 例: API バージョン 1.3 の場合、メジャーバージョンは 1 でマイナーバージョンは 3 です。 デフォルトでは、API メジャーバージョンは 1 に設定されています。 - Anaplan によって発行された証明書を使用するには、1 を選択します。API バージョン 1.x は、Anaplan によって発行された証明書をサポートします。 - 認証局によって発行された証明書を使用するには、2 を選択します。API バージョン 2.x は、認証局によって発行された証明書をサポートします。
API マイナーバージョン	デフォルトでは、API マイナーバージョンは 3 に設定されています。 - API バージョン x.3 を使用する場合は、3 を選択します。例: バージョン 1.3 - API バージョン x.0 を使用する場合は、0 を選択します。例: バージョン 2.0
最大タスク再試行回数	デフォルトでは、最大タスク再試行回数は 2 に設定されています。 これより大きい値を選択すると、同期タスクの速度が遅くなる可能性があります。
エラーダンプパスの場所	Secure Agent マシン上のエラーファイルの絶対パス。 Secure Agent は、プロセス操作ごとにエラーダンプパスの場所にサブフォルダを作成します。
API ベースのメタデータの使用	API ベースのメタデータを Anaplan からインポートし、同期タスクでファイルベースのフィールドマッピングの代わりに API ベースのフィールドマッピングを使用できます。API ベースのメタデータをインポートする際、Anaplan V2 コネクタは、Anaplan のファイルを参照せずに、Anaplan API からカラムヘッダー情報を直接読み取ります。

接続プロパティ	説明
キーストアパスの場所	Secure Agent を使用するシステム上の JAVA KeyStore ファイルへのパス。 **注**: キーストアパスの場所、キーストアのエイリアス、およびキーストアのパスワードが必要になるのは、認証局によって発行された証明書を使用する接続を設定し、API バージョン 2.0 を使用する場合のみです。
キーストアのエイリアス	キーストアファイルに保存されている証明書のエイリアス。
キーストアのパスワード	キーストアファイル内の証明書エイリアスのパスワード。

Ariba V2 接続のプロパティ

Ariba 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。

ITK または SOAP 接続を作成できます。ITK 接続を作成すると、Ariba では共有済みシークレットまたは SSL 証明書を使用した認証が可能です。

次の表に、Ariba 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	Ariba V2 コネクタの名前。
説明	Ariba V2 コネクタの説明。
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。
接続タイプ	接続のタイプ SOAP または ITK を選択できます。
サービスの URL	Ariba サービスの URL。
領域/サイト	Ariba インスタンスの領域。
データディクショナリファイルの場所	ローカルマシン上のデータディクショナリファイルの場所。
SSL 認証の使用	ITK 接続に適用されます。Secure Agent が Ariba へのセキュア接続を確立するかどうかを決定します。このオプションを選択すると、Secure Agent は暗号化された接続を確立します。 SSL 認証には［クライアントキーストア］、［クライアントキーストアパスワード］、および［クライアントキーパスワード］が必要です。
共有済みシークレット	（ITK）接続の共有済みシークレット。 Ariba ネットワークで SSL 証明書を使用して認証する場合、［共有済みシークレット］は空白のままにします。

接続プロパティ	説明
クライアントキーストア	クライアントキーストアファイルの場所。
クライアントキーストアパスワード	通信を安全に行うために必要なクライアントキーストアファイルのパスワードです。
クライアントキーパスワード	クライアントキーのパスワード。
ユーザー名	SOAP 接続の場合は必須です。Ariba アカウントのユーザー名。
パスワード	SOAP 接続の場合は必須です。Ariba アカウントのパスワード。

AS2 接続のプロパティ

AS2 サーバーの接続プロパティを設定します。

Administrator の **[接続]** ページで次のプロパティを設定します。

- AS2 接続プロパティ。AS2 サーバーへの接続を定義して、AS2 サーバーへのアクセスを有効にします。
- メッセージプロパティ。プライベートキーとパブリックキーへのアクセスおよびメッセージ暗号化設定を指定します。メッセージプロパティは、メッセージを圧縮するかどうか、およびメッセージの受信確認を送信または受信するかなど、メッセージを組織に渡す方法も定義します。
- 受信確認プロパティ。MDN 受信確認を要求するかどうか、証明書および転送エンコードのプロパティ、および MDN 受信確認を受け取る方法を指定します。
- プロキシプロパティ。プロキシサーバーを使用するかどうか、およびプロキシサーバーの詳細を指定します。

接続プロパティ

以下の表に、AS2 接続のプロパティを示します。

接続プロパティ	説明
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。
URL	メッセージを受信するサーバーの URL。URL 構文は、有効なサーバーと場所を指す必要があります。ホスト名には、IP アドレスまたはドメイン名を指定できます。ポート番号は、AS2 サーバーがリスンするポートです。
AS2 送信元 ID	送信者の名前または ID。受信側のサーバーがこの ID でフィルタリングする場合、ID が一致する必要があります。 値は大文字と小文字が区別され、1 から 128 文字の印刷可能な ASCII 文字を使用できます。値にスペースを含めることはできません。

接続プロパティ	説明
AS2 送信先 ID	受信者の名前または ID。 値は大文字と小文字が区別され、1 から 128 文字の印刷可能な ASCII 文字を使用できます。値にスペースを含めることはできません。
ユーザー名	リモート AS2 サーバーに接続するためのユーザー名。
パスワード	リモート AS2 サーバーに接続するためのパスワード。
接続タイムアウト	サーバーへの接続を試行するときに待機する最大秒数。指定された時間内に接続が成功しない場合、タイムアウトが発生します。 値が 0 または空白の場合、待機時間は無限です。 デフォルトは 60 秒です。
読み取りタイムアウト	サーバーからファイルの読み取りを試行するときに待機する最大秒数。指定された時間内にファイルが読み取られない場合、タイムアウトが発生します。 値が 0 または空白の場合、待機時間は無限です。 デフォルトは 0 秒です。
接続の再試行	接続に成功しなかった場合に、AS2 サーバーへの接続を再試行する回数。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適用されます。 値が空白の場合、再試行は行われません。 デフォルトは空白です。
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、5 秒間隔で最大 10 回接続を再試行する場合、**［接続の再試行］** を 10、**［接続再試行の間隔］** を 5 に設定します。 値が空白の場合、間隔は 0 秒になります。 デフォルトは空白です。
リダイレクトのフォロー	接続の作成時に、リダイレクトリンクをフォローするかどうか。 デフォルトは false です。
ユーザーエージェント	メッセージを作成または送信したアプリケーションを示すためにメッセージヘッダーで使用される値。
チャンクエンコードの使用	要求の長さを事前計算するかどうか、または要求をチャンクで送信するかどうか。大きなファイルを送信する場合、コンテンツの長さを事前計算すると、パフォーマンスが低下することがあります。ただし、すべての AS2 サーバーでチャンクエンコードがサポートされるわけではありません。 デフォルトは false です。
クライアント証明書エイリアス	受信側の AS2 サーバーから要求された場合に、クライアント認証に使用するデフォルトのキーストア内のキーのエイリアス。
SSL コンテキストプロトコル	SSLContext の作成時に使用されるプロトコル。指定するプロトコルは、Java Runtime Environment（JRE）にインストールされているセキュリティプロバイダによって異なります。 **注**: ほとんどの場合、デフォルト値の SSL が適しています。ただし、一部の IBM JRE 実装では、接続先のサーバーが SSLv3 をサポートしていない場合、デフォルト値の SSL は機能しません。 デフォルトは SSL です。

このセクションに実際の情報を入力します（オプション）。

接続プロパティ

メッセージのプロパティ

以下の表に、AS2 接続メッセージのプロパティを示します。

接続プロパティ	説明
トラストストアの場所	パブリックキー証明書を格納するトラストストアへのパス。Secure Agent マシン上、または Secure Agent がアクセス可能なサーバー上にある必要があります。
トラストストアのパスワード	トラストストアにアクセスするためのパスワード。
メッセージの暗号化	転送時にメッセージを暗号化するかどうか。暗号化されたトンネル内でのメッセージの暗号化は任意ですが、強く推奨されます。 デフォルトは false です。
暗号化アルゴリズム	メッセージの暗号化に使用するアルゴリズム。次のいずれかのアルゴリズムを選択します。 - AES128 - AES256 - CAST5 - IDEA - TRIPLE-DES - RC2 デフォルトは AES128 です。
暗号化証明書エイリアス	デフォルトの信頼済み証明書キーストアで送信メッセージを暗号化するために使用する証明書エイリアス。
メッセージの署名	メッセージをデジタル署名で署名するかどうか。メッセージの署名は任意ですが、強く推奨されます。 デフォルトは false です。
プライベートキーストアの場所	プライベートキーおよび関連する証明書を格納するキーストアの場所。メッセージの署名が有効になっている場合に適用されます。
プライベートキーストアのパスワード	キーストアにアクセスするためのパスワード。メッセージの署名が有効になっている場合に適用されます。
署名アルゴリズム	メッセージの署名に使用するアルゴリズム。メッセージの署名が有効になっている場合に適用されます。 次のいずれかのアルゴリズムを選択します。 - SHA1 - SHA224 - SHA256 - SHA384 - SHA512 - MD5 デフォルトは SHA1 です。

接続プロパティ	説明
署名証明書エイリアス	メッセージの署名に使用するプライベートキーエイリアス。プライベートキーは、デフォルトのプライベートキーストアにあります。
メッセージの圧縮	帯域幅を削減するためにメッセージを圧縮するかどうか。このオプションを有効にすると、Informatica Intelligent Cloud Services は zlib 形式でメッセージを圧縮します。 デフォルトは false です。

受信確認のプロパティ

以下の表に、AS2 接続の受信確認のプロパティを示します。

接続プロパティ	説明
受信確認証明書エイリアス	受信確認証明書のエイリアス。署名付き受信確認を要求するように接続を設定する場合に適用されます。 AS2 コネクタは受信確認証明書を使用して、受信確認に署名した証明書が、デフォルトの信頼済み証明書キーストアの証明書であることを確認します。 受信確認署名に埋め込み証明書が含まれる場合は、オプションです。受信確認署名に埋め込み証明書が含まれない場合は、受信確認証明書エイリアスを指定する必要があります。
受信確認転送エンコード	メッセージの受信確認に使用するエンコードのタイプ。これは、受信確認に転送エンコードが含まれない場合に便利です。 以下のいずれかの値を使用します。 - base64 - quoted-printable - 7bit - 8bit - binary
受信確認要求	サーバーがメッセージを受信するときに、MDN 受信確認を要求するかどうか。次のいずれかのオプションを選択します。 - なし。受信確認を要求しません。 - 署名済み。デジタル署名で署名された受信確認を要求します。 - 署名なし。デジタル署名なしの受信確認を要求します。 デフォルトは［なし］です。
宛先	MDN を受け取るモード。受信確認を要求する場合に適用されます。 次のいずれかの値を選択します。 - Joblog。MDN を、モニタでアクセスできるジョブログで受け取ります。 - ファイル。MDN をファイルで受け取ります。 - 電子メール。MDN を電子メールで受け取ります。 - URL。MDN を、URL を介して受け取ります。 - 破棄。MDN を破棄します。 デフォルトは Joblog です。
ファイル	MDN を保存するファイル名を含むパス。ファイルの宛先に適用されます。

接続プロパティ	説明
ファイルが存在する場合	受信確認ファイルがすでに存在する場合に、名前の競合を解決する方法を決定します。ファイルの宛先に適用されます。 次のいずれかの値を選択します。 - 名前の変更。連番を追加して、新しい受信確認ファイルの名前を変更します。例: fileMdn 2.txt、fileMdn 3.txt - 付加。既存のファイルに受信確認を付加します。 - 上書き。既存の受信確認ファイルの内容を上書きします。 - スキップ。受信確認をアップロードしません。 - エラー。ファイル名が重複するとエラーが発生します。 デフォルトは［名前の変更］です。
電子メールアドレス	受信確認の送信先の電子メールアドレス。電子メールの宛先に適用されます。
受信確認 URL	受信確認を投稿する URL。URL の宛先に適用されます。

プロキシのプロパティ

以下の表に、AS2 接続のプロキシのプロパティを示します。

接続プロパティ	説明
有効	プロキシサーバーがコネクタに対して有効かどうかを決定します。 デフォルトでは無効になっています。
プロキシタイプ	この接続に使用するプロキシサーバーのタイプ。 次のいずれかのタイプを選択します。 - SOCKS。SOCKS バージョン 4 または 5 を使用できます。 - HTTPS。 - Informatica ファイルサーバープロキシ。 使用するプロキシサーバーのタイプをネットワーク管理者に確認してください。
ホスト	ネットワークのプロキシサーバーのホスト名または IP アドレス。
代替ホスト	ネットワークの代替プロキシサーバーのホスト名または IP アドレス。代替プロキシサーバーは、プライマリプロキシサーバーが使用できないときに使用されます。
ポート	ネットワークのプロキシサーバーのポート番号。空欄のままにした場合、HTTP のデフォルトポートは 80 であり、SOCKS のデフォルトポートは 1080 です。
ユーザー	プロキシサーバーに接続するときのログインに使用するユーザー名。
パスワード	プロキシサーバーに接続するためのパスワード。HTTP 接続または HTTPS 接続を作成するためのネットワークがプロキシサーバーを使用する場合に必須。

Birst Cloud 接続のプロパティ

Birst 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する必要があります。

次の表に、Birst Cloud 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	Birst Cloud 接続コネクタの名前。
説明	Birst Cloud 接続コネクタの説明。
タイプ	Birst Cloud 接続を選択します。
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	Birst Cloud 接続アプリケーションのユーザー名。
パスワード	Birst Cloud 接続アプリケーションのパスワード。
エンドポイント URL	Birst Web サービスのエンドポイント URL。
スペース ID	データのアップロード元の Birst スペースの UDID。
デバッグロガーを有効にする	デバッグログを有効にする場合に選択します。
設定場所	内部設定の一時ストレージ。

Business 360 接続のプロパティ

Business 360 接続の作成時に、接続のプロパティを設定する必要があります。

次の表に、Business 360 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 100 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	接続タイプ。[Business 360] を選択します。
ランタイム環境	マッピング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。
ランタイムパラメータ	入力ジョブとエクスポートジョブを処理するためのシステム生成のジョブインスタンス ID。 **注**: この属性は変更しないでください。

Business 360 イベント接続のプロパティ

Business 360 イベント接続の作成時に、接続のプロパティを設定する必要があります。

次の表に、Business 360 イベント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 100 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	接続タイプ。[Business 360 **イベント**] を選択します。
ランタイム環境	マッピング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。
開始タイムスタンプ	Business 360 データストアからイベントを取得する時間範囲の開始時刻を設定するための、システム生成のタイムスタンプ変数。 **注**: この属性を変更することはできません。
終了タイムスタンプ	Business 360 データストアからイベントを取得する時間範囲の終了時刻を設定するための、システム生成のタイムスタンプ変数。 **注**: この属性を変更することはできません。

Business 360 FEP 接続のプロパティ

Business 360 FEP 接続の作成時に、接続のプロパティを設定する必要があります。

次の表に、Business 360 FEP 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 100 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	接続タイプ。[Business 360 FEP **コネクタ**] を選択します。
ランタイム環境	マッピング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。
ランタイムパラメータ	入力ジョブを処理するための、システム生成のジョブインスタンス ID。 **注**: この属性は変更しないでください。

CallidusCloud Commissions 接続のプロパティ

CallidusCloud Commissions 接続を作成する際には、接続プロパティを設定する必要があります。

次の表に、CallidusCloud Commissions 接続のプロパティを示します。

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。
UserName	CallidusCloud ポータルログインのユーザー名。
Password	CallidusCloud ポータルログインのパスワード。
BaseURL	CallidusCloud アプリケーションに接続するためのベース URL。 ベース URL を指定するには、次のサンプルを使用します。 https://<domainName>/TrueComp-SaaS/services/rest/
PageSize	読み取り操作のページサイズ。 デフォルト値は 10 です。

CallidusCloud Commissions 接続のガイドライン

Secure Agent の JVM オプションを使用して、要件に応じてセッションタイムアウトプロパティの値を設定できます。

以下のプロパティを設定することができます。

- セッションタイムアウト: CallidusCloud Commissions エンドポイントとのセッションがタイムアウトするまでの秒単位の時間。
- 試行回数: CallidusCloud Commissions エンドポイントへの再接続の試行回数。
- 再試行までの待機時間: 2 回の試行間の秒単位の時間。

プロパティの値をデフォルト値よりも高く設定する必要があります。そうしないと、デフォルト値が考慮されます。

デフォルト値は次のとおりです。

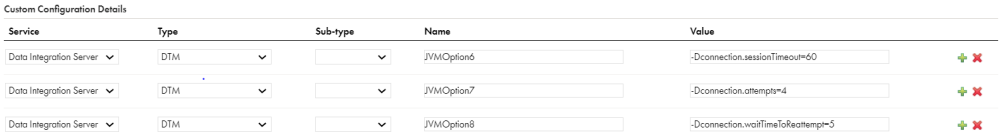
```
-Dconnection.sessionTimeout=50

-Dconnection.attempts=3

-Dconnection.waitTimeToReattempt=5
```

次の手順を実行して、JVM オプションを設定します。

1. Administrator で、**[ランタイム環境]** タブにリストされている Secure Agent を選択します。
2. **[編集]** をクリックします。
3. **[システム構成の詳細]** セクションで、サービスとして **[データ統合サーバー]** を選択し、タイプとして **[DTM]** を選択します。
4. JVM オプションの値を指定します。



5. **［保存］**をクリックします。

CallidusCloud File Processor 接続のプロパティ

CallidusCloud File Processor 接続を作成する際には、接続プロパティを設定する必要があります。

次の表に、CallidusCloud File Processor 接続のプロパティを示します。

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。
UserName	SFTP サーバーへの接続に使用するユーザー名。
Password	SFTP サーバーへの接続に使用するパスワード。
SFTP キー	SFTP サーバーへの接続に使用するプライベートキー。SFTP キーは単一の行内に指定する必要があります。
SFTP キーパスフレーズ	SFTP サーバーに接続するためのパスフレーズ。SFTP キーパスフレーズは単一の行内に指定する必要があります。
ホスト	SFTP サーバーのホスト名。
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 22 になります。
リモートディレクトリ	Secure Agent にアクセス可能な SFTP ホストのディレクトリ。 **注**: 指定するパスの末尾に/を追加します。
Charset	エンコードデータに使用する文字セットを指定します。 CallidusCloud File Processor コネクタでは、次の文字セットがサポートされます。 - Big5 - Big5-HKSCS - CESU-8 - EUC-JP - EUC-KR - GB18030 - GB2312 - GBK - IBM00858 - IBM01140 - IBM01141 - IBM01142 - IBM01143 - IBM01144 - IBM01145 - UTF-8 デフォルト値は UTF-8 であり、すべての文字データに対して機能します。
区切り文字	データのカラムを区切るためにファイル内で使用される区切り文字。 区切り文字を選択します。デフォルトの区切り文字はカンマです。

プロパティ	説明
圧縮モード	バイナリファイルの圧縮形式。次のいずれかのオプションを選択します。 - なし - gzip デフォルトは［なし］です。
暗号化モード	SFTP サーバーがデータの暗号化に使用する暗号化のタイプ。次のいずれかのオプションを選択します。 - なし - GPG デフォルトは［なし］です。
暗号化パブリックキー	[GPG] を **[暗号化モード]** として選択したときに必須です。データを暗号化するパブリックキーは、単一の行内に指定する必要があります。
暗号化プライベートキー	[GPG] を **[暗号化モード]** として選択したときに必須です。データを復号化するプライベートキーは、単一の行内に指定する必要があります。
暗号化パスフレーズ	[GPG] を **[暗号化モード]** として選択したときに必須です。データを暗号化するパスフレーズは、単一の行内に指定する必要があります。

複数行のキーファイルまたはパスフレーズを単一行のキー文字列に変換する方法の詳細については、CallidusCloud File Processor のドキュメントを参照してください。

Chatter 接続のプロパティ

Chatter コネクタを同期タスクで使用するには、データ統合で接続を作成し、接続プロパティを設定する必要があります。

次の表に、Chatter 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。
タイプ	接続タイプ。[Chatter] 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	Chatter アカウントのユーザー名。
パスワード	Chatter アカウントのパスワード。
セキュリティトークン	Salesforce から生成されたセキュリティトークン。
サービスの URL	API バージョンが付いたサービスエンドポイント URL。Chatter コネクタは、API バージョン 34.0 までをサポートします。 例: `https://login.salesforce.com/services/Soap/u/34.0`
添付パス	フィードの添付ファイルがコピーされる必要がある場所のパス。

Concur V2 接続のプロパティ

Concur V2 接続をセットアップするとき、ユーザーを認証して Concur データへのアクセスを承認するために混合 OAuth 2 または OAuth 2 接続を指定できます。OAuth 2 接続タイプを使用することをお勧めします。

次の表に、混合 OAuth 2 接続タイプ用の Concur V2 接続のプロパティを示します。

接続プロパティ	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。
認証	Secure Agent は、Concur データに対してユーザーを認証してアクセスを承認するために OAuth 2 を使用します。
ユーザー名	Concur Web ページにログインするためのユーザー名。
[パスワード]	ユーザー名に関連付けられるパスワード。
コンシューマキー	Concur 管理者が組織のパートナーアプリケーションの登録時に生成したキー。 **注**: Informatica は、将来のリリースでコンシューマキー認証のサポートを廃止する予定です。コンシューマキー認証が廃止される前に、OAuth 認証を使用する方法に移行する必要があります。
フォルダ	Concur からアクセスするオブジェクトへの相対パス。 例えば、API 呼び出しの URL が `https://us-impl.api.concursolutions.com` で、Concur から経費レポートを取得する API を呼び出すための絶対パスが `https://us-impl.api.concursolutions.com/api/expense/report` の場合は、*/expense/report* という相対パスを入力します。

次の表に、OAuth 2 接続タイプ用の接続プロパティを示します。

接続プロパティ	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。
認証	Secure Agent は、Concur データに対してユーザーを認証してアクセスを承認するために OAuth 2 を使用します。
ユーザー名	Concur Web ページにログインするためのユーザー名。
[パスワード]	ユーザー名に関連付けられるパスワード。
OAuth 2 を使用	Secure Agent は、Concur データに対してユーザーを認証してアクセスを承認するために OAuth 2 を使用します。 新規 OAuth 2 資格情報を取得するには SAP Concur にお問い合わせください。 OAuth 2 の使用を指定しない場合、混合 OAuth 2 接続タイプが使用されます。

接続プロパティ	説明
認証用ベース URL	アカウント作成時に Concur から受け取った認証用 URL。 ［認証用ベース URL］は、承認 URL から派生したものです。 例えば、承認 URL が https://us-impl.api.concursolutions.com/oauth2/v0/token の場合、［認証用ベース URL］は https://us-impl.api.concursolutions.com です。
API 呼び出し用ベース URL	アカウント作成時に Concur から受け取った API 呼び出し用 URL。
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一意の ID。
シークレット ID	Active Directory で OAuth 認証を完了するためのアプリケーションのパスワード。
フォルダ	Concur からアクセスするオブジェクトへの相対パス。 例えば、API 呼び出しの URL が https://us-impl.api.concursolutions.com で、Concur から経費レポートを取得する API を呼び出すための絶対パスが https://us-impl.api.concursolutions.com/api/expense/report の場合は、*/expense/report* という相対パスを入力します。

Couchbase 接続のプロパティ

Couchbase 接続を作成する際には、接続プロパティを設定する必要があります。

次の表に、Couchbase 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	接続タイプ。[Couchbase] 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。
ホスト名	Couchbase サーバーのホスト名または IP アドレス。
ポート	Couchbase サーバーのポート番号。デフォルトは 9042 です。
ユーザー名	Couchbase サーバーにアクセスするためのユーザー名。

プロパティ	説明
パスワード	Couchbase サーバーにアクセスするためのユーザー名に対応するパスワード。
SSL モード	Couchbase コネクタには適用されません。 **[無効]** を選択します。
SSL 証明書パス	Couchbase コネクタには適用されません。
追加接続プロパティ	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>` Couchbase コネクタは、次の接続パラメータをサポートします。 QueryMode Couchbase サーバーへのクエリの送信に使用します。 LogLevel Secure Agent がセッションログにエラーメッセージを記録するかどうかを指定します。 LogPath ロギングが有効な場合にドライバがログファイルを保存するフォルダの完全パス。 AuthMech ドライバが Couchbase サーバーへの接続に使用する認証メカニズム。

Coupa V2 接続のプロパティ

Coupa V2 接続を作成する際には、接続プロパティを設定する必要があります。

次の表に、Coupa V2 接続のプロパティを示します。

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。
認証	**[Coupa V2]** を選択します。
ベース URL	Coupa API に接続するためのベース URL。ベース URL を次の形式で指定します。 `https://{instance_name}.coupahost.com/` 例: https://companyname.coupahost.com/
認証タイプ	Coupa V2 接続の認証タイプ。 API キー認証または OAuth 2.0 認証を選択できます。 **注:** Informatica では、OAuth 2.0 認証を使用して Coupa に接続することをお勧めします。

プロパティ	説明
COUPA API KEY	API キー認証に必要です。 Coupa インスタンスに接続するための固有の API キー。 Coupa API キーの作成方法の詳細については、Coupa documentation を参照してください。
クライアント ID	OAuth 2.0 認証に必要です。 有効なアクセストークンを生成するために必要な Coupa クライアント ID。 クライアント ID として Coupa ID を指定します。
クライアントシークレット	OAuth 2.0 認証に必要です。 有効なアクセストークンを生成するために必要な Coupa クライアントシークレット。 Coupa シークレットをクライアントシークレットとして指定します。
スコープ	OAuth 2.0 認証に必要です。 Coupa へのアクセスを承認するために使用されるスコープ。 Coupa のユーザーに定義されたスコープを入力します。複数のスコープを入力するには、スコープをスペースで区切って指定します。

カスタムフィールド設定	Coupa オブジェクトのカスタムフィールドを指定します。
	次の形式を使用して Coupa のカスタムフィールドを指定します。FieldName は Coupa のカスタムフィールド名の値、FieldType はカスタムフィールドのタイプです。IsAPIGlobalNamespace は、**[フィールドマッピング]** タブでカスタムフィールドをルートタグとカスタムフィールドタグのどちらに表示するかを決定します。
	`Object1=FieldName1,FieldType,DataType, IsAPIGlobalNamespace;\`
	`FieldName2,FieldType,DataType, IsAPIGlobalNamespace;\`
	`FieldName3,FieldType,DataType,IsAPIGlobalNamespace`
	`Object2=FieldName1,FieldType,DataType, IsAPIGlobalNamespace;\`
	`FieldName2,FieldType,DataType, IsAPIGlobalNamespace`
	`Object3=FieldName1,FieldType,DataType,IsAPIGlobalNamespace;\`
	`FieldName2,FieldType,DataType,IsAPIGlobalNamespace;\`
	`FieldName3,FieldType,DataType,IsAPIGlobalNamespace`
	Coupa V2 コネクタは、簡易カスタムフィールドのみをサポートします。
	以下に例を示します。
	`user-summary=custom_field1,Simple,String,true;\`
	`custom_field2,Simple,String, false`
	`requisition-header=requisition_cf1,Simple,String,true;\`
	`requisition_cf2,Simple,Integer,false;\`
	`requisition_cf3,Simple,Integer`
	`user=user_customfield1,Simple,String,false;\`
	`user_customfield_2,Simple,String,true`
	注: Secure Agent は、カスタムフィールド名内のアンダースコアをハイフンに置き換えて、**[フィールドマッピング]** タブ内のカスタムフィールド名を表示します。

Cvent 接続のプロパティ

Cvent 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、Cvent 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	Cvent 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マッピングに指定できます。
アカウント番号	アカウント番号を指定します。
ユーザー名	Cvent API のユーザー名。
パスワード	Cvent API のパスワード。
エンドポイント URL	Cvent アプリケーションのエンドポイント URL。
バッチサイズ	一度に取得するレコード数。 最大値は 200 です。
UTC タイムゾーン	Coupa UTC タイムゾーン。 日付と時刻のフィールドにタイムゾーンを入力します。 タイムゾーンは、日付と時刻のフィールドのフィルタ値に追加されます。
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。

Databricks Delta 接続のプロパティ

Databricks Delta 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、Databricks Delta 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	Databricks Delta 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指定できます。 Hosted Agent は、詳細モードのマッピングには適用されません。 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、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。
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。 以下の構文を使用します。 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> **注**: URL は、Databricks Delta のアナリティクスクラスタまたは汎用クラスタにある、JDBC または ODBC の［詳細オプション］から取得できます。 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	Databricks アナリティクスクラスタの ID。 クラスタ ID は、JDBC URL から取得できます。 以下の構文を使用します。 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。 以下の構文を使用します。 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 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。 クラスタに接続するための権限が、**［クラスタ** ID］プロパティに指定されていることを確認します。 マッピングの場合は、データエンジニアリングクラスタを作成するための追加の権限が必要です。

プロパティ	説明

SQL エンドポイント JDBC URL	Databricks SQL エンドポイントの JDBC 接続 URL。
	以下の構文を使用します。
	`jdbc:spark://<Databricks Host>:443/default;transportMode=http;ssl=1;AuthMech=3;httpPath=/sql/1.0/endpoints/<SQL endpoint cluster ID>;`
	アプリケーションの取り込みタスクとデータベースの取り込みタスクの場合、次のように、URL の先頭にプレフィックス jdbc:databricks://を付けます。
	`jdbc:databricks://<Databricks Host>:443/default;transportMode=http;ssl=1;AuthMech=3;httpPath=/sql/1.0/endpoints/<SQL endpoint cluster ID>;`
	このフィールドは、Databricks SQL エンドポイントに接続するために必要です。
	データ統合の場合、このフィールドは Databricks SQL エンドポイントに接続するために必要です。Secure Agent で必要な環境変数を設定してください。
	注: ［SQL エンドポイント 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。
	Databricks Delta SQL エンドポイントの詳細については、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。

データベース	接続先となる Databricks Delta のデータベース。 データ統合の場合、デフォルトでは、ワークスペースで使用可能なすべてのデータベースが一覧表示されます。
JDBC ドライバクラス名	JDBC ドライバクラスの名前。 ドライバクラス名を `com.simba.spark.jdbc.Driver` として指定します。 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。
クラスタ環境	Databricks クラスタがデプロイされるクラウドプロバイダ。 次のオプションから選択します。 - AWS - Azure デフォルトは AWS です。 接続属性は、選択したクラスタ環境に応じて異なります。詳細については、AWS クラスタおよび Azure クラスタのプロパティに関するセクションを参照してください。
最小ワーカー数 [1]	Spark ジョブに使用される最小のワーカーノードの数。 マッピングの場合は必須で、最小値は 1 です。
最大ワーカー数 [1]	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に設定するか、最大ワーカー数を設定しないでください。
DB ランタイムバージョン [1]	Databricks ランタイムバージョン。 リストから［7.3 LTS］を選択します。
ワーカーノードタイプ [1]	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。 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 [1]	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。 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[1]	Spark クラスタに使用されるインスタンスプール ID。 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
Elastic Disk を有効にする [1]	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。 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 [1]	Databricks クラスタで使用される Spark 設定。
	設定は次の形式である必要があります。
	`"key1"="value1";"key2"="value2";....`
	以下に例を示します。
	`"spark.executor.userClassPathFirst"="False"`

Spark 環境変数 [1]	Spark ドライバとワーカーの起動前にエクスポートする環境変数。
	この変数は、以下の形式で指定する必要があります。
	`"key1"="value1";"key2"="value2";....`
	以下に例を示します。
	`"MY_ENVIRONMENT_VARIABLE"="true"`

[1] 詳細モードのマッピングには適用されません。	

実行時にジョブクラスタを起動するには、マッピングタスクに次のプロパティが必要です。

- 最小ワーカー数
- 最大ワーカー数
- DB ランタイムバージョン
- ワーカーノードタイプ
- ドライバノードタイプ
- Elastic Disk を有効にする
- Spark 設定
- Spark 環境変数
- ゾーン ID
- EBS ボリュームタイプ
- EBS ボリューム数

- EBS ボリュームサイズ

AWS クラスタのプロパティ

Databricks Delta 接続をセットアップする際には、選択したクラスタ環境に基づいて接続プロパティを設定します。

次の表に、AWS クラスタ環境を選択した場合に適用される Databricks Delta の接続プロパティを示します。

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。 デフォルトは永続的な IAM 認証情報です。
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 [1]	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。
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。 デフォルトは `s3.amazonaws.com` です。
ゾーン ID[1]	Databricks ジョブクラスタのゾーン ID。 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 [1]	クラスタで起動される EBS ボリュームのタイプ。
EBS ボリューム数 [1]	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。 **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 [1]	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）。
[1] 詳細モードのマッピングには適用されません。	

Azure クラスタのプロパティ

Databricks Delta 接続をセットアップする際には、選択したクラスタ環境に基づいて接続プロパティを設定します。

次の表に、Azure クラスタ環境を選択した場合に適用される Databricks Delta の接続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秘密鍵。
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 データ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 [1]	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。
[1] 詳細モードのマッピングには適用されません。	

Datacom CDC 接続のプロパティ

Datacom CDC 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、Datacom CDC 接続のプロパティを示します。

プロパティ	説明
接続名	Datacom CDC 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	Datacom CDC 接続の説明。最大長は 4000 文字です。
タイプ	接続タイプ。Datacom CDC の場合、タイプは［Datacom CDC］である必要があります。
ランタイム環境	マッピングタスクの実行に使用する Secure Agent が含まれるランタイム環境の名前。

プロパティ	説明
リスナの場所	Datacom 変更データのための PWX CDC リーダー要求を処理する PowerExchange リスナがあり、PowerExchange ロッガー（Linux、UNIX、Windows 用）を実行するシステムのホスト名または IP アドレス。リスナのポート番号も含めます。次の形式で値を入力します。 *host_name* は、ホスト名または IP アドレスにできます。 *host_name*:*port_number* 以下に例を示します。 ADACDC1A:1467
ユーザー名	PowerExchange リスナセキュリティが有効化されているときに、PowerExchange リスナにアクセスするために使用できるユーザー名。詳細については、『PowerExchange リファレンスマニュアル』の「SECURITY 文」を参照してください。
パスワード	**［ユーザー名］**プロパティで指定されるユーザー名と関連付けられたパスワード。
コレクション名	Datacom ソーステーブルのキャプチャ登録が含まれる登録グループの**［データベースインスタンス］**フィールドに指定される Datacom インスタンス。この値は、接続の使用時に、PWX CDC メタデータアダプタがインポートする抽出マップメタデータをフィルタするために使用されます。
CAPI 接続名	PowerExchange DBMOVER コンフィギュレーションファイル内に定義される CAPX CAPI_CONNECTION 文の名前。この文には、PWX CDC リーダーが PowerExchange ロッガー（Linux、UNIX、Windows 用）ログファイルからの変更データを抽出するために使用するパラメータが含まれます。PWX CDC リーダーにこのプロパティ値が必要であり、DBMOVER コンフィギュレーションファイル内に定義される任意のデフォルトの CAPI_CONNECTION 文を無視します。
接続リトライ期限	初期接続の試行の失敗後、PWX CDC リーダーが PowerExchange リスナへの再接続を試行する秒数。接続が再試行時間中に確立できない場合、マッピングタスクに失敗します。デフォルト値は 0 であり、接続の再試行は無効になります。
圧縮	変更データをネットワーク経由で PWX CDC リーダーに送信する前に、PowerExchange リスナがデータを圧縮するかどうかを制御します。データを圧縮するには、このプロパティを選択します。デフォルトでは、このプロパティは選択されていません。
暗号化	変更データをネットワーク経由で PWX CDC リーダーに送信する前に、PowerExchange リスナがデータを暗号化するかどうかを制御します。また、使用する暗号化の種類も指定します。次のいずれかのオプションを選択します。 - **なし**。暗号化は使用しません。 - AES 128 **ビット**。128 ビットの暗号化キーを使用します。 - AES 192 **ビット**。192 ビットの暗号化キーを使用します。 - AES 256 **ビット**。256 暗号化キーを使用します。 デフォルトは**［なし］**です。
ペーシングサイズ	後続データ用に次の PWX CDC リーダー要求を待機する一時停止までに、ソースシステムが PowerExchange リスナに渡す行数またはキロバイト単位でのデータ量。この値を減らすと、セッションのパフォーマンスが向上します。パフォーマンスを最大にするには、0 を使用します。 デフォルトである最小値は 0 です。
ペーシング単位	**［ペーシングサイズ］**プロパティと一緒に使用する単位の種類。 **［行］**または**［キロバイト］**のいずれかを選択します。

プロパティ	説明
マップの場所	抽出マップがあるシステムのホスト名または IP アドレス。ポート番号も含めます。 この値は、PowerExchange リスナが、抽出マップからリモートにある PowerExchange ロッガー（Linux、UNIX、Windows 用）マシン上で実行されている場合に必要です。リスナは、変更データ抽出要求を処理するために、抽出マップへのアクセスを必要とします。 次の形式で値を入力します。*host_name* は、ホスト名または IP アドレスにできます。 *host_name*:*port_number* 以下に例を示します。 ADACDC01:25100 **注**: 接続をテストして抽出マップメタデータをインポートするための **[マップの場所]** の値は、**[リスナの場所]** の値よりも優先されます。
マップの場所のユーザー	**[マップの場所]** プロパティ内に指定された場所の PowerExchange リスナにアクセスできるユーザー名。
マップの場所のパスワード	**[マップの場所のユーザー]** プロパティで指定されるユーザー名と関連付けられたパスワード。
イベントテーブル	ユーザー定義イベントに基づく変更データ抽出を停止するためにイベントテーブルを作成した場合、イベントテーブルの PowerExchange 抽出マップの名前を入力します。イベントテーブルは、CDC ソースシステム上の Datacom テーブルである必要があります。
低値をスペースに置き換える	文字データ内の NULL をスペースに置き換えるかどうかを制御します。文字データ内の NULL を置き換えるには、このプロパティを選択します。デフォルトでは、このプロパティが選択されています。
カスタムプロパティ	PowerExchange のデフォルト設定よりも優先するために指定できるカスタムプロパティ。セミコロン（;）を区切り文字として使用することで、複数のプロパティを入力できます。通常は、Informatica グローバルカスタマサポートの指示の下でのみ、カスタムプロパティを設定します。 **注**: これらのプロパティは、PowerCenter の PowerExchange Client for PowerCenter（PWXPC）Datacom CDC 接続の **[PWX オーバーライド]** オプションと同じです。

Datacom 接続のプロパティ

Datacom 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。

以下の表に、Datacom 接続のプロパティを示します。

プロパティ	説明
接続名	Datacom 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	Datacom 接続の説明。最大長は 4000 文字です。
タイプ	接続タイプ。Datacom の場合、タイプは［Datacom］である必要があります。
ランタイム環境	マッピングタスクの実行に使用する Secure Agent が含まれるランタイム環境の名前。
リスナの場所	Datacom の要求を処理する PowerExchange リスナを実行するシステムのホスト名または IP アドレス。リスナのポート番号も含めます。次の形式で値を入力します。*host_name* は、ホスト名または IP アドレスにできます。 *host_name*: *port_number* 以下に例を示します。 LSNR1:1467?
ユーザー名	PowerExchange リスナセキュリティが有効化されているときに、PowerExchange リスナにアクセスするために使用できるユーザー名。詳細については、『PowerExchange リファレンスマニュアル』の「SECURITY 文」を参照してください。
パスワード	**［ユーザー名］**プロパティで指定されるユーザー名と関連付けられたパスワード。
スキーマ名	データマップのスキーマ名。
コードページ	ソースデータベースからデータを抽出するために、データ統合サービスの Secure Agent が使用するコードページ。
オフロード処理	オフロード処理を使用するかどうかを制御します。オフロード処理は、バルクデータ処理をソースシステムからターゲットシステムに転送します。次のオプションがあります。 - **自動**。オフロード処理を使用するかどうかが Cloud データ統合によって決定されます。 - **事後フィルタ**。データのフィルタリングなど、バルクデータ処理をターゲットにオフロードします。 - **事前フィルタ**。処理はターゲットにオフロードされますが、データは引き続きソースシステム上でフィルタリングされます。 - **いいえ**。オフロード処理を無効化します。 デフォルトは［いいえ］です。

プロパティ	説明
オフロードスレッド	Cloud データ統合がバルクデータを処理するために使用するスレッドの数。 最適なパフォーマンスを得るためには、統合サービスマシンにインストールされているプロセッサまたはこのマシンで使用可能なプロセッサの数を超えないようにこの値を設定します。 有効な値は 1〜64 です。 デフォルトは 0 です。マルチスレッド処理は無効になります。リーダーまたはライタパイプラインのパーティション化を使用する場合は、デフォルト値の 0 を受け入れる。複数のオフロードスレッドとパーティション化の両方を使用することはできません。 すべての接続タイプがオフロードスレッドをサポートしているわけではありません。これらのうち、いずれかの接続の**［オフロードスレッド］**接続属性がゼロ以外の値に設定されている場合は、スレッドなしで処理が続行されます。
配列サイズ	有効な値は 1〜5000 です。デフォルトは 25 です。
低値をスペースに置き換える	文字データ内の NULL をスペースに置き換えるかどうかを制御します。文字データ内の NULL を置き換えるには、このプロパティを選択します。デフォルトでは、このプロパティが選択されています。
接続リトライ期限	初期接続の試行の失敗後、PowerExchange Bulk Reader が PowerExchange リスナへの再接続を試行する秒数。接続が再試行時間中に確立できない場合、マッピングタスクに失敗します。デフォルト値は 0 であり、接続の再試行は無効になります。
カスタムプロパティ	PowerExchange のデフォルト設定よりも優先するために指定できるカスタムプロパティ。セミコロン（;）を区切り文字として使用することで、複数のプロパティを入力できます。通常は、Informatica グローバルカスタマサポートの指示の下でのみ、カスタムプロパティを設定します。 **注**: これらのプロパティは、PowerCenter の PowerExchange Client for PowerCenter（PWXPC）Datacom 接続の［PWX **オーバーライド**］オプションと同じです。
書き込みモード	書き込みモード。次のオプションがあります。 - **書き込み確認オン**。PowerExchange リスナにデータを送信し、成功/失敗の応答を待ってから、以降のデータを送信します。このモードではデータをバッファしないで、PowerExchange リスナにデータを同期的に送信します。 - **書き込み確認オフ**。データをバッファして PowerExchange リスナにデータを非同期的に送信します。このモードでは、成功または失敗応答を待機しません。

Db2 for i CDC 接続のプロパティ

Db2 for i CDC 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、Db2 for i CDC 接続のプロパティを示します。

プロパティ	説明
接続名	Db2 for i CDC 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	Db2 for i CDC 接続の説明。最大長は 4000 文字です。
タイプ	接続タイプ。Db2 for i CDC の場合、タイプは Db2 for i CDC である必要があります。
ランタイム環境	マッピングタスクの実行に使用する Secure Agent が含まれるランタイム環境の名前。
リスナの場所	Db2 変更データのための PWX CDC リーダー要求を処理する PowerExchange リスナがあり、PowerExchange ロッガー（Linux、UNIX、Windows 用）を実行するシステムのホスト名または IP アドレス。リスナのポート番号も含めます。次の形式で値を入力します。*host_name* は、ホスト名または IP アドレスにできます。 *host_name*:*port_number* 以下に例を示します。 `DB2CDC1A:1467`
ユーザー名	PowerExchange リスナセキュリティが有効化されているときに、PowerExchange リスナにアクセスするために使用できるユーザー名。詳細については、『PowerExchange リファレンスマニュアル』の「SECURITY 文」を参照してください。
パスワード	**［ユーザー名］**プロパティで指定されるユーザー名と関連付けられたパスワード。
コレクション名	Db2 ソーステーブルのキャプチャ登録が含まれる登録グループの**［インスタンス］**フィールド内に指定される Db2 for i インスタンス名。このインスタンス名は、DBMOVER メンバの AS4J CAPI_CONNECTION 文の INST パラメータでも指定されます。この値は、接続の使用時に、PWX CDC メタデータアダプタがインポートする抽出マップメタデータをフィルタするために使用されます。
CAPI 接続名	PowerExchange DBMOVER コンフィギュレーションファイル内に定義される CAPX CAPI_CONNECTION 文の名前。この文には、PWX CDC リーダーが PowerExchange ロッガー（Linux、UNIX、Windows 用）ログファイルからの変更データを抽出するために使用するパラメータが含まれます。PWX CDC リーダーにこのプロパティ値が必要であり、DBMOVER コンフィギュレーションファイル内に定義される任意のデフォルトの CAPI_CONNECTION 文を無視します。
接続リトライ期限	初期接続の試行の失敗後、PWX CDC リーダーが PowerExchange リスナへの再接続を試行する秒数。接続が再試行時間中に確立できない場合、マッピングタスクに失敗します。デフォルト値は 0 であり、接続の再試行は無効になります。
圧縮	変更データをネットワーク経由で PWX CDC リーダーに送信する前に、PowerExchange リスナがデータを圧縮するかどうかを制御します。データを圧縮するには、このプロパティを選択します。デフォルトでは、このプロパティは選択されていません。

プロパティ	説明
暗号化	変更データをネットワーク経由で PWX CDC リーダーに送信する前に、PowerExchange リスナがデータを暗号化するかどうかを制御します。また、使用する暗号化の種類も指定します。次のいずれかのオプションを選択します。 - **なし**。暗号化は使用しません。 - AES 128 **ビット**。128 ビットの暗号化キーを使用します。 - AES 192 **ビット**。192 ビットの暗号化キーを使用します。 - AES 256 **ビット**。256 暗号化キーを使用します。 デフォルトは **［なし］** です。
ペーシングサイズ	後続データ用に次の PWX CDC リーダー要求を待機する一時停止までに、ソースシステムが PowerExchange リスナに渡す行数またはキロバイト単位でのデータ量。この値を減らすと、セッションのパフォーマンスが向上します。パフォーマンスを最大にするには、0 を使用します。 デフォルトである最小値は 0 です。
ペーシング単位	**［ペーシングサイズ］** プロパティと一緒に使用する単位の種類。 **［行］** または **［キロバイト］** のいずれかを選択します。デフォルトは［行］です。
マップの場所	抽出マップがあるシステムのホスト名または IP アドレス。ポート番号も含めます。 この値は、PowerExchange リスナが、抽出マップからリモートにある PowerExchange ロッガー（Linux、UNIX、Windows 用）マシン上で実行されている場合に必要です。リスナは、変更データ抽出要求を処理するために、抽出マップへのアクセスを必要とします。 次の形式で値を入力します。*host_name* は、ホスト名または IP アドレスにできます。 *host_name*:*port_number* 以下に例を示します。 DB2CDC01:25100 **注**: 接続をテストして抽出マップメタデータをインポートするための **［マップの場所］** の値は、**［リスナの場所］** の値よりも優先されます。
マップの場所のユーザー	**［マップの場所］** プロパティ内に指定された場所の PowerExchange リスナにアクセスできるユーザー名。
マップの場所のパスワード	**［マップの場所のユーザー］** プロパティで指定されるユーザー名と関連付けられたパスワード。
イベントテーブル	ユーザー定義イベントに基づく変更データ抽出を停止するためにイベントテーブルを作成した場合、イベントテーブルの PowerExchange 抽出マップの名前を入力します。イベントテーブルは、CDC ソースシステム上の Db2 for i テーブルである必要があります。
低値をスペースに置き換える	文字データ内の NULL をスペースに置き換えるかどうかを制御します。文字データ内の NULL を置き換えるには、このプロパティを選択します。デフォルトでは、このプロパティが選択されています。
カスタムプロパティ	PowerExchange のデフォルト設定よりも優先するために指定できるカスタムプロパティ。セミコロン（;）を区切り文字として使用することで、複数のプロパティを入力できます。通常は、Informatica グローバルカスタマサポートの指示の下でのみ、カスタムプロパティを設定します。 **注**: これらのプロパティは、PowerCenter の PowerExchange Client for PowerCenter（PWXPC）Db2 CDC アプリケーション接続の **［PWX オーバーライド］** オプションと同じです。

Db2 for i 接続のプロパティ

Db2 for i 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、Db2 for i 接続のプロパティを示します。

プロパティ	説明
接続名	Db2 for i 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	Db2 for i 接続の説明。最大長は 4000 文字です。
タイプ	接続タイプ。Db2 for i の場合、タイプは Db2 for i である必要があります。
ランタイム環境	マッピングタスクの実行に使用する Secure Agent が含まれるランタイム環境の名前。
リスナの場所	Db2 for i の要求を処理する PowerExchange リスナを実行するシステムのホスト名または IP アドレス。リスナのポート番号も含めます。次の形式で値を入力します。*host_name* は、ホスト名または IP アドレスにできます。 *host_name*:*port_number* 以下に例を示します。 DB2ILSNR:14675
データベース名	Db2 for i サブシステムまたはデータベース名。
ユーザー名	PowerExchange リスナセキュリティが有効化されているときに、PowerExchange リスナにアクセスするために使用できるユーザー名。詳細については、『PowerExchange リファレンスマニュアル』の「SECURITY 文」を参照してください。
パスワード	**[ユーザー名]** プロパティで指定されるユーザー名と関連付けられたパスワード。
スキーマ名	Db2 for i のソースまたはターゲットのスキーマ名。
コードページ	ソースデータベースからデータを抽出するために、データ統合サービスの Secure Agent が使用するコードページ。
分離レベル	ソースデータベースに使用する Db2 for i 分離レベル。次のオプションがあります。 - ALL - CS - CHG - なし - RR デフォルトは CS です
データベースファイルのオーバーライド:	データベースファイルのデフォルトをオーバーライドする値。 この値は、PowerExchange DBMOVER 構成ファイルの DB_FILE 文の値をオーバーライドします。

プロパティ	説明
ライブラリリスト:	接続に使用する Db2 for i ライブラリリストの名前。
環境 SQL	データベース環境で実行する SQL コマンド。
配列サイズ	有効な値は 1〜5000 です。デフォルトは 25 です。
低値をスペースに置き換える	文字データ内の NULL をスペースに置き換えるかどうかを制御します。文字データ内の NULL を置き換えるには、このプロパティを選択します。デフォルトでは、このプロパティが選択されています。
接続リトライ期限	初期接続の試行の失敗後、PowerExchange Bulk Reader が PowerExchange リスナへの再接続を試行する秒数。接続が再試行時間中に確立できない場合、マッピングタスクに失敗します。デフォルト値は 0 であり、接続の再試行は無効になります。
カスタムプロパティ	PowerExchange のデフォルト設定よりも優先するために指定できるカスタムプロパティ。セミコロン（;）を区切り文字として使用することで、複数のプロパティを入力できます。通常は、Informatica グローバルカスタマサポートの指示の下でのみ、カスタムプロパティを設定します。 **注**: これらのプロパティは、PowerCenter の PowerExchange Client for PowerCenter（PWXPC）Db2 for i 接続の **［PWX オーバーライド］** オプションと同じです。
書き込みプロパティ	書き込みモード。次のオプションがあります。 - **書き込み確認オン**。PowerExchange リスナにデータを送信し、成功/失敗の応答を待ってから、以降のデータを送信します。このモードではデータをバッファしないで、PowerExchange リスナにデータを同期的に送信します。 - **書き込み確認オフ**。データをバッファして PowerExchange リスナにデータを非同期的に送信します。このモードでは、成功または失敗応答を待機しません。 - **フォールトトレランスを持つ非同期**。**［書き込み確認オフ］** の速度で **［書き込み確認オン］** のエラー検出を実行できます。このモードではデータをバッファして、PowerExchange リスナにデータを非同期に送信します。SQL エラーが発生すると、PowerExchange はターゲットマシン上に拒否ファイルを作成します。このファイルには、ライタがターゲットに書き込めなかったデータレコードが含まれます。テーブル全体をリロードせず、ファイルの内容を表示してエラーを識別して修正します。特定の SQL 戻りコードの処理方法を指定することもできます。 デフォルト値は **［書き込み確認オン］** です。
拒否ファイル	拒否ファイルに対して PWXR のデフォルトのプレフィックスをオーバーライドします。 書き込みモードが［フォールトトレランスを持つ非同期］の場合、PowerExchange はターゲットマシン上に拒否ファイルを作成します。 **注**: PWXDISABLE を入力すると、拒否ファイルの作成を防ぐことができます。

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。
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。
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 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。

Db2 for LUW CDC 接続のプロパティ

Db2 for LUW CDC 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、Db2 for LUW CDC 接続のプロパティを示します。

プロパティ	説明
接続名	Db2 for LUW CDC 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	Db2 for LUW CDC 接続の説明。最大長は 4000 文字です。
タイプ	接続タイプ。Db2 for LUW CDC の場合、タイプは Db2 for LUW CDC である必要があります。
ランタイム環境	マッピングタスクの実行に使用する Secure Agent が含まれるランタイム環境の名前。
リスナの場所	Db2 変更データのための PWX CDC リーダー要求を処理する PowerExchange リスナがあり、PowerExchange ロッガー（LUW 用）を実行するシステムのホスト名または IP アドレス。リスナのポート番号も含めます。次の形式で値を入力します。*host_name* は、ホスト名または IP アドレスにできます。 *host_name*:*port_number* 以下に例を示します。 DB2RHL1:1467
ユーザー名	PowerExchange リスナセキュリティが有効化されているときに、PowerExchange リスナにアクセスするために使用できるユーザー名。PowerExchange LDAP ユーザー認証を有効にした場合、ユーザー名はエンタープライズユーザー名です。詳細については、『PowerExchange リファレンスマニュアル』の「SECURITY 文」を参照してください。
パスワード	**[ユーザー名]** プロパティで指定されるユーザー名と関連付けられたパスワード。
コレクション名	Db2 ソーステーブルのキャプチャ登録が含まれる登録グループの **[データベース]** フィールド内に指定される Db2 インスタンス名。この値は、接続の使用時に、PWX CDC メタデータアダプタがインポートする抽出マップメタデータをフィルタするために使用されます。
CAPI 接続名	PowerExchange DBMOVER コンフィギュレーションファイル内に定義される CAPX CAPI_CONNECTION 文の名前。この文には、PWX CDC リーダーが PowerExchange ロッガー（Linux、UNIX、Windows 用）ログファイルからの変更データを抽出するために使用するパラメータが含まれます。PWX CDC リーダーにこのプロパティ値が必要であり、DBMOVER コンフィギュレーションファイル内に定義される任意のデフォルトの CAPI_CONNECTION 文を無視します。

プロパティ	説明
接続リトライ時間	初期接続の試行の失敗後、PWX CDC リーダーが PowerExchange リスナへの再接続を試行する秒数。接続が再試行時間中に確立できない場合、マッピングタスクに失敗します。デフォルト値は 0 であり、接続の再試行は無効になります。
圧縮	変更データをネットワーク経由で PWX CDC リーダーに送信する前に、PowerExchange リスナがデータを圧縮するかどうかを制御します。データを圧縮するには、このプロパティを選択します。デフォルトでは、このプロパティは選択されていません。
暗号化	変更データをネットワーク経由で PWX CDC リーダーに送信する前に、PowerExchange リスナがデータを暗号化するかどうかを制御します。また、使用する暗号化の種類も指定します。次のいずれかのオプションを選択します。 - **なし**。暗号化は使用しません。 - AES 128 **ビット**。128 ビットの暗号化キーを使用します。 - AES 192 **ビット**。192 ビットの暗号化キーを使用します。 - AES 256 **ビット**。256 暗号化キーを使用します。 デフォルトは **［なし］** です。
ペーシングサイズ	後続データ用に次の PWX CDC リーダー要求を待機する一時停止までに、ソースシステムが PowerExchange リスナに渡す行数またはキロバイト単位でのデータ量。この値を減らすと、セッションのパフォーマンスが向上します。パフォーマンスを最大にするには、0 を使用します。 デフォルトである最小値は 0 です。
ペーシング単位	**［ペーシングサイズ］** プロパティと一緒に使用する単位の種類。 **［行］** または **［キロバイト］** のいずれかを選択します。
マップの場所	抽出マップが含まれるシステムのホスト名または IP アドレスを入力します。ポート番号も含めます。 この値は、PowerExchange リスナが、抽出マップからリモートにある PowerExchange ロッガー（Linux、UNIX、Windows 用）マシン上で実行されている場合に必要です。リスナは、変更データ抽出要求を処理するために、抽出マップへのアクセスを必要とします。 次の形式で値を入力します。*host_name* は、ホスト名または IP アドレスにできます。 *host_name*:*port_number* 以下に例を示します。 DB2UNX2B:25100 接続をテストして抽出マップメタデータをインポートするための **［マップの場所］** の値は、**［リスナの場所］** の値よりも優先されます。
マップの場所のユーザー	**［マップの場所］** プロパティ内に指定された場所の PowerExchange リスナにアクセスできるユーザー名。
マップの場所のパスワード	**［マップの場所のユーザー］** プロパティで指定されるユーザー名と関連付けられたパスワード。
イベントテーブル	ユーザー定義イベントに基づく変更データ抽出を停止するためにイベントテーブルを作成した場合、イベントテーブルの PowerExchange 抽出マップの名前を入力します。イベントテーブルは、CDC ソースシステム上の Db2 テーブルである必要があります。

プロパティ	説明
低値をスペースに置き換える	文字データ内の NULL をスペースに置き換えるかどうかを制御します。文字データ内の NULL を置き換えるには、このプロパティを選択します。デフォルトでは、このプロパティが選択されています。
カスタムプロパティ	PowerExchange のデフォルト設定よりも優先するために指定できるカスタムプロパティ。セミコロン（;）を区切り文字として使用することで、複数のプロパティを入力できます。通常は、Informatica グローバルカスタマサポートの指示の下でのみ、カスタムプロパティを設定します。 **注**: これらのプロパティは、PowerCenter の PowerExchange Client for PowerCenter（PWXPC）Db2 CDC 接続の［PWX **オーバーライド**］オプションと同じです。

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。
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。

プロパティ	説明
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、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、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 z/OS CDC 接続のプロパティ

Db2 for z/OS CDC 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、Db2 for z/OS CDC 接続のプロパティを示します。

プロパティ	説明
接続名	Db2 for z/OS CDC 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	Db2 for z/OS CDC 接続の説明。最大長は 4000 文字です。
タイプ	接続タイプ。Db2 for z/OS CDC の場合、このタイプは Db2 for zOS CDC である必要があります。
ランタイム環境	マッピングタスクの実行に使用する Secure Agent が含まれるランタイム環境の名前。
リスナの場所	Db2 変更データのための PWX CDC リーダー要求を処理する PowerExchange リスナがあり、PowerExchange ロッガー（Linux、UNIX、Windows 用）を実行するシステムのホスト名または IP アドレス。リスナのポート番号も含めます。次の形式で値を入力します。*host_name* は、ホスト名または IP アドレスにできます。 *host_name*:*port_number* 以下に例を示します。 `DB2CDC1A:1467`
ユーザー名	PowerExchange リスナセキュリティが有効化されているときに、PowerExchange リスナにアクセスするために使用できるユーザー名。詳細については、『PowerExchange リファレンスマニュアル』の「SECURITY 文」を参照してください。
パスワード	**［ユーザー名］**プロパティで指定されるユーザー名と関連付けられたパスワード。

プロパティ	説明
コレクション名	Db2 ソーステーブルのキャプチャ登録が含まれる登録グループの **[データベースインスタンス名]** フィールド内に指定される Db2 for z/OS サブシステム ID またはデータ共有グループ名。この値は、接続の使用時に、PWX CDC メタデータアダプタがインポートする抽出マップメタデータをフィルタするために使用されます。
CAPI 接続名	PowerExchange DBMOVER コンフィギュレーションファイル内に定義される CAPX CAPI_CONNECTION 文の名前。この文には、PWX CDC リーダーが PowerExchange ロッガー（Linux、UNIX、Windows 用）ログファイルからの変更データを抽出するために使用するパラメータが含まれます。PWX CDC リーダーにこのプロパティ値が必要であり、DBMOVER コンフィギュレーションファイル内に定義される任意のデフォルトの CAPI_CONNECTION 文を無視します。
接続リトライ期限	初期接続の試行の失敗後、PWX CDC リーダーが PowerExchange リスナへの再接続を試行する秒数。接続が再試行時間中に確立できない場合、マッピングタスクに失敗します。デフォルト値は 0 であり、接続の再試行は無効になります。
圧縮	変更データをネットワーク経由で PWX CDC リーダーに送信する前に、PowerExchange リスナがデータを圧縮するかどうかを制御します。データを圧縮するには、このプロパティを選択します。デフォルトでは、このプロパティは選択されていません。
暗号化	変更データをネットワーク経由で PWX CDC リーダーに送信する前に、PowerExchange リスナがデータを暗号化するかどうかを制御します。また、使用する暗号化の種類も指定します。次のいずれかのオプションを選択します。 - **なし**。暗号化は使用しません。 - AES 128 **ビット**。128 ビットの暗号化キーを使用します。 - AES 192 **ビット**。192 ビットの暗号化キーを使用します。 - AES 256 **ビット**。256 暗号化キーを使用します。 デフォルトは **[なし]** です。
ペーシングサイズ	後続データ用に次の PWX CDC リーダー要求を待機する一時停止までに、ソースシステムが PowerExchange リスナに渡す行数またはキロバイト単位でのデータ量。この値を減らすと、セッションのパフォーマンスが向上します。パフォーマンスを最大にするには、0 を使用します。 デフォルトである最小値は 0 です。
ペーシング単位	**[ペーシングサイズ]** プロパティと一緒に使用する単位の種類。 **[行]** または **[キロバイト]** のいずれかを選択します。
マップの場所	抽出マップがあるシステムのホスト名または IP アドレス。ポート番号も含めます。 この値は、PowerExchange リスナが、抽出マップからリモートにある PowerExchange ロッガー（Linux、UNIX、Windows 用）マシン上で実行されている場合に必要です。リスナは、変更データ抽出要求を処理するために、抽出マップへのアクセスを必要とします。 次の形式で値を入力します。*host_name* は、ホスト名または IP アドレスにできます。 *host_name*:*port_number* 以下に例を示します。 DB2CDC01:25100 **注**: 接続をテストして抽出マップメタデータをインポートするための **[マップの場所]** の値は、**[リスナの場所]** の値よりも優先されます。
マップの場所のユーザー	**[マップの場所]** プロパティ内に指定された場所の PowerExchange リスナにアクセスできるユーザー名。

プロパティ	説明
マップの場所のパスワード	**[マップの場所のユーザー]** プロパティで指定されるユーザー名と関連付けられたパスワード。
イベントテーブル	ユーザー定義イベントに基づく変更データ抽出を停止するためにイベントテーブルを作成した場合、イベントテーブルの PowerExchange 抽出マップの名前を入力します。イベントテーブルは、CDC ソースシステム上の Db2 for z/OS テーブルである必要があります。
低値をスペースに置き換える	文字データ内の NULL をスペースに置き換えるかどうかを制御します。文字データ内の NULL を置き換えるには、このプロパティを選択します。デフォルトでは、このプロパティが選択されています。
カスタムプロパティ	PowerExchange のデフォルト設定よりも優先するために指定できるカスタムプロパティ。セミコロン（;）を区切り文字として使用することで、複数のプロパティを入力できます。通常は、Informatica グローバルカスタマサポートの指示の下でのみ、カスタムプロパティを設定します。 **注**: これらのプロパティは、PowerCenter の PowerExchange Client for PowerCenter（PWXPC）Db2 CDC 接続の **[PWX オーバーライド]** オプションと同じです。

Db2 for z/OS 接続のプロパティ

Db2 for z/OS 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、Db2 for z/OS 接続のプロパティを示します。

プロパティ	説明
接続名	Db2 for z/OS 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	Db2 for z/OS 接続の説明。最大長は 4000 文字です。
タイプ	接続タイプ。Db2 for z/OS の場合、このタイプは Db2 for z/OS である必要があります。
ランタイム環境	マッピングタスクの実行に使用する Secure Agent が含まれるランタイム環境の名前。
リスナの場所	Db2 for z/OS の要求を処理する PowerExchange リスナを実行するシステムのホスト名または IP アドレス。リスナのポート番号も含めます。次の形式で値を入力します。*host_name* は、ホスト名または IP アドレスにできます。 *host_name*:*port_number* 以下に例を示します。 LSNR1:1467?

プロパティ	説明
データベース名	Db2 サブシステムまたはデータベース名。
ユーザー名	PowerExchange リスナセキュリティが有効化されているときに、PowerExchange リスナにアクセスするために使用できるユーザー名。詳細については、『PowerExchange リファレンスマニュアル』の「SECURITY 文」を参照してください。
パスワード	**[ユーザー名]** プロパティで指定されるユーザー名と関連付けられたパスワード。
スキーマ名	ソースまたはターゲットに使用されるスキーマ。
コードページ	ソースデータベースからデータを抽出するために、データ統合サービスの Secure Agent が使用するコードページ。
環境 SQL	データベース環境で実行する SQL コマンド。
相関 ID	Db2 要求の Db2 相関 ID として使用される値。 この値は、PowerExchange DBMOVER 構成ファイルの SESSID 文の値をオーバーライドします。
オフロード処理	オフロード処理を使用するかどうかを制御します。オフロード処理は、バルクデータ処理をソースシステムからターゲットシステムに転送します。次のオプションがあります。 - **自動**。オフロード処理を使用するかどうかが Cloud データ統合によって決定されます。 - **事後フィルタ**。データのフィルタリングなど、バルクデータ処理をターゲットにオフロードします。 - **事前フィルタ**。処理はターゲットにオフロードされますが、データは引き続きソースシステム上でフィルタリングされます。 - **いいえ**。オフロード処理を無効化します。 デフォルトは［いいえ］です。
オフロードスレッド	Cloud データ統合がバルクデータを処理するために使用するスレッドの数。 最適なパフォーマンスを得るためには、統合サービスマシンにインストールされているプロセッサまたはこのマシンで使用可能なプロセッサの数を超えないようにこの値を設定します。 有効な値は 1〜64 です。 デフォルトは 0 です。マルチスレッド処理は無効になります。リーダーまたはライタパイプラインのパーティション化を使用する場合は、デフォルト値の 0 を受け入れる。複数のオフロードスレッドとパーティション化の両方を使用することはできません。 すべての接続タイプがオフロードスレッドをサポートしているわけではありません。これらのうち、いずれかの接続の **[オフロードスレッド]** 接続属性がゼロ以外の値に設定されている場合は、スレッドなしで処理が続行されます。
配列サイズ	有効な値は 1〜5000 です。デフォルトは 25 です。
低値をスペースに置き換える	文字データ内の NULL をスペースに置き換えるかどうかを制御します。文字データ内の NULL を置き換えるには、このプロパティを選択します。デフォルトでは、このプロパティが選択されています。
接続リトライ期限	初期接続の試行の失敗後、PowerExchange Bulk Reader が PowerExchange リスナへの再接続を試行する秒数。接続が再試行時間中に確立できない場合、マッピングタスクに失敗します。デフォルト値は 0 であり、接続の再試行は無効になります。

プロパティ	説明
カスタムプロパティ	PowerExchange のデフォルト設定よりも優先するために指定できるカスタムプロパティ。セミコロン（;）を区切り文字として使用することで、複数のプロパティを入力できます。通常は、Informatica グローバルカスタマサポートの指示の下でのみ、カスタムプロパティを設定します。 **注**: これらのプロパティは、PowerCenter の PowerExchange Client for PowerCenter（PWXPC）Db2 for z/OS 接続の **［PWX オーバーライド］** オプションと同じです。
フォールトトレランスと非同期	**［書き込み確認オフ］** の速度で **［書き込み確認オン］** のエラー検出を実行できます。このモードではデータをバッファして、PowerExchange リスナにデータを非同期に送信します。SQL エラーが発生すると、PowerExchange はターゲットマシン上に拒否ファイルを作成します。このファイルには、ライタがターゲットに書き込めなかった行が含まれます。テーブル全体をリロードせず、ファイルの内容を表示してエラーを識別して修正します。特定の SQL 戻りコードの処理方法を指定することもできます。セッションが致命的でないエラーを検出したときにセッションの実行を停止するには、［タスクの編集］ダイアログボックスの **［設定オブジェクト］** タブにある **［停止するエラー数］** セッション属性で 0 より大きい値を指定します。 デフォルト値は **［書き込み確認オン］** です。
書き込みプロパティ	書き込みモード。次のオプションがあります。 - **書き込み確認オン**。PowerExchange リスナにデータを送信し、成功/失敗の応答を待ってから、以降のデータを送信します。このモードではデータをバッファしないで、PowerExchange リスナにデータを同期的に送信します。 - **書き込み確認オフ**。データをバッファして PowerExchange リスナにデータを非同期的に送信します。このモードでは、成功または失敗応答を待機しません。
拒否ファイル	拒否ファイルに対して PWXR のデフォルトのプレフィックスをオーバーライドします。 書き込みモードが［フォールトトレランスを持つ非同期］の場合、PowerExchange はターゲットマシン上に拒否ファイルを作成します。 **注**: PWXDISABLE を入力すると、拒否ファイルの作成を防ぐことができます。

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。

プロパティ	説明
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。
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。

Db2 Warehouse on Cloud 接続のプロパティ

Db2 Warehouse on 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する必要があります。

次の表に、Db2 Warehouse on Cloud 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	Db2 Warehouse on Cloud 接続の説明。最大長は 255 文字です。
タイプ	接続タイプ。【Db2 Warehouse on Cloud】を選択します。

接続プロパティ	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。
ユーザー ID	IBM Db2 Warehouse on Cloud にログインするためのユーザー ID。
パスワード	IBM Db2 Warehouse on Cloud に接続するユーザー ID のパスワード。
ホスト名	IBM Db2 Warehouse on Cloud のホスト名。
ポート番号	IBM Db2 Warehouse サーバーへの接続に使用するネットワークポート番号。
データベース名	接続する IBM Db2 Warehouse のデータベース名。
SSL 接続	Secure Agent が IBM Db2 Warehouse とのセキュアな接続を確立するかどうかを決定します。 IBM Db2 Warehouse とのセキュアな接続を確立するには、SSL を選択します。 **注**: サーバーレスランタイム環境を使用する場合、SSL を使用して Db2 Warehouse データベースと安全に通信するように Db2 Warehouse 接続を設定することはできません。
高度な接続のプロパティ	オプション。使用する追加接続パラメータ。 接続パラメータをキーと値のペアとして次の形式で指定し、キーと値の各ペアをセミコロンで区切ります。`<param1>=<value>&<param2>=<value>&<param3>=<value>....`
スキーマ	メタデータをフェッチする IBM Db2 Warehouse on Cloud のスキーマ名。 **注**: スキーマ名を指定しないと、Secure Agent は IBM Db2 Warehouse on Cloud 内のすべてのスキーマを参照します。

Domo 接続のプロパティ

Domo 接続を設定するときは、接続プロパティを設定する必要があります。

次の表に、Domo 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	Domo 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。
タイプ	接続タイプ。Domo 接続を選択します。
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。
Customer	Domo アカウントに接続するユーザー名。
開発トークン	Domo アカウントに接続するアクセストークン。

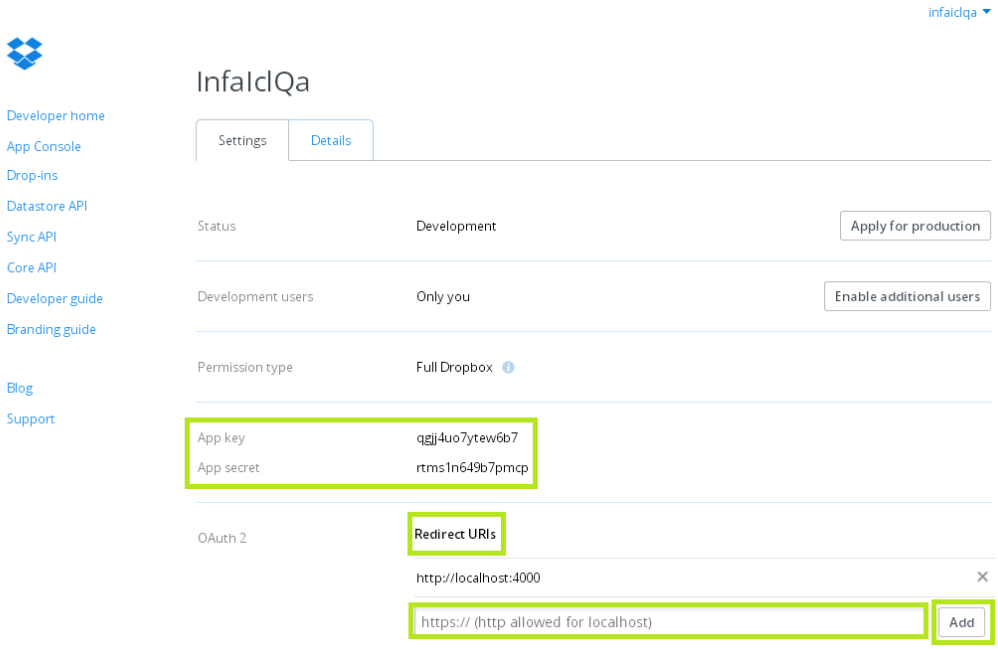
接続プロパティ	説明
UpdateMode	データを更新するための次のいずれかのオプションを選択できます。 - APPEND - REPLACE - UPSERT
キーの更新/挿入	UPSERT モードに適用されます。一意の値を入力し、各値をカンマで区切ります。

Dropbox 接続のプロパティ

次の表に、Dropbox 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。
説明	接続の説明。
タイプ	接続タイプ。一覧から Dropbox を選択します。
Secure Agent	すべての Secure Agent が一覧表示されます。一覧から該当する Secure Agent を選択します。
App キー	Dropbox アカウント名。Dropbox App **コンソール**から取得した App キーを入力します。
App シークレット	Dropbox アカウントのパスワード。Dropbox App **コンソール**から取得した App シークレットを入力します。
このシステム上でホストされるエージェント	システムが Secure Agent をホストするかどうかを指定します。
承認コード	- システムが Secure Agent をホストする場合は該当しません。 - システムが Secure Agent をホストしない場合、アクセストークンを取得するために承認コードを入力する必要があります。ターゲットフォルダを接続パラメータで指定後、接続をテストします。接続のテスト時に、承認コードを指定する接続ページに URL リンクが表示されます。
アクセストークン	接続のテスト後に取得されるアクセストークン。
ターゲットフォルダ	Dropbox がダウンロードするファイルを保存するためのターゲットディレクトリの場所。例; \..\..\Dropbox\Target\
ロギングの有効化	接続を作成するユーザーをログに記録します。ロギングを有効化するチェックボックスを選択します。

注: 接続の作成中、Dropbox App 設定ページ内にリダイレクト URI http://localhost:4000 を指定します。



Elasticsearch 接続のプロパティ

Elasticsearch 接続を作成する際には、接続プロパティを設定する必要があります。

次の表に、Elasticsearch 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	Elasticsearch 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 またはサーバーレスランタイム環境を指定できます。
ホスト	Elasticsearch サーバーのホスト名または IP アドレスです。
ポート	Elasticsearch サーバーのポート番号。デフォルトは 9243 です。

プロパティ	説明
SSL トラストストアファイルパス	SSL サーバーの証明書を含む SSL トラストストアファイルの絶対パス。
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。
認証	Elasticsearch リソースにアクセスするための認証方法です。 次のいずれかの認証方法を選択します。 - 基本。ユーザー名とパスワードの資格情報を使用して、Elasticsearch サーバーに接続します。 - 証明書ベース。証明書を使用して Elasticsearch サーバーに接続します。
ユーザー名	基本認証タイプに適用されます。 Elasticsearch サーバーにアクセスするためのユーザー名です。
パスワード	基本認証タイプに適用されます。 Elasticsearch サーバーにアクセスするためのユーザー名に対応するパスワード。
SSL KeyStore ファイルパス	証明書ベース認証タイプに適用されます。 安全な通信を確立するために必要なキーと証明書を格納する、Secure Agent マシンにあるキーストアファイルの絶対パス。 このパラメータを指定する前に、証明書をダウンロードして Secure Agent マシンに配置してください。
SSL KeyStore パスワード	証明書ベース認証タイプに適用されます。 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。

Eloqua Bulk API 接続のプロパティ

Eloqua Bulk API 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、Eloqua Bulk API 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	Eloqua-Bulk API 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。
ベース URL	Eloqua アプリケーションに接続するためのベース URL。 次のいずれかの形式を使用して、ベース URL を指定します。 - https://secure.eloqua.com - https://<host>.eloqua.com/api/bulk/<version number> ホストには、Eloqua インスタンスをホストするポッドに基づいて、secure、www02.secure、または secure.p03 を入力できます。 https://<host>.eloqua.com/api/bulk/2.0 の URL では、2.0 はバージョン番号を表します。ベース URL にバージョン番号を指定しない場合、Secure Agent では、デフォルトバージョンを使用すると見なされます。 Eloqua アプリケーションに接続するためのベース URL を決定するには、Determining Base URL を参照してください。
認証タイプ	Eloqua アプリケーションへの接続に必要なユーザー認証のタイプです。
ドメイン名	Eloqua アプリケーションの会社名。
ユーザー名	Eloqua アカウントのユーザー名。
パスワード	Eloqua アカウントのパスワード。
クライアント ID	Eloqua への接続の OAuth 2.0 認証を完了するためのクライアント ID。OAuth 2.0 認証タイプを選択した場合に適用されます。
クライアントシークレット	Eloqua への接続の OAuth 2.0 認証を完了するためのクライアント秘密鍵。OAuth 2.0 認証タイプを選択した場合に適用されます。
タイムゾーンオフセット	Eloqua アプリケーション内での GMT との相対タイムゾーン。
デバッグロガーを有効にする	デバッグロガーによる、セッションログへの SOAP 要求と応答の登録を有効にします。
プレビュー用のデータの取得	Eloqua Bulk API オブジェクトにある、最初の 5 カラムの最初の 10 行をプレビュー用に取得します。 デフォルトではオンに設定されています。
アクティビティまたはカスタムフィールド設定	ソースとターゲットにある、アクティビティオブジェクトと、コンタクトオブジェクトとアカウントオブジェクトのカスタムフィールド。 アクティビティオブジェクトとカスタムフィールドを JSON 形式で入力します。

Eloqua REST 接続のプロパティ

Eloqua REST 接続を作成する際には、接続プロパティを設定する必要があります。

次の表に、Eloqua REST 接続のプロパティを示します。

プロパティ	説明
ランタイム環境	Eloqua にアクセスする際に使用される Secure Agent が稼働しているランタイム環境。
ベース URL	Eloqua アプリケーションサーバーのエンドポイント URL。ベース URL と一緒にクエリパラメータを指定しないでください。 例: `https://rest.apisandbox.eloqua.com`
ユーザー名	Eloqua アプリケーションのユーザー名。
ドメイン	Eloqua アプリケーションのドメイン。
パスワード	Eloqua アプリケーションのパスワード。
クライアント ID	Eloqua アプリケーションで作成されるクライアント ID。 **[認証タイプ]** として [OAuth 2.0] を選択した場合、クライアント ID を入力する必要があります。
クライアントシークレット	Eloqua アプリケーションで作成されるクライアント秘密鍵。 **[認証タイプ]** として [OAuth 2.0] を選択した場合、クライアント秘密鍵を入力する必要があります。
認証タイプ	Eloqua アプリケーションへの接続に必要なユーザー認証のタイプです。Eloqua REST コネクタが Eloqua アプリケーションにログインにするために使用する必要がある認証タイプを選択します。 次の認証タイプを選択できます。 - 基本認証 - OAuth 2.0 デフォルトは OAuth 2.0 です。
デバッグロガーを有効にする	マッピングをデバッグするためのセッションログ内のメッセージを表示します。 デフォルトは false です。
Eloqua Swagger	Eloqua REST 接続に使用する Swagger ファイル。[Eloqua Swagger API V1_2017_09_06] を選択します。

FileIO 接続のプロパティ

FileIO 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。

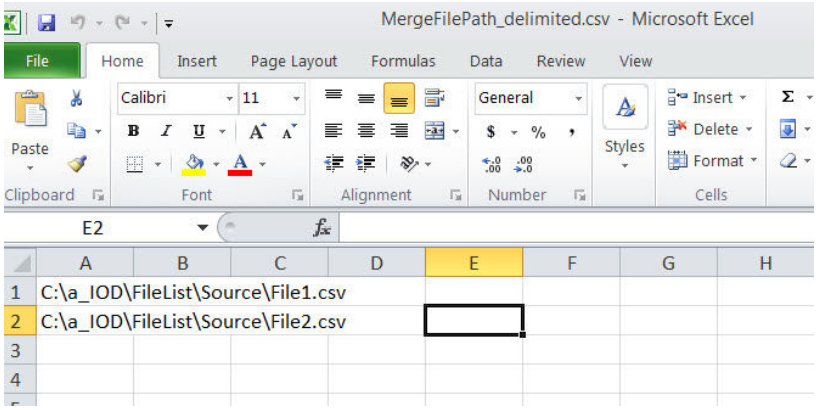
次の表に、FileIO 接続のプロパティを示します。

接続プロパティ	説明
接続名	接続に固有の名前を入力します。
説明	接続に関連する説明を入力します。
タイプ	一覧から［FileIo］を選択します。
Secure Agent	一覧から該当する Secure Agent を選択します。
親ディレクトリ	親ディレクトリパスを入力します。親ディレクトリは、読み取り操作および書き込み操作を実行するためのファイルが格納されたフォルダです。親ディレクトリには、空の.infaccess ファイルが格納される必要があります。 親ディレクトリ内に、inprocess、success、error 以外の任意の名前でフォルダを作成します。例えば、read、write、test などのフォルダを作成できます。空のファイルは、タスク内でこの接続をソースまたはターゲットとして選択するときに、オブジェクトとして表示されます。
ファイルコンテンツを次の形式で処理	ファイルコンテンツを処理するための選択可能なオプションの一覧から、必要なオプションを選択します。次のファイル処理オプションを使用できます。 - バイナリ: バイナリを選択した場合、同期タスクの**［フィールドマッピング］**タブ内で FileContentAsBinary をマップする必要があります。 - base 64 のエンコードされた文字列: デフォルトでは、このオプションが選択されています。このオプションを選択した場合、同期タスクの**［フィールドマッピング］**タブ内で FileContentAsBase64String をマップする必要があります。
ターゲットファイルの上書き	ターゲットファイルの上書きを有効にするには、このボックスを選択します。そうしないと、カウンタを使用した増分の命名順で、同じ名前を持つファイルが作成されます。例えば、ターゲットファイルの上書きオプションを有効にしないと、既存のファイル ABCD は上書きされません。代わりに、新しい ABCD(1)ファイルが作成されます。
ソースファイルの自動アーカイブ	ソースファイルの自動アーカイブを有効にするには、このボックスを選択します。このオプションによって、ファイルの処理後、ソースディレクトリからファイルを移動できます。
処理中のディレクトリ	ファイルの処理に使用されるディレクトリパスを指定します。デフォルトでは、親ディレクトリと見なされます。
成功ディレクトリ	処理後にファイルが移動されるディレクトリパスを指定します。デフォルトでは、親ディレクトリと見なされます。成功ディレクトリパスは、**［ソースファイルの自動アーカイブ］**オプションが有効な場合にのみ指定します。
エラーディレクトリ	エラーディレクトリパスを指定します。ファイルの処理中に問題やエラーが発生する場合があります。このようなファイルは、エラーディレクトリに移動されます。

File List 接続のプロパティ

File List 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、File List 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	接続に固有の名前を入力します。
説明	接続の説明を入力します。
タイプ	一覧から［File List］を選択します。
Secure Agent	一覧から Secure Agent を選択します。
ファイルタイプ	一覧からファイル形式を選択します。接続では、固定長形式と区切り文字ファイル形式がサポートされます。
区切り文字	区切り文字を選択します。デフォルトの区切り文字はカンマです。
スキーマファイルのパス	スキーマファイルパスを指定します。Informatica Secure Agent フォルダ内に、スキーマファイルのサンプルがあります。パスは<Secure Agent のインストールディレクトリ>\apps\Data_Integration_Server\ext\deploy_to_main\tomcat\plugins\<プラグイン ID>です。
カスタムヘッダーファイルパス	ヘッダーファイルパスを指定します。header.hdr ファイルは Informatica Secure Agent フォルダ内にあります。パスは<Secure Agent のインストールディレクトリ>\apps\Data_Integration_Server\ext\deploy_to_main\tomcat\plugins\<プラグイン ID>です。
ファイルの先頭の N 行をスキップ	ファイルのマージ中にスキップする行数を指定します。この設定によって、ファイルの先頭から行をスキップできます。
ファイルの末尾の N 行をスキップ	ファイルのマージ中にスキップする行数を指定します。この設定によって、ファイルの末尾から行をスキップできます。
ファイルパスのマージ	これは、File List コネクタを使用してマージする必要がある複数のすべてのファイルの詳細が格納されたファイルです。 このファイルの場所のパスを指定します。次の図に、File1 と File2 がマージ対象の 2 つのファイルであるマージファイルのパスを示します。 

接続プロパティ	説明
バッチごとの行数	パフォーマンスを最適化するために必要なバッチサイズを指定します。デフォルト値は 100 です。
日付形式	日付形式を指定します。デフォルトの日付形式は dd-MM-yyyy HH:mm:ss です。

File Processor 接続のプロパティ

File Processor 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、File Processor 接続のプロパティを示します。

接続プロパティ	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。
ソースファイルディレクトリ	転送するファイルが含まれる場所。
ターゲットファイルディレクトリ	転送されたファイルを配置する場所。
ファイルの選択	転送するファイル。フィールドに基づいてファイルを選択することができます。
ファイルパターン	転送するファイルのパターン。例えば、日付パターンに基づいてファイルを選択する場合は、［ファイルパターン］フィールドに日付形式を DD/MM/YYYY として指定できます。 注: **［ファイルの選択］**接続プロパティから **［すべて］**を選択した場合は、［ファイルパターン］フィールドは適用できません。
日数計算	日数計算を使用して、指定された日付より前または指定された日付の後に作成または変更されたファイルを選択します。［日付パターンを含む］に基づいてファイルを選択し、指定された日付の前後に変更されたファイルを選択できるように**日数計算**の値を指定します。値を日数で指定します。月と年で値を指定することはできません。 例えば、［日付パターンを含む］に基づいてファイルを選択した場合は、データフィルタを使用して、LastModDate を DD/MM/YYYY 形式で 02/02/2016 と指定し、日数計算を-1 と指定します。01/02/2016 までに変更されたファイルが選択されます。
PassKey	FTP サーバーまたは SFTP サーバーに接続するための資格情報。例えば、FTP サーバーまたは SFTP サーバーのパスワードおよびパスフレーズを値 passkey1 および passkey2 として指定できます。

フラットファイル接続

フラットファイル接続を使用すると、フラットファイルの作成、アクセス、保存を実行できます。フラットファイル接続は、マッピングおよびマッピングタスク、PowerCenter タスク、レプリケーションタスク、同期タスクなどのタスクで使用できます。

フラットファイル接続を設定するときは、接続で使用するランタイム環境を選択する必要があります。Linux 上で動作する Secure Agent を使用したランタイム環境を選択した場合は、フラットファイルターゲットに Windows ディレクトリを指定することはできません。

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。したがって、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。

マッピングまたはタスクでフラットファイル接続を選択する際には、フラットファイルの書式設定オプションを選択します。ソース、ルックアップ、またはターゲットの各トランスフォーメーションの書式設定オプションを選択する際には、フラットファイルが区切り形式なのか固定長なのかを指定します。フラットファイルが固定長の場合は、設定した固定長形式のリストからいずれかの固定長形式を選択します。固定長フラットファイルを使用する予定の場合は、Mapping Designer で固定長フラットファイルを選択する前に少なくとも 1 つの固定長形式を作成しておく必要があります。

フラットファイル接続のプロパティ

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
ランタイム環境	フラットファイルにアクセスする際に使用する Secure Agent が稼働しているランタイム環境。 **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。
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。[マイネットワークプレイス] を参照して目的のディレクトリを特定するか、次の形式でディレクトリ名を入力します: \\<サーバー名>\<ディレクトリパス>。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。 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。

接続プロパティ	説明
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
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-16 エンコード（ビッグエンディアン）。 - Unicode の UTF-16 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 エラスティックマッピングでは、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。

Linux でのフラットファイル接続のロケールの設定

Linux 上で、フラットファイル接続を使用する同期タスクまたはレプリケーションタスクでマルチバイトデータをサポートするには、デフォルトのロケールを UTF-8 に設定する必要があります。

1. 現在のロケールを表示するには、シェルコマンドラインに、「locale」と入力します。
2. デフォルトのロケールを UTF-8 に設定する場合は、次の例を参照してください。
   - bash 系 UNIX シェルの場合:

     ```
     export LC_ALL=en_US.UTF-8
     ```
   - csh 系 UNIX シェルの場合:

     ```
     setenv LC_ALL en_US.UTF-8
     ```
3. Secure Agent を再起動します。

FTP/SFTP 接続

File Transfer Protocol（FTP）接続を使用すると、FTP を使用してソースファイルおよびターゲットファイルにアクセスできます。Secure File Transfer Protocol（SFTP）接続を使用すると、SSH などの安全なプロトコルを使用して、ソースファイルとターゲットファイルにアクセスできます。

FTP/SFTP 接続を設定する際には、次のディレクトリを指定します。

ローカルディレクトリ

ソースファイルまたはターゲットファイルのコピーを保存する Secure Agent のローカルディレクトリ。

リモートディレクトリ

ソースまたはターゲットとして使用するファイルの場所。

Informatica Intelligent Cloud Services は、リモートディレクトリではなく、ローカルディレクトリにあるファイルを検証します。FTP/SFTP 接続を設定する際には、ローカルディレクトリに、すべてのソースファイルおよびターゲットファイルの有効なコピーが保存されていることを確認してください。ユーザーが FTP/SFTP 接続を使用するタスクを設定する場合、Informatica Intelligent Cloud Services は、ローカルファイルのファイル構造を使用して、タスクのソースまたはターゲットを定義します。ローカルファイルのファイル構造は、リモートディレクトリにあるソースファイルまたはターゲットファイルと一致していなければなりません。また、Informatica Intelligent Cloud Services はローカルファイルを使用してデータプレビューも生成します。ローカルファイルのデータがリモートディレクトリにあるソースファイルまたはターゲットファイルと一致しない場合は、データプレビューによって間違った結果が表示される可能性があります。

Informatica Intelligent Cloud Services は、FTP/SFTP ターゲット接続を使用したデータ統合タスクを実行する際に、そのタスクに定義されているターゲットに基づいてターゲットファイルを作成します。Informatica Intelligent Cloud Services は、タスクが完了すると、ターゲットファイルをリモートディレクトリに書き込んで、既存のファイルを上書きします。

FTP/SFTP 接続のプロパティ

次の表に、FTP/SFTP 接続のプロパティを示します。

接続プロパティ	説明
ランタイム環境	ファイルにアクセスする際に使用する Secure Agent が稼働しているランタイム環境。
ユーザー名	FTP サーバーにログインするために使用するユーザー名。
パスワード	FTP サーバーにログインするために使用するユーザー名に対するパスワードです。
ホスト	FTP/SFTP ホストのホスト名または IP アドレス。
ポート	FTP/SFTP 接続に接続するときに使用するネットワークポート番号。デフォルトポートは、FTP の場合は 21、SFTP の場合は 22 です。
ローカルディレクトリ	ローカルファイルを保存するローカルマシン上のディレクトリ。ローカルマシンでは、対応するタスクを実行するために使用する Secure Agent も稼働している必要があります。ローカルディレクトリを入力するか、［参照］ボタンを使用してローカルディレクトリを選択します。

接続プロパティ	説明
リモートディレクトリ	リモートフラットファイルが保存されている FTP/SFTP ホスト上のディレクトリ。FTP/SFTP サーバーによっては、ディレクトリを入力するためのオプションが限定されている場合があります。詳細については、FTP/SFTP サーバーのドキュメントを参照してください。
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、MM/dd/yyyy HH:mm:ss です。
コードページ	ソースまたはターゲットのフラットファイルが存在するシステムと互換性のあるコードページ。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 データの場合に選択します。 - 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)
これはセキュアな FTP 接続です	接続がセキュアかどうかを示します。SFTP 接続を作成する場合に選択します。

キー交換アルゴリズムと暗号

SFTP 接続には、次のキー交換アルゴリズムと暗号を使用できます。

キー交換アルゴリズム

- diffie-hellman-group14-sha1
- diffie-hellman-group-exchange-sha1
- diffie-hellman-group1-sha1

暗号

- aes256-ctr
- aes192-ctr
- aes128-ctr
- aes256-cbc (rijndael-cbc@lysator.liu.se)

- aes192-cbc
- aes128-cbc
- 3des-cbc
- blowfish-cbc
- cast128-cbc
- arcfour
- arcfour128
- なし

FTP/SFTP 接続のルールとガイドライン

FTP/SFTP 接続に関するルールおよびガイドラインは、次のとおりです。

- Informatica Intelligent Cloud Services はファイルへの書き込み中にターゲットファイルをロックしません。ファイルの破損を防ぐため、いかなるときでも複数のタスクが同時に 1 つのターゲットファイルに書き込むことがないことを確認してください。
- ローカルターゲットファイルとリモートターゲットファイルのメタデータが異なっている場合、Informatica Intelligent Cloud Services は、実行時に、リモートターゲットファイルのメタデータをローカルターゲットファイルで上書きします。Informatica Intelligent Cloud Services
- ローカルターゲットファイルにロードされた行の行数を確認するには、**［すべてのジョブ］**ページまたは**［自分のジョブ］**からジョブの詳細を開きます。
- Windows では、**［ディレクトリの参照］**ダイアログボックスを使用してマッピング済みドライブ上の FTP/SFTP ディレクトリを選択することはできません。ネットワークディレクトリにアクセスするには、［マイネットワーク］を探します。次の形式でディレクトリを入力することもできます。

  `\\<server_name>\<directory_path>`

  ［ディレクトリの参照］ダイアログボックスに［マイネットワーク］が表示されない場合は、Secure Agent サービスのネットワークログインを設定する必要があります。
- FTP/SFTP 接続のエラーメッセージは、FTP または SFTP のみを参照していることがあります。FTP または SFTP を参照しているエラーメッセージは FTP/SFTP 接続のエラーメッセージと理解してください。

Google Ads 接続のプロパティ

Google Ads 接続を作成する際には、接続プロパティを設定する必要があります。

次の表に、Google Ads 接続のプロパティを示します。

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。
クライアント ID	必須。Google 開発者コンソールからの OAuth 2.0 クライアント ID。
クライアントシークレット	必須。Google 開発者コンソールからの OAuth 2.0 クライアントシークレット。

プロパティ	説明
リフレッシュトークン	必須。Google Ads の認証コードを交換した後に受信する OAuth 2.0 リフレッシュトークン。
開発者トークン	必須。Google Ads マネージャアカウントからの開発者トークン。
アカウントカスタマ ID	必須。マネージャアカウントを介して Google Ads アカウントにアクセスするための一意のログインカスタマ ID。

Google Analytics 接続のプロパティ

Google Analytics 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 Analytics 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 Analytics 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。
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。
APIVersion	Google Analytics レポートからの読み取りに使用される API。 次の値から選択できます。 - Core Reporting API v3 - Analytics Reporting API v4
AccountId	Google Analytics プロジェクトに関連付けられた Google Analytics アカウント ID。 次のレポートからデータを読み取る場合にのみ適用されます。 - Content Grouping - Ecommerce - Goal Conversions その他のレポートからデータを読み取る場合は、このプロパティを空白のままにしてください。

プロパティ	説明
PropertyId	Google Analytics プロジェクトに関連付けられた Google Analytics プロパティ ID。 次のレポートからデータを読み取る場合にのみ適用されます。 - Content Grouping - Ecommerce - Goal Conversions その他のレポートからデータを読み取る場合は、このプロパティを空白のままにしてください。
ViewId	Google Analytics プロジェクトに関連付けられた Google Analytics ビュー ID。 **注:** Goal Conversions レポートからデータを読み取る場合のみ適用されます。その他のレポートからデータを読み取る場合は、このプロパティを空白のままにしてください。

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
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 値を指定します。
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 値を指定します。

Google BigQuery 接続のプロパティ

Google BigQuery 接続を作成する際には、接続プロパティを設定する必要があります。

次の表に、Google BigQuery 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	Google BigQuery の接続タイプ。
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。
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 値を指定します。
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 値を指定します。
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 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必要がある場所の Secure Agent マシン上のディレクトリを指定します。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。
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 値を指定します。 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。

プロパティ	説明
データセット ID	接続先のソーステーブルとターゲットテーブルが含まれるデータセットの名前。
ストレージパス	このプロパティは、大量のデータを読み書きするときに適用されます。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必要です。 データを一時的に格納するために、Secure Agent がローカルステージファイルを作成する場所の Google Cloud Storage 内のパス。 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。 例えば、gs://<bucket_name>または gs://<bucket_name>/<folder_name>を入力します。

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。

接続モード

Google BigQuery 接続は、次のいずれかの接続モードを使用するように設定できます。

簡易モード

簡易モードを使用する場合、Google BigQuery コネクタは、レコードデータ型フィールド内の各フィールドを、フィールド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。

混合モード

混合モードを使用する場合、Google BigQuery コネクタは、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 コネクタは、最上位のレコードデータ型のフィールドを、フィールド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。

複合モード

複合モードを使用する場合、Google BigQuery は、Google BigQuery テーブル内のすべての列を、フィールド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。

接続モードの例

Google BigQuery コネクタは、Google BigQuery 接続に対して設定する接続モードに基づいて、Google BigQuery データを読み書きします。

プリミティブフィールドとレコードデータ型の **Address** フィールドを持つ Google BigQuery 内に、Customers テーブルがあります。この Address フィールドには、2 つのプリミティブサブフィールドである、文字列データ型の **City** と **State** が含まれます。

次の図に、Google BigQuery 内の Customers テーブルのスキーマを示します。

ID	INTEGER	NULLABLE
Name	STRING	NULLABLE
Address	RECORD	NULLABLE
Address.City	STRING	NULLABLE
Address.State	STRING	NULLABLE
Mobile	STRING	REPEATED
Totalpayments	FLOAT	NULLABLE
age	INTEGER	REPEATED

次の表に、Google BigQuery 内の Customers テーブルのデータを示します。

ID	**名前**	Address.City	Address.State	Mobile	Totalpayments
14	John	LOS ANGELES	CALIFORNIA	+1-9744884744	18433.90
				+1-8267389993	
29	Jane	BOSTON	MANHATTAN	+1-8789390309	28397.33
				+1-9876553784	
				+1-8456437848	

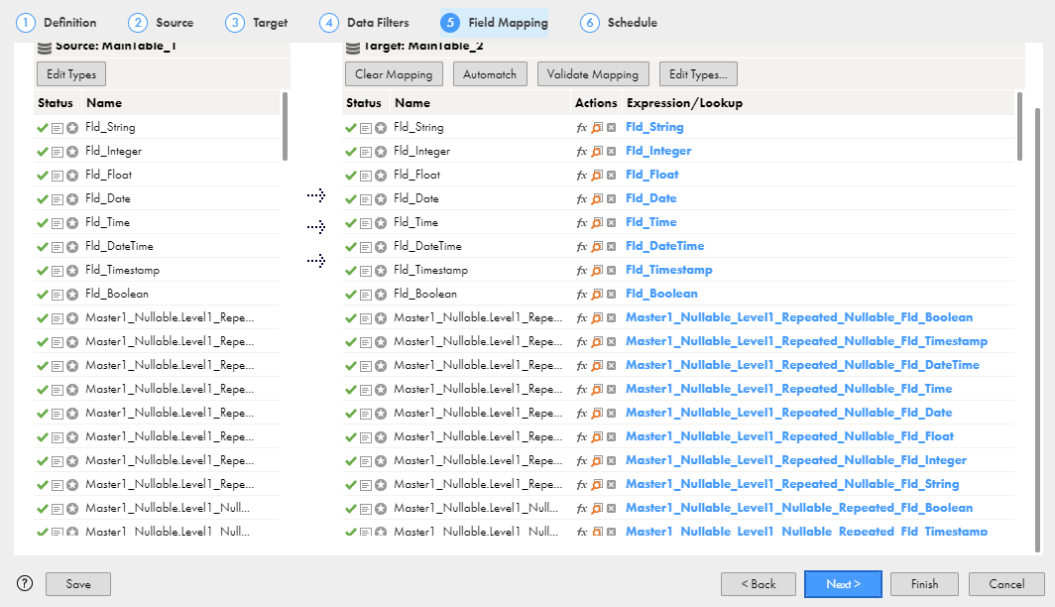
簡易モード

簡易モード接続を使用する場合、Google BigQuery コネクタは、レコードデータ型フィールド内の各フィールドを、**[フィールドマッピング]** タブ内の個別のフィールドとしてフラット化します。

次の表に、Customers テーブル内の Address Record フィールドの各サブフィールドに対応する Address_City と Address_State の 2 つの個別のフィールドを示します。

ID	**名前**	Address_City	Address_State	Mobile	Totalpayments
14	John	LOS ANGELES	CALIFORNIA	+1-9744884744	18433.90
14	John	LOS ANGELES	CALIFORNIA	+1-8267389993	18433.90
29	Jane	BOSTON	MANHATTAN	+1-8789390309	28397.33
29	Jane	BOSTON	MANHATTAN	+1-9876553784	28397.33
29	Jane	BOSTON	MANHATTAN	+1-8456437848	28397.33

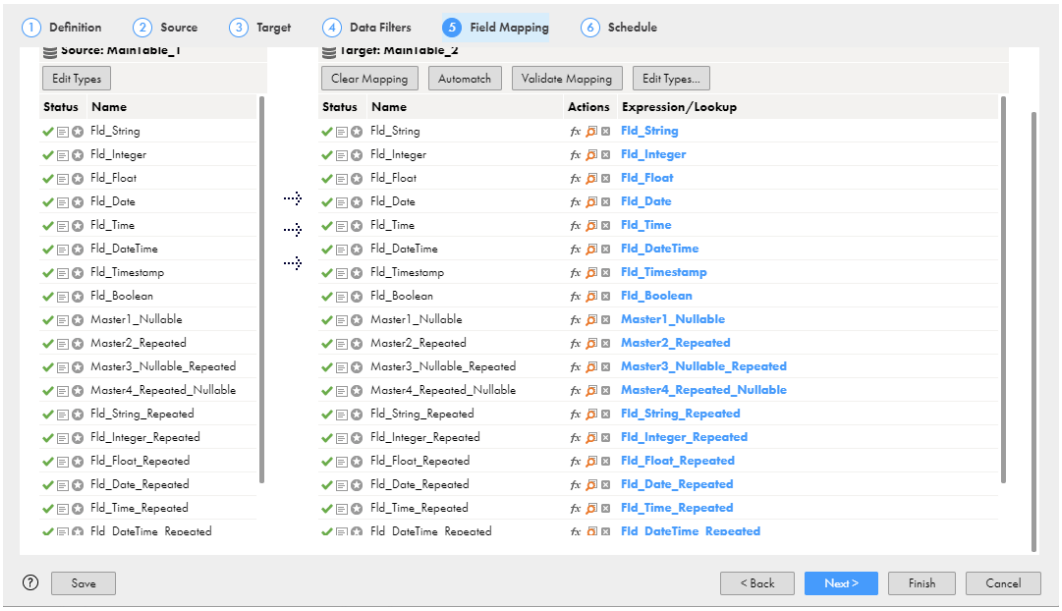
次の図に、同期タスクの［**フィールドマッピング**］タブ内のフィールドを示します。



混合モード

混合モード接続を使用する場合、Google BigQuery コネクタは、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 コネクタは、最上位のレコードデータ型のフィールドを、［**フィールドマッピング**］タブ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。

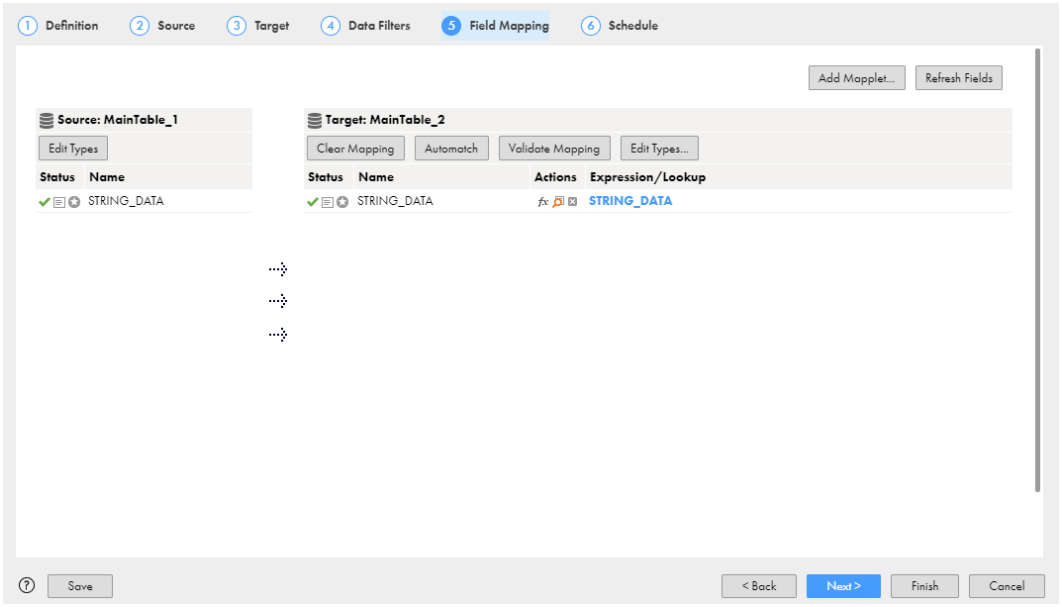
次の図に、同期タスクの［**フィールドマッピング**］タブを示します。



複合モード

複合モード接続を使用する場合、Google BigQuery コネクタは、Google BigQuery テーブル内のすべての列を、**［フィールドマッピング］**タブ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。

次の図に、同期タスクの**［フィールドマッピング］**タブ内の［STRING_DATA］フィールドを示します。



Google BigQuery 接続モードのルールとガイドライン

簡易モード

Google BigQuery 接続を設定して簡易接続モードを使用する場合は、次のルールとガイドラインを考慮します。

- 繰り返しカラムが含まれる Google BigQuery ターゲットテーブルは、**［ターゲットの作成］**オプションを使用して作成できません。
- Google BigQuery ソーステーブルに繰り返しカラムが含まれる場合は、これらのカラムに対してデータフィルタを設定できません。
- Google BigQuery テーブルに複数の繰り返しカラムが含まれる場合は、データをプレビューできません。
- Google BigQuery ターゲットテーブルに繰り返しカラムが含まれる場合は、これらのカラムに対して更新操作や削除操作を設定できません。
- Record データ型のカラムや繰り返しカラムに更新/挿入操作を設定できません。
- Google BigQuery ソースからデータを読み取るときは、1 つのマッピングに複数の繰り返しカラムをマッピングすることはできません。繰り返しカラムごとに、複数のマッピングを作成する必要があります。

混合モード

Google BigQuery 接続を設定して混合接続モードを使用する場合は、次のルールとガイドラインを考慮します。

- データはプレビューできません。
- Google BigQuery ターゲットテーブルは、**［ターゲットの作成］**オプションを使用して作成できません。
- Google BigQuery ソーステーブルに、Record データ型のカラムと繰り返しカラムが含まれる場合は、これらのカラムに対してデータフィルタを設定できません。
- Record データ型のカラムや繰り返しカラムに、更新、更新/挿入、および削除の操作を設定できません。
- 詳細ターゲットプロパティのステージングファイルのデータ形式として、JSON（改行区切り）形式を選択する必要があります。Google BigQuery テーブルに Record データ型のカラムまたは繰り返しカラムが含まれていない限り、ステージングファイルのデータ形式として CSV 形式を使用できます。
- 詳細ターゲットプロパティの次の CSV 形式オプションは、適用されません。
  - 引用符付きの改行の許可
  - フィールド区切り文字
  - ジャグ行の許可

複合モード

Google BigQuery 接続を設定して複合接続モードを使用する場合は、次のルールとガイドラインを考慮します。

- データはプレビューできません。
- Google BigQuery ターゲットテーブルは、**［ターゲットの作成］**オプションを使用して作成できません。
- Google BigQuery ソース接続を設定して複合接続モードを使用する場合は、ソースにデータフィルタを設定できません。
- 更新、更新/挿入、および削除の操作は設定できません。
- 詳細ターゲットプロパティのステージングファイルのデータ形式として、JSON（改行区切り）形式を選択する必要があります。

- ステージングファイルのデータ形式として CSV 形式を使用できません。詳細ターゲットプロパティの次の CSV 形式オプションは、適用されません。
  - 引用符付きの改行の許可
  - フィールド区切り文字
  - ジャグ行の許可
- Google BigQuery ソースには、キー範囲パーティションを使用できません。

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 Big Query 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。
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>

プロパティ	説明
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[1]。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[1]。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[1]	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。 **注**: サーバーレスランタイム環境を使用する場合は、Google Cloud Storage でストレージパスを指定する必要があります。
従来の SQL をカスタムクエリに使用[1]	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。
カスタムクエリのデータセット名[1]	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。
地域 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[1]	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。

プロパティ	説明
オプションのプロパティ[1]	カスタムプロパティを介してソースおよびターゲットの機能を設定できるかどうかを指定します。 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。 - なし。カスタムプロパティを設定しない場合は、［なし］を選択します。 - 必須。カスタムプロパティを指定して、ソースおよびターゲットの機能を設定する場合。 デフォルトは［なし］です。
オプションのプロパティの指定[1]	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。 オプションのプロパティで **［必須］** を選択した場合に表示されます。 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
[1] 詳細モードのマッピングには適用されません。	

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。

再試行ストラテジ

ステージングモードで Google BigQuery からデータを読み取る際は、Google BigQuery V2 接続が Google BigQuery ソースへの接続に失敗した場合の再試行ストラテジを設定できます。

次の表に、Google BigQuery V2 接続の再試行プロパティを示します。

プロパティ	説明
再試行の有効化[1]	障害が発生した場合に、Secure Agent が接続の再試行を試みることを示します。 接続の再試行を有効にするには、このオプションを選択します。 デフォルトでは選択されていません。
最大再試行回数[1]	Secure Agent が Google BigQuery エンドポイントからの応答を受信するために実行する再試行の最大回数。 Secure Agent が最大再試行回数内に Google BigQuery に接続できない場合、接続は失敗します。 デフォルト値は 6 です。 **［再試行の有効化］** プロパティを選択すると表示されます。
初期再試行遅延[1]	Secure Agent が接続の再試行を行うまでの初期待機時間（秒単位）。 デフォルトは 1 です。 **［再試行の有効化］** プロパティを選択すると表示されます。
再試行遅延乗数[1]	Secure Agent が、連続する再試行間の待機時間を最大再試行遅延時間まで指数関数的に増加させるために使用する乗数。 デフォルトは 2.0 です。 **［再試行の有効化］** プロパティを選択すると表示されます。
最大再試行遅延[1]	連続する再試行の間に Secure Agent が待機する最大待機時間（秒単位）。 デフォルトは 32 です。 **［再試行の有効化］** プロパティを選択すると表示されます。

プロパティ	説明
合計タイムアウト[1]	Secure Agent が接続を再試行してから接続が失敗するまでの合計時間（秒単位）。 デフォルトは 50 です。 **［再試行の有効化］**プロパティを選択すると表示されます。
[1] マッピングにのみ適用されます。	

接続モード

Google BigQuery V2 接続は、次のいずれかの接続モードを使用するように設定できます。

簡易モード

簡易モードを使用する場合、Google BigQuery V2 コネクタは、レコードデータ型フィールド内の各フィールドを、フィールド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。

混合モード

混合モードを使用する場合、Google BigQuery V2 コネクタは、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、フィールド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。

複合モード

複合モードを使用する場合、Google BigQuery は、Google BigQuery テーブル内のすべての列を、フィールド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。

接続モードの例

Google BigQuery V2 コネクタは、Google BigQuery V2 接続に対して設定する接続モードに基づいて、Google BigQuery データを読み書きします。

プリミティブフィールドとレコードデータ型の **Address** フィールドを持つ Google BigQuery 内に、Customers テーブルがあります。この Address フィールドには、2 つのプリミティブサブフィールドである、文字列データ型の **City** と **State** が含まれます。

次の図に、Google BigQuery 内の Customers テーブルのスキーマを示します。

ID	INTEGER	NULLABLE
Name	STRING	NULLABLE
Address	RECORD	NULLABLE
Address.City	STRING	NULLABLE
Address.State	STRING	NULLABLE
Mobile	STRING	REPEATED
Totalpayments	FLOAT	NULLABLE
age	INTEGER	REPEATED

次の表に、Google BigQuery 内の Customers テーブルのデータを示します。

ID	**名前**	Address.City	Address.State	Mobile	Totalpayments
14	John	LOS ANGELES	CALIFORNIA	+1-9744884744	18433.90
				+1-8267389993	
29	Jane	BOSTON	MANHATTAN	+1-8789390309	28397.33
				+1-9876553784	
				+1-8456437848	

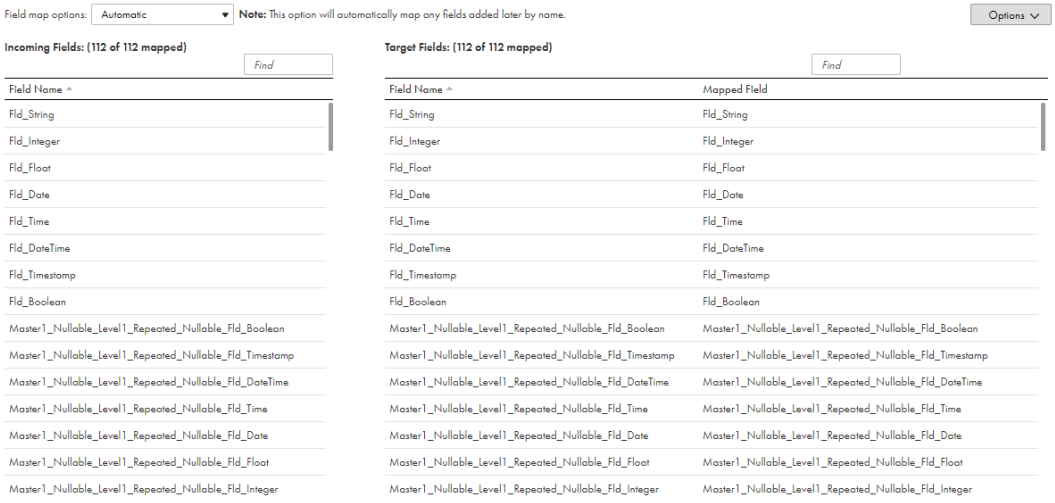
簡易モード

簡易モード接続を使用する場合、Google BigQuery V2 コネクタは、レコードデータ型フィールド内の各フィールドを、**［フィールドマッピング］**タブ内の個別のフィールドとしてフラット化します。

次の表に、Customers テーブル内の Address Record フィールドの各サブフィールドに対応する Address_City と Address_State の 2 つの個別のフィールドを示します。

ID	**名前**	Address_City	Address_State	Mobile	Totalpayments
14	John	LOS ANGELES	CALIFORNIA	+1-9744884744	18433.90
14	John	LOS ANGELES	CALIFORNIA	+1-8267389993	18433.90
29	Jane	BOSTON	MANHATTAN	+1-8789390309	28397.33
29	Jane	BOSTON	MANHATTAN	+1-9876553784	28397.33
29	Jane	BOSTON	MANHATTAN	+1-8456437848	28397.33

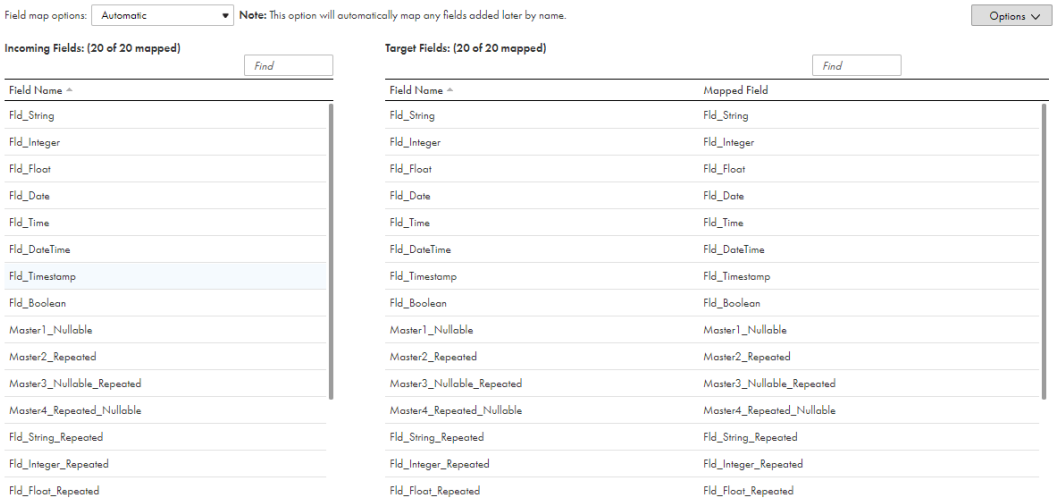
次の図に、ターゲットトランスフォーメーションの［**フィールドマッピング**］タブ内のフィールドを示します。



混合モード

混合モード接続を使用する場合、Google BigQuery V2 コネクタは、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、［**フィールドマッピング**］タブ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。

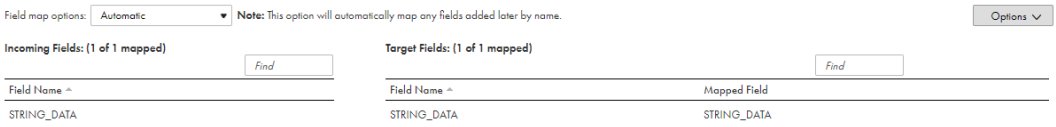
次の図に、ターゲットトランスフォーメーションの［**フィールドマッピング**］タブを示します。



複合モード

複合モード接続を使用する場合、Google BigQuery V2 コネクタは、Google BigQuery テーブル内のすべての列を、**［フィールドマッピング］**タブ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。

次の図に、ターゲットトランスフォーメーションの**［フィールドマッピング］**タブ内の［STRING_DATA］フィールドを示します。



Google BigQuery V2 接続モードのルールとガイドライン

簡易モード

Google BigQuery V2 接続を設定して簡易接続モードを使用する場合は、次のルールとガイドラインを考慮します。

- 詳細モードのマッピングは設定できません。
- **［読み取りモード］**に**［直接］**を選択した場合にのみ、Google BigQuery ソーステーブルの繰り返しカラムからデータを読み取ることができます。
- **［ターゲットの作成］**オプションを使用して、繰り返しカラムが含まれる Google BigQuery ターゲットテーブルを作成することはできません。
- Google BigQuery ソーステーブルに繰り返しカラムが含まれる場合は、これらのカラムに対してデータフィルタを設定できません。
- Google BigQuery テーブルに複数の繰り返しカラムが含まれる場合は、データをプレビューできません。
- Google BigQuery ターゲットテーブルにレコードデータ型の繰り返しカラムが含まれている場合、これらのカラムに更新操作、更新/挿入操作、および削除操作を設定することはできません。
- Google BigQuery テーブルに Record データ型のカラムまたは繰り返しカラムが含まれていない場合のみ、ステージングファイルのデータ形式として CSV 形式を使用できます。

- Google BigQuery ターゲットテーブルに、Record データ型のカラムと繰り返しカラムが含まれる場合は、更新を設定できません。マージクエリを使用しない場合は、これらのカラムの操作を更新/挿入および削除します。
- Google BigQuery ソースからデータを読み取るときは、1 つのマッピングに複数の繰り返しカラムをマッピングすることはできません。繰り返しカラムごとに、複数のマッピングを作成する必要があります。
- ソーストランスフォーメーションで複数のソーステーブルをインポートすることはできません。

混合モード

Google BigQuery V2 接続を設定して混合接続モードを使用する場合は、次のルールとガイドラインを考慮します。

- データはプレビューできません。
- 従来の SQL ステートメントを使用してカスタムクエリを定義することはできません。カスタムクエリを定義するには、標準 SQL を使用する必要があります
- Google BigQuery ソーステーブルに、Record データ型のカラムと繰り返しカラムが含まれる場合は、これらのカラムに対してデータフィルタを設定できません。
- マージクエリを使用せず、キーフィールドが Record データ型のカラムまたは繰り返しカラムである場合、更新、更新/挿入、および削除操作を設定することはできません。
- 詳細ターゲットプロパティのステージングファイルのデータ形式として、JSON（改行区切り）形式を選択する必要があります。Google BigQuery テーブルに Record データ型のカラムまたは繰り返しカラムが含まれていない場合のみ、ステージングファイルのデータ形式として CSV 形式を使用できます。
- 詳細ターゲットプロパティの次の CSV 形式オプションは、適用されません。

  - 引用符付きの改行の許可

  - フィールド区切り文字

  - ジャグ行の許可

複合モード

Google BigQuery V2 接続を設定して複合接続モードを使用する場合は、次のルールとガイドラインを考慮します。

- 詳細モードのマッピングは設定できません。
- ソーストランスフォーメーションで複数のソーステーブルをインポートすることはできません。
- データはプレビューできません。
- 従来の SQL ステートメントを使用してカスタムクエリを定義することはできません。カスタムクエリを定義するには、標準 SQL を使用する必要があります
- Google BigQuery ターゲットテーブルは、**［ターゲットの作成］**オプションを使用して作成できません。
- **［ターゲットテーブルの切り詰め］**オプションを使用してデータをターゲットにロードする前に、Google BigQuery ターゲットテーブルを切り詰めることはできません。
- Google BigQuery ソース接続を設定して複合接続モードを使用する場合は、ソースにデータフィルタを設定できません。
- 更新、更新/挿入、および削除の操作は設定できません。
- 詳細ターゲットプロパティのステージングファイルのデータ形式として、JSON（改行区切り）形式を選択する必要があります。
- ステージングファイルのデータ形式として CSV 形式を使用できません。詳細ターゲットプロパティの次の CSV 形式オプションは、適用されません。

  - 引用符付きの改行の許可

- フィールド区切り文字
- ジャグ行の許可

- Google BigQuery ソースには、キー範囲パーティションを使用できません。

Google Bigtable 接続のプロパティ

Google Bigtable 接続を作成する際には、接続プロパティを設定する必要があります。

次の表に、Google Cloud Bigtable 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	googleBigTable 接続タイプ。
ランタイム環境	Google Cloud Bigtable にアクセスする際に使用される Secure Agent が稼働しているランタイム環境。
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 値を指定します。
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 値を指定します。
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 値を指定します。

Google Cloud Spanner 接続のプロパティ

Google Cloud Spanner 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 Spanner 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	Google Cloud Spanner の接続タイプ。
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。
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 Cloud Spanner インスタンスが含まれるプロジェクトの ID を入力します。
インスタンス ID	Google Cloud Spanner 内で作成したインスタンスの名前。
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 Cloud Storage 接続のプロパティ

Google Cloud Storage 接続を作成する際には、接続プロパティを設定する必要があります。

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

プロパティ	説明
ランタイム環境	Google Cloud Storage にアクセスする際に使用される Secure Agent が稼働しているランタイム環境。
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 値を指定します。 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。
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 値を指定します。
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 値を指定します。
ファイルパス	データを読み書きする場所の Google Cloud Storage 内のパス。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。 例えば、<bucket name>または<bucket name>/<folder name>と入力します。

Google Cloud Storage V2 接続のプロパティ

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 の接続タイプ。
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 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。
暗号化済みファイルである[1]	ファイルを暗号化するかどうかを指定します。 Google Cloud Storage から暗号化されたファイルをインポートする場合は、このオプションを選択します。 デフォルトでは選択されていません。
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またはマッピングでターゲット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、ソースまたはターゲットオブジェクトを選択できます。

プロパティ	説明
オブジェクトメタデータのインポートの最適化[1]	バケットで使用可能な他のオブジェクト、フォルダ、またはサブフォルダを解析せずに、選択したオブジェクトのメタデータのインポートを最適化します。 選択したオブジェクトのメタデータを直接インポートすると、バケットで使用可能な各オブジェクトの解析にかかるオーバーヘッドと時間が削減されるため、パフォーマンスが向上します。 デフォルトでは選択されていません。
[1] 詳細モードのマッピングにのみ適用されます。	

Google Drive 接続のプロパティ

Google Drive 接続を作成する際には、接続プロパティを設定する必要があります。

次の表に、Google Drive 接続のプロパティを示します。

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。
クライアント ID	Google 開発者コンソールからのクライアント ID。
クライアントシークレット	Google 開発者コンソールからのクライアントシークレット。
リフレッシュトークン	承認コードの交換後に受け取るリフレッシュトークン。
ファイルのダウンロードパス	ファイルをダウンロードする必要がある場所のディレクトリ。
ファイルのアップロードパス	ファイルを格納し、アップロードする必要がある場所のディレクトリ。
PageSize	読み取り操作のページサイズ。デフォルト値は 10 です。

Google PubSub 接続のプロパティ

Google PubSub 接続を作成する際には、接続プロパティを設定する必要があります。

次の表に、Google 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。接続の説明。説明は 4000 文字以下にする必要があります。

プロパティ	説明
タイプ	GooglePubSub 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。
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 値を指定します。
サービスアカウントキー	安全な方法でサービスアカウントを作成後にダウンロードする JSON ファイル内にある private_key 値を指定します。
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 値を指定します。
maxMessageForBatch	Secure Agent がバッチでパブリッシュできるメッセージの数を指定します。デフォルトは 100 です。最大値は 1000 です。

Google PubSub V2 接続のプロパティ

Google PubSub V2 接続を作成する際には、接続プロパティを設定する必要があります。

次の表に、Google PubSub 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。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 4000 文字以下にする必要があります。
タイプ	GooglePubSubV2 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。
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 値を指定します。
サービスアカウントキー	安全な方法でサービスアカウントを作成後にダウンロードする JSON ファイル内にある private_key 値を指定します。
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 値を指定します。

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。

Google Sheets 接続のプロパティ

Google Sheets 接続を作成する際には、接続プロパティを設定する必要があります。

次の表に、Google Sheets 接続のプロパティを示します。

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。
ClientId	必須。Google 開発者コンソールからのクライアント ID。

プロパティ	説明
ClientSecret	必須。Google 開発者コンソールからのクライアントシークレット。
RefreshTokenForSheet	必須。Google Sheets のための承認コードの交換後に受け取るリフレッシュトークン。
RefreshTokenForDrive	オプション。Google Drive のための承認コードの交換後に受け取るリフレッシュトークン。このオプションは、[SpreadSheetName] フィールド内にスプレッドシート名を入力した場合に必要です。
SpreadSheetName	Google Sheets 内のスプレッドシート名。
SpreadSheetId	Google Sheets 内のスプレッドシート ID。
InitialColumnRange	データの読み取りを開始する Google スプレッドシートのデータ範囲の最初のカラム名を指定します。 例えば、InitialColumnRange 値を Sheet1!C5 と指定します。
FinalColumnRange	データの読み取りを停止する Google スプレッドシートのデータ範囲の最後のカラム名を指定します。 例えば、FinalColumnRange 値を Sheet1!G20 と指定します。
HeaderPresent	このオプションは、シートにヘッダーが含まれることを指定する場合に選択します。このオプションを選択し、シートにヘッダーが含まれていない場合、最初の行はヘッダーとして扱われます。
CreateNewSpreadsheet	このオプションは、Google Sheets 内に新しいスプレッドシートを作成する場合に選択します。 Google Sheets コネクタは、[SpreadSheetName] フィールドで指定する名前を使用して、空のスプレッドシートを作成します。 接続のテスト後は、このオプションを無効にします。そうしないと、Google Sheets コネクタは、毎回同じ名前の新しいスプレッドシートを作成します。

Google Sheets V2 接続のプロパティ

Google Sheets V2 接続を作成する際には、接続プロパティを設定する必要があります。

次の表に、Google Sheets V2 接続のプロパティを示します。

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。
クライアント ID	必須。Google 開発者コンソールからのクライアント ID。
クライアントシークレット	必須。Google 開発者コンソールからのクライアントシークレット。
リフレッシュトークン	必須。Google Sheets の認証コードを交換した後に受け取るリフレッシュトークン。

プロパティ	説明
スプレッドシート ID	Google Sheets 内のスプレッドシート ID。
ヘッダーあり	シートにヘッダーが含まれていることを示します。このオプションを選択し、シートにヘッダーが含まれていない場合、最初の行はヘッダーとして扱われます。

Greenplum 接続のプロパティ

Greenplum 接続を設定するときは、接続プロパティを設定する必要があります。

次の表に、Greenplum 接続のプロパティを示します。

接続プロパティ	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。
ホスト名	Greenplum サーバーのホスト名または IP アドレス。
ポート	Greenplum サーバーのポート番号。0 を入力すると、gpload ユーティリティは環境変数 $PGPORT から読み取ります。デフォルトは 5432 です。
データベース	データベースの名前。
スキーマ	Greenplum ソースまたはターゲットのメタデータを含むスキーマの名前。 デフォルトは public です。
証明書パス	Greenplum サーバーの SSL 証明書が保存されている場所へのパス。gpload ユーティリティと Greenplum サーバーの間に SSL 経由のセキュアな接続を確立する場合は、パスを指定します。 証明書パスで使用可能にする必要があるファイルの詳細については、gpload のマニュアルを参照してください。 **注**: SSL 設定は、Greenplum ライタにのみ適用されます。
メタデータ追加接続設定	使用する追加のメタデータ接続プロパティ。 次の形式を使用します。 `<parameter name1>=<value1>, <parameter name2>=<value2>`
ドライバ名	ドライバ名。DataDirect 7.1 Greenplum Wire プロトコルを指定します。
ユーザー名	Greenplum データベースにアクセスする権限を持つユーザー名。
パスワード	Greenplum データベースに接続するためのパスワード。

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。
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。

接続プロパティ	説明
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。
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: リモートファイルの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。ローカルファイルの読み取りまたは書き込みを行う場合、**［ローカルパス］**フィールドのみが必要です。

Hive 接続のプロパティ

Hive コネクタをマッピングタスクで使用するには、データ統合で接続を作成する必要があります。

Hive 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、Hive 接続のプロパティを示します。

接続プロパティ	説明
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。 - Kerberos。Kerberos クラスタに対して［Kerberos］を選択します。 - LDAP。LDAP 対応クラスタに対して［LDAP］を選択します。 **注**: LDAP は、詳細モードのマッピングには適用されません。 - なし。保護されていない、または LDAP 対応でない Hadoop クラスタの場合は**［なし］**を選択します。
JDBC URL *	Hive に接続するための JDBC URL。 要件に基づいて、次の形式を指定します。 - 単一のデータベースからテーブルを表示およびインポートするには、次の形式を使用します: `jdbc:hive2://<host>:<port>/<database name>` - 複数のデータベースからテーブルを表示およびインポートする場合は、データベース名を入力しないでください。次の JDBC URL 形式を使用します: `jdbc:hive2://<host>:<port>/` **注**: ポート番号の後にスラッシュを入力します。 - TLS が有効な Hadoop クラスタの Hive にアクセスするには、次の形式で JDBC URL に詳細を指定します: `jdbc:hive2://<host>:<port>/<database name>;ssl=true;sslTrustStore=<TrustStore_path>;trustStorePassword=<TrustStore_password>` ここで、トラストストアパスは、エージェントマシン上の TLS 証明書を含むトラストストアファイルのディレクトリパスです。
JDBC ドライバ*	Hive に接続するための JDBC ドライバクラス。
ユーザー名	LDAP モードまたはなしモードで Hive に接続するためのユーザー名。
パスワード	LDAP モードまたはなしモードで Hive に接続するためのパスワード。
プリンシパル名	Kerberos 認証を介して Hive に接続するためのプリンシパル名。
偽装ユーザー名	Hadoop クラスタでマッピングを実行するために Secure Agent が偽装するユーザーのユーザー名。マッピングの実行または Hive への接続に別のユーザーを有効にするために、ユーザーの偽装を設定できます。Hadoop クラスタが Kerberos 認証を使用する場合、Hadoop 接続に偽装名が必要です。
キータブの場所	Kerberos ログインのためのキータブファイルへのパスとファイル名。
構成ファイルパス*	クライアントのための Hadoop 設定ファイルが格納されているディレクトリ。 Hadoop クラスタから site.xml ファイルをコピーし、Linux ボックスのフォルダに追加します。マッピングで接続を使用して Hadoop クラスタ上の Hive にアクセスする前に、このフィールドにパスを指定します。 - マッピングには、core-site.xml、hdfs-site.xml、および hive-site.xml ファイルが必要です。 - 詳細モードのマッピングには、core-site.xml、hdfs-site.xml、hive-site.xml、mapred-site.xml、および yarn-site.xml ファイルが必要です。

接続プロパティ	説明
DFS URI *	Amazon S3、Microsoft Azure Data Lake Storage、HDFS などの分散ファイルシステム（DFS）にアクセスするための URI。 **注:** 詳細クラスタで実行される詳細モードのマッピングの場合、Azure Data Lake Storage Gen2 は Azure HDinsight クラスタでサポートされます。 アクセスする DFS に基づいて、必要なストレージとバケット名を指定します。 例えば、HDFS の場合は、Hadoop クラスタの core-site.xml ファイル内にある fs.defaultFS プロパティの値を参照し、同じ値を【DFS URI】フィールドに入力します。
DFS ステージングディレクトリ	Secure Agent がデータをステージングする Hadoop クラスタのステージングディレクトリ。DFS ステージングディレクトリに対する完全な権限が必要です。 ステージングディレクトリとして、透過的な暗号化フォルダを指定します。
Hive ステージングデータベース	外部テーブルまたは一時テーブルが作成される Hive データベース。Hive ステージングデータベースに対する完全な権限が必要です。

追加プロパティ	詳細モードのマッピングに適用されます。
	DFS にアクセスするために必要な追加のプロパティ。
	プロパティを次のように設定します。
	<DFS property name>=<value>;<DFS property name>=<value>
	以下に例を示します。
	Amazon S3 ファイルシステムにアクセスするには、アクセスキー、秘密鍵、および Amazon S3 プロパティ名をそれぞれセミコロンで区切って指定します。
	`fs.s3a.<bucket_name>.access.key=<access key value>;`
	`fs.s3a.<bucket_name>.secret.key=<secret key value>;`
	`fs.s3a.impl=org.apache.hadoop.fs.s3a.S3AFileSystem;`
	Azure Data Lake Storage Gen2 ファイルシステムにアクセスするには、認証タイプ、認証プロバイダ、クライアント ID、クライアントシークレット、およびクライアントエンドポイントをそれぞれセミコロンで区切って指定します。
	`fs.azure.account.auth.type=<Authentication type>;`
	`fs.azure.account.oauth.provider.type=<Authentication_provider>;`
	`fs.azure.account.oauth2.client.id=<Client_ID>;`
	`fs.azure.account.oauth2.client.secret=<Client-secret>;`
	`fs.azure.account.oauth2.client.endpoint=<ADLS Gen2 endpoint>`

* これらのフィールドは必須パラメータです。	

HubSpot 接続のプロパティ

HubSpot 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、HubSpot 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	HubSpot 接続の名前。
説明	接続の説明。
タイプ	接続のタイプ。HubSpot 接続を選択します。
クライアント ID	HubSpot へのアクセスを認証するためのアプリケーションの ID。クライアント ID 値は、HubSpot アプリケーションから取得できます。
クライアントシークレット	HubSpot へのアクセスを認証するためのクライアント秘密鍵。クライアントシークレット値は、HubSpot アプリケーションから取得できます。
RefreshToken	HubSpot へのアクセスを認証するために必要な更新トークン。

IDMS CDC 接続のプロパティ

IDMS CDC 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、IDMS CDC 接続のプロパティを示します。

プロパティ	説明
接続名	IDMS CDC 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	IDMS CDC 接続の説明。最大長は 4000 文字です。
タイプ	接続タイプ。IDMS CDC の場合、タイプは【IDMS CDC】である必要があります。
ランタイム環境	マッピングタスクの実行に使用する Secure Agent が含まれるランタイム環境の名前。
リスナの場所	IDMS の要求を処理する PowerExchange リスナを実行するシステムのホスト名または IP アドレス。リスナのポート番号も含めます。次の形式で値を入力します。*host_name* は、ホスト名または IP アドレスにできます。 *host_name*:*port_number* 以下に例を示します。 LSNR1:1467

プロパティ	説明
ユーザー名	PowerExchange リスナセキュリティが有効化されているときに、PowerExchange リスナにアクセスするために使用できるユーザー名。詳細については、『PowerExchange リファレンスマニュアル』の「SECURITY 文」を参照してください。
パスワード	**［ユーザー名］**プロパティで指定されるユーザー名と関連付けられたパスワード。
コレクション名	IDMS データソースのキャプチャ登録が含まれる登録グループの **［コレクション** ID］フィールド内に指定されるインスタンス名。この値は、接続の使用時に、PWX CDC メタデータアダプタがインポートする抽出マップメタデータをフィルタするために使用されます。
CAPI 接続名	PowerExchange DBMOVER コンフィギュレーションファイル内に定義される CAPX CAPI_CONNECTION 文の名前。この文には、PWX CDC リーダーが PowerExchange ロッガー（Linux、UNIX、Windows 用）ログファイルからの変更データを抽出するために使用するパラメータが含まれます。PWX CDC リーダーにこのプロパティ値が必要であり、DBMOVER コンフィギュレーションファイル内に定義される任意のデフォルトの CAPI_CONNECTION 文を無視します。
接続リトライ期限	初期接続の試行の失敗後、PWX CDC リーダーが PowerExchange リスナへの再接続を試行する秒数。接続が再試行時間中に確立できない場合、マッピングタスクに失敗します。デフォルト値は 0 であり、接続の再試行は無効になります。
圧縮	変更データをネットワーク経由で PWX CDC リーダーに送信する前に、PowerExchange リスナがデータを圧縮するかどうかを制御します。データを圧縮するには、このプロパティを選択します。デフォルトでは、このプロパティは選択されていません。
暗号化	変更データをネットワーク経由で PWX CDC リーダーに送信する前に、PowerExchange リスナがデータを暗号化するかどうかを制御します。また、使用する暗号化の種類も指定します。次のいずれかのオプションを選択します。 - **なし**。暗号化は使用しません。 - AES 128 **ビット**。128 ビットの暗号化キーを使用します。 - AES 192 **ビット**。192 ビットの暗号化キーを使用します。 - AES 256 **ビット**。256 暗号化キーを使用します。 デフォルトは **［なし］**です。
ペーシングサイズ	後続データ用に次の PWX CDC リーダー要求を待機する一時停止までに、ソースシステムが PowerExchange リスナに渡す行数またはキロバイト単位でのデータ量。この値を減らすと、セッションのパフォーマンスが向上します。パフォーマンスを最大にするには、0 を使用します。 デフォルトである最小値は 0 です。
ペーシング単位	**［ペーシングサイズ］**プロパティと一緒に使用する単位の種類。 **［行］**または **［キロバイト］**のいずれかを選択します。

プロパティ	説明
マップの場所	抽出マップがあるシステムのホスト名または IP アドレス。ポート番号も含めます。 この値は、PowerExchange リスナが、抽出マップからリモートにある PowerExchange ロッガー（Linux、UNIX、Windows 用）マシン上で実行されている場合に必要です。リスナは、変更データ抽出要求を処理するために、抽出マップへのアクセスを必要とします。 次の形式で値を入力します。*host_name* は、ホスト名または IP アドレスにできます。 *host_name*:*port_number* 以下に例を示します。 CDC01:25100 **注**: 接続をテストして抽出マップメタデータをインポートするための **[マップの場所]** の値は、**[リスナの場所]** の値よりも優先されます。
マップの場所のユーザー	**[マップの場所]** プロパティ内に指定された場所の PowerExchange リスナにアクセスできるユーザー名。
マップの場所のパスワード	**[マップの場所のユーザー]** プロパティで指定されるユーザー名と関連付けられたパスワード。
イベントテーブル	ユーザー定義イベントに基づく変更データ抽出を停止するためにイベントテーブルを作成した場合、イベントテーブルの PowerExchange 抽出マップの名前を入力します。IDMS イベントテーブルは、CDC ソースシステム上に存在する必要があります。
低値をスペースに置き換える	文字データ内の NULL をスペースに置き換えるかどうかを制御します。文字データ内の NULL を置き換えるには、このプロパティを選択します。デフォルトでは、このプロパティが選択されています。
カスタムプロパティ	PowerExchange のデフォルト設定よりも優先するために指定できるカスタムプロパティ。セミコロン（;）を区切り文字として使用することで、複数のプロパティを入力できます。通常は、Informatica グローバルカスタマサポートの指示の下でのみ、カスタムプロパティを設定します。 **注**: これらのプロパティは、PowerCenter の PowerExchange Client for PowerCenter（PWXPC）IDMS CDC 接続の **[PWX オーバーライド]** オプションと同じです。

IDMS 接続のプロパティ

IDMS 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。

以下の表に、IDMS 接続のプロパティを示します。

プロパティ	説明
接続名	IDMS 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	IDMS 接続の説明。最大長は 4000 文字です。
タイプ	接続タイプ。IDMS の場合、タイプは［IDMS］である必要があります。
ランタイム環境	マッピングタスクの実行に使用する Secure Agent が含まれるランタイム環境の名前。
リスナの場所	IDMS の要求を処理する PowerExchange リスナを実行するシステムのホスト名または IP アドレス。リスナのポート番号も含めます。次の形式で値を入力します。*host_name* は、ホスト名または IP アドレスにできます。 *host_name*:*port_number* 以下に例を示します。 PWXMLSNR:14673
ユーザー名	PowerExchange リスナセキュリティが有効化されているときに、PowerExchange リスナにアクセスするために使用できるユーザー名。詳細については、『PowerExchange リファレンスマニュアル』の「SECURITY 文」を参照してください。
パスワード	**［ユーザー名］**プロパティで指定されるユーザー名と関連付けられたパスワード。
スキーマ名	IDMS ソースのスキーマ名。
コードページ	ソースデータベースからデータを抽出するために、データ統合サービスの Secure Agent が使用するコードページ。
オフロード処理	オフロード処理を使用するかどうかを制御します。オフロード処理は、バルクデータ処理をソースシステムからターゲットシステムに転送します。次のオプションがあります。 - **自動**。オフロード処理を使用するかどうかが Cloud データ統合によって決定されます。 - **事後フィルタ**。データのフィルタリングなど、バルクデータ処理をターゲットにオフロードします。 - **事前フィルタ**。処理はターゲットにオフロードされますが、データは引き続きソースシステム上でフィルタリングされます。 - **いいえ**。オフロード処理を無効化します。 デフォルトは［いいえ］です。

プロパティ	説明
オフロードスレッド	Cloud データ統合がバルクデータを処理するために使用するスレッドの数。 最適なパフォーマンスを得るには、この値が、Secure Agent が実行されているマシンに搭載済み、またはこのマシンで使用可能なプロセッサ数より大きくならないようにします。 有効な値は 1〜64 です。 デフォルトは 0 です。マルチスレッド処理は無効になります。 すべての接続タイプがオフロードスレッドをサポートしているわけではありません。これらのうち、いずれかの接続の**［オフロードスレッド］**接続プロパティがゼロ以外の値に設定されている場合は、スレッドなしで処理が続行されます。
配列サイズ	IDMS データソースおよびシーケンシャルファイルの場合は、パーティション化されたセッションまたはマルチスレッドセッションで使用されるストレージ配列のサイズ（単位はレコード数）。 パーティション化されたセッションの場合、この配列サイズはパーティション間で共有されます。マルチスレッドセッションの場合、各スレッドでこの配列サイズが使用されます。 有効な値は 1〜5000 です。デフォルトは 25 です。 特に**［書き込みモード］**プロパティで**［書き込み確認オン］**が指定されている場合、パーティション化されたセッションを調整するために配列サイズを増やします。
低値をスペースに置き換える	文字データ内の NULL をスペースに置き換えるかどうかを制御します。文字データ内の NULL を置き換えるには、このプロパティを選択します。デフォルトでは、このプロパティが選択されています。
接続リトライ期限	初期接続の試行の失敗後、PowerExchange Bulk Reader が PowerExchange リスナへの再接続を試行する秒数。接続が再試行時間中に確立できない場合、マッピングタスクに失敗します。デフォルト値は 0 であり、接続の再試行は無効になります。
カスタムプロパティ	PowerExchange のデフォルト設定よりも優先するために指定できるカスタムプロパティ。セミコロン（;）を区切り文字として使用することで、複数のプロパティを入力できます。カスタムプロパティの設定は、Informatica グローバルカスタマサポートの指示の下でのみ行ってください。 **注**: これらのプロパティは、PowerCenter の PowerExchange Client for PowerCenter（PWXPC）IDMS 接続の**［PWX オーバーライド］**オプションと同じです。
書き込みプロパティ> 書き込みモード	次のオプションがあります。 - **書き込み確認オン**。PowerExchange リスナにデータを送信し、成功/失敗の応答を待ってから、以降のデータを送信します。このモードではデータをバッファしないで、PowerExchange リスナにデータを同期的に送信します。 - **書き込み確認オフ**。データをバッファして PowerExchange リスナにデータを非同期的に送信します。このモードでは、成功または失敗応答を待機しません。 デフォルト値は**［書き込み確認オン］**です。

IMS CDC 接続のプロパティ

IMS CDC 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、IMS CDC 接続のプロパティを示します。

プロパティ	説明
接続名	IMS CDC 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	IMS CDC 接続の説明。最大長は 4000 文字です。
タイプ	接続タイプ。IMS CDC の場合、タイプは［IMS CDC］である必要があります。
ランタイム環境	マッピングタスクの実行に使用する Secure Agent が含まれるランタイム環境の名前。
リスナの場所	IMS 変更データのための PWX CDC リーダー要求を処理する PowerExchange リスナがあり、PowerExchange ロッガー（Linux、UNIX、Windows 用）を実行するシステムのホスト名または IP アドレス。リスナのポート番号も含めます。次の形式で値を入力します。*host_name* は、ホスト名または IP アドレスにできます。 *host_name*:*port_number* 以下に例を示します。 ADACDC1A:1467
ユーザー名	PowerExchange リスナセキュリティが有効化されているときに、PowerExchange リスナにアクセスするために使用できるユーザー名。詳細については、『PowerExchange リファレンスマニュアル』の「SECURITY 文」を参照してください。
パスワード	**［ユーザー名］**プロパティで指定されるユーザー名と関連付けられたパスワード。
コレクション名	IMS ソーステーブルのキャプチャ登録が含まれる登録グループの**［データベースインスタンス］**フィールド内に指定される IMS インスタンス。この値は、接続の使用時に、PWX CDC メタデータアダプタがインポートする抽出マップメタデータをフィルタするために使用されます。
CAPI 接続名	PowerExchange DBMOVER コンフィギュレーションファイル内に定義される CAPX CAPI_CONNECTION 文の名前。この文には、PWX CDC リーダーが PowerExchange ロッガー（Linux、UNIX、Windows 用）ログファイルからの変更データを抽出するために使用するパラメータが含まれます。PWX CDC リーダーにこのプロパティ値が必要であり、DBMOVER コンフィギュレーションファイル内に定義される任意のデフォルトの CAPI_CONNECTION 文を無視します。
接続リトライ期限	初期接続の試行の失敗後、PWX CDC リーダーが PowerExchange リスナへの再接続を試行する秒数。接続が再試行時間中に確立できない場合、マッピングタスクに失敗します。デフォルト値は 0 であり、接続の再試行は無効になります。
圧縮	変更データをネットワーク経由で PWX CDC リーダーに送信する前に、PowerExchange リスナがデータを圧縮するかどうかを制御します。データを圧縮するには、このプロパティを選択します。デフォルトでは、このプロパティは選択されていません。

プロパティ	説明
暗号化	変更データをネットワーク経由で PWX CDC リーダーに送信する前に、PowerExchange リスナがデータを暗号化するかどうかを制御します。また、使用する暗号化の種類も指定します。次のいずれかのオプションを選択します。 - **なし**。暗号化は使用しません。 - AES 128 **ビット**。128 ビットの暗号化キーを使用します。 - AES 192 **ビット**。192 ビットの暗号化キーを使用します。 - AES 256 **ビット**。256 暗号化キーを使用します。 デフォルトは **［なし］** です。
ペーシングサイズ	後続データ用に次の PWX CDC リーダー要求を待機する一時停止までに、ソースシステムが PowerExchange リスナに渡す行数またはキロバイト単位でのデータ量。この値を減らすと、セッションのパフォーマンスが向上します。パフォーマンスを最大にするには、0 を使用します。 デフォルトである最小値は 0 です。
ペーシング単位	**［ペーシングサイズ］** プロパティと一緒に使用する単位の種類。 **［行］** または **［キロバイト］** のいずれかを選択します。
マップの場所	抽出マップがあるシステムのホスト名または IP アドレス。ポート番号も含めます。 この値は、PowerExchange リスナが、抽出マップからリモートにある PowerExchange ロッガー（Linux、UNIX、Windows 用）マシン上で実行されている場合に必要です。リスナは、変更データ抽出要求を処理するために、抽出マップへのアクセスを必要とします。 次の形式で値を入力します。*host_name* は、ホスト名または IP アドレスにできます。 *host_name*:*port_number* 以下に例を示します。 ADACDC01:25100 **注**: 接続をテストして抽出マップメタデータをインポートするための **［マップの場所］** の値は、**［リスナの場所］** の値よりも優先されます。
マップの場所のユーザー	**［マップの場所］** プロパティ内に指定された場所の PowerExchange リスナにアクセスできるユーザー名。
マップの場所のパスワード	**［マップの場所のユーザー］** プロパティで指定されるユーザー名と関連付けられたパスワード。
イベントテーブル	ユーザー定義イベントに基づく変更データ抽出を停止するためにイベントテーブルを作成した場合、イベントテーブルの PowerExchange 抽出マップの名前を入力します。イベントテーブルは、CDC ソースシステム上の IMS テーブルである必要があります。
低値をスペースに置き換える	文字データ内の NULL をスペースに置き換えるかどうかを制御します。文字データ内の NULL を置き換えるには、このプロパティを選択します。デフォルトでは、このプロパティが選択されています。
カスタムプロパティ	PowerExchange のデフォルト設定よりも優先するために指定できるカスタムプロパティ。セミコロン（;）を区切り文字として使用することで、複数のプロパティを入力できます。通常は、Informatica グローバルカスタマサポートの指示の下でのみ、カスタムプロパティを設定します。 **注**: これらのプロパティは、PowerCenter の PowerExchange Client for PowerCenter（PWXPC）IMS CDC 接続の **［PWX オーバーライド］** オプションと同じです。

IMS 接続のプロパティ

IMS 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、IMS 接続のプロパティを示します。

プロパティ	説明
接続名	IMS 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	IMS 接続の説明。最大長は 4000 文字です。
タイプ	接続タイプ。IMS の場合、タイプは［IMS］である必要があります。
ランタイム環境	マッピングタスクの実行に使用する Secure Agent が含まれるランタイム環境の名前。
リスナの場所	IMS の要求を処理する PowerExchange リスナを実行するシステムのホスト名または IP アドレス。リスナのポート番号も含めます。次の形式で値を入力します。*host_name* は、ホスト名または IP アドレスにできます。 *host_name*:*port_number* 以下に例を示します。 PWXMLSNR:14673
ユーザー名	PowerExchange リスナセキュリティが有効化されているときに、PowerExchange リスナにアクセスするために使用できるユーザー名。詳細については、『PowerExchange リファレンスマニュアル』の「SECURITY 文」を参照してください。
パスワード	**［ユーザー名］**プロパティで指定されるユーザー名と関連付けられたパスワード。
スキーマ名	IMS ソースのスキーマ名。
コードページ	ソースデータベースからデータを抽出するために、データ統合サービスの Secure Agent が使用するコードページ。
オフロード処理	オフロード処理を使用するかどうかを制御します。オフロード処理は、バルクデータ処理をソースシステムからターゲットシステムに転送します。次のオプションがあります。 - **自動**。オフロード処理を使用するかどうかが Cloud データ統合によって決定されます。 - **事後フィルタ**。データのフィルタリングなど、バルクデータ処理をターゲットにオフロードします。 - **事前フィルタ**。処理はターゲットにオフロードされますが、データは引き続きソースシステム上でフィルタリングされます。 - **いいえ**。オフロード処理を無効化します。 デフォルトは［いいえ］です。

プロパティ	説明
オフロードスレッド	Cloud データ統合がバルクデータを処理するために使用するスレッドの数。 最適なパフォーマンスを得るには、この値が、Secure Agent が実行されているマシンに搭載済み、またはこのマシンで使用可能なプロセッサ数より大きくならないようにします。 有効な値は 1〜64 です。 デフォルトは 0 です。マルチスレッド処理は無効になります。 すべての接続タイプがオフロードスレッドをサポートしているわけではありません。これらのうち、いずれかの接続の**［オフロードスレッド］**接続属性がゼロ以外の値に設定されている場合は、スレッドなしで処理が続行されます。
配列サイズ	IMS データセットおよびシーケンシャルファイルの場合は、パーティション化されたセッションまたはマルチスレッドセッションで使用されるストレージ配列のサイズ（単位はレコード数）。 パーティション化されたセッションの場合、この配列サイズはパーティション間で共有されます。マルチスレッドセッションの場合、各スレッドでこの配列サイズが使用されます。 有効な値は 1〜5000 です。デフォルトは 25 です。 特に**［書き込みモード］**属性で**[書き込み確認オン]**が指定されている場合、パーティション化されたセッションを調整するために配列サイズを増やします。
低値をスペースに置き換える	文字データ内の NULL をスペースに置き換えるかどうかを制御します。文字データ内の NULL を置き換えるには、このプロパティを選択します。デフォルトでは、このプロパティが選択されています。
接続リトライ期限	初期接続の試行の失敗後、PowerExchange Bulk Reader が PowerExchange リスナへの再接続を試行する秒数。接続が再試行時間中に確立できない場合、マッピングタスクに失敗します。デフォルト値は 0 であり、接続の再試行は無効になります。
カスタムプロパティ	PowerExchange のデフォルト設定よりも優先するために指定できるカスタムプロパティ。セミコロン（;）を区切り文字として使用することで、複数のプロパティを入力できます。通常は、Informatica グローバルカスタマサポートの指示の下でのみ、カスタムプロパティを設定します。 **注**: これらのプロパティは、PowerCenter の PowerExchange Client for PowerCenter（PWXPC）IMS 接続の**［PWX オーバーライド］**オプションと同じです。
書き込みプロパティ	書き込みモード。次のオプションがあります。 - **書き込み確認オン**。PowerExchange リスナにデータを送信し、成功/失敗の応答を待ってから、以降のデータを送信します。このモードではデータをバッファしないで、PowerExchange リスナにデータを同期的に送信します。 - **書き込み確認オフ**。データをバッファして PowerExchange リスナにデータを非同期的に送信します。このモードでは、成功または失敗応答を待機しません。 デフォルト値は**［書き込み確認オン］**です。

JDBC 接続プロパティ

JDBC 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、JDBC 接続のプロパティを示します。

接続プロパティ	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。
JDBC 接続 URL	データベースに接続するための JDBC URL 文字列。 JDBC URL の形式は次のとおりです: `jdbc:<サブプロトコル>:<サブネーム>` ここで、サブプロトコルは、1 つ以上のドライバがサポートするデータベース接続メカニズムを定義します。サブネームの内容と構文は、サブプロトコルに応じて異なります。 JDBC URL 接続文字列のフォーマット要件については、JDBC ドライバベンダ固有のドキュメントを参照してください。
JDBC Jar ディレクトリ	オプション。JDBC ドライバ jar ファイルへのパス。例えば、次のディレクトリを入力できます: `C:/jdbc`。ディレクトリパスを指定しない場合、Secure Agent は、CLASSPATH システム変数に指定されたディレクトリから jar ファイルを取得します。 JDBC 接続にサーバーレスランタイム環境を使用するには、次の場所を指定します: `/home/cldagnt/SystemAgent/serverless/configurations/jdbc`
JDBC ドライバクラス名	オプション。JDBC ドライバを自動クラス読み込み機能なしで使用している場合、JDBC ドライバのクラス名を指定します。このプロパティを指定しない場合、Secure Agent は JDBC ドライバの jar ファイルからドライバのクラス名を読み込みます。
スキーマ	スキーマ名。データベースによって異なります。以下に例を示します。 - Informix。オプション。スキーマ名はデータベース名です。 JDBC 接続 URL から十分なコンテキストが得られない場合は、スキーマ名を入力してメタデータを取得する必要があります。
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	データベースに接続するためのパスワード。

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 またはサーバーレスランタイム環境を指定できます。
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。
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。
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。

プロパティ	説明
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。
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。

JD Edwards EnterpriseOne 接続のプロパティ

JD Edwards EnterpriseOne 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、JD Edwards EnterpriseOne 接続プロパティを示します。

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。
ホスト名	JD Edwards EnterpriseOne サーバーのホスト名。
エンタープライズポート	JD Edwards EnterpriseOne サーバーのポート番号。デフォルトは 6016 です。
ユーザー名	JD Edwards EnterpriseOne データベースユーザーの名前。
パスワード	JD Edwards EnterpriseOne データベースユーザーのパスワード。
環境	接続先の JD Edwards EnterpriseOne 環境の名前。
ロール	JD Edwards EnterpriseOne ユーザーのロール。デフォルトは［*すべて］です。
ユーザー名	JD Edwards EnterpriseOne データベースユーザーの名前。
パスワード	データベースユーザーのパスワード。

プロパティ	説明
ドライバクラス名	該当するデータベースタイプに入力できるドライバクラス名を示します。インタフェーステーブルの書き込みオプションを使用して、データを一括で書き込むために必要です。次の JDBC ドライバクラス名を使用します。 - Oracle 用 DataDirect JDBC ドライバクラス名: `com.informatica.jdbc.oracle.OracleDriver` - IBM DB2 用 DataDirect JDBC ドライバクラス名: `com.informatica.jdbc.db2.DB2Driver` - Microsoft SQL Server 用 DataDirect JDBC ドライバクラス名: `com.informatica.jdbc.sqlserver.SQLServerDriver` 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、ベンダ提供のドキュメントを参照してください。
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。インタフェーステーブルの書き込みオプションを使用して、データを一括で書き込むために必要です。 JDBC 接続文字列では、次の構文を使用します。 - Oracle の場合: `jdbc:informatica:oracle://<host name>:<port>,ServiceName=<db service name>` - DB2 の場合: `jdbc:informatica:db2://<host name>:<port>;databaseName=<db name>` - Microsoft SQL の場合: `jdbc:informatica:sqlserver://<host name>:<port>;databaseName=<db name>`
JDE 製品コード	JD Edwards EnterpriseOne 内のテーブルとビューのための製品コード。 **注**: 説明なしで、製品コードのみを指定する必要があります。有効でないスキーマを指定した場合、Java の例外が表示されます。

JIRA 接続のプロパティ

JIRA 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、JIRA 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	JIRA 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 または Hosted Agent を選択します。
ユーザー名	JIRA アカウントのユーザー名。

プロパティ	説明
パスワード	JIRA アカウントの API トークン。 API トークンの作成方法の詳細については、ナレッジベースの記事 KB 576517 を参照してください。
URI	接続先の JIRA インスタンスのベース JIRA URI。例: https://<abcd>.atlassian.net/
UTC オフセット	日時フィールドに追加するための UTC 時間のオフセットを選択します。デフォルト値は UTC です。
ロギングの有効化	必要に応じてロギングを有効にするには、このボックスを選択します。

JIRA Cloud 接続のプロパティ

JIRA 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する必要があります。

次の表に、JIRA Cloud 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	JIRA Cloud 接続の名前。
説明	JIRA Cloud 接続の説明。
タイプ	接続タイプ。一覧から［JiraCloud（Informatica)］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。
認証	接続の認証タイプ。［JiraCloud］を選択します。
URI	接続先の JIRA インスタンスのベース JIRA URI。例えば、https://abcd.atlassian.net。
ユーザー名	JIRA アカウントのユーザー名。
パスワード	JIRA アカウントの API トークン。 API トークンの作成方法の詳細については、 https://kb.informatica.com/solution/23/Pages/70/576517.aspx を参照してください。

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。

JSON Target 接続のプロパティ

JSON Target 接続を作成する際には、接続プロパティを設定する必要があります。

次の表に、JSON Target 接続のプロパティを示します。

接続プロパティ	説明
Secure Agent	一覧から該当する Secure Agent を選択します。
サンプル JSON スキーマ名	サンプル JSON ファイルパスを入力します。 例: ABCD.JSON
JSON 作業ディレクトリ	JSON 作業ディレクトリのフォルダパスを入力します。
最終 JSON ファイル名	最終 JSON ファイルのパスとファイル名を入力します。
JSON カスタマイズが必要	JSON のカスタマイズを可能にします。 デフォルトは **［いいえ］** です。
最終カスタマイズ JSON ファイル名	最終カスタマイズ JSON ファイルのパスとファイル名を入力します。

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。

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。 詳細クラスタで実行されるマッピングに対して、Secure Agent またはサーバーレスランタイム環境を指定します。
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。
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。
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。

プロパティ	説明
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。
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。

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。

プロパティ	説明
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。
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。

LDAP 接続のプロパティ

LDAP 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、LDAP 接続のプロパティを示します。

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。 **注**: Secure Agent のみを、LDAP 接続のランタイム環境として指定できます。

ホスト名	必須。LDAP ディレクトリサーバーのホスト名。
	LDAP または LDAPS プロトコルを LDAP サーバーへの接続に使用できます。
	- LDAP プロトコルを使用するには、次の形式のいずれかを使用します。
	  - `ldap://<hostname>`
	  - `<hostname>`
	- LDAPS プロトコルを使用するには、`ldaps://<hostname>`の形式を使用します。
	注: SSL を使用する場合、SSL 証明書内に指定したホスト名を使用します。

ポート	必須。LDAP ディレクトリサーバーのポート番号。デフォルトは 389 です。
匿名接続	LDAP ディレクトリサーバーとの匿名接続を確立します。匿名接続を選択し、認証不要の匿名ユーザーとしてディレクトリサーバーにアクセスします。 **注**: Active Directory とは匿名接続を確立できません。
ユーザー名	LDAP ディレクトリサーバーに接続するための LDAP ユーザー名。 Active Directory に接続する場合に必要です。
パスワード	LDAP ディレクトリサーバーに接続するためのパスワード。パスワードを入力しないと、クライアントは匿名接続を確立します。 Active Directory に接続する場合に必要です。
セキュアな接続	TLS プロトコル経由で LDAP ディレクトリサーバーとのセキュアな接続を確立します。
TrustStore のファイル名	LDAP ディレクトリサーバーとの一方向のセキュア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のファイル名。 トラストストアのファイル名とパスワードについては、LDAP 管理者にお問い合わせください。
TrustStore 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。
KeyStore のファイル名	LDAP ディレクトリサーバーとの双方向のセキュアな通信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のファイル名。 キーストアのファイル名とパスワードについては、LDAP 管理者にお問い合わせください。

プロパティ	説明
KeyStore 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。
ベース DN。	必須。LDAP ディレクトリサーバー内のルートディレクトリの識別名 (DN)。 例えば、Informatica ドメインに接続するには、`dc=informatica-connector,dc=com` というベース DN を使用します。 ベース DN を指定しない場合、Secure Agent はメタデータの取得に失敗します。

Litmos 接続のプロパティ

Litmos 接続を作成する際には、接続プロパティを設定する必要があります。

次の表に、Litmos 接続のプロパティを示します。

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。
apikey	アカウント所有者のプロファイルからの API キー。
ソース	アカウント所有者のプロファイルからのソース。
pageSize	読み取り操作のページサイズ。 デフォルト値は 100 です。
baseURI	Litmos API に接続するためのエンドポイント URI を指定します。 例: https://api.litmos.com/v1.sv
apiLimit	1 分あたりの API コールの数。 デフォルト値は 100 です。
waittime	Litmos API コール数が API 制限を超えてから API コールを再試行するまでの待機時間。

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。 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。
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	管理者が Marketo REST API を呼び出して Marketo に対してデータの読み取りおよび書き込みを実行するためのアクセス権限。 Marketo では、client_credentials 許可タイプのみサポートしています。
REST API URL	Secure Agent が Marketo REST API に接続するために使用する 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	proxy.ini ファイルで定義されているプロキシサーバー設定を使用するか、Secure Agent Manager を使用して Marketo に接続するオプション。 [プロキシのバイパス] を選択すると、Secure Agent Manager を使用して Marketo に接続します。[プロキシのバイパス] をオフにすると、プロキシサーバーを使用して Marketo に接続します。 デフォルトは、プロキシのバイパスです。 **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。

MemSQL V2 接続のプロパティ

MemSQL V2 接続を作成する際には、接続プロパティを設定する必要があります。

次の表に、MemSQL V2 接続のプロパティを示します。

プロパティ	説明
ランタイム環境	マッピングタスクの実行に使用する Secure Agent が含まれるランタイム環境の名前。
ユーザー名	MemSQL データベースに接続するためのユーザー名。
パスワード	MemSQL データベースに接続するためのパスワード。
ホスト名	MemSQL データベースサーバーのホスト名または IP アドレス。
ポート番号	MemSQL データベースのポート番号。
カタログ	MemSQL データベースインスタンスの名前。
カスタム URL を使用	オプション。チェックボックスを選択して MemSQL データベース接続の URL を入力します。
カスタム URL	オプション。MemSQL データベース接続のカスタム URL。
ステージングパス	MemSQL V2 コネクタがファイルをステージング出来るステージングディレクトリのパス。

Microsoft Access 接続のプロパティ

Microsoft Access 接続をセットアップするときは、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。

接続プロパティ	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。
データソース名	システム DSN 名。
コードページ	Microsoft Access ソースと互換性のあるコードページ。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。 - 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。

Microsoft Azure Blob Storage V2 接続のプロパティ

Microsoft Azure Blob ストレージ V2 接続を作成するときには、接続プロパティを設定する必要があります。

以下の表に、Microsoft Azure Blob ストレージ V2 接続プロパティを示します。

接続プロパティ	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。
アカウント名	Microsoft Azure Blob ストレージアカウント名。
アカウントキー	Microsoft Azure Blob ストレージアクセスキー。
コンテナ名	Microsoft Azure Blob ストレージコンテナ名。

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。
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リソースへのアクセス許可を付与します。
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。

プロパティ	説明
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 Cosmos DB SQL API 接続のプロパティ

Microsoft Azure Cosmos DB SQL API 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 Cosmos DB SQL API 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	Microsoft Azure Cosmos DB SQL API の接続タイプ。
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指定します。 Hosted Agent は、詳細モードのマッピングには適用されません。
Cosmos DB URI	Microsoft Azure Cosmos DB アカウントの URI。
キー	Microsoft Azure Cosmos DB アカウント内のリソースへの完全な管理アクセス権限を提供するプライマリキーまたはセカンダリキー。
データベース	JSON ドキュメントとの間での読み書きするコレクションが格納されているデータベース名。

Microsoft Azure Data Lake Storage Gen1 V2 接続のプロパティ

Microsoft Azure Data Lake Storage Gen1 V2 接続をセットアップするときは、接続プロパティを設定する必要があります。

以下の表に、Microsoft Azure Data Lake Storage Gen1 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	Microsoft Azure Data Lake Storage Gen1 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。
タイプ	接続タイプ。Microsoft Azure Data Lake Storage Gen1 V2 接続を選択します。
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。
ADLS アカウント名	Microsoft Azure Data Lake Storage Gen1 アカウントの名前。
ClientID	Active Directory で OAuth 認証を完了するための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	データの読み取りまたは書き込みに使用する Microsoft Azure Data Lake Storage Gen1 ディレクトリ。デフォルトはルートディレクトリです。
AuthEndpoint	クライアント ID および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。

クライアント ID、クライアントシークレット、および AuthEndpoint の作成の詳細については、『*Microsoft Azure Data Lake Storage Gen1 のドキュメント*』を参照してください。

Microsoft Azure Data Lake Storage Gen1 V3 接続のプロパティ

Microsoft Azure Data Lake Storage Gen1 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する必要があります。

以下の表に、Microsoft Azure Data Lake Storage Gen1 V3 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	Microsoft Azure Data Lake Storage Gen1 V3 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。
タイプ	接続タイプ。Microsoft Azure Data Lake Storage Gen1 V3 接続を選択します。

接続プロパティ	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。
ADLS アカウント名	Microsoft Azure Data Lake Storage Gen1 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	データの読み取りまたは書き込みに使用する Microsoft Azure Data Lake Storage Gen1 ディレクトリ。デフォルトはルートディレクトリです。
AuthEndpoint	クライアント ID および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。
サブフォルダの表示	指定したディレクトリのサブフォルダからオブジェクトをインポートするために、サブフォルダを有効にします。

クライアント ID、クライアントシークレット、AuthEndpoint の作成の詳細については、*Microsoft Azure Data Lake Store のドキュメント*を参照してください。

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。
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 は、詳細モードのマッピングには適用されません。 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。

プロパティ	説明
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。システム割り当てマネージド ID によって権限が提供されている場合は、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 つしかない場合は、フィールドを空のままにしておくこともできます。
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。
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 **注**: 詳細モードでは、マッピング用に Azure Government エンドポイントを設定することはできません。

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。
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 SQL Data Warehouse - データベース取り込み接続のプロパティ

Microsoft Azure SQL Data Warehouse データベース取り込み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 Gen1 用です。一括取り込みデータベースは、Microsoft Azure Data Lake Storage Gen1 を使用して、データを Microsoft Azure SQL Database Warehouse 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。Microsoft Azure SQL Data Warehouse - データベース取り込みのタイプを選択してい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。

Azure DW JDBC URL	Microsoft Azure SQL Data Warehouse 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 DW JDBC ユーザー名	Microsoft Azure SQL Data Warehouse 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 DW JDBC パスワード	Microsoft Azure SQL Data Warehouse アカウントに接続するために使用するパスワード。
Azure DW スキーマ名	Microsoft Azure SQL Data Warehouse ターゲット内のスキーマの名前。
ADLS アカウント名	Microsoft Azure Data Lake Storage Gen1 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。

プロパティ	説明
ディレクトリ	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 Gen1 ディレクトリ。デフォルトはルートディレクトリです。
AuthEndpoint	クライアント ID および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。

Microsoft Azure SQL Data Warehouse V2 接続のプロパティ

次の表に、Microsoft Azure SQL Data Warehouse V2 接続のプロパティを示します。

接続プロパティ	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。

Azure DW JDBC URL	Microsoft Azure Data Warehouse JDBC 接続文字列。
	Microsoft SQL Server 認証の例:
	`jdbc:sqlserver://<Server>.database.windows.net:1433;database=<Database>`
	Azure Active Directory（AAD）認証の例:
	`jdbc:sqlserver://<Server>.database.windows.net:1433;database=<Database>;encrypt=true;trustServerCertificate=false;hostNameInCertificate=*.database.windows.net;loginTimeout=30;Authentication=ActiveDirectoryPassword;`
	デフォルトの認証は、Microsoft SQL Server 認証です。

Azure DW JDBC ユーザー名	Microsoft Azure SQL Data Warehouse 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 SQL Data Warehouse アカウントに接続するためのパスワード。
Azure DW スキーマ名	Microsoft Azure SQL Data Warehouse 内のスキーマの名前。
Azure Blob アカウント名	ファイルをステージングする Microsoft Azure ストレージアカウントの名前。
Azure Blob アカウントキー	ファイルをステージングするための Microsoft Azure ストレージアクセスキー。

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。 Hosted Agent は、詳細モードのマッピングには適用されません。

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;`
	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。
Azure DW スキーマ名	Microsoft Azure Synapse SQL 内のスキーマの名前。
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。

プロパティ	説明
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。
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。

プロパティ	説明
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 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 CDM Folders V2 接続プロパティ

Microsoft CDM Folders V2 接続をセットアップする場合は、接続プロパティを設定します。

次の表に、Microsoft CDM Folders 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。 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 CDM Folders 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 または Hosted Agent を選択します。
ADLSGen2 ストレージアカウント名	ADLS Gen2 ストレージアカウントの名前。
Azure AD アプリクライアント ID	ストレージアカウントへのユーザーアクセスの認証を行う Azure Active Directory アカウントのクライアント ID。 アプリケーション ID は Microsoft Azure Active Directory 管理者から取得できます。
Azure AD アプリクライアントシークレット	ストレージアカウントへのアクセスの認証を行う Azure Active Directory アプリケーションのクライアント秘密鍵。 キーの値は Microsoft Azure Active Directory 管理者から取得できます。
Azure テナント ID	ストレージアカウントへのユーザーアクセスの認証を行う Azure Active Directory アカウントのテナント ID。 Microsoft Azure Active Directory 管理者からディレクトリ ID を取得できます。
ADLS Gen2 ファイルシステム名	Azure Storage Explorer アプリケーションで作成したファイルシステムの名前。 ファイルシステムには複数の共通データモデルフォルダを含める事ができます。
CDM フォルダパス	ファイルシステム内に作成した共通のデータモデルフォルダのパスです。 CDM フォルダパスには次の値を使用できます。 - / - /folder1 - /folder1/folder2 推奨される CDM フォルダパスは/folder1 です。 デフォルトは空白です。
ADLS Gen2 エンドポイント	ADLS Gen2 エンドポイントの core.windows.net。

Microsoft Dynamics 365 for Operations 接続のプロパティ

Microsoft Dynamics 365 for Operations 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、Microsoft Dynamics 365 for Operations 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 Dynamics 365 for Operations 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 または Hosted Agent を選択します。
認証タイプ	Web アプリケーションへログインするためにコネクタで使用する認証方法。 次のいずれかの認証タイプを選択します。 - OAuth 2.0。サービス URL、ユーザー名、パスワード、およびアプリケーション ID が必要です。 - OAuth 2.0 クライアントシークレットグラント。サービス URL、アプリケーション ID、テナント ID、およびクライアントシークレットが必要です。 - OAuth 2.0 クライアント証明書付与。キーストアファイル、キーストアパスワード、キーエイリアス、およびキーパスワードが必要です。該当なし。

サービス URL	Microsoft Dynamics 365 for Operations サービスの URL を次の形式で入力します。
	`https:<server name>:<port number>`
	または
	`http:<server name>:<port number>`
	URL にポート番号を指定しない場合、エージェントはポート番号 443 をクエリに使用します。

ユーザー名	Microsoft Dynamics 365 for Operations アカウントに接続するためのユーザー名。
パスワード	Microsoft Dynamics 365 for Operations アカウントに接続するためのパスワード。
アプリケーション ID	Microsoft Dynamics 365 for Operations のネイティブアプリケーション ID。
テナント ID	Azure Active Directory のディレクトリ ID。
クライアントシークレット	Microsoft Dynamics 365 for Operations アカウントのクライアントシークレット。
再試行エラーコード	再試行を実行するカンマ区切りの HTTP エラーコード。

プロパティ	説明
RETRY_COUNT	再試行間隔に基づいて、エンドポイントから応答を取得する再試行回数。 デフォルトは 0 です。
再試行間隔	Microsoft Dynamics 365 for Operations コネクタが応答を再試行するまでに待機する秒数。 デフォルトは 60 秒です。

Microsoft Dynamics 365 for Sales 接続のプロパティ

Microsoft Dynamics 365 for Sales 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、Microsoft Dynamics 365 for Sales 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 Dynamics 365 for Sales 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指定します。 Hosted Agent を使用して Microsoft Dynamics 365 for Sales にアクセスする場合は、接続で OAuth 2.0 パスワード認証承認を使用する必要があります。
認証タイプ	オンラインまたはオンプレミスで Microsoft Dynamics 365 for Sales にログインするためにコネクタが使用する必要のある認証方法。 次のいずれかの認証タイプを選択します。 - OAuth 2.0 パスワード付与。Web API URL、ユーザー名、パスワード、およびアプリケーション ID が必要です。さらに、オンプレミスの Microsoft Dynamics 365 for Sales にアクセスするには、セキュリティトークンサービスの URL が必要です。オンラインおよびオンプレミスの Microsoft Dynamics 365 for Sales に適用されます。 - OAuth 2.0 クライアント証明書付与。Web API URL、アプリケーション ID、テナント ID、キーストアファイル、キーストアパスワード、キーエイリアス、およびキーパスワードが必要です。Microsoft Dynamics 365 for Sales オンラインに適用されます。 - OAuth 2.0 クライアントシークレットグラント。アプリケーション ID とクライアントシークレットが必要です。Microsoft Dynamics 365 for Sales オンラインに適用されます。
Web API URL	Microsoft Dynamics 365 for Sales エンドポイントの URL。
ユーザー名	Microsoft Dynamics 365 for Sales アカウントに接続するためのユーザー名。

プロパティ	説明
パスワード	Microsoft Dynamics 365 for Sales アカウントに接続するためのパスワード。
アプリケーション ID	Microsoft Dynamics 365 for Sales の Azure アプリケーション ID。
テナント ID	Azure Active Directory のディレクトリ ID。
キーストアファイル	キーストアの場所とファイル名。 Hosted Agent を使用する場合には適用されません。 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次の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/<certificate file>`
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。
キーエイリアス	個々のキーのエイリアス名。
キーパスワード	通信を安全に行うために必要なキーストアファイルの個々のキーのパスワード。Hosted Agent を使用する場合には適用されません。
再試行エラーコード	再試行を実行するカンマ区切りの HTTP エラーコード。
RETRY_COUNT	再試行間隔に基づいて、エンドポイントから応答を取得する再試行回数。 デフォルトは 5 です。
再試行間隔	Microsoft Dynamics 365 for Sales コネクタが応答を再試行するまでに待機する秒数。 デフォルトは 60 秒です。
クライアントシークレット	Microsoft Dynamics 365 for Sales アカウントに接続するためのクライアントシークレットキー。
サーバータイプ	アクセスする Microsoft Dynamics 365 for Sales サーバー。 次のリストからサーバータイプを選択できます。 - Microsoft Dynamics オンライン。オンラインでデプロイされた Microsoft Dynamics 365 for Sales に接続します。 - Microsoft Dynamics オンプレミス。オンプレミスでデプロイされた Microsoft Dynamics 365 for Sales に接続します。
セキュリティトークンサービス URL	Microsoft Dynamics 365 for Sales セキュリティトークンサービスの URL。 Microsoft Dynamics 365 for Sales オンプレミスにアクセスするため、OAuth 2.0 のパスワード付与に適用されます。 例: `https://sts1.<company>.com/adfs/oauth2/token`

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
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
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
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。

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 Dynamics AX V3 接続のプロパティ

Microsoft Dynamics AX 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する必要があります。

次の表に、Microsoft Dynamics AX V3 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	接続に固有の名前を入力します。
説明	オプション。接続に関連する説明を入力します。
タイプ	一覧から［Microsoft Dynamics AX V3］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。

接続プロパティ	説明
認証	Microsoft Dynamics AX 2012 にアクセスするユーザーの認証。Microsoft Dynamics AX V3 コネクタは、基本認証と NTLM 認証をサポートしています。
WSDL URI	必要な WSDL ファイルパスを入力します。 **注**: WSDL URI を見つけるには、Microsoft Dynamics AX 2012 インスタンスの **[システム管理]** > **[受信ポート]** に移動します。例えば、WSDL URI の形式は `http://<Hostname>:<Port>/<App_Pool_Name>/<Port name>/xppservice.svc` のようになります。
ユーザー名	Microsoft Dynamics AX 2012 Web ページにログインするユーザーの名前。
パスワード	NT ログインユーザーに関連付けられているパスワード。
会社名	オプション。会社名を入力します。複数の会社名をセミコロンで区切って入力することができます。例: `ceu;ceed`。
言語	オプション。Microsoft Dynamics AX 2012 に対して読み書きするデータをローカライズします。言語コードを指定します。

Microsoft Excel 接続のプロパティ

Microsoft Excel 接続をセットアップするときは、接続プロパティを設定する必要があります。

次の表に、Microsoft Excel 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	Microsoft Excel 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。
タイプ	接続タイプ。一覧から Microsoft Excel ソースを選択します。
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。
フォルダ URI	Microsoft Excel ファイルが格納されているディレクトリ。Microsoft Excel ファイルは、Secure Agent が実行されているのと同じマシン上にある必要があります。
TreatFirstRowAsHeader	ファイル内の最初の行がヘッダー行かどうかを指定します。
ファイル名	Microsoft Excel ファイルの名前。 **注**: ファイル名に、.xlsx 拡張子を追加する必要があります。

Microsoft SharePoint 接続のプロパティ

Microsoft SharePoint 接続を作成する際には、接続プロパティを設定する必要があります。

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

プロパティ	説明
接続名	Microsoft SharePoint 接続の名前を入力します。
説明	接続に関連する説明を入力します。
タイプ	Microsoft SharePoint 接続の接続タイプを選択します。
ランタイム環境	Microsoft SharePoint にアクセスする際に使用される Secure Agent が稼働しているランタイム環境。
ユーザー名	Microsoft SharePoint アカウントのユーザー名を入力します。
パスワード	Microsoft SharePoint アカウントのパスワードを入力します。
SharePoint の URL	OData プロトコルレイヤを介して公開するデータソースの URI を入力します。すべての要求は、この URI の拡張です。例: `https://infasharepoint.abcd.com/ Site/_vti_bin/Data.svc`
UTC オフセット	日時フィールドに追加するための UTC 時間のオフセットを選択します。デフォルト値は UTC です。 データフィルタで$LastRuntime 変数を使用するときは、$LastRuntime 変数をオフセットするために、タイムゾーンを使用します。
添付ファイルパス	オプション。Microsoft SharePoint との間でのファイルのダウンロードと添付の場所のフォルダパスを指定します。
バッチサイズ	Microsoft SharePoint サーバーから取得する行数を定義します。
ロギングの有効化	ロギングを有効化するチェックボックスを選択します。

Microsoft Sharepoint Online 接続のプロパティ

Microsoft Sharepoint Online 接続を作成する際には、接続プロパティを設定する必要があります。

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

プロパティ	説明
接続名	Microsoft Sharepoint Online 接続の名前を入力します。
説明	接続に関連する説明を入力します。
タイプ	Microsoft Sharepoint Online 接続の接続タイプを選択します。

プロパティ	説明
ランタイム環境	Microsoft Sharepoint Online にアクセスする際に使用される Secure Agent が稼働しているランタイム環境。
Client_Id	有効なアクセストークンを生成するために必要な Microsoft Sharepoint Online 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 Microsoft Sharepoint Online のクライアントシークレット。
Refresh_Token	Microsoft Sharepoint Online のリフレッシュトークン。
Redirect_URL	Microsoft Sharepoint Online アカウントからのリダイレクト先の URL を入力します。
URL	Microsoft Sharepoint Online アカウントへの URL を入力します。
Attachment_File_Path	Microsoft Sharepoint Online との間でのファイルのダウンロードと添付の場所のフォルダパスを指定します。
Subsite_URL	オプション。Microsoft Sharepoint Online アカウントのサブサイト URL を入力します。 サブサイト URL を入力しない場合、Microsoft Sharepoint Online コネクタはファイルを URL プロパティに指定した URL から読み取ります。

Microsoft SQL Server CDC 接続のプロパティ

SQL Server CDC 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、SQL Server CDC 接続のプロパティを示します。

プロパティ	説明
接続名	SQL Server CDC 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	SQL Server CDC 接続の説明。最大長は 4000 文字です。
タイプ	接続タイプ。SQL Server CDC の場合、タイプは SQL Server CDC である必要があります。
ランタイム環境	マッピングタスクの実行に使用する Secure Agent が含まれるランタイム環境の名前。

プロパティ	説明
リスナの場所	SQL Server 変更データのための PWX CDC リーダー要求を処理する PowerExchange リスナがあり、PowerExchange ロッガー（Linux、UNIX、Windows 用）を実行するシステムのホスト名または IP アドレス。リスナのポート番号も含めます。次の形式で値を入力します。*host_name* は、ホスト名または IP アドレスにできます。 *host_name*:*port_number* 以下に例を示します。 MSSCDC1A:1467
ユーザー名	PowerExchange リスナセキュリティが有効化されているときに、PowerExchange リスナにアクセスするために使用できるユーザー名。PowerExchange LDAP ユーザー認証を有効にした場合、ユーザー名はエンタープライズユーザー名です。詳細については、『PowerExchange リファレンスマニュアル』の「SECURITY 文」を参照してください。
パスワード	**［ユーザー名］**プロパティで指定されるユーザー名と関連付けられたパスワード。
コレクション名	SQL Server ソーステーブルの登録が含まれる登録グループの**［インスタンス］**フィールド内に指定される SQL Server インスタンス名。この値は、接続の使用時に、PWX CDC メタデータアダプタがインポートする抽出マップメタデータをフィルタするために使用されます。
CAPI 接続名	PowerExchange DBMOVER コンフィギュレーションファイル内に定義される CAPX CAPI_CONNECTION 文の名前。この文には、PWX CDC リーダーが PowerExchange ロッガー（Linux、UNIX、Windows 用）ログファイルからの変更データを抽出するために使用するパラメータが含まれます。PWX CDC リーダーにこのプロパティ値が必要であり、DBMOVER コンフィギュレーションファイル内に定義される任意のデフォルトの CAPI_CONNECTION 文を無視します。
ロッガー DBID	PowerExchange ロッガー（Linux、UNIX、Windows 用）構成ファイル pwxccl.cfg で指定されている DBID パラメータ値。 この値は、PowerExchange ロッガーで複数のパブリケーションデータベース内の記事の変更データを抽出する場合にのみ必要です。この場合は、PowerExchange dbmover.cfg 構成ファイルで MSQL CAPI_CONNECTION 文の MULTIPUB パラメータを Y に設定する必要があります。設定しない場合、抽出に失敗します。
接続リトライ期限	初期接続の試行の失敗後、PWX CDC リーダーが PowerExchange リスナへの再接続を試行する秒数。接続が再試行時間中に確立できない場合、マッピングタスクに失敗します。デフォルト値は 0 であり、接続の再試行は無効になります。
圧縮	変更データをネットワーク経由で PWX CDC リーダーに送信する前に、PowerExchange リスナがデータを圧縮するかどうかを制御します。データを圧縮するには、このプロパティを選択します。デフォルトでは、このプロパティは選択されていません。
暗号化	変更データをネットワーク経由で PWX CDC リーダーに送信する前に、PowerExchange リスナがデータを暗号化するかどうかを制御します。また、使用する暗号化の種類も指定します。次のいずれかのオプションを選択します。 - **なし**。暗号化は使用しません。 - AES 128 **ビット**。128 ビットの暗号化キーを使用します。 - AES 192 **ビット**。192 ビットの暗号化キーを使用します。 - AES 256 **ビット**。256 暗号化キーを使用します。 デフォルトは**［なし］**です。

プロパティ	説明
ページングサイズ	後続データ用に次の PWX CDC リーダー要求を待機する一時停止までに、ソースシステムが PowerExchange リスナに渡す行数またはキロバイト単位でのデータ量。この値を減らすと、セッションのパフォーマンスが向上します。パフォーマンスを最大にするには、0 を使用します。 デフォルトである最小値は 0 です。
ページング単位	**［ページングサイズ］**プロパティと一緒に使用する単位の種類。 **［行］**または**［キロバイト］**のいずれかを選択します。
マップの場所	抽出マップがあるシステムのホスト名または IP アドレス。ポート番号も含めます。 この値は、PowerExchange リスナが、抽出マップからリモートにある PowerExchange ロッガー（Linux、UNIX、Windows 用）マシン上で実行されている場合に必要です。リスナは、変更データ抽出要求を処理するために、抽出マップへのアクセスを必要とします。 次の形式で値を入力します。*host_name* は、ホスト名または IP アドレスにできます。 *host_name*:*port_number* 以下に例を示します。 MSSCDC2B:25100 **注**: 接続をテストして抽出マップメタデータをインポートするための**［マップの場所］**の値は、**［リスナの場所］**の値よりも優先されます。
マップの場所のユーザー	**［マップの場所］**プロパティ内に指定された場所の PowerExchange リスナにアクセスできるユーザー名。
マップの場所のパスワード	**［マップの場所のユーザー］**プロパティで指定されるユーザー名と関連付けられたパスワード。
イベントテーブル	ユーザー定義イベントに基づく変更データ抽出を停止するためにイベントテーブルを作成した場合、イベントテーブルの PowerExchange 抽出マップの名前を入力します。イベントテーブルは、CDC ソースシステム上の SQL Server テーブルである必要があります。
低値をスペースに置き換える	文字データ内の NULL をスペースに置き換えるかどうかを制御します。文字データ内の NULL を置き換えるには、このプロパティを選択します。デフォルトでは、このプロパティが選択されています。
カスタムプロパティ	PowerExchange のデフォルト設定よりも優先するために指定できるカスタムプロパティ。セミコロン（;）を区切り文字として使用することで、複数のプロパティを入力できます。通常は、Informatica グローバルカスタマサポートの指示の下でのみ、カスタムプロパティを設定します。 **注**: これらのプロパティは、PowerCenter の PowerExchange Client for PowerCenter（PWXPC）Microsoft SQL Server CDC 接続の**［PWX オーバーライド］**オプションと同じです。

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 Microsoft 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。 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。 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。
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または一括取り込みにアクセス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。 一括取り込みデータベースを使用しており、Windows 認証を使用する場合は、このオプションを選択します。 **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から Microsoft SQL Server にアクセスします。 このオプションを選択するときは、ドメイン名と Microsoft Windows の資格情報を入力して Microsoft SQL Server にアクセスし、Secure Agent サービスを開始するユーザーアカウントが、Windows エージェントを使用するときに Microsoft SQL Server データベースで使用可能であることを確認します。 **注**: 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。

プロパティ	説明
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 認証 v2 の場合、Windows NT のユーザー名を指定します。 **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。
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 認証 v2 の場合、Windows NT のパスワードを指定します。 **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。 **注**: サーバーレスランタイム環境を使用する場合、SSL を使用して Microsoft SQL Server データベースとのセキュアな通信を行うように Microsoft SQL Server 接続を設定することはできません。
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。

プロパティ	説明
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機関（CA）の一覧が含まれています。 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次の証明書パスを指定します。 /home/cldagnt/SystemAgent/serverless/configurations/ssl_store/<TrustStore_filename>
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。
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。
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。

MongoDB V2 接続のプロパティ

MongoDB V2 接続を作成する際には、接続プロパティを設定する必要があります。

次の表に、MongoDB 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。 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	MongoDB 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 またはサーバーレスランタイム環境を指定できます。
ホスト	MongoDB クラスタのプライマリシャードのノード名または IP アドレス。
サービスレコードルックアップが有効	ホスト名が DNS サービスレコードルックアップに対応することを示す接続形式。 これによりコネクタは、DNS に照会して、MongoDB インスタンスを実行する使用可能なサーバーリストを作成できます。 ホスト名が DNS SRV レコードに対応している場合は、このチェックボックスをオンにします。このチェックボックスが選択されている場合、ポートは考慮されません。

プロパティ	説明
ポート	MongoDB サーバーのポート番号。デフォルトは 27017 です。
認証	MongoDB リソースにアクセスするための認証方法です。 次のいずれかの認証方法を選択します。 - ユーザー名およびパスワード。ユーザー名とパスワードの資格情報を使用して、MongoDB サーバーに接続します。 - X.509。Atlas または自己管理型 X.509 証明書を使用して、MongoDB サーバーに接続します。
ユーザー名	MongoDB サーバーにアクセスするためのユーザー名。
パスワード	MongoDB サーバーにアクセスするためのユーザー名に対応するパスワード。
SSL KeyStore ファイルパス	安全な通信を確立するために必要なキーと証明書を格納する、Secure Agent マシンにあるキーストアファイルの絶対パス。 このパラメータを指定する前に、証明書をダウンロードして Secure Agent マシンに配置してください。 X.509 認証タイプを選択した場合に適用されます。
SSL KeyStore 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。 X.509 認証タイプを選択した場合に適用されます。
データベース名	接続する MongoDB データベースの名前。
追加プロパティ	Azure CosmosDB MongoDB API、Amazon DocumentDB、およびその他の非 SSL MongoDB デプロイメントに対してデータの読み取りや書き込みを行うために設定できるオプションのプロパティ。 複数のプロパティを指定するには、キーと値のペアをアンパサンドで区切ります。 プロパティは次の形式で指定できます。 *propertyName1=<value1>&propertyName2=<value2>*

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 URI	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>`
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。

プロパティ	説明
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。
TrustStore 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のパスワード name。
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

MRI Software 接続のプロパティ

MRI Software 接続の設定時に、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、MRI Software 接続のプロパティを示します。

プロパティ	説明
接続名	接続の名前を入力します。
説明	オプション。接続の説明を入力します。
タイプ	接続タイプ。[MRISoftware] 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。
URL	MRI Software アプリケーションのエンドポイント URL。
ユーザー名	MRI Software アプリケーションのユーザー名。
パスワード	MRI Software アプリケーションのパスワード。

プロパティ	説明
クライアント ID	MRI Software アプリケーションで作成されたクライアント ID。
データベース名	MRI データベースの名前。
パートナーキー	MRI Software が提供するパートナーキー。
API Type	接続する MRI Software API のタイプ。 次のいずれかのオプションを選択します。 - 【Data Pipeline】。大量のデータを読み取るために Data Pipeline API に接続する場合に選択します。 - 【REST】。REST API に接続する場合に選択します。

MySQL CDC 接続のプロパティ

MySQL CDC 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、MySQL CDC 接続のプロパティを示します。

プロパティ	説明
接続名	MySQL CDC 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	MySQL CDC 接続の説明。最大長は 4000 文字です。
タイプ	接続タイプ。MySQL CDC の場合、タイプは MySQL CDC である必要があります。
ランタイム環境	マッピングタスクの実行に使用する Secure Agent が含まれるランタイム環境の名前。
リスナの場所	MySQL 変更データのための PWX CDC リーダー要求を処理する PowerExchange リスナがあり、PowerExchange ロッガー（Linux、UNIX、Windows 用）を実行するシステムのホスト名または IP アドレス。リスナのポート番号も含めます。次の形式で値を入力します。 *host_name* は、ホスト名または IP アドレスにできます。 *host_name*:*port_number* 以下に例を示します。 MYSCDC1A:1467
ユーザー名	PowerExchange リスナセキュリティが有効化されているときに、PowerExchange リスナにアクセスするために使用できるユーザー名。PowerExchange LDAP ユーザー認証を有効にした場合、ユーザー名はエンタープライズユーザー名です。詳細については、『PowerExchange リファレンスマニュアル』の「SECURITY 文」を参照してください。
パスワード	**【ユーザー名】**プロパティで指定されるユーザー名と関連付けられたパスワード。

プロパティ	説明
コレクション名	MySQL ソーステーブルのキャプチャ登録が含まれる登録グループの［**インスタンス**］フィールド内に指定される MySQL インスタンス名。この値は、接続の使用時に、PWX CDC メタデータアダプタがインポートする抽出マップメタデータをフィルタするために使用されます。
CAPI 接続名	PowerExchange DBMOVER コンフィギュレーションファイル内に定義される CAPX CAPI_CONNECTION 文の名前。この文には、PWX CDC リーダーが PowerExchange ロッガー（Linux、UNIX、Windows 用）ログファイルからの変更データを抽出するために使用するパラメータが含まれます。PWX CDC リーダーにこのプロパティ値が必要であり、DBMOVER コンフィギュレーションファイル内に定義される任意のデフォルトの CAPI_CONNECTION 文を無視します。
接続リトライ期限	初期接続の試行の失敗後、PWX CDC リーダーが PowerExchange リスナへの再接続を試行する秒数。接続が再試行時間中に確立できない場合、マッピングタスクに失敗します。デフォルト値は 0 であり、接続の再試行は無効になります。
圧縮	変更データをネットワーク経由で PWX CDC リーダーに送信する前に、PowerExchange リスナがデータを圧縮するかどうかを制御します。データを圧縮するには、このプロパティを選択します。デフォルトでは、このプロパティは選択されていません。
暗号化	変更データをネットワーク経由で PWX CDC リーダーに送信する前に、PowerExchange リスナがデータを暗号化するかどうかを制御します。また、使用する暗号化の種類も指定します。次のいずれかのオプションを選択します。 - **なし**。暗号化は使用しません。 - AES 128 **ビット**。128 ビットの暗号化キーを使用します。 - AES 192 **ビット**。192 ビットの暗号化キーを使用します。 - AES 256 **ビット**。256 暗号化キーを使用します。 デフォルトは［**なし**］です。
ペーシングサイズ	後続データ用に次の PWX CDC リーダー要求を待機する一時停止までに、ソースシステムが PowerExchange リスナに渡す行数またはキロバイト単位でのデータ量。この値を減らすと、セッションのパフォーマンスが向上します。パフォーマンスを最大にするには、0 を使用します。 デフォルトである最小値は 0 です。
ペーシング単位	［**ペーシングサイズ**］プロパティと一緒に使用する単位の種類。 ［**行**］または［**キロバイト**］のいずれかを選択します。
マップの場所	抽出マップが含まれるシステムのホスト名または IP アドレス。ポート番号も含めます。 この値は、PowerExchange リスナが、抽出マップからリモートにある PowerExchange ロッガー（Linux、UNIX、Windows 用）マシン上で実行されている場合に必要です。リスナは、変更データ抽出要求を処理するために、抽出マップへのアクセスを必要とします。 次の形式で値を入力します。*host_name* は、ホスト名または IP アドレスにできます。 *host_name*:*port_number* 以下に例を示します。 MYSCDC2B:25100 **注**: 接続をテストして抽出マップメタデータをインポートするための［**マップの場所**］の値は、［**リスナの場所**］の値よりも優先されます。
マップの場所のユーザー	［**マップの場所**］プロパティ内に指定された場所の PowerExchange リスナにアクセスできるユーザー名。

プロパティ	説明
マップの場所のパスワード	**[マップの場所のユーザー]** プロパティで指定されるユーザー名と関連付けられたパスワード。
イベントテーブル	ユーザー定義イベントに基づく変更データ抽出を停止するためにイベントテーブルを作成した場合、イベントテーブルの PowerExchange 抽出マップの名前を入力します。イベントテーブルは、CDC ソースシステム上の MySQL テーブルである必要があります。
低値をスペースに置き換える	文字データ内の NULL をスペースに置き換えるかどうかを制御します。文字データ内の NULL を置き換えるには、このプロパティを選択します。デフォルトでは、このプロパティが選択されています。
カスタムプロパティ	PowerExchange のデフォルト設定よりも優先するために指定できるカスタムプロパティ。セミコロン（;）を区切り文字として使用することで、複数のプロパティを入力できます。通常は、Informatica グローバルカスタマサポートの指示の下でのみ、カスタムプロパティを設定します。 **注**: これらのプロパティは、PowerCenter の PowerExchange Client for PowerCenter（PWXPC）MySQL CDC 接続の **[PWX オーバーライド]** オプションと同じです。

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。 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。 **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。

プロパティ	説明
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。 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。
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。

SSL プロパティ

MySQL データベースとの通信を安全に行うため、SSL を使用するように MySQL 接続を設定できます。

注: SSL を MySQL 接続に対して有効にできるのは、8.x MySQL JDBC ドライバおよび ODBC ドライバを使用する場合のみです。MySQL JDBC ドライバと ODBC ドライバの両方がバージョン 8.x になるようにします。

SSL を設定するには、まず、MySQL ODBC ドライバと JDBC ドライバのバージョン 8.x をダウンロードしてインストールする必要があります。バージョン 8.x の MySQL ODBC ドライバと JDBC ドライバのインストールの詳細については、ナレッジベースの記事 561573 を参照してください。

ドライバをインストールしたら、MySQL の接続プロパティで SSL を有効にし、セキュア通信に使用する TLS プロトコルを指定します。

SSL を MySQL 接続に対して有効にする場合、MySQL JDBC ドライバと ODBC ドライバの両方に対して SSL プロパティを設定する必要があります。JDBC ドライバに対して必要な SSL プロパティを設定することで、Secure Agent は MySQL から安全にメタデータにアクセスできます。また、ODBC ドライバに対して必要な SSL プロパティを設定することで、Secure Agent は、MySQL との間で安全にデータの読み書きを行うためのマッピングを実行します。

注: Hosted Agent を使用する場合、SSL は適用できません。Secure Agent またはサーバーレスランタイム環境を使用する場合は、SSL を設定できます。

次の表に、MySQL 接続の SSL プロパティを示します。

接続プロパティ	説明
SSL の使用	Secure Agent が MySQL データベースへのセキュア接続を確立するかどうかを決定します。 このオプションを選択し、データベースサーバーが SSL をサポートする場合、Secure Agent は暗号化された接続を確立します。MySQL データベースサーバーが SSL を設定できない場合、**[SSL が必要]** チェックボックスを有効にしたか無効にしたかに応じて、接続は失敗するか、Secure Agent が暗号化されていない接続を確立します。 **[SSL の使用]** チェックボックスを選択しない場合、Secure Agent は暗号化されていない接続の確立を試行します。
サーバー証明書の検証	**[SSL の使用]** とこのオプションを選択すると、クライアントは、データベースサーバーによって送信されたサーバー証明書を検証します。
SSL が必要	**[SSL の使用]** を選択した場合にのみ適用されます。 **[SSL が必要]** チェックボックスを選択していて、MySQL データベースが SSL をサポートする場合、Secure Agent は SSL 接続を確立します。 **[SSL が必要]** チェックボックスを選択していて、MySQL データベースが SSL を設定できない場合、Secure Agent は SSL 接続を確立しようとしますが失敗します。 **[SSL が必要]** チェックボックスをクリアしていて、MySQL データベースが SSL を設定できない場合、Secure Agent は暗号化されていない接続を確立します。
TLS プロトコル	**[SSL の使用]** を選択した場合にセキュア通信に使用される TLS プロトコルです。 以下のプロトコルから選択できます。 - TLSv1 - TLSv1.1 - TLSv1.2 デフォルトは TLSv1.2 です。TLSv1 および TLSv1.1 プロトコルは適用されません。

次の表に、**[SSL の使用]** を有効にした場合の、JDBC ドライババージョン 8.x の MySQL 接続のプロパティを示します。

接続プロパティ	説明
信頼証明書キーストア	トラストストアファイルのパスおよびファイル名。ファイルパスには、file とコロン（file:）のプレフィックスが必要です。 例: `file:C:\SSL\mysql_new\truststore` 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次の証明書パスを指定します。 `/home/cldagnt/SystemAgent/serverless/configurations/ssl_store/<TrustStore_filename>`
信頼証明書キー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。
クライアント証明書キーストア	キーストアファイルのパスおよびファイル名。ファイルパスには、file とコロン（file:）のプレフィックスが必要です。 例: `file:C:\SSL\mysql_new\keystore` 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次の証明書パスを指定します。 `/home/cldagnt/SystemAgent/serverless/configurations/ssl_store/<KeyStore_filename>`

接続プロパティ	説明
クライアント証明書キーストアのパスワード	キーストアファイルにアクセスするためのパスワード。

JDBC 暗号スイート	RFC 形式でコロンで区切られた暗号スイートの値。
	以下に例を示します。
	`TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256:`
	`TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256`

次の表に、**［SSL の使用］**を有効にした場合の、ODBC ドライババージョン 8.x の MySQL 接続のプロパティを示します。

接続プロパティ	説明
SSL 証明機関	CA 証明書のパスと名前。 例: `C:\SSL\mysql_new\ca.pem`
SSL 証明書	クライアント証明書のパスと名前。 例: `C:\SSL\mysql_new\client-cert.pem`
SSL キー	クライアントのプライベートキーのパスと名前。 例: `C:\SSL\mysql_new\client-key.pem`

SSL 暗号	OpenSSL 形式でコロンで区切られた暗号スイートの値。
	以下に例を示します。
	`ECDHE-ECDSA-AES128-GCM-SHA256:`
	`ECDHE-ECDSA-AES256-GCM-SHA384:`
	`ECDHE-RSA-AES128-GCM-SHA256:`

サーバーの ID の検証	サーバー CA 証明書の検証中に行われる、証明書に含まれるホスト名の検証。 このプロパティは、SSL プロパティで［サーバー証明書の検証］を有効にした場合にのみ適用されます。

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
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。
データベース	Netezza データベースの名前。

接続プロパティ	説明
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込み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
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。

接続プロパティ	説明
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。
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。

NICE Satmetrix 接続のプロパティ

NICE Satmetrix 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、NICE Satmetrix 接続プロパティを示します。

接続プロパティ	説明
接続名	NICE Satmetrix 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。
タイプ	接続タイプ。NICE Satmetrix 接続を選択します。
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。
Satmetrix URL	Secure Agent が Satmetrix API に接続するために使用する URL。 URL の形式: *http://<会社名>.satmetrix.com*
ユーザー名	Satmetrix 統合ユーザーアカウントのユーザー名。
パスワード	Satmetrix 統合ユーザーアカウントのパスワード。

OData 接続のプロパティ

OData 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。

以下の表に、OData 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	OData 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 または Hosted Agent を指定します。
ユーザー名	OData サービスに接続するユーザー名。
パスワード	ユーザー名に関連付けられているパスワード。
サービスルート URI	OData プロトコルを介して提供されるデータソースのルート URI。 **注**: サービスルート URI は、OData URI Conventions に準拠する必要があります。

プロパティ	説明
OData パラメータファイルのパス	URL に付加するファイルの絶対パス。ファイルには、改行で区切ったキーと値のペアが格納されています。このファイルは、URL に必要な追加のパラメータ値を確認するために使用できます。 **注**: ファイル内のキーと値のペアをエンコードするには、必ずパーセントエンコードを使用してください。
データのシリアル化形式	転送するデータの形式。 ATOM/XML または JSON から選択します。 デフォルトは ATOM/XML です。

OData V2 Protocol Writer 接続のプロパティ

OData V2 Protocol Writer 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、OData V2 Protocol Writer 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	OData V2 Protocol Writer 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。
認証タイプ	OData V2 サービスに接続するためのユーザー認証のタイプ。 以下の認証タイプから選択できます。 - **[基本認証]**。OData V2 アプリケーションにログインするには、ユーザー名とパスワードが必要です。 - **[API キー]**。OData V2 アプリケーションに接続するには、一意の API キーが必要です。
トークンタイプ	必要な CRUD 操作を実行するために OData V2 アプリケーションエンドポイントによって使用されるトークン。 デフォルトは［CSRF トークン］です。
サービスタイプ	接続する OData V2 アプリケーションエンドポイントのサービスタイプ。 デフォルトは［カタログサービス］です。

接続プロパティ	説明

サービスの URL	OData V2 アプリケーションによって公開される API を含んだカタログサービスの OData サービス URL。
	例えば、サービス URL を入力して、SAP カタログサービスのデータに次の形式でアクセスします。
	`http://<SAP サーバーのホスト名>:<ポート番号>/sap/opu/odata/iwfnd/CATALOGSERVICE;v=2/`
	ホスト名とポート番号が *inpha1.informatica.com:8001* で、サービスエンドポイントが *CATALOGSERVICE* の場合は、次の URL を入力します。
	`https://inpha1.informatica.com:8001/sap/opu/odata/iwfnd/CATALOGSERVICE;v=2/`

データのシリアル化形式	OData V2 カタログサービスでサポートされているデータシリアライズフォーマット。 次のいずれかの形式から選択できます。 - ATOM/XML - JSON デフォルトは［ATOM/XML］です。
ユーザ名	基本認証で必須です。 OData V2 アプリケーションに接続するためのユーザー名。
パスワード	基本認証で必須です。 OData V2 アプリケーションのユーザー名に関連付けられているパスワード。
API キー	API キー認証に必要です。 OData V2 サービスへの API 呼び出しを行う場合に、OData V2 アプリケーションクライアントが認証のために提供する一意の API キー。

OData V2 Protocol Reader 接続のプロパティ

OData V2 Protocol Reader 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、OData V2 Protocol Reader 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	OData V2 Protocol Reader 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。

接続プロパティ	説明
サービスタイプ	接続する OData V2 アプリケーションエンドポイントのサービスタイプ。 次のいずれかのサービスタイプを選択します。 - SAP S/4HANA カタログ。SAP S/4HANA カタログのサービスタイプは、特殊な OData V2 サービスを公開する SAP S/4HANA などのエンドポイントに使用して、エンドポイントにあるサービスを一覧表示します。 - デフォルト。それ以外のすべてのエンドポイントには、デフォルトのサービスタイプを使用します。

サービス URL	選択した OData V2 サービスタイプのサービス URL。
	デフォルトのサービスタイプには、サービスのルート URL を入力します。
	例えば、次の形式でサービス URL を入力します。
	`https://sandbox.api.sap.com/s4hanacloud/sap/opu/odata/sap/API_CHARTOFACCOUNTS_SRV`
	URL が有効かどうかは、URL に`$metadata` を追加することで行えます。
	サービスタイプが SAP S/4HANA カタログの場合は、SAP S/4HANA にカタログサービスの URL を入力します。
	例えば、SAP S/4HANA カタログサービスのデータにアクセスするには、サービス URL を次の形式で入力します。
	`http://<OData サーバーのホスト名>:<ポート番号>/sap/opu/odata/iwfnd/CATALOGSERVICE;v=2/`
	ホスト名とポート番号が `inpha1.informatica.com:8001` で、サービスエンドポイントが SAP S/4HANA カタログの場合は、次の URL を入力します。
	`https://inpha1.informatica.com:8001/sap/opu/odata/iwfnd/CATALOGSERVICE;v=2/`

認証タイプ	OData サービスに接続するためのユーザー認証のタイプ。 次の認証タイプから選択します。 - 基本。OData V2 アプリケーションにログインするには、ユーザー名とパスワードが必要です。 - API キー。OData V2 アプリケーションに接続するには、一意の API キーが必要です。
ユーザ名	基本認証に適用されます。 OData V2 アプリケーションに接続するためのユーザー名。
パスワード	基本認証に適用されます。 OData V2 アプリケーションのユーザー名に関連付けられているパスワード。
API キー	API キー認証に適用されます。 OData V2 アプリケーションへの接続に必要な一意の API キー。

ODBC 接続のプロパティ

ODBC 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。

以下の表に、ODBC 接続のプロパティを示します。

プロパティ	説明
ランタイム環境	システムへのアクセスに使用する Secure Agent が稼働しているランタイム環境。
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。
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。
データソース名	システム DSN。
スキーマ	ソースまたはターゲットに使用されるスキーマ。

プロパティ	説明
コードページ	接続に定義されているデータベースサーバーまたはフラットファイルのコードページ。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。 - 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 Extended UNIX Code (incl.JIS x 0212) - Japanese EUC（\ <-> Yen マッピングあり） - Japanese EUC（Packed Format） - IBM EBCDIC Japanese - IBM EBCDIC Japanese CP939 - Japanese EBCDIC Fujitsu - HITACHI KEIS Japanese - NEC ACOS JIPSE Japanese - UNISYS Japanese - MITSUBISHI MELCOM Japanese - Japanese EBCDIC-Kana Fujitsu - HITACHI KEIS-Kana Japanese - NEC ACOS JIPSE-Kana Japanese - UNISYS-Kana Japanese - MITSUBISHI MELCOM-Kana Japanese - EBCDIC Japanese - EBCDIK Japanese - PC Japanese SJIS-78 syntax (IBM-942) - PC Japanese SJIS-90 (IBM-943) - EBCDIC Japanese Katakana SBCS - EBCDIC Japanese Katakana（ユーロあり） - EBCDIC Japanese Latin-Kanji（ユーロあり） - EBCDIC Japanese Extended（DBCS IBM-1390 と DBCS IBM-1399 との組み合わせ） - EBCDIC Japanese Latin（ユーロアップデートあり） - EBCDIC Japanese Katakana SBCS（ユーロアップデートあり） - MS Taiwan Big-5 w/ HKSCS extensions - MS Windows Traditional Chinese、Big 5 のスーパーセット - Taiwan Big-5（ユーロアップデートあり） - Taiwan Big-5（ユーロアップデートなし） - PC Chinese GBK（IBM-1386） - Chinese EUC - Simplified Chinese (GB2312-80) - Hong Kong Supplementary Character Set - ISO 8859-8 Hebrew - PC Hebrew (old) - PC Hebrew（ユーロアップデートなし） - PC Hebrew（ユーロアップデートあり） - MS Windows Hebrew（旧バージョン） - MS Windows Hebrew（ユーロアップデートなし） - Lotus MBCS encoding for Windows Hebrew - EBCDIC Hebrew (updated with sheqel, control characters) - EBCDIC Hebrew（ユーロあり） - EBCDIC Hebrew (updated w/ euro and new sheqel, control characters) - Israeli Standard 960（7 ビット Hebrew エンコーディング）

プロパティ	説明
ODBC サブタイプ	特定のデータベースに接続するために選択する必要がある ODBC 接続サブタイプ。サブタイプは、マッピングの作成中に設定できる機能を定義します。 接続するデータベースに基づいて、サポートされている次のサブタイプから選択できます。 - Azure DW。Microsoft Azure SQL Data Warehouse に対する読み取りまたは書き込み時にプッシュダウンの最適化を有効にするには、Azure DW を選択します。 - DB2。DB2 に対する読み取りまたは書き込み時にプッシュダウンの最適化を有効にするには、DB2 を選択します。 - Google BigQuery。Google BigQuery に対する読み取りまたは書き込み時にプッシュダウンの最適化を有効にするには、Google BigQuery を選択します。 - PostgreSQL。PostgreSQL に対する読み取りまたは書き込み時にプッシュダウンの最適化を有効にするには、PostgreSQL を選択します。 - Redshift。Amazon Redshift に対する読み取りまたは書き込み時にプッシュダウンの最適化を有効にするには、Amazon Redshift を選択します。 - SAP IQ。SAP IQ データベースからデータを読み取るには、SAP IQ を選択します。 - Snowflake。Snowflake に対する読み取りまたは書き込み時にプッシュダウンの最適化を有効にするには、Snowflake を選択します。 - Teradata。Teradata に対する読み取りまたは書き込み時にプッシュダウンの最適化を有効にするには、Teradata を選択します。マッピングで SQL トランスフォーメーションを有効にして Teradata のストアドプロシージャを呼び出すか、Teradata データベースに対して SQL の保存済みクエリを処理することができます。 **注**: SSL 対応の ODBC Teradata 接続に接続する場合は、Teradata ODBC ドライバの設定中に、【WebSocket】の【SSL **モード**】オプションが適切な値に設定されているかどうかを確認してください。 - その他。Microsoft Access、Microsoft Excel、または Netezza に対して読み取りまたは書き込みを行う際に、プッシュダウンの最適化を有効にするには、［その他］を選択します。
Linux 用のドライバマネージャ	Linux プラットフォームで新しい ODBC 接続を作成するとき、Linux Secure Agent 用のドライバマネージャを選択できます。次のいずれかのドライバマネージャを選択します。 - Data Direct - unixODBC2.3.0 - unixODBC2.3.4 デフォルトのドライバマネージャは UnixODBC2.3.0 です。 Teradata に接続するには、Linux のドライバマネージャとして Data Direct のみを使用できます。

OpenAir 接続のプロパティ

OpenAir 接続を作成する際には、接続プロパティを設定する必要があります。

次の表に、OpenAir 接続のプロパティを示します。

プロパティ	説明
Secure Agent	OpenAir へのアクセスに使用される Secure Agent。
ユーザー名	OpenAir アカウントのユーザー名。
パスワード	OpenAir アカウントのパスワード。

プロパティ	説明
会社名	会社名を入力します。
API 名前空間	API 名前空間を入力します。
API キー	API キーを入力します。
クライアント名	クライアント名を入力します。
WSDL Url	WSDL URL を入力します。
エンドポイント URL	エンドポイントの URL を入力します。
バッチサイズ	OpenAir 書き込みバッチサイズを入力します。 デフォルトは 100 です。
バージョン	バージョン番号を入力します。
ロギングの有効化	ログを有効にする場合に選択します。

Oracle Business Intelligence Publisher V1 接続のプロパティ

Oracle Business Intelligence Publisher V1 接続を作成する際には、接続のプロパティを設定する必要があります。

次の表に、Oracle Business Intelligence Publisher V1 接続のプロパティを示します。

接続プロパティ	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。
BI Publisher の URL	アクセスする Oracle Business Intelligence Publisher アプリケーションの URL。 **注**: BI Publisher URL を検証するには、Web ブラウザに次の URL を入力します。 `<BI Publisher URL>/xmlpserver/services/ExternalReportWSSService?wsdl` この URL で WSDL ファイルが開く場合、BI Publisher URL は有効です。
認証タイプ	Oracle Business Intelligence Publisher アプリケーションに接続するためのユーザー認証のタイプ。 **基本認証**タイプを選択できます。
ユーザー名	Oracle Business Intelligence Publisher アカウントのユーザー名。
パスワード	Oracle Business Intelligence Publisher アカウントのパスワード。

接続プロパティ	説明
レポートディレクトリ	Oracle Business Intelligence Publisher アプリケーションでレポートが格納されるディレクトリパス。 次のフォルダからレポートを読み取ることができます。 - 共有フォルダ - マイフォルダ 共有フォルダからレポートを読み取るには、ディレクトリパスから Shared Folders を除外します。 例えば、レポートが Shared Folders/Samples/Sales にある場合は、次のようにレポートディレクトリを指定します。 /Samples/Sales マイフォルダからレポートを読み取るには、ディレクトリパスから My Folders を除外し、ディレクトリパスの最初のノードとして~username を含めます。 例えば、レポートが My Folders/Samples/Sales にあり、ユーザー名が weblogic の場合は、次のようにレポートディレクトリを指定します。 /~weblogic/Samples/Sales レポートディレクトリのデフォルト値は/Custom です。
出力ディレクトリ	.csv ファイルをダウンロードする Secure Agent マシン上のディレクトリパス。 **注**: このフィールドは、.csv データ形式でデータを読み取る Oracle Business Intelligence Publisher 接続を作成する場合に適用されます。

Oracle CDC V2 接続のプロパティ

Oracle CDC 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、Oracle CDC 接続のプロパティを示します。

プロパティ	説明
接続名	Oracle CDC 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	Oracle CDC 接続の説明。最大長は 4000 文字です。
タイプ	接続タイプ。Oracle CDC の場合、タイプは Oracle CDC V2 である必要があります。
ランタイム環境	マッピングタスクの実行に使用する Secure Agent が含まれるランタイム環境の名前。

プロパティ	説明
リスナの場所	Oracle 変更データのための PWX CDC リーダー要求を処理する PowerExchange リスナがあり、PowerExchange ロッガー（Linux、UNIX、Windows 用）を実行するシステムのホスト名または IP アドレス。リスナのポート番号も含めます。次の形式で値を入力します。*host_name* は、ホスト名または IP アドレスにできます。 *host_name*:*port_number* 以下に例を示します。 ORACDC1A:1467
ユーザー名	PowerExchange リスナセキュリティが有効化されているときに、PowerExchange リスナにアクセスするために使用できるユーザー名。PowerExchange LDAP ユーザー認証を有効にした場合、ユーザー名はエンタープライズユーザー名です。詳細については、『PowerExchange リファレンスマニュアル』の「SECURITY 文」を参照してください。
パスワード	**［ユーザー名］**プロパティで指定されるユーザー名と関連付けられたパスワード。
コレクション名	Oracle ソーステーブルのキャプチャ登録が含まれ、PowerExchange DBMOVER コンフィギュレーションファイル内の ORACLEID 文に含まれる登録グループの**［コレクション ID］**フィールド内に指定される Oracle インスタンス名。この値は、接続の使用時に、PWX CDC メタデータアダプタがインポートする抽出マップメタデータをフィルタするために使用されます。
CAPI 接続名	PowerExchange DBMOVER コンフィギュレーションファイル内に定義される CAPX CAPI_CONNECTION 文の名前。この文には、PWX CDC リーダーが PowerExchange ロッガー（Linux、UNIX、Windows 用）ログファイルからの変更データを抽出するために使用するパラメータが含まれます。PWX CDC リーダーにこのプロパティ値が必要であり、DBMOVER コンフィギュレーションファイル内に定義される任意のデフォルトの CAPI_CONNECTION 文を無視します。
ソーススキーマのオーバーライド	テーブル名が同じでスキーマが異なるソーステーブルセットの単一のキャプチャ登録を作成し、オーバーライドするスキーマ名を PowerExchange ロッガーグループ定義ファイル内で定義した場合、そのオーバーライドするスキーマ名を入力します。そうしないと、PowerExchange は、オーバーライドするスキーマを持つソーステーブルの変更データをログファイルから抽出できません。PowerExchange ロッガーグループ定義の詳細については、『PowerExchange CDC ガイド（Linux、UNIX、Windows 版）』を参照してください。
接続リトライ期限	初期接続の試行の失敗後、PWX CDC リーダーが PowerExchange リスナへの再接続を試行する秒数。接続が再試行時間中に確立できない場合、マッピングタスクに失敗します。デフォルト値は 0 であり、接続の再試行は無効になります。
圧縮	変更データをネットワーク経由で PWX CDC リーダーに送信する前に、PowerExchange リスナがデータを圧縮するかどうかを制御します。データを圧縮するには、このプロパティを選択します。デフォルトでは、このプロパティは選択されていません。
暗号化	変更データをネットワーク経由で PWX CDC リーダーに送信する前に、PowerExchange リスナがデータを暗号化するかどうかを制御します。また、使用する暗号化の種類も指定します。次のいずれかのオプションを選択します。 - **なし**。暗号化は使用しません。 - AES 128 **ビット**。128 ビットの暗号化キーを使用します。 - AES 192 **ビット**。192 ビットの暗号化キーを使用します。 - AES 256 **ビット**。256 暗号化キーを使用します。 デフォルトは**［なし］**です。

プロパティ	説明
ページングサイズ	後続データ用に次の PWX CDC リーダー要求を待機する一時停止までに、ソースシステムが PowerExchange リスナに渡す行数またはキロバイト単位でのデータ量。この値を減らすと、セッションのパフォーマンスが向上します。パフォーマンスを最大にするには、0 を使用します。 デフォルトである最小値は 0 です。
ページング単位	**［ページングサイズ］**プロパティと一緒に使用する単位の種類。 **［行］**または**［キロバイト］**のいずれかを選択します。
マップの場所	抽出マップが含まれるシステムのホスト名または IP アドレスを入力します。ポート番号も含めます。 この値は、PowerExchange リスナが、抽出マップからリモートにある PowerExchange ロッガー（Linux、UNIX、Windows 用）マシン上で実行されている場合に必要です。リスナは、変更データ抽出要求を処理するために、抽出マップへのアクセスを必要とします。 次の形式で値を入力します。*host_name* は、ホスト名または IP アドレスにできます。 *host_name*:*port_number* 以下に例を示します。 ORACDC2B:25100 接続をテストして抽出マップメタデータをインポートするための**［マップの場所］**の値は、**［リスナの場所］**の値よりも優先されます。
マップの場所のユーザー	**［マップの場所］**プロパティ内に指定された場所の PowerExchange リスナにアクセスできるユーザー名。
マップの場所のパスワード	**［マップの場所のユーザー］**プロパティで指定されるユーザー名と関連付けられたパスワード。
イベントテーブル	ユーザー定義イベントに基づく変更データ抽出を停止するためにイベントテーブルを作成した場合、イベントテーブルの PowerExchange 抽出マップの名前を入力します。イベントテーブルは、CDC ソースシステム上の Oracle テーブルである必要があります。
低値をスペースに置き換える	文字データ内の NULL をスペースに置き換えるかどうかを制御します。文字データ内の NULL を置き換えるには、このプロパティを選択します。デフォルトでは、このプロパティが選択されています。
カスタムプロパティ	PowerExchange のデフォルト設定よりも優先するために指定できるカスタムプロパティ。セミコロン（;）を区切り文字として使用することで、複数のプロパティを入力できます。通常は、Informatica グローバルカスタマサポートの指示の下でのみ、カスタムプロパティを設定します。 **注:** これらのプロパティは、PowerCenter の PowerExchange Client for PowerCenter（PWXPC）Oracle CDC 接続の**［PWX オーバーライド］**オプションと同じです。

Oracle 接続のプロパティ

Oracle 接続を作成する際には、接続プロパティを設定する必要があります。

次の表に、Oracle 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 Oracle 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、Hosted Agent、またはサーバーレスランタイム環境を指定します。
Oracle サブタイプ	Oracle オンプレミスまたは Oracle Autonomous Database への接続に使用できる Oracle 接続サブタイプ。 次のいずれかのオプションを選択します。 - Oracle ADB。Oracle Autonomous Database に接続します。 - Oracle オンプレミス。Oracle オンプレミスに接続します。
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 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 を次の形式で指定します。 `SID:<ORACLE_SID>`
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。
暗号化方法	Secure Agent が、Secure Agent とデータベースサーバーとの間で交換されるデータの暗号化に使用する方法。 Hosted Agent またはサーバーレスランタイム環境を使用する場合は適用されません。
暗号プロトコルバージョン	SSL 暗号化を有効化する際に使用する暗号プロトコル。 Hosted Agent またはサーバーレスランタイム環境を使用する場合は適用されません。

プロパティ	説明
サーバー証明書の検証	データベースサーバーによって送信される証明書を検証します。HostNameInCertificate パラメータを指定すると、Secure Agent では証明書内のホスト名も検証されます。
トラストストア	トラストストアファイルの場所と名前。 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次の証明書パスを指定します。 /home/cldagnt/SystemAgent/serverless/configurations/ssl_store/<TrustStore_filename>
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内容にアクセスするためのパスワード。
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 では接続に含まれるホスト名を SSL 証明書内のホスト名と照らし合わせて検証します。
キーストア	キーストアの場所およびファイル名。 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次の証明書パスを指定します。 /home/cldagnt/SystemAgent/serverless/configurations/ssl_store/<KeyStore_filename>
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個々のキーのパスワード。
接続リトライ期限	Oracle データベースへの接続が失敗した場合に Secure Agent が再接続を試行する秒数。Secure Agent がリトライ期限内にデータベースに接続できなかった場合、操作は失敗します。 すべての操作に使用されます。デフォルト値は 0 です。
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: ConnectionRetryCount=2; ConnectionRetryDelay=20 Advanced Security が有効になっている Oracle データベースに接続するには、JDBC ドライバの Oracle Advanced Security オプションを指定します。 例: EncryptionTypes=AES256; EncryptionLevel=accepted;DataIntegrityLevel=accepted; DataIntegrityTypes=SHA1
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: charset=sjis;readtimeout=180 Advanced Security が有効になっている Oracle データベースに接続するには、ODBC ドライバの Oracle Advanced Security オプションを指定します。 例: EncryptionTypes=AES256;EncryptionLevel=1; DataIntegrityLevel=1;DataIntegrityTypes=SHA1; DataIntegrityTypes=SHA1

Secure Agent 設定プロパティで、次の Oracle 固有のカスタムプロパティを設定できます。

カスタムプロパティ	説明
OdbcDataDirectNonWapi	リレーショナルマルチバイトデータを使用するレプリケーションタスク、同期タスク、マッピング、およびマッピングタスクで、Unicode データを処理するためには、プロパティ OdbcDataDirectNonWapi を追加し、このプロパティを 0 に設定します。 **注**: このプロパティを 0 に設定すると、シングルバイトデータの処理時間が増加する場合があります。 次の値を入力します。 - ［タイプ］では、【DTM】を選択します。 - ［サブタイプ］では、【INFO】を選択します。 - ［名前］には、「OdbcDataDirectNonWapi」と入力します。 - ［値］には、「0」と入力します。
oracle.use.varchar.for.number	ソースが Oracle でターゲットが Salesforce のレプリケーションタスク、同期タスク、マッピング、およびマッピングタスクで、Oracle ソースに Number データ型のフィールドが多数含まれる場合、カスタムプロパティ oracle.use.varchar.for.number を設定します。Number データ型のフィールドの値は Salesforce では正しくロードされません。次の値を入力します。 - ［タイプ］では、【Tomcat】を選択します。 - ［名前］には、「oracle.use.varchar.for.number」と入力します。 - ［値］には、「true」と入力します。

Oracle CRM Cloud V1 接続のプロパティ

次の表に、Oracle CRM Cloud V1 接続のプロパティを示します。

接続プロパティ	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。
エンドポイント URL	CRM アプリケーションサーバーの URL。
認証タイプ	Oracle CRM Cloud アプリケーションへの接続に必要なユーザー認証のタイプ。 次の認証タイプを選択できます。 - 基本認証 - JWT 認証
ユーザー名	Oracle CRM Cloud アカウントのユーザー名。
パスワード	Oracle CRM Cloud アカウントのパスワード。
JWT ID	JWT 認証タイプの ID。 認証タイプに［JWT 認証］を選択した場合、JWT ID を入力する必要があります。
REST API バージョン	CRM REST API のバージョン番号。

Oracle CRM On Demand 接続のプロパティ

Oracle CRM On Demand 接続を作成する際には、接続プロパティを設定する必要があります。

次の表に、Oracle CRM On Demand 接続のプロパティを示します。

接続プロパティ	説明
ユーザー名	Oracle CRM On Demand ユーザー名。次の形式を使用します。 `<domain>/<user_name>` 以下に例を示します。domain/jsmith@companyname.com
パスワード	Oracle CRM On Demand のパスワード。
サービス URL	Oracle CRM On Demand サービスの URL。例: `https://secure-company.crmondemand.com`

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。
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。

プロパティ	説明
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 を次の形式で指定します。 `SID:<ORACLE_SID>`
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。
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。

プロパティ	説明
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	データベース統合タスクが 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 の Transparent Data Encryption（TDE）で使用される Oracle ウォレットファイルのパスとファイル名。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。
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。

プロパティ	説明
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。 **注**: 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。 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。
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。

プロパティ	説明
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]** 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。
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。

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。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 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のみのアクセスに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。

プロパティ	説明
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クリアテキストのパスワード。
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。
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。

Oracle E-Business Suite 接続のプロパティ

Oracle E-Business Suite 接続を作成する際には、接続プロパティを設定する必要があります。

次の表に、Oracle E-Business Suite 接続のプロパティを示します。

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。
ユーザー名	Oracle E-Business Suite アカウントのユーザー名。

プロパティ	説明
パスワード	Oracle E-Business Suite アカウントのパスワード。
サービス設定名	ファイル拡張子付きの構成ファイルの名前。 例: EBSWSDLConfig.ini 構成ファイルの先頭の行には、ユーザー認証のための URL が含まれている必要があります。例: http://HostName:Port Number/webservices/SOAProvider/plsql/fnd_user_pkg/?wsdl **注**: 構成ファイルは、Oracle E-Business Suite の新しい接続を作成する前に、次の場所に設定する必要があります: <Secure Agent のインストールディレクトリ>\apps\Data_Integration_Server\ext\deploy_to_main\bin\rdtm-extra\reserved\userfiles\EBSMidStream

。

Oracle E-Business Suite インタフェース接続のプロパティ

Oracle E-Business Suite インタフェース接続を作成する際には、接続プロパティを設定する必要があります。

次の表に、Oracle E-Business Suite インタフェース接続のプロパティを示します。

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。
Oracle ホスト名	必要な Oracle ホスト名。
Oracle ポート番号	ポート番号。
Oracle サービス名	Oracle サービスの名前。
ユーザー名	Oracle E-Business Suite インタフェースアカウントのユーザー名。
パスワード	Oracle E-Business Suite インタフェースアカウントのパスワード。
アプリケーションユーザー名	Oracle E-Business Suite インタフェースアカウントのアプリケーションユーザー名。

プロパティ	説明
サービス構成ファイル名	ファイル拡張子付きの構成ファイルの名前。 例: EBSInterfaceTablesConfig.ini Oracle E-Business Suite への接続プロパティを設定し、インタフェーステーブル名を追加するために構成ファイルが必要になります。 **注:** インタフェーステーブル名は、書き込み操作でのみ使用されます。 構成ファイルは、次のディレクトリに配置する必要があります: <Secure Agent のインストールディレクトリ>\apps\Data_Integration_Server\ext\deploy_to_main\bin\rdtm-extra\reserved\userfiles\oraclEBS\。 構成ファイルは、次の形式にする必要があります: <スキーマ>, <同時プログラム名>, FALSE_TABLELIST_<顧客インタフェーステーブル 1>, <顧客インタフェーステーブル 2>....<顧客インタフェーステーブル n>。 例: AR,RACUST,CustomerInterface,FALSE_TABLELIST_RA_CUSTOMERS_INTERFACE_ALL,RA_CUSTOMER_PROFILES_INT_ALL
パラメータ構成ファイル名	ファイル拡張子付きの構成ファイルの名前。 例: EBSConcurrentProgramConfig.ini 同時プログラムを呼び出すパラメータを渡すために、構成ファイルが必要になります。 **注:** この構成ファイルは、書き込み操作でのみ使用されます。 構成ファイルは、次のディレクトリに配置する必要があります: <Secure Agent のインストールディレクトリ>\apps\Data_Integration_Server\ext\deploy_to_main\bin\rdtm-extra\reserved\userfiles\oraclEBS\。 構成ファイルは、次の形式にする必要があります: <モジュール名>_ PARAMLIST_Parameter List Start, <パラメータ 1>, <パラメータ 2>...., <パラメータ n>, Parameter List End。 例: CustomerInterface_PARAMLIST_Parameter List Start, CREATE_RECIPROCAL_CUSTOMER :=N,ORG_ID :=204,Parameter List End

。

Oracle Financials Cloud 接続のプロパティ

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

接続プロパティ	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。
認証	【Oracle Financials Cloud】を選択。

接続プロパティ	説明
ERP エンドポイント URL	Oracle Financials Cloud アプリケーションの ERP サーバーのエンドポイント URL。
認証タイプ	コネクタが Oracle Financials Cloud アプリケーションにログインする際に使用する必要がある、認証方法を選択。 **基本認証**タイプを選択できます。
ユーザー名	Oracle Financials Cloud アカウントのユーザー名。
パスワード	Oracle Financials Cloud アカウントのパスワード。
IO ディレクトリ	Secure Agent がインストールされたマシン上で、スキーマファイルやデータが保存されるディレクトリパス。 Oracle Financials Cloud 接続の作成後に、**［テスト］**ボタンをクリックする必要があります。 Secure Agent は、IO ディレクトリの下に次のディレクトリを作成します。 - Reader: Reader ディレクトリには、Output サブディレクトリがあります。Oracle Financials Cloud アプリケーションからダウンロードした CSV ファイルは、zip ファイル形式でダウンロードされて `IO Directory\Reader\Output` ディレクトリに保存されます。 **注**: CSV ファイルをダウンロードするディレクトリパスは、Outbound_Output_Directory の詳細プロパティフィールドでオーバーライドできます。 - Writer: Writer ディレクトリには、Logs サブディレクトリと Schema サブディレクトリがあります。ダウンロードした XLSM ファイルと CTL ファイルは、すべて `IO Directory\Writer\Schema` ディレクトリに配置する必要があります。 - Temp: Temp ディレクトリには、ロード前のステージングファイルを格納する WorkingDirectory サブディレクトリが含まれます。
暗号化モード	暗号化方法に基づいてデータを暗号化または復号化するために使用する方法。次のいずれかのオプションを選択します。 **なし** データは暗号化されません。 PGPUNSIGNED PGP 暗号化方法を使用してデータを暗号化する場合に、このオプションを選択します。 Oracle Financials Cloud アプリケーションで設定したものと同じ暗号化キーを使用する必要があります。 PGPSIGNED PGP 暗号化方法を使用してデータを暗号化して署名する場合に、このオプションを選択します。 **注**: このプロパティは、ターゲットにデータを書き込むためのマッピングを実行する場合に使用します。
パスフレーズ	プライベートキーを暗号化するために使用するパスフレーズ。 **注**: このプロパティは、PGPSigned の暗号化方法を使用して、ターゲットにデータを書き込むためのマッピングを実行する場合に使用します。

接続プロパティ	説明
PrivateKey パス	Secure Agent がインストールされたマシン上で、プライベートキーが保存されるファイルパス。 Oracle Financials Cloud アプリケーションでアップロードしたパブリックキーに対応するプライベートキーを指定する必要があります。 **注**: このプロパティは、PGPSigned の暗号化方法を使用して、ターゲットにデータを書き込むためのマッピングを実行する場合に使用します。
ERP パブリックキーパス	Secure Agent がインストールされたマシン上で、Fusion パブリックキーが保存されるファイルパス。 Fusion パブリックキーを取得するには、Oracle Financials Cloud にサービス要求を提示する必要があります。 **注**: このプロパティは、ターゲットにデータを書き込むためのマッピングを実行する場合に使用します。 Fusion パブリックキーの詳細については、Oracle のマニュアルを参照してください。
ERP プライベートキーエイリアス名	プライベート/パブリックキーペアを使用して Oracle Financials アプリケーションで生成した Fusion キーエイリアス名。 **注**: このプロパティは、ターゲットにデータを書き込むためのマッピングを実行する場合に使用します。
顧客パブリックキーエイリアス名	パブリックキーと一緒に Oracle Financials アプリケーションでアップロードした顧客パブリックキーエイリアス名。 **注**: このプロパティは、PGPSigned の暗号化方法を使用して、ターゲットにデータを書き込むためのマッピングを実行する場合に使用します。

Oracle Financials Cloud V1 接続のプロパティ

次の表に、Oracle Financials Cloud V1 接続のプロパティを示します。

接続プロパティ	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。
ERP エンドポイント URL	Oracle Financials アプリケーションサーバーのエンドポイント URL。 **注**: ERP エンドポイント URL を検証するには、Web ブラウザに次の URL を入力します。 `<ERP Endpoint URL>/publicFinancialCommonErpIntegration/ErpIntegrationService?WSDL` この URL で、ERP エンドポイント URL が有効であることを示す WSDL ファイルが開く必要があります。
認証タイプ	Oracle Financials Cloud アプリケーションに接続するためのユーザー認証のタイプ。 **基本認証**タイプを選択できます。
ユーザー名	Oracle Financials Cloud アカウントのユーザー名。
パスワード	Oracle Financials Cloud アカウントのパスワード。

接続プロパティ	説明
IO ディレクトリ	スキーマファイルとデータが保存されているディレクトリパス。スキーマファイルは、Secure Agent がインストールされているマシンに保存する必要があります。 Oracle Financials Cloud V1 接続の作成後に、**［テスト］**ボタンをクリックする必要があります。 Secure Agent は、IO ディレクトリの下に次のディレクトリを作成します。 - Reader: Reader ディレクトリには、Output サブディレクトリがあります。Oracle Financials Cloud アプリケーションからダウンロードした.cvs ファイルは、zip ファイル形式でダウンロードされて IO Directory\Reader\Output ディレクトリに保存されます。 **注**: CSV ファイルをダウンロードするディレクトリパスは、Outbound_Output_Directory の詳細プロパティフィールドでオーバーライドできます。 - Writer: Writer ディレクトリには、Logs サブディレクトリと Schema サブディレクトリがあります。ダウンロードした XLSM ファイルと CTL ファイルは、すべて IO Directory\Writer\Schema ディレクトリに配置する必要があります。 - Temp: Temp ディレクトリには、ロード前のステージングファイルを格納する WorkingDirectory サブディレクトリが含まれます。
暗号化モード	マッピングを実行してターゲットにデータを書き込むときに、データの暗号化または復号化に使用する暗号化のタイプ。 次のいずれかのオプションを選択します。 **なし** データは暗号化されません。 PGPUNSIGNED マッピングを実行して PGP 暗号化方法を使用してターゲットにデータを書き込むときにデータを暗号化するには、このオプションを選択します。 Oracle Financials Cloud アプリケーションで設定したものと同じ暗号化キーを使用する必要があります。 PGPSIGNED マッピングを実行して PGP 暗号化方法を使用してターゲットにデータを書き込むときにデータを暗号化して署名するには、このオプションを選択します。
パスフレーズ	プライベートキーを暗号化するために使用するパスフレーズ。 **注**: PGPSigned 暗号化方法を使用する場合は、このプロパティを使用します。
PrivateKey パス	プライベートキーのファイルパス。プライベートキーは、Secure Agent がインストールされているマシンに保存する必要があります。 Oracle Financials Cloud アプリケーションでアップロードしたパブリックキーに対応するプライベートキーを指定する必要があります。 **注**: PGPSigned 暗号化方法を使用する場合は、このプロパティを使用します。
ERP パブリックキーパス	Fusion パブリックキーのファイルパス。Fusion パブリックキーは、Secure Agent がインストールされているマシンに保存する必要があります。マッピングを実行してターゲットにデータを書き込むときに、Fusion パブリックキーのファイルパスを使用できます。 Fusion パブリックキーを取得するには、Oracle Financials Cloud にサービス要求を提示する必要があります。 Fusion パブリックキーの詳細については、Oracle のマニュアルを参照してください。

接続プロパティ	説明
ERP プライベートキーエイリアス名	プライベート/パブリックキーペアを生成するときに Oracle Financials アプリケーションで指定した Fusion キーエイリアス名。マッピングを実行してターゲットにデータを書き込むときに、Fusion キーエイリアス名を使用できます。
顧客パブリックキーエイリアス名	パブリックキーをアップロードしたときに Oracle Financials アプリケーションで指定した顧客パブリックキーエイリアス名。 **注:** PGPSigned 暗号化方法を使用する場合は、このプロパティを使用します。

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
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。

Oracle HCM Cloud 接続のプロパティ

Oracle HCM Cloud 接続を作成する際には、接続プロパティを設定する必要があります。

次の表に、Oracle HCM Cloud 接続のプロパティを示します。

接続プロパティ	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。
認証	【Oracle HCM Cloud】を選択。
WebCenter コンテンツ URL	Oracle HCM Cloud が出力 XML データをアップロードする WebCenter Content Server の URL。
HCM URL	Secure Agent が WebServer Content Server から HCM Application Server に XML データをロードした後に新しく作成されたデータを格納する、HCM Application Server の URL。 次の URL は、サンプルの HCM URL です: `https://adc-xxx-hcm.oracledemo.com/`。 **注**: Oracle HCM Cloud アプリケーションにデータを書き込むために Oracle HCM Cloud 接続を作成するときに適用されます。
認証タイプ	コネクタが Oracle HCM Cloud アプリケーションにログインする際に使用する必要がある、認証方法を選択します。 **基本認証**タイプを選択できます。
ユーザー名	Oracle HCM Cloud アカウントのユーザー名。
パスワード	Oracle HCM Cloud アカウントのパスワード。
スキーマディレクトリ	Secure Agent がインストールされたマシン上で、HCM 抽出定義の XSD、XLS、および `FlexFieldReport.xls` のファイルが保存されるディレクトリパス。 Oracle HCM Cloud 接続の作成後に、**[テスト]** ボタンをクリックする必要があります。Secure Agent は、スキーマディレクトリの下に次のディレクトリを作成します。 Reader Reader ディレクトリには XSD ファイルが格納されます。生成した XSD ファイルは、すべて Reader ディレクトリに配置する必要があります。 Writer Writer ディレクトリには XLS ファイルが格納されます。ダウンロードした XLS ファイルと `FlexFieldReport.xls` ファイルは、すべて Writer ディレクトリに配置する必要があります。 Temp Temp ディレクトリには、ロード前のステージングファイルが格納されます。

接続プロパティ	説明
暗号化モード	暗号化方法に基づいてデータを暗号化または復号化するために使用する方法。次のいずれかのオプションを選択します。 **なし** データは暗号化されません。 PGPUNSIGNED PGPUnsigned 暗号化方法を使用してデータを暗号化または復号化する場合に、このオプションを選択します。 PGPSIGNED PGPSigned 暗号化方法を使用してデータを暗号化または復号化する場合に、このオプションを選択します。 **注**: Oracle HCM Cloud ソースからデータを読み取るときに、Oracle HCM Cloud アプリケーションで使用したのと同じ **[暗号化モード]** オプションを指定する必要があります。
PrivateKey パスフレーズ	プライベートキーを暗号化するために使用するパスフレーズ。 プライベートキーパスフレーズの詳細については、Oracle のマニュアルを参照してください。
PrivateKey パス	Secure Agent がインストールされたマシン上で、プライベートキーが保存されるファイルパス。 **注**: Oracle HCM Cloud アプリケーションでアップロードしたパブリックキーに対応するプライベートキーを指定する必要があります。
Fusion PublicKey パス	Secure Agent がインストールされたマシン上で、Fusion パブリックキーが保存されるファイルパス。 **注**: Fusion パブリックキーを取得するには、Oracle HCM Cloud にサービス要求を提示する必要があります。 Fusion パブリックキーの詳細については、Oracle のマニュアルを参照してください。
抽出の送信	要求メッセージに指定したパラメータ値を使用した、HCM 抽出定義の送信。デフォルトでは無効になっています。 **[抽出の送信]** オプションを使用すると、Secure Agent は、指定した HCM 抽出定義のインスタンスを送信し、この HCM 抽出定義に対応する最新の出力データファイルを、WebCenter Content Server からダウンロードします。 HCM 抽出定義は、Oracle HCM Cloud アプリケーションディレクトリから送信することもできます。 **注**: このプロパティは、Oracle HCM Cloud アプリケーションからデータを読み取る場合に適用します。

Oracle HCM Cloud V1 接続のプロパティ

Oracle HCM Cloud V1 接続を作成する際には、接続プロパティを設定する必要があります。

次の表に、Oracle HCM Cloud V1 接続のプロパティを示します。

接続プロパティ	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。
WebCenter コンテンツ URL	Oracle HCM Cloud が出力 XML データをアップロードする WebCenter Content Server の URL。 **注**: WebCenter Content URL を検証するには、Web ブラウザに次の URL を入力します。 `<Webcenter Content URL>/idcws/GenericSoapPort?WSDL` この URL で WSDL ファイルが開く場合、WebCenter Content URL は有効です。
HCM URL	Secure Agent が WebServer Content Server から HCM Application Server に XML データをロードした後に新しく作成されたデータを格納する、HCM Application Server の URL。 次の URL は、サンプルの HCM URL です: `https://adc-xxx-hcm.oracledemo.com/`。 HCM URL を検証するには、Web ブラウザに次の URL を入力します。 `<HCM URL>/hcmProcFlowCoreController/FlowActionsService?WSDL` この URL で WSDL ファイルが開く場合、HCM URL は有効です。 **注**: Oracle HCM Cloud アプリケーションにデータを書き込むために Oracle HCM Cloud V1 接続を作成するとき、または接続プロパティで **［抽出の送信］** を選択したときに、適用されます。
認証タイプ	Oracle HCM Cloud アプリケーションに接続するためのユーザー認証のタイプ。 **基本認証**タイプを選択できます。
ユーザー名	Oracle HCM Cloud アカウントのユーザー名。
パスワード	Oracle HCM Cloud アカウントのパスワード。
スキーマディレクトリ	Secure Agent がインストールされたマシン上で、HCM 抽出定義の XSD、および XLSX が保存されるディレクトリパス。 Oracle HCM Cloud V1 接続の作成後に、**［テスト］** ボタンをクリックする必要があります。Secure Agent は、スキーマディレクトリの下に次のディレクトリを作成します。 Reader Reader ディレクトリには XSD ファイルが格納されます。生成した XSD ファイルは、すべて Reader ディレクトリに配置する必要があります。 Writer Writer ディレクトリには XLSX ファイルが格納されます。ダウンロードした XLSX ファイルは、すべて Writer ディレクトリに配置する必要があります。 Temp Temp ディレクトリには、ロード前のステージングファイルが格納されます。

接続プロパティ	説明
暗号化モード	データの暗号化または復号化に使用する暗号化タイプ。次のいずれかのオプションを選択します。 **なし** データは暗号化されません。 PGPUNSIGNED PGPUnsigned 暗号化方法を使用してデータを暗号化または復号化する場合に、このオプションを選択します。 PGPSIGNED PGPSigned 暗号化方法を使用してデータを暗号化または復号化する場合に、このオプションを選択します。 **注**: Oracle HCM Cloud V1 ソースからデータを読み取るときに、Oracle HCM Cloud アプリケーションで使用したのと同じ**［暗号化モード］**オプションを指定する必要があります。
PrivateKey パスフレーズ	プライベートキーを暗号化するために使用したパスフレーズ。 プライベートキーパスフレーズの詳細については、Oracle のマニュアルを参照してください。
PrivateKey パス	プライベートキーのファイルパスを入力します。プライベートキーは、Secure Agent がインストールされているマシンに保存する必要があります。 **注**: Oracle HCM Cloud アプリケーションでアップロードしたパブリックキーに対応するプライベートキーを指定する必要があります。
Fusion PublicKey パス	Fusion パブリックキーのファイルパス。Fusion パブリックキーは、Secure Agent がインストールされているマシンに保存する必要があります。 **注**: Fusion パブリックキーを取得するには、Oracle HCM Cloud にサービス要求を提示する必要があります。 Fusion パブリックキーの詳細については、Oracle のマニュアルを参照してください。
抽出の送信	要求メッセージに指定したパラメータ値を使用した、HCM 抽出定義の送信。デフォルトでは無効になっています。 **［抽出の送信］**オプションを使用すると、Secure Agent は、指定した HCM 抽出定義のインスタンスを送信し、この HCM 抽出定義に対応する最新の出力データファイルを、WebCenter Content Server からダウンロードします。 HCM 抽出定義は、Oracle HCM Cloud アプリケーションディレクトリから送信することもできます。 **注**: このプロパティは、Oracle HCM Cloud アプリケーションからデータを読み取る場合に適用します。

PostgreSQL CDC 接続のプロパティ

PostgreSQL CDC 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、PostgreSQL CDC 接続のプロパティを示します。

プロパティ	説明
接続名	PostgreSQL CDC 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	PostgreSQL CDC 接続の説明。最大長は 4000 文字です。
タイプ	接続タイプ。PostgreSQL CDC の場合、タイプは［PostgreSQL CDC］である必要があります。
ランタイム環境	マッピングタスクの実行に使用する Secure Agent が含まれるランタイム環境の名前。
リスナの場所	PostgreSQL CDC 変更データのための PWX CDC リーダー要求を処理する PowerExchange リスナがあり、PowerExchange ロッガー（Linux、UNIX、Windows 用）を実行するシステムのホスト名または IP アドレス。リスナのポート番号も含めます。次の形式で値を入力します。*host_name* は、ホスト名または IP アドレスにできます。 *host_name*:*port_number* 以下に例を示します。 `MYSCDC1A:1467`
ユーザー名	PowerExchange リスナセキュリティが有効化されているときに、PowerExchange リスナにアクセスするために使用できるユーザー名。PowerExchange LDAP ユーザー認証を有効にした場合、ユーザー名はエンタープライズユーザー名です。詳細については、『PowerExchange リファレンスマニュアル』の「SECURITY 文」を参照してください。
パスワード	**［ユーザー名］**プロパティで指定されるユーザー名と関連付けられたパスワード。
コレクション名	PostgreSQL ソーステーブルのキャプチャ登録が含まれる登録グループの**［インスタンス］**フィールド内に指定される PostgreSQL インスタンス名。この値は、接続の使用時に、PWX CDC メタデータアダプタがインポートする抽出マップメタデータをフィルタするために使用されます。
CAPI 接続名	PowerExchange DBMOVER コンフィギュレーションファイル内に定義される CAPX CAPI_CONNECTION 文の名前。この文には、PWX CDC リーダーが PowerExchange ロッガー（Linux、UNIX、Windows 用）ログファイルからの変更データを抽出するために使用するパラメータが含まれます。PWX CDC リーダーにこのプロパティ値が必要であり、DBMOVER コンフィギュレーションファイル内に定義される任意のデフォルトの CAPI_CONNECTION 文を無視します。
接続リトライ期限	初期接続の試行の失敗後、PWX CDC リーダーが PowerExchange リスナへの再接続を試行する秒数。接続が再試行時間中に確立できない場合、マッピングタスクに失敗します。デフォルト値は 0 であり、接続の再試行は無効になります。
圧縮	変更データをネットワーク経由で PWX CDC リーダーに送信する前に、PowerExchange リスナがデータを圧縮するかどうかを制御します。データを圧縮するには、このプロパティを選択します。デフォルトでは、このプロパティは選択されていません。

プロパティ	説明
暗号化	変更データをネットワーク経由で PWX CDC リーダーに送信する前に、PowerExchange リスナがデータを暗号化するかどうかを制御します。また、使用する暗号化の種類も指定します。次のいずれかのオプションを選択します。 - **なし**。暗号化は使用しません。 - AES 128 **ビット**。128 ビットの暗号化キーを使用します。 - AES 192 **ビット**。192 ビットの暗号化キーを使用します。 - AES 256 **ビット**。256 暗号化キーを使用します。 デフォルトは **[なし]** です。
ペーシングサイズ	後続データ用に次の PWX CDC リーダー要求を待機する一時停止までに、ソースシステムが PowerExchange リスナに渡す行数またはキロバイト単位でのデータ量。この値を減らすと、セッションのパフォーマンスが向上します。パフォーマンスを最大にするには、0 を使用します。 デフォルトである最小値は 0 です。
ペーシング単位	**[ペーシングサイズ]** プロパティと一緒に使用する単位の種類。 **[行]** または **[キロバイト]** のいずれかを選択します。
マップの場所	抽出マップが含まれるシステムのホスト名または IP アドレス。ポート番号も含めます。 この値は、PowerExchange リスナが、抽出マップからリモートにある PowerExchange ロッガー（Linux、UNIX、Windows 用）マシン上で実行されている場合に必要です。リスナは、変更データ抽出要求を処理するために、抽出マップへのアクセスを必要とします。 次の形式で値を入力します。*host_name* は、ホスト名または IP アドレスにできます。 *host_name*:*port_number* 以下に例を示します。 PSQCDC2B:25100 **注**: 接続をテストして抽出マップメタデータをインポートするための **[マップの場所]** の値は、**[リスナの場所]** の値よりも優先されます。
マップの場所のユーザー	**[マップの場所]** プロパティ内に指定された場所の PowerExchange リスナにアクセスできるユーザー名。
マップの場所のパスワード	**[マップの場所のユーザー]** プロパティで指定されるユーザー名と関連付けられたパスワード。
イベントテーブル	ユーザー定義イベントに基づく変更データ抽出を停止するためにイベントテーブルを作成した場合、イベントテーブルの PowerExchange 抽出マップの名前を入力します。イベントテーブルは、CDC ソースシステム上の PostgreSQL テーブルである必要があります。
低値をスペースに置き換える	文字データ内の NULL をスペースに置き換えるかどうかを制御します。文字データ内の NULL を置き換えるには、このプロパティを選択します。デフォルトでは、このプロパティが選択されています。
カスタムプロパティ	PowerExchange のデフォルト設定よりも優先するために指定できるカスタムプロパティ。セミコロン（;）を区切り文字として使用することで、複数のプロパティを入力できます。通常は、Informatica グローバルカスタマサポートの指示の下でのみ、カスタムプロパティを設定します。 **注**: これらのプロパティは、PowerCenter の PowerExchange Client for PowerCenter（PWXPC）PostgreSQL CDC 接続の **[PWX オーバーライド]** オプションと同じです。

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。 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。 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の決定。 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。 **注:** Hosted Agent を使用する場合、SSL は適用できません。Secure Agent またはサーバーレスランタイム環境を使用する場合は、SSL を設定できます。

プロパティ	説明
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。
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。 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次の証明書パスを指定します。 /home/cldagnt/SystemAgent/serverless/configurations/ssl_store/<TrustStore_filename>
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。 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次の証明書パスを指定します。 /home/cldagnt/SystemAgent/serverless/configurations/ssl_store/<KeyStore_filename>
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。

QuickBooks V2 接続のプロパティ

QuickBooks 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、QuickBooks V2 接続のプロパティを示します。

接続プロパティ	説明
ユーザー名	QuickBooks アカウントのユーザー名。
パスワード	QuickBooks アカウントのパスワード。
接続 URL	QuickBooks アプリケーションに接続するための接続 URL。
スキーマ	スキーマの値は自動的にデフォルトに設定されます。
QBXML バージョン	QuickBooks の QBXML バージョン。デフォルトの QBXML バージョンは 6.0 です。
ロギングの有効化	タスクのセッションログを表示するには、ロギングを有効にします。

Redis 接続のプロパティ

Redis 接続を作成する場合は、接続プロパティを設定する必要があります。

次の表に、Redis 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	Redis 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 またはサーバーレスランタイム環境を指定できます。
ホスト	Redis サーバーのホスト名または IP アドレスです。
ポート	Redis サーバーのポート番号。
ユーザー	Redis サーバーにアクセスするためのユーザー名。
パスワード	Redis サーバーにアクセスするためのパスワード。

プロパティ	説明
ワーカーごとの最大クライアント数	各ワーカーノードで使用される Redis クライアント接続の最大数。
フラット階層	読み取ったデータに基づいて次のアクションを実行するには、このプロパティを有効にします。 - トップレベルの HASH キーを、ハッシュ内の 1 つのキーと値のペアを 1 行とする複数の行として読み取ります。 - トップレベルの LIST キーを、リスト内の 1 つの文字列値を 1 行とする複数の行として読み取ります。
TLS の使用	TLS を使用して、Redis サーバーとの通信を保護します。
キーストアファイルパス	プライベートキーと Redis サーバーの証明書を格納する、Secure Agent マシンにあるキーストアファイルの絶対パス。
キーストアパスフレーズ	キーストアファイルのパスフレーズ。
トラストストアファイルパス	Redis サーバーの証明書を含むトラストストアファイルの絶対パス。
トラストストアパスフレーズ	トラストストアファイルのパスフレーズ。

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における REST V2 接続のプロパティを示します。

接続プロパティ	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。 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。
認証タイプ	コネクタが Web サーバーアプリケーションにログインする際に認証が必要な場合に使用される認証メソッドを選択します。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。

接続プロパティ	説明
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。
Swagger ファイルパス	Swagger 仕様ファイルのファイル名を含む絶対パスまたはホストされた URL。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。 Swagger 仕様ファイルの絶対パスを指定する場合、Swagger 仕様ファイルは Secure Agent をホストするマシン上にある必要があります。ユーザーは、フォルダーと仕様ファイルの読み取り権限を持っている必要があります。例: `C:\swagger\sampleSwagger.json` **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 マシンのランタイム環境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名	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 マシンのランタイム環境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。

接続プロパティ	説明
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。エージェントレベルで設定されたプロキシが考慮されます。 - カスタムプロキシ。接続レベルで設定されたプロキシが考慮されます。
プロキシ設定	プロキシ設定形式: <host>:<port> 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	Secure Agent 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。

OAuth 2.0 クライアント資格情報認証

以下の表に、「OAuth 2.0 - クライアント資格情報」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
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。以下に例を示します。 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。以下に例を示します。 [{"Name":"resource","Value":"https://<serverName>"}]

接続プロパティ	説明
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。
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 仕様ファイルのファイル名を含む絶対パスまたはホストされた URL。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。 Swagger 仕様ファイルの絶対パスを指定する場合、Swagger 仕様ファイルは Secure Agent をホストするマシン上にある必要があります。ユーザーは、フォルダーと仕様ファイルの読み取り権限を持っている必要があります。例: `C:\swagger\sampleSwagger.json` **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 マシンのランタイム環境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名	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 マシンのランタイム環境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。

接続プロパティ	説明
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: エージェントレベルで設定されたプロキシが考慮されます。 - カスタムプロキシ: 接続レベルで設定されたプロキシが考慮されます。
プロキシ設定	プロキシ設定形式: <host>:<port> 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	Secure Agent 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 エンドポイントに応答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。

OAuth 2.0 認証コード認証

認証コードの認証を使用するには、アプリケーションで次の Informatica リダイレクト URL を登録する必要があります。

https://*<組織の Informatica クラウドホスティング設備>*/ma/proxy/oauthcallback

アクセストークンの有効期限が切れ、応答でエラーコード 400、401 および 403 が返された場合に、顧客のファイアウォールの外側にある Informatica リダイレクト URL からエンドポイントに接続し、新しいアクセストークンの取得を試みます。

以下の表に、「OAuth 2.0 - 認証コード」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
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。

接続プロパティ	説明
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。以下に例を示します。 `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。以下に例を示します。 `[{"Name":"resource","Value":"https://<serverName>"}]`
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。以下に例を示します。 `[{"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。
リフレッシュトークン	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 仕様ファイルのファイル名を含む絶対パスまたはホストされた URL。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。 Swagger 仕様ファイルの絶対パスを指定する場合、Swagger 仕様ファイルは Secure Agent をホストするマシン上にある必要があります。ユーザーは、フォルダーと仕様ファイルの読み取り権限を持っている必要があります。例: `C:\swagger\sampleSwagger.json` **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。

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 マシンのランタイム環境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名	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 マシンのランタイム環境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: エージェントレベルで設定されたプロキシが考慮されます。 - カスタムプロキシ: 接続レベルで設定されたプロキシが考慮されます。
プロキシ設定	プロキシ設定形式: <host>:<port> 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	Secure Agent 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 エンドポイントに応答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。

JWT ベアラートークン認証

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。

次の表では、JWT ベアラートークン認証を使用する場合の REST V2 接続のプロパティについて説明します。

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"
	}
	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。以下に例を示します。
	"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。以下に例を示します。
	"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。以下に例を示します。 [\{"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 マシンのランタイム環境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 マシンのランタイム環境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。 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。
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 仕様ファイルのファイル名を含む絶対パスまたはホストされた URL。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。 Swagger 仕様ファイルの絶対パスを指定する場合、Swagger 仕様ファイルは Secure Agent をホストするマシン上にある必要があります。ユーザーは、フォルダーと仕様ファイルの読み取り権限を持っている必要があります。例: `C:\swagger\sampleSwagger.json` **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。

接続プロパティ	説明
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: エージェントレベルで設定されたプロキシが考慮されます。 - カスタムプロキシ: 接続レベルで設定されたプロキシが考慮されます。
プロキシ設定	プロキシ設定形式: <host>:<port> 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	Secure Agent 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 エンドポイントに応答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。

重要: JWT ヘッダーでの HS256 アルゴリズムのサポートをプレビューできます。評価目的でのプレビュー機能はサポートされていますが、保証対象外で本番環境には対応していません。非本番環境でのみ使用することをお勧めします。Informatica では、本番環境用に次のリリースでプレビュー機能を導入するつもりですが、市場や技術的な状況の変化に応じて導入しない場合もあります。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。機能を使用するには、組織が適切なライセンスを所有している必要があります。

REST V2 接続についてのルールおよびガイドライン

REST V2 接続についてのルールとガイドラインは次のとおりです。

- 接続をテストすると、Secure Agent が次のパラメータを検証します。

  - ローカルの Swagger ファイルのパス、またはホストされた Swagger ファイルの URL。

  - Swagger ファイルの JSON 形式。

  ただし、接続をテストすると、Secure Agent はエンドポイント資格情報を検証しません。

- エージェントレベルまたは接続レベルでプロキシを設定できます。接続レベルでシステムプロキシおよびプロキシを定義する場合に優先されるプロキシ設定を理解するには、次の表を参照してください。

システムプロキシ	REST V2 **接続属性**			**結果**
	プロキシなし	**プラットフォームプロキシ**	**カスタムプロキシ**	
×	○	×	いいえ	プロキシを考慮しません。
×	×	○	×	プロキシを考慮しません。
×	×	×	○	カスタムプロキシを考慮します。
○	はい	×	いいえ	プロキシを考慮しません。
○	×	○	×	プラットフォームプロキシを考慮します。
○	×	×	○	カスタムプロキシを考慮します。

REST V3 接続のプロパティ

REST 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する必要があります。

接続を作成する際に、次の認証方法を指定できます。

- なし。REST エンドポイントに接続するための認証方法は必要ありません。
- 基本。REST エンドポイントに接続するには、ユーザー ID とパスワードが必要です。
- OAuth 2.0 認証コード。REST エンドポイントに接続するには認証サーバーが必要です。認証コードを使用すると、資格情報を共有または保存せずにエンドポイントへの承認済みアクセスが可能になります。
- OAuth 2.0 クライアント資格情報。REST エンドポイントに接続するには、クライアント ID とクライアントシークレットが必要です。

次の表に、認証タイプが基本の接続における REST V3 接続のプロパティを示します。

接続プロパティ	**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 またはサーバーレスランタイム環境を指定します。
認証タイプ	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。 **[基本]** を選択します。 デフォルトは［なし］です。
認証ユーザー ID	［基本］認証タイプを選択したときに 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。
認証パスワード	［基本］認証タイプを選択した場合の、ユーザー名に関連付けられたパスワード。

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。 トラストストアファイルが.jks 形式であることを確認してください。各 Secure Agent マシンのランタイム環境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。
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。 キーストアファイルが.jks 形式であることを確認してください。各 Secure Agent マシンのランタイム環境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。
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。 - 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。 - カスタム。接続レベルで設定されたプロキシが考慮されます。 - プラットフォーム。エージェントレベルで設定されたプロキシが考慮されます。 サーバーレスランタイム環境を使用する場合、プロキシは適用されません。
プロキシホスト	プロキシサーバーの IP アドレスまたはホスト名。 ［カスタム］プロキシタイプにのみ必要です。
プロキシポート	プロキシサーバーのポート番号。 ［カスタム］プロキシタイプにのみ必要です。
プロキシユーザー	プロキシサーバーのユーザー名。 ［カスタム］プロキシタイプにのみ必要です。
プロキシパスワード	プロキシサーバーのパスワード。 ［カスタム］プロキシタイプにのみ必要です。
接続タイムアウト	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（秒単位）。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 60 秒です。 **注**: REST V3 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。
再試行回数	応答で、100、300、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を試行する回数。 デフォルトは 0 です。再試行を無効にするには 0 を指定します。 408 のエラーコードの場合、サイレントでの再試行が実行されます。したがって、再試行の回数は、指定した値より多くなる可能性があります。

接続プロパティ	説明
再試行の遅延	再試行が行われるまでの待機時間（秒）。デフォルトは 0 です。
HTTP バージョン	REST エンドポイントに接続するための HTTP バージョン。 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。 - HTTP 2 - HTTP 1.1 デフォルトは HTTP 2 です。

認証コードの認証

認証コードの認証を使用するには、アプリケーションで次の Informatica リダイレクト URL を登録する必要があります。

https://*<組織の Informatica クラウドホスティング設備>*/ma/proxy/oauthcallback

アクセストークンの有効期限が切れ、応答でエラーコード 400、401 および 403 が返された場合に、顧客のファイアウォールの外側にある Informatica リダイレクト URL からエンドポイントに接続し、新しいアクセストークンの取得を試みます。

次の表に、「OAuth 2.0 - 認証コード」認証タイプ接続の REST V3 接続プロパティを示します。

接続プロパティ	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 またはサーバーレスランタイム環境を指定します。
認証タイプ	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。 **【**OAuth 2.0 **認証コード】**を選択します。 デフォルトは［なし］です。
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	アプリケーション登録プロセス中に発行されるクライアント識別子。
クライアントシークレット	アプリケーション登録プロセス中に発行されるクライアントシークレット。
スコープ	REST 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のアクセス要求のスコープ。 スペース区切りのスコープ属性を入力します。以下に例を示します。 `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。 パラメータを JSON 形式で定義します。以下に例を示します。 `[{"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。 パラメータを JSON 形式で定義します。以下に例を示します。 `[{"Name":"max_age","Value":60},{"Name":"state","Value":"test"}]`
クライアント認証	承認のためのクライアント認証の詳細。 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	指定した認証の詳細に基づいて、アクセストークンとリフレッシュトークンを生成します。
アクセストークン	認証サーバーによって付与された、特定のロールを使用してデータにアクセスするためのアクセストークン。 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 レベルでプロキシサーバーを設定する必要があります。REST V3 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。
リフレッシュトークン	アクセストークンが有効でないか期限切れになった場合でも、Secure Agent が新しいアクセストークンを取得できるようにします。 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。 リフレッシュトークンの有効期限が切れた場合は、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再生成する必要があります。
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。 トラストストアファイルが.jks 形式であることを確認してください。各 Secure Agent マシンのランタイム環境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。
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。 キーストアファイルが.jks 形式であることを確認してください。各 Secure Agent マシンのランタイム環境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。

接続プロパティ	説明
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。 - 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。 - カスタム。接続レベルで設定されたプロキシが考慮されます。 - Platform。エージェントレベルで設定されたプロキシが考慮されます。 サーバーレスランタイム環境を使用する場合、プロキシは適用されません。
プロキシホスト	プロキシサーバーの IP アドレスまたはホスト名。 [カスタム] プロキシタイプにのみ必要です。
プロキシポート	プロキシサーバのポート番号。 [カスタム] プロキシタイプにのみ必要です。
プロキシユーザー	プロキシサーバーのユーザー名。 [カスタム] プロキシタイプにのみ必要です。
プロキシパスワード	プロキシサーバーのパスワード。 [カスタム] プロキシタイプにのみ必要です。
接続タイムアウト	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（秒単位）。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 60 秒です。 **注**: REST V3 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。
再試行回数	応答で、100、300、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を試行する回数。 デフォルトは 0 です。再試行を無効にするには 0 を指定します。 408 のエラーコードの場合、サイレントでの再試行が実行されます。したがって、再試行の回数は、指定した値より多くなる可能性があります。
再試行の遅延	再試行が行われるまでの待機時間（秒）。 デフォルトは 0 です。
HTTP バージョン	REST エンドポイントに接続するための HTTP バージョン。 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。 - HTTP 2 - HTTP 1.1 デフォルトは HTTP 2 です。

クライアント資格情報の認証

次の表に、OAuth 2.0 クライアント資格情報認証タイプ接続の REST V3 接続プロパティを示します。

接続プロパティ	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 またはサーバーレスランタイム環境を指定します。
認証タイプ	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。 **[**OAuth 2.0 **クライアント資格情報]** を選択します。 デフォルトは［なし］です。
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	アプリケーション登録プロセス中に発行されるクライアント識別子。
クライアントシークレット	アプリケーション登録プロセス中に発行されるクライアントシークレット。
スコープ	REST 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のアクセス要求のスコープ。スペース区切りのスコープ属性を入力します。 以下に例を示します。 `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。パラメータを JSON 形式で定義します。 以下に例を示します。 `[{"Name":"resource","Value":"https://<serverName>"}]`
クライアント認証	承認のためのクライアント認証の詳細。 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	指定した認証の詳細に基づいて、アクセストークンを生成します。
アクセストークン	認証サーバーによって付与された、特定のロールを使用してデータにアクセスするためのアクセストークン。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 レベルでプロキシサーバーを設定する必要があります。REST V3 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。
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。 トラストストアファイルが.jks 形式であることを確認してください。各 Secure Agent マシンのランタイム環境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。

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。 キーストアファイルが.jks 形式であることを確認してください。各 Secure Agent マシンのランタイム環境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。
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。 - 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。 - カスタム。接続レベルで設定されたプロキシが考慮されます。 - Platform。エージェントレベルで設定されたプロキシが考慮されます。 サーバーレスランタイム環境を使用する場合、プロキシは適用されません。
プロキシホスト	プロキシサーバーの IP アドレスまたはホスト名。 [カスタム] プロキシタイプにのみ必要です。
プロキシポート	プロキシサーバのポート番号。 [カスタム] プロキシタイプにのみ必要です。
プロキシユーザー	プロキシサーバーのユーザー名。 [カスタム] プロキシタイプにのみ必要です。
プロキシパスワード	プロキシサーバーのパスワード。 [カスタム] プロキシタイプにのみ必要です。
接続タイムアウト	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（秒単位）。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 60 秒です。 **注:** REST V3 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。
再試行回数	応答で、100、300、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を試行する回数。 デフォルトは 0 です。再試行を無効にするには 0 を指定します。 408 のエラーコードの場合、サイレントでの再試行が実行されます。したがって、再試行の回数は、指定した値より多くなる可能性があります。
再試行の遅延	再試行が行われるまでの待機時間（秒）。 デフォルトは 0 です。
HTTP バージョン	REST エンドポイントに接続するための HTTP バージョン。 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。 - HTTP 2 - HTTP 1.1 デフォルトは HTTP 2 です。

REST V3 接続についてのルールおよびガイドライン

REST V3 接続についてのルールとガイドラインは次のとおりです。

- 接続をテストして、必須パラメータが有効かどうかを確認します。
- エージェントレベルまたは接続レベルでプロキシを設定できます。次の表を参照して、接続レベルでシステムプロキシとプロキシを定義するときに優先されるプロキシ設定を理解してください。

システムプロキシ	REST V3 **接続属性**			**結果**
	プロキシなし	**プラットフォームプロキシ**	**カスタムプロキシ**	
×	○	×	いいえ	プロキシを考慮しません。
×	×	○	×	プロキシを考慮しません。
×	×	×	○	カスタムプロキシを考慮します。
○	はい	×	いいえ	プロキシを考慮しません。
○	×	○	×	プラットフォームプロキシを考慮します。
○	×	×	○	カスタムプロキシを考慮します。

Salesforce Analytics 接続のプロパティ

Salesforce Analytics 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、Salesforce Analytics 接続のプロパティを示します。

接続プロパティ	**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。
ユーザー名	Salesforce Analytics アカウントのユーザー名
パスワード	Salesforce Analytics アカウントのパスワード。
セキュリティトークン	信頼されていないネットワークから Salesforce Analytics にログインするときに使用するトークン。
サービス URL	アクセス先の Salesforce Analytics サービスの URL。例: `https://login.salesforce.com/services/Soap/u/48.0` テストまたは開発環境で、Salesforce Analytics Sandbox テスト環境にアクセスできます。

接続プロパティ	説明
一時フォルダ名	Secure Agent が JSON ファイルと Data Archive ファイルを格納するディレクトリ。タスクが正常に実行された後、一時的な.gz ファイルは削除されます。
デフォルトの日付形式	JSON ファイルの日付列を読み取るための日付形式。

Salesforce 接続のプロパティ

Salesforce 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 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	Salesforce 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指定します。
Salesforce 接続タイプ	Salesforce 接続のタイプ。標準接続または OAuth 接続を選択できます。 **重要:** Informatica では、OAuth 認証を使用して Salesforce に安全に接続することをお勧めします。OAuth 認証を使用する場合は、OAuth 2.0 を使用してください。

注: サーバーレスランタイム環境を使用する場合、プロキシサーバーを使用して Informatica Intelligent Cloud Services に接続することはできません。

以下の表に、標準接続タイプの接続プロパティ一覧を示します。

プロパティ	説明
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 アプリケーションから生成されたセキュリティトークンです。

プロパティ	説明
サービス URL	Salesforce サービスの URL。 例: `https://login.salesforce.com/services/Soap/u/55.0` 既存の標準接続のサービス URL を編集する場合、パスワードとセキュリティトークンを再入力する必要があります。 最大長は 100 文字です。
Secure Agent に対して定義されたプロキシサーバー設定をバイパス	Secure Agent の Secure Agent Manager で定義されているプロキシサーバー設定をバイパスします。プロキシサーバー設定をバイパスするときは、Salesforce への直接接続を使用します。

以下の表に、OAuth 接続タイプのプロパティ一覧を示します。

プロパティ	説明
OAuth コンシューマキー	Salesforce から取得するコンシューマキー。有効な更新トークンを生成するために必要です。
OAuth コンシューマシークレット	Salesforce から取得するコンシューマシークレット。有効な更新トークンを生成するために必要です。
OAuth 更新トークン	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 Salesforce で生成された更新トークン。
サービスの URL	Salesforce サービスエンドポイントの URL です。 例: `https://login.salesforce.com/services/Soap/u/55.0` 既存の OAuth 接続のサービス URL を編集する場合、コンシューマキー、コンシューマシークレット、およびリフレッシュトークンを再入力する必要があります。 最大長は 100 文字です。

Secure Agent 設定プロパティで、次の Salesforce 固有のプロパティを設定できます。

プロパティ	タイプ	説明
SalesForceConnectionTimeout	DTM	Salesforce Web サービスで、タイムアウトするまでに待機を要求する秒数。

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。
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。 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。
	次に、OAuth 1.0 URL の URL の例を示します。
	`https://webservice.s7.exacttarget.com/etframework.wsdl`
	次に、OAuth 2.0 URL の URL の例を示します。
	`https://<SUBDOMAIN>.soap.marketingcloudapis.com/etframework.wsdl`
	重要: Salesforce は、2022 年 9 月 30 日までに OAuth 1.0 API を廃止する予定です。Informatica では、新規および既存のパッケージを OAuth 2.0 にアップグレードすることをお勧めします。

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**: サーバーレスランタイム環境を使用する場合、プロキシサーバーを使用して Informatica Intelligent Cloud Services に接続することはできません。 **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。

プロパティ	説明
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
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。
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。
ベース URI	Salesforce 組織の URL。 次の形式でベース URI を入力する必要があります。 `https://<salesforce_org>.salesforce.com`
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`

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
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。
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。
ベース URI	Salesforce 組織の URL。 次の形式でベース URI を入力する必要があります。 `https://<salesforce_org>.salesforce.com`
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`

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 ADSO Writer 接続のプロパティ

[SAP ADSO Writer] の接続タイプを選択し、接続プロパティを設定します。

次の表に、SAP ADSO Writer の接続プロパティを示します。

接続プロパティ	説明
ランタイム環境	SAP BW/4HANA にアクセスする際に使用する Secure Agent が稼働しているランタイム環境。

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。

接続プロパティ	説明
SAP パスワード	SAP パスワード。

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`

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 メッセージサーバーの IP アドレスまたはホスト名。
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。

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`

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。
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。

接続プロパティ	説明
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。

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`

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 メッセージサーバーの IP アドレスまたはホスト名。
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）。
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。

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。
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

SAP BW Reader 接続のプロパティ

SAP BW オブジェクトからデータを読み取るには、**[SAP BW コネクタ]** 接続タイプを選択し、接続プロパティを設定します。

次の表に、SAP BW 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。
説明	接続の説明。
タイプ	接続タイプ。
ランタイム環境	必須。SAP BW オブジェクトからのデータの読み取りに使用する Secure Agent が含まれるランタイム環境。
ユーザー名	必須。適切なユーザー権限が付与された SAP ユーザー名。
パスワード	必須。SAP パスワード。

プロパティ	説明
接続タイプ	必須。作成する接続のタイプ。 次のいずれかの値を選択します。 - アプリケーション。特定の SAP BW サーバーに接続する際にアプリケーション接続を作成します。 - 負荷分散。SAP 負荷分散を使用する場合は、負荷分散接続を作成します。 デフォルトは［アプリケーション］です。
ホスト名	SAP アプリケーション接続を作成する場合は必須。 接続先の SAP BW サーバーのホスト名または IP アドレス。
システム番号	SAP アプリケーション接続を作成する場合は必須。 SAP システム番号。
メッセージホスト名	SAP 負荷分散接続を作成する場合は必須。 SAP メッセージサーバーのホスト名。
R3 名/SysID	SAP 負荷分散接続を作成する場合は必須。 SAP システム名。
グループ	SAP 負荷分散接続を作成する場合は必須。 SAP アプリケーションサーバーのグループ名。
クライアント	必須。SAP クライアント番号。
言語	SAP システムで使用される言語に対応する言語コード。
トレース	このオプションは、SAP システムによる JCo 呼び出しを追跡する場合に使用します。 次のいずれかの値を指定します。 - 0. オフ - 1. フル デフォルトは 0 です。 SAP では、JCo 呼び出しについての情報をトレースファイルに保存しています。 以下のディレクトリからトレースファイルにアクセスできます。 - 設計時の情報: `<Informatica Secure Agent installation directory>\apps\Data_Integration_Server\<Latest version>\ICS\main\tomcat` - 実行時の情報: `<Informatica Secure Agent installation directory>\apps\Data_Integration_Server\<Latest version>\ICS\main\bin\rdtm`
追加パラメータ	使用する追加 JCo 接続パラメータ。 次の形式を使用します。 `<parameter name1>=<value1>, <parameter name2>=<value2>`
ポート範囲	Secure Agent が、SAP BW サーバーからストリーミングモードでデータを読み取る際に使用する必要がある HTTP ポート範囲。 最小ポート番号と最大ポート番号をハイフンでつないで入力します。最小ポート番号と最大ポート番号は、10000 - 65535 の範囲内で指定します。 デフォルトは 10000 - 65535 です。
HTTPS の使用	このオプションは、https ストリーミングを有効にする場合に選択します。
キーストアの場所	JKS キーストアファイルへの絶対パス。

プロパティ	説明
キーストアのパスワード	.JKS ファイルのパスワード。
プライベートキーのパスワード	.P12 ファイルに指定されたパスワードをエクスポートします。
SAP の追加パラメータ	Secure Agent が RFC クライアントとして 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。 必要な RFC 固有のパラメータと接続情報を指定して、データ統合と SAP 間の通信を有効化することができます。 例えば、SAP に接続するための追加の引数として次の SNC 接続パラメータを指定できます。 GROUP=interfaces ASHOST=tzxscs20.bmwgroup.net SYSNR=20 SNC_MODE=1 SNC_PARTNERNAME=p:CN=ZXS, OU=SAP system, O=BMW Group SNC_MYNAME=p:CN=CMDB_SWP-2596, OU=SNC partner system, O=BMW Group SNC_LIB=/global/informatica/104/server/bin/libsapcrypto.so X509CERT=/global/informatica/104/SAPSNCertfiles/ROOT_CA_V3.crt TRACE=2 **注**: このフィールドで設定できる SNC パラメータについては、Informatica How-To Library article を参照してください。 **注**: 接続で必須の接続パラメータを指定した場合、それらの値によって追加のパラメータ引数が上書きされます。

SAP HANA CDC 接続のプロパティ

SAP HANA CDC 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 HANA CDC 接続のプロパティを示します。

プロパティ	説明
接続名	SAP HANA CDC 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	SAP HANA CDC 接続の説明。最大長は 4000 文字です。
タイプ	接続タイプ。SAP HANA CDC の場合、タイプは【SAP HANA CDC】である必要があります。
ランタイム環境	マッピングタスクの実行に使用する Secure Agent が含まれるランタイム環境の名前。

プロパティ	説明
リスナの場所	SAP HANA 変更データのための PWX CDC リーダー要求を処理する PowerExchange リスナがあり、PowerExchange ロッガー（LUW 用）を実行するシステムのホスト名または IP アドレス。リスナのポート番号も含めます。次の形式で値を入力します。*host_name* は、ホスト名または IP アドレスにできます。 *host_name*:*port_number* 以下に例を示します。 HANADB1:1467
ユーザー名	PowerExchange リスナセキュリティが有効化されているときに、PowerExchange リスナにアクセスするために使用できるユーザー名。PowerExchange LDAP ユーザー認証を有効にした場合、ユーザー名はエンタープライズユーザー名です。詳細については、『PowerExchange リファレンスマニュアル』の「SECURITY 文」を参照してください。
パスワード	**［ユーザー名］**プロパティで指定されるユーザー名と関連付けられたパスワード。
コレクション名	SAP HANA ソーステーブルのキャプチャ登録が含まれる登録グループの**［データベース］**フィールド内に指定される SAP HANA インスタンス名。この値は、接続の使用時に、PWX CDC メタデータアダプタがインポートする抽出マップメタデータをフィルタするために使用されます。
CAPI 接続名	PowerExchange DBMOVER コンフィギュレーションファイル内に定義される CAPX CAPI_CONNECTION 文の名前。この文には、PWX CDC リーダーが PowerExchange ロッガー（Linux、UNIX、Windows 用）ログファイルからの変更データを抽出するために使用するパラメータが含まれます。PWX CDC リーダーにこのプロパティ値が必要であり、DBMOVER コンフィギュレーションファイル内に定義される任意のデフォルトの CAPI_CONNECTION 文を無視します。
接続リトライ時間	初期接続の試行の失敗後、PWX CDC リーダーが PowerExchange リスナへの再接続を試行する秒数。接続が再試行時間中に確立できない場合、マッピングタスクに失敗します。デフォルト値は 0 であり、接続の再試行は無効になります。
圧縮	変更データをネットワーク経由で PWX CDC リーダーに送信する前に、PowerExchange リスナがデータを圧縮するかどうかを制御します。データを圧縮するには、このプロパティを選択します。デフォルトでは、このプロパティは選択されていません。
暗号化	変更データをネットワーク経由で PWX CDC リーダーに送信する前に、PowerExchange リスナがデータを暗号化するかどうかを制御します。また、使用する暗号化の種類も指定します。次のいずれかのオプションを選択します。 - **なし**。暗号化は使用しません。 - AES 128 **ビット**。128 ビットの暗号化キーを使用します。 - AES 192 **ビット**。192 ビットの暗号化キーを使用します。 - AES 256 **ビット**。256 暗号化キーを使用します。 デフォルトは**［なし］**です。

プロパティ	説明
ペーシングサイズ	後続データ用に次の PWX CDC リーダー要求を待機する一時停止までに、ソースシステムが PowerExchange リスナに渡す行数またはキロバイト単位でのデータ量。この値を減らすと、セッションのパフォーマンスが向上します。パフォーマンスを最大にするには、0 を使用します。 デフォルトである最小値は 0 です。
ペーシング単位	**[ペーシングサイズ]** プロパティと一緒に使用する単位の種類。 **[行]** または **[キロバイト]** のいずれかを選択します。
マップの場所	抽出マップが含まれるシステムのホスト名または IP アドレスを入力します。ポート番号も含めます。 この値は、PowerExchange リスナが、抽出マップからリモートにある PowerExchange ロッガー（Linux、UNIX、Windows 用）マシン上で実行されている場合に必要です。リスナは、変更データ抽出要求を処理するために、抽出マップへのアクセスを必要とします。 次の形式で値を入力します。*host_name* は、ホスト名または IP アドレスにできます。 *host_name*:*port_number* 以下に例を示します。 SAPHANA2B:25100 接続をテストして抽出マップメタデータをインポートするための **[マップの場所]** の値は、**[リスナの場所]** の値よりも優先されます。
マップの場所のユーザー	**[マップの場所]** プロパティ内に指定された場所の PowerExchange リスナにアクセスできるユーザー名。
マップの場所のパスワード	**[マップの場所のユーザー]** プロパティで指定されるユーザー名と関連付けられたパスワード。
イベントテーブル	ユーザー定義イベントに基づく変更データ抽出を停止するためにイベントテーブルを作成した場合、イベントテーブルの PowerExchange 抽出マップの名前を入力します。イベントテーブルは、CDC ソースシステム上の SAP HANA テーブルである必要があります。
低値をスペースに置き換える	文字データ内の NULL をスペースに置き換えるかどうかを制御します。文字データ内の NULL を置き換えるには、このプロパティを選択します。デフォルトでは、このプロパティが選択されています。
カスタムプロパティ	PowerExchange のデフォルト設定よりも優先するために指定できるカスタムプロパティ。セミコロン（;）を区切り文字として使用することで、複数のプロパティを入力できます。通常は、Informatica グローバルカスタマサポートの指示の下でのみ、カスタムプロパティを設定します。 **注**: これらのプロパティは、PowerCenter の PowerExchange Client for PowerCenter（PWXPC）SAP HANA CDC 接続の **[PWX オーバーライド]** オプションと同じです。

SAP HANA 接続のプロパティ

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します。

以下の表に、SAP HANA 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 SAP HANA 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 またはサーバーレスランタイム環境を指定します。
ホスト	SAP HANA サーバーのホスト名。
ポート	SAP HANA サーバーのポート番号。
データベース名	SAP HANA データベースの名前。
現在のスキーマ	SAP HANA データベースのスキーマ名。 SAP HANA データベースモデリングビューを使用する場合は、[_SYS_BIC] を指定します。
コードページ	接続に定義されているデータベースサーバーのコードページ。 UTF-8 コードページを選択します。
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オプションのプロパティ。 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。 以下に例を示します。 `connectTimeout=180000`
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オプションのプロパティ。 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。 以下に例を示します。 `charset=sjis;readtimeout=180`
ユーザー名	SAP HANA アカウントのユーザー名。
パスワード	SAP HANA アカウントのパスワード。 パスワードには、英数字と次の特殊文字を含めることができます: ~ ` ! @ # $ % ^ & * ( ) _ - + = { [}] | : ; ' < , > . ? / **注**: セミコロン文字を、左波括弧または右波括弧と組み合わせて使用することはできません。

SAP HANA Database Ingestion 接続のプロパティ

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	接続のタイプ。タイプが【SAP HANA Database Ingestion】であることを確認します。
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。

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	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します。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。

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 IDoc Reader 接続のプロパティ

IDoc インタフェース経由で SAP データを読み取るには、**[iDoc Reader]** 接続タイプを選択し、接続プロパティを設定します。

次の表に、SAP IDoc Reader の接続プロパティを示します。

接続プロパティ	説明
接続先エントリ	必須。SAP ゲートウェイで登録した RFC サーバープログラム用に sapnwrfc.ini ファイルで指定した DEST エントリ。IDoc を受信するには、この宛先エントリのプログラム ID が、SAP で定義した論理システムのプログラム ID と同じである必要があります。
コードページ	必須。SAP ソースと互換性のあるコードページ。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 データの場合に選択します。 - 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。

SAP IDoc Writer 接続のプロパティ

IDoc インタフェース経由で SAP データを書き込むには、**[iDoc Writer]** 接続タイプを選択し、接続プロパティを設定します。

次の表に、SAP IDoc Writer の接続プロパティを示します。

接続プロパティ	説明
ユーザー名	必須。S_DATASET、S_TABU_DIS、S_PROGRAM、B_BTCH_JOB の各オブジェクトに対する権限を付与された SAP ユーザ名。
パスワード	必須。SAP パスワード。
接続文字列	必須。SAP アプリケーションサーバー用に sapnwrfc.ini ファイルで指定した DEST エントリ。
コードページ	必須。SAP ターゲットと互換性のあるコードページ。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 データの場合に選択します。 - 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。
言語コード	必須。SAP 言語に対応する言語コード。
クライアントコード	必須。SAP クライアント番号。

SAP IQ 接続のプロパティ

SAP IQ 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。

次の表に、SAP IQ 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	オプション。接続の識別に使用する SAP IQ 接続の説明。
タイプ	接続タイプ。 接続タイプとして［SAP IQ］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。 ランタイム環境としてリストから Secure Agent を選択します。

接続プロパティ	説明
ホスト名	SAP IQ 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	SAP IQ データベースサーバーに接続するために使用するネットワークポート番号。 デフォルトは 2638 です。
データベース	接続する SAP IQ データベース。
スキーマ	メタデータを取得するための SAP IQ サーバーのスキーマ名。
ユーザー名	SAP IQ 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	SAP IQ データベースにログインするためのパスワード。
チェックポイント	有効にした場合、SAP IQ データベースはテーブルを正常にロードしたあとでチェックポイントを発行します。無効にした場合、データベースはチェックポイントを発行しません。 デフォルトでは有効になっています。
通知間隔	SAP IQ 外部ローダが、外部ローダログにステータスメッセージを書き込む前にロードする行数。 デフォルトは 1000 です。
データファイルディレクトリ	実行時にデータファイルを格納する SAP IQ ディレクトリ。 このディレクトリは、Secure Agent マシンからアクセスできる必要があります。 ディレクトリが Windows システム上にある場合は、パスにバックスラッシュ（\）を使用します。 例えば、`D:\mydirectory\inputfile.out` のようにします。 ディレクトリが UNIX システム上にある場合は、パスにフォワードスラッシュ（/）を使用します。 例えば、`/mydirectory/inputfile.out` のようにします。
外部ローダ実行可能	外部ローダ実行可能のファイル名とファイルパス。 SAP IQ 外部ローダ接続を作成する際、デフォルトでは、外部ローダ実行可能ファイルの名前は dbisql と設定されます。 別の名前で実行可能ファイルを使用する場合は、**[外部ローダ実行可能]** フィールドを更新する必要があります。外部ローダ実行ファイルのディレクトリがシステムパスに含まれていない場合は、このフィールドにファイルのパスとファイル名を入力する必要があります。 Windows で接続を設定する場合は、dbisql -nogui と入力する必要があります。
ステージング済み	データのロード方法。 データベースにロードする前に、フラットファイルのステージング領域にデータをロードするには、**[ステージング済み]** を選択します。 デフォルトでは有効になっています。

SAP RFC/BAPI インタフェース接続のプロパティ

RFC/BAPI インタフェース経由で SAP データにアクセスするには、**[SAP RFC/BAPI インタフェース]** 接続タイプを選択し、接続プロパティを設定します。

次の表に、SAP RFC/BAPI インタフェース接続プロパティを示します。

接続プロパティ	説明
ユーザー名	必須。S_DATASET、S_TABU_DIS、S_PROGRAM、B_BTCH_JOB の各オブジェクトに対する権限を付与された SAP ユーザ名。
パスワード	必須。SAP パスワード。
接続文字列	必須。SAP アプリケーションサーバー用に sapnwrfc.ini ファイルで指定した DEST エントリ。
コードページ	SAP ターゲットと互換性のあるコードページ。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 データの場合に選択します。 - 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。
言語コード	必須。SAP 言語に対応する言語コード。
クライアントコード	必須。SAP クライアント番号。

SAP テーブル接続のプロパティ

SAP テーブルデータを処理するには、**[SAP テーブルコネクタ]** 接続タイプを選択し、接続プロパティを設定します。

次の表に、SAP テーブル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。
説明	接続の説明。
タイプ	接続タイプ。
ランタイム環境	必須。SAP テーブルにアクセスする際に使用する Secure Agent が稼働しているランタイム環境。

プロパティ	説明
ユーザー名	必須。適切なユーザー権限が付与された SAP ユーザー名。
パスワード	必須。SAP パスワード。
クライアント	必須。SAP クライアント番号。
言語	SAP 言語に対応する言語コード。
Saprfc.ini パス	必須。sapnwrfc.ini ファイルへのローカルディレクトリ。 SAP テーブルに書き込むには、次のディレクトリを使用します。 <Informatica Secure Agent installation directory>/apps/Data_Integration_Server/ext/deploy_to_main/bin/rdtm
宛先	必須。SAP アプリケーションサーバー用に sapnwrfc.ini ファイルで指定した DEST エントリ。 宛先の大文字と小文字は区別されます。 **注**: 宛先にはすべて大文字を使用してください。
ポート範囲	HTTP ポート範囲。SAP テーブル接続では、指定されたポート番号と HTTP プロトコルを使用して、SAP テーブルに接続します。接続エラーにならないように、有効な数値を指定したことを確認します。デフォルト: 10000-65535 デフォルトの範囲内の範囲、例えば、「10000-20000」のように入力します。範囲がデフォルトの範囲外の場合、接続はデフォルトの範囲を使用します。
ストリーミングのテスト	接続をテストします。選択すると、RFC と HTTP プロトコルの両方を使用して、接続をテストします。選択しない場合は、HTTP プロトコルを使用して接続をテストします。
HTTPS 接続	選択すると、HTTPS プロトコル経由で SAP に接続します。HTTPS 経由で正常に SAP に接続するため、管理者が Secure Agent と SAP システムをホストするマシンを設定したことを確認します。
キーストアの場所	JKS キーストアファイルの絶対パス。
キーストアのパスワード	.JKS ファイルに指定されている接続先パスワード。
プライベートキーのパスワード	.P12 ファイルに指定されているエクスポートパスワード。

SAP ODP Extractor 接続のプロパティ

[SAP ODP Extractor] の接続タイプを選択し、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。

接続プロパティ	説明
ランタイム環境	SAP S/4HANA または SAP ECC へのアクセスに使用する Secure Agent が稼働しているランタイム環境。

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`

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。

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`

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。
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。

接続プロパティ	説明
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`

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。
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。

接続プロパティ	説明
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。

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`

SAS 接続のプロパティ

SAS 接続を作成する場合は、接続プロパティを設定する必要があります。

次の表に、SAS 接続のプロパティを示します。

プロパティ	説明
名前	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	SAS 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 ランタイム環境を指定します。
ホスト	SPI サーバーを実行するマシンのホスト名。
ポート	SPI サーバーを実行するマシンのポート番号。
ユーザ名	SPI サーバー構成で指定されたユーザー名。
パスワード	ユーザーのパスワード。

Satmetrix 接続のプロパティ

Satmetrix 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、Satmetrix 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	Satmetrix 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。
タイプ	接続タイプ。Satmetrix 接続を選択。
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。
Satmetrix URL	Secure Agent が Satmetrix API に接続するために使用する URL。 URL の形式: *http://<会社名>.satmetrix.com*
ユーザー名	Satmetrix 統合ユーザーアカウントのユーザー名。
パスワード	Satmetrix 統合ユーザーアカウントのパスワード。

ServiceNow 接続のプロパティ

ServiceNow 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、ServiceNow 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	ServiceNow 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指定します。
ユーザー名	ServiceNow インスタンスのユーザー名。
パスワード	ServiceNow インスタンスのパスワード。
エンドポイント URL	ServiceNow エンドポイントの URL。
インスタンスタイプ	ServiceNow インスタンスのタイプ。 JSONv2 を選択します。

シーケンシャルファイル接続のプロパティ

シーケンシャルファイル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、シーケンシャルファイル接続のプロパティを示します。

プロパティ	説明
接続名	シーケンシャルファイル接続の名前。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	シーケンシャルファイル接続の説明。最大長は 4000 文字です。
タイプ	接続タイプ。シーケンシャルファイルの場合、タイプ［**シーケンシャルファイル**］である必要があります。

プロパティ	説明
ランタイム環境	マッピングタスクの実行に使用する Secure Agent が含まれるランタイム環境の名前。
リスナの場所	シーケンシャルファイルの要求を処理する PowerExchange リスナを実行するシステムのホスト名または IP アドレス。リスナのポート番号も含めます。次の形式で値を入力します。 *host_name* は、ホスト名または IP アドレスにできます。 *host_name*:*port_number* 以下に例を示します。 LSNR1:1467
ユーザー名	PowerExchange リスナセキュリティが有効化されているときに、PowerExchange リスナにアクセスするために使用できるユーザー名。詳細については、『PowerExchange リファレンスマニュアル』の「SECURITY 文」を参照してください。
パスワード	**［ユーザー名］**プロパティで指定されるユーザー名と関連付けられたパスワード。
スキーマ名	データマップのスキーマ名。
コードページ	ソースファイルからデータを抽出するために、データ統合サービスの Secure Agent が使用するコードページ。
オフロード処理	オフロード処理を使用するかどうかを制御します。オフロード処理は、バルクデータ処理をソースシステムからターゲットシステムに転送します。次のオプションがあります。 - **自動**。オフロード処理を使用するかどうかが Cloud データ統合によって決定されます。 - **事後フィルタ**。データのフィルタリングなど、バルクデータ処理をターゲットにオフロードします。 - **事前フィルタ**。処理はターゲットにオフロードされますが、データは引き続きソースシステム上でフィルタリングされます。 - **いいえ**。オフロード処理を無効化します。 デフォルトは［いいえ］です。
オフロードスレッド	Cloud データ統合がバルクデータを処理するために使用するスレッドの数。 最適なパフォーマンスを得るには、この値が、Secure Agent が実行されているマシンに搭載済み、またはこのマシンで使用可能なプロセッサ数より大きくならないようにします。 有効な値は 1〜64 です。 デフォルトは 0 です。マルチスレッド処理は無効になります。 すべての接続タイプがオフロードスレッドをサポートしているわけではありません。これらのうち、いずれかの接続の**［オフロードスレッド］**接続属性がゼロ以外の値に設定されている場合は、スレッドなしで処理が続行されます。
配列サイズ	VSAM データセットおよびシーケンシャルファイルの場合は、パーティション化されたセッションまたはマルチスレッドセッションで使用されるストレージ配列のサイズ（単位はレコード数）。 パーティション化されたセッションの場合、この配列サイズはパーティション間で共有されます。マルチスレッドセッションの場合、各スレッドでこの配列サイズが使用されます。 有効な値は 1〜5000 です。デフォルトは 25 です。 特に**［書き込みモード］**属性で**［書き込み確認オン］**が指定されている場合、パーティション化されたセッションを調整するために配列サイズを増やします。

プロパティ	説明
低値をスペースに置き換える	文字データ内の NULL をスペースに置き換えるかどうかを制御します。文字データ内の NULL を置き換えるには、このプロパティを選択します。デフォルトでは、このプロパティが選択されています。
接続リトライ期限	初期接続の試行の失敗後、PowerExchange Bulk Reader が PowerExchange リスナへの再接続を試行する秒数。接続が再試行時間中に確立できない場合、マッピングタスクに失敗します。デフォルト値は 0 であり、接続の再試行は無効になります。
カスタムプロパティ	PowerExchange のデフォルト設定よりも優先するために指定できるカスタムプロパティ。セミコロン（;）を区切り文字として使用することで、複数のプロパティを入力できます。通常は、Informatica グローバルカスタマサポートの指示の下でのみ、カスタムプロパティを設定します。**注**: これらのプロパティは、PowerCenter の PowerExchange Client for PowerCenter（PWXPC）シーケンシャルファイル接続の［PWX **オーバーライド**］オプションと同じです。
書き込みプロパティ	書き込みモード。次のオプションがあります。 - **書き込み確認オン**。PowerExchange リスナにデータを送信し、成功/失敗の応答を待ってから、以降のデータを送信します。このモードではデータをバッファしないで、PowerExchange リスナにデータを同期的に送信します。 - **書き込み確認オフ**。データをバッファして PowerExchange リスナにデータを非同期的に送信します。このモードでは、成功または失敗応答を待機しません。

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
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
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。
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。

［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。
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できます。 Hosted Agent は、詳細モードのマッピングには適用されません。 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。

プロパティ	説明
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です。ここでは、123abc.us-east-2 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 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>....`
	以下に例を示します。
	`user=jon&warehouse=mywh&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。 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。 **注**: サーバーレスランタイム環境を使用する場合、プロキシサーバーを使用して Informatica Intelligent Cloud Services に接続することはできません。 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。 **注**: 詳細モードのマッピングには適用されません。

プロパティ	説明
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です。ここでは、123abc.us-east-2 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 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>....`
	以下に例を示します。
	`user=jon&warehouse=mywh&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。
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	登録プロセス中に Snowflake から提供され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	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。

プロパティ	説明
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"}]
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"}]
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。
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。

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。 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。 **注**: サーバーレスランタイム環境を使用する場合、プロキシサーバーを使用して Informatica Intelligent Cloud Services に接続することはできません。Hosted Agent は、詳細クラスタで実行されるマッピングには適用されません。 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。

接続プロパティ	説明
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です。ここでは、123abc.us-east-2 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 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	オプション。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>....`
	以下に例を示します。
	`user=jon&warehouse=mywh&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。 **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。

SuccessFactors LMS 接続のプロパティ

SuccessFactors LMS 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。

以下の表に、SuccessFactors LMS 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	SuccessFactors LMS 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。

サービスの URL	読み取る必要があるデータを公開している OData サービスのルート URL。
	URL は次の形式で入力します。
	`https://<rooturl>/learning/odatav4/<webservicename>/v1/`
	例えば、ルート URL が `partner0370.scdemo.successfactors.com:443` で、Web サービス名が `curriculum` の場合、次のように URL を入力します。
	`https://partner0370.scdemo.successfactors.com:443/learning/odatav4/curriculum/v1/`
	Web サービス名については、*SuccessFactors Learning Web Services OData API リファレンスガイド*を参照してください。

クライアント ID	SAP SuccessFactors Learning サーバーに対して認証する Web サービスクライアントの一意の ID。
クライアントシークレット	管理者が SAP SuccessFactors Learning サーバーから OAuth トークンを取得するために生成するシークレットコード。次に、Web サービスクライアントはクライアントシークレットを使用して OAuth トークンを要求します。
ユーザー ID	SAP SuccessFactors Learning サーバーに対して認証するユーザーの一意の ID。
企業 ID	SAP SuccessFactors Learning サーバーに対して認証する企業のテナント ID。テナント ID は、クライアント ID とクライアントシークレットを生成するページで使用できます。
ユーザータイプ	Web サービスを実行するユーザーアカウントのタイプ。 次のいずれかの値を選択します。 - 管理者。管理者ユーザーアカウントで Web サービスを実行する場合は、**[管理者]** を選択します。 - ユーザー。エンドユーザーアカウントで Web サービスを実行する場合は、**[ユーザー]** を選択します。

SuccessFactors ODATA 接続のプロパティ

SuccessFactors ODATA 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。

以下の表に、SuccessFactors ODATA 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	SuccessFactors ODATA 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 または Hosted Agent を指定します。
ユーザー名	SuccessFactors ODATA アカウントにアクセスするためのユーザー名。例えば、「username@companyID」と入力します。
パスワード	SuccessFactors ODATA アカウントにアクセスするためのパスワード。 **重要**: OAuth 2.0 認証を使用している場合でも、SuccessFactors ODATA アカウントのユーザー名とパスワードを入力する必要があります。
URL	SuccessFactors サービスのルート URL。例えば、https://apisalesdemo8.successfactors.com/odata/v2 と入力します。
セキュリティタイプ	SuccessFactors サーバーとの間にセキュアな接続を確立するために使用できるセキュリティプロトコル。SSL または TLS を選択します。
トラストストアファイル名	セキュリティタイプに適用されます。 SuccessFactors サーバーの公開証明書が含まれるトラストストアファイルの名前。
TrustStore のパスワード	セキュリティタイプに適用されます。 SuccessFactors サーバーの公開証明書が含まれるトラストストアファイルのパスワード。
キーストアファイル名	セキュリティタイプに適用されます。 SuccessFactors サーバーのプライベートキーが含まれるキーストアファイルの名前。
キーストアのパスワード	セキュリティタイプに適用されます。 SuccessFactors サーバーのプライベートキーが含まれるキーストアファイルのパスワード。
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。 - HTTP 基本認証。OData API への管理者アクセス権を持ち、有効なアカウントの資格情報があることが必要です。 - OAuth 2.0。有効なトークンと、登録済みの OAuth 2.0 クライアントアプリケーションが必要です。

プロパティ	説明
API キー	OAuth 2.0 クライアントアプリケーションを登録したときに OAuth ユーティリティが返す API キーを入力します。API キーの詳細については、SuccessFactors のマニュアルを参照してください。
プライベートキー	X.509 証明書を生成したときに OAuth ユーティリティが返すプライベートキーを入力します。プライベートキーの詳細については、SuccessFactors のマニュアルを参照してください。
企業 ID	OAuth 2.0 認証を選択した場合、アカウントを SuccessFactors で作成したときに SuccessFactors が返す企業 ID を入力します。

SuccessFactors SOAP 接続のプロパティ

SuccessFactors SOAP 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、SuccessFactors SOAP 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	接続に固有の名前を入力します。
説明	接続に関連する説明を入力します。
タイプ	一覧から SuccessFactors SOAP 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、Hosted Agent、またはサーバーレスランタイム環境を指定します。
URL	SuccessFactors サービスのルート URL。例えば、https://apisalesdemo8.successfactors.com/sfapi/v1/soap?wsdl と入力します。
企業 ID	所属する企業の ID を入力します。
ユーザー名	ユーザー名を入力します。
パスワード	パスワードを入力してください。

Tableau V3 接続のプロパティ

Tableau 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する必要があります。

次の表に、Tableau V3 接続のプロパティを示します。

接続プロパティ	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。
Tableau 製品	接続する Tableau 製品の名前。 .hyper ファイルをパブリッシュするには次のいずれかの Tableau 製品を選択できます。 Tableau **デスクトップ。** Secure Agent マシンに.hyper ファイルまたは TWBX ファイルを作成します。作成したら、.hyper ファイルまたは TWBX ファイルを Tableau Desktop に手動でインポートし、これらのファイルを使用して付加または上書きの操作を実行できます。 Tableau Server。 生成した.hyper ファイルを Tableau サーバーにパブリッシュします。 Tableau Online。 生成した.hyper ファイルを Tableau Online にパブリッシュします。
接続 URL	.hyper ファイルのパブリッシュ先となる Tableau サーバーまたは Tableau Online の URL。 URL の形式は次のとおりです: `http://<Tableau サーバーまたは Tableau Online のホスト名>:<ポート>` **注**: このプロパティは、Tableau サーバーまたは Tableau Online の値として Tableau **製品**を選択した場合に適用されます。
ユーザー名	Tableau サーバーまたは Tableau Online アカウントのユーザー名。 **注**: このプロパティは、Tableau サーバーまたは Tableau Online の値として Tableau **製品**を選択した場合に適用されます。
パスワード	Tableau サーバーまたは Tableau Online アカウントのパスワード。 **注**: このプロパティは、Tableau サーバーまたは Tableau Online の値として Tableau **製品**を選択した場合に適用されます。

接続プロパティ	説明
サイト ID	.hyper ファイルのパブリッシュ先となる Tableau サーバーまたは Tableau Online 上のサイトの ID。 サイト ID を入力するには、Tableau 管理者にお問い合わせください。 **注**: このプロパティは、Tableau サーバーまたは Tableau Online の値として Tableau **製品**を選択した場合に適用されます。
スキーマファイルのパス	Secure Agent による Tableau メタデータのインポート元のサンプル.hyper ファイルへのパス。 スキーマファイルパスについて、次のいずれかのオプションを入力します。 - .hyper ファイルへの絶対パス。 - .hyper ファイルへのディレクトリパス。 - 空のディレクトリパス。 .hyper ファイルを Tableau Server または Tableau Online にパブリッシュする場合は、空のディレクトリのみ指定できます。 スキーマファイルパスを指定しない場合、**[オブジェクト]** ターゲットプロパティでターゲットオブジェクトを選択する際に、Secure Agent は Tableau Server または Tableau Online にあるプロジェクトとデータソースを表示します。Secure Agent は、ターゲット.hyper ファイルに次のデフォルトファイルパスを使用します。 <Secure Agent のインストールディレクトリ>/apps/Data_Integration_Server/<最新バージョン>/main/bin/rdtm

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	接続のタイプ。Teradata 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。 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。

接続プロパティ	説明
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（単位: 時間）。 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。
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 コンフィギュレーション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。

接続プロパティ	説明
ユーザー名	データベースへのアクセスに必要な読み込み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。

UKGPro 接続のプロパティ

UKGPro 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、UKGPro 接続のプロパティを示します。

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。
ユーザー名	UKGPro サービスアカウントのユーザー名。 次のいずれかのユーザー名を指定します。 - HR、給与、人材、福利厚生、または統合イベントのデータを読み取るには、UKGPro のサービスアカウントのユーザー名を指定します。 - 時間管理のデータを読み取るには、UKG のサポートに関連付けられた ODataService のユーザー名を指定します。
パスワード	UKGPro サービスアカウントのパスワード。 次のいずれかのパスワードを指定します。 - HR、給与、人材、福利厚生、または統合イベントのデータを読み取るには、UKGPro のサービスアカウントのパスワードを指定します。 - 時間管理のデータを読み取るには、UKG のサポートに関連付けられた ODataService のパスワードを指定します。
サービスホスト名	HR、給与、人材、福利厚生、または統合イベントのモジュールからデータを読み取るための、UKGPro の組織ドメイン。 サービスホスト名を取得するには、[UKGPro] > **[メニュー]** > **[システム構成]** > **[セキュリティ]** > [Web **サービス]** の順に移動します。 サービスホスト名を次の形式で指定します: `service$.ultipro.com`。 ここで、$は数値です。 時間管理のデータを読み取るには、UKG のサポートから提供されるクロックサーバーの URL を指定します。

プロパティ	説明
ユーザー API キー	HR、給与、人材、福利厚生、または統合イベントのモジュールからデータを読み取る際の、ユーザー API キー。 ユーザー API キーを取得するには、[UKGPro] > **[メニュー]** > **[管理]** > **[統合スタジオ]** > **[統合スタジオダッシュボード]** > **[サービスアカウント] グラフィックタイル**の順に移動します。 時間管理データを読み取るには、ユーザー API キーの値として［なし］を指定します。
顧客 API キー	HR、給与、人材、福利厚生、または統合イベントのモジュールからデータを読み取るための、顧客 API キー。 顧客 API キーを取得するには、**[ダッシュボード]** > **[サービスアカウント] グラフィックタイル** > [UKGPro] > **[メニュー]** > **[管理]** > **[統合スタジオ]** > **[統合スタジオ]** の順に移動します。
アプリケーションモジュール	接続を通じてアクセスできるオブジェクトのタイプを決定。 UKGPro からデータにアクセスするには、次のモジュールから選択できます。 **HR、給与、人材、および福利厚生** HR、給与、人材、および福利厚生のオブジェクトにアクセスします。 **統合イベント** 完了したイベントの日付や時刻などの、サブスクライブ済み統合イベントを読み取るために統合イベントオブジェクトにアクセスします。 **その他** 時間管理オブジェクトにアクセスします。

UKGPro V2 接続のプロパティ

UKGPro 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、UKGPro V2 接続のプロパティを示します。

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。
ユーザー名	UKGPro サービスアカウントのユーザー名。 次のいずれかのユーザー名を指定します。 - HR、給与、人材、福利厚生、または統合イベントのデータを読み取るには、UKGPro のサービスアカウントのユーザー名を指定します。 - 時間管理のデータを読み取るには、UKG のサポートに関連付けられた ODataService のユーザー名を指定します。

プロパティ	説明
パスワード	UKGPro サービスアカウントのパスワード。 次のいずれかのパスワードを指定します。 - HR、給与、人材、福利厚生、または統合イベントのデータを読み取るには、UKGPro のサービスアカウントのパスワードを指定します。 - 時間管理のデータを読み取るには、UKG のサポートに関連付けられた ODataService のパスワードを指定します。
サービスホスト名	HR、給与、人材、福利厚生、または統合イベントのモジュールからデータを読み取るための、UKGPro の組織ドメイン。 サービスホスト名を取得するには、[UKGPro] > **[メニュー]** > **[システム構成]** > **[セキュリティ]** > [Web **サービス]** の順に移動します。 サービスホスト名を次の形式で指定します: `service$.ultipro.com`。 ここで、$は数値です。 時間管理のデータを読み取るには、UKG のサポートから提供されるクロックサーバーの URL を指定します。
ユーザー API キー	HR、給与、人材、福利厚生、または統合イベントのモジュールからデータを読み取る際の、ユーザー API キー。 ユーザー API キーを取得するには、[UKGPro] > **[メニュー]** > **[管理]** > **[統合スタジオ]** > **[統合スタジオダッシュボード]** > **[サービスアカウント] グラフィックタイル**の順に移動します。 時間管理データを読み取るには、ユーザー API キーの値として［なし］を指定します。
顧客 API キー	HR、給与、人材、福利厚生、または統合イベントのモジュールからデータを読み取るための、顧客 API キー。 顧客 API キーを取得するには、**[ダッシュボード]** > **[サービスアカウント] グラフィックタイル** > [UKGPro] > **[メニュー]** > **[管理]** > **[統合スタジオ]** > **[統合スタジオ]** の順に移動します。
アプリケーションモジュール	接続を通じてアクセスできるオブジェクトのタイプを決定。 UKGPro からデータにアクセスするには、次のモジュールから選択できます。 **HR、給与、人材、および福利厚生** HR、給与、人材、および福利厚生のオブジェクトにアクセスします。 **統合イベント** 完了したイベントの日付や時刻などの、サブスクライブ済み統合イベントを読み取るために統合イベントオブジェクトにアクセスします。 **その他** 時間管理オブジェクトにアクセスします。

UltiPro 接続のプロパティ

UltiPro 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、UltiPro 接続のプロパティを示します。

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。
パスワード	UltiPro サービスアカウントのパスワード。次のいずれかのパスワードを指定します。 - HR、給与、人材、福利厚生、または統合イベントのデータを読み取るには、サービスアカウントのパスワードを UltiPro に指定します。 - 時間管理のデータを読み取るには、UKG のサポートに関連付けられた ODataService のパスワードを指定します。
ユーザー名	UltiPro サービスアカウントのユーザー名。次のいずれかのユーザー名を指定します。 - HR、給与、人材、福利厚生、または統合イベントのデータを読み取るには、サービスアカウントのユーザー名を UltiPro に指定します。 - 時間管理のデータを読み取るには、UKG のサポートに関連付けられた ODataService のユーザー名を指定します。
サービスホスト名	HR、給与、人材、福利厚生、または統合イベントのモジュールからデータを読み取るための、UltiPro の組織ドメイン。 サービスホスト名を取得するには、[UltiPro] > **[メニュー]** > **[システム構成]** > **[セキュリティ]** > [Web **サービス]** の順に移動します。 サービスホスト名を次の形式で指定します: `service$.ultipro.com`。 ここで、$は数値です。 時間管理のデータを読み取るには、UKG のサポートから提供されるクロックサーバーの URL を指定します。
顧客 API キー	HR、給与、人材、福利厚生、または統合イベントのモジュールからデータを読み取る際の、顧客 API キー。 顧客 API キーを取得するには、**[ダッシュボード]** > **サービスアカウントのグラフィックタイル** > [UltiPro] > **[メニュー]** > **[管理]** > **[統合スタジオ]** > **[統合スタジオ]** の順に移動します。

プロパティ	説明
ユーザー API キー	HR、給与、人材、福利厚生、または統合イベントのモジュールからデータを読み取る際の、ユーザー API キー。 ユーザー API キーを取得するには、[UltiPro] > **[メニュー]** > **[管理]** > **[統合スタジオ]** > **[統合スタジオダッシュボード]** > **サービスアカウントのグラフィックタイル**の順に移動します。 時間管理データを読み取るには、ユーザー API キーの値として［なし］を指定します。
アプリケーションモジュール	接続を通じてアクセスできるオブジェクトのタイプを決定。 Ultipro からデータにアクセスするには、次のモジュールから選択できます。 **HR、給与、人材、および福利厚生** HR、給与、人材、および福利厚生のオブジェクトにアクセスします。 **統合イベント** 完了したイベントの日付や時刻などの、サブスクライブ済み統合イベントを読み取るために統合イベントオブジェクトにアクセスします。 **その他** 時間管理オブジェクトにアクセスします。

VSAM CDC 接続のプロパティ

VSAM CDC 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、VSAM CDC 接続のプロパティを示します。

プロパティ	説明
接続名	VSAM CDC 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	VSAM CDC 接続の説明。最大長は 4000 文字です。
タイプ	接続タイプ。VSAM CDC の場合、タイプは［VSAM CDC］である必要があります。
ランタイム環境	マッピングタスクの実行に使用する Secure Agent が含まれるランタイム環境の名前。

プロパティ	説明
リスナの場所	VSAM CDC 変更データのための PWX CDC リーダー要求を処理する PowerExchange リスナがあり、PowerExchange ロッガー（Linux、UNIX、Windows 用）を実行するシステムのホスト名または IP アドレス。リスナのポート番号も含めます。次の形式で値を入力します。*host_name* は、ホスト名または IP アドレスにできます。 *host_name*:*port_number* 以下に例を示します。 CDC1A:1467
ユーザー名	PowerExchange リスナセキュリティが有効化されているときに、PowerExchange リスナにアクセスするために使用できるユーザー名。詳細については、『PowerExchange リファレンスマニュアル』の「SECURITY 文」を参照してください。
パスワード	**［ユーザー名］**プロパティで指定されるユーザー名と関連付けられたパスワード。
コレクション名	VSAM ソースデータセットのキャプチャ登録が含まれる登録グループの**［コレクション** ID］フィールド内に指定されるインスタンス名。この値は、接続の使用時に、PWX CDC メタデータアダプタがインポートする抽出マップメタデータをフィルタするために使用されます。
CAPI 接続名	PowerExchange DBMOVER コンフィギュレーションファイル内に定義される CAPX CAPI_CONNECTION 文の名前。この文には、PWX CDC リーダーが PowerExchange ロッガー（Linux、UNIX、Windows 用）ログファイルからの変更データを抽出するために使用するパラメータが含まれます。PWX CDC リーダーにこのプロパティ値が必要であり、DBMOVER コンフィギュレーションファイル内に定義される任意のデフォルトの CAPI_CONNECTION 文を無視します。
接続リトライ期限	初期接続の試行の失敗後、PWX CDC リーダーが PowerExchange リスナへの再接続を試行する秒数。接続が再試行時間中に確立できない場合、マッピングタスクに失敗します。デフォルト値は 0 であり、接続の再試行は無効になります。
圧縮	変更データをネットワーク経由で PWX CDC リーダーに送信する前に、PowerExchange リスナがデータを圧縮するかどうかを制御します。データを圧縮するには、このプロパティを選択します。デフォルトでは、このプロパティは選択されていません。
暗号化	変更データをネットワーク経由で PWX CDC リーダーに送信する前に、PowerExchange リスナがデータを暗号化するかどうかを制御します。また、使用する暗号化の種類も指定します。次のいずれかのオプションを選択します。 - **なし**。暗号化は使用しません。 - AES 128 **ビット**。128 ビットの暗号化キーを使用します。 - AES 192 **ビット**。192 ビットの暗号化キーを使用します。 - AES 256 **ビット**。256 暗号化キーを使用します。 デフォルトは**［なし］**です。
ページングサイズ	後続データ用に次の PWX CDC リーダー要求を待機する一時停止までに、ソースシステムが PowerExchange リスナに渡す行数またはキロバイト単位でのデータ量。この値を減らすと、セッションのパフォーマンスが向上します。パフォーマンスを最大にするには、0 を使用します。 デフォルトである最小値は 0 です。
ページング単位	**［ページングサイズ］**プロパティと一緒に使用する単位の種類。 **［行］**または**［キロバイト］**のいずれかを選択します。

プロパティ	説明
マップの場所	抽出マップがあるシステムのホスト名または IP アドレス。ポート番号も含めます。 この値は、PowerExchange リスナが、抽出マップからリモートにある PowerExchange ロッガー（Linux、UNIX、Windows 用）マシン上で実行されている場合に必要です。リスナは、変更データ抽出要求を処理するために、抽出マップへのアクセスを必要とします。 次の形式で値を入力します。*host_name* は、ホスト名または IP アドレスにできます。 *host_name*:*port_number* 以下に例を示します。 CDC01:25100 **注**: 接続をテストして抽出マップメタデータをインポートするための **[マップの場所]** の値は、**[リスナの場所]** の値よりも優先されます。
マップの場所のユーザー	**[マップの場所]** プロパティ内に指定された場所の PowerExchange リスナにアクセスできるユーザー名。
マップの場所のパスワード	**[マップの場所のユーザー]** プロパティで指定されるユーザー名と関連付けられたパスワード。
イベントテーブル	ユーザー定義イベントに基づく変更データ抽出を停止するためにイベントテーブルを作成した場合、イベントテーブルの PowerExchange 抽出マップの名前を入力します。VSAM イベントテーブルは、CDC ソースシステム上に存在する必要があります。
低値をスペースに置き換える	文字データ内の NULL をスペースに置き換えるかどうかを制御します。文字データ内の NULL を置き換えるには、このプロパティを選択します。デフォルトでは、このプロパティが選択されています。
カスタムプロパティ	PowerExchange のデフォルト設定よりも優先するために指定できるカスタムプロパティ。セミコロン（;）を区切り文字として使用することで、複数のプロパティを入力できます。通常は、Informatica グローバルカスタマサポートの指示の下でのみ、カスタムプロパティを設定します。 **注**: これらのプロパティは、PowerCenter の PowerExchange Client for PowerCenter（PWXPC）VSAM CDC 接続の **[PWX オーバーライド]** オプションと同じです。

VSAM 接続のプロパティ

VSAM 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、VSAM 接続のプロパティを示します。

プロパティ	説明
接続名	VSAM 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	VSAM 接続の説明。最大長は 4000 文字です。
タイプ	接続タイプ。VSAM の場合、タイプは［VSAM］である必要があります。
ランタイム環境	マッピングタスクの実行に使用する Secure Agent が含まれるランタイム環境の名前。
リスナの場所	VSAM の要求を処理する PowerExchange リスナを実行するシステムのホスト名または IP アドレス。リスナのポート番号も含めます。次の形式で値を入力します。*host_name* は、ホスト名または IP アドレスにできます。 *host_name*:*port_number* 以下に例を示します。 LSNR1:1467
ユーザー名	PowerExchange リスナセキュリティが有効化されているときに、PowerExchange リスナにアクセスするために使用できるユーザー名。詳細については、『PowerExchange リファレンスマニュアル』の「SECURITY 文」を参照してください。
パスワード	**［ユーザー名］**プロパティで指定されるユーザー名と関連付けられたパスワード。
スキーマ名	データマップのスキーマ名。
コードページ	ソースファイルからデータを抽出するために、データ統合サービスの Secure Agent が使用するコードページ。
オフロード処理	オフロード処理を使用するかどうかを制御します。オフロード処理は、バルクデータ処理をソースシステムからターゲットシステムに転送します。次のオプションがあります。 - **自動**。オフロード処理を使用するかどうかが Cloud データ統合によって決定されます。 - **事後フィルタ**。データのフィルタリングなど、バルクデータ処理をターゲットにオフロードします。 - **事前フィルタ**。処理はターゲットにオフロードされますが、データは引き続きソースシステム上でフィルタリングされます。 - **いいえ**。オフロード処理を無効化します。 デフォルトは［いいえ］です。

プロパティ	説明
オフロードスレッド	Cloud データ統合がバルクデータを処理するために使用するスレッドの数。 最適なパフォーマンスを得るには、この値が、Secure Agent が実行されているマシンに搭載済み、またはこのマシンで使用可能なプロセッサ数より大きくならないようにします。 有効な値は 1〜64 です。 デフォルトは 0 です。マルチスレッド処理は無効になります。 すべての接続タイプがオフロードスレッドをサポートしているわけではありません。これらのうち、いずれかの接続の**［オフロードスレッド］**接続属性がゼロ以外の値に設定されている場合は、スレッドなしで処理が続行されます。
配列サイズ	VSAM データセットおよびシーケンシャルファイルの場合は、パーティション化されたセッションまたはマルチスレッドセッションで使用されるストレージ配列のサイズ（単位はレコード数）。 パーティション化されたセッションの場合、この配列サイズはパーティション間で共有されます。マルチスレッドセッションの場合、各スレッドでこの配列サイズが使用されます。 有効な値は 1〜5000 です。デフォルトは 25 です。 特に**［書き込みモード］**属性で[**書き込み確認オン**]が指定されている場合、パーティション化されたセッションを調整するために配列サイズを増やします。
低値をスペースに置き換える	文字データ内の NULL をスペースに置き換えるかどうかを制御します。文字データ内の NULL を置き換えるには、このプロパティを選択します。デフォルトでは、このプロパティが選択されています。
接続リトライ期限	初期接続の試行の失敗後、PowerExchange Bulk Reader が PowerExchange リスナへの再接続を試行する秒数。接続が再試行時間中に確立できない場合、マッピングタスクに失敗します。デフォルト値は 0 であり、接続の再試行は無効になります。
カスタムプロパティ	PowerExchange のデフォルト設定よりも優先するために指定できるカスタムプロパティ。セミコロン（;）を区切り文字として使用することで、複数のプロパティを入力できます。通常は、Informatica グローバルカスタマサポートの指示の下でのみ、カスタムプロパティを設定します。 **注**: これらのプロパティは、PowerCenter の PowerExchange Client for PowerCenter（PWXPC）VSAM 接続の［PWX **オーバーライド**］オプションと同じです。
書き込みプロパティ	書き込みモード。次のオプションがあります。 - **書き込み確認オン**。PowerExchange リスナにデータを送信し、成功/失敗の応答を待ってから、以降のデータを送信します。このモードではデータをバッファしないで、PowerExchange リスナにデータを同期的に送信します。 - **書き込み確認オフ**。データをバッファして PowerExchange リスナにデータを非同期的に送信します。このモードでは、成功または失敗応答を待機しません。

Web サービスコンシューマ接続のプロパティ

Web サービスコンシューマ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。

以下の表に、Web サービスコンシューマ接続のプロパティを示します。

プロパティ	説明
接続名	接続に固有の名前を入力します。
説明	接続に関連する説明を入力します。
タイプ	リストから Web サービスコンシューマを選択します。
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。
認証	接続で使用を設定できる認証のタイプは、次のとおりです。 **ユーザー名トークン** ユーザー名トークンとパスワードを使用して、Web サービスを認証します。 **その他の認証** WSDL URL およびエンドポイント URL を使用して、Web サービスを認証します。 **NTLM 認証** NTLM V2 認証を使用して、Web サービスを認証します。
WSDL URL	Web サービスによって指定される URL。
エンドポイント URL	Web サービスのエンドポイント URL。WSDL ファイルは、この URL を位置要素の中で指定します。
ユーザー名	ユーザー名トークンまたは NTLM 認証を使用する場合に適用されます。 Web サービスに認証するためのユーザー名。
パスワード	ユーザー名トークンまたは NTLM 認証を使用する場合に適用されます。 Web サービスの認証のためのパスワード。
DOMAIN_NAME	NTLM 認証を使用する場合に適用されます。アカウントを認証するドメインの名前。
パスワードの暗号化	ユーザー名トークン認証を使用する場合に適用されます。PasswordDigest プロパティを有効にして、ナンスとタイムスタンプをパスワードに組み合わせます。マッピングタスクでは、そのパスワードに SHA ハッシュを適用して base64 エンコーディングでエンコードし、エンコードしたパスワードを SOAP ヘッダー内で使用します。
認識必須	ユーザー名トークン認証を使用する場合に適用されます。ヘッダーエントリを処理するかどうかを指定します。
HTTP ユーザー名	Web サービスにアクセスするためのユーザー名。
HTTP パスワード	Web サービスにアクセスするためのパスワード。

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
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	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
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	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。
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。

Workday V2 接続のプロパティ

Workday 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、Workday V2 接続のプロパティを示します。

接続プロパティ	説明
タイプ	Workday リソースにアクセスするための接続。Workday 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、Hosted Agent、またはサーバーレスランタイム環境を指定します。
認証	Workday モジュールにアクセスするユーザーに対する、Workday サービスによる認証。

接続プロパティ	説明
ユーザー名	Workday サービスにログインするための、Workday テナントのユーザー名。 ユーザー名、またはユーザー名とテナントを「<ユーザー名>@<テナント名>」の形式で入力できます。例: jjoe@informatica_pt1 テナント名を指定しない場合、Secure Agent は、接続プロパティに指定したテナント名の値をユーザー名に内部的に付加します。
パスワード	ユーザー名に関連付けられているパスワード。
ドメイン名	アクセスするリソースが含まれる 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 ID。例: informatica_pt1
モジュール名	アクセスする Workday サービス。例として、Human_Resources、Financial_Management、Staffing などがあります。 例えば、Web サービスのバージョン 26.1 の利用可能なモジュールを表示するには、次のリンクを参照してください。https://community.workday.com/custom/developer/API/index.html
バージョン	Workday から取得するサービスの、Web Service Description Language（WSDL）のバージョン。サービスでサポートされる操作のリストは、選択した WSDL のバージョンによって決まります。 サポートされるバージョンについては、次のリンクを参照してください。 https://community.workday.com/custom/developer/API/versions/index.html
カスタマイズ	Workday オブジェクトのフィールドを取得するための、標準またはカスタムの WSDL。 Workday カスタムオブジェクトフィールドを取得するには、［カスタマイズ］を選択します。デフォルトは標準の WSDL です。

Xactly 接続のプロパティ

Xactly 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、Xactly 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	Xactly 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。 マッピング用の Secure Agent または Hosted Agent を指定できます。
ユーザー ID	Xactly ポータルにアクセスするためのユーザー ID。
PassKey	Xactly ポータルにアクセスするためのパスワード。
Xactly アプリ名	Xactly にサインインするためのアプリケーション名。
WSDL URL	WSDL URL。
エンドポイント URL	要求を送信するエンドポイント URL。
ロギングの有効化	タスクのロギングを有効にします。 セッションログファイルに SOAP 要求と応答を記録するために選択します。

XML ソース接続のプロパティ

XML ソース接続を作成する際には、接続プロパティを設定する必要があります。

以下の表に、XML ソース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	XML ソース接続の名前。
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。
タイプ	接続タイプ。 一覧から XML ソースを選択します。
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。
サンプル XML ファイル名	XML ファイルパスを入力。
サンプル XSD スキーマ名	XSD ファイルパスを入力。

XML ターゲット接続のプロパティ

XML ターゲット接続を作成する際には、接続プロパティを設定する必要があります。

以下の表に、XML ターゲット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	接続の名前を入力します。
説明	接続の説明を入力します。
タイプ	一覧から XML ターゲットを選択します。
Secure Agent	一覧から Secure Agent を選択します。
サンプル XML/XSD スキーマ名	XSD ファイルパスまたは XML ファイルパスを入力します。
XML 作業ディレクトリ	XML 作業ディレクトリのファイルパスを入力します。
最終 XML ファイル名	ファイル名を含む、最終 XML ファイルパスを入力します。

注: XML ターゲットコネクタは、XML 作業ディレクトリ内に内部処理用のその他のファイルを作成します。これらは、最終 XML の生成後は、容量を節約するために削除できます。

Yellowbrick Data Warehouse の接続プロパティ

Yellowbrick Data Warehouse 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、Yellowbrick Data Warehouse 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。
説明	オプション。接続を識別するために使用する説明。
タイプ	接続タイプとして［Yellowbrick］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。
データベース	接続する Yellowbrick Data Warehouse の名前。
ホスト名	Yellowbrick サーバーのホスト名または IP アドレス。
パスワード	Yellowbrick Data Warehouse のパスワード。
ポート番号	Yellowbrick Data Warehouse のポート番号。
スキーマ名	スキーマの名前。［スキーマポリシーに指定］を選択した場合に必要です。

接続プロパティ	説明
スキーマポリシー	テーブルのスキーマに名前を付けるためのポリシー。 次のいずれかのオプションを選択します。 - なし - 指定 - FromImport: 該当なし
ユーザ名	Yellowbrick Data Warehouse のユーザー名。
セキュアな接続	TLS を使用して Yellowbrick との通信を保護するには、このオプションを選択します。 デフォルトは false です。
セキュアな CA 証明書	カスタム PEM でエンコードされた証明書ファイルの名前または JKS キーストアファイルの名前とパスワードを使用して、セキュアな通信でトラストをカスタマイズします。JKS キーストアファイルの名前とパスワードは、次の形式で指定する必要があります。 FILENAME:PASSWORD ファイル名が指定されていない場合は、次のフォールバックルート CA 証明書ファイルが使用されます。 Windows: `%APPDATA%\postgresql\root.crt` ファイルが存在する場合は、指定されたセキュアな CA 証明書ファイルと同じように扱われます。詳細については、Yellowbrick Documentation Library を参照してください。
セキュアな、無効化されたトラスト	保護された接続を使用している場合に SSL トラストおよび TLS トラストを無効にするには、このオプションを選択します。 デフォルトは false です。

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
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
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。

Zendesk V2 接続のプロパティ

Zendesk 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、Zendesk 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。 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	Zendesk 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指定します。
ユーザー名	Zendesk アカウントのユーザー名。
パスワード	Zendesk アカウントのパスワード。
URL	Zendesk アカウントの URL。完全な URL を指定します。 例えば、https://informaticabusinesssolution13.zendesk.com/api/v2 です。
ロギングの有効化	ロギングを有効化するチェックボックスを選択します。
プロキシの使用	プロキシサーバー経由で Zendesk に接続します。プロキシサーバーを使用するにはチェックボックスを選択します。
カスタムフィールド	Zendesk オブジェクトのカスタムフィールドを指定します。

カスタムフィールドのルールおよびガイドライン

カスタムフィールドを設定するときは、次のルールおよびガイドラインを考慮します。

- Zendesk のカスタムフィールドは、次の形式を使用して指定します。ここで、FieldKey は、Zendesk の **[フィールドキー]** の値です。

  ```
  Object1=”FieldKey1,DataType,Size,Filterable,PrimaryKey”;”FieldKey2,DataType,Size,Filterable,PrimaryKey”
  Object2=”FieldKey1,DataType,Size,Filterable,PrimaryKey”;”FieldKey2,DataType,Size,Filterable,PrimaryKey”
  ```

  例えば、Organizations オブジェクトと Users オブジェクトに、次のカスタムフィールドを指定できます。

  ```
  Organizations="support_description,String,255,true,false"
  Users="problems,String,255,true,false";age,Double,0,true,false";"required,Boolean,0,true,false";"select,
  String,255,true,false";"support_description,String,255,true,false";"reg_ex,String,255,true,false"
  ```

- Tickets オブジェクトのカスタムフィールドを指定する場合は、次の形式でカスタムフィールドを指定する必要があります。

  ```
  Tickets=”CF_FieldID1,DataType,Size,Filterable,PrimaryKey”;”CF_FieldID2,DataType,Size,Filterable,
  PrimaryKey”
  ```

以下に例を示します。

```
Tickets="CF_360003199614,String,255,true,false;"CF_360003373654,String,255,true,false"
```

- さまざまなオブジェクトのカスタムフィールドを新しい行に指定します。
- あるオブジェクトに対して複数のカスタムフィールドを指定する場合は、カスタムフィールドをセミコロン（;）で区切る必要があります。
- カスタムフィールドのサイズを指定する場合、エージェントは文字列データ型のサイズのみを考慮します。その他のデータ型のカスタムフィールドのサイズはゼロに設定する必要があります。
- カスタムフィールドのフィールドキーに、特殊文字を含めることはできません。
- Zendesk Web サイトで、Tickets オブジェクトのフィールドキーを検索するには、**［設定］** > **［チケットフィールドの管理］**に移動します。

Zuora AQuA 接続のプロパティ

Zuora AQuA 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、Zuora AQuA 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	Zoura AQuA 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 のランタイム環境を選択します。
エンドポイント URL	Zuora サーバーの URL。 例えば、URL を「https://www.zuora.com/apps/api/」のように指定できます。
ユーザー名	Zuora アカウントのユーザー名。
パスワード	Zuora アカウントのパスワード。
エンティティ ID	複数のエンティティを含むテナントにある特定のエンティティに接続するためのエンティティ ID。
エンティティ名	複数のエンティティを含むテナントにある特定のエンティティに接続するためのエンティティ名。
WSDL バージョン	Zuora WSDL のバージョン番号。

プロパティ	説明
削除した行の取得	オプション。増分モードで、削除した行を取得します。 デフォルトは false です。
UTC オフセット	特定の場所と日付での協定世界時（UTC）との時差。 UTC オフセット値は、lastruntime データフィルタフィールドを使用して、指定したタイムゾーンに基づいて Zuora からデータを読み取る場合に使用できます。

Zuora マルチエンティティ接続のプロパティ

Zuora マルチエンティティ接続を作成する際には、接続プロパティを設定する必要があります。

次の表に、Zuora マルチエンティティ接続のプロパティを示します。

プロパティ	説明
ランタイム環境	Zuora にアクセスする際に使用される Secure Agent が稼働しているランタイム環境。
ユーザー名	Zuora ポータルログインのユーザー名。
パスワード	Zuora ポータルログインのパスワード。
WSDL URL	Zuora WSDL URL のパス。
エンドポイント URL	Zuora エンドポイント URL のパス。
UTC オフセット	特定の場所と日付での協定世界時（UTC）との時差。 指定したタイムゾーンに基づいて Zuora マルチエンティティからデータを読み取るために$LastRuntime データフィルタフィールドを使用するときに、UTC オフセット値を使用できます。 デフォルトの UTC 値は 0 です。
バッチのレコード数	Secure Agent がバッチで読み取るレコードの数。
バッチ書き込みのレコード数	Secure Agent がエンドポイントにバッチで書き込むレコードの数。デフォルトでは、フィールドの値は 100 です。
デバッグロガーを有効にする	SOAP 要求と応答をセッションログに出力するかどうかを決定します。
エンティティ ID	複数のエンティティが単一のテナント内にある場合、特定のエンティティに接続するには、エンティティ ID を指定します。
エンティティ名	複数のエンティティが単一のテナント内にある場合、特定のエンティティに接続するには、エンティティ名を指定します。

Zuora REST V2 接続のプロパティ

Zuora REST V2 接続を作成する際には、接続プロパティを設定する必要があります。

次の表に、Zuora REST V2 接続のプロパティを示します。

プロパティ	説明
ランタイム環境	Zuora にアクセスする際に使用される Secure Agent が稼働しているランタイム環境。
認証	【ZuoraRESTV2】を選択します。
ベース URL	呼び出し先の REST API のエンドポイント URL。ベース URL と一緒にクエリパラメータを指定しないで下さい。 例: https://rest.apisandbox.zuora.com/
認証タイプ	Zuora ポータルログインへの接続に必要なユーザー認証のタイプ。コネクタが Zuora ポータルログインにログインするために使用する必要がある認証メソッドを選択します。 次の認証タイプを選択出来ます。 - 基本認証 - OAuth 2.0 デフォルトは OAuth 2.0 です。
ユーザー名	Zuora ポータルログインのユーザー名。**【認証タイプ】**として**【基本認証】**を選択した場合、ユーザー名を入力する必要があります。
パスワード	Zuora ポータルログインのパスワード。**【認証タイプ】**として**【基本認証】**を選択した場合、パスワードを入力する必要があります。
クライアント ID	Zuora への接続の OAuth 2.0 認証を完了するためのクライアント ID。**【認証タイプ】**として【OAuth 2.0】を選択した場合、クライアント ID を入力する必要があります。
クライアントシークレット	Zuora への接続の OAuth 2.0 認証を完了するためのクライアント秘密鍵。**【認証タイプ】**として【OAuth 2.0】を選択した場合、クライアント秘密鍵を入力する必要があります。
許可タイプ	トークンを取得するために使用される認証のタイプ。client_credentials を使用します。
エンティティ ID	複数のエンティティが単一のテナント内にある場合、特定のエンティティに接続するには、エンティティ ID を指定します。 要求メッセージエディタ内でエンティティ ID を指定することも出来ます。エンティティ ID を接続プロパティ内と要求メッセージエディタで指定した場合、接続プロパティで指定したエンティティ ID が優先されます。 **注**: **【認証タイプ】**として【OAuth 2.0】を選択し、**【カスタムフィールド設定】**プロパティでカスタムフィールドを指定した場合、**【エンティティ ID】**は必須です。

プロパティ	説明
Zuora API バージョン	Zuora REST V2 接続に使用する Swagger ファイル。 Zuora Swagger API V1_2017_09_06 または Zuora Swagger API V1_2018_08_23 swagger ファイルを選択出来ます。
カスタムフィールド設定	カスタムフィールドを設定する Zuora オブジェクトの名前をカンマ区切り値として指定します。 カスタムフィールドをサポートする以下の Zuora オブジェクトを指定出来ます。 - 取引先 - 会計コード - 会計期間 - 修正 - 担当者 - CreditBalanceAdjustment - CreditMemoItem - CreditMemo - DebitMemoItem - DebitMemo - 特徴 - InvoiceAdjustment - InvoiceItemAdjustment - InvoiceItem - 請求書 - JournalEntryItem - JournalEntry - OrderAction - 順序 - 支払 - ProductFeature - 製品 - ProductRatePlanCharge - ProductRatePlan - RatePlanCharge - RatePlan - 払い戻し - RevenueEventItem - RevenueEvent - RevenueScheduleItem - RevenueSchedule - サブスクリプション - SubscriptionProductFeature - TaxationItem - 使用方法 **注**: 【Zuora API **バージョン**】の値に 【Zuora Swagger API V1_2018_08_23】を選択した場合にのみ適用されます。 カスタムフィールドをサポートする Zuora オブジェクトの詳細については、https://knowledgecenter.zuora.com/BB_Introducing_Z_Business/Manage_Custom_Fields/Objects_that_Support_Custom_Fields_in_Zuora を参照して下さい。

第 4 章

REST V2 接続用の Swagger ファイルの生成

REST V2 コネクタでは、接続を設定するときに、REST サービスを定義する Swagger ファイルのパスを指定する必要があります。Informatica Intelligent Cloud Services を使用すると Swagger ファイルを生成出来ます。

Informatica Intelligent Cloud Services は Swagger 仕様バージョン 2.0 をサポートしています。Informatica Intelligent Cloud Services で Swagger ファイルを生成する場合、同じ要求を使用して API 呼び出しをサービスに送信します。API 呼び出しをサービスに送信する権限がない場合は、API 呼び出しを送信せずに、サンプル要求とサンプル応答を使用して、Swagger ファイルを生成できます。

Swagger ファイルの作成後に変更することはできません。Swagger ファイルを変更する場合は、新しい Swagger ファイルを作成します。

注: Swagger ファイル生成機能は、REST V2 カスタマの便宜のために使用出来ます。すべてのカスタマのシナリオについて Swagger ファイルの互換性を保証するわけではありません。

Swagger ファイルの生成

REST V2 接続用の swagger ファイルは、管理者の **[Swagger ファイル]** ページから生成できます。

1. **[新規]** をクリックします。
2. swagger ファイルの名前と説明を入力します。
3. swagger の詳細を指定します。次の表は、swagger ファイルを作成する際のパラメータを示しています。

パラメータ	説明
ランタイム環境	必須。swagger ファイルの生成に使用されるランタイム環境の名前。
URL	必須。URL は、ホスト名とポート番号から構成されます。以下に例を示します。 `http://localhost:8000`
動詞	Web サービスで使用されている REST メソッドを選択します。サポートされているメソッドは、GET、POST、PUT、および DELETE です。
認証タイプ	必要な場合、Web サービスアプリケーションにログインする際の認証方式を選択します。デフォルトは［なし］です。

パラメータ	説明
API の基本パス	API が動作するパス。基本パスはホスト名とポートの後に指定します。例えば、REST Web サービス URL が http://localhost:8000/greetings/hello?Status=GoodMorning の場合、基本パスは/greetings になります。
API のパス	基本パスの後に指定するパスが、API のパスです。例えば、REST Web サービス URL が http://localhost:8000/greetings/hello?Status=GoodMorning の場合、API パスは/hello?Status=GoodMorning になります。 パスパラメータを定義するには、変数として処理されるように中括弧{}でパスを囲みます。 例えば、REST Web サービス URL が https://localhost:8080/sample/Stringoperation/concat/str1/str2?id=123 で、concat がこのパスの変数の場合、API パスは次のように定義します。 Stringoperation/{concat}/str1/str2?id=123 パスパラメータの数を定義できます。 **注**: ［API のパス］には、クエリパラメータを指定できます。［API のパス］でクエリパラメータを定義する場合は、**［クエリパラメータ］** フィールドでクエリパラメータを指定しないでください。
ユーザー名	Web サービスアプリケーションにログインするユーザーの名前。 認証タイプが［基本］および［ダイジェスト］の場合に必要です。
パスワード	ユーザー名に関連付けられるパスワード。 認証タイプが［基本］および［ダイジェスト］の場合に必要です。
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。
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］の場合に必要です。
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］の場合に必要です。
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。
承認	MIME タイプを選択します。
ヘッダー	JSON 形式のヘッダーパラメータを定義します。例えば、{"Accept-Charset":"utf-8"}のように指定します。
クエリパラメータ	JSON 形式のクエリパラメータを指定します。例えば、{"name":"subject","description":"The subject to be greeted."}のように指定します。 ［クエリパラメータ］フィールドでクエリパラメータを定義すると、Swagger 仕様ファイルの入力パラメータとしてクエリパラメータが追加されます。 **［クエリパラメータ］** でクエリパラメータを定義する場合は、**［API のパス］** フィールドでクエリパラメータを指定しないでください。
操作 ID	必須。API のパスの一意のテキスト識別子。

パラメータ	説明
コンテンツタイプ	MIME タイプを選択します。
生データ本文	リクエスト本文のコンテンツを入力します。コンテンツタイプで application/x-www-form-urlencoded を選択した場合は、生データ本文パラメータをキーと値のペアで指定します。キーと値のペアごとに、新規行で開始します。例: a : b c : d e : f GET メソッドには適用されません。
JSON 応答ファイル	オプション。JSON 応答ファイルから swagger ファイルを生成する場合は、この応答ファイルをアップロードします。JSON 応答ファイルを選択した場合は、REST エンドポイントへの呼び出しが行われません。 JSON 応答ファイルを選択しない場合は、REST エンドポイントへの呼び出しが行われ、swagger ファイル生成用の応答を取得します。

注: REST V2 コネクタによってサポートされる swagger 定義オブジェクトとフィールドの詳細については、REST V2 コネクタのドキュメントを参照してください。

4. **［保存］**をクリックして swagger ファイルを生成します。swagger ファイルのエントリは**［Swagger ファイル］**ページに表示されます。

   Web サービスへの接続中にエラーが発生すると、Web サービスから取得した障害応答が**［Swagger ファイル］**ページに記録されます。

5. ダウンロードアイコンをクリックして Swagger ファイルをローカルディレクトリに保存します。

   REST V2 接続で swagger ファイルを使用するには、REST V2 接続が作成される Secure Agent システムにこのファイルをコピーします。

索引

N

O

P

Q

R

S

T

U

V

W

X

Y

Z

あ

き

し

す

て

ふ

め