



Informatica® Intelligent Cloud Services
October 2025

接続

本ソフトウェアおよびマニュアルは、使用および開示の制限を定めた個別の使用許諾契約のもとでのみ提供されています。本マニュアルのいかなる部分も、いかなる手段（電子的複写、写真複写、録音など）によっても、Informatica LLC の事前の承諾なしに複製または転載することは禁じられています。

米政府の権利プログラム、ソフトウェア、データベース、および関連文書や技術データは、米国政府の顧客に配信され、「商用コンピュータソフトウェア」または「商業技術データ」は、該当する連邦政府の取得規制と代理店固有の補足規定に基づきます。このように、使用、複製、開示、変更、および適応は、適用される政府の契約に規定されている制限およびライセンス条項に従うものとし、政府契約の条項によって適当な範囲において、FAR 52.227-19、商用コンピュータソフトウェアライセンスの追加権利を規定します。

Informatica、Informatica Cloud、Informatica Intelligent Cloud Services、PowerCenter、PowerExchange、および Informatica ロゴは、米国およびその他の国における Informatica LLC の商標または登録商標です。Informatica の商標の最新リストは、Web (<https://www.informatica.com/trademarks.html>) にあります。その他の企業名および製品名は、それぞれの企業の商標または登録商標です。

本ソフトウェアまたはドキュメンテーション（あるいはその両方）の一部は、第三者が保有する著作権の対象となります。必要な第三者の通知は、製品に含まれています。

本マニュアルの情報は、予告なしに変更されることがあります。このドキュメントで問題が見つかった場合は、infa_documentation@informatica.com までご報告ください。

Informatica 製品は、それらが提供される契約の条件に従って保証されます。Informatica は、商品性、特定目的への適合性、非侵害性の保証等を含めて、明示的または黙示的ないかなる種類の保証をせず、本マニュアルの情報を「現状のまま」提供するものとします。

発行日: 2025-11-23

目次

序文	30
Informatica のリソース.....	30
Informatica マニュアル.....	30
Informatica Intelligent Cloud Services Web サイト.....	30
Informatica Intelligent Cloud Services コミュニティ.....	30
Informatica Intelligent Cloud Services マーケットプレイス.....	31
データ統合のコネクタのドキュメント.....	31
Informatica ナレッジベース.....	31
Informatica Intelligent Cloud Services Trust Center.....	31
Informatica グローバルカスタマサポート.....	31
 第 1 章 : コネクタと接続	32
アドオンコネクタ.....	32
アドオンコネクタのインストール.....	32
 第 2 章 : 接続設定	34
接続の設定.....	35
サンプルデータを使用した接続の設定.....	37
接続依存関係の表示.....	37
 第 3 章 : ActiveCampaign 接続プロパティ	39
 第 4 章 : Adabas CDC 接続のプロパティ	40
 第 5 章 : Adabas 接続のプロパティ	43
 第 6 章 : Adaptive Insights 接続プロパティ	46
 第 7 章 : Adobe Analytics 接続のプロパティ	47
 第 8 章 : Adobe Analytics Mass Ingestion 接続のプロパティ	49
 第 9 章 : Adobe Experience Platform 接続のプロパティ	51
 第 10 章 : 高度な FTP 接続のプロパティ	52
 第 11 章 : Advanced FTP V2 接続のプロパティ	54
 第 12 章 : 高度な FTPS 接続のプロパティ	56
 第 13 章 : Advanced FTPS V2 接続のプロパティ	58

第 14 章 : 高度な SFTP 接続のプロパティ	61
第 15 章 : Advanced SFTP V2 接続のプロパティ	62
第 16 章 : Amazon Athena 接続のプロパティ	64
認証の準備.	64
Amazon S3 ポリシーの作成.	64
AWS Glue データカタログポリシーの作成.	65
Amazon Athena ポリシーの作成.	65
ロールを引き受けるための EC2 ロールの設定.	66
Amazon Athena への接続.	67
始める前に.	68
接続の詳細.	68
認証タイプ.	68
詳細設定.	70
プロキシサーバーの設定.	70
Amazon Athena のワークグループ.	71
第 17 章 : Amazon Aurora 接続のプロパティ	72
第 18 章 : Amazon DynamoDB 接続のプロパティ	74
第 19 章 : Amazon DynamoDB V2 接続のプロパティ	75
第 20 章 : Amazon Kinesis 接続のプロパティ	77
Amazon Kinesis Firehose 接続のプロパティ.	77
Amazon Kinesis Streams 接続のプロパティ.	79
第 21 章 : Amazon Redshift 接続のプロパティ	81
第 22 章 : Amazon Redshift V2 接続のプロパティ	83
認証の準備.	83
最小限の Amazon IAM ポリシーの作成.	85
IAM 認証の設定.	85
Amazon Redshift の引き受けロールの設定.	86
Amazon Redshift の一時的なセキュリティ資格情報ポリシーの生成.	86
EC2 に AssumeRole を使用した一時的なセキュリティ資格情報の生成.	88
Amazon S3 ステージングの引き受けロールの設定.	90
Amazon S3 ステージングに AssumeRole を使用した一時的なセキュリティ資格情報の生成. . .	90
EC2 に AssumeRole を使用した一時的なセキュリティ資格情報の生成.	92
暗号化を有効にする.	93
Amazon Redshift への接続.	94
始める前に.	94

接続の詳細.	94
認証タイプ.	95
プロキシサーバーの設定.	105
Amazon Redshift でのデータ共有.	105
SSL の設定.	106
サーバーレスランタイム環境での SSL の設定.	106
詳細モードのマッピングに対する SSE-KMS 暗号化の設定.	108
Amazon Redshift サーバーレス接続.	108
Amazon Redshift Spectrum を使用するための要件.	108
Amazon Redshift とのプライベート通信.	109
Amazon S3 とのプライベート通信.	109
サーバーレスランタイム環境と Amazon Redshift 間の VPC ピアリング.	109
第 23 章 : Amazon S3 接続のプロパティ.	110
第 24 章 : Amazon S3 V2 接続プロパティ.	112
認証の準備.	112
最小限の Amazon IAM ポリシーの作成.	112
IAM 認証.	113
EC2 ロールと IAM ユーザーを使用した AssumeRole	114
資格情報プロファイルファイルの認証.	116
IAM Roles Anywhere 認証.	117
Amazon S3 への接続.	118
始める前に.	118
接続の詳細.	118
認証タイプ.	119
詳細設定.	130
Amazon S3 とのプライベート通信.	132
KMS を使用したサーバーサイド暗号化.	132
サーバーレスランタイム環境でのクライアント側の暗号化.	133
詳細モードのマッピングに対する SSE-KMS 暗号化.	133
プロキシサーバーの設定.	134
プロキシサーバーのバイパス.	134
IAM ユーザー経由の AssumeRole のルールとガイドライン認証.	135
AWS リージョンのルールとガイドライン.	136
S3 互換ストレージのルールおよびガイドライン.	136
第 25 章 : Amazon SageMaker レイクハウスの接続プロパティ.	138
前提条件.	138
最小限の IAM ポリシーの作成.	138
ロールを引き受けるための EC2 ロールの設定.	140
Amazon SageMaker レイクハウスへの接続.	141
始める前に.	142

接続の詳細.....	142
ストレージ認証タイプ.....	143
詳細設定.....	144
第 26 章 : Amplitude 接続プロパティ.....	145
第 27 章 : AMQP 接続プロパティ.....	146
第 28 章 : Anaplan V2 接続のプロパティ.....	148
第 29 章 : Ariba V2 接続のプロパティ.....	151
第 30 章 : AS2 接続のプロパティ.....	153
接続プロパティ.....	153
メッセージのプロパティ.....	155
受信確認のプロパティ.....	156
プロキシのプロパティ.....	157
第 31 章 : Azure AI Search 接続のプロパティ.....	158
前提条件.....	158
Azure AI Search への接続.....	158
始める前に.....	158
接続の詳細.....	159
第 32 章 : BigMachines 接続のプロパティ.....	160
第 33 章 : Birst Cloud 接続のプロパティ.....	162
第 34 章 : Box 接続のプロパティ.....	163
Box への接続.....	163
始める前に.....	163
接続の詳細.....	164
OAuth アクセストークンの生成.....	166
URI 要求パラメータ.....	167
第 35 章 : Business 360 接続のプロパティ.....	168
第 36 章 : Business 360 Events 接続のプロパティ.....	169
第 37 章 : Business 360 FEP 接続のプロパティ.....	170
第 38 章 : CallidusCloud Commissions 接続のプロパティ.....	171
第 39 章 : CallidusCloud File Processor 接続のプロパティ.....	173

第 40 章 : Cassandra V2 接続のプロパティ	175
第 41 章 : Chatter 接続のプロパティ	177
第 42 章 : Cloud 統合ハブ接続プロパティ	178
第 43 章 : Concur 接続のプロパティ	180
第 44 章 : Concur V2 接続のプロパティ	182
第 45 章 : Couchbase 接続のプロパティ	184
第 46 章 : Coupa 接続のプロパティ	186
第 47 章 : Coupa V2 接続のプロパティ	187
Coupa V2 への接続.....	187
始める前に.....	187
接続の詳細.....	187
詳細設定.....	189
Coupa V2 カスタムフィールド.....	189
プロキシサーバーの設定.....	190
第 48 章 : Cvent 接続のプロパティ	191
Cvent への接続.....	191
始める前に.....	191
接続の詳細.....	191
詳細設定.....	192
プロキシサーバーの設定.....	193
第 49 章 : Cvent V2 接続のプロパティ	194
前提条件.....	194
Cvent への接続.....	194
始める前に.....	194
接続の詳細.....	194
認証タイプ.....	195
詳細設定.....	196
プロキシサーバーの設定.....	196
第 50 章 : Databricks 接続プロパティ	197
ステージングの前提条件.....	197
SQL ウェアハウス.....	197
AWS ステージングの設定.....	197
Azure ステージングの設定.....	201

Databricks ボリュームでのデータのステージング.....	202
汎用クラスター.....	202
Secure Agent のプロパティの設定.....	202
ジョブクラスター.....	203
Spark 設定.....	203
Secure Agent のプロパティの設定.....	203
Databricks への接続.....	204
始める前に.....	204
接続の詳細.....	204
認証タイプ.....	205
詳細設定.....	207
JDBC URL パラメータ.....	212
プロキシサーバーの設定.....	212
Databricks にアクセスするためのプライベートリンク.....	213
個人用ステージングの場所についてのルールおよびガイドライン.....	213
第 51 章 : Datacom CDC 接続のプロパティ.....	215
第 52 章 : Datacom 接続のプロパティ.....	218
第 53 章 : Db2 データマップ接続のプロパティ.....	221
第 54 章 : Db2 for i CDC 接続のプロパティ.....	224
第 55 章 : Db2 for i 接続のプロパティ.....	227
第 56 章 : Db2 for i Database Ingestion 接続のプロパティ.....	229
第 57 章 : Db2 for LUW CDC 接続のプロパティ.....	231
第 58 章 : Db2 for LUW Database Ingestion 接続のプロパティ.....	234
第 59 章 : Db2 for z/OS バルクロード接続のプロパティ.....	235
第 60 章 : Db2 for z/OS CDC 接続のプロパティ.....	237
第 61 章 : Db2 for z/OS 接続のプロパティ.....	240
第 62 章 : Db2 for z/OS Database Ingestion 接続のプロパティ.....	243
第 63 章 : Db2 for z/OS イメージコピー接続のプロパティ.....	245
第 64 章 : Db2 for z/OS アンロードファイル接続のプロパティ.....	247

第 65 章 : DB2 ロードー接続のプロパティ	250
前提条件.....	250
DB2 ロードー JDBC ドライバと DB2 クライアントのインストール.....	250
DB2 ロードーへの接続.....	251
始める前に.....	251
接続の詳細.....	251
第 66 章 : Db2 Warehouse on Cloud 接続のプロパティ	255
第 67 章 : Denode 接続のプロパティ	257
Denodo への接続.....	257
始める前に.....	257
接続の詳細.....	257
第 68 章 : Domo 接続のプロパティ	259
第 69 章 : Dropbox 接続のプロパティ	260
第 70 章 : Elasticsearch 接続のプロパティ	262
第 71 章 : Eloqua Bulk API 接続のプロパティ	264
Eloqua への接続.....	264
始める前に.....	264
接続の詳細.....	265
詳細設定.....	266
アクティビティまたはカスタムフィールド設定.....	266
カスタムオブジェクトへの、フィールド API の一部ではないフィールドの追加.....	267
タイムゾーンのオフセットについて.....	273
プロキシサーバーの設定.....	273
第 72 章 : Eloqua REST 接続のプロパティ	275
第 73 章 : FHIR 接続プロパティ	277
FHIR 接続.....	277
接続の詳細.....	277
認証タイプ.....	279
第 74 章 : File List 接続のプロパティ	282
第 75 章 : File Processor 接続のプロパティ	284
第 76 章 : FileIO 接続のプロパティ	286

第 77 章 : フラットファイル接続	288
フラットファイル接続のプロパティ	288
Linux でのフラットファイル接続のロケールの設定	292
第 78 章 : FTP/SFTP 接続	293
FTP/SFTP 接続のプロパティ	293
キー交換アルゴリズムと暗号	294
FTP/SFTP 接続のルールとガイドライン	295
第 79 章 : Google Ads 接続のプロパティ	296
第 80 章 : Google Analytics 接続のプロパティ	298
前提条件	298
Google Analytics への接続	299
始める前に	299
接続の詳細	300
API バージョン	300
第 81 章 : Google Analytics Mass Ingestion 接続のプロパティ	302
第 82 章 : Google BigQuery 接続のプロパティ	303
接続モード	304
接続モードの例	305
Google BigQuery 接続モードのルールとガイドライン	308
第 83 章 : Google BigQuery V2 接続のプロパティ	310
Google BigQuery への接続	310
始める前に	310
接続の詳細	311
認証タイプ	311
接続の再試行	316
プロキシサーバーの設定	316
NTLM 認証用のプロキシの設定	317
第 84 章 : Google Bigtable 接続のプロパティ	318
第 85 章 : Google Cloud Storage 接続のプロパティ	319
第 86 章 : Google Cloud Storage V2 接続のプロパティ	320
Google Cloud Storage V2 への接続	320
始める前に	320
接続の詳細	321
詳細設定	322

プロキシサーバーの設定.	322
NTLM 認証のプロキシの設定.	323
第 87 章 : Google Drive 接続のプロパティ.	324
第 88 章 : Google PubSub - ストリーミング取り込みとレプリケーション接続のプロパティ.	326
第 89 章 : Google PubSub 接続のプロパティ.	327
第 90 章 : Google PubSub V2 接続のプロパティ.	328
第 91 章 : Google Sheets 接続のプロパティ.	329
第 92 章 : Google Sheets V2 接続のプロパティ.	331
第 93 章 : Greenplum 接続のプロパティ.	333
前提条件.	333
JDBC ドライバおよび ODBC ドライバの設定.	333
Kerberos 認証の設定.	335
Greenplum への接続.	336
始める前に.	336
接続の詳細.	337
認証タイプ.	337
第 94 章 : Hadoop 接続プロパティ.	340
JDBC URL.	341
JDBC ドライバクラス.	342
第 95 章 : Hadoop ファイル接続のプロパティ.	343
第 96 章 : Hadoop Files V2 接続のプロパティ.	345
第 97 章 : Hive 接続のプロパティ.	348
第 98 章 : HubSpot 接続のプロパティ.	351
第 99 章 : IBM MQ 接続のプロパティ.	352
第 100 章 : IMS CDC 接続のプロパティ.	355
第 101 章 : IMS 接続のプロパティ.	358
第 102 章 : JD Edwards EnterpriseOne 接続のプロパティ.	361
第 103 章 : JDBC 接続プロパティ.	363

第 104 章 : JDBC V2 接続のプロパティ	365
前提条件.....	365
Type 4 JDBC ドライバのインストール.....	365
JDBC V2 への接続.....	366
始める前に.....	366
接続の詳細.....	366
詳細モードのマッピング用の SSL 対応データベースへの接続.....	368
サーバーレスランタイム環境の設定.....	369
エラスティックランタイム環境の設定.....	370
第 105 章 : JIRA Cloud 接続のプロパティ	371
第 106 章 : JMS 接続のプロパティ	372
前提条件.....	372
JMS への接続.....	372
始める前に.....	372
接続の詳細.....	373
第 107 章 : JIRA 接続のプロパティ	375
Jira への接続.....	375
始める前に.....	375
接続の詳細.....	375
第 108 章 : JSON Target 接続のプロパティ	377
第 109 章 : Kafka 接続のプロパティ	378
第 110 章 : Klaviyo 接続のプロパティ	382
第 111 章 : 大規模言語モデル接続のプロパティ	383
認証の準備.....	383
API キーの取得.....	383
大規模言語モデルへの接続.....	384
始める前に.....	384
接続の詳細.....	384
第 112 章 : LDAP 接続のプロパティ	386
第 113 章 : Magento V1 接続のプロパティ	388
第 114 章 : Mailchimp 接続のプロパティ	389

第 115 章 : Marketo V3 接続のプロパティ	390
Marketo への接続	390
始める前に	390
接続の詳細	390
詳細設定	391
プロキシサーバーの設定	392
第 116 章 : Microsoft Access 接続のプロパティ	393
第 117 章 : Microsoft Azure Analysis Services 接続のプロパティ	395
認証の準備	395
Microsoft Azure Analysis Services への接続	396
始める前に	396
接続の詳細	396
認証タイプ	397
第 118 章 : Microsoft Azure Blob Storage V2 接続のプロパティ	398
第 119 章 : Microsoft Azure Blob Storage V3 接続のプロパティ	399
認証の準備	399
共有キー認証	399
共有アクセス署名	400
Microsoft Azure Blob Storage V3 への接続	401
始める前に	401
接続の詳細	402
認証タイプ	402
プロキシサーバーの設定	403
第 120 章 : Microsoft Azure Cosmos DB SQL API 接続のプロパティ	405
Microsoft Azure Cosmos DB SQL API への接続	405
始める前に	405
接続の詳細	405
第 121 章 : Microsoft Azure Data Lake Storage Gen2 接続のプロパティ	407
認証の準備	407
マネージド ID 認証	408
Microsoft Azure Data Lake Storage Gen2 への接続	408
始める前に	408
接続の詳細	409
認証タイプ	410
プロキシサーバーの設定	411
プロキシサーバーのバイパス	412

第 122 章 : Microsoft DocumentDB 接続のプロパティ.....	413
第 123 章 : Microsoft Azure Event Hub 接続のプロパティ.....	414
第 124 章 : Microsoft Azure SQL Data Warehouse - データベース取り 込み接続のプロパティ.....	415
第 125 章 : Microsoft Azure SQL Data Warehouse 接続のプロパティ...	417
第 126 章 : Microsoft Azure SQL Data Warehouse V2 接続のプロパティ	419
第 127 章 : Microsoft Azure Synapse Analytics 接続のプロパティ.....	420
認証の準備.....	420
Microsoft Azure Synapse Analytics への接続.....	421
始める前に.....	421
接続の詳細.....	421
認証タイプ.....	421
プロキシのプロパティ.....	422
第 128 章 : Microsoft Azure Synapse Analytics Database Ingestion 接 続のプロパティ.....	424
第 129 章 : Microsoft Azure Synapse SQL 接続のプロパティ.....	426
前提条件.....	426
Azure Active Directory 認証.....	426
サービスプリンシパル認証.....	428
マネージド ID 認証.....	428
サーバーレス SQL プール.....	428
権限.....	429
Microsoft Azure Synapse SQL への接続.....	430
始める前に.....	430
接続の詳細.....	430
Azure ストレージタイプ.....	433
詳細設定.....	436
第 130 章 : Microsoft CDM Folders V2 接続プロパティ.....	437
第 131 章 : Microsoft Dynamics 365 for Operations 接続のプロパティ..	439
認証の準備.....	439
OAuth 2.0 認証.....	439
OAuth 2.0 クライアントシークレット付与認証.....	439
-dlog4j.configuration プロパティの設定.....	440
Microsoft 365 for Operations への接続.....	440

始める前に.....	440
接続の詳細.....	440
認証タイプ.....	441
詳細設定.....	442
プロキシサーバーの設定.....	443
第 132 章 : Microsoft Dynamics 365 for Sales 接続.....	444
認証の準備.....	444
OAuth 2.0 パスワード付与.....	444
OAuth 2.0 クライアントシークレット付与.....	444
OAuth 2.0 クライアント証明書付与.....	446
Microsoft Dynamics 365 for Sales への接続.....	448
始める前に.....	448
接続の詳細.....	449
認証タイプ.....	449
詳細設定.....	451
サーバーレスランタイム環境の設定.....	451
Microsoft Dynamics 365 for Sales 接続のトラブルシューティング.....	452
第 133 章 : Microsoft Dynamics 365 Mass Ingestion 接続のプロパティ.....	453
第 134 章 : Microsoft Dynamics CRM 接続のプロパティ.....	457
第 135 章 : Microsoft Dynamics NAV 接続のプロパティ.....	459
第 136 章 : Microsoft Excel 接続のプロパティ.....	460
第 137 章 : Microsoft Fabric データウェアハウスの接続プロパティ.....	462
前提条件.....	462
Microsoft Fabric データウェアハウスへの接続.....	463
始める前に.....	463
接続の詳細.....	463
詳細設定.....	464
Microsoft Fabric データウェアハウスにアクセスするためのプライベートリンク.....	464
第 138 章 : Microsoft Fabric レイクハウスの接続プロパティ.....	466
前提条件.....	466
Microsoft Fabric レイクハウスへの接続.....	467
始める前に.....	467
接続の詳細.....	467
Microsoft Fabric レイクハウスにアクセスするためのプライベートリンク.....	468

第 139 章 : Microsoft Fabric OneLake 接続のプロパティ	470
前提条件	470
Microsoft Fabric OneLake への接続	471
始める前に	471
接続の詳細	471
プロキシサーバーの設定	472
プロキシサーバーのバイパス	472
Microsoft Fabric OneLake にアクセスするためのプライベートリンク	473
第 140 章 : Microsoft Power BI 接続のプロパティ	475
認証の準備	475
Microsoft Power BI への接続	476
始める前に	476
接続の詳細	476
認証タイプ	477
プロキシのプロパティ	478
第 141 章 : Microsoft SharePoint 接続のプロパティ	479
第 142 章 : Microsoft Sharepoint Online 接続のプロパティ	481
認証の準備	481
Access Control Service	481
Microsoft Entra ID	484
Microsoft SharePoint Online への接続	487
始める前に	487
接続の詳細	487
SharePoint Online 認証タイプ	487
第 143 章 : Microsoft SQL Server CDC 接続のプロパティ	490
第 144 章 : Microsoft SQL Server 接続のプロパティ	493
認証の準備	493
Kerberos 認証の準備	493
Microsoft SQL Server への接続	495
始める前に	495
接続の詳細	496
認証モード	496
詳細設定	502
サーバーレスランタイム環境での SSL の設定	503
第 145 章 : Mixpanel 接続のプロパティ	505

第 146 章 : MLLP 接続プロパティ	506
第 147 章 : MongoDB Mass Ingestion 接続のプロパティ	508
第 148 章 : MongoDB 接続のプロパティ	510
第 149 章 : MongoDB V2 接続のプロパティ	512
認証の準備.....	512
ユーザー名およびパスワード.....	512
X.509 標準.....	512
LDAP.....	512
MongoDB への接続.....	513
始める前に.....	513
接続の詳細.....	513
認証タイプ.....	514
詳細設定.....	515
追加接続プロパティ.....	516
サーバーレスランタイム環境の SSL の設定.....	517
プロキシサーバーの設定.....	518
第 150 章 : MQTT 接続のプロパティ	519
第 151 章 : MRI Software 接続のプロパティ	521
第 152 章 : MySQL CDC 接続のプロパティ	522
第 153 章 : MySQL 接続のプロパティ	525
SSL プロパティ.....	526
エラスティックランタイム環境の設定.....	528
第 154 章 : Netezza 接続のプロパティ	530
前提条件.....	530
Netezza JDBC ドライバのダウンロード.....	530
Netezza ODBC ドライバのダウンロード.....	530
Netezza への接続.....	531
始める前に.....	531
接続の詳細.....	531
詳細設定.....	533
データベース特権.....	533
第 155 章 : NetSuite 接続のプロパティ	534
NetSuite への接続.....	534
始める前に.....	534

接続の詳細.	534
詳細設定.	536
NetSuite アカウント固有のサービス URL.	538
トークンベースの認証.	539
NetSuite 接続についてのルールおよびガイドライン.	539
NetSuite 接続のトラブルシューティング.	540
 第 156 章 : NetSuite Mass Ingestion 接続のプロパティ	541
 第 157 章 : NetSuite RESTlet V2 接続のプロパティ	543
 第 158 章 : NICE Satmetrix 接続のプロパティ	545
 第 159 章 : OData の接続プロパティ	546
OData への接続.	546
始める前に.	546
接続の詳細.	546
詳細設定.	547
プロキシサーバーの設定.	547
 第 160 章 : OData Consumer の接続プロパティ	548
OData Consumer への接続.	548
始める前に.	548
接続の詳細.	548
詳細設定.	549
プロキシサーバーの設定.	550
一方向 SSL のセットアップ.	550
 第 161 章 : OData V2 Protocol Reader 接続のプロパティ	552
認証コードの認証.	553
クライアント資格情報の認証.	555
 第 162 章 : OData V2 Protocol Writer 接続のプロパティ	557
 第 163 章 : ODBC 接続のプロパティ	559
前提条件.	559
ODBC ドライバの設定.	559
Kerberos 認証の準備.	565
ODBC 接続.	567
始める前に.	568
接続の詳細.	568
ODBC 接続のルールとガイドライン.	572
サーバーレスランタイム環境の設定.	572

エラスティックランタイム環境の設定.	574
第 164 章 : OpenAir 接続のプロパティ.	576
第 165 章 : オープンテーブル接続プロパティ.	577
前提条件.	577
最小限の IAM ポリシーの作成.	578
JDBC ドライバのインストール.	580
ロールを引き受けるための EC2 ロールの設定.	580
オープンテーブルへの接続.	581
始める前に.	581
オープンテーブル形式、および関連するカタログタイプとストレージタイプ.	581
接続の詳細.	582
カタログタイプ.	583
ストレージタイプ.	585
第 166 章 : Oracle 接続のプロパティ.	587
前提条件.	587
SSL 設定.	587
Kerberos 認証.	589
Oracle への接続.	590
始める前に.	590
接続の詳細.	591
認証モード.	591
詳細設定.	593
サーバーレスランタイム環境での SSL の設定.	594
Oracle 接続のルールおよびガイドライン.	595
第 167 章 : Oracle Autonomous Database 接続.	596
前提条件.	596
メモリ要件.	596
オブジェクトストレージ認証の準備.	596
Oracle Autonomous Database への接続.	597
始める前に.	597
接続の詳細.	597
認証タイプ.	598
オブジェクトストレージ認証タイプ.	599
第 168 章 : Oracle Business Intelligence Publisher の接続プロパティ.	600
Oracle Business Intelligence Publisher への接続.	600
始める前に.	600
接続の詳細.	601
詳細設定.	602

プロキシサーバーの設定.	602
第 169 章 : Oracle CDC V2 接続のプロパティ.	604
第 170 章 : Oracle Cloud Object Storage 接続.	607
前提条件.	607
Oracle Cloud Infrastructure ポリシーの設定.	607
認証の準備.	608
Oracle Cloud Object Storage への接続.	609
始める前に.	609
接続の詳細.	609
認証タイプ.	609
プロキシサーバーの設定.	611
第 171 章 : Oracle CRM Cloud V1 接続のプロパティ.	612
第 172 章 : Oracle CRM On Demand 接続のプロパティ.	614
第 173 章 : Oracle Database Ingestion 接続のプロパティ.	615
Kerberos 認証の前提条件.	623
Kerberos 認証の設定.	623
第 174 章 : Oracle Financials Cloud V1 接続のプロパティ.	625
前提条件.	625
XLSM テンプレートファイルへのアクセス.	625
ERP エンドポイント URL の取得.	626
Oracle Financials Cloud への接続.	626
始める前に.	626
接続の詳細.	627
暗号化モード.	628
プロキシサーバーの設定.	629
第 175 章 : Oracle Fusion Cloud Mass Ingestion 接続のプロパティ.	631
第 176 章 : Oracle HCM Cloud V1 接続のプロパティ.	632
前提条件.	632
WebCenter コンテンツ URL の取得.	632
ロールの確認.	633
Oracle HCM への接続.	633
始める前に.	633
接続の詳細.	634
詳細設定.	635
暗号化モード.	635

抽出定義.	637
Excel テンプレートのダウンロード.	637
ADF デスクトップ統合ツールのダウンロードとインストール.	639
Excel テンプレートの設定.	640
プロキシサーバーの設定.	641
第 177 章 : SAP の接続プロパティ.	642
認証の準備.	642
Pinecone API キーの取得.	642
Pinecone への接続.	642
始める前に.	642
接続の詳細.	643
第 178 章 : PostgreSQL CDC 接続のプロパティ.	644
第 179 章 : PostgreSQL 接続のプロパティ.	647
認証の準備.	647
Kerberos 認証の準備.	647
PostgreSQL への接続.	649
始める前に.	649
接続の詳細.	649
認証タイプ.	650
詳細設定.	652
暗号化タイプ.	652
サーバーレスランタイム環境での SSL の設定.	654
第 180 章 : QuickBooks V2 接続のプロパティ.	655
第 181 章 : Redis 接続のプロパティ.	657
第 182 章 : REST API 接続のプロパティ.	659
第 183 章 : REST V2 接続のプロパティ.	660
前提条件.	660
REST V2 への接続.	660
始める前に.	660
接続の詳細.	660
認証タイプ.	661
詳細設定.	670
TLS 認証によるセキュアな通信.	672
トラストストアの生成.	672
キーストアの生成.	672
一方向または双方向のセキュアな通信の設定.	673

サーバーレスランタイム環境での安全な通信.	674
サーバーレスランタイム環境の Swagger 仕様ファイル.	674
エラスティックランタイム環境の設定.	675
ランタイム環境のルールとガイドライン.	676
REST V2 接続のルールとガイドライン.	676
第 184 章 : REST V3 接続のプロパティ.	678
認証コードの認証.	680
クライアント資格情報の認証.	682
REST V3 接続についてのルールおよびガイドライン.	684
第 185 章 : Salesforce Analytics 接続のプロパティ.	686
第 186 章 : Salesforce Commerce Cloud 接続のプロパティ.	688
第 187 章 : Salesforce 接続のプロパティ.	689
認証の準備.	689
標準.	689
OAuth.	689
Salesforce への接続.	690
始める前に.	690
接続の詳細.	690
Salesforce 接続タイプ.	691
ファイアウォール設定.	693
プロキシサーバーの設定.	693
接続タイムアウト.	693
Salesforce 接続のトラブルシューティング.	694
第 188 章 : Salesforce Data Cloud 接続のプロパティ.	695
Salesforce Data Cloud への接続.	695
始める前に.	695
接続の詳細.	695
詳細設定.	697
第 189 章 : Salesforce Marketing Cloud 接続のプロパティ.	698
第 190 章 : Salesforce Mass Ingestion 接続のプロパティ.	700
第 191 章 : Salesforce Pardot 接続のプロパティ.	703
第 192 章 : SAP 接続プロパティ.	705
前提条件.	705
SAP ライブラリのダウンロードと設定.	705
SAP ユーザー権限の設定.	707

sapnwrfc.ini ファイルの設定.	707
SAP の論理システムとしての SAP コネクタの定義.	710
SAP 接続.	713
始める前に.	713
接続の詳細.	714
SAP 接続タイプ.	714
サーバーレスランタイム環境の使用.	716
第 193 章 : SAP ADSO Writer 接続のプロパティ.	718
第 194 章 : SAP BAPI 接続のプロパティ.	724
前提条件.	724
SAP ライブラリのダウンロードと設定.	724
SAP ユーザー権限の設定.	725
SAP BAPI への接続.	726
始める前に.	726
接続の詳細.	726
詳細設定.	727
ビジネスサービスとしての SAP BAPI コネクタの設定.	728
サーバーレスランタイム環境の設定.	728
エラスティックランタイム環境の設定.	729
第 195 章 : SAP BW コネクタ接続プロパティ.	731
前提条件.	731
SAP ライブラリのダウンロードと設定.	731
SAP ユーザー権限の設定.	733
SAP BW へのトランスポートファイルのインストール.	734
SAP BW への接続.	735
始める前に.	735
接続の詳細.	735
接続タイプ.	736
SAP に接続するための HTTPS の設定.	740
OpenSSL 証明書の作成.	740
OpenSSL 証明書から PSE 形式への変換.	742
SAP システムでの HTTPS サービスの有効化.	742
SAP システムのトラストストアへの証明書のインポート.	743
第 196 章 : SAP BW BEx クエリ接続のプロパティ.	744
前提条件.	744
SAP ライブラリのダウンロードと設定.	744
SAP ユーザー権限の設定.	745
SAP BW BEx クエリへの接続.	746
始める前に.	746

接続の詳細.	746
接続タイプ.	747
サーバーレスランタイム環境の使用.	750
第 197 章 : SAP HANA CDC 接続のプロパティ.	752
第 198 章 : SAP HANA 接続のプロパティ.	755
前提条件.	755
Windows 上での HANA ODBC データソースの作成.	755
Linux オペレーティングシステムでのエントリの追加.	757
ライブラリのダウンロードと設定.	758
SAP HANA への接続.	758
始める前に.	758
接続の詳細.	758
詳細設定.	760
サーバーレスランタイム環境の設定.	760
エラスティックランタイム環境の設定.	761
Secure Socket Layer プロトコルの設定.	762
第 199 章 : SAP HANA Database Ingestion 接続のプロパティ.	763
第 200 章 : SAP IQ 接続のプロパティ.	766
前提条件.	766
SAP IQ JDBC ドライバと Sybase クライアントのインストール.	766
SAP IQ への接続.	767
始める前に.	767
接続の詳細.	767
第 201 章 : SAP Mass Ingestion 接続のプロパティ.	769
第 202 章 : SAP OData V2 接続のプロパティ.	776
前提条件.	776
SAP ユーザーアカウントの設定.	776
認証の準備.	776
SAP OData V2 への接続.	778
始める前に.	778
接続の詳細.	778
認証タイプ.	779
負荷分散接続の設定.	785
プロキシサーバーの設定.	786
第 203 章 : SAP OData V4 接続のプロパティ.	787
認証の準備.	787

基本.....	787
承認コード.....	787
SAP OData V4 への接続.....	788
始める前に.....	788
接続の詳細.....	788
認証タイプ.....	789
プロキシサーバーの設定.....	790
第 204 章 : SAP ODP Extractor 接続のプロパティ.....	792
前提条件.....	792
SAP サーバーに必要な SAP Notes の確認.....	792
SAP ライブラリのダウンロードと設定.....	793
SAP ユーザー権限の設定.....	794
セキュアなネットワーク通信プロトコルの設定.....	797
SAP ODP への接続.....	797
始める前に.....	797
接続の詳細.....	797
SAP サーバー接続タイプ.....	798
詳細設定.....	803
SAP ODP オブジェクトからの階層データ抽出.....	803
サーバーレスランタイム環境の使用.....	804
Chapter 205: SAP Table Connector connection properties.....	806
前提条件.....	806
SAP ライブラリのダウンロードと設定.....	806
SAP ユーザー権限の設定.....	808
SAP テーブルから読み取るトランスポートファイルのインストール.....	809
SAP テーブルに書き込むトランスポートファイルのインストール.....	810
SAP テーブルへの接続.....	810
始める前に.....	810
接続の詳細.....	811
sapnwrfc.ini ファイルの設定.....	813
接続タイプのサンプル sapnwrfc.ini ファイル.....	814
SAP に接続するための HTTPS の設定.....	816
OpenSSL 証明書の作成.....	816
OpenSSL 証明書から PSE 形式への変換.....	818
SAP システムで HTTPS サービスを有効にします.....	818
SAP システムのトラストストアへの証明書のインポート.....	818
セキュアなネットワーク通信プロトコルの設定.....	819
Secure Agent が SAP でホワイトリストに登録されたホストとして動作するようにする（オプション）.....	819
サーバーレスランタイム環境の使用.....	820
SAP テーブル接続のトラブルシューティング.....	821

第 206 章 : SAS 接続のプロパティ	823
第 207 章 : Satmetrix 接続のプロパティ	824
第 208 章 : シーケンシャルファイル接続のプロパティ	825
第 209 章 : ServiceNow 接続のプロパティ	828
ServiceNow への接続.	828
始める前に.	828
接続の詳細.	828
詳細設定.	829
ファイアウォール設定.	829
プロキシサーバーの設定.	830
proxy.ini ファイルを介したプロキシサーバーの設定.	830
ServiceNow 接続のテスト.	830
第 210 章 : ServiceNow Mass Ingestion 接続のプロパティ	833
第 211 章 : Shopify 接続のプロパティ	835
Shopify への接続.	835
始める前に.	835
接続の詳細.	835
第 212 章 : Slack の接続プロパティ	837
認証の準備.	837
OAuth 2.0 認証.	837
ベアラートークン認証.	838
Slack への接続.	838
始める前に.	838
接続の詳細.	838
認証タイプ.	839
Slack のスコープ.	840
第 213 章 : Snowflake 接続プロパティ	843
第 214 章 : Snowflake Data Cloud 接続のプロパティ	845
認証の準備.	845
標準.	845
承認コード.	846
キーペア.	847
クライアント資格情報.	848
Snowflake への接続.	848
始める前に.	848

接続の詳細.	849
認証タイプ.	849
JDBC URL パラメータ.	856
外部 OAuth 認証用の Microsoft Azure Active Directory.	858
プロキシサーバーの設定.	858
Snowflake にアクセスするためのプライベートリンク.	859
キーペア認証でのサーバーレスランタイム環境の使用.	859
第 215 章 : Strategy Cloud 接続のプロパティ.	861
Strategy Cloud への接続.	861
始める前に.	861
接続の詳細.	861
第 216 章 : Stripe 接続のプロパティ.	863
Stripe への接続.	863
始める前に.	863
接続の詳細.	863
第 217 章 : SuccessFactors LMS 接続のプロパティ.	865
第 218 章 : SuccessFactors ODATA 接続プロパティ.	867
SuccessFactors への接続.	867
始める前に.	867
接続の詳細.	868
詳細設定.	869
プロキシサーバーの設定.	869
第 219 章 : SuccessFactors SOAP 接続のプロパティ.	871
第 220 章 : SurveyMonkey 接続のプロパティ.	872
第 221 章 : Tableau V2 接続のプロパティ.	874
第 222 章 : Tableau V3 接続のプロパティ.	876
第 223 章 : Teradata 接続のプロパティ.	879
前提条件.	879
Teradata Parallel Transporter Utilities.	879
Kerberos 認証の準備.	879
環境変数の設定.	881
Teradata への接続.	882
始める前に.	882
接続の詳細.	882
認証タイプ.	883

詳細設定.	884
データベース特権.	885
第 224 章 : UKGPro V2 接続のプロパティ.	886
第 225 章 : UltiPro 接続のプロパティ.	888
第 226 章 : Veeva Vault 接続のプロパティ.	890
認証の準備.	890
基本.	890
承認コード.	890
Veeva Vault への接続.	891
始める前に.	891
接続の詳細.	891
認証タイプ.	891
第 227 章 : VSAM CDC 接続のプロパティ.	895
第 228 章 : VSAM 接続のプロパティ.	898
第 229 章 : Web サービスコンシューマ接続のプロパティ.	901
第 230 章 : Web サービス V2 接続のプロパティ.	903
第 231 章 : Workday 接続のプロパティ.	905
第 232 章 : Workday Mass Ingestion 接続のプロパティ.	906
第 233 章 : Workday V2 接続のプロパティ.	908
Workday への接続.	908
接続の詳細.	908
詳細設定.	909
第 234 章 : Xactly 接続のプロパティ.	910
第 235 章 : Xero 接続のプロパティ.	911
第 236 章 : XML ソース接続のプロパティ.	913
第 237 章 : XML ターゲット接続のプロパティ.	914
第 238 章 : Yellowbrick Data Warehouse の接続プロパティ.	915
第 239 章 : Zendesk 接続のプロパティ.	917

第 240 章 : Zendesk Mass Ingestion 接続のプロパティ	918
第 241 章 : Zendesk V2 接続のプロパティ	919
認証の準備.....	919
基本認証.....	919
API トークン認証.....	919
OAuth 2.0 クライアント資格情報認証.....	919
Zendesk への接続.....	920
始める前に.....	920
接続の詳細.....	920
認証タイプ.....	921
Zendesk のカスタムフィールド.....	923
プロキシサーバーの設定.....	924
第 242 章 : Zuora AQuA の接続プロパティ	926
Zuora への接続.....	926
始める前に.....	926
接続の詳細.....	926
詳細設定.....	927
第 243 章 : Zuora 接続のプロパティ	928
第 244 章 : Zuora REST V2 接続のプロパティ	929
索引	931

序文

『*Informatica Intelligent Cloud ServicesSM 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 マーケットプレイス

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

<https://marketplace.informatica.com/>

データ統合のコネクタのドキュメント

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

Informatica ナレッジベース

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

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

Informatica Intelligent Cloud Services Trust Center

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

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

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

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

Informatica グローバルカスタマサポート

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

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

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

第 1 章

コネクタと接続

接続は、クラウドとオンプレミスのアプリケーション、プラットフォーム、データベース、およびフラットファイルのデータへのアクセスを提供します。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るには、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えるようになります。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。

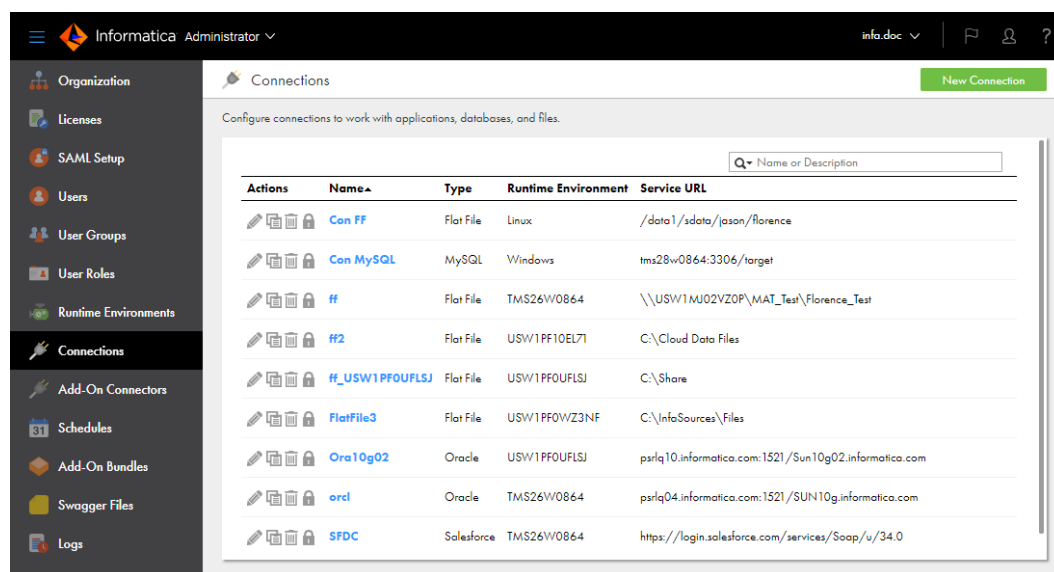
第 2 章

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、接続を作成できます。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できます。

次の図は、【接続】 ページを示しています。



接続を設定する際には、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。接続内のランタイム環境は、マッピングタスクまたはマッピングタスクから上書きできます。

ランタイム環境により、Informatica Intelligent Cloud Services と接続エンドポイント間の接続を管理します。これは、次のようなタスクを実行する場合に役立ちます。

- エンドポイントへの接続をテストする。
- アセットで接続を使用するときに、接続に使用できるオブジェクトを表示し、メタデータを取得する。アセットで選択したソース、ターゲット、またはルックアップオブジェクトのデータをプレビューできます。
- 接続を使用してソースからの読み取り、データの変換、またはターゲットへのデータの書き込みを行うアセットを実行する。

データベース、クラウドデータウェアハウス、またはその他のエンドポイントタイプへの接続を設定することができます。データベースまたはクラウドデータウェアハウスへのソース接続またはターゲット接続を作成する場合は、テーブル、エイリアス、またはビューに接続します。例えば、Snowflake Data Cloud 接続を作成

する場合は、Snowflake テーブルまたはビューに接続します。さまざまなタイプのエンドポイントへの接続の作成の詳細については、該当するコネクタのヘルプを参照してください。

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際に接続でコードページを指定する必要がある場合は、コードページが同一のものであることを確認してください。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できます。

接続の設定

Informatica Intelligent Cloud Services にインストールされているコネクタに対する接続を作成できます。接続は、管理者の **【接続】** ページで作成するか、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作成するときに作成できます。

接続を設定する際に、接続の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。

注: 外部シークレットマネージャから機密性の高い接続資格情報を取得するように設定されている一部の組織では、データ統合で接続を作成または編集することはできません。これらの組織では、管理者で接続を作成する必要があります。管理者での接続の設定の詳細については、「**組織管理**」を参照してください。

1. 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。

2. 組織が外部シークレットマネージャを使用して機密性の高い接続資格情報を保存する場合は、次の手順を実行します。
 - a. **【接続プロパティ】** 領域で、**【シークレットコンテナの使用】** を選択します。
 - b. シークレットマネージャに保存するそれぞれのプロパティの横にあるオプションを有効にし、対応するフィールドにシークレット名を含めたパスを入力します。シークレットが JSON オブジェクトの場合は、シークレットキーも含める必要があります。

次の表は、シークレットの形式に応じて入力する値を示しています。

シークレットの形式	入力する値の形式
次のような JSON オブジェクト <pre>{ "engine": "mysql", "username": "tsmith", "password": "Hello123", "host": "my-database- endpoint.us- west-2.rds.amazonaws.com", "dbname": "myDatabase", "port": "1234" }</pre>	<code><secret_path>:<key></code> または、AWS Secrets Manager を使用する場合は、シークレットの完全な ARN を次の形式で入力できます*。 <code>arn:aws:secretsmanager:<region>:<account_ID>:secret:<secret_name>-<6_random_characters>:<secret_path></code>
次のような単純な値 <pre>--name "MyPassword" -- value "Hello123"</pre>	<code><secret_path></code> または、AWS Secrets Manager を使用する場合は、シークレットの完全な ARN を次の形式で入力できます*。 <code>arn:aws:secretsmanager:<region>:<account_ID>:secret:<secret_name>-<6_random_characters></code>
* AWS Secrets Manager を使用しており、Secure Agent をホストするアカウントがシークレットをホストするアカウントと異なる場合は、シークレットの完全な ARN を入力する必要があります。	

例えば、リレーショナル接続を設定し、データベースのパスワードを HashiCorp Vault に保存とします。シークレットへのパスは `secret/data/MyCredentials` で、シークレットキーは `MyPassword` です。HashiCorp Vault からパスワードを取得するには、**【シークレットコンテナの使用】** を選択し、**【パスワード】** フィールドの横にあるオプションを有効にして、**【パスワード】** フィールドに「`secret/data/MyCredentials:MyPassword`」と入力します。

次の図は、接続の詳細を示しています。

Configure Connection : SQL Server
 Follow the setup guide on the right to configure the connection : ☒ Use Secret Vault

Runtime Environment: *

SQL Server Version: *

Authentication Mode: *

User Name: *

Password: * ☒

Host: *

Port: *

注: 2025 年 7 月リリースでは、組織でシークレットマネージャを使用している場合に、データ統合で接続を作成する機能をプライベートプレビューで利用できるようになりました。プレビュー機能は評価を目的としてサポートされていますが、保証対象外で、本番環境または本番環境にプッシュする予定の環境には対応していません。Informatica は、本番環境用の今後のリリースにプレビュー機能を含める予定ですが、市場や技術的な状況の変化に応じて導入を行わ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。

3. 接続で使用するランタイム環境を選択します。

外部シークレットマネージャを使用する場合は、ランタイム環境内のすべての Secure Agent がローカルマシンまたは VM にインストールされており、シークレットマネージャにアクセスできる必要があります。さらに、SecretManagerApp サービスが各エージェントで実行されている必要があります。

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、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。

5. 接続をテストするには、**[テスト接続]** をクリックします。
6. **[保存]** をクリックします。

サンプルデータを使用した接続の設定

サンプルデータを使用するように接続を設定できます。組織のデータに影響を与えずにマッピングをテストする場合は、サンプルデータを使用することをお勧めします。

サンプルデータを使用するように接続を設定する場合は、Snowflake、Google BigQuery、Salesforce などのさまざまなコネクタタイプからモックコネクタを選択できます。接続プロパティはすでに設定されています。

1. **[新しい接続]** ページで、**[サンプルデータ]** を選択します。
2. 接続に使用するモックコネクタを選択し、**[OK]** をクリックします。

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。

ff_USW1PFOUFLSJ Dependencies

UsesUsed By

Used By (8)

Name	Type	Location	Updated By	Status
m_FilterCust	Mapping	Default	ltroy05	Valid
m_FilterCust - Copy 1	Mapping	Default	rlannan05	Valid
m_FilterCust - Copy 1 - Copy 1	Mapping	Default	rlannan05	Valid
Mapping2	Mapping	Default	jrandolp05	Valid
MappingTask1	Mapping Task	Default	jrandolp05	Invalid
MappingTask2	Mapping Task	Default	jrandolp05	Valid
mt_FilterCust	Mapping Task	Default	ltroy05	Valid
Synchronization Task1	Synchronization Task	Default	jrandolp05	Valid

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

ActiveCampaign 接続プロパティ

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

次の表に、ActiveCampaign 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。
シークレットコンテナの使用	組織に対して設定されている Secrets Manager にこの接続の機密資格情報を保存します。 このプロパティは、組織に Secrets Manager が設定されている場合にのみ表示されます。 このプロパティは、データ取り込みおよびレプリケーションとデータアクセス管理サービスではサポートされていません。 接続でシークレットコンテナを有効にすると、Secure Agent が Secrets Manager からどの資格情報を取得するかを選択できます。このオプションを無効にした場合、資格情報は組織の設定方法に応じてリポジトリまたはローカル Secure Agent に保存されます。 注: この接続を使用してプッシュダウンまたはプロキシサービスを介してデータアクセスポリシーを適用する場合、シークレットコンテナ設定オプションを使用することはできません。 Secrets Manager を設定および使用する方法については、Administrator のヘルプにある「Secrets Manager の設定」を参照してください。
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。 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。 ランタイム環境の設定および使用方法の詳細については、Administrator のヘルプにある「ランタイム環境」を参照してください。
API のベース URL	ActiveCampaign アプリケーションに接続するためのベース URL。 例: https://youraccountname.api-us1.com
API トークン	トークンベースの認証を使用して ActiveCampaign アカウントにアクセスするための API トークン。

第 4 章

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。
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gger（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。 <i>host_name</i> は、ホスト名または IP アドレスにできます。 <i>host_name:port_number</i> 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	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gger（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	<p>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。</p> <ul style="list-style-type: none"> - 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。 <p>デフォルトは【なし】です。</p>
ペーシングサイズ	<p>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。</p> <p>デフォルトである最小値は 0 です。</p>
ペーシング単位	<p>【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。</p> <p>【行】 または 【キロバイト】 のいずれかを選択します。</p>
マップの場所	<p>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。</p> <p>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。</p> <p>次の形式で値を入力します。<i>host_name</i> は、ホスト名または IP アドレスにできます。</p> <p><i>host_name:port_number</i></p> <p>以下に例を示します。</p> <p>ADACDC01:25100</p> <p>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。</p>
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。

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	<p>カスタムプロパティまたは接続プロパティのオーバーライド。カスタムプロパティとは、PowerExchange のデフォルトの設定よりも優先するために指定できるプロパティです。セミコロン (;) を区切り文字として使用して複数のプロパティを入力するか、パラメータファイルを使用して接続プロパティの上書きを指定するパラメータを指定することができます。</p> <p>例:</p> <pre><property>=<value>;<property>=<value></pre> <p>多くの場合、Informatica グローバルカスタマサポートからの指示を受けたいので、カスタムプロパティの設定を行います。</p> <p>注: これらのプロパティは、PowerCenter の PowerExchange Client for PowerCenter (PWXPC) CDC 接続の【PWX オーバーライド】オプションと同じです。</p> <p>パラメータファイルを使用して接続プロパティのオーバーライドを指定するには、\$<ParameterName>の形式でパラメータを設定し、ユーザー定義パラメータ名の前にドル記号 (\$) を付けます。次に、【ランタイムオプション】タブの【パラメータファイル名】フィールドにパラメータファイル名を指定することで、ユーザー定義パラメータ定義を含むパラメータファイルを使用するようにマッピングのマッピングタスクを設定します。</p> <p>注:</p> <ul style="list-style-type: none"> - マッピングおよび接続に同じパラメータを入力した場合は、接続カスタムプロパティが優先されます。 - パラメータファイルがある場合、このフィールドで指定するパラメータ名は、パラメータファイルで定義されたエントリと一致する必要があります。 <p>詳細については、「接続オーバーライドのリファレンス」の章を参照してください。</p>

第 5 章

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。
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 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。 <i>host_name</i> は、ホスト名または IP アドレスにできます。 <i>host_name:port_number</i> 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。

プロパティ	説明
オフロード処理	<p>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。</p> <ul style="list-style-type: none"> - 自動。オフロード処理を使用するかどうか 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。 <p>デフォルトは「いいえ」です。</p>
オフロードスレッド	<p>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。</p> <p>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。</p> <p>有効な値は 1～64 です。</p> <p>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。</p> <p>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。</p>
配列サイズ	<p>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）。</p> <p>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。</p> <p>有効な値は 1～5000 です。デフォルトは 25 です。</p> <p>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。</p>
低値をスペースに置き換える	<p>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。</p>
接続リトライ期限	<p>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。</p>

プロパティ	説明
カスタムプロパティ	<p>カスタムプロパティまたは接続プロパティのオーバーライド。カスタムプロパティとは、PowerExchange のデフォルトの設定よりも優先するために指定できるプロパティです。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。</p> <p>例:</p> <pre><property>=<value>;<property>=<value></pre> <p>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。</p> <p>注: これらのプロパティは、PowerCenter の PowerExchange Client for PWX NRDB Batch 接続の 【PWX オーバーライド】 オプションと同じです。</p> <p>また、このフィールドまたはパラメータファイルを使用して、接続プロパティのオーバーライドを指定することもできます。パラメータファイルを使用して接続プロパティのオーバーライドを指定するには、\$<ParameterName>の形式でパラメータを設定し、ユーザー定義パラメータ名の前にドル記号 (\$) を付けます。次に、【ランタイムオプション】 タブの 【パラメータファイル名】 フィールドにパラメータファイル名を指定することで、ユーザー定義パラメータ定義を含むパラメータファイルを使用するようにマッピングのマッピングタスクを設定します。</p> <p>注:</p> <ul style="list-style-type: none"> - マッピングおよび接続に同じパラメータを入力した場合は、接続カスタムプロパティが優先されます。 - パラメータファイルがある場合、このフィールドで指定するパラメータ名は、パラメータファイルで定義されたエントリと一致している必要があります。 <p>詳細については、「接続オーバーライドのリファレンス」の章を参照してください。</p>
書き込みモード	<p>次のオプションがあります。</p> <ul style="list-style-type: none"> - 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。 <p>デフォルト値は 【書き込み確認オン】 です。</p>

第 6 章

Adaptive Insights 接続プロパティ

接続は、**【接続】** ページで作成するか、タスクの作成時に作成できます。Adaptive Insights 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。接続を作成すると、組織へのアクセス権を持つすべてのユーザーがその接続を使用できるようになります。

次の表に、Adaptive Insights 接続のプロパティを示します。

接続属性	説明
ユーザー名	必須。登録されたユーザーのユーザー名。
パスワード	必須。ユーザーが設定したパスワード。
ロケール	オプション。システム応答メッセージが表示される言語。また、受信および送信される数値と日付を解釈し、書式を設定するために使用されます。
インスタンスコード	必須。このコードは、特定のユーザーがデフォルトのインスタンスを介してログインしているか、別のインスタンスを介してログインしているかを示します。デフォルト値は <code>https://api.AdaptiveInsights.com/v1.svc</code> です
開始日	オプション。Secure Agent がデータを読み取る必要がある範囲属性の開始日を示します。
終了日	オプション。Secure Agent がデータを読み取る必要がある範囲属性の終了日を示します。
ディメンション	オプション。データの各行がグループ化され、特定のディメンションタグに対してエクスポートされるディメンションを示します。

第 7 章

Adobe Analytics 接続のプロパティ

Adobe Analytics 接続を作成する際に、接続プロパティを設定します。

次の表に、Adobe Analytics 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。
シークレットコンテナの使用	組織に対して設定されている Secrets Manager にこの接続の機密資格情報を保存します。 このプロパティは、組織に Secrets Manager が設定されている場合にのみ表示されます。 このプロパティは、データ取り込みおよびレプリケーションとデータアクセス管理サービスではサポートされていません。 接続でシークレットコンテナを有効にすると、Secure Agent が Secrets Manager からどの資格情報を取得するかを選択できます。このオプションを無効にした場合、資格情報は組織の設定方法に応じてリポジトリまたはローカル Secure Agent に保存されます。 注: この接続を使用してプッシュダウンまたはプロキシサービスを介してデータアクセスポリシーを適用する場合、シークレットコンテナ設定オプションを使用することはできません。 Secrets Manager を設定および使用する方法については、Administrator のヘルプにある「Secrets Manager の設定」を参照してください。
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。 Secure Agent または Hosted Agent を指定できます。 ランタイム環境の設定および使用方法の詳細については、Administrator のヘルプにある「ランタイム環境」を参照してください。
クライアント ID	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	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
技術アカウント ID	サービスアカウントの技術アカウント ID。
組織 ID	サービスアカウントの組織 ID。
プライベートキー	サービスアカウント統合の設定時に生成されるプライベートキー。
IMS ホスト	Adobe Identity Management System のベース URL。
IMS 交換	Adobe Identity Management System の交換 URL。

第 8 章

Adobe Analytics Mass Ingestion 接続のプロパティ

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

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

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

接続プロパティ	説明
接続名	接続の名前。この名前は、組織内で一意にする必要があります。接続名には、英数字、スペース、および次のような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。
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とレプリケーションタスクを実行することはできません。
クライアント ID	Adobe Developer Console で作成したサービスアカウントのクライアント ID。
クライアントシークレット	Adobe Developer Console で作成したサービスアカウントのクライアントシークレット。
テクニカルアカウント ID	サービスアカウントのテクニカルアカウント ID。
組織 ID	サービスアカウントの組織 ID。
秘密鍵	サービスアカウント統合を作成するときに生成される秘密鍵。JWT を生成するには、秘密鍵が必要です。

接続プロパティ	説明
IMS ホスト	<p>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。</p> <p><code>ims-na1.adobelogin.com</code></p>
IMS 交換	<p>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。</p> <p><code>https://ims-na1.adobelogin.com/ims/exchange/jwt</code></p>

第 9 章

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。

重要: Adobe Experience Platform コネクタは非推奨となり、メンテナンスモードに移行されました。Informatica は将来のリリースでサポートを廃止する予定です。

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。
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。

第 10 章

高度な FTP 接続のプロパティ

高度な FTP 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、高度な FTP 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。
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は 21 になります。
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	高度な FTP 接続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。 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。 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。そのため、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。
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、デフォルトのタイムアウトは 120 秒になります。

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 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 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。
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 接続は 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。

第 11 章

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。
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	<p>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。</p> <p>デフォルト値は 【はい】 です。</p> <p>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。</p> <p>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。</p>

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

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

第 12 章

高度な FTPS 接続のプロパティ

高度な FTPS 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、高度な FTPS 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。
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。 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。 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。そのため、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。
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、デフォルトのタイムアウトは 120 秒になります。

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 FTPS 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。FTPS 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、高度な FTPS 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。

第 13 章

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。
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	<p>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。</p> <p>デフォルト値は 【はい】 です。</p> <p>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。</p> <p>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。</p>

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 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。 <ul style="list-style-type: none"> - 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。

接続プロパティ	説明
キーストアファイル	キーストアファイルのパスおよびファイル名。キーストアファイルには、FTPS サーバーを認証するための証明書が含まれます。
キーストアのパスワード	信頼済みサーバーの証明書ストアにアクセスするために必要なキーストアファイルのパスワード。
キーエイリアス	個別のキーのエイリアス。
キーストアタイプ	キーストアのタイプが Java KeyStore (JKS) または Public Key Cryptology Standard (PKCS12) のどちらであるかを指定します。 デフォルトは JKS です。
帯域幅	ファイル転送に使用されるネットワークリソースの最大量を制御します。この値は、ファイルのアップロードとダウンロードに適用されます。デフォルトは 0 です。0 は帯域幅が制限されていないことを示します。
帯域幅単位	ファイル転送に使用されるネットワーク帯域幅の単位。以下のいずれかの単位を選択することができます。 <ul style="list-style-type: none"> - キロバイト/秒 (KBps) - メガバイト/秒 (MBps)

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

第 14 章

高度な SFTP 接続のプロパティ

高度な SFTP 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、高度な 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	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、デフォルトのタイムアウトは 120 秒になります。
接続の再試行	接続を確立できない場合に SFTP 接続の再試行のために接続する回数。この設定は、最初の接続と接続の切断による再接続の試行の両方に使用されます。空白のままにすると、再試行は行われません。
接続再試行の間隔	接続の再試行ごとに待機する秒数。 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。

第 15 章

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。
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。ホスト名は大文字と小文字が区別されません。また、ホスト名はドメイン内で一意である必要があります。名前は 24 文字を超えることはできません。文字 (A から Z)、数字 (0 から 9)、ピリオド (.)、特殊文字、およびマイナス (-) 記号を含めることができます。
ポート	サーバーへの接続に使用するポート番号。デフォルトは 21 です。
ユーザー名	SFTP サーバーに接続するためのユーザー名。
パスワード	SFTP サーバーに接続するためのパスワード。
フォルダパス	サーバーへの接続後に使用するディレクトリ。
タイムアウト	サーバーへの接続を試行するときに待機する秒数。指定した時間内に接続を確立できない場合、タイムアウトになります。空白のままにすると、デフォルト値の 120 秒が使用されます。
接続の再試行	接続を確立できない場合に SFTP 接続の再試行のために接続する回数。この設定は、最初の接続と接続の切断による再接続の試行の両方に使用されます。空白のままにすると、再試行は行われません。
接続再試行の間隔	接続の再試行ごとに待機する秒数。 例えば、再試行ごとに 5 秒間空けて最大 10 回接続しようとする場合は、接続の再試行回수에 10 を指定し、接続再試行の間隔に 5 を指定します。

接続プロパティ	説明
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。
帯域幅	ファイル転送に使用されるネットワークリソースの最大量を制御します。この値は、ファイルのアップロードとダウンロードに適用されます。デフォルトは 0 です。0 は帯域幅が制限されていないことを示します。
帯域幅単位	ファイル転送に使用されるネットワーク帯域幅の単位。以下のいずれかの単位を選択することができます。 <ul style="list-style-type: none"> - キロバイト/秒 (KBps) - メガバイト/秒 (MBps)
ファイル統合プロキシサーバーの使用	コネクタは、ファイル統合プロキシサーバー経由で SFTP サーバーに接続します。 次の前提条件が満たされていることを確認してください。 <ul style="list-style-type: none"> - このオプションを使用するには、ファイル統合サービスのライセンスが必要です。 - ファイルサーバーでプロキシサーバーを定義する必要があります。 - ファイル統合サービスプロキシがない場合は、proxy.ini ファイル経由でエージェントプロキシを使用する必要があります。
プロキシサーバーのホスト名	送信ファイル統合サービスプロキシサーバーのホスト名または IP アドレス。
プロキシサーバーのポート	送信ファイル統合サービスプロキシサーバーのポート番号。

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

第 16 章

Amazon Athena 接続のプロパティ

Amazon Athena から読み取りを行うための Amazon Athena 接続を作成します。

認証の準備

永続的な IAM 資格情報認証タイプ、EC2 インスタンスプロファイル認証タイプ、ロールを引き受けるための EC2 ロール認証タイプを設定して、Amazon Athena にアクセスすることができます。

永続的な IAM 資格情報認証を使用するには、AWS コンソールで IAM ユーザーを作成し、必要なポリシーをアタッチして、アクセスキーとシークレットキーを生成します。これらの詳細は、接続プロパティで使用できるように手元に用意しておいてください。

EC2 インスタンスプロファイル認証を使用するには、EC2 インスタンスに Secure Agent をインストールし、EC2 ロールを EC2 インスタンスにアタッチします。

別の IAM ロールを引き受けるように EC2 ロールを設定するには、EC2 インスタンスに Secure Agent をインストールし、EC2 ロールを EC2 インスタンスにアタッチして、EC2 ロールが IAM ロール ARN で指定された別の IAM ロールを引き受けられるようにします。

接続プロパティを設定する前に、最小限の Amazon S3 ポリシー、AWS Glue データカタログポリシー、および Amazon Athena ポリシーを作成します。ポリシーで IAM ユーザーまたは EC2 ロールに必要な権限を定義します。

設定する認証タイプに基づいて、ポリシーを IAM ユーザーまたは EC2 ロールにアタッチします。

Amazon S3 ポリシーの作成

AWS コンソールで Amazon S3 ポリシーを作成して、Amazon Athena の結果を Amazon S3 に保存するための権限を定義します。

Amazon Athena の結果を Amazon S3 に保存するには、次のような、必要な最小の権限を使用します。

- PutObject
- GetObject
- DeleteObject
- ListBucket
- GetBucketLocation

- ListAllMyBuckets
- GetBucketAcl

次のサンプル Amazon S3 ポリシーを使用できます。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": [
        "s3:PutObject",
        "s3:GetObject",
        "s3:ListBucket",
        "s3:DeleteObject"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:ListBucket",
        "s3:GetBucketLocation",
        "s3:ListAllMyBuckets",
        "s3:GetBucketAcl"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

AWS Glue データカタログポリシーの作成

AWS IAM を使用して、AWS Glue が使用するリソースにアクセスするためのポリシーとロールを定義できます。

Amazon Athena は、AWS Glue Data Catalog を使用して、AWS アカウントの Amazon S3 データのテーブルメタデータを保存および取得します。

AWS Glue Data Catalog には次のサンプルポリシーを使用できます。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "glue:*"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

Amazon Athena ポリシーの作成

AWS Glue データカタログのビューと外部テーブルからデータを読み取り、Amazon S3 ファイルを読み取ってクエリするために Amazon Athena コネクタに必要な最小の権限を指定します。

次のような、必要な最小の権限を使用できます。

- GetWorkGroup

- GetTableMetadata
- StartQueryExecution
- GetQueryResultsStream
- ListDatabases
- GetQueryExecution
- GetQueryResults
- GetDatabase
- ListTableMetadata
- GetDataCatalog
- CreatePreparedStatement
- DeletePreparedStatement

Amazon Athena には次のサンプルポリシーを使用できます。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "athena:GetWorkGroup",
        "athena:GetTableMetadata",
        "athena:StartQueryExecution",
        "athena:GetQueryResultsStream",
        "athena:ListDatabases",
        "athena:GetQueryExecution",
        "athena:GetQueryResults",
        "athena:GetDatabase",
        "athena:ListTableMetadata",
        "athena:GetDataCatalog",
        "athena:CreatePreparedStatement",
        "athena>DeletePreparedStatement"
      ],
      "Resource": [
        "arn:aws:athena:*:*:workgroup/*",
        "arn:aws:athena:*:*:datacatalog/*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "athena:ListDataCatalogs",
        "athena:ListWorkGroups"
      ],
      "Resource": "*"
    }
  ]
}
```

ルールを引き受けるための EC2 ロールの設定

EC2 ロールを設定して IAM ロールを引き受け、一時的なセキュリティ資格情報を生成して、同じ AWS アカウントまたは異なる AWS アカウントの Amazon Athena に接続することができます。

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

ルールを引き受けるように EC2 ロールを設定する場合は、一時的なセキュリティ資格情報を使用するための **sts:AssumeRole** 権限が割り当てられており、AWS アカウント内で信頼関係が確立されていることを確認して

ください。信頼関係は、ロールを作成するときに、IAM ロールの信頼ポリシーで定義されます。IAM ロールにより、EC2 ロールを信頼されたエンティティとして追加し、EC2 ロールに一時的なセキュリティ資格情報の使用と AWS アカウントへのアクセスを許可します。

信頼された EC2 ロールが一時的なセキュリティ資格情報を要求すると、AWS Security Token Service (AWS STS) によって、指定した期間有効な一時的なセキュリティ資格情報が動的に生成され、信頼された EC2 ロールにその資格情報が提供されます。

ロールを引き受けるための EC2 ロール認証を使用する前に、次の前提条件を考慮してください。

- AWS EC2 インスタンスに Secure Agent をインストールします。
- AWS EC2 インスタンスにアタッチされた EC2 ロールには Amazon Athena へのアクセス権は必要ありませんが、別の IAM ロールを引き受ける権限が割り当てられている必要があります。
以下は、EC2 ロールが別の IAM ロールを引き受けることを許可する、EC2 ロールにアタッチされた信頼ポリシーの例です。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Statement1",
      "Effect": "Allow",
      "Action": "sts:AssumeRole",
      "Resource": "arn:aws:iam::001234567890:role/aws_athena_assumeRole"
    }
  ]
}
```

- EC2 ロールが引き受ける必要のある IAM ロールには、Amazon Athena にアクセスするための権限ポリシーと信頼ポリシーがアタッチされている必要があります。

信頼ポリシーには、EC2 ロールの ARN が含まれている必要があります。

また、AWS アカウントの外部 ID を指定して、Amazon Athena へのより安全なアクセスを行うこともできます。外部 ID は文字列である必要があります。

次のサンプルは、EC2 ロールの ARN と外部 ID を使用した、引き受けた IAM ロールの信頼ポリシーを示しています。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::001234567890:root" //anyone in this account 001234567890 can assume
this role, this can also be limited to one role.
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "sts:ExternalId": "athena_externalid"
        }
      }
    }
  ]
}
```

注: Amazon Athena 接続を設定するときは、EC2 ロールが引き受ける IAM ロールの ARN を指定する必要があります。必要に応じて、Amazon Athena へのより安全なアクセスのために外部 ID を指定できます。

Amazon Athena への接続

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

始める前に

開始する前に、設定する認証タイプに基づいて Amazon Athena アカウントから情報を取得する必要があります。

永続的な IAM 資格情報認証を設定するには、アクセスキーとシークレットキーを取得します。

EC2 インスタンスプロファイル認証を設定するには、EC2 インスタンスをセットアップし、EC2 ロールを EC2 インスタンスにアタッチします。

別の IAM ロールを引き受けるように EC2 を設定するには、EC2 インスタンスを設定し、EC2 ロールを EC2 インスタンスにアタッチして、EC2 ロールが IAM ロール ARN で指定された別の IAM ロールを引き受けられるようにします。

選択した認証方法に応じて、適切なポリシーを IAM ユーザーまたは EC2 ロールにアタッチします。

認証の前提条件の詳細については、「[認証の準備](#)」(ページ 64)を参照してください。

接続の詳細

次の表に、基本接続プロパティを示します。

プロパティ	説明
接続名	接続の名前。 各接続名は組織内で一意である必要があります。接続名には、英数字、スペース、および次の特殊文字を含めることができます。_ . + - , 最大長は 255 文字です。
説明	接続の説明。最大長は 4000 文字です。
シークレットコンテナの使用	組織に対して設定されている Secrets Manager にこの接続の機密資格情報を保存します。 このプロパティは、組織に Secrets Manager が設定されている場合にのみ表示されます。 このプロパティは、データ取り込みおよびレプリケーションとデータアクセス管理サービスではサポートされていません。 接続でシークレットコンテナを有効にすると、Secure Agent が Secrets Manager からどの資格情報を取得するかを選択できます。このオプションを無効にした場合、資格情報は組織の設定方法に応じてリポジトリまたはローカル Secure Agent に保存されます。 注: この接続を使用してプッシュダウンまたはプロキシサービスを介してデータアクセスポリシーを適用する場合、シークレットコンテナ設定オプションを使用することはできません。 Secrets Manager を設定および使用方法については、Administrator のヘルプにある「Secrets Manager の設定」を参照してください。
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。 Secure Agent、ホステッドエージェント、サーバーレスランタイム環境、またはエラスティックランタイム環境を選択します。 ランタイム環境の設定および使用方法の詳細については、Administrator のヘルプにある「ランタイム環境」を参照してください。

認証タイプ

永続的な IAM 資格情報認証タイプ、EC2 インスタンスプロファイル認証タイプ、およびロールを引き受けるための EC2 ロール認証タイプを設定して、Amazon Athena にアクセスすることができます。

永続的な IAM 資格情報

永続的な IAM 資格情報認証は、Amazon Athena に接続するために IAM ユーザーのアクセスキーとシークレットキーを必要とするデフォルトのタイプです。

次の表に、永続的な IAM 資格情報認証の基本的な接続プロパティとその説明を示します。

プロパティ	説明
アクセスキー	Amazon Athena に接続するための IAM ユーザーのアクセスキー。
秘密鍵	Amazon Athena に接続するための IAM ユーザーのシークレットキー。
JDBC URL	Amazon Athena に接続するための URL。 JDBC URL は次の形式で入力します。 <code>jdbc:awsathena://</code> <code>AwsRegion=<region_name>;S3OutputLocation=<S3_Output_Location>;Workgroup=<Workgroup_Name>;</code> 注: ユーザー管理クエリの結果を含むワークグループを使用する場合は、JDBC URL に 2 つのパラメータのうち少なくとも 1 つ (S3 の出力場所またはワークグループ名) を指定します。Athena の管理クエリの結果を含むワークグループの場合は、ワークグループ名のみを指定し、JDBC URL に S3 出力場所を含めないこと。

EC2 インスタンスプロファイル

Secure Agent が Amazon Elastic Compute Cloud (EC2) システムにインストールされている場合に、Amazon Athena に接続するように AWS Identity and Access Management (IAM) 認証を設定できます。

次の表に、EC2 インスタンスプロファイル認証の基本的な接続プロパティとその説明を示します。

プロパティ	説明
JDBC URL	Amazon Athena 接続の URL。 JDBC URL は次の形式で入力します。 <code>jdbc:awsathena://</code> <code>AwsRegion=<region_name>;S3OutputLocation=<S3_Output_Location>;Workgroup=<Workgroup_Name>;</code> 注: ユーザー管理クエリの結果を含むワークグループを使用する場合は、JDBC URL に 2 つのパラメータのうち少なくとも 1 つ (S3 の出力場所またはワークグループ名) を指定します。Athena の管理クエリの結果を含むワークグループの場合は、ワークグループ名のみを指定し、JDBC URL に S3 出力場所を含めないこと。

ルールを引き受けるための EC2 ロール

IAM ロールを引き受け、Amazon Athena に接続するための一時的なセキュリティ資格情報を生成するように EC2 ロールを設定できます。

次の表に、ロールを引き受けるための EC2 ロール認証の基本的な接続プロパティとその説明を示します。

プロパティ	説明
JDBC URL	Amazon Athena に接続するための URL。 JDBC URL は次の形式で入力します。 <code>jdbc:awsathena://</code> <code>AwsRegion=<region_name>;S3OutputLocation=<S3_Output_Location>;Workgroup=<Workgroup_Name>;</code> 注: ユーザー管理クエリの結果を含むワークグループを使用する場合は、JDBC URL に 2 つのパラメータのうち少なくとも 1 つ (S3 の出力場所またはワークグループ名) を指定します。Athena の管理クエリの結果を含むワークグループの場合は、ワークグループ名のみを指定し、JDBC URL に S3 出力場所を含めないこと。
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 EC2 ロールが引き受ける AWS Identity and Access Management (IAM) ロールの Amazon Resource Name (ARN)。

詳細設定

次の表に、詳細接続のプロパティを示します。

プロパティ	説明
顧客マスターキー ID	AWS Key Management Service (AWS KMS) によって生成された顧客マスターキー ID、または Amazon S3 でデータをステージングする場合のアカウント間アクセス用のカスタムキーの ARN。 顧客マスターキーは、Amazon S3 への保存前にコピー先でデータを暗号化します。顧客が生成した顧客マスターキー ID またはデフォルトの顧客マスターキー ID を入力することができます。 Amazon S3 バケットが存在するリージョンと同じリージョンの顧客マスターキーを生成するようにしてください。 Amazon Athena での顧客マスターキーの使用の詳細については、AWS ドキュメントの「 Encryption 」を参照してください。
外部 ID	IAM ロールに関連付けられた外部 ID。 外部 ID は、sts:AssumeRole API を呼び出すときに IAM ロールが EC2 ロールに指定する必要がある一意のユーザー定義の文字列値です。

プロキシサーバーの設定

組織が送信プロキシサーバーを使用してインターネットに接続している場合、サーバーレスランタイム環境を使用して、プロキシサーバー経由で Informatica Intelligent Cloud Services に接続できます。

認証されていないプロキシサーバーまたは認証されたプロキシサーバーを使用できます。

サーバーレスランタイム環境のプロキシを設定するには、Administrator のヘルプの「ランタイム環境」を参照してください。

Amazon Athena のワークグループ

Amazon Athena のワークグループを使用して、さまざまなユーザー、チーム、またはアプリケーションのクエリを分離して管理できます。クエリの処理方法と結果の保存方法を制御するには、S3 のデフォルトの出力場所や暗号化オプションなどの特定の設定で各ワークグループを設定します。

Amazon Athena 接続を作成するとき、Amazon Athena JDBC URL 内にワークグループを指定できます。

Amazon Athena のワークグループを使用するときには、次のガイドラインを参照してください。

- ユーザー管理クエリの結果を含むワークグループを使用する場合、クエリのストレージを管理し、必要な期間、結果を保持します。

ユーザー管理クエリの結果を含むワークグループを使用するには、JDBC URL 内に 2 つのパラメータのうち少なくとも 1 つ（クエリ結果を保存する S3 出力場所、または事前設定されたデフォルトの S3 出力場所が設定されているワークグループの名前）を指定する必要があります。

JDBC URL で指定された S3 の出力場所と暗号化設定をオーバーライドするには、Amazon Athena でユーザー管理クエリの結果を含むワークグループを作成するときに、**[Override client-side settings]** プロパティを有効化します。

- Athena の管理クエリの結果を含むワークグループを使用すると、Amazon Athena はクエリのストレージを管理し、クエリ結果を 24 時間保持します。

Athena の管理クエリの結果を含むワークグループを使用する場合は、ワークグループ名のみを指定し、JDBC URL に S3 出力場所を含めないこと。

第 17 章

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。

重要: Amazon Aurora コネクタは非推奨となり、メンテナンスモードに移行されました。Informatica は将来のリリースでサポートを廃止する予定です。MySQL コネクタを使用して Amazon Aurora MySQL にアクセスすることをお勧めします。

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、ホステッドエージェント、またはエラスティックランタイム環境を選択します。 ランタイム環境の設定および使用方法の詳細については、Administrator のヘルプにある「ランタイム環境」を参照してください。
ホスト	Amazon Aurora サーバーのホスト名。 例: xyzcloud-cluster.cluster-cj8irztllmku.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。 <ul style="list-style-type: none">- 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

プロパティ	説明
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。

第 18 章

Amazon DynamoDB 接続のプロパティ

Amazon DynamoDB 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。

重要: Amazon DynamoDB コネクタは非推奨となり、メンテナンスモードに移行されました。Informatica は将来のリリースでサポートを廃止する予定です。

次の表に、Amazon DynamoDB 接続のプロパティを示します。

接続プロパティ	説明
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。 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。
リージョン	アカウントに関連付けられている AWS リージョン。

第 19 章

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。
シークレットコンテナの使用	組織に対して設定されている Secrets Manager にこの接続の機密資格情報を保存します。 このプロパティは、組織に Secrets Manager が設定されている場合にのみ表示されます。 このプロパティは、データ取り込みおよびレプリケーションとデータアクセス管理サービスではサポートされていません。 接続でシークレットコンテナを有効にすると、Secure Agent が Secrets Manager からどの資格情報を取得するかを選択できます。このオプションを無効にした場合、資格情報は組織の設定方法に応じてリポジトリまたはローカル Secure Agent に保存されます。 注: この接続を使用してプッシュダウンまたはプロキシサービスを介してデータアクセスポリシーを適用する場合、シークレットコンテナ設定オプションを使用することはできません。 Secrets Manager を設定および使用する方法については、Administrator のヘルプにある「Secrets Manager の設定」を参照してください。
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。 Secure Agent、またはサーバーレスランタイム環境を選択します。 ランタイム環境の設定および使用方法の詳細については、Administrator のヘルプにある「ランタイム環境」を参照してください。
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。

接続プロパティ	説明
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。
追加オプション	<p>Amazon DynamoDB との間でデータの読み取りまたは書き込みを行う場合に設定できる、キーと値のペア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には、キーと値のペアをアンパサンドで区切ります。例: propertyName1=<value1>&propertyName2=<value2></p> <p>次のパラメータを設定できます: prefixFieldNames=true。</p> <p>このパラメータをソース接続で設定すると、テーブルをインポートするときにすべてのカラムにアンダースコア文字がプレフィックスとして付加されます。このパラメータをターゲット接続で設定すると、すべてのターゲットカラムから最初の文字が削除されます。</p>

第 20 章

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。

プロパティ	説明
リージョン	<p>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。</p> <ul style="list-style-type: none"> - 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。 <p>ストリーミング取り込みとレプリケーションタスクは、ap-northeast-3 リージョンをサポートしていません。</p>
接続タイムアウト（ミリ秒）	<p>オプション。Kinesis Firehose への接続の確立がタイムアウトした後に、データ取り込みおよびレプリケーションサービスが接続の確立を待機する時間（ミリ秒）。</p> <p>デフォルトは 10,000 ミリ秒です。</p>
AWS 認証情報プロファイル名	<p>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。</p> <p>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。</p>
IAM ロールの ARN	<p>IAM ユーザーのロールを指定する Amazon リソースネーム。アカウント間の IAM ロール認証に適用されます。</p>
外部 ID	<p>IAM ロールの外部 ID は、IAM ロールを引き受けることができるユーザーを指定するために、IAM ロールの信頼ポリシーで使用する追加の制限です。アカウント間の IAM ロール認証に適用されます。</p>

Amazon Kinesis Streams 接続のプロパティ

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

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

プロパティ	説明
接続名	接続の名前。 この名前では、大文字と小文字が区別されず、ドメイン内で一意にする必要があります。 このプロパティは、接続を作成した後に変更できます。名前は 128 文字以内で指定し、空白および以下の特殊文字は使用できません。 ~ ` ! \$ % ^ & * () - + = { [] } \ : ; " ' < , > . ? /
説明	オプション。接続を識別するために使用できる説明。 説明は、4,000 文字を超える事は出来ません。
タイプ	Amazon Kinesis 接続タイプ。 Amazon Kinesis 接続タイプが見つからない場合は、[アドオンコネクタ] ページに移動し、コネクタをインストールしてください。
ランタイム環境	タスクを実行するランタイム環境の名前。
サービス	使用する Kinesis サービスのタイプ。[Kinesis Streams] を選択します。
AWS アクセスキー ID	Amazon AWS ユーザーアカウントのアクセスキー ID。
AWS シークレットアクセスキー	Amazon AWS ユーザーアカウントのシークレットアクセスキー。
リージョン	サービスのエンドポイントを利用できるリージョン。次の値から選択する事ができます。 <ul style="list-style-type: none">- 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とレプリケーションタスクは、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。Kinesis Streams への接続の確立がタイムアウトした後に、データ取り込みおよびレプリケーションサービスが接続の確立を待機する時間（ミリ秒）。デフォルトは 10,000 ミリ秒です。
AWS 認証情報プロファイル名	認証情報ファイル内で定義された AWS 認証情報プロファイル。 マッピングは実行時のプロファイル名を使用して AWS 認証情報にアクセスします。AWS 認証情報プロファイル名を指定しない場合、接続を作成するときに指定したアクセスキー ID とシークレットアクセスキーを使用します。
IAM ロールの ARN	IAM ユーザーのロールを指定する Amazon リソースネーム。アカウント間の IAM ロール認証に適用されます。
外部 ID	IAM ロールの外部 ID は、IAM ロールを引き受けることができるユーザーを指定するために、IAM ロールの信頼ポリシーで使用する追加の制限です。アカウント間の IAM ロール認証に適用されます。

第 21 章

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。

重要: Amazon Redshift コネクタは非推奨となり、メンテナンスモードに移行されました。Informatica は将来のリリースでサポートを廃止する予定です。Amazon Redshift V2 コネクタを使用して Amazon Redshift にアクセスすることをお勧めします。

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	<p>[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。</p> <p>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。</p>

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。

第 22 章

Amazon Redshift V2 接続のプロパティ

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

認証の準備

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

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

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

認証の前提条件

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

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

デフォルト認証	引き受けロールによる Redshift IAM 認証
<ul style="list-style-type: none">- JDBC URL- ユーザー名- パスワード	<ul style="list-style-type: none">- JDBC URL- ユーザー名- データベース名- クラスタ識別子- Redshift IAM ロール ARN*
<p>*Redshift IAM ロール ARN を使用するには、必要な信頼ポリシーを使用して Redshift IAM ロール ARN を設定し、Amazon Redshift にアクセスするための一時的なセキュリティ資格情報を生成します。</p> <p>詳細については、「Amazon Redshift の引き受けロールの設定」 (ページ 86)を参照してください。</p>	

ステージングの前提条件

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

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

S3 ステージングオプション	タスク
S3 ステージングにアクセスするために S3 IAM ロールを引き受ける IAM ユーザーの一時的な資格情報を生成します。	AWS の設定 IAM ユーザーが S3 IAM ロールを引き受け、一時的な資格情報を生成できるようにします。 手順については、次の参考資料を参照してください。 - 「Amazon S3 ステージングに AssumeRole を使用した一時的なセキュリティ資格情報の生成」 (ページ 90) 。 - Using an assume role for Amazon S3 resources を参照してください。 Redshift V2 接続設定 - S3 IAM ロール ARN の値を入力します。 - [S3 アクセスキー ID] と [S3 シークレットアクセスキー] の値を入力します。
S3 ステージングにアクセスするために S3 IAM ロールを引き受ける EC2 インスタンスの一時的なセキュリティ資格情報を生成します。	AWS の設定 S3 IAM ロールを引き受けて S3 ステージング用の一時的な資格情報を生成するように EC2 インスタンスを定義します。 詳細については、 「EC2 に AssumeRole を使用した一時的なセキュリティ資格情報の生成」 (ページ 92) を参照してください。 Redshift V2 接続設定 次の最小限必要なプロパティを設定します。 - [ロールの引き受けに EC2 ロールを使用] を有効にします。 - S3 IAM ロール ARN の値を入力します。
S3 バケットへのアクセス権を持つ IAM ユーザーの S3 アクセスキーとシークレットアクセスキーを生成します。	AWS の設定 資格情報を生成するには、次のタスクを実行します。 1. 「最小限の Amazon IAM ポリシーの作成」 (ページ 85) 。 2. IAM ユーザーを作成し、そのユーザーにポリシーを割り当てて、AWS コンソールで S3 アクセスキー ID と S3 シークレットアクセスキーを生成します。 IAM ユーザーの作成方法とキーの生成方法の詳細については、AWS のマニュアルを参照してください。 Redshift V2 接続設定 [S3 アクセスキー ID] と [S3 シークレットアクセスキー] の値を入力します。
IAM 認証の設定	AWS の設定 EC2 インスタンスがあり、キーを指定したり、IAM ロール ARN を使用したりしない場合は、S3 バケットにアクセスできる EC2 に最小限のポリシーを割り当てます。 詳細については、 「IAM 認証の設定」 (ページ 85) を参照してください。 Redshift V2 接続設定 この場合、接続でステージングプロパティを有効にしたり指定したりする必要はありません。

暗号化の前提条件

ステージング時のデフォルト認証と AssumeRole による Redshift IAM 認証にクライアントサイド暗号化とサーバーサイド暗号化を設定するには、[「暗号化を有効にする」 \(ページ 93\)](#)を参照してください。

最小限の Amazon IAM ポリシーの作成

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

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

ポリシーには、次の最低限必要な権限を設定する必要があります。

- PutObject
- GetObject
- DeleteObject
- ListBucket
- ListBucketMultipartUploads. 詳細モードのマッピングにのみ適用されます。

次のサンプル Amazon IAM ポリシーを使用できます。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:PutObject",
        "s3:GetObject",
        "s3:DeleteObject",
        "s3:ListBucket",
        "s3:ListBucketMultipartUploads"
      ],
      "Resource": [
        "arn:aws:s3:::<bucket_name>/*",
        "arn:aws:s3:::<bucket_name>"
      ]
    }
  ]
}
```

詳細モードでのマッピングでは、ソース接続とターゲット接続で同じ AWS リージョン内の異なる AWS アカウントを使用できます。マッピングで指定された AWS アカウントへのアクセスが Amazon IAM ポリシーで承認されていることを確認します。

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

IAM 認証の設定

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

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

Amazon Redshift の引き受けロールの設定

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

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

AWS の設定	接続の詳細
オプション 1: IAM ユーザーを有効にするように AssumeRole を設定します。	IAM ユーザーに AssumeRole を使用するには、以下の IAM ユーザーの詳細を指定します。 <ul style="list-style-type: none">- Redshift アクセスキー ID- Redshift シークレットアクセスキー- Redshift IAM ロール ARN
オプション 2: EC2 インスタンスを定義して、Redshift IAM ロールを引き受けます。	Amazon EC2 の AssumeRole を使用するには、次のようにします。 <ul style="list-style-type: none">- [Redshift IAM ロール ARN] 値を指定します。- [ロールの引き受けに EC2 ロールを使用] チェックボックスをオンにします。

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

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

[Configure AssumeRole authentication for Amazon Redshift V2 Connector](#)

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

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

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

IAM ユーザー

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

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

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

注: 詳細モードでマッピングを実行するには、このポリシーを必ずワーカーノードロールに割り当ててください。

Redshift IAM ロールの信頼ポリシー

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

次のポリシーは、サンプルの信頼ポリシーです。

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

例えば、ロールまたはユーザーを次の形式で指定できます。

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

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

詳細モードでのマッピングの Redshift IAM ロール信頼ポリシー

ワーカーノードが Redshift ロールを引き受け、AssumeRole を介して Amazon Redshift にアクセスできるようにするには、IAM ロールに信頼ポリシーがアタッチされている必要があります。

次のポリシーは、サンプルの信頼ポリシーです。

```
{
  "Effect": "Allow",
  "Principal": { "AWS": "arn:aws:iam::<ACCOUNT-ID>:role/<WORKER-NODE-ROLE-ARN>" },
  "Action": "sts:AssumeRole"
}
```

Redshift IAM ロールの最小限のアクセス許可ポリシー

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

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

```
{
  "Effect": "Allow",
  "Action": [
    "redshift:GetClusterCredentials",
    "redshift:DescribeClusters"
  ],
  "Resource": [
    "arn:aws:redshift:<REGION>:<ACCOUNT-ID>:dbuser:<Cluster_Identifier>/<USER_NAME>",
    "arn:aws:redshift:<REGION>:<ACCOUNT-ID>:dbname:<Cluster_Identifier>/<DATABASE_NAME>"
  ]
}
}
```

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

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "redshift:GetClusterCredentials",
        "redshift:DescribeClusters",
        "redshift:CreateClusterUser",
        "redshift:JoinGroup"
      ],
      "Resource": [
        "arn:aws:redshift:<REGION>:<ACCOUNT-ID>:dbuser:<Cluster_Identifier>/<USER_NAME>",
        "arn:aws:redshift:<REGION>:<ACCOUNT-ID>:dbname:<Cluster_Identifier>/<DATABASE_NAME>",
        "arn:aws:redshift:<REGION>:<ACCOUNT-ID>:dbgroup:<Cluster_Identifier>/<GROUP_NAME>"
      ]
    }
  ]
}
```

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

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

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

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

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

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

EC2 サービスロールの信頼ポリシー

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

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

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

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

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

Amazon S3 ステージングの引き受けロールの設定

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

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

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

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

要件に基づいて一時的なセキュリティ資格情報を生成します。

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

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

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

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

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

外部 ID

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

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

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

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

```
"Statement": [
  {
    "Effect": "Allow",
    "Principal": {
```

```

    "AWS": "arn:aws:iam::AWS_Account_ID : user/user_name"
  },
  "Action": "sts:AssumeRole",
  "Condition": {
    "StringEquals": {
      "sts:ExternalId": "dummy_external_id"
    }
  }
}
]

```

一時的なセキュリティ資格情報のポリシー

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

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

IAM ユーザー

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

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

```

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

```

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

```

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

```

IAM ロール

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

次のポリシーは、サンプルの信頼ポリシーです。

```

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

```

KMS に対する一時的なセキュリティ資格情報

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

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

- GenerateDataKey
- DescribeKey
- Encrypt
- Decrypt
- ReEncrypt

次のサンプルポリシーを使用できます。

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

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

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

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

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

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

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

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

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

暗号化を有効にする

Amazon S3 でデータをステージングするために、Amazon Redshift V2 接続でサーバーサイド暗号化を有効にすることができます。

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

Amazon S3 ステージングバケットが存在するリージョンの顧客マスタキー ID を生成します。

顧客マスタキーの生成の詳細については、AWS のドキュメントを参照してください。

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

AWS KMS を使用するための最小限のポリシーの作成

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

KMS を使用した暗号化を有効にするには、次の操作を実行します。

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

サンプルポリシー:

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

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

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

Amazon Redshift への接続

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

始める前に

開始する前に、設定する認証タイプに基づいて Amazon Redshift アカウントから情報を取得する必要があります。

接続を設定する前に、「[認証の準備](#)」(ページ 83)を参照して認証要件を確認してください。

接続の詳細

次の表に、基本接続プロパティを示します。

プロパティ	説明
接続名	接続の名前。各接続名は組織内で一意である必要があります。接続名には、英数字、スペース、および次の特殊文字を含めることができます。_+-. 最大長は 255 文字です。
説明	接続の説明。最大長は 4000 文字です。
シークレットコンテナの使用	<p>組織に対して設定されている Secrets Manager にこの接続の機密資格情報を保存します。</p> <p>このプロパティは、組織に Secrets Manager が設定されている場合にのみ表示されます。</p> <p>このプロパティは、データ取り込みおよびレプリケーションとデータアクセス管理サービスではサポートされていません。</p> <p>接続でシークレットコンテナを有効にすると、Secure Agent が Secrets Manager からどの資格情報を取得するかを選択できます。このオプションを無効にした場合、資格情報は組織の設定方法に応じてリポジトリまたはローカル Secure Agent に保存されます。</p> <p>注: この接続を使用してプッシュダウンまたはプロキシサービスを介してデータアクセスポリシーを適用する場合、シークレットコンテナ設定オプションを使用することはできません。</p> <p>Secrets Manager を設定および使用する方法については、Administrator のヘルプにある「Secrets Manager の設定」を参照してください。</p>
ランタイム環境	<p>タスクを実行するランタイム環境の名前。</p> <p>Secure Agent、ホステッドエージェント、サーバーレスランタイム環境、またはエラスティックランタイム環境を選択します。</p> <p>アプリケーション取り込みとレプリケーションタスクとデータベース取り込みとレプリケーションタスクでは、Secure Agent またはサーバーレスランタイム環境を使用できます。タスクには、サーバーレス使用がサポートされているソースタイプが必要です。ファイル取り込みおよびレプリケーションタスクには、Secure Agent を使用します。ホステッドエージェントまたはエラスティックランタイム環境で、アプリケーション取り込みとレプリケーションタスク、データベース取り込みとレプリケーションタスク、またはファイル取り込みおよびレプリケーションタスクを実行することはできません。</p> <p>注: ホステッドエージェントは、詳細クラスターで実行されるマッピングには適用されません。また、IAM 認証および EC2 AssumeRole 認証にホステッドエージェントを使用することはできません。</p> <p>ランタイム環境の設定および使用方法の詳細については、Administrator のヘルプにある「ランタイム環境」を参照してください。</p>

認証タイプ

Amazon Redshift にアクセスするために、デフォルトの認証タイプおよび Redshift IAM AssumeRole 認証タイプを設定できます。

注: アプリケーション取り込みとレプリケーションタスクおよびデータベース取り込みとレプリケーションタスクは、EC2 インスタンスが定義されていない Redshift IAM AssumeRole 認証をサポートしていません。

必要な認証方法を選択し、認証固有のパラメータを設定します。

デフォルト認証

次の表に、デフォルト認証の基本接続プロパティを示します。

プロパティ	説明
JDBC URL	Amazon Redshift クラスタに接続するための JDBC URL。 JDBC URL は、Amazon AWS Redshift クラスタ設定ページから取得できます。 JDBC URL は次の形式で入力します。 <code>jdbc:redshift://<cluster_endpoint>:<port_number>/<database_name></code> ここで、エンドポイントには Redshift クラスタ名とリージョンが含まれます。 例: <code>jdbc:redshift://infa-rs-cluster.abc.us-west-2.redshift.amazonaws.com:5439/rsdb</code> この例では、 <ul style="list-style-type: none">- <code>infa-rs-qa-cluster</code> は Redshift クラスタの名前です。- <code>us-west-2.redshift.amazonaws.com</code> は、米国西部（オレゴン）リージョンである Redshift クラスタエンドポイントです。- <code>5439</code> は Redshift クラスタのポート番号です。- <code>rsdb</code> は、接続先の Redshift クラスタ内の特定のデータベースインスタンスです。
ユーザー名	Amazon Redshift クラスタ内のデータベースインスタンスのユーザー名。
パスワード	Amazon Redshift データベースユーザーのパスワード。

プロパティ	説明
ロールの引き受けに EC2 ロールを使用	<p>S3 IAM ロールを引き受ける EC2 インスタンスが S3 リソースにアクセスし、一時的なセキュリティ資格情報を使用してデータをステージングできるようにします。</p> <p>EC2 ロールには、S3 IAM ロールを引き受ける権限がアタッチされたポリシーが必要です。S3 IAM ロールと EC2 インスタンスは、同じ AWS アカウントでも異なる AWS アカウントでもかまいません。</p> <p>このチェックボックスを選択すると、EC2 ロールが [S3 IAM ロール ARN] オプションで指定された S3 IAM ロールを引き受けて、ステージングデータ用の S3 リソースにアクセスできるようになります。</p> <p>このプロパティは、アプリケーション取り込みとレプリケーションタスク、およびデータベース取り込みとレプリケーションタスクには適用されません。デフォルトでは、このチェックボックスは選択されていません。</p> <p>詳細については、「EC2 に AssumeRole を使用した一時的なセキュリティ資格情報の生成」(ページ 92)を参照してください。</p>
S3 IAM ロール ARN	<p>Amazon S3 にデータをステージングする目的で動的に生成された一時的なセキュリティ資格情報を使用するために IAM ユーザーまたは EC2 に引き受けられた IAM ロールの Amazon Resource Number (ARN)。</p> <p>このプロパティは、EC2 インスタンス、または S3 IAM ロールを引き受ける IAM ユーザーを使用して S3 ステージングバケットにアクセスするための一時的なセキュリティ資格情報を生成する場合に適用されます。</p> <p>一時的なセキュリティ資格情報を使用して Amazon S3 ステージングバケットにアクセスするための S3 IAM ロール名を指定します。</p> <p>S3 IAM ロールの ARN の取得方法の詳細については、AWS documentation を参照してください。</p> <p>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とレプリケーションタスクまたはデータベース取り込みとレプリケーションタスクの接続を使用している場合、AWS クラスターのデフォルトの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。</p>

詳細設定

次の表に、デフォルト認証の詳細接続プロパティを示します。

プロパティ	説明
S3 アクセスキー ID	<p>Amazon S3 ステージングバケットにアクセスするための IAM ユーザーのアクセスキー ID。</p> <p>S3 ステージングに次の方法を使用する場合は、アクセスキー ID を入力します。</p> <ul style="list-style-type: none">- IAM ユーザーが S3 ステージングにアクセスできる場合。- S3 IAM ロールを引き受ける IAM ユーザーが一時的なセキュリティ資格情報を使用して S3 にアクセスする場合。 <p>S3 アクセスキー ID は実行時にのみ検証されるため、実行時のエラーを防ぐために、接続を保存する前にそれが正確であることを確認してください。</p> <p>IAM 認証または EC2 の引き受けロールを使用して S3 にアクセスする場合は、S3 アクセスキー ID を入力する必要はありません。</p> <p>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とレプリケーションタスクまたはデータベース取り込みとレプリケーション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。</p>
S3 シークレットアクセスキー	<p>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。</p> <p>シークレットアクセスキーはアクセスキー ID に関連付けられており、アカウントを一意に識別します。</p> <p>S3 ステージングに次の方法を使用する場合は、シークレットアクセスキー値を入力します。</p> <ul style="list-style-type: none">- IAM ユーザーが S3 ステージングにアクセスできる場合。- S3 IAM ロールを引き受ける IAM ユーザーが一時的なセキュリティ資格情報を使用して S3 にアクセスする場合。 <p>S3 シークレットアクセスキーは実行時にのみ検証されるため、実行時のエラーを防ぐために、接続を保存する前にそれが正確であることを確認してください。</p> <p>IAM 認証または EC2 の引き受けロールを使用して S3 にアクセスする場合は、S3 シークレットアクセスキーを入力する必要はありません。</p> <p>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とレプリケーションタスクまたはデータベース取り込みとレプリケーション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。</p>
S3 VPC エンドポイントタイプ ¹	<p>Amazon S3 用の Amazon Virtual Private Cloud エンドポイントのタイプ。</p> <p>VPC エンドポイントを使用して、Amazon S3 とのプライベート通信を有効にすることができます。</p> <p>次のいずれかのオプションを選択します。</p> <ul style="list-style-type: none">- デフォルト。VPC エンドポイントを使用しない場合に選択します。- インタフェースエンドポイント。サブネットの IP アドレス範囲のプライベート IP アドレスを使用しているインタフェースエンドポイント経由で Amazon S3 とのプライベート通信を確立する場合に選択します。これは、AWS のサービス宛てのトラフィックのエントリポイントとして機能します。
Amazon S3 のエンドポイント DNS 名 ¹	<p>Amazon S3 インタフェースエンドポイントの DNS 名。</p> <p>DNS 名のアスタリスク記号を bucket キーワードで置き換えます。</p> <p>DNS 名は以下の形式で入力します。</p> <p>bucket.<インタフェースエンドポイントの DNS 名></p> <p>例: bucket.vpce-s3.us-west-2.vpce.amazonaws.com</p>

プロパティ	説明
STS VPC エンドポイントタイプ ¹	<p>AWS Security Token Service 用の Amazon Virtual Private Cloud エンドポイントのタイプ。VPC エンドポイントを使用して、Amazon Security Token Service とのプライベート通信を有効にすることができます。</p> <p>次のいずれかのオプションを選択します。</p> <ul style="list-style-type: none"> - デフォルト。VPC エンドポイントを使用しない場合に選択します。 - インタフェースエンドポイント。サブネットの IP アドレス範囲のプライベート IP アドレスを持つインタフェースエンドポイント経由で Amazon Security Token Service とのプライベート通信を確立する場合に選択します。
AWS STS のエンドポイント DNS 名 ¹	<p>AWS STS インタフェースエンドポイントの DNS 名。</p> <p>例: <code>vpce-01f22cc14558c241f-s8039x4c.sts.us-west-2.vpce.amazonaws.com</code></p>
KMS VPC エンドポイントタイプ ¹	<p>AWS Key Management Service 用の Amazon Virtual Private Cloud エンドポイントのタイプ。</p> <p>VPC エンドポイントを使用して、Amazon Key Management Service とのプライベート通信を有効にすることができます。</p> <p>次のいずれかのオプションを選択します。</p> <ul style="list-style-type: none"> - デフォルト。VPC エンドポイントを使用しない場合に選択します。 - インタフェースエンドポイント。サブネットの IP アドレス範囲のプライベート IP アドレスを持つインタフェースエンドポイント経由で Amazon Key Management Service とのプライベート通信を確立する場合に選択します。
AWS KMS のエンドポイント DNS 名 ¹	<p>AWS KMS インタフェースエンドポイントの DNS 名。</p> <p>例: <code>vpce-0e722f5c721e19232-g2pkm2r7.kms.us-west-2.vpce.amazonaws.com</code></p>
外部 ID	<p>IAM ロールに関連付けられた外部 ID。</p> <p>Amazon S3 バケットへのより安全なアクセスを提供する場合は、外部 ID を指定できます。Amazon S3 ステージングバケットと IAM ロールは、同じ AWS アカウントでも異なる AWS アカウントでもかまいません。</p> <p>必要に応じて、引き受けた IAM ロールの信頼ポリシーの外部 ID 条件を使用して、AWS Security Token Service (STS) への AssumeRole 要求で外部 ID を指定することもできます。</p> <p>外部 ID の使用方法の詳細については、External ID when granting access to your AWS resources を参照してください。</p> <p>このプロパティは、アプリケーション取り込みとレプリケーションタスク、およびデータベース取り込みとレプリケーションタスクには適用されません。</p>

プロパティ	説明
クラスターリージョン	<p>Redshift クラスターが存在する AWS クラスターリージョン。</p> <p>【JDBC URL】 フィールドプロパティで指定されているものとは異なるクラスターリージョンのカスタム JDBC URL を指定する場合は、リストからクラスターリージョンを選択します。【JDBC URL】 フィールドプロパティで指定されているクラスターリージョン名を引き続き使用するには、このプロパティでクラスターリージョンとして【なし】を選択します。</p> <p>AWS SDK によってサポートされるクラスターリージョンとの間でのみ、データの読み取りと書き込みを行うことができます。</p> <p>次のいずれかのクラスターリージョンを選択します。</p> <p>なし</p> <p>アジアパシフィック（ムンバイ）</p> <p>アジアパシフィック（ソウル）</p> <p>アジアパシフィック（シンガポール）</p> <p>アジアパシフィック（シドニー）</p> <p>アジアパシフィック（東京）</p> <p>アジアパシフィック（香港）</p> <p>AWS GovCloud(米国)</p> <p>AWS GovCloud（米国東部）</p> <p>カナダ（中部）</p> <p>中国（北京）</p> <p>中国（寧夏）</p> <p>欧州（アイルランド）</p> <p>欧州（フランクフルト）</p> <p>欧州(パリ)</p> <p>欧州(ストックホルム)</p> <p>南米（サンパウロ）</p> <p>中東(バーレーン)</p> <p>米国東部（バージニア北部）</p> <p>米国東部（オハイオ）</p> <p>米国西部（北カリフォルニア）</p> <p>米国西部（オレゴン）</p> <p>デフォルトは【なし】です。</p> <p>注: アプリケーション取り込みとレプリケーションタスク、およびデータベース取り込みとレプリケーションタスクには、リージョン値が必要です。</p>
接続環境 SQL	<p>セッション全体に適用されるデータベース環境を設定するための SQL 文。</p> <p>複数の値をセミコロン (;) で区切ります。</p> <p>SQL 文では、データベース環境の設定のみを指定してください。SQL 文には DDL コマンドや DML コマンドを指定しないようにしてください。</p>
マスタ対称キー	<p>Amazon Redshift V2 コネクタにクライアントサイド暗号化タイプを使用することはできません。そのため、マスター対称キーを指定すると、そのキーは無視されます。</p> <p>このプロパティは、アプリケーション取り込みとレプリケーションタスク、およびデータベース取り込みとレプリケーションタスクには適用されません。</p>

プロパティ	説明
顧客マスタキー ID	<p>AWS Key Management Service (AWS KMS) によって生成されたカスタママスタキー ID、または Amazon S3 でデータをステージングする際にクロスアカウントアクセスするためのカスタムキーの ARN。カスタママスタキーは、データが Amazon S3 に保存される前にコピー先で暗号化するためのものです。</p> <p>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。</p> <p>クロスアカウント KMS キーは、詳細モードのマッピングの接続で使用できます。クラスタとステージングバケットは、同じリージョンに存在する必要があります。</p> <p>このプロパティは、アプリケーション取り込みとレプリケーションタスク、およびデータベース取り込みとレプリケーションタスクには適用されません。</p>
¹ 詳細モードのマッピングには適用されません。	

AssumeRole による Redshift の IAM 認証。

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

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

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

プロパティ	説明
JDBC URL	<p>Amazon Redshift クラスタに接続するための JDBC URL。</p> <p>JDBC URL は、Amazon AWS Redshift クラスタ構成ページから取得することができます。</p> <p>JDBC URL は次の形式で入力します。</p> <p><code>jdbc:redshift://<cluster_endpoint>:<port_number>/<database_name></code>。ここで、エンドポイントには Redshift クラスタ名とリージョンが含まれます。</p> <p>例: <code>jdbc:redshift://infa-rs-cluster.abc.us-west-2.redshift.amazonaws.com:5439/rsdb</code></p> <p>この例では、</p> <ul style="list-style-type: none"> - <code>infa-rs-qa-cluster</code> は Redshift クラスタの名前です。 - <code>us-west-2.redshift.amazonaws.com</code> は、米国西部（オレゴン）リージョンである Redshift クラスタエンドポイントです。 - <code>5439</code> は Redshift クラスタのポート番号です。 - <code>rsdb</code> は、接続先の Redshift クラスタ内の特定のデータベースインスタンスです。
ユーザー名	Amazon Redshift クラスタ内のデータベースインスタンスのユーザー名。
クラスタ識別子	<p>Amazon Redshift をホストするクラスタの一意の識別子。</p> <p>Amazon Redshift クラスタ名を指定します。</p>
データベース名	アクセスするテーブルが保存されている Amazon Redshift データベースの名前。
Redshift IAM ロール ARN	<p>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して Amazon Redshift にアクセスするために EC2 が引き受ける IAM ロールの Amazon リソース番号 (ARN)。</p> <p>Redshift IAM ロール ARN を入力して、Amazon Redshift クラスタにアクセスします。</p>

プロパティ	説明
ロールの引き受けに EC2 ロールを使用	<p>EC2 ロールが IAM ロールを引き受けて、Redshift に接続するか、一時的なセキュリティ資格情報を使用してデータをステージングできるようにします。</p> <p>EC2 ロールを使用した IAM 認証による Redshift への接続</p> <p>このチェックボックスをオンにすると、[Redshift IAM ロール ARN] フィールドで指定された Redshift IAM ロールを引き受ける EC2 ロールが Amazon Redshift にアクセスできるようになります。</p> <p>EC2 ロールには、同じアカウントまたは異なるアカウントから Redshift IAM ロールを引き受けるための権限がアタッチされたポリシーが必要です。</p> <p>データのステージングのための S3 リソースへのアクセス</p> <p>このチェックボックスをオンにすると、[S3 IAM ロール ARN] フィールドで指定された S3 IAM ロールを EC2 ロールが引き受け、S3 ステージングバケットにアクセスするための一時的なセキュリティ資格情報を動的に生成できるようになります。</p> <p>EC2 ロールには、同じ AWS アカウントまたは異なる AWS アカウントから S3 IAM ロールを引き受けるための権限がアタッチされたポリシーが必要です。</p>
S3 IAM ロール ARN	<p>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して Amazon S3 にデータをステージングするために、IAM ユーザーまたは EC2 が引き受ける S3 IAM ロールの Amazon リソース番号 (ARN)。</p> <p>このプロパティは、EC2 インスタンスまたは S3 IAM ロールを引き受ける IAM ユーザーを使用して、S3 ステージングバケットにアクセスするための一時的なセキュリティ資格情報を生成する場合に適用されます。</p> <p>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 S3 IAM ロール名を指定します。</p> <p>IAM ロールの ARN の取得方法の詳細については、「AWS documentation」を参照してください。</p> <p>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とレプリケーションタスクまたはデータベース取り込みとレプリケーションタスクの接続を使用している場合、AWS クラスターのデフォルトの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。</p>

詳細設定

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

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

プロパティ	説明
データベースグループ	<p>この接続プロパティで 【DBUser の自動作成】 オプションを選択した場合に、データベースユーザーを追加するデータベースグループの名前。</p> <p>このデータベースグループに追加したユーザーは、指定されたグループ特権を継承します。</p> <p>データベースグループ名が指定されていない場合、ユーザーはパブリックグループに追加され、関連する特権を継承します。</p> <p>また、複数のデータベースグループをカンマで区切って入力し、指定した各データベースグループにユーザーを追加することもできます。</p>
有効期限	<p>Amazon Redshift データベースユーザーのパスワードの有効期限。</p> <p>900 秒から 3600 秒の間の値を指定します。</p> <p>デフォルトは 900 です。</p>
DBUser の自動作成	<p>実行時に新しい Amazon Redshift データベースユーザーの作成を選択します。</p> <p>エージェントは、【ユーザー名】 フィールドで指定したユーザーをデータベースグループに追加します。追加されたユーザーは、データベースグループに割り当てられた特権を引き受けます。</p> <p>デフォルトでは無効になっています。</p>
S3 アクセスキー ID	<p>Amazon S3 ステージングバケットにアクセスするための IAM ユーザーのアクセスキー。</p> <p>S3 ステージングに次の方法を使用する場合は、アクセスキー ID を入力します。</p> <ul style="list-style-type: none"> - IAM ユーザーが S3 ステージングにアクセスできる場合。 - S3 IAM ロールを引き受ける IAM ユーザーが一時的なセキュリティ資格情報を使用して S3 にアクセスできる場合。 <p>S3 アクセスキー ID は実行時にのみ検証されるため、実行時のエラーを防ぐために、接続を保存する前にそれが正確であることを確認してください。</p> <p>IAM 認証または EC2 のロールの引き受けを使用して S3 にアクセスする場合、S3 アクセスキー ID を入力する必要はありません。</p> <p>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とレプリケーションタスクまたはデータベース取り込みとレプリケーション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。</p>
S3 シークレットアクセスキー	<p>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。</p> <p>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。</p> <p>S3 ステージングに次の方法を使用する場合は、シークレットアクセスキーの値を入力します。</p> <ul style="list-style-type: none"> - IAM ユーザーが S3 ステージングにアクセスできる場合。 - S3 IAM ロールを引き受ける IAM ユーザーが一時的なセキュリティ資格情報を使用して S3 にアクセスできる場合。 <p>S3 シークレットアクセスキーは実行時にのみ検証されるため、実行時のエラーを防ぐために、接続を保存する前にそれが正確であることを確認してください。</p> <p>IAM 認証または EC2 のロールの引き受けを使用して S3 にアクセスする場合、S3 シークレットアクセスキーを入力する必要はありません。</p> <p>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とレプリケーションタスクまたはデータベース取り込みとレプリケーション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。</p>

プロパティ	説明
S3 VPC エンドポイントタイプ ¹	<p>Amazon S3 用の Amazon Virtual Private Cloud エンドポイントのタイプ。</p> <p>VPC エンドポイントを使用して、Amazon S3 とのプライベート通信を有効にすることができます。</p> <p>次のいずれかのオプションを選択します。</p> <ul style="list-style-type: none"> - デフォルト。VPC エンドポイントを使用しない場合に選択します。 - インタフェースエンドポイント。サブネットの IP アドレス範囲のプライベート IP アドレスを使用しているインタフェースエンドポイント経由で Amazon S3 とのプライベート通信を確立する場合に選択します。これは、AWS のサービス宛てのトラフィックのエントリポイントとして機能します。
Amazon S3 のエンドポイント DNS 名 ¹	<p>Amazon S3 インタフェースエンドポイントの DNS 名。</p> <p>アスタリスク記号を DNS 名内の bucket キーワードで置き換えます。</p> <p>DNS 名は以下の形式で入力します。</p> <p>bucket.<インタフェースエンドポイントの DNS 名></p> <p>例: bucket.vpce-s3.us-west-2.vpce.amazonaws.com</p>
STS VPC エンドポイントタイプ ¹	<p>AWS Security Token Service 用の Amazon Virtual Private Cloud エンドポイントのタイプ。</p> <p>VPC エンドポイントを使用して、Amazon Security Token Service とのプライベート通信を有効にすることができます。</p> <p>次のいずれかのオプションを選択します。</p> <ul style="list-style-type: none"> - デフォルト。VPC エンドポイントを使用しない場合に選択します。 - インタフェースエンドポイント。サブネットの IP アドレス範囲のプライベート IP アドレスを持つインタフェースエンドポイント経由で Amazon Security Token Service とのプライベート通信を確立する場合に選択します。
AWS STS のエンドポイント DNS 名 ¹	<p>AWS STS インタフェースエンドポイントの DNS 名。</p> <p>例: vpce-01f22cc14558c241f-s8039x4c.sts.us-west-2.vpce.amazonaws.com</p>
KMS VPC エンドポイントタイプ ¹	<p>AWS Key Management Service 用の Amazon Virtual Private Cloud エンドポイントのタイプ。</p> <p>VPC エンドポイントを使用して、Amazon Key Management Service とのプライベート通信を有効にすることができます。</p> <p>次のいずれかのオプションを選択します。</p> <ul style="list-style-type: none"> - デフォルト。VPC エンドポイントを使用しない場合に選択します。 - インタフェースエンドポイント。サブネットの IP アドレス範囲のプライベート IP アドレスを持つインタフェースエンドポイント経由で Amazon Key Management Service とのプライベート通信を確立する場合に選択します。
AWS KMS のエンドポイント DNS 名 ¹	<p>AWS KMS インタフェースエンドポイントの DNS 名。</p> <p>例: vpce-0e722f5c721e19232-g2pkm2r7.kms.us-west-2.vpce.amazonaws.com</p>
外部 ID	<p>IAM ロールに関連付けられた外部 ID。</p> <p>Amazon S3 ステージングバケットが同じ AWS アカウントまたは異なる AWS アカウントにある場合に、Amazon S3 バケットへのより安全なアクセスを提供するには、外部 ID を指定します。</p> <p>また、必要に応じて、引き受けた IAM ロールの信頼ポリシーの外部 ID 条件を使用して、AWS Security Token Service (STS) への AssumeRole 要求で外部 ID を指定することもできます。</p> <p>外部 ID の使用方法の詳細については、「External ID when granting access to your AWS resources」 を参照してください。</p> <p>このプロパティは、アプリケーション取り込みとレプリケーションタスク、およびデータベース取り込みとレプリケーションタスクには適用されません。</p>

プロパティ	説明
クラスタリー ジョン	<p>Redshift クラスタが存在する AWS ジオグラフィカルリージョン。</p> <p>【JDBC URL】 フィールドプロパティで指定されたリージョンとは異なるクラスタリージョンを持つカスタム JDBC URL を指定する場合は、リストからクラスタリージョンを選択します。【JDBC URL】 フィールドプロパティで指定されたクラスタリージョン名を引き続き使用するには、このプロパティでクラスタリージョンとして【なし】を選択します。</p> <p>AWS SDK によってサポートされるクラスタリージョンとの間でのみ、データの読み取りと書き込みを行うことができます。</p> <p>次のいずれかのクラスタリージョンを選択します。</p> <p>なし</p> <p>アジアパシフィック（ムンバイ）</p> <p>アジアパシフィック（ソウル）</p> <p>アジアパシフィック（シンガポール）</p> <p>アジアパシフィック（シドニー）</p> <p>アジアパシフィック（東京）</p> <p>アジアパシフィック（香港）</p> <p>AWS GovCloud（米国）</p> <p>AWS GovCloud（米国東部）</p> <p>カナダ（中部）</p> <p>中国（北京）</p> <p>中国（寧夏）</p> <p>欧州（アイルランド）</p> <p>欧州（フランクフルト）</p> <p>EU（パリ）</p> <p>EU（ストックホルム）</p> <p>南米（サンパウロ）</p> <p>中東（バーレーン）</p> <p>米国東部（バージニア北部）</p> <p>米国東部（オハイオ）</p> <p>米国西部（北カリフォルニア）</p> <p>米国西部（オレゴン）</p> <p>デフォルトは【なし】です。</p> <p>注: リージョンの値は、アプリケーション取り込みとレプリケーションタスクとデータベース取り込みとレプリケーションタスクでは必須です。</p>
接続環境 SQL	<p>セッション全体に適用されるデータベース環境を設定するための SQL 文。</p> <p>複数の値をセミコロン（;）で区切ります。</p> <p>SQL 文では、データベース環境の設定のみを指定してください。SQL 文には DDL コマンドや DML コマンドを指定しないようにしてください。</p>
マスタ対称キー	<p>Amazon Redshift V2 コネクタにクライアントサイド暗号化タイプを使用することはできません。そのため、マスター対称キーを指定すると、そのキーは無視されます。</p> <p>このプロパティは、アプリケーション取り込みとレプリケーションタスク、およびデータベース取り込みとレプリケーションタスクには適用されません。</p>

プロパティ	説明
顧客マスタキー ID	<p>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 Amazon S3 でデータをステージングする場合のアカウント間アクセス用のカスタムキーの ARN。顧客マスタキーは、データが Amazon S3 に保存される前に保存先でデータを暗号化します。</p> <p>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。</p> <p>クロスアカウント KMS キーは、詳細モードのマッピングの接続で使用することができます。クラスタとステージングバケットは、同じリージョンに存在している必要があります。</p> <p>サーバー側の暗号化を設定する方法の詳細については、「「暗号化を有効にする」 (ページ 93)」を参照してください。</p> <p>このプロパティは、アプリケーション取り込みとレプリケーションタスク、およびデータベース取り込みとレプリケーションタスクには適用されません。</p>
¹ 詳細モードのマッピングには適用されません。	

プロキシサーバーの設定

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

Windows および Linux でプロキシサーバーを使用するように Secure Agent を設定できます。認証されていないプロキシサーバーのみを使用できます。プロキシ設定は、マッピングおよび詳細モードのマッピングで使用する接続に適用されます。

注: Secure Agent は、Amazon S3 に接続してデータをステージングするときのみプロキシサーバーを使用し、Amazon Redshift に接続するときは使用しません。

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

- Windows の場合は Secure Agent Manager を使用し、Linux の場合はシェルコマンドを使用して Secure Agent を設定します。
手順については、データ統合のヘルプの『または「Windows でのプロキシ設定」または「Linux でのプロキシ設定」を参照してください。
- Secure Agent のプロパティで、DTM の JVM オプションを設定します。手順については、ナレッジベースの記事「[Proxy server settings](#)」を参照してください。

サーバーレスランタイム環境のプロキシの設定を行う方法については、Administrator ヘルプの「「プロキシサーバーの使用」を参照してください。

Amazon Redshift でのデータ共有

Amazon Redshift でのデータ共有が有効になっているテーブルからデータを読み取ることができます。データ共有により、Amazon Redshift クラスター間でデータを共有できます。データをコピーまたは移動したり、ストレージを複製したりする必要はありません。

Amazon Redshift データ共有には、次のコンポーネントが含まれます。

- プロデューサークラスター。データを所有し、他のクラスターと共有する Amazon Redshift クラスター。
- コンシューマークラスター。プロデューサークラスターから共有データを受信してアクセスする Amazon Redshift クラスター。
- データ共有。プロデューサークラスターで作成され、共有する特定のデータベースオブジェクトを含む、共有の論理単位。

データ共有を使用するには、Amazon Redshift V2 接続を作成するときに、JDBC URL 内にコンシューマークラスターのデータベース名を指定します。

SSL の設定

SSL を使用して Amazon Redshift に接続するには、Secure Agent を SSL 用に設定し、Amazon Redshift V2 接続プロパティで JDBC URL を介して SSL を有効にする必要があります。

1. Amazon Redshift の SSL 証明書をダウンロードします。
2. 証明書ファイルをキーストアに追加するには、コマンドプロンプトで以下のコマンドを実行します。

```
${JAVA_HOME}/bin/keytool -keystore {JAVA_HOME}/lib/security/cacerts -import -alias <alias_name> -file <certificate_filepath>
```


プロンプトが表示されたら、キーストアのパスワードを入力します。
3. Informatica Intelligent Cloud Services アカウントにログインします。
4. 管理者で、**ランタイム環境** をクリックします。
5. Secure Agent を選択し、[アクション] メニューで **Secure Agent の編集** をクリックします。
6. **システム構成の詳細** セクションで、次のプロパティを設定します。
 - a. **【サービス】** として **【データ統合サーバー】** を選択します。
 - b. **【タイプ】** として **【DTM】** を選択します。
 - c. **【JVMOption1】** の横にある **【エージェント設定の編集】** アイコンをクリックし、次の値を入力します。

```
-Djavax.net.ssl.trustStore=<truststore_path>
```
 - d. **【JVMOption2】** の横にある **【エージェント設定の編集】** アイコンをクリックし、次のコマンドを追加します。

```
-Djavax.net.ssl.trustStorePassword=<password>
```


パスワードとしては、手順 2 で証明書をインポートするときに使用したのと同じものを指定します。
7. **【保存】** をクリックします。
8. 管理者で、**接続** をクリックします。
9. Amazon Redshift V2 接続を編集し、JDBC URL に次のパラメータを追加します: ssl=true。
例: jdbc:redshift://mycluster.xyz789.us-west-2.redshift.amazonaws.com:5439/dev?ssl=true
10. **【保存】** をクリックします。

サーバーレスランタイム環境での SSL の設定

Amazon Redshift V2 接続でサーバーレスランタイム環境を使用して、SSL 対応の Amazon Redshift データベースに接続できます。

サーバーレスランタイム環境を使用して安全な Amazon Redshift V2 接続を設定する前に、次のタスクを実行します。

- Amazon S3 バケットに SSL 証明書を追加するまたは Azure コンテナ。
- .yaml サーバーレス構成ファイルを設定する。
- サーバーレス環境を設定する。
- SSL を使用するように接続プロパティを設定する。

Amazon S3 バケットに SSL 証明書を追加するまたは Azure コンテナ

サーバーレスランタイム環境で SSL 接続を設定するには、次の手順を実行します。

1. AWS または Azure のサーバーレスエージェント設定用に次の構造を作成します: <補足ファイルの場所>/serverless_agent_config
2. AWS アカウントまたは Azure アカウントの次の場所にある Amazon S3 バケットあるいは Azure コンテナに証明書名とソースパスを追加します: <補足ファイルの場所>/serverless_agent_config/SSL

.yaml サーバーレス構成ファイルを設定する

次の手順を実行して、サーバーレスランタイム環境で.yaml サーバーレス構成ファイルを設定し、証明書名とパスエントリを追加して、Amazon Redshift V2 コネクタが SSL を使用できるようにします。

1. 次のコードスニペットをテキストエディタにコピーします。

```
version: 1
agent:
  agentAutoApply:
    general:
      sslStore:
        - fileCopy:
            sourcePath: SSL/<cert_name>
        - importCerts:
            certName: <cert_name>
            alias: <alias name of the certificate>
```

ここで、ソースパスは AWS または Azure の証明書ファイルのディレクトリパスです。

2. 構文とインデントが有効であることを確認してから、ファイルを serverlessUserAgentConfig.yaml として次の AWS または Azure の場所に保存します: <補足ファイルの場所>/serverless_agent_config.yaml ファイルの実行時に、SSL 証明書が AWS または Azure の場所からサーバーレスエージェントディレクトリにコピーされます。

サーバーレス環境を設定する

サーバーレスランタイム環境で SSL の [JVMOption1] プロパティと [JVMOption2] プロパティを設定します。

1. サーバーレスランタイム環境のプロパティに移動し、[編集] をクリックします。
2. [ランタイム設定のプロパティ] タブで [JVMOption1] をクリックし、次のプロパティを追加します。
-Djavax.net.ssl.trustStore=/home/cldagnt/SystemAgent/jdk/jre/lib/security/cacerts
3. [JVMOption2] をクリックして、次のプロパティを追加します。
-Djavax.net.ssl.trustStorePassword=changeit
4. [保存] をクリックします。
5. ランタイム環境を再デプロイします。

SSL を使用するように接続プロパティを設定する

サーバーレスランタイム環境でランタイムプロパティを設定した後、[JDBC URL] 接続プロパティで ssl=true と指定します。

例: jdbc:redshift://mycluster.xyz789.us-west-2.redshift.amazonaws.com:5439/dev?ssl=true

詳細モードのマッピングに対する SSE-KMS 暗号化の設定

詳細モードのマッピングで使用する接続に SSE-KMS 暗号化を使用するには、次のいずれかのタスクを実行します。

- `~/.aws/credentials` という場所からの資格情報を使用するには、AWS でマスタインスタンスプロファイルとワーカーインスタンスプロファイルを作成し、KMS ポリシーをワーカープロファイルにアタッチして、そのプロファイルをクラスタ設定に指定します。
- Amazon EC2 で Secure Agent を使用し、AWS でマスタインスタンスプロファイルとワーカーインスタンスプロファイルを作成して、KMS ポリシーをワーカープロファイルにアタッチします。
- Amazon EC2 で Secure Agent を使用し、デフォルトの IAM ロールを使用して、KMS ポリシーを Secure Agent ロールにアタッチします。

Amazon Redshift サーバーレス接続

Amazon Redshift Serverless は Amazon Web Services (AWS) のサーバーレス製品で、プロビジョニングされた Redshift クラスタのセットアップや管理を必要とせずに、Amazon Redshift と同じ拡張性と機能を実現します。

Amazon Redshift V2 コネクタは、Amazon Redshift Serverless エンドポイントに接続するための追加設定不要なサポートを提供します。

Amazon Redshift Serverless エンドポイントにアクセスする方法の詳細については、次の How-To ライブラリの記事を参照してください: [Using Amazon Redshift Serverless with Cloud Data Integration](#)

Amazon Redshift Spectrum を使用するための要件

マッピングで接続を使用して Amazon Redshift Spectrum 外部テーブルからデータの読み取りを行う場合は、Amazon S3 のデータカタログとデータファイルにアクセスするために必要な認証を Amazon Redshift クラスタに提供します。

重要: Amazon Redshift クラスタとデータファイルを含む Amazon S3 バケットは、同じリージョンに属している必要があります。Amazon Redshift クラスタは、バージョン 1.0.1294 以降である必要があります。

1. AWS Identity and Access Management (IAM) ロールを作成して、Amazon S3 内の外部データカタログとデータファイルへの Amazon Redshift クラスタのアクセスを承認します。
2. 指定した Amazon Redshift クラスタに IAM ロールを関連付けます。
3. 外部スキーマを作成します。
4. 外部スキーマ内で、IAM ロールに Amazon Redshift ロール ARN を指定します。
5. 外部スキーマ内に外部テーブルを作成し、データの読み取り元に Amazon S3 の場所を指定します。外部テーブルの作成の詳細については、AWS のマニュアルを参照してください。
6. Amazon Redshift Spectrum を使用して Amazon S3 のデータカタログとデータファイルにアクセスするには、Amazon Redshift クラスタに必要な認証があることを確認します。

Amazon Redshift とのプライベート通信

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

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

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

- クラスタサブネットグループを作成します。
- Redshift 管理の VPC エンドポイントを作成します。
- ゲートウェイエンドポイントを設定します。

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

詳細については、

「[Configuring private communication with Amazon Redshift using the Amazon Redshift V2 Connector](#)」を参照してください。

Amazon S3 とのプライベート通信

ステージング用に Amazon S3 とのプライベート通信を確立するように Amazon Redshift V2 接続を設定できます。

AWS コンソールでインタフェースエンドポイントを設定して、Amazon S3 でデータをステージングするためのプライベート通信を有効にする必要があります。AWS S3 VPC エンドポイントを使用すると、インターネットに接続せずに S3 要求を Amazon S3 サービスにルーティングすることができます。

Amazon S3 とのプライベート通信を確立する場合は、次のガイドラインを考慮してください。

- Amazon Redshift クラスタが生成されると、サブネット内のクラスタに対して Elastic Network Interface (ENI) が生成されます。S3 ゲートウェイエンドポイントのルートテーブルが、Redshift クラスタ ENI が作成されたサブネットと同じサブネットに対応していることを確認します。
- VPC エンドポイントを使用して Amazon S3 バケットに接続するには、Amazon Redshift クラスタと接続先の Amazon S3 バケットが同じ AWS リージョンに存在している必要があります。

サーバーレスランタイム環境と Amazon Redshift 間の VPC ピアリング

サーバーレスランタイム環境を使用する際にサーバーレスランタイム環境と Amazon Redshift クラスタが異なる VPC にある場合は、VPC ピアリングを設定する必要があります。

VPC ピアリングの設定の詳細については、次の How-To ライブラリの記事を参照してください:

[Configure VPC peering between Amazon Redshift clusters](#)

第 23 章

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。

重要: Amazon S3 コネクタは非推奨となり、メンテナンスモードに移行されました。Informatica は将来のリリースでサポートを廃止する予定です。Amazon S3 V2 コネクタを使用して Amazon S3 にアクセスすることをお勧めします。

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	<p>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。</p> <ul style="list-style-type: none"> - 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	<p>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。</p> <ul style="list-style-type: none"> - 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) <p>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。</p>

第 24 章

Amazon S3 V2 接続プロパティ

Amazon S3 に対して読み取りおよび書き込みを行う Amazon S3 V2 接続を作成します。

認証の準備

Amazon S3 にアクセスするために、複数の認証タイプを設定できます。

接続プロパティを設定する前に、使用する認証のタイプに基づいて認証の詳細を用意しておく必要があります。

- 基本認証には、AWS アカウントからのアクセスキーとシークレットキーの値が必要です。
- IAM 認証では、特定のフォルダパスへのアクセスを許可し、Amazon S3 オブジェクトにアクセスするために、EC2 ロールにポリシーをアタッチする必要があります。
- EC2 ロール認証を使用した AssumeRole では、EC2 ロールが IAM ロール ARN で指定された別の IAM ロールを引き受けることができるようにする必要があります。
- IAM ユーザー認証を使用した AssumeRole には、IAM ユーザーのアクセスキーとシークレットキーの値、および IAM ロールの ARN が必要です。
- 資格情報プロファイルファイル認証には、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が必要です。資格情報プロファイルファイルには、アクセスキーが含まれています。
- IAM Roles Anywhere 認証には、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が必要です。資格情報プロファイルファイルには、CA 証明書ファイルとキーファイルの ARN やパスが含まれています。
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設定するには、Amazon S3 V2 接続プロパティで認証タイプとして「資格情報プロファイルファイル認証」を選択する必要があります。
- フェデレーティッドユーザーシングルサインオン認証には、フェデレーティッドユーザーのユーザー名とパスワード、IdP SSO URL、SAML ID プロバイダの ARN、およびフェデレーティッドユーザーが引き受ける IAM ロールの ARN が必要です。SSO には ADFS 3.0 (IDP) のみを使用できます。

最小限の Amazon IAM ポリシーの作成

AWS コンソールで IAM ポリシーを設定できます。AWS IAM 認証を使用すると、Amazon S3 リソースへのアクセスを安全に制御できます。

ユーザーが、Amazon S3 バケットからデータの読み取りを行うことができるようにするには、次に示す最低限必要なポリシーを使用します。

- GetObject
- ListBucket

ユーザーが、Amazon S3 バケットにデータの書き込みを行うことができるようにするには、次に示す最低限必要なポリシーを使用します。

- PutObject
- GetObject
- DeleteObject
- ListBucket
- ListBucketMultipartUploads.詳細モードのマッピングにのみ適用されます。

次のサンプルポリシーは、Amazon S3 バケットにデータを書き込むための最小限の Amazon IAM ポリシーを示しています。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:PutObject",
        "s3:GetObject",
        "s3:DeleteObject",
        "s3:ListBucket",
        "s3:ListBucketMultipartUploads"
      ],
      "Resource": [
        "arn:aws:s3:::<bucket_name>/*",
        "arn:aws:s3:::<bucket_name>"
      ]
    }
  ]
}
```

詳細モードでバケットレベルのアクセスを行うには、ListBucketMultipartUploads 権限とともに、バケットレベルで AllowListBucketMultipartUploads 権限を付与する必要があります。

次のサンプルポリシーは、詳細モードのバケットレベルで S3 バケットにアクセスするための最小限の Amazon IAM ポリシーを示しています。

```
{
  "Sid": "AllowListBucketMultipartUploads",
  "Action": [
    "s3:ListBucketMultipartUploads"
  ],
  "Effect": "Allow",
  "Resource": [
    "arn:aws:s3:::infa.qa.minimum.access.bucket"
  ]
},
```

詳細モードのマッピングの場合、同じ AWS リージョン内で異なる AWS アカウントを使用できます。マッピングで使用する AWS アカウントへのアクセスが Amazon IAM ポリシーで承認されていることを確認します。

IAM 認証

IAM 認証を設定するには、Secure Agent を Amazon Elastic Compute Cloud (EC2) システム上で実行する必要があります。キーを指定したり、IAM ロール ARN を使用したりしない場合は、S3 バケットにアクセスできる EC2 に最小限のポリシーを割り当てます。

サーバーレスランタイム環境を使用している場合、IAM 認証を設定することはできません。

接続でアクセスキーとシークレットキーが指定されていない場合、Amazon S3 V2 コネクタでは、必要に応じて AWS 資格情報プロバイダチェーンが使用され、資格情報が次の順序で検索されます。

1. **AWS_ACCESS_KEY_ID** と **AWS_SECRET_ACCESS_KEY** または **AWS_ACCESS_KEY** と **AWS_SECRET_KEY** 環境変数。
2. **aws.accessKeyId** と **aws.secretKey** java システムプロパティ。
3. デフォルトの場所 `~/.aws/credentials` にある資格情報プロファイルファイル。
4. Amazon EC2 メタデータサービスによって配信されるインスタンスプロファイル資格情報。

EC2 で IAM 認証を設定するには、次の手順を実行します。

1. 最小限の Amazon IAM ポリシーを作成します。
2. Amazon EC2 ロールを作成します。Amazon EC2 ロールは、EC2 システムを作成する場合に使用されます。Amazon EC2 ロールの作成の詳細については、AWS のマニュアルを参照してください。
3. 最小限の Amazon IAM ポリシーを Amazon EC2 ロールにリンクします。
4. EC2 インスタンスを作成します。手順 2 で作成した Amazon EC2 ロールを EC2 インスタンスに割り当てます。
5. EC2 システムにセキュアエージェントをインストールします。

EC2 ロールと IAM ユーザーを使用した AssumeRole

EC2 ロールまたは IAM ユーザーを使用した AssumeRole を設定し、Amazon S3 に接続できます。

AssumeRole を使用した一時的なセキュリティ資格情報を使用すると、同じ AWS アカウントまたは異なる AWS アカウントから AWS リソースにアクセスできます。

EC2 ロールまたは IAM ユーザーを使用した AssumeRole を設定する場合は、一時的なセキュリティ資格情報を使用するために、**[sts:AssumeRole]** 権限と AWS アカウント内で確立された信頼関係があることを確認してください。信頼関係は、ロールを作成するときに、IAM ロールの信頼ポリシーで定義されます。IAM ロールにより、EC2 ロールまたは IAM ユーザーを信頼されたエンティティとして追加し、EC2 ロールまたは IAM ユーザーに一時的なセキュリティ資格情報の使用と AWS アカウントへのアクセスを許可します。

信頼関係を構築する方法の詳細については、AWS のマニュアルを参照してください。

信頼された EC2 ロールまたは IAM ユーザーが一時的なセキュリティ資格情報を要求すると、AWS Security Token Service (AWS STS) によって、指定した期間有効な一時的なセキュリティ資格情報が動的に生成され、信頼された EC2 ロールまたは IAM ユーザーにその資格情報が提供されます。

EC2 ロールを使用した AssumeRole

[IAM ロール ARN] 接続プロパティで指定した IAM ロールを引き受けるように EC2 ロールを設定するには、Amazon S3 V2 接続プロパティの **[ロールの引き受けに EC2 ロールを使用]** チェックボックスをオンにします。

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

EC2 ロールを使用した AssumeRole を設定する前に、次の前提条件を考慮してください。

- Secure Agent を Amazon EC2 などの AWS サービスにインストールします。
- AWS EC2 サービスにアタッチされた EC2 ロールは、Amazon S3 へのアクセス権を持ってはいけませんが、別の IAM ロールを引き受ける権限が必要です。
- EC2 ロールが引き受ける必要のある IAM ロールには、アクセス許可ポリシーと信頼ポリシーがアタッチされている必要があります。

IAM ユーザーを使用した AssumeRole

IAM ユーザーを使用した AssumeRole を設定するには、Amazon S3 V2 接続の作成時に **[IAM ロール ARN]** 接続プロパティの値を指定します。IAM ロール ARN は、AWS リソースを一意に識別します。次に、**[一時的な資格情報の期間]** 詳細ソースプロパティおよびターゲットプロパティで、一時的なセキュリティ資格情報を使用できる期間を秒単位で指定します。

IAM ユーザーを使用して AssumeRole を設定する場合は、いくつかのガイドラインに従う必要があります。詳細については、「[IAM ユーザー経由の AssumeRole のルールとガイドライン認証](#)」(ページ 135)を参照してください。

外部 ID

Amazon S3 バケットが同じ AWS アカウントまたは異なる AWS アカウントにある場合に、Amazon S3 バケットへのより安全なアクセスのために、AWS アカウントの外部 ID を指定できます。

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

外部 ID は文字列である必要があります。

次のサンプルは、引き継がれた IAM ロールの信頼ポリシー内の外部 ID 条件を示しています。

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

AssumeRole ポリシー

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には、IAM ユーザーと IAM ロールの両方にポリシーが必要です。

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

IAM ユーザー

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

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

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

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

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

IAM ロール

IAM ロールは、IAM ユーザーに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ことを許可するために、sts:AssumeRole ポリシーと、IAM ロールにアタッチされた信頼ポリシーを持っています。ポリシーは、IAM ユーザーがアクセスできる AWS リソースと、IAM ユーザーが実行できるアクションを指定します。信頼ポリシーは、AWS リソースにアクセスできる AWS アカウントの IAM ユーザーを指定します。

次のポリシーは、サンプルの信頼ポリシーです。

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

このポリシーでは、Principal 属性で、IAM ユーザーの ARN を入力して、指定されたユーザーが一時的なセキュリティ資格情報を動的に生成できるようにすることもでき、それ以上のアクセスを制限できます。

以下に例を示します。

```
"Principal" : { "AWS" : "arn:aws:iam:: AWS-account-ID :user/ user-name " }
```

資格情報プロファイルファイルの認証

Amazon S3 との接続を確立するために必要な資格情報は、資格情報プロファイルファイルで指定できます。

認証情報プロファイルファイルについては、次のルールを考慮してください。

- 資格情報ファイルは、Secure Agent をインストールしたマシンと同じマシン上にある必要があります。
 - 資格情報プロファイルファイル名は、.credentials で終わる必要があります。
 - 資格情報プロファイルのパスを指定しない場合、Secure Agent はホームディレクトリの次のデフォルトの場所にある資格情報プロファイルファイルを使用します。
~/aws/credentials
- 注:** Windows では、環境変数%UserProfile%を使用してホームディレクトリを参照できます。Unix 系のシステムでは、環境変数\$HOME を使用できます。
- プロファイル名を指定しない場合、認証情報は認証情報ファイルのデフォルトプロファイルから使用されません。

次の例は、資格情報プロファイルファイルを示しています：

```
[default]
```

```
aws_access_key_id = 1233333
```

```
aws_secret_access_key = abcabcabc
```

```
[test-profile]
```

```
aws_access_key_id = 1233333
```

```
aws_secret_access_key = abcabcabc
```

```
aws_session_token = jahaheieomdrftflmlioerp
```

aws_access_key_id と aws_secret_access_key は、ユーザーを認証するための認証情報の一部として使用される AWS アクセスキーとシークレットキーです。

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

IAM Roles Anywhere 認証

AWS IAM Roles Anywhere 認証を設定して、長期的な認証情報の代わりに X.509 証明書を使用して、AWS 外部のサーバー、アプリケーション、またはコンテナから Amazon S3 リソースに安全にアクセスするための一時的なセキュリティ資格情報を生成できます。

IAM Roles Anywhere 認証を設定するには、CA 証明書の作成、一時的な資格情報の生成、資格情報プロファイルファイルの作成など、特定の前提条件を完了する必要があります。

資格情報プロファイルファイルには、トラストアンカー、プロファイル、IAM ロールの各 ARN、および CA 証明書とプライベートキーのファイルパスが含まれている必要があります。

IAM Roles Anywhere 認証を使用するには、次の前提条件を満たす必要があります。

1. 認証局を設定します。
AWS Private Certificate Authority を使用して認証局を作成し、CA 証明書をインストールして認証局をアクティブ化します。
2. IAM Roles Anywhere を設定します。
 - a. IAM Roles Anywhere で、作成した認証局を使用してトラストアンカーを作成します。
 - b. 最小限の S3 権限を持つ IAM ロールと、IAM Roles Anywhere がそのロールを引き受けることを許可する信頼ポリシーを作成します。
 - c. IAM Roles Anywhere コンソールでプロファイルを作成し、IAM ロールをトラストアンカーにリンクします。
3. 証明書を生成してダウンロードします。
 - a. AWS Certificate Manager で、認証局に関連付けられたプライベート証明書を要求して取得します。
 - b. 証明書本体、証明書チェーン、および証明書プライベートキーをダウンロードしてエクスポートします。
 - c. OpenSSL を使用してプライベートキーを復号します。
 - d. プライベートキー、復号されたプライベートキー、および証明書をローカルディレクトリに配置します。
4. IAM 資格情報ヘルパーをインストールし、aws_signing_helper ツールを使用して、CreateSession API を介して一時的な資格情報を要求します。
5. 証明書ファイルとキーファイルへの ARN やパスなど、プロファイルの詳細が含まれる AWS 資格情報ファイルを作成します。
資格情報プロファイルファイルで以下のパラメータを指定します。
 - **<agent_loc>\aws_signing_helper.exe** AWS 資格情報ヘルパーツールへのパス。
 - **--certificate <agent_loc>\certificate.pem** X.509 証明書ファイルへのパス。この証明書は、IAM Roles Anywhere から一時的な資格情報を要求する ID を認証するために使用されます。
 - **--private-key <agent_loc>\decrypted_private_key.pem** 証明書に対応する復号されたプライベートキーへのパス。
 - **--trust-anchor-arn <arn of trust anchor>** IAM Roles Anywhere と認証局の間の信頼を確立するトラストアンカーの Amazon リソースネーム (ARN)。
 - **--profile-arn <arn of profile>** IAM Roles Anywhere で設定したプロファイルの ARN。プロファイルは、引き受けることができる IAM ロールや、発行された一時的なセキュリティ資格情報で実行できる操作を指定します。
 - **--role-arn <arn of role>** 資格情報ヘルパーが引き受ける IAM ロールの ARN。
 - **--session-duration <time in seconds>** 一時セッション資格情報が有効な期間。このパラメータはオプションです。

次の例は、資格情報プロファイルファイルを示しています：

```
[profile_name]
credential_process = <Secure Agent installation directory>\aws_signing_helper.exe credential-process --
certificate <agent_loc>\certificate.pem --private-key <agent_loc>\decrypted_private_key.pem --trust-
anchor-arn <arn of trust anchor> --profile-arn <arn of profile> --role-arn <arn of role> --session-
duration <time in seconds>
```

Amazon S3 V2 接続の作成時に【**その他の認証タイプ**】フィールドで【**資格情報プロファイルファイル認証**】を選択し、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指定します。

資格情報プロファイルファイルのルール

認証情報プロファイルファイルについては、次のルールを考慮してください。

- 資格情報プロファイルファイルは、セキュアエージェントマシン上にある必要があります。
- 資格情報プロファイルファイルには、.credentials 拡張子が付いている必要があります。
- 資格情報プロファイルのパスを指定しない場合、セキュアエージェントはホームディレクトリの次のデフォルトの場所にある資格情報プロファイルファイルを使用します。

~/.aws/credentials

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

IAM Roles Anywhere 認証の設定方法の詳細については、[AWS documentation](#) を参照してください。

Amazon S3 への接続

Amazon S3 に接続するように Amazon S3 接続プロパティを設定してみましょう。

始める前に

開始する前に、設定する認証タイプに基づいて Amazon S3 アカウントから情報を取得する必要があります。

認証の前提条件の詳細については、「[認証の準備](#)」 ([ページ 112](#))を参照してください。

接続の詳細

次の表に、基本接続プロパティを示します。

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

プロパティ	説明
シークレットコンテナの使用	<p>組織に対して設定されている Secrets Manager にこの接続の機密資格情報を保存します。</p> <p>このプロパティは、組織に Secrets Manager が設定されている場合にのみ表示されます。</p> <p>このプロパティは、データ取り込みおよびレプリケーションとデータアクセス管理サービスではサポートされていません。</p> <p>接続でシークレットコンテナを有効にすると、Secure Agent が Secrets Manager からどの資格情報を取得するかを選択できます。このオプションを無効にした場合、資格情報は組織の設定方法に応じてリポジトリまたはローカル Secure Agent に保存されます。</p> <p>注: この接続を使用してプッシュダウンまたはプロキシサービスを介してデータアクセスポリシーを適用する場合、シークレットコンテナ設定オプションを使用することはできません。</p> <p>Secrets Manager を設定および使用する方法については、Administrator のヘルプにある「Secrets Manager の設定」を参照してください。</p>
ランタイム環境	<p>タスクを実行するランタイム環境の名前。</p> <p>Secure Agent、ホステッドエージェント、サーバーレスランタイム環境、またはエラスティックランタイム環境を選択します。</p> <p>アプリケーション取り込みとレプリケーションの初期ロードタスクとデータベース取り込みとレプリケーションタスクでは、Secure Agent またはサーバーレスランタイム環境を使用できます。タスクには、サーバーレス使用がサポートされているソースタイプが必要です。ファイル取り込みおよびレプリケーションタスクとストリーミング取り込みおよびレプリケーションタスクには、Secure Agent を使用します。ホステッドエージェントまたはエラスティックランタイム環境で、アプリケーション取り込みとレプリケーションタスク、データベース取り込みとレプリケーションタスク、ファイル取り込みおよびレプリケーションタスク、またはストリーミング取り込みおよびレプリケーションタスクを実行することはできません。</p> <p>ランタイム環境の設定および使用方法の詳細については、Administrator のヘルプにある「ランタイム環境」を参照してください。</p>

認証タイプ

Amazon S3 にアクセスするには、基本認証、AWS Identity and Access Management (IAM)、一時的なセキュリティ認証情報、EC2 のロールの引き受け、資格情報プロファイルファイル、およびフェデレーティッドユーザーシングルサインオン認証タイプを設定します。

必要な認証方法を選択し、認証固有のパラメータを設定します。

基本認証

基本認証には、AWS アカウントからのアクセスキーとシークレットキーの値が必要です。

次の表に、標準認証の基本的な接続プロパティとその説明を示します。

プロパティ	説明
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。
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。

プロパティ	説明
フォルダパス	<p>Amazon S3 バケット名、または Amazon S3 オブジェクトが保存されている Amazon S3 バケット内のフォルダパス。</p> <p>例: <バケット名>/<フォルダ名></p> <p>アプリケーション取り込みとレプリケーションタスク、およびデータベース取り込みとレプリケーションタスクの場合は、末尾にスラッシュを追加します。</p> <p>例: <バケット名>/<フォルダ名>/。</p>
リージョン名	<p>アクセス先のバケットの AWS リージョン。</p> <p>次のいずれかのリージョンを選択します。</p> <ul style="list-style-type: none"> - アフリカ(ケープタウン) - アジアパシフィック(香港) - アジアパシフィック (ハイデラバード) - アジアパシフィック(ジャカルタ) - アジアパシフィック (メルボルン) - アジアパシフィック(大阪) - 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) - 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 (ミラノ) - 欧州(パリ) - EU (スペイン) - 欧州(ストックホルム) - EU (チューリッヒ) - 欧州 (フランクフルト) - 欧州 (アイルランド) - 欧州(ロンドン) - イスラエル (テルアビブ) - 中東(バーレーン) - 中東 (UAE) - 南米 (サンパウロ) - 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 ISO 西部 - 米国 ISOB 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) <p>デフォルトは [米国東部 (バージニア北部)] です。</p>

IAM 認証

IAM 認証には、Amazon S3 オブジェクトへのフォルダパスのみが必要です。EC2 ロールには、フォルダへのアクセス権が割り当てられている必要があります。

次の表に、AWS IAM 認証の基本接続プロパティとその説明を示します。

プロパティ	説明
フォルダパス	<p>Amazon S3 バケット名、または Amazon S3 オブジェクトが保存されている Amazon S3 バケット内のフォルダパス。</p> <p>例: <バケット名>/<フォルダ名></p> <p>アプリケーション取り込みとレプリケーションタスク、およびデータベース取り込みとレプリケーションタスクの場合は、末尾にスラッシュを追加します。</p> <p>例: <バケット名>/<フォルダ名>/。</p>
リージョン名	<p>アクセス先のバケットの AWS リージョン。</p> <p>次のいずれかのリージョンを選択します。</p> <ul style="list-style-type: none"> - アフリカ(ケープタウン) - アジアパシフィック(香港) - アジアパシフィック (ハイデラバード) - アジアパシフィック(ジャカルタ) - アジアパシフィック (メルボルン) - アジアパシフィック(大阪) - 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) - 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 (ミラノ) - 欧州(パリ) - EU (スペイン) - 欧州(ストックホルム) - EU (チューリッヒ) - 欧州 (フランクフルト) - 欧州 (アイルランド) - 欧州(ロンドン) - イスラエル (テルアビブ) - 中東(バーレーン) - 中東 (UAE) - 南米 (サンパウロ) - 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 ISO 西部 - 米国 ISOB 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) <p>デフォルトは [米国東部 (バージニア北部)] です。</p>

EC2 ロール認証経由の AssumeRole

EC2 ロール認証経由の AssumeRole では、EC2 ロールが IAM ロール ARN オプションで指定された別の IAM ロールを引き受けることができるようにする必要があります。

次の表に、EC2 ロール認証経由の AssumeRole の基本的な接続プロパティとその説明を示します。

プロパティ	説明
フォルダパス	<p>Amazon S3 バケット名、または Amazon S3 オブジェクトが保存されている Amazon S3 バケット内のフォルダパス。</p> <p>例: <バケット名>/<フォルダ名></p> <p>アプリケーション取り込みとレプリケーションタスク、およびデータベース取り込みとレプリケーションタスクの場合は、末尾にスラッシュを追加します。</p> <p>例: <バケット名>/<フォルダ名>/。</p>
領域名	<p>アクセス先のバケットの AWS 領域。</p> <p>次のいずれかのリージョンを選択します。</p> <ul style="list-style-type: none"> - アフリカ(ケープタウン) - アジアパシフィック(香港) - アジアパシフィック (ハイデラバード) - アジアパシフィック(ジャカルタ) - アジアパシフィック (メルボルン) - アジアパシフィック(大阪) - 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) - 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 (ミラノ) - 欧州(パリ) - EU (スペイン) - 欧州(ストックホルム) - EU (チューリッヒ) - 欧州 (フランクフルト) - 欧州 (アイルランド) - 欧州(ロンドン) - イスラエル (テルアビブ) - 中東(バーレーン) - 中東 (UAE) - 南米 (サンパウロ) - 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 ISO 西部 - 米国 ISOB 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) <p>デフォルトは [米国東部 (バージニア北部)] です。</p>

プロパティ	説明
IAM ロール ARN	<p>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が引き受ける AWS Identity and Access Management (IAM) ロールの Amazon Resource Name (ARN)。</p> <p>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、ARN 値を入力します。</p> <p>このプロパティは、アプリケーション取り込みとレプリケーションタスクには適用されません。</p> <p>注: エージェントに Amazon S3 バケットへのアクセス権限を付与する IAM ロールを削除しても、テスト接続は成功します。</p> <p>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。</p>
外部 ID	<p>AWS アカウントの外部 ID。</p> <p>外部 ID を使用すると、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が可能になります。</p>
ロールの引き受けに EC2 ロールを使用	<p>IAM ロール ARN オプションで指定された別の IAM ロールを EC2 ロールが引き受けることができますようになります。</p> <p>デフォルトでは、このプロパティは選択されていません。</p> <p>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権限がアタッチされたポリシーが必要です。</p> <p>注: ストリーミング取り込みとレプリケーションタスクでこのプロパティを有効にする場合は、[IAM ロール ARN] プロパティの値を入力します。</p>

IAM ユーザー認証経由の AssumeRole

IAM ユーザー認証経由の AssumeRole には、IAM ユーザーのアクセスキーとシークレットキーの値、および IAM ロールの ARN が必要です。

次の表に、IAM ユーザー認証経由の AssumeRole の基本的な接続プロパティとその説明を示します。

プロパティ	説明
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。
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。
フォルダパス	<p>Amazon S3 バケット名、または Amazon S3 オブジェクトが保存されている Amazon S3 バケット内のフォルダパス。</p> <p>例: <バケット名>/<フォルダ名></p> <p>アプリケーション取り込みとレプリケーションタスク、およびデータベース取り込みとレプリケーションタスクの場合は、末尾にスラッシュを追加します。</p> <p>例: <バケット名>/<フォルダ名>/。</p>

プロパティ	説明
リージョン名	<p>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。</p> <ul style="list-style-type: none"> - アフリカ(ケープタウン) - アジアパシフィック(香港) - アジアパシフィック (ハイデラバード) - アジアパシフィック(ジャカルタ) - アジアパシフィック (メルボルン) - アジアパシフィック(大阪) - 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) - 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 (ミラノ) - 欧州(パリ) - EU (スペイン) - 欧州(ストックホルム) - EU (チューリッヒ) - 欧州 (フランクフルト) - 欧州 (アイルランド) - 欧州(ロンドン) - イスラエル (テルアビブ) - 中東(バーレーン) - 中東 (UAE) - 南米 (サンパウロ) - 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 ISO 西部 - 米国 ISOB 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) <p>デフォルトは [米国東部 (バージニア北部)] です。</p>
IAM ロール ARN	<p>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が引き受ける AWS Identity and Access Management (IAM) ロールの Amazon Resource Name (ARN)。</p> <p>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。</p> <p>このプロパティは、アプリケーション取り込みとレプリケーションタスクには適用されません。</p> <p>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。</p> <p>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。</p>
外部 ID	<p>AWS アカウントの外部 ID。</p> <p>外部 ID を使用すると、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が可能になります。</p>

資格情報プロファイルファイルの認証

資格情報プロファイルファイル認証には、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が必要です。

資格情報プロファイルファイルの認証は、詳細モードのマッピングには適用されません。

次の表に、資格情報プロファイルファイル認証の基本的な接続プロパティを示します。

プロパティ	説明
フォルダパス	Amazon S3 バケット名、または Amazon S3 オブジェクトが保存されている Amazon S3 バケット内のフォルダパス。 例: <バケット名>/<フォルダ名> アプリケーション取り込みとレプリケーションタスク、およびデータベース取り込みとレプリケーションタスクの場合は、末尾にスラッシュを追加します。 例: <バケット名>/<フォルダ名>/。
領域名	アクセス先のバケットの AWS 領域。 次のいずれかのリージョンを選択します。 <ul style="list-style-type: none">- アフリカ(ケープタウン)- アジアパシフィック(香港)- アジアパシフィック (ハイデラバード)- アジアパシフィック(ジャカルタ)- アジアパシフィック (メルボルン)- アジアパシフィック(大阪)- 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)- 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 (ミラノ)- 欧州(パリ)- EU (スペイン)- 欧州(ストックホルム)- EU (チューリッヒ)- 欧州 (フランクフルト)- 欧州 (アイルランド)- 欧州(ロンドン)- イスラエル (テルアビブ)- 中東(バーレーン)- 中東 (UAE)- 南米 (サンパウロ)- 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 ISO 西部- 米国 ISOB 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 [米国東部 (バージニア北部)] です。

プロパティ	説明
その他の認証タイプ	<p>資格情報プロファイルファイル認証を使用して Amazon S3 に接続するかどうかを決定します。</p> <p>次のいずれかの認証タイプを選択します。</p> <ul style="list-style-type: none"> - NONE。資格情報プロファイルファイル認証を使用しない場合に選択します。 - 認証情報プロファイルファイルの認証。資格情報プロファイルファイル認証を使用して、認証情報ファイルから Amazon S3 認証情報にアクセスする場合に選択します。 <p>注: IAM Roles Anywhere 認証も使用する場合は、認証タイプとして [資格情報プロファイルファイル認証] を選択する必要があります。</p> <p>認証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 に接続します。</p> <p>資格情報プロファイルファイル認証を設定する際は、永続的な IAM 資格情報または一時セッショントークンを使用できます。</p> <p>デフォルトは [なし] です。</p>
資格情報プロファイルのファイルパス	<p>資格情報プロファイルファイルへのパス。</p> <p>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、使用可能な資格情報プロファイルファイルを使用します。</p> <p>~/.aws/credentials</p> <p>注: データベース取り込みとレプリケーションは、[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。データベース取り込みとレプリケーションは、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。</p>
プロファイル名	<p>Amazon S3 リソースにアクセスするための資格情報を取得するため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。</p> <p>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。</p>

IAM Roles Anywhere 認証

AWS IAM Roles Anywhere 認証を設定して、長期資格情報の代わりに X.509 証明書を使用して、AWS 外部のサーバー、アプリケーション、またはコンテナから Amazon S3 リソースに安全にアクセスするための一時的なセキュリティ資格情報を生成できます。

IAM Roles Anywhere 認証には、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が必要です。

IAM Roles Anywhere 認証は、詳細モードのマッピングには適用されません。

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

プロパティ	説明
フォルダパス	<p>Amazon S3 バケット名、または Amazon S3 オブジェクトが保存されている Amazon S3 バケット内のフォルダパス。</p> <p>例: <バケット名>/<フォルダ名></p> <p>アプリケーション取り込みとレプリケーションタスク、およびデータベース取り込みとレプリケーションタスクの場合は、末尾にスラッシュを追加します。</p> <p>例: <バケット名>/<フォルダ名>/。</p>
領域名	<p>アクセス先のバケットの AWS 領域。</p> <p>次のいずれかのリージョンを選択します。</p> <ul style="list-style-type: none"> - アフリカ(ケープタウン) - アジアパシフィック(香港) - アジアパシフィック (ハイデラバード) - アジアパシフィック(ジャカルタ) - アジアパシフィック (メルボルン) - アジアパシフィック(大阪) - 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) - 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 (ミラノ) - 欧州(パリ) - EU (スペイン) - 欧州(ストックホルム) - EU (チューリッヒ) - 欧州 (フランクフルト) - 欧州 (アイルランド) - 欧州(ロンドン) - イスラエル (テルアビブ) - 中東(バーレーン) - 中東 (UAE) - 南米 (サンパウロ) - 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 ISO 西部 - 米国 ISOB 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) <p>デフォルトは [米国東部 (バージニア北部)] です。</p>
その他の認証タイプ	<p>IAM Roles Anywhere 認証を使用して Amazon S3 に接続するかどうかを指定します。</p> <p>IAM Roles Anywhere 認証を使用するには、[資格情報プロファイルファイルの認証] を選択します。</p> <p>認証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 に接続します。</p>

プロパティ	説明
資格情報プロファイルのファイルパス	資格情報プロファイルファイルへのパス。 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、使用可能な資格情報プロファイルファイルを使用します。 ~/.aws/credentials
プロファイル名	Amazon S3 リソースにアクセスするための資格情報を取得するため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、Secure Agent は資格情報プロファイルファイル内のデフォルトのプロファイルの資格情報を使用します。

フェデレーテッドシングルサインオン認証

フェデレーティッドユーザーシングルサインオン認証には、フェデレーティッドユーザーのユーザー名とパスワード、IdP SSO URL、SAML ID プロバイダの ARN、およびフェデレーティッドユーザーが引き受ける IAM ロールの ARN が必要です。SSO には ADFS 3.0 (IDP) のみを使用できます。

フェデレーションユーザーシングルサインオン認証は、詳細モードのマッピングには適用されません。

次の表に、フェデレーションシングルサインオン認証の基本的な接続プロパティとその説明を示します。

プロパティ	説明
フォルダパス	<p>Amazon S3 バケット名、または Amazon S3 オブジェクトが保存されている Amazon S3 バケット内のフォルダパス。</p> <p>例: <バケット名>/<フォルダ名></p> <p>アプリケーション取り込みとレプリケーションタスク、およびデータベース取り込みとレプリケーションタスクの場合は、末尾にスラッシュを追加します。</p> <p>例: <バケット名>/<フォルダ名>/。</p>
領域名	<p>アクセス先のバケットの AWS 領域。</p> <p>次のいずれかのリージョンを選択します。</p> <ul style="list-style-type: none"> - アフリカ(ケープタウン) - アジアパシフィック(香港) - アジアパシフィック (ハイデラバード) - アジアパシフィック(ジャカルタ) - アジアパシフィック (メルボルン) - アジアパシフィック(大阪) - 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) - 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 (ミラノ) - 欧州(パリ) - EU (スペイン) - 欧州(ストックホルム) - EU (チューリッヒ) - 欧州 (フランクフルト) - 欧州 (アイルランド) - 欧州(ロンドン) - イスラエル (テルアビブ) - 中東(バーレーン) - 中東 (UAE) - 南米 (サンパウロ) - 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 ISO 西部 - 米国 ISOB 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) <p>デフォルトは [米国東部 (バージニア北部)] です。</p>
フェデレーション SSO IDp	<p>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。</p> <p>SSO には ADFS 3.0 (IDP) のみを使用できます。</p> <p>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。</p> <p>注: フェデレーション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とレプリケーションタスク、データベース取り込みとレプリケーションタスク、およびストリーミング取り込みとレプリケーションタスクには適用されません。</p>

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とレプリケーション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。

詳細設定

次の表に、詳細接続のプロパティを示します。

プロパティ	説明
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。 <ul style="list-style-type: none"> - 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、 <code>http://s3.isv.scality.com</code> と指定します。
S3 VPC エンドポイントタイプ ¹	Amazon S3 用の Amazon Virtual Private Cloud エンドポイントのタイプ。 VPC エンドポイントを使用して、Amazon S3 とのプライベート通信を有効にすることができます。 次のいずれかのオプションを選択します。 <ul style="list-style-type: none"> - なし。VPC エンドポイントを使用しない場合に選択します。 - 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を介して Amazon S3 とのプライベート通信を確立する場合に選択します。ゲートウェイエンドポイントは、S3 トラフィックを S3 ゲートウェイエンドポイントに転送するために使用されるルートテーブル内のルートのターゲットです。 - インタフェースエンドポイント。サブネットの IP アドレス範囲のプライベート IP アドレスを使用するインタフェースエンドポイント経由で Amazon S3 とのプライベート通信を確立する場合に選択します。これは、AWS のサービス宛てのトラフィックのエントリポイントとして機能します。 デフォルトは「なし」です。 アプリケーション取り込みとレプリケーションタスク、またはデータベース取り込みとレプリケーションタスクには適用されません。

プロパティ	説明
Amazon S3 のエンドポイント DNS 名 ¹	<p>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。</p> <p>bucket.<インタフェースエンドポイントの DNS 名></p> <p>アプリケーション取り込みとレプリケーションタスク、またはデータベース取り込みとレプリケーションタスクには適用されません。</p>
STS VPC エンドポイントタイプ ¹	<p>AWS Security Token Service 用の Amazon Virtual Private Cloud エンドポイントのタイプ。</p> <p>このオプションは、S3 VPC インタフェースエンドポイントを選択し、IAM ユーザーまたは EC2 ロール認証またはフェデレーション SSO IdP 認証を介して AssumeRole を使用する場合に適用されます。</p> <p>アプリケーション取り込みとレプリケーションタスク、ストリーミング取り込みとレプリケーションタスク、またはデータベース取り込みとレプリケーションタスクには適用されません。</p>
AWS STS のエンドポイント DNS 名 ¹	<p>AWS STS インタフェースエンドポイントの DNS 名。</p> <p>アプリケーション取り込みとレプリケーションタスク、またはデータベース取り込みとレプリケーションタスクには適用されません。</p>
KMS VPC エンドポイントタイプ ¹	<p>AWS Key Management Service 用の Amazon Virtual Private Cloud エンドポイントのタイプ。</p> <p>このオプションは、S3 VPC インタフェースエンドポイントを選択したときに適用され、カスタママスターキー ID を指定するときに必要になります。</p> <p>アプリケーション取り込みとレプリケーションタスク、またはデータベース取り込みとレプリケーションタスクには適用されません。</p>
AWS KMS のエンドポイント DNS 名 ¹	<p>AWS KMS インタフェースエンドポイントの DNS 名。</p> <p>アプリケーション取り込みとレプリケーションタスク、またはデータベース取り込みとレプリケーションタスクには適用されません。</p>
マスタ対称キー	<p>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。</p> <p>アプリケーション取り込みとレプリケーションタスク、データベース取り込みとレプリケーションタスク、またはストリーミング取り込みとレプリケーションタスクには適用されません。</p>
顧客マスタキー ID	<p>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)。</p> <p>注: 詳細モードのマッピングでは、アカウント間アクセスは使用できません。</p> <p>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。</p> <p>次のマスタキーを指定できます。</p> <ul style="list-style-type: none"> - 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。 <p>アプリケーション取り込みとレプリケーションタスク、データベース取り込みとレプリケーションタスク、またはストリーミング取り込みとレプリケーションタスクには適用されません。</p>
¹ マッピングにのみ適用されます。	

Amazon S3 とのプライベート通信

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

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

詳細については、

「[Configuring private communication with Amazon S3 using the Amazon S3 V2 Connector](#)」を参照してください。

KMS を使用したサーバーサイド暗号化

AWS Key Management Service (AWS KMS) によって管理される顧客マスタキーを使用し、KMS による暗号化を有効にするには、KMS ポリシーを作成する必要があります。

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

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

参考までに、次のサンプル KMS ポリシーを参照してください。

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

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

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


サーバーレスランタイム環境でのクライアント側の暗号化

Amazon S3 V2 コネクタでサーバーレスランタイム環境を使用して、クライアントサイドの暗号化を設定できます。

サーバーレスランタイム環境を使用してクライアントサイド暗号化を設定する前に、.yaml サーバーレス構成ファイルを設定する必要があります。

.yaml サーバーレス構成ファイルを設定する

次の手順を実行して、サーバーレスランタイム環境で.yaml サーバーレス構成ファイルを設定し、Amazon S3 V2 コネクタがクライアントサイド暗号化を使用できるようにします。

1. 次のコードスニペットをテキストエディタにコピーします。

```
version: 1
agent:
  agentAutoApply:
    general:
      jdk:
        security:
          policyJars:
            - local_policy.jar
            - US_export_policy.jar
```

2. 構文とインデントが有効であることを確認してから、ファイルを serverlessUserAgentConfig.yaml として次の AWS または Azure の場所に保存します。

<Supplementary file location>/serverless_agent_config

.yaml ファイルの実行時に、ポリシー jar が AWS または Azure の場所からサーバーレスエージェントディレクトリにコピーされます。

3. .yaml 構成ファイルを更新した後、サーバーレスランタイム環境を再デプロイします。

接続プロパティでマスタ対称キーを指定し、詳細ソースプロパティおよび詳細ターゲットプロパティでクライアントサイドの暗号化タイプを指定します。

詳細モードのマッピングに対する SSE-KMS 暗号化

KMS による暗号化を有効にするには、AWS Key Management Service (AWS KMS) ポリシーと AWS KMS 管理の顧客マスタキーを作成します。

詳細モードのマッピングに SSE-KMS 暗号化を使用するには、次のいずれかのタスクを実行します。

- ~/.aws/credentials という場所からの資格情報を使用するには、AWS でマスタインスタンスプロファイルとワーカーインスタンスプロファイルを作成し、KMS ポリシーをワーカープロファイルにアタッチして、そのプロファイルをクラスタ設定に指定します。
- Amazon EC2 で Secure Agent を設定して AWS でマスタインスタンスプロファイルとワーカーインスタンスプロファイルを作成し、KMS ポリシーをワーカープロファイルにアタッチします。
- Amazon EC2 で Secure Agent を設定して、デフォルトの IAM ロールを使用し、KMS ポリシーを Secure Agent ロールにアタッチします。

プロキシサーバーの設定

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

Windows および Linux で、プロキシサーバーを使用するように Secure Agent を設定できます。

認証されていないプロキシサーバーのみを使用して Informatica Intelligent Cloud Services に接続できます。

Secure Agent のプロキシの設定を行うには、次のタスクを実行します。

- Windows の場合は Secure Agent Manager を使用し、Linux の場合はシェルコマンドを使用して Secure Agent を設定します。
手順については、データ統合のヘルプの『または「Windows でのプロキシ設定」または「Linux でのプロキシ設定」を参照してください。
- Secure Agent のプロパティで、DTM の JVM オプションを設定します。手順については、ナレッジベースの記事「[Proxy server settings](#)」を参照してください。
- proxy.ini ファイルでプロキシサーバーのプロパティを設定します。

サーバーレスランタイム環境を使用している場合、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。

プロキシサーバーのバイパス

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

ただし、特定の IP アドレスとホスト名をプロキシから除外する場合は、プロキシをバイパスできます。proxy.ini ファイルで *InfraAgent.NonProxyHost* プロパティを設定し、Secure Agent プロパティの JVM オプションで *-Dhttp.nonProxyHosts* プロパティを設定して、除外する IP アドレスとホスト名を含めます。

次の表は、proxy.ini ファイルまたは JVM オプションを使用して設定できるプロキシ設定を示しています。

プロキシ設定	プロキシフラグの設定
Proxy.ini	<code>InfraAgent.NonProxyHost=localhost <your_bucket_name>.s3. 127.* [\:\:1]</code> 例えば、単一の S3 バケット <code>iam.qa.bucket</code> をバイパスするには、次のプロキシ設定を使用します。 <code>InfraAgent.NonProxyHost=localhost iam.qa.bucket.s3. 127.* [\:\:1]</code> すべての S3 バケットをバイパスするには、次のプロキシ設定を使用します。 <code>InfraAgent.NonProxyHost=localhost *.s3.* 127.* [\:\:1]</code>
JVM オプション	<code>-Dhttp.nonProxyHosts=localhost <your_bucket_name>.s3. 127.* [\:\:1]</code> 例えば、単一の S3 バケット <code>iam.qa.bucket</code> をバイパスするには、次のプロキシ設定を使用します。 <code>-Dhttp.nonProxyHosts=localhost iam.qa.bucket.s3. 127.* [\:\:1]</code> すべての S3 バケットをバイパスするには、次のプロキシ設定を使用します。 <code>-Dhttp.nonProxyHosts=localhost *.s3.* 127.* [\:\:1]</code>

詳細モードでのプロキシサーバーのバイパス

プロキシサーバーをバイパスするには、proxy.ini ファイルの *NonProxyHost* 値を更新する必要があります。エージェントコアパスでプロパティを設定して、詳細クラスタ設定で *NonProxyHost* を設定できます。

Amazon S3 エンドポイントでプロキシをバイパスするには、次の手順を実行します。

1. proxy.ini ファイルを編集し、NonProxyHost のプロパティにクラスタリージョンを設定します。
2. 適切なリージョン名をプロパティに次の形式で入力します。
`InfAgent.NonProxyHost=localhost|127.*|[\:\:1]|169.254.169.254|. <REGION_NAME>.elb.amazonaws.com|
*. <REGION_NAME>.elb.amazonaws.com`
次の例は、proxy.ini ファイルでの、米国西部リージョンの場合の NonProxyHost を更新する方法を示しています。
`InfAgent.NonProxyHost=localhost|127.*|[\:\:1]|169.254.169.254|.us-west-2.elb.amazonaws.com|*.us-
west-2.elb.amazonaws.com|s3.us-west-2.amazonaws.com|*.s3.us-west-2.amazonaws.com|s3.amazonaws.com`
3. proxy.ini ファイルを編集したら、詳細クラスタのランタイムプロパティで、プロパティ `ccs.enable.storage.proxy.settings` を `false` に設定する必要があります。
プロパティを設定するには、次の手順を実行します。
 - a. **Administrator** に移動します。
 - b. **【詳細クラスタ】** ページで、編集する設定の名前を詳細設定のリストから選択します。
 - c. プロパティ `ccs.enable.storage.proxy.settings` を `false` に設定し、クラスタ設定を特定のクラスタの **【ランタイムプロパティ】** に保存します。
次の図は、設定したクラスタのランタイムプロパティを示しています。

Runtime Properties (4): ?

Key ↑ ▲	Value
ccs.enable.storage.proxy.settings	false
ccs.k8s.api.access.cidr	172.31.74.13/32
ccs.k8s.ssh.access.cidr	172.31.74.13/32
ccs.ssh.access.cidr	172.31.74.13/32

IAM ユーザー経由の AssumeRole のルールとガイドライン認証

IAM ユーザー認証によるロールの引き受けについては、次のガイドラインを考慮してください。

- 一時的なセキュリティ認証情報を要求する IAM ユーザーまたは IAM ロールは、AWS リソースへのアクセス権を持ってはいけません。
- 認証済み IAM ユーザーまたは IAM ロールのみ、AWS Security Token Service (AWS STS) から一時セキュリティ資格情報を要求できます。
- タスクを実行する前に、一時セキュリティ資格情報の有効期間が、そのタスクを実行するのに十分な長さであることを確認してください。実行中のタスクに対して、一時セキュリティ資格情報の有効期間を延長することはできません。
例えば、Amazon S3 に対して読み取りと書き込みを行って、一時的なセキュリティ資格情報の有効期限が切れた場合、一時的なセキュリティ資格情報の期間を延長することはできないため、タスクが失敗します。

- 一時セキュリティ資格情報の有効期限が切れると、AWS は、その資格情報を使ったリソースへのアクセスを IAM ユーザーまたは IAM ロールに許可しません。マッピングで現在使用している一時セキュリティ資格情報の有効期限が切れる前に、新しい一時セキュリティ資格情報を要求する必要があります。
- 詳細モードのマッピングの場合、**【一時的な資格情報の期間】**の詳細なソースプロパティで設定した時間が経過した後でも、一時的なセキュリティ資格情報は期限切れにはなりません。
- 一時セキュリティ資格情報を使用するのに、AWS アカウントのルートユーザー資格情報を使用しないでください。一時セキュリティ資格情報を使用するには、IAM ユーザーの資格情報を使用する必要があります。
- マッピング内のソースとターゲットの両方が同じ Amazon S3 バケットを指している場合は、ソーストランスフォーメーションとターゲットトランスフォーメーションで同じ Amazon S3 接続が使用されます。異なる 2 つの Amazon S3 接続を使用する場合は、両方の接続に対して接続プロパティで同じ値を設定します。
- マッピング内のソースとターゲットが異なる Amazon S3 バケットを指している場合、異なる 2 つの Amazon S3 接続を使用できます。
両方の接続に対して、接続プロパティで異なる値を設定できます。ただし、接続プロパティで**【ロールの引き受けに EC2 ロールを使用】**チェックボックスをオンにする必要があります。また、ソースプロパティとターゲットプロパティの**【一時的な資格情報の期間】**フィールドにも同じ値を指定する必要があります。
- マッピングで、異なる IAM ロールを持つ同じ Amazon S3 バケットに対して 2 つ以上の Amazon S3 データソースを設定した場合、各 IAM ロールが他の IAM ロールのデータソースにアクセスできるようにする必要があります。
- 2 つのデータソースを持つマッピングで、一方の Amazon S3 データソースはユーザー資格情報を使用するように設定し、もう一方のデータソースは IAM ロールを使用するように設定する場合は、次のルールを考慮してください。
 - 最初のデータソースの IAM ユーザーは、2 番目の Amazon S3 データソースの IAM ロールを引き受けることもできるようにする必要があります。
 - 2 番目のデータソース用に設定した IAM ロールは、最初の Amazon S3 データソースへのアクセス権を持つようにする必要もあります。

AWS リージョンのルールとガイドライン

接続プロパティでバケットのリージョン名を設定する場合は、次のルールとガイドラインを考慮してください。

- 既存の接続のランタイム環境を変更すると、リージョンはデフォルトのリージョン US East (N. Virginia) に変更されます。リージョンを手動で選択して、デフォルトのリージョンを変更します。
- 既存の接続を編集すると、リージョンのエントリが重複して表示されます。これらのリージョンは AWS SDK から入力されるため、スペースを含むリージョンを使用します。例えば、US West (Oregon) ではなく US West(Oregon)を使用します。

S3 互換ストレージのルールおよびガイドライン

Amazon S3 V2 接続で S3 互換のストレージを設定する場合は、次のルールとガイドラインを考慮してください。

- S3 互換ストレージを使用する場合にのみ、基本認証を設定できます。
- Scality RING S3 互換ストレージに SSE-KMS 暗号化を設定することはできません。MinIO S3 互換ストレージに SSE および SSE-KMS 暗号化を設定することはできません。

- Amazon S3 ソースから Amazon Redshift にデータをロードするように SQL ELT の最適化を設定することはできません。

第 25 章

Amazon SageMaker レイクハウスの接続プロパティ

Amazon SageMaker レイクハウス接続を作成することで、AWS Glue データカタログまたは S3 テーブルカタログによって管理されて Amazon S3 に保存されている Apache Iceberg テーブルのデータを、安全に読み書きできます。

Amazon SageMaker レイクハウス接続を使用することで、詳細モードのマッピングとマッピングタスクでソースとターゲットを指定できます。

前提条件

Amazon SageMaker レイクハウス接続を作成する前に、「AWS Glue カタログまたは S3 テーブルカタログによって管理される Apache Iceberg テーブルを操作するには最小限のアクセス許可が必要である」とする IAM ポリシーを作成する必要があります。

Amazon S3 で「EC2 ロールによるロール引き受け」認証を使用するには、IAM ロールの ARN で指定されている別の IAM ロール引き受けを設定する必要があります。

最小限の IAM ポリシーの作成

「AWS Glue カタログまたは S3 テーブルカタログによって管理される Apache Iceberg テーブルを操作するには、最小限の権限を持つ必要がある」とする IAM ポリシーを作成する必要があります。これらのポリシーの設定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。

Amazon Athena の最小限のポリシー

次のサンプルポリシーは、Amazon Athena にアクセスするための最小限の Amazon IAM ポリシーを示しています。

```
{
  "Version": "2025-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": [
        "athena:CreatePreparedStatement",
        "athena:GetPreparedStatement",
        "athena:GetWorkGroup",
        "athena:GetTableMetadata",
        "athena:StartQueryExecution",
        "athena:GetQueryResultsStream",
```

```

        "athena:ListDatabases",
        "athena:GetQueryExecution",
        "athena:GetQueryResults",
        "athena:GetDatabase",
        "athena:ListTableMetadata",
        "athena:GetDataCatalog",
        "athena>DeletePreparedStatement"
    ],
    "Resource": [
        "arn:aws:athena:*:*:workgroup/*",
        "arn:aws:athena:*:*:datacatalog/*"
    ]
},
{
    "Sid": "VisualEditor1",
    "Effect": "Allow",
    "Action": [
        "athena:ListDataCatalogs",
        "athena:GetQueryExecution",
        "athena:ListWorkGroups",
        "athena:GetPreparedStatement"
    ],
    "Resource": "*"
}
]
}

```

AWS Glue の最小限のポリシー

次のサンプルポリシーは、AWS Glue カタログにアクセスするための最小限の Amazon IAM ポリシーを示しています。

```

{
    "Version": "2025-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "glue:*"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}

```

Amazon S3 の最小限のポリシー

次のサンプルポリシーは、Amazon S3 バケットに対してデータの読み取りと書き込みを行うための最小限の Amazon IAM ポリシーを示しています。

```

{
    "Version": "2025-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "s3:PutObject",
                "s3:GetObject",
                "s3:ListBucket",
                "s3:DeleteObject"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:ListBucket",
                "s3:GetBucketLocation",

```

```

        "s3:ListAllMyBuckets",
        "s3:GetBucketAcl"
    ],
    "Resource": [
        "*"
    ]
}
]
}

```

S3 テーブルに対する最小限のポリシー

次のサンプルポリシーは、S3 テーブルに対してデータの読み取りと書き込みを行うための最小限の Amazon IAM ポリシーを示しています。

```

{
  "Version": "2025-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "sts:AssumeRole",
      "Resource": "arn:aws:iam::001234567890:role/S3TableSparkrole"
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3tables:CreateTable",
        "s3tables:GetTable",
        "s3tables:ListTables",
        "s3tables:DeleteTable",
        "s3tables:GetTableMetadataLocation",
        "s3tables:GetTableData",
        "s3tables:PutTableData",
        "s3tables:UpdateTableMetadataLocation"
      ],
      "Resource": [
        "arn:aws:s3tables:us-east-1:001234567890:bucket/sagemaker-s3tables",
        "arn:aws:s3tables:us-east-1:001234567890:bucket/sagemaker-s3tables/*",
        "arn:aws:s3tables:us-east-1:001234567890:bucket/sagemaker-s3tables/table/*"
      ]
    }
  ]
}

```

AWS Lake Formation に対する最小限のポリシー

次のサンプルポリシーは、AWS Lake Formation にアクセスするための最小限の Amazon IAM ポリシーを示しています。

```

{
  "Version": "2025-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": "lakeformation:*",
      "Resource": "*"
    }
  ]
}

```

ロールを引き受けるための EC2 ロールの設定

IAM ロールを引き受けるように EC2 ロールを設定し、同じ AWS アカウントまたは異なる AWS アカウントから Amazon S3 に接続するための一時的なセキュリティ資格情報を生成できます。

IAM ロールを引き受けるように EC2 ロールを設定する場合は、一時的なセキュリティ資格情報を使用するための **sts:AssumeRole** 権限が割り当てられており、AWS アカウント内で信頼関係が確立されていることを確認

してください。信頼関係は、ロールを作成するときに、IAM ロールの信頼ポリシーで定義されます。IAM ロールにより、EC2 ロールを信頼されたエンティティとして追加し、EC2 ロールに一時的なセキュリティ資格情報の使用と AWS アカウントへのアクセスを許可します。

信頼された EC2 ロールが一時的なセキュリティ資格情報を要求すると、AWS Security Token Service (AWS STS) によって、指定した期間有効な一時的なセキュリティ資格情報が動的に生成され、信頼された EC2 ロールにその資格情報が提供されます。

ロール認証を引き受けるための EC2 ロールを使用する前に、次の前提条件を考慮してください。

- AWS EC2 インスタンスに Secure Agent をインストールします。
- AWS EC2 インスタンスにアタッチされた EC2 ロールには、別の IAM ロールを引き受ける権限が必要です。以下のコードスニペットは、AWS EC2 インスタンスにアタッチされている EC2 ロールの権限ポリシーの例です。

```
{
  "Version": "2025-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "sts:AssumeRole",
      "Resource": "arn:aws:iam::001234567890:role/sagemaker_rolearn"
    }
  ]
}
```

リソース値には、EC2 ロールが引き受ける必要がある IAM ロールの ARN を含める必要があります。

- EC2 ロールが引き受ける必要のある IAM ロールには、AWS Glue カタログ、Amazon Athena、および Amazon S3 にアクセスするための権限ポリシーと信頼ポリシーがアタッチされている必要があります。また、より安全なアクセスのために、AWS アカウントの外部 ID を指定することもできます。外部 ID は文字列である必要があります。

次のコードスニペットは、引き受けられる IAM ロールの信頼ポリシー、および外部 ID を示しています。

```
{
  "Version": "2025-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::001234567890:root" // anyone in the account 001234567890 can assume
        this role, this can also be limited to one role.
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "sts:ExternalId": "aws_externalid"
        }
      }
    }
  ]
}
```

Amazon SageMaker レイクハウスへの接続

Amazon SageMaker レイクハウスに接続して AWS Glue カタログまたは S3 テーブルカタログによって管理されている Apache Iceberg テーブルを読み取ることができるように、Amazon SageMaker レイクハウスの接続プロパティを設定してみましょう。

始める前に

開始する前に、Apache Iceberg テーブルを操作して Amazon S3 ストレージの認証固有の前提条件を設定するために必要な、最小限の権限を持つ IAM ポリシーを作成する必要があります。

ポリシーの作成方法と認証固有の前提条件の設定方法の詳細については、「[「前提条件」 \(ページ 138\)](#)」を参照してください。

接続の詳細

次の表に、基本接続プロパティを示します。

プロパティ	説明
接続名	接続の名前。 各接続名は組織内で一意である必要があります。接続名には、英数字、スペース、および次の特殊文字を含めることができます。_ . + - , 最大長は 255 文字です。
説明	接続の説明。最大長は 4000 文字です。
シークレットコンテナの使用	組織に対して設定されている Secrets Manager にこの接続の機密資格情報を保存します。 このプロパティは、組織に Secrets Manager が設定されている場合にのみ表示されます。 このプロパティは、データ取り込みおよびレプリケーションとデータアクセス管理サービスではサポートされていません。 接続でシークレットコンテナを有効にすると、Secure Agent が Secrets Manager からどの資格情報を取得するかを選択できます。このオプションを無効にした場合、資格情報は組織の設定方法に応じてリポジトリまたはローカル Secure Agent に保存されます。 注: この接続を使用してプッシュダウンまたはプロキシサービスを介してデータアクセスポリシーを適用する場合、シークレットコンテナ設定オプションを使用することはできません。 Secrets Manager を設定および使用方法については、Administrator のヘルプにある「Secrets Manager の設定」を参照してください。
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。 Secure Agent を選択します。 Hosted Agent、エラスティックランタイム環境、およびサーバーレスランタイム環境は使用できません。 ランタイム環境の設定および使用方法の詳細については、Administrator のヘルプにある「ランタイム環境」を参照してください。

プロパティ	説明
レイクハウスのパターン	<p>Amazon SageMaker Lakehouse のパターン。パターンとは、接続先のカatalogタイプとストレージタイプの組み合わせです。</p> <p>次のいずれかのオプションを選択します。</p> <ul style="list-style-type: none"> - [S3 データレイク]。AWS Glue データCatalogによって管理されて Amazon S3 に保存されている Apache Iceberg テーブルの読み取りと書き込みを行う場合に選択します。 - [S3 テーブル]。S3 テーブルデータCatalogによって管理されて Amazon S3 に保存されている Apache Iceberg テーブルの読み取りと書き込みを行う場合に選択します。 <p>S3 テーブルのレイクハウスパターンがプレビュー可能です。プレビュー機能は評価を目的としてサポートされていますが、保証対象外で、本番環境または本番環境にプッシュする予定の環境には対応していません。Informatica は、本番環境用の今後のリリースにプレビュー機能を含める予定ですが、市場や技術的な状況の変化に応じて導入を行わ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。</p>
Athena JDBC URL	<p>Amazon Athena に接続するための JDBC URL。</p> <p>S3 データレイクのレイクハウスパターンの場合は、JDBC URL を次の形式で入力します。</p> <pre>jdbc:athena://Region=<AWS_Region>;OutputLocation=<S3_Location></pre> <p>S3 テーブルのレイクハウスパターンの場合は、JDBC URL を次の形式で入力します。</p> <pre>jdbc:athena://AwsRegion=us-east-1;Catalog=s3tablescatalog/your-bucket-name;Schema=your_namespace;</pre> <p>s3tablescatalog/your-bucket-name は S3 テーブルバケットCatalogで、your_namespace はテーブルが保存されている名前空間です。</p>

ストレージ認証タイプ

Amazon S3 ストレージに接続するには、永続的な IAM 資格情報または「EC2 ロールによるロール引き受け」認証を使用します。

永続的な IAM 資格情報認証

永続的な IAM 資格情報認証には、Amazon S3 ストレージに接続するためのアクセスキーとシークレットキーの値が必要です。

次の表に、永続的な IAM 資格情報認証を設定するためのプロパティを示します。

プロパティ	説明
アクセスキー	Amazon S3 ストレージにアクセスするための IAM ユーザー資格情報を一意に識別する AWS アクセスキー ID。
シークレットキー	S3 データに安全にアクセスするためにアクセスキー ID を認証する AWS シークレットアクセスキー。

ロール認証を引き受けるための EC2 ロール

ロール認証を引き受けるための EC2 ロール（「EC2 ロールによるロール引き受け」認証）には、EC2 ロールが引き受ける IAM ロールの ARN が必要です。

次の表に、ロール認証を引き受けるように EC2 ロール（「EC2 ロールによるロール引き受け」認証）を設定するためのプロパティを示します。

プロパティ	説明
IAM ロール ARN	EC2 ロールが一時的なセキュリティ資格情報を生成するために引き受ける IAM ロールの ARN。

詳細設定

次の表に、詳細接続のプロパティを示します。

プロパティ	説明
外部 ID	sts:AssumeRole API を呼び出すときに IAM ロールが EC2 ロールに指定するように求めるユーザー定義の一意的文字列値。

第 26 章

Amplitude 接続プロパティ

Amplitude 接続を作成する際に、接続プロパティを設定します。

次の表に、Amplitude 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。
シークレットコンテナの使用	組織に対して設定されている Secrets Manager にこの接続の機密資格情報を保存します。 このプロパティは、組織に Secrets Manager が設定されている場合にのみ表示されます。 このプロパティは、データ取り込みおよびレプリケーションとデータアクセス管理サービスではサポートされていません。 接続でシークレットコンテナを有効にすると、Secure Agent が Secrets Manager からどの資格情報を取得するかを選択できます。このオプションを無効にした場合、資格情報は組織の設定方法に応じてリポジトリまたはローカル Secure Agent に保存されます。 注: この接続を使用してプッシュダウンまたはプロキシサービスを介してデータアクセスポリシーを適用する場合、シークレットコンテナ設定オプションを使用することはできません。 Secrets Manager を設定および使用方法については、Administrator のヘルプにある「Secrets Manager の設定」を参照してください。
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。 Secure Agent または Hosted Agent を指定できます。 ランタイム環境の設定および使用方法の詳細については、Administrator のヘルプにある「ランタイム環境」を参照してください。
API キー	Amplitude アカウントにアクセスするための API キー。
シークレットキー	Amplitude アカウントのシークレットキー。

第 27 章

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。
ランタイム環境	タスクを実行するランタイム環境の名前。
ホスト名	AMQP ブローカーのネットワークアドレス。
ポート	基盤となる TCP 接続が確立される AMQP ブローカーのポート番号。 デフォルトは 5672 です。
仮想ホスト	AMQP システムを識別する仮想ホスト名。 セキュリティを強化するために仮想ホスト名を使用します。
ユーザー名	AMQP ブローカーのユーザー名。
パスワード	AMQP ブローカーのパスワード。
SSL の使用	安全な送信のために SSL を使用するには、このオプションを有効にします。 SSL 認証を有効にする場合は、ストリーミング取り込みとレプリケーションタスクで 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。

プロパティ	説明
キーストアのタイプ	<p>使用するキーストアのタイプ。</p> <p>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。</p> <p>次のいずれかのタイプを使用してください:</p> <ul style="list-style-type: none"> - 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	<p>使用するトラストストアのタイプ。</p> <p>次のいずれかのタイプを使用してください:</p> <ul style="list-style-type: none"> - JKS - PKCS12
TLS プロトコル	<p>使用するトランスポートプロトコル。</p> <p>次のいずれかのタイプを使用してください:</p> <ul style="list-style-type: none"> - SSL - SSLv2Hello - SSLv3 - TLS - TLSv1 - TLSv1.1 - TLSv1.2
クライアント認証	<p>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。</p> <p>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。</p> <ul style="list-style-type: none"> - WANT - REQUIRED - NONE

第 28 章

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。
シークレットコンテナの使用	<p>組織に対して設定されている Secrets Manager にこの接続の機密資格情報を保存します。このプロパティは、組織に Secrets Manager が設定されている場合にのみ表示されます。このプロパティは、データ取り込みおよびレプリケーションとデータアクセス管理サービスではサポートされていません。</p> <p>接続でシークレットコンテナを有効にすると、Secure Agent が Secrets Manager からどの資格情報を取得するかを選択できます。このオプションを無効にした場合、資格情報は組織の設定方法に応じてリポジトリまたはローカル Secure Agent に保存されます。</p> <p>注: この接続を使用してプッシュダウンまたはプロキシサービスを介してデータアクセスポリシーを適用する場合、シークレットコンテナ設定オプションを使用することはできません。</p> <p>Secrets Manager を設定および使用方法については、Administrator のヘルプにある「Secrets Manager の設定」を参照してください。</p>
ランタイム環境	<p>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。</p> <p>ランタイム環境の設定および使用方法の詳細については、Administrator のヘルプにある「ランタイム環境」を参照してください。</p>
認証タイプ	<p>コネクタが Anaplan へログインするために使用する認証のタイプ。</p> <p>以下のいずれかの認証タイプを選択できます。</p> <ul style="list-style-type: none">- 基本認証。Anaplan に接続するには、Anaplan アカウントのユーザー名とパスワードが必要です。- 証明書認証。認証トークンを取得するには認証局（CA）が必要です。- OAuth デバイスフロー。アプリ間でユーザーデータを認証するには、OAuth 2.0 クライアント資格情報が必要です。 <p>デフォルトは基本認証です。</p> <p>注: Windows 環境を使用し、認証タイプとして [OAuth デバイスフロー] を選択して Anaplan にログインする場合は、Secure Agent がシステムルートディレクトリと同じドライブにインストールされていることを確認してください。</p>
ユーザー名	<p>Anaplan にログインするユーザー名。例: firstname.lastname@anaplan.com。</p> <p>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。</p>

接続プロパティ	説明
パスワード	[ユーザー名] プロパティで指定されたユーザー名に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 を使用する場合があります。 これは、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」で、メジャーバージョンが 1、マイナーバージョンが 3 である場合のみであることを意味します。
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://us1a.app.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。
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 を使用する場合があります。
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。

接続プロパティ	説明
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。
ClientId	OAuth デバイスフローの場合は必須です。アプリケーション登録プロセス中にクライアントに発行されるクライアント識別子。
トークン	<p>OAuth デバイスフローの場合は必須です。更新トークンは、新しいアクセストークンを取得するために使用されます。</p> <p>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。</p> <ul style="list-style-type: none"> - ローテーション可能。更新トークンを有効期間中に 1 回使用します。 - ローテーション不可。更新トークンを複数回使用します。ローテーション不可のトークンには有効期限がありません。

第 29 章

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	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。
シークレットコンテナの使用	組織に対して設定されている Secrets Manager にこの接続の機密資格情報を保存します。 このプロパティは、組織に Secrets Manager が設定されている場合にのみ表示されます。 このプロパティは、データ取り込みおよびレプリケーションとデータアクセス管理サービスではサポートされていません。 接続でシークレットコンテナを有効にすると、Secure Agent が Secrets Manager からどの資格情報を取得するかを選択できます。このオプションを無効にした場合、資格情報は組織の設定方法に応じてリポジトリまたはローカル Secure Agent に保存されます。 注: この接続を使用してプッシュダウンまたはプロキシサービスを介してデータアクセスポリシーを適用する場合、シークレットコンテナ設定オプションを使用することはできません。 Secrets Manager を設定および使用する方法については、Administrator のヘルプにある「Secrets Manager の設定」を参照してください。
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。 Secure Agent、ホステッドエージェント、サーバーレスランタイム環境、またはエラスティックランタイム環境を選択します。 ランタイム環境の設定および使用方法の詳細については、Administrator のヘルプにある「ランタイム環境」を参照してください。
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。

接続プロパティ	説明
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。
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。

第 30 章

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。
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。

接続プロパティ	説明
接続タイムアウト	<p>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。</p> <p>値が 0 または空白の場合、待機時間は無限です。</p> <p>デフォルトは 60 秒です。</p>
読み取りタイムアウト	<p>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。</p> <p>値が 0 または空白の場合、待機時間は無限です。</p> <p>デフォルトは 0 秒です。</p>
接続の再試行	<p>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。</p> <p>値が空白の場合、再試行は行われません。</p> <p>デフォルトは空白です。</p>
接続再試行の間隔	<p>接続の再試行ごとに待機する秒数。</p> <p>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。</p> <p>値が空白の場合、間隔は 0 秒になります。</p> <p>デフォルトは空白です。</p>
リダイレクトのフォロー	<p>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。</p> <p>デフォルトは false です。</p>
ユーザーエージェント	<p>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われる値。</p>
チャンクエンコードの使用	<p>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。</p> <p>デフォルトは false です。</p>
クライアント証明書エイリアス	<p>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。</p>
SSL コンテキストプロトコル	<p>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。</p> <p>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。</p> <p>デフォルトは SSL です。</p>

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。 <ul style="list-style-type: none">- 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。 <ul style="list-style-type: none">- SHA1- SHA224- SHA256- SHA384- SHA512- MD5 デフォルトは SHA1 です。
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。

接続プロパティ	説明
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。
コンテンツタイプ	ソースファイルの MIME タイプ。 デフォルトは application/EDI-Consent 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	<p>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。</p> <p>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。</p> <p>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。</p>
受信確認転送エンコード	<p>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。</p> <p>以下のいずれかの値を使用します。</p> <ul style="list-style-type: none"> - base64 - quoted-printable - 7bit - 8bit - binary
受信確認要求	<p>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。</p> <ul style="list-style-type: none"> - 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。 <p>デフォルトは [なし] です。</p>
宛先	<p>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。</p> <p>次のいずれかの値を選択します。</p> <ul style="list-style-type: none"> - 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。 <p>デフォルトは Joblog です。</p>
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	<p>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。</p> <p>次のいずれかの値を選択します。</p> <ul style="list-style-type: none"> - 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。 <p>デフォルトは「名前の変更」です。</p>
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	<p>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。</p> <p>デフォルトでは無効になっています。</p>
プロキシタイプ	<p>この接続に使用するプロキシサーバーのタイプ。</p> <p>次のいずれかのタイプを選択します。</p> <ul style="list-style-type: none"> - 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。 <p>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。</p>
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。

第 31 章

Azure AI Search 接続のプロパティ

Azure AI Search ベクトルデータベースにデータを安全に書き込むために、Azure AI Search 接続を作成します。

前提条件

接続プロパティを設定する前に、次の前提条件を完了してください。

1. Azure ポータルで Azure AI Search サービスを作成します。
2. Azure AI Search API へのアクセスを認証するために、Azure AI Search サービスの API キーを生成します。
サービスの作成方法と API キーの生成方法の詳細については、「[Create an Azure AI Search service](#)」を参照してください。

Azure AI Search への接続

Azure AI Search に Azure AI Search 接続プロパティを設定してみましょう。

始める前に

開始する前に、Azure AI Search サービスアカウントから API キーを取得する必要があります。

接続を設定する前に、「[前提条件](#)」 ([ページ 158](#))を参照して認証要件を確認してください。

接続の詳細

次の表に、基本接続プロパティを示します。

プロパティ	説明
接続名	接続の名前。 各接続名は組織内で一意である必要があります。接続名には、英数字、スペース、および次の特殊文字を含めることができます。_ . + - , 最大長は 255 文字です。
説明	接続の説明。最大長は 4000 文字です。
シークレットコンテナの使用	組織に対して設定されている Secrets Manager にこの接続の機密資格情報を保存します。 このプロパティは、組織に Secrets Manager が設定されている場合にのみ表示されます。 このプロパティは、データ取り込みおよびレプリケーションとデータアクセス管理サービスではサポートされていません。 接続でシークレットコンテナを有効にすると、Secure Agent が Secrets Manager からどの資格情報を取得するかを選択できます。このオプションを無効にした場合、資格情報は組織の設定方法に応じてリポジトリまたはローカル Secure Agent に保存されます。 注: この接続を使用してプッシュダウンまたはプロキシサービスを介してデータアクセスポリシーを適用する場合、シークレットコンテナ設定オプションを使用することはできません。 Secrets Manager を設定および使用方法については、Administrator のヘルプにある「Secrets Manager の設定」を参照してください。
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。 Secure 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。 ランタイム環境の設定および使用方法の詳細については、Administrator のヘルプにある「ランタイム環境」を参照してください。
ホスト名	接続する Azure 検索サービスのホスト名。 例: https://rnddev.search.windows.net
API キー	Azure AI Search 接続要求を認証するための管理 API キー。 例: yavMPJHTY11p08JTPkM3NW1ImhJraYycrLAzSeCEQQ5j

第 32 章

BigMachines 接続のプロパティ

BigMachines 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、BigMachines 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。
シークレットコンテナの使用	組織に対して設定されている Secrets Manager にこの接続の機密資格情報を保存します。 このプロパティは、組織に Secrets Manager が設定されている場合にのみ表示されます。 このプロパティは、データ取り込みおよびレプリケーションとデータアクセス管理サービスではサポートされていません。 接続でシークレットコンテナを有効にすると、Secure Agent が Secrets Manager からどの資格情報を取得するかを選択できます。このオプションを無効にした場合、資格情報は組織の設定方法に応じてリポジトリまたはローカル Secure Agent に保存されます。 注: この接続を使用してプッシュダウンまたはプロキシサービスを介してデータアクセスポリシーを適用する場合、シークレットコンテナ設定オプションを使用することはできません。 Secrets Manager を設定および使用方法については、Administrator のヘルプにある「Secrets Manager の設定」を参照してください。
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。 Secure Agent、ホステッドエージェント、サーバーレスランタイム環境、またはエラスティックランタイム環境を選択します。 ランタイム環境の設定および使用方法の詳細については、Administrator のヘルプにある「ランタイム環境」を参照してください。
ユーザー名	BigMachines アカウントのユーザー名。
パスワード	BigMachines アカウントのパスワード。

プロパティ	説明
DataTables スキーマのパス	<p>データテーブルスキーマファイルのパスを指定します。</p> <p>例: <code>:\...\...\BigMachines\config\Datatables.tbl</code></p> <p>注: データテーブルスキーマファイルの名前には、.tbl 拡張子が含まれる必要があります。スキーマファイル内に記述されるテーブルヘッダー名には、同じディレクトリ内の個別の.sch ファイルがある必要があります。.sch ファイルによって、スキーマファイル内にあるテーブル名のフィールドの詳細が定義されます。</p>
WSDL フォルダのパス	<p>WSDL ファイルのパスを指定します。</p> <p>注: 接続プロパティで WSDL URL を指定しないと、デフォルトの WSDL ファイルのパスが、WSDL URL として選択されます。</p> <p>デフォルトの WSDL URL ファイルのパスは次のとおりです。<Secure Agent のインストールディレクトリ>\downloads\<最新のコネクタ zip パッケージ>\package\plugins\<プラグイン ID>\<WSDL>\</p>
エンドポイント URL	BigMachines エンドポイント URL のパス。
属性制御ファイルのパス	<p>属性制御のパスを指定します。属性制御のパスによって、メタデータが制御されます。デフォルトの制御ファイルのパスは次のとおりです。<Secure Agent のインストールディレクトリ>\downloads\<最新のコネクタ zip パッケージ>\package\plugins\</p>
ロギングの有効化	ロギングを有効にするには、このプロパティを選択します。
ページサイズ	各要求につき取得するレコード数。
トランザクションスキーマ名	トランザクションを取得するための REST ドキュメント名。
トランザクション行項目スキーマ名	トランザクション行項目の詳細を取得するための REST ドキュメント名。
バッチサイズ	データテーブルオブジェクトに対して一括更新/挿入操作操作を実行するためのバッチサイズを指定します。

第 33 章

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。
シークレットコンテナの使用	<p>組織に対して設定されている Secrets Manager にこの接続の機密資格情報を保存します。</p> <p>このプロパティは、組織に Secrets Manager が設定されている場合にのみ表示されます。</p> <p>このプロパティは、データ取り込みおよびレプリケーションとデータアクセス管理サービスではサポートされていません。</p> <p>接続でシークレットコンテナを有効にすると、Secure Agent が Secrets Manager からどの資格情報を取得するかを選択できます。このオプションを無効にした場合、資格情報は組織の設定方法に応じてリポジトリまたはローカル Secure Agent に保存されます。</p> <p>注: この接続を使用してプッシュダウンまたはプロキシサービスを介してデータアクセスポリシーを適用する場合、シークレットコンテナ設定オプションを使用することはできません。</p> <p>Secrets Manager を設定および使用する方法については、Administrator のヘルプにある「Secrets Manager の設定」を参照してください。</p>
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。

第 34 章

Box 接続のプロパティ

Box 接続を作成して、Box に対するデータの読み取りおよび Box へのデータの書き込みを行います。

Box への接続

Box に接続するように Box の接続プロパティを設定してみましょう。

始める前に

開始する前に、Box アカウントの OAuth を設定する必要があります。

OAuth を設定する場合は、`redirect_URI` パラメータを指定します。Box は、Box 接続の認証 URL で渡された `redirect_uri` パラメータが、アプリケーション用に設定されたリダイレクト URI と一致することを確認します。

Box 接続を設定する場合は、接続でアクセストークンを自動生成するか、手動でトークンを生成するかを選択することができます。トークン生成プロセスを自分で処理する場合は、Box で OAuth の設定時に、アクセストークンと、認証タイプ、クライアント ID、クライアントシークレットを手動で生成することができます。

Box にアクセスするための OAuth の設定方法の詳細については、Box のマニュアルを参照してください。

次のビデオでは、Box 接続の設定時に OAuth アクセストークンを自動生成する方法について説明します。



接続の詳細

次の表に、基本接続プロパティを示します。

財産	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。
シークレットコンテナの使用	組織に対して設定されている Secrets Manager にこの接続の機密資格情報を保存します。 このプロパティは、組織に Secrets Manager が設定されている場合にのみ表示されます。 このプロパティは、データ取り込みおよびレプリケーションとデータアクセス管理サービスではサポートされていません。 接続でシークレットコンテナを有効にすると、Secure Agent が Secrets Manager からどの資格情報を取得するかを選択できます。このオプションを無効にした場合、資格情報は組織の設定方法に応じてリポジトリまたはローカル Secure Agent に保存されます。 注: この接続を使用してプッシュダウンまたはプロキシサービスを介してデータアクセスポリシーを適用する場合、シークレットコンテナ設定オプションを使用することはできません。 Secrets Manager を設定および使用する方法については、Administrator のヘルプにある「Secrets Manager の設定」を参照してください。
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。 Secure Agent、ホステッドエージェント、サーバーレスランタイム環境、またはエラスティックランタイム環境を選択します。 ホステッドエージェントは、詳細モードのマッピングには適用されません。 ランタイム環境の設定および使用方法の詳細については、Administrator のヘルプにある「ランタイム環境」を参照してください。
アクセストークンタイプ	エンドポイントサーバー内のリソースへのアクセスを認証および承認するためのアクセストークン。 次のオプションから選択できます。 <ul style="list-style-type: none">- 自動生成。【トークンの取得】をクリックすると、Box は接続でアクセストークンを自動生成します。- 手動。Box アカウントから OAuth の詳細を取得し、接続に詳細を手動で入力します。 デフォルトは【自動生成】です。

アクセストークンの自動生成

デフォルトでは、接続が自動生成されるように選択されています。

次の表に、Box からアクセストークンを自動生成するために必要なプロパティとアクション、およびその説明を示します。

プロパティ	説明
OAuth アクセストークン	Box によって生成されるアクセストークン。 【トークンの取得】をクリックすると、アクセストークンが Box によって生成され、このフィールドが自動的に入力されます。 詳細については、「 OAuth アクセストークンの生成 」(ページ 166)を参照してください。視覚的なプレゼンテーションについては、 Generating the access token video を確認してください。

手動でのアクセストークンの生成

OAuth プロパティを手動で入力するには、**【アクセストークンタイプ】** で**【手動】**を選択し、必要なプロパティを入力します。

次の表に、Box に手動で接続する必要がある OAuth プロパティとその説明を示します。

プロパティ	説明
アクセストークン	手動で生成した OAuth アクセストークンの値を Box に入力します。
クライアント ID	Box でアプリケーション登録プロセス中にクライアント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	Box でアプリケーション登録プロセス中にクライアントに発行されるクライアントシークレットキー。
認証タイプ	Box に接続する認証タイプ。 文字列 refresh_token を入力します。
更新トークン	リフレッシュトークンの値を入力します。 アクセストークンの有効期限が切れた場合は、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生成できます。 注: 手動アクセストークンタイプを使用しており、更新トークンの有効期限が切れた場合は、接続プロパティを再入力する必要があります。

詳細設定

次の表に、詳細接続のプロパティを示します。

プロパティ	説明
URI 要求パラメータ	Box 内のファイルまたはフォルダを検索するためのパラメータ。 検索文字列は以下の書式で指定します。 <code>query=search_string;content_types=<name description file_content comments tags;limit=<number>;offset=<number></code> 例えば、「generate」という語を含むオブジェクトを検索するには、 <code>query=generate;content_types=name;limit=0;offset=0</code> という文字列を入力します。 ワイルドカード文字を使用し、語句または複数のクエリ文字列を二重引用符で囲むことで、検索条件を絞り込むことができます。 詳細については、「 「URI 要求パラメータ」 (ページ 167) 」を参照してください。
ソースファイルのパス	このプロパティは、Box 接続には適用されません。
ターゲットファイルのパス	オプション。Box からオブジェクトをダウンロードできる Secure Agent マシン上のディレクトリ。 ファイルまたはフォルダを特定のディレクトリにダウンロードするためのパスを入力します。 デフォルトでは、Secure Agent マシンのルートディレクトリにすべての Box オブジェクトがダウンロードされます。
応答フォルダのパス	このプロパティは、Box 接続には適用されません。
[Box ファイル ID または Box フォルダ ID]	データの読み取りまたは書き込み先となる、Box 内のファイルまたはフォルダのファイル ID またはフォルダ ID。 ファイル ID またはフォルダ ID は、ファイルまたはフォルダの Box URL から取得することができます。 例えば、Box の [レポート] フォルダの URL は <code>https://app.box.com/folder/50016834230</code> です URL の 50016834230 は、レポートのフォルダ ID です。 注: この値は、Box で CSV ファイルの読み取りまたは書き込みを行うときに上書きすることができます。

OAuth アクセストークンの生成

Box 接続の作成時に、OAuth アクセストークンを生成する必要があります。Secure Agent は、このトークンを使用して、Box に安全に接続します。

1. **【接続】** ページの **【OAuth アクセストークン】** フィールドで、**【トークンの取得】** をクリックします。
Box の **【ログイン】** ページが表示されます。
2. ユーザー資格情報を入力します。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。

- Box ユーザーアカウントの資格情報を使用するには、そのユーザーに関連付けられている電子メールアドレスとパスワードを入力する。
 - シングルサインオンオプションを使用するには、**[シングルサインオン (SSO) を使用する]** をクリックし、ユーザーに関連付けられている電子メールアドレスを入力します。
3. **[承認]** をクリックします。
4. **[Box へのアクセスを許可]** をクリックします。
- [接続]** ページの **[OAuth アクセストークン]** フィールドが、生成されたトークンで更新されます。

URI 要求パラメータ

URI 要求パラメータを使用して、Box オブジェクトを検索します。

[URI 要求パラメータ] フィールドに検索文字列を指定するときは、次の構文を使用します。

`query=search_string;content_types=<name|description|file_content|comments|tags;limit=<number>;offset=<number>`

次の表に、**[URI 要求パラメータ]** フィールドのオプションを示します。

オプション	説明
Query	指定された単語またはフレーズに基づいて Box オブジェクトを検索します。フレーズを指定するときは、フレーズが単一引用符で囲まれていることを確認します。
content_types	検索の範囲を指定します。次のいずれかの値を使用できます。 <ul style="list-style-type: none"> - Name - Box オブジェクトの名前に基づいて検索を行います。 - Description - Box オブジェクトに関連付けられている説明に基づいて検索を行います。 - File_content - Box オブジェクトのコンテンツに基づいて検索を行います。 - Comments - Box オブジェクトに関連付けられているコメントに基づいて検索を行います。 - Tags - Box オブジェクトに関連付けられているタグに基づいて検索を行います。
limit	Secure Agent がターゲットに書き込む検索結果の数を制限します。
offset	指定されたオフセット値に基づいて検索結果をオフセットします。例えば、オフセット値として 12 が指定された場合、Secure Agent は、検索結果の先頭の 11 行を無視し、12 番目の行からの結果を書き込みます。

第 35 章

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 を選択します。 注: Business 360 接続を作成する場合は、ホステッドエージェントまたはサーバーレスランタイム環境を選択しないでください。
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。

第 36 章

Business 360 Events 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。
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。

第 37 章

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 を選択します。 注: Business 360 接続を作成する場合は、ホステッドエージェントまたはサーバーレスランタイム環境を選択しないでください。
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。

第 38 章

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
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。
シークレットコンテナの使用	組織に対して設定されている Secrets Manager にこの接続の機密資格情報を保存します。 このプロパティは、組織に Secrets Manager が設定されている場合にのみ表示されます。 このプロパティは、データ取り込みおよびレプリケーションとデータアクセス管理サービスではサポートされていません。 接続でシークレットコンテナを有効にすると、Secure Agent が Secrets Manager からどの資格情報を取得するかを選択できます。このオプションを無効にした場合、資格情報は組織の設定方法に応じてリポジトリまたはローカル Secure Agent に保存されます。 注: この接続を使用してプッシュダウンまたはプロキシサービスを介してデータアクセスポリシーを適用する場合、シークレットコンテナ設定オプションを使用することはできません。 Secrets Manager を設定および使用する方法については、Administrator のヘルプにある「Secrets Manager の設定」を参照してください。
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。
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。

プロパティ	説明
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。

Custom Configuration Details					
Service	Type	Sub-type	Name	Value	
Data Integration Server ▼	DTM ▼	▼	JVMOption6	-Dconnection.sessionTimeout=60	✚ ✖
Data Integration Server ▼	DTM ▼	▼	JVMOption7	-Dconnection.attempts=4	✚ ✖
Data Integration Server ▼	DTM ▼	▼	JVMOption8	-Dconnection.waitTimeToReattempt=5	✚ ✖

5. **保存** をクリックします。

第 39 章

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
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。
シークレットコンテナの使用	組織に対して設定されている Secrets Manager にこの接続の機密資格情報を保存します。 このプロパティは、組織に Secrets Manager が設定されている場合にのみ表示されます。 このプロパティは、データ取り込みおよびレプリケーションとデータアクセス管理サービスではサポートされていません。 接続でシークレットコンテナを有効にすると、Secure Agent が Secrets Manager からどの資格情報を取得するかを選択できます。このオプションを無効にした場合、資格情報は組織の設定方法に応じてリポジトリまたはローカル Secure Agent に保存されます。 注: この接続を使用してプッシュダウンまたはプロキシサービスを介してデータアクセスポリシーを適用する場合、シークレットコンテナ設定オプションを使用することはできません。 Secrets Manager を設定および使用する方法については、Administrator のヘルプにある「Secrets Manager の設定」を参照してください。
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。
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。

プロパティ	説明
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。 <ul style="list-style-type: none"> - 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。
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。 <ul style="list-style-type: none"> - 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。 <ul style="list-style-type: none"> - 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。

第 40 章

Cassandra V2 接続のプロパティ

Cassandra 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、Cassandra 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。
シークレット コンテナの使用	組織に対して設定されている Secrets Manager にこの接続の機密資格情報を保存します。 このプロパティは、組織に Secrets Manager が設定されている場合にのみ表示されます。 このプロパティは、データ取り込みおよびレプリケーションとデータアクセス管理サービスではサポートされていません。 接続でシークレットコンテナを有効にすると、Secure Agent が Secrets Manager からどの資格情報を取得するかを選択できます。このオプションを無効にした場合、資格情報は組織の設定方法に応じてリポジトリまたはローカル Secure Agent に保存されます。 注: この接続を使用してプッシュダウンまたはプロキシサービスを介してデータアクセスポリシーを適用する場合、シークレットコンテナ設定オプションを使用することはできません。 Secrets Manager を設定および使用する方法については、Administrator のヘルプにある「Secrets Manager の設定」を参照してください。
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。 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。 ランタイム環境の設定および使用方法の詳細については、Administrator のヘルプにある「ランタイム環境」を参照してください。
ホスト	Cassandra サーバーのホスト名または IP アドレス。
ポート	Cassandra サーバーのポート番号です。 デフォルトは 9042 です。
データセンター	接続先の Cassandra データセンターの名前。 デフォルトは datacenter1。
キースペース	接続先の Cassandra データセンター内の Cassandra キースペースの名前。
ユーザー名	Cassandra サーバーにアクセスするためのユーザー名です。

プロパティ	説明
パスワード	Cassandra サーバーにアクセスするためのパスワードです。
SSL 有効	次のオプションから選択します。 - はい。SSL 暗号化を有効にします。 - いいえ SSL 暗号化を無効にします。 デフォルトは【いいえ】です。
SSL キーストアファイルパス	SSL を有効にする場合に適用されます。 SSL サーバーのプライベートキーと証明書を格納する、Secure Agent マシンにある SSL キーストアファイルの絶対パス。
SSL キーストアパスワード	SSL を有効にする場合に適用されます。 SSL キーストアのパスワード。
SSL TrustStore ファイルパス	SSL を有効にする場合に適用されます。 SSL サーバーのプライベートキーと証明書を格納する、Secure Agent マシンにある SSL TrustStore ファイルの絶対パス。
SSL TrustStore パスワード	SSL を有効にする場合に適用されます。 SSL TrustStore のパスワード。

第 41 章

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。

重要: Chatter コネクタは非推奨となり、メンテナンスモードに移行されました。Informatica は将来のリリースでサポートを廃止する予定です。

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。

第 42 章

Cloud 統合ハブ接続プロパティ

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

次の表に、Cloud 統合ハブ接続の接続プロパティを示します。

接続プロパティ	説明	編集可能
接続名	接続の名前。大文字と小文字は区別されず、ドメイン内で一意である必要があります。 名前は 128 文字以内で指定し、空白および以下の特殊文字は使用できません。 ~ ` ! \$ % ^ & * () - + = { [] } \ : ; " ' < , > . ? /	編集しないでください。
説明	オプション。接続の説明。説明は、4,000 文字を超えることはできません。	○
シークレット Vault を有効にする	接続用のパブリケーションリポジトリパスワードを、組織に設定されたランタイム環境のシークレットマネージャに保存します。 このプロパティは、組織にシークレットマネージャが設定されている場合にのみ表示されます。 シークレットマネージャの資格情報を使用するには、このオプションを選択します。このオプションを有効にしない場合、資格情報は組織の設定に応じてリポジトリまたはローカル Secure Agent に保存されます。 シークレットマネージャの設定および使用方法については、Administrator ヘルプの「シークレットマネージャの設定」を参照してください。	編集しないでください。
ランタイム環境	タスクを実行するランタイム環境の名前。	編集しないでください。

接続プロパティ	説明	編集可能
サブスクリプションフローに中間ステージングを使用しない	中間ステージングへの書き込みを無効にします。中間ステージングに書き込みたくない場合は、このプロパティを有効にします。データ統合タスクは Cloud 統合ハブからデータを読み取り、ターゲットの場所にデータを直接書き込みます。中間ステージングへの書き込みを無効にすると、システムパフォーマンスに影響を与える可能性があります。	<input type="radio"/>
プライベートパブリケーションリポジトリに JDBC を使用する	<p>プライベートパブリケーションリポジトリのゼロダウンタイムを設定する場合。このプロパティを有効にすると、プライベートパブリケーションリポジトリ上のデータに中断なくアクセスできるようになります。データ統合タスクをトリガするパブリケーションおよびサブスクリプションのゼロダウンタイムを有効にできます。</p> <p>ホストされたパブリケーションリポジトリでは、Cloud 統合ハブはすべてのパブリケーションおよびサブスクリプションタイプに対してデフォルトでゼロダウンタイムを適用します。</p>	<input type="radio"/>

第 43 章

Concur 接続のプロパティ

Concur 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する必要があります。

重要: Concur コネクタは非推奨となり、メンテナンスモードに移行されました。Informatica は将来のリリースでサポートを廃止する予定です。

データ統合で Concur 接続を作成するには、次の手順を実行します。

1. **【管理者】** > **【接続】** をクリックし、**【新しい接続】** をクリックして接続を作成します。

【新しい接続】 ページが表示されます。

OKCancelTest

Connection Details

Connection Name:*Concur

Description:

Type:*concur (ICL)

concur (ICL) Connection Properties

Secure Agent:* ?s158519-vm

Username*Cloud123@informatica.com

Password*.....

Key*.....

Company Domaind0049258g

Service URL*https://www.concursolutions.com

Enable Logging☒

Paging Size100

2. 以下の詳細を指定します。

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	リストから [Concur] を選択します。
Secure Agent	リストから該当する Secure Agent を選択します。
ユーザー名	関連するユーザー名を入力します。
パスワード	関連するパスワードを入力します。
キー	Concur OAUTH 2.0 キーを入力します。詳細については、「キー」を参照してください。
会社のドメイン	OAUTH 2.0 を使用した Concur 認証の一部である Concur の会社のドメインアドレスを入力します。
サービス URL	サービス URL を入力して Concur アカウントに接続します。
ロギングの有効化	ロギングを有効にする場合に選択します。
ページングサイズ	Concur にプッシュするレコードの数を入力します。デフォルト値は 100 です。

3. **【テスト接続】** をクリックして、接続をテストします。
4. **【保存】** をクリックして接続を保存します。

第 44 章

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 OAuth 2 認証またはコンシューマキー認証を指定できます。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、基本接続プロパティを示します

プロパティ	説明
接続名	接続の名前。 各接続名は組織内で一意である必要があります。接続名には、英数字、スペース、および次の特殊文字を含めることができます。_ . + , 最大長は 255 文字です。
説明	接続の説明。最大長は 4000 文字です。
シークレット コンテナの使用	組織に対して設定されている Secrets Manager にこの接続の機密資格情報を保存します。 このプロパティは、組織に Secrets Manager が設定されている場合にのみ表示されます。 このプロパティは、データ取り込みおよびレプリケーションとデータアクセス管理サービスではサポートされていません。 接続でシークレットコンテナを有効にすると、Secure Agent が Secrets Manager からどの資格情報を取得するかを選択できます。このオプションを無効にした場合、資格情報は組織の設定方法に応じてリポジトリまたはローカル Secure Agent に保存されます。 注: この接続を使用してプッシュダウンまたはプロキシサービスを介してデータアクセスポリシーを適用する場合、シークレットコンテナ設定オプションを使用することはできません。 Secrets Manager を設定および使用する方法については、Administrator のヘルプにある「Secrets Manager の設定」を参照してください。
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。 Secure Agent、ホステッドエージェント、サーバーレスランタイム環境、またはエラスティックランタイム環境を選択します。 ランタイム環境の設定および使用方法の詳細については、Administrator のヘルプにある「ランタイム環境」を参照してください。
認証	接続の認証方法。 接続には必ず【Concur V2】を選択してください。
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。

プロパティ	説明
OAuth2 を使用	<p>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 OAuth 2 を使用します。</p> <p>[OAuth 2] を選択します。[OAuth 2] を選択しない場合、接続はコンシューマキー認証を使用します。</p> <p>SAP Concur から OAuth 2 資格情報を取得します。</p>
認証用ベース URL	<p>アカウント作成時に Concur から受け取った認証用 URL。</p> <p>[認証用ベース URL] は、承認 URL から派生したものです。</p> <p>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。</p>
API 呼び出し用ベース URL	<p>アカウント作成時に Concur から受け取った API 呼び出し用 URL。</p>
クライアント ID	<p>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。</p>
シークレット ID	<p>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。</p>
フォルダ	<p>Concur からアクセスするオブジェクトへの相対パス。</p> <p>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、<code>expense/report</code> という相対パスを入力します。</p>

次の表に、詳細接続のプロパティを示します。

プロパティ	説明
コンシューマキー	<p>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。</p> <p>コンシューマキー認証を使用するには、接続プロパティで Concur アカウントのユーザー名とパスワードを指定してください。</p> <p>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。</p>

第 45 章

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。 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。
シークレットコンテナの使用	組織に対して設定されている Secrets Manager にこの接続の機密資格情報を保存します。 このプロパティは、組織に Secrets Manager が設定されている場合にのみ表示されます。 このプロパティは、データ取り込みおよびレプリケーションとデータアクセス管理サービスではサポートされていません。 接続でシークレットコンテナを有効にすると、Secure Agent が Secrets Manager からどの資格情報を取得するかを選択できます。このオプションを無効にした場合、資格情報は組織の設定方法に応じてリポジトリまたはローカル Secure Agent に保存されます。 注: この接続を使用してプッシュダウンまたはプロキシサービスを介してデータアクセスポリシーを適用する場合、シークレットコンテナ設定オプションを使用することはできません。 Secrets Manager を設定および使用方法については、Administrator のヘルプにある「Secrets Manager の設定」を参照してください。
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	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。
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。

プロパティ	説明
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	<p>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></p> <p>Couchbase コネクタは、次の接続パラメータをサポートします。</p> <p>QueryMode Couchbase サーバーへのクエリの送信に使用します。</p> <p>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。</p> <p>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。</p> <p>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。</p>

第 46 章

Coupa 接続のプロパティ

Coupa 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。

重要: Coupa コネクタは非推奨となり、メンテナンスモードに移行されました。Informatica は将来のリリースでサポートを廃止する予定です。Coupa V2 コネクタを使用して Coupa にアクセスすることをお勧めします。

次の表に、Coupa 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	Coupa 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。
ドメイン名	Coupa ドメイン名。
Coupa API キー	Coupa の固有の API キー。
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。

第 47 章

Coupa V2 接続のプロパティ

Coupa に対してデータの安全な読み取りまたは書き込みを行うための Coupa V2 接続を作成します。

Coupa V2 への接続

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

始める前に

開始する前に、Coupa アカウントの OAuth 認証を設定してください。クライアントシークレット認証を使用して Coupa Success Portal に登録し、クライアントの詳細を取得します。

Coupa Cloud にログインし、次の詳細を取得します。

- 識別子
- シークレット
- スcope

接続の作成時に、識別子をクライアント ID に、シークレットをクライアントシークレットに、スコープを接続プロパティにそれぞれ指定します。

接続の詳細

次の表に、基本接続プロパティを示します。

財産	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。

財産	説明
シークレットコンテナの使用	<p>組織に対して設定されている Secrets Manager にこの接続の機密資格情報を保存します。このプロパティは、組織に Secrets Manager が設定されている場合にのみ表示されます。このプロパティは、データ取り込みおよびレプリケーションとデータアクセス管理サービスではサポートされていません。</p> <p>接続でシークレットコンテナを有効にすると、Secure Agent が Secrets Manager からどの資格情報を取得するかを選択できます。このオプションを無効にした場合、資格情報は組織の設定方法に応じてリポジトリまたはローカル Secure Agent に保存されます。</p> <p>注: この接続を使用してプッシュダウンまたはプロキシサービスを介してデータアクセスポリシーを適用する場合、シークレットコンテナ設定オプションを使用することはできません。</p> <p>Secrets Manager を設定および使用する方法については、Administrator のヘルプにある「Secrets Manager の設定」を参照してください。</p>
ランタイム環境	<p>タスクを実行するランタイム環境の名前。</p> <p>Secure Agent、ホステッドエージェント、サーバーレスランタイム環境、またはエラスティックランタイム環境を選択します。</p> <p>ホステッドエージェントは、詳細モードのマッピングには適用されません。</p> <p>ランタイム環境の設定および使用方法の詳細については、Administrator のヘルプにある「ランタイム環境」を参照してください。</p>
認証	[Coupa V2] を選択します。
ベース URL	<p>Coupa API に接続するためのベース URL。</p> <p>ベース URL を次の形式で指定します。</p> <p><code>https://{instance_name}.coupahost.com/</code></p> <p>例: <code>https://companyname.coupahost.com/</code></p>
クライアント ID	<p>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。</p> <p>クライアント ID として Coupa ID を指定します。</p>
クライアントシークレット	<p>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。</p> <p>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。</p>
スコープ	<p>Coupa へのアクセスを承認するために使用されるスコープ。</p> <p>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。</p>

詳細設定

次の表に、詳細接続のプロパティを示します。

プロパティ	説明
カスタムフィールド設定	<p>Coupa オブジェクトのカスタムフィールドを指定します。</p> <p>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。</p> <p>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。</p> <pre>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</pre> <p>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。</p> <p>例:</p> <pre>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</pre> <p>Coupa V2 のカスタムフィールドのオブジェクト、およびルールとガイドラインの詳細については、「Coupa V2 カスタムフィールド」 (ページ 189)を参照してください。</p>

Coupa V2 カスタムフィールド

Coupa のカスタムフィールドからデータの読み取りを行ったり、カスタムフィールドにデータを挿入したりするには、Coupa V2 接続を作成するときに **【カスタムフィールド設定】** プロパティを設定する必要があります。

カスタムオブジェクトのフィールド名、フィールドタイプ、および IsAPIGlobalNamespace を指定する必要があります。

カスタムフィールドは、異なるオブジェクトに対して改行で区切って指定することができます。特定の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空の新しい行に分けて区切ります。最後のエントリ以外の行の末尾に;\を入力します。

注: フィールド名にアンダースコアが含まれている場合、Secure Agent ではアンダースコアがハイフンに置き換えられます。

プロキシサーバーの設定

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

Windows および Linux で、プロキシサーバーを使用するように Secure Agent を設定できます。

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

手順については、データ統合のヘルプの『または「Windows でのプロキシ設定」または「Linux でのプロキシ設定」を参照してください。

Secure Agent のプロパティで、DTM の JVM オプションを設定します。手順については、ナレッジベースの記事「[Proxy server settings](#)」を参照してください。

サーバーレスランタイム環境のプロキシの設定を行う方法については、Administrator ヘルプの「「プロキシサーバーの使用」を参照してください。

第 48 章

Cvent 接続のプロパティ

Cvent 接続を作成して、Cvent から安全にデータの読み取りを行うことができます。

Cvent 接続を使用して、マッピングタスクと同期タスクのソースを指定します。接続を作成して、同期タスク、マッピング、またはマッピングタスクに関連付けます。

Cvent への接続

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

重要: Cvent コネクタは廃止され、メンテナンスモードに移行されました。Informatica は将来のリリースでサポートを廃止する予定です。Cvent にアクセスするには、Cvent V2 コネクタを使用することをお勧めします。

始める前に

接続プロパティを設定する前に、Cvent アカウントから API ユーザー名とエンドポイント URL を取得する必要があります。

次のビデオには、必要な情報を取得するための説明が含まれています。



接続の詳細

次の表に、基本接続プロパティを示します。

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

プロパティ	説明
シークレットコンテナの使用	<p>組織に対して設定されている Secrets Manager にこの接続の機密資格情報を保存します。</p> <p>このプロパティは、組織に Secrets Manager が設定されている場合にのみ表示されます。</p> <p>このプロパティは、データ取り込みおよびレプリケーションとデータアクセス管理サービスではサポートされていません。</p> <p>接続でシークレットコンテナを有効にすると、Secure Agent が Secrets Manager からどの資格情報を取得するかを選択できます。このオプションを無効にした場合、資格情報は組織の設定方法に応じてリポジトリまたはローカル Secure Agent に保存されます。</p> <p>注: この接続を使用してプッシュダウンまたはプロキシサービスを介してデータアクセスポリシーを適用する場合、シークレットコンテナ設定オプションを使用することはできません。</p> <p>Secrets Manager を設定および使用する方法については、Administrator のヘルプにある「Secrets Manager の設定」を参照してください。</p>
ランタイム環境	<p>タスクを実行するランタイム環境の名前。</p> <p>Secure Agent、ホステッドエージェント、またはサーバーレスランタイム環境を選択します。</p>
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。

詳細設定

次の表に、詳細接続のプロパティを示します。

プロパティ	説明
バッチサイズ	<p>一度に取得するレコード数。</p> <p>最大値は 200 です。</p>
UTC タイムゾーン	<p>Cvent UTC タイムゾーン。</p> <p>日付と時刻のフィールドにタイムゾーンを入力します。</p> <p>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。</p>
ログgingsの有効化	<p>タスクのログgingsを有効にします。</p> <p>ログgings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。</p>

プロキシサーバーの設定

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

Windows および Linux でプロキシサーバーを使用するように Secure Agent を設定できます。認証されていないプロキシサーバーのみを使用できます。プロキシ設定は、マッピングおよび詳細モードのマッピングで使用する接続に適用されます。

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

- Windows の場合は Secure Agent Manager を使用し、Linux の場合はシェルコマンドを使用して Secure Agent を設定します。
手順については、データ統合のヘルプの『または「Windows でのプロキシ設定」または「Linux でのプロキシ設定」を参照してください。
- Secure Agent のプロパティで、DTM の JVM オプションを設定します。手順については、ナレッジベースの記事「[Proxy server settings](#)」を参照してください。

サーバーレスランタイム環境のプロキシの設定を行う方法については、Administrator ヘルプの「「プロキシサーバーの使用」を参照してください。

第 49 章

Cvent V2 接続のプロパティ

Cvent V2 接続を作成することで、Cvent からデータを安全に読み取ることができます。

前提条件

Cvent アカウントのユーザーは、ワークスペースを作成し、読み取りスコープを定義して、開発者を Cvent REST API にアクセスするように招待する必要があります。開発者のユーザーは、アプリケーションを作成し、定義されたスコープを選択する必要があります。
接続プロパティを設定する前に、次の前提条件を完了してください。

Cvent への接続

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

始める前に

接続プロパティを設定する前に、アカウントを作成し、Cvent ポータルでアプリケーションを作成する必要があります。

接続を設定する前に、[「前提条件」 \(ページ 194\)](#)を参照して要件を確認してください。

接続の詳細

次の表に、基本接続プロパティを示します。

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

プロパティ	説明
シークレットコンテナの使用	<p>組織に対して設定されている Secrets Manager にこの接続の機密資格情報を保存します。このプロパティは、組織に Secrets Manager が設定されている場合にのみ表示されます。このプロパティは、データ取り込みおよびレプリケーションとデータアクセス管理サービスではサポートされていません。</p> <p>接続でシークレットコンテナを有効にすると、Secure Agent が Secrets Manager からどの資格情報を取得するかを選択できます。このオプションを無効にした場合、資格情報は組織の設定方法に応じてリポジトリまたはローカル Secure Agent に保存されます。</p> <p>注: この接続を使用してプッシュダウンまたはプロキシサービスを介してデータアクセスポリシーを適用する場合、シークレットコンテナ設定オプションを使用することはできません。</p> <p>Secrets Manager を設定および使用方法については、Administrator のヘルプにある「Secrets Manager の設定」を参照してください。</p>
ランタイム環境	<p>タスクを実行するランタイム環境の名前。</p> <p>Secure Agent または Hosted Agent を選択します。</p> <p>ランタイム環境の設定および使用方法の詳細については、Administrator のヘルプにある「ランタイム環境」を参照してください。</p>

認証タイプ

OAuth 2.0 クライアント資格情報認証を設定することで、Cvent アカウントにアクセスできます。

この認証タイプを選択し、その認証に固有のパラメータを設定します。

OAuth 2.0 クライアント資格情報認証

OAuth 2.0 クライアント資格情報認証では、クライアント ID、クライアントシークレット、およびアクセストークン URL を使用して Cvent に接続します。

次の表に、OAuth 2.0 クライアント資格情報認証の基本的な接続プロパティに関する説明を示します。

プロパティ	説明
アクセストークン URL	Cvent アクセストークンを取得するために OAuth 2.0 要求を送信する URL。
クライアント ID	Cvent に接続するための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	クライアント ID に関連付けら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。
アクセストークン	<p>アクセストークンの値。</p> <p>[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入力します。</p>

詳細設定

次の表に、詳細接続のプロパティを示します。

プロパティ	説明
スコープ	アクセストークンが Cvent REST エンドポイントに付与する権限を定義するスコープパラメータ。 例: event/admission-items:read、event/contacts:read、budget/payments:read。 複数のスコープをスペースで区切って指定します。 このプロパティに値を指定しない場合、アクセストークンは、アプリケーションレベルで設定されたスコープに基づいて生成されます。
再試行回数	エラー発生後に Cvent REST エンドポイントからの応答の受信を再試行する際の最大試行回数。 デフォルトは 3 です。
再試行間隔	各再試行間の待機時間(ミリ秒)。 デフォルトは 5000 ミリ秒です。

プロキシサーバーの設定

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

Windows および Linux でプロキシサーバーを使用するように Secure Agent を設定できます。Cvent に接続するためには、認証なしのプロキシサーバーのみを使用できます。

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

手順については、データ統合のヘルプの『または「Windows でのプロキシ設定」または「Linux でのプロキシ設定」を参照してください。

第 50 章

Databricks 接続プロパティ

Databricks に対してデータの安全な読み取りまたは書き込みを行うための ServiceNow 接続を作成します。

ステージングの前提条件

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

SQL ウェアハウス

デプロイメント環境に応じて、SQL ウェアハウスのステージング環境として AWS、Azure、または Databricks ボリュームを設定します。さらに、Azure または AWS のステージング環境を使用するように SQL ウェアハウスの Spark パラメータを設定します。

SQL ウェアハウスは、Windows および Linux オペレーティングシステムで 사용할 수 있습니다。

接続できる SQL ウェアハウスのタイプの詳細については、ナレッジベースの記事「[Databricks SQL warehouses](#)」を参照してください。

AWS ステージングの設定

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

IAM AssumeRole 認証

Databricks で IAM AssumeRole 認証を有効にすると、マッピングおよびマッピングタスクの実行時に、Amazon S3 ステージングバケットへの安全かつ制御されたアクセスができるようになります。Secure Agent が Amazon Elastic Compute Cloud (EC2) システムで実行されている場合は、IAM 認証を設定できます。サーバーレスランタイム環境を使用している場合、IAM 認証を設定することはできません。

注: データ取り込みおよびレプリケーションでは、Amazon S3 ステージングにアクセスするための IAM 認証はサポートされていません。

EC2 で IAM 認証を設定するには、次の手順を実行します。

1. 最小限の Amazon IAM ポリシーを作成します。

2. Amazon EC2 ロールを作成します。Amazon EC2 ロールは、EC2 システムを作成する場合に使用されます。
Amazon EC2 ロールの作成の詳細については、*AWS のマニュアル*を参照してください。
3. 最小限の Amazon IAM ポリシーを Amazon EC2 ロールにリンクします。
4. EC2 インスタンスを作成します。作成した Amazon EC2 ロールを EC2 インスタンスに割り当てます。
5. EC2 システムにセキュアエージェントをインストールします。

AssumeRole を使用した一時的なセキュリティ資格情報

AssumeRole を使用した一時的なセキュリティ資格情報を使用すると、同じ AWS アカウントまたは異なる AWS アカウントから AWS リソースにアクセスできます。

注: データ取り込みおよびレプリケーションでは、IAM ユーザーに対する一時的なセキュリティ資格情報の使用はサポートされていません。

sts:AssumeRole 権限が割り当てられており、AWS アカウント内に一時的なセキュリティ資格情報を使用するための信頼関係が構築されていることを確認します。信頼関係は、ロールを作成するときに、IAM ロールの信頼ポリシーで定義されます。IAM ロールにより、IAM ユーザーを信頼されたエンティティとして追加し、IAM ユーザーによる一時的なセキュリティ資格情報の使用と AWS アカウントへのアクセスを許可します。

信頼関係を構築する方法の詳細については、*AWS のマニュアル*を参照してください。

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

動的に生成された一時的なセキュリティ資格情報を使用するには、Databricks 接続を作成するときに **[IAM ロール ARN]** 接続プロパティの値を入力します。IAM ロール ARN は、AWS リソースを一意に識別します。次に、**[一時的な資格情報の期間]** 詳細ソースプロパティおよびターゲットプロパティで、一時的なセキュリティ資格情報を使用できる期間を秒単位で指定します。

外部 ID

Amazon S3 バケットが別の 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クロスアカウントアクセスを確立するための外部 ID を指定できます。

必要に応じて、AWS セキュリティトークンサービス (STS) への AssumeRole 要求で外部 ID を指定できます。

外部 ID は文字列である必要があります。

次のサンプルは、引き継がれた IAM ロールの信頼ポリシー内の外部 ID 条件を示しています。

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

注: データ取り込みおよびレプリケーションでは、外部 ID はサポートされていません。

一時的なセキュリティ資格情報のポリシー

一時的なセキュリティ資格情報を使用して AWS リソースにアクセスするには、IAM ユーザーと IAM ロールの両方にポリシーが必要です。

Amazon S3 権限ポリシー

次の S3 権限ポリシーをアタッチして、Amazon S3 パケットへのアクセスを許可します。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "s3:DeleteObject",
        "s3:GetObject",
        "s3:ListBucket",
        "s3:PutObject",
        "s3:PutObjectTagging",
        "s3:GetBucketAcl"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::com.amk"
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:DeleteObject",
        "s3:GetObject",
        "s3:ListBucket",
        "s3:PutObject",
        "s3:PutObjectTagging",
        "s3:GetBucketAcl"
      ],
      "Resource": "arn:aws:s3:::com.amk/*"
    }
  ]
}
```

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

IAM ユーザー

同じ AWS アカウントまたは異なる AWS アカウントで一時的なセキュリティ資格情報を使用するためには、IAM ユーザーに sts:AssumeRole ポリシーが割り当てられている必要があります。

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

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

IAM ロール

IAM ユーザーに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ことを許可するためには、IAM ロールに sts:AssumeRole ポリシーおよび IAM ロールにアタッチされた信頼ポリシーが割り当てられている必要があります。ポリシーは、IAM ユーザーがアクセスできる AWS リソースと、IAM ユーザーが実行できるアクションを指定します。信頼ポリシーは、AWS リソースにアクセスできる AWS アカウントの IAM ユーザーを指定します。

次のポリシーは、サンプルの信頼ポリシーです。

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

```
}
}
}
```

このポリシーでは、Principal 属性で、動的に生成された一時的なセキュリティ資格情報を使用できる IAM ユーザーの ARN も入力することができ、それ以上のアクセスを制限できます。以下に例を示します。

```
"Principal" : { "AWS" : "arn:aws:iam:: AWS-account-ID :user/ user-name " }
```

AssumeRole for EC2 を使用した一時的なセキュリティ 認証情報

Amazon EC2 ロールに AssumeRole を使用した一時的なセキュリティ資格情報を使用すると、同じ AWS アカウントまたは異なる AWS アカウントから AWS リソースにアクセスできます。

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

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

- Secure Agent を Amazon EC2 などの AWS サービスにインストールします。
- AWS EC2 サービスにアタッチされた EC2 ロールには Amazon S3 へのアクセス権は必要ありませんが、別の IAM ロールを引き受けるための権限が必要です。
- EC2 ロールが引き受ける必要のある IAM ロールには、アクセス許可ポリシーと信頼ポリシーがアタッチされている必要があります。

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

最小限の Amazon IAM ポリシーの作成

Amazon S3 でデータをステージングするには、次の最小限必要な権限を使用します。

- PutObject
- GetObject
- DeleteObject
- ListBucket
- ListBucketMultipartUploads. 詳細モードのマッピングにのみ適用されます。

次のサンプル Amazon IAM ポリシーを使用できます。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:PutObject",
        "s3:GetObject",
        "s3:DeleteObject",
        "s3:ListBucket",
        "s3:ListBucketMultipartUploads"
      ],
      "Resource": [
        "arn:aws:s3:::<bucket_name>/*",
        "arn:aws:s3:::<bucket_name>"
      ]
    }
  ]
}
```

詳細モードのマッピングの場合、同じ AWS リージョン内で異なる AWS アカウントを使用できます。これらのマッピングで使用する AWS アカウントへのアクセスが Amazon IAM ポリシーで承認されていることを確認します。

注: **【テスト接続】** はユーザーに割り当てられた IAM ポリシーを検証しません。ソースおよびターゲットの詳細プロパティで Amazon S3 バケット名を指定できます。

AWS ステージング用の Spark パラメータの設定

Databricks SQL ウェアハウスを使用してマッピングを実行する前に、Databricks SQL 管理コンソールで SQL ウェアハウスの Spark パラメータを設定します。

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

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

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

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

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

Azure ステージングの設定

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

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

注: ロールの割り当てを追加または削除するには、[Owner] ロールなどの書き込みおよび削除権限が必要です。

- Azure Active Directory にアプリケーションを登録して、Microsoft Azure Data LakeStorage Gen2 アカウントにアクセスするユーザーを認証します。
ロールベースのアクセス制御を使用してアプリケーションを許可できます。アプリケーションに Storage Blob Data Contributor ロールまたは Storage Blob Data Reader ロールを割り当てます。Storage Blob Data Contributor ロールを割り当てた場合は、ストレージアカウント内の Azure Storage コンテナと Blob の読み取り、書き込み、および削除を行うことができます。Storage Blob Data Reader ロールを割り当てた場合は、ストレージアカウント内の Azure Storage コンテナと Blob の読み取りおよび一覧表示のみを行うことができます。

- Microsoft Azure Data Lake Storage Gen2 でのサービス間認証用に Azure Active Directory Web アプリケーションを作成します。

注: コネクタを使用してアプリケーションで作成されたフォルダまたはファイルにアクセスするためのスーパーユーザー特権があることを確認します。

- 複合ファイルの読み取りおよび書き込みを行うには、タイプ DTM の JVM オプションを設定して、Secure Agent のシステム構成の詳細で-Xms および-Xmx 値を増やし、Java ヒープ領域不足のエラーを回避します。推奨される-Xms 値は 512MB、-Xmx 値は 1024MB です。

Azure ステージング用の Spark パラメータの設定

Databricks SQL ウェアハウスを使用してマッピングを実行する前に、Databricks SQL 管理コンソールで SQL ウェアハウスの Spark パラメータを設定します。

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

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

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

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

Databricks ボリュームでのデータのステージング

Databricks のボリュームにデータをステージングできます。ボリュームは、ファイルやディレクトリなどの表形式以外のデータセットを管理および保護するために使用される Unity Catalog オブジェクトです。

ボリュームは、Linux または Windows マシン上で、Databricks JDBC ドライバと組み合わせて使用できます。

ボリュームを使用するには、以下の前提条件を完了する必要があります。

- Unity Catalog に対して Databricks ワークスペースが有効になっていることを確認します。
- データをステージングするボリューム内のパスを取得します。Databricks 接続プロパティでボリュームパスを指定しない場合、セキュアエージェントは Databricks にマネージドボリュームを作成します。そのボリュームは、ジョブが完了すると自動的に削除されます。パスを指定しない場合は、マネージドボリュームの作成権限と削除権限があることを確認してください。

汎用クラスタ

汎用クラスタでの設計時処理用の Secure Agent プロパティを有効にします。

汎用クラスタは、Linux オペレーティングシステムでのみ使用できます。

Secure Agent のプロパティの設定

汎用クラスタに接続するには、設計時に Secure Agent のプロパティを有効にします。

1. **Administrator** で、**[ランタイム環境]** タブに一覧表示されている 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 **【Tomcat JRE】** を選択します。
4. **【JRE_OPTS】** フィールドを編集して、値を `-DUseDatabricksSql=false` に設定します。

Tomcat JRE	JRE_OPTS	'-Xrs -DUseDatabricksSql=false'
------------	----------	---------------------------------

ジョブクラスタ

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

また、ジョブクラスタでの実行時の処理に対して Secure Agent プロパティを有効にする必要があります。

ジョブクラスタは、Linux オペレーティングシステムでのみ使用できます。

Spark 設定

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

AWS での設定

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

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

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

Azure での設定

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

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

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

Secure Agent のプロパティの設定

ジョブクラスタに接続するには、実行時に Secure Agent プロパティを有効にします。

注: このトピックは、データ取り込みおよびレプリケーションに関連するものではありません。

1. **Administrator** で、**【ランタイム環境】** タブに一覧表示されている 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】** に **【データ統合サーバー】** を選択し、**【タイプ】** に **【DTM】** を選択します。
4. **【JVMOption】** フィールドを編集して、値を `-DUseDatabricksSql=false` に設定します。

DTM

JVMOption2

'-DUseDatabricksSql=false'

Databricks への接続

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

始める前に

Databricks 接続を使用して、Databricks テーブルの読み取りと書き込みを行うことができます。

次のコンピューティングリソースを設定して、Databricks に接続できます。

- **SQL ウェアハウス（推奨）**
Secure Agent は、設計時と実行時に SQL ウェアハウスに接続します。
- **汎用クラスタとジョブクラスタ**
Secure Agent は、汎用クラスタに接続して設計時にメタデータをインポートし、ジョブクラスタに接続してマッピングを実行します。

注: 汎用クラスタまたはジョブクラスタを使用している場合は SQL ウェアハウスに移行することをお勧めします。汎用クラスタとジョブクラスタが新しい機能の更新プログラムや拡張機能を受け取ることはありません。しかし、安定性と安全性を維持するために重要なセキュリティ更新プログラムは引き続き受け取ります。SQL ウェアハウスに切り替えると、最新の機能と拡張機能を利用することができます。

開始する前に、Databricks 接続を使用するように AWS または Azure ステージング環境を設定する必要があります。

Azure または AWS 環境の前提条件については、「[「ステージングの前提条件」（ページ 197）」](#)を確認してください。

接続の詳細

次の表に、基本接続プロパティを示します。

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

プロパティ	説明
シークレットコンテナの使用	<p>組織に対して設定されている Secrets Manager にこの接続の機密資格情報を保存します。このプロパティは、組織に Secrets Manager が設定されている場合にのみ表示されます。このプロパティは、データ取り込みおよびレプリケーションとデータアクセス管理サービスではサポートされていません。</p> <p>接続でシークレットコンテナを有効にすると、Secure Agent が Secrets Manager からどの資格情報を取得するかを選択できます。このオプションを無効にした場合、資格情報は組織の設定方法に応じてリポジトリまたはローカル Secure Agent に保存されます。</p> <p>注: この接続を使用してプッシュダウンまたはプロキシサービスを介してデータアクセスポリシーを適用する場合、シークレットコンテナ設定オプションを使用することはできません。</p> <p>Secrets Manager を設定および使用方法については、Administrator のヘルプにある「Secrets Manager の設定」を参照してください。</p>
ランタイム環境	<p>タスクを実行するランタイム環境の名前。</p> <p>セキュアエージェント、ホステッドエージェント、サーバーレスランタイム環境、またはエラスティックランタイム環境を選択します。</p> <p>Hosted Agent は、詳細モードのマッピングには適用されません。</p> <p>アプリケーション取り込みとレプリケーションタスクとデータベース取り込みとレプリケーションタスクでは、Secure Agent またはサーバーレスランタイム環境を使用できます。タスクには、サーバーレス使用がサポートされているソースタイプが必要です。ファイル取り込みおよびレプリケーションタスクまたはストリーミング取り込みおよびレプリケーションタスクには、Secure Agent を使用します。ホステッドエージェントまたはエラスティックランタイム環境で、アプリケーション取り込みとレプリケーションタスク、データベース取り込みとレプリケーションタスク、ファイル取り込みおよびレプリケーションタスク、またはストリーミング取り込みとレプリケーションタスクを実行することはできません。</p> <p>ランタイム環境の設定および使用方法の詳細については、Administrator のヘルプにある「ランタイム環境」を参照してください。</p>
SQL ウェアハウス JDBC URL	<p>Databricks SQL ウェアハウスの JDBC 接続 URL。</p> <p>このプロパティは、Databricks SQL ウェアハウスにのみ必要です。汎用クラスタとジョブクラスタには適用されません。</p> <p>SQL ウェアハウス JDBC URL を取得するには、Databricks コンソールに移動し、[JDBC URL] メニューから JDBC ドライババージョンを選択します。</p> <p>Databricks JDBC ドライババージョン 2.6.25 以降の JDBC URL を次の形式で指定します。</p> <pre>jdbc:databricks://<Databricks ホスト>:443/default;transportMode=http;ssl=1;AuthMech=3;httpPath=/sql/1.0/endpoints/<SQL エンドポイントのクラスタ ID>;</pre> <p>アプリケーション取り込みとレプリケーションタスクとデータベース取り込みとレプリケーションタスクでは、JDBC URL バージョン 2.6.25 以降または 2.6.22 以前を使用できます。URL は次のように、プレフィックス jdbc:databricks:// で始まる必要があります。</p> <pre>jdbc:databricks://<Databricks ホスト>:443/default;transportMode=http;ssl=1;AuthMech=3;httpPath=/sql/1.0/endpoints/<SQL エンドポイントのクラスタ ID>;</pre> <p>Secure Agent で必要な環境変数を設定してください。また、詳細接続設定で正しい [JDBC ドライバクラス名] を指定します。</p> <p>注: データベース名は [データベース名] 接続プロパティで指定します。JDBC URL でデータベース名を指定した場合、そのデータベース名は考慮されません。</p>

認証タイプ

Databricks にアクセスする場合に、パーソナルアクセストークン認証および OAuth Machine-to-Machine 認証のタイプを設定することができます。

必要な認証方法を選択し、認証固有のパラメータを設定します。

パーソナルアクセストークン認証にはパーソナルアクセストークンが必要となり、OAuth Machine-to-Machine 認証には Databricks アカウントのクライアント ID とクライアントシークレットが必要です。

パーソナルアクセストークン、クライアント ID、およびクライアントシークレットを取得する方法の詳細については、Databricks のマニュアルを参照してください。

パーソナルアクセストークン認証

パーソナルアクセストークン認証には、Databricks アカウントのパーソナルアクセストークンが必要です。次の表に、パーソナルアクセストークン認証の接続プロパティとその説明を示します。

プロパティ	説明
Databricks トークン	Databricks にアクセスするためのパーソナルアクセストークン。 このプロパティは、SQL ウェアハウス、汎用クラスタ、ジョブクラスタでは必須です。
カタログ名	Unity Catalog を使用する場合のメタストア内の既存のカタログの名前。 このプロパティは、SQL ウェアハウスでは省略可能です。汎用クラスタとジョブクラスタには適用されません。 カタログ名に特殊文字を含めることはできません。 Unity Catalog の詳細については、Databricks のマニュアルを参照してください。

OAuth Machine-to-Machine 認証

OAuth Machine-to-Machine 認証には、Databricks アカウントのクライアント ID とクライアントシークレットが必要です。

OAuth Machine-to-Machine 認証は、汎用クラスタ、ジョブクラスタ、および詳細モードのマッピングには適用されません。OAuth Machine-to-Machine 認証は、JDBC ドライババージョン 2.6.25 以降でのみ使用することができます。

次の表に、OAuth Machine-to-Machine 認証の接続プロパティとその説明を示します。

プロパティ	説明
クライアント ID	サービスプリンシパルのクライアント ID。
クライアントシークレット	サービスプリンシパルのクライアント ID に関連付けられているクライアントシークレット。
カタログ名	Unity Catalog を使用する場合のメタストア内の既存のカタログの名前。 このプロパティは、SQL ウェアハウスでは省略可能です。汎用クラスタとジョブクラスタには適用されません。 カタログ名に特殊文字を含めることはできません。 Unity Catalog の詳細については、Databricks のマニュアルを参照してください。

詳細設定

次の表に、詳細接続のプロパティを示します。

プロパティ	説明
データベース	<p>Databricks のスキーマの名前。</p> <p>名前には、英数字とハイフン (-) のみを含めることができます。</p> <p>このプロパティは、SQL ウェアハウス、汎用クラスタ、ジョブクラスタでは省略可能です。</p> <p>値を指定しない場合、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。指定した値は、[SQL ウェアハウス JDBC URL] 接続プロパティで指定したスキーマよりも優先されます。</p>
JDBC ドライバクラス名	<p>JDBC ドライバクラスの名前。</p> <p>このプロパティは、SQL ウェアハウス、汎用クラスタ、ジョブクラスタでは省略可能です。</p> <p>デフォルトは <code>com.databricks.client.jdbc.Driver</code> です</p>
ステージング環境	<p>処理前にデータが一時的に保存されるステージング環境。</p> <p>このプロパティは、SQL ウェアハウス、汎用クラスタ、ジョブクラスタでは必須です。</p> <p>ステージング環境として次のいずれかのオプションを選択します。</p> <ul style="list-style-type: none">- AWS。Databricks が AWS プラットフォームでホストされている場合。- Azure。Databricks が Azure プラットフォームでホストされている場合。- 個人用ステージングの場所¹。ローカルの個人用ストレージの場所にデータをステージングする場合。 <p>データ取り込みおよびレプリケーションで使用する接続に [個人用ステージングの場所] を選択した場合は、アプリケーション取り込みとレプリケーションジョブまたはデータベース取り込みとレプリケーションジョブの Parquet データファイルをローカルの個人用ストレージの場所にステージングできます。データ保持期間は 7 日間です。また、[データベースホスト] の値も指定する必要があります。Unity Catalog を使用する場合は、個人用ストレージの場所が自動的にプロビジョニングされます。ただし、Databricks アンマネージドテーブルで個人用ステージングの場所を使用することはできません。</p> <ul style="list-style-type: none">- ボリューム¹。Databricks のボリュームにデータをステージングする場合。ボリュームは、ファイルやディレクトリなどの表形式以外のデータセットを管理および保護するために使用される Unity Catalog オブジェクトです。 <p>注: Google Cloud Platform でホストされている Databricks エンドポイントに接続するように Databricks 接続を設定する場合は、ボリュームを使用してデータをステージングする必要があります。</p> <p>ボリュームと個人用ステージングの場所はどちらも、汎用クラスタとジョブクラスタには適用されません。</p> <p>デフォルトは [ボリューム] です。</p> <p>注: 接続を確立した後にクラスタを切り替えることはできません。</p> <p>重要: 2024 年 10 月リリースから、個人用ステージングの場所は非推奨になりました。非推奨になった機能はまだサポートされていますが、今後のリリースではサポートが廃止される予定です。ボリュームを使用してデータをステージングすることをお勧めします。</p>
ボリュームパス	<p>データを一時的にステージングするボリュームの絶対パス。</p> <p>次の形式でパスを指定します。</p> <p><code>/Volumes/<catalog_identifier>/<schema_identifier>/<volume_identifier>/</code></p> <p>ボリュームパスを指定しない場合、セキュアエージェントは Databricks にマネージドボリュームを作成します。</p>

プロパティ	説明
Databricks ホスト	<p>Databricks アカウントが属するエンドポイントのホスト名。</p> <p>このプロパティは、汎用クラスタとジョブクラスタにのみ必要です。SQL ウェアハウスには適用されません。</p> <p>Databricks ホストは、JDBC URL から取得することができます。この URL は、Databricks 汎用クラスタの JDBC または ODBC の [詳細オプション] で確認できます。</p> <p>次の例に、JDBC URL の Databricks ホストを示します。</p> <pre>jdbc:databricks://<Databricks Host>:443/ default;transportMode=http; ssl=1;httpPath=sql/protocolv1/o/<Org Id>/<Cluster ID>; AuthMech=3; UID=token; PWD=<personal-access-token></pre> <p>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。</p>
クラスタ ID	<p>クラスタの ID。</p> <p>このプロパティは、汎用クラスタとジョブクラスタにのみ必要です。SQL ウェアハウスには適用されません。</p> <p>クラスタ ID は、JDBC URL から取得できます。この URL は、Databricks 汎用クラスタの JDBC または ODBC の [詳細オプション] で確認できます</p> <p>次の例に、JDBC URL のクラスタ ID を示します。</p> <pre>jdbc:databricks://<Databricks Host>:443/ default;transportMode=http; ssl=1;httpPath=sql/protocolv1/o/<Org Id>/<Cluster ID>; AuthMech=3;UID=token; PWD=<personal-access-token></pre>
組織 ID	<p>Databricks のワークスペースの一意的組織 ID。</p> <p>このプロパティは、汎用クラスタとジョブクラスタにのみ必要です。SQL ウェアハウスには適用されません。</p> <p>組織 ID は、JDBC URL から取得できます。この URL は、Databricks 汎用クラスタの JDBC または ODBC の [詳細オプション] で確認できます</p> <p>次の例に、JDBC URL の組織 ID を示します。</p> <pre>jdbc:databricks://<Databricks Host>:443/ default;transportMode=http; ssl=1;httpPath=sql/protocolv1/o/<Organization ID>/ <Cluster ID>;AuthMech=3;UID=token; PWD=<personal-access-token></pre>
最小ワーカー数 ¹	<p>Spark ジョブに使用される最小のワーカーノードの数。最小値は 1 です。</p> <p>このプロパティは、ジョブクラスタにのみ必要です。SQL ウェアハウスと汎用クラスタには適用されません。</p>
最大ワーカー数 ¹	<p>Spark ジョブに使用される最大のワーカーノードの数。自動スケーリングを行わない場合は、最大ワーカー数を最小ワーカー数と同じ値に設定するか、最大ワーカー数を設定しないでください。</p> <p>このプロパティは、ジョブクラスタでは省略可能です。SQL ウェアハウスと汎用クラスタには適用されません。</p>
DB ランタイムバージョン ¹	<p>ジョブクラスタに接続してマッピングを処理するときに生成するジョブクラスタのバージョン。</p> <p>このプロパティは、ジョブクラスタにのみ必要です。SQL ウェアハウスと汎用クラスタには適用されません。</p> <p>Databricks ランタイムバージョン 9.1 LTS、13.3 LTS、または 15.4 LTS を選択します。</p> <p>バージョン 15.4 LTS を使用するには、Spark 設定接続プロパティの <code>spark.databricks.driver.dbfsLibraryInstallationAllowed</code> パラメーターを <code>true</code> に設定します。</p>

プロパティ	説明
ワーカーノードタイプ ¹	<p>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。</p> <p>このプロパティは、汎用クラスタとジョブクラスタにのみ必要です。SQL ウェアハウスには適用されません。</p> <p>例えば、AWS のワーカーノードタイプは <code>i3.2xlarge</code> にすることができます。Azure のワーカーノードタイプは <code>Standard_DS3_v2</code> にすることができます。</p>
ドライバノードタイプ ¹	<p>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。</p> <p>このプロパティは、ジョブクラスタでは省略可能です。SQL ウェアハウスと汎用クラスタには適用されません。</p> <p>例えば、AWS のドライバノードタイプは <code>i3.2xlarge</code> にすることができます。Azure のドライバノードタイプは <code>Standard_DS3_v2</code> にすることができます。</p> <p>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。</p>
インスタンスプール ID ¹	<p>Spark クラスタに使用されるインスタンスプール ID。</p> <p>このプロパティは、ジョブクラスタでは省略可能です。SQL ウェアハウスと汎用クラスタには適用されません。</p> <p>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。</p> <ul style="list-style-type: none"> - ドライバノードタイプ - EBS ボリューム数 - EBS ボリュームタイプ - EBS ボリュームサイズ - Elastic Disk を有効にする - ワーカーノードタイプ - ゾーン ID
エラスティックディスク ¹	<p>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。</p> <p>このプロパティは、ジョブクラスタでは省略可能です。SQL ウェアハウスと汎用クラスタには適用されません。</p> <p>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。</p>
Spark 設定 ¹	<p>ジョブクラスタで使用される Spark 設定。</p> <p>このプロパティは、ジョブクラスタでは省略可能です。SQL ウェアハウスと汎用クラスタには適用されません。</p> <p>設定は次の形式である必要があります。</p> <pre>"key1"="value1";"key2"="value2";...</pre> <p>例: <code>"spark.executor.userClassPathFirst"="False"</code></p> <p>Databricks ランタイムバージョン 15.4 を使用するには、次のパラメーターを指定します。</p> <pre>'spark.databricks.driver.dbfsLibraryInstallationAllowed'='true'</pre> <p>データ取り込みおよびレプリケーションタスクには適用されません。</p>
Spark 環境変数 ¹	<p>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。</p> <p>このプロパティは、ジョブクラスタでは省略可能です。SQL ウェアハウスと汎用クラスタには適用されません。</p> <p>この変数は、以下の形式で指定する必要があります。</p> <pre>"key1"="value1";"key2"="value2";...</pre> <p>例: <code>"MY_ENVIRONMENT_VARIABLE"="true"</code></p> <p>データ取り込みおよびレプリケーションタスクには適用されません。</p>
¹ 詳細モードのマッピングには適用されません。	

AWS ステージング環境

次の表に、AWS ステージング環境のプロパティを示します。

プロパティ	説明
S3 認証モード	Amazon S3 に接続するための認証モード。 次のいずれかの認証モードを選択します。 <ul style="list-style-type: none">- 永続的な IAM 資格情報。S3 アクセスキーと S3 シークレットキーを使用して Amazon S3 に接続します。- IAM Assume Role¹IAM 認証に AssumeRole を使用して Amazon S3 に接続します。 この認証モードは、SQL ウェアハウスにのみ適用されます。
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 データを格納するための既存の S3 バケット。
S3 ステージングバケット	ステージングファイルを保存するための既存のバケット。
S3 VPC エンドポイントタイプ ¹	Amazon S3 用の Amazon Virtual Private Cloud エンドポイントのタイプ。 VPC エンドポイントを使用して、Amazon S3 とのプライベート通信を有効にすることができます。 次のいずれかのオプションを選択します。 <ul style="list-style-type: none">- なし。VPC エンドポイントを使用しない場合に選択します。- インタフェースエンドポイント。サブネットの IP アドレス範囲のプライベート IP アドレスを使用しているインタフェースエンドポイント経由で Amazon S3 とのプライベート通信を確立する場合に選択します。これは、AWS のサービス宛てのトラフィックのエントリポイントとして機能します。
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。 アスタリスク記号を DNS 名内の bucket キーワードで置き換えます。 DNS 名は以下の形式で入力します。 bucket.<インタフェースエンドポイントの DNS 名> 例: bucket.vpce-s3.us-west-2.vpce.amazonaws.com
IAM ロール ARN ¹	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、 <i>AWS のマニュアル</i> を参照してください。
ロールの引き受けに EC2 ロールを使用 ¹	オプション。EC2 ロールが IAM ロール ARN オプションで指定された別の IAM ロールを引き受けることができるようにするには、このチェックボックスをオンにします。 EC2 ロールには、同じ AWS アカウントまたは異なる AWS アカウントから IAM ロールを引き受けす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。

プロパティ	説明
STS VPC エンドポイントタイプ ¹	<p>AWS Security Token Service 用の Amazon Virtual Private Cloud エンドポイントのタイプ。VPC エンドポイントを使用して、Amazon Security Token Service とのプライベート通信を有効にすることができます。</p> <p>次のいずれかのオプションを選択します。</p> <ul style="list-style-type: none"> - なし。VPC エンドポイントを使用しない場合に選択します。 - インタフェースエンドポイント。サブネットの IP アドレス範囲のプライベート IP アドレスを持つインタフェースエンドポイント経由で Amazon Security Token Service とのプライベート通信を確立する場合に選択します。
AWS STS のエンドポイント DNS 名 ¹	<p>AWS STS インタフェースエンドポイントの DNS 名。</p> <p>例: <code>vpce-01f22cc14558c241f-s8039x4c.sts.us-west-2.vpce.amazonaws.com</code></p>
S3 サービスリージョナルエンドポイント	<p>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。このプロパティは、SQL ウェアハウスでは省略可能です。汎用クラスタとジョブクラスタには適用されません。</p> <p>デフォルトは <code>s3.amazonaws.com</code> です。</p>
S3 リージョン名 ¹	<p>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。</p> <p>[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。</p>
ゾーン ID ¹	<p>Databricks ジョブクラスタのゾーン ID。</p> <p>このプロパティは、ジョブクラスタでは省略可能です。SQL ウェアハウスと汎用クラスタには適用されません。</p> <p>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、ゾーン ID を指定します。</p> <p>例: <code>us-west-2a</code>。</p> <p>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。</p>
EBS ボリュームタイプ ¹	<p>クラスタで起動される EBS ボリュームのタイプ。</p> <p>このプロパティは、ジョブクラスタでは省略可能です。SQL ウェアハウスと汎用クラスタには適用されません。</p>
EBS ボリューム数 ¹	<p>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。</p> <p>このプロパティは、ジョブクラスタでは省略可能です。SQL ウェアハウスと汎用クラスタには適用されません。</p> <p>注: Databricks 接続では、インスタンスストアを使用せずに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。</p>
EBS ボリュームサイズ ¹	<p>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)。</p> <p>このプロパティは、ジョブクラスタでは省略可能です。SQL ウェアハウスと汎用クラスタには適用されません。</p>
¹ 詳細モードのマッピングには適用されません。	

Azure ステージング環境

次の表に、Azure ステージング環境のプロパティを示します。

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

JDBC URL パラメータ

Databricks 接続の追加の JDBC URL パラメータフィールドを利用して、Databricks への接続に必要な追加パラメータをカスタマイズおよび設定できます。

Databricks 接続では、追加の JDBC URL パラメータとして次のようなプロパティを設定することができます。

- プロキシサーバーを使用して Databricks に接続するには、次のパラメータを入力します。
`jdbc:databricks://<Databricks Host>:443/default;transportMode=http;ssl=1;AuthMech=3;httpPath=/sql/1.0/warehouses/219fe3013963cdce;UseProxy=<Proxy=true>;ProxyHost=<proxy host IPaddress>;ProxyPort=<proxy server port number>;ProxyAuth=<Auth_true>;`
注: データ取り込みおよびレプリケーションでは、プロキシサーバーを使用した Databricks への接続はサポートされていません。
- SSL 対応の Databricks に接続するには、JDBC URL に次の形式で値を指定します。
`jdbc:databricks://<Databricks Host>:443/default;transportMode=http;ssl=1;AuthMech=3;httpPath=/sql/1.0/endpoints/<SQL endpoint cluster ID>;`

プロキシサーバーの設定

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

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

Secure Agent のプロキシの設定を行うには、次のタスクを実行します。

- Windows の場合は Secure Agent Manager を使用し、Linux の場合はシェルコマンドを使用して Secure Agent を設定します。
手順については、データ統合のヘルプの『または「Windows でのプロキシ設定」または「Linux でのプロキシ設定」を参照してください。』
- Secure Agent のプロパティで、DTM の JVM オプションを設定します。手順については、ナレッジベースの記事「[Proxy server settings](#)」を参照してください。

プロキシ設定は、AWS ステージング環境を使用している場合にのみ設定できます。サーバーレスランタイム環境を使用している場合は、プロキシサーバーを使用することはできません。

データ取り込みおよびレプリケーションでは、プロキシサーバーの設定はサポートされていません。

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

Databricks にアクセスするためのプライベートリンク

Secure Agent と Microsoft Azure プラットフォームまたは AWS プラットフォームでホストされている Databricks エンドポイント間のプライベート通信を有効にすることができます。

Azure Private Link

パーソナルアクセストークンまたは OAuth Machine-to-Machine 認証を使用して、Secure Agent と Microsoft Azure プラットフォームでホストされている Databricks エンドポイント間のプライベート通信が有効になるように Azure Private Link を設定できます。

プライベート Azure ネットワーク経由で Databricks アカウントに接続するには、「[Secure connectivity to Azure Data Services](#)」を参照してください。

AWS Private Link

パーソナルアクセストークンを使用して、Secure Agent と AWS プラットフォームでホストされている Databricks エンドポイント間のプライベート通信が有効になるように AWS Private Link を設定できます。

データ取り込みおよびレプリケーションでは、Azure Private Link を使用した Databricks へのアクセスはサポートされていません。

個人用ステージングの場所についてのルールおよびガイドライン

ステージング環境として個人用ステージングの場所を選択すると、データは最初に Java の一時的な場所にステージングされ、次に Unity カタログの個人用ステージングの場所にコピーされます。タスクが正常に実行された後に、ステージングされたファイルはどちらも削除されます。

ただし、データを別のディレクトリにステージングするには、Administrator サービスのシステム構成設定の JVM オプションで DTM プロパティ -Djava.io.tmpdir=/my/dir/path を設定します。

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

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

- SQL ウェアハウス JDBC URL では、Unity 対応カタログのみを指定できます。
- OAuth Machine-to-Machine 認証を使用するステージング環境として、個人用ステージングの場所を使用することはできません。
- マッピングは SQL ELT の最適化なしで実行されます。
- データはフォルダ `stage://tmp/<user_name>` にステージングされます。ここで、`<user_name>` は接続で提供される Databricks トークンから選択され、これには AWS および Azure のルートのある個人用ステージングの場所への読み取りおよび書き込みアクセス権が必要となります。

重要: 2024 年 10 月リリースから、個人用ステージングの場所は非推奨になりました。現在のリリースではこの機能を使用できますが、Informatica は将来のリリースでこの機能のサポートを終了する予定です。ポリシーを使用してデータをステージングすることをお勧めします。

第 51 章

Datacom CDC 接続のプロパティ

Datacom CDC 接続を設定するには、接続プロパティを設定する必要があります。

次の表に、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。
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gger（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。 <i>host_name</i> は、ホスト名または IP アドレスにできます。 <i>host_name:port_number</i> 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。

プロパティ	説明
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gger (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。 <ul style="list-style-type: none"> - 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gger (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。

プロパティ	説明
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	<p>カスタムプロパティまたは接続プロパティのオーバーライド。カスタムプロパティとは、PowerExchange のデフォルトの設定よりも優先するために指定できるプロパティです。セミコロン (;) を区切り文字として使用して複数のプロパティを入力するか、パラメータファイルを使用して接続プロパティの上書きを指定するパラメータを指定することができます。</p> <p>例:</p> <pre><property>=<value>;<property>=<value></pre> <p>多くの場合、Informatica グローバルカスタマサポートからの指示を受けたうえで、カスタムプロパティの設定を行います。</p> <p>注: これらのプロパティは、PowerCenter の PowerExchange Client for PowerCenter (PWXPC) CDC 接続の 【PWX オーバーライド】 オプションと同じです。</p> <p>パラメータファイルを使用して接続プロパティのオーバーライドを指定するには、\$<ParameterName>の形式でパラメータを設定し、ユーザー定義パラメータ名の前にドル記号 (\$) を付けます。次に、【ランタイムオプション】 タブの 【パラメータファイル名】 フィールドにパラメータファイル名を指定することで、ユーザー定義パラメータ定義を含むパラメータファイルを使用するようにマッピングのマッピングタスクを設定します。</p> <p>注:</p> <ul style="list-style-type: none"> - マッピングおよび接続に同じパラメータを入力した場合は、接続カスタムプロパティが優先されます。 - パラメータファイルがある場合、このフィールドで指定するパラメータ名は、パラメータファイルで定義されたエントリと一致している必要があります。 <p>詳細については、「接続オーバーライドのリファレンス」の章を参照してください。</p>

第 52 章

Datacom 接続のプロパティ

Datacom 接続を設定するには、接続プロパティを設定する必要があります。

以下の表に、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。
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。 <i>host_name</i> は、ホスト名または IP アドレスにできます。 <i>host_name: port_number</i> 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。

プロパティ	説明
オフロード処理	<p>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。</p> <ul style="list-style-type: none"> - 自動。オフロード処理を使用するかどうかは 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。 <p>デフォルトは [いいえ] です。</p>
オフロードスレッド	<p>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。</p> <p>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。</p> <p>有効な値は 1~64 です。</p> <p>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。</p> <p>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。</p>
配列サイズ	<p>有効な値は 1~5000 です。デフォルトは 25 です。</p>
低値をスペースに置き換える	<p>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。</p>
接続リトライ期限	<p>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。</p>

プロパティ	説明
カスタムプロパティ	<p>カスタムプロパティまたは接続プロパティのオーバーライド。カスタムプロパティとは、PowerExchange のデフォルトの設定よりも優先するために指定できるプロパティです。セミコロンの (;) 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。</p> <p>例:</p> <pre><property>=<value>;<property>=<value></pre> <p>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。</p> <p>注: これらのプロパティは、PowerCenter の PowerExchange Client for PWX NRDB Batch 接続の [PWX オーバーライド] オプションと同じです。</p> <p>また、このフィールドまたはパラメータファイルを使用して、接続プロパティのオーバーライドを指定することもできます。パラメータファイルを使用して接続プロパティのオーバーライドを指定するには、\$<ParameterName>の形式でパラメータを設定し、ユーザー定義パラメータ名の前にドル記号 (\$) を付けます。次に、[ランタイムオプション] タブの [パラメータファイル名] フィールドにパラメータファイル名を指定することで、ユーザー定義パラメータ定義を含むパラメータファイルを使用するようにマッピングのマッピングタスクを設定します。</p> <p>注:</p> <ul style="list-style-type: none"> - マッピングおよび接続に同じパラメータを入力した場合は、接続カスタムプロパティが優先されます。 - パラメータファイルがある場合、このフィールドで指定するパラメータ名は、パラメータファイルで定義されたエントリと一致している必要があります。 <p>詳細については、「接続オーバーライドのリファレンス」の章を参照してください。</p>
書き込みモード	<p>書き込みモード。次のオプションがあります。</p> <ul style="list-style-type: none"> - 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。

第 53 章

Db2 データマップ接続のプロパティ

Db2 データマップ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 データマップ接続プロパティを示します。

プロパティ	説明
接続名	Db2 データマップ接続の名前。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 データマップ接続の説明（オプション）。最大長は 4000 文字です。
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 データマップの要求を処理する PowerExchange Listener 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。 <i>host_name</i> は、ホスト名または IP アドレスにできます。 <i>host_name:port_number</i> 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。

プロパティ	説明
オフロード処理	<p>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。</p> <ul style="list-style-type: none"> - 自動。オフロード処理を使用するかどうかは 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と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。ソースシステムでデータをフィルタリングし、バルクデータ処理をターゲットにオフロードします。 - いいえ。オフロード処理を無効化します。 <p>デフォルトは [いいえ] です。</p>
オフロードスレッド	<p>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。</p> <p>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であるか同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。</p> <p>有効な値は 1～64 です。</p> <p>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。</p> <p>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。</p>
配列サイズ	<p>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）。</p> <p>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。</p> <p>有効な値は 1～5000 です。デフォルトは 25 です。</p> <p>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。</p>
低値をスペースに置き換える	<p>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。</p>

プロパティ	説明
接続リトライ期限	最初の接続の試行が失敗してから、PowerExchange Bulk Reader が PowerExchange Listener 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、その場合、接続の再試行は無効になります。
カスタムプロパティ	<p>カスタムプロパティまたは接続プロパティのオーバーライド。カスタムプロパティとは、PowerExchange のデフォルトの設定よりも優先するために指定できるプロパティです。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。</p> <p>例:</p> <pre><property>=<value>;<property>=<value></pre> <p>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。</p> <p>注: これらのプロパティは、PowerCenter の PowerExchange Client for PWX NRDB Batch 接続の [PWX オーバーライド] オプションと同じです。</p> <p>また、このフィールドまたはパラメータファイルを使用して、接続プロパティのオーバーライドを指定することもできます。パラメータファイルを使用して接続プロパティのオーバーライドを指定するには、<code>\$<ParameterName></code> の形式でパラメータを設定し、ユーザー定義パラメータ名の前にドル記号 (\$) を付けます。次に、[ランタイムオプション] タブの [パラメータファイル名] フィールドにパラメータファイル名を指定することで、ユーザー定義パラメータ定義を含むパラメータファイルを使用するようにマッピングのマッピングタスクを設定します。</p> <p>注:</p> <ul style="list-style-type: none"> - マッピングおよび接続に同じパラメータを入力した場合は、接続カスタムプロパティが優先されます。 - パラメータファイルがある場合、このフィールドで指定するパラメータ名は、パラメータファイルで定義されたエントリと一致している必要があります。 <p>詳細については、「接続オーバーライドのリファレンス」の章を参照してください。</p>

第 54 章

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。
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gger（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。 <i>host_name</i> は、ホスト名または IP アドレスにできます。 <i>host_name:port_number</i> 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、DBMOVE 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。

プロパティ	説明
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gger (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	<p>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。</p> <ul style="list-style-type: none"> - 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。 <p>デフォルトは [なし] です。</p>
ページングサイズ	<p>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。</p> <p>デフォルトである最小値は 0 です。</p>
ページング単位	<p>[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。</p> <p>[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。</p>
マップの場所	<p>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。</p> <p>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gger (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。</p> <p>次の形式で値を入力します。<i>host_name</i> は、ホスト名または IP アドレスにできます。</p> <p><i>host_name:port_number</i></p> <p>以下に例を示します。</p> <p>DB2CDC01:25100</p> <p>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。</p>
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。

プロパティ	説明
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	<p>カスタムプロパティまたは接続プロパティのオーバーライド。カスタムプロパティとは、PowerExchange のデフォルトの設定よりも優先するために指定できるプロパティです。セミコロン (;) を区切り文字として使用して複数のプロパティを入力するか、パラメータファイルを使用して接続プロパティの上書きを指定するパラメータを指定することができます。</p> <p>例:</p> <pre><property>=<value>;<property>=<value></pre> <p>多くの場合、Informatica グローバルカスタマサポートからの指示を受けたうえで、カスタムプロパティの設定を行います。</p> <p>注: これらのプロパティは、PowerCenter の PowerExchange Client for PowerCenter (PWXPC) CDC 接続の [PWX オーバーライド] オプションと同じです。</p> <p>パラメータファイルを使用して接続プロパティのオーバーライドを指定するには、\$<ParameterName>の形式でパラメータを設定し、ユーザー定義パラメータ名の前にドル記号 (\$) を付けます。次に、[ランタイムオプション] タブの [パラメータファイル名] フィールドにパラメータファイル名を指定することで、ユーザー定義パラメータ定義を含むパラメータファイルを使用するようにマッピングのマッピングタスクを設定します。</p> <p>注:</p> <ul style="list-style-type: none"> - マッピングおよび接続に同じパラメータを入力した場合は、接続カスタムプロパティが優先されます。 - パラメータファイルがある場合、このフィールドで指定するパラメータ名は、パラメータファイルで定義されたエントリと一致している必要があります。 <p>詳細については、「接続オーバーライドのリファレンス」の章を参照してください。</p>

第 55 章

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。
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。 <i>host_name</i> は、ホスト名または IP アドレスにできます。 <i>host_name:port_number</i> 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。

プロパティ	説明
分離レベル	<p>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。</p> <ul style="list-style-type: none"> - ALL - CS - CHG - なし - RR <p>デフォルトは CS です</p>
データベースファイルのオーバーライド:	<p>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。</p> <p>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。</p>
ライブラリリスト:	<p>接続に使用する Db2 for i ライブラリリストの名前。</p>
環境 SQL	<p>データベース環境で実行する SQL コマンド。</p>
配列サイズ	<p>有効な値は 1～5000 です。デフォルトは 25 です。</p>
低値をスペースに置き換える	<p>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。</p>
接続リトライ期限	<p>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。</p>
カスタムプロパティ	<p>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。</p> <p>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。</p>
書き込みプロパティ	<p>書き込みモード。次のオプションがあります。</p> <ul style="list-style-type: none"> - 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的に送信します。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。 <p>デフォルト値は【書き込み確認オン】です。</p>
拒否ファイル	<p>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。</p> <p>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。</p> <p>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。</p>

第 56 章

Db2 for i Database Ingestion 接続のプロパティ

Db2 for i データベース取り込み接続を定義するには、接続プロパティを設定します。この接続タイプは、データ取り込みおよびレプリケーションで設定したデータベース取り込みとレプリケーションタスクで使用することができます。

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。
ランタイム環境	データベース取り込みとレプリケーション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。 ローカルの Secure Agent インストールまたはサーバーレスランタイム環境のいずれかを使用できます。サーバーレスランタイム環境は、クラウドソースタイプおよびクラウドターゲットタイプに使用できます。ホステッドエージェントでデータベース取り込みとレプリケーションタスクを実行することはできません。
ユーザー名	Db2 for i インスタンスへの接続に使用するユーザー名。
パスワード	Db2 for i インスタンスへの接続に使用するパスワード。
ホスト	データベースサーバをホストするマシンの名前。
ポート	データベースサーバーへの接続時に使用するネットワークポート番号。
場所名	アクセスする Db2 for i ロケーションの名前。システム管理者は、WRKRDBDIRE コマンドを使用して、Db2 ロケーションの名前を判別できます。出力で *LOCAL としてリストされているデータベースの名前を見つけ、その値をこのプロパティの値として使用します。
JDBC ドライバ	Db2 for i ソースへの接続に使用する JDBC ドライバのタイプ。次のオプションがあります。 - Progress DataDirect Db2 JDBC。Db2 用の DataDirect JDBC ドライバを使用します。 - IBM JTOpen JDBC。IBM JTOpen JDBC ドライバを使用します。 デフォルトは Progress DataDirect Db2 JDBC です。

プロパティ	説明
ビットデータのコードページ	データベース取り込みとレプリケーション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	<p>Db2 for i ソースへの接続に使用される JDBC ドライバの詳細プロパティ。property=value エントリを複数指定する場合は、セミコロン (;) で区切ります。</p> <p>Progress DataDirect Db2 JDBC ドライバ接続プロパティの詳細については、Progress DataDirect documentation を参照してください。例えば、ConnectionRetryCount プロパティを設定して、ドライバがプライマリデータベースサーバーへの接続を再試行する回数を制御できます。</p> <p>IBM JTOpen JDBC ドライバ接続プロパティの詳細については、IBM Toolbox for Java JDBC properties を参照してください。</p>
暗号化方法	<p>IBM JTOpen JDBC ドライバのデータ暗号化方式。次のオプションがあります。</p> <ul style="list-style-type: none"> - 暗号化なし - SSL <p>デフォルトは [暗号化なし] です。</p> <p>SSL を選択する場合は、次のいずれかの場所にある Informatica Cloud Secure Agent JRE cacerts キーストアに必要な証明書を追加する必要があります。</p> <p>Linux の場合:</p> <p><i>Secure Agent Directory\jdk\jre\lib\security\cacerts</i></p> <p>Windows の場合:</p> <p><i>Secure Agent Directory\apps\jdkLatestVersion\jre</i></p>

第 57 章

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。
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gger（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まれます。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。 <i>host_name:port_number</i> 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 リフレッシュマニユアル』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。

プロパティ	説明
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gger（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	<p>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。</p> <ul style="list-style-type: none"> - 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。 <p>デフォルトは [なし] です。</p>
ページングサイズ	<p>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。</p> <p>デフォルトである最小値は 0 です。</p>
ページング単位	<p>[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。</p> <p>[行] または [キロバイト] のいずれかを選択します。</p>
マップの場所	<p>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。</p> <p>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gger（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。</p> <p>次の形式で値を入力します。<i>host_name</i> は、ホスト名または IP アドレスにできます。</p> <p><i>host_name:port_number</i></p> <p>以下に例を示します。</p> <p>DB2UNIX2B:25100</p> <p>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。</p>
マップの場所のユーザー	<p>[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。</p>

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 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	<p>カスタムプロパティまたは接続プロパティのオーバーライド。カスタムプロパティとは、PowerExchange のデフォルトの設定よりも優先するために指定できるプロパティです。セミコロン (;) を区切り文字として使用して複数のプロパティを入力するか、パラメータファイルを使用して接続プロパティの上書きを指定するパラメータを指定することができます。</p> <p>例:</p> <pre><property>=<value>;<property>=<value></pre> <p>多くの場合、Informatica グローバルカスタマサポートからの指示を受けたいうえで、カスタムプロパティの設定を行います。</p> <p>注: これらのプロパティは、PowerCenter の PowerExchange Client for PowerCenter (PWXPC) CDC 接続の 【PWX オーバーライド】 オプションと同じです。</p> <p>パラメータファイルを使用して接続プロパティのオーバーライドを指定するには、\$<ParameterName>の形式でパラメータを設定し、ユーザー定義パラメータ名の前にドル記号 (\$) を付けます。次に、【ランタイムオプション】 タブの 【パラメータファイル名】 フィールドにパラメータファイル名を指定することで、ユーザー定義パラメータ定義を含むパラメータファイルを使用するようにマッピングのマッピングタスクを設定します。</p> <p>注:</p> <ul style="list-style-type: none"> - マッピングおよび接続に同じパラメータを入力した場合は、接続カスタムプロパティが優先されます。 - パラメータファイルがある場合、このフィールドで指定するパラメータ名は、パラメータファイルで定義されたエントリと一致している必要があります。 <p>詳細については、「接続オーバーライドのリファレンス」の章を参照してください。</p>

第 58 章

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

Db2 for LUW データベース取り込み接続を定義するには、接続プロパティを設定します。この接続タイプは、データ取り込みおよびレプリケーションで設定したデータベース取り込みとレプリケーションタスクで使用することができます。

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。
ランタイム環境	データベース取り込みとレプリケーション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への接続時に使用するネットワークポート番号。
データベース名	アクセスする Db2 for LUW ロケーションの名前。
詳細接続プロパティ	Db2 for LUW ソースへの接続に使用される Progress DataDirect JDBC DB2 ドライバの詳細プロパティ。 <i>property=value</i> エントリを複数指定する場合は、セミコロン (;) で区切ります。 このフィールドに入力できるドライバのプロパティについては、 connection properties にある Progress DataDirect のドキュメントで説明されています。例えば、EncryptionMethod プロパティを設定して、ドライバとデータベースサーバ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。

第 59 章

Db2 for z/OS バルクロード接続のプロパティ

Db2 for z/OS バルクロード接続を設定するには、接続プロパティを設定する必要があります。

次の表に、Db2 for z/OS バルクロード接続プロパティを示します。

プロパティ	説明
接続名	Db2 for z/OS バルクロード接続の名前。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 バルクロード接続の説明。最大長は 4000 文字です。
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 バルクロードの要求を処理する PowerExchange Listener 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。 <i>host_name</i> は、ホスト名または IP アドレスにできます。 <i>host_name:port_number</i> 以下に例を示します。 LSNR1:1467?
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。

プロパティ	説明
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。
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。
書き込みモード	次のオプションがあります。 <ul style="list-style-type: none"> - 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。
カスタムプロパティ	<p>カスタムプロパティまたは接続プロパティのオーバーライド。カスタムプロパティとは、PowerExchange のデフォルトの設定よりも優先するために指定できるプロパティです。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。</p> <p>例:</p> <pre><property>=<value>;<property>=<value></pre> <p>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。</p> <p>注: これらのプロパティは、PowerCenter の PowerExchange Client for PWX NRDB Batch 接続の [PWX オーバーライド] オプションと同じです。</p> <p>また、このフィールドまたはパラメータファイルを使用して、接続プロパティのオーバーライドを指定することもできます。パラメータファイルを使用して接続プロパティのオーバーライドを指定するには、\$<ParameterName>の形式でパラメータを設定し、ユーザー定義パラメータ名の前にドル記号 (\$) を付けます。次に、[ランタイムオプション] タブの [パラメータファイル名] フィールドにパラメータファイル名を指定することで、ユーザー定義パラメータ定義を含むパラメータファイルを使用するようにマッピングのマッピングタスクを設定します。</p> <p>注:</p> <ul style="list-style-type: none"> - マッピングおよび接続に同じパラメータを入力した場合は、接続カスタムプロパティが優先されます。 - パラメータファイルがある場合、このフィールドで指定するパラメータ名は、パラメータファイルで定義されたエントリと一致している必要があります。 <p>詳細については、「接続オーバーライドのリファレンス」の章を参照してください。</p>

第 60 章

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。
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gger（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。 <i>host_name</i> は、ホスト名または IP アドレスにできます。 <i>host_name:port_number</i> 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 【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。

プロパティ	説明
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gger (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	<p>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。</p> <ul style="list-style-type: none"> - 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。 <p>デフォルトは【なし】です。</p>
ページングサイズ	<p>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。</p> <p>デフォルトである最小値は 0 です。</p>
ページング単位	<p>【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。</p> <p>【行】 または 【キロバイト】 のいずれかを選択します。</p>
マップの場所	<p>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。</p> <p>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gger (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。</p> <p>次の形式で値を入力します。 <i>host_name</i> は、ホスト名または IP アドレスにできます。</p> <p><i>host_name:port_number</i></p> <p>以下に例を示します。</p> <p>DB2CDC01:25100</p> <p>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。</p>
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。

プロパティ	説明
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	<p>カスタムプロパティまたは接続プロパティのオーバーライド。カスタムプロパティとは、PowerExchange のデフォルトの設定よりも優先するために指定できるプロパティです。セミコロン (;) を区切り文字として使用して複数のプロパティを入力するか、パラメータファイルを使用して接続プロパティの上書きを指定するパラメータを指定することができます。</p> <p>例:</p> <pre><property>=<value>;<property>=<value></pre> <p>多くの場合、Informatica グローバルカスタマサポートからの指示を受けたうえで、カスタムプロパティの設定を行います。</p> <p>注: これらのプロパティは、PowerCenter の PowerExchange Client for PowerCenter (PWXPC) CDC 接続の【PWX オーバーライド】オプションと同じです。</p> <p>パラメータファイルを使用して接続プロパティのオーバーライドを指定するには、\$<ParameterName>の形式でパラメータを設定し、ユーザー定義パラメータ名の前にドル記号 (\$) を付けます。次に、【ランタイムオプション】タブの【パラメータファイル名】フィールドにパラメータファイル名を指定することで、ユーザー定義パラメータ定義を含むパラメータファイルを使用するようにマッピングのマッピングタスクを設定します。</p> <p>注:</p> <ul style="list-style-type: none"> - マッピングおよび接続に同じパラメータを入力した場合は、接続カスタムプロパティが優先されます。 - パラメータファイルがある場合、このフィールドで指定するパラメータ名は、パラメータファイルで定義されたエントリと一致している必要があります。 <p>詳細については、「接続オーバーライドのリファレンス」の章を参照してください。</p>

第 61 章

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。 <i>host_name</i> は、ホスト名または IP アドレスにできます。 <i>host_name:port_number</i> 以下に例を示します。 LSNR1:1467?
DB2 サブシステム ID	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。

プロパティ	説明
環境 SQL	データベース環境で実行する SQL コマンド。
関連 ID	Db2 要求の Db2 関連 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。 <ul style="list-style-type: none"> - 自動。オフロード処理を使用するかどうか 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。
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。

プロパティ	説明
フォールトトレランスと非同期	<p>【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。</p>
書き込みプロパティ	<p>書き込みモード。次のオプションがあります。</p> <ul style="list-style-type: none"> - 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	<p>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。</p>

第 62 章

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

Db2 for zOS データベース取り込み接続を定義するには、接続プロパティを設定します。この接続タイプは、データ取り込みおよびレプリケーションで設定したデータベース取り込みとレプリケーションタスクで使用することができます。

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。
ランタイム環境	データベース取り込みとレプリケーション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。 ローカルの Secure Agent インストールまたはサーバーレスランタイム環境のいずれかを使用できます。サーバーレスランタイム環境は、クラウドソースタイプおよびクラウドターゲットタイプに使用できます。ホステッドエージェントでデータベース取り込みとレプリケーションタスクを実行することはできません。
ユーザー名	Db2 for z/OS 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 z/OS 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 z/OS の場所の名前。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 の場所の名前を判別できます。
ビットデータのコードページ	データベース取り込みとレプリケーションがビットデータとして保存された文字データを読み取るために使用するコードページ。この値は、java.io API および java.lang API の正規名である必要があります。詳細については、Oracle Java のマニュアルで、サポートされているエンコーディングを参照してください。FOR BIT DATA ソースカラムがある場合は、このプロパティを指定します。

プロパティ	説明
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。 <i>property=value</i> 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。

第 63 章

Db2 for z/OS イメージコピー接続のプロパティ

Db2 for z/OS イメージコピー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 イメージコピー接続プロパティを示します。

プロパティ	説明
接続名	Db2 for z/OS イメージコピー接続の名前。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 イメージコピー接続の説明。最大長は 4000 文字です。
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 イメージコピーの要求を処理する PowerExchange Listener 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。 <i>host_name</i> は、ホスト名または IP アドレスにできます。 <i>host_name:port_number</i> 以下に例を示します。 LSNR1:1467?
DB2 サブシステム ID	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。

プロパティ	説明
オフロード処理	<p>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。</p> <ul style="list-style-type: none"> - 自動。オフロード処理を使用するかどうか 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。 <p>デフォルトは [いいえ] です。</p>
オフロードスレッド	<p>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。</p> <p>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。</p> <p>有効な値は 1~64 です。</p> <p>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。</p> <p>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。</p>
配列サイズ	<p>有効な値は 1~5000 です。デフォルトは 25 です。</p>
低値をスペースに置き換える	<p>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。</p>
接続リトライ期限	<p>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。</p>
カスタムプロパティ	<p>カスタムプロパティまたは接続プロパティのオーバーライド。カスタムプロパティとは、PowerExchange のデフォルトの設定よりも優先するために指定できるプロパティです。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。</p> <p>例:</p> <pre><property>=<value>;<property>=<value></pre> <p>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。</p> <p>注: これらのプロパティは、PowerCenter の PowerExchange Client for PWX NRDB Batch 接続の【PWX オーバーライド】オプションと同じです。</p> <p>また、このフィールドまたはパラメータファイルを使用して、接続プロパティのオーバーライドを指定することもできます。パラメータファイルを使用して接続プロパティのオーバーライドを指定するには、\$<ParameterName>の形式でパラメータを設定し、ユーザー定義パラメータ名の前にドル記号 (\$) を付けます。次に、【ランタイムオプション】タブの【パラメータファイル名】フィールドにパラメータファイル名を指定することで、ユーザー定義パラメータ定義を含むパラメータファイルを使用するようにマッピングのマッピングタスクを設定します。</p> <p>注:</p> <ul style="list-style-type: none"> - マッピングおよび接続に同じパラメータを入力した場合は、接続カスタムプロパティが優先されます。 - パラメータファイルがある場合、このフィールドで指定するパラメータ名は、パラメータファイルで定義されたエントリと一致する必要があります。 <p>詳細については、「接続オーバーライドのリファレンス」の章を参照してください。</p>

第 64 章

Db2 for z/OS アンロードファイル 接続のプロパティ

Db2 for z/OS アンロードファイル接続を設定するには、接続プロパティを設定する必要があります。

次の表に、Db2 for z/OS アンロードファイル接続プロパティを示します。

プロパティ	説明
接続名	Db2 for z/OS アンロード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	Db2 for z/OS アンロードファイル接続の説明。最大長は 4000 文字です。
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 アンロードファイルの要求を処理する PowerExchange Listener 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。 <i>host_name</i> は、ホスト名または IP アドレスにできます。 <i>host_name:port_number</i> 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。

プロパティ	説明
オフロード処理	<p>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。</p> <ul style="list-style-type: none"> - 自動。オフロード処理を使用するかどうか 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。 <p>デフォルトは [いいえ] です。</p>
オフロードスレッド	<p>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。</p> <p>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であるか同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。</p> <p>有効な値は 1～64 です。</p> <p>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。</p> <p>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。</p>
配列サイズ	<p>VSAM データセットおよび Db2 for z/OS アンロードファイルの場合は、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するストレージ配列のサイズ（単位はレコード数）。</p> <p>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。</p> <p>有効な値は 1～5000 です。デフォルトは 25 です。</p> <p>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。</p>
低値をスペースに置き換える	<p>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。</p>

プロパティ	説明
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	<p>カスタムプロパティまたは接続プロパティのオーバーライド。カスタムプロパティとは、PowerExchange のデフォルトの設定よりも優先するために指定できるプロパティです。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。</p> <p>例:</p> <pre><property>=<value>;<property>=<value></pre> <p>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。</p> <p>注: これらのプロパティは、PowerCenter の PowerExchange Client for PWX NRDB Batch 接続の [PWX オーバーライド] オプションと同じです。</p> <p>また、このフィールドまたはパラメータファイルを使用して、接続プロパティのオーバーライドを指定することもできます。パラメータファイルを使用して接続プロパティのオーバーライドを指定するには、\$<ParameterName>の形式でパラメータを設定し、ユーザー定義パラメータ名の前にドル記号 (\$) を付けます。次に、[ランタイムオプション] タブの [パラメータファイル名] フィールドにパラメータファイル名を指定することで、ユーザー定義パラメータ定義を含むパラメータファイルを使用するようにマッピングのマッピングタスクを設定します。</p> <p>注:</p> <ul style="list-style-type: none"> - マッピングおよび接続に同じパラメータを入力した場合は、接続カスタムプロパティが優先されます。 - パラメータファイルがある場合、このフィールドで指定するパラメータ名は、パラメータファイルで定義されたエントリと一致している必要があります。 <p>詳細については、「接続オーバーライドのリファレンス」の章を参照してください。</p>

第 65 章

DB2 ロードー接続のプロパティ

DB2 ロードー接続を作成して、DB2 に安全にデータの書き込みを行います。

前提条件

DB2 に書き込みを行うための DB2 ロードー接続を作成する前に、前提条件を必ず満たすようにしてください。

DB2 ロードー JDBC ドライバと DB2 クライアントのインストール

DB2 データベースにデータの書き込みを行うには、DB2 ロードー JDBC ドライバと DB2 クライアントを Secure Agent マシンにインストールする必要があります。

- DB2 ロードー JDBC ドライバを Secure Agent マシンにインストールします。
ドライバをインストールするには、次の手順を実行します。
 - DB2 ロードー JDBC ドライバを取得する方法については、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。
 - Secure Agent マシンが Windows マシンであるか Linux マシンであるかに基づいて、次のディレクトリに `informatica.db2loader` フォルダを手動で作成します:

Secure Agent マシン	ディレクトリ
Linux	<Secure Agent のインストールディレクトリ>/ext/connectors/thirdparty/informatica.db2loader
Windows	<Secure Agent のインストールディレクトリ>\ext\connectors\thirdparty\informatica.db2loader

- DB2 ロードー JDBC ドライバを `informatica.db2loader` フォルダにコピーします。
- DB2 ロードー LUW ドライバを Secure Agent マシンにインストールします。
DB2 LUW クライアントをインストールするには、次の手順を実行します。
 - IBM Web サイトから DB2 LUW クライアントおよびインスタンスをダウンロードしてインストールします。

2. Secure Agent マシンが Windows マシンであるか Linux マシンであるかに基づいて、次の環境変数を設定します。

Secure Agent マシン	環境変数
Linux	<ul style="list-style-type: none">- setenv DB2INSTANCE <DB2 インスタンスディレクトリ>- setenv DB2CLP DB20FADE- setenv PATH <DB2 クライアントディレクトリ>/bin- setenv LD_LIBRARY_PATH <DB2 クライアントディレクトリ>/lib64
Windows	setenv DB2CLP DB20FADE

DB2 ロードー JDBC ドライバをインストールし、環境変数を設定した後に、Secure Agent を再起動する必要があります。

DB2 ロードーへの接続

DB2 データベースに接続するように DB2 ロードーの接続プロパティを設定してみましょう。

始める前に

開始する前に、DB2 ロードー JDBC ドライバと DB2 クライアントを Secure Agent マシンにインストールして、DB2 ロードー接続を確立する必要があります。

設定の前提条件の詳細については、「[「前提条件」 \(ページ 250\)](#)」を参照してください。

接続の詳細

次の表に、基本接続プロパティを示します。

財産	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。

財産	説明
シークレット コンテナの使用	<p>組織に対して設定されている Secrets Manager にこの接続の機密資格情報を保存します。このプロパティは、組織に Secrets Manager が設定されている場合にのみ表示されます。このプロパティは、データ取り込みおよびレプリケーションとデータアクセス管理サービスではサポートされていません。</p> <p>接続でシークレットコンテナを有効にすると、Secure Agent が Secrets Manager からどの資格情報を取得するかを選択できます。このオプションを無効にした場合、資格情報は組織の設定方法に応じてリポジトリまたはローカル Secure Agent に保存されます。</p> <p>注: この接続を使用してプッシュダウンまたはプロキシサービスを介してデータアクセスポリシーを適用する場合、シークレットコンテナ設定オプションを使用することはできません。</p> <p>Secrets Manager を設定および使用方法については、Administrator のヘルプにある「Secrets Manager の設定」を参照してください。</p>
ランタイム環境	<p>タスクを実行するランタイム環境の名前。</p> <p>Secure Agent を選択します。</p>
ホスト名	DB2 データベースサーバをホストするマシンの名前。
データベース名	DB2 データベースの名前。
ポート番号	<p>DB2 データベースサーバーに接続するためのポート番号。</p> <p>デフォルトは 50000 です。</p>
スキーマ名	<p>メタデータを取得するための DB2 データベースサーバー内のスキーマ名。</p> <p>このプロパティは、DB2 ローダー接続を設定する場合には適用されません。</p>
ユーザー名	DB2 アカウントに接続するためのユーザー名。
パスワード	DB2 アカウントに接続するためのパスワード。
接続文字列	DB2 データベースに接続するためのエイリアス名。

詳細設定

次の表に、詳細接続のプロパティを示します。

プロパティ	説明
暗号化方法	Secure Agent とデータベースサーバー間で交換されるデータを暗号化します。 リストから次のいずれかの暗号化方法を選択します。 - 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。 - 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。 デフォルトは [暗号化なし] です。
サーバー証明書の検証	Secure Agent がデータベースサーバーから送信された証明書を検証するかどうかを指定します。 このプロパティは、暗号化方法に [SSL] を選択した場合にのみ表示されます。 リストから次のいずれかのオプションを選択します。 - False。Secure Agent は証明書を検証しません。 - True。Secure Agent は証明書を検証します。 デフォルトは False です。
トラストストア	DB2 に接続するための SSL 証明書を含むトラストストアファイルのパスとファイル名。 このプロパティは、暗号化方法に [SSL] を選択し、サーバー証明書に [True] を選択して検証した場合にのみ表示されます。 ディレクトリとファイル名を次の形式で指定します。 /root/<フォルダ名>/<トラストストアファイル名>.p12
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にアクセスするためのパスワード。 このプロパティは、暗号化方法に [SSL] を選択し、サーバー証明書に [True] を選択して検証した場合にのみ表示されます。
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名前。 このプロパティは、暗号化方法に [SSL] を選択し、サーバー証明書に [True] を選択して検証した場合にのみ表示されます。 Secure Agent は、このプロパティで指定したホスト名を SSL 証明書内のホスト名と照合して検証します。
認証方法	ドライバが接続を確立するために使用する認証方法。 リストから次のいずれかの認証方法を選択します。 - クリアテキスト。認証用にクリアテキストのユーザー ID とパスワードを DB2 サーバーに送信します。 - 暗号化パスワード。認証用にクリアテキストのユーザー ID と暗号化されたパスワードを DB2 サーバーに送信します。 デフォルトは [クリアテキスト] です。
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。 デフォルトでは無効になっています。
リカバリ可能	バックアップ保留中状態の DB2 テーブルスペースを設定します。 [リカバリ可能] オプションを有効にしてマッピングを実行する前に、データベースを完全にバックアップして、テーブルスペースで他の操作を実行する必要があります。 デフォルトでは有効になっています。

プロパティ	説明
DB2 サーバーの場所	<p>DB2 データベースサーバーの場所。</p> <p>リストから次の場所のいずれかを選択します。</p> <ul style="list-style-type: none"> - リモート。DB2 データベースサーバーは別のマシン上にあります。 - ローカル。DB2 データベースサーバーは、Secure Agent マシン上にあります。 <p>デフォルトは [リモート] です。</p>
外部ローダー実行可能	<p>DB2 外部ローダーの実行可能ファイル名。</p> <p>Secure Agent は、IBM データサーバクライアントバージョン 9.5 以降の DB2 外部ローダー実行可能ファイルを使用します。</p> <p>デフォルトは db2load です。</p>
操作モード	<p>DB2 外部ローダーが実行する操作。</p> <p>次のいずれかの操作モードを選択して、DB2 外部ローダーで選択したモードに基づいて、DB2 外部ローダーがターゲットテーブルにデータの書き込みを行う方法を指定します。</p> <ul style="list-style-type: none"> - 挿入。テーブルにデータをロードします。 - 置換。テーブルの既存のデータを削除してから、テーブルにデータを追加します。 - 再起動。以前に中断されたロード操作を再開します。 - 終了。以前に中断されたロード操作を中止して、（整合点を超えている場合でも）操作を開始時点までロールバックします。 <p>デフォルト値は [挿入] です。</p>
追加メタデータ接続プロパティ	<p>ドライバに渡す追加のメタデータ接続プロパティ。複数のプロパティを指定する場合は、キーと値のペアをそれぞれセミコロンで区切ります。</p> <p>例: <パラメータ名 1>=<値 1>; <パラメータ名 2>=<値 2></p>

第 66 章

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。

重要: Db2 Warehouse on Cloud コネクタは廃止され、メンテナンスモードに移行されました。Informatica は将来のリリースでサポートを廃止する予定です。

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
Connection 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。
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、ホステッドエージェント、サーバーレスランタイム環境、またはエラスティックランタイム環境を指定します。 ランタイム環境の設定および使用方法の詳細については、Administrator のヘルプにある「ランタイム環境」を参照してください。
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。

接続プロパティ	説明
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。

第 67 章

Denode 接続のプロパティ

Denode 接続を設定するには、接続プロパティを設定する必要があります。

Denodo への接続

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

始める前に

接続を設定するには、その前に、Denodo アカウントのホスト名、ポート番号、データベース名、ユーザー名、およびパスワードを取得する必要があります。

接続の詳細

次の表に、Denodo 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。
シークレットコンテナの使用	組織に対して設定されている Secrets Manager にこの接続の機密資格情報を保存します。 このプロパティは、組織に Secrets Manager が設定されている場合にのみ表示されます。 このプロパティは、データ取り込みおよびレプリケーションとデータアクセス管理サービスではサポートされていません。 接続でシークレットコンテナを有効にすると、Secure Agent が Secrets Manager からどの資格情報を取得するかを選択できます。このオプションを無効にした場合、資格情報は組織の設定方法に応じてリポジトリまたはローカル Secure Agent に保存されます。 注: この接続を使用してプッシュダウンまたはプロキシサービスを介してデータアクセスポリシーを適用する場合、シークレットコンテナ設定オプションを使用することはできません。 Secrets Manager を設定および使用する方法については、Administrator のヘルプにある「Secrets Manager の設定」を参照してください。

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。Secure 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	Denodo データベースをホストするマシンのホスト名または IP アドレス。
ポート	Denodo データベース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 9999 で、JDBC 接続用です。
データベース	Denodo データベース名。
ユーザー名	Denodo データベースに接続するためのユーザー名。
[パスワード]	ユーザー名のパスワード

第 68 章

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。
シークレットコンテナの使用	<p>組織に対して設定されている Secrets Manager にこの接続の機密資格情報を保存します。</p> <p>このプロパティは、組織に Secrets Manager が設定されている場合にのみ表示されます。</p> <p>このプロパティは、データ取り込みおよびレプリケーションとデータアクセス管理サービスではサポートされていません。</p> <p>接続でシークレットコンテナを有効にすると、Secure Agent が Secrets Manager からどの資格情報を取得するかを選択できます。このオプションを無効にした場合、資格情報は組織の設定方法に応じてリポジトリまたはローカル Secure Agent に保存されます。</p> <p>注: この接続を使用してプッシュダウンまたはプロキシサービスを介してデータアクセスポリシーを適用する場合、シークレットコンテナ設定オプションを使用することはできません。</p> <p>Secrets Manager を設定および使用する方法については、Administrator のヘルプにある「Secrets Manager の設定」を参照してください。</p>
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。
UpdateMode	<p>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。</p> <ul style="list-style-type: none">- 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。

第 69 章

Dropbox 接続のプロパティ

Dropbox 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。

重要: Dropbox コネクタは非推奨となり、メンテナンスモードに移行されました。Informatica は将来のリリースでサポートを廃止する予定です。

次の表に、Dropbox 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。
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。
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	システムがエージェントをホストするかどうかを指定します。
承認コード	<ul style="list-style-type: none">- 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。

InfalclQa ▼



[Developer home](#)

[App Console](#)

[Drop-ins](#)

[Datastore API](#)

[Sync API](#)

[Core API](#)

[Developer guide](#)

[Branding guide](#)

[Blog](#)

[Support](#)

InfalclQa

Settings

Details

Status Development

Apply for production

Development users Only you

Enable additional users

Permission type Full Dropbox ⓘ

App key	qgij4uo7ytew6b7
App secret	rtms1n649b7pmcp

OAuth 2

Redirect URIs

http://localhost:4000

×

https:// (http allowed for localhost)

Add

第 70 章

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。
シークレットコンテナの使用	組織に対して設定されている Secrets Manager にこの接続の機密資格情報を保存します。 このプロパティは、組織に Secrets Manager が設定されている場合にのみ表示されます。 このプロパティは、データ取り込みおよびレプリケーションとデータアクセス管理サービスではサポートされていません。 接続でシークレットコンテナを有効にすると、Secure Agent が Secrets Manager からどの資格情報を取得するかを選択できます。このオプションを無効にした場合、資格情報は組織の設定方法に応じてリポジトリまたはローカル Secure Agent に保存されます。 注: この接続を使用してプッシュダウンまたはプロキシサービスを介してデータアクセスポリシーを適用する場合、シークレットコンテナ設定オプションを使用することはできません。 Secrets Manager を設定および使用する方法については、Administrator のヘルプにある「Secrets Manager の設定」を参照してください。
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。 Secure Agent、またはサーバーレスランタイム環境を選択します。 ランタイム環境の設定および使用方法の詳細については、Administrator のヘルプにある「ランタイム環境」を参照してください。
ホスト	Elasticsearch サーバーのホスト名または IP アドレスです。

プロパティ	説明
ポート	Elasticsearch サーバーのポート番号。デフォルトは 9243 です。
認証	Elasticsearch リソースにアクセスするための認証方法です。 基本認証で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。
ユーザー名	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	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。

第 71 章

Eloqua Bulk API 接続のプロパティ

Eloqua Bulk API 接続を作成して、Eloqua Bulk API からのデータの読み取りや Eloqua Bulk API へのデータの書き込みを行います。Eloqua Bulk API 接続は、マッピングおよびマッピングタスクで使用できます。Eloqua Bulk API 接続を使用すると、マッピングおよびマッピングタスクでソースおよびターゲットを指定できます。

Eloqua への接続

Eloqua に接続するように Eloqua Bulk API の接続プロパティを設定してみましょう。

始める前に

接続プロパティを設定する前に、Oracle Eloqua アカウントから情報を取得する必要があります。Oracle Eloqua にアクセスするための基本認証タイプと OAuth 認証タイプを設定できます。

基本認証を使用するには、Oracle Eloqua ベース URL、ドメイン名、ユーザー名およびパスワードが必要です。

OAuth 認証を使用するには、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が追加が必要です。

これらの詳細を生成する方法の詳細については、「[Oracle Eloqua documentation](#)」を参照してください。

次のビデオでは、必要な情報の入手先を確認することができます。



接続の詳細

次の表に、基本接続プロパティを示します。

プロパティ	説明
接続名	接続の名前。 各接続名は組織内で一意である必要があります。接続名には、英数字、スペース、および次の特殊文字を含めることができます。_ . + , 最大長は 255 文字です。
説明	接続の説明。最大長は 4000 文字です。
シークレット コンテナの使用	組織に対して設定されている Secrets Manager にこの接続の機密資格情報を保存します。 このプロパティは、組織に Secrets Manager が設定されている場合にのみ表示されます。 このプロパティは、データ取り込みおよびレプリケーションとデータアクセス管理サービスではサポートされていません。 接続でシークレットコンテナを有効にすると、Secure Agent が Secrets Manager からどの資格情報を取得するかを選択できます。このオプションを無効にした場合、資格情報は組織の設定方法に応じてリポジトリまたはローカル Secure Agent に保存されます。 注: この接続を使用してプッシュダウンまたはプロキシサービスを介してデータアクセスポリシーを適用する場合、シークレットコンテナ設定オプションを使用することはできません。 Secrets Manager を設定および使用方法については、Administrator のヘルプにある「Secrets Manager の設定」を参照してください。
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。 Secure Agent、ホステッドエージェント、またはサーバーレスランタイム環境を選択します。
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 と入力することができます。 https://<host>.eloqua.com/api/bulk/2.0 という 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 の詳細については、「 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。

詳細設定

次の表に、詳細接続のプロパティを示します。

プロパティ	説明
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。 詳細については、「 タイムゾーンのオフセットについて 」 (ページ 273)を参照してください。
デバッグロガー を有効にする	デバッグロガーによって SOAP 要求と応答をセッションログに登録するかどうかを指定します。 接続でデバッグロガーを有効にしてタスクを実行すると、読み取り操作のセッションログで応答のみを表示することができますが、要求を表示することはできません。書き込み操作の場合、要求はセッションログに表示されますが、応答はセッションログには表示されません。 デフォルトでは有効になっています。
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り得します。 デフォルトでは有効になっています。
アクティビティ またはカスタム フィールド設定	Eloqua のアクティビティオブジェクトと、Eloqua の連絡先オブジェクトおよびアカウントオブジェクトのカスタムフィールドのうち、読み取りまたは書き込みを行うもの。 このフィールドに入力されたメタデータを使用して、アクティビティオブジェクト、および連絡先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に対して読み取りまたは書き込みを行うことができます。他のフィールドまたはメタデータを含める場合は、匿名ルート構造から始まる JSON 形式で追加してください。 例: { "address": { "city": "city name", "state": "state name", }} 詳細については、「 「アクティビティまたはカスタムフィールド設定」 (ページ 266)」を参照してください。 フィールド API に含まれないカスタムオブジェクトにフィールドを含める方法の詳細については、「 カスタムオブジェクトへの、フィールド API の一部ではないフィールドの追加 」 (ページ 267)のトピックを参照してください。

アクティビティまたはカスタムフィールド設定

アクティビティオブジェクト、および連絡先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に対して読み取りまたは書き込みを行うことができます。

Eloqua Bulk 接続プロパティの【**アクティビティまたはカスタムフィールド設定**】プロパティにメタデータ情報を JSON 形式で追加します。アクティビティオブジェクトとカスタムフィールドの仕様には、次のようなセクションが含まれています。

アクティビティ

すべてのアクティビティが名前と値のペアとして一覧で表示されます（値はフィールド名の配列です）。

例:

```
{ "EmailAddress", "johns@gmail.com" },  
{ "FirstName", "Johns" }
```

ActivityItem

フィールドの配列を定義します。各フィールドには、次のような名前と値のペアがあります。

- **name:** フィールドの名前。フィールド名は、[アクティビティ] セクションに入力するフィールド名と同じである必要があります。
- **internalName:** フィールドラベルの名前。名前と一意の名前が表示されます。
- **datatype:** フィールドのデータ型。デフォルトの値は文字列データ型です。アクティビティフィールドまたはユーザー設定フィールドは、次のデータ型をサポートしています。
 - 数値または整数
 - 日付またはタイムスタンプ
 - 文字列
- **maxLength:** データ型フィールドの最大長または精度。
- **hasReadOnlyConstraint:** フィールドが読み取り専用かどうかを示します。
- **hasNotNullConstraint:** フィールドが必須かどうかを示します。
- **hasUniquenessConstraint:** フィールドがキーであるかどうかを示します。
- **statement:** Eloqua REST 要求で使用される文。

ContactItem

[連絡先] ユーザー設定フィールドの配列を定義します。各フィールドには、[ActivityItem] セクションの名前と値のペアがあります。

AccountItem

[アカウント] ユーザー設定フィールドの配列を定義します。各フィールドには、[ActivityItem] セクションの名前と値のペアがあります。

カスタムオブジェクトへの、フィールド API の一部ではないフィールドの追加

標準フィールドに含まれていないフィールドをカスタムオブジェクトに追加するには、次の手順を実行します。

1. Eloqua Bulk 接続を編集します。
2. **[アクティビティまたはカスタムフィールド設定]** 接続属性で、接続属性で使用可能な JSON テンプレートに次の JSON 要素を追加します:

```
"CustomObjects" : {  
  "CO_CustomObject1": ["MappedEntityId", "UniqueId"],  
  "CO_CustomObject2": ["MappedEntityId", "UniqueId"]  
}
```

ここで、CO_CustomObject1 と CO_CustomObject2 はカスタムオブジェクトの名前で、MappedEntityId と UniqueId はフィールドです。

3. 次に、次のフィールドの詳細を JSON テンプレートに追加します:

これらの詳細は、前の手順で追加した CustomObjects 要素で定義したフィールドの詳細です。

```
"CustomItem": [  
  {  
    "name": "MappedEntityId",  
    "internalName": "MappedEntityId",
```

```

        "dataType": "integer",
        "hasReadOnlyConstraint": true,
        "hasNotNullConstraint": false,
        "hasUniquenessConstraint": true,
        "statement": "{{CustomObject[id].MappedEntityId}}"
    },
    {
        "name": "UniqueId",
        "internalName": "UniqueId",
        "dataType": "integer",
        "hasReadOnlyConstraint": true,
        "hasNotNullConstraint": false,
        "hasUniquenessConstraint": true,
        "statement": "{{CustomObject[id].UniqueId}}"
    }
]

```

上記の詳細を追加した後に、JSON 構造が有効であることを確認します。

4. **【テスト接続】** をクリックします。

5. **【保存】** をクリックします。

新しいマッピングで接続を使用すると、JSON テンプレートで定義したフィールドがマッピングに表示されます。以前のリリースから引き継いだ既存のマッピングについては、フィールドマッピングを更新してターゲットにマッピングする必要があります。

6. 既存のマッピングについては、前述の定義済みのフィールドが必要な場合、フィールドマッピングを更新し、ターゲットにマッピングします。

次の例に、[アクティビティまたはカスタムフィールド設定] のサンプルを示します。

```

{
  "Activities": {
    "EmailOpen": ["ActivityId", "ActivityType", "ActivityDate", "EmailAddress", "ContactId",
    "IpAddress", "VisitorId", "EmailRecipientId", "AssetType", "AssetName", "AssetId", "SubjectLine",
    "EmailWebLink", "VisitorExternalId", "CampaignId", "ExternalId", "DeploymentId", "EmailSendType"],
    "EmailClickthrough": ["ActivityId", "ActivityType", "ActivityDate", "EmailAddress", "ContactId",
    "IpAddress", "VisitorId", "EmailRecipientId", "AssetType", "AssetName", "AssetId", "SubjectLine",
    "EmailWebLink", "EmailClickedThruLink", "VisitorExternalId", "CampaignId", "ExternalId", "DeploymentId",
    "EmailSendType"],
    "EmailSend": ["ActivityId", "ActivityType", "ActivityDate", "EmailAddress", "ContactId",
    "EmailRecipientId", "AssetType", "AssetId", "AssetName", "SubjectLine", "EmailWebLink", "CampaignId",
    "ExternalId", "DeploymentId", "EmailSendType"],
    "Subscribe": ["ActivityId", "ActivityType", "AssetId", "ActivityDate", "EmailAddress",
    "EmailRecipientId", "AssetType", "AssetName", "CampaignId", "ExternalId"],
    "Unsubscribe": ["ActivityId", "ActivityType", "AssetId", "ActivityDate", "EmailAddress",
    "EmailRecipientId", "AssetType", "AssetName", "CampaignId", "ExternalId"],
    "Bounceback": ["ActivityId", "ActivityType", "AssetId", "ActivityDate", "EmailAddress",
    "AssetType", "AssetName", "CampaignId", "ExternalId"],
    "WebVisit": ["ActivityId", "ActivityType", "ActivityDate", "ContactId", "VisitorId",
    "VisitorExternalId", "ReferrerUrl", "IpAddress", "NumberOfPages", "FirstPageViewUrl", "Duration",
    "ExternalId"],
    "PageView": ["ActivityId", "ActivityType", "ActivityDate", "ContactId", "CampaignId",
    "VisitorId", "VisitorExternalId", "WebVisitId", "Url", "ReferrerUrl", "IpAddress",
    "IsWebTrackingOptedIn", "ExternalId"],
    "FormSubmit": ["ActivityId", "ActivityType", "ActivityDate", "ContactId", "VisitorId",
    "VisitorExternalId", "AssetType", "AssetId", "AssetName", "RawData", "CampaignId", "ExternalId"]
  },
  "CustomObjects": {
    "CO_CustomObject1": ["MappedEntityId", "UniqueId"],
    "CO_CustomObject2": ["MappedEntityId", "UniqueId"]
  },
  "ActivityItem": [{
    "name": "ActivityId",
    "internalName": "ActivityId",
    "dataType": "integer",
    "hasReadOnlyConstraint": true,
    "hasNotNullConstraint": false,
    "hasUniquenessConstraint": true,

```



```

        "statement": "{{Activity.Id}}"
    },
    {
        "name": "ActivityType",
        "internalName": "ActivityType",
        "dataType": "string",
        "maxLength": 100,
        "hasReadOnlyConstraint": false,
        "hasNotNullConstraint": false,
        "hasUniquenessConstraint": false,
        "statement": "{{Activity.Type}}"
    },
    {
        "name": "ActivityDate",
        "internalName": "ActivityDate",
        "dataType": "date",
        "hasReadOnlyConstraint": true,
        "hasNotNullConstraint": false,
        "hasUniquenessConstraint": false,
        "statement": "{{Activity.CreatedAt}}"
    },
    {
        "name": "EmailAddress",
        "internalName": "EmailAddress",
        "dataType": "emailAddress",
        "maxLength": 400,
        "hasReadOnlyConstraint": false,
        "hasNotNullConstraint": false,
        "hasUniquenessConstraint": false,
        "statement": "{{Activity.Field(EmailAddress)}}"
    },
    {
        "name": "ContactId",
        "internalName": "ContactId",
        "dataType": "integer",
        "hasReadOnlyConstraint": false,
        "hasNotNullConstraint": false,
        "hasUniquenessConstraint": false,
        "statement": "{{Activity.Contact.Id}}"
    },
    {
        "name": "IpAddress",
        "internalName": "IpAddress",
        "dataType": "string",
        "maxLength": 50,
        "hasReadOnlyConstraint": false,
        "hasNotNullConstraint": false,
        "hasUniquenessConstraint": false,
        "statement": "{{Activity.Field(IpAddress)}}"
    },
    {
        "name": "VisitorId",
        "internalName": "VisitorId",
        "dataType": "integer",
        "hasReadOnlyConstraint": false,
        "hasNotNullConstraint": false,
        "hasUniquenessConstraint": false,
        "statement": "{{Activity.Visitor.Id}}"
    },
    {
        "name": "EmailRecipientId",
        "internalName": "EmailRecipientId",
        "dataType": "string",
        "maxLength": 38,
        "hasReadOnlyConstraint": false,
        "hasNotNullConstraint": false,
        "hasUniquenessConstraint": false,
        "statement": "{{Activity.Field(EmailRecipientId)}}"
    },

```

```

{
  "name": "AssetType",
  "internalName": "AssetType",
  "dataType": "string",
  "maxLength": 100,
  "hasReadOnlyConstraint": false,
  "hasNotNullConstraint": false,
  "hasUniquenessConstraint": false,
  "statement": "{{Activity.Asset.Type}}"
},
{
  "name": "AssetName",
  "internalName": "AssetName",
  "dataType": "string",
  "maxLength": 100,
  "hasReadOnlyConstraint": false,
  "hasNotNullConstraint": false,
  "hasUniquenessConstraint": false,
  "statement": "{{Activity.Asset.Name}}"
},
{
  "name": "AssetId",
  "internalName": "AssetId",
  "dataType": "integer",
  "hasReadOnlyConstraint": false,
  "hasNotNullConstraint": false,
  "hasUniquenessConstraint": false,
  "statement": "{{Activity.Asset.Id}}"
},
{
  "name": "SubjectLine",
  "internalName": "SubjectLine",
  "dataType": "string",
  "maxLength": 500,
  "hasReadOnlyConstraint": false,
  "hasNotNullConstraint": false,
  "hasUniquenessConstraint": false,
  "statement": "{{Activity.Field(SubjectLine) }}"
},
{
  "name": "EmailWebLink",
  "internalName": "EmailWebLink",
  "dataType": "string",
  "maxLength": 8192,
  "hasReadOnlyConstraint": false,
  "hasNotNullConstraint": false,
  "hasUniquenessConstraint": false,
  "statement": "{{Activity.Field(EmailWebLink) }}"
},
{
  "name": "VisitorExternalId",
  "internalName": "VisitorExternalId",
  "dataType": "string",
  "maxLength": 38,
  "hasReadOnlyConstraint": false,
  "hasNotNullConstraint": false,
  "hasUniquenessConstraint": false,
  "statement": "{{Activity.Visitor.ExternalId }}"
},
{
  "name": "CampaignId",
  "internalName": "CampaignId",
  "dataType": "integer",
  "hasReadOnlyConstraint": false,
  "hasNotNullConstraint": false,
  "hasUniquenessConstraint": false,
  "statement": "{{Activity.Campaign.Id }}"
},
{

```

```

        "name": "ExternalId",
        "internalName": "ExternalId",
        "dataType": "string",
        "maxLength": 20,
        "hasReadOnlyConstraint": false,
        "hasNotNullConstraint": false,
        "hasUniquenessConstraint": false,
        "statement": "{{Activity.ExternalId}}"
    },
    {
        "name": "DeploymentId",
        "internalName": "DeploymentId",
        "dataType": "integer",
        "hasReadOnlyConstraint": false,
        "hasNotNullConstraint": false,
        "hasUniquenessConstraint": false,
        "statement": "{{Activity.Field(EmailDeploymentId)}}"
    },
    {
        "name": "EmailSendType",
        "internalName": "EmailSendType",
        "dataType": "string",
        "maxLength": 100,
        "hasReadOnlyConstraint": false,
        "hasNotNullConstraint": false,
        "hasUniquenessConstraint": false,
        "statement": "{{Activity.Field(EmailSendType)}}"
    },
    {
        "name": "EmailClickedThruLink",
        "internalName": "EmailClickedThruLink",
        "dataType": "string",
        "maxLength": 8192,
        "hasReadOnlyConstraint": false,
        "hasNotNullConstraint": false,
        "hasUniquenessConstraint": false,
        "statement": "{{Activity.Field(EmailClickedThruLink)}}"
    },
    {
        "name": "RawData",
        "internalName": "RawData",
        "dataType": "string",
        "maxLength": 64000,
        "hasReadOnlyConstraint": false,
        "hasNotNullConstraint": false,
        "hasUniquenessConstraint": false,
        "statement": "{{Activity.Field(RawData)}}"
    },
    {
        "name": "ReferrerUrl",
        "internalName": "ReferrerUrl",
        "dataType": "string",
        "maxLength": 8192,
        "hasReadOnlyConstraint": false,
        "hasNotNullConstraint": false,
        "hasUniquenessConstraint": false,
        "statement": "{{Activity.Field(ReferrerUrl)}}"
    },
    {
        "name": "WebVisitId",
        "internalName": "WebVisitId",
        "dataType": "integer",
        "hasReadOnlyConstraint": false,
        "hasNotNullConstraint": false,
        "hasUniquenessConstraint": false,
        "statement": "{{Activity.Field(WebVisitId)}}"
    },
    {
        "name": "Url",

```

```

        "internalName": "Url",
        "dataType": "string",
        "maxLength": 8192,
        "hasReadOnlyConstraint": false,
        "hasNotNullConstraint": false,
        "hasUniquenessConstraint": false,
        "statement": "{{Activity.Field(Url)}}"
    },
    {
        "name": "IsWebTrackingOptedIn",
        "internalName": "IsWebTrackingOptedIn",
        "dataType": "boolean",
        "hasReadOnlyConstraint": false,
        "hasNotNullConstraint": false,
        "hasUniquenessConstraint": false,
        "statement": "{{Activity.Field(IsWebTrackingOptedIn)}}"
    },
    {
        "name": "NumberOfPages",
        "internalName": "NumberOfPages",
        "dataType": "integer",
        "hasReadOnlyConstraint": false,
        "hasNotNullConstraint": false,
        "hasUniquenessConstraint": false,
        "statement": "{{Activity.Field(NumberOfPages)}}"
    },
    {
        "name": "FirstPageViewUrl",
        "internalName": "FirstPageViewUrl",
        "dataType": "string",
        "maxLength": 8192,
        "hasReadOnlyConstraint": false,
        "hasNotNullConstraint": false,
        "hasUniquenessConstraint": false,
        "statement": "{{Activity.Field(FirstPageViewUrl)}}"
    },
    {
        "name": "Duration",
        "internalName": "Duration",
        "dataType": "string",
        "maxLength": 100,
        "hasReadOnlyConstraint": false,
        "hasNotNullConstraint": false,
        "hasUniquenessConstraint": false,
        "statement": "{{Activity.Field(Duration)}}"
    }
},
"ContactItem": [{
    "name": "ContactId",
    "internalName": "ContactId",
    "dataType": "integer",
    "hasReadOnlyConstraint": true,
    "hasNotNullConstraint": false,
    "hasUniquenessConstraint": true,
    "statement": "{{Contact.Id}}"
}],
"AccountItem": [],
"CustomItem": [{
    "name": "MappedEntityId",
    "internalName": "MappedEntityId",
    "dataType": "integer",
    "hasReadOnlyConstraint": true,
    "hasNotNullConstraint": false,
    "hasUniquenessConstraint": true,
    "statement": "{{CustomObject[id].MappedEntityId}}"
}],
{
    "name": "UniqueId",
    "internalName": "UniqueId",

```

```

      "dataType": "integer",
      "hasReadOnlyConstraint": true,
      "hasNotNullConstraint": false,
      "hasUniquenessConstraint": true,
      "statement": "{{CustomObject[id].UniqueId}}"
    }
  ]
}

```

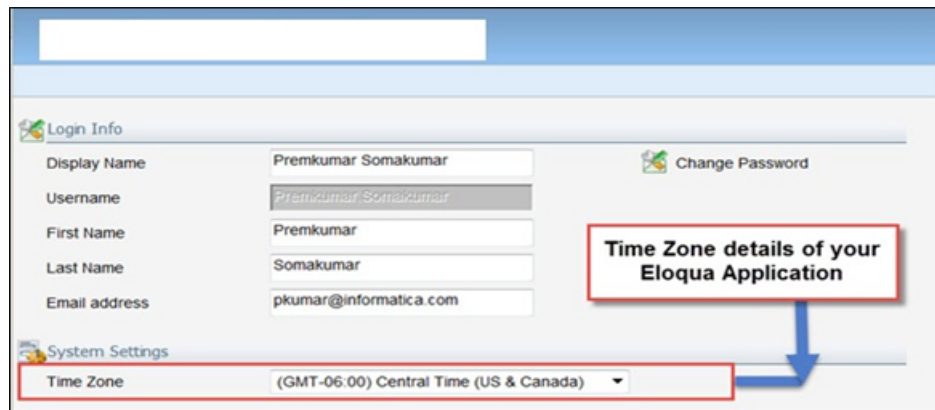
タイムゾーンのオフセットについて

Eloqua Bulk API 接続で設定されたタイムゾーンは、Eloqua アプリケーションのタイムゾーンと同期している必要があります。

次のタスクを実行して、Eloqua アプリケーションのタイムゾーンを設定します：

1. Eloqua アプリケーションアカウントにログインします。
2. **【設定】** をクリックします。
3. **【設定】** を選択します。
[設定] ページが表示されます。
4. **【エージェント設定の編集】** をクリックし、該当するタイムゾーンを入力します。

次の画像は、Eloqua で設定されたタイムゾーンの例を示しています。



例えば、Eloqua アプリケーションのタイムゾーンが GMT+06:00 である場合、このフィールドには+06:00 と入力する必要があります。

夏時間が有効になっている場合は、時刻を調整します。例えば、タイムゾーンが GMT-06:00 である場合、このフィールドには-06:00 と入力します。

プロキシサーバーの設定

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

Windows および Linux でプロキシサーバーを使用するように Secure Agent を設定できます。認証されていないプロキシサーバーまたは認証されたプロキシサーバーを使用できます。プロキシ設定は、マッピングおよび詳細モードのマッピングで使用される接続に適用されます。

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

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

手順については、データ統合のヘルプの『または「Windows でのプロキシ設定」または「Linux でのプロキシ設定」を参照してください。

- Secure Agent のプロパティで、DTM の JVM オプションを設定します。手順については、ナレッジベースの記事「[Proxy server settings](#)」を参照してください。

サーバーレスランタイム環境のプロキシの設定を行う方法については、Administrator ヘルプの「「プロキシサーバーの使用」を参照してください。

第 72 章

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
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。
シークレットコンテナの使用	組織に対して設定されている Secrets Manager にこの接続の機密資格情報を保存します。 このプロパティは、組織に Secrets Manager が設定されている場合にのみ表示されます。 このプロパティは、データ取り込みおよびレプリケーションとデータアクセス管理サービスではサポートされていません。 接続でシークレットコンテナを有効にすると、Secure Agent が Secrets Manager からどの資格情報を取得するかを選択できます。このオプションを無効にした場合、資格情報は組織の設定方法に応じてリポジトリまたはローカル Secure Agent に保存されます。 注: この接続を使用してプッシュダウンまたはプロキシサービスを介してデータアクセスポリシーを適用する場合、シークレットコンテナ設定オプションを使用することはできません。 Secrets Manager を設定および使用方法については、Administrator のヘルプにある「Secrets Manager の設定」を参照してください。
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。 Secure Agent 環境またはエラスティックランタイム環境を選択します。 ランタイム環境の設定および使用方法の詳細については、Administrator のヘルプにある「ランタイム環境」を参照してください。
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: <code>https://rest.apisandbox.eloqua.com</code>
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。

プロパティ	説明
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。

第 73 章

FHIR 接続プロパティ

FHIR（Fast Healthcare Interoperability Resources）サーバーとの間で読み取りと書き込みを行う FHIR 接続を作成します。

FHIR 接続

FHIR サーバーに接続するように FHIR の接続プロパティを設定してみましょう。

接続の詳細

次の表に、基本接続プロパティを示します。

プロパティ	説明
接続名	接続の名前。 各接続名は組織内で一意である必要があります。接続名には、英数字、スペース、および次の特殊文字を含めることができます。_ + -, 最大長は 255 文字です。
説明	接続の説明。最大長は 4000 文字です。
シークレットコンテナの使用	組織に対して設定されている Secrets Manager にこの接続の機密資格情報を保存します。 このプロパティは、組織に Secrets Manager が設定されている場合にのみ表示されます。 このプロパティは、データ取り込みおよびレプリケーションとデータアクセス管理サービスではサポートされていません。 接続でシークレットコンテナを有効にすると、Secure Agent が Secrets Manager からどの資格情報を取得するかを選択できます。このオプションを無効にした場合、資格情報は組織の設定方法に応じてリポジトリまたはローカル Secure Agent に保存されます。 注: この接続を使用してプッシュダウンまたはプロキシサービスを介してデータアクセスポリシーを適用する場合、シークレットコンテナ設定オプションを使用することはできません。 Secrets Manager を設定および使用方法については、Administrator のヘルプにある「Secrets Manager の設定」を参照してください。
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。Secure Agent グループまたはホストされているエージェントを選択します。

プロパティ	説明
ホスト	FHIR サーバーのホスト名または IP アドレス（ポート番号を含む）。 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
HTTP メソッド	要求の送信に使用される HTTP メソッド。 次のいずれかの HTTP 方式を選択します。 - HTTP - HTTPS デフォルトは HTTP です。
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は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 30 秒です。
キープアライブ	複数の HTTP 要求または応答に対して接続を開いたままにするかどうかを示します。 デフォルトは true 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たどるかどうかを示します。 デフォルトは true です。
接続の再試行	接続に成功しなかった場合に、FHIR 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。 デフォルトは 0 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 回の接続を再試行する場合は、 【接続の再試行】 を 10 に設定し、 【接続再試行の間隔】 を 5 に設定します。 デフォルトは 0 です。
基本パス	FHIR サーバーの基本パス。API の最初の URL セグメント。
テスト接続のリソースパス	接続をテストするためにベースパスに追加するリソースパス。
コンテンツタイプ	要求のメディアタイプ。 次のいずれかのオプションを選択します。 - application/fhir+xml - application/fhir+json - application/xml - application/json
承認	応答のメディアタイプ。 次のいずれかのオプションを選択します。 - application/fhir+xml - application/fhir+json - application/xml - application/json

プロパティ	説明
追加のヘッダー	<p>接続に必要な追加のヘッダー。 ヘッダーを JSON 形式で定義します。例:</p> <pre>[{"Name": "Content-Type", "Value": "application/fhir+json"}, {"Name": "accept", "Value": "text/xml"}]</pre>
認証タイプ	<p>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。 次のいずれかのオプションを使用できます。</p> <ul style="list-style-type: none"> - なし - 基本。詳細については、「基本認証」 (ページ 280) を参照してください。 - OAuth 2.0 認証コード。詳細については、「OAuth 2.0 認証コード認証」 (ページ 280) を参照してください。 - OAuth 2.0 クライアント資格情報。詳細については、「OAuth 2.0 クライアント資格情報認証」 (ページ 281) を参照してください。 <p>デフォルトは [なし] です。</p>
トラストストアのファイルパス	<p>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。</p>
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。
キーストアのファイルパス	<p>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。</p>
キーストアのパスワード	安全な通信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	<p>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。</p> <ul style="list-style-type: none"> - 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したプロキシが考慮されます。 - カスタムプロキシ。接続レベルで設定したプロキシが考慮されます。 <p>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。</p>
プロキシ設定	<p>プロキシサーバーのホスト名または IP アドレス (ポート番号を含む)。 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</p>

認証タイプ

FHIR サーバーにアクセスする場合に、基本認証、OAuth 2.0 認証コード、OAuth 2.0 クライアント資格情報、または AWS 署名認証を設定することができます。

必要な認証方法を選択し、認証固有のパラメータを設定します。

基本認証

基本認証には、FHIR サーバーからのユーザー名とパスワードが必要です。

次の表に、標準認証の基本的な接続プロパティとその説明を示します。

プロパティ	説明
認証ユーザー ID	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名。
認証パスワード	ユーザ名に関連付けられているパスワード。

OAuth 2.0 認証コード認証

OAuth 2.0 認証コードを使用するように FHIR 接続の認証プロパティを設定します。

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 を登録します。

`https://<Informatica cloud hosting facility for your organization>/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、または 403 を受け取った場合、Informatica リダイレクト URL はエンドポイントに接続して新しいアクセストークンを取得するよう試みます。Informatica リダイレクト URL は通常、組織のファイアウォールの外側にあることに注意してください。

次の表では、OAuth 2.0 認証コードを使用する FHIR 接続の認証プロパティについて説明します。

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。 例: <code>https://login.microsoftonline.com/<ID>/oauth2/authorize</code>
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。 例: <code>https://login.microsoftonline.com/<ID>/oauth2/token</code>
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。スコープ属性はスペースで区切ります。 例: <code>root_readonly root_readwrite manage_app_users</code>
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。 パラメータを次の JSON 形式で定義します: <code>[{"Name": "resource", "Value": "https://<serverName>"}]</code> 例: <code>[{"Name": "resource", "Value": "https://fhirtest.fhir.azurehealthcareapis.com"}]</code>
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: <code>[{"Name": "max_age", "Value": 60}, {"Name": "state", "Value": "test"}]</code>
クライアント認証	認証のために要求本文または要求ヘッダーのいずれかでクライアント ID とクライアントシークレットを送信するオプションを選択します。 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。

プロパティ	説明
アクセストークン	アクセストークンの値を入力するか、 【アクセストークンの生成】 をクリックして、アクセストークンの値を指定します。 プロキシサーバー経由でアクセストークンを生成するには、Secure Agent 上で未認証のプロキシサーバーを構成します。FHIR 接続レベルのプロキシ構成は、アクセストークンの生成時には適用されません。
更新トークン	リフレッシュトークンの値を入力するか、 【アクセストークンの生成】 をクリックして、リフレッシュトークンの値を指定します。アクセストークンが有効でないか、有効期限切れの場合、Secure Agent は、リフレッシュトークンを使用して新しいアクセストークンを生成します。 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入力するか、 【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。

OAuth 2.0 クライアント資格情報認証

OAuth 2.0 クライアント資格情報を使用するように FHIR 接続の認証プロパティを設定します。

次の表では、OAuth 2.0 クライアント資格情報を使用する FHIR 接続の認証プロパティについて説明します。

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。スコープ属性はスペースで区切ります。 例: root_readonly root_readwrite manage_app_users
アクセストークンパラメータ	アクセストークン URL で使用する追加パラメータ。パラメータを JSON 形式で定義します。 例: [{"Name": "resource", "Value": "https://<serverName>"}]
クライアント認証	認証のために要求本文または要求ヘッダーのいずれかでクライアント ID とクライアントシークレットを送信するオプションを選択します。 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	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。 プロキシサーバー経由でアクセストークンを生成するには、Secure Agent 上で未認証のプロキシサーバーを構成します。FHIR 接続レベルのプロキシ構成は、アクセストークンの生成時には適用されません。

第 74 章

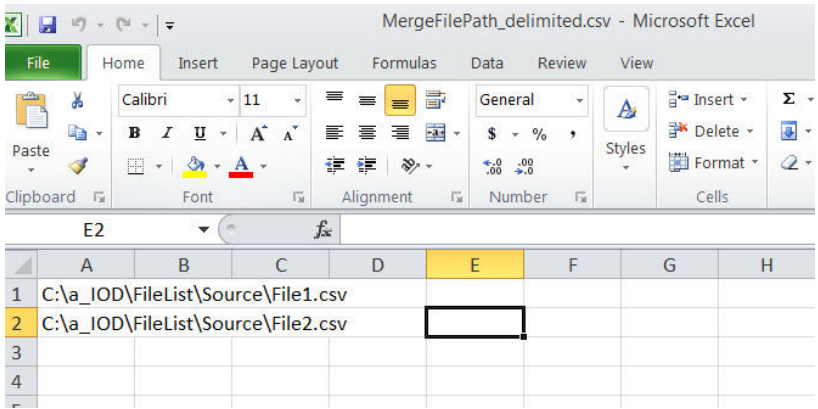
File List 接続のプロパティ

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。

重要: File List コネクタは非推奨となり、メンテナンスモードに移行されました。Informatica は将来のリリースでサポートを廃止する予定です。フラットファイルへのアクセスにはフラットファイルコネクタを使用することをお勧めします。

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。

接続プロパティ	説明
ファイルパスのマージ	<p>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。</p> <p>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。</p>  <p>The screenshot shows a Microsoft Excel spreadsheet titled 'MergeFilePath_delimited.csv'. The spreadsheet has columns A through H and rows 1 through 4. Row 1 contains the file path 'C:\a_IOD\FileList\Source\File1.csv' in column A. Row 2 contains the file path 'C:\a_IOD\FileList\Source\File2.csv' in column A. The cell in row 2, column E is highlighted with a black border.</p>
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。

第 75 章

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
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。
シークレットコンテナの使用	組織に対して設定されている Secrets Manager にこの接続の機密資格情報を保存します。 このプロパティは、組織に Secrets Manager が設定されている場合にのみ表示されます。 このプロパティは、データ取り込みおよびレプリケーションとデータアクセス管理サービスではサポートされていません。 接続でシークレットコンテナを有効にすると、Secure Agent が Secrets Manager からどの資格情報を取得するかを選択できます。このオプションを無効にした場合、資格情報は組織の設定方法に応じてリポジトリまたはローカル Secure Agent に保存されます。 注: この接続を使用してプッシュダウンまたはプロキシサービスを介してデータアクセスポリシーを適用する場合、シークレットコンテナ設定オプションを使用することはできません。 Secrets Manager を設定および使用方法については、Administrator のヘルプにある「Secrets Manager の設定」を参照してください。
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。 Secure Agent またはエラスティックランタイム環境を選択します。 ランタイム環境の設定および使用方法の詳細については、Administrator のヘルプにある「ランタイム環境」を参照してください。
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。

接続プロパティ	説明
ファイルパターン	<p>転送するファイルのパターン。</p> <p>例えば、日付パターンに基づいてファイルを選択するには、ファイルパターンフィールドで日付形式を DD/MM/YYYY、MM-dd-yyyy、yyyy-MM-dd、または yyyy-MM-d と指定できます。</p> <p>注: 【ファイルの選択】 接続プロパティで 【すべて】 を選択した場合、【ファイルパターン】 フィールドは適用されません。</p>
日数計算	<p>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。</p> <p>次の日付形式を指定できます: DD/MM/YYYY、MM-dd-yyyy、または yyyy-MM-d 形式。</p> <p>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、データフィルタを使用して LastModDate を 02/02/2016 と指定して、日数の計算を-1 と指定したとします。01/02/2016 までに変更されたファイルが選択されます。</p>
PassKey	<p>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。</p>

第 76 章

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。
シークレットコンテナの使用	<p>組織に対して設定されている Secrets Manager にこの接続の機密資格情報を保存します。このプロパティは、組織に Secrets Manager が設定されている場合にのみ表示されます。このプロパティは、データ取り込みおよびレプリケーションとデータアクセス管理サービスではサポートされていません。</p> <p>接続でシークレットコンテナを有効にすると、Secure Agent が Secrets Manager からどの資格情報を取得するかを選択できます。このオプションを無効にした場合、資格情報は組織の設定方法に応じてリポジトリまたはローカル Secure Agent に保存されます。</p> <p>注: この接続を使用してプッシュダウンまたはプロキシサービスを介してデータアクセスポリシーを適用する場合、シークレットコンテナ設定オプションを使用することはできません。</p> <p>Secrets Manager を設定および使用する方法については、Administrator のヘルプにある「Secrets Manager の設定」を参照してください。</p>
ランタイム環境	<p>タスクを実行するランタイム環境の名前。</p> <p>Secure Agent を選択します。</p> <p>ランタイム環境の設定および使用方法の詳細については、Administrator のヘルプにある「ランタイム環境」を参照してください。</p>
親ディレクトリ	<p>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。</p> <p>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。</p>
ファイルコンテンツを次の形式で処理	<p>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。</p> <ul style="list-style-type: none">- 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。

接続プロパティ	説明
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。

第 77 章

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。

データディスクが構成されているサーバーレスランタイム環境では、マウントされたディレクトリまたはそのサブディレクトリのいずれかを選択して、フラットファイル接続で使用できます。

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

フラットファイルソース接続に割り当てる必要があるプロパティを定義します。

次の表に、フラットファイル接続のプロパティを示します。

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

接続プロパティ	説明
シークレットコンテナの使用	<p>組織に対して設定されている Secrets Manager にこの接続の機密資格情報を保存します。このプロパティは、組織に Secrets Manager が設定されている場合にのみ表示されます。このプロパティは、データ取り込みおよびレプリケーションとデータアクセス管理サービスではサポートされていません。</p> <p>接続でシークレットコンテナを有効にすると、Secure Agent が Secrets Manager からどの資格情報を取得するかを選択できます。このオプションを無効にした場合、資格情報は組織の設定方法に応じてリポジトリまたはローカル Secure Agent に保存されます。</p> <p>注: この接続を使用してプッシュダウンまたはプロキシサービスを介してデータアクセスポリシーを適用する場合、シークレットコンテナ設定オプションを使用することはできません。</p> <p>Secrets Manager を設定および使用する方法については、Administrator のヘルプにある「Secrets Manager の設定」を参照してください。</p>
ランタイム環境	<p>フラットファイルへのアクセスに使用する Secure Agent が含まれるランタイム環境。セキュアエージェント、サーバーレスランタイム環境、またはエラスティックランタイム環境を選択します。</p> <p>サーバーレスランタイム環境に、フラットファイルが格納されているマウント済みの EFS ディレクトリまたは NFS ディレクトリが含まれていることを確認します。</p> <p>データベース取り込みとレプリケーションタスクには、Secure Agent を選択します。ホステッドエージェント、サーバーレスランタイム環境、またはエラスティックランタイム環境は使用できません。</p> <p>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。</p>

接続プロパティ	説明
ディレクトリ	<p>フラットファイルが格納されている選択したランタイム環境内のすべてのセキュアエージェントからアクセス可能なディレクトリ。</p> <p>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。</p> <p>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。</p> <p>このディレクトリは、サーバーレスランタイム環境用に設定されたデータディスクでも使用されます。</p> <p>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。</p> <p>/ \ : _ ~</p> <p>ディレクトリは、この接続タイプのサービス URL です。</p> <p>注: Windows では、【ディレクトリの参照】 ダイアログボックスにマッピング済みドライブは表示されません。Windows エクスプローラで 【マイネットワーク】 を参照してディレクトリを検索し、アドレスバーからその場所をコピーするか、ディレクトリ名を \<server_name>\<directory_path> の形式で入力できます。ネットワークディレクトリが表示されない場合は、Secure Agent サービスのログインを設定します。この機能は、新しいバージョンの Windows では使用できない場合があります。</p> <p>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。</p> <p>サーバーレスランタイム環境では、このディレクトリはデータディスク内のマウントされたディレクトリまたはそのサブディレクトリのいずれかである必要があります。</p> <p>フラットファイルのデータを処理し、エラスティックランタイム環境を選択する場合は、そのフラットファイルを EFS ファイルシステムに格納して、次のディレクトリパスを指定します。</p> <p>/etc/infra/pod/<elastic runtime environment ID>/</p> <p>エラスティックランタイム環境 ID をを見つけるには、Administrator の 【ランタイム環境】 ページに移動して、URL からエラスティックランタイム環境 ID をコピーします。</p> <p>例えば、URL https://usw1.dmr-us.informaticacloud.com/cloudUI/products/administer/main/elastic-agent/KUBERNETES/0141GU250000000000002/overview の場合、エラスティックランタイム環境 ID は 0141GU250000000000002 です。</p>
【参照】 ボタン	フラットファイルの保存先ディレクトリを特定および選択するために使用します。
日付形式	<p>フラットファイルの日付フィールドの日付形式。次のいずれかの日付形式を選択します。</p> <ul style="list-style-type: none"> - MM/dd/yyyy HH:mm:ss - YYYY-MM-DD HH24:MI:SS.US

接続プロパティ	説明
コードページ	<p>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。</p> <ul style="list-style-type: none"> - MS Windows Latin 1。ISO 8859-1 Western European データの場合に選択します - UTF-8。Unicode データの場合に選択します - Unicode の UTF-32 エンコード (ビッグエンディアン) - Unicode の UTF-32 エンコード (ロウワーエンディアン) - Shift-JIS。ダブルバイト文字データの場合に選択します。 - ISO 8859-15 Latin 9 (Western European) - ISO 8859-2 Eastern European - ISO 8859-3 Southeast European - ISO 8859-5 Cyrillic - ISO 8859-9 Latin 5 (Turkish) - IBM EBCDIC International Latin-1 - Japanese EUC (with \ <-> Yen mapping) - IBM EBCDIC Japanese - IBM EBCDIC Japanese CP939 - PC Japanese SJIS-78 syntax (IBM-942) - PC Japanese SJIS-90 (IBM-943) - MS Windows Traditional Chinese, superset of Big 5 - Taiwan Big-5 (w/o euro update) - Chinese EUC - ISO 8859-8 Hebrew - PC Hebrew (old) - PC Hebrew (w/o euro update) - EBCDIC Hebrew (updated with new sheqel, control characters) - IBM EBCDIC US English IBM037 - Unicode の UTF-32 エンコード (ロウワーエンディアン) - ISO 8859-1 Western European - IBM EBCDIC French - ISO 8859-10 Latin 6 (Nordic) * - EBCDIC Finland, Sweden - MOS-DOS Thai, superset of TIS 620 - 7-bit ASCII - EBCDIC Finland, Sweden (w/ euro update) - MS-DOS Windows Latin 2 (Central Europe) - Japanese EBCDIC-Kana Fujitsu - ISO 8859-7 Greek <p>ファイル内の文字は 2 バイト以下でなければなりません。</p> <p>詳細マッピングでは、クラウドストレージ接続のフラットファイルオブジェクトは UTF-8 エンコードを使用する必要があります。</p> <p>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。</p> <p>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。</p>
<p>* データプレビューでは、類似した ISO 8859-4 Scandinavian/Baltic コードページが使用されますが、ランタイム処理では ISO 8859-10 Latin 6 (Nordic) が使用されるため、データプレビューとランタイムエンコーディングは一致しません。</p>	

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。

第 78 章

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。

接続プロパティ	説明
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。
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。 <ul style="list-style-type: none"> - 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。

第 79 章

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
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。
シークレットコンテナの使用	組織に対して設定されている Secrets Manager にこの接続の機密資格情報を保存します。 このプロパティは、組織に Secrets Manager が設定されている場合にのみ表示されます。 このプロパティは、データ取り込みおよびレプリケーションとデータアクセス管理サービスではサポートされていません。 接続でシークレットコンテナを有効にすると、Secure Agent が Secrets Manager からどの資格情報を取得するかを選択できます。このオプションを無効にした場合、資格情報は組織の設定方法に応じてリポジトリまたはローカル Secure Agent に保存されます。 注: この接続を使用してプッシュダウンまたはプロキシサービスを介してデータアクセスポリシーを適用する場合、シークレットコンテナ設定オプションを使用することはできません。 Secrets Manager を設定および使用する方法については、Administrator のヘルプにある「Secrets Manager の設定」を参照してください。
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。
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。
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。

プロパティ	説明
属性を含む	属性リソースフィールドの選択を有効にします。 デフォルトで選択されています。
メトリックを含める	メトリックリソースフィールドの選択を有効にします。 デフォルトで選択されています。
セグメントを含める	セグメントリソースフィールドの選択を有効にします。 デフォルトでは選択されていません。

第 80 章

Google Analytics 接続のプロパティ

Google Analytics レポートからデータの読み取りを行うための Google Analytics 接続を作成します。Google Analytics 接続は、マッピングタスクとマッピングで使用できます。

前提条件

Google Analytics コネクタを設定する前に、次のような前提条件のタスクを完了してください。

1. Google Analytics アナリティクスにアクセスするための Google アカウントを作成します。
2. **【資格情報】** ページで、**【API と認証】** セクションに移動し、**【サービスアカウントの作成】** をクリックします。
3. **【サービスアカウントの作成】** ダイアログボックスで、**【新しいシークレットキーを指定する】** と **【G Suite ドメイン全体の委任を有効にする】** を選択します。
注: **【キータイプ】** として **【JSON】** を選択し、生成されたキーを client_secrets.json として保存する必要があります。
4. **【作成】** をクリックします。
5. サービスアカウントを作成すると、client_email 値と private_key 値を含む JSON ファイルをダウンロードできるようになります。これらの詳細は、Google Analytics アカウントにユーザーを追加する場合、およびデータ統合で Google Analytics 接続を作成する場合に入力する必要があります。

次の画像は、サービスアカウントとキーを作成する【資格情報】ページを示しています。

Create service account

Service account name [?] Role [?] Owner

Service account ID

☒ Furnish a new private key
Downloads a file that contains the private key. Store the file securely because this key can't be recovered if lost.

Key type
☒ JSON
Recommended
☐ P12
For backward compatibility with code using the P12 format

☒ Enable G Suite Domain-wide Delegation
Allows this service account to be authorized to access all users' data on a G Suite domain without manual authorization on their part. [Learn more](#)

CANCEL CREATE

6. Analytics API を有効にするには、次の手順を実行します。
注: Google Analytics コネクタは、Google Analytics 4 API を使用して Google Analytics と統合します。
 - a. 次の Web サイトにアクセスします: <https://console.developers.google.com/>
 - b. 【ダッシュボード】 ページで、【Analytics API】 を有効にします。
7. Google Analytics でアカウントとプロパティを作成します。
8. Google Analytics アカウントに対する次の権限がユーザーに割り当てられていることを確認します。
 - 連携
 - 編集
 - ユーザーの管理
 - 読み取りと分析

Google Analytics への接続

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

始める前に

開始する前に、Google サービスアカウントを作成し、Analytics API を有効にして、Google Analytics アカウントを設定する必要があります。

これらのタスクの詳細については、「[「前提条件」 \(ページ 298\)](#)」を参照してください。

次のビデオでは、Google サービスアカウントから情報を取得して Google Analytics 接続を設定する方法について説明します。



接続の詳細

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。
シークレットコンテナの使用	組織に対して設定されている Secrets Manager にこの接続の機密資格情報を保存します。 このプロパティは、組織に Secrets Manager が設定されている場合にのみ表示されます。 このプロパティは、データ取り込みおよびレプリケーションとデータアクセス管理サービスではサポートされていません。 接続でシークレットコンテナを有効にすると、Secure Agent が Secrets Manager からどの資格情報を取得するかを選択できます。このオプションを無効にした場合、資格情報は組織の設定方法に応じてリポジトリまたはローカル Secure Agent に保存されます。 注: この接続を使用してプッシュダウンまたはプロキシサービスを介してデータアクセスポリシーを適用する場合、シークレットコンテナ設定オプションを使用することはできません。 Secrets Manager を設定および使用方法については、Administrator のヘルプにある「Secrets Manager の設定」を参照してください。
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。 Secure Agent、ホステッドエージェント、サーバーレスランタイム環境、またはエラスティックランタイム環境を選択します。 ランタイム環境の設定および使用方法の詳細については、Administrator のヘルプにある「ランタイム環境」を参照してください。
サービスアカウントの電子メール	サービスアカウントの作成後にダウンロードする JSON ファイル内にある client_email 値。
サービスアカウントキー	サービスアカウントの作成後にダウンロードする JSON ファイル内にある private_key 値。 JSON ファイルから取得したプライベートキーを使用する場合は、private_key フィールドの二重引用符内にある、-----BEGIN PRIVATE KEY-----\n で始まって-----END PRIVATE KEY-----\n で終わるテキストブロック全体を入力します。

API バージョン

デフォルトの Google Analytics 4 API を Google Analytics レポートから読み取るように設定できます。Google Analytics 4 API を選択し、特定のパラメータを設定します。

Google Analytics コネクタでは、Analytics Reporting API v4 と Core Reporting API v3 のサポートは廃止されました。

Google Analytics 4

次の表に、Google Analytics 4 の接続プロパティとその説明を示します。

プロパティ	説明
プロパティ ID	Google Analytics プロジェクトに関連付けられた Google Analytics プロパティ ID。 プロパティ ID を指定して、次のようなレポートからデータの読み取りを行うことができます。 <ul style="list-style-type: none">- 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。

Core Reporting API v3

次の表に、Core Reporting API v3 の接続プロパティとその説明を示します。

プロパティ	説明
アカウント ID	Google Analytics コネクタには適用されません。
プロパティ ID	Google Analytics コネクタには適用されません。
ビュー ID	Google Analytics コネクタには適用されません。

Analytics Reporting API v4

次の表に、Analytics Reporting API v4 の接続プロパティとその説明を示します。

プロパティ	説明
アカウント ID	Google Analytics コネクタには適用されません。
プロパティ ID	Google Analytics コネクタには適用されません。
ビュー ID	Google Analytics コネクタには適用されません。

第 81 章

Google Analytics Mass Ingestion 接続のプロパティ

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

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

接続プロパティ	説明
接続名	接続の名前。この名前は、組織内で一意にする必要があります。接続名には、英数字、スペース、および次のような特殊文字を含めることができます: <code>_ . + -</code> 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。
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とレプリケーション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 <code>client_email</code> 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 <code>private_key</code> 値。

第 82 章

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。

重要: 2024 年 11 月リリースから、Google BigQuery コネクタは非推奨となり、メンテナンスモードに移行されました。Informatica は将来のリリースでサポートを廃止する予定です。Google BigQuery V2 コネクタを使用して Google BigQuery にアクセスすることをお勧めします。

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	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。 <ul style="list-style-type: none">- 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。

プロパティ	説明
スキーマ定義のファイルパス	<p>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。</p> <p>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。</p> <p>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。</p> <ul style="list-style-type: none"> - 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	<p>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 <code>project_id</code> 値を指定します。</p> <p>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。</p>
データセット ID	<p>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。</p> <p>注: Google BigQuery は、米国リージョンにのみ存在するデータセットをサポートしています。</p>
ストレージパス	<p>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。</p> <p>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。</p> <p>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。</p> <p>例えば、<code>gs://<bucket_name></code>または<code>gs://<bucket_name>/<folder_name></code>を入力します。</p>

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	

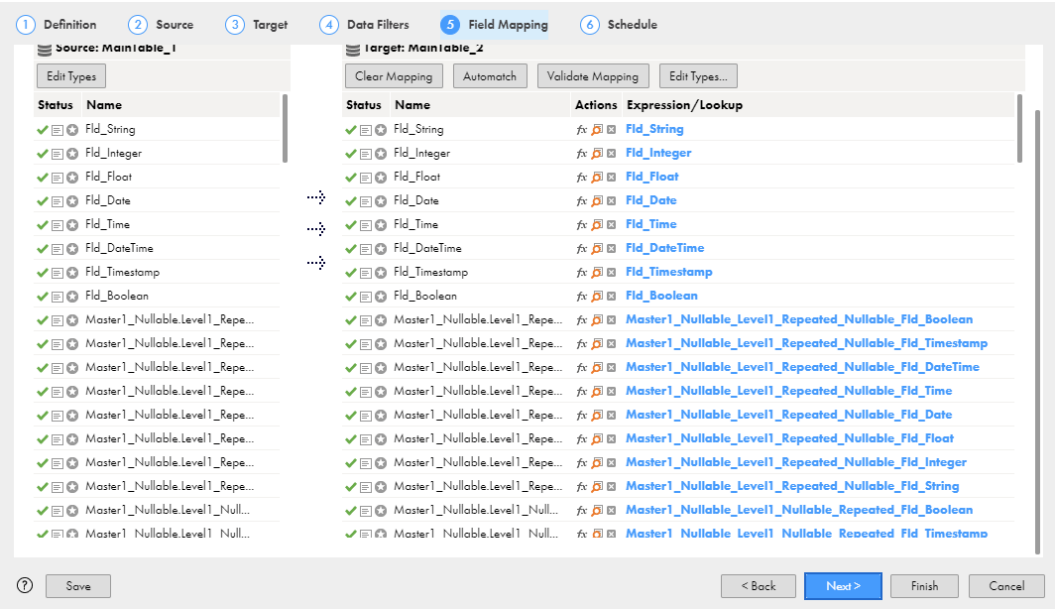
簡易モード

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

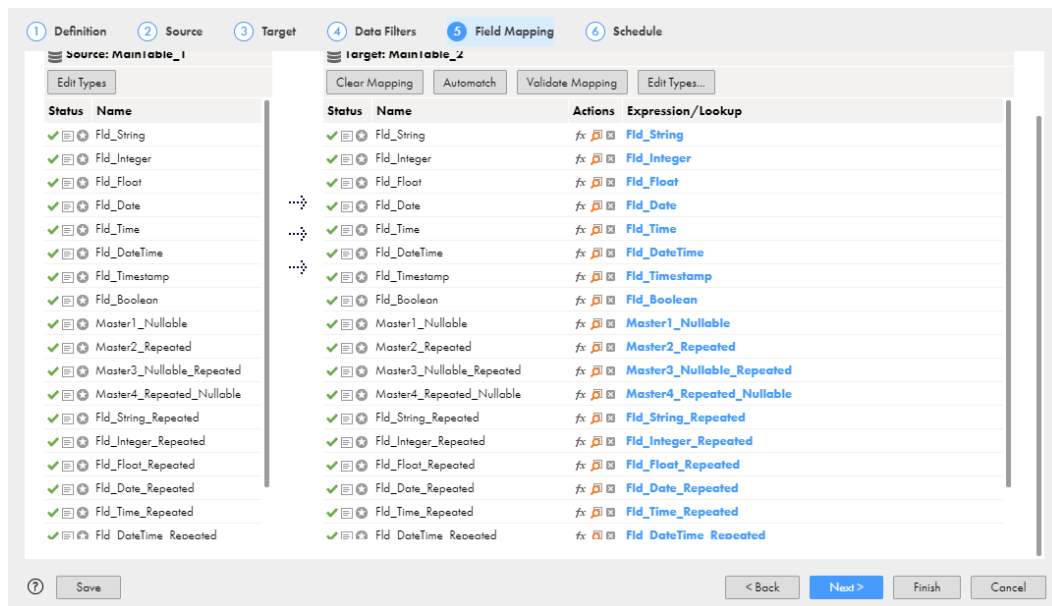
次の図に、同期タスクの【フィールドマッピング】タブ内のフィールドを示します。



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。

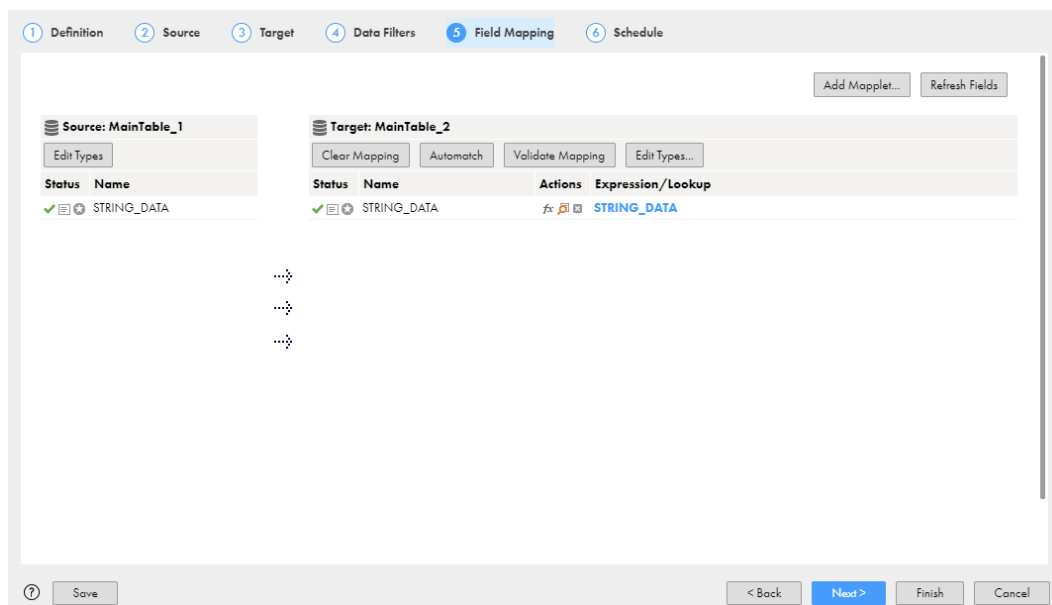
次の図に、同期タスクの【フィールドマッピング】タブを示します。



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。

第 83 章

Google BigQuery V2 接続のプロパティ

Google BigQuery との間でデータの安全な読み取りまたは書き込みを行うための Google BigQuery V2 接続を作成します。

Google BigQuery への接続

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

始める前に

接続を設定する前に、必ず Google サービスアカウントキーファイルを JSON 形式でダウンロードしてください。サービスアカウントキーファイルは、Google サービスアカウントの作成時に作成されます。

Google BigQuery 接続を作成するには、サービスアカウントキー JSON ファイルからのクライアントの電子メール、プライベートキー、およびプロジェクト ID が必要です。

次のビデオでは、Google BigQuery アカウントから必要な情報を取得する方法について説明します。



接続の詳細

次の表に、基本接続プロパティを示します。

プロパティ	説明
接続名	接続の名前。 各接続名は組織内で一意である必要があります。接続名には、英数字、スペース、および次の特殊文字を含めることができます。_ . + , 最大長は 255 文字です。
説明	接続の説明。最大長は 4000 文字です。
シークレットコンテナの使用	組織に対して設定されている Secrets Manager にこの接続の機密資格情報を保存します。 このプロパティは、組織に Secrets Manager が設定されている場合にのみ表示されます。 このプロパティは、データ取り込みおよびレプリケーションとデータアクセス管理サービスではサポートされていません。 接続でシークレットコンテナを有効にすると、Secure Agent が Secrets Manager からどの資格情報を取得するかを選択できます。このオプションを無効にした場合、資格情報は組織の設定方法に応じてリポジトリまたはローカル Secure Agent に保存されます。 注: この接続を使用してプッシュダウンまたはプロキシサービスを介してデータアクセスポリシーを適用する場合、シークレットコンテナ設定オプションを使用することはできません。 Secrets Manager を設定および使用方法については、Administrator のヘルプにある「Secrets Manager の設定」を参照してください。
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。 セキュアエージェント、ホステッドエージェント、サーバーレスランタイム環境、またはエラスティックランタイム環境を選択します。 アプリケーション取り込みとレプリケーションタスクとデータベース取り込みとレプリケーションタスクでは、Secure Agent またはサーバーレスランタイム環境を使用できます。タスクには、サーバーレス使用がサポートされているソースタイプが必要です。ホステッドエージェントまたはエラスティックランタイム環境で、アプリケーション取り込みとレプリケーションタスク、データベース取り込みとレプリケーションタスク、ファイル取り込みおよびレプリケーションタスク、またはストリーミング取り込みとレプリケーションタスクを実行することはできません。 ランタイム環境の設定および使用方法の詳細については、Administrator のヘルプにある「ランタイム環境」を参照してください。

認証タイプ

サービスアカウント認証方式または Workload Identity 連携認証方式を設定して、Google BigQuery にアクセスすることができます。Workload Identity 連携認証方式を使用する場合は、Okta を ID プロバイダとして設定できます。

必要な認証方式を選択し、認証固有のパラメータを設定します。

デフォルトはサービスアカウント認証方式です。

サービスアカウント認証

サービスアカウント認証では、少なくとも Google BigQuery サービスアカウントの電子メール、サービスアカウントキー、およびプロジェクト ID が必要です。

次の表に、サービスアカウント認証の基本接続プロパティを示します。

プロパティ	説明
サービスアカウントの電子メール	Google サービスアカウントキー JSON ファイルの client_email 値。
サービスアカウントキー	Google サービスアカウントキー JSON ファイルの private_key 値。 JSON ファイルから取得したプライベートキーを使用する場合は、private_key フィールドの二重引用符内にある、-----BEGIN PRIVATE KEY-----\n で始まって-----END PRIVATE KEY-----\n で終わるテキストブロック全体を入力します。
プロジェクト ID	Google サービスアカウントキー JSON ファイルの 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は、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。

注: テスト接続中にサービスアカウントの電子メール、サービスアカウントキー、およびプロジェクト ID の資格情報を検証する場合は、詳細設定の **【オプションのプロパティの指定】** フィールドでフラグ `CredentialValidation:true` を設定します。

詳細設定

次の表に、サービスアカウント認証の詳細接続プロパティを示します。

プロパティ	説明
BigQuery Storage API の有効化	データの読み取りまたは書き込み時に Google BigQuery Storage を使用してファイルをステージングします。 デフォルトでは選択されていません。
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。エージェントは、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、このストレージを使用します。 次のいずれかの形式を使用します。 - gs://<bucket_name> - gs://<bucket_name>/<folder_name> Google BigQuery でのクロスリージョンレプリケーションを有効にする場合、デュアルリージョンストレージをサポートする Google Cloud Storage パスを入力します。 このプロパティは、Google BigQuery Storage を使用してファイルをステージングする場合には適用されません。

プロパティ	説明
接続モード	<p>Google BigQuery との間でデータの読み取りまたは書き込みを行う場合に使用するモード。</p> <p>次のいずれかの接続モードを選択します。</p> <ul style="list-style-type: none"> - 簡易。レコードデータ型フィールド内の各フィールドがマッピング内の個別のフィールドとしてフラット化されます。 - 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 コネクタに、最上位のレコードデータ型のフィールドが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されます。 - 複合 1。Google BigQuery テーブル内のすべてのカラムが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されます。 <p>デフォルトは「簡易」です。</p> <p>このプロパティは、Google Cloud Storage を使用してファイルをステージングする場合に適用されます。</p>
カスタムクエリにレガシー SQL を使用 1	<p>このオプションは、カスタムクエリを定義するためにレガシー SQL を使用する場合に選択します。標準 SQL を使用してカスタムクエリを定義する場合は、このオプションをオフにします。</p> <p>このプロパティは、Google Cloud Storage を使用してファイルをステージングする場合に適用されます。</p> <p>このプロパティは、Google BigQuery V2 接続を混合モードまたは複合モードで設定した場合には適用されません。</p>
カスタムクエリのデータセット名 1	<p>カスタムクエリで指定する Google BigQuery データセットの名前。</p>
スキーマ定義のファイルパス 1	<p>Secure Agent によって Google BigQuery テーブルのサンプルスキーマとともに JSON ファイルが作成される、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。</p> <p>または、Secure Agent によって Google BigQuery テーブルのサンプルスキーマとともに JSON ファイルが作成される、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。</p> <p>複合接続モードを次のようなシナリオで設定する場合は、スキーマ定義ファイルが必要です。</p> <ul style="list-style-type: none"> - 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を行うために、マッピング内に階層ビルダトランスフォーマーションを追加した場合。 - 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を行うために、マッピング内に階層パーサトランスフォーマーションを追加した場合。 <p>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します。</p> <p>このプロパティは、Google Cloud Storage を使用してファイルをステージングする場合に適用されます。</p>
リージョン ID	<p>アクセスする Google BigQuery データセットが存在する地域名。</p> <p>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】プロパティで指定します。</p> <p>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。</p>

プロパティ	説明
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。 このプロパティは、Google Cloud Storage を使用してファイルをステージングする場合に適用されます。
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。 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、次のナレッジベースの記事を参照してください: Optional Properties configuration
¹ 詳細モードのマッピングには適用されません。	

ワークロード ID フェデレーション認証

次の表に、ワークロード ID フェデレーション認証の基本接続プロパティとその説明を示します。

プロパティ	説明
プロジェクト番号	接続するデータセットが含まれている Google サービスアカウントのプロジェクトの一意の数値識別子。
認証 URL	承認プロセスを開始するためにユーザー認証要求がリダイレクトされる、ID プロバイダによって指定されるエンドポイント URL。
アクセストークン URL	アクセストークンを取得するためにクライアントが承認コードまたは資格情報を交換する、ID プロバイダによって指定されるエンドポイント URL。
クライアント ID	ID プロバイダによってアプリケーションに割り当てられる一意の識別子。この ID は、認証および承認プロセス中に要求者を認識するために使用されます。
クライアントシークレット	クライアント ID とともに発行される機密キーで、トークン交換中にクライアントの信頼性を証明するためのアプリケーションと ID プロバイダの間のパスワードとして機能します。
プール ID	信頼できる外部 ID を集約する Google Cloud Platform で設定されたワークロード ID プールの識別子。
プロバイダ ID	ワークロード ID プール内で設定された特定の外部 ID プロバイダの ID。
アクセストークン	Google BigQuery リソースに安全にアクセスするために Google Cloud Platform によって付与されるアクセストークン。新しいアクセストークンを生成するには、 [アクセストークンの生成] をクリックします。

詳細設定

次の表に、ワークロード ID フェデレーション認証の詳細接続プロパティとその説明を示します。

プロパティ	説明
BigQuery Storage API の有効化	Google BigQuery Storage を使用して、データの読み取りまたは書き込み時にファイルをステージングします。 デフォルトでは選択されていません。
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。エージェントは、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、このストレージを使用します。 次のいずれかの形式を使用します。 - gs://<bucket_name> - gs://<bucket_name>/<folder_name> Google BigQuery でのクロスリージョンレプリケーションを有効にする場合、デュアルリージョンストレージをサポートする Google Cloud Storage パスを入力します。 このプロパティは、Google BigQuery Storage を使用してファイルをステージングする場合には適用されません。
カスタムクエリのデータセット名	カスタムクエリで指定する Google BigQuery データセットの名前。
リージョン ID	アクセスする Google BigQuery データセットが存在する地域名。 注: 指定された地域に存在するバケット名またはバケット名とフォルダ名を 【ストレージパス】 プロパティで指定します。 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。
オプションのプロパティの指定	特定のソースおよびターゲット機能を設定するための、Google BigQuery V2 接続のカスタムプロパティのカンマ区切りのキーと値のペア。 指定できるカスタムプロパティのリストの詳細については、ナレッジベースの記事「 Optional Properties configuration 」を参照してください。

接続の再試行

次の表に、接続の再試行のプロパティとその説明を示します。

プロパティ	説明
再試行の有効化 ¹	Secure Agent が Google BigQuery エンドポイントからの応答の受信を再試行するようにする場合は、このオプションを選択します。 直接モードまたはステージングモードで Google BigQuery からデータの読み取りを行い、一括モードで Google BigQuery にデータの書き込みを行うように再試行ストラテジを設定することができます。 Google BigQuery ターゲットにデータを書き込む場合、再試行ストラテジは CDC モードおよびストリーミングモードでは適用されません。 接続再試行オプションは、プロキシサーバーを使用してエンドポイントに接続するように設定された接続にも適用されます。 デフォルトでは選択されていません。
最大再試行回数	【再試行の有効化】 プロパティを選択した場合にのみ表示されます。 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。 デフォルトの試行回数は 6 回です。
初期再試行遅延	【再試行の有効化】 プロパティを選択した場合にのみ表示されます。 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 秒です。
再試行遅延乗数	【再試行の有効化】 プロパティを選択した場合にのみ表示されます。 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。 デフォルトの乗数は 2.0 です。小数値を使用することもできます。
最大再試行遅延	【再試行の有効化】 プロパティを選択した場合にのみ表示されます。 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 秒です。
合計タイムアウト	【再試行の有効化】 プロパティを選択した場合にのみ表示されます。 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 秒です。
¹ 詳細モードのマッピングには適用されません。	

プロキシサーバーの設定

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

Windows および Linux でプロキシサーバーを使用するように Secure Agent を設定できます。認証されていないプロキシサーバーまたは認証されたプロキシサーバーを使用できます。プロキシ設定は、マッピングおよび詳細モードのマッピングで使用される接続に適用されます。

Secure Agent のプロキシの設定を行うには、次のタスクを実行します。

- Windows の場合は Secure Agent Manager を使用し、Linux の場合はシェルコマンドを使用して Secure Agent を設定します。
手順については、データ統合のヘルプの『または「Windows でのプロキシ設定」または「Linux でのプロキシ設定」を参照してください。』
- Secure Agent のプロパティで、DTM の JVM オプションを設定します。手順については、ナレッジベースの記事「[Proxy server settings](#)」を参照してください。

proxy.ini 構成ファイルで指定したプロキシ設定は設計時に適用され、JVM オプションを使用して指定したプロキシ設定は実行時に適用されます。

サーバーレスランタイム環境のプロキシの設定を行うには、Administrator ヘルプの「ランタイム環境」にある「プロキシサーバーの使用」を参照してください。

NTLM 認証用のプロキシの設定

NTLM 認証を使用するプロキシサーバーを使用して、Google BigQuery に接続できます。NTLM 認証用のプロキシの設定を行うには、次の手順を実行します。

1. 管理者で、**[ランタイム環境]** を選択します。
2. 利用可能な Secure Agent のリストから、設定する Secure Agent を選択します。
3. 右上隅の **[編集]** をクリックします。
4. **[システム構成の詳細]** セクションで、データ統合サーバーの **[タイプ]** に **[DTM]** を選択します。
5. **[JVMOption1]** を編集し、次の値を追加します。
-Dhttp.auth.ntlm.domain=<domain name>
6. データ統合サーバーの **[プラットフォーム]** として **[タイプ]** を選択します。
7. **[INFA_DEBUG]** プロパティを編集し、次の値を追加します。
-Dhttp.auth.ntlm.domain=<domain name>
8. **[保存]** をクリックします。
9. Secure Agent を再起動します。

第 84 章

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。
シークレットコンテナの使用	<p>組織に対して設定されている Secrets Manager にこの接続の機密資格情報を保存します。このプロパティは、組織に Secrets Manager が設定されている場合にのみ表示されます。このプロパティは、データ取り込みおよびレプリケーションとデータアクセス管理サービスではサポートされていません。</p> <p>接続でシークレットコンテナを有効にすると、Secure Agent が Secrets Manager からどの資格情報を取得するかを選択できます。このオプションを無効にした場合、資格情報は組織の設定方法に応じてリポジトリまたはローカル Secure Agent に保存されます。</p> <p>注: この接続を使用してプッシュダウンまたはプロキシサービスを介してデータアクセスポリシーを適用する場合、シークレットコンテナ設定オプションを使用することはできません。</p> <p>Secrets Manager を設定および使用する方法については、Administrator のヘルプにある「Secrets Manager の設定」を参照してください。</p>
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。

第 85 章

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。

重要: 2024 年 11 月リリースから、Google Cloud Storage コネクタは非推奨となり、メンテナンスモードに移行されました。Informatica は将来のリリースでサポートを廃止する予定です。Google Cloud Storage V2 コネクタを使用して Google Cloud Storage にアクセスすることをお勧めします。

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
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 <code>project_id</code> 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 <code>client_email</code> 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 <code>private_key</code> 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。

第 86 章

Google Cloud Storage V2 接続のプロパティ

Google Cloud Storage ファイルに対してデータの安全な読み取りまたは書き込みを行うための Google Cloud Storage V2 接続を作成します。

Google Cloud Storage V2 接続を使用して、マッピングおよびマッピングタスクのソースとターゲットを指定できます。

Google Cloud Storage V2 への接続

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

始める前に

Google Cloud Storage V2 コネクタを設定する前に、次の前提条件のタスクを完了してください。

1. Google Cloud Storage にアクセスするための Google サービスアカウントを持っていることを確認します。
2. サービスアカウントのクライアント電子メール、プロジェクト ID、およびプライベートキーの値があることを確認します。Google Cloud Storage V2 接続の作成時に、これらの詳細を入力する必要があります。
3. サービスアカウントで Google Cloud Storage JSON API が有効になっていることを確認します。Google Cloud Storage V2 コネクタは、Google API を使用して Google Cloud Storage との統合を行います。
4. ソースファイルとターゲットファイルを含む Google Cloud Storage バケットに対する読み取りおよび書き込みアクセス権が付与されていることを確認します。
5. マッピングで Google Cloud Storage ファイルに対してデータの読み取りまたは書き込みを行う場合は、マッピングを正常に実行するために必要な権限が付与されている必要があります。
6. Informatica の暗号化方式を使用するには、次のタスクを実行します。
 - Administrator で Informatica 暗号ライブラリのライセンスが有効になっていることを確認します。
 - Google Cloud Platform の詳細クラスタ上の VPC ネットワークに次のファイアウォールルールを追加していることを確認します。
 - [ソースフィルタ] セクションの Secure Agent の IP アドレス範囲のリスト。
 - [ソースフィルタ] セクションの Google Cloud Platform クラスタの IP アドレス範囲。

- [プロトコル] セクションと [ポート] セクションのポート番号 0-65535 および udp:443。
- Secure Agent をホストする仮想マシンの VPC ネットワークタグの値が、ファイアウォールルールのソースタグおよびターゲットタグの値と同じであることを確認します。

接続の詳細

次の表に、Google Cloud Storage V2 接続のプロパティとその説明を示します。

プロパティ	説明
接続名	<p>接続の名前。</p> <p>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。_ . + - ,</p> <p>最大長は 255 文字です。</p>
説明	<p>接続の説明。最大長は 4000 文字です。</p>
シークレットコンテナの使用	<p>組織に対して設定されている Secrets Manager にこの接続の機密資格情報を保存します。このプロパティは、組織に Secrets Manager が設定されている場合にのみ表示されます。このプロパティは、データ取り込みおよびレプリケーションとデータアクセス管理サービスではサポートされていません。</p> <p>接続でシークレットコンテナを有効にすると、Secure Agent が Secrets Manager からどの資格情報を取得するかを選択できます。このオプションを無効にした場合、資格情報は組織の設定方法に応じてリポジトリまたはローカル Secure Agent に保存されます。</p> <p>注: この接続を使用してプッシュダウンまたはプロキシサービスを介してデータアクセスポリシーを適用する場合、シークレットコンテナ設定オプションを使用することはできません。</p> <p>Secrets Manager を設定および使用方法については、Administrator のヘルプにある「Secrets Manager の設定」を参照してください。</p>
ランタイム環境	<p>タスクを実行するランタイム環境の名前。</p> <p>Secure Agent、ホステッドエージェント、サーバーレスランタイム環境、またはエラスティックランタイム環境を選択します。</p> <p>ホステッドエージェントまたはサーバーレスランタイム環境でデータベース取り込みとレプリケーションタスクまたはストリーミング取り込みとレプリケーションタスクを実行することはできません。</p> <p>ランタイム環境の設定および使用方法の詳細については、Administrator のヘルプにある「ランタイム環境」を参照してください。</p>
サービスアカウント ID	<p>Google サービスアカウントキー JSON ファイルの client_email 値。</p>
サービスアカウントキー	<p>Google サービスアカウントキーの JSON ファイルの private_key 値。</p> <p>JSON ファイルから取得したプライベートキーを使用する場合は、private_key フィールドの二重引用符内にある、-----BEGIN PRIVATE KEY-----\n で始まって -----END PRIVATE KEY-----\n で終わるテキストブロック全体を入力します。</p>

プロパティ	説明
プロジェクト ID	Google サービスアカウントキー JSON ファイルの <code>project_id</code> 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は、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。
オブジェクトメタデータのインポートの最適化	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をインポートします。 このアプローチにより、バケットで使用可能な各オブジェクトの解析にかかる時間とオーバーヘッドが削減され、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。

詳細設定

次の表に、詳細接続のプロパティを示します。

プロパティ	説明
プライベートキー ID	このプロパティは、Google Cloud Storage V2 コネクタには適用されません。 Google サービスアカウントキーの JSON ファイルの <code>private_key_id</code> 値。 このプロパティは、データベース取り込みとレプリケーションタスクまたはストリーミング取り込みとレプリケーションタスクにのみ適用されます。
クライアント ID	このプロパティは、Google Cloud Storage V2 コネクタには適用されません。 Google サービスアカウントキーの JSON ファイルの <code>client_id</code> 値。 このプロパティは、データベース取り込みとレプリケーションタスクまたはストリーミング取り込みとレプリケーションタスクにのみ適用されます。
暗号化済みファイルである	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。 このプロパティは、詳細モードのマッピング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、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 Package Explorer に一覧表示されます。 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。

プロキシサーバーの設定

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

Windows および Linux でプロキシサーバーを使用するように Secure Agent を設定できます。認証されていないプロキシサーバーまたは認証されたプロキシサーバーを使用できます。プロキシ設定は、マッピングおよび詳細モードのマッピングで使用される接続に適用されます。

Secure Agent のプロキシの設定を行うには、次のタスクを実行します。

- Windows の場合は Secure Agent Manager を使用し、Linux の場合はシェルコマンドを使用して Secure Agent を設定します。
手順については、データ統合のヘルプの『または「Windows でのプロキシ設定」または「Linux でのプロキシ設定」を参照してください。
- Secure Agent のプロパティで、DTM の JVM オプションを設定します。手順については、ナレッジベースの記事「[Proxy server settings](#)」を参照してください。

サーバーレスランタイム環境のプロキシの設定を行うには、Administrator ヘルプの「ランタイム環境」にある「プロキシサーバーの使用」を参照してください。

NTLM 認証のプロキシの設定

NTLM 認証を使用するプロキシサーバーを使用して、Google Cloud Storage に接続できます。

NTLM 認証用のプロキシの設定を行うには、次の手順を実行します。

1. 管理者で、**[ランタイム環境]** を選択します。
2. 利用可能な Secure Agent のリストから、設定する Secure Agent を選択します。
3. 右上隅の **[編集]** をクリックします。
4. **[システム構成の詳細]** セクションで、データ統合サーバーの **[タイプ]** に **[DTM]** を選択します。
5. **[JVMOption1]** を編集し、次の値を追加します。
-Dhttp.auth.ntlm.domain=<domain name>
6. データ統合サーバーの **[プラットフォーム]** として **[タイプ]** を選択します。
7. **[INFA_DEBUG]** プロパティを編集し、次の値を追加します。
-Dhttp.auth.ntlm.domain=<domain name>
8. **[保存]** をクリックします。
9. Secure Agent を再起動します。

第 87 章

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
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。
シークレットコンテナの使用	組織に対して設定されている Secrets Manager にこの接続の機密資格情報を保存します。 このプロパティは、組織に Secrets Manager が設定されている場合にのみ表示されます。 このプロパティは、データ取り込みおよびレプリケーションとデータアクセス管理サービスではサポートされていません。 接続でシークレットコンテナを有効にすると、Secure Agent が Secrets Manager からどの資格情報を取得するかを選択できます。このオプションを無効にした場合、資格情報は組織の設定方法に応じてリポジトリまたはローカル Secure Agent に保存されます。 注: この接続を使用してプッシュダウンまたはプロキシサービスを介してデータアクセスポリシーを適用する場合、シークレットコンテナ設定オプションを使用することはできません。 Secrets Manager を設定および使用する方法については、Administrator のヘルプにある「Secrets Manager の設定」を参照してください。
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。
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更新トークン。
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ディレクトリ。
ファイルのアップロードパス	アップロードするファイルが保存されるディレクトリ。

プロパティ	説明
ページサイズ	読み取り操作のページサイズ。デフォルト値は 10 です。
ファイル ID パス	Google Drive の Files_GetAll オブジェクトに割り当てられた一意のファイル ID を含むディレクトリで、ID で複数のファイルを追跡、整理、および取得できます。

第 88 章

Google PubSub - ストリーミング 取り込みとレプリケーション接続 のプロパティ

Google PubSub ストリーミング取り込みとレプリケーション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、データ取り込みおよびレプリケーションサービスで設定するストリーミング取り込みとレプリケーション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。
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。

第 89 章

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。
シークレットコンテナの使用	<p>組織に対して設定されている Secrets Manager にこの接続の機密資格情報を保存します。</p> <p>このプロパティは、組織に Secrets Manager が設定されている場合にのみ表示されます。</p> <p>このプロパティは、データ取り込みおよびレプリケーションとデータアクセス管理サービスではサポートされていません。</p> <p>接続でシークレットコンテナを有効にすると、Secure Agent が Secrets Manager からどの資格情報を取得するかを選択できます。このオプションを無効にした場合、資格情報は組織の設定方法に応じてリポジトリまたはローカル Secure Agent に保存されます。</p> <p>注: この接続を使用してプッシュダウンまたはプロキシサービスを介してデータアクセスポリシーを適用する場合、シークレットコンテナ設定オプションを使用することはできません。</p> <p>Secrets Manager を設定および使用する方法については、Administrator のヘルプにある「Secrets Manager の設定」を参照してください。</p>
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。

第 90 章

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。
シークレットコンテナの使用	<p>組織に対して設定されている Secrets Manager にこの接続の機密資格情報を保存します。このプロパティは、組織に Secrets Manager が設定されている場合にのみ表示されます。このプロパティは、データ取り込みおよびレプリケーションとデータアクセス管理サービスではサポートされていません。</p> <p>接続でシークレットコンテナを有効にすると、Secure Agent が Secrets Manager からどの資格情報を取得するかを選択できます。このオプションを無効にした場合、資格情報は組織の設定方法に応じてリポジトリまたはローカル Secure Agent に保存されます。</p> <p>注: この接続を使用してプッシュダウンまたはプロキシサービスを介してデータアクセスポリシーを適用する場合、シークレットコンテナ設定オプションを使用することはできません。</p> <p>Secrets Manager を設定および使用する方法については、Administrator のヘルプにある「Secrets Manager の設定」を参照してください。</p>
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。

第 91 章

Google Sheets 接続のプロパティ

Google スプレッドシート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 Sheets 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。
シークレットコンテナの使用	組織に対して設定されている Secrets Manager にこの接続の機密資格情報を保存します。 このプロパティは、組織に Secrets Manager が設定されている場合にのみ表示されます。 このプロパティは、データ取り込みおよびレプリケーションとデータアクセス管理サービスではサポートされていません。 接続でシークレットコンテナを有効にすると、Secure Agent が Secrets Manager からどの資格情報を取得するかを選択できます。このオプションを無効にした場合、資格情報は組織の設定方法に応じてリポジトリまたはローカル Secure Agent に保存されます。 注: この接続を使用してプッシュダウンまたはプロキシサービスを介してデータアクセスポリシーを適用する場合、シークレットコンテナ設定オプションを使用することはできません。 Secrets Manager を設定および使用する方法については、Administrator のヘルプにある「Secrets Manager の設定」を参照してください。
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。
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 (シート用)	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。
ドライブ用の更新トークン	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、[スプレッドシート名] 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となります。

プロパティ	説明
スプレッドシート名	Google Sheets 内のスプレッドシート名。
スプレッドシート ID	Google Sheets 内のスプレッドシート ID。
初期カラム範囲	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、初期カラム範囲の値は <code>Sheet1!C5</code> と指定します。
最終カラム範囲	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、最終カラム範囲の値は <code>Sheet1!G20</code> と指定します。
ヘッダーあり	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。
新しいスプレッドシートの作成	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、 [スプレッドシート名] フィールドで指定した名前を使用して、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。このオプションが無効ではない場合、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。

第 92 章

Google Sheets V2 接続のプロパティ

Google スプレッドシート 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 Sheets 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。
シークレットコンテナの使用	組織に対して設定されている Secrets Manager にこの接続の機密資格情報を保存します。 このプロパティは、組織に Secrets Manager が設定されている場合にのみ表示されます。 このプロパティは、データ取り込みおよびレプリケーションとデータアクセス管理サービスではサポートされていません。 接続でシークレットコンテナを有効にすると、Secure Agent が Secrets Manager からどの資格情報を取得するかを選択できます。このオプションを無効にした場合、資格情報は組織の設定方法に応じてリポジトリまたはローカル Secure Agent に保存されます。 注: この接続を使用してプッシュダウンまたはプロキシサービスを介してデータアクセスポリシーを適用する場合、シークレットコンテナ設定オプションを使用することはできません。 Secrets Manager を設定および使用する方法については、Administrator のヘルプにある「Secrets Manager の設定」を参照してください。
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。
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。

第 93 章

Greenplum 接続のプロパティ

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

前提条件

Greenplum コネクタを使用する前に、前提条件を満たしていることを確認してください。

以下の前提条件タスクを実行します。

1. Greenplum ローダーパッケージを Secure Agent マシンにインストールします。ローダーパッケージには gpload ユーティリティが含まれています。Greenplum ローダーパッケージは、Pivotal Greenplum の Web サイトからダウンロードできます。
2. Secure Agent マシンで DataDirect Greenplum ODBC ドライバと JDBC ドライバを設定します。
3. Greenplum データベースに接続するための認証の前提条件を設定します。データベース認証または Kerberos 認証を設定できます。使用する認証タイプに基づいて、次の認証の詳細を手元に用意してください。
 - データベース認証を設定するには、Greenplum アカウントのユーザー名、パスワード、ホスト名、ポート、データベース名が必要です。
 - Kerberos 認証を設定するには、Greenplum アカウントのサービスプリンシパル名、ホスト名、ポート、およびデータベース名が必要です。

JDBC ドライバおよび ODBC ドライバの設定

Greenplum コネクタを使用する前に、Windows と Linux で DataDirect Greenplum の JDBC ドライバおよび ODBC ドライバを設定してください。

Linux での DataDirect Greenplum JDBC ドライバの設定

1. DataDirect Greenplum JDBC ドライババージョン 6.x を Pivotal Greenplum の Web サイトからダウンロードします。
2. Greenplum JDBC ドライバを Secure Agent マシン上の次のディレクトリにコピーします: <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/Greenplum
注: deploy_to_main/bin/rdtm-extra ディレクトリを手動で作成する必要があります。
3. Secure Agent を再起動します。

Windows での DataDirect Greenplum JDBC ドライバの設定

1. DataDirect Greenplum JDBC ドライババージョン 6.x を Pivotal Greenplum の Web サイトからダウンロードします。
2. Greenplum JDBC ドライバを Secure Agent マシンの次のディレクトリにコピーします。
<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\Greenplum

deploy_to_main\bin\rdtm-extra\Greenplum ディレクトリを手動で作成する必要があります。
3. Secure Agent を再起動します。

Linux での DataDirect Greenplum ODBC ドライバの設定

1. Pivotal の Web サイトから DataDirect Greenplum ODBC ドライババージョン 7.1.6 をダウンロードし、Secure Agent マシンに DataDirect Greenplum ODBC ドライバをインストールします。
2. 次のディレクトリにある odbcinst.ini ファイルに次のドライバエントリを追加します: <Secure Agent のインストールディレクトリ>/odbcinst.ini
以下の構文を使用します。

```
[DataDirect 7.1 Greenplum Wire Protocol]
Driver=<ODBC driver path>/lib/ddgplm27.so
Setup=<ODBC driver path>/lib/ddgplm27.so
DriverODBCVer=<ODBC Driver version>
HelpRootDirectory=<ODBC Driver path>/help
GSSClient=libgssapi_krb5.so.2
```

例 :

```
[DataDirect 7.1 Greenplum Wire Protocol]
Driver=/opt/Progress/DataDirect/Connect64_for_ODBC_71/lib/ddgplm27.so
Setup=/opt/Progress/DataDirect/Connect64_for_ODBC_71/lib/ddgplm27.so
APILevel=0
ConnectFunctions=YYY
DriverODBCVer=3.52
FileUsage=0
HelpRootDirectory=/opt/Progress/DataDirect/Connect64_for_ODBC_71/help
SQLLevel=0
GSSClient=libgssapi_krb5.so.2
```

3. ドライバの GPHOME_LOADERS、PATH、および LD_LIBRARY_PATH 環境変数を設定します。
以下のタスクを実行します。
 - a. GPHOME_LOADERS 環境変数を、Greenplum ローダーライブラリを含むディレクトリに設定します。C シェルを使用して、次のコマンドを実行します。

setenv GPHOME_LOADERS /export/qa_adp/thirdparty/greenplum/rhel.64/loaders
 - b. PATH 環境変数を、Greenplum ローダーライブラリを含むディレクトリに設定します。C シェルを使用して、次のコマンドを実行します。

setenv PATH \${GPHOME_LOADERS}/bin:\${PATH}
 - c. LD_LIBRARY_PATH 環境変数を設定して、Greenplum ドライバと DataDirect Greenplum ODBC ライブラリを含む次のディレクトリを含めます。C シェルを使用して、次のコマンドを実行します。

setenv LD_LIBRARY_PATH .:\${GPHOME_LOADERS}/lib:/export/qa_adp/thirdparty/greenplum/rhel.64/loaders/ext/python/lib
setenv LD_LIBRARY_PATH /opt/Progress/DataDirect/Connect64_for_ODBC_71/lib:\${LD_LIBRARY_PATH}
4. 環境変数を更新した後に、Secure Agent を再起動します。

Windows での DataDirect Greenplum ODBC ドライバの設定

1. Pivotal の Web サイトから DataDirect Greenplum ODBC ドライババージョン 7.1.6 をダウンロードし、Secure Agent マシンに DataDirect Greenplum ODBC ドライバをインストールします。
2. Python 2.5.4 32 ビットをインストールします。
3. Windows 用の 5.18 Greenplum クライアントソフトウェアをインストールします。
4. Windows 用の 5.18 Greenplum ローダーソフトウェアをインストールします。
5. コマンドラインから次の環境変数をドライバに設定します。
 - GPHOME_LOADERS 環境変数を、Greenplum ローダーライブラリを含むディレクトリに設定します。
例: Set GPHOME_LOADERS = C:\Program Files (x86)\Greenplum\greenplum-loaders-5.18.0
 - GPHOME_CLIENTS 環境変数を、Greenplum クライアントライブラリを含むディレクトリに設定します。
例: set GPHOME_CLIENTS=C:\Program Files (x86)\Greenplum\greenplum-clients-5.18.0\
 - PYTHONPATH 環境変数を設定します。
Set PYTHONPATH=%GPHOME_LOADERS%\bin\lib
 - DDCPATH 環境変数を、DataDirect ライブラリを含むディレクトリに設定します。
例: DDCPATH=C:\Program Files\Progress\DataDirect\Connect64_for_ODBC_71\drivers;C:\Program Files\Progress\DataDirect\Connect64_for_ODBC_71\jre\bin;C:\Program Files\Progress\DataDirect\Connect64_for_ODBC_71\jre\bin\server
 - Path 環境変数を、Greenplum クライアント、Greenplum ローダー、Python、および Greenplum ODBC Datadirect ドライバライブラリを含むディレクトリに設定します。
例: Path=C:\Python25;C:\Program Files (x86)\Greenplum\greenplum-loaders-5.18.0\lib;C:\Program Files (x86)\Greenplum\greenplum-loaders-5.18.0\bin;C:\Program Files (x86)\Greenplum\greenplum-clients-5.18.0\lib;C:\Program Files (x86)\Greenplum\greenplum-clients-5.18.0\bin;%DDCPATH%

Kerberos 認証の設定

Kerberos 認証を使用して Linux または Windows 上の Greenplum に接続する前に、組織の管理者は前提条件のタスクを実行する必要があります。

1. Java Authentication and Authorization Service 構成ファイル（JAAS）を設定するには、次のタスクを実行します。
 - a. Secure Agent マシン上に JAAS 構成ファイルを作成します。
 - b. 以下のエントリを JAAS 構成ファイルに追加します。

```
JDBC_DRIVER_01 {  
    com.sun.security.auth.module.Krb5LoginModule required useTicketCache=true;  
};
```
2. krb5.conf ファイルを設定するには、次のタスクを実行します。
 - a. Secure Agent マシン上に krb5.conf ファイルを作成します。
 - b. Key Distribution Center（KDC）と管理サーバーの詳細を、次の形式で krb5.conf ファイルに追加します。

```
[libdefaults]  
default_realm = <Realm name>  
forwardable = true  
ticket_lifetime = 24h  
  
[realms]  
<REALM NAME> = {  
    kdc = <Location where KDC is installed>  
    admin_server = <Location where KDC is installed>
```

```

    }
    [domain_realm]
    <domain name or host name> = <Domain name or host name of Kerberos>
    <domain name or host name> = <Domain name or host name of Kerberos>

```

3. Secure Agent マシン上で環境変数を設定します。
4. Secure Agent を再起動します。
5. Secure Agent マシン上で資格情報キャッシュファイルを生成し、Kerberos 認証を使用して Greenplum に接続するには、次のタスクを実行します。
 - a. Secure Agent マシン上のコマンドラインで次のコマンドを実行し、Greenplum ユーザー名とレルム名を指定します。
`Kinit <user name>@<realm_name>`
 - b. 要求されたら、Kerberos プリンシパルユーザーのパスワードを入力します。

環境変数の設定

Kerberos 認証を使用して Greenplum に接続するには、Secure Agent マシン上で必要な環境変数を設定する必要があります。

環境変数を設定するには、次のコマンドを実行します。

- `setenv KRB5CCNAME <資格情報キャッシュファイルの絶対パスとファイル名>`
- `setenv KRB5_CONFIG <Kerberos 構成ファイルの絶対パス>\krb5.conf`
- `setenv JAASCONFIG <JAAS 構成ファイルの絶対パス>\<ファイル名>.conf`

環境変数を設定した後に、Secure Agent を再起動する必要があります。

または、Greenplum 接続の作成時に KRB5_CONFIG および JAASCONFIG 環境変数を追加することもできます。

Kerberos 認証を使用した接続の設定時に環境変数を追加するには、Greenplum 接続の **[Kerberos 接続プロパティ]** フィールドに `KRB5_CONFIG` プロパティと `JAASCONFIG` プロパティを追加する必要があります。

例えば、次の形式でプロパティを追加します。

```
KRB5_CONFIG=<Absolute path of the Kerberos configuration file>\krb5.conf;JAASCONFIG=<Absolute path of the JAAS config file>\<File name>.conf
```

注: キーと値のペアはそれぞれセミコロンで区切ってください。

Greenplum への接続

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

始める前に

開始する前に、前提条件を必ず満たすようにしてください。

認証の前提条件と実行する必要があるその他のタスクの詳細については、「[「前提条件」 \(ページ 333\)](#)」を参照してください。

接続の詳細

次の表に、基本接続プロパティを示します。

プロパティ	説明
接続名	接続の名前。 各接続名は組織内で一意である必要があります。接続名には、英数字、スペース、および次の特殊文字を含めることができます。_ . + -, 最大長は 255 文字です。
説明	接続の説明。最大長は 4000 文字です。
シークレットコンテナの使用	組織に対して設定されている Secrets Manager にこの接続の機密資格情報を保存します。 このプロパティは、組織に Secrets Manager が設定されている場合にのみ表示されます。 このプロパティは、データ取り込みおよびレプリケーションとデータアクセス管理サービスではサポートされていません。 接続でシークレットコンテナを有効にすると、Secure Agent が Secrets Manager からどの資格情報を取得するかを選択できます。このオプションを無効にした場合、資格情報は組織の設定方法に応じてリポジトリまたはローカル Secure Agent に保存されます。 注: この接続を使用してプッシュダウンまたはプロキシサービスを介してデータアクセスポリシーを適用する場合、シークレットコンテナ設定オプションを使用することはできません。 Secrets Manager を設定および使用方法については、Administrator のヘルプにある「Secrets Manager の設定」を参照してください。
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。 Secure Agent、ホステッドエージェント、またはサーバーレスランタイム環境を指定できます。
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 に設定されたポート番号から読み取りを行います。 デフォルトは 5432 です。
データベース	Greenplum 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。

認証タイプ

Greenplum データベースに接続するようにデータベース認証タイプまたは Kerberos 認証タイプを設定できます。

必要な認証タイプを選択し、認証固有のパラメータを設定します。

データベース認証

データベース認証を設定するには、Greenplum アカウントのユーザー名とパスワードが必要です。

次の表に、データベース認証の基本接続プロパティとその説明を示します。

プロパティ	説明
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。

次の表に、データベース認証の詳細接続プロパティを示します。

プロパティ	説明
証明書のパス	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 ベースの接続は、Greenplum に書き込むマッピングのターゲットトランスフォーメーションでのみ使用できます。
メタデータ追加接続設定	Greenplum からメタデータを取得するために設定する追加の接続プロパティ。 プロパティは次の形式で入力します。 <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。

Kerberos 認証

Kerberos 認証を設定するには、Greenplum アカウントの Kerberos 接続プロパティ、サービスプリンシパル名、ホスト名、ポート、データベース名、および Greenplum アカウントの詳細が必要です。

次の表に、Kerberos 認証の基本接続プロパティとその説明を示します。

プロパティ	説明
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	Greenplum データベースの名前。

次の表に、Kerberos 認証の詳細接続プロパティとその説明を示します。

プロパティ	説明
Kerberos 接続 プロパティ	<p>Kerberos 認証を使用して Greenplum データベースに接続するための追加の接続プロパティ。</p> <p>プロパティを次の形式で入力します:</p> <p><パラメータ名>=<パラメータ値></p> <p>複数のプロパティを指定する場合は、キーと値のペアをそれぞれセミコロンで区切ります。</p>
サービスプリン シパル名です	<p>Kerberos 認証に使用するサービスプリンシパル名。</p> <p>サービスプリンシパル名は次の形式で指定します:</p> <p><サービス名>/<完全修飾ドメイン名>@<REALM.COM></p> <ul style="list-style-type: none"> - サービス名は、Greenplum インスタンスをホストするサービスの名前です。 - 完全修飾ドメイン名は、ホストマシンの完全修飾ドメイン名です。 - REALM.COM は、ホストマシンのドメイン名です。この値はオプションです。レルム名が指定されていない場合は、デフォルトのレルムが使用されます。

第 94 章

Hadoop 接続プロパティ

同期タスクで Hadoop コネクタを使用するには、接続プロパティを設定する必要があります。

重要: Hadoop コネクタは非推奨となり、メンテナンスモードに移行されました。Informatica は将来のリリースでサポートを廃止する予定です。Hive コネクタを使用して Hadoop クラスタにアクセスすることをお勧めします。

次の表に、Hadoop 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	Hadoop コンポーネントのスキーマのユーザー名。
パスワード	Hadoop コンポーネントのスキーマのパスワード。
JDBC 接続 URL	Hadoop コンポーネントに接続するための JDBC URL。『 「JDBC URL」 (ページ 341) 』を参照してください
ドライバ	Hadoop コンポーネントに接続するための JDBC ドライバクラス。 詳細については、『さまざまな Hadoop ディストリビューションに対する Hadoop クラスパスの設定』トピックを参照してください。
コミット間隔	データを Hive にロードするためのバッチサイズ（行数単位）。
Hadoop のインストールパス	Hadoop コンポーネントのインストールパス。 Kerberos クラスタには適用されません。
Hive のインストールパス	Hive のインストールパス Kerberos クラスタには適用されません。
HDFS インストールパス	HDFS インストールパス。 Kerberos クラスタには適用されません。
HBase のインストールパス	HBase のインストールパス。 Kerberos クラスタには適用されません。
Impala のインストールパス	Impala のインストールパス。 Kerberos クラスタには適用されません。
その他のライブラリパス	Hadoop と通信するライブラリ。 Kerberos クラスタには適用されません。

接続プロパティ	説明
ロギングの有効化	ロギングを有効にすると、ログメッセージが有効になります。 注: [ロギングの有効化] 接続パラメータは将来のリリースのプレースホルダであり、このパラメータの状態はコネクタの機能には影響しません。
Hadoop ディストリビューション	Kerberos 認証を使用できる Hadoop ディストリビューション。Cloudera と HDP Hadoop ディストリビューションに、Kerberos 認証を使用できます。
認証タイプ	ネイティブ認証または Kerberos 認証を選択できます。
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。
Hive サイト XML	core-site.xml、hive-site.xml、および hdfs-site.xml が配置されるディレクトリ。3 つの XML ファイルは同じ場所に存在する必要があります。
スーパーユーザーのプリンシパル名	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	さまざまなユーザーが Kerberos 認証を使用する Hadoop クラスタ内でマッピングを実行したり、Kerberos 認証を使用するソースおよびターゲットに接続したりできるようにすることができます。さまざまなユーザーがマッピングを実行したり、ビッグデータのソースおよびターゲットに接続できるようにするには、ユーザーの偽装を設定する必要があります。

注: インストールパスは、Hadoop jar を配置するパスです。Hadoop コネクタは、Hadoop に命令を送信する前に、インストールパスからライブラリをロードします。Kerberos 認証タイプを使用する場合、Hadoop インストールパス、Hive インストールパス、HDFS インストールパス、HBase インストールパス、Impala インストールパス、およびその他のライブラリパスを指定する必要はありません。

Kerberos 認証を使用せず、インストールパスを指定しない場合は、Amazon EMR、HortonWorks、MapR、および Cloudera の Hadoop クラスパスを設定できます。

非 Kerberos クラスタで挿入操作を実行すると、Secure Agent は `hadoop fs -put <FS> <HDFS>` コマンドを使用してファイルを HDFS にアップロードし、`hadoop fs -rm -r <HDFS>` コマンドを使用して HDFS からファイルを削除します。Kerberos 認証を有効にした場合、Secure Agent は、Hadoop コマンドを使用せずに HDFS へのデータの書き込みまたは HDFS からのデータの削除を行います。

JDBC URL

コネクタは、JDBC を使用して Hadoop のさまざまなコンポーネントに接続します。URL の形式とパラメータはコンポーネントごとに異なります。

Hive は次の JDBC URL 形式を使用します。

```
jdbc:hive/hive2://<server>:<port>/<schema>
```

URL パラメータの重要性については以下で説明します。

- hive/hive2: プロトコル情報が含まれます。Thrift サーバーのバージョン、つまり、HiveServer の場合は hive、HiveServer2 の場合は hive2。
- サーバー、ポート - Thrift サーバーのサーバーおよびポート情報。
- スキーマ - コネクタがアクセスする必要がある Hive スキーマ。

例えば、`jdbc:hive2://invrlx63iso7:10000/default` は Hive のデフォルトのスキーマに接続し、サーバー `invrlx63iso7` のポート 10000 で起動する Hive Thrift サーバー `HiveServer2` を使用します。

Hadoop コネクタは、Hive Thrift サーバーを使用して Hive と通信します。

Thrift サーバーを起動するコマンドは、`-hive -service hiveserver2` です。

Cloudera Impala は、次の形式の JDBC URL を使用します。

`jdbc:hive2://<サーバー>:<ポート>/;auth=<認証メカニズム>`

JDBC ドライバクラス

JDBC ドライバクラスは、Hadoop コンポーネントに応じて異なります。例えば、Hive および Impala に対しては `org.apache.hive.jdbc.HiveDriver` となります。

第 95 章

Hadoop ファイル接続のプロパティ

Hadoop ファイル接続を設定するときに、接続プロパティを設定する必要があります。

重要: Hadoop ファイルコネクタは非推奨となり、メンテナンスモードに移行されました。Informatica は将来のリリースでサポートを廃止する予定です。Hadoop Files V2 コネクタを使用して Hadoop Distributed File System (HDFS) にアクセスすることをお勧めします。

次の表に、Hadoop ファイル接続のプロパティを示します。

接続プロパティ	説明
接続名	Hadoop ファイル接続の名前。
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 ファイルを選択します。
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。

接続プロパティ	説明
NameNode の URI	<p>HDFS にアクセスするための URI。</p> <p>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。</p> <pre>hdfs://<namenode>:<port>/</pre> <p>ここで</p> <ul style="list-style-type: none"> - <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。 <p>Hadoop クラスタが高可用性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。</p> <p>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。</p> <pre><property> <name>fs.defaultFS</name> <value>hdfs://nameservice1</value> <source>core-site.xml</source> </property></pre> <p>上のスニペットで、fs.defaultFS 値は次のとおりです。</p> <pre>hdfs://nameservice1</pre> <p>対応する名前ノード URI は次のとおりです。</p> <pre>hdfs://nameservice1/</pre> <p>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。</p>
ローカルパス	<p>データを読み書きする場所のローカルファイルシステムパス。HDFS との間でデータを読み書きする場合、ローカルパスは指定しません。ローカルパスを指定するには、次の条件を参照します。</p> <ul style="list-style-type: none"> - 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、ロ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。
Hadoop ディストリビューション	<p>Hadoop ディストリビューション名。接続に使用する HDFS インスタンスに基づいて、CLOUDERA、EMR、または HDP を入力します。</p> <p>Cloudera CDH と Hortonworks HDP Hadoop ディストリビューションに、Kerberos 認証を使用できます。</p> <p>注: Hadoop ディストリビューション名を指定するには、すべて大文字を使用します。</p>
キータブファイル	<p>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。</p>
プリンシパル名	<p>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。</p>
偽装ユーザー名	<p>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。</p>

第 96 章

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。
シークレットコンテナの使用	<p>組織に対して設定されている Secrets Manager にこの接続の機密資格情報を保存します。</p> <p>このプロパティは、組織に Secrets Manager が設定されている場合にのみ表示されます。</p> <p>このプロパティは、データ取り込みおよびレプリケーションとデータアクセス管理サービスではサポートされていません。</p> <p>接続でシークレットコンテナを有効にすると、Secure Agent が Secrets Manager からどの資格情報を取得するかを選択できます。このオプションを無効にした場合、資格情報は組織の設定方法に応じてリポジトリまたはローカル Secure Agent に保存されます。</p> <p>注: この接続を使用してプッシュダウンまたはプロキシサービスを介してデータアクセスポリシーを適用する場合、シークレットコンテナ設定オプションを使用することはできません。</p> <p>Secrets Manager を設定および使用方法については、Administrator のヘルプにある「Secrets Manager の設定」を参照してください。</p>
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。

接続プロパティ	説明
NameNode の URI	<p>HDFS にアクセスするための URI。</p> <p>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。</p> <pre>hdfs://<namenode>:<port>/</pre> <p>ここで、</p> <ul style="list-style-type: none"> - <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。 <p>Hadoop クラスタに接続するには、ネームノードポート fs.defaultFS を指定します。</p> <p>Hadoop クラスタが高可用性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。</p> <p>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。</p> <pre><property> <name>fs.defaultFS</name> <value>hdfs://nameservice1</value> <source>core-site.xml</source> </property></pre> <p>上のスニペットで、fs.defaultFS 値は次のとおりです。</p> <pre>hdfs://nameservice1</pre> <p>対応する名前ノード URI は次のとおりです。</p> <pre>hdfs://nameservice1/</pre> <p>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。</p>
ローカルパス	<p>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。</p> <ul style="list-style-type: none"> - 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、ロ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。 <p>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。</p> <p>[ローカルパス] のデフォルト値は [NA] です。</p>
構成ファイルのパス	<p>Hadoop 構成ファイルを格納するディレクトリ。</p> <p>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。</p>
キータブファイル	<p>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。</p>
プリンシパル名	<p>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。</p>
偽装ユーザー名	<p>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。</p>

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

第 97 章

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
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。
シークレットコンテナの使用	組織に対して設定されている Secrets Manager にこの接続の機密資格情報を保存します。 このプロパティは、組織に Secrets Manager が設定されている場合にのみ表示されます。 このプロパティは、データ取り込みおよびレプリケーションとデータアクセス管理サービスではサポートされていません。 接続でシークレットコンテナを有効にすると、Secure Agent が Secrets Manager からどの資格情報を取得するかを選択できます。このオプションを無効にした場合、資格情報は組織の設定方法に応じてリポジトリまたはローカル Secure Agent に保存されます。 注: この接続を使用してプッシュダウンまたはプロキシサービスを介してデータアクセスポリシーを適用する場合、シークレットコンテナ設定オプションを使用することはできません。 Secrets Manager を設定および使用方法については、Administrator のヘルプにある「Secrets Manager の設定」を参照してください。
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。

接続プロパティ	説明
JDBC URL *	<p>Hive に接続するための JDBC URL。</p> <p>要件に基づいて、次の形式を指定します。</p> <ul style="list-style-type: none"> - 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>/ <p>注: ポート番号の後にスラッシュを入力します。</p> <ul style="list-style-type: none"> - 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> <p>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。</p>
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*	<p>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。</p> <p>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。</p> <ul style="list-style-type: none"> - 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。
DFS URI *	<p>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。</p> <p>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。</p> <p>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。</p> <p>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。</p>
DFS ステージングディレクトリ	<p>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。</p> <p>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。</p>

接続プロパティ	説明
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	<p>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。</p> <p>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。</p> <pre>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;</pre> <p>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。</p> <pre>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></pre>
* これらのフィールドは必須パラメータです。	

第 98 章

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	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。
シークレットコンテナの使用	組織に対して設定されている Secrets Manager にこの接続の機密資格情報を保存します。 このプロパティは、組織に Secrets Manager が設定されている場合にのみ表示されます。 このプロパティは、データ取り込みおよびレプリケーションとデータアクセス管理サービスではサポートされていません。 接続でシークレットコンテナを有効にすると、Secure Agent が Secrets Manager からどの資格情報を取得するかを選択できます。このオプションを無効にした場合、資格情報は組織の設定方法に応じてリポジトリまたはローカル Secure Agent に保存されます。 注: この接続を使用してプッシュダウンまたはプロキシサービスを介してデータアクセスポリシーを適用する場合、シークレットコンテナ設定オプションを使用することはできません。 Secrets Manager を設定および使用方法については、Administrator のヘルプにある「Secrets Manager の設定」を参照してください。
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。 Secure Agent 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。

第 99 章

IBM MQ 接続のプロパティ

IBM MQ 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、IBM MQ 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。
シークレットコンテナの使用	組織に対して設定されている Secrets Manager にこの接続の機密資格情報を保存します。 このプロパティは、組織に Secrets Manager が設定されている場合にのみ表示されます。 このプロパティは、データ取り込みおよびレプリケーションとデータアクセス管理サービスではサポートされていません。 接続でシークレットコンテナを有効にすると、Secure Agent が Secrets Manager からどの資格情報を取得するかを選択できます。このオプションを無効にした場合、資格情報は組織の設定方法に応じてリポジトリまたはローカル Secure Agent に保存されます。 注: この接続を使用してプッシュダウンまたはプロキシサービスを介してデータアクセスポリシーを適用する場合、シークレットコンテナ設定オプションを使用することはできません。 Secrets Manager を設定および使用する方法については、Administrator のヘルプにある「Secrets Manager の設定」を参照してください。
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。 Secure Agent 環境またはエラスティックランタイム環境を選択します。 ランタイム環境の設定および使用方法の詳細については、Administrator のヘルプにある「ランタイム環境」を参照してください。
ホスト	キューマネージャコンポーネントをホストするマシン。
ポート	キューマネージャコンポーネントに接続するポート番号。
ユーザー名	キューマネージャコンポーネントの接続チャンネルに接続するためのユーザー名。 キューマネージャコンポーネントのチャンネル認証が有効になっていない場合は、ユーザー名を指定しないでください。
パスワード	キューマネージャコンポーネントの接続チャンネルに接続するためのパスワード。 キューマネージャコンポーネントのチャンネル認証が有効になっていない場合は、パスワードを指定しないでください。

プロパティ	説明
キューマネージャ	メッセージを送受信するためにキューをリストする必要があるキューマネージャコンポーネント。
チャンネル	キューマネージャのキューに接続するサーバー接続チャンネル。 キューマネージャコンポーネントのチャンネル認証を有効にしない場合、IBM MQ サービスのデフォルトのユーザーアカウントがデータをターゲットに書き込みます。
コードページ	Secure Agent が IBM MQ に対して読み取りまたは書き込みを行うために使用するキューマネージャコンポーネントのコードページ。 リストから次のいずれかのコードページを選択します。 - UTF-8 - UTF-16 - MS Windows Latin 1 デフォルトは UTF-8 です。
SSL	IBM MQ への接続に SSL ソケットを使用するかどうかを指定します。 デフォルトでは無効になっています。
トラストストアファイルパス	IBM MQ に接続するための証明書を格納する SSL トラストストアファイルのパスとファイル名。 ディレクトリとファイル名を次の形式で指定します。 /root/<folder name>/<truststore file 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にアクセスするためのパスワード。
キーストアファイルパス	IBM MQ との双方向の安全な通信を確立するためのプライベートキーと SSL 証明書を含む SSL キーストアファイルのパスとファイル名。 ディレクトリとファイル名を次の形式で指定します。 /root/<フォルダ名>/<キーストアファイル名>.jks 注: IBM MQ との双方向の安全な通信を確立するには、[トラストストアファイルパス]、[トラストストアパスワード]、および [キーストアパスワード] フィールドに値を入力する必要もあります。
キーストアのパスワード	SSL 証明書を含むキーストアファイルにアクセスするためのパスワード。

プロパティ	説明
メタデータの取得をスキップ	<p>ソースまたはターゲットの設定時に、データ統合で IBM MQ キュー名の取得と一覧表示をバイパスするかどうかを指定します。</p> <ul style="list-style-type: none"> - このオプションを有効にすると、データ統合での IBM MQ キュー名の取得と一覧表示がバイパスされます。代わりに、ソースまたはターゲットの設定時にプレースホルダキュー名がオブジェクトリストに表示されるため、マッピングの詳細ランタイムプロパティでソースまたはターゲットのキュー名を指定する必要があります。 - このオプションが有効ではない場合、マッピングでのソースまたはターゲットの設定時に、データ統合では使用可能なすべての IBM MQ キュー名がオブジェクトリストに取得され、表示されます。 <p>デフォルトでは無効になっています。</p>
暗号スイート	<p>SSL 対応の IBM MQ 接続を IBM MQ に安全に接続するための暗号スイート。</p> <p>暗号スイート名は次の形式で入力します。</p> <p><TLS プロトコル>:<暗号スイート名></p> <p>例えば、暗号プロトコルが TLSv1.2 であるときに TLS_RSA_WITH_AES_128_CBC_SHA256 暗号スイートを使用する場合は、次の値を入力します。</p> <p>TLSv1.2:TLS_RSA_WITH_AES_128_CBC_SHA256</p> <p>注: デフォルトでは、データ統合は、暗号化された接続の暗号プロトコルとして TLSv1.2 を使用します。</p> <p>IBM MQ 接続に使用できる互換性のある暗号スイートのリストについては、IBM MQ のマニュアルの「Cipher specs and cipher suites in IBM MQ classes for Java」を参照してください。</p>

第 100 章

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。
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gger（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。 <i>host_name</i> は、ホスト名または IP アドレスにできます。 <i>host_name:port_number</i> 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gger（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	<p>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。</p> <ul style="list-style-type: none"> - 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。 <p>デフォルトは [なし] です。</p>
ペーシングサイズ	<p>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。</p> <p>デフォルトである最小値は 0 です。</p>
ペーシング単位	<p>[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。</p> <p>[行] または [キロバイト] のいずれかを選択します。</p>
マップの場所	<p>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。</p> <p>この値は、PowerExchange リスナが、抽出マップからリモートにある PowerExchange ログガー（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。</p> <p>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。</p> <p>host_name:port_number</p> <p>以下に例を示します。</p> <p>ADACDC01:25100</p> <p>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。</p>
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。

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	<p>カスタムプロパティまたは接続プロパティのオーバーライド。カスタムプロパティとは、PowerExchange のデフォルトの設定よりも優先するために指定できるプロパティです。セミコロン (;) を区切り文字として使用して複数のプロパティを入力するか、パラメータファイルを使用して接続プロパティの上書きを指定するパラメータを指定することができます。</p> <p>例:</p> <pre><property>=<value>;<property>=<value></pre> <p>多くの場合、Informatica グローバルカスタマサポートからの指示を受けただけで、カスタムプロパティの設定を行います。</p> <p>注: これらのプロパティは、PowerCenter の PowerExchange Client for PowerCenter (PWXPC) CDC 接続の 【PWX オーバーライド】 オプションと同じです。</p> <p>パラメータファイルを使用して接続プロパティのオーバーライドを指定するには、\$<ParameterName>の形式でパラメータを設定し、ユーザー定義パラメータ名の前にドル記号 (\$) を付けます。次に、【ランタイムオプション】 タブの 【パラメータファイル名】 フィールドにパラメータファイル名を指定することで、ユーザー定義パラメータ定義を含むパラメータファイルを使用するようにマッピングのマッピングタスクを設定します。</p> <p>注:</p> <ul style="list-style-type: none"> - マッピングおよび接続に同じパラメータを入力した場合は、接続カスタムプロパティが優先されます。 - パラメータファイルがある場合、このフィールドで指定するパラメータ名は、パラメータファイルで定義されたエントリと一致する必要があります。 <p>詳細については、「接続オーバーライドのリファレンス」の章を参照してください。</p>

第 101 章

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。
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。 <i>host_name</i> は、ホスト名または IP アドレスにできます。 <i>host_name:port_number</i> 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。

プロパティ	説明
オフロード処理	<p>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。</p> <ul style="list-style-type: none"> - 自動。オフロード処理を使用するかどうか 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。 <p>デフォルトは [いいえ] です。</p>
オフロードスレッド	<p>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。</p> <p>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。</p> <p>有効な値は 1~64 です。</p> <p>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。</p> <p>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。</p>
配列サイズ	<p>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）。</p> <p>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。</p> <p>有効な値は 1~5000 です。デフォルトは 25 です。</p> <p>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。</p>
低値をスペースに置き換える	<p>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。</p>
接続リトライ期限	<p>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。</p>

プロパティ	説明
カスタムプロパティ	<p>カスタムプロパティまたは接続プロパティのオーバーライド。カスタムプロパティとは、PowerExchange のデフォルトの設定よりも優先するために指定できるプロパティです。セミコロンの (;) 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。</p> <p>例:</p> <pre><property>=<value>;<property>=<value></pre> <p>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。</p> <p>注: これらのプロパティは、PowerCenter の PowerExchange Client for PWX NRDB Batch 接続の [PWX オーバーライド] オプションと同じです。</p> <p>また、このフィールドまたはパラメータファイルを使用して、接続プロパティのオーバーライドを指定することもできます。パラメータファイルを使用して接続プロパティのオーバーライドを指定するには、<code>\$<ParameterName></code> の形式でパラメータを設定し、ユーザー定義パラメータ名の前にドル記号 (\$) を付けます。次に、[ランタイムオプション] タブの [パラメータファイル名] フィールドにパラメータファイル名を指定することで、ユーザー定義パラメータ定義を含むパラメータファイルを使用するようにマッピングのマッピングタスクを設定します。</p> <p>注:</p> <ul style="list-style-type: none"> - マッピングおよび接続に同じパラメータを入力した場合は、接続カスタムプロパティが優先されます。 - パラメータファイルがある場合、このフィールドで指定するパラメータ名は、パラメータファイルで定義されたエントリと一致している必要があります。 <p>詳細については、「接続オーバーライドのリファレンス」の章を参照してください。</p>
書き込みプロパティ	<p>書き込みモード。次のオプションがあります。</p> <ul style="list-style-type: none"> - 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。 <p>デフォルト値は [書き込み確認オン] です。</p>

第 102 章

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
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。
シークレットコンテナの使用	組織に対して設定されている Secrets Manager にこの接続の機密資格情報を保存します。 このプロパティは、組織に Secrets Manager が設定されている場合にのみ表示されます。 このプロパティは、データ取り込みおよびレプリケーションとデータアクセス管理サービスではサポートされていません。 接続でシークレットコンテナを有効にすると、Secure Agent が Secrets Manager からどの資格情報を取得するかを選択できます。このオプションを無効にした場合、資格情報は組織の設定方法に応じてリポジトリまたはローカル Secure Agent に保存されます。 注: この接続を使用してプッシュダウンまたはプロキシサービスを介してデータアクセスポリシーを適用する場合、シークレットコンテナ設定オプションを使用することはできません。 Secrets Manager を設定および使用する方法については、Administrator のヘルプにある「Secrets Manager の設定」を参照してください。
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。 Secure Agent、ホステッドエージェント、またはサーバーレスランタイム環境を選択します。 ランタイム環境の設定および使用方法の詳細については、Administrator のヘルプにある「ランタイム環境」を参照してください。
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。

プロパティ	説明
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。
ドライバクラス名	<p>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。</p> <ul style="list-style-type: none"> - 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 <p>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。</p>
接続文字列	<p>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。</p> <p>JDBC 接続文字列では、次の構文を使用します。</p> <ul style="list-style-type: none"> - 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	<p>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。</p>

第 103 章

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。

重要: JDBC コネクタは非推奨となり、メンテナンスモードに移行されました。Informatica は将来のリリースでサポートを廃止する予定です。JDBC V2 コネクタを使用して、JDBC タイプ 4 ドライバでデータベースからデータにアクセスすることをお勧めします。

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。 Secure Agent、ホステッドエージェント、またはサーバーレスランタイム環境を選択します。
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。

接続プロパティ	説明
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。

第 104 章

JDBC V2 接続のプロパティ

JDBC V2 接続を作成して、Aurora PostgreSQL または Type 4 JDBC ドライバをサポートする任意のデータベースからデータにアクセスします。

前提条件

JDBC Type 4 ドライバをサポートするデータベースに対して読み取りまたは書き込みを行う JDBC V2 接続を作成する前に、前提条件を満たすようにしてください。

Type 4 JDBC ドライバのインストール

JDBC V2 オブジェクトに対して読み取りまたは書き込みを行うには、Secure Agent マシンに Type 4 JDBC ドライバをインストールする必要があります。

1. データベースがサポートする最新の Type 4 JDBC ドライババージョンを、サードパーティーベンダーのサイトからダウンロードします。

JDBC V2 コネクタを使用して Aurora PostgreSQL に接続する場合は、Aurora PostgreSQL ドライバをダウンロードします。JDBC V2 コネクタ用の Aurora PostgreSQL ドライバ 42.2.6 は、Informatica による認証済みです。

2. データベースの Type 4 JDBC ドライバを Secure Agent マシンにインストールし、次のタスクを実行します。

- a. Secure Agent マシンの次のディレクトリに移動します。
<Secure Agent のインストールディレクトリ>/ext/connectors/thirdparty/

- b. フォルダを作成し、設定するマッピングのタイプに基づいてドライバを追加します。
マッピングの場合は、次のフォルダにドライバを追加します:

`informatica.jdbc_v2/common`

詳細モードのマッピングの場合は、次のフォルダにドライバを追加します:

`informatica.jdbc_v2/common`

`informatica.jdbc_v2/spark`

3. Secure Agent を再起動します。
詳細モードのマッピングの実行中に Secure Agent マシンのドライバを更新する場合は、Secure Agent を再起動する必要があります。

JDBC V2 への接続

JDBC 準拠のデータベースに接続するように JDBC V2 の接続プロパティを設定してみましょう。

始める前に

開始する前に、Secure Agent マシンに Type 4 JDBC ドライバをインストールして、JDBC V2 接続を確立する必要があります。

設定の前提条件の詳細については、「[「前提条件」 \(ページ 365\)](#)」を参照してください。

接続の詳細

次の表に、基本接続プロパティを示します。

財産	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。
シークレットコンテナの使用	組織に対して設定されている Secrets Manager にこの接続の機密資格情報を保存します。 このプロパティは、組織に Secrets Manager が設定されている場合にのみ表示されます。 このプロパティは、データ取り込みおよびレプリケーションとデータアクセス管理サービスではサポートされていません。 接続でシークレットコンテナを有効にすると、Secure Agent が Secrets Manager からどの資格情報を取得するかを選択できます。このオプションを無効にした場合、資格情報は組織の設定方法に応じてリポジトリまたはローカル Secure Agent に保存されます。 注: この接続を使用してプッシュダウンまたはプロキシサービスを介してデータアクセスポリシーを適用する場合、シークレットコンテナ設定オプションを使用することはできません。 Secrets Manager を設定および使用する方法については、Administrator のヘルプにある「Secrets Manager の設定」を参照してください。
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。 Secure Agent、サーバーレスランタイム環境、またはエラスティックランタイム環境を選択します。 データ取り込みおよびレプリケーションでは、ホステッドエージェント、サーバーレスランタイム環境、またはエラスティックランタイム環境でストリーミング取り込みとレプリケーションタスクを実行することはできません。 サーバーレス環境の設定の詳細については、「 「サーバーレスランタイム環境の設定」 (ページ 369) 」を参照してください。 エラスティック環境の設定方法の詳細については、「 「エラスティックランタイム環境の設定」 (ページ 370) 」を参照してください。
JDBC ドライバクラス名	JDBC ドライバクラスの名前。 例えば、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。

財産	説明
接続文字列	<p>データベースへの接続に使用する接続文字列。</p> <p>以下の形式を使用して、接続文字列を指定します: jdbc:<subprotocol>:<subname></p> <p>例えば、Aurora PostgreSQL データベースタイプの接続文字列は、jdbc:postgresql://<ホスト>:<ポート>[/dbname] です。</p> <p>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。</p> <p>詳細モードのマッピングで SSL 対応の Aurora PostgreSQL データベースに接続することもできます。</p> <p>詳細については、「「詳細モードのマッピング用の SSL 対応データベースへの接続」 (ページ 368)」を参照してください。</p>
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。

詳細設定

次の表に、詳細接続のプロパティを示します。

プロパティ	説明
データベースタイプ	<p>接続先のデータベースタイプ。</p> <p>次のいずれかのデータベースタイプを選択します。</p> <ul style="list-style-type: none"> - 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。Type 4 JDBC ドライバをサポートする任意のデータベース（Salesforce Data Cloud など）に接続します。 <p>デフォルトは [その他] です。</p>
スキーマ名	<p>JDBC オブジェクトに使用されるスキーマ名。</p> <p>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。</p> <p>Oracle のパブリックシノニムに対して読み取りまたは書き込みを行うには、「PUBLIC」と入力します。</p>
接続環境 SQL	<p>PostgreSQL データベースに接続する場合に、データベース環境を設定する SQL 文。データベース環境は、この接続を使用するセッション全体に適用されます。</p> <p>例えば、次の文を入力してタイムゾーンを設定できます。</p> <pre>SET timezone to 'America/New_York';</pre>
追加セキュリティプロパティ	<p>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。</p> <p>接続文字列のうち、マスクする部分を指定します。</p> <p>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。</p>

プロパティ	説明
自動コミットを有効化	<p>ドライバが、SQL 文の実行時にデータベースにデータを自動的にコミットする接続をサポートするかどうかを指定します。</p> <p>無効にすると、JDBC ドライバで自動コミットモードが有効になっている場合でも、ドライバはデータを自動的にコミットする接続をサポートしません。</p> <p>デフォルトでは無効になっています。</p> <p>このプロパティは、詳細モードのマッピングには適用されません。</p>
大文字と小文字が混在する識別子をサポート	<p>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。</p> <p>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。</p> <p>デフォルトでは無効になっています。</p>
SQL 識別子文字	<p>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。</p> <p>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。</p> <p>データベースが識別子に使用する区切り文字に基づいて、リストから文字を選択します。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。</p>

詳細モードのマッピング用の SSL 対応データベースへの接続

詳細モードのマッピングで JDBC V2 接続を使用して、SSL 対応の JDBC 準拠データベースに接続できます。SSL 対応の JDBC 準拠データベースを使用して詳細モードでマッピングを実行するには、SSL 証明書を Secure Agent マシンにダウンロードし、特定の前提条件のタスクを実行する必要があります。

- JDBC V2 接続プロパティで JDBC URL を指定します。
SSL 対応の Aurora PostgreSQL データベースに接続するには、次の JDBC URL を指定します：
`jdbc:postgresql://<host>:<port>/dbname?sslmode=verify-ca&sslrootcert=<Secure Agent マシン上の SSL 証明書の場所>。`ここで、`sslmode` の値は `verify-ca` と `verify-ca` をサポートします。
例: `jdbc:postgresql://aurorapostgres-appsdk.abc.ap-south-1.rds.amazonaws.com:5432/JDBC_V2?sslmode=verify-full&sslrootcert=/data/home/qamercury/cloud_td/Aurora_cert/rds-combined-ca-bundle.pem。`
- JDBC V2 接続プロパティで JDBC URL を指定した後に、マッピングタスクの詳細セッションプロパティで、セッションプロパティ名として **advanced.custom.property** を選択します。
- セッションプロパティ値で、次の値を指定します：
`Spark.NeedUserCredentialFileForAdapter=true&Spark.UserCredentialDirOnDIS=<Secure Agent マシン上の SSL 証明書の場所>`
 - `Spark.NeedUserCredentialFileForAdapter` このプロパティを `true` に設定すると、Secure Agent は SSL 証明書を Secure Agent マシンから詳細クラスタにコピーします。
 - `Spark.UserCredentialDirOnDIS` このプロパティを SSL 証明書の場所に設定すると、Secure Agent は指定された場所を使用して SSL 証明書を取得します。
このプロパティはオプションです。このプロパティが指定されていない場合、Secure Agent はデフォルトの場所 `/infa/user/credentials` を考慮します。

サーバーレスランタイム環境の設定

AWS または Azure でホストされているサーバーレスランタイム環境を使用して、JDBC 準拠のデータベースに接続できます。

サーバーレスランタイム環境を使用して安全な JDBC V2 接続を設定する前に、次のタスクを実行します。

- AWS または Azure アカウントの Amazon S3 バケットあるいは Azure コンテナに JDBC ドライバの JAR ファイルを追加します。
- .yaml サーバーレス構成ファイルを設定する。

AWS または Azure アカウントの Amazon S3 バケットあるいは Azure コンテナに JDBC ドライバの JAR ファイルを追加します

サーバーレスランタイム環境で JDBC V2 接続を設定するには、次の手順を実行します。

1. AWS または Azure のサーバーレスエージェント設定用に次の構造を作成します:
<補足ファイルの場所>/serverless_agent_config
2. AWS または Azure アカウントの次の場所にある Amazon S3 バケットあるいは Azure コンテナに JDBC ドライバファイルを追加します:
<補足ファイルの場所>/serverless_agent_config/common
3. 詳細モードでのマッピングの場合は、Amazon S3 バケットまたは Azure コンテナの次の場所に JDBC ドライバファイルを追加します:
<補足ファイルの場所>/serverless_agent_config/spark

.yaml サーバーレス構成ファイルを設定する

サーバーレスランタイム環境で .yaml サーバーレス構成ファイルを設定するには、次の手順を実行します。

1. 次のコードスニペットを、サーバーレス環境で実行するマッピングに基づいてテキストエディタにコピーします。
- 詳細モードで適用されないマッピングの場合は、次のコードスニペットを追加します:

```
version: 1
agent:
  dataIntegrationServer:
    autoDeploy:
      jdbcv2:
        common:
          - fileCopy:
              sourcePath: common/<Driver_filename>
          - fileCopy:
              sourcePath: common/<Driver_filename>
```

- 詳細モードのマッピングの場合は、次のコードスニペットを追加します:

```
version: 1
agent:
  elasticServer:
    autoApply:
      jdbcv2:
        common:
          - fileCopy:
              sourcePath: common/<Driver_filename>
          - fileCopy:
              sourcePath: common/<Driver_filename>
        spark:
          - fileCopy:
              sourcePath: spark/<Driver_filename>
          - fileCopy:
              sourcePath: spark/<Driver_filename>
```

ここで、ソースパスは AWS のドライバファイルのディレクトリパスです。

2. 構文とインデントが有効であることを確認してから、ファイルを `serverlessUserAgentConfig.yml` として次の AWS または Azure の場所に保存します: <補足ファイルの場所>/`serverless_agent_config.yml` ファイルの実行時に、JDBC ドライバファイルが AWS または Azure の場所からサーバーレスエージェントディレクトリにコピーされます。

サーバーレスランタイム環境の設定および使用方法の詳細については、Administrator のヘルプにある「サーバーレスランタイム環境」を参照してください。

エラスティックランタイム環境の設定

エラスティックランタイム環境でカスタムバイナリファイルを設定し、マッピング実行中にランタイム環境でこれらのファイルにアクセスして実行できるようにします。

カスタムバイナリファイルを設定する前に、必ず AWS にエラスティックランタイム環境をデプロイして、Informatica Intelligent Cloud Services 内でデータを処理できる Kubernetes クラスタを作成してください。

エラスティックランタイム環境のデプロイの詳細については、「[Deploy an elastic runtime environment](#)」を参照してください。

エラスティックランタイム環境をデプロイした後、マウントされたディスクにカスタムバイナリファイルを配置し、POST 要求で使用するバイナリファイルの正確なパスをコピーします。

Informatica Intelligent Cloud Services 内でエラスティックランタイム環境に対する次の手順を実行して、カスタムバイナリファイルを管理します。

1. 組織にログインして、セッション ID とランタイム環境 ID を取得します。
2. REST API への POST 呼び出しを行い、セッション ID、ランタイム環境 ID、およびマウントされたディスクから先ほどコピーしたバイナリファイルパスを渡します。
POST 呼び出しの詳細については、『REST API リファレンス』ガイドの「[Supplementary files](#)」を参照してください。

POST 要求の例を次に示します。

```
POST <base URL>/api/v3/RuntimeEnvironment/<runtime environment ID>/ElasticConfig
Content-Type: application/json
Accept: application/json
INFA-SESSION-ID: <SessionId>
{
  "rteId": "rte-12345",
  "specification": {
    "agent": {
      "dataIntegrationServer": {
        "jdbcv2": {
          "common": [{"sourcePath": "<path to binaries>/common1.jar"}],
          "spark": [{"sourcePath": "<path to binaries>/spark1.jar"}]
        }
      }
    }
  }
}
```

POST 呼び出しによって、データ統合サーバーの再起動がトリガされます。

3. Administrator でデータ統合サーバーのステータスを確認して、エラスティックランタイム環境が実行されていることを確認します。
4. 接続をテストするか、マッピングを実行して、エラスティックランタイム環境でカスタムバイナリファイルにアクセスして使用できることを確認します。

第 105 章

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	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。
シークレットコンテナの使用	組織に対して設定されている Secrets Manager にこの接続の機密資格情報を保存します。 このプロパティは、組織に Secrets Manager が設定されている場合にのみ表示されます。 このプロパティは、データ取り込みおよびレプリケーションとデータアクセス管理サービスではサポートされていません。 接続でシークレットコンテナを有効にすると、Secure Agent が Secrets Manager からどの資格情報を取得するかを選択できます。このオプションを無効にした場合、資格情報は組織の設定方法に応じてリポジトリまたはローカル Secure Agent に保存されます。 注: この接続を使用してプッシュダウンまたはプロキシサービスを介してデータアクセスポリシーを適用する場合、シークレットコンテナ設定オプションを使用することはできません。 Secrets Manager を設定および使用する方法については、Administrator のヘルプにある「Secrets Manager の設定」を参照してください。
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。 Secure Agent 環境またはエラスティックランタイム環境を選択します。 ランタイム環境の設定および使用方法の詳細については、Administrator のヘルプにある「ランタイム環境」を参照してください。
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。

第 106 章

JMS 接続のプロパティ

JMS に対してデータの安全な読み取りまたは書き込みを行うための JMS 接続を作成します。

前提条件

接続プロパティを構成する前に、JMS プロバイダ固有のサードパーティクライアントライブラリを次の場所にコピーし、クライアントライブラリをコピーした後に、セキュアエージェントを再起動してください。

<Informatica Secure Agent installation directory>/ext/connectors/thirdparty/infa.jms

フォルダ構造がまだ存在しない場合は作成します。

必要なサードパーティクライアントライブラリの詳細については、JMS プロバイダのドキュメントを参照してください。

JMS への接続

JMS に接続するように JMS 接続プロパティを設定してみましょう。

始める前に

開始する前に、JNDI 命名プロバイダ、JNDI コンテキストファクトリ、および JMS 接続の資格情報の詳細を手元に用意しておく必要があります。

接続を設定する前に、[「前提条件」 \(ページ 372\)](#)を参照して要件を確認してください。

接続の詳細

次の表に、基本接続プロパティを示します。

プロパティ	説明
接続名	接続の名前。 各接続名は組織内で一意である必要があります。接続名には、英数字、スペース、および次の特殊文字を含めることができます。_ . + , 最大長は 255 文字です。
説明	接続の説明。最大長は 4000 文字です。
シークレットコンテナの使用	組織に対して設定されている Secrets Manager にこの接続の機密資格情報を保存します。 このプロパティは、組織に Secrets Manager が設定されている場合のみ表示されます。 このプロパティは、データ取り込みおよびレプリケーションとデータアクセス管理サービスではサポートされていません。 接続でシークレットコンテナを有効にすると、Secure Agent が Secrets Manager からどの資格情報を取得するかを選択できます。このオプションを無効にした場合、資格情報は組織の設定方法に応じてリポジトリまたはローカル Secure Agent に保存されます。 注: この接続を使用してプッシュダウンまたはプロキシサービスを介してデータアクセスポリシーを適用する場合、シークレットコンテナ設定オプションを使用することはできません。 Secrets Manager を設定および使用する方法については、Administrator のヘルプにある「Secrets Manager の設定」を参照してください。
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。 Secure Agent を選択します。 ストリーミング取り込みおよびレプリケーション向けのセキュアエージェントを選択します。
接続 URL	JNDI 命名プロバイダの URL。 次の形式で URL を指定します。 protocol://hostname:port 例: tcp://INWV201:61616 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	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	JNDI コンテキストファクトリに接続するためのパスワード。
JNDI コンテキストファクトリ	JNDI サービスに接続できる完全修飾クラス名。 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。

プロパティ	説明
JNDI パッケージプレフィックス	<p>適切なコンテキストファクトリクラスを識別してロードするために JNDI コンテキストファクトリに設定するパッケージ名プレフィックスのコロン区切りリスト。</p> <p>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。</p> <p>例えば、<code>java.naming.factory.url.pkgs=org.apache.activemq.jndi</code> です</p> <p>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。</p>
JMS 接続ファクトリ	<p>JMS クライアントが接続を作成するために使用する JNDI オブジェクトの名前。</p> <p>例えば、<code>jms/QCF</code> または <code>jmsSalesSystem</code> です。</p>
接続ユーザー名	JMS 接続ファクトリに接続するために JMS プロバイダを認証するユーザー名。
接続パスワード	JMS 接続ファクトリに接続するために JMS プロバイダを認証するパスワード。

第 107 章

JIRA 接続のプロパティ

JIRA 接続を作成して JIRA に接続し、JIRA との間でデータの読み取りおよび書き込みを行うことができるようになります。JIRA 接続を使用すると、同期タスク、マッピング、およびマッピングタスクでソースオブジェクトまたはターゲットオブジェクトを指定できます。

Jira への接続

JIRA に接続するように JIRA 接続プロパティを設定してみましょう。

始める前に

接続を設定する前に、Jira アカウントからユーザー名、パスワード、ベース URL を取得する必要があります。次のビデオは、必要な情報を取得する方法を示しています。



接続の詳細

次の表に、基本接続プロパティを示します。

財産	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。

財産	説明
シークレットコンテナの使用	<p>組織に対して設定されている Secrets Manager にこの接続の機密資格情報を保存します。このプロパティは、組織に Secrets Manager が設定されている場合にのみ表示されます。このプロパティは、データ取り込みおよびレプリケーションとデータアクセス管理サービスではサポートされていません。</p> <p>接続でシークレットコンテナを有効にすると、Secure Agent が Secrets Manager からどの資格情報を取得するかを選択できます。このオプションを無効にした場合、資格情報は組織の設定方法に応じてリポジトリまたはローカル Secure Agent に保存されます。</p> <p>注: この接続を使用してプッシュダウンまたはプロキシサービスを介してデータアクセスポリシーを適用する場合、シークレットコンテナ設定オプションを使用することはできません。</p> <p>Secrets Manager を設定および使用方法については、Administrator のヘルプにある「Secrets Manager の設定」を参照してください。</p>
ランタイム環境	<p>タスクを実行するランタイム環境の名前。</p> <p>Secure Agent、ホステッドエージェント、サーバーレスランタイム環境、またはエラスティックランタイム環境を選択します。</p> <p>ホステッドエージェントは、詳細モードのマッピングには適用されません。</p> <p>ホステッドエージェントまたはサーバーレスランタイム環境では、アプリケーション取り込みタスクとデータベース取り込みタスクを実行できません。</p> <p>ランタイム環境の設定および使用方法の詳細については、Administrator のヘルプにある「ランタイム環境」を参照してください。</p>
ユーザー名	JIRA アカウントのユーザー名。
パスワード	JIRA アカウントのパスワード。
URI	<p>Jira インスタンスのベース URL。</p> <p>例えば、JIRA インスタンスが mycompany.atlassian.net でホストされている場合、URI は https://mycompany.atlassian.net/ になります。</p>

詳細設定

次の表に、詳細接続のプロパティを示します。

プロパティ	説明
UTC オフセット	<p>タイムゾーンの時刻を表すように、協定世界時 (UTC) を datetime フィールドに追加します。タイムゾーンに基づいてリストから UTC オフセットを選択します。</p> <p>UTC への調整を行うと、地域に基づいてローカルタイムが生成されます。UTC は UTC±として表され、UTC より進んでいる時間を示すプラス記号 (+) と UTC より遅れている時間を示すマイナス記号 (-) が付記されます。例えば、現在地が UTC より 5 時間進んでいる場合は、[UTC +5] を選択します。現在地が UTC より 3 時間遅れている場合は、[UTC-3] を選択します。デフォルトは UTC です。</p>
ロギングの有効化	<p>コネクタのログ記録を有効にします。</p> <p>このチェックボックスをオンにすると、接続の作成時にログ記録が有効になり、その接続を使用してメタデータのインポートやタスクの実行を行います。</p> <p>Tomcat の接続ログと設計時ログには、<Secure Agent のインストールディレクトリ>\apps\Data_Integration_Server\logs\tomcat からアクセスすることができます。</p> <p>ランタイムログについては、[マイジョブ] ページのセッションログを参照してください。</p>

第 108 章

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。

重要: JSON Target コネクタは非推奨となり、メンテナンスモードに移行されました。Informatica は将来のリリースでサポートを廃止する予定です。JSON ターゲットへのアクセスには Hadoop Files V2 コネクタを使用することを推奨します。

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	リストから該当する 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。

第 109 章

Kafka 接続のプロパティ

Kafka 接続のセットアップ時に、接続プロパティを設定します。

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。
シークレットコンテナの使用	組織に対して設定されている Secrets Manager にこの接続の機密資格情報を保存します。このプロパティは、組織に Secrets Manager が設定されている場合にのみ表示されます。このプロパティは、データ取り込みおよびレプリケーションとデータアクセス管理サービスではサポートされていません。 接続でシークレットコンテナを有効にすると、Secure Agent が Secrets Manager からどの資格情報を取得するかを選択できます。このオプションを無効にした場合、資格情報は組織の設定方法に応じてリポジトリまたはローカル Secure Agent に保存されます。 注: この接続を使用してプッシュダウンまたはプロキシサービスを介してデータアクセスポリシーを適用する場合、シークレットコンテナ設定オプションを使用することはできません。 Secrets Manager を設定および使用方法については、Administrator のヘルプにある「Secrets Manager の設定」を参照してください。
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。 詳細クラスターで実行されるマッピングに対して、Secure Agent、サーバーレスランタイム環境、またはエラスティックランタイム環境を指定します。 データ取り込みおよびレプリケーションでは、アプリケーション取り込みとレプリケーションタスク、ファイル取り込みとレプリケーションタスク、およびストリーミング取り込みとレプリケーションタスクで Secure Agent を使用できます。データベース取り込みとレプリケーションタスクでは、Secure Agent またはサーバーレスランタイム環境を使用できます。 ランタイム環境の設定および使用方法の詳細については、Administrator のヘルプにある「ランタイム環境」を参照してください。

プロパティ	説明
Kafka Broker リスト	<p>Kafka Broker のカンマ区切りリスト。</p> <p>Kafka Broker を一覧表示するには、次の形式を使用します。</p> <p><code><HostName>:<PortNumber></code></p> <p>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。</p>
再試行タイムアウト	<p>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。</p> <p>デフォルトは 180 秒です。</p> <p>このプロパティは、データベース取り込みとレプリケーション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。</p>
Kafka Broker のバージョン	<p>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。</p> <p>ストリーミング取り込みとレプリケーションタスクではオプションです。</p>
追加接続プロパティ	<p>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。</p> <p>ストリーミング取り込みとレプリケーションタスクで <code><Security Protocol></code> を SASL_PLAINTEXT または SASL_SSL に設定する場合は、<code><kerberos name></code> プロパティを設定してください。</p> <p>データベース取り込みとレプリケーションタスクでセキュリティプロトコルとプロパティを指定する場合は、[追加セキュリティプロパティ] プロパティではなく、ここで指定します。例: <code>security.protocol=SSL,ssl.truststore.location=/opt/kafka/config/kafka.truststore.jks,ssl.truststore.password=<truststore_password></code></p>
Confluent スキーマレジストリの URL	<p>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。</p> <p>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。</p> <p><code><https>://<HostName or IP>:<PortNumber></code></p> <p>または</p> <p><code><http>://<HostName or IP>:<PortNumber></code></p> <p>スキーマレジストリの URL の例:</p> <p><code>https://kafkarnd.informatica.com:8082</code></p> <p>または</p> <p><code>http://10.65.146.181:8084</code></p> <p>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。</p> <p>このプロパティは、データベース取り込みとレプリケーション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。</p>
SSL モード	<p>必須。接続に使用する暗号化タイプを決定します。</p> <p>次の SSL モードからモードを選択できます。</p> <ul style="list-style-type: none"> - 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。 <p>このプロパティは、データベース取り込みとレプリケーション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。</p>

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。

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。これらのプロパティは、詳細モードのマッピングにのみ適用されます。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。 <ul style="list-style-type: none"> - 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、データベース取り込みとレプリケーションでは使用されません。[追加接続プロパティ] で同等の Kafka プロパティを指定できます。
SSL TrustStore ファイルパス スキーマレジストリ ¹	一方向または双方向 SSL モードを使用するときは必須です。 Confluent スキーマレジストリに接続するための SSL 証明書を格納する SSL トラストストアファイルの絶対パスとファイル名。
SSL TrustStore パスワード スキーマレジストリ ¹	一方向または双方向 SSL モードを使用するときは必須です。 SSL トラストストアのパスワード。

プロパティ	説明
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 ²	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。 <code>basic.auth.credentials.source=USER_INFO,basic.auth.user.info=<username>:<password></code> 【追加接続プロパティ】と【追加のセキ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、データベース取り込みとレプリケーションでは使用されません。
¹ 詳細モードのマッピングにのみ適用されます。 ² マッピングおよび詳細モードのマッピングに適用されます。	

第 110 章

Klaviyo 接続のプロパティ

Klaviyo 接続を作成する際には、接続プロパティを設定します。

重要: 2024 年 11 月リリースから、Klaviyo コネクタは非推奨となり、メンテナンスモードに移行されました。Informatica は将来のリリースでサポートを廃止する予定です。

次の表に、Klaviyo 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	接続の名称。 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	Klaviyo
ランタイム環境	タスクを実行するランタイム環境の名称。 Secure Agent または Hosted Agent を指定できます。
プライベート API キー	Klaviyo アカウントへのアクセスを認証するための Klaviyo プライベート API キー。 プライベートキーの詳細については、Klaviyo のマニュアルを参照してください。

第 111 章

大規模言語モデル接続のプロパティ

Azure OpenAI に接続するための大規模言語モデル接続を作成します。Azure OpenAI のチャットモデルを使用して、インテリジェント構造モデル内の非構造化データを処理および解釈することができます。埋め込みモデルを使用して、ベクトル埋め込みトランスフォーメーションでベクトル埋め込みを生成します。

注: 大規模言語モデル接続は、大規模言語モデルとのインタフェース用に特別に設計されています。この接続は、インテリジェント構造モデルとベクトル埋め込みトランスフォーメーション内でのみ使用できます。この接続を使用して、他のコネクタがデータベースまたはファイルを処理する方法でモデルに対して直接読み取りまたは書き込みを行うことはできません。

認証の準備

大規模言語モデル接続を設定する前に、Azure ポータルから Azure OpenAI アカウントの API キーとエンドポイント URL を取得する必要があります。

API キーの取得

Azure OpenAI チャットモデルまたは埋め込みモデルへの API 呼び出しを行うには、API キーとエンドポイント URL が必要です。

1. Azure ポータルにログインし、Azure OpenAI サービスを開きます。
2. 接続先の Azure OpenAI リソースの名前をクリックします。
3. **【概要】** ページで、**【Azure AI Foundry ポータルを参照】** をクリックします。
4. **【共有リソース】** で、**【デプロイメント】** をクリックします。
5. **【モデルデプロイメント】** タブで、API キーとエンドポイント URL が必要なチャットモデルまたは埋め込みモデルの名前をクリックします。
6. **【詳細】** タブで、キーとエンドポイント URL をコピーします。

大規模言語モデルへの接続

Azure OpenAI に接続するように大規模言語モデル接続を設定してみましょう。Azure OpenAI のチャットモデルを使用して、インテリジェント構造モデル内の非構造化データを処理および解釈することができます。埋め込みモデルを使用して、ベクトル埋め込みトランスフォーメーションでベクトル埋め込みを生成します。

注: 大規模言語モデル接続は、大規模言語モデルとのインタフェース用に特別に設計されています。この接続は、インテリジェント構造モデルとベクトル埋め込みトランスフォーメーション内でのみ使用できます。この接続を使用して、他のコネクタがデータベースまたはファイルを処理する方法でモデルに対して直接読み取りまたは書き込みを行うことはできません。

始める前に

大規模言語モデル接続を作成する前に、Azure OpenAI アカウントの API キーとエンドポイント URL を取得する必要があります。

接続を設定する前に、[Prepare for authentication \(ページ 383\)](#) を参照して認証要件を確認してください。

Azure OpenAI のチャットモデルを使用してインテリジェント構造モデルを生成する場合は、API とデータのやり取りを行ってデータを前処理するために Python 統合を有効にする必要があります。

Python 統合を有効にする方法の詳細については、データ統合のマニュアルの「コンポーネント」を参照してください。

接続の詳細

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。 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。
シークレットコンテナの使用	組織に対して設定されている Secrets Manager にこの接続の機密資格情報を保存します。 このプロパティは、組織に Secrets Manager が設定されている場合にのみ表示されます。 このプロパティは、データ取り込みおよびレプリケーションとデータアクセス管理サービスではサポートされていません。 接続でシークレットコンテナを有効にすると、Secure Agent が Secrets Manager からどの資格情報を取得するかを選択できます。このオプションを無効にした場合、資格情報は組織の設定方法に応じてリポジトリまたはローカル Secure Agent に保存されます。 注: この接続を使用してプッシュダウンまたはプロキシサービスを介してデータアクセスポリシーを適用する場合、シークレットコンテナ設定オプションを使用することはできません。 Secrets Manager を設定および使用する方法については、Administrator のヘルプにある「Secrets Manager の設定」を参照してください。
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。 Secure Agent 環境またはエラスティックランタイム環境を選択します。 [ホステッドエージェント] は適用されません。

プロパティ	説明
モデルカテゴリ	<p>大規模言語モデルのタイプ。</p> <p>次のいずれかのオプションを選択します。</p> <ul style="list-style-type: none"> - チャット。会話 API を使用して、インテリジェント構造モデル内の非構造化データを処理および解釈します。 - 埋め込み。テキスト埋め込み API を使用して、ベクトル埋め込みトランスフォーメーションでベクトル埋め込みを生成します。
モデルプロバイダ	<p>大規模言語モデルのプロバイダ。</p> <p>[Azure OpenAI] を選択します。</p>
認証	<p>選択したモデルプロバイダに接続するための認証タイプ。</p> <p>[API キー] を選択します。</p>
エンドポイント	<p>モデルプロバイダによって提供された大規模言語モデル API のエンドポイント URL。</p> <p>チャットモデルの例:</p> <p><code>https://<RESOURCE_NAME>/openai/deployments/<DEPLOYMENT_NAME>/chat/completions?api-version=<API_VERSION></code></p> <p>埋め込みモデルの例:</p> <p><code>https://<RESOURCE_NAME>/openai/deployments/<DEPLOYMENT_NAME>/embeddings?api-version=<API_VERSION></code></p>
API キー	<p>大規模言語モデル API へのアクセスを認証するために使用するアカウントの API キー。</p>

第 112 章

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
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。
シークレットコンテナの使用	組織に対して設定されている Secrets Manager にこの接続の機密資格情報を保存します。 このプロパティは、組織に Secrets Manager が設定されている場合にのみ表示されます。 このプロパティは、データ取り込みおよびレプリケーションとデータアクセス管理サービスではサポートされていません。 接続でシークレットコンテナを有効にすると、Secure Agent が Secrets Manager からどの資格情報を取得するかを選択できます。このオプションを無効にした場合、資格情報は組織の設定方法に応じてリポジトリまたはローカル Secure Agent に保存されます。 注: この接続を使用してプッシュダウンまたはプロキシサービスを介してデータアクセスポリシーを適用する場合、シークレットコンテナ設定オプションを使用することはできません。 Secrets Manager を設定および使用する方法については、Administrator のヘルプにある「Secrets Manager の設定」を参照してください。
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。 Secure Agent 環境またはエラスティックランタイム環境を選択します。 ランタイム環境の設定および使用方法の詳細については、Administrator のヘルプにある「ランタイム環境」を参照してください。
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。

プロパティ	説明
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。
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。

第 113 章

Magento V1 接続のプロパティ

Magento V1 接続を作成するときは、接続プロパティを設定します。

Magento には次の認証方法を使用して接続できます。

- トークン。Magento アカウントのユーザー名、パスワード、およびストア URL を使用して Magento に接続します。
- OAuth 1.0。OAuth 1.0 プロトコルをストア URL、コンシューマキー、コンシューマシークレット、アクセストークン、およびトークンシークレットとともに使用して、Magento に接続します。

第 114 章

Mailchimp 接続のプロパティ

Mailchimp 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、Mailchimp 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。
シークレットコンテナの使用	組織に対して設定されている Secrets Manager にこの接続の機密資格情報を保存します。 このプロパティは、組織に Secrets Manager が設定されている場合にのみ表示されます。 このプロパティは、データ取り込みおよびレプリケーションとデータアクセス管理サービスではサポートされていません。 接続でシークレットコンテナを有効にすると、Secure Agent が Secrets Manager からどの資格情報を取得するかを選択できます。このオプションを無効にした場合、資格情報は組織の設定方法に応じてリポジトリまたはローカル Secure Agent に保存されます。 注: この接続を使用してプッシュダウンまたはプロキシサービスを介してデータアクセスポリシーを適用する場合、シークレットコンテナ設定オプションを使用することはできません。 Secrets Manager を設定および使用する方法については、Administrator のヘルプにある「Secrets Manager の設定」を参照してください。
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。 Secure Agent または Hosted Agent を指定できます。
サーバープレフィックス	Mailchimp アカウントのデータセンターに対応する URL のサーバーパラメータ。 例えば、<https://us19.admin.mailchimp.com>の場合、us19 がサーバープレフィックスです。
API キー	アカウントへのアクセスを認証するための Mailchimp API キー。 API キーを生成するユーザーのロールによって、各 Mailchimp エンドポイントへのアクセスが決まります。

第 115 章

Marketo V3 接続のプロパティ

Marketo との間でデータの安全な読み取りまたは書き込みを行うための Marketo V3 接続を作成します。

Marketo への接続

Marketo に接続するように Marketo V3 接続プロパティを設定してみましょう。

始める前に

接続を設定する前に、API ユーザーを作成し、そのユーザーを API ロールに関連付けて、Marketo REST API のアクセス権限を付与します。また、Marketo カスタムサービスを認証するには、Marketo アカウントからクライアント ID、クライアントシークレット、REST API URL を取得する必要があります。API ユーザーを作成し、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方法の詳細については、Marketo のマニュアルの「[Custom Services](#)」を参照してください。

次のビデオは、必要な情報を取得する方法を示しています。



接続の詳細

次の表に、基本接続プロパティを示します。

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

プロパティ	説明
シークレット コンテナの使用	<p>組織に対して設定されている Secrets Manager にこの接続の機密資格情報を保存します。このプロパティは、組織に Secrets Manager が設定されている場合にのみ表示されます。このプロパティは、データ取り込みおよびレプリケーションとデータアクセス管理サービスではサポートされていません。</p> <p>接続でシークレットコンテナを有効にすると、Secure Agent が Secrets Manager からどの資格情報を取得するかを選択できます。このオプションを無効にした場合、資格情報は組織の設定方法に応じてリポジトリまたはローカル Secure Agent に保存されます。</p> <p>注: この接続を使用してプッシュダウンまたはプロキシサービスを介してデータアクセスポリシーを適用する場合、シークレットコンテナ設定オプションを使用することはできません。</p> <p>Secrets Manager を設定および使用方法については、Administrator のヘルプにある「Secrets Manager の設定」を参照してください。</p>
ランタイム環境	<p>タスクを実行するランタイム環境の名前。</p> <p>Secure Agent、ホステッドエージェント、サーバーレスランタイム環境、またはエラスティックランタイム環境を選択します。</p> <p>注: アプリケーション取り込みとレプリケーションタスクでは、Secure Agent またはサーバーレスランタイム環境を選択できます。ホステッドエージェントまたはエラスティックランタイム環境は使用できません。</p> <p>ランタイム環境の設定および使用方法の詳細については、Administrator のヘルプにある「ランタイム環境」を参照してください。</p>
クライアント ID	<p>Marketo サービスのクライアント ID。</p> <p>Marketo サービスへのアクセスを認証するためのアクセストークンを生成するには、クライアント ID が必要です。</p>
クライアントシークレット	<p>Marketo サービスのクライアントシークレット。</p>
REST API URL	<p>Marketo REST API に接続するための URL。</p> <p>URL は次の形式で入力します: https://<Marketo Rest API Server のホスト名>。</p>

詳細設定

次の表に、詳細接続のプロパティを示します。

プロパティ	説明
grant_type	<p>管理者が Marketo REST API を呼び出して Marketo に対して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。</p> <p>認証タイプとして client_credentials と入力します。認証タイプが指定されていない場合、エラーが発生し、接続が失敗します。</p>
プロキシのバイパス	<p>Secure Agent が Marketo への接続に proxy.ini ファイルまたは Secure Agent Manager で定義されたプロキシサーバー設定を使用するかどうかを示します。</p> <p>「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。「プロキシをバイパス」を選択しない場合は、プロキシサーバーを使用して Marketo に接続します。</p> <p>デフォルトでは有効になっています。</p> <p>注: このプロパティは、アプリケーション取り込みとレプリケーションタスク用に設定された接続には適用されません。</p>

プロキシサーバーの設定

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

Windows および Linux で、プロキシサーバーを使用するように Secure Agent を設定できます。

認証されていないプロキシサーバーまたは認証されたプロキシサーバーを使用できます。マッピングおよび詳細モードのマッピングで使用される接続に対してプロキシを設定できます。

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

- Windows の場合は Secure Agent Manager を使用し、Linux の場合はシェルコマンドを使用して Secure Agent を設定します。
手順については、データ統合のヘルプの『または「Windows でのプロキシ設定」または「Linux でのプロキシ設定」を参照してください。
- Secure Agent のプロパティで、DTM の JVM オプションを設定します。手順については、ナレッジベースの記事「[Proxy server settings](#)」を参照してください。

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するには、接続の詳細設定で「プロキシのバイパス」を選択します。

第 116 章

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
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。
シークレットコンテナの使用	組織に対して設定されている Secrets Manager にこの接続の機密資格情報を保存します。 このプロパティは、組織に Secrets Manager が設定されている場合にのみ表示されます。 このプロパティは、データ取り込みおよびレプリケーションとデータアクセス管理サービスではサポートされていません。 接続でシークレットコンテナを有効にすると、Secure Agent が Secrets Manager からどの資格情報を取得するかを選択できます。このオプションを無効にした場合、資格情報は組織の設定方法に応じてリポジトリまたはローカル Secure Agent に保存されます。 注: この接続を使用してプッシュダウンまたはプロキシサービスを介してデータアクセスポリシーを適用する場合、シークレットコンテナ設定オプションを使用することはできません。 Secrets Manager を設定および使用する方法については、Administrator のヘルプにある「Secrets Manager の設定」を参照してください。
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。
ユーザー名	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。 トークンベースの認証を使用して NetSuite にアクセスする場合は省略可能です。

接続プロパティ	説明
データソース名	システム DSN 名。
コードページ	<p>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。</p> <ul style="list-style-type: none"> - 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。

第 117 章

Microsoft Azure Analysis Services 接続のプロパティ

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

認証の準備

Microsoft Azure Analysis Services にアクセスするために、管理者ユーザー認証タイプおよびサービスプリンシパル認証タイプを設定できます。認証を設定する前に、環境の設定を行い、認証の詳細を取得しておく必要があります。

ストレージアカウントの作成とアクセスの設定

Microsoft Azure Analysis Services にアクセスするには、次の手順に従って環境を設定します。

- 次のいずれかの認証タイプを使用して、ソースシステムにアクセスする組織を認証してください。
 - 管理者ユーザー。Microsoft Azure Analysis Services で認証にユーザー名とパスワードが許可されている場合に必要です。
 - サービスプリンシパル。Microsoft Azure Analysis Services が認証に Microsoft Entra ID サービスプリンシパル（以前の Azure Active Directory）を使用する場合に必要です。
- 管理者特権を持つユーザーを使用してサービスに対して組織を認証する場合は、ユーザーアカウントを作成します。
- サービスプリンシパル認証を使用してサービスに対して組織を認証する場合は、Microsoft Entra アプリケーションを登録し、サービスプリンシパルを作成します。
- Azure Analysis Services サーバー管理操作を実行するには、サービスプリンシパルをサーバー管理者ロールに追加します。

注: サービスプリンシパルをサーバー管理者ロールに直接追加します。サービスプリンシパルをセキュリティグループに追加してから、そのセキュリティグループをサーバー管理者ロールに追加することはできません。

認証の詳細の取得

使用する認証方法に基づいて、必要なすべての認証詳細を取得していることを確認します。

管理者ユーザー

Microsoft Azure Analysis Services インスタンスに接続するには、Azure Active Directory に登録されているアプリケーションのクライアント ID、ユーザー名、およびパスワードが必要です。

サービスプリンシパル

Azure Active Directory に登録されているアプリケーションのクライアント ID、クライアントシークレット、およびテナント ID が必要です。

Microsoft Azure Analysis Services への接続

Microsoft Azure Analysis Services に接続するように Microsoft Azure Analysis Services 接続プロパティを設定します。

始める前に

開始する前に、設定する接続モードに基づいて、Microsoft Azure Analysis Services アカウントから情報を取得する必要があります。

認証の前提条件の詳細については、「[「認証の準備」 \(ページ 395\)](#)」を参照してください。

接続の詳細

次の表に、基本接続プロパティを示します。

プロパティ	説明
シークレットコンテナの使用	組織に対して設定されている Secrets Manager にこの接続の機密資格情報を保存します。 このプロパティは、組織に Secrets Manager が設定されている場合にのみ表示されます。 このプロパティは、データ取り込みおよびレプリケーションとデータアクセス管理サービスではサポートされていません。 接続でシークレットコンテナを有効にすると、Secure Agent が Secrets Manager からどの資格情報を取得するかを選択できます。このオプションを無効にした場合、資格情報は組織の設定方法に応じてリポジトリまたはローカル Secure Agent に保存されます。 注: この接続を使用してプッシュダウンまたはプロキシサービスを介してデータアクセスポリシーを適用する場合、シークレットコンテナ設定オプションを使用することはできません。 Secrets Manager を設定および使用する方法については、Administrator のヘルプにある「Secrets Manager の設定」を参照してください。
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。
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選択します。
認証タイプ	接続に使用する認証タイプ。接続に使用するオプションを [管理者ユーザー] または [サービスプリンシパル] から選択します。
サーバー名	Microsoft Azure Analysis Services インスタンスの一意の識別子。

認証タイプ

管理者ユーザー認証タイプまたはサービスプリンシパル認証タイプを使用するように Microsoft Azure Analysis Services 接続を設定できます。

必要な認証タイプを選択し、認証固有のパラメータを設定します。

管理者ユーザー認証

管理者ユーザー認証には、Microsoft Azure Analysis Services アカウントのユーザー名とパスワードが必要です。

次の表に、管理者ユーザー認証の接続プロパティとその説明を示します。

プロパティ	説明
ユーザー名	Microsoft Azure Analysis Services インスタンスに接続するための完全修飾ユーザー名。
パスワード	ユーザー名のパスワード

サービスプリンシパル認証

サービスプリンシパル認証には、Azure Active Directory に登録されているアプリケーションのテナント ID とクライアントシークレットが必要です。

次の表に、サービスプリンシパル認証の接続プロパティとその説明を示します。

プロパティ	説明
クライアント ID	サービスプリンシパル認証を完了するための登録済みのアプリケーションのクライアント ID またはアプリケーション ID。
テナント ID	サービスプリンシパル認証を完了するための登録済みのアプリケーションのテナント ID。
クライアントシークレット	サービスプリンシパル認証を完了するために接続するクライアントシークレットキー。

第 118 章

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

Microsoft Azure Blob Storage 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。

重要: Microsoft Azure Blob Storage V2 コネクタは非推奨となり、メンテナンスモードに移行されました。Informatica は将来のリリースでサポートを廃止する予定です。Microsoft Azure Blob Storage V3 コネクタを使用して Microsoft Azure Blob Storage にアクセスすることをお勧めします。

以下の表に、Microsoft Azure Blob Storage 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 Storage アカウント名。
アカウントキー	Microsoft Azure Blob Storage アクセスキー。
コンテナ名	Microsoft Azure Blob Storage コンテナ名。

第 119 章

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

Microsoft Azure Blob Storage V3 接続を作成して、Microsoft Azure Blob Storage に対してデータの読み取りや書き込みを行うことができます。

認証の準備

Microsoft Azure Blob Storage V3 接続で共有キー認証または Shared Access Signature 認証を使用して、Microsoft Azure Blob Storage に接続できます。

認証を設定してする前に、Microsoft Azure Blob Storage で使用するストレージアカウントを作成し、そのストレージアカウントに BLOB コンテナを作成します。ストレージアカウントと BLOB コンテナの作成方法の詳細については、Informatica How-To ライブラリの記事、[「Prerequisites to create a Microsoft Azure Blob Storage V3 connection」](#)を参照してください。

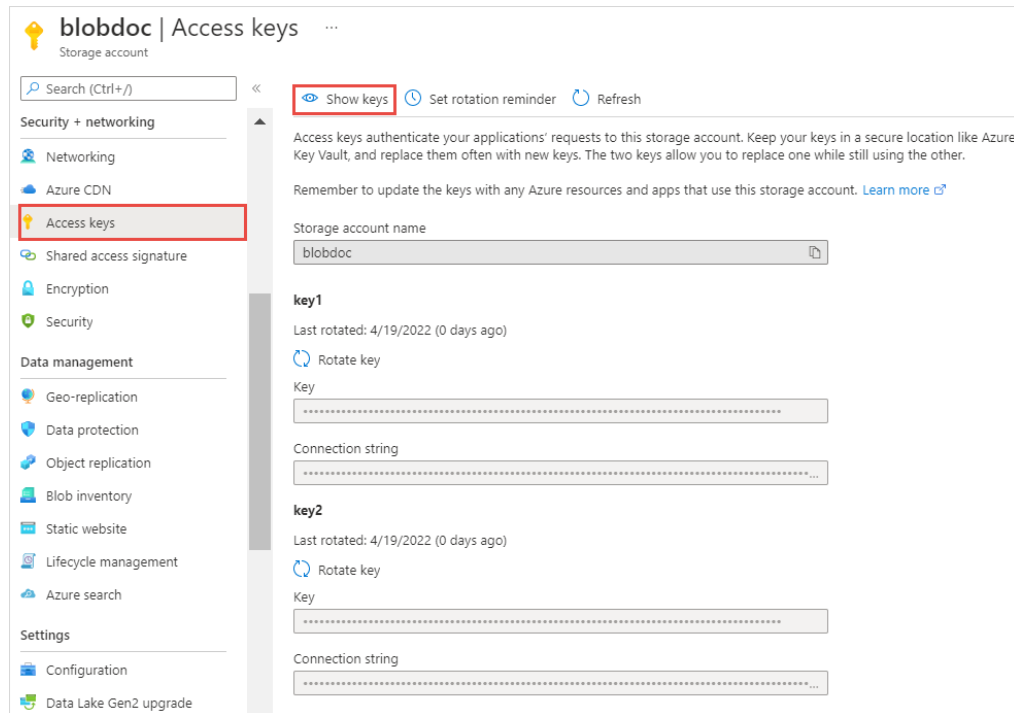
接続プロパティを設定する前に、使用する認証のタイプに基づいて認証の詳細を手元に用意しておく必要があります。

共有キー認証

共有キー認証を使用して Microsoft Azure Blob Storage に接続するには、ストレージアカウント名とアカウントキーが必要です。

1. ストレージアカウントを開きます。
2. **【セキュリティ + ネットワーク】** で、**【アクセスキー】** をクリックします。

3. [キーを表示] をクリックします。



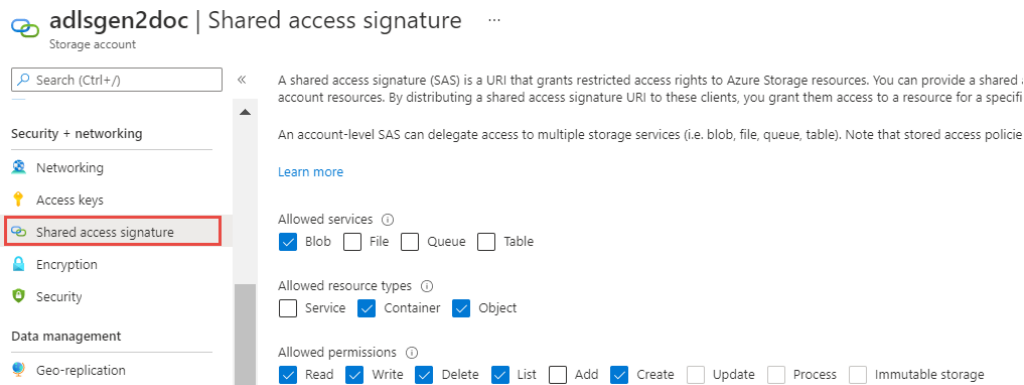
4. ストレージアカウント名とアカウントキーをメモします。key1 または key2 を使用することができます。

共有アクセス署名

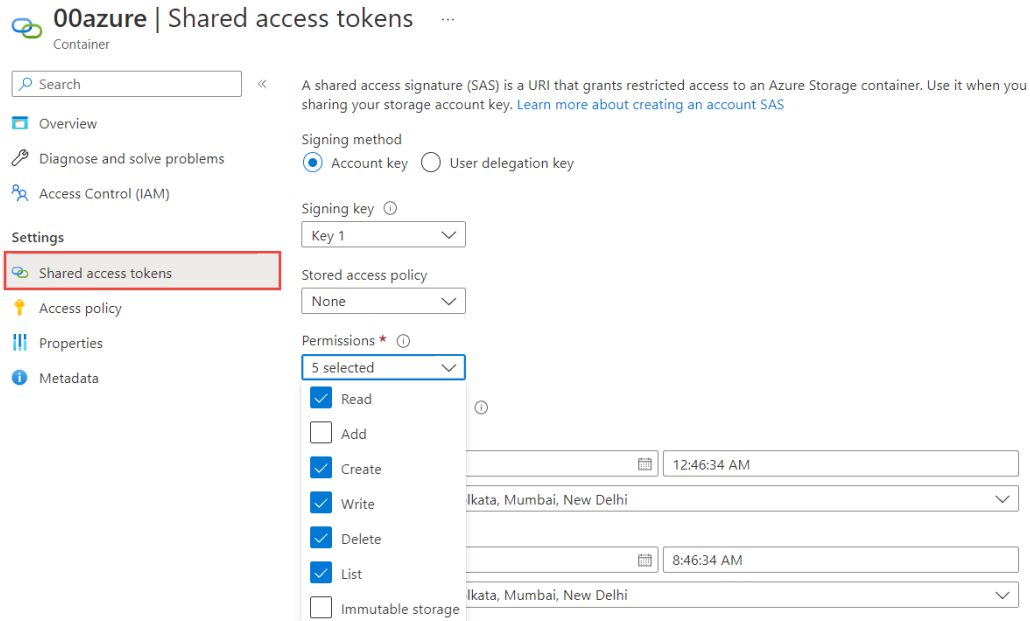
Shared Access Signature を使用して Microsoft Azure Blob Storage に接続するには、Shared Access Signature 認証の最小限の権限を設定し、Azure ポータルで SAS トークンを生成する必要があります。

ストレージアカウント用またはコンテナ用の SAS トークンを生成できます。

- ストレージアカウントの SAS トークンを生成するには、Azure ポータルで **【セキュリティ + ネットワーキング】** に移動し、**【共有アクセス署名】** をクリックします。
次の図に示すように、Shared Access Signature 認証に必要な最小限の権限を選択します。



- Blob コンテナ用の SAS トークンを生成するには、コンテナの【設定】に移動し、【共有アクセストークン】をクリックします。アカウントキー署名方式またはユーザー委任キー署名方式を使用することができます。ユーザー委任キー署名方式を使用する場合は、コンテナまたはストレージアカウントの【ストレージ BLOB データ所有者】ロールがあることを確認してください。
次の図に示すように、Shared Access Signature 認証に必要な最小限の権限を選択します。



Microsoft Azure Blob Storage V3 への接続

Microsoft Azure Blob Storage に接続するように Microsoft Azure Blob Storage V3 の接続プロパティを設定してみましょう。

始める前に

開始する前に、ストレージアカウントから BLOB コンテナ名と Azure エンドポイントのタイプを取得する必要があります。また、設定してする認証のタイプに基づいて、Microsoft Azure Blob Storage アカウントから情報を取得する必要があります。

共有キー認証を使用するには、ストレージアカウント名とアカウントキーを取得する必要があります。Shared Access Signature 認証を使用するには、Azure ポータルの Shared Access Signature トークンが必要です。

認証の前提条件の詳細については、「[認証の準備](#)」(ページ 399)を参照してください。

接続の詳細

次の表に、基本接続プロパティを示します。

プロパティ	説明
接続名	接続の名前。 各接続名は組織内で一意である必要があります。接続名には、英数字、スペース、および次の特殊文字を含めることができます。_ . + , 最大長は 255 文字です。
説明	接続の説明。最大長は 4000 文字です。
シークレットコンテナの使用	組織に対して設定されている Secrets Manager にこの接続の機密資格情報を保存します。 このプロパティは、組織に Secrets Manager が設定されている場合にのみ表示されます。 このプロパティは、データ取り込みおよびレプリケーションとデータアクセス管理サービスではサポートされていません。 接続でシークレットコンテナを有効にすると、Secure Agent が Secrets Manager からどの資格情報を取得するかを選択できます。このオプションを無効にした場合、資格情報は組織の設定方法に応じてリポジトリまたはローカル Secure Agent に保存されます。 注: この接続を使用してプッシュダウンまたはプロキシサービスを介してデータアクセスポリシーを適用する場合、シークレットコンテナ設定オプションを使用することはできません。 Secrets Manager を設定および使用方法については、Administrator のヘルプにある「Secrets Manager の設定」を参照してください。
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。 Secure Agent、ホステッドエージェント、サーバーレスランタイム環境、またはエラスティックランタイム環境を選択します。 Secure Agent を選択します。 ランタイム環境の設定および使用方法の詳細については、Administrator のヘルプにある「ランタイム環境」を参照してください。
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 にアクセスするように、共有キー認証と Shared Access Signature 認証のタイプを設定できます。

必要な認証方法を選択し、認証固有のパラメータを設定します。

共有キー認証

共有キー認証では、ストレージアカウント名とアカウントキーを使用して Microsoft Azure Blob Storage に接続します。

次の表に、共有キー認証の接続プロパティとその説明を示します。

プロパティ	説明
アカウントキー	Microsoft Azure Blob Storage アカウントのアカウントキー。
コンテナ名	Microsoft Azure Blob Storage アカウントの Blob コンテナの名前。
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。 <ul style="list-style-type: none">- 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

共有アクセス署名認証

Shared Access Signature 認証では、SAS トークンを使用して Microsoft Azure Blob Storage に接続します。SAS トークンを使用して、アカウントキーを共有せずに、特定の時間範囲でストレージアカウントまたはコンテナのリソースへのアクセス許可を付与します。

注: このオプションがコンテナレベルにあり、別のコンテナを使用している場合、ファイル取り込みタスクは失敗します。

次の表に、Shared Access Signature 認証の接続プロパティとその説明を示します。

プロパティ	説明
SAS トークン	正常に認証され、Microsoft Azure Blob Storage リソースにアクセスするために Azure ポータルで生成された Shared Access Signature トークン。
コンテナ名	Microsoft Azure Blob Storage アカウントの Blob コンテナの名前。
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。 <ul style="list-style-type: none">- 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

プロキシサーバーの設定

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

Windows および Linux 上でプロキシサーバーを使用するように Secure Agent とサーバーレスランタイム環境を設定できます。設定にホストとポートアドレスのみを必要とする非認証プロキシサーバーを使用できます。

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

- Windows の場合は Secure Agent Manager を使用し、Linux の場合はシェルコマンドを使用して Secure Agent を設定します。
手順については、データ統合のヘルプの『または「Windows でのプロキシ設定」または「Linux でのプロキシ設定」を参照してください。
- JVM オプションを使用してプロキシサーバーを設定します。この操作を行うには、次の手順を実行します。
 1. Informatica Intelligent Cloud Services にログインします。
 2. [管理] を開いて [ランタイム環境] を選択します。
 3. プロキシサーバーを設定する Secure Agent を選択します。
 4. ページの右上隅にある [編集] をクリックします。
 5. [システム構成の詳細] セクションで、データ統合サービスの [タイプ] に [DTM] を選択します。
 6. [JVMOption] フィールドに次のパラメータを追加して、各パラメータに適切な値を指定します。

パラメータ	説明
-DproxyEnabled=	必須。プロキシサーバーを有効にするには、値を true に設定します。
-Dhttp.proxyHost=	必須。送信 HTTP プロキシサーバーのホスト名。
-Dhttp.proxyPort=	必須。送信 HTTP プロキシサーバーのポート番号。

HTTP の例。

```
JVMOption1=-DproxyEnabled=true
```

```
JVMOption2=-Dhttp.proxyHost=<proxy_server_hostname>
```

```
JVMOption3=-Dhttp.proxyPort=8081
```

7. [保存] をクリックします。
Secure Agent が再起動して設定が適用されます。

サーバーレスランタイム環境のプロキシの設定を行う方法については、Administrator ヘルプの「「プロキシサーバーの使用」を参照してください。

第 120 章

Microsoft Azure Cosmos DB SQL API 接続のプロパティ

Microsoft Azure Cosmos DB SQL API 接続を作成し、Microsoft Azure Cosmos DB SQL API に対して安全にデータの読み書きを行います。

Microsoft Azure Cosmos DB SQL API への接続

Microsoft Azure Cosmos DB SQL API に接続するように Microsoft Azure Cosmos DB SQL API の接続プロパティを設定してみましょう。

始める前に

接続プロパティを設定する前に、Microsoft Azure Cosmos DB SQL API アカウントから Cosmos DB URI、データベース名、キー値を取得する必要があります。キーの詳細は、Microsoft Azure Cosmos DB SQL API 設定の【キー】タブで確認することができます。

接続の詳細

次の表に、基本接続プロパティを示します。

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

プロパティ	説明
シークレットコンテナの使用	<p>組織に対して設定されている Secrets Manager にこの接続の機密資格情報を保存します。このプロパティは、組織に Secrets Manager が設定されている場合にのみ表示されます。このプロパティは、データ取り込みおよびレプリケーションとデータアクセス管理サービスではサポートされていません。</p> <p>接続でシークレットコンテナを有効にすると、Secure Agent が Secrets Manager からどの資格情報を取得するかを選択できます。このオプションを無効にした場合、資格情報は組織の設定方法に応じてリポジトリまたはローカル Secure Agent に保存されます。</p> <p>注: この接続を使用してプッシュダウンまたはプロキシサービスを介してデータアクセスポリシーを適用する場合、シークレットコンテナ設定オプションを使用することはできません。</p> <p>Secrets Manager を設定および使用する方法については、Administrator のヘルプにある「Secrets Manager の設定」を参照してください。</p>
ランタイム環境	<p>タスクを実行するランタイム環境の名前。</p> <p>Secure Agent、ホステッドエージェント、サーバーレスランタイム環境、またはエラスティックランタイム環境を選択します。</p> <p>詳細モードのマッピングで接続を使用する場合は、ホステッドエージェントを使用しないでください。</p> <p>ランタイム環境の設定および使用方法の詳細については、Administrator のヘルプにある「ランタイム環境」を参照してください。</p>
Cosmos DB URI	Microsoft Azure Cosmos DB アカウントにアクセスするための 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を付与するプライマリキーまたはセカンダリキー。
データベース名	JSON ドキュメントの読み取りまたは書き込みを行うコンテナが格納されているデータベース名。

第 121 章

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

Microsoft Azure Lake Storage Gen2 接続を作成すると、Microsoft Azure Data Lake Storage Gen2 に対するデータの読み書きを安全に行うことができます。

認証の準備

Microsoft Azure Data Lake Storage Gen2 にアクセスするように、共有キー、マネージド ID、サービスプリンシパル認証のタイプを設定できます。認証を設定する前に、環境の設定を行い、認証の詳細を手元に用意しておく必要があります。

ストレージアカウントの作成とアクセスの設定

Microsoft Azure Data Lake Storage Gen2 にアクセスするには、次の手順に従って環境を設定します。

1. Microsoft Azure Data Lake Storage Gen2 で使用するストレージアカウントを設定し、ストレージアカウントに BLOB コンテナを作成します。ロールベースのアクセス制御またはアクセス制御リストを使用して、ユーザーがストレージアカウントのリソースにアクセスすることを許可できます。
2. Azure Active Directory にアプリケーションを登録して、Microsoft Azure Data LakeStorage Gen2 アカウントにアクセスするユーザーを認証します。ロールベースのアクセス制御またはアクセス制御リストを使用して、アプリケーションを許可できます。
3. Microsoft Azure Data Lake Storage Gen2 でのサービス間認証用に Azure Active Directory Web アプリケーションを作成します。アプリケーションで作成されたフォルダまたはファイルにアクセスするためのスーパーユーザー特権が割り当てられていることを確認します。
これらの前提条件のタスクの詳細については、Informatica How-To ライブラリの記事、[「Prerequisites to create a Microsoft Azure Data Lake Storage Gen2 connection」](#)を参照してください。

認証の詳細の取得

接続で使用する認証方法に基づいて、必要なすべての認証詳細を取得していることを確認します。

サービスプリンシパル認証

Azure Active Directory に登録されているアプリケーションのクライアント ID、クライアントシークレット、およびテナント ID が必要です。

共有キー認証

Microsoft Azure Data Lake Storage Gen2 アカウントのアカウントキーが必要です。

マネージド ID 認証

Azure Active Directory に登録されているアプリケーションのクライアント ID またはアプリケーション ID が必要です。クライアント ID またはアプリケーション ID を取得する前に、特定の前提条件を満たす必要があります。

マネージド ID 認証

マネージド ID 認証では、Azure Active Directory のマネージド ID を使用して Azure リソースへのアクセスを安全に認証および承認します。

マネージド ID 認証を使用して Microsoft Azure Data Lake Storage Gen2 に接続する前に、特定の前提条件を満たす必要があります。

1. Azure 仮想マシンを作成する。
Microsoft Azure Data Lake Storage Gen2 接続でマネージド ID 認証を設定するには、Secure Agent をインストールした Azure 仮想マシンを選択します。
2. Secure Agent を Azure 仮想マシンにインストールする。
3. Azure 仮想マシンのシステム割り当て ID またはユーザー割り当て ID を有効にする。
システム割り当て ID を有効にする場合は、必要なロールまたは権限を Azure 仮想マシンに割り当てて、マッピングとタスクを実行します。ユーザー割り当て ID を有効にする場合は、ユーザー割り当て ID に必要なロールまたは権限を割り当てます。例えば、ロールベースのアクセス制御を使用する場合は、Storage Blob Data Contributor ロールを割り当て、アクセス制御リストを使用する場合は、読み取り、書き込み、および実行権限を割り当てます。両方の ID を有効にしてもクライアント ID が指定されていない場合は、システムで割り当てられた ID が認証に使用されます。
4. マネージド ID を追加または削除した後に、Azure 仮想マシンを再起動する。

Microsoft Azure Data Lake Storage Gen2 への接続

Microsoft Azure Data Lake Storage Gen2 に接続するように Microsoft Azure Data Lake Storage Gen2 の接続プロパティを設定してみましょう。

始める前に

開始する前に、設定する認証タイプに基づいて Microsoft Azure Data Lake Storage Gen2 アカウントから情報を取得する必要があります。

認証の前提条件の詳細については、[「認証の準備」 \(ページ 407\)](#)を参照してください。

接続の詳細

次の表に、基本接続プロパティを示します。

プロパティ	説明
接続名	接続の名前。 各接続名は組織内で一意である必要があります。接続名には、英数字、スペース、および次の特殊文字を含めることができます。_ . + , 最大長は 255 文字です。
説明	接続の説明。最大長は 4000 文字です。
シークレットコンテンツの使用	組織に対して設定されている Secrets Manager にこの接続の機密資格情報を保存します。 このプロパティは、組織に Secrets Manager が設定されている場合のみ表示されます。 このプロパティは、データ取り込みおよびレプリケーションとデータアクセス管理サービスではサポートされていません。 接続でシークレットコンテンツを有効にすると、Secure Agent が Secrets Manager からどの資格情報を取得するかを選択できます。このオプションを無効にした場合、資格情報は組織の設定方法に応じてリポジトリまたはローカル Secure Agent に保存されます。 注: この接続を使用してプッシュダウンまたはプロキシサービスを介してデータアクセスポリシーを適用する場合、シークレットコンテンツ設定オプションを使用することはできません。 Secrets Manager を設定および使用方法については、Administrator のヘルプにある「Secrets Manager の設定」を参照してください。
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。 Secure Agent、ホステッドエージェント、サーバーレスランタイム環境、またはエラスティックランタイム環境を選択します。 詳細モードのマッピングで接続を使用する場合は、ホステッドエージェントを使用しないでください。 サポートされているソースタイプを持つデータベース取り込みとレプリケーションタスクでは、サーバーレスランタイム環境を使用できます。ホステッドエージェントまたはエラスティックランタイム環境で、アプリケーション取り込みとレプリケーションタスク、データベース取り込みとレプリケーションタスク、またはストリーミング取り込みとレプリケーションタスクを実行することはできません。 ランタイム環境の設定および使用方法の詳細については、Administrator のヘルプにある「ランタイム環境」を参照してください。
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。
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ディレクトリのパス。 次のディレクトリ構造から選択することができます。 - / (ルートディレクトリの場合)。 - /dir1 - dir1/dir2 デフォルトは/です。

認証タイプ

サービスプリンシパル認証、共有キー認証、マネージド ID 認証を選択して、Microsoft Azure Data Lake Storage Gen2 アカウントにアクセスできます。

注: データ取り込みおよびレプリケーションでは、マネージド ID 認証がサポートされています。ただし、ストリーミング取り込みとレプリケーションは、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。

希望する認証タイプを選択し、認証固有のパラメータを設定します。

サービスプリンシパル認証

サービスプリンシパル認証では、クライアント ID、クライアントシークレット、およびテナント ID を使用して Microsoft Azure Data Lake Storage Gen2 に接続します。

次の表に、サービスプリンシパル認証の基本接続プロパティを示します。

プロパティ	説明
クライアント ID	アプリケーションのクライアント ID。 Azure Active Directory に登録されているアプリケーションのクライアント ID を指定します。
クライアントシークレット	クライアント ID に生成されたクライアントシークレットキー。 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を指定します。
テナント ID	Azure Active Directory のディレクトリ ID。
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。 次のいずれかのエンドポイントを選択します。 <ul style="list-style-type: none">- 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: 詳細モードのマッピングに、Azure Government エンドポイントを設定することはできません。

共有キー認証

共有キー認証では、アカウントキーを使用して Microsoft Azure Data Lake Storage Gen2 に接続します。

次の表に、共有キー認証の基本接続プロパティを示します。

プロパティ	説明
アカウントキー	Microsoft Azure Data Lake Storage Gen2 アカウントのアカウントキー。
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。 次のいずれかのエンドポイントを選択します。 <ul style="list-style-type: none">- 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: 詳細モードのマッピングに、Azure Government エンドポイントを設定することはできません。

マネージド ID 認証

マネージド ID 認証は、Microsoft Azure Data Lake Storage Gen2 の Azure リソースにアクセスするために、Azure のアプリケーションに割り当てられた ID を使用して認証を行います。

次の表に、マネージド ID 認証の基本接続プロパティを示します。

プロパティ	説明
クライアント ID	アプリケーションのクライアント ID。 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。 次のシナリオでは、このフィールドを空白のままにします。 <ul style="list-style-type: none">- 権限がシステム割り当てマネージド ID によって提供されている場合。- 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。
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。 次のいずれかのエンドポイントを選択します。 <ul style="list-style-type: none">- 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: 詳細モードのマッピングに、Azure Government エンドポイントを設定することはできません。

プロキシサーバーの設定

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

Windows および Linux 上でプロキシサーバーを使用するように Secure Agent とサーバーレスランタイム環境を設定できます。認証されていないプロキシサーバーまたは認証されたプロキシサーバーを使用できます。

注: マネージド ID 認証でプロキシサーバーを使用することはできません。

次のいずれかのタイプのプロキシサーバーを使用できます。

- 認証されていないプロキシ - 設定を行う場合はホストとポートアドレスのみが必要です。
- 認証されたプロキシ - 設定を行う場合は、ホストアドレス、ポートアドレス、ユーザー名、およびパスワードが必要です。

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

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

手順については、データ統合のヘルプの『または「Windows でのプロキシ設定」または「Linux でのプロキシ設定」を参照してください。

- Secure Agent のプロパティで、DTM の JVM オプションを設定します。手順については、ナレッジベースの記事「[Proxy server settings](#)」を参照してください。

サーバーレスランタイム環境のプロキシの設定を行う方法については、Administrator ヘルプの「「プロキシサーバーの使用」を参照してください。

プロキシサーバーのバイパス

Secure Agent 用に設定されたプロキシサーバー設定をバイパスできます。

プロキシサーバーをバイパスするには、次の手順を実行します。

1. 次のディレクトリに移動します。
<Secure Agent のインストールディレクトリ>/apps/agentcore
2. proxy.ini ファイルで次のコマンドを入力します。
`InfAgent.NonProxyHost=localhost|{*}core.windows.net|127.*|[\:\:1]*`
 - サービスプリンシパル認証を行うためにプロキシサーバーをバイパスするには、コマンドに `login.microsoftonline.com` を追加します。
 - マネージド ID 認証を行うためにプロキシサーバーをバイパスするには、コマンドに `169.254.169.254` を追加します。

例: `InfAgent.NonProxyHost=localhost|127.*|[\:\:1]|<accountname>.blob.core.windows.net|<accountname>.dfs.core.windows.net|<accountname>.blob.core.windows.net|login.microsoftonline.com|169.254.169.254`
3. Secure Agent を再起動します。

第 122 章

Microsoft DocumentDB 接続のプロパティ

Microsoft Azure DocumentDB 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。

重要: Microsoft Azure DocumentDB は非推奨となり、メンテナンスモードに移行されました。Informatica は将来のリリースでサポートを廃止する予定です。Microsoft Azure Cosmos DB SQL API コネクタを使用して Microsoft Azure DocumentDB にアクセスすることをお勧めします。

次の表に、Microsoft Azure DocumentDB 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。
DocumentDB URI	Microsoft Azure DocumentDB アカウントの URI。
キー	Microsoft Azure DocumentDB アカウント内のリソースへの完全な管理アクセスを提供するプライマリキーとセカンダリキー。
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。

第 123 章

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。
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。

第 124 章

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。データベース取り込みとレプリケーションは、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	データベース取り込みとレプリケーション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: <code>jdbc:sqlserver://server.database.windows.net:1433;database=database</code> Azure Active Directory (AAD) 認証の接続文字列の例: <code>jdbc:sqlserver://server.database.windows.net:1433; database=database;encrypt=true;trustServerCertificate=false; hostNameInCertificate=*.database.windows.net;loginTimeout=30; Authentication=ActiveDirectoryPassword;</code> 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。

プロパティ	説明
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。
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。

第 125 章

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

次の表に、Microsoft Azure SQL Data Warehouse 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。
シークレットコンテナの使用	組織に対して設定されている Secrets Manager にこの接続の機密資格情報を保存します。 このプロパティは、組織に Secrets Manager が設定されている場合にのみ表示されます。 このプロパティは、データ取り込みおよびレプリケーションとデータアクセス管理サービスではサポートされていません。 接続でシークレットコンテナを有効にすると、Secure Agent が Secrets Manager からどの資格情報を取得するかを選択できます。このオプションを無効にした場合、資格情報は組織の設定方法に応じてリポジトリまたはローカル Secure Agent に保存されます。 注: この接続を使用してプッシュダウンまたはプロキシサービスを介してデータアクセスポリシーを適用する場合、シークレットコンテナ設定オプションを使用することはできません。 Secrets Manager を設定および使用する方法については、Administrator のヘルプにある「Secrets Manager の設定」を参照してください。
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。
Azure DW JDBC URL	Microsoft Azure Data Warehouse JDBC 接続文字列。例えば、次の接続文字列を入力できます: jdbc:sqlserver:// <Server>.database.windows.net:1433;database=<Database>。
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。
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。

接続プロパティ	説明
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。

第 126 章

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。

重要: Microsoft Azure SQL Data Warehouse V2 コネクタは非推奨となり、メンテナンスモードに移行されました。Informatica は将来のリリースでサポートを廃止する予定です。Microsoft Azure Synapse SQL コネクタを使用して Microsoft Azure SQL Data Warehouse にアクセスすることをお勧めします。

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: <code>jdbc:sqlserver://<Server>.database.windows.net:1433;database=<Database></code> Azure Active Directory (AAD) 認証の例: <code>jdbc:sqlserver://<Server>.database.windows.net:1433; database=<Database>;encrypt=true;trustServerCertificate=false; hostNameInCertificate=*.database.windows.net;loginTimeout=30; Authentication=ActiveDirectoryPassword;</code> 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。

第 127 章

Microsoft Azure Synapse Analytics 接続のプロパティ

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

認証の準備

Microsoft Azure Synapse Analytics にアクセスするために、管理者ユーザー認証タイプおよびサービスプリンシパル認証タイプを設定できます。認証を設定する前に、環境の設定を行い、認証の詳細を手元に用意しておく必要があります。

ストレージアカウントの作成とアクセスの設定

Microsoft Azure Synapse Analytics にアクセスするには、次の手順に従って環境を設定します。

1. Microsoft Azure Synapse Analytics で使用するストレージアカウントを設定し、ストレージアカウントに BLOB コンテナを作成します。ロールベースのアクセス制御またはアクセス制御リストを使用して、ユーザーがストレージアカウントのリソースにアクセスすることを許可できます。
2. Azure Active Directory にアプリケーションを登録して、Microsoft Azure Synapse Analytics アカウントにアクセスするユーザーを認証します。ロールベースのアクセス制御またはアクセス制御リストを使用して、アプリケーションを許可できます。

認証の詳細の取得

接続で使用する認証方法に基づいて、必要なすべての認証詳細を取得していることを確認します。

管理者ユーザー認証タイプ

Microsoft Azure Synapse Analytics インスタンスに接続するには、Azure Active Directory に登録されているアプリケーションのクライアント ID、ユーザー名、およびパスワードが必要です。

サービスプリンシパル認証タイプ

Azure Active Directory に登録されているアプリケーションのクライアント ID、クライアントシークレット、およびテナント ID が必要です。

Microsoft Azure Synapse Analytics への接続

Microsoft Azure Synapse Analytics に接続するように Microsoft Azure Synapse Analytics 接続プロパティを設定してみましょう。

始める前に

開始する前に、設定する認証タイプに基づいて Microsoft Azure Synapse Analytics アカウントから情報を取得する必要があります。

認証の前提条件の詳細については、「[「認証の準備」 \(ページ 420\)](#)」を参照してください。

接続の詳細

次の表に、基本接続プロパティを示します。

プロパティ	説明
接続名	接続の名前。 各接続名は組織内で一意である必要があります。接続名には、英数字、スペース、および次の特殊文字を含めることができます。_ . + , 最大長は 255 文字です。
説明	接続の説明。最大長は 4000 文字です。
タイプ	Microsoft Azure Synapse Analytics
シークレットコンテナの使用	組織に対して設定されている Secrets Manager にこの接続の機密資格情報を保存します。 このプロパティは、組織に Secrets Manager が設定されている場合にのみ表示されます。 このプロパティは、データ取り込みおよびレプリケーションとデータアクセス管理サービスではサポートされていません。 接続でシークレットコンテナを有効にすると、Secure Agent が Secrets Manager からどの資格情報を取得するかを選択できます。このオプションを無効にした場合、資格情報は組織の設定方法に応じてリポジトリまたはローカル Secure Agent に保存されます。 注: この接続を使用してプッシュダウンまたはプロキシサービスを介してデータアクセスポリシーを適用する場合、シークレットコンテナ設定オプションを使用することはできません。 Secrets Manager を設定および使用する方法については、Administrator のヘルプにある「Secrets Manager の設定」を参照してください。
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。Secure Agent、またはサーバーレスランタイム環境を選択します。

認証タイプ

管理者ユーザー認証タイプまたはサービスプリンシパル認証タイプを使用するように Microsoft Azure Synapse Analytics 接続を設定できます。

必要な認証タイプを選択し、認証固有のパラメータを設定します。

管理者ユーザー認証

管理者ユーザー認証には、Microsoft Azure Synapse Analytics アカウントのユーザー名とパスワードが必要です。

次の表に、管理者ユーザー認証の接続プロパティとその説明を示します。

サブスクリプション ID	Microsoft Azure Synapse Analytics のサブスクリプション ID。
クライアント ID	Azure Active Directory に登録されているアプリケーションのアプリケーション ID またはクライアント ID。
ユーザー名	Microsoft Azure Synapse Analytics インスタンスに接続するための完全修飾ユーザー名。ユーザー名については管理者に問い合わせてください。
パスワード	ユーザーに関連付けられているパスワード。パスワードについては管理者に問い合わせてください。

サービスプリンシパル認証

サービスプリンシパル認証には、Azure Active Directory に登録されているアプリケーションのテナント ID とクライアントシークレットが必要です。

次の表に、サービスプリンシパル認証の接続プロパティとその説明を示します。

サブスクリプション ID	Microsoft Azure Synapse Analytics のサブスクリプション ID。
クライアント ID	Azure Active Directory に登録されているアプリケーションのアプリケーション ID またはクライアント ID。
テナント ID	Azure Active Directory に登録されているアプリケーションのテナント ID。
クライアントシークレット	Azure Active Directory を介して Microsoft Azure Synapse Analytics インスタンスに接続するためのクライアントシークレットキー。クライアントシークレットキーについては管理者に問い合わせてください。

プロキシのプロパティ

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

次の表に、Microsoft Azure Synapse Analytics 接続プロキシのプロパティを示します。

接続プロパティ	説明
プロキシの使用	接続でプロキシサーバーを使用して Microsoft Azure Synapse Analytics に接続するかどうかを決定します。 プロキシサーバーを使用する場合に選択します。 デフォルトでは無効になっています。
ホスト	送信プロキシサーバーのホスト名。
ポート	送信プロキシサーバーのポート番号。

接続プロパティ	説明
ユーザー名	プロキシサーバーの認証済みのユーザーの名前。プロキシサーバーで認証が必要となる場合に必須です。
パスワード	認証されたユーザのパスワード。プロキシサーバーで認証が必要となる場合に必須です。

第 128 章

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、データ取り込みおよびレプリケーションサービスで設定を行うアプリケーション取り込みとレプリケーションタスクおよびデータベース取り込みとレプリケーションタスクで使用することができます。

注: 一部のプロパティは、Microsoft Azure Data Lake Storage Gen2 用です。アプリケーション取り込みとレプリケーションおよびデータベース取り込みとレプリケーションは、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、そのデータを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。
ランタイム環境	アプリケーション取り込みとレプリケーションタスクまたはデータベース取り込みとレプリケーション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。 サポートされているソースタイプを持つアプリケーション取り込みとレプリケーションタスクとデータベース取り込みとレプリケーションタスクでは、サーバーレスランタイム環境を使用できます。ホステッドエージェントでアプリケーション取り込みとレプリケーションタスクとデータベース取り込みとレプリケーションタスクを実行することはできません。

プロパティ	説明
Azure Synapse Analytics JDBC URL	<p>Microsoft Azure Synapse Analytics（以前の SQL Data Warehouse）の JDBC 接続文字列。</p> <p>Microsoft SQL Server 認証の接続文字列の例:</p> <pre>jdbc:sqlserver://server.database.windows.net:1433;database=database</pre> <p>Azure Active Directory（AAD）認証の接続文字列の例:</p> <pre>jdbc:sqlserver://server.database.windows.net:1433; database=database;encrypt=true;trustServerCertificate=false; hostNameInCertificate=*.database.windows.net;loginTimeout=30; Authentication=ActiveDirectoryPassword;</pre> <p>注: デフォルトの認証タイプは、Microsoft SQL Server 認証です。</p>
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	アプリケーション取り込みとレプリケーションおよびデータベース取り込みとレプリケーション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。

第 129 章

Microsoft Azure Synapse SQL 接続のプロパティ

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

前提条件

Microsoft Azure Synapse SQL にアクセスするように、Microsoft SQL Server 認証、Azure Active Directory 認証、マネージド ID 認証、およびサービスプリンシパル認証タイプを設定できます。

また、Microsoft Azure Synapse SQL からデータの読み取りを行うときに、サーバーレス SQL プールに接続することができます。サーバーレス SQL プールへの接続時に Microsoft Azure Synapse SQL にアクセスするように、Microsoft SQL Server 認証、Azure Active Directory 認証、およびマネージド ID 認証タイプを設定できます。認証の詳細については、Informatica How-To ライブラリの記事「[Prerequisites to connect to a serverless SQL pool](#)」を参照してください。

接続プロパティを設定する前に、使用する認証のタイプに基づいて認証の詳細を用意しておく必要があります。

Azure Active Directory 認証

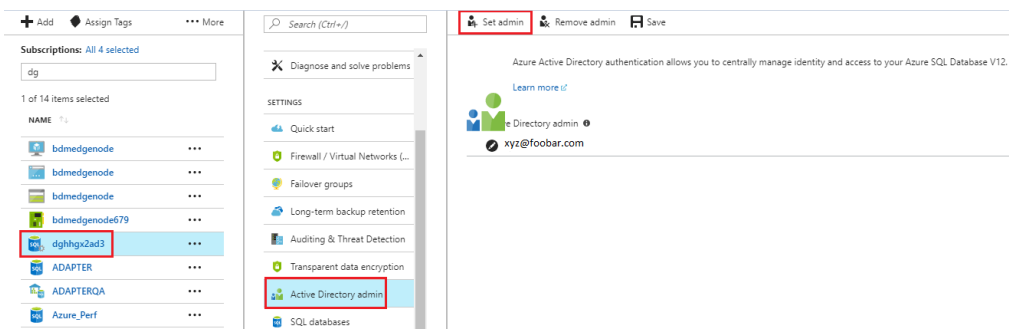
Azure Active Directory (AAD) 認証を使用して Microsoft Azure Synapse SQL に接続するには、Azure Active Directory 管理者と Azure Active Directory ユーザーを作成する必要があります。

Azure Active Directory 管理者の作成

Azure Active Directory に新しいユーザーを追加するには、管理者ロールが必要です。

Microsoft Azure Synapse SQL をホストする AAD と Microsoft SQL Server の Azure Active Directory 管理者を設定するには、次の手順を実行します。

1. 資格情報を使用して、Microsoft Azure ポータルにログオンします。
[ダッシュボード] ページが表示されます。
2. [すべてのリソース] ページで、Microsoft Azure Synapse SQL をホストしている Microsoft SQL Server を選択します。
3. Microsoft SQL Server に表示された [設定] で、**[Active Directory 管理者]** オプションを選択します。
以下の図に、Active Directory 管理者設定を示します。



4. **【管理者の設定】** をクリックします。
【管理者の追加】 ページが表示されます。
5. 管理者として使用する電子メール ID を入力してから、**【選択】** をクリックします。
6. **【保存】** をクリックします。

Azure Active Directory ユーザーの作成

AAD ユーザーを作成し、AAD 認証を使用して Microsoft Azure Synapse SQL 接続を設定するときに AAD ユーザー資格情報を使用します。

AAD ユーザーを作成するには、次の手順を実行します。

1. 前の手順で作成した Azure Active Directory 管理者を使用して、Microsoft Azure Synapse SQL に接続します。
Microsoft SQL Server Management Studio を使用して、Microsoft Azure Synapse SQL に接続できます。
2. Microsoft SQL Server Management Studio の新しいクエリウィンドウで、次のコマンドを実行して AAD ユーザーを作成します:
create user [user@foobar.com] from external provider;
3. 次の特権をユーザーに割り当てます:
CREATE USER [username] FROM EXTERNAL PROVIDER;
ALTER ROLE db_datareader ADD MEMBER [username]
ALTER ROLE db_datawriter ADD MEMBER [username]
GRANT EXECUTE TO [username]
grant ALTER ANY EXTERNAL DATA SOURCE to [username];
grant create table to [username];
grant create schema to [username];
grant select to [username];
grant update to [username];
grant insert to [username];
grant delete to [username];
grant create view to [username];
grant select on schema :: sys to [username];
grant control to [username];
EXEC sp_addrolemember 'db_owner', '[username]';
ALTER ROLE db_owner ADD MEMBER [username]

サービスプリンシパル認証

サービスプリンシパル認証では、サービスプリンシパル ID を使用して Azure リソースへのアクセスを認証および承認します。サービスプリンシパル認証を使用して Microsoft Azure Synapse SQL に接続する前に、特定の前提条件を必ず満たすようにしてください。

1. サービスプリンシパルアプリケーションを登録する。
2. サーバーレス SQL プールのサービスプリンシパルユーザーを設定する。
3. 専用 SQL プールのサービスプリンシパルユーザーを設定する。

詳細については、Informatica How-To ライブラリの記事

「[Prerequisites to use service principal authentication](#)」を参照してください。

マネージド ID 認証

マネージド ID 認証では、Azure Active Directory のマネージド ID を使用して Azure リソースへのアクセスを安全に認証および承認します。

マネージド ID 認証を使用して Microsoft Azure Synapse SQL に接続する場合、システム割り当て ID のユーザーは、その ID を有効にした仮想マシンになります。ユーザー割り当て ID のユーザーは、Azure portal で作成したユーザー ID になります。

マネージド ID 認証を使用して Microsoft Azure Synapse SQL または Microsoft Azure Data Lake Storage Gen2 に接続する前に、特定の前提条件を必ず満たすようにしてください。

1. Azure 仮想マシンを作成する。
2. Secure Agent を Azure 仮想マシンにインストールする。
3. Azure 仮想マシンのシステム割り当て ID またはユーザー割り当て ID を有効にする。
両方の ID を有効にしてもクライアント ID が指定されていない場合は、システムで割り当てられた ID が認証に使用されます。
4. マネージド ID を追加または削除した後に、Azure 仮想マシンを再起動する。

サーバーレス SQL プール

サーバーレス SQL プールに接続するように Microsoft Azure Synapse SQL 接続を設定できます。サーバーレス SQL プールでは、データの格納や事前設定されたインフラストラクチャが必要となることはありません。サーバーレス SQL プールに接続するのは、Microsoft Azure Data Lake Storage Gen2 に格納されているデータを参照する外部テーブルに対してクエリを実行する場合、または OPENROWSET 関数を使ったクエリを使用する場合です。

サーバーレス SQL プールに接続するには、Microsoft Azure Synapse SQL 接続でサーバーレス SQL プールに対して Azure DW JDBC URL 接続文字列を指定します。

サーバーレス SQL プールに接続して Microsoft Azure SQL Data Warehouse から読み取りを行う前に、次の前提条件を必ず満たすようにしてください。

1. Azure Analytics サーバーレスプールワークスペースを設定します。
2. サーバーレスプールワークスペースに SQL データベースを作成します。
3. 次の認証タイプの JDBC URL を取得します。
 - Microsoft SQL Server の認証
 - Azure Active Directory (AAD) 認証
 - マネージド ID 認証

- サービスプリンシパル認証
4. サービスプリンシパル認証を使用して Microsoft Azure Data Lake Storage Gen2 に接続し、ファイルをステージングするには、サービスプリンシパルの資格情報を取得します。
 5. OPENROWSET クエリを使用するか、外部テーブルを作成して、ファイルからデータを読み取る手順を設定します。

詳細については、Informatica How-To ライブラリの記事

「[Prerequisites to connect to a serverless SQL pool](#)」を参照してください。

権限

権限により、Microsoft Azure Synapse SQL で実行できる操作のアクセスレベルを定義します。

次のような権限を確認する必要があります。

- デフォルトのスキーマがアカウントレベルまたはユーザーあるいはグループレベルで Microsoft Azure SQL Data Warehouse に存在することを確認します。
- Microsoft Azure SQL Data Warehouse に接続して操作を正常に実行するための db_owner 特権、または次のようなより詳細な特権のいずれかがユーザーに付与されていることを確認します。
 - EXEC sp_addrolemember 'db_datareader', '<user>'; // または、個々のテーブルに対する権限を割り当てます。
 - EXEC sp_addrolemember 'db_datawriter', '<user>'; // または、個々のテーブルに対する権限を割り当てます。
 - GRANT ALTER ANY EXTERNAL DATA SOURCE TO <user>;
 - GRANT ALTER ANY EXTERNAL FILE FORMAT TO <user>;
 - GRANT CONTROL TO <user>;// データベースに対するすべての権限を付与します。
 - または
 - GRANT ALTER ANY SCHEMA TO <user>;// スキーマに対してのみ権限を付与します。
 - GRANT CREATE TABLE TO <user>;
 - Pre-SQL コマンドと Post-SQL コマンドでタスクを実行するのに必要な特権を割り当てます。
- 接続プロパティでステージングスキーマ名を設定する場合は、次の追加の権限がユーザーに付与されていることを確認してください:
 - ALTER ROLE db_datareader ADD MEMBER <user>;
 - GRANT ALTER ANY EXTERNAL DATA SOURCE TO <user>;
 - GRANT ALTER ANY EXTERNAL FILE FORMAT TO <user>;
 - GRANT CREATE TABLE TO <user>;
 - GRANT ALTER ON SCHEMA::<staging_schema_name> TO <user>;// 別のスキーマで外部テーブルを作成または削除するためのアクセス権がこのユーザーに割り当てられていないことを確認します。
 - GRANT REFERENCES ON DATABASE SCOPED CREDENTIAL::<db_credential_name> TO <user>;// 資格情報を削除するためのアクセス権がこのユーザーに割り当てられていないことを確認します。
 - 例: GRANT REFERENCES ON DATABASE SCOPED CREDENTIAL::db_creds1 TO srvls;
- ALTER ANY SCHEMA 権限を持っている場合は、Microsoft Azure Synapse SQL でマスタキー、データベーススコープ資格情報、および外部データソースを作成する必要があります。これには、データベースに対する CONTROL 権限が必要であり、接続の作成時に外部データソースを指定する必要があります。また、Microsoft Azure Synapse SQL コネクタは、データベーススコープ資格情報と外部データソースを削除しません。データベーススコープ資格情報と外部データソースを手動で削除する必要があります。
- マネージド ID 認証を使用して Microsoft Azure Synapse SQL に接続する場合は、仮想マシンとユーザー ID に権限を付与してください。例: GRANT CONTROL TO <virtual machine name>;および GRANT CONTROL TO <user identity name>;

Microsoft Azure Synapse SQL への接続

Microsoft Azure Synapse SQL に接続するように Microsoft Azure Synapse SQL 接続プロパティを設定してみましょう。

始める前に

開始する前に、設定する認証タイプに基づいて Microsoft Azure Synapse SQL アカウントから情報を取得する必要があります。

Microsoft Azure Synapse SQL から必要な情報については、[Azure Active Directory authentication](#)、[Managed Identity authentication](#)、および「[サービスプリンシパル認証](#)」(ページ 428)を参照してください。

Azure アカウントから JDBC URL を取得する方法については、How-To ライブラリの記事「[Obtaining the JDBC URL](#)」を参照してください。

サーバーレス SQL プールに接続するために必要な情報については、「[serverless SQL pool](#)」を参照してください。

接続の詳細

次の表に、基本接続プロパティを示します。

財産	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。
シークレットコンテナの使用	組織に対して設定されている Secrets Manager にこの接続の機密資格情報を保存します。 このプロパティは、組織に Secrets Manager が設定されている場合にのみ表示されます。 このプロパティは、データ取り込みおよびレプリケーションとデータアクセス管理サービスではサポートされていません。 接続でシークレットコンテナを有効にすると、Secure Agent が Secrets Manager からどの資格情報を取得するかを選択できます。このオプションを無効にした場合、資格情報は組織の設定方法に応じてリポジトリまたはローカル Secure Agent に保存されます。 注: この接続を使用してプッシュダウンまたはプロキシサービスを介してデータアクセスポリシーを適用する場合、シークレットコンテナ設定オプションを使用することはできません。 Secrets Manager を設定および使用する方法については、Administrator のヘルプにある「Secrets Manager の設定」を参照してください。

財産	説明
ランタイム環境	<p>タスクを実行するランタイム環境の名前。</p> <p>Secure Agent、ホステッドエージェント、サーバーレスランタイム環境、またはエラスティックランタイム環境を選択します。</p> <p>ファイル取り込みとレプリケーションタスクでは、ホステッドエージェントを使用できますが、サーバーレス環境を使用することはできません。</p> <p>ホステッドエージェントは、詳細モードのマッピングには適用されません。</p> <p>ランタイム環境の設定および使用方法の詳細については、Administrator のヘルプにある「ランタイム環境」を参照してください。</p>

財産	説明
Azure DW JDBC URL	<p>Microsoft Azure Synapse SQL JDBC 接続文字列。 次の文字列を使用して、Microsoft Azure Synapse SQL に接続します。</p> <pre>jdbc:sqlserver:// <Server>.database.windows.net:1433;database=<Database></pre> <p>接続文字列に認証パラメータを含めて、認証タイプを指定できます。Microsoft Azure Synapse SQL に接続するための次の認証タイプを設定できます。</p> <ul style="list-style-type: none"> - Microsoft SQL Server - Azure Active Directory - マネージド ID - サービスプリンシパル <p>接続文字列に認証パラメータを含めない場合、Secure Agent では認証タイプとして Microsoft SQL Server 認証が使用されます。</p> <p>Microsoft Azure Synapse SQL のサーバーレス SQL プールに接続するには、次の文字列を使用します：</p> <pre>jdbc:sqlserver://<サーバーレス SQL エンドポイント>:1433;database=<データベース>;Authentication=ActiveDirectoryMsi;</pre> <p>Microsoft SQL Server 認証の接続文字列形式</p> <pre>jdbc:sqlserver:// <Server>.database.windows.net:1433;database=<Database></pre> <p>Azure Active Directory (AAD) 認証の接続文字列形式</p> <pre>jdbc:sqlserver://<サーバー>.database.windows.net:1433; database=<データベース>;encrypt=true;trustServerCertificate=false;hostNameInCertificate=*.database.windows.net;loginTimeout=30; Authentication=ActiveDirectoryPassword;</pre> <p>サービスプリンシパル認証の接続文字列形式</p> <pre>jdbc:sqlserver://<Server>.database.windows.net:1433; database=<Database>;encrypt=true;trustServerCertificate=false;hostNameInCertificate=*.database.windows.net;loginTimeout=30; Authentication=ActiveDirectoryServicePrincipal;</pre> <p>マネージド ID 認証の接続文字列形式</p> <pre>jdbc:sqlserver://<サーバー>.database.windows.net:1433;database=<データベース>;Authentication=ActiveDirectoryMsi;</pre>

財産	説明
Azure DW JDBC ユーザー名	<p>Microsoft Azure Synapse SQL アカウントに接続するためのユーザー名。</p> <ul style="list-style-type: none"> - AAD 認証の場合は、AAD ユーザー名を指定します。 - Microsoft SQL Server 認証の場合は、SQL 認証ユーザー名を指定します。 - サービスプリンシパル認証の場合は、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 を指定します。 <p>このプロパティは、マネージド ID 認証には適用されません。</p>
Azure DW JDBC パスワード	<p>Microsoft Azure Synapse SQL アカウントに接続するためのパスワード。</p> <ul style="list-style-type: none"> - AAD 認証の場合は、AAD ユーザーのパスワードを指定します。 - Microsoft SQL Server 認証の場合は、SQL 認証ユーザーのパスワードを指定します。 - サービスプリンシパル認証の場合は、Azure Active Directory に登録されているアプリケーションのクライアントシークレットを指定します。 <p>このプロパティは、マネージド ID 認証には適用されません。</p>
Azure DW クライアント ID	<p>マネージド ID 認証でユーザー割り当てマネージド ID を使用して Microsoft Azure Synapse SQL に接続する場合は必須です。</p> <p>ユーザー割り当てマネージド ID のクライアント ID。システム割り当てのマネージド ID を使用する場合は、フィールドを空のままにします。</p>
Azure DW スキーマ名	Microsoft Azure Synapse SQL 内のスキーマの名前。

Azure ストレージタイプ

データファイルをステージングする Azure ストレージタイプとして、Microsoft Azure Blob Storage または Microsoft Azure Data Lake Storage Gen2 を選択できます。デフォルトは Azure Blob です。

希望するストレージタイプを選択し、ストレージ固有のパラメータを設定します。

Microsoft Azure Blob Storage または Microsoft Azure Data Lake Storage Gen2 に接続してファイルをステージングするときに、共有キー認証の資格情報を取得する方法については、How-To ライブラリの記事「[Get credentials for shared key authentication](#)」を参照してください。

Microsoft Azure Data Lake Storage Gen2 に接続してファイルをステージングするときに、サービスプリンシパル認証の資格情報を取得する方法については、How-To ライブラリの記事「[Get credentials for service principal authentication](#)」を参照してください。

Azure Blob Storage

ストレージタイプとして Microsoft Azure Blob を選択すると、ファイルをステージングするための認証タイプとして共有キー認証を設定できます。

注: サーバーレス SQL プールに接続する場合は、ストレージタイプとして Microsoft Azure Data Lake Storage Gen2 を設定する必要があります。

次の表に、Microsoft Azure BLOB Storage に対して設定できる認証タイプを示します。

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 Microsoft Azure Blob Storage に接続するための認証タイプ。ファイルをステージングするための認証タイプとして共有キー認証を設定できます。

共有キー認証

ストレージアカウント名とアカウントキーを使用して、Microsoft Azure Blob Storage に接続します。

次の表に、共有キー認証の基本接続プロパティを示します。

プロパティ	説明
Azure Blob アカウント名	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	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	Azure Blob Storage アカウントのコンテナの名前。

ADLS Gen2 ストレージ

ストレージタイプとして Microsoft Azure Data Lake Storage Gen2 を選択すると、ファイルをステージングするためのさまざまな認証タイプを設定できます。

次の表に、Microsoft Azure Data Lake Storage Gen2 ストレージに対して設定できる認証タイプを示します。

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。 <ul style="list-style-type: none">- 共有キー認証- サービスプリンシパル認証- マネージド ID 認証 認証タイプの設定方法の詳細については、 「Setting up authentication to connect to Microsoft Azure Synapse SQL」 を参照してください。

共有キー認証

ストレージアカウント名とアカウントキーを使用して、Microsoft Azure Data Lake Storage Gen2 に接続します。

注: サーバーレス SQL プールに接続する場合は、共有キー認証の種類を選択できません。

次の表に、共有キー認証の基本接続プロパティを示します。

プロパティ	説明
ADLS Gen2 ストレージアカウント名	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	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。
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。

サービスプリンシパル認証

アカウント名、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。

次の表に、サービスプリンシパル認証の基本接続プロパティを示します。

プロパティ	説明
ADLS Gen2 ストレージアカウント名	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。
クライアント ID	アプリケーションのクライアント ID。 Azure Active Directory に登録されているアプリケーションのアプリケーション ID またはクライアント ID を入力します。
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。
テナント ID	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 アカウントのファイルシステムの名前。

マネージド ID 認証

Microsoft Azure Data Lake Storage Gen2 の Azure リソースにアクセスするために、Azure のアプリケーションに割り当てられたシステム割り当て ID またはユーザー割り当て ID を使用して認証するには、この認証タイプを選択します。

次の表に、マネージド ID 認証の基本接続プロパティを示します。

プロパティ	説明
ADLS Gen2 ストレージアカウント名	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。
クライアント ID	アプリケーションのクライアント ID。 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。
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。

ファイル取り込みとレプリケーションタスクで、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。

詳細設定

次の表に、詳細接続のプロパティを示します。

プロパティ	説明
外部データソース	外部テーブルを作成するデータソース。 外部データソースが Microsoft Azure Synapse SQL に存在していること、および外部データソースにアクセスする権限があることを確認してください。 コピーコマンド方式を使用してステージングの場所から Microsoft Azure Synapse SQL にデータのロードを行う場合、外部データソースを指定する必要はありません。
ステージングスキーマ名	Secure Agent がデータファイルをステージングする外部テーブルを作成するのに使用するスキーマの名前。 ステージングスキーマ名が指定されていない場合、Secure Agent は設定された Azure DW スキーマ名を考慮します。
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。 <ul style="list-style-type: none">- core.windows.net。Azure エンドポイントに接続します。サーバーレス SQL プールに接続する場合は、このエンドポイントを使用します。- 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。 このプロパティは、サーバーレスランタイム環境には適用されません。

第 130 章

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。

重要: Microsoft CDM Folders V2 コネクタは非推奨となり、メンテナンスモードに移行されました。Informatica は将来のリリースでサポートを廃止する予定です。

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、ホステッドエージェント、サーバーレスランタイム環境、またはエラスティックランタイム環境を選択します。 ランタイム環境の設定および使用方法の詳細については、Administrator のヘルプにある「ランタイム環境」を参照してください。
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。

プロパティ	説明
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	<p>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。</p> <p>CDM フォルダパスには次の値を使用できます。</p> <ul style="list-style-type: none"> - / - /folder1 - /folder1/folder2 <p>推奨される CDM フォルダパスは/folder1 です。</p> <p>デフォルトは空白です。</p>
ADLS Gen2 エンドポイント	ADLS Gen2 エンドポイントの core.windows.net。

第 131 章

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

Microsoft Dynamics 365 for Operations との間でデータの安全な読み取りと書き込みを行うための Microsoft Dynamics 365 for Operations 接続を作成します。

認証の準備

OAuth 2.0 および OAuth2.0 クライアントシークレット付与認証タイプを接続して、Microsoft Dynamics 365 for Operations に接続できます。

接続プロパティを設定する前に、使用する認証のタイプに基づいて認証の詳細を用意しておく必要があります。

また、Microsoft Dynamics 365 for Operations に接続するために必要なドメインを承認済みの IP アドレスのリストに追加する必要があります。

承認済みの IP アドレスのリストに追加する必要があるドメインの詳細については、ナレッジの記事「[List of domains](#)」を参照してください。

注: OAuth 2.0 クライアント証明書付与認証を使用して Microsoft Dynamics 365 for Operations にアクセスすることはできません。

OAuth 2.0 認証

Microsoft Dynamics 365 for Operations にアクセスするための OAuth 2.0 認証を設定するには、Microsoft Dynamics 365 for Operations のユーザー名とパスワードが必要です。

さらに、OAuth 2.0 認証用のサービス URL とアプリケーション ID が必要です。

これらの詳細を取得する場合、組織の管理者は Microsoft Dynamics 365 for Operations アプリケーションを Azure Active Directory に登録する必要があります。

Azure Active Directory への登録手順の詳細については、「[Register your application](#)」を参照してください。

OAuth 2.0 クライアントシークレット付与認証

Microsoft Dynamics 365 for Operations にアクセスするには、テナント ID とクライアントシークレット、および OAuth 2.0 クライアントシークレット付与認証を使用する必要があります。

テナント ID とクライアントシークレットを取得するには、Microsoft Dynamics 365 for Operations アプリケーションを Azure Active Directory に登録する必要があります。

さらに、OAuth 2.0 クライアントシークレット付与認証用のサービス URL とアプリケーション ID が必要です。

-Dlog4j.configuration プロパティの設定

1. log4j.properties ファイルを<Secure Agent のインストールディレクトリ>\downloads\package-MSDAX7.<バージョン>\package\plugins\449700 ディレクトリからコピーし、Secure Agent マシン内の場所に配置します。
2. Secure Agent のシステム設定の詳細で、タイプ DTM の JVM オプションを-Dlog4j.configuration=<log4j.propertyfile location>\log4j.properties に設定します。
3. Secure Agent を再起動します。

Microsoft 365 for Operations への接続

Microsoft Dynamics 365 for Operations に接続するように Microsoft Dynamics 365 for Operations の接続プロパティを設定してみましょう。

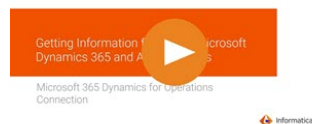
始める前に

開始する前に、設定する認証タイプに基づいて Microsoft Dynamics 365 for Operations および AAD アカウントから情報を取得する必要があります。

OAuth 2.0 認証を設定するには、Microsoft Dynamics 365 for Operations のユーザー名とパスワードを取得します。

OAuth 2.0 クライアントシークレット付与認証を設定するには、Azure Active Directory (AAD) アカウントからテナント ID とクライアントシークレットを取得します。

次のビデオは、Microsoft Dynamics 365 および AAD アカウントから情報を取得する方法を示しています。



認証の前提条件の詳細については、「[認証の準備](#)」(ページ 439)を参照してください。

接続の詳細

次の表に、基本接続プロパティを示します。

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

プロパティ	説明
シークレットコンテナの使用	<p>組織に対して設定されている Secrets Manager にこの接続の機密資格情報を保存します。</p> <p>このプロパティは、組織に Secrets Manager が設定されている場合にのみ表示されます。</p> <p>このプロパティは、データ取り込みおよびレプリケーションとデータアクセス管理サービスではサポートされていません。</p> <p>接続でシークレットコンテナを有効にすると、Secure Agent が Secrets Manager からどの資格情報を取得するかを選択できます。このオプションを無効にした場合、資格情報は組織の設定方法に応じてリポジトリまたはローカル Secure Agent に保存されます。</p> <p>注: この接続を使用してプッシュダウンまたはプロキシサービスを介してデータアクセスポリシーを適用する場合、シークレットコンテナ設定オプションを使用することはできません。</p> <p>Secrets Manager を設定および使用する方法については、Administrator のヘルプにある「Secrets Manager の設定」を参照してください。</p>
ランタイム環境	<p>タスクを実行するランタイム環境の名前。</p> <p>Secure Agent、ホステッドエージェント、サーバーレスランタイム環境、またはエラスティックランタイム環境を選択します。</p> <p>ランタイム環境の設定および使用方法の詳細については、Administrator のヘルプにある「ランタイム環境」を参照してください。</p>

認証タイプ

OAuth 2.0 および OAuth 2.0 クライアントシークレット付与認証タイプを設定して、Microsoft Dynamics 365 for Operations にアクセスできます。

必要な認証方法を選択し、認証固有のパラメータを設定します。

注: OAuth 2.0 クライアント証明書付与認証を使用して Microsoft Dynamics 365 for Operations にアクセスすることはできません。クライアント証明書付与認証に表示される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のプロパティは、Microsoft Dynamics 365 for Operations 接続には適用されません。

OAuth 2.0 認証

OAuth 2.0 認証には、Microsoft Dynamics 365 for Operations アカウントのユーザー名、パスワード、サービス URL、および AAD アプリケーション ID が必要です。

次の表に、OAuth 2.0 認証の基本接続プロパティとその説明を示します。

プロパティ	説明
サービス URL	<p>Microsoft Dynamics 365 for Operations サービスの URL。</p> <p>URL は次の形式で入力します。</p> <p><code>https:<server name>:<port number></code></p> <p>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。</p>
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。

プロパティ	説明
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 AAD アプリケーション ID。

OAuth 2.0 クライアントシークレット付与認証

OAuth 2.0 クライアントシークレット付与認証には、Microsoft Dynamics 365 for Operations アカウントのテナント ID、クライアントシークレット、サービス URL、および AAD アプリケーション ID が必要です。

次の表に、OAuth 2.0 クライアントシークレット付与認証の基本接続プロパティを示します。

プロパティ	説明
サービス URL	Microsoft Dynamics 365 for Operations サービスの URL。 URL は次の形式で入力します。 <code>https:<server name>:<port number></code> 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。
アプリケーション ID	Microsoft Dynamics 365 for Operations の AAD 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。

詳細設定

次の表に、詳細接続のプロパティを示します。

プロパティ	説明
再試行エラーコード	Microsoft Dynamics 365 for Sales 接続が再試行するネットワーク要求または操作の一時的な問題またはエラーの HTTP エラーコード。 HTTP エラーコードはカンマで区切って入力することができます。
RETRY_COUNT	指定した再試行間隔によって決定される、Microsoft Dynamics 365 for Operations エンドポイントから応答を取得するための再試行の合計回数。 デフォルトは 0 です。 再試行回数を有効にしてタスクを実行すると、Microsoft Dynamics 365 for Operations サーバーがダウンしている場合、またはセキュリティで保護されたエージェントから到達できない場合に、タスクの応答が停止します。
再試行間隔	Microsoft Dynamics 365 for Operations 接続が応答の受信を再試行するまでに待機する時間（秒単位）。 デフォルトは 60 秒です。

プロキシサーバーの設定

組織が送信プロキシサーバーを使用してインターネットに接続している場合、サーバーレスランタイム環境を使用して、プロキシサーバー経由で Informatica Intelligent Cloud Services に接続できます。

認証されていないプロキシサーバーまたは認証されたプロキシサーバーを使用できます。マッピングと詳細モードのマッピングでプロキシを設定できます。

サーバーレスランタイム環境のプロキシの設定を行うには、Administrator のヘルプの「ランタイム環境」を参照してください。

第 132 章

Microsoft Dynamics 365 for Sales 接続

Microsoft Dynamics 365 for Sales との間でデータの安全な読み取りと書き込みを行うための Microsoft Dynamics 365 for Sales 接続を作成します。

認証の準備

OAuth 2.0 パスワード付与認証、OAuth 2.0 クライアント証明書付与認証、および OAuth 2.0 クライアントシークレット付与認証を設定して、オンラインまたはオンプレミスでデプロイされた Microsoft Dynamics 365 for Sales に接続できます。

接続プロパティを設定する前に、使用する認証のタイプに基づいて認証の詳細を用意しておく必要があります。

OAuth 2.0 パスワード付与

オンラインまたはオンプレミスにデプロイされた Microsoft Dynamics 365 for Sales にアクセスするための OAuth 2.0 パスワード付与認証を設定するには、Microsoft Dynamics 365 for Sales のユーザー名とパスワードが必要です。さらに、オンプレミスにデプロイされたインスタンス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。

これらの詳細を取得する場合、組織の管理者はオンプレミス Microsoft Dynamics 365 for Sales アプリケーションを Azure Active Directory に登録する必要があります。

Azure Active Directory への登録手順の詳細については、「[Register your application](#)」を参照してください。

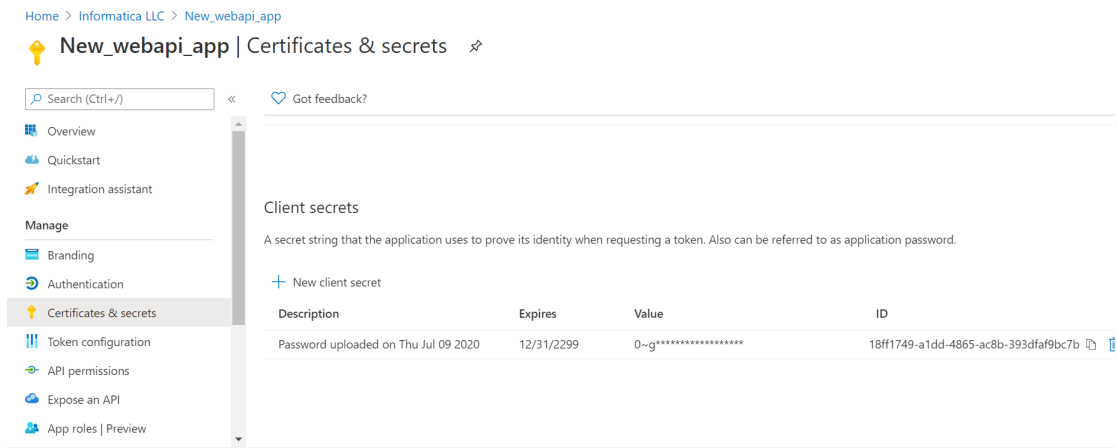
OAuth 2.0 クライアントシークレット付与

OAuth 2.0 クライアントシークレット付与認証を使用して Microsoft Dynamics 365 for Sales にアクセスするには、クライアントシークレットが必要です。

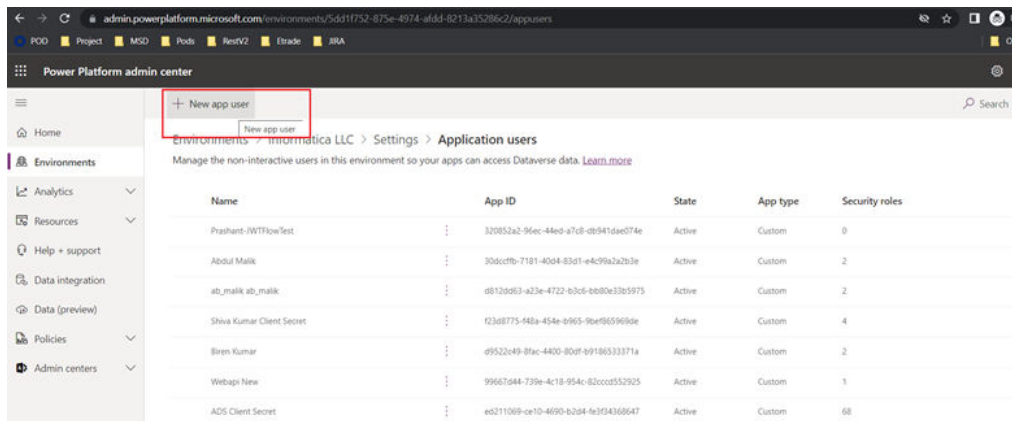
クライアントシークレットを取得するには、Microsoft Dynamics 365 for Sales Web アプリケーションを登録し、登録したアプリケーションに新しいアプリケーションユーザーを作成する必要があります。

登録したアプリケーションに新しいアプリケーションユーザーを作成するには、次のタスクを実行します。

1. Azure Active Directory の Azure 登録アプリケーションページに移動します。
2. アプリケーションを選択します。

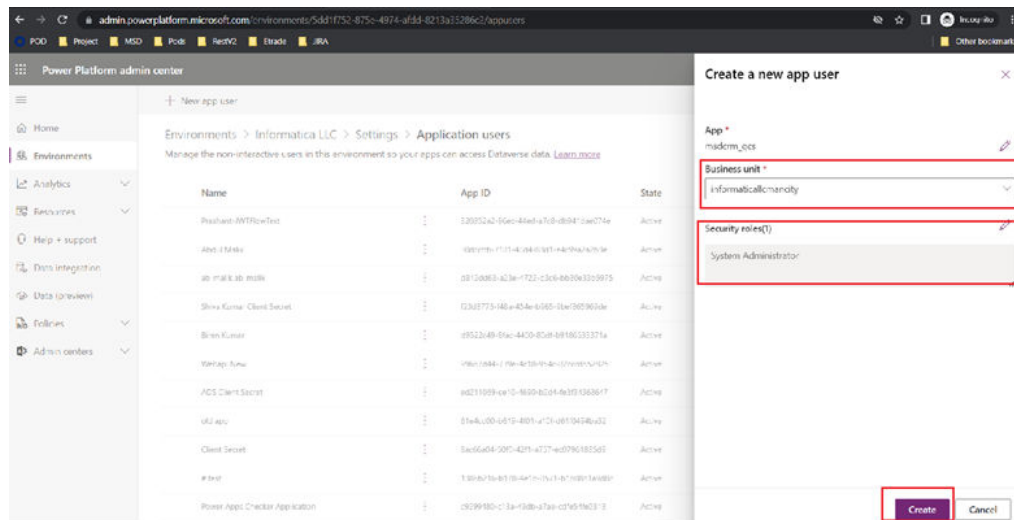


3. **【新しいクライアントシークレット】** をクリックしてクライアントシークレットを生成します。
4. <https://admin.powerplatform.microsoft.com/> にログインして、登録したアプリケーションに新しいアプリケーションユーザーを作成します。
5. **【環境】** に移動し、必要な環境を選択します。
6. 環境の **【設定】** オプションで、**【ユーザー+権限】** をクリックします。
7. **【アプリケーションユーザー】** オプションを選択します。
8. **【+新規アプリケーションユーザー】** をクリックします。



右側に、アプリケーションとユーザーの詳細を要求するためのタブが開きます。

9. 新しいアプリケーションユーザーを作成して次の図に示すように詳細を入力します。



新しいアプリケーションユーザーのアプリケーション、ビジネスユニット、およびセキュリティロールを選択できます。

10. 【作成】をクリックします。

生成されたアプリケーション ID とクライアントシークレットは、Microsoft Dynamics 365 for Sales 接続で使えるように保管しておいてください。

OAuth 2.0 クライアント証明書付与

クライアント証明書付与認証タイプを使用するには、有効なクライアント証明書が必要です。

クライアント証明書を取得するには、Microsoft Dynamics 365 for Sales Web アプリケーションを登録し、登録したアプリケーションに新しいアプリケーションユーザーを作成する必要があります。

コマンドラインから、任意のマシンで次のコマンドを実行し、Azure Active Directory アプリケーションの証明書を使用します。

- パブリックキーとプライベートキーのペアを作成するには、次のコマンドを実行します。
`keytool -genkey -alias <keypair_name1> -keyalg <key_algorithm> -validity <number_days> -keystore <生成された証明書のパスとファイル名> -storetype <store_type> -keypass <key_password> -storepass <store_password>`
 例: `keytool -genkey -alias keyalias -keyalg RSA -validity 1825 -keystore "C:\Cdrive\Cloud\R27\MSDCRM_WebAPI\MSDCRM_WebAPI\certificate\iicsdummy.com\federated.jks" -storetype JKS -keypass keypassword -storepass changeit`
- ルート CA 証明書とそれに続くユーザーの署名付き証明書をキーストアにインポートするには、次のコマンドを実行します。
 - `keytool -import -trustcacerts -alias <keypair_name2> -file <CA_certificate_name> -keystore <path and file name of the generated certificate>`
`keytool -import -trustcacerts -alias <keypair_name2> -file <CA_certificate_name> -keystore <path and file name of the generated certificate>`

- b. `keytool -import -trustcacerts -alias <keypair_name1> -file <user's_signed_certificate_name> -keystore <生成された証明書のパスとファイル名>`

例: `keytool -import -trustcacerts -alias keyalias -file b2024001944cdb12.crt -keystore "C:\Cdrive\Cloud\R27\MSDCRM_WebAPI\MSDCRM_WebAPI\certificate\iicsdummy.com\federated.jks"`

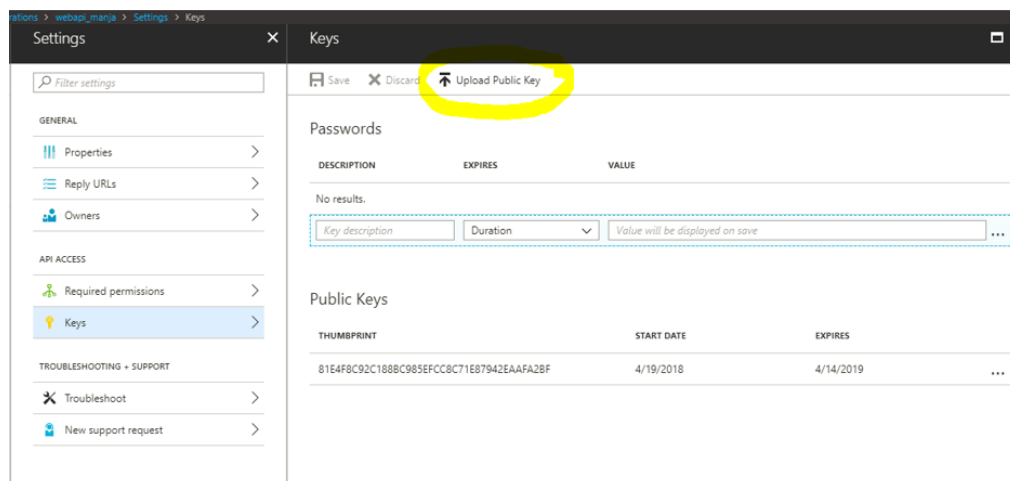
注: これらの手順は、CA から受信したファイルのタイプに応じて異なる場合があります。すべての証明書を含む 1 つのファイルを受け取った場合は、手順 b のみを実行します。自己署名証明書に対しては、これらの手順を実行しないでください。

3. キーストアから証明書をエクスポートするには、次のコマンドを実行します。

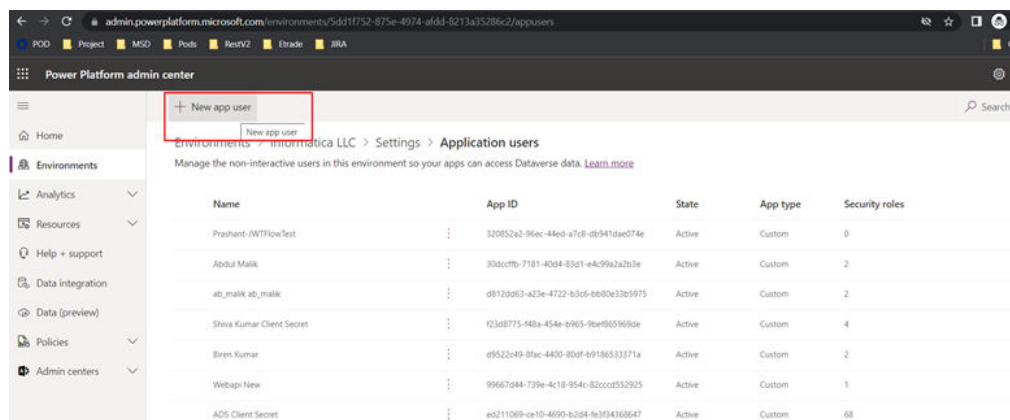
`keytool -export -alias <keypair_name1> -file <certificate_name> -keystore <生成された証明書のパスとファイル名>`

例: `keytool -export -alias keyalias -file keyalias.crt -keystore "C:\Cdrive\Cloud\R27\MSDCRM_WebAPI\MSDCRM_WebAPI\certificate\iicsdummy.com\federated.jks"`

4. 新しい Web アプリケーションの下に証明書またはパブリックキーをアップロードします。

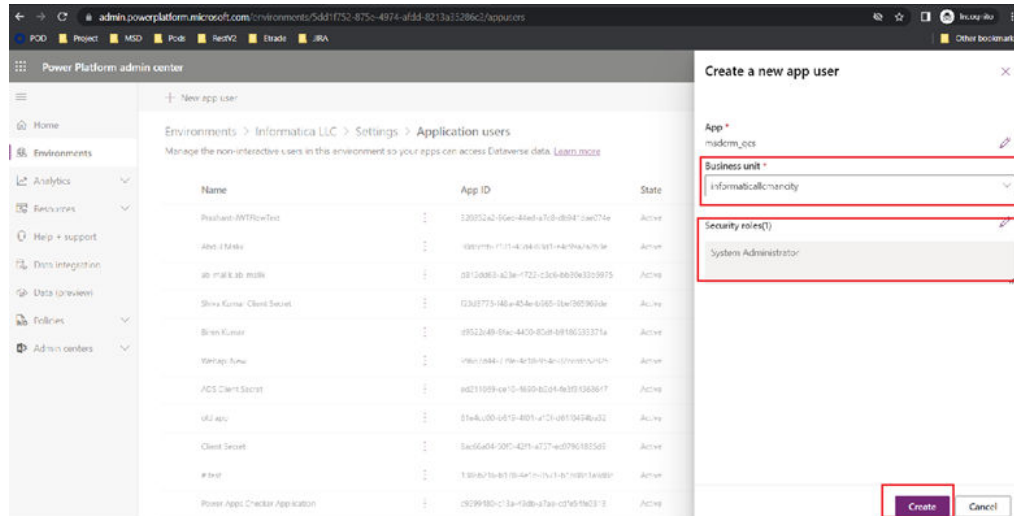


5. <https://admin.powerplatform.microsoft.com/>にログインして、登録したアプリケーションに新しいアプリケーションユーザーを作成します。
6. **【環境】**に移動し、必要な環境を選択します。
7. 環境の**【設定】**オプションで、**【ユーザー+権限】**をクリックします。
8. **【アプリケーションユーザー】**オプションを選択します。
9. **【+新規アプリケーションユーザー】**をクリックします。



右側に、アプリケーションとユーザーの詳細を要求するためのタブが開きます。

10. 新しいアプリケーションユーザーを作成して、次の図に示すように詳細を入力します。



新しいアプリケーションユーザーのアプリケーション、ビジネスユニット、およびセキュリティロールを選択できます。

11. **【作成】** をクリックします。

生成されたアプリケーション 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は、Microsoft Dynamics 365 for Sales 接続で使用できるように保管しておいてください。

Microsoft Dynamics 365 for Sales への接続

Microsoft Dynamics 365 for Sales に接続するように Microsoft Dynamics 365 for Sales 接続プロパティを設定してみましょう。

始める前に

開始する前に、組織の管理者は、オンラインまたはオンプレミスにデプロイされた Microsoft Dynamics 365 for Sales アプリケーションを Azure Active Directory に登録する必要があります。

Microsoft Dynamics 365 for Sales にアクセスするために設定する認証タイプに基づいて、Microsoft Dynamics 365 for Sales および Azure Active Directory (AAD) アカウントから情報を取得する必要があります。

認証の前提条件の詳細については、「[認証の準備](#)」(ページ 444)を参照してください。

接続の詳細

次の表に、基本接続プロパティを示します。

財産	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。
シークレットコンテナの使用	組織に対して設定されている Secrets Manager にこの接続の機密資格情報を保存します。 このプロパティは、組織に Secrets Manager が設定されている場合にのみ表示されます。 このプロパティは、データ取り込みおよびレプリケーションとデータアクセス管理サービスではサポートされていません。 接続でシークレットコンテナを有効にすると、Secure Agent が Secrets Manager からどの資格情報を取得するかを選択できます。このオプションを無効にした場合、資格情報は組織の設定方法に応じてリポジトリまたはローカル Secure Agent に保存されます。 注: この接続を使用してプッシュダウンまたはプロキシサービスを介してデータアクセスポリシーを適用する場合、シークレットコンテナ設定オプションを使用することはできません。 Secrets Manager を設定および使用する方法については、Administrator のヘルプにある「Secrets Manager の設定」を参照してください。
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。 Secure Agent、ホステッドエージェント、サーバーレスランタイム環境、またはエラスティックランタイム環境を選択します。 ランタイム環境の設定および使用方法の詳細については、Administrator のヘルプにある「ランタイム環境」を参照してください。 ホステッドエージェントを使用して Microsoft Dynamics 365 for Sales にアクセスする場合は、接続で OAuth 2.0 パスワード付与認証を使用する必要があります。

認証タイプ

インスタンスがデプロイされている場所、およびデータ統合から Microsoft Dynamics 365 for Sales にアクセスするための Microsoft Dynamics 365 for Sales 接続プロパティの該当する認証タイプに基づいて、Microsoft Dynamics 365 for Sales サーバーのタイプをオンプレミスまたはオンラインとして選択できます。

注: セキュリティを強化するには、OAuth 2.0 シークレット付与または OAuth 2.0 証明書付与認証タイプを使用した接続の確立を検討してください。

OAuth 2.0 パスワード付与認証

OAuth 2.0 パスワード付与認証を設定して、オンラインまたはオンプレミスにデプロイされた Microsoft Dynamics 365 for Sales に接続できます。

次の表に、OAuth 2.0 パスワード付与認証の基本接続プロパティを示します。

プロパティ	説明
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	Azure Active Directory に登録されている Microsoft Dynamics 365 for Sales のアプリケーション ID。
サーバータイプ	<p>アクセスする Microsoft Dynamics 365 for Sales サーバー。</p> <p>次のリストからサーバータイプを選択できます。</p> <ul style="list-style-type: none"> - 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	<p>Microsoft Dynamics 365 for Sales セキュリティトークンサービスの URL。</p> <p>この URL は、オンプレミス Microsoft Dynamics 365 for Sales にアクセスする場合に必要です。</p> <p>セキュリティトークンサービス URL を次の形式で指定します: <code>https://sts1.<company>.com/adfs/oauth2/token</code></p>

OAuth 2.0 クライアントシークレット付与認証

オンラインで Microsoft Dynamics 365 for Sales に接続するときに、OAuth 2.0 クライアントシークレット付与認証を設定できます。

次の表に、OAuth 2.0 クライアントシークレット付与認証の基本接続プロパティを示します。

プロパティ	説明
Web API URL	Microsoft Dynamics 365 for Sales エンドポイントの URL。
アプリケーション ID	Azure Active Directory に登録されている Microsoft Dynamics 365 for Sales のアプリケーション 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 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	<p>アクセスする Microsoft Dynamics 365 for Sales サーバー。</p> <p>オンラインでデプロイされた Microsoft Dynamics 365 for Sales に接続するには、Microsoft Dynamics Online サーバーのタイプを選択します。</p>

OAuth 2.0 クライアント証明書付与認証

Microsoft Dynamics 365 for Sales Online に接続するための OAuth 2.0 クライアント証明書付与認証を設定できます。

次の表に、OAuth 2.0 クライアント証明書付与認証の基本接続プロパティを示します。

プロパティ	説明
Web API URL	Microsoft Dynamics 365 for Sales エンドポイントの URL。
アプリケーション ID	Azure Active Directory に登録されている Microsoft Dynamics 365 for Sales のアプリケーション 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。 このプロパティは、ホステッドエージェント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は、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/<証明書ファイル>
キーストアのパスワード	通信を安全に行うために必要なキーストアファイルのパスワードです。
キーエイリアス	キーストアファイル内の個々のキーの別名。
キーパスワード	強化された安全な通信に使用されるキーストアファイル内の個々のキーのパスワード。 このプロパティは、ホステッドエージェントを使用する場合には適用されません。
サーバータイプ	アクセスする Microsoft Dynamics 365 for Sales サーバー。 オンラインでデプロイされた Microsoft Dynamics 365 for Sales に接続するには、Microsoft Dynamics Online サーバーのタイプを選択します。

詳細設定

次の表に、詳細接続のプロパティを示します。

プロパティ	説明
再試行エラーコード	Microsoft Dynamics 365 for Sales 接続が再試行するネットワーク要求または操作の一時的な問題またはエラーの HTTP エラーコード。 HTTP エラーコードはカンマで区切って入力することができます。
RETRY_COUNT	指定した再試行間隔によって決定される、Microsoft Dynamics 365 for Sales エンドポイントから応答を取得するための再試行の合計回数。 デフォルトは 5 です。
再試行間隔	Microsoft Dynamics 365 for Sales 接続が応答の受信を再試行するまでの待機時間 (秒単位)。 デフォルトは 60 秒です。

サーバーレスランタイム環境の設定

Microsoft Dynamics 365 for Sales への接続時に、サーバーレスランタイム環境を使用することを選択できます。

サーバーレス環境の設定および使用方法の詳細については、Administrator のヘルプにある「ランタイム環境」の「サーバーレスランタイム環境のセットアップ」を参照してください。

サーバーレスランタイム環境を使用している場合、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。

クライアント証明書付与認証を使用してサーバーレスランタイム環境を使用するには、クライアント証明書をサーバーレスランタイムの場所に追加する必要があります。

次のタスクを実行して、クライアント証明書付与認証で使用するサーバーレスランタイム環境を設定します。

1. AWS または Azure のサーバーレスエージェント設定用に次の構造を作成します: <補足ファイルの場所>/serverless_agent_config
2. AWS アカウントまたは Azure アカウントの次の場所にある Amazon S3 バケットあるいは Azure コンテナに証明書を追加します: <補足ファイルの場所>/serverless_agent_config/SSL
3. 次のコードスニペットをテキストエディタにコピーします。

```
version: 1
agent:
  agentAutoApply:
    general:
      sslStore:
        - fileCopy:
            sourcePath: SSL/<certificate_file_name>
```

ここで、ソースパスは AWS または Azure の証明書ファイルのディレクトリパスです。

4. 構文とインデントが有効であることを確認してから、ファイルを serverlessUserAgentConfig.yml として次の AWS または Azure の場所に保存します: <補足ファイルの場所>/serverless_agent_config.yml ファイルの実行時に、SSL 証明書が AWS または Azure の場所からサーバーレスエージェントディレクトリにコピーされます。
5. Microsoft Dynamics 365 for Sales の接続プロパティで、サーバーレスエージェントディレクトリ内の次の証明書パスを【**トラストストア**】フィールドと【**キーストア**】フィールドに指定します。
/home/cldagnt/SystemAgent/serverless/configurations/ssl_store/<cert.p12>

Microsoft Dynamics 365 for Sales 接続のトラブルシューティング

テスト接続に時間がかかる場合は、vocabularies.odata.org ドメインと login.microsoftonline.com ドメインがエージェントサーバーのネットワークファイアウォールにアクセスできることを確認してから、接続を再テストします。

詳細については、ナレッジベースの記事「[Domain access in firewall](#)」を参照してください。

第 133 章

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

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

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

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

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

OAuth 2.0 ユーザー名パスワードフロー認証の接続プロパティ

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

接続プロパティ	説明
接続名	接続の名前。この名前は、組織内で一意にする必要があります。接続名には、英数字、スペース、および次のような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。
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。 アプリケーション取り込みとレプリケーションタスクでは、Secure Agent またはサーバーレスランタイム環境を選択できます。ホステッドエージェントは使用できません。

接続プロパティ	説明
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。 <code>https://<Microsoft_Dynamics_365_org_name>.api.crm8.dynamics.com</code>
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。 <code>https://login.windows.net/common/oauth2/token</code>

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

OAuth 2.0 クライアントシークレットフロー認証の接続プロパティ

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

接続プロパティ	説明
接続名	接続の名前。この名前は、組織内で一意にする必要があります。接続名には、英数字、スペース、および次のような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。
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。 アプリケーション取り込みとレプリケーションタスクでは、Secure Agent またはサーバーレスランタイム環境を選択できます。ホステッドエージェントは使用できません。
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。

接続プロパティ	説明
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。 <code>https://<Microsoft_Dynamics_365_org_name>.api.crm8.dynamics.com</code>
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。 <code>https://login.microsoftonline.com/<tentant_id>/oauth2/token</code>

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

OAuth 2.0 JWT ベアラーフロー認証の接続プロパティ

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

接続プロパティ	説明
接続名	接続の名前。この名前は、組織内で一意にする必要があります。接続名には、英数字、スペース、および次のような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。
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。 アプリケーション取り込みとレプリケーションタスクでは、Secure Agent またはサーバーレスランタイム環境を選択できます。ホステッドエージェントは使用できません。
クライアント ID	Azure AD に登録されているアプリケーションのクライアント ID。
証明書の署名	X509 証明書の SHA-1 フィンガープリントを表す 16 進値をエンコードする Base64URL 文字列。
キーストアのパス	JSON Web Token (JWT) を検証して Microsoft Dynamics 365 との安全な接続を確立するために必要な X509 証明書を含むキーストアファイルへの絶対パス。 キーストアファイルは Java KeyStore (JKS) 形式である必要があります。
キーストアのパスワード	キーストアファイルのパスワード。
プライベートキーのエイリアス	JWT の署名に使用されるプライベートキーのエイリアス名。
プライベートキーのパスワード	プライベートキーのパスワード。

接続プロパティ	説明
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。 <code>https://login.microsoftonline.com/<tenant_id>/oauth2/token</code>
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。 <code>https://<Microsoft_Dynamics_365_org_name>.api.crm8.dynamics.com</code>
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。 <code>https://login.microsoftonline.com/<tenant_id>/oauth2/token</code>

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。

第 134 章

Microsoft Dynamics CRM 接続のプロパティ

Microsoft Dynamics CRM 接続を使用して、Microsoft Dynamics CRM オブジェクトに接続します。

重要: Microsoft Dynamics CRM コネクタは非推奨となり、メンテナンスモードに移行されました。Informatica は将来のリリースでサポートを廃止する予定です。Microsoft Dynamics 365 for Sales コネクタを使用して Microsoft Dynamics CRM にアクセスすることをお勧めします。

次の表に、Microsoft Dynamics CRM 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	接続の認証タイプ。有効な認証タイプを選択してください。次のいずれかの認証タイプを使用します。 <ul style="list-style-type: none">- Active Directory- インターネットに接続する展開 (IFD)- OAuth 認証を使用した Microsoft Live 認証 注: サーバーレスランタイム環境を使用している場合、Active Directory および IFD 認証を設定することはできません。
ユーザー名	Microsoft Dynamics CRM アカウントに接続するためのユーザー名。 OAuth を使用した Microsoft Live 認証の場合は、アプリケーション ID をユーザー名として使用します。
パスワード	Microsoft Dynamics CRM アカウントに接続するためのパスワード。 OAuth を使用した Microsoft Live 認証の場合は、クライアントシークレットをパスワードとして使用します。
組織名	Microsoft Dynamics CRM 組織名。組織名の大きい文字と小さい文字は区別されます。 OAuth を使用した Microsoft Live 認証の場合は、組織に登録されているテナント ID を使用します。
ドメイン	Microsoft Dynamics CRM ドメイン名。 IFD と Active Directory 認証のために、接続プロパティに指定するドメインを使用できます。

接続プロパティ	説明
サービス URL	<p>Microsoft Dynamics CRM サービスの URL。</p> <p>Active Directory 認証の場合は、次のいずれかの形式を使用します。</p> <p><code>http://<server.company.com>:<port></code>または <code>https://<server.company.com>:<port></code></p> <p>IFD 認証の場合は、次の形式を使用します。</p> <p><code>https://<server.company.com>:<port></code></p> <p>OAuth を使用した Microsoft Live 認証の場合は、CRM 組織サービスの Web サービス URL を指定します。</p>
セキュリティトークンサービス URL	<p>Microsoft Dynamics CRM セキュリティトークンサービス URL。例えば、<code>sts1.company.com</code> です。</p> <p>IFD 認証の場合のみ。</p>

第 135 章

Microsoft Dynamics NAV 接続のプロパティ

Microsoft Dynamics NAV 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。

重要: Microsoft Dynamics NAV コネクタは非推奨となり、メンテナンスモードに移行されました。Informatica は将来のリリースでサポートを廃止する予定です。

次の表に、Microsoft Dynamics NAV 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	NAV アカウントのユーザー名。
パスワード	NAV アカウントのパスワード。
ホスト名	NAV サーバーのホストの名前。
ポート	NAV Web サービスのポート番号。
サービスインスタンス	Web サービスのための Microsoft Dynamics NAV サーバーインスタンスの名前。
会社名	NAV 内のユーザーが属する会社名。
Domain_Name	ドメイン名。

第 136 章

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	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。
シークレットコンテナの使用	組織に対して設定されている Secrets Manager にこの接続の機密資格情報を保存します。 このプロパティは、組織に Secrets Manager が設定されている場合にのみ表示されます。 このプロパティは、データ取り込みおよびレプリケーションとデータアクセス管理サービスではサポートされていません。 接続でシークレットコンテナを有効にすると、Secure Agent が Secrets Manager からどの資格情報を取得するかを選択できます。このオプションを無効にした場合、資格情報は組織の設定方法に応じてリポジトリまたはローカル Secure Agent に保存されます。 注: この接続を使用してプッシュダウンまたはプロキシサービスを介してデータアクセスポリシーを適用する場合、シークレットコンテナ設定オプションを使用することはできません。 Secrets Manager を設定および使用する方法については、Administrator のヘルプにある「Secrets Manager の設定」を参照してください。
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。 Secure Agent 環境またはエラスティックランタイム環境を選択します。 ランタイム環境の設定および使用方法の詳細については、Administrator のヘルプにある「ランタイム環境」を参照してください。
フォルダ URI	読み取る Microsoft Excel ファイルを含むディレクトリ。 このディレクトリは、Secure Agent マシンに存在する必要があります。
最初の行をヘッダーとして扱う	ファイルの最初の行をヘッダー行として扱う必要があるかどうかを指定します。 true または false を選択します。

接続プロパティ	説明
フォルダアクセス	<p>フォルダ URI プロパティで指定されたディレクトリから複数の Microsoft Excel ファイルを読み取ります。</p> <p>デフォルトでは、このチェックボックスは選択されていません。</p>
ファイル名	<p>読み取る Microsoft Excel ファイルの名前。</p> <p>複数のファイルから読み取るために [フォルダアクセス] オプションを選択した場合は、フォルダ URI 接続プロパティで指定されたディレクトリから少なくとも 1 つのファイルの名前を指定する必要があります。</p> <p>ファイル名には .xlsx 拡張子が必要です。</p>

第 137 章

Microsoft Fabric データウェアハウスの接続プロパティ

Microsoft Fabric データウェアハウス接続を作成して、Microsoft Fabric データウェアハウスに対する安全な読み書きを行います。

前提条件

接続プロパティを設定する前に、次の前提条件を完了してください。

1. Power BI が満たすべき前提条件:

- a. ワークスペースがまだ存在しない場合は、ワークスペースを作成します。
- b. ワークスペースにレイクハウスを作成します。レイクハウスを作成するために必要な管理者特権があることを確認します。

ワークスペースとレイクハウスの作成の詳細については、「[Creating a workspace and lakehouse](#)」を参照してください。

2. Microsoft Azure ポータルが満たすべき前提条件:

- a. Microsoft Entra ID にアプリケーションを登録し、クライアント ID、テナント ID、クライアントシークレットを生成します。
Microsoft Fabric データウェアハウスコネクタでは、アプリケーションに割り当てる API 権限は必要ありません。また、アプリケーションに API 権限を割り当てた場合でも、その API 権限を削除して問題ありません。
- b. Microsoft Entra ID で、所有者またはメンバが割り当てられたセキュリティグループを作成します。
セキュリティグループの作成の詳細については、「[Creating a security group](#)」を参照してください。

3. Microsoft Entra アプリで Power BI API を使用できるようにするには、Power BI サービス管理者設定を有効にし、次いで Microsoft Entra アプリを Power BI のワークスペースに追加します。

注: Microsoft Entra アプリの[アクセスの管理]ウィンドウでは、必要な機能に応じたロールを追加できます。このウィンドウには管理者、メンバ、共同作成者、および閲覧者のロールが表示されます。最大数の機能は管理者ロールに関連付けられています。ただし、Microsoft Fabric OneLake にアクセスして読み取りおよび書き込み操作を実行するには、少なくとも共同作成者ロールが必要です。

Power BI 管理ポータルでアクセスを有効にし、ワークスペースに Microsoft Entra アプリを追加する方法の詳細については、「[Enabling access in the Power BI portal](#)」を参照してください。

Microsoft Fabric データウェアハウスへの接続

Microsoft Fabric データウェアハウスに接続するように、Microsoft Fabric データウェアハウスの接続プロパティを設定しましょう。

始める前に

開始する前に、クライアント ID、クライアントシークレット、ワークスペース名、データベース名、テナント ID の詳細を手元に用意しておく必要があります。

接続を設定する前にセットアップが完了していて、かつすべての前提条件が整っていることを確認する方法については、「[「前提条件」 \(ページ 462\)](#)」を参照してください。

接続の詳細

次の表に、基本接続プロパティを示します。

プロパティ	説明
接続名	接続の名前。 各接続名は組織内で一意である必要があります。接続名には、英数字、スペース、および次の特殊文字を含めることができます。_ . + , 最大長は 255 文字です。
説明	接続の説明。最大長は 4000 文字です。
シークレットコンテナの使用	組織に対して設定されている Secrets Manager にこの接続の機密資格情報を保存します。 このプロパティは、組織に Secrets Manager が設定されている場合にのみ表示されます。 このプロパティは、データ取り込みおよびレプリケーションとデータアクセス管理サービスではサポートされていません。 接続でシークレットコンテナを有効にすると、Secure Agent が Secrets Manager からどの資格情報を取得するかを選択できます。このオプションを無効にした場合、資格情報は組織の設定方法に応じてリポジトリまたはローカル Secure Agent に保存されます。 注: この接続を使用してプッシュダウンまたはプロキシサービスを介してデータアクセスポリシーを適用する場合、シークレットコンテナ設定オプションを使用することはできません。 Secrets Manager を設定および使用方法については、Administrator のヘルプにある「Secrets Manager の設定」を参照してください。
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。 Secure Agent、ホステッドエージェント、サーバーレスランタイム環境、またはエラスティックランタイム環境を選択します。 ランタイム環境の設定および使用方法の詳細については、Administrator のヘルプにある「ランタイム環境」を参照してください。
SQL 接続文字列	Microsoft Fabric データウェアハウスに接続する SQL 接続文字列。 接続文字列は以下の書式で指定します。 <Server>.datawarehouse.pbidedicated.windows.net
クライアント ID	サービスプリンシパル認証用の 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。

プロパティ	説明
クライアントシークレット	Azure Active Directory に登録されているアプリケーションのクライアントシークレット。
テナント ID	Azure Active Directory に登録されているアプリケーションのテナント ID。
ワークスペース	接続する Microsoft Fabric データウェアハウスのワークスペースの名前。
データベース	接続する Microsoft Fabric データウェアハウスのデータベースの名前。

詳細設定

次の表に、詳細接続のプロパティを示します。

プロパティ	説明
スキーマ名	テーブルが格納される Microsoft Fabric データウェアハウスのスキーマの名前。

Microsoft Fabric データウェアハウスにアクセスするためのプライベートリンク

Azure Private Link エンドポイントを使用して、Microsoft Fabric データウェアハウスにアクセスできます。

プライベート Azure ネットワーク経由で Microsoft Fabric データウェアハウスアカウントに接続する方法については、「[Secure connectivity to Microsoft Fabric](#)」を参照してください。

プライベート Azure ネットワークを介して詳細モードでマッピングを実行するには、必要な前提条件を満たした後で、次の追加手順を実行する必要があります。

1. Informatica Intelligent Cloud Services にログインし、**[Administrator]** をクリックします。
2. **[Administrator]** から **[詳細クラスタ]** に移動して、詳細設定を作成または変更します。

3. [詳細設定] タブで、プライベート DNS ゾーンにリンクされている [Vnet]、[サブネット]、および [IP アドレス範囲] プロパティを追加します。これにより、このサブネットの下にクラスターソースが生成され、プライベート DNS ゾーンへのアクセスが提供されます。

Platform Configuration

Advanced Configuration

Runtime Configuration

Resource group (Cluster): ?

AzureRnD

Service Principal Client ID: * ?

f57725fa-09cc

Key Vault: * ?

AKCKeyVault

Secret Name: * ?

SPClientSecKey

VNet: ?

private

Subnet:

default

IP Address Range: ?

10.0.0.0

Initialization Script Path: ?

Master Security Group ID: ?

Worker Security Group ID: ?

第 138 章

Microsoft Fabric レイクハウスの 接続プロパティ

Microsoft Fabric レイクハウス接続を作成して、Microsoft Fabric レイクハウスに対する安全な読み書きを行います。

前提条件

接続プロパティを設定する前に、次の前提条件を完了してください。

1. Power BI が満たすべき前提条件:

- a. ワークスペースがまだ存在しない場合は、ワークスペースを作成します。
- b. ワークスペースにレイクハウスを作成します。レイクハウスを作成するために必要な管理者特権があることを確認します。

ワークスペースとレイクハウスの作成の詳細については、「[Creating a workspace and lakehouse](#)」を参照してください。

2. Microsoft Azure ポータルが満たすべき前提条件:

- a. Microsoft Entra ID にアプリケーションを登録し、クライアント ID、テナント ID、クライアントシークレットを生成します。
コネクタ (Microsoft Entra ID) に登録したアプリケーションには、API 権限を割り当てる必要はありません。また、アプリケーションに API 権限を割り当てた場合でも、その API 権限を削除して問題ありません。
- b. Microsoft Entra ID で、所有者またはメンバが割り当てられたセキュリティグループを作成します。
セキュリティグループの作成の詳細については、「[Creating a security group](#)」を参照してください。

3. Microsoft Entra アプリで Power BI API を使用できるようにするには、Power BI サービス管理者設定を有効にし、次いで Microsoft Entra アプリを Power BI のワークスペースに追加します。

注: Microsoft Entra アプリの[アクセスの管理]ウィンドウでは、必要な機能に応じたロールを追加できます。このウィンドウには管理者、メンバ、共同作成者、および閲覧者のロールが表示されます。最大数の機能は管理者ロールに関連付けられています。ただし、Microsoft Fabric OneLake にアクセスして読み取りおよび書き込み操作を実行するには、少なくとも共同作成者ロールが必要です。

Power BI 管理ポータルでアクセスを有効にし、ワークスペースに Microsoft Entra アプリを追加する方法の詳細については、「[Enabling access in the Power BI portal](#)」を参照してください。

Microsoft Fabric レイクハウスへの接続

Microsoft Fabric レイクハウスに接続するように、Microsoft Fabric レイクハウスの接続プロパティを設定しましょう。

始める前に

開始する前に、クライアント ID、クライアントシークレット、テナント ID、ワークスペース、データベースの詳細を手元に用意しておく必要があります。

接続を設定する前にセットアップが完了していて、かつすべての前提条件が整っていることを確認する方法については、「[「前提条件」 \(ページ 466\)](#)」を参照してください。

接続の詳細

次の表に、基本接続プロパティを示します。

プロパティ	説明
接続名	接続の名前。 各接続名は組織内で一意である必要があります。接続名には、英数字、スペース、および次の特殊文字を含めることができます。_ . + -, 最大長は 255 文字です。
説明	接続の説明。最大長は 4000 文字です。
シークレットコンテナの使用	組織に対して設定されている Secrets Manager にこの接続の機密資格情報を保存します。 このプロパティは、組織に Secrets Manager が設定されている場合にのみ表示されます。 このプロパティは、データ取り込みおよびレプリケーションとデータアクセス管理サービスではサポートされていません。 接続でシークレットコンテナを有効にすると、Secure Agent が Secrets Manager からどの資格情報を取得するかを選択できます。このオプションを無効にした場合、資格情報は組織の設定方法に応じてリポジトリまたはローカル Secure Agent に保存されます。 注: この接続を使用してプッシュダウンまたはプロキシサービスを介してデータアクセスポリシーを適用する場合、シークレットコンテナ設定オプションを使用することはできません。 Secrets Manager を設定および使用する方法については、Administrator のヘルプにある「Secrets Manager の設定」を参照してください。
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。 Secure Agent、ホステッドエージェント、サーバーレスランタイム環境、またはエラスティックランタイム環境を選択します。 ランタイム環境の設定および使用方法の詳細については、Administrator のヘルプにある「ランタイム環境」を参照してください。
SQL 接続文字列	Microsoft Fabric レイクハウスに接続する SQL 接続文字列。 接続文字列は以下の書式で指定します。 <Server>.lakehouse.pbidedicated.windows.net
クライアント ID	サービスプリンシパル認証用の Azure Active Directory に登録されているアプリケーションのアプリケーション ID またはクライアント ID。
クライアントシークレット	Azure Active Directory に登録されているアプリケーションのクライアントシークレット。

プロパティ	説明
テナント ID	Azure Active Directory に登録されているアプリケーションのテナント ID。
ワークスペース	接続する Microsoft Fabric レイクハウスのワークスペースの名前。
データベース	接続する Microsoft Fabric レイクハウスのデータベースの名前。

Microsoft Fabric レイクハウスにアクセスするためのプライベートリンク

Azure Private Link エンドポイントを使用して、Microsoft Fabric Lakehouse にアクセスできます。

プライベート Azure ネットワーク経由で Microsoft Fabric レイクハウスアカウントに接続する方法については、「[Secure connectivity to Microsoft Fabric](#)」を参照してください。

プライベート Azure ネットワークを介して詳細モードでマッピングを実行するには、必要な前提条件を満たした後で、次の追加手順を実行する必要があります。

1. Informatica Intelligent Cloud Services にログインし、**[Administrator]** をクリックします。
2. **[Administrator]** から **[詳細クラスタ]** に移動して、詳細設定を作成または変更します。

3. **【詳細設定】** タブで、プライベート DNS ゾーンにリンクされている [Vnet]、[サブネット]、および [IP アドレス範囲] プロパティを追加します。これにより、このサブネットの下にクラスターソースが生成され、プライベート DNS ゾーンへのアクセスが提供されます。

Platform Configuration

Advanced Configuration

Runtime Configuration

Resource group (Cluster): ?

AzureRnD

Service Principal Client ID: * ?

f57725fa-09cc

Key Vault: * ?

AKCKeyVault

Secret Name: * ?

SPClientSecKey

VNet: ?

private

Subnet:

default

IP Address Range: ?

10.0.0.0

Initialization Script Path: ?

Master Security Group ID: ?

Worker Security Group ID: ?

第 139 章

Microsoft Fabric OneLake 接続のプロパティ

Microsoft Fabric OneLake 接続を作成して、Microsoft Fabric OneLake に対する安全な読み書きを行います。

前提条件

接続プロパティを設定する前に、次の前提条件を完了してください。

1. Power BI が満たすべき前提条件:

- a. ワークスペースがまだ存在しない場合は、ワークスペースを作成します。
- b. ワークスペースにレイクハウスを作成します。レイクハウスを作成するために必要な管理者特権があることを確認します。

ワークスペースとレイクハウスの作成の詳細については、「[Creating a workspace and lakehouse](#)」を参照してください。

2. Microsoft Azure ポータルが満たすべき前提条件:

- a. Microsoft Entra ID にアプリケーションを登録し、クライアント ID、テナント ID、クライアントシークレットを生成します。
コネクタ（Microsoft Entra ID）に登録したアプリケーションには、API 権限を割り当てる必要はありません。また、アプリケーションに API 権限を割り当てた場合でも、その API 権限を削除して問題ありません。
- b. Microsoft Entra ID で、所有者またはメンバが割り当てられたセキュリティグループを作成します。
セキュリティグループの作成の詳細については、「[Creating a security group](#)」を参照してください。

3. Microsoft Entra アプリで Power BI API を使用できるようにするには、Power BI サービス管理者設定を有効にし、次いで Microsoft Entra アプリを Power BI のワークスペースに追加します。

注: Microsoft Entra アプリの[アクセスの管理]ウィンドウでは、必要な機能に応じたロールを追加できます。このウィンドウには管理者、メンバ、共同作成者、および閲覧者のロールが表示されます。最大数の機能は管理者ロールに関連付けられています。ただし、Microsoft Fabric OneLake にアクセスして読み取りおよび書き込み操作を実行するには、少なくとも共同作成者ロールが必要です。

Power BI 管理ポータルでアクセスを有効にし、ワークスペースに Microsoft Entra アプリを追加する方法の詳細については、「[Enabling access in the Power BI portal](#)」を参照してください。

Microsoft Fabric OneLake への接続

Microsoft Fabric OneLake に接続するように、Microsoft Fabric OneLake の接続プロパティを設定しましょう。

始める前に

開始する前に、ワークスペース名、レイクハウスパス、クライアント ID、クライアントシークレット、テナント ID などの詳細を手元に用意しておく必要があります。

接続を設定する前にセットアップが完了していて、かつすべての前提条件が整っていることを確認する方法については、「[「前提条件」 \(ページ 470\)](#)」を参照してください。

接続の詳細

次の表に、基本接続プロパティを示します。

プロパティ	説明
接続名	接続の名前。 各接続名は組織内で一意である必要があります。接続名には、英数字、スペース、および次の特殊文字を含めることができます。_ . + - , 最大長は 255 文字です。
説明	接続の説明。最大長は 4000 文字です。
シークレットコンテナの使用	組織に対して設定されている Secrets Manager にこの接続の機密資格情報を保存します。 このプロパティは、組織に Secrets Manager が設定されている場合にのみ表示されます。 このプロパティは、データ取り込みおよびレプリケーションとデータアクセス管理サービスではサポートされていません。 接続でシークレットコンテナを有効にすると、Secure Agent が Secrets Manager からどの資格情報を取得するかを選択できます。このオプションを無効にした場合、資格情報は組織の設定方法に応じてリポジトリまたはローカル Secure Agent に保存されます。 注: この接続を使用してプッシュダウンまたはプロキシサービスを介してデータアクセスポリシーを適用する場合、シークレットコンテナ設定オプションを使用することはできません。 Secrets Manager を設定および使用する方法については、Administrator のヘルプにある「Secrets Manager の設定」を参照してください。
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。 Secure Agent、ホステッドエージェント、サーバーレスランタイム環境、またはエラスティックランタイム環境を選択します。 注: ホステッドエージェントとサーバーレスランタイム環境は、アプリケーション取り込みとレプリケーション、データベース取り込みとレプリケーション、およびファイル取り込みとレプリケーションタスクではサポートされていません。 ランタイム環境の設定および使用方法の詳細については、Administrator のヘルプにある「ランタイム環境」を参照してください。
ワークスペース名	Microsoft Fabric OneLake のワークスペースの名前。 ワークスペース名に特殊文字やスペースを含めることはできません。

プロパティ	説明
レイクハウスのパス	ワークスペースに存在するレイクハウスのパスまたは名前。 パスは、次のいずれかの方法で指定できます。 - ワークスペース内のファイルにアクセスするには、 <i>ルートディレクトリ (/)</i> を使用します。 - レイクハウスに存在するファイルにアクセスするには、 <i>lakehouse name/Files</i> を使用します。
認証タイプ	Microsoft Fabric OneLake にアクセスするための認証タイプ。 サービスプリンシパル認証は、クライアント ID、クライアントシークレット、およびテナント ID を使用して Microsoft Fabric OneLake に接続します。
クライアント ID	Azure Active Directory に登録されているアプリケーションのアプリケーション ID またはクライアント ID。
クライアントシークレット	Azure Active Directory に登録されているアプリケーションのクライアントシークレット。
テナント ID	アプリケーションを作成した Azure Active Directory インスタンスの ID。
Microsoft Fabric OneLake エンドポイント	接続先の Microsoft Fabric OneLake エンドポイントのタイプ。 デフォルトは <code>[fabric.microsoft.com]</code> です。

プロキシサーバーの設定

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

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

次のいずれかのタイプのプロキシサーバーを使用できます。

- 認証されていないプロキシ - 設定を行う場合はホストとポートアドレスのみが必要です。
- 認証されたプロキシ - 設定を行う場合は、ホストアドレス、ポートアドレス、ユーザー名、およびパスワードが必要です。

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

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

手順については、データ統合のヘルプの『または「Windows でのプロキシ設定」または「Linux でのプロキシ設定」を参照してください。

- Secure Agent のプロパティで、DTM の JVM オプションを設定します。手順については、ナレッジベースの記事「[Proxy server settings](#)」を参照してください。

プロキシサーバーのバイパス

Secure Agent 用に設定されたプロキシサーバー設定をバイパスできます。

プロキシサーバーをバイパスするには、次の手順を実行します。

1. 次のディレクトリに移動します。
<Secure Agent のインストールディレクトリ>/apps/agentcore
2. proxy.ini ファイルで次のコマンドを指定します。
InfaAgent.NonProxyHost=localhost|{*}onelake.blob.fabric.microsoft.com|onelake.dfs.fabric.microsoft.com |
127.0.0.1|[\:\:1]*
3. Secure Agent を再起動します。

Microsoft Fabric OneLake にアクセスするためのプライベートリンク

Azure Private Link エンドポイントを使用して、Microsoft Fabric OneLake にアクセスできます。

プライベート Azure ネットワーク経由で Microsoft Fabric OneLake アカウントに接続する方法については、「[Secure connectivity to Microsoft Fabric](#)」を参照してください。

プライベート Azure ネットワークを介して詳細モードでマッピングを実行するには、必要な前提条件を満たした後で、次の追加手順を実行する必要があります。

1. Informatica Intelligent Cloud Services にログインし、**[Administrator]** をクリックします。
2. **[Administrator]** から **[詳細クラスタ]** に移動して、詳細設定を作成または変更します。

3. [詳細設定] タブで、プライベート DNS ゾーンにリンクされている [Vnet]、[サブネット]、および [IP アドレス範囲] プロパティを追加します。これにより、このサブネットの下にクラスターソースが生成され、プライベート DNS ゾーンへのアクセスが提供されます。

Platform Configuration

Advanced Configuration

Runtime Configuration

Resource group (Cluster): ?

AzureRnD

Service Principal Client ID: * ?

f57725fa-09cc

Key Vault: * ?

AKCKeyVault

Secret Name: * ?

SPClientSecKey

VNet: ?

private

Subnet:

default

IP Address Range: ?

10.0.0.0

Initialization Script Path: ?

Master Security Group ID: ?

Worker Security Group ID: ?

第 140 章

Microsoft Power BI 接続のプロパティ

Microsoft Power BI 接続のセットアップ時に、接続プロパティを設定する必要があります。

認証の準備

Microsoft Power BI にアクセスするために、管理者ユーザー認証タイプまたはサービスプリンシパル認証タイプを設定できます。認証を設定する前に、環境の設定を行い、認証の詳細を取得しておく必要があります。

アクセスの設定

Microsoft Power BI にアクセスするには、次の手順に従って環境を設定します。

- Administrator で Microsoft Power BI ソースシステムへの接続を設定します。
- ポート 443 を有効にし、トラフィックがポート 443 を通過できるようにファイアウォールを設定します。Secure Agent はインターネットに接続するためにポート 443 を使用します。
- サービスプリンシパル認証を使用して Microsoft Power BI サービスに対して組織を認証する場合は、Power BI 管理 API への読み取り専用アクセスを有効にします。読み取り専用の管理 API に対するサービスプリンシパルの設定については、「[HOW TO: Configure Service Principal for Microsoft Power BI](#)」を参照してください。
- Power BI 管理ポータル の **【管理 API 設定】** セクションで、**【DAX およびマッシュアップ式を使用した管理者 API 応答の強化】** オプションを有効にします。
- 管理者特権またはサービスプリンシパルを使用して認証するかどうかにかかわらず、組織のプレビュー機能を有効にして、Microsoft Power BI ソースシステムからメタデータを抽出します。さらに、拡張メタデータスキャン機能を有効にして、Microsoft Power BI 環境で更新および再パブリッシュされたデータセットからリネージュを抽出します。
Microsoft Power BI でプレビューを有効にする方法については、「[HOW TO: Enable Preview in Microsoft Power BI](#)」を参照してください。
- 管理者ユーザーロールを使用して、REST API を介して Microsoft Power BI を Microsoft Azure に接続する場合は、次のタスクを実行します。
 1. 次の Power BI 管理者権限のいずれかを管理者ユーザーロールに割り当てます。
 - Microsoft 365 グローバル管理者
 - Power BI サービス管理者
 2. ワークスペースレベルで管理者アクセス権を取得します。

認証の詳細の取得

使用する認証方法に基づいて、必要なすべての認証詳細を取得していることを確認します。

管理者ユーザー

Microsoft Power BI インスタンスに接続するには、Azure Active Directory に登録されているアプリケーションのクライアント ID、ユーザー名、およびパスワードが必要です。

サービスプリンシパル

Azure Active Directory に登録されているアプリケーションのクライアント ID、クライアントシークレット、およびテナント ID が必要です。

Microsoft Power BI への接続

Microsoft Power BI に接続するように Microsoft Power BI 接続プロパティを設定します。

始める前に

開始する前に、設定する接続モードに基づいて、Microsoft Power BI アカウントから情報を取得する必要があります。

認証の前提条件の詳細については、「[「認証の準備」 \(ページ 475\)](#)」を参照してください。

接続の詳細

次の表に、基本接続プロパティを示します。

プロパティ	説明
シークレットコンテナの使用	<p>組織に対して設定されている Secrets Manager にこの接続の機密資格情報を保存します。このプロパティは、組織に Secrets Manager が設定されている場合にのみ表示されます。このプロパティは、データ取り込みおよびレプリケーションとデータアクセス管理サービスではサポートされていません。</p> <p>接続でシークレットコンテナを有効にすると、Secure Agent が Secrets Manager からどの資格情報を取得するかを選択できます。このオプションを無効にした場合、資格情報は組織の設定方法に応じてリポジトリまたはローカル Secure Agent に保存されます。</p> <p>注: この接続を使用してプッシュダウンまたはプロキシサービスを介してデータアクセスポリシーを適用する場合、シークレットコンテナ設定オプションを使用することはできません。</p> <p>Secrets Manager を設定および使用する方法については、Administrator のヘルプにある「Secrets Manager の設定」を参照してください。</p>
接続名	<p>接続の名前。</p> <p>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。_ . + - ,</p> <p>最大長は 255 文字です。</p>
説明	接続の説明。最大長は 4000 文字です。
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選択します。

プロパティ	説明
認証タイプ	接続に使用する認証タイプ。接続に使用するオプションを [管理者ユーザー] または [サービスプリンシパル] から選択します。
Power BI サービス URL	Microsoft Power BI にアクセスし、REST API に接続するための URL。例: https://api.powerbi.com/

認証タイプ

管理者ユーザー認証タイプまたはサービスプリンシパル認証タイプを使用するように Microsoft Power BI 接続を設定できます。

必要な認証タイプを選択し、認証固有のパラメータを設定します。

管理者ユーザー認証

管理者ユーザー認証には、Microsoft Power BI アカウントのユーザー名とパスワードが必要です。

次の表に、管理者ユーザー認証の接続プロパティとその説明を示します。

プロパティ	説明
クライアント ID	Microsoft Power BI クラウドホストに接続するための ID。 Microsoft Azure ポータルに登録されている Power BI アプリ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。
ユーザー名	Microsoft Power BI クラウドホストに接続するための管理者のユーザー名。
パスワード	Microsoft Power BI サーバーに接続するための管理者アカウントのパスワード。

サービスプリンシパル認証

サービスプリンシパル認証には、Azure Active Directory に登録されているアプリケーションのテナント ID とクライアントシークレットが必要です。

次の表に、サービスプリンシパル認証の接続プロパティとその説明を示します。

プロパティ	説明
認証 URL	ユーザー認証用の URL。
スコープ	エンドポイントでユーザーの認証に使用されるパラメータ。
クライアント ID	Microsoft Power BI クラウドホストに接続するための ID。 Microsoft Azure ポータルに登録されている Power BI アプリ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。
テナント ID	Azure Active Directory テナントの名前。
クライアントシークレット	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。

プロキシのプロパティ

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

以下のプロパティを指定します。

プロパティ	説明
プロキシホスト	送信プロキシサーバーのホスト名または IP アドレス。
プロキシポート	送信プロキシサーバーのポート番号。
プロキシユーザー名	プロキシサーバーの認証済みのユーザーの名前。 プロキシサーバーで認証が必要となる場合に必須です。
プロキシパスワード	認証されたユーザーのパスワード。 プロキシサーバーで認証が必要となる場合に必須です。

第 141 章

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	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。
シークレットコンテナの使用	組織に対して設定されている Secrets Manager にこの接続の機密資格情報を保存します。 このプロパティは、組織に Secrets Manager が設定されている場合にのみ表示されます。 このプロパティは、データ取り込みおよびレプリケーションとデータアクセス管理サービスではサポートされていません。 接続でシークレットコンテナを有効にすると、Secure Agent が Secrets Manager からどの資格情報を取得するかを選択できます。このオプションを無効にした場合、資格情報は組織の設定方法に応じてリポジトリまたはローカル Secure Agent に保存されます。 注: この接続を使用してプッシュダウンまたはプロキシサービスを介してデータアクセスポリシーを適用する場合、シークレットコンテナ設定オプションを使用することはできません。 Secrets Manager を設定および使用する方法については、Administrator のヘルプにある「Secrets Manager の設定」を参照してください。
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。 Secure Agent 環境またはエラスティックランタイム環境を選択します。 ランタイム環境の設定および使用方法の詳細については、Administrator のヘルプにある「ランタイム環境」を参照してください。
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。

プロパティ	説明
SharePoint の URL	<p>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: <code>https://infasharepoint.abcd.com/ Site/_vti_bin/Data.svc</code></p>
UTC オフセット	<p>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。</p> <p>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。</p>
添付ファイルパス	<p>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。</p>
バッチサイズ	<p>Microsoft SharePoint サーバーから取得する行数を定義します。</p>
ロギングの有効化	<p>ロギングを有効化するチェックボックスを選択します。</p>

第 142 章

Microsoft Sharepoint Online 接続のプロパティ

Microsoft SharePoint Online に接続するための Microsoft SharePoint Online 接続を作成します。

Microsoft SharePoint Online アプリケーションでデータを整理し、サブサイトアカウントを設定している場合は、Microsoft SharePoint Online のサブサイトに接続することもできます。

認証の準備

Access Control Service 認証タイプと Microsoft Entra ID 認証タイプを設定して、Microsoft SharePoint Online にアクセスできます。Microsoft SharePoint Online により安全に接続するために、Microsoft Entra ID 認証の使用を検討してください。

接続プロパティを設定する前に、使用する認証のタイプに基づいて認証の詳細を用意しておく必要があります。

Access Control Service

Microsoft SharePoint Online では、Access Control Service にアプリケーションを登録してアプリ専用アクセスを許可することができ、管理者は SharePoint 管理センターを通じてサイトアクセスを制限できます。

クライアント ID とクライアントシークレットの生成

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 クライアント ID とクライアントシークレット。

1. Microsoft SharePoint Online アカウントにログインします。
2. 次のサイトまたはサブサイトの URL を入力します。
サイト: `https://<sitename.com>/_layouts/15/appregnew.aspx`
サブサイト: `https://<sitename.com>/<subsitdomain>/_layouts/15/appregnew.aspx`
【アプリ情報】 ページが表示されます。
3. 【クライアント ID】 フィールドの隣にある 【生成】 をクリックします。

クライアント ID の値が、**【クライアント ID】** フィールドに表示されます。次の図は、クライアント ID とクライアントシークレットの値を生成できる **【アプリ情報】** ページを示しています。

Client Id:

Client Secret:

Title:

App Domain:
Example: "www.contoso.com"

Redirect URL:
Example: "https://www.contoso.com/default.aspx"

4. **【クライアントシークレット】** フィールドの隣にある **【生成】** をクリックします。
クライアントシークレットの値が、**【クライアントシークレット】** フィールドに表示されます。
5. **【タイトル】** フィールドに、アプリケーションの適切なタイトルを入力します。
6. アプリケーションのドメイン名を **【アプリドメイン】** フィールドに入力します。
例: www.google.com
7. **【リダイレクト URL】** フィールドに URL を入力します。
例: https://localhost/接続プロパティに同じリダイレクト URL を入力する必要があります。
8. **【作成】** をクリックします。
ページが Microsoft SharePoint Online ページにリダイレクトされ、次のメッセージが表示されます。
アプリ ID が正常に作成されました。
クライアント ID、クライアントシークレット、タイトル、およびリダイレクト URL の値が表示されます。

ベアラーレلمの生成

ベアラーレلمは、ユーザーごとに提供される一意の ID です。認証コードを取得するためのベアラーレلمを生成します。

1. PostMan アプリケーションを開きます。
2. PostMan アプリケーションに次のサイトまたはサブサイトの URL を入力します。
サイト: https://<sitename.com>/_layouts/15/appregnew.aspx
サブサイト: https://<sitename.com>/<subsitdomain>/_layouts/15/appregnew.aspx
次の画像は、ベアラー領域の値を生成できる **【BearerToken】** ページを示しています。

GET Params

Authorization Headers (1) Body Pre-request Script Tests

Key	Value	Description
<input checked="" type="checkbox"/> Authorization	Bearer	
New key	Value	Description

3. **【GET】** メソッドを選択します。
4. **【ヘッダー】** タブで、**【キー】** フィールドに **【Authorization】** と入力し、**【値】** フィールドに **【Bearer】** と入力します。

5. **【送信】** をクリックします。
6. **【応答】** ヘッダーの **【ヘッダー】** タブを選択します。
ベアラーレームの値が **【WWW-Authenticate】** セクションに表示されます。
例:
Bearer realm="77baf95d-f3e0-42b-aa08-9b798b8c177b"

認証コードの生成

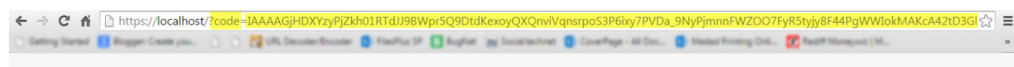
認証コードを生成して Microsoft SharePoint Online サイトまたはサブサイトにアクセスし、有効な更新トークンを生成します。

1. Google Chrome ブラウザに次のサイトまたはサブサイトの URL を入力します。
サイト: `https://<site.sharepoint.com>/_layouts/15/OAuthAuthorize.aspx?client_id=<client_GUID>&scope=<app_permissions_list>&response_type=code&redirect_uri=<redirect_uri>`
例: `https://icloudconnectivitydev.sharepoint.com/_layouts/15/oauthauthorize.aspx?client_id=ecea5b1b-80e4-4f3e-a269-48b85c1797a8&scope=AllSites.Manage&response_type=code&redirect_uri=https%3A%2F%2Flocalhost%2F`
サブサイト: `https://<site.sharepoint.com>/<subsiteid>/_layouts/15/OAuthAuthorize.aspx?client_id=<client_GUID>&scope=<app_permissions_list>&response_type=code&redirect_uri=<redirect_uri>`
例: `https://informaticaone.sharepoint.com/sites/TEST/_layouts/15/oauthauthorize.aspx?client_id=ecea5b1b-80e4-4f3e-a269-48b85c1797a8&scope=AllSites.Manage&response_type=code&redirect_uri=https%3A%2F%2Flocalhost%2F`
2. **【信頼する】** をクリックして、接続プロパティで指定したリダイレクト URL ページにページがリダイレクトされた後に、Microsoft SharePoint Online サイトまたはサブサイトへの読み取りアクセス権をアプリケーションに付与します。

リダイレクト URL ページには、認証コードが次の形式のクエリ文字列として含まれています:

`https://<redirect_url>/?code=<authcode>`

次の画像は、URI の認証コードを示しています。



注: 生成された認証コードは 5 分間有効です。

更新トークンの生成

PostMan アプリケーションで POST メソッドと GET メソッドを実行するためには、更新トークンが必要です。生成したリフレッシュトークンは、6 か月間有効です。

1. PostMan アプリケーションに次の URL を入力します。

https://accounts.accesscontrol.windows.net/<bearer_realm>/tokens/0Auth/2

次の画像は、更新トークンを生成するためのプロパティを設定する PostMan アプリケーションの **【標準】** タブを示しています。

Normal

Basic Auth

Digest Auth

OAuth 1.0

OAuth 2.0

https://accounts.accesscontrol.windows.net/d2076ad5-6179-41cb-b792-24716a55ea90/tokens/OAuth/2

POST

URL params

Headers (1)

Content-Type

application/x-www-form-urlencoded

Add preset

Manage presets

Header

Value

form-data

x-www-form-urlencoded

raw

binary

Text

1

grant_type=authorization_code&client_id=d1a29424-c89d-4195-a29e-cf5796d98dd6&code=d2076ad6-6179-41cb-b792-24716a55e&rfr=ipdryLexv%ISHr%518K4d4%3D&code=IAAAAP

Send

Preview

Pre-request script

Tests

Add to collection

Reset

2. **[POST]** メソッドを選択します。
3. **[ヘッダー]** タブで、**[キー名]** フィールドに **[Content-Type]** と入力し、**[値]** フィールドに **[application/x-www-form-urlencoded]** と入力します。
4. **[本文]** タブで、XML 要求を次の形式で入力します：

```
grant_type=authorization_code &client_id=<client_id>@<bearer_realms> &client_secret=<client_secret>
&code=<auth_code> &redirect_uri=<redirect_url> &resource=< audience principal ID >/
<site host>@<bearer realms>
```

5. **[送信]** をクリックします。
- [応答]** タブで更新トークンが生成されます。

次の画像は、更新トークンが生成される [応答] タブを示しています。

[illegible]

Microsoft Entra ID

Microsoft Entra ID を使用すると、Microsoft SharePoint Online データに安全にアクセスし、管理できます。

Azure Active Directory への Azure アプリケーションの登録

データ統合から Microsoft SharePoint Online との接続を確立するには、接続プロパティで Microsoft SharePoint Online 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。

クライアント ID とクライアントシークレットを取得するには、Microsoft ID プラットフォームを通じて Azure Active Directory (AAD) にアプリケーションを登録します。

1. Microsoft SharePoint Online の資格情報を使用して portal.azure.com にログインします。
2. [Azure サービス] セクションの **【アプリの登録】** に移動します。
3. **【新規登録】** をクリックします。
4. アプリケーションの表示名とサポートされているアカウントタイプを指定し、リダイレクト URL を入力して、**【登録】** をクリックします。

アカウントタイプとして [シングルテナント] または [マルチテナント] が選択されていることを確認します。個人用の Microsoft アカウントタイプを使用することはできません。

クライアント ID が生成されます。クライアント ID をコピーし、認証コードを生成して Microsoft SharePoint 接続を設定するときに使用できるように保管しておいてください。

5. **【証明書またはシークレットを追加】** をクリックします。
6. **【新しいクライアントシークレット】** をクリックし、説明と有効期限を追加します。
クライアントシークレット値が生成されます。シークレット値をコピーし、認証コードを生成して Microsoft SharePoint 接続を設定するときに使用できるように保管しておいてください。
7. 次に、左側のペインで **【API の権限】** をクリックします。
8. **【権限の追加】** をクリックします。
9. **【SharePoint】** をクリックし、[API 権限のリクエスト] ページにある **【委任されたアクセス許可】** をクリックします。
10. サインインしているユーザーに代わってクライアントアプリケーションが持っている必要がある権限を選択します。

次のリストは、権限とそれぞれの権限によって提供されるアクセスレベルの概要を示しています。

- **AllSites.FullControl**。フルコントロールアクセス。
- **AllSites.Manage**。読み取りおよび書き込みアクセス。
- **AllSites.Read**。読み取りアクセス。
- **AllSites.Write**。書き込みアクセス。

Microsoft SharePoint Online への適切なアクセス権を確保するために、AllSites.Manage 権限を選択することを検討してください。

11. **【権限の追加】** をクリックします。

Entra ID の認証コードの生成

認証コードを生成するには、必要なクエリパラメータを含む GET メソッドを選択し、SharePoint Online アプリケーションに対して認証を行った後に、リダイレクト URL からコードを取得します。

1. PostMan アプリケーションを開きます。
2. Postman で、アカウントタイプに基づいて次のいずれかの URL を入力します。
 - シングルテナントアカウントの場合は、次の URL を入力します: `https://login.microsoftonline.com/<Single_Tenant_Id_value>/oauth2/v2.0/authorize`
 - マルチテナントアカウントの場合は、次の URL を入力します: `https://login.microsoftonline.com/organizations/oauth2/v2.0/authorize`

シングルテナントアカウントを使用している場合は、<Single_Tenant_Id_value>を、登録したアプリケーションの概要セクションにあるテナント ID に置き換えます。マルチテナントアカウントの場合は、組織のエンドポイントを使用します。

3. **【GET】** メソッドを選択します。

4. **【パラメータ】** タブで、名前と値を入力します。

アクセス権限を認証および確認するには、次のクエリパラメータを入力します。

```
client_id=<client_id> &response_type=code &redirect_uri=<redirect_URI> &scope=<sharepoint_url>/<委任された  
アクセス権限> offline_access &client_secret=<client_secret>
```

スコープクエリには、Azure アプリケーションに対する委任されたアクセス権限が含まれています。
Azure アプリケーションを Azure Active Directory に登録したときに委任されたアクセス権限として
【AllSites.Manage】 を選択した場合は、次の例に示すように、スコープクエリパラメータでアクセス権
限を指定します。

```
client_id=<client_id> &response_type=code &redirect_uri=<redirect_URI> &scope=<sharepoint_url>/  
AllSites.Manage offline_access &client_secret=<client_secret>
```

5. URL をコピーしてブラウザに貼り付けます。

6. SharePoint Online のログイン資格情報を入力します。

7. 同意画面で確認し、**【承認】** をクリックします。

リダイレクト URL ページには、認証コードが次の形式のクエリ文字列として含まれています：

```
https://<redirect_url>/?code=<authcode>
```

認証コードをコピーし、更新トークンを生成するときに使用できるように保管しておいてください。

Entra ID のリフレッシュトークンの生成

PostMan アプリケーションで更新トークンを生成します。

1. PostMan アプリケーションで、アカウントタイプに基づいて次のいずれかの URL を入力します。

- シングルテナントアカウントの場合は、次の URL を入力します：https://login.microsoftonline.com/<Single_Tenant_Id_value>/oauth2/v2.0/token
- マルチテナントアカウントの場合は、次の URL を入力します：<https://login.microsoftonline.com/organizations/oauth2/v2.0/token>

シングルテナントアカウントを使用している場合は、<Single_Tenant_Id_value>を、登録したアプリケーションの概要セクションにあるテナント ID に置き換えます。マルチテナントアカウントの場合は、組織のエンドポイントを使用します。

2. **【POST】** メソッドを選択します。

3. **【ヘッダー】** タブで、**【キー名】** フィールドに **【Content-Type】** と入力し、**【値】** フィールドに **【application/x-www-form-urlencoded】** と入力します。

4. **【本文】** タブで、XML 要求を次の形式で入力します：

```
grant_type=authorization_code &client_id=<client_id>&client_secret=<client_secret> &code=<auth_code>  
&redirect_uri=<redirect_url>
```

Azure アプリケーションを Azure Active Directory に登録したときに生成したクライアント ID とクライアントシークレットを入力する必要があります。

5. **【送信】** をクリックします。

【応答】 タブで更新トークンが生成されます。

更新トークンをコピーし、Microsoft SharePoint Online 接続を設定するときに使用できるように保管しておいてください。

Microsoft SharePoint Online への接続

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

始める前に

開始する前に、設定する認証タイプに基づいて Microsoft SharePoint Online アカウントから情報を取得する必要があります。

Access Control Service 認証を設定するには、Microsoft SharePoint Online アカウントからクライアント ID、クライアントシークレット、ベアラーレلم、認証コード、および更新コードを生成します。

Microsoft Entra ID 認証を設定するには、Microsoft SharePoint Online アカウントからクライアント ID、クライアントシークレット、および更新トークンを取得します。

これらのタスクの詳細については、「[「認証の準備」 \(ページ 481\)](#)」を参照してください。

接続の詳細

次の表に、基本接続プロパティを示します。

プロパティ	説明
接続名	接続の名前。 各接続名は組織内で一意である必要があります。接続名には、英数字、スペース、および次の特殊文字を含めることができます。_ . + , 最大長は 255 文字です。
説明	接続の説明。最大長は 4000 文字です。
シークレットコンテナの使用	組織に対して設定されている Secrets Manager にこの接続の機密資格情報を保存します。 このプロパティは、組織に Secrets Manager が設定されている場合にのみ表示されます。 このプロパティは、データ取り込みおよびレプリケーションとデータアクセス管理サービスではサポートされていません。 接続でシークレットコンテナを有効にすると、Secure Agent が Secrets Manager からどの資格情報を取得するかを選択できます。このオプションを無効にした場合、資格情報は組織の設定方法に応じてリポジトリまたはローカル Secure Agent に保存されます。 注: この接続を使用してプッシュダウンまたはプロキシサービスを介してデータアクセスポリシーを適用する場合、シークレットコンテナ設定オプションを使用することはできません。 Secrets Manager を設定および使用する方法については、Administrator のヘルプにある「Secrets Manager の設定」を参照してください。
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。 Secure Agent、ホステッドエージェント、サーバーレスランタイム環境、またはエラスティックランタイム環境を選択します。 ランタイム環境の設定および使用方法の詳細については、Administrator のヘルプにある「ランタイム環境」を参照してください。

SharePoint Online 認証タイプ

Access Control Service 認証タイプと Microsoft Entra ID 認証タイプを設定して、Microsoft SharePoint Online にアクセスできます。

必要な接続タイプを選択し、認証固有のパラメータを設定します。

Access Control Service

Access Control Service 認証を使用して、SharePoint API にアクセスできます。

次の表に、Access Control Service 認証の基本接続プロパティとその説明を示します。

プロパティ	説明
Client_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 ID を取得するには、Microsoft ID プラットフォームを通じて Azure Active Directory (AAD) にアプリケーションを登録します。
Client_Secret	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。 クライアントシークレットを取得するには、Microsoft ID プラットフォームを通じて Azure Active Directory (AAD) にアプリケーションを登録します。
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。
URL	Microsoft SharePoint Online アカウントへの URL。
Attachment_File_Path	Microsoft SharePoint Online にファイルをダウンロードまたは添付する Secure Agent マシン上のディレクトリ。

次の表に、Access Control Service 認証の詳細接続プロパティをその説明を示します。

プロパティ	説明
Subsite_URL	Microsoft SharePoint サイト内の Microsoft SharePoint Online アカウントの URL。 Microsoft SharePoint Online アプリケーションでデータを整理し、サブサイトアカウントを設定している場合は、サブサイトの URL を入力します。Microsoft SharePoint Online アカウントのサイトとサブサイトの詳細については、「 Create sites and subsites 」を参照してください。 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 Entra ID

Microsoft Entra ID 認証を使用して、Microsoft SharePoint リソースに安全にアクセスできます。

次の表に、Microsoft Entra ID 認証の基本接続プロパティを示します。

プロパティ	説明
アカウントタイプ	アプリケーションへのアクセスに使用するテナント。 次のオプションから選択します。 - シングルテナント。対象ユーザーが組織内にいる場合に選択します。 - マルチテナント。対象ユーザーに企業または教育の顧客が含まれ、マルチテナントのサポートが必要な場合に選択します。 - デフォルトは [なし] です。
シングルテナント ID	シングルテナントアカウントタイプを選択した場合にのみ必須です。 リソース、アプリケーション、デバイス、サービスへのアクセスを管理および制御するための組織の一意の ID。
Client_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 ID を取得するには、Microsoft ID プラットフォームを通じて Azure Active Directory (AAD) にアプリケーションを登録します。
Client_Secret	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。 クライアントシークレットを取得するには、Microsoft ID プラットフォームを通じて Azure Active Directory (AAD) にアプリケーションを登録します。
Refresh_Token	Microsoft SharePoint Online のリフレッシュトークン。
Redirect_URL	Microsoft Entra ID 認証には適用されません。
URL	Microsoft SharePoint Online アカウントへの URL。
Attachment_File_Path	Microsoft SharePoint Online にファイルをダウンロードまたは添付する Secure Agent マシン上のディレクトリ。

次の表に、Microsoft Entra ID 認証の詳細接続プロパティを示します。

プロパティ	説明
Subsite_URL	Microsoft SharePoint サイト内の Microsoft SharePoint Online アカウントの URL。 Microsoft SharePoint Online アプリケーションでデータを整理し、サブサイトアカウントを設定している場合は、サブサイトの URL を入力します。Microsoft SharePoint Online アカウントのサイトとサブサイトの詳細については、「 Create sites and subsites 」を参照してください。 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。

第 143 章

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。
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	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gger（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。 <i>host_name</i> は、ホスト名または IP アドレスにできます。 <i>host_name:port_number</i> 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。

プロパティ	説明
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gger (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gger DBID	PowerExchange ロgger (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gger 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 MSQ 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。 <ul style="list-style-type: none"> - 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。
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gger (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。 <i>host_name:port_number</i> 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。

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 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	<p>カスタムプロパティまたは接続プロパティのオーバーライド。カスタムプロパティとは、PowerExchange のデフォルトの設定よりも優先するために指定できるプロパティです。セミコロン (;) を区切り文字として使用して複数のプロパティを入力するか、パラメータファイルを使用して接続プロパティの上書きを指定するパラメータを指定することができます。</p> <p>例:</p> <pre><property>=<value>;<property>=<value></pre> <p>多くの場合、Informatica グローバルカスタマサポートからの指示を受けたうえで、カスタムプロパティの設定を行います。</p> <p>注: これらのプロパティは、PowerCenter の PowerExchange Client for PowerCenter (PWXPC) CDC 接続の 【PWX オーバーライド】 オプションと同じです。</p> <p>パラメータファイルを使用して接続プロパティのオーバーライドを指定するには、\$<ParameterName>の形式でパラメータを設定し、ユーザー定義パラメータ名の前にドル記号 (\$) を付けます。次に、【ランタイムオプション】 タブの 【パラメータファイル名】 フィールドにパラメータファイル名を指定することで、ユーザー定義パラメータ定義を含むパラメータファイルを使用するようにマッピングのマッピングタスクを設定します。</p> <p>注:</p> <ul style="list-style-type: none"> - マッピングおよび接続に同じパラメータを入力した場合は、接続カスタムプロパティが優先されます。 - パラメータファイルがある場合、このフィールドで指定するパラメータ名は、パラメータファイルで定義されたエントリと一致している必要があります。 <p>詳細については、「接続オーバーライドのリファレンス」の章を参照してください。</p>

第 144 章

Microsoft SQL Server 接続のプロパティ

Microsoft SQL Server に対してデータの読み取りまたは書き込みを行うための Microsoft SQL Server 接続を作成します。

認証の準備

Microsoft SQL Server に接続するようにデータベースまたは Kerberos 認証方法を設定できます。接続プロパティを設定する前に、使用する認証のタイプに基づいて認証の詳細を用意しておく必要があります。Kerberos 認証では、特定の前提条件を設定する必要があります。

注: データ取り込みおよびレプリケーションでは、Kerberos 認証はサポートされていません。

Kerberos 認証の準備

必要な構成ファイルを Secure Agent マシンに配置することで、Kerberos 認証を使用して Microsoft SQL Server データベースに接続できます。また、Kerberos 認証を使用して、SSL 対応の Microsoft SQL Server データベースに接続することもできます。

注: データ取り込みおよびレプリケーションでは、Kerberos 認証はサポートされていません。

Microsoft SQL Server に接続するように Kerberos 認証を設定する場合は、次のガイドラインを考慮してください。

- ホステッドエージェントまたはサーバーレスランタイム環境は使用できません。
- 使用する Secure Agent とデータベースサーバーが KDC サーバーに登録されていることを確認してください。
- krb5.conf ファイルに複数の KDC を追加することはできません。
- 資格情報キャッシュファイルを生成するには、以下のガイドラインを考慮してください。
 - Linux では、複数の Kerberos プリンシパルユーザーに対して資格情報キャッシュファイルを接続内に生成することができます。ただし、マッピング内で使用できる Kerberos プリンシパルユーザーは 1 人だけです。
 - Windows では、複数の Kerberos プリンシパルユーザーに対して資格情報キャッシュファイルを接続内に生成することはできません。

Kerberos 認証の設定

Kerberos 認証を使用して Linux または Windows 上の Microsoft SQL Server に接続する前に、組織管理者は前提条件のタスクを実行する必要があります。

1. Java Authentication and Authorization Service 構成ファイル（JAAS）を設定するには、次のタスクを実行します。

- a. Secure Agent マシン上に JAAS 構成ファイルを作成します。
- b. 以下のエントリを JAAS 構成ファイルに追加します。

```
JDBC_DRIVER_01 {  
  com.sun.security.auth.module.Krb5LoginModule required  
  useTicketCache=true;  
};
```

注: キーと値の各ペアは独立した行に指定してください。

2. krb5.conf ファイルを設定するには、次のタスクを実行します。

- a. Secure Agent マシン上に krb5.conf ファイルを作成します。
- b. Key Distribution Center（KDC）と管理サーバーの詳細を、次の形式で krb5.conf ファイルに追加します。

```
[libdefaults]  
default_realm = <Realm name>  
forwardable = true  
ticket_lifetime = 24h  
  
[realms]  
<REALM NAME> = {  
  kdc = <Location where KDC is installed>  
  admin_server = <Location where KDC is installed>  
}  
[domain_realm]  
<domain name or host name> = <Domain name or host name of Kerberos>  
<domain name or host name> = <Domain name or host name of Kerberos>
```

3. Secure Agent マシン上で次の環境変数を設定します。
必要な環境変数については、[「環境変数の設定」](#)（ページ 495）を参照してください。
4. Secure Agent を再起動します。
5. Secure Agent マシン上で認証情報キャッシュファイルを生成し、Kerberos 認証を使用して Microsoft SQL Server に接続するには、次のタスクを実行します。
 - a. Secure Agent マシンで次のコマンドを実行し、Microsoft SQL Server のユーザー名とレルム名を指定します。
`Kinit <user name>@<realm_name>`
 - b. オプションで、Linux 上の DB2 データベースに接続する際に、Secure Agent マシン上に指定されたディレクトリとファイル名を使用して資格情報キャッシュファイルを生成するには、次のコマンドを実行します。
`Kinit -c <Directory and file name where you want to create the credential cache> <user name>@<realm_name>`
 - c. 要求されたら、Kerberos プリンシパルユーザーのパスワードを入力します。

環境変数の設定

Kerberos 認証を使用して Microsoft SQL Server に接続するには、Secure Agent マシン上で必要な環境変数を設定する必要があります。

環境変数を設定するには、次の手順を実行します。

1. 以下の環境変数を設定します。
 - `setenv KRB5CCNAME <資格情報キャッシュファイルの絶対パスとファイル名>`
 - `setenv KRB5_CONFIG <Kerberos 構成ファイルの絶対パス>\krb5.conf`
 - `setenv JAASCONFIG <JAAS 構成ファイルの絶対パス>\<ファイル名>.conf`
2. Secure Agent を再起動します。
3. Microsoft SQL Server 接続において、**【メタデータの詳細接続のプロパティ】** フィールドに `KRB5_CONFIG`、`KRB5CCNAME`、および `JAASCONFIG` プロパティを追加します。
例えば、次の形式でプロパティを追加します。
`KRB5_CONFIG=<Absolute path of the Kerberos configuration file>\krb5.conf;KRB5CCNAME=<Absolute path of the credential cache file>/<File name>;JAASCONFIG=<Absolute path of the JAAS config file>\<File name>.conf`
注: キーと値のペアはそれぞれセミコロンで区切ってください。
4. Microsoft SQL Server 接続において、**【ランタイムの詳細接続のプロパティ】** フィールドに `KRB5_CONFIG`、`KRB5CCNAME`、および `JAASCONFIG` プロパティを追加します。
例えば、次の形式でプロパティを追加します。
`KRB5_CONFIG=<Absolute path of the Kerberos configuration file>\krb5.conf;KRB5CCNAME=<Absolute path of the credential cache file>/<File name>;JAASCONFIG=<Absolute path of the JAAS config file>\<File name>.conf`
注: キーと値のペアはそれぞれセミコロンで区切ってください。

Microsoft SQL Server への接続

Microsoft SQL Server データベースに接続するように Microsoft SQL Server 接続のプロパティを設定してみましょう。

始める前に

開始する前に、認証方法と接続先の SQL Server DB のタイプに基づいて、SQL Server DB アカウントから情報を取得する必要があります。

認証の前提条件の詳細については、[「認証の準備」 \(ページ 493\)](#)を参照してください。

接続の詳細

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。
シークレットコンテナの使用	組織に対して設定されている Secrets Manager にこの接続の機密資格情報を保存します。 このプロパティは、組織に Secrets Manager が設定されている場合にのみ表示されます。 このプロパティは、データ取り込みおよびレプリケーションとデータアクセス管理サービスではサポートされていません。 接続でシークレットコンテナを有効にすると、Secure Agent が Secrets Manager からどの資格情報を取得するかを選択できます。このオプションを無効にした場合、資格情報は組織の設定方法に応じてリポジトリまたはローカル Secure Agent に保存されます。 注: この接続を使用してプッシュダウンまたはプロキシサービスを介してデータアクセスポリシーを適用する場合、シークレットコンテナ設定オプションを使用することはできません。 Secrets Manager を設定および使用方法については、Administrator のヘルプにある「Secrets Manager の設定」を参照してください。
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。 Secure Agent、ホステッドエージェント、サーバーレスランタイム環境、またはエラスティックランタイム環境を選択します。 アプリケーション取り込みとレプリケーションタスクとデータベース取り込みとレプリケーションタスクでは、Secure Agent またはサーバーレスランタイム環境を使用できます。 ホステッドエージェントまたはエラスティックランタイム環境で、アプリケーション取り込みとレプリケーションタスクまたはデータベース取り込みとレプリケーションタスクを実行することはできません。 ランタイム環境の設定および使用方法の詳細については、Administrator のヘルプにある「ランタイム環境」を参照してください。
SQL Server のバージョン	このプロパティは使用されなくなりました。バージョンを選択しても、選択したバージョンは無視されます。

認証モード

次のいずれかの認証モードを設定して、Microsoft SQL Server データベースに接続できます。

- SQL Server 認証
- Windows 認証（非推奨）
- Active Directory パスワード認証
- Windows 認証 V2
- Kerberos 認証
- サービスプリンシパル認証

必要な認証モードを選択し、認証固有のパラメータを設定します。

データベース取り込みとレプリケーションタスクの SQL Server ソースの場合、[SQL Server 認証]、[Windows 認証 v2]、または [Active Directory パスワード] を選択する必要があります。Kerberos またはサービスプリンシパル認証モードは使用しないでください。

アプリケーション取り込みとレプリケーションタスクとデータベース取り込みとレプリケーションタスクの SQL Server ターゲットの場合、[SQL Server 認証] または [Windows 認証 v2] のいずれかを選択する必要があります。他の認証タイプは使用しないでください。

SQL Server の認証

SQL Server 認証では Microsoft SQL Server にアクセスするための Microsoft SQL Server のユーザー名とパスワードを使用します。

次の表に、SQL Server 認証の基本接続プロパティとその説明を示します。

プロパティ	説明
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
パスワード	データベースログインに使用するパスワード。パスワードにセミコロンを含めることはできません。
ホスト	データベースサーバーをホストするマシンの名前。 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、vmjcmwxsfbheng.westus.cloudapp.azure.com のように指定します。
ポート	データベースサーバーに接続するときに使用するネットワークポート番号。 デフォルトは 1433 です。
インスタンス名	Microsoft SQL Server データベースのインスタンス名。
データベース名	Microsoft SQL Server ターゲット接続のデータベース名。データベースで大文字と小文字が区別される場合は、データベース名の太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	マッピングでのオブジェクト選択時にテーブルを選択するためのスキーマ名。 マッピング内のオブジェクトを選択すると、アクセス権を持つすべてのスキーマが表示され、使用可能なスキーマからテーブルを選択できます。
コードページ	データベースサーバーのコードページ。
ドメイン	このプロパティは SQL Server 認証には適用されません。

Windows 認証

Windows 認証（非推奨）では Microsoft SQL Server にアクセスするために Microsoft Windows 認証を使用します。このオプションは、Microsoft Windows を使用してデータ統合にアクセスする場合に使用できます。

このオプションを選択する場合、Microsoft SQL Server にアクセスするために資格情報を入力する必要はなく、Secure Agent サービスを開始するユーザーアカウントが、Microsoft SQL Server データベースで使用可能になっていることを確認します。

注: Windows 認証は、Linux でホストされる Microsoft SQL Server 2017 バージョンでは使用できません。サーバーレスランタイム環境を使用している場合、Windows 認証を設定することはできません。

データ取り込みおよびレプリケーションでは、Windows Authentication v2 認証を使用します。

次の表に、Windows 認証の基本接続プロパティとその説明を示します。

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。 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、vmjcmwxsfbheng.westus.cloudapp.azure.com のように指定します。
ポート	データベースサーバーに接続するときに使用するネットワークポート番号。 デフォルトは 1433 です。
インスタンス名	Microsoft SQL Server データベースのインスタンス名。
データベース名	Microsoft SQL Server ターゲット接続のデータベース名。 データベースで大文字と小文字が区別される場合は、データベース名の大文字と小文字も区別されます。最大長は 100 文字です。 データベース名には英数字とアンダースコアのみを使用できます。
スキーマ	マッピングでのオブジェクト選択時にテーブルを選択するためのスキーマ名。 マッピング内のオブジェクトを選択すると、アクセス権を持つすべてのスキーマが表示され、使用可能なスキーマからテーブルを選択できます。
コードページ	データベースサーバーのコードページ。
ドメイン	このプロパティは Windows 認証には適用されません。

Active Directory パスワード認証

Active Directory パスワード認証では、Azure Active Directory のユーザー名とパスワードを使用して、Microsoft Azure SQL データベースの認証とアクセスを行います。

注: データベース取り込みとレプリケーションでは、初期ロードジョブのソース、および【CDC テーブル】または【ログベース】のキャプチャメソッドを使用する増分ロードジョブおよび初期ロードと増分ロードの組み合わせジョブのソースに対してこの認証モードがサポートされています。これらのジョブにこのオプションを使用する場合は、【サーバー証明書の検証】の値が False であることを確認してください。

次の表に、Active Directory パスワード認証の基本的な接続プロパティとその説明を示します。

プロパティ	説明
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
パスワード	データベースログインに使用するパスワード。パスワードにセミコロンを含めることはできません。
ホスト	データベースサーバーをホストするマシンの名前。 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、vmjcmwxsfbheng.westus.cloudapp.azure.com のように指定します。
ポート	データベースサーバーに接続するときに使用するネットワークポート番号。 デフォルトは 1433 です。
インスタンス名	Microsoft SQL Server データベースのインスタンス名。
データベース名	Microsoft SQL Server ターゲット接続のデータベース名。 データベースで大文字と小文字が区別される場合は、データベース名の大文字と小文字も区別されます。最大長は 100 文字です。 データベース名には英数字とアンダースコアのみを使用できます。
スキーマ	マッピングでのオブジェクト選択時にテーブルを選択するためのスキーマ名。 マッピング内のオブジェクトを選択すると、アクセス権を持つすべてのスキーマが表示され、使用可能なスキーマからテーブルを選択できます。
コードページ	データベースサーバーのコードページ。
ドメイン	このプロパティは、Active Directory パスワード認証には適用されません。

Windows 認証 v2

Windows 認証 V2 では、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いるデータ統合またはデータ取り込みおよびレプリケーションから Microsoft SQL Server にアクセスします。

Linux でこのオプションを選択する場合は、ドメイン名と Microsoft Windows 資格情報を入力して Microsoft SQL Server にアクセスします。

Windows でこのオプションを選択すると、エージェントは接続で指定されたユーザー資格情報のみを使用して接続をテストします。実行時に、エージェントは Secure Agent サービスを開始したユーザーの資格情報を使用します。Secure Agent サービスを開始するユーザーアカウントが、Microsoft SQL Server データベースで使用可能になっていることを確認します。

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。

次の表に、Windows 認証 v2 の基本接続プロパティとその説明を示します。

プロパティ	説明
ユーザー名	<p>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。</p> <p>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</p> <p>Windows で Windows 認証 v2 を使用した場合、ユーザー名は次のように使用されます。</p> <ul style="list-style-type: none">- 設計時に、エージェントはここで指定したユーザー名を使用して接続をテストします。- 実行時に、Microsoft SQL Server ドライバは、このフィールドに指定されたユーザー名を無視し、Secure Agent サービスを開始したユーザーの資格情報を使用します。 <p>Linux で Windows 認証 v2 を使用した場合、ここで指定したユーザー名は、設計時および実行時に使用されます。</p>
パスワード	<p>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。</p> <p>Windows で Windows 認証 v2 を使用する場合、パスワードは次のように使用されます。</p> <ul style="list-style-type: none">- 設計時に、エージェントはここで指定したパスワードを使用して接続をテストします。- 実行時に、Microsoft SQL Server ドライバは、このフィールドに指定されたパスワードを無視し、Secure Agent サービスを開始したユーザーの資格情報を使用します。 <p>Linux で Windows 認証 v2 を使用した場合、ここで指定したパスワードは、設計時および実行時に使用されます。</p>
ホスト	<p>データベースサーバーをホストするマシンの名前。</p> <p>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。</p> <p>例えば、vmjcmwxsfbheng.westus.cloudapp.azure.com のように指定します。</p>
ポート	<p>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。</p> <p>デフォルトは 1433 です。</p>
インスタンス名	<p>Microsoft SQL Server データベースのインスタンス名。</p>
データベース名	<p>Microsoft SQL Server ターゲット接続のデータベース名。</p> <p>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。</p> <p>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。</p>
スキーマ	<p>マッピングでのオブジェクト選択時にテーブルを選択するためのスキーマ名。</p> <p>マッピング内のオブジェクトを選択すると、アクセス権を持つすべてのスキーマが表示され、使用可能なスキーマからテーブルを選択できます。</p>
コードページ	<p>データベースサーバーのコードページ。</p>
ドメイン	<p>Windows ユーザーのドメイン名。</p>

Kerberos 認証

Kerberos 認証を使用して Microsoft SQL Server に接続することができます。データ取り込みとレプリケーションでは、この認証タイプはサポートされていません。

Windows でこのオプションを選択する場合は、Secure Agent サービスを開始するユーザーアカウントが、Microsoft SQL Server データベースで使用可能になっていることを確認します。Microsoft SQL Server にアクセスする際に資格情報を入力する必要はありません。

注: Hosted Agent またはサーバーレスランタイム環境を使用している場合は、Kerberos 認証を設定できません。

次の表に、Kerberos 認証の基本接続プロパティとその説明を示します。

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。 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、vmjcmwxsfbheng.westus.cloudapp.azure.com のように指定します。
ポート	データベースサーバーに接続するときに使用するネットワークポート番号。 デフォルトは 1433 です。
インスタンス名	Microsoft SQL Server データベースのインスタンス名。
データベース名	Microsoft SQL Server ターゲット接続のデータベース名。 データベースで大文字と小文字が区別される場合は、データベース名の大文字と小文字も区別されます。最大長は 100 文字です。 データベース名には英数字とアンダースコアのみを使用できます。
スキーマ	マッピングでのオブジェクト選択時にテーブルを選択するためのスキーマ名。 マッピング内のオブジェクトを選択すると、アクセス権を持つすべてのスキーマが表示され、使用可能なスキーマからテーブルを選択できます。
コードページ	データベースサーバーのコードページ。
ドメイン	このプロパティは、Kerberos 認証には適用されません。

サービスプリンシパル認証

コネクタで Secure Agent インストールディレクトリの LATEST フォルダにある JDBC および ODBC ドライバが使用されている場合は、サービスプリンシパル認証を設定できます。

注: 接続でシークレットボルトを有効にすると、Microsoft SQL Server データベースに接続するようにサービスプリンシパル認証を設定できなくなります。

サービスプリンシパル認証を設定するには、Microsoft Entra ID 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取得する必要があります。

次の表に、サービスプリンシパル認証の接続プロパティとその説明を示します。

プロパティ	説明
クライアント ID	Microsoft Entra ID に登録されているアプリケーションのクライアント ID またはアプリケーション ID。
クライアントシークレット	Microsoft Entra ID で OAuth 認証を完了するためにクライアント ID 用に生成されたクライアントシークレットキー。
ホスト	データベースサーバーをホストするマシンの名前。 Microsoft Azure SQL Database に接続するには、完全修飾ホスト名を指定します。 例えば、vmjcmwxsfboheng.westus.cloudapp.azure.com のように指定します。
ポート	データベースサーバーに接続するときに使用するネットワークポート番号。 デフォルトは 1433 です。
インスタンス名	Microsoft SQL Server データベースのインスタンス名。
データベース名	Microsoft SQL Server ターゲット接続のデータベース名。 データベースで大文字と小文字が区別される場合は、データベース名の大文字と小文字も区別されます。最大長は 100 文字です。 データベース名には英数字とアンダースコアのみを使用できます。
スキーマ	マッピングでのオブジェクト選択時にテーブルを選択するためのスキーマ名。 マッピング内のオブジェクトを選択すると、アクセス権を持つすべてのスキーマが表示され、使用可能なスキーマからテーブルを選択できます。
コードページ	データベースサーバーのコードページ。
ドメイン	このプロパティは、サービスプリンシパル認証には適用されません。

詳細設定

次の表に、詳細接続のプロパティを示します。

プロパティ	説明
暗号化方法	Secure Agent が、ドライバとデータベースサーバーとの間で送信されるデータの暗号化に使用する方法。暗号化方法を使用して、Microsoft Azure SQL Database に接続できます。 デフォルトは [なし] です。
暗号プロトコルバージョン	SSL 暗号化を有効化する際に使用する暗号プロトコル。

プロパティ	説明
サーバー証明書の検証	True に設定すると、Secure Agent が、データベースサーバーによって送信された証明書を検証します。 HostNameInCertificate パラメータを指定すると、Secure Agent は証明書内のホスト名も検証します。 False に設定すると、Secure Agent は、データベースサーバーによって送信された証明書を検証しません。
トラストストア	トラストストアファイルの場所と名前。トラストストアファイルには、ドライバが SSL サーバー認証に使用する認証局（CA）の一覧が含まれています。 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。
メタデータの詳細接続プロパティ	JDBC ドライバがメタデータを取得するための追加プロパティ。 プロパティは次の形式で入力します: <パラメータ名>=<パラメータ値> 複数のプロパティを入力する場合は、それぞれのキーと値のペアをセミコロンで区切ります。 例えば、接続をテストするときに接続タイムアウトを設定するには、次のプロパティを入力します: LoginTimeout=<value_in_seconds> 注: デフォルトの接続のタイムアウトは 270 秒です。
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な追加プロパティ。 複数のプロパティを指定する場合は、キーと値のペアをそれぞれセミコロンで区切ります。

サーバーレスランタイム環境での SSL の設定

Microsoft SQL Server コネクタでサーバーレスランタイム環境を使用して、SSL 対応の Microsoft SQL Server データベースに接続できます。

サーバーレスランタイム環境を使用して安全な Microsoft SQL Server 接続を設定する前に、次の前提条件タスクを完了して、SSL 証明書をサーバーレスランタイムの場所に追加します。

1. AWS または Azure のサーバーレスエージェント設定用に次の構造を作成します: <補足ファイルの場所>/serverless_agent_config
注: データ取り込みおよびレプリケーションは、AWS でホストされているサーバーレスランタイム環境をサポートしていません。
2. AWS アカウントまたは Azure アカウントの次の場所にある Amazon S3 バケットあるいは Azure コンテナにトラストストア証明書を追加します: <Supplementary file location>/serverless_agent_config/SSL

3. 次のコードスニペットをテキストエディタにコピーします。

```
version: 1
agent:
  agentAutoApply:
    general:
      sslStore:
        - fileCopy:
            sourcePath: SSL/<TrustStore_filename>
```

ここで、ソースパスは AWS または Azure の証明書ファイルのディレクトリパスです。

4. 構文とインデントが有効であることを確認してから、ファイルを `serverlessUserAgentConfig.yml` として次の AWS または Azure の場所に保存します: <補足ファイルの場所>/`serverless_agent_config.yml` ファイルの実行時に、SSL 証明書が AWS または Azure の場所からサーバーレスエージェントディレクトリにコピーされます。
5. Microsoft SQL Server 接続のプロパティで、**【トラストストア】** フィールドの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/<cert_filename>`

第 145 章

Mixpanel 接続のプロパティ

Mixpanel 接続を作成する際に、接続プロパティを設定します。

次の表に、Mixpanel 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。
シークレットコンテナの使用	組織に対して設定されている Secrets Manager にこの接続の機密資格情報を保存します。 このプロパティは、組織に Secrets Manager が設定されている場合にのみ表示されます。 このプロパティは、データ取り込みおよびレプリケーションとデータアクセス管理サービスではサポートされていません。 接続でシークレットコンテナを有効にすると、Secure Agent が Secrets Manager からどの資格情報を取得するかを選択できます。このオプションを無効にした場合、資格情報は組織の設定方法に応じてリポジトリまたはローカル Secure Agent に保存されます。 注: この接続を使用してプッシュダウンまたはプロキシサービスを介してデータアクセスポリシーを適用する場合、シークレットコンテナ設定オプションを使用することはできません。 Secrets Manager を設定および使用する方法については、Administrator のヘルプにある「Secrets Manager の設定」を参照してください。
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。 Secure Agent または Hosted Agent を指定します。
ユーザー名	Mixpanel アカウントのユーザー名。
パスワード	Mixpanel アカウントのパスワード。

第 146 章

MLLP 接続プロパティ

Minimal Lower Layer Protocol (MLLP) 接続を構成する場合は、接続プロパティを設定する必要があります。

次の表に、MLLP 接続プロパティを示します。

プロパティ	説明
接続名	MLLP 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	MLLP 接続の説明。最大長は 4000 文字です。
タイプ	接続タイプ。MLLP 接続の場合、このタイプは【MLLP】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。
ホスト	MLLP サーバーのホスト名または IP アドレス。
ポート	MLLP サーバーのポート番号。 デフォルトは 2575 です。
応答タイムアウト	メッセージの送信後、指定されている MLLP サーバーからのメッセージを受信するまでの待機時間（秒単位）。タイムアウト値がゼロの場合、タイムアウトが無限であるとみなされます。 デフォルトは 60 秒です。
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 30 秒です。
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。 デフォルトは 0 です。
接続の再試行	接続に成功しなかった場合に、MLLP 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。 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。

プロパティ	説明
プロキシタイプ	<p>この接続に使用するプロキシサーバーのタイプ。 次のいずれかのオプションを選択します。</p> <ul style="list-style-type: none"> - 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。 - HTTP。HTTP プロキシを使用します。 - SOCKS。SOCKS（バージョン 4 および 5）プロキシを使用します。 - 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。 <p>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。</p>
プロキシホスト	プロキシサーバーのホスト名または IP アドレス（自社ネットワーク上）。
プロキシポート	プロキシサーバーのポート番号（自社ネットワーク上）。
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。

第 147 章

MongoDB Mass Ingestion 接続のプロパティ

MongoDB 一括取り込み接続を定義するには、接続プロパティを設定します。この接続タイプは、データ取り込みおよびレプリケーションで設定したデータベース取り込みとレプリケーションタスクのソースに使用することができます。

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
接続名	接続の名前。この名前では、大文字と小文字が区別されず、ドメイン内で一意にする必要があります。このプロパティは、接続を作成した後に変更できます。名前は 255 文字以内で指定し、空白および以下の特殊文字は使用できません。 ~`!\$%^&*()-+={ }\:;'"<,>.\?/
説明	オプション。接続の説明。説明は、4,000 文字を超えることはできません。
ランタイム環境	タスクを実行するランタイム環境の名前。
ホストとポート	SRV レコード、または <i>host_name:port</i> ペアのカンマ区切りのリスト。 注: MongoDB レプリカセットモードを使用している場合は、回復機能用として複数のホスト名を入力できます。1 つのホストが使用できない場合は、指定した別のホストが使用されます。
SRV	【ホストとポート】 プロパティで SRV レコードを指定した場合は、このチェックボックスをオンにします。
認証	セキュアな接続を確立するための認証方法。次のいずれかの認証モードを選択します。 - 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 。X.509 証明書を使用して、MongoDB サーバーに接続します。 デフォルトは 【ユーザー名とパスワード】 です。
ユーザー名	【ユーザー名とパスワード】 認証を選択した場合は、データベースへのログインに使用するユーザー名を入力します。
パスワード	【ユーザー名とパスワード】 認証を選択した場合は、指定したデータベースユーザーのパスワードを入力します。

接続プロパティ	説明
SSL キーストアファイルパス	<p>[X.509] 認証を選択した場合は、安全な通信に必要なキーと証明書が含まれる Secure Agent マシン上のキーストアファイルの絶対パス。キーストアファイルは JKS 形式である必要があります。</p> <p>このプロパティを指定する前に、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。</p> <p>接続を正常にテストするには、Secure Agent が、指定されたパスワードを使用して、指定されたキーストアファイルとトラストストアファイルにアクセスできる必要があります。Secure Agent グループを使用する場合、すべてのエージェントがこれらのファイルにアクセスできる必要があります。Secure Agent が実行されているすべてのマシンにファイルのコピーを配置します。</p>
SSL キーストアパスワード	[X.509] 認証を選択した場合は、安全な通信に必要なキーストアファイルのパスワード。
SSL トラストストアファイルパス	[X.509] 認証を選択した場合は、Secure Agent マシン上の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	[X.509] 認証を選択した場合は、トラストストアファイルのパスワード。
認証データベース	指定ユーザーに関連付けられている認証データベースの名前。
レプリカセット名	ソースデータのレプリカを含む MongoDB サーバーで構成されているレプリカセットの名前。このフィールドは、MongoDB レプリカセットモードを使用している場合に関連します。
追加接続プロパティ	<p>使用する 1 つ以上の追加の MongoDB 接続文字列オプション。キーと値のペアとしてプロパティを指定します。複数のプロパティを指定する場合は、アンパサンド記号 (&) で区切ります。接続プロパティでは大文字小文字が区別されます。</p> <p>例:</p> <p>authSource=admin&replicaSet=rsprimary</p> <p>MongoDB 接続文字列オプションの詳細については、以下を参照してください: https://www.mongodb.com/docs/v5.2/reference/connection-string/#connection-string-options</p>

第 148 章

MongoDB 接続のプロパティ

MongoDB 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。

重要: MongoDB コネクタは非推奨となり、メンテナンスモードに移行されました。Informatica は将来のリリースでサポートを廃止する予定です。

次の表に、MongoDB 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 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、ホステッドエージェント、サーバーレスランタイム環境、またはエラスティックランタイム環境を選択します。 ランタイム環境の設定および使用方法の詳細については、Administrator のヘルプにある「ランタイム環境」を参照してください。
ホスト名*	MongoDB サーバーのホスト名または IP アドレス。
ポート*	MongoDB サーバーのポート番号。デフォルトは 27017 です。
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。
データベース名	接続する MongoDB データベースの名前。

プロパティ	説明
追加接続プロパティ	<p>MongoDB 接続に必要な 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> JDBC パラメータは、キーと値のペアをアンパサンドで区切って指定します。 MongoDB 接続では、次の JDBC 接続パラメータを設定します。</p> <ul style="list-style-type: none"> - AuthSource - BatchSize - connectTimeoutMS - DefaultStringColumnLength - DmlBatchSize - EnableDoubleBuffer - EnableTransaction - LogLevel - LogPath - SamplingLimit - SamplingStepSize - SamplingStrategy <p>以下に例を示します。 DefaultStringColumnLength=512&DmlBatchSize=1000& EnableDoubleBuffer=false&EnableTransaction=true& SamplingLimit=200&SamplingStepSize=2&SamplingStrategy=Backwards</p>
SSL モード	<p>接続に使用する暗号化タイプを示す SSL モード。 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。 注: MongoDB Atlas に接続するために 【必須】 に設定します。</p>
SSL トラストストアパス	MongoDB コネクタには適用されません。
SSL トラストストアパスワード	MongoDB コネクタには適用されません。
*接続プロパティと追加接続プロパティのフィールドに、MongoDB サーバーのホスト名、ポート、ユーザー名、およびパスワードを指定した場合、追加接続プロパティの値が優先されます。	

MongoDB JDBC 接続パラメータの設定の詳細については、Informatica How-To ライブラリの記事「Configuring the Simba MongoDB JDBC Driver Options for MongoDB Connector」を参照してください。

<https://docs.informatica.com/integration-cloud/cloud-data-integration-connectors/h2l/configuring-the-simba-mongodb-jdbc-driver-options-for-mongodb-co/abstract.html>

第 149 章

MongoDB V2 接続のプロパティ

MongoDB V2 接続を作成して、MongoDB 内のコレクションに対してデータの読み取りまたは書き込みを行います。

認証の準備

MongoDB にアクセスするために、ユーザー名とパスワード、X.509 標準認証、および LDAP 認証タイプを設定できます。

接続プロパティを設定する前に、管理者特権が割り当てられた MongoDB ユーザーアカウントがあることを確認してください。また、MongoDB のプライマリノードのホスト名をコピーし、使用する認証タイプに基づいて認証の詳細を手元に用意しておく必要があります。

ユーザー名およびパスワード

ユーザー名とパスワード認証を使用して MongoDB に接続するには、MongoDB アカウントのユーザー名、パスワード、およびデータベース名が必要です。

接続先の MongoDB アカウントから必要な詳細を取得します。

MongoDB のユーザー名とパスワード認証の詳細については、[「Authenticate a user with self-managed deployments」](#)を参照してください。

X.509 標準

X.509 標準認証を使用して MongoDB に接続するには、SSL キーストアファイル、SSL キーストアファイルのパスワード、およびデータベース名が必要です。

接続先の MongoDB アカウントから必要な詳細を取得します。

MongoDB の X.509 標準認証の詳細については、[「X.509 certificate」](#)を参照してください。

LDAP

LDAP 認証を使用して MongoDB に接続するには、MongoDB アカウントのユーザー名、パスワード、およびデータベース名が必要です。

LDAP 認証を使用する前に、次のタスクを完了してください。

1. MongoDB Atlas アカウントにログインします。
2. 使用する LDAP サーバーを設定します。

3. 認証ドメイン、サーバー URL、および資格情報を使用して LDAP 統合を作成します。

MongoDB の LDAP 認証の詳細については、「[LDAP authorization on self-managed deployments](#)」を参照してください。

注: 詳細モードのマッピングでは、LDAP 認証で設定された接続を使用することはできません。

MongoDB への接続

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

始める前に

開始する前に、設定する認証タイプに基づいて、関連する設定の詳細を MongoDB アカウントから取得する必要があります。

認証の前提条件の詳細については、「[「認証の準備」 \(ページ 512\)](#)」を参照してください。

接続の詳細

次の表に、基本接続プロパティを示します。

財産	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。
シークレットコンテナの使用	組織に対して設定されている Secrets Manager にこの接続の機密資格情報を保存します。このプロパティは、組織に Secrets Manager が設定されている場合にのみ表示されます。このプロパティは、データ取り込みおよびレプリケーションとデータアクセス管理サービスではサポートされていません。 接続でシークレットコンテナを有効にすると、Secure Agent が Secrets Manager からどの資格情報を取得するかを選択できます。このオプションを無効にした場合、資格情報は組織の設定方法に応じてリポジトリまたはローカル Secure Agent に保存されます。 注: この接続を使用してプッシュダウンまたはプロキシサービスを介してデータアクセスポリシーを適用する場合、シークレットコンテナ設定オプションを使用することはできません。 Secrets Manager を設定および使用方法については、Administrator のヘルプにある「Secrets Manager の設定」を参照してください。
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。 Secure Agent、サーバーレスランタイム環境 ¹ 、またはエラスティックランタイム環境を選択します。 ランタイム環境の設定および使用方法の詳細については、Administrator のヘルプにある「ランタイム環境」を参照してください。
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。

財産	説明
サービスレコードルックアップが有効	<p>コネクタが DNS にクエリを実行して、MongoDB クラスタで使用可能なすべての MongoDB サーバーを検出できるようにします。このプロパティは、ホスト名が DNS SRV レコードに関連付けられている場合に有効にすることができます。</p> <p>このプロパティを有効にした場合、DNS レコードによって必要なすべての詳細が提供されるため、ポートを指定する必要はありません。</p> <p>このプロパティを有効にしない場合は、接続プロパティで MongoDB サーバーのホスト名とポートを手動で指定してください。</p>
ポート	<p>MongoDB サーバーのポート番号。</p> <p>デフォルトは 27017 です。</p>
¹ 詳細モードのマッピングにのみ適用されます。	

認証タイプ

MongoDB にアクセスするために、ユーザー名とパスワード、X.509 標準認証、および LDAP 認証タイプを設定できます。

必要な認証タイプを選択し、認証固有のパラメータを設定します。

ユーザー名とパスワード認証

ユーザー名とパスワード認証はデフォルトのタイプで、MongoDB に接続するには少なくとも MongoDB アカウントのユーザー名、パスワード、およびデータベース名が必要です。

次の表に、ユーザー名とパスワード認証の基本接続プロパティとその説明を示します。

財産	説明
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のパスワード。
データベース名	接続する MongoDB データベースの名前。

X.509 標準認証

X.509 標準認証では、X.509 証明書を使用して MongoDB サーバーに接続するために、SSL キーストアファイルのパスと SSL キーストアファイルのパスワードが必要です。

次の表に、X.509 標準認証の基本的な接続プロパティとその説明を示します。

財産	説明
SSL キーストアファイルパス	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。 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。 <code>/home/cldagnt/SystemAgent/serverless/configurations/ssl_store/<keystore_filename></code> 詳細については、「 「サーバーレスランタイム環境の SSL の設定」 (ページ 517) 」を参照してください。
SSL キーストアパスワード	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。
データベース名	接続する MongoDB データベースの名前。

LDAP 認証

LDAP 認証の最小要件は、MongoDB に接続するための MongoDB ユーザー名、パスワード、およびデータベース名です。

次の表に、LDAP 認証の基本接続プロパティを示します。

財産	説明
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のパスワード。
データベース名	接続する MongoDB データベースの名前。

詳細設定

次の表に、詳細接続のプロパティを示します。

プロパティ	説明
追加プロパティ	MongoDB に対してデータの読み取りまたは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。 設定できる追加のプロパティについては、「 「追加接続プロパティ」 (ページ 516) 」を参照してください。 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。 <code>propertyName1=<value1>&propertyName2=<value2></code>

追加接続プロパティ

MongoDB V2 接続の【追加プロパティ】フィールドで、マッピングまたは詳細モードのマッピングに適用される特定の追加オプションを設定できます。

サンプリングのプロパティ

次のサンプリングプロパティは、マッピングまたは詳細モードのマッピングで設定できます。

samplesize

MongoDB ソースからスキーマを推測するためにスキャンするドキュメントの数。

例: samplesize=100。

デフォルトは 100 です。

samplemethod

MongoDB ソースからスキーマを推測するためにドキュメントをサンプリングする方式。

以下のいずれかの方式を指定できます。

- firstpage。MongoDB から最初の n 個のドキュメントをスキャンします。n はサンプルサイズを示します。スキャンする行の順序は MongoDB が決定します。
- random。MongoDB から n 個のランダムなドキュメントをスキャンします。
- all。コレクション全体をスキャンしてスキーマを推測します。
- none。コレクション全体をスキャンして、マッピング内のマルチレベルの階層データを MongoDB ソースから MongoDB ターゲットにフラット化せずに書き込みます。この機能は、詳細モードのマッピングには適用されません。
[samplemethod] として [none] を指定した場合にのみ、空の MongoDB コレクションに書き込むことができます。

非 SSL MongoDB デプロイメント

次の追加プロパティを設定して、マッピングまたは詳細モードのマッピングで非 SSL MongoDB デプロイメントに接続することができます。

ssl

接続で SSL と非 SSL のどちらを使用するかを決定します。

SSL を使用しない MongoDB デプロイメントに接続するには、接続プロパティでこのパラメータを false に設定します。

デフォルトは true です。

authsource

ユーザー資格証明を認証できるデータベース名を指定できます。

例: authsource=testadmin。

デフォルトは admin です。

Amazon DocumentDB

次の追加プロパティを設定して、詳細モードのマッピングで Amazon DocumentDB に接続することができます。

ssltruststorefilepath

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 マシンにあるトラストストアファイルの絶対パス。

例: ssltruststorefilepath= <path_of_truststore_file>

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への次の証明書パスを指定します。

/home/cldagnt/SystemAgent/serverless/configurations/ssl_store/<truststore_filename>

詳細については、「[「サーバーレスランタイム環境の SSL の設定」 \(ページ 517\)](#)」を参照してください。

ssltruststorepassword

通信を安全に行うために必要なトラストストアファイルのパスワードです。

例: ssltruststorepassword=<password>。

スキーマ検証のバイパス

次の追加プロパティを設定して、マッピング内の MongoDB コレクションに設定された検証ルールをバイパスすることができます。

bypassdocumentvalidation

MongoDB にデータを挿入、更新、または更新/挿入するときに、MongoDB コレクションに設定された検証ルールを接続でバイパスするかどうかを指定します。

例えば、検証ルールをバイパスするには、bypassdocumentvalidation=true と入力します。

このパラメータが設定されていない場合、MongoDB へのデータの書き込み時に、MongoDB V2 接続は MongoDB コレクションに定義された検証ルールを使用します。

MongoDB コレクションに設定された検証ルールをバイパスする前に、MongoDB に対する dbAdmin 特権または restore 特権があることを確認してください。

詳細については、MongoDB のマニュアルの「[Bypass schema validation](#)」を参照してください。

Azure CosmosDB

マッピングで MongoDB API が有効になっている Azure CosmosDB に書き込むために、次の追加プロパティを設定できます。

retryWrites

Azure CosmosDB への書き込み試行をマッピングが自動的に再試行できるかどうかを指定します。

例えば、Azure CosmosDB に書き込むには、retryWrites=false と入力します。

このパラメータを設定すると、ターゲット接続では、Azure CosmosDB への書き込み時に自動再試行メカニズムが無効になり、Azure CosmosDB コレクションの検証ルールを設定できなくなります。

このパラメータを設定しない場合、ターゲット接続ではデフォルトで自動再試行メカニズムが有効になります。

デフォルトは true です。

Azure CosmosDB から読み取りを行う場合、このプロパティを false に設定する必要はありません。

詳細については、MongoDB のマニュアルの「[Retryable Writes](#)」を参照してください。

サーバーレスランタイム環境の SSL の設定

詳細モードのマッピングで SSL 対応の MongoDB データベースに接続する場合は、MongoDB V2 コネクタでサーバーレスランタイム環境を使用することができます。

サーバーレスランタイム環境を使用するセキュアな MongoDB V2 接続を設定する前に、特定の前提条件を実行する必要があります。

1. トラストストアとキースタアの証明書ファイルが JKS 形式であることを確認します。
2. AWS アカウントまたは Azure アカウントの次の場所にある Amazon S3 バケットあるいは Azure コンテナにトラストストアとキースタアの証明書を追加します: <補足ファイルの場所>/serverless_agent_config/SSL
3. 次のコードスニペットをテキストエディタにコピーします。

```
version: 1
agent:
  agentAutoApply:
    general:
      sslStore:
        - fileCopy:
            sourcePath: SSL/<cert_filename>
        - fileCopy:
            sourcePath: SSL/<cert_filename>
```

ここで、ソースパスは AWS または Azure の証明書ファイルのディレクトリパスです。

注: 複数の *fileCopy* タグを追加することで、証明書ファイルの複数のソースパスを追加できます。

4. 構文とインデントが有効であることを確認してから、ファイルを `serverlessUserAgentConfig.yml` として次の AWS または Azure の場所に保存します: <補足ファイルの場所>/serverless_agent_config.yml ファイルの実行時に、SSL 証明書が AWS または Azure の場所からサーバーレスエージェントディレクトリにコピーされます。
5. サーバーレスエージェントをデプロイします。
6. [トラストストアファイルパス] および [キースタアファイルパス] フィールドの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/<cert_filename>`

プロキシサーバーの設定

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

Windows および Linux でプロキシサーバーを使用するように Secure Agent を設定できます。認証されていないプロキシサーバーまたは認証されたプロキシサーバーを使用できます。プロキシ設定は、詳細モードのマッピングで使用される接続に適用されます。

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

手順については、データ統合のヘルプの『または「Windows でのプロキシ設定」または「Linux でのプロキシ設定」を参照してください。

サーバーレスランタイム環境のプロキシの設定を行う方法については、Administrator ヘルプの「「プロキシサーバーの使用」を参照してください。

第 150 章

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。
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とレプリケーションタスクで 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。

プロパティ	説明
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	<p>使用するキーストアのタイプ。</p> <p>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。</p> <p>次のいずれかのタイプを使用してください:</p> <ul style="list-style-type: none"> - JKS。プライベートキーと証明書を格納します。 - PKCS12。プライベートキー、秘密鍵、証明書を格納します。
トラストストアのファイル名	トラストストアファイルのファイル名。
トラストストアのパスワード	トラストストアファイルのパスワード <code>name</code> 。
トラストストアのタイプ	<p>使用するトラストストアのタイプ。</p> <p>次のいずれかのタイプを使用してください:</p> <ul style="list-style-type: none"> - JKS - PKCS12
TLS プロトコル	<p>使用するトランスポートプロトコル。</p> <p>次のいずれかのタイプを使用してください:</p> <ul style="list-style-type: none"> - SSL - SSLv3 - TLS - TLSv1 - TLSv1.1 - TLSv1.2

第 151 章

MRI Software 接続のプロパティ

重要: 2024 年 11 月リリースから、MRI Software コネクタは非推奨となり、メンテナンスモードに移行されました。Informatica は将来のリリースでサポートを廃止する予定です。

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。
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。 <ul style="list-style-type: none">- [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。

第 152 章

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。
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gger（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。 <i>host_name</i> は、ホスト名または IP アドレスにできます。 <i>host_name:port_number</i> 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	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 CAPI_CONNECTION 文の名前。この文には、PWX CDC リーダーが PowerExchange ロgger（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	<p>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。</p> <ul style="list-style-type: none"> - 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。 <p>デフォルトは【なし】です。</p>
ページングサイズ	<p>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。</p> <p>デフォルトである最小値は 0 です。</p>
ページング単位	<p>【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。</p> <p>【行】 または 【キロバイト】 のいずれかを選択します。</p>
マップの場所	<p>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。</p> <p>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。</p> <p>次の形式で値を入力します。<i>host_name</i> は、ホスト名または IP アドレスにできます。</p> <p><i>host_name:port_number</i></p> <p>以下に例を示します。</p> <p>MYSCDC2B:25100</p> <p>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。</p>
マップの場所のユーザー	<p>【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。</p>
マップの場所のパスワード	<p>【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。</p>
イベントテーブル	<p>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。</p>

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	<p>カスタムプロパティまたは接続プロパティのオーバーライド。カスタムプロパティとは、PowerExchange のデフォルトの設定よりも優先するために指定できるプロパティです。セミコロン (;) を区切り文字として使用して複数のプロパティを入力するか、パラメータファイルを使用して接続プロパティの上書きを指定するパラメータを指定することができます。</p> <p>例:</p> <pre><property>=<value>;<property>=<value></pre> <p>多くの場合、Informatica グローバルカスタマサポートからの指示を受けたいので、カスタムプロパティの設定を行います。</p> <p>注: これらのプロパティは、PowerCenter の PowerExchange Client for PowerCenter (PWXPC) CDC 接続の 【PWX オーバーライド】 オプションと同じです。</p> <p>パラメータファイルを使用して接続プロパティのオーバーライドを指定するには、\$<ParameterName>の形式でパラメータを設定し、ユーザー定義パラメータ名の前にドル記号 (\$) を付けます。次に、【ランタイムオプション】 タブの 【パラメータファイル名】 フィールドにパラメータファイル名を指定することで、ユーザー定義パラメータ定義を含むパラメータファイルを使用するようにマッピングのマッピングタスクを設定します。</p> <p>注:</p> <ul style="list-style-type: none"> - マッピングおよび接続に同じパラメータを入力した場合は、接続カスタムプロパティが優先されます。 - パラメータファイルがある場合、このフィールドで指定するパラメータ名は、パラメータファイルで定義されたエントリと一致する必要があります。 <p>詳細については、「接続オーバーライドのリファレンス」の章を参照してください。</p>

第 153 章

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。
シークレットコンテナの使用	組織に対して設定されている Secrets Manager にこの接続の機密資格情報を保存します。 このプロパティは、組織に Secrets Manager が設定されている場合にのみ表示されます。 このプロパティは、データ取り込みおよびレプリケーションとデータアクセス管理サービスではサポートされていません。 接続でシークレットコンテナを有効にすると、Secure Agent が Secrets Manager からどの資格情報を取得するかを選択できます。このオプションを無効にした場合、資格情報は組織の設定方法に応じてリポジトリまたはローカル Secure Agent に保存されます。 注: この接続を使用してプッシュダウンまたはプロキシサービスを介してデータアクセスポリシーを適用する場合、シークレットコンテナ設定オプションを使用することはできません。 Secrets Manager を設定および使用する方法については、Administrator のヘルプにある「Secrets Manager の設定」を参照してください。
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。 Secure Agent、ホステッドエージェント、サーバーレスランタイム環境、またはエラスティックランタイム環境を指定します。 データ取り込みおよびレプリケーションの場合、ローカルのセキュアエージェントインストール環境またはサーバーレスランタイム環境を使用できます。サーバーレスランタイム環境は、クラウドソースタイプに使用できます。ホステッドエージェントでデータベース取り込みとレプリケーションタスクを実行することはできません。 エラスティックランタイム環境の設定方法の詳細については、「 「エラスティックランタイム環境の設定」 (ページ 528) 」を参照してください。
ユーザー名	データベースログインに使用するユーザー名。ユーザー名にセミコロンを含めることはできません。
パスワード	データベースログインに使用するパスワード。パスワードにセミコロンを含めることはできません。
ホスト	データベースサーバーをホストするマシンの名前。

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 3306 です。
データベース名	接続する MySQL データベースの名前。 注: データベース名は大文字と小文字が区別されます。 最大長は 64 文字です。データベース名には英数字とアンダースコアのみを使用してください。
コードページ	データベースサーバーのコードページ。
メタデータの詳細 接続プロパティ	JDBC ドライバがメタデータを取得するための追加プロパティ。プロパティを次の形式で入力します。 <parameter name>=<parameter value> 複数のプロパティを入力する場合は、キーと値のそれぞれのペアをアンパサンド (&) で区切ります。 例えば、次のプロパティを入力して、接続をテストする際の接続タイムアウトを設定します。 connectTimeout=<milliseconds> 注: デフォルトの接続タイムアウトは 270000 ミリ秒です。
ランタイムの詳細 接続プロパティ	ODBC ドライバがマッピング取り込みとレプリケーション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 とコロンの (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 とコロンの (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。

エラスティックランタイム環境の設定

エラスティックランタイム環境でカスタムバイナリファイルを設定し、マッピング実行中にランタイム環境でこれらのファイルにアクセスして実行できるようにします。

カスタムバイナリファイルを設定する前に、必ず AWS にエラスティックランタイム環境をデプロイして、Informatica Intelligent Cloud Services 内でデータを処理できる Kubernetes クラスタを作成してください。

エラスティックランタイム環境のデプロイの詳細については、「[Deploy an elastic runtime environment](#)」を参照してください。

エラスティックランタイム環境をデプロイした後、マウントされたディスクにカスタムバイナリファイルを配置し、POST 要求で使用するバイナリファイルの正確なパスをコピーします。

Informatica Intelligent Cloud Services 内でエラスティックランタイム環境に対する次の手順を実行して、カスタムバイナリファイルを管理します。

1. 組織にログインして、セッション ID とランタイム環境 ID を取得します。
2. REST API への POST 呼び出しを行い、セッション ID、ランタイム環境 ID、およびマウントされたディスクから先ほどコピーしたバイナリファイルパスを渡します。
POST 呼び出しの詳細については、『REST API リファレンス』ガイドの「[Supplementary files](#)」を参照してください。

POST 要求の例を次に示します。

```
POST <base URL>/api/v3/RuntimeEnvironment/<runtime environment ID>/ElasticConfig
Content-Type: application/json
Accept: application/json
INFA-SESSION-ID: <SessionId>
{
  "rteId": "rte-12345",
  "specification": {
    "agent": {
      "dataIntegrationServer": },
      "mysql": {
        "jdbcDrivers": [{"sourcePath": "/<path to binaries>/jdbc1.jar"}],
        "odbcDrivers": [{"sourcePath": "/<path to binaries>/odbc1.so"}],
        "version": "8.0"
      }
    }
  }
```

POST 呼び出しによって、データ統合サーバーの再起動がトリガされます。

3. Administrator でデータ統合サーバーのステータスを確認して、エラスティックランタイム環境が実行されていることを確認します。
4. 接続をテストするか、マッピングを実行して、エラスティックランタイム環境でカスタムバイナリファイルにアクセスして使用できることを確認します。

第 154 章

Netezza 接続のプロパティ

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

前提条件

Netezza コネクタを使用する前に、Windows または Linux に Netezza クライアントをインストールしてください。

成功ファイルおよびエラーファイルが含まれている Secure Agent ディレクトリにアクセスできることを確認します。このディレクトリパスは、接続用に選択したランタイム環境の各 Secure Agent マシンで同じである必要があります。

Netezza 接続を作成する前に、必ず Netezza ODBC ドライバと JDBC ドライバを設定してください。

Netezza JDBC ドライバのダウンロード

1. Netezza JDBC ドライババージョンを IBM Web サイトからダウンロードします。
Windows で Netezza JDBC ドライバをダウンロードするには、
[How to download the Netezza JDBC driver](#) のナレッジベースの記事の手順に従ってください。
Linux で Netezza JDBC ドライバを使用する場合、Linux マシンで Windows 用にダウンロードされた Netezza JDBC ドライバを使用できます。
2. Netezza JDBC ドライバをダウンロードしたら、次の場所に移動します。
<Secure Agent のインストールディレクトリ>/apps/Data_Integration_Server/ext/
3. 次のディレクトリ構造を手動で作成します。
deploy_to_main/bin/rdtm-extra/Netezza
4. Netezza JDBC ドライバの jar ファイル nzjdbc.jar を Secure Agent マシンに作成した次のディレクトリにコピーします。
<Secure Agent installation directory>/apps/Data_Integration_Server/ext/deploy_to_main/bin/rdtm-extra/Netezza
5. Secure Agent を再起動します。

Netezza ODBC ドライバのダウンロード

1. Netezza ODBC ドライババージョンを IBM Web サイトからダウンロードします。
Netezza ODBC ドライバをダウンロードするには、[How to download the Netezza ODBC driver](#) のナレッジベースの記事の手順に従ってください。

2. オペレーティングシステムに基づいて Netezza ODBC ドライバを使用するには、次のタスクを実行します。
- Windows では、NetezzaSQL ドライバが ODBC Data Source Administrator ドライバリストに表示されているかどうかを確認します。
 - Linux では、Secure Agent のインストールディレクトリにある `odbcinst.ini` ファイルにドライバーエントリを追加します。
- 次のコードはサンプルエントリを示しています。

```
[NetezzaSQL]
Driver          = /data/home/adputf_9/cloud_td/Netezza/installer/linux64/lib64/libnzodbc.so
Setup           = /data/home/adputf_9/cloud_td/Netezza/installer/linux64/lib64/libnzodbc.so
APILevel        = 1
ConnectFunctions = YYN
Description      = Netezza ODBC driver
DriverODBCVer   = 03.51
DebugLogging     = true
LogPath          = /tmp
UnicodeTranslationOption = utf8
CharacterTranslationOption = all
PreFetch        = 256
Socket          = 16384
```

Netezza への接続

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

始める前に

開始する前に、Netezza アカウントから Netezza データベースと認証の詳細を取得する必要があります。また、Netezza クライアントとドライバもインストールする必要があります。

実行する必要があるタスクの詳細については、「[「前提条件」 \(ページ 530\)](#)」を参照してください。

接続の詳細

次の表に、基本接続プロパティを示します。

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

プロパティ	説明
シークレットコンテナの使用	<p>組織に対して設定されている Secrets Manager にこの接続の機密資格情報を保存します。</p> <p>このプロパティは、組織に Secrets Manager が設定されている場合にのみ表示されます。</p> <p>このプロパティは、データ取り込みおよびレプリケーションとデータアクセス管理サービスではサポートされていません。</p> <p>接続でシークレットコンテナを有効にすると、Secure Agent が Secrets Manager からどの資格情報を取得するかを選択できます。このオプションを無効にした場合、資格情報は組織の設定方法に応じてリポジトリまたはローカル Secure Agent に保存されます。</p> <p>注: この接続を使用してプッシュダウンまたはプロキシサービスを介してデータアクセスポリシーを適用する場合、シークレットコンテナ設定オプションを使用することはできません。</p> <p>Secrets Manager を設定および使用する方法については、Administrator のヘルプにある「Secrets Manager の設定」を参照してください。</p>
ランタイム環境	<p>タスクを実行するランタイム環境の名前。</p> <p>Secure Agent、ホステッドエージェント、またはサーバーレスランタイム環境を指定します。</p> <p>Secure Agent を指定します。</p>
データベース	Netezza データベースの名前。
スキーマ名	<p>Netezza ソースまたはターゲットに使用されるスキーマ。</p> <p>スキーマ名は大文字と小文字が区別されます。</p>
サーバ名	Netezza データベースホスト名。
ポート	<p>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。</p> <p>デフォルトは 1521 です。</p>
ユーザー名	データベースへのアクセスに必要な読み取りおよび書き込みデータベース権限を持つデータベースユーザー名。
パスワード	上記データベースユーザー名のパスワード。

詳細設定

次の表に、詳細接続のプロパティを示します。

プロパティ	説明
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。 Netezza ODBC ドライバ名は NetezzaSQL です。
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。

データベース特権

データベース特権により、Netezza データベースで実行できる操作のアクセスレベルが定義されます。

Netezza データベースに対する次の特権があることを確認します。

- CREATE TABLE
- CREATE EXTERNAL TABLE
- DELETE
- DROP
- INSERT
- LIST
- SELECT
- TRUNCATE
- UPDATE

第 155 章

NetSuite 接続のプロパティ

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

NetSuite への接続

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

始める前に

接続プロパティを設定する前に、NetSuite アカウントからサービス URL、アカウント、トークン ID、およびトークンシークレットを取得する必要があります。
次のビデオは、必要な情報を取得する方法を示しています。



接続の詳細

次の表に、基本接続プロパティを示します。

財産	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。

財産	説明
シークレットコンテナの使用	<p>組織に対して設定されている Secrets Manager にこの接続の機密資格情報を保存します。このプロパティは、組織に Secrets Manager が設定されている場合にのみ表示されます。このプロパティは、データ取り込みおよびレプリケーションとデータアクセス管理サービスではサポートされていません。</p> <p>接続でシークレットコンテナを有効にすると、Secure Agent が Secrets Manager からどの資格情報を取得するかを選択できます。このオプションを無効にした場合、資格情報は組織の設定方法に応じてリポジトリまたはローカル Secure Agent に保存されます。</p> <p>注: この接続を使用してプッシュダウンまたはプロキシサービスを介してデータアクセスポリシーを適用する場合、シークレットコンテナ設定オプションを使用することはできません。</p> <p>Secrets Manager を設定および使用方法については、Administrator のヘルプにある「Secrets Manager の設定」を参照してください。</p>
ランタイム環境	<p>タスクを実行するランタイム環境の名前。</p> <p>Secure Agent、ホステッドエージェント、サーバーレスランタイム環境、またはエラスティックランタイム環境を選択します。</p> <p>詳細モードのマッピングで接続を使用する場合は、ホステッドエージェントを使用しないでください。</p> <p>ランタイム環境の設定および使用方法の詳細については、Administrator のヘルプにある「ランタイム環境」を参照してください。</p>
サービス URL	<p>NetSuite データにアクセスするための NetSuite Web Service Description Language (WSDL) の URL。</p> <p>WSDL バージョンに使用できる認証タイプについては、次のルールを考慮してください。</p> <ul style="list-style-type: none"> - WSDL バージョン 2018_1-2019_2。ユーザー名とパスワード、またはトークンベースの認証を使用できます。両方を使用した場合、エージェントは、NetSuite にアクセスする場合にトークンベースの認証を考慮します。 <p>注: NetSuite へのより安全なアクセスのためにトークンベースの認証を使用することをお勧めします。</p> <ul style="list-style-type: none"> - WSDL バージョン 2020_1 以降 - トークンベースの認証のみ使用できます。 <p>NetSuite WSDL URL のバージョン 2019_2 以降では、デフォルトサービス URL ではなく、NetSuite アカウントが使用する WSDL URL を入力できます。</p> <p>NetSuite アカウントが使用するサービス URL は、次の形式です。</p> <p><NetSuite account URL>/wsdl/v2019_2_0/netsuite.wsdl</p> <p>Informatica では、NetSuite アカウント固有の WSDL URL を使用することをお勧めしています。詳細については、「<i>NetSuite アカウント固有のサービス URL の設定</i>」を参照してください。</p> <p>デフォルトでは、NetSuite 接続は、次の URL に示すとおり、NetSuite WSDL URL バージョン 2024_2_0 を使用します。</p> <p>https://webservices.netsuite.com/wsdl/v2024_2_0/netsuite.wsdl</p> <p>Informatica は、2024_2、2024_1、2023_2、2023_1、2022_2、および 2022_1 WSDL のサポートを表明しています。2021_2 よりも古い WSDL バージョンは引き続き使用できます。ただし、これらのバージョンでバグ修正やサポートを受けることはできません。</p>
アカウント	<p>NetSuite アカウント ID。</p> <p>アカウント ID を取得するには、NetSuite にログインしてから、[Setup] > [Integration] > [SOAP Web Services Preferences] に移動します。</p>

財産	説明
トークン ID	NetSuite で生成されたトークン ID。 トークンベースの認証に適用されます。
トークン シークレット	NetSuite で生成されたトークンシークレット。 トークンベースの認証に適用されます。

詳細設定

次の表に、高度な接続のプロパティを示します。

プロパティ	説明
ユーザー名	認証にユーザー名とパスワードを使用する場合にのみ適用されます。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	認証にユーザー名とパスワードを使用する場合にのみ適用されます。NetSuite アカウントのパスワード。
アプリケーション ID	オプション。NetSuite のアプリケーション ID。 アプリケーション ID プロパティが空白の場合、エージェントは Informatica アプリケーション ID を使用します。 アプリケーション ID を検索するには、NetSuite にログインして、 [Setup] > [Integration] > [Manage Integrations] をクリックします。 アプリケーション ID がない場合は作成します。 [Manage Integrations] ページで [New] をクリックします。アプリケーション ID の保存後、 [Manage Integrations] ページでアプリケーション ID 番号を表示できます。

プロパティ	説明
レコードカスタムフィールド	<p>カスタムの NetSuite フィールドを指定します。</p> <ul style="list-style-type: none"> - 次のフォーマットを使用してカスタムフィールドを追加します。scriptId の値は、各カスタムフィールドの NetSuite ユーザーインターフェース内の ID フィールドです。 [<オブジェクト名>] scriptIds = <カスタムフィールド名 1>, <カスタムフィールド名 2>, <カスタムフィールド名 3> 例: [Sales] scriptIds = discountPrice, salesDescription, salesEvent3 - 次のフォーマットを使用して、NetSuite 詳細検索のカスタムフィールドを追加します。scriptId の値は、各カスタムフィールドの NetSuite ユーザーインターフェース内の ID フィールドです。 [<オブジェクト名>] scriptIds = <カスタムフィールド名 1>, <カスタムフィールド名 2>, <カスタムフィールド名 3> 例: [EmployeeSearchAdvanced] scriptIds = custentity74, custentity66 - カスタムセグメントデータを読み取るには、次の形式を使用して、カスタムセグメントフィールドを追加します。 [<オブジェクト名>] custSegScriptIds=custseg1: select, custseg2: multiselect, custseg3: select.... ここで scriptId の値は、各カスタムセグメントフィールドの NetSuite ユーザーインターフェース内の ID フィールドです。 例: [Employee] custSegScriptIds=custentity_cseg1: select, custentity_csegcs_multisel: multiselect - 子レコードカスタムセグメントからデータを読み取るには、次の形式を使用して、子カスタムセグメントフィールドを追加します。 [<オブジェクト名>] custSegScriptIds =custseg1:select, custseg2: multiselect, custseg3:select.... 例: [JournalEntry] custSegScriptIds =custbody_cseg1:select, custbody_cseg2:select, custbody_cseg3:select [JournalEntryLineList] custSegScriptIds =custcol_cseg1:select, custcol_cseg2:select, custcol_cseg3:select

プロパティ	説明
レコードフィルタフィールド	<p>NetSuite レコードフィールドの名前を関連する NetSuite 検索レコードフィールドの名前にマップして、フィルタ内でフィールドを使用できるようにします。</p> <p>次のように、レコードフィールド名と関連する SearchBasic フィールド名のリストを記述します。</p> <p>[<レコード 1>] <レコードフィールド名> =<SearchBasic フィールド名><レコードフィールド名 2> =<SearchBasic フィールド名 2> [<レコード 2>] <レコードフィールド名> =<SearchBasic フィールド名><レコードフィールド名 2> =<SearchBasic フィールド名 2><レコードフィールド名 3> =<SearchBasic フィールド名 3></p> <p>例: [Account] acctName=nameaddr1=address1</p> <p>記憶されたトランザクションが NetSuite アカунト内で有効な場合、NetSuite からのトランザクションデータを読み取るには、次の形式でレコードフィールド名と関連 SearchBasic フィールド名を追加します。</p> <p>[<レコード 1>] <レコードフィールド名> =<SearchBasic フィールド名> 例: [JournalEntry] reversalEntry=memorized</p>
保存済みの検索レコードフィールド	<p>一意の scriptId で識別される保存済み検索フィールドを追加する NetSuite 保存済み検索レコードごとに、個別のセクションを作成します。</p> <ul style="list-style-type: none"> 次のフォーマットを使用して検索フィールドを追加します。 <p><savedSearchId1>=<savedSearchDeclaredField1Name>,<savedSearchDeclaredField2Name>,<savedSearchCustomFieldScriptId1>,<savedSearchCustomFieldScriptId2>,<StandardJoin> <FieldName1>,<customSearchJoin <scriptId1></p> <p>例: 1000=phone,email,custentity78,custentity65, userJoin email,customSearchJoin custrecord1424</p> <ul style="list-style-type: none"> カスタムセグメントデータを読み取るには、次の形式を使用して、検索カスタムセグメントフィールドを追加します。 <p>[savedSearchId1]=custseg1:select, custseg2:multiselect, custseg3:select...</p> <p>例: [741]=custseg1:select,custentity_cseg1:select, custentity_csegcs_multisel:multiselect</p> <ul style="list-style-type: none"> カスタム結合を使用してカスタムレコード標準フィールドを読み取るために作成される、タスクのメタデータをオーバーライドするには、次の形式を使用して、検索カスタムレコード標準フィールドを追加します。 <p><savedSearchId1>=CustomSearchJoin <scriptId of custom record>__<standard field name></p> <p>For example, 356=CustomSearchJoin uss_custom_code__internalId</p>

NetSuite アカунト固有のサービス URL

NetSuite アカунト固有のサービス URL を使用するには、次の手順を実行します。

1. NetSuite にログインし、[設定] > [会社] > [会社情報] をクリックします。
2. [会社情報] ページで、[会社 URL] をクリックします。
[SUITETALK (SOAP AND REST WEB SERVICES)] フィールドに、アカунト固有の URL が次の形式で表示されます。

https://<NetSuite_account_ID>.suitetalk.api.netsuite.com
3. 手順 2 のアカунト固有の URL をコピーし、次の形式でサービス URL に貼り付けます。
https://<Netsuite_account_ID>.suitetalk.api.netsuite.com/wsdl/v2019_2_0/netsuite.wsdl

トークンベースの認証

トークンベースの認証は、NetSuite にアクセスする場合に使用されることが多い認証方法です。接続でトークンベースの認証を使用した場合、エージェントは、ユーザー名とパスワードの代わりにトークン ID とトークンシークレットを使用して NetSuite にアクセスします。

トークンベースの認証を使用するには、Informatica トークンベースの認証バンドルをインストールし、NetSuite でトークン ID とトークンシークレットを生成します。NetSuite アカウントから削除しないかぎり、トークンが期限切れになることはありません。ただし、Informatica が将来バンドルバージョンを更新した場合は、バンドルを更新し、新しいトークンを生成する必要があります。

1. フルアクセスまたは管理者アカウントを使用して NetSuite にログインします。
2. **【カスタマイズ】 > 【SuiteBundler】 > 【バンドルの検索とインストール】** に移動します。
3. キーワード「InformaticaTBABundle」を検索します。
116143 というバンドル ID のバンドルが検索結果に表示されます。
4. [InformaticaTBABundle] を選択してインストールします。
5. **【セットアップ】 > 【ユーザー/ロール】 > 【アクセストークン】 > 【新規】** に移動します。
6. **【アプリケーション名】** に、InformaticaTBAIntegration を選択します。
7. ページに表示されたアクセストークンとトークンシークレットを書き留めます。
NetSuite 接続を設定するときに、データ統合でトークン ID とトークンシークレットを入力します。

注: トークン情報がわからない場合は、NetSuite で別のトークンを生成する必要があります。以前に生成したトークンのトークン情報を NetSuite から取得することはできません。

NetSuite 接続についてのルールおよびガイドライン

NetSuite 接続については、次のルールとガイドラインを考慮してください。

- マッピング、同期タスク、またはマッピングタスクウィザードで接続を選択するときに、使用するオブジェクトを検索できます。名前、ラベル、説明、またはタイプパラメータを使用してオブジェクトを検索できます。
- デフォルトでは、技術名ではなくビジネス名が接続のフィールド名に表示されます。**【ラベルの代わりに技術名を表示】** オプションを使用すると、ビジネス名の代わりに技術名を表示するようにタスクを設定できます。
- タスクが行う同じ NetSuite アカウントへの接続ごとに個別のライセンスが必要です。例えば、同じ NetSuite アカウントをタスクのソース、ターゲット、およびルックアップとして使用する場合は、3 つの NetSuite ライセンスが必要です。
- NetSuite を使用する場合、複数の同時実行スレッドを使用してタスクのパフォーマンスを向上させることができます。NetSuite の基本アカウントを持っている場合は、パフォーマンスを向上させるためにトークンベースの認証を使用することをお勧めします。

注: 認証に要求レベルの資格情報を使用する Web サービスの場合、NetSuite の基本アカウント（SuiteCloud Plus ライセンスなし）の同時要求のガバナンス制限は 1 に設定されます。トークンベースの認証を使用する Web サービスの場合、NetSuite の基本アカウント（SuiteCloud Plus ライセンスなし）の同時要求の制限は 5 に設定されます。

NetSuite 接続のトラブルシューティング

NetSuite 接続を作成すると、次のエラーが発生する場合があります。

Test Connection Failed for <connection name>. ConnectionFailedException: [Connection].

ExceededRequestLimitFault: Only one request may be made against a session at a time.

NetSuite 接続は一度に 1 つしか使用できないため、このメッセージが表示されることがあります。この問題を解決するには、NetSuite から Suite Cloud Plus アカウントを要求します。これにより、ユーザーごとに最大 10 個のマッピングが可能になります。

第 156 章

NetSuite Mass Ingestion 接続のプロパティ

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

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

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

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

接続プロパティ	説明
接続名	接続の名前。この名前は、組織内で一意にする必要があります。接続名には、英数字、スペース、および次のような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。
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。 アプリケーション取り込みとレプリケーションタスクでは、Secure Agent またはサーバーレスランタイム環境を選択できます。ホステッドエージェントは使用できません。
電子メール ID	NetSuite アカウントのユーザー名。ユーザー名は、電子メールアドレスです。
パスワード	NetSuite アカウントのパスワード。
サービスホスト	SuiteAnalytics Connect サービスホストの名前。 このフィールドの値は、NetSuite の 【SuiteAnalytics Connect ドライバのダウンロード】 ページの 【構成】 セクションにある 【サービスホスト】 フィールドで指定した値と一致している必要があります。 【SuiteAnalytics Connect ドライバのダウンロード】 ページにアクセスするには、NetSuite にログインし、 【設定】 ポートレットの 【SuiteAnalytics 接続のセットアップ】 リンクをクリックします。
サービスポート	SuiteAnalytics Connect サーバーがリッスンしている TCP/IP ポート。デフォルトは 1708 です。

接続プロパティ	説明
サービスデータソース	<p>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。</p> <ul style="list-style-type: none"> - NetSuite.com - NetSuite2.com <p>デフォルトは NetSuite2.com です。</p> <p>注:</p> <ul style="list-style-type: none"> - 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	<p>NetSuite アカウント ID。</p> <p>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。</p> <p>[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。</p>
ロール ID	<p>NetSuite アカウントに関連付けられているロール ID。</p>
追加接続プロパティ	<p>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。</p> <p>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。</p> <ul style="list-style-type: none"> - 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。 <p>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。</p>

第 157 章

NetSuite RESTlet V2 接続のプロパティ

NetSuite RESTlet 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、NetSuite RESTlet 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。
シークレットコンテナの使用	組織に対して設定されている Secrets Manager にこの接続の機密資格情報を保存します。 このプロパティは、組織に Secrets Manager が設定されている場合にのみ表示されます。 このプロパティは、データ取り込みおよびレプリケーションとデータアクセス管理サービスではサポートされていません。 接続でシークレットコンテナを有効にすると、Secure Agent が Secrets Manager からどの資格情報を取得するかを選択できます。このオプションを無効にした場合、資格情報は組織の設定方法に応じてリポジトリまたはローカル Secure Agent に保存されます。 注: この接続を使用してプッシュダウンまたはプロキシサービスを介してデータアクセスポリシーを適用する場合、シークレットコンテナ設定オプションを使用することはできません。 Secrets Manager を設定および使用方法については、Administrator のヘルプにある「Secrets Manager の設定」を参照してください。
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。 Secure Agent、ホステッドエージェント、サーバーレスランタイム環境、またはエラスティックランタイム環境を選択します。 ランタイム環境の設定および使用方法の詳細については、Administrator のヘルプにある「ランタイム環境」を参照してください。
ユーザー名	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。 トークンベースの認証を使用して NetSuite にアクセスする場合は省略可能です。
パスワード	NetSuite アカウントのパスワード。 トークンベースの認証を使用して NetSuite にアクセスする場合は省略可能です。

プロパティ	説明
REST ドメイン	<p>REST ドメイン名: https://rest.netsuite.com 例えば、次の値を入力できます。</p> <ul style="list-style-type: none"> - rest.na1.beta.netsuite.com (ベータ環境用) - rest.sandbox.netsuite.com (サンドボックスアカウント用) - rest.netsuite.com または rest.na1.netsuite.com (本番アカウント用) <p>デフォルトのドメイン名 URL の代わりに、NetSuite アカウントに固有のドメイン名 URL を入力することもできます。</p> <p>NetSuite アカウントが使用するドメイン名 URL は、次の形式です。 <a href="https://<NetSuite_account_ID>.restlets.api.netsuite.com">https://<NetSuite_account_ID>.restlets.api.netsuite.com.</p> <p>使用する NetSuite アカウントに固有のドメイン名 URL を使用することをお勧めします。 注: NetSuite コネクタは、NetSuite 2023_1 サンドボックスアカウントまたはリリースプレビューアカウントで使用できます。</p>
アカウント ID	<p>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。</p> <p>[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。</p>
コンシューマキー	<p>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。</p> <p>トークンベースの認証の場合のみ必要です。</p>
コンシューマシークレット	<p>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。</p> <p>トークンベースの認証の場合のみ必要です。</p>
トークン ID	<p>NetSuite で生成されたトークン ID。</p> <p>トークンベースの認証を使用して NetSuite にアクセスする場合は必須です。ユーザー名とパスワードを使用して NetSuite にアクセスする場合は省略可能です。</p>
トークンシークレット	<p>NetSuite で生成されたトークンシークレット。</p> <p>トークンベースの認証を使用して NetSuite にアクセスする場合は必須です。ユーザー名とパスワードを使用して NetSuite にアクセスする場合は省略可能です。</p>

第 158 章

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。
シークレットコンテナの使用	<p>組織に対して設定されている Secrets Manager にこの接続の機密資格情報を保存します。</p> <p>このプロパティは、組織に Secrets Manager が設定されている場合にのみ表示されます。</p> <p>このプロパティは、データ取り込みおよびレプリケーションとデータアクセス管理サービスではサポートされていません。</p> <p>接続でシークレットコンテナを有効にすると、Secure Agent が Secrets Manager からどの資格情報を取得するかを選択できます。このオプションを無効にした場合、資格情報は組織の設定方法に応じてリポジトリまたはローカル Secure Agent に保存されます。</p> <p>注: この接続を使用してプッシュダウンまたはプロキシサービスを介してデータアクセスポリシーを適用する場合、シークレットコンテナ設定オプションを使用することはできません。</p> <p>Secrets Manager を設定および使用する方法については、Administrator のヘルプにある「Secrets Manager の設定」を参照してください。</p>
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: <i>http://<会社名>.satmetrix.com</i>
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。

第 159 章

OData の接続プロパティ

OData サービスに対してデータの読み取りおよび書き込みを行うための OData 接続を作成します。
接続を使用して、マッピングおよびマッピングタスクで、ソースおよびターゲットを指定します。

OData への接続

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

始める前に

接続プロパティを設定する前に、OData サービスのユーザー名、パスワード、およびエンドポイント URI を手元に用意しておいてください。

接続の詳細

次の表に、基本接続プロパティを示します。

プロパティ	説明
接続名	接続の名前。 各接続名は組織内で一意である必要があります。接続名には、英数字、スペース、および次の特殊文字を含めることができます。_ . + - , 最大長は 255 文字です。
説明	接続の説明。最大長は 4000 文字です。
シークレットコンテナの使用	組織に対して設定されている Secrets Manager にこの接続の機密資格情報を保存します。 このプロパティは、組織に Secrets Manager が設定されている場合にのみ表示されます。 このプロパティは、データ取り込みおよびレプリケーションとデータアクセス管理サービスではサポートされていません。 接続でシークレットコンテナを有効にすると、Secure Agent が Secrets Manager からどの資格情報を取得するかを選択できます。このオプションを無効にした場合、資格情報は組織の設定方法に応じてリポジトリまたはローカル Secure Agent に保存されます。 注: この接続を使用してプッシュダウンまたはプロキシサービスを介してデータアクセスポリシーを適用する場合、シークレットコンテナ設定オプションを使用することはできません。 Secrets Manager を設定および使用方法については、Administrator のヘルプにある「Secrets Manager の設定」を参照してください。

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。 Secure Agent、ホステッドエージェント、またはサーバーレスランタイム環境を選択します。 ランタイム環境の設定および使用方法の詳細については、Administrator のヘルプにある「ランタイム環境」を参照してください。
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 サービスのルート URI。 サービスルート URI は、 OData URI conventions に準拠する必要があります。

詳細設定

次の表に、詳細接続のプロパティを示します。

プロパティ	説明
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。

プロキシサーバーの設定

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

Windows および Linux でプロキシサーバーを使用するように Secure Agent とサーバーレスランタイム環境を設定できます。認証されていないプロキシサーバーまたは認証されたプロキシサーバーを使用できます。プロキシ設定は、マッピングおよび詳細モードのマッピングで使用される接続に適用されます。

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

- Windows の場合は Secure Agent Manager を使用し、Linux の場合はシェルコマンドを使用して Secure Agent を設定します。
手順については、データ統合のヘルプの『または「Windows でのプロキシ設定」または「Linux でのプロキシ設定」を参照してください。
- Secure Agent のプロパティで、DTM の JVM オプションを設定します。手順については、ナレッジベースの記事「[Proxy server settings](#)」を参照してください。

サーバーレスランタイム環境のプロキシの設定を行う方法については、Administrator ヘルプの「「プロキシサーバーの使用」を参照してください。

第 160 章

OData Consumer の接続プロパティ

OData Consumer 接続を使用して、OData Consumer サービスに対してデータの読み取りおよび書き込みを行います。

接続を作成して、同期タスク、マッピング、またはマッピングタスクに関連付けます。ソースのプロパティを定義して、OData Consumer オブジェクトに対してデータの読み取りおよび書き込みを行います。また、要件に基づいてデータフィルタを設定することもできます。

マッピングを作成する場合は Mapping Designer でこの接続を使用し、タスクを作成する場合は同期タスクウィザードでこの接続を使用します。

OData Consumer への接続

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

始める前に

接続プロパティを設定する前に、OData Consumer サービスのユーザー名、パスワード、および URL を手元に用意しておいてください。

接続の詳細

次の表に、基本接続プロパティを示します。

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

プロパティ	説明
シークレットコンテナの使用	<p>組織に対して設定されている Secrets Manager にこの接続の機密資格情報を保存します。このプロパティは、組織に Secrets Manager が設定されている場合にのみ表示されます。このプロパティは、データ取り込みおよびレプリケーションとデータアクセス管理サービスではサポートされていません。</p> <p>接続でシークレットコンテナを有効にすると、Secure Agent が Secrets Manager からどの資格情報を取得するかを選択できます。このオプションを無効にした場合、資格情報は組織の設定方法に応じてリポジトリまたはローカル Secure Agent に保存されます。</p> <p>注: この接続を使用してプッシュダウンまたはプロキシサービスを介してデータアクセスポリシーを適用する場合、シークレットコンテナ設定オプションを使用することはできません。</p> <p>Secrets Manager を設定および使用方法については、Administrator のヘルプにある「Secrets Manager の設定」を参照してください。</p>
ランタイム環境	<p>タスクを実行するランタイム環境の名前。</p> <p>Secure Agent、ホステッドエージェント、サーバーレスランタイム環境、またはエラスティックランタイム環境を選択します。</p> <p>ランタイム環境の設定および使用方法の詳細については、Administrator のヘルプにある「ランタイム環境」を参照してください。</p>
ユーザー名	OData Consumer 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。
URL	<p>OData V4 プロトコルを介して提供される OData Consumer サービスデータソースの URL。URL には、\$metadata またはオブジェクト名を含めることはできません。</p> <p>例: http://services.odata.org/V4/Northwind/Northwind.svc/</p> <p>注: URL 規則の詳細については、http://docs.oasis-open.org/odata/odata/v4.0/odata-v4.0-part2-url-conventions.html を参照してください。</p>

詳細設定

次の表に、詳細接続のプロパティを示します。

プロパティ	説明
データ直列化フォーマット	<p>転送するデータの形式。[JSON] を選択します。</p> <p>[ATOM/XML] は適用されません。</p>
セキュリティタイプ	<p>OData Consumer サーバーとの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。</p> <p>次のオプションから選択できます。</p> <ul style="list-style-type: none"> - SSL。双方向 SSL は適用されません。 - なし <p>デフォルトは [なし] です。</p> <p>TLS は適用されません。</p> <p>一方向 SSL の使用方法の詳細については、「一方向 SSL のセットアップ」(ページ 550) を参照してください。</p>
トラストストアファイル名	<p>SSL セキュリティタイプを選択した場合は必須です。</p> <p>OData Consumer 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。</p> <p>トラストストアファイルは JKS 形式である必要があります。</p>

プロパティ	説明
トラストストアのパスワード	OData Consumer 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を選択する場合、必須です。 OData Consumer 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。 キーストアファイルは JKS 形式である必要があります。
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です。

プロキシサーバーの設定

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

Windows および Linux でプロキシサーバーを使用するように Secure Agent とサーバーレスランタイム環境を設定できます。認証されていないプロキシサーバーまたは認証されたプロキシサーバーを使用できます。プロキシ設定は、マッピングおよび詳細モードのマッピングで使用される接続に適用されます。

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

- Windows の場合は Secure Agent Manager を使用し、Linux の場合はシェルコマンドを使用して Secure Agent を設定します。
手順については、データ統合のヘルプの『または「Windows でのプロキシ設定」または「Linux でのプロキシ設定」を参照してください。
- Secure Agent のプロパティで、DTM の JVM オプションを設定します。手順については、ナレッジベースの記事「[Proxy server settings](#)」を参照してください。

サーバーレスランタイム環境のプロキシの設定を行う方法については、Administrator ヘルプの「「プロキシサーバーの使用」を参照してください。

一方向 SSL のセットアップ

トラストストア証明書とキーストア証明書を作成すると、OData Consumer コネクタを使用して、SSL 対応の OData Consumer サービスに接続できます。一方向 SSL を使用して、OData Consumer とのセキュリティで保護された接続を確立することができます。

一方向 SSL を使用するには、次の手順を実行します。

- Secure Agent インストール内の次の 1 つ以上の場所にある jdk ディレクトリにサーバー証明書をインポートします。
 - <Secure Agent インストールディレクトリ>/jdk/jre/lib/security
 - <Secure Agent インストールディレクトリ>/jdk/lib/security
 - <Secure Agent インストールディレクトリ>/jdk8/jre/lib/security

使用可能なすべてのディレクトリに証明書を追加してください。

- <Secure Agent インストールディレクトリ>\apps フォルダ内に jdk ディレクトリがある場合は、次のディレクトリに移動し、Secure Agent インストール内の次の 1 つ以上の場所にある jdk ディレクトリにサーバー証明書をインポートします。
 - <Secure Agent インストールディレクトリ>\apps\jdk\zulu8<latest_version>\jre\lib\security
 - <Secure Agent インストールディレクトリ>\apps\jdk\zulu17<latest_version>\lib\security
- 証明書を含むディレクトリパスに *INFA_TRUSTSTORE* 環境変数を設定するには、次の手順を実行します。
 - Secure Agent マシンのシステム変数に次の環境変数を追加します: *INFA_TRUSTSTORE*
 - *INFA_TRUSTSTORE* 変数の値を、トラストストア証明書とキーストア証明書を含むディレクトリに設定します。

これらの更新を行った後に、Secure Agent を再起動します。

第 161 章

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。
シークレットコンテナの使用	組織に対して設定されている Secrets Manager にこの接続の機密資格情報を保存します。 このプロパティは、組織に Secrets Manager が設定されている場合にのみ表示されます。 このプロパティは、データ取り込みおよびレプリケーションとデータアクセス管理サービスではサポートされていません。 接続でシークレットコンテナを有効にすると、Secure Agent が Secrets Manager からどの資格情報を取得するかを選択できます。このオプションを無効にした場合、資格情報は組織の設定方法に応じてリポジトリまたはローカル Secure Agent に保存されます。 注: この接続を使用してプッシュダウンまたはプロキシサービスを介してデータアクセスポリシーを適用する場合、シークレットコンテナ設定オプションを使用することはできません。 Secrets Manager を設定および使用方法については、Administrator のヘルプにある「Secrets Manager の設定」を参照してください。
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。 Secure Agent、ホステッドエージェント、サーバーレスランタイム環境、またはエラスティックランタイム環境を選択します。 ランタイム環境の設定および使用方法の詳細については、Administrator のヘルプにある「ランタイム環境」を参照してください。
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。

接続プロパティ	説明
サービス URL	<p>選択した OData V2 サービスタイプのサービス URL。</p> <p>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。</p> <p>例えば、次の形式でサービス URL を入力します。</p> <p><code>https://sandbox.api.sap.com/s4hanacCloud/sap/opu/odata/sap/API_CHARTOFACCOUNTS_SRV</code></p> <p>URL が有効かどうかは、URL に\$metadataを追加することで行えます。</p> <p>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。</p> <p>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。</p> <p><code>http://<OData サーバーのホスト名>:<ポート番号>/sap/opu/odata/iwfnd/CATALOGSERVICE;v=2/</code></p> <p>ホスト名とポート番号が <code>inpha1.informatica.com:8001</code> 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。</p> <p><code>https://inpha1.informatica.com:8001/sap/opu/odata/iwfnd/CATALOGSERVICE;v=2/</code></p>
認証タイプ	<p>OData サービスに接続するためのユーザー認証のタイプ。</p> <p>次の認証タイプから選択します。</p> <ul style="list-style-type: none"> - 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。 - OAuth 2.0 認証コード。OData V2 エンドポイントに接続するには、承認済みアクセスが必要です。 - OAuth 2.0 クライアント資格情報。OData V2 エンドポイントに接続するには、クライアント資格情報が必要です。
ユーザ名	<p>基本認証に適用されます。</p> <p>OData V2 アプリケーションに接続するためのユーザー名。</p>
パスワード	<p>基本認証に適用されます。</p> <p>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。</p>
API キー	<p>API キー認証に適用されます。</p> <p>OData V2 アプリケーションへの接続に必要な一意の API キー。</p>

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 401 エラーコードが返された場合に、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 OData V2 Protocol Reader 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。
認証タイプ	コネクタが OData V2 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 [基本] 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	OData V2 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。 ZGWSAMPLE_BASIC_0001 /IWFND/SG_MED_CATALOG_0002 ZAPI_CHARTOFACCOUNTS_SRV_0001
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>"}]
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。 認証のために要求本文または要求ヘッダーのいずれかでクライアント ID とクライアントシークレットを送信するオプションを選択します。 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更新トークンを生成します。

接続プロパティ	説明
アクセストークン	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。
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。

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 OData V2 Protocol Reader 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。
認証タイプ	コネクタが OData V2 エンドポイントに接続するために使用する必要がある認証方法。 【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 【基本】 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。 ZGWSAMPLE_BASIC_0001 /IWFND/SG_MED_CATALOG_0002 ZAPI_CHARTOFACCOUNTS_SRV_0001
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
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。 認証のために要求本文または要求ヘッダーのいずれかでクライアント ID とクライアントシークレットを送信するオプションを選択します。 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。

第 162 章

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。
シークレットコンテナの使用	組織に対して設定されている Secrets Manager にこの接続の機密資格情報を保存します。 このプロパティは、組織に Secrets Manager が設定されている場合にのみ表示されます。 このプロパティは、データ取り込みおよびレプリケーションとデータアクセス管理サービスではサポートされていません。 接続でシークレットコンテナを有効にすると、Secure Agent が Secrets Manager からどの資格情報を取得するかを選択できます。このオプションを無効にした場合、資格情報は組織の設定方法に応じてリポジトリまたはローカル Secure Agent に保存されます。 注: この接続を使用してプッシュダウンまたはプロキシサービスを介してデータアクセスポリシーを適用する場合、シークレットコンテナ設定オプションを使用することはできません。 Secrets Manager を設定および使用する方法については、Administrator のヘルプにある「Secrets Manager の設定」を参照してください。
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。 Secure Agent 環境またはエラスティックランタイム環境を選択します。 ランタイム環境の設定および使用方法の詳細については、Administrator のヘルプにある「ランタイム環境」を参照してください。
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。

接続プロパティ	説明
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。
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 <i>inpha1.informatica.com:8001</i> で、サービスエンドポイントが <i>CATALOGSERVICE</i> 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ル化フォーマット。 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。

第 163 章

ODBC 接続のプロパティ

ODBC 接続を作成して、ODBC 準拠のデータベースまたはデータウェアハウスに対してデータの安全な読み取りおよび書き込みを行います。

前提条件

特定の ODBC 準拠のエンドポイントに接続するには、データベースまたはデータウェアハウス固有の ODBC ドライバと ODBC クライアントを Secure Agent マシンにインストールして、データベースまたはデータウェアハウスに接続するための特定の前提条件タスクを実行する必要があります。

さらに、Kerberos 認証を使用して DB2 または SAP Sybase ASE に接続する場合は、Kerberos 認証の前提条件を完了する必要があります。

ODBC ドライバの設定

ODBC 接続を使用するには、データベースまたはデータウェアハウス固有の ODBC ドライバのシステムデータソース名 (DSN) を設定し、その ODBC ドライバと ODBC クライアントを Secure Agent マシンにインストールする必要があります。

ODBC クライアントは、ODBC ドライバをインストールした任意のデータベースとデータウェアハウスにアクセスすることができます。インストールした ODBC ドライバが、接続先の ODBC 準拠のエンドポイントに準拠していることを確認してください。

ODBC 接続では、システム DSN のみが使用されます。ODBC ドライバの設定時に、ユーザー DSN を使用することはできません。システム DSN の設定時に、データソース名と接続文字列を指定する必要があります。

このセクションでは、Secure Agent をホストする Windows および Linux マシンで ODBC ドライバを設定する手順について説明します。これらの手順を使用して、エンドポイント固有の ODBC ドライバを設定することができます。場合によっては、ドライバの設定後に環境変数を設定する必要があります。ドライバの設定を行う際は、例を参照することもできます。

Linux での ODBC ドライバの設定

ODBC 接続を確立して Linux 上の ODBC 準拠のデータベースまたはデータウェアハウスに接続する前に、ODBC ドライバを設定してください。

1. データベースまたはデータウェアハウス固有の Web サイトから ODBC ドライバをダウンロードします。
注: DB2 ODBC (64 ビット) ドライバおよび SAP IQ ODBC (64 ビット) ドライバを取得する方法については、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。
2. ODBC ドライバを Secure Agent マシンにインストールします。

- odbc.ini ファイルにデータソースのエントリを追加します。
さまざまな接続タイプに使用できる odbc.ini ファイルのサンプルの詳細については、「[「ODBC 接続タイプ のサンプル odbc.ini ファイル」 \(ページ 560\)](#)」を参照してください。
- コマンドラインから次のコマンドを実行して、odbc.ini ファイルをエクスポートします:
Export ODBCINI=/<odbc.ini file path>/odbc.ini
- また、Secure Agent マシン上の特定の ODBC ドライバの環境変数を設定します。
例えば、次の ODBC ドライバの環境変数を設定します。

ODBC ドライバ	環境変数
Microsoft Azure SQL Data Warehouse ODBC ドライバ	以下の環境変数を設定します。 - setenv ODBCINI "/data/home/adputf_9/cloud_td/ODBCINI/odbc.ini" - setenv LD_LIBRARY_PATH "/opt/microsoft/msodbcsql/lib64/libmsodbcsql-11.0.so.2270.0"
Netezza ODBC ドライバ	以下の環境変数を設定します。 - setenv ODBCINI "/data/home/qamercury/cloud_td/ODBCINI/odbc.ini" - setenv ODBCINST /data/home/qamercury/cloud_td/ODBCINI/odbcinst.ini - setenv LD_LIBRARY_PATH ".: /export/qa_adp/thirdparty/netezza/linux.64/lib64:\$LD_LIBRARY_PATH"
Teradata ODBC ドライバ	以下の環境変数を設定します。 - setenv ODBCINI "/data/home/adputf_9/cloud_td/ODBCINI/odbc.ini" - setenv LD_LIBRARY_PATH "/opt/teradata/client/<Version>/lib64"

- Secure Agent を再起動します。

ODBC 接続タイプのサンプル odbc.ini ファイル

ODBC 接続の作成時に、odbc.ini ファイルを使用してデータソースを設定できます。

このセクションでは、odbc.ini ファイル内の特定の ODBC 接続タイプのサンプルエントリを示します。これらのサンプルを参照して、特定のエンドポイントの接続エントリを指定することができます。

DB2 ODBC 接続

この接続を作成して、DB2 エンドポイントに接続します。

次のサンプルは、odbc.ini ファイル内の DB2 データソースの接続エントリを示しています。

```
[Sample DB2 ODBC DSN]
Driver=/<Path to the DB2 ODBC library>/DWdb228.so
Description=DataDirect <Version number> DB2 Wire Protocol
AccountingInfo=
AddStringToCreateTable=
AlternateID=
AlternateServers=
ApplicationName=
ApplicationUsingThreads=1
AuthenticationMethod=0
BulkBinaryThreshold=32
BulkCharacterThreshold=-1
BulkLoadBatchSize=1024
BulkLoadFieldDelimiter=
BulkLoadRecordDelimiter=
CatalogSchema=
CharsetFor65535=0
ClientHostName=
ClientUser=
#Collection applies to z/OS and iSeries only
Collection=
```

```

ConcurrentAccessResolution=0
ConnectionReset=0
ConnectionRetryCount=0
ConnectionRetryDelay=3
CurrentFuncPath=
#Database applies to DB2 UDB only
Database=<Database name>
DefaultIsolationLevel=1
DynamicSections=1000
EnableBulkLoad=0
EncryptionMethod=0
FailoverGranularity=0
FailoverMode=0
FailoverPreconnect=0
GrantAuthid=PUBLIC
GrantExecute=1
GSSClient=native
HostNameInCertificate=
IpAddress=<DB2 server host name>
KeyPassword=
KeyStore=
KeyStorePassword=
LoadBalanceTimeout=0
LoadBalancing=0
#Location applies to z/OS and iSeries only
Location=<Location name>
LogonID=
MaxPoolSize=100
MinPoolSize=0
Password=
PackageCollection=NULLID
PackageNamePrefix=DD
PackageOwner=
Pooling=0
ProgramID=
QueryTimeout=0
ReportCodePageConversionErrors=0
TcpPort=50000
TrustStore=
TrustStorePassword=
UseCurrentSchema=0
ValidateServerCertificate=1
WithHold=1
XMLDescribeType=-10

```

Microsoft Azure SQL Data Warehouse 接続

この接続を作成して、Microsoft Azure SQL Data Warehouse エンドポイントに接続します。

次のサンプルは、odbc.ini ファイル内の Microsoft Azure SQL Data Warehouse データソースの接続エントリを示しています。

```

[Sample Azure DW ODBC DSN]
[SD_Azure_DW]
Driver=/opt/microsoft/msodbcsql/lib64/libmsodbcsql-11.0.so.2270.0
Description=Microsoft ODBC Driver 11 for SQL Server
Server=<Server name>
Database=<Database name>
LogonID=<User name>
Password=<Password>
QuotedId=Yes
AnsiNPW=Yes
EncryptionMethod=1
SeedBeforeConnect=1
EnableQuotedIdentifiers=1
ValidateServerCertificate=0
DriverUnicodeType=1

```

Netezza ODBC 接続

この接続を作成して、Netezza エンドポイントに接続します。

次のサンプルは、odbc.ini ファイル内の Netezza データソースの接続エントリを示しています。

```
[Sample Netezza ODBC DSN]
Driver=/export/qa_adp/thirdparty/netezza/linux.64/lib64/libnzodbc.so
Description=NetezzaSQL ODBC
Servername=<Server name>
Port=5480
Database=<Database name>
Username=<User name>
Password=<Password>
StripCRLF=false
ReadOnly=false
ShowSystemTables=false
DateFormat=1
NumericAsChar=false
DebugLogging=true
```

SAP Sybase ASE ODBC 接続

この接続を作成して、SAP Sybase ASE エンドポイントに接続します。

次のサンプルは、odbc.ini ファイル内の SAP Sybase ASE データソースの接続エントリを示しています。

```
[Sample SAP Sybase ASE ODBC DSN]
Driver=/<Path to the SAP Sybase ASE library>/DWase27.so
Description=DataDirect <Version number> Sybase Wire protocol
AlternateServers=
ApplicationName=
ApplicationUsingThreads=1
ArraySize=50
AuthenticationMethod=0
BulkBinaryThreshold=32
BulkCharacterThreshold=-1
BulkLoadBatchSize=1024
BulkLoadFieldDelimiter=
BulkLoadRecordDelimiter=
Charset=
ConnectionReset=0
ConnectionRetryCount=0
ConnectionRetryDelay=3
CursorCacheSize=1
Database=<database_name>
DefaultLongDataBuffLen=1024
EnableBulkLoad=0
EnableDescribeParam=0
EnableQuotedIdentifiers=0
EncryptionMethod=0
FailoverGranularity=0
FailoverMode=0
FailoverPreconnect=0
GSSClient=native
HostNameInCertificate=
InitializationString=
Language=
LoadBalancing=0
LoadBalanceTimeout=0
LoginTimeout=15
LogonID=
MaxPoolSize=100
MinPoolSize=0
NetworkAddress=<SAP Sybase host name,SAP Sybase server port number>
OptimizePrepare=1
PacketSize=0
Password=
Pooling=0
```

```
QueryTimeout=0
RaiseErrorPositionBehavior=0
ReportCodePageConversionErrors=0
SelectMethod=0
ServicePrincipalName=
TruncateTimeTypeFractions=0
TrustStore=
TrustStorePassword=
ValidateServerCertificate=1
WorkStationID=
```

Teradata ODBC 接続

この接続を作成して、Teradata エンドポイントに接続します。

次のサンプルは、odbc.ini ファイル内の Teradata データソースの接続エントリを示しています。

```
[Sample Teradata ODBC DSN]
[ODBC Data Sources]
<DSN_NAME>=tdata.so

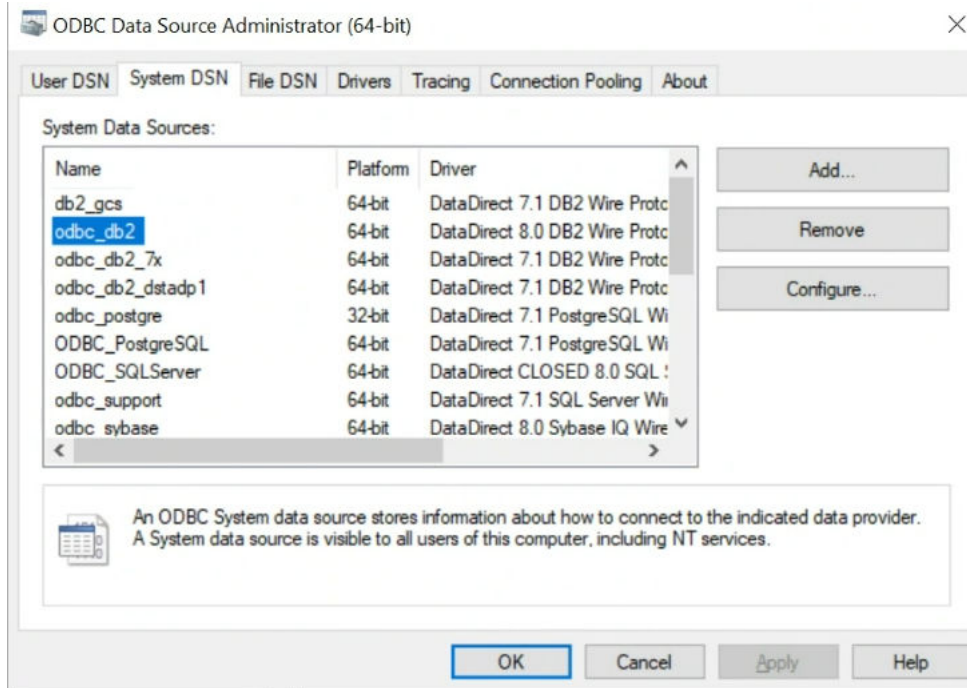
[<DSN_NAME>]
Driver=<Teradata_ClientHome>/lib64/tdata.so
Description=DataDirect 7.1 Teradata
AccountString=
AuthenticationDomain=
AuthenticationPassword=
AuthenticationUserid=
CharacterSet=ASCII
DBCName=<Teradata Server>
Database=<Database name>
EnableDataEncryption=0
EnableExtendedStmtInfo=0
EnableLOBs=1
EnableReconnect=0
IntegratedSecurity=0
LoginTimeout=20
LogonID=<User name>
MapCallEscapeToExec=0
MaxRespSize=8192
Password=<Password>
PortNumber=1025
PrintOption=N
ProcedureWithSplSource=Y
ReportCodePageConversionErrors=0
SecurityMechanism=
SecurityParameter=
ShowSelectableTables=1
TDProfile=
TDRole=
TDUserName=
```

Windows での ODBC ドライバの設定

Windows 上の ODBC 準拠のデータベースまたはデータウェアハウスに接続するように ODBC 接続を確立する前に、ODBC ドライバを設定します。

1. データベースまたはデータウェアハウス固有の Web サイトから ODBC ドライバをダウンロードします。
注: DB2 ODBC (64 ビット) ドライバおよび SAP IQ ODBC (64 ビット) ドライバを取得する方法については、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。
2. ODBC ドライバを Secure Agent マシンにインストールします。
3. ODBC データソースファイルのインストール先のフォルダを開きます。
4. odbcad32.exe ファイルを実行します。
[ODBC データソースアドミニストレータ] ダイアログボックスが表示されます。

5. **【システム DSN】** をクリックします。

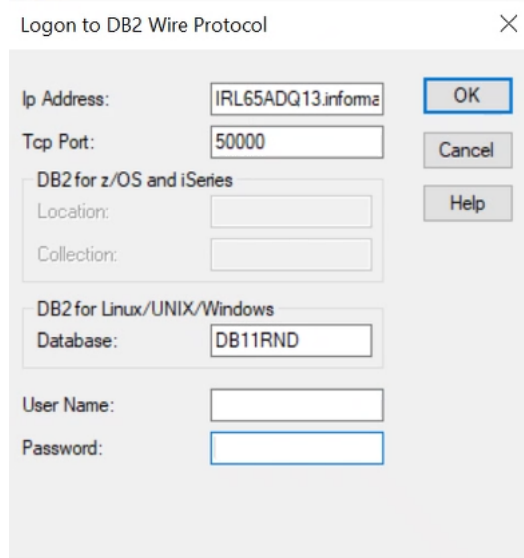


注: ODBC 接続では、システム DSN のみが使用されます。ODBC ドライバの設定時にユーザー DSN を使用することはできません。

6. 使用するシステムデータソースを選択し、**【追加】** をクリックします。
- 【データソースの新規作成】** ダイアログボックスが表示されます。
7. データソースを設定する ODBC ドライバを選択します。
8. **【完了】** をクリックします。
- 選択したドライバを設定するためのダイアログボックスが表示されます。
9. ドライバに必要な接続プロパティを指定します。

10. **[OK]** をクリックして、設定した ODBC ドライバの変更を保存します。

注: DB2 ODBC ドライバを設定する場合は、**[接続のテスト]** をクリックして設定した接続をテストし、**[DB2 ワイヤプロトコルへのログオン]** ダイアログボックスで DB2 データベースの資格情報を指定して、変更を保存します。



Kerberos 認証の準備

必要な構成ファイルを Secure Agent マシンに配置することで、Kerberos 認証を使用して DB2 または SAP Sybase ASE データベースに接続できます。また、Kerberos 認証を使用して、SSL 対応の DB2 または SAP Sybase ASE データベースに接続することもできます。

DB2 または SAP Sybase ASE に接続するように Kerberos 認証を設定する場合は、次のガイドラインを考慮してください。

- ホステッドエージェントまたはサーバーレスランタイム環境は使用できません。
- 使用する Secure Agent とデータベースサーバーが KDC サーバーに登録されていることを確認してください。
- krb5.conf ファイルに複数の KDC を追加することはできません。
- 資格情報キャッシュファイルを生成するには、以下のガイドラインを考慮してください。
 - Linux 上の DB2 データベースに接続する場合、接続内の複数の Kerberos プリンシパルユーザーに対して、資格情報キャッシュファイルを生成できます。ただし、マッピング内で使用できる Kerberos プリンシパルユーザーは 1 人だけです。
 - Windows 上の DB2 データベースまたは SAP Sybase ASE データベースに接続する場合、接続内の複数の Kerberos プリンシパルユーザーに対して、資格情報キャッシュファイルを生成することはできません。
- odbc.ini ファイルの接続エントリに次の値を指定していることを確認してください。
 - AuthenticationMethod=4
 - GSSClient=libgssapi_krb5.so.2

odbc.ini ファイルの接続エントリの詳細については、「[「ODBC 接続タイプのサンプル odbc.ini ファイル」\(ページ 560\)](#)」を参照してください。

Kerberos 認証の設定

Kerberos 認証を使用して Linux または Windows 上の DB2 または SAP Sybase ASE に接続する前に、組織の管理者は前提条件のタスクを実行する必要があります。

1. krb5.conf ファイルを設定するには、次のタスクを実行します。
 - a. Secure Agent マシン上に krb5.conf ファイルを作成します。
 - b. Key Distribution Center (KDC) と管理サーバーの詳細を、次の形式で krb5.conf ファイルに追加します。

```
[libdefaults]
default_realm = <Realm name>
forwardable = true
ticket_lifetime = 24h

[realms]
<REALM NAME> = {
kdc = <Location where KDC is installed>
admin_server = <Location where KDC is installed>
}

[domain_realm]
<domain name or host name> = <Domain name or host name of Kerberos>
<domain name or host name> = <Domain name or host name of Kerberos>
```
2. Secure Agent マシン上で次の環境変数を設定します。
必要な環境変数については、[「環境変数の設定」 \(ページ 566\)](#)を参照してください。
3. Secure Agent を再起動します。
4. Secure Agent マシン上で認証情報キャッシュファイルを生成し、選択した ODBC サブタイプに Kerberos 認証を使用して接続するには、次のタスクを実行します。
 - a. Secure Agent マシンで次のコマンドを実行し、選択した ODBC サブタイプのユーザー名とレルム名を指定します。

```
Kinit <user name>@<realm_name>
```
 - b. オプションで、Linux 上の DB2 データベースに接続する際に、Secure Agent マシン上に指定されたディレクトリとファイル名を使用して資格情報キャッシュファイルを生成するには、次のコマンドを実行します。

```
Kinit -c <Directory and file name where you want to create the credential cache> <user name>@<realm_name>
```
 - c. 要求されたら、Kerberos プリンシパルユーザーのパスワードを入力します。

環境変数の設定

Kerberos 認証を使用して DB2 または SAP Sybase ASE に接続するには、Secure Agent マシン上で必要な環境変数を設定する必要があります。

- setenv KRB5CCNAME <資格情報キャッシュファイルの絶対パスとファイル名>
- setenv KRB5_CONFIG <Kerberos 構成ファイルの絶対パス>\krb5.conf

環境変数を設定した後に、Secure Agent を再起動する必要があります。

または、サブタイプが **[DB2]** あるいは **[SAP Sybase ASE]** の ODBC 接続を作成するときに、環境変数を追加することもできます。

ODBC 接続の **[Kerberos 接続プロパティ]** フィールドに *KRB5_CONFIG* と *KRB5CCNAME* の詳細を入力します。

例えば、次の形式でプロパティを追加します。

```
KRB5_CONFIG=<Absolute path of the Kerberos configuration file>\krb5.conf;KRB5CCNAME=<Absolute path of the credential cache file>/<File name>
```

注: キーと値のペアはそれぞれセミコロンで区切ってください。

ODBC 接続

ODBC 準拠のデータベースまたはデータウェアハウスに接続するように ODBC の接続プロパティを設定してみましょう。

ODBC 接続を使用して、任意の ODBC 準拠のエンドポイントに接続することができます。ただし、この接続では、特定のエンドポイントに接続するための ODBC サブタイプも提供されます。サブタイプにより、エンドポイントに接続してデータの読み取りまたは書き込みを行うときに、接続またはマッピングで設定できる追加機能を定義します。

ODBC のサブタイプと定義済みの機能については、次の表を参照してください。

ODBC サブタイプ	エンドポイント	機能
Azure DW	Microsoft Azure SQL Data Warehouse	読み取りおよび書き込み操作に対する、マッピングでの SQL ELT の最適化の有効化。
DB2	DB2 データベース	<ul style="list-style-type: none">- 読み取りおよび書き込み操作に対する、マッピングでの SQL ELT の最適化の有効化。- SQL トランスフォーメーションを使用した、ストアードプロシージャの呼び出し。- Kerberos 認証を使用して DB2 に接続します。
Google BigQuery	Google BigQuery	読み取りおよび書き込み操作に対する、マッピングでの SQL ELT の最適化の有効化。
PostgreSQL	PostgreSQL	読み取りおよび書き込み操作に対する、マッピングでの SQL ELT の最適化の有効化。
Redshift	Amazon Redshift	読み取りおよび書き込み操作に対する、マッピングでの SQL ELT の最適化の有効化。
SAP IQ	SAP IQ データベース	SAP IQ データベースからのデータの読み取り。
SAP Sybase ASE	Sybase ASE データベース	<ul style="list-style-type: none">- Sybase ASE データベースに対する読み取りまたは書き込み。- Kerberos 認証を使用して SAP Sybase ASE に接続します。
Snowflake	Snowflake	読み取りおよび書き込み操作に対する、マッピングでの SQL ELT の最適化の有効化。

ODBC サブタイプ	エンドポイント	機能
Teradata	Teradata	<ul style="list-style-type: none"> - Teradata データベースからの読み取りと書き込みを行います。 - 読み取りおよび書き込み操作に対する、マッピングでの SQL ELT の最適化の有効化。 - SQL トランスフォーメーションを使用した、ストアードプロシージャの呼び出し。 - SQL トランスフォーメーションから保存されたクエリを使用した、Teradata での SQL クエリの実行。 <p>注: SSL 対応の ODBC Teradata 接続を使用する場合は、Teradata ODBC ドライバの設定時に、[WebSocket] の [SSL モード] オプションに適切な値を設定してください。</p>
その他	Greenplum、Microsoft Access、Microsoft Excel、および Netezza	<ul style="list-style-type: none"> - Microsoft Access、Microsoft Excel、または Netezza エンドポイントでの読み取りおよび書き込み操作のマッピングで SQL ELT の最適化を有効にします。 - また、【その他】 サブタイプを使用して、ODBC 準拠のエンドポイントに接続し、データの読み取りまたは書き込みを行うこともできます。 - Greenplum データベースに接続する際に、SCRAM-SHA-256 パスワード認証を設定できます。 <p>詳細については、Configure SCRAM-SHA-256 password authentication に関する Knowledge の記事を参照してください。</p>

始める前に

開始する前に、ODBC ドライバと ODBC クライアントを Secure Agent マシンにインストールして、ODBC 接続を確立する必要があります。

設定の前提条件の詳細については、「[「前提条件」 \(ページ 559\)](#)」を参照してください。

接続の詳細

次の表に、基本接続プロパティを示します。

財産	説明
接続名	<p>接続の名前。</p> <p>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。_ . + - ,</p> <p>最大長は 255 文字です。</p>
説明	<p>接続の説明。最大長は 4000 文字です。</p>

財産	説明
シークレットコンテナの使用	<p>組織に対して設定されている Secrets Manager にこの接続の機密資格情報を保存します。このプロパティは、組織に Secrets Manager が設定されている場合にのみ表示されます。このプロパティは、データ取り込みおよびレプリケーションとデータアクセス管理サービスではサポートされていません。</p> <p>接続でシークレットコンテナを有効にすると、Secure Agent が Secrets Manager からどの資格情報を取得するかを選択できます。このオプションを無効にした場合、資格情報は組織の設定方法に応じてリポジトリまたはローカル Secure Agent に保存されます。</p> <p>注: この接続を使用してプッシュダウンまたはプロキシサービスを介してデータアクセスポリシーを適用する場合、シークレットコンテナ設定オプションを使用することはできません。</p> <p>Secrets Manager を設定および使用する方法については、Administrator のヘルプにある「Secrets Manager の設定」を参照してください。</p>
ランタイム環境	<p>タスクを実行するランタイム環境の名前。</p> <p>Secure Agent、ホステッドエージェント、サーバーレスランタイム環境、またはエラスティックランタイム環境を選択します。</p> <p>サーバーレス環境の設定の詳細については、「サーバーレスランタイム環境の設定」 (ページ 572)を参照してください。</p> <p>エラスティック環境の設定の詳細については、「エラスティックランタイム環境の設定」 (ページ 574)」を参照してください。</p>
ODBC サブタイプ	<p>特定の ODBC 準拠のエンドポイント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。</p> <p>ODBC サブタイプとその機能については、を参照してください。 「ODBC 接続」 (ページ 567)。</p>
認証モード	<p>DB2 または SAP Sybase ASE に接続するための認証方法。</p> <p>このプロパティは、ODBC サブタイプに [DB2] または [SAP Sybase ASE] を選択した場合にのみ表示されます。</p> <p>リストから次のいずれかの認証モードを選択します。</p> <ul style="list-style-type: none"> - データベース。ユーザー名とパスワードを使用して、選択した ODBC サブタイプに接続します。 - Kerberos。Kerberos 認証を使用して、選択した ODBC サブタイプに接続します。 <p>Windows でこのオプションを選択する場合は、選択した ODBC サブタイプのエンドポイントに Secure Agent サービスを開始するユーザーアカウントが存在し、そのサブタイプとデータのやり取りを行うために必要な権限が割り当てられていることを確認してください。</p> <p>注: ホステッドエージェントまたはサーバーレスランタイム環境を使用している場合は、Kerberos 認証を設定できません。</p> <p>デフォルトは [データベース] です。</p>
Kerberos 接続プロパティ	<p>Kerberos 認証を使用して DB2 または SAP Sybase ASE に接続するための追加の接続プロパティ。</p> <p>このプロパティは、ODBC サブタイプに [DB2] または [SAP Sybase ASE] を選択し、認証モードに [Kerberos] を選択した場合にのみ表示されます。</p> <p>複数のプロパティを指定する場合は、キーと値のペアをそれぞれセミコロンで区切ります。</p> <p>例えば、Secure Agent マシンに必要な環境変数が設定されていない場合は、Kerberos 認証を使用する前に次の形式で <code>KRB5_CONFIG</code> プロパティと <code>KRB5CCNAME</code> プロパティを追加します。</p> <p><code>KRB5_CONFIG=<Kerberos 構成ファイルの絶対パス>\krb5.conf;KRB5CCNAME=<資格情報キャッシュファイルの絶対パス>/<ファイル名></code></p>

財産	説明
ユーザー名	ODBC 準拠のエンドポイントに接続するためのユーザー名。
パスワード	ODBC 準拠のエンドポイントに接続するためのパスワード。 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	ODBC オブジェクトのデータソース名。

財産	説明
スキーマ	ODBC オブジェクトのスキーマ名。
コードページ	<p>接続で定義された ODBC 準拠のエンドポイントサーバーまたはフラットファイルのコードページ。</p> <p>次のいずれかのコードページを選択します。</p> <ul style="list-style-type: none"> - 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 - EBCDIC 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)

財産	説明
	- Israeli Standard 960 (7 ビット Hebrew エンコーディング)

詳細設定

次の表に、詳細接続のプロパティを示します。

プロパティ	説明
Linux 用のドライバマネージャ	Linux でホストされている Secure Agent マシンのドライバマネージャ。 Linux で新しい ODBC 接続を作成する場合は、リストから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。
接続環境 SQL	PostgreSQL または Teradata データベースに接続する場合に、ODBC 準拠のエンドポイントを設定するための SQL 文。データベース環境は、この接続を使用するセッション全体に適用されます。 1 つまたは複数の SQL 文を追加できます。それぞれの SQL 文はセミコロンで区切ります。 例えば、次の文を入力してタイムゾーンを設定できます。 SET timezone to 'America/New_York'; SQL ELT の最適化の有無にかかわらず、マッピングで使用する Teradata 接続で SQL 文を設定することができます。ただし、PostgreSQL データベースに接続する場合、このプロパティはマッピングで SQL ELT の最適化を有効にした場合にのみ適用されます。

ODBC 接続のルールとガイドライン

ODBC 接続を作成する場合のルールおよびガイドラインは、次のとおりです。

- Secure Agent マシンが SUSE Linux でホストされている場合、Snowflake ODBC ドライバを使用することはできません。
Snowflake への接続に使用できる Snowflake ODBC ドライバの詳細および Snowflake ODBC 接続を設定する手順については、Informatica How-To ライブラリの記事「[Configure SQL ELT optimization for Snowflake using ODBC Connector](#)」を参照してください。
- 接続で ODBC サブタイプとして Teradata を使用している場合、**【接続環境 SQL】** プロパティで指定できる SQL 文は 1 つだけです。

サーバーレスランタイム環境の設定

AWS または Azure でホストされているサーバーレスランタイム環境を使用して、ODBC 準拠のデータベースに接続できます。

サーバーレスランタイム環境を使用して ODBC 接続を設定する前に、次のタスクを実行してください。

- AWS または Azure アカウントの Amazon S3 バケットあるいは Azure コンテナに ODBC ドライバを追加します。
- .yaml サーバーレス構成ファイルを設定する。

AWS または Azure アカウントの Amazon S3 バケットあるいは Azure コンテナに ODBC ドライバを追加します

ODBC 接続でサーバーレスランタイム環境を使用するには、次の手順を実行します。

1. AWS または Azure のサーバーレスエージェント設定用に次の構造を作成します: <補足ファイルの場所>/serverless_agent_config
2. AWS アカウントまたは Azure アカウントの次の場所にある Amazon S3 バケットあるいは Azure コンテナに ODBC ドライバを追加します: <補足ファイルの場所>/serverless_agent_config/ODBC

.yaml サーバーレス構成ファイルを設定する

サーバーレスランタイム環境で.yaml サーバーレス構成ファイルを設定するには、次の手順を実行します。

1. 次のコードスニペットをテキストエディタにコピーし、ドライバファイル名と DSN エントリを指定します:

```
version: 1
agent:
  dataIntegrationServer:
    autoDeploy:
      odbc:
        drivers:
          - fileCopy:
              sourcePath: ODBC/<Driver_file name>
          - fileCopy:
              sourcePath: ODBC/<Driver_file name>
        dsns:
          - name: "<Name of the ODBC database>"
            entries:
              - key: Driver
                value: <Driver_file name>
              - key: Description
                value: "<Description of the driver>"
```

ここで、ソースパスは AWS または Azure の ODBC ドライバのディレクトリパスです。

注: DSN エントリは、サーバーレスランタイムの場所に追加するドライバに応じて異なります。

次の例に、Microsoft SQL Server ドライバの DSN エントリを示します。

```
version: 1
agent:
  dataIntegrationServer:
    autoDeploy:
      odbc:
        drivers:
          - fileCopy:
              sourcePath: ODBC/DWdb227.so
          - fileCopy:
              sourcePath: ODBC/DWdb227.so
        dsns:
          - name: "<SQL server>"
            entries:
              - key: Driver
                value: DWSqls227.so
              - key: Description
                value: "SQL Server 2014 Connection for ODL"
              - key: HostName
                value: INWV16SQL19
              - key: PortNumber
                value: 1433
```

```

- key: Database
  value: adapter_semantic
- key: QuotedId
  value: No
- key: AnsiNPW
  value: Yes

```

2. 構文とインデントが有効であることを確認してから、ファイルを `serverlessUserAgentConfig.yml` として次の AWS または Azure の場所に保存します: <補足ファイルの場所>/`serverless_agent_config.yml` ファイルの実行時に、ODBC ドライバが AWS または Azure の場所からサーバーレスエージェントディレクトリにコピーされ、`odbc.ini` ファイルの DNS エントリが更新されます。

サーバーレスランタイム環境の設定および使用方法の詳細については、Administrator のヘルプにある「サーバーレスランタイム環境」を参照してください。

エラスティックランタイム環境の設定

マッピング実行中にエラスティックランタイム環境がカスタムバイナリファイルにアクセスして実行できるよう、ランタイム環境でこれらのファイルを設定することができます。

カスタムバイナリファイルを設定する前に、Informatica Intelligent Cloud Services 内でデータを処理できる Kubernetes クラスタを作成できるエラスティックランタイム環境を必ず AWS にデプロイしてください。

エラスティックランタイム環境のデプロイの詳細については、「[Deploy an elastic runtime environment](#)」を参照してください。

エラスティックランタイム環境をデプロイした後、マウントされたディスクにカスタムバイナリファイルを配置し、使用するバイナリファイルの正確なパスを POST 要求内にコピーします。

カスタムバイナリファイルを管理するには、Informatica Intelligent Cloud Services for Elastic Runtime Environment 内で以下の手順を実行します。

1. 組織にログインし、セッション ID とランタイム環境 ID を取得します。
2. REST API への POST 呼び出しを、セッション ID、ランタイム環境 ID、および、マウントされたディスクから以前にコピーしたバイナリファイルのパスを渡して行います。
POST 呼び出しの詳細については、『REST API リファレンス』ガイド内の「[Supplementary files](#)」を参照してください。

POST 要求の例を以下に示します。

```

POST <base URL>/api/v3/RuntimeEnvironment/<runtime environment ID>/ElasticConfig
Content-Type: application/json
Accept: application/json
INFA-SESSION-ID: <SessionId>
{
  "rteId": "rte-12345",
  "specification": {
    "agent": {
      "dataIntegrationServer": {
        "odbc": {
          "drivers": [
            {
              "sourcePath": "/<path of driver in data disk>/DWSqls18.so"
            }
          ],
          "dsns": [
            {
              "name": "ODBC_SQLServer",
              "entries": [

```

```

    {
      "key": "Driver",
      "value": "DWSqls18.so"
    },
    {
      "key": "Description",
      "value": "Test Connection"
    },
    {
      "key": "HostName",
      "value": "<"
    },
    {
      "key": "PortNumber",
      "value": "1234"
    },
    {
      "key": "Database",
      "value": "cloud_DB"
    },
    {
      "key": "QuotedId",
      "value": "No"
    },
    {
      "key": "AnsiNPW",
      "value": "Yes"
    }
  ]
}

```

注: キーと値のペアが odbc.ini ファイル内のキーと値のペアと同じであることを確認します。

この POST 呼び出しにより、データ統合サーバーの再起動がトリガーされます。

3. Administrator でデータ統合サーバーの状態を確認することで、エラスティックランタイム環境が起動されて稼働していることを確認します。
4. 接続をテストするかマッピングを実行することで、エラスティックランタイム環境がカスタムバイナリファイルにアクセスして使用できることを確認します。

第 164 章

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。

重要: OpenAir コネクタは非推奨となり、メンテナンスモードに移行されました。Informatica は将来のリリースでサポートを廃止する予定です。

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。
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。

第 165 章

オープンテーブル接続プロパティ

オープンテーブル接続を作成して、カタログで使用可能なオープンテーブル形式に対してデータの読み取りまたは書き込みを安全に行います。

オープンテーブル接続を使用して、マッピングおよびマッピングタスクでソース、ターゲット、およびルックアップを指定できます。

前提条件

オープンテーブル接続を作成する前に、前提条件を満たしてください。

AWS Glue カタログと Amazon S3 ストレージを使用した Apache Iceberg または Delta Lake テーブルの操作

AWS Glue カタログと Amazon S3 ストレージを使用して Apache Iceberg または Delta Lake テーブルを操作する場合は、AWS 上のテーブルを管理する次の AWS サービスにアクセスする必要があります。

- AWS Glue カタログ: AWS Glue カタログにより、Apache Iceberg テーブルまたは Delta Lake テーブルに関連付けられたメタデータを管理します。
- Amazon S3 Storage: Amazon S3 は、実際のレコードを含む Apache Iceberg テーブルまたは Delta Lake テーブルをカラム形式で保存し、パーティション化されたディレクトリに整理します。
- Amazon Athena: Amazon Athena は、AWS Glue データカタログを使用して、Amazon S3 に保存されるデータのテーブル名や列名などのメタデータを保存します。オープンテーブルコネクタは、Amazon Athena JDBC driver を使用して AWS Glue カタログに接続し、Apache Iceberg テーブルまたは Delta Lake テーブルのメタデータにアクセスして、Amazon S3 ストレージに保存されたデータに対して SQL クエリを実行します。

これらのサービスにアクセスするには、個別のポリシーを作成する必要があります。

Hive メタストアカタログと Microsoft Azure Delta Lake Storage Gen2 を使用した Apache Iceberg テーブルの操作

Hive メタストアカタログと Microsoft Azure Delta Lake Storage Gen2 を使用して Apache Iceberg テーブルを操作する場合は、Microsoft Azure Delta Lake Storage Gen2 上のテーブルを管理する次のサービスにアクセスする必要があります。

- Hive メタストアカタログ: Hive メタストアカタログにより、Apache Iceberg テーブルに関連付けられたメタデータを管理します。
- Microsoft Azure Delta Lake Storage Gen2: Microsoft Azure Delta Lake Storage Gen2 は、実際のレコードを含む Apache Iceberg テーブルをカラム形式で保存し、パーティション化されたディレクトリに整理します。

- Hive JDBC ドライバ: Hive JDBC ドライバにより、Hive メタストアカタログに接続して Apache Iceberg テーブルのメタデータにアクセスし、Microsoft Azure Delta Lake Storage Gen2 に保存されたデータに対して SQL クエリを実行します。

Hive メタストアカタログと Amazon S3 ストレージを使用した Apache Iceberg テーブルの操作

Hive メタストアカタログと Amazon S3 ストレージを使用して Apache Iceberg テーブルを操作する場合は、Amazon S3 ストレージ上のテーブルを管理する次のサービスにアクセスする必要があります。

- Hive メタストアカタログ: Hive メタストアカタログにより、Apache Iceberg テーブルに関連付けられたメタデータを管理します。
- Amazon S3 ストレージ: Amazon S3 により、実際のレコードを含む Apache Iceberg テーブルをカラム形式で保存し、パーティション化されたディレクトリに整理します。
- Hive JDBC ドライバ: Hive JDBC ドライバは Hive4 サーバーに接続して、Apache Iceberg テーブルのメタデータにアクセスします。

REST カタログと Amazon S3 を使用した Apache Iceberg テーブルの操作

Polaris カタログなどの REST カタログと Amazon S3 ストレージを使用して Apache Iceberg テーブルを操作する場合は、Amazon S3 ストレージ上のテーブルを管理する次のサービスにアクセスする必要があります。

- REST カタログ: REST カタログは、Apache Iceberg テーブルに関連付けられたメタデータを管理します。
- Amazon S3 ストレージ: Amazon S3 により、実際のレコードを含む Apache Iceberg テーブルをカラム形式で保存し、パーティション化されたディレクトリに整理します。

最小限の IAM ポリシーの作成

AWS Glue カタログによって管理される Apache Iceberg テーブルまたは Delta Lake テーブルを操作するために最低限必要な権限を持つ IAM ポリシーを作成する必要があります。これらのポリシーの設定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。

Amazon Athena の最小限のポリシー

次のサンプルポリシーは、Amazon Athena にアクセスするための最小限の Amazon IAM ポリシーを示しています。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": [
        "athena:CreatePreparedStatement",
        "athena:GetPreparedStatement",
        "athena:GetWorkGroup",
        "athena:GetTableMetadata",
        "athena:StartQueryExecution",
        "athena:GetQueryResultsStream",
        "athena:ListDatabases",
        "athena:GetQueryExecution",
        "athena:GetQueryResults",
        "athena:GetDatabase",
        "athena:ListTableMetadata",
        "athena:GetDataCatalog",
        "athena>DeletePreparedStatement"
      ],
      "Resource": [
        "arn:aws:athena:*:*:workgroup/*",
        "arn:aws:athena:*:*:datacatalog/*"
      ]
    }
  ]
}
```

```

    },
    {
      "Sid": "VisualEditor1",
      "Effect": "Allow",
      "Action": [
        "athena:ListDataCatalogs",
        "athena:GetQueryExecution",
        "athena:ListWorkGroups",
        "athena:GetPreparedStatement"
      ],
      "Resource": "*"
    }
  ]
}

```

AWS Glue の最小限のポリシー

次のサンプルポリシーは、AWS Glue カタログにアクセスするための最小限の Amazon IAM ポリシーを示しています。

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "glue:*"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}

```

AWS S3 の最小限のポリシー

次のサンプルポリシーは、Amazon S3 バケットに対してデータの読み取りと書き込みを行うための最小限の Amazon IAM ポリシーを示しています。

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": [
        "s3:PutObject",
        "s3:GetObject",
        "s3:ListBucket",
        "s3:DeleteObject"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:ListBucket",
        "s3:GetBucketLocation",
        "s3:ListAllMyBuckets",
        "s3:GetBucketAcl"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}

```

JDBC ドライバのインストール

オープンテーブルコネクタを使用する前に、Secure Agent をインストールした Linux マシンに Amazon Athena または Hive JDBC ドライバをコピーする必要があります。AWS Glue カタログには Amazon Athena ドライバを使用し、Hive メタストアカタログには Hive JDBC ドライバを使用する必要があります。

1. 最新の Hive JDBC ドライバを Web サイトからダウンロードしてください。
2. Secure Agent マシンの次のディレクトリに移動します。<Secure Agent のインストールディレクトリ>/ext/connectors/thirdparty/
3. 次のフォルダを作成します: `informatica.opentableformat/common`
4. JDBC ドライバをフォルダに追加します。
5. Secure Agent を再起動します。

ロールを引き受けるための EC2 ロールの設定

IAM ロールを引き受けるように EC2 ロールを設定し、同じ AWS アカウントまたは異なる AWS アカウントから Amazon S3 に接続するための一時的なセキュリティ資格情報を生成できます。

ロールを引き受けるように EC2 ロールを設定する場合は、一時的なセキュリティ資格情報を使用するための **sts:AssumeRole** 権限が割り当てられており、AWS アカウント内で信頼関係が確立されていることを確認してください。信頼関係は、ロールを作成するときに、IAM ロールの信頼ポリシーで定義されます。IAM ロールにより、EC2 ロールを信頼されたエンティティとして追加し、EC2 ロールに一時的なセキュリティ資格情報の使用と AWS アカウントへのアクセスを許可します。

信頼された EC2 ロールが一時的なセキュリティ資格情報を要求すると、AWS Security Token Service (AWS STS) によって、指定した期間有効な一時的なセキュリティ資格情報が動的に生成され、信頼された EC2 ロールにその資格情報が提供されます。

ロール認証を引き受けるための EC2 ロールを使用する前に、次の前提条件を考慮してください。

- AWS EC2 インスタンスに Secure Agent をインストールします。
- AWS EC2 インスタンスにアタッチされた EC2 ロールには、別の IAM ロールを引き受ける権限が必要です。以下に、AWS EC2 インスタンスにアタッチされている EC2 ロールの権限ポリシーの例を示します。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "sts:AssumeRole",
      "Resource": "arn:aws:iam::001234567890:role/open_table_rolearn"
    }
  ]
}
```

リソース値には、EC2 ロールが引き受ける必要がある IAM ロールの ARN を含める必要があります。

- EC2 ロールが引き受ける必要のある IAM ロールには、AWS Glue カタログ、Amazon Athena、および Amazon S3 にアクセスするための権限ポリシーと信頼ポリシーがアタッチされている必要があります。また、より安全なアクセスのために、AWS アカウントの外部 ID を指定することもできます。外部 ID は文字列である必要があります。

次のサンプルに、外部 ID を指定した、引き受けた IAM ロールの信頼ポリシーを示します。

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



```

    "AWS": "arn:aws:iam::001234567890:root" //anyone in this account 001234567890 can assume
this role, this can also be limited to one role.
    },
    "Action": "sts:AssumeRole",
    "Condition": {
      "StringEquals": {
        "sts:ExternalId": "aws_externalid"
      }
    }
  }
]
}

```

最小の権限ポリシーの詳細については、「[「最小限の IAM ポリシーの作成」 \(ページ 578\)](#)」を参照してください。

オープンテーブルへの接続

AWS Glue カタログ、Hive メタストア、または Polaris REST カタログに接続するようにオープンテーブルへの接続プロパティを設定しましょう。

始める前に

始める前に、AWS Glue カタログによって管理される Apache Iceberg または Delta Lake テーブルを操作するために必要な最低限の IAM ポリシーを作成し、Hive メタストア用に Hive JDBC ドライバをインストールする必要があります。また、Amazon S3 または Microsoft Azure Delta Lake Storage Gen2 ストレージに接続するための認証固有の前提条件を設定する必要もあります。

Amazon S3 用の永続的な IAM 資格情報認証には、IAM ユーザーのアクセスキーとシークレットキーの値が必要です。Amazon S3 にアクセスするために EC2 ロールがロール引き受け (Assume Role) 認証を行うには、一時的なセキュリティ認証情報を生成するために、EC2 ロールが引き受ける IAM ロールの ARN を必要とします。

Microsoft Azure Delta Lake Storage Gen2 用にサービスプリンシパル認証を設定するには、Azure Active Directory に登録されているアプリケーションの Azure アカウント名、クライアントシークレット、クライアント ID、およびテナント ID が必要です。

Apache Iceberg テーブルまたは Delta Lake テーブルにアクセスするためのポリシーとロールの設定方法の詳細については、「[「前提条件」 \(ページ 577\)](#)」を参照してください。

オープンテーブル形式、および関連するカタログタイプとストレージタイプ

使用するオープンテーブル形式と、それに関連付けられたカタログタイプおよびストレージタイプを選択して、データを操作できます。

次の表は、使用できるオープンテーブル形式、カタログタイプ、ストレージタイプ、および各ストレージタイプで使用可能な認証オプションをまとめたものです。

オープンテーブル形式	カタログタイプ	カタログ認証タイプ	ストレージタイプ	ストレージ認証タイプ
Apache Iceberg	AWS Glue カタログ*	なし	Amazon S3*	<ul style="list-style-type: none"> - 永続的な IAM 資格情報認証 - ロールを引き受けるための EC2 ロール
	Hive Metastore	なし	Amazon S3	永続的な IAM 資格情報認証
	Hive Metastore	なし	Microsoft Azure Delta Lake Storage Gen2	サービスプリンシパル認証
	REST カタログ	OAuth 2.0 資格情報	Amazon S3	永続的な IAM 資格情報認証
Delta Lake	AWS Glue カタログ	なし	Amazon S3	永続的な IAM 資格情報認証

*Amazon S3 ストレージを使用して AWS Glue カタログによって管理される Apache Iceberg テーブルは、通常のマッピングおよび詳細モードのマッピングに適用されます。
他のカタログおよびストレージタイプを含むオープンテーブル形式は、詳細モードのマッピングにのみ適用されます。

接続の詳細

次の表に、オープン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	<p>接続の名前。</p> <p>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。_ . + - ,</p> <p>最大長は 255 文字です。</p>
説明	<p>接続の説明。最大長は 4000 文字です。</p>
シークレットコンテナの使用	<p>組織に対して設定されている Secrets Manager にこの接続の機密資格情報を保存します。このプロパティは、組織に Secrets Manager が設定されている場合にのみ表示されます。このプロパティは、データ取り込みおよびレプリケーションとデータアクセス管理サービスではサポートされていません。</p> <p>接続でシークレットコンテナを有効にすると、Secure Agent が Secrets Manager からどの資格情報を取得するかを選択できます。このオプションを無効にした場合、資格情報は組織の設定方法に応じてリポジトリまたはローカル Secure Agent に保存されます。</p> <p>注: この接続を使用してプッシュダウンまたはプロキシサービスを介してデータアクセスポリシーを適用する場合、シークレットコンテナ設定オプションを使用することはできません。</p> <p>Secrets Manager を設定および使用する方法については、Administrator のヘルプにある「Secrets Manager の設定」を参照してください。</p>

プロパティ	説明
ランタイム環境	<p>タスクを実行するランタイム環境の名前。</p> <p>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。</p> <p>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。</p> <p>ランタイム環境の設定および使用方法の詳細については、Administrator のヘルプにある「ランタイム環境」を参照してください。</p>
オープンテーブルフォーマット	<p>カタログに対してデータの読み取りまたは書き込みを行う際に使用するオープンテーブル形式。</p> <p>リストから [Apache Iceberg] または [Delta Lake] を選択します。</p>

カタログタイプ

選択したオープンテーブル形式のメタデータを管理する場合に、カタログタイプとして AWS Glue カタログ、Hive メタストア、または REST カタログを選択することができます。

オープンテーブル形式で使用するカタログのタイプを選択し、カタログ固有のパラメータを設定します。

AWS Glue カタログ

Apache Iceberg または Delta Lake オープンテーブル形式でカタログタイプとして AWS Glue カタログを使用する場合は、AWS Glue カタログに固有のプロパティを設定します。

次の表に、AWS Glue カタログを設定するためのプロパティとその説明を示します。

プロパティ	説明
Athena JDBC URL	<p>JDBC URL は次の形式で入力します。</p> <p><code>jdbc:athena://Region=<AWS_Region>;OutputLocation=<S3_Location></code></p> <p>例: <code>jdbc:athena://Region=us-west1;OutputLocation=s3://working/dir</code></p>
カタログ認証タイプ	<p>カタログに接続するための認証方法。</p> <p>次のいずれかのオプションを選択します。</p> <ul style="list-style-type: none"> - なし。認証資格情報を使用せずに AWS Glue カタログまたは Hive メタストアに接続します。 - OAuth 2.0 クライアント資格情報。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 REST カタログに接続し、認証サーバーからアクセストークンを取得します。

Hive Metastore

Apache Iceberg オープンテーブル形式でカタログタイプとして Hive メタストアを使用する場合は、Hive メタストアに固有のプロパティを設定します。

次の表に、Hive メタストアを設定するためのプロパティとその説明を示します。

プロパティ	説明
Hive メタストア URI	Hive Metastore に接続するための Hive Thrift サーバー URL。
Hive JDBC URL	Hive4 サーバーに接続するための JDBC URL。
Hive ユーザー名	Hive Metastore に接続するための Hive アカウントのユーザー名。
HIVE パスワード	Hive Metastore に接続するための Hive アカウントのパスワード。
カタログ認証タイプ	カタログに接続するための認証方法。 次のいずれかのオプションを選択します。 <ul style="list-style-type: none">- なし。認証資格情報を使用せずに AWS Glue カatalog または Hive メタストアに接続します。- OAuth 2.0 クライアント資格情報。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 REST カatalog に接続し、認証サーバーからアクセストークンを取得します。

REST カatalog

Apache Iceberg オープンテーブル形式で Catalog タイプとして REST カatalog を使用する場合は、REST カatalog に固有のプロパティを設定します。

次の表に、REST カatalog を設定するためのプロパティとその説明を示します。

プロパティ	説明
REST カatalog タイプ	接続する REST カatalog のタイプ。 [Polaris カatalog] を選択します。
カタログエンドポイント URL	REST カatalog のエンドポイント URL。
カタログ認証タイプ	カタログに接続するための認証方法。 次のいずれかのオプションを選択します。 <ul style="list-style-type: none">- なし。認証資格情報を使用せずに AWS Glue カatalog または Hive メタストアに接続します。- OAuth 2.0 クライアント資格情報。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 REST カatalog に接続し、OAuth 2.0 認証サーバーからアクセストークンを取得します。
アクセストークン URL	アクセストークンを取得するために OAuth 2.0 認証サーバーによって提供される URL。
クライアント ID	OAuth 2.0 認証サーバーに登録されている REST エンドポイントのクライアント ID。
クライアントシークレット	OAuth 2.0 認証サーバーに登録されている REST エンドポイントのクライアントシークレット。

プロパティ	説明
スコープ	アクセストークンが REST エンドポイントに付与する権限を定義するスコープパラメータ。
資格情報ベンディング	REST カタログのストレージに認証が必要かどうかを指定します。 資格情報ベンディングが有効になっている場合は、関連付けられたストレージにアクセスするための一時的な資格情報を自動的に生成するように REST カタログが設定されていることを示します。ストレージ資格情報を個別に指定する必要はありません。 資格情報ベンディングが無効になっている場合は、ストレージ資格情報を個別に指定する必要があることを示します。 資格情報ベンディングが無効になっている場合、更新、更新/挿入、および削除操作のために、テーブルストレージの場所から一時ステージングディレクトリが削除されることはありません。

ストレージタイプ

オープンテーブル形式のテーブルを保存する場合に、Amazon S3 または Microsoft Azure Data Lake Storage Gen2 をストレージタイプとして選択することができます。

ストレージタイプを選択し、ストレージ固有の認証パラメータを設定します。

Amazon S3

カタログタイプとして AWS Glue カタログ、Hive メタストア、または REST カタログを使用する場合は、Amazon S3 ストレージに固有のプロパティを設定します。

永続的な IAM 資格情報認証

AWS Glue カタログ、Hive メタストア、または REST カタログに接続する場合は、Amazon S3 ストレージの永続的な IAM 資格情報認証を使用できます。

次の表に、Permanent IAM Credentials authentication を設定するためのプロパティを示します。

プロパティ	説明
アクセスキー	AWS Glue カタログにアクセスするためのキー。
シークレットキー	AWS Glue カタログにアクセスするためのシークレットキー。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。

ロール認証を引き受けるための EC2 ロール

EC2 ロールを使用して Amazon S3 ストレージのロール認証を引き受けることができるのは、AWS Glue カタログから Apache Iceberg テーブルを読み取る場合のみです。

次の表に、ロール認証を引き受けるように EC2 ロールを設定するためのプロパティを示します。

プロパティ	説明
IAM ロール ARN	一時的なセッション資格情報を生成するために EC2 ロールが引き受ける IAM ロールの ARN。
外部 ID	IAM ロールが sts:AssumeRole API を呼び出すときに EC2 ロールに指定する必要がある一意のユーザー定義の文字列値。

Microsoft Azure Data Lake Storage Gen2

カタログタイプとして Hive メタストアを使用する場合は、Microsoft Azure Data Lake Storage Gen2 に固有のプロパティを設定します。

認証タイプとして [サービスプリンシパル認証] を選択し、Microsoft Azure Data Lake Storage Gen2 のオープンテーブル形式にアクセスします。

サービスプリンシパル認証

次の表に、サービスプリンシパル認証を設定するためのプロパティとその説明を示します。

プロパティ	説明
Azure アカウント名	ファイルをステージングするための Microsoft Azure Data Lake Storage Gen2 アカウントの名前。
Azure クライアント ID	アプリケーションのクライアント ID。 Azure Active Directory に登録されているアプリケーションのアプリケーション ID またはクライアント ID を入力します。
Azure 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。
Azure テナント ID	アプリケーションのディレクトリ ID またはテナント ID。

第 166 章

Oracle 接続のプロパティ

Oracle データベースに対してデータの安全な読み取りまたは書き込みを行うための Oracle 接続を作成します。

前提条件

Oracle コネクタを使用すると、Oracle データベース認証または Kerberos 認証を使用して、SSL 対応の Oracle データベースに接続できます。

SSL が有効な Oracle データベースに接続するには、[「SSL 設定」 \(ページ 587\)](#)を参照してください。

Kerberos 認証を使用して Oracle データベースに接続するには、[「Kerberos 認証」 \(ページ 589\)](#)を参照してください。

SSL 設定

Oracle データベース認証または Kerberos 認証を使用した安全な Oracle 接続を使用して、SSL 対応の Oracle データベースに接続する前に、組織管理者は前提条件のタスクを実行する必要があります。

1. トラストストア証明書を作成します。
2. キーストア証明書を作成します。Oracle データベースでクライアント認証が有効になっている場合のみ、この操作を実行します。

トラストストアへのサーバー証明書の追加

サーバー証明書をクライアントのトラストストアに追加して、安全な Oracle 接続を確立します。

次の keytool コマンドを使用して、サーバー証明書をクライアントのトラストストアに追加します。

```
keytool -import -trustcacerts -alias ca -file <server certificate with path> -keystore  
<name of truststore to be generated with extension> -storepass <password for truststore> -storetype <store  
type>
```

例として、C:\SSL\oracle にサーバー証明書 oratls_server.cert があるとします。

1. 次のコマンドを実行し、トラストパスワード「password」を使用してトラストストア truststore.jks を作成します。

```
C:\SSL\oracle> keytool -import -trustcacerts -alias ca -file oratls_server.cert -keystore truststore.jks -  
storepass password -storetype JKS
```

2. 次のコマンドを実行し、トラストストアパスワード「password」を使用して PKCS12 トラストストア truststore.p12 を作成します。

```
C:\SSL\oracle> keytool -import -trustcacerts -alias ca -file oratls_server.cert -keystore truststore.p12 -  
storepass password -storetype PKCS12
```

キーストア証明書の作成

Oracle サーバーでクライアント認証が有効になっている場合にキーストア証明書を作成します。Oracle 接続を確立するため、クライアント証明書をすべて含むキーストア証明書を作成する必要があります。

次の手順を実行してキーストア証明書を作成します。

1. Oracle クライアントを Oracle の Web サイトからダウンロードし、インストールします。
2. 次のコマンドを実行して Oracle ウォレットを作成します。
`orapki wallet create -wallet <Path where wallet is to be created> -auto_login -pwd <wallet password>`
3. 次のコマンドを実行して、Oracle ウォレットへの自己署名クライアント証明書を作成します。
`orapki wallet add -wallet <Path where wallet is to be created> -dn "CN=<common name>, OU=<organization unit>, O=<organization>, L=<locality>, ST=<state>, C=<country>" -keysize <key size in bits> -self_signed -validity <number of days> -pwd <wallet password>`
コマンドが実行され、指定された場所に pkcs12 証明書が作成されます。
サーバー証明書から、CN=<共通名>、OU=<組織単位>、O=<組織>、L=<市区町村>、ST=<都道府県>、C=<国>、keysize <キーサイズ (ビット)>、self_signed -validity <日数>、および pwd <ウォレットパスワード>の値を指定する必要があります。
4. 次の orapki コマンドを実行して自己署名クライアント証明書をエクスポートします。
`orapki wallet export -wallet <wallet path> -dn "CN=<common name>, OU=<organization unit>, O=<organization>, L=<locality>, ST=<state>, C=<country>" -cert <Name of the exported certificate with path>`
-dn コマンドでクライアント証明書を一意に特定します。サーバーウォレットにはインストール済みのクライアント証明書が複数含まれているためです。
5. 自己署名クライアント証明書をサーバー Oracle ウォレットにインストールします。
注: 自己署名クライアント証明書をサーバーデータベース Oracle ウォレットに追加しないと、クライアント認証は失敗します。
6. サーバー証明書を、信頼されている証明書として Oracle ウォレットに追加します。
次のコマンドを実行してサーバー証明書を追加します。
`orapki wallet add -wallet <wallet path> -trusted_cert -cert <Name of the server certificate with path> -pwd <wallet password>`
注: すべての orapki コマンドに同じウォレットパスワードを使用する必要があります。

サンプルタスク

次のタスクを実行してキーストア証明書を作成します。

1. 次のコマンドを実行して Oracle ウォレットを作成します。
`C:\app\client\ksuwalka\product\12.1.0\client_1\BIN>orapki wallet create -wallet C:\app\client\ksuwalka\product\12.1.0\client_1\owm\wallet -auto_login -pwd oracle4u`
2. 次のコマンドを実行して、Oracle ウォレットへの自己署名クライアント証明書を作成します。
`C:\app\client\ksuwalka\product\12.1.0\client_1\BIN>orapki wallet add -wallet C:\app\client\ksuwalka\product\12.1.0\client_1\owm\wallet -dn "CN=inw1pc07_kriti, OU=DEV, O=infa,L=blr, ST=ka, C=IN" -keysize 2048 -self_signed -validity 3650 -pwd oracle4u`
ewallet.p12 証明書が次の場所に作成されます。C:\app\client\ksuwalka\product\12.1.0\client_1\owm\wallet
3. 次の orapki コマンドを実行して自己署名クライアント証明書をエクスポートします。
`C:\app\client\ksuwalka\product\12.1.0\client_1\BIN>orapki wallet export -wallet C:\app\client\ksuwalka\product\12.1.0\client_1\owm\wallet -dn "CN=inw1pc07_kriti, OU=DEV, O=infa,L=blr, ST=ka, C=IN" -cert C:\Users\ksuwalka\Desktop\client_inw1pc07.cert`

4. サーバー証明書を、信頼されている証明書として Oracle ウォレットに追加します。次のコマンドを実行してサーバー証明書を追加します。

```
C:\app\client\ksuwalka\product\12.1.0\client_1\BIN>orapki wallet add -wallet C:\app\client\ksuwalka\product\12.1.0\client_1\owm\wallet -trusted_cert -cert C:\SSL\oracle\oratsls_server.cert -pwd oracle4u
```

キーストア C:\app\client\ksuwalka\product\12.1.0\client_1\owm\wallet\ewallet.p12 を、キーストアパスワード oracle4u で使用できるようになりました。

Kerberos 認証

必要な構成ファイルを Secure Agent マシンに配置することで、Kerberos 認証を使用して Oracle データベースに接続できます。また、Kerberos 認証を使用して、SSL 対応の Oracle データベースに接続することもできます。

Oracle に接続するために Kerberos 認証を設定する場合は、次のガイドラインを考慮してください。

- ホステッドエージェントまたはサーバーレスランタイム環境は使用できません。
- 使用する Secure Agent とデータベースサーバーが KDC サーバーに登録されていることを確認してください。
- krb5.conf ファイルに複数の KDC を追加することはできません。
- 複数の Kerberos プリンシパルユーザーに対して資格情報キャッシュファイルを生成することはできません。

Kerberos 認証の設定

Kerberos 認証を使用して Linux または Windows 上の Oracle に接続する前に、組織の管理者は前提条件のタスクを実行する必要があります。

1. Java Authentication and Authorization Service 構成ファイル（JAAS）を設定するには、次のタスクを実行します。

- a. Secure Agent マシン上に JAAS 構成ファイルを作成します。
- b. 以下のエントリを JAAS 構成ファイルに追加します。

```
JDBC_DRIVER_01 {  
    com.sun.security.auth.module.Krb5LoginModule required useTicketCache=true;  
};
```

2. krb5.conf ファイルを設定するには、次のタスクを実行します。

- a. Secure Agent マシン上に krb5.conf ファイルを作成します。
- b. Key Distribution Center（KDC）と管理サーバーの詳細を、次の形式で krb5.conf ファイルに追加します。

```
[libdefaults]  
default_realm = <Realm name>  
forwardable = true  
ticket_lifetime = 24h  
  
[realms]  
<REALM NAME> = {  
    kdc = <Location where KDC is installed>  
    admin_server = <Location where KDC is installed>  
}  
  
[domain_realm]  
<domain name or host name> = <Domain name or host name of Kerberos>  
<domain name or host name> = <Domain name or host name of Kerberos>
```

3. Secure Agent マシン上で次の環境変数を設定します。

必要な環境変数については、[「環境変数の設定」 \(ページ 590\)](#)を参照してください。

4. Secure Agent を再起動します。
5. Secure Agent マシン上で資格情報キャッシュファイルを生成し、Kerberos 認証を使用して Oracle に接続するには、次のタスクを実行します。
 - a. Secure Agent マシンで次のコマンドを実行し、Oracle ユーザー名とレルム名を指定します。
`kinit <user name>@<realm_name>`
 - b. 要求されたら、Kerberos プリンシパルユーザーのパスワードを入力します。

環境変数の設定

Kerberos 認証を使用して Oracle に接続するには、Secure Agent マシン上で必要な環境変数を設定する必要があります。

以下の環境変数を設定します。

- `setenv KRB5CCNAME <資格情報キャッシュファイルの絶対パスとファイル名>`
- `setenv KRB5_CONFIG <Kerberos 構成ファイルの絶対パス>\krb5.conf`
- `setenv JAASCONFIG <JAAS 構成ファイルの絶対パス>\<ファイル名>.conf`

環境変数を設定した後に、Secure Agent を再起動する必要があります。

または、Oracle 接続の作成時に環境変数を追加することもできます。

接続を設定して Kerberos 認証を使用する場合に環境変数を追加するには、Oracle 接続の **【メタデータの詳細 接続プロパティ】** フィールドに `KRB5CONFIG`、`KRB5CCNAME`、および `JAASCONFIG` プロパティを追加する必要があります。

例えば、次の形式でプロパティを追加します。

```
KRB5_CONFIG=<Absolute path of the Kerberos configuration file>\krb5.conf;KRB5CCNAME=<Absolute path of the credential cache file>/<File name>;JAASCONFIG=<Absolute path of the JAAS config file>\<File name>.conf
```

注: キーと値のペアはそれぞれセミコロンで区切ってください。

Oracle への接続

Oracle データベースに接続するように Oracle 接続のプロパティを設定してみましょう。

始める前に

接続を設定する前に、[「前提条件」 \(ページ 587\)](#)を参照して認証要件を確認してください。

接続の詳細

次の表に、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。
シークレット コンテナの使 用	組織に対して設定されている Secrets Manager にこの接続の機密資格情報を保存します。 このプロパティは、組織に Secrets Manager が設定されている場合にのみ表示されます。 このプロパティは、データ取り込みおよびレプリケーションとデータアクセス管理サービスではサポートされていません。 接続でシークレットコンテナを有効にすると、Secure Agent が Secrets Manager からどの資格情報を取得するかを選択できます。このオプションを無効にした場合、資格情報は組織の設定方法に応じてリポジトリまたはローカル Secure Agent に保存されます。 注: この接続を使用してプッシュダウンまたはプロキシサービスを介してデータアクセスポリシーを適用する場合、シークレットコンテナ設定オプションを使用することはできません。 Secrets Manager を設定および使用する方法については、Administrator のヘルプにある「Secrets Manager の設定」を参照してください。
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。 Secure Agent、ホステッドエージェント、サーバーレスランタイム環境、またはエラスティックランタイム環境を選択します。 ランタイム環境の設定および使用方法の詳細については、Administrator のヘルプにある「ランタイム環境」を参照してください。
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。

認証モード

次のいずれかの認証モードを設定して、Oracle データベースに接続できます。

- Oracle データベース認証
- Kerberos 認証

注: Oracle データベースに接続する場合に、LDAP 認証を設定することはできません。

必要な認証モードを選択し、認証固有のパラメータを設定します。

デフォルトは Oracle データベース認証です。

Oracle データベース認証

Oracle データベース認証では Oracle ユーザー名とパスワードを使用して Oracle に接続します。

次の表に、Oracle データベース認証の基本接続プロパティとその説明を示します。

プロパティ	説明
ユーザー名	データベースログインに使用するユーザー名。ユーザー名にセミコロンを含めることはできません。
パスワード	データベースログインに使用するパスワード。パスワードにセミコロンを含めることはできません。
ホスト	データベースサーバーをホストするマシンの名前。
ポート	データベースサーバーに接続するときに使用するネットワークポート番号。 デフォルトは 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	マッピングでのオブジェクト選択時にテーブルを選択するためのスキーマ名。 複数のスキーマからテーブルを選択する場合は、フィールドを空白のままにします。空白のままにすると、アクセス権を持つすべてのスキーマが表示され、使用可能なスキーマからテーブルを選択できます。
コードページ	データベースサーバーのコードページ。

Kerberos 認証

Kerberos 認証を使用して Oracle に接続します。

Windows でこのオプションを選択する場合は、Secure Agent サービスを開始するユーザーアカウントが Oracle データベースで使用可能になっていることを確認してください。Oracle にアクセスするために資格情報を入力する必要はありません。

注: ホステッドエージェントまたはサーバーレスランタイム環境を使用している場合は、Kerberos 認証を設定できません。

次の表に、Kerberos 認証の基本接続プロパティとその説明を示します。

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 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>

プロパティ	説明
スキーマ	マッピングでのオブジェクト選択時にテーブルを選択するためのスキーマ名。 複数のスキーマからテーブルを選択する場合は、フィールドを空白のままにします。空白のままにすると、アクセス権を持つすべてのスキーマが表示され、使用可能なスキーマからテーブルを選択できます。
コードページ	データベースサーバーのコードページ。

詳細設定

次の表に、Oracle データベース認証の詳細接続プロパティとその説明を示します。

プロパティ	説明
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。 デフォルトは「暗号化なし」です。 このプロパティは、ホステッドエージェントを使用する場合には適用されません。
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。
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。 <code>/home/cldagnt/SystemAgent/serverless/configurations/ssl_store/<TrustStore_filename></code>
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。 <code>/home/cldagnt/SystemAgent/serverless/configurations/ssl_store/<KeyStore_filename></code>
キーストアのパスワード	通信を安全に行うために必要なキーストアファイルのパスワードです。

プロパティ	説明
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別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	<p>JDBC ドライバがメタデータを取得するための追加プロパティ。プロパティは次の形式で入力します:</p> <p><パラメータ名>=<パラメータ値></p> <p>複数のプロパティを入力する場合は、それぞれのキーと値のペアをセミコロンで区切ります。例えば、接続をテストするときに接続タイムアウトを設定するには、次のプロパティを入力します:</p> <p>LoginTimeout=<value_in_seconds></p> <p>注: デフォルトの接続のタイムアウトは 270 秒です。</p> <p>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。</p> <p>例: EncryptionTypes=AES256;</p> <p>EncryptionLevel=accepted;DataIntegrityLevel=accepted;</p> <p>DataIntegrityTypes=SHA1</p>
ランタイムの詳細 接続プロパティ	<p>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。</p> <p>複数のプロパティを指定する場合は、キーと値のペアをそれぞれセミコロンで区切ります。</p> <p>例: charset=sjis;</p> <p>readtimeout=180</p> <p>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。</p> <p>例: EncryptionTypes=AES256;EncryptionLevel=1;</p> <p>DataIntegrityLevel=1;DataIntegrityTypes=SHA1;</p> <p>DataIntegrityTypes=SHA1</p>

サーバーレスランタイム環境での SSL の設定

Oracle コネクタでサーバーレスランタイム環境を使用して、SSL 対応の Oracle データベースに接続できます。

サーバーレスランタイム環境を使用して安全な Oracle 接続を設定する前に、次の前提条件タスクを完了して、SSL 証明書をサーバーレスランタイムの場所に追加します。

1. AWS または Azure のサーバーレスエージェント設定用に次の構造を作成します: <補足ファイルの場所>/serverless_agent_config
2. AWS アカウントまたは Azure アカウントの次の場所にある Amazon S3 バケットあるいは Azure コンテナにトラストストアとキーストアの証明書を追加します: <補足ファイルの場所>/serverless_agent_config/SSL
3. 次のコードスニペットをテキストエディタにコピーします。

```
version: 1
agent:
  agentAutoApply:
```

```
general:
  sslStore:
    - fileCopy:
        sourcePath: SSL/<TrustStore_filename>
    - fileCopy:
        sourcePath: SSL/<KeyStore_filename>
```

ここで、ソースパスは AWS または Azure の証明書ファイルのディレクトリパスです。

4. 構文とインデントが有効であることを確認してから、ファイルを `serverlessUserAgentConfig.yml` として次の AWS または Azure の場所に保存します: <補足ファイルの場所>/serverless_agent_config.yml ファイルの実行時に、SSL 証明書が AWS または Azure の場所からサーバーレスエージェントディレクトリにコピーされます。
5. Oracle 接続のプロパティで、**[トラストストア]** フィールドと **[キーストア]** フィールドの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/<cert_filename>`

Oracle 接続のルールおよびガイドライン

Oracle 接続を作成する場合のルールおよびガイドラインは、次のとおりです。

- Oracle テーブル名には最大 30 文字を使用できます。
- Public スキーマ内に Oracle データベースを含むタスクを実行する場合、そのスキーマに含まれるオブジェクト数が多過ぎないようにします。スキーマに含まれるオブジェクト数が多過ぎると、タスクでタイムアウトが発生します。その場合は、Oracle データベースから一部のオブジェクトを削除するか、別のデータベーススキーマにオブジェクトを移動してください。
- Oracle データベースターゲットのタスクを実行する場合は、UTF-8 文字列が varchar または char フィールドの最大長を超えないようにします。varchar または char フィールドの最大長を超える UTF-8 文字列は、データ統合によって切り詰められることがあります。
- フラットファイルから Oracle に書き込むデータにポルトガル語の文字が含まれている場合、Oracle サーバーのコードページが MS Windows Latin 1 に設定されていないことを確認します。Oracle 接続の作成時に、コードページに ISO 8859-15 Latin 1 を選択します。
- スキーマ名にハイフンが含まれている場合、スキーマ名では大文字と小文字が区別されます。

第 167 章

Oracle Autonomous Database 接続

Oracle Autonomous Database に対するデータの読み取りまたは書き込みを行うための Oracle Autonomous Database 接続を作成します。Oracle Autonomous Database 接続を使用すると、マッピングおよびマッピングタスクでソースおよびターゲットを指定することができます。

前提条件

Oracle Autonomous Database に対して読み取りまたは書き込みを行うための Oracle Autonomous Database 接続を作成する前に、前提条件を必ず満たすようにしてください。

メモリ要件

Oracle Autonomous Database コネクタを使用する際に、Secure Agent に `INFA_MEMORY` および `JVM` オプションを設定してパフォーマンスを最適化し、Java ヒープおよびメモリ関連のエラーを回避できます。これらのプロパティは、Administrator のエージェントの詳細ページで定義します。

Secure Agent に必要な設定と詳細な手順の詳細については、『データ統合のパフォーマンスのチューニング』ドキュメントの「`INFA_MEMORY` および `JVM` オプション」を参照してください。

オブジェクトストレージ認証の準備

Oracle Autonomous Database コネクタに対して、次のようなオブジェクトストレージ認証方法を設定することができます。

ConfigFile 認証

ConfigFile 認証では、認証用の構成ファイルを介して提供される Oracle Cloud Infrastructure (OCI) アカウントの ID 資格情報が使用されます。この認証方法は、構成ファイルで選択されたプロファイルに基づきます。

構成ファイルは、次の形式で作成することができます：

```
[<profile name>]
user=<user ocid>
fingerprint=<fingerprint>
tenancy=<tenancy ocid>
region=<region>
key_file=<private key file location>
```


構成ファイルの OCI アカウントからのユーザー OCID、フィンガープリント、およびテナンシ OCID 情報が必要です。

Oracle Cloud Infrastructure コンソールからアイデンティティ資格証明を抽出するステップの詳細については、「[Oracle Cloud Infrastructure documentation](#)」を参照してください。

デフォルトでは、OCI 構成ファイルは Secure Agent マシンの ~/.oci/config にあります。~/.oci/config ファイルには、複数のプロファイルを含めることができます。デフォルトのプロファイル名は DEFAULT です。デフォルトのプロファイル名は、~/.oci/config ファイルに追加するプロファイルに基づいて、新しいプロファイル名に変更することもできます。~/.oci/config ファイルに同じ名前の 2 つのプロファイルを含めることはできません。

簡易認証

簡易認証では、認証に API キーを使用します。認証の詳細は、Oracle Autonomous Database 接続で指定することができます。シークレットキーファイルを Secure Agent マシンに配置する必要があります。

Oracle Autonomous Database 接続を作成するには、Oracle Cloud Infrastructure アカウントからのユーザー OCID、フィンガープリント、およびテナンシ OCID 情報が必要です。

Oracle Cloud Infrastructure コンソールからアイデンティティ資格証明を抽出するステップの詳細については、「[Oracle Cloud Infrastructure documentation](#)」を参照してください。

Oracle Autonomous Database への接続

Oracle Autonomous Database データベースに接続するように Oracle Autonomous Database の接続プロパティを設定してみましょう。

始める前に

開始する前に、次の前提条件を満たすようにしてください。

- コネクタのメモリ要件を設定します。
- 設定するオブジェクトストレージ認証タイプに基づいて、Oracle Cloud Infrastructure アカウントから必要な情報を取得します。

このタスクの詳細については、「[前提条件](#)」 (ページ 596) を参照してください。

接続の詳細

Oracle Autonomous Database 接続の作成時に、接続プロパティを設定します。

次の表に、基本接続プロパティを示します。

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

プロパティ	説明
シークレット コンテナの使用	<p>組織に対して設定されている Secrets Manager にこの接続の機密資格情報を保存します。このプロパティは、組織に Secrets Manager が設定されている場合にのみ表示されます。このプロパティは、データ取り込みおよびレプリケーションとデータアクセス管理サービスではサポートされていません。</p> <p>接続でシークレットコンテナを有効にすると、Secure Agent が Secrets Manager からどの資格情報を取得するかを選択できます。このオプションを無効にした場合、資格情報は組織の設定方法に応じてリポジトリまたはローカル Secure Agent に保存されます。</p> <p>注: この接続を使用してプッシュダウンまたはプロキシサービスを介してデータアクセスポリシーを適用する場合、シークレットコンテナ設定オプションを使用することはできません。</p> <p>Secrets Manager を設定および使用方法については、Administrator のヘルプにある「Secrets Manager の設定」を参照してください。</p>
ランタイム環境	<p>タスクを実行するランタイム環境の名前。</p> <p>Secure Agent 環境またはエラスティックランタイム環境を選択します。</p> <p>ランタイム環境の設定および使用方法の詳細については、Administrator のヘルプにある「ランタイム環境」を参照してください。</p>
ユーザー名	Oracle Autonomous Database にアクセスするためのユーザー名。これは、接続の認証に使用されます。
[パスワード]	ユーザー名のパスワード

認証タイプ

Oracle Autonomous Database に接続する場合に、TLS 認証または相互 TLS 認証を設定することができます。必要な認証タイプを選択し、認証固有のパラメータを設定します。デフォルトは相互 TLS 認証です。

相互 TLS 認証

次の表に、相互 TLS 認証の基本接続プロパティとその説明を示します。

プロパティ	説明
サービス名	セキュア接続にアクセスした特定のデータベースサービス。
ウォレットパス	セキュア接続のウォレットファイルの場所。

TLS 認証

次の表に、TLS 認証の基本接続プロパティを示します。

プロパティ	説明
TNS 名	<p>TNS 名は tnsnames.ora ファイルで定義されます。</p> <p>例: String tnsEntry = "(description= ... (security=(ssl_server_dn_match=yes)))"</p>

オブジェクトストレージ認証タイプ

Oracle Autonomous Database への接続時に、接続をステージングするための ConfigFile または簡易認証を設定できます。必要な認証タイプを選択し、認証固有のパラメータを設定します。
デフォルトは [ConfigFile 認証] です。

ConfigFile 認証

次の表に、デフォルト認証の基本接続プロパティとその説明を示します。

プロパティ	説明
リージョン	オブジェクトストレージバケットが存在する Oracle Cloud Infrastructure リージョン。 リストから Oracle Cloud Object Storage リージョンを選択します。

詳細設定

次の表に、ConfigFile 認証の詳細接続プロパティとその説明を示します。

プロパティ	説明
設定ファイルの場所	Secure Agent マシン上の構成ファイルの絶対パス。 この値を入力しない場合、Secure Agent は ~/.oci/config にある構成ファイルを使用します。
プロファイル名	使用する設定ファイルのプロファイル名。 デフォルトは DEFAULT です。

簡易認証

次の表に、簡易認証の基本接続プロパティとその説明を示します。

プロパティ	説明
ユーザー OCID	Oracle Cloud Infrastructure でのユーザーの一意の識別子。 例: ocid1.user.oc1..aaaaaaaaherdgpkjqzrwbdc7n5ksokkot7c5jngtx3pgolr7oqbw7xzksza
フィンガープリント	パブリックキーのフィンガープリント。
テナンシー OCID	Oracle Cloud Infrastructure でのテナンシーの一意の識別子。テナンシーは、Oracle Cloud Infrastructure アカウントのグローバルに一意な名前です。 例: ocid1.tenancy.oc1..aaaaaaaaba3pv6wkcr4jqae5f44n2b2m2yt2j6rx32uzr4h25vqstifsfdsq
プライベートキーファイルの場所	Secure Agent マシン上にある PEM 形式のプライベートキーファイルの場所。
リージョン	オブジェクトストレージバケットが存在する Oracle Cloud Infrastructure リージョン。 リストから Oracle Cloud Object Storage リージョンを選択します。

第 168 章

Oracle Business Intelligence Publisher の接続プロパティ

Oracle Business Intelligence Publisher V1 接続を作成して Oracle Business Intelligence Publisher に接続し、Oracle Business Intelligence Publisher からデータの読み取りを行います。Oracle Business Intelligence Publisher V1 接続を使用すると、マッピングでソースを指定できます。

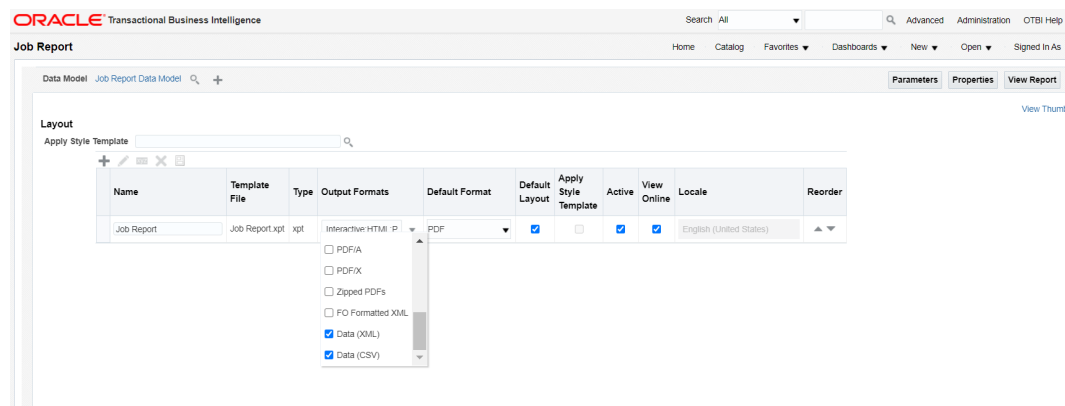
Oracle Business Intelligence Publisher への接続

Oracle Business Intelligence Publisher に接続するように Oracle Business Intelligence Publisher の接続プロパティを設定してみましょう。

始める前に

Oracle Business Intelligence Publisher V1 接続を使用して Oracle Business Intelligence Publisher からデータの読み取りを行う前に、レポートの出力形式を【データ (XML)】および【データ (CSV)】として設定します。Oracle Business Intelligence Publisher アプリケーション内。Oracle Business Intelligence Publisher アプリケーションは、少量のデータのみのデータ抽出に使用することを検討してください。

次の画像は、出力形式の値を設定できるページを示しています。



接続の詳細

次の表に、基本接続プロパティを示します。

プロパティ	説明
接続名	接続の名前。 各接続名は組織内で一意である必要があります。接続名には、英数字、スペース、および次の特殊文字を含めることができます。_ . + -, 最大長は 255 文字です。
説明	接続の説明。最大長は 4000 文字です。
シークレットコンテナの使用	組織に対して設定されている Secrets Manager にこの接続の機密資格情報を保存します。このプロパティは、組織に Secrets Manager が設定されている場合にのみ表示されます。このプロパティは、データ取り込みおよびレプリケーションとデータアクセス管理サービスではサポートされていません。 接続でシークレットコンテナを有効にすると、Secure Agent が Secrets Manager からどの資格情報を取得するかを選択できます。このオプションを無効にした場合、資格情報は組織の設定方法に応じてリポジトリまたはローカル Secure Agent に保存されます。 注: この接続を使用してプッシュダウンまたはプロキシサービスを介してデータアクセスポリシーを適用する場合、シークレットコンテナ設定オプションを使用することはできません。 Secrets Manager を設定および使用する方法については、Administrator のヘルプにある「Secrets Manager の設定」を参照してください。
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。 Secure Agent、ホステッドエージェント、またはサーバーレスランタイム環境を選択します。
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、Business Intelligence Publisher の 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。

プロパティ	説明
パスワード	Oracle Business Intelligence Publisher アカウントのパスワード。
レポートディレクトリ	<p>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。</p> <p>次のフォルダからレポートを読み取ることができます。</p> <ul style="list-style-type: none"> - 共有フォルダ - マイフォルダ <p>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。</p> <p>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。</p> <p>/Samples/Sales</p> <p>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。</p> <p>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。</p> <p>/~weblogic/Samples/Sales</p> <p>レポートディレクトリのデフォルト値は/Custom です。</p>

詳細設定

次の表に、詳細接続のプロパティを示します。

プロパティ	説明
出力ディレクトリ	<p>Oracle Business Intelligence Publisher から 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。</p> <p>注: このプロパティは、CSV データ形式でデータの読み取りを行う場合にのみ適用されます。</p>

プロキシサーバーの設定

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

Windows および Linux でプロキシサーバーを使用するように Secure Agent とサーバーレスランタイム環境を設定できます。認証されていないプロキシサーバーまたは認証されたプロキシサーバーを使用できます。プロキシ設定は、マッピングおよび詳細モードのマッピングで使用される接続に適用されます。

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

- Windows の場合は Secure Agent Manager を使用し、Linux の場合はシェルコマンドを使用して Secure Agent を設定します。
手順については、データ統合のヘルプの『または「Windows でのプロキシ設定」または「Linux でのプロキシ設定」を参照してください。
- Secure Agent のプロパティで、DTM の JVM オプションを設定します。手順については、ナレッジベースの記事「[Proxy server settings](#)」を参照してください。

サーバーレスランタイム環境のプロキシの設定を行う方法については、Administrator ヘルプの「「プロキシサーバーの使用」を参照してください。

第 169 章

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。
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	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gger（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。 <i>host_name</i> は、ホスト名または IP アドレスにできます。 <i>host_name:port_number</i> 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。

プロパティ	説明
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gger (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gger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gger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	<p>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。</p> <ul style="list-style-type: none"> - 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。 <p>デフォルトは【なし】です。</p>
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	<p>【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。</p> <p>【行】 または 【キロバイト】 のいずれかを選択します。</p>
マップの場所	<p>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。</p> <p>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gger (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。</p> <p>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。</p> <p>host_name:port_number</p> <p>以下に例を示します。</p> <p>ORACDC2B:25100</p> <p>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。</p>

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 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	<p>カスタムプロパティまたは接続プロパティのオーバーライド。カスタムプロパティとは、PowerExchange のデフォルトの設定よりも優先するために指定できるプロパティです。セミコロン (;) を区切り文字として使用して複数のプロパティを入力するか、パラメータファイルを使用して接続プロパティの上書きを指定するパラメータを指定することができます。</p> <p>例:</p> <pre><property>=<value>;<property>=<value></pre> <p>多くの場合、Informatica グローバルカスタマサポートからの指示を受けたいので、カスタムプロパティの設定を行います。</p> <p>注: これらのプロパティは、PowerCenter の PowerExchange Client for PowerCenter (PWXPC) CDC 接続の 【PWX オーバーライド】 オプションと同じです。</p> <p>パラメータファイルを使用して接続プロパティのオーバーライドを指定するには、\$<ParameterName>の形式でパラメータを設定し、ユーザー定義パラメータ名の前にドル記号 (\$) を付けます。次に、【ランタイムオプション】 タブの 【パラメータファイル名】 フィールドにパラメータファイル名を指定することで、ユーザー定義パラメータ定義を含むパラメータファイルを使用するようにマッピングのマッピングタスクを設定します。</p> <p>注:</p> <ul style="list-style-type: none"> - マッピングおよび接続に同じパラメータを入力した場合は、接続カスタムプロパティが優先されます。 - パラメータファイルがある場合、このフィールドで指定するパラメータ名は、パラメータファイルで定義されたエントリと一致する必要があります。 <p>詳細については、「接続オーバーライドのリファレンス」の章を参照してください。</p>

第 170 章

Oracle Cloud Object Storage 接続

Oracle Cloud Object Storage ファイルに対してデータを読み取りおよび書き込みをするための Oracle Cloud Object Storage 接続を作成します。Oracle Cloud Object Storage 接続を使用すると、マッピングおよびマッピングタスクでソースおよびターゲットを指定できます。

前提条件

Oracle Cloud Object Storage に対して読み取りまたは書き込みを行うための Oracle Cloud Object Storage 接続を作成する前に、前提条件を必ず満たすようにしてください。

Oracle Cloud Infrastructure ポリシーの設定

組織の管理者が Oracle Cloud Object Storage コネクタに最小限の Oracle Cloud Infrastructure (OCI) ID および Access Management (IAM) ポリシーを作成すると、ユーザーは Oracle Cloud Object Storage コネクタを使用できるようになります。

Oracle Cloud Infrastructure ポリシーにより、OCI アカウントでユーザーおよびグループがアクセスできるリソースと、それらのリソースにアクセスする方法を定義します。ポリシーを使用して、特定のコンパートメント内の特定のタイプのリソースを特定の方法で管理することができます。

次のタスクを実行する必要があります。

1. ユーザー、グループおよび 1 つ以上のコンパートメントを定義して、組織のクラウドリソースを保持します。
2. ポリシーを作成します。
3. 操作する必要があるコンパートメントおよびリソースに応じて、ユーザーを適切なグループに配置します。
4. コンソールにアクセスしてコンパートメントを操作するために必要なワンタイムパスワードをユーザーに提供します。

ユーザー、グループ、およびポリシーの追加の詳細については、「[Oracle Cloud Infrastructure documentation](#)」を参照してください。

ポリシーは、次の形式で作成することができます：

Allow group <group_name> to <verb> <resource-type> in compartment <compartment_name>

例:

Allow group ObjectReaders to read buckets in compartment ABC

Allow group ObjectWriters to manage objects in compartment ABC where any {request.permission='OBJECT_CREATE', request.permission='OBJECT_INSPECT'}

Oracle Cloud Object Storage 接続を設定し、オブジェクトにアクセスして、マッピングを実行するには、次のポリシーを追加する必要があります:

- Oracle Cloud Object Storage テスト接続のポリシー
Allow group <group_name> to inspect object-family in compartment <compartment_name>
Allow group <group_name> to inspect buckets in compartment <compartment_name>
- Oracle Cloud Object Storage ソースのポリシー
Allow group <group_name> to inspect buckets in compartment <compartment_name>
Allow group <group_name> to read object-family in compartment <compartment_name>
- Oracle Cloud Object Storage ターゲットのポリシー
Allow group <group_name> to manage inspect buckets in compartment <compartment_name>
Allow group <group_name> to manage object-family in compartment <compartment_name>

認証の準備

Oracle Cloud Object Storage コネクタでは、次の認証方法を設定できます。

ConfigFile 認証

ConfigFile 認証では、認証用の構成ファイルを介して提供される Oracle Cloud Infrastructure (OCI) アカウントの ID 資格情報が使用されます。この認証方法は、構成ファイルで選択されたプロファイルに基づきます。

構成ファイルは、次の形式で作成することができます:

```
[<profile name>]
user=<user ocid>
fingerprint=<fingerprint>
tenancy=<tenancy ocid>
region=<region>
key_file=<private key file location>
```

構成ファイルの OCI アカウントからのユーザー OCID、フィンガープリント、およびテナンシ OCID 情報が必要です。

Oracle Cloud Infrastructure コンソールからアイデンティティ資格証明を抽出するステップの詳細については、「[Oracle Cloud Infrastructure documentation](#)」を参照してください。

デフォルトでは、OCI 構成ファイルは Secure Agent マシンの ~/.oci/config にあります。~/.oci/config ファイルには、複数のプロファイルを含めることができます。デフォルトのプロファイル名は DEFAULT です。デフォルトのプロファイル名は、~/.oci/config ファイルに追加するプロファイルに基づいて、新しいプロファイル名に変更することもできます。~/.oci/config ファイルに同じ名前の 2 つのプロファイルを含めることはできません。

簡易認証

簡易認証では、認証に API キーを使用します。認証の詳細は、Oracle Cloud Object Storage 接続で指定することができます。シークレットキーファイルを Secure Agent マシンに配置する必要があります。

Oracle Cloud Object Storage 接続を作成するには、Oracle Cloud Infrastructure アカウントからのユーザー OCID、フィンガープリント、およびテナンシ OCID 情報が必要です。

Oracle Cloud Infrastructure コンソールからアイデンティティ資格証明を抽出するステップの詳細については、「[Oracle Cloud Infrastructure documentation](#)」を参照してください。

Oracle Cloud Object Storage への接続

Oracle Cloud Object Storage に接続するように Oracle Cloud Object Storage の接続プロパティを設定してみましょう。

始める前に

開始する前に、Oracle Cloud Infrastructure ポリシーを設定し、設定する認証タイプに基づいて Oracle Cloud Infrastructure アカウントから必要な情報を取得します。

これらのタスクの詳細については、「[「前提条件」 \(ページ 607\)](#)」を参照してください。

接続の詳細

Oracle Cloud Object Storage 接続の作成時に、接続プロパティを設定します。

次の表に、基本接続プロパティを示します。

プロパティ	説明
接続名	接続の名前。 各接続名は組織内で一意である必要があります。接続名には、英数字、スペース、および次の特殊文字を含めることができます。_ + -, 最大長は 255 文字です。
説明	接続の説明。最大長は 4000 文字です。
シークレットコンテナの使用	組織に対して設定されている Secrets Manager にこの接続の機密資格情報を保存します。 このプロパティは、組織に Secrets Manager が設定されている場合にのみ表示されます。 このプロパティは、データ取り込みおよびレプリケーションとデータアクセス管理サービスではサポートされていません。 接続でシークレットコンテナを有効にすると、Secure Agent が Secrets Manager からどの資格情報を取得するかを選択できます。このオプションを無効にした場合、資格情報は組織の設定方法に応じてリポジトリまたはローカル Secure Agent に保存されます。 注: この接続を使用してプッシュダウンまたはプロキシサービスを介してデータアクセスポリシーを適用する場合、シークレットコンテナ設定オプションを使用することはできません。 Secrets Manager を設定および使用する方法については、Administrator のヘルプにある「Secrets Manager の設定」を参照してください。
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。 Secure Agent またはエラスティックランタイム環境を選択します。 ランタイム環境の設定および使用方法の詳細については、Administrator のヘルプにある「ランタイム環境」を参照してください。 データベース取り込みとレプリケーションタスクでは、Secure Agent またはサーバーレスランタイム環境を使用できます。ホステッドエージェントまたはエラスティックランタイム環境でタスクを実行することはできません。

認証タイプ

ConfigFile または簡易認証を設定して、Oracle Cloud Object Storage に接続できます。必要な認証タイプを選択し、認証固有のパラメータを設定します。

デフォルトは [ConfigFile 認証] です。

ConfigFile 認証

次の表に、デフォルト認証の基本接続プロパティとその説明を示します。

プロパティ	説明
リージョン	オブジェクトストレージバケットが存在する Oracle Cloud Infrastructure リージョン。 リストから Oracle Cloud Object Storage リージョンを選択します。
バケット名	オブジェクトが格納されている Oracle Cloud Object Storage バケット名。

詳細設定

次の表に、ConfigFile 認証の詳細接続プロパティとその説明を示します。

プロパティ	説明
設定ファイルの場所	Secure Agent マシン上の構成ファイルの絶対パス。 この値を入力しない場合、Secure Agent は ~/.oci/config にある構成ファイルを使用します。
プロファイル名	使用する設定ファイルのプロファイル名。 デフォルトは DEFAULT です。
フォルダパス	指定した Oracle Cloud Object Storage バケットの配下のフォルダ。 次はその例です: bucket/Dir_1/Dir_2/FileName.txt。ここで、Dir_1/Dir_2 はフォルダパスです。

簡易認証

次の表に、簡易認証の基本接続プロパティとその説明を示します。

プロパティ	説明
ユーザー OCID	Oracle Cloud Infrastructure でのユーザーの一意の識別子。 例: ocid1.user.oc1..aaaaaaaaherdgpkjqzrwbdc7n5sokkot7c5jngtx3pgolr7oqb7xzksza
フィンガープリント	パブリックキーのフィンガープリント。
テナンシー OCID	Oracle Cloud Infrastructure でのテナンシーの一意の識別子。テナンシーは、Oracle Cloud Infrastructure アカウントのグローバルに一意な名前です。 例: ocid1.tenancy.oc1..aaaaaaaaba3pv6wkr4jqae5f44n2b2m2yt2j6rx32uzr4h25vqstifsfdsq
プライベートキーファイルの場所	Secure Agent マシン上にある .PEM 形式のプライベートキーファイルの場所。

プロパティ	説明
リージョン	オブジェクトストレージバケットが存在する Oracle Cloud Infrastructure リージョン。リストから Oracle Cloud Object Storage リージョンを選択します。
バケット名	オブジェクトが格納されている Oracle Cloud Object Storage バケット名。

詳細設定

次の表に、簡易認証の詳細接続プロパティとその説明を示します。

プロパティ	説明
フォルダパス	指定した Oracle Cloud Object Storage バケットの配下のフォルダ。 次はその例です: bucket/Dir_1/Dir_2/FileName.txt。ここで、Dir_1/Dir_2 はフォルダパスです。

プロキシサーバーの設定

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

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

注: マネージド ID 認証でプロキシサーバーを使用することはできません。

次のいずれかのタイプのプロキシサーバーを使用できます。

- 認証されていないプロキシ - 設定を行う場合はホストとポートアドレスのみが必要です。
- 認証されたプロキシ - 設定を行う場合は、ホストアドレス、ポートアドレス、ユーザー名、およびパスワードが必要です。

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

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

手順については、データ統合のヘルプの『または「Windows でのプロキシ設定」または「Linux でのプロキシ設定」を参照してください。

- Secure Agent のプロパティで、DTM の JVM オプションを設定します。手順については、ナレッジベースの記事「[Proxy server settings](#)」を参照してください。

第 171 章

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
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。
シークレットコンテナの使用	組織に対して設定されている Secrets Manager にこの接続の機密資格情報を保存します。 このプロパティは、組織に Secrets Manager が設定されている場合にのみ表示されます。 このプロパティは、データ取り込みおよびレプリケーションとデータアクセス管理サービスではサポートされていません。 接続でシークレットコンテナを有効にすると、Secure Agent が Secrets Manager からどの資格情報を取得するかを選択できます。このオプションを無効にした場合、資格情報は組織の設定方法に応じてリポジトリまたはローカル Secure Agent に保存されます。 注: この接続を使用してプッシュダウンまたはプロキシサービスを介してデータアクセスポリシーを適用する場合、シークレットコンテナ設定オプションを使用することはできません。 Secrets Manager を設定および使用方法については、Administrator のヘルプにある「Secrets Manager の設定」を参照してください。
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。 Secure Agent 環境またはエラスティックランタイム環境を選択します。 ランタイム環境の設定および使用方法の詳細については、Administrator のヘルプにある「ランタイム環境」を参照してください。
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。 <ul style="list-style-type: none">- 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。

接続プロパティ	説明
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。

第 172 章

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。

重要: Oracle CRM On Demand コネクタは非推奨となり、メンテナンスモードに移行されました。Informatica は将来のリリースでサポートを廃止する予定です。

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> 例：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

第 173 章

Oracle Database Ingestion 接続 のプロパティ

Oracle データベース取り込み接続を定義するには、接続プロパティを設定します。この接続は、データ取り込みおよびレプリケーションで設定したデータベース取り込みとレプリケーションタスクのソースまたはターゲットに使用することができます。また、アプリケーション取り込みとレプリケーションタスクのターゲットにも使用できます。

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。
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。ランタイム環境は、管理者で定義します。 サポートされているソースタイプを持つアプリケーション取り込みとレプリケーションタスクとデータベース取り込みとレプリケーションタスクでは、サーバーレスランタイム環境を使用できます。ホステッドエージェントで、アプリケーション取り込みとレプリケーションタスクまたはデータベース取り込みとレプリケーションタスクを実行することはできません。

プロパティ	説明
認証モード	<p>コネクタが Oracle へのログインに使用する必要がある認証モード。次のオプションがあります。</p> <ul style="list-style-type: none"> - Oracle データベース認証。Oracle のユーザー名とパスワードを使用して Oracle に接続します。 - Kerberos。Kerberos 認証を使用して Oracle に接続します。 <p>注: [Kerberos] を選択した場合、アプリケーションまたはデータベース取り込みおよびレプリケーションタスクで Oracle ソースまたはターゲットを定義するときに表示されるスキーマリストには、自分のスキーマだけでなく、他の Kerberos ユーザーのスキーマも表示されます。</p> <p>注: サーバーレスランタイム環境を Kerberos 認証と合わせて使用することはできません。</p> <p>デフォルトは Oracle データベース認証です。</p>
ドライバの種類	<p>Oracle ソースまたはターゲットへの接続に使用する JDBC ドライバのタイプ。次のオプションがあります。</p> <ul style="list-style-type: none"> - Progress DataDirect Oracle JDBC。Progress DataDirect for JDBC for Oracle ドライバを使用します。 - Native Oracle JDBC。Oracle JDBC ドライバを使用します。このドライバは、ソースからデータを読み取るときのパフォーマンスが向上することが実証されています。ただし、SSL 暗号化と一緒に使用しないでください。 <p>デフォルトは Progress DataDirect Oracle JDBC です。</p> <p>注: Native Oracle JDBC ドライバを選択した場合、この接続は新しいデータベース取り込みおよびレプリケーションジョブでのみ使用してください。</p> <p>DataDirect ドライバを使用して実行した既存のジョブの場合、Native Oracle JDBC ドライバへの切り替えはお勧めしません。</p>
ユーザー名	<p>Oracle データベース認証を使用する場合は、Oracle データベースログインのユーザー名。ユーザー名にセミコロンを含めることはできません。</p> <p>注: このプロパティは、Kerberos 認証を使用している場合は表示されません。</p>
パスワード	<p>Oracle データベース認証を使用する場合は、Oracle データベースログインのパスワード。パスワードにセミコロンを含めることはできません。</p> <p>注: このプロパティは、Kerberos 認証を使用している場合は表示されません。</p>
ホスト	データベースサーバーのホスト名。
ポート	データベースサーバーに接続するときに使用するネットワークポート番号。デフォルトは 1521 です。
サービス名	<p>Oracle データベースを一意に識別するサービス名またはシステム ID (SID)。Oracle データベースに接続するための SID を ;SID=<ORACLE_SID>の形式で指定します。先頭のセミコロン (;) も含めてください。</p>

プロパティ	説明
コードページ	データベースサーバーのコードページ。データベース取り込みとレプリケーションタスクは、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	<p>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。</p> <p>次のオプションがあります。</p> <ul style="list-style-type: none"> - 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。 <p>デフォルトは [暗号化なし] です。</p> <p>注: SSL を有効にするには、Secure Agent のインストールに固有の適切な JDK または JRE フォルダにある cacerts ファイルに Oracle SSL 証明書をインポートします。</p>
暗号プロトコルバージョン	<p>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。</p> <ul style="list-style-type: none"> - SSLv2 - SSLv3 - TLSv1.2 <p>デフォルトは TLSv1.2 です。</p>
サーバー証明書の検証	<p>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。</p> <ul style="list-style-type: none"> - 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。 <p>デフォルトは False です。</p> <p>[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。</p>
トラストストア	暗号化方法として SSL を選択し、サーバー証明書の検証を有効にした場合は、クライアントが SSL 認証のために信頼する認証局 (CA) のリストを含むトラストストアファイルのパスと名前を指定します。
トラストストアのパスワード	暗号化方法として SSL を選択し、サーバー証明書の検証を有効にした場合は、トラストストアファイルのコンテンツにアクセスするためのパスワードを指定します。
証明書内のホスト名	暗号化方法として SSL を選択し、サーバー証明書の検証を有効にした場合は、セキュリティを強化するために、Oracle データベースをホストするマシンのホスト名を指定します。Secure Agent は、SSL 証明書のホスト名との接続に含まれるホスト名を検証します。

プロパティ	説明
キーストア	暗号化方法として SSL を選択し、Oracle データベースサーバーでクライアント認証が有効になっている場合は、キーストアファイルのパスと名前を指定します。キーストアファイルには、クライアントが、Oracle サーバーの証明書要求に応答して送信する証明書が含まれます。
キーストアのパスワード	暗号化方法として SSL を選択し、Oracle データベースサーバーでクライアント認証が有効になっている場合は、キーストアファイルのパスワードを指定します。
キーパスワード	暗号化方法として SSL を選択し、Oracle データベースサーバーでクライアント認証が有効になっている場合は、キーストアファイルのキーのパスワードを指定します。キーのパスワードがキーストアファイルと異なる場合は、このプロパティを使用します。
データベース接続文字列	OCI が Oracle への接続に使用する TNS 名、Oracle Net のキーワードと値のペア、または SQL 接続文字列 URL。
TDE ウォレットディレクトリ	Oracle 透過的データ暗号化 (TDE) に使用される Oracle ウォレットファイルを含むディレクトリへのパス。このプロパティ値は、TDE 暗号化テーブルスペースから変更データをキャプチャし、次のいずれかの条件が当てはまる場合にのみ指定してください。 <ul style="list-style-type: none"> - 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	<p>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。</p> <ul style="list-style-type: none"> - 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。 <p>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。</p> <p>次の形式で 1 つまたは複数の置換を定義できます。</p> <pre>server_path_prefix,local_path_prefix;server_path_prefix,local_path_prefix;...</pre> <p>注: このプロパティは、Oracle ターゲットには適用されません。</p>
リーダーアクティブログマスク	<p>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。</p> <p>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。</p> <p>注: このプロパティは、Oracle ターゲットには適用されません。</p>
リーダーアーカイブ保存先 1	<p>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_<i>n</i> 初期化パラメータの <i>n</i> 値に対応する数値を入力します。ここで <i>n</i> は、1~10 の値です。</p> <p>[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。</p> <p>注: このプロパティは、Oracle ターゲットには適用されません。</p>

プロパティ	説明
リーダーアーカイブ保存先 2	<p>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_<i>n</i> 初期化パラメータの <i>n</i> 値に対応する数値を入力します。ここで <i>n</i> は、1～10 の値です。この値は通常、1 より大きい数値です。</p> <p>注: このプロパティは、Oracle ターゲットには適用されません。</p>
リーダー ASM 接続文字列	<p>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する、TNS で定義された Oracle 接続文字列です。</p> <p>注: このプロパティは、Oracle ターゲットには適用されません。</p>
リーダー ASM ユーザー名	<p>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する、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。</p> <p>注: このプロパティは、Oracle ターゲットには適用されません。</p>
リーダー ASM パスワード	<p>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。</p> <p>注: このプロパティは、Oracle ターゲットには適用されません。</p>
SYSASM としてリーダー ASM 接続	<p>Oracle 11gASM 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。</p> <p>注: このプロパティは、Oracle ターゲットには適用されません。</p>

プロパティ	説明
リーダーモード	<p>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。</p> <ul style="list-style-type: none"> - ACTIVE。アクティブおよびアーカイブ REDO ログを Oracle オンラインシステムから読み取ります。オプションで、【リーダーアクティブログマスク】 プロパティを使用してアクティブ REDO ログをフィルタしたり、【リーダーアーカイブ保存先 1】 および 【リーダーアーカイブ保存先 2】 プロパティを使用してアーカイブログの読み取り元となるアーカイブログ保存先を制限したりすることができます。 - ARCHIVEONLY。アーカイブ REDO ログのみを読み取ります。オプションで、【リーダーアーカイブ保存先 1】 および 【リーダーアーカイブ保存先 2】 プロパティを使用して、アーカイブログの読み取り元となるアーカイブログ保存先を制限できます。 - ARCHIVECOPY。代替ファイルシステムにコピーされたアーカイブ REDO ログを読み取ります。初期ロードジョブと増分ロードジョブの組み合わせの場合は、Informatica グローバルカスタマサポートの指示に従って、ソースカスタムプロパティ <code>pwxcddreader.oracle.reader.additional</code> を、<code>dir</code> パラメータと <code>file</code> パラメータを指定して設定する必要があります。 <p>このオプションは次の状況で使用できます。</p> <ul style="list-style-type: none"> - 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。 <p>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。</p> <p>デフォルトは ACTIVE です。</p> <p>注: このプロパティは、Oracle ターゲットには適用されません。</p>
リーダースタンバイログマスク	<p>Oracle 物理スタンバイデータベースで REDO ログの多重化を使用しているときに、ログリーダーがデータベースの REDO ログを選択するために使用するマスク。ログリーダーは、REDO ロググループ内のメンバ名とマスクを比較して、読み取るログを決定します。マスクでは、アスタリスク (*) ワイルドカードを使用して、0 個以上の文字を表すことができます。</p> <p>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。</p> <p>注: このプロパティは、Oracle ターゲットには適用されません。</p>

プロパティ	説明
スタンバイ接続文字列	データベースが読み取り専用アクセスで開かれていない場合の変更のキャプチャ用に、ログリーダーが Oracle 物理スタンバイデータベースへ接続するために使用する、TNS で定義された Oracle 接続文字列。 注: このプロパティは、Oracle ターゲットには適用されません。
スタンバイユーザー名	変更のキャプチャ用に、ログリーダーが Oracle 物理スタンバイデータベースへ接続するために使用するユーザー ID。このユーザー ID には SYSDBA 権限が必要です。 注: このプロパティは、Oracle ターゲットには適用されません。
スタンバイパスワード	変更のキャプチャ用に、ログリーダーが Oracle 物理スタンバイデータベースへ接続するために使用するパスワード。 注: このプロパティは、Oracle ターゲットには適用されません。
RAC メンバ	Oracle Real Application Cluster (RAC) 内で、追跡可能なアクティブ REDO ログスレッド (メンバ) の最大数。RAC 環境でプライマリデータベースをサポートする Data Guard 物理スタンバイデータベースの場合、この値はプライマリデータベースのアクティブなスレッドの数です。 有効な値は 1~100 です。デフォルトは 0 で、適切なログスレッド数が自動的に決定されます。この値がお使いの環境で適切でない場合は、このプロパティを 0 より大きい値に設定してください。 注: このプロパティは、Oracle ターゲットには適用されません。
BFILE アクセス	次の状況では、このチェックボックスをオンにします。 <ul style="list-style-type: none"> - BFILE アクセスを使用して、ローカル Oracle サーバーファイルシステム上の物理ディレクトリの REDO ログにアクセスする。BFILE アクセスは、Oracle ディレクトリオブジェクトを使用して、ファイルシステムの REDO ログにリモートアクセスします。この方法は、ASM や NFS マウントなどの他のログアクセス方法に代わるものです。 - Amazon Relational Database Service (RDS) for Oracle ソースがある。この場合、このオプションを使用すると、RDS にデプロイされたクラウドベースのデータベースインスタンスの REDO ログにアクセスできます。 デフォルトでは、このチェックボックスはオフです。 注: このプロパティは、Oracle ターゲットには適用されません。

Kerberos 認証の前提条件

Kerberos 認証を使用して Oracle ソースデータベースまたはターゲットデータベースに接続するには、必要な構成ファイルを Secure Agent マシンに配置し、環境変数を設定する必要があります。

Oracle に接続するために Kerberos 認証を設定する場合は、次のガイドラインを考慮してください。

- 使用する Secure Agent とデータベースサーバーが KDC サーバーに登録されている必要があります。
- krb5.conf ファイルに複数の KDC を追加することはできません。複数の KDC はサポートされていません
- 複数の Kerberos プリンシパルユーザーに対して資格情報キャッシュファイルを生成することはできません。
- Kerberos クロスレルム認証はサポートされていません。
- Kerberos 認証用に定義する環境変数は、Oracle sqlnet.ora ファイルおよび tnsnames.ora ファイルのエントリと一致している必要があります。

Kerberos 認証の設定

Kerberos 認証を使用して Linux または Windows 上の Oracle データベースに接続する前に、組織の管理者はいくつかの構成ファイルを作成し、環境変数を設定する必要があります。

1. JDBC ドライバが Java クライアント認証に使用する Java Authentication and Authorization Service 構成ファイル (JAAS) を設定します。
 - a. Secure Agent マシン上に JAAS 構成ファイルを作成します。
 - b. JAAS 構成ファイルに、特定のドライバに使用する認証テクノロジーを指定するエントリを追加します。

例:

```
JDBC_DRIVER_01 {  
    com.sun.security.auth.module.Krb5LoginModule required  
    useTicketCache=true  
    principal="user@EXAMPLE.COM";  
};
```

Krb5LoginModule は、Kerberos プロトコルを使用してユーザーを認証します。必要に応じて、useTicketCache や principal などの LoginModule オプションを追加することができます。詳細については、

<https://docs.oracle.com/javase/8/docs/technotes/guides/security/jgss/tutorials/LoginConfigFile.html> にある Oracle Java のマニュアルを参照してください。

2. Kerberos 構成ファイル krb5.conf を設定します。この構成ファイルにより、Kerberos の設定とレルムの詳細を定義します。
 - a. Secure Agent マシン上に krb5.conf ファイルを作成します。
 - b. Key Distribution Center (KDC) と管理サーバーの詳細を次の形式で krb5.conf ファイルに追加します。

```
[libdefaults]  
    default_realm = <realm_name>  
  
[realms]  
<realm_name> = {  
    kdc = <location where KDC is installed>  
    admin_server = <location where KDC is installed>  
}
```

ここで、[libdefaults]はデフォルトのレルムを設定し、[realms]はレルムの KDC と管理サーバーを指定します。

例:

```
[libdefaults]
default_realm = EXAMPLE.COM

[realms]
EXAMPLE.COM = {
    kdc = rnd.EXAMPLE.COM
    admin_server = rnd.EXAMPLE.COM
}
```

詳細については、https://docs.oracle.com/cd/E86824_01/html/E54775/krb5.conf-4.html にある Oracle のマニュアルを参照してください。

3. データ取り込みおよびレプリケーションと Secure Agent が実行されているマシンで次の環境変数を設定します。

```
setenv JAASCONFIG <Absolute path of the JAAS config file>\<File name>.conf>
setenv KRB5_CONFIG <Absolute path of the Kerberos configuration file>\krb5.conf>
setenv KRB5CCNAME <Absolute path and file name of the credentials cache file>
```

これらの変数は、Oracle Database Ingestion 接続のテスト、タスクのデプロイ、および Kerberos 認証の使用中のジョブの実行に必要です。

または、Secure Agent 用の Administrator でこれらの環境変数を指定することもできます。

Administrator と Secure Agent マシンで環境変数を設定した場合は、Administrator で指定した変数が優先されます。

Administrator で Secure Agent の環境変数を定義するには、[ランタイム環境] に移動します。次に、Secure Agent を開き、[編集] をクリックします。[システム構成の詳細] > [カスタム構成の詳細] で、データベース取り込みサービスと DBMI_AGEN_ENV タイプの変数を入力します。例:

The screenshot shows the 'System Configuration Details' section with a 'Reset All' button. Below it, 'Service' is set to 'Database Ingestion' and 'Type' is set to 'DBMI_AGEN_ENV'. A table lists the configuration for 'DBMI_AGEN_ENV' with columns 'Type', 'Name', 'Value', and 'Sensitive'. The table shows 'testProperty' with value 'testValue' and 'Sensitive' set to false. Below this is the 'Custom Configuration Details' section, which contains a table with columns 'Service', 'Type', 'Sub-type', 'Name', 'Value', and 'Sensitive'. It lists three configurations for 'Database Ingestion' with 'DBMI_AGEN_ENV' type: 'KRB5_CONFIG' with value 'C:\Users\arapun\Perforce\MyModule\untitled\...', 'JAASCONFIG' with value 'C:\Users\arapun\Perforce\MyModule\untitled\...', and 'KRB5CCNAME' with value 'C:\DBML_WORKSPACE\krb5cc_5-1-5-21-38895'.

Type	Name	Value	Sensitive
DBMI_AGEN_ENV	testProperty	'testValue'	<input type="checkbox"/>

Service	Type	Sub-type	Name	Value	Sensitive
Database Ingestion	DBMI_AGEN_ENV		KRB5_CONFIG	C:\Users\arapun\Perforce\MyModule\untitled\...	<input type="checkbox"/>
Database Ingestion	DBMI_AGEN_ENV		JAASCONFIG	C:\Users\arapun\Perforce\MyModule\untitled\...	<input type="checkbox"/>
Database Ingestion	DBMI_AGEN_ENV		KRB5CCNAME	C:\DBML_WORKSPACE\krb5cc_5-1-5-21-38895	<input type="checkbox"/>

4. Secure Agent を再起動します。
5. kinit または okinit ツールを使用して、資格情報キャッシュファイルを生成します。
 - Windows で kinit ツールを使用するには、最初に MIT Kerberos クライアントをインストールし、krb5.conf の [libdefaults] セクションの KRB5CCNAME システム環境変数または default_ccache_name 変数が設定されていることを確認します。次に、次のコマンドを発行して kinit ツールを実行します。パスワードの入力を求められるので、パスワードを入力します。
kinit user@<realm_name>
 - Linux で kinit ツールを使用するには、最初に kinit ツールをインストールし、KRB5CCNAME システム環境変数が設定されていることを確認します。次に、次のコマンドを発行して kinit ツールを実行します。パスワードの入力を求められるので、パスワードを入力します。
kinit user@<realm_name>
 - okinit ツールを使用するには、最初に Oracle Instant Client をインストールします。資格情報キャッシュファイルは、sqlnet.ora ファイルの SQLNET.KERBEROS5_CC_NAME プロパティに基づいて作成されます。次に、次のコマンドを発行して okinit ツールを実行します。パスワードの入力を求められるので、パスワードを入力します。
okinit user@<realm_name>

第 174 章

Oracle Financials Cloud V1 接続のプロパティ

Oracle Financials Cloud との間でデータの安全な読み取りまたは書き込みを行うための Oracle Financials Cloud V1 接続を作成します。

前提条件

Oracle Financials Cloud アプリケーションとの間で読み取りまたは書き込みを行うための Oracle Financials Cloud V1 接続を作成する前に、前提条件を必ず満たすようにしてください。

XLSM テンプレートファイルへのアクセス

Oracle Financials Cloud アプリケーションに書き込むには、制御ファイルを必要とするオブジェクトの XLSM テンプレートファイルおよび CTL ファイルにアクセスします。

1. Oracle ドキュメントの「**Financials のファイルベースのデータのインポート**」ページから特定の Oracle Financials Cloud インスタンスのバージョンを選択します。

例えば、Oracle Financials Cloud インスタンス 20A の XLSM テンプレートにアクセスするには、次の URL に移動します:

<https://docs.oracle.com/en/cloud/saas/financials/20a/oefbf/overview.html#overview>

2. **【ファイルベースのデータのインポート】** セクションにリストされている、使用する必要な操作を選択します。
選択した操作ページが表示されます。
3. **【XLSM テンプレートファイルリンク】** をクリックして、**【ファイルリンク】** セクションから操作の XLSM テンプレートファイルをダウンロードします。
次の図に、**【ファイルリンク】** セクションからダウンロードしたサンプル XLSM テンプレートファイルリンクを示します。

File Links

File	Link
XLSM template	AutoInvoiceImportTemplate.xlsm

4. Secure Agent マシンまたは **【IO ディレクトリ】** 接続プロパティで指定したディレクトリパスにアクセスできることを確認します。

5. XLSM テンプレートファイルを、**[IO ディレクトリ]** 接続プロパティで指定した次のディレクトリパスに配置します: IO Directory/Writer/Schema
次のような書き込みオブジェクトの場合は、XLSM テンプレートファイルと CTL ファイルをディレクトリに配置します。

- 請求データのインポート
- 収益ベースのデータのインポート
- 自動インボイスのインポート

注: 選択した操作を使用してマッピングを作成するには、Oracle が提供する XLSM テンプレートファイルまたは CTL ファイルの名前を保持します。ファイル名を保持した場合にのみ、ファイル名が **[オブジェクトの選択]** ウィンドウに表示されます。

ERP エンドポイント URL の取得

Oracle Financials Cloud アプリケーションとの間でデータの読み取りまたは書き込みを行うための ERP 統合サービスエンドポイント URL を取得します。

1. Oracle Financials Cloud アプリケーションで、**[ナビゲータ]** をクリックします。
2. **[ツール]** セクションで **[開発者接続]** をクリックします。
3. **[WebServices]** セクションの **[検索]** フィールドに **[ERP 統合サービス]** と入力します。
[Web サービス: 統合サービス: 概要] ページが表示され、ERP エンドポイント URL が表示されます。次の例に、ERP 統合サービスエンドポイント URL のサンプルを示します:

`https://adc-fap0011-fin.oraclecloud.com:443/publicFinancialCommonErpIntegration/ErpIntegrationService`

4. 次のパスを削除して URL を編集します: 443/publicFinancialCommonErpIntegration/ErpIntegrationService
次の URL は、ERP エンドポイント URL のサンプルです。

`https://adc-fap0011-fin.oraclecloud.com`

Oracle Financials Cloud への接続

Oracle Financials Cloud に接続するように Oracle Financials Cloud V1 接続プロパティを設定してみましょう。

始める前に

接続を設定する前に、XLSM テンプレートファイルにアクセスし、Oracle Financials Cloud アプリケーションの ERP エンドポイント URL を取得します。

これらのタスクの詳細については、「[Prerequisites](#)」を参照してください。

接続の詳細

次の表に、基本接続プロパティを示します。

財産	説明
接続名	<p>接続の名前。</p> <p>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。_ . + - ,</p> <p>最大長は 255 文字です。</p>
説明	<p>接続の説明。最大長は 4000 文字です。</p>
シークレットコンテナの使用	<p>組織に対して設定されている Secrets Manager にこの接続の機密資格情報を保存します。</p> <p>このプロパティは、組織に Secrets Manager が設定されている場合にのみ表示されます。</p> <p>このプロパティは、データ取り込みおよびレプリケーションとデータアクセス管理サービスではサポートされていません。</p> <p>接続でシークレットコンテナを有効にすると、Secure Agent が Secrets Manager からどの資格情報を取得するかを選択できます。このオプションを無効にした場合、資格情報は組織の設定方法に応じてリポジトリまたはローカル Secure Agent に保存されます。</p> <p>注: この接続を使用してプッシュダウンまたはプロキシサービスを介してデータアクセスポリシーを適用する場合、シークレットコンテナ設定オプションを使用することはできません。</p> <p>Secrets Manager を設定および使用する方法については、Administrator のヘルプにある「Secrets Manager の設定」を参照してください。</p>
ランタイム環境	<p>タスクを実行するランタイム環境の名前。</p> <p>Secure Agent、ホステッドエージェント、サーバーレスランタイム環境、またはエラスティックランタイム環境を指定します。</p> <p>ランタイム環境の設定および使用方法の詳細については、Administrator のヘルプにある「ランタイム環境」を参照してください。</p>
ERP エンドポイント URL	<p>Oracle Financials アプリケーションサーバーのエンドポイント URL。</p> <p>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。</p> <p><ERP エンドポイント URL>/publicFinancialCommonErpIntegration/ErpIntegrationService?WSDL</p> <p>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 ファイルが開きます。</p>
認証タイプ	<p>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。</p> <p>[基本認証] タイプを選択します。</p>
ユーザー名	<p>Oracle Financials Cloud アカountのユーザー名。</p>

財産	説明
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	<p>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。スキーマファイルを Secure Agent マシンに保存します。</p> <p>Oracle Financials Cloud V1 接続の作成後に、【テスト】 ボタンをクリックします。</p> <p>Secure Agent で、IO ディレクトリの下に次のディレクトリが作成されます。</p> <ul style="list-style-type: none"> - 【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、IO Directory\Reader\Output ディレクトリに保存されます。 <p>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することができます。</p> <ul style="list-style-type: none"> - 【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。すべての XLSM ファイルと CTL ファイルをダウンロードした後に、次のディレクトリに配置します: IO Directory\Writer\Schema - 【Temp】 : Temp ディレクトリには、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あります。

暗号化モード

Oracle Financials Cloud にアクセスするには、PGPUNSIGNED および PGPSIGNED 暗号化モードを設定します。デフォルトは [なし] です。

Oracle Financials Cloud アプリケーションに対してデータの読み取りまたは書き込みを行うマッピングを実行する際に、データを暗号化または復号化するために必要な暗号化モードを選択します。

PGPSIGNED

PGP 暗号化方法を使用してデータを暗号化し、署名を行います。

次の表に、PGP 暗号化方法の基本接続プロパティを示します。

プロパティ	説明
パスフレーズ	プライベートキーを暗号化するためのパスフレーズ。
PrivateKey パス	<p>プライベートキーのファイルパス。</p> <p>プライベートキーを Secure Agent マシンに保存します。</p> <p>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します。</p>
ERP 公開鍵パス	<p>Fusion パブリックキーのファイルパス。</p> <p>Fusion パブリックキーを Secure Agent マシンに保存します。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。</p> <p>Fusion パブリックキーを取得するには、Oracle Financials Cloud にサービス要求を送信します。</p> <p>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。</p>

プロパティ	説明
ERP 秘密鍵エイリアス名	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 Cloud 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ソースからのデータの読み取りまたはターゲットへのデータの書き込みを行う際に、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 Cloud 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。 マッピングを実行してソースからデータを読み取る際に、顧客パブリックキーエイリアス名を使用できます。

PGPUNSIGNED

PGP 暗号化方法を使用してデータを暗号化します。Oracle Financials Cloud アプリケーションで設定した暗号化キーと同じ暗号化キーを使用します。

次の表に、Oracle Financials Cloud アプリケーションに書き込みを行う PGP 暗号化方法の基本接続プロパティを示します。

プロパティ	説明
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 パブリックキーを Secure Agent マシンに保存します。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 でサービス要求を送信します。 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生成するときに Oracle Financials Cloud 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ソースからのデータの読み取りまたはターゲットへのデータの書き込みを行う際に、融合キーエイリアス名を使用できます。

プロキシサーバーの設定

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

Windows および Linux 上でプロキシサーバーを使用するように、Secure Agent とサーバーレスランタイム環境を設定できます。認証されていないプロキシサーバーのみを使用できます。プロキシ設定は、マッピングおよび詳細モードのマッピングで使用される接続に適用されます。

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

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

手順については、データ統合のヘルプの『または「Windows でのプロキシ設定」または「Linux でのプロキシ設定」を参照してください。

- Secure Agent のプロパティで、DTM の JVM オプションを設定します。手順については、ナレッジベースの記事「[Proxy server settings](#)」を参照してください。

サーバーレスランタイム環境のプロキシの設定を行う方法については、Administrator ヘルプの「[「プロキシサーバーの使用](#)」を参照してください。

第 175 章

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

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

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

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

接続プロパティ	説明
接続名	接続の名前。この名前は、組織内で一意にする必要があります。接続名には、英数字、スペース、および次のような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。
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。 アプリケーション取り込みとレプリケーションタスクでは、Secure Agent またはサーバーレスランタイム環境を選択できます。ホステッドエージェントは使用できません。
認証	接続の認証方法。 デフォルトでは、接続は基本認証方式を使用します。
ユーザー名	Oracle Cloud アカウントのユーザー名。
パスワード	Oracle Cloud アカウントのパスワード。
サーバーの URL	アクセス先の Oracle Cloud サービスの URL。
API バージョン	接続に使用する Oracle Cloud REST API のバージョン。 BICC レプリケーションアプローチの場合はオプションです。

第 176 章

Oracle HCM Cloud V1 接続のプロパティ

Oracle HCM Cloud との間でデータの安全な読み取りまたは書き込みを行うための Oracle HCM Cloud V1 接続を作成します。

前提条件

Oracle HCM Cloud アプリケーションに対して読み取りまたは書き込みを行うための Oracle HCM Cloud V1 接続を作成する前に、特定の前提条件を満たしていることを確認してください。

WebCenter コンテンツ URL の取得

Oracle HCM Cloud が出力 XML データをアップロードする WebCenter Content URL を取得します。

1. Oracle から送付されるクラウド環境プロビジョニング電子メールの **【サービスの詳細】** セクションから、Oracle HCM Cloud のセットアップとメンテナンス用の URL を取得します。
次の例にサンプルの URL を示します。

`https://fs-<domain_name>.oracleoutsourcing.com/setup/faces/TaskListManagerTop`

2. URL から `/setup/faces/TaskListManagerTop` を削除します。
残りの部分が、WebCenter Content URL となります。

例:

`https://fs-<domain_name>.oracleoutsourcing.com`

WebCenter Content URL をコピーし、Oracle HCM Cloud V1 接続を設定するときに使用できるように保管しておいてください。

ロールの確認

[ユーザーアカウントの詳細] ページで、次のロールが割り当てられていることを確認します。

ロール	ロールコード
アプリケーション管理者	ORA_FND_APPLICATION_ADMINISTRATOR_JOB
アプリケーション開発者	ORA_FND_APPLICATION_DEVELOPER_JOB
アプリケーション診断管理者	ORA_FND_DIAG_ADMINISTRATOR_JOB
アプリケーション実装管理者	ORA_ASM_APPLICATION_IMPLEMENTATION_ADMIN_ABSTRACT
アプリケーション実装コンサルタント	ORA_ASM_APPLICATION_IMPLEMENTATION_CONSULTANT_JOB
アプリケーション実装マネージャ	ORA_ASM_APPLICATION_IMPLEMENTATION_MANAGER_JOB
人材管理アプリケーション管理者	ORA_HRC_HUMAN_CAPITAL_MANAGEMENT_APPLICATION_ADMINISTRATOR_JOB
人材管理統合スペシャリスト	ORA_HRC_HUMAN_CAPITAL_MANAGEMENT_INTEGRATION_SPECIALIST_JOB
IT セキュリティマネージャ	ORA_FND_IT_SECURITY_MANAGER_JOB
統合スペシャリスト	ORA_FND_INTEGRATION_SPECIALIST_JOB

Oracle HCM への接続

Oracle HCM Cloud に接続するように Oracle HCM Cloud V1 接続プロパティを設定してみましょう。

始める前に

接続を設定する前に、Oracle から WebCenter Content URL を取得し、必要なロールが割り当てられていることを確認してください。

これらのタスクの詳細については、「[Prerequisites](#)」を参照してください。

接続の詳細

次の表に、基本接続プロパティを示します。

財産	説明
接続名	<p>接続の名前。</p> <p>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。</p>
説明	<p>接続の説明。最大長は 4000 文字です。</p>
シークレットコンテナの使用	<p>組織に対して設定されている Secrets Manager にこの接続の機密資格情報を保存します。</p> <p>このプロパティは、組織に Secrets Manager が設定されている場合にのみ表示されます。</p> <p>このプロパティは、データ取り込みおよびレプリケーションとデータアクセス管理サービスではサポートされていません。</p> <p>接続でシークレットコンテナを有効にすると、Secure Agent が Secrets Manager からどの資格情報を取得するかを選択できます。このオプションを無効にした場合、資格情報は組織の設定方法に応じてリポジトリまたはローカル Secure Agent に保存されます。</p> <p>注: この接続を使用してプッシュダウンまたはプロキシサービスを介してデータアクセスポリシーを適用する場合、シークレットコンテナ設定オプションを使用することはできません。</p> <p>Secrets Manager を設定および使用する方法については、Administrator のヘルプにある「Secrets Manager の設定」を参照してください。</p>
ランタイム環境	<p>タスクを実行するランタイム環境の名前。</p> <p>Secure Agent、ホステッドエージェント、サーバーレスランタイム環境、またはエラスティックランタイム環境を選択します。</p> <p>ランタイム環境の設定および使用方法の詳細については、Administrator のヘルプにある「ランタイム環境」を参照してください。</p>
WebCenter コンテンツ URL	<p>Oracle HCM Cloud が出力 XML データをアップロードする WebCenter Content Server の URL。</p> <p>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 ファイルが開いた場合、WebCenter Content の URL は有効です。</p>
HCM URL	<p>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が格納される HCM Application Server の URL。</p> <p>次の URL は、HCM の URL の例です: https://adc-xxx-hcm.oracledemo.com/。</p> <p>HCM の URL を検証するには、Web ブラウザに次の URL を入力します。 <HCM の URL>/hcmProcFlowCoreController/FlowActionsService?WSDL この URL で WSDL ファイルが開いた場合、HCM の URL は有効です。</p> <p>注: このプロパティは、Oracle HCM Cloud アプリケーションにデータの書き込みを行うために Oracle HCM Cloud V1 接続を作成したとき、または読み取り操作の詳細接続プロパティで 【抽出の送信】 を選択したときに適用されます。</p>
認証タイプ	<p>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。</p> <p>【基本認証】 タイプを選択します。</p>
ユーザー名	<p>Oracle HCM Cloud アカウントのユーザー名。</p>

財産	説明
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	<p>Secure Agent 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。</p> <p>Oracle HCM Cloud V1 接続の作成後に、【テスト】 ボタンをクリックします。</p> <p>Secure Agent で、スキーマディレクトリの下に次のディレクトリが作成されます。</p> <p>Reader</p> <p>このディレクトリには XSD ファイルが格納されます。XSD ファイルを生成した後に、すべての XSD ファイルを Reader ディレクトリに配置します。</p> <p>Writer</p> <p>このディレクトリには XLSX ファイルが格納されます。XLSX ファイルをダウンロードした後に、すべての XLSX ファイルを Writer ディレクトリの下に配置します。</p> <p>Temp</p> <p>このディレクトリには、ロード前のステージングファイルが格納されます。</p>

詳細設定

次の表に、詳細接続のプロパティを示します。

プロパティ	説明
抽出の送信	<p>要求メッセージで指定したパラメータ値を使用した、HCM 抽出定義の送信。</p> <p>【抽出の送信】 オプションを有効にすると、Secure Agent は、指定された HCM 抽出定義のインスタンスを Oracle HCM Cloud アプリケーションに送信し、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。</p> <p>HCM 抽出定義は、Oracle HCM Cloud アプリケーションから直接送信することもできます。</p> <p>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されます。</p> <p>デフォルトでは無効になっています。</p>

暗号化モード

Oracle HCM Cloud にアクセスするように PGPUNSIGNED および PGPSIGNED 暗号化モードを設定できます。

ターゲットにデータの書き込みを行うマッピングを実行したときにデータを暗号化または復号化するために必要な暗号化モードを選択します。デフォルトは [なし] です。

PGPSIGNED

PGP 暗号化方法を使用してデータを暗号化し、署名を行います。

次の表に、PGP 暗号化方法の基本接続プロパティを示します。

プロパティ	説明
プライベートキーパスフレーズ	プライベートキーを暗号化するためのパスフレーズ。 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。
秘密鍵パス	プライベートキーのファイルパス。 プライベートキーを Secure Agent マシンに保存します。 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します。
融合公開鍵パス	Fusion パブリックキーのファイルパス。 Fusion パブリックキーを Secure Agent マシンに保存します。 注: Fusion パブリックキーを取得するには、Oracle HCM Cloud にサービス要求を送信します。 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。

PGPUNSIGNED

PGP 暗号化方法を使用してデータを暗号化します。Oracle HCM Cloud アプリケーションで設定した暗号化キーと同じ暗号化キーを使用します。

次の表に、Oracle HCM Cloud から読み取りを行う PGP 暗号化方法の基本接続プロパティを示します。

プロパティ	説明
プライベートキーパスフレーズ	プライベートキーを暗号化するためのパスフレーズ。 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。
融合公開鍵パス	Fusion パブリックキーのファイルパス。 Fusion パブリックキーを Secure Agent マシンに保存します。 注: Fusion パブリックキーを取得するには、Oracle HCM Cloud にサービス要求を送信します。 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。

次の表に、Oracle HCM Cloud に書き込みを行う PGP 暗号化方法の基本接続プロパティを示します。

プロパティ	説明
プライベートキーパスフレーズ	プライベートキーを暗号化するためのパスフレーズ。 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。
プライベートキーパス	プライベートキーのファイルパス。 プライベートキーを Secure Agent マシンに保存します。 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します。

抽出定義

Oracle HCM Cloud ソースからデータの読み取りを行うには、Oracle HCM Cloud アプリケーションから抽出するデータの HCM 抽出定義を作成します。

1. HCM 抽出定義を作成するには、Oracle HCM Cloud アプリケーションで次のプロパティを設定します。
 - a. **【抽出定義の管理】** タブの **【抽出の配信オプション】** ページで、**【出力タイプ】** フィールドの値を **【データ】** に設定し、**【配信タイプ】** フィールドの値を **【WebCenter Content】** に設定します。
 - b. **【統合名】** フィールドと **【暗号化モード】** フィールドの値を指定します。
次の図に、**【出力タイプ】**、**【配信タイプ】**、**【統合名】**、および **【暗号化モード】** フィールドの値を設定する **【抽出の配信オプション】** ページを示します。

Extract Delivery Options

View ▼ Format ▼ + Add ✕ Delete ✎ Edit

Start Date	End Date	* Delivery Option Name	* Output Type	Report	Template Name	* Output Name	* Delivery Type
1/1/01	12/31/12		Data				WebCenter C

Columns Hidden 3

Additional Details:

View ▼ Format ▼

Property	Value	Attribute
Compress		
Time Zone		
Locale		
Key		
Integration Name		
Run Time File Name		
Encryption Mode		

2. HCM 抽出定義を Oracle HCM Cloud アプリケーションから Oracle WebCenter Content サーバーに送信します。**【抽出の送信】** 接続プロパティを使用して、HCM 抽出定義を Oracle WebCenter Content サーバーに送信することもできます。
3. すべての HCM 抽出定義の XML スキーマを XSD ファイル形式で生成し、XSD ファイルとスキーマディレクトリを Secure Agent マシン上の次のディレクトリに保存します。
Schema Directory\Reader

このディレクトリは、**【スキーマディレクトリ】** 接続プロパティで指定された場所に基づいてエージェントによって作成されます。

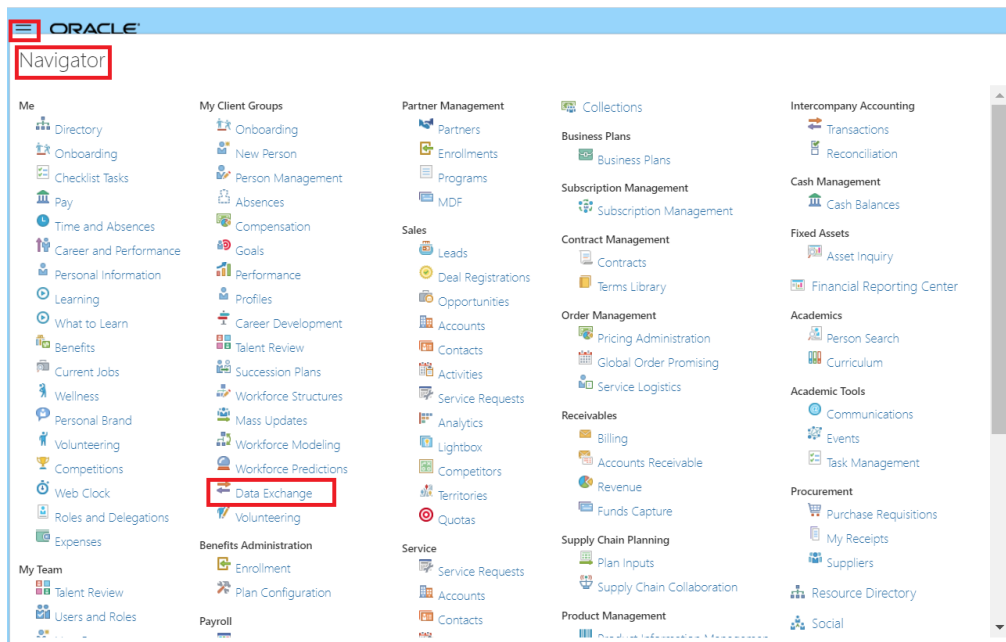
Oracle HCM Cloud V1 コネクタは、単一ルート要素 DATA_DS を持つ XSD ファイルをサポートします。

注: Oracle HCM Cloud の出力 XML データから XML スキーマを生成するには、サードパーティツールを使用します。XSD ファイルに出力 XML データとの互換性があることを確認し、<TemplateName>.xsd という形式で名前を付けます。

Excel テンプレートのダウンロード

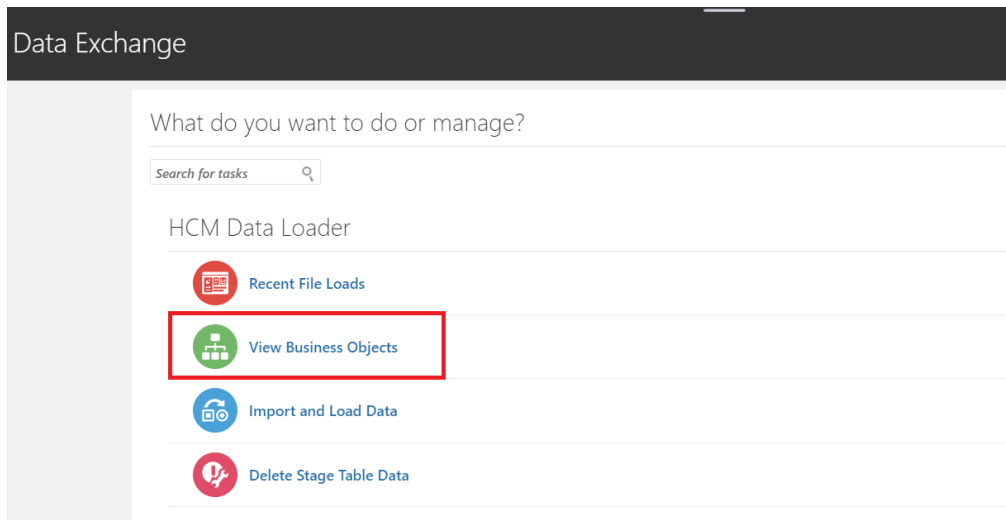
データの書き込みを行うオブジェクトに関連する Excel テンプレートをダウンロードします。

1. Oracle HCM Cloud アプリケーションにログインします。
2. **【ナビゲータ】** > **【データ交換】** をクリックします。

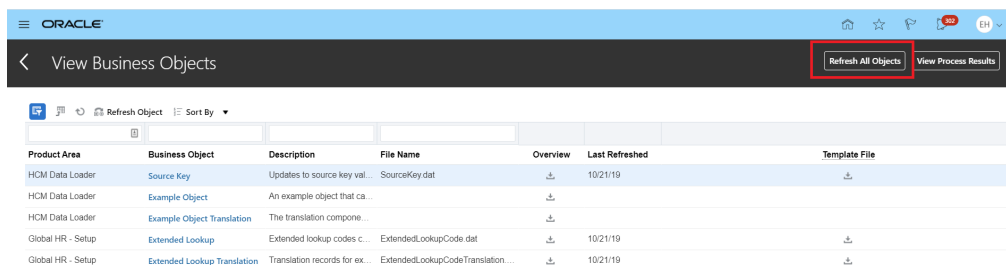


【データ交換】 ページが表示されます。

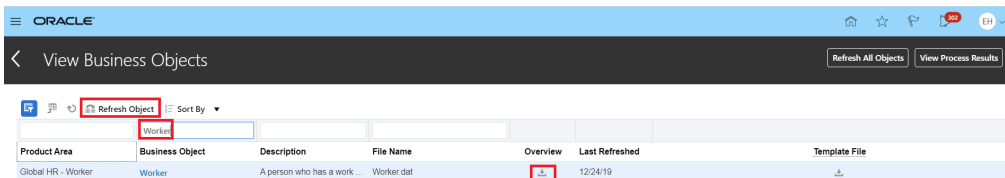
3. HCM データローダーセクションで **【ビジネスオブジェクトの表示】** をクリックします。



4. **【すべてのオブジェクトを更新】** をクリックします。



5. 特定のビジネスオブジェクトをフィルタリングし、その特定のオブジェクトを更新できます。[ビジネスオブジェクトの表示] ページの [概要] カラムの下にある [ダウンロード] アイコンをクリックします。



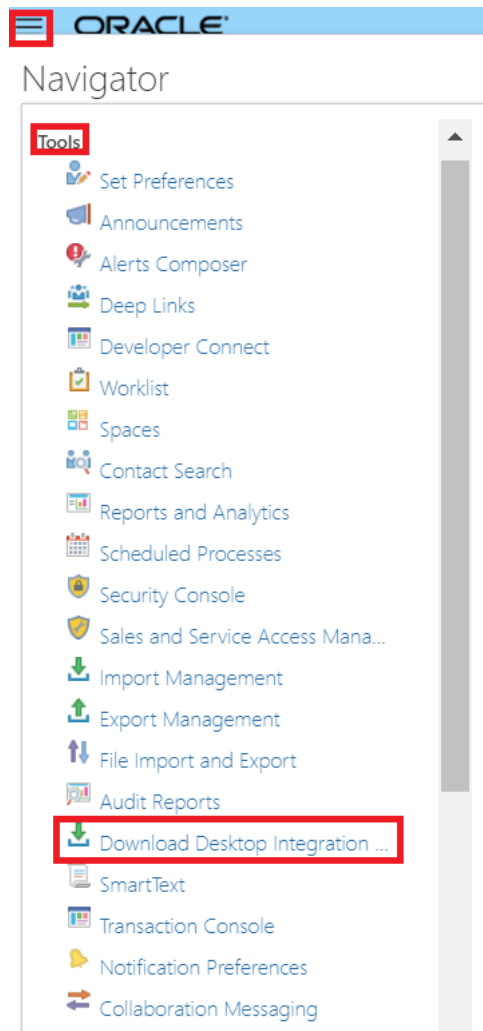
[GenericBusObjDetails.xlsx] テンプレートがダウンロードされます。

注: すべての Excel テンプレートは、[GenericBusObjDetails.xlsx] という同じ名前でダウンロードされます。必要に応じて、Excel テンプレートの名前を変更します。

ADF デスクトップ統合ツールのダウンロードとインストール

Excel テンプレートをダウンロードした後に、Excel テンプレートを介してエンドポイントに接続するためのツールをインストールします。このツールにより、エンドポイントからデータをダウンロードし、Excel テンプレートを自動入力します。

1. Oracle HCM Cloud アプリケーションにログインします。
2. [ナビゲータ] > [ツール] > [デスクトップ統合インストーラのダウンロード] をクリックします。



アプリケーションがデスクトップにダウンロードされます。

3. インストーラ `adfdi-excel-addin-installer.exe` を実行します。

注: ADF デスクトップ統合と連携するための Excel の設定については、次の Oracle のドキュメントを参照してください。

<https://docs.oracle.com/middleware/11119/adf/develop-desktop-integration/adf-desktop-config-env.htm>

Excel テンプレートの設定

書き込み操作を有効にするには、Excel テンプレートを設定します。

1. ダウンロードした Excel テンプレートを開きます。
2. 特定のオブジェクトに対するメタデータを生成するには、[接続] ダイアログボックスで [はい] をクリックします。

Oracle HCM Cloud V1 アプリケーションにログインしていない場合は、ログインするように求めるメッセージが表示されます。

3. テンプレートに完全なメタデータを確実に入力するには、**【階層の詳細】** シート、**【属性】** シート、および **【フレックスフィールド属性】** シートに移動し、Excel テンプレートを保存します。

注: Excel テンプレートにデータが入力されていない場合は、手順を正確に実行しているかどうかを確認するか、**Oracle サポート**に問い合わせてください。

4. すべての Excel テンプレートを **【スキーマ】** ディレクトリの下 **【ライタ】** サブディレクトリに配置します。

注: Oracle Cloud の最新リリースバージョンに対応する Excel テンプレートの使用を検討してください。

プロキシサーバーの設定

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

Windows および Linux でプロキシサーバーを使用するように Secure Agent とサーバーレスランタイム環境を設定できます。認証されていないプロキシサーバーのみを使用できます。プロキシ設定は、マッピングおよび詳細モードのマッピングで使用される接続に適用されます。

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

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

手順については、データ統合のヘルプの『または「Windows でのプロキシ設定」または「Linux でのプロキシ設定」を参照してください。

- Secure Agent のプロパティで、DTM の JVM オプションを設定します。手順については、ナレッジベースの記事「[Proxy server settings](#)」を参照してください。

サーバーレスランタイム環境のプロキシの設定を行う方法については、Administrator ヘルプの「「プロキシサーバーの使用」を参照してください。

第 177 章

SAP の接続プロパティ

Pinecone ベクトルデータベースに安全なデータの書き込みを行うための Pinecone 接続を作成します。

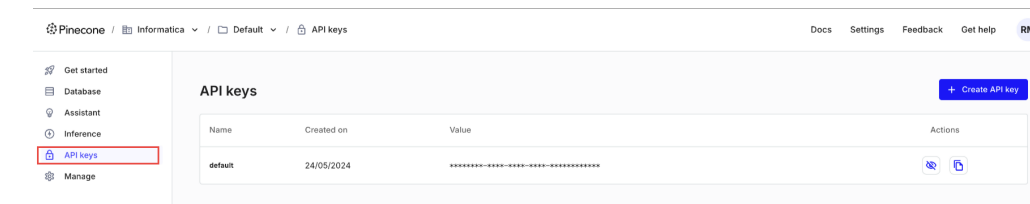
認証の準備

接続プロパティを設定する前に、Pinecone API へのアクセスを認証するために、Pinecone アカウントの API キーを取得する必要があります。

Pinecone API キーの取得

Pinecone プロジェクトへの API 呼び出しを行うには、API キーが必要です。
Pinecone API キーを取得するには、次の手順を実行します。

1. Pinecone コンソールを開きます。
2. プロジェクトを選択します。
3. **[API キー]** に移動します。



4. API キーをコピーします。

Pinecone への接続

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

始める前に

開始する前に、Pinecone アカウントから API キーを取得する必要があります。

接続を設定する前に、[「認証の準備」 \(ページ 642\)](#)を参照して認証要件を確認してください。

接続の詳細

次の表に、基本接続プロパティを示します。

プロパティ	説明
接続名	接続の名前。 各接続名は組織内で一意である必要があります。接続名には、英数字、スペース、および次の特殊文字を含めることができます。_ . + -, 最大長は 255 文字です。
説明	接続の説明。最大長は 4000 文字です。
シークレットコンテナの使用	組織に対して設定されている Secrets Manager にこの接続の機密資格情報を保存します。 このプロパティは、組織に Secrets Manager が設定されている場合にのみ表示されます。 このプロパティは、データ取り込みおよびレプリケーションとデータアクセス管理サービスではサポートされていません。 接続でシークレットコンテナを有効にすると、Secure Agent が Secrets Manager からどの資格情報を取得するかを選択できます。このオプションを無効にした場合、資格情報は組織の設定方法に応じてリポジトリまたはローカル Secure Agent に保存されます。 注: この接続を使用してプッシュダウンまたはプロキシサービスを介してデータアクセスポリシーを適用する場合、シークレットコンテナ設定オプションを使用することはできません。 Secrets Manager を設定および使用方法については、Administrator のヘルプにある「Secrets Manager の設定」を参照してください。
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。 Secure 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。
API キー	Pinecone API へのアクセスを認証するための Pinecone アカウントの API キー。

第 178 章

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。
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gger（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。 <i>host_name</i> は、ホスト名または IP アドレスにできます。 <i>host_name:port_number</i> 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せん。

プロパティ	説明
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gger (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。 <ul style="list-style-type: none"> - 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gger (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。 <i>host_name</i> は、ホスト名または IP アドレスにできます。 <i>host_name:port_number</i> 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。

プロパティ	説明
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	<p>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。</p> <p>注: これらのプロパティは、PowerCenter の PowerExchange Client for PowerCenter (PWXPC) CDC 接続の【PWX オーバーライド】オプションと同じです。</p> <p>パラメータファイルを使用して接続プロパティのオーバーライドを指定するには、\$<ParameterName>の形式でパラメータを設定し、ユーザー定義パラメータ名の前にドル記号 (\$) を付けます。次に、【ランタイムオプション】タブの【パラメータファイル名】フィールドにパラメータファイル名を指定することで、ユーザー定義パラメータ定義を含むパラメータファイルを使用するようにマッピングのマッピングタスクを設定します。パラメータファイルで、パラメータの接続オーバーライドを名前と値のペアの形式で設定し、複数の値をセミコロンで区切ります。</p> <p>例:</p> <pre>\$UserPass="User Name=jdoe;Password=mypassword"</pre> <p>このフィールドに指定するパラメータ名は、パラメータファイルで定義されたエントリと一致している必要があります。</p> <p>詳細については、「接続オーバーライドのリファレンス」の章を参照してください。</p>

第 179 章

PostgreSQL 接続のプロパティ

PostgreSQL に対してデータの安全な読み取りまたは書き込みを行うための PostgreSQL 接続を作成します。

認証の準備

PostgreSQL データベースに接続するようにデータベース認証方法または Kerberos 認証方法を設定できます。

注: データ取り込みおよびレプリケーションでは、Kerberos 認証はサポートされていません。

接続プロパティを設定する前に、使用する認証のタイプに基づいて認証の詳細を用意しておく必要があります。

データベース認証を設定するには、PostgreSQL アカウントのユーザー名、パスワード、ホスト名、ポート、データベース名が必要です。

Kerberos 認証を設定するには、PostgreSQL アカウントのサービスプリンシパル名、ホスト名、ポート、およびデータベース名が必要です。また、特定の前提条件タスクを実行する必要もあります。

Kerberos 認証の準備

Kerberos 認証を使用して PostgreSQL データベースに接続するには、必要な Kerberos 構成ファイルを Secure Agent マシンに配置します。

PostgreSQL に接続するために Kerberos 認証を設定する場合は、次のガイドラインを考慮してください。

- ホステッドエージェントまたはサーバーレスランタイム環境は使用できません。
- 使用する Secure Agent とデータベースサーバーが KDC サーバーに登録されていることを確認してください。
- krb5.conf ファイルに複数の KDC を追加することはできません。
- 複数の Kerberos プリンシパルユーザーに対して資格情報キャッシュファイルを生成することはできません。
- Windows で Kerberos 認証を使用する場合は、Secure Agent サービスを開始するユーザーアカウントが PostgreSQL データベースで使用可能になっていることを確認してください。PostgreSQL にアクセスするために資格情報を入力する必要はありません。

Kerberos 認証の設定

Kerberos 認証を使用して Linux または Windows 上の PostgreSQL に接続する前に、組織の管理者は前提条件のタスクを実行する必要があります。

1. Java Authentication and Authorization Service 構成ファイル（JAAS）を設定するには、次のタスクを実行します。
 - a. Secure Agent マシン上に JAAS 構成ファイルを作成します。
 - b. 以下のエントリを JAAS 構成ファイルに追加します。

```
JDBC_DRIVER_01 {
  com.sun.security.auth.module.Krb5LoginModule required useTicketCache=true;
};
```
2. krb5.conf ファイルを設定するには、次のタスクを実行します。
 - a. Secure Agent マシン上に krb5.conf ファイルを作成します。
 - b. Key Distribution Center（KDC）と管理サーバーの詳細を、次の形式で krb5.conf ファイルに追加します。

```
[libdefaults]
default_realm = <Realm name>
forwardable = true
ticket_lifetime = 24h

[realms]
<REALM NAME> = {
  kdc = <Location where KDC is installed>
  admin_server = <Location where KDC is installed>
}

[domain_realm]
<domain name or host name> = <Domain name or host name of Kerberos>
<domain name or host name> = <Domain name or host name of Kerberos>
```
3. Secure Agent マシン上で次の環境変数を設定します。
必要な環境変数については、[「環境変数の設定」](#)（ページ 648）を参照してください。
4. Secure Agent を再起動します。
5. Secure Agent マシン上で資格情報キャッシュファイルを生成し、Kerberos 認証を使用して PostgreSQL に接続するには、次のタスクを実行します。
 - a. Secure Agent マシン上のコマンドラインで次のコマンドを実行し、PostgreSQL ユーザー名とレルム名を指定します。

```
Kinit <user name>@<realm_name>
```
 - b. 要求されたら、Kerberos プリンシパルユーザーのパスワードを入力します。

環境変数の設定

Kerberos 認証を使用して PostgreSQL に接続するには、Secure Agent マシン上で必要な環境変数を設定する必要があります。

環境変数を設定するには、次のコマンドを実行します。

- `setenv KRB5CCNAME <資格情報キャッシュファイルの絶対パスとファイル名>`
- `setenv KRB5_CONFIG <Kerberos 構成ファイルの絶対パス>\krb5.conf`
- `setenv JAASCONFIG <JAAS 構成ファイルの絶対パス>\<ファイル名>.conf`

環境変数を設定した後に、Secure Agent を再起動する必要があります。

または、PostgreSQL 接続の作成時に KRB5_CONFIG および JAASCONFIG 環境変数を追加することもできます。

Kerberos 認証を使用した接続の設定時に環境変数を追加するには、PostgreSQL 接続の **【追加の Kerberos プロパティ】** フィールドに `KRB5_CONFIG` プロパティと `JAASCONFIG` プロパティを追加する必要があります。

例えば、次の形式でプロパティを追加します。

```
KRB5_CONFIG=<Absolute path of the Kerberos configuration file>\krb5.conf;JAASCONFIG=<Absolute path of the JAAS config file>\<File name>.conf
```

注: キーと値のペアはそれぞれセミコロンで区切ってください。

PostgreSQL への接続

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

始める前に

開始する前に、使用する認証方法に基づいて、PostgreSQL アカウントから必要な情報を取得します。

認証の前提条件の詳細については、[「認証の準備」 \(ページ 647\)](#)を参照してください。

接続の詳細

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。

プロパティ	説明
シークレットコンテナの使用	<p>組織に対して設定されている Secrets Manager にこの接続の機密資格情報を保存します。</p> <p>このプロパティは、組織に Secrets Manager が設定されている場合にのみ表示されます。</p> <p>このプロパティは、データ取り込みおよびレプリケーションとデータアクセス管理サービスではサポートされていません。</p> <p>接続でシークレットコンテナを有効にすると、Secure Agent が Secrets Manager からどの資格情報を取得するかを選択できます。このオプションを無効にした場合、資格情報は組織の設定方法に応じてリポジトリまたはローカル Secure Agent に保存されます。</p> <p>注: この接続を使用してプッシュダウンまたはプロキシサービスを介してデータアクセスポリシーを適用する場合、シークレットコンテナ設定オプションを使用することはできません。</p> <p>Secrets Manager を設定および使用する方法については、Administrator のヘルプにある「Secrets Manager の設定」を参照してください。</p>
ランタイム環境	<p>タスクを実行するランタイム環境の名前。</p> <p>Secure Agent、ホステッドエージェント、サーバーレスランタイム環境、またはエラスティックランタイム環境を選択します。</p> <p>アプリケーション取り込みとレプリケーションタスクとデータベース取り込みとレプリケーションタスクでは、Secure Agent を使用できます。PostgreSQL をソースとして使用するデータベース取り込みとレプリケーションの初期ロードタスクと、PostgreSQL をターゲットとして使用するアプリケーション取り込みとレプリケーションタスクおよびデータベース取り込みとレプリケーションタスクでは、サーバーレスランタイム環境も使用できます。ホステッドエージェントまたはエラスティックランタイム環境で、アプリケーション取り込みとレプリケーションタスクまたはデータベース取り込みとレプリケーションタスクを実行することはできません。</p> <p>ランタイム環境の設定および使用方法の詳細については、Administrator のヘルプにある「ランタイム環境」を参照してください。</p>

認証タイプ

PostgreSQL データベースに接続するようにデータベース認証方法または Kerberos 認証方法を設定できます。

注: データ取り込みおよびレプリケーションでは、データベース認証を使用する必要があります。

必要な認証タイプを選択し、認証固有のパラメータを設定します。

データベース認証

データベース認証を設定するには、PostgreSQL アカウントのユーザー名、パスワード、ホスト名、ポート、データベース名が必要です。

次の表に、データベース認証の基本接続プロパティとその説明を示します。

プロパティ	説明
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。
ホスト名	接続先の PostgreSQL サーバーのホスト名。

プロパティ	説明
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。
データベース名	PostgreSQL データベース名。

Kerberos 認証

Kerberos 認証を設定するには、PostgreSQL アカウントのサービスプリンシパル名、ホスト名、ポート、およびデータベース名が必要です。

次の表に、Kerberos 認証の基本接続プロパティとその説明を示します。

プロパティ	説明
サービスプリンシパル名です	Kerberos 認証に使用するサービスプリンシパル名。サービスプリンシパル名は次の形式で指定します: <Service_Name>/<Fully_Qualified_Domain_Name>@<REALM.COM> <ul style="list-style-type: none"> - Service_Name は、インスタンスをホストするサービスの名前です。 - Fully_Qualified_Domain_Name は、ホストマシンの完全修飾ドメイン名です。 - REALM.COM は、ホストマシンのドメイン名です。この値はオプションです。レルム名が指定されていない場合は、デフォルトのレルムが使用されます。
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。
データベース名	PostgreSQL データベース名。

次の表に、Kerberos 認証の詳細接続プロパティとその説明を示します。

プロパティ	説明
追加 Kerberos プロパティ	Kerberos 認証を使用して PostgreSQL に接続するための追加の接続プロパティ。 プロパティを次の形式で入力します: <パラメータ名>=<パラメータ値> 複数のプロパティを入力する場合は、キーと値のそれぞれのペアをセミコロンで区切ります。

詳細設定

次の表に、詳細接続のプロパティを示します。

プロパティ	説明
スキーマ名	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。
接続環境 SQL	データベースに接続する場合に、データベース環境を設定する SQL 文。データベース環境は、この接続を使用するセッション全体に適用されます。例えば、次の文を入力してタイムゾーンを設定できます: SET timezone to 'America/New_York';
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。

暗号化タイプ

暗号化方法によって、Secure Agent と PostgreSQL データベースサーバーで暗号化されたデータをやり取りするかどうかが決まります。SSL を使用した接続を確立しない場合は、[暗号化なし] を選択します。PostgreSQL は 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 noEncryption です。

SSL を使用するには、必要な暗号化方法を選択してから、暗号化固有のパラメータを設定します。

注: 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。Hosted Agent を使用する場合は SSL を設定できません。

SSL

SSL 暗号化方法を使用すると、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。

次の表に、SSL 暗号化の詳細接続プロパティとその説明を示します。

注: 一部の SSL プロパティの [サーバー証明書の検証] チェックボックスをオンにする必要があり、それ以外にも PostgreSQL サーバーでクライアント認証を有効にする必要があるプロパティがあります。

プロパティ	説明
サーバー証明書の検証	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を Secure Agent で検証するかどうかを決定します。[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。サーバー証明書を検証するにはこのオプションを選択します。
トラストストア	このプロパティは、[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されます。 トラストストアファイルのパスおよび名前、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>

プロパティ	説明
トラストストアのパスワード	このプロパティは、[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されます。 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	[サーバー証明書の検証] オプションを選択した場合に必要な応じて設定します。 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	このプロパティは、PostgreSQL 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に適用されます。 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回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。 <code>/home/cldagnt/SystemAgent/serverless/configurations/ssl_store/<KeyStore_filename></code>
キーストアのパスワード	このプロパティは、PostgreSQL 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。
キーパスワード	このプロパティは、PostgreSQL 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に適用されます。 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。
SSLv3 を使用	暗号化された接続の暗号プロトコルとして SSLv3 を使用します。
TLSv1.2 を使用	暗号化された接続の暗号プロトコルとして TLSv1.2 を使用します。

要求 SSL

requestSSL 暗号化方式を使用すると、PostgreSQL は SSL を使用して接続を確立するよう試みます。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。

次の表に、SSL 暗号化の要求の詳細接続プロパティとその説明を示します。

プロパティ	説明
サーバー証明書の検証	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を Secure Agent で検証するかどうかを決定します。[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。 サーバー証明書を検証するにはこのオプションを選択します。
トラストストア	このプロパティは、[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されます。 トラストストアファイルのパスおよび名前、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。 <code>/home/cldagnt/SystemAgent/serverless/configurations/ssl_store/<TrustStore_filename></code>

プロパティ	説明
トラストストアのパスワード	このプロパティは、[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されます。 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	[サーバー証明書の検証] オプションを選択した場合に必要な応じて設定します。 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。
SSLv3 を使用	暗号化された接続の暗号プロトコルとして SSLv3 を使用します。
TLSv1.2 を使用	暗号化された接続の暗号プロトコルとして TLSv1.2 を使用します。

サーバーレスランタイム環境での SSL の設定

PostgreSQL コネクタでサーバーレスランタイム環境を使用して、SSL 対応の PostgreSQL データベースに接続できます。

サーバーレスランタイム環境を使用して安全な PostgreSQL 接続を設定する前に、次の前提条件のタスクを完了して、SSL 証明書をサーバーレスランタイムの場所に追加します。

1. AWS または Azure のサーバーレスエージェント設定用に次の構造を作成します: <補足ファイルの場所>/serverless_agent_config
注: データ取り込みおよびレプリケーションは、AWS でホストされているサーバーレスランタイム環境をサポートしていません。
2. AWS アカウントまたは Azure アカウントの次の場所にある Amazon S3 バケットあるいは Azure コンテナにトラストストアとキースタアの証明書を追加します: <補足ファイルの場所>/serverless_agent_config/SSL
3. 次のコードスニペットをテキストエディタにコピーします。

```
version: 1
agent:
  agentAutoApply:
    general:
      sslStore:
        - fileCopy:
            sourcePath: SSL/<TrustStore_filename>
        - fileCopy:
            sourcePath: SSL/<KeyStore_filename>
```

ここで、sourcePath は AWS または Azure の証明書ファイルのディレクトリパスです。

4. 構文とインデントが有効であることを確認してから、ファイルを serverlessUserAgentConfig.yml として次の AWS または Azure の場所に保存します: <補足ファイルの場所>/serverless_agent_config.yml ファイルの実行時に、SSL 証明書が AWS または Azure の場所からサーバーレスエージェントディレクトリにコピーされます。
5. PostgreSQL 接続のプロパティで、[トラストストア] フィールドと [キースタア] フィールドのサーバーレスエージェントディレクトリに次の証明書パスを指定します: /home/cldagnt/SystemAgent/serverless/configurations/ssl_store/<cert_filename>

第 180 章

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
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。
シークレットコンテナの使用	組織に対して設定されている Secrets Manager にこの接続の機密資格情報を保存します。 このプロパティは、組織に Secrets Manager が設定されている場合にのみ表示されます。 このプロパティは、データ取り込みおよびレプリケーションとデータアクセス管理サービスではサポートされていません。 接続でシークレットコンテナを有効にすると、Secure Agent が Secrets Manager からどの資格情報を取得するかを選択できます。このオプションを無効にした場合、資格情報は組織の設定方法に応じてリポジトリまたはローカル Secure Agent に保存されます。 注: この接続を使用してプッシュダウンまたはプロキシサービスを介してデータアクセスポリシーを適用する場合、シークレットコンテナ設定オプションを使用することはできません。 Secrets Manager を設定および使用方法については、Administrator のヘルプにある「Secrets Manager の設定」を参照してください。
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。 Secure Agent 環境またはエラスティックランタイム環境を選択します。 ランタイム環境の設定および使用方法の詳細については、Administrator のヘルプにある「ランタイム環境」を参照してください。
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。

接続プロパティ	説明
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。
ログgingsの有効化	タスクのセッションログを表示するには、ログgingsを有効にします。

第 181 章

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。
シークレットコンテナの使用	組織に対して設定されている Secrets Manager にこの接続の機密資格情報を保存します。 このプロパティは、組織に Secrets Manager が設定されている場合にのみ表示されます。 このプロパティは、データ取り込みおよびレプリケーションとデータアクセス管理サービスではサポートされていません。 接続でシークレットコンテナを有効にすると、Secure Agent が Secrets Manager からどの資格情報を取得するかを選択できます。このオプションを無効にした場合、資格情報は組織の設定方法に応じてリポジトリまたはローカル Secure Agent に保存されます。 注: この接続を使用してプッシュダウンまたはプロキシサービスを介してデータアクセスポリシーを適用する場合、シークレットコンテナ設定オプションを使用することはできません。 Secrets Manager を設定および使用する方法については、Administrator のヘルプにある「Secrets Manager の設定」を参照してください。
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。 Secure Agent、またはサーバーレスランタイム環境を選択します。 ランタイム環境の設定および使用方法の詳細については、Administrator のヘルプにある「ランタイム環境」を参照してください。
ホスト	Redis サーバーのホスト名または IP アドレスです。

プロパティ	説明
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。
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。 <ul style="list-style-type: none"> - 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。

第 182 章

REST API 接続のプロパティ

REST API 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。

REST API 接続のプロパティについては、次のカテゴリを考慮してください。

- 全般的なプロパティ
- URL プロパティ
- フォームプロパティ
- ヘッダープロパティ
- 認証プロパティ

第 183 章

REST V2 接続のプロパティ

REST アーキテクチャで構築された Web サービスアプリケーションと対話するための REST V2 コネクタを作成します。

前提条件

REST V2 接続を設定する前に、前提条件を必ず満たすようにしてください。

- 64 ビットマシンに Secure Agent をインストールする。
- Secure Agent をホスティングしているマシンのメモリサイズが、2048 MB 以上であることを確認する。

REST V2 への接続

REST アーキテクチャ上に構築された Web サービスアプリケーションと対話するように REST V2 の接続プロパティを設定してみましょう。

始める前に

開始する前に、前提条件を必ず満たすようにしてください。

接続の詳細

次の表に、基本接続プロパティを示します。

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

プロパティ	説明
シークレットコンテナの使用	<p>組織に対して設定されている Secrets Manager にこの接続の機密資格情報を保存します。</p> <p>このプロパティは、組織に Secrets Manager が設定されている場合にのみ表示されます。</p> <p>このプロパティは、データ取り込みおよびレプリケーションとデータアクセス管理サービスではサポートされていません。</p> <p>接続でシークレットコンテナを有効にすると、Secure Agent が Secrets Manager からどの資格情報を取得するかを選択できます。このオプションを無効にした場合、資格情報は組織の設定方法に応じてリポジトリまたはローカル Secure Agent に保存されます。</p> <p>注: この接続を使用してプッシュダウンまたはプロキシサービスを介してデータアクセスポリシーを適用する場合、シークレットコンテナ設定オプションを使用することはできません。</p> <p>Secrets Manager を設定および使用方法については、Administrator のヘルプにある「Secrets Manager の設定」を参照してください。</p>
ランタイム環境	<p>タスクを実行するランタイム環境の名前。</p> <p>Secure Agent、ホステッドエージェント、サーバーレスランタイム環境、またはエラスティックランタイム環境を選択します。</p> <p>ホステッドエージェント、サーバーレスランタイム環境、またはエラスティックランタイム環境で、ストリーミング取り込みとレプリケーションタスクを実行することはできません。</p> <p>ランタイム環境の設定および使用方法の詳細については、Administrator のヘルプにある「ランタイム環境」を参照してください。</p>

認証タイプ

標準の OAuth 2.0 クライアント資格情報、OAuth 2.0 認証コード、JWT ベアラートークンおよび API キー認証タイプを設定して、REST エンドポイントに接続できます。

必要な認証方法を選択し、認証固有のパラメータを設定します。

標準認証

標準認証では、REST エンドポイントに接続するために認証ユーザー ID とパスワードが必要です。標準認証タイプを設定する場合は、基本認証タイプと OAuth 認証タイプをさらに設定することができます。

注: ダイジェスト認証は適用されません。

次の表に、標準認証の基本的な接続プロパティに関する説明を示します。

プロパティ	説明
認証タイプ	<p>標準認証を選択した場合に使用できる認証タイプ。</p> <p>以下のいずれかの認証タイプを選択できます。</p> <ul style="list-style-type: none"> - 基本 - OAuth - なし <p>デフォルトは NONE です。</p>
認証ユーザー ID	<p>標準認証を選択した場合に 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。</p> <p>基本認証タイプの場合は必須です。</p>

プロパティ	説明
認証パスワード	標準認証を選択したときにユーザー名に関連付けたパスワード。 基本認証タイプの場合は必須です。
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 ファイルまたは OpenAPI ファイルのパス。 次のいずれかのファイルパスを指定できます。 <ul style="list-style-type: none"> - Secure Agent マシン上の Swagger または OpenAPI ファイルのパスとファイル名。 - Swagger または OpenAPI ファイルがホストされている 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。 例えば、Swagger ファイルのパスは次のようになります。 C:\swagger\sampleSwagger.json ユーザーにはフォルダとファイルの読み取り権限が必要です。

OAuth 2.0 クライアント資格情報認証

OAuth 2.0 クライアント資格情報認証には、少なくともクライアント ID、アクセストークン URL、クライアントシークレット、スコープ、およびアクセストークンが必要です。

次の表に、OAuth 2.0 クライアント資格情報認証の基本的な接続プロパティに関する説明を示します。

プロパティ	説明
アクセストークン URL	アプリケーションで設定されているアクセストークン URL。
クライアント ID	アプリケーションのクライアント ID。
クライアントシークレット	アプリケーションのクライアントシークレット。
スコープ	API エンドポイントでカスタムスコープが定義されている場合に、アクセス制御を指定します。スコープ属性をスペースで区切って入力します。例: root_readonly root_readwrite manage_app_users

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。パラメータは JSON 形式で定義します。 例: [{"Name": "resource", "Value": "https://<serverName>"}]
クライアント認証	認証のために要求本文または要求ヘッダーのいずれかでクライアント ID とクライアントシークレットを送信するオプションを選択します。 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した情報に基づいて、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。 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 プロパティ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。接続設定で設定されたプロキシは、アクセストークンの生成呼び出しには適用されません。
Swagger ファイルパス	Swagger ファイルまたは OpenAPI ファイルのパス。 次のいずれかのファイルパスを指定できます。 - Secure Agent マシン上の Swagger または OpenAPI ファイルのパスとファイル名。 - Swagger または OpenAPI ファイルがホストされている 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。 例えば、Swagger ファイルのパスは次のようになります。 C:\swagger\sampleSwagger.json ユーザーにはフォルダとファイルの読み取り権限が必要です。 注: ストリーミング取り込みとレプリケーションタスクでは、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。

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 を登録します。

`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 認証コードの認証の基本的な接続プロパティに関する説明を示します。

プロパティ	説明
認証トークン URL	アプリケーションで設定されている認証サーバー URL。
アクセストークン URL	アプリケーションで設定されているアクセストークン URL。
クライアント ID	アプリケーションのクライアント ID。
クライアントシークレット	アプリケーションのクライアントシークレット。
スコープ	API エンドポイントでカスタムスコープが定義されている場合に、アクセス制御を指定します。スコープ属性をスペースで区切って入力します。 例: root_readonly root_readwrite manage_app_users
アクセストークンパラメータ	アクセストークン URL で使用する追加パラメータ。パラメータは JSON 形式で定義します。 例: [{"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 形式で定義します。 例: [{"Name": "max_age", "Value": 60}, {"Name": "state", "Value": "test"}]
クライアント認証	認証のために要求本文または要求ヘッダーのいずれかでクライアント ID とクライアントシークレットを送信するオプションを選択します。 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した情報に基づいて、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。 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 プロパティ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。接続設定で設定されたプロキシは、アクセストークンの生成呼び出しには適用されません。

プロパティ	説明
更新トークン	<p>更新トークンの値。 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。</p> <p>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。</p>
Swagger ファイルパス	<p>Swagger ファイルまたは OpenAPI ファイルのパス。 次のいずれかのファイルパスを指定できます。</p> <ul style="list-style-type: none"> - Secure Agent マシン上の Swagger または OpenAPI ファイルのパスとファイル名。 - Swagger または OpenAPI ファイルがホストされている 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。 <p>例えば、Swagger ファイルのパスは次のようになります。 C:\swagger\sampleSwagger.json</p> <p>ユーザーにはフォルダとファイルの読み取り権限が必要です。</p> <p>注: ストリーミング取り込みとレプリケーションタスクでは、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。</p>

JWT ベアラートークン認証

JWT ベアラートークン認証には、少なくとも JWT ヘッダー、JWT ペイロード、および認可サーバー URL が必要です。

次の表に、JWT ベアラートークン認証の基本的な接続プロパティとその説明を示します。

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: <pre>{ "alg": "RS256", "kid": "xxyyzz" }</pre> 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: <pre>{ "iss": "abc", "sub": "678", "aud": "https://api.box.com/oauth2/token", "box_sub_type": "enterprise", "exp": "120", "jti": "3ee9364e" }</pre> exp として表される有効期限は、秒単位の相対時間です。 有効期限は、トークン発行者の時間 (iat) から UTC 形式で計算されます。 ペイロードに iat が定義されており、有効期限に達すると、マッピングとアクセストークンの生成が失敗します。 新しいアクセストークンを生成するには、ペイロードに有効な iat を指定する必要があります。 iat がペイロードで定義されていない場合、有効期限は現在のタイムスタンプから計算されます。 有効期限を文字列値として渡すには、値を二重引用符で囲みます。例: "exp": "120" 有効期限を整数値として渡すには、値を二重引用符で囲まないでください。 例: "exp": "120"
認証サーバー	アプリケーションで設定されているアクセストークン URL。

プロパティ	説明
キーストアファイルパス	<p>REST API との双方向の安全な接続を確立するために必要なキーと証明書を含むキーストアファイルの絶対パス。各 Secure Agent マシンで使用可能なディレクトリパスを指定します。</p> <p>また、キーストアファイル名とパスを JVM オプションとして設定するか、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。</p> <p>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。</p> <p>例: /home/cldagnt/SystemAgent/serverless/configurations/ssl_store/<cert_name>.jks</p>
キーストアのパスワード	<p>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。</p> <p>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。</p>
プライベートキーのエイリアス	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	<p>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。</p>
アクセストークン	<p>アクセストークンの値。</p> <p>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。</p> <p>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 プロパティ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。接続設定で設定されたプロキシは、アクセストークンの生成呼び出しには適用されません。</p>
Swagger ファイルパス	<p>Swagger ファイルまたは OpenAPI ファイルのパス。</p> <p>次のいずれかのファイルパスを指定できます。</p> <ul style="list-style-type: none"> - Secure Agent マシン上の Swagger または OpenAPI ファイルのパスとファイル名。 - Swagger または OpenAPI ファイルがホストされている 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。 <p>例えば、Swagger ファイルのパスは次のようになります。 C:\swagger\sampleSwagger.json</p> <p>ユーザーにはフォルダとファイルの読み取り権限が必要です。</p> <p>注: ストリーミング取り込みとレプリケーションタスクでは、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。</p>

詳細設定

次の表に、JWT ベアラートークン認証の詳細接続プロパティをその説明を示します。

プロパティ	説明
認証の詳細プロパティ	<p>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。</p> <p>例:</p> <pre>[{"Name": "client_id", "Value": "abc"}, \ {"Name": "client_secret", "Value": "abc"}]</pre>
トラストストアファイルパス	<p>REST API との一方向または双方向の安全な接続を確立するための TLS 証明書を含むトラストストアファイルの絶対パス。各 Secure Agent マシンで使用可能なディレクトリパスを指定します。</p> <p>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。</p> <p><Secure Agent のインストールディレクトリ>\jre\lib\security\cacerts</p> <p>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。</p> <p>例: /home/cldagnt/SystemAgent/serverless/configurations/ssl_store/<cert_name>.jks</p>
トラストストアのパスワード	<p>SSL 証明書を含むトラストストアファイルのパスワード。</p> <p>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。</p>
プロキシタイプ	<p>プロキシのタイプ。</p> <p>次のいずれかのオプションを選択します。</p> <ul style="list-style-type: none">- プロキシなし。エージェントレベルまたは接続プロパティで設定されたプロキシサーバーをバイパスします。- プラットフォームプロキシ。エージェントで設定されたプロキシを考慮します。- カスタムプロキシ。接続プロパティで設定されたプロキシを考慮します。

プロパティ	説明
プロキシ構成	<p>プロキシを設定するために必要な形式。 プロキシは、次の形式を使用して設定することができます:</p> <p><ホスト>:<ポート></p> <p>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。</p>
詳細フィールド	<p>エージェントが REST エンドポイントに接続するときに使用する引数を入力します。 複数の引数を指定する場合は、それぞれの引数をセミコロンで区切ります。</p> <p>例:</p> <pre>connectiondelaytime:10000;retryattempts:5</pre> <p>次のような引数を指定することができます。</p> <ul style="list-style-type: none"> - 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。 <p>注: ストリーミング取り込みとレプリケーションタスクでは、ConnectionTimeout および retryattempts のみが適用されます。</p>

API キー認証

API キー認証を使用すると、一意のキーおよび対応する値を指定して、REST エンドポイントに対して実行される API 呼び出しを認証できます。

次の表に、共有キー認証の基本接続プロパティとその説明を示します。

プロパティ	説明
キー	REST V2 コネクタが REST エンドポイントに対して実行される API 呼び出しを認証するために使用する一意の API キー。
値	API 呼び出しを実行するために必要な API キーに対応する値。

プロパティ	説明
API キーの追加先	<p>REST エンドポイントに API 呼び出しを実行するために、API キーとそれに対応する値を要求ヘッダーまたはクエリパラメータとして送信する必要があるかどうかを指定します。</p> <p>次のいずれかのオプションを選択します。</p> <ul style="list-style-type: none"> - 要求ヘッダー - クエリパラメータ
Swagger ファイルパス	<p>Swagger ファイルまたは OpenAPI ファイルのパス。</p> <p>次のいずれかのファイルパスを指定できます。</p> <ul style="list-style-type: none"> - Secure Agent マシン上の Swagger または OpenAPI ファイルのパスとファイル名。 - Swagger または OpenAPI ファイルがホストされている 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。 <p>例えば、Swagger ファイルのパスは次のようになります。</p> <p>C:\swagger\sampleSwagger.json</p> <p>ユーザーにはフォルダとファイルの読み取り権限が必要です。</p> <p>注: ストリーミング取り込みとレプリケーションタスクでは、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。</p>

詳細設定

次の表に、詳細接続のプロパティを示します。

プロパティ	説明
トラストストアファイルパス	<p>REST API との一方または双方向の安全な接続を確立するための TLS 証明書を含むトラストストアファイルの絶対パス。各 Secure Agent マシンで使用可能なディレクトリパスを指定します。</p> <p>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。</p> <p><Secure Agent のインストールディレクトリ>\jre\lib\security\cacerts</p> <p>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。</p> <p>例: /home/cldagnt/SystemAgent/serverless/configurations/ssl_store/<cert_name>.jks</p>
トラストストアのパスワード	<p>SSL 証明書を含むトラストストアファイルのパスワード。</p> <p>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。</p>

プロパティ	説明
キーストアファイルパス	<p>REST API との双方向の安全な接続を確立するために必要なキーと証明書を含むキーストアファイルの絶対パス。各 Secure Agent マシンで使用可能なディレクトリパスを指定します。</p> <p>また、キーストアファイル名とパスを JVM オプションとして設定するか、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。</p> <p>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。</p> <p>例: <code>/home/cldagnt/SystemAgent/serverless/configurations/ssl_store/<cert_name>.jks</code></p>
キーストアのパスワード	<p>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。</p> <p>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。</p>
プロキシタイプ	<p>プロキシのタイプ。</p> <p>次のいずれかのオプションを選択します。</p> <ul style="list-style-type: none"> - プロキシなし: エージェントレベルまたは接続レベルで設定されたプロキシサーバーをバイパスします。 - プラットフォームプロキシ: エージェントで設定されたプロキシを考慮します。 - カスタムプロキシ: 接続プロパティで設定されたプロキシを考慮します。
プロキシ構成	<p>プロキシを設定するために必要な形式。</p> <p>次の形式を使用してプロキシを設定します:</p> <p><code><ホスト>:<ポート></code></p> <p>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。</p>
詳細フィールド	<p>エージェントが REST エンドポイントに接続するときに使用する引数を入力します。</p> <p>複数の引数を指定する場合は、それぞれの引数をセミコロンで区切ります。</p> <p>例:</p> <p><code>connectiondelaytime:10000;retryattempts:5</code></p> <p>次のような引数を指定することができます。</p> <ul style="list-style-type: none"> - <code>ConnectionTimeout</code>。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。 - <code>connectiondelaytime</code>。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。 - <code>retryattempts</code>。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。 - <code>qualifiedSchema</code>。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 <code>false</code> です。 - <code>encodeQueryParams</code>。REST V2 コネクタが REST エンドポイントに対して API 呼び出しを行うときに、URL のクエリパラメータをエンコードする必要があるかどうかを決定します。この引数を <code>false</code> に設定すると、クエリパラメータのエンコードがスキップされます。 デフォルトは <code>true</code> です。 <p>注: ストリーミング取り込みとレプリケーションタスクでは、<code>ConnectionTimeout</code> および <code>retryattempts</code> のみが適用されます。</p>

TLS 認証によるセキュアな通信

TLS 認証を設定して、Secure Agent と REST API over TLS との間に一方向または双方向のセキュアな通信を確立します。

一方向のセキュアな通信を確立するには、次の手順を実行します。

1. トラストストアを生成します。手順の詳細については、「トラストストアの生成」を参照してください。
2. REST V2 接続を一方向 SSL 用に設定します。トラストストアファイルとトラストストアパスワードは、接続で指定するか、Secure Agent の JVM オプションで設定することができます。

双方向のセキュアな通信を確立するには、まず一方向のセキュアな通信を設定してから、次の手順を実行する必要があります。

1. キーストアを生成します。手順の詳細については、「キーストアの生成」を参照してください。
2. REST V2 接続を双方向 SSL 用に設定します。キーストアファイルとキーストアパスワードは、接続で指定するか、Secure Agent の JVM オプションで設定することができます。

接続と JVM オプションでキーストアとトラストストアのプロパティを指定すると、Secure Agent では接続で設定されたプロパティに基づいて証明書が処理されます。

トラストストアの生成

トラストストアを生成するには、サーバー証明書が必要です。サーバー証明書を取得し、次の手順を実行してトラストストアを生成します。

1. サーバー証明書を、Secure Agent インストール内で使用可能な次のいずれかのディレクトリにインポートします。
 - <Secure Agent のインストールディレクトリ>\jdk\jre\lib\security\cacerts
 - <Secure Agent のインストールディレクトリ>\jdk8\jre\lib\security\cacerts
2. トラストストアを生成するには、コマンドラインから次のコマンドを実行します。
keytool -importcert -alias <エイリアス名をここで指定します> -file <サーバー証明書をここで指定します> -keystore <生成するカスタムトラストストアの名前を指定します> -storepass <カスタムトラストストアのパスワードを指定します>

例: keytool -importcert -alias RESTV2CACert -file ca.pem -keystore sampletruststore -storepass JKSTrustStorePassword

この例では、*sampletruststore* という名前と *JKSTrustStorePassword* というパスワードでトラストストアファイルが生成されます。

キーストアの生成

キーストアを生成するには、クライアント証明書とクライアントシークレットキーが必要です。クライアント証明書とクライアントシークレットキーを取得し、次の手順を実行してキーストアを生成します。

1. サーバー証明書を、Secure Agent インストール内で使用可能な次のいずれかのディレクトリにインポートします。
 - <Secure Agent のインストールディレクトリ>\jdk\jre\lib\security\cacerts
 - <Secure Agent のインストールディレクトリ>\jdk8\jre\lib\security\cacerts

2. キーストアを生成するには、コマンドラインから次のコマンドを実行します。

```
openssl pkcs12 -export -in <ここでクライアント証明書を指定します> -inkey <ここでプライベートキーを指定します> -name "<ここに任意の名前を指定します>" -passout pass:<生成するキーストアのパスワードを指定します> -out <p12 拡張子を使用してキーストアの名前を指定します>
```

```
例: openssl pkcs12 -export -in /home/samplefolder/certs/client-cert.pem -inkey /home/samplefolder/certs/client-key.pem -name "restclient" -passout pass:PKCSKeyStorePassword -out samplekeystore.p12
```

この例では、*samplekeystore.p12* は PKCS12 形式で生成されます。

キーストアファイルを .p12 形式から .jks 形式に変換するには、コマンドラインから次のコマンドを実行します。

```
keytool -importkeystore -srckeystore <p12 キーストアファイルの名前を指定します> -srcstoretype pkcs12 -srcstorepass <生成された p12 キーストアファイルのパスワードを指定します> -destkeystore <JKS キーストアファイルの名前を指定します> -deststoretype JKS -deststorepass <JKS キーストアファイルのパスワードを指定します>
```

注: -srcstorepass で指定されたパスワードは -deststorepass と同じである必要があります。

```
例: keytool -importkeystore -srckeystore samplekeystore.p12 -srcstoretype pkcs12 -srcstorepass PKCSKeyStorePassword -destkeystore keystore -deststoretype JKS -deststorepass PKCSKeyStorePassword
```

この例では、*samplekeystore* という名前と *PKCSKeyStorePassword* というパスワードでキーストアファイルが生成されます。

一方向または双方向のセキュアな通信の設定

接続は、一方向または双方向 SSL 用に設定できます。

一方向 SSL 用の接続の設定

接続プロパティの [トラストストアファイル名] フィールドと [トラストストアのパスワード] フィールドで、トラストファイルの名前とトラストストアのパスワードを指定することができます。または、Secure Agent プロパティの JVM オプションでトラストストアファイル名とトラストストアパスワードを設定することもできます。

1. [管理] > [ランタイム環境] をクリックして、エージェントを選択します。
2. [システム構成の詳細] の [タイプ] で [DTM] を選択します。
3. 次の JVM オプションを追加します。
 - JVMOption1=-Djavax.net.ssl.trustStore=<.jks トラストストアファイルの絶対パス>
 - JVMOption2=-Djavax.net.ssl.trustStorePassword=<トラストストアのパスワード>

双方向 SSL 用の接続の設定

接続プロパティ [キーストアファイル名] および [キーストアのパスワード] で、キーファイルの名前とキーストアのパスワードを指定することができます。または、Secure Agent プロパティの JVM オプションでキーストアファイルとキーストアパスワードを設定することもできます。

双方向の SSL を使用するには、最初に一方向 SSL の手順を実行してから、次の手順を実行して双方向 SSL を設定する必要があります。

1. [管理] > [ランタイム環境] をクリックして、エージェントを選択します。
2. [システム構成の詳細] の [タイプ] で [DTM] を選択します。
3. 次の JVM オプションを追加します。
 - JVMOption3=-Djavax.net.ssl.keyStore=<.jks キーストアファイルの絶対パス>
 - JVMOption4=-Djavax.net.ssl.keyStorePassword=<キーストアのパスワード>

サーバーレスランタイム環境での安全な通信

サーバーレスランタイム環境を使用している場合は、TLS 認証を設定すると、REST API との安全な一方向または双方向通信を確立できます。

証明書が .jks 形式であることを確認してください。

サーバーレスランタイム環境を使用して安全な REST V2 接続を設定するには、次の前提条件タスクを完了して、TLS 証明書をサーバーレスランタイムの場所に追加します。

1. AWS のサーバーレスエージェント設定用に次の構造を作成します:
<Supplementary file location>/serverless_agent_config
2. AWS アカウントの次の場所にある Amazon S3 バケットに、一方向の安全な通信の場合はトラストストア証明書を追加し、双方向の安全な通信の場合はトラストストア証明書とキーストア証明書を追加します:
<補足ファイルの場所>/serverless_agent_config/SSL
3. 次のコードスニペットをテキストエディタにコピーします。

```
version: 1
agent:
  agentAutoApply:
    general:
      sslStore:
        - fileCopy:
            sourcePath: SSL/<RESTV2_trustStore_cert_name>.jks
        - fileCopy:
            sourcePath: SSL/<RESTV2_keyStore_cert_name>.jks
```

ここで、ソースパスは AWS の証明書ファイルのディレクトリです。

4. 構文とインデントが有効であることを確認してから、ファイルを serverlessUserAgentConfig.yml として次の AWS の場所に保存します。

<Supplementary file location>/serverless_agent_config

.yml ファイルが実行されると、SSL 証明書が AWS の場所からサーバーレスエージェントディレクトリにコピーされます。

5. REST V2 接続プロパティの【トラストストアファイルパス】フィールドと【キーストアファイルパス】フィールドで、サーバーレスエージェントディレクトリ内の次の証明書パスを指定します:
/home/cldagnt/SystemAgent/serverless/configurations/ssl_store/<cert_name>.jks

サーバーレスランタイム環境の Swagger 仕様ファイル

サーバーレスランタイム環境で Swagger ファイルを設定するには、前提条件を必ず満たすようにしてください。

サーバーレスランタイム環境では、次のいずれかの方法で Swagger ファイルを設定することができます。

- Swagger ファイルのパブリックホスト URL を **Swagger ファイルパス** 接続プロパティで指定します。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ることを確認します。
- Swagger ファイルをサーバーレスエージェントディレクトリに配置します。

サーバーレスランタイム環境で Swagger ファイルを設定するには、次の前提条件のタスクを完了して、Swagger ファイルをサーバーレスランタイムの場所に追加します。

1. AWS または Azure のサーバーレスエージェント設定用に次の構造を作成します:
<Supplementary file location>/serverless_agent_config
2. AWS または Azure アカウントの次の場所にある Amazon S3 バケットあるいは Azure コンテナに Swagger 仕様ファイルを追加します:
<補足ファイルの場所>/serverless_agent_config
 - a. 次のコードスニペットをテキストエディタにコピーします。

```
version: 1
agent:
  dataIntegrationServer:
    autoApply:
      restv2:
        swaggers:
          - fileCopy:
              sourcePath: restv2/<swagger_file_name1>.json
          - fileCopy:
              sourcePath: restv2/<swagger_file_name2>.json
```

ここで、ソースパスは AWS または Azure の Swagger ファイルのディレクトリパスです。

3. 構文とインデントが有効であることを確認してから、ファイルを serverlessUserAgentConfig.yml として次の AWS または Azure の場所に保存します:
<Supplementary file location>/serverless_agent_config

.yml ファイルの実行時に、SSL 証明書が AWS または Azure の場所からサーバーレスエージェントディレクトリにコピーされます。
4. REST V2 接続プロパティで、**[Swagger ファイルパス]** フィールドのサーバーレスエージェントディレクトリの次の Swagger パスを指定します:
/home/cldagnt/SystemAgent/serverless/configurations/restv2/<swagger_file_name>.json

サーバーレスランタイム環境の設定および使用方法の詳細については、Administrator のヘルプにある「サーバーレスランタイム環境」を参照してください。

エラスティックランタイム環境の設定

エラスティックランタイム環境でカスタムバイナリファイルを設定し、マッピング実行中にランタイム環境でこれらのファイルにアクセスして実行できるようにします。

カスタムバイナリファイルを設定する前に、必ず AWS にエラスティックランタイム環境をデプロイして、Informatica Intelligent Cloud Services 内でデータを処理できる Kubernetes クラスタを作成してください。

エラスティックランタイム環境のデプロイの詳細については、「[Deploy an elastic runtime environment](#)」を参照してください。

エラスティックランタイム環境をデプロイした後、マウントされたディスクにカスタムバイナリファイルを配置し、POST 要求で使用するバイナリファイルの正確なパスをコピーします。

Informatica Intelligent Cloud Services 内でエラスティックランタイム環境に対する次の手順を実行して、カスタムバイナリファイルを管理します。

1. 組織にログインして、セッション ID とランタイム環境 ID を取得します。
2. REST API への POST 呼び出しを行い、セッション ID、ランタイム環境 ID、およびマウントされたディスクから先ほどコピーしたバイナリファイルパスを渡します。

POST 呼び出しの詳細については、『REST API リファレンス』ガイドの「[Supplementary files](#)」を参照してください。

POST 要求の例を次に示します。

```
POST <base URL>/api/v3/RuntimeEnvironment/<runtime environment ID>/ElasticConfig
Content-Type: application/json
Accept: application/json
INFA-SESSION-ID: <SessionId>
{
  "rteId": "rte-12345",
  "specification": {
    "agent": {
      "dataIntegrationServer": {
        "restv2": {
          "swaggers": [{"sourcePath": "<path to binaries>/swagger.json"}],
          "keystores": [{"sourcePath": "<path to binaries>/keystore.jks"}],
          "truststores": [{"sourcePath": "<path to binaries>/truststore.jks"}]
        }
      }
    }
  }
}
```

POST 呼び出しによって、データ統合サーバーの再起動がトリガされます。

3. Administrator でデータ統合サーバーのステータスを確認して、エラスティックランタイム環境が実行されていることを確認します。
4. 接続をテストするか、マッピングを実行して、エラスティックランタイム環境でカスタムバイナリファイルにアクセスして使用できることを確認します。

ランタイム環境のルールとガイドライン

異なるランタイム環境でタスクを実行する場合は、次のガイドラインを考慮してください。

- ホステッドエージェントまたはサーバーレスランタイム環境を使用している場合、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。
- ホステッドエージェントを使用している場合、CA によって署名されたカスタムサーバー証明書を必要とし、Informatica cacerts トラストストアの一部ではない REST API エンドポイントに接続することはできません。
- ホステッドエージェントを使用している場合、JWT ベアラートークン認証を設定することはできません。
- Swagger 仕様ファイルの URL がパブリック URL であり、ホステッドエージェントを使用しているときに、追加の認証とリダイレクトが求められることなく Swagger 仕様ファイルによってファイルのコンテンツが返されることを確認してください。

REST V2 接続のルールとガイドライン

Rest V2 接続については、次のルールとガイドラインを考慮してください。

- 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。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 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	
×	○	×	×	プロキシを考慮しません。
×	×	○	いいえ	プロキシを考慮しません。
×	×	×	はい	カスタムプロキシを考慮します。
○	○	×	×	プロキシを考慮しません。
はい	×	○	いいえ	プラットフォームプロキシを考慮します。
はい	×	×	はい	カスタムプロキシを考慮します。

第 184 章

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がある認証方法。 [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。
トラストストアファイルパス	REST API との一方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。

接続プロパティ	説明
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	<p>プロキシのタイプ。</p> <p>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。</p> <ul style="list-style-type: none"> - 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。 <p>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。</p>
プロキシホスト	<p>プロキシサーバーの IP アドレスまたはホスト名。</p> <p>[カスタム] プロキシタイプにのみ必要です。</p>
プロキシポート	<p>プロキシサーバーのポート番号。</p> <p>[カスタム] プロキシタイプにのみ必要です。</p>
プロキシユーザー	<p>プロキシサーバーのユーザー名。</p> <p>[カスタム] プロキシタイプにのみ必要です。</p>
プロキシパスワード	<p>プロキシサーバーのパスワード。</p> <p>[カスタム] プロキシタイプにのみ必要です。</p>
接続タイムアウト	<p>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。</p> <p>デフォルトは 60 秒です。</p> <p>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。</p>
再試行回数	<p>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。</p> <p>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。</p> <p>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。</p>
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	<p>REST エンドポイントに接続するための HTTP バージョン。</p> <p>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。</p> <ul style="list-style-type: none"> - HTTP 2 - HTTP 1.1 <p>デフォルトは HTTP 2 です。</p>

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がある認証方法。 【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>"}]
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。

接続プロパティ	説明
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	<p>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。</p> <p>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。</p> <p>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。</p>
リフレッシュトークン	<p>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。</p> <p>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。</p> <p>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。</p>
トラストストアファイルパス	<p>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。</p> <p>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。</p>
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	<p>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。</p> <p>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。</p>
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	<p>プロキシのタイプ。</p> <p>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。</p> <ul style="list-style-type: none"> - 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。 <p>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。</p>
プロキシホスト	<p>プロキシサーバーの IP アドレスまたはホスト名。</p> <p>[カスタム] プロキシタイプにのみ必要です。</p>
プロキシポート	<p>プロキシサーバのポート番号。</p> <p>[カスタム] プロキシタイプにのみ必要です。</p>

接続プロパティ	説明
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。

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。
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。 <ul style="list-style-type: none"> - 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。

接続プロパティ	説明
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。
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。

第 185 章

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
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。
シークレットコンテナの使用	組織に対して設定されている Secrets Manager にこの接続の機密資格情報を保存します。このプロパティは、組織に Secrets Manager が設定されている場合にのみ表示されます。このプロパティは、データ取り込みおよびレプリケーションとデータアクセス管理サービスではサポートされていません。 接続でシークレットコンテナを有効にすると、Secure Agent が Secrets Manager からどの資格情報を取得するかを選択できます。このオプションを無効にした場合、資格情報は組織の設定方法に応じてリポジトリまたはローカル Secure Agent に保存されます。 注: この接続を使用してプッシュダウンまたはプロキシサービスを介してデータアクセスポリシーを適用する場合、シークレットコンテナ設定オプションを使用することはできません。 Secrets Manager を設定および使用方法については、Administrator のヘルプにある「Secrets Manager の設定」を参照してください。
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。
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。

第 186 章

Salesforce Commerce Cloud 接続のプロパティ

Salesforce Commerce 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。

重要: Salesforce Commerce Cloud コネクタは非推奨となり、メンテナンスモードに移行されました。Informatica は将来のリリースでサポートを廃止する予定です。

次の表に、Salesforce Commerce 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	オプション。接続の説明。
タイプ	接続タイプ。【Salesforce Commerce Cloud】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。
ベース URL	Salesforce Commerce Cloud に接続するためのベース URL。 例: https://demo-ocapi.demandware.net
クライアント ID	Salesforce Commerce Cloud に接続するための OAuth 2.0 認証用クライアント ID。
クライアントシークレット	Salesforce Commerce Cloud に接続するための OAuth 2.0 認証用クライアント秘密鍵。
API タイプ	使用する Salesforce Commerce Cloud API のタイプ。次のいずれかの API を選択します。 <ul style="list-style-type: none">- data。製品在庫や顧客リストといったバックエンドシステムリソースにアクセスします。- meta。Salesforce Commerce Cloud から OCAPI リソースのメタデータを取得します。- shop。カートアクティビティ、製品情報、製品価格といった買物客のペルソナに関連する詳細を取得します。
API バージョン	接続する data API、meta API、または shop API のバージョン。
サイト ID	shop API で必須です。接続するサイトの ID。

第 187 章

Salesforce 接続のプロパティ

Salesforce との間でデータの安全な読み取りまたは書き込みを行うための Salesforce 接続を作成します。Salesforce 接続を使用して、Salesforce アプリケーションのオブジェクトにアクセスします。

認証の準備

Salesforce にアクセスするための標準認証タイプと OAuth 接続タイプを設定できます。OAuth 認証を使用して、Salesforce へのより安全な接続を検討してください。
接続プロパティを設定する前に、使用する認証のタイプに基づいて認証の詳細を用意しておく必要があります。

標準

標準接続を使用するには、Salesforce アカウントのユーザー名、パスワード、およびサービス URL が必要です。また、Salesforce に接続するには Salesforce セキュリティトークンが必要です。セキュリティトークンを使用しない場合は、Salesforce アカウントの信頼できる IP 範囲にデータ統合の IP アドレスを追加する必要があります。

Secure Agent とサービスで使用される IP アドレス範囲のリストの詳細については、「[POD Availability and Networking](#)」を参照してください。Salesforce アカウントでの IP アドレスの設定については、Salesforce のマニュアルを参照してください。

OAuth

OAuth 2.0 プロトコルを使用して Salesforce API 経由で Salesforce にアクセスする OAuth 接続を作成します。OAuth は、セキュアな API 承認に使用できる標準プロトコルです。

OAuth 接続を作成するには、OAuth 更新トークンが必要です。Informatica は、OAuth 更新トークンを生成するための SFDC OAuth 2.0 ツールを提供しています。

また、OAuth 更新トークンを生成するには、Salesforce アカウントのコンシューマキーとコンシューマシークレットが必要です。

1. [Informatica Marketplace](#) から SFDC OAuth ツールをダウンロードします。
2. OAuth.zip ファイルを展開します。
3. oauth\conf フォルダに移動して server.xml ファイルを開き、mystore.jks ファイルのパスをシステム上のパスに更新します。保存してから、ファイルを閉じます。
4. \oauth\bin に移動して、コマンド catalina.bat start を実行します。
5. ブラウザで <http://localhost:8090/salesforce> を開きます。
6. Salesforce のユーザー名とパスワードを入力してログインします。

7. クライアント ID とクライアントシークレットを入力し、**[送信]** をクリックします。
クライアント ID は Salesforce のコンシューマキーで、クライアントシークレットは Salesforce のコンシューマシークレットです。
OAuth 更新トークンが生成されます。

Salesforce への接続

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

デフォルトでは、新しい組織の Salesforce 接続は Salesforce API バージョン 63.0 を使用します。既存の Salesforce 接続を編集することや、新しい接続を作成して、バージョン 58.0 とバージョン 61.0 を除くバージョン 63.0 以前の Salesforce API を使用することもできます。

始める前に

開始する前に、設定する接続タイプに基づいて Salesforce アカウントから情報を取得する必要があります。

標準接続を設定するには、Salesforce アカウントから Salesforce ユーザー名、パスワード、サービス URL、およびセキュリティトークンを取得します。

OAuth 接続を設定するには、Salesforce アカウントからコンシューマキー、コンシューマシークレット、およびサービス URL を取得します。また、Informatica が提供する SFDC OAuth ツールで生成された OAuth 更新トークンを取得する必要があります。

認証の前提条件の詳細については、「[「認証の準備」 \(ページ 689\)](#)」を参照してください。

次のビデオでは、Salesforce アカウントから必要な情報を取得する方法、および SFDC OAuth ツールを使用して OAuth 更新トークンを生成する方法について説明します。



接続の詳細

次の表に、基本接続プロパティを示します。

財産	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。

財産	説明
シークレットコンテナの使用	<p>組織に対して設定されている Secrets Manager にこの接続の機密資格情報を保存します。このプロパティは、組織に Secrets Manager が設定されている場合にのみ表示されます。このプロパティは、データ取り込みおよびレプリケーションとデータアクセス管理サービスではサポートされていません。</p> <p>接続でシークレットコンテナを有効にすると、Secure Agent が Secrets Manager からどの資格情報を取得するかを選択できます。このオプションを無効にした場合、資格情報は組織の設定方法に応じてリポジトリまたはローカル Secure Agent に保存されます。</p> <p>注: この接続を使用してプッシュダウンまたはプロキシサービスを介してデータアクセスポリシーを適用する場合、シークレットコンテナ設定オプションを使用することはできません。</p> <p>Secrets Manager を設定および使用する方法については、Administrator のヘルプにある「Secrets Manager の設定」を参照してください。</p>
ランタイム環境	<p>タスクを実行するランタイム環境の名前。</p> <p>Secure Agent、ホステッドエージェント、サーバーレスランタイム環境、またはエラスティックランタイム環境を選択します。</p> <p>ホステッドエージェントは、詳細モードのマッピングには適用されません。</p> <p>ホステッドエージェントまたはサーバーレスランタイム環境では、アプリケーション取り込みタスクとデータベース取り込みタスクを実行できません。</p> <p>ランタイム環境の設定および使用方法の詳細については、Administrator のヘルプにある「ランタイム環境」を参照してください。</p>

Salesforce 接続タイプ

Salesforce にアクセスするための標準接続タイプと OAuth 接続タイプを設定できます。必要な接続タイプを選択し、接続固有のパラメータを設定します。

標準接続

Salesforce 標準接続には、少なくとも Salesforce アカウントのユーザー名、パスワード、サービス URL が必要です。

次の表に、標準接続の基本的な接続プロパティとその説明を示します。

プロパティ	説明
ユーザー名	Salesforce アカウントに接続するためのユーザー名。
パスワード	Salesforce アカウントに接続するためのパスワード。
サービス URL	<p>Salesforce サービスの URL。</p> <p>例: <code>https://login.salesforce.com/services/Soap/u/63.0</code></p> <p>デフォルトでは、新しい組織の Salesforce 接続には Salesforce API バージョン 63.0 が使用されます。バージョン 58.0 とバージョン 61.0 を除く、63.0 以前のすべての Salesforce API バージョンを使用することができます。</p> <p>最大長は 100 文字です。</p> <p>既存の標準接続のサービス URL を編集する場合は、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。</p>

詳細設定

次の表に、標準接続の詳細接続プロパティとその説明を示します。

プロパティ	説明
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。 注: このフィールドに Salesforce セキュリティトークンを入力しない場合は、Salesforce アカウントの信頼できる IP 範囲にデータ統合の IP アドレスを追加する必要があります。Salesforce アカウントの信頼できる IP 範囲にデータ統合の IP アドレスが追加されていない場合、接続が失敗する可能性があります。IP アドレス範囲のリストの詳細については、「 標準 」(ページ 689)を参照してください。
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 Manager で Secure Agent に定義されたプロキシサーバー設定をバイパスし、Salesforce に直接接続します。 このオプションが選択されていない場合、Salesforce 接続は、Salesforce への接続用に Secure Agent に定義されたプロキシサーバー設定を使用します。

OAuth 接続

OAuth 接続には、Salesforce コンシューマキー、シークレット、および更新トークンが必要です。OAuth 接続を使用する場合は、OAuth2.0 プロトコルを使用する必要があります。

次の表に、OAuth 接続の基本的な接続プロパティとその説明を示します。

プロパティ	説明
OAuth コンシューマキー	更新トークンを生成するためのコンシューマキー。
OAuth コンシューマシークレット	更新トークンを生成するためのコンシューマシークレット。
OAuth 更新トークン	SFDC OAuth 2.0 ツールを使用して生成した更新トークン。 OAuth 更新トークンを生成する方法の詳細については、「 始める前に 」セクションを参照してください。
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/63.0 バージョン 58.0 とバージョン 61.0 を除く、63.0 以前のすべての Salesforce API バージョンを使用することができます。 最大長は 100 文字です。 既存の OAuth 接続のサービス URL を編集する場合は、コンシューマキー、コンシューマシークレット、および更新トークンを再入力する必要があります。

詳細設定

【サービスエンドポイント】および【OAuth アクセストークン】フィールドは、OAuth 認証には適用されません。

ファイアウォール設定

組織のデータがファイアウォールを通過する場合は、Salesforce へのアクセスを許可するようにファイアウォールを設定する必要があります。

Salesforce サーバーに接続できずに接続エラーが発生した場合は、ネットワーク管理者に問い合わせ、Salesforce サーバーへのアクセスを許可するように設定の変更を依頼してください。

詳細については、次のナレッジベースの記事を参照してください: [Firewall rules](#)

注: Salesforce サーバーの IP アドレスは変更されることがあります。Salesforce のサーバーの IP アドレスに関する最新情報については、Salesforce のマニュアルを参照してください。

プロキシサーバーの設定

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

Windows および Linux でプロキシサーバーを使用するように Secure Agent を設定できます。未認証のプロキシサーバーまたは認証済みのプロキシサーバーを Salesforce Standard API または Bulk API で使用することができます。Bulk API 2.0 を使用して Salesforce に接続する場合は、未認証のプロキシサーバーのみを使用できます。プロキシ設定は、マッピングおよび詳細モードのマッピングで使用する接続に適用されます。

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

- Windows の場合は Secure Agent Manager を使用し、Linux の場合はシェルコマンドを使用して Secure Agent を設定します。
手順については、データ統合のヘルプの『または「Windows でのプロキシ設定」または「Linux でのプロキシ設定」を参照してください。
- Secure Agent のプロパティで、DTM の JVM オプションを設定します。手順については、ナレッジベースの記事「[Proxy server settings](#)」を参照してください。

サーバーレスランタイム環境のプロキシの設定を行う方法については、Administrator ヘルプの「「プロキシサーバーの使用」を参照してください。

接続タイムアウト

Secure Agent 設定プロパティの DTM に対する SalesforceConnectionTimeout プロパティを、接続が Salesforce Web サービスからの要求に対する応答を待機する期間（秒単位）に設定できます。指定されたタイムアウト期間内に Web サービスが応答しない場合、要求はタイムアウトします。

次の画像は、Secure Agent に対する設定済みの SalesforceConnectionTimeout プロパティを示しています。

System Configuration Details Reset All

Service: Data Integration Server

Type: DTM

Type	Name	Value
DTM	SalesForceConnectionTimeout	300

Salesforce 接続のトラブルシューティング

Salesforce 接続の設定時にエラーが発生した場合は、Salesforce 接続プロパティに Salesforce セキュリティトークンの入力が必要となることがあります。

セキュリティトークンが要求され、Salesforce 接続の **【セキュリティトークン】** フィールドが空か有効ではない場合、接続をテストまたは作成したときに次のエラーメッセージが表示されます。

The login to Salesforce.com failed with the following message - LOGIN_MUST_USE_SECURITY_TOKEN:

Salesforce の Web サイトへ移動してセキュリティトークンを取得します。接続の詳細へのセキュリティトークンの追加が求められないようにするには、Salesforce アカウントの **【信頼済み IP 範囲】** にデータ統合の IP アドレスを追加します。

第 188 章

Salesforce Data Cloud 接続のプロパティ

Salesforce Data Cloud 接続を作成して、Salesforce へのデータの安全な書き込みを行います。Salesforce Data Cloud 接続を使用して、マッピングおよびマッピングタスクでターゲットを指定できます。

Salesforce Data Cloud への接続

Salesforce Data Cloud に接続するように Salesforce Data Cloud 接続プロパティを設定しましょう。

始める前に

開始する前に、必要なスコープを使用して、Salesforce Data Cloud で Data Cloud Ingestion API の接続アプリケーションを作成します。

Salesforce Data Cloud には、少なくとも *Manage user data via APIs (api)* スコープと *Manage Data Cloud Ingestion API data (cdp_ingest_api)* スコープが必要です。

データをロードするには、取り込み API データストリームを作成する必要もあります。

接続アプリケーションを設定し、コンシューマキーとコンシューマシークレットを取得して、アクセストークンを生成します。

これらの手順の詳細については、Salesforce Data Cloud のマニュアルを参照してください。

接続の詳細

次の表に、基本接続プロパティを示します。

財産	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。

財産	説明
シークレットコンテナの使用	<p>組織に対して設定されている Secrets Manager にこの接続の機密資格情報を保存します。このプロパティは、組織に Secrets Manager が設定されている場合にのみ表示されます。このプロパティは、データ取り込みおよびレプリケーションとデータアクセス管理サービスではサポートされていません。</p> <p>接続でシークレットコンテナを有効にすると、Secure Agent が Secrets Manager からどの資格情報を取得するかを選択できます。このオプションを無効にした場合、資格情報は組織の設定方法に応じてリポジトリまたはローカル Secure Agent に保存されます。</p> <p>注: この接続を使用してプッシュダウンまたはプロキシサービスを介してデータアクセスポリシーを適用する場合、シークレットコンテナ設定オプションを使用することはできません。</p> <p>Secrets Manager を設定および使用方法については、Administrator のヘルプにある「Secrets Manager の設定」を参照してください。</p>
ランタイム環境	<p>タスクを実行するランタイム環境の名前。</p> <p>Secure Agent、ホステッドエージェント、またはエラスティックランタイム環境を選択します。</p> <p>ランタイム環境の設定および使用方法の詳細については、Administrator のヘルプにある「ランタイム環境」を参照してください。</p>
認証タイプ	<p>Salesforce Data Cloud に接続するための認証方法。</p> <p>デフォルトは OAuth 2.0 クライアント資格情報です。</p>
アクセストークン URL	<p>Salesforce Data Cloud インスタンスに接続するためのアクセストークンを取得するために OAuth 2.0 要求が送信されるエンドポイント。</p> <p>URL の形式は次のとおりです: <code>https://<Salesforce Data Cloud 組織 ID>my.salesforce.com/services/oauth2/token</code></p>
クライアント ID	<p>Salesforce Data Cloud に接続するためのアプリケーションのクライアント ID。</p>
クライアントシークレット	<p>クライアント ID と関連付けられたクライアントシークレット。</p>
アクセストークン	<p>アクセストークンの値。</p> <p>[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入力します。</p>

詳細設定

次の表に、詳細接続のプロパティを示します。

プロパティ	説明
再試行回数	Salesforce Data Cloud エンドポイントから応答を取得するまでの総再試行回数。 正の整数を入力してください。 デフォルトは 3 です。
再試行間隔	Salesforce Data Cloud 接続が応答の受信をもう一度試みることができるまでの待機時間（ミリ秒単位）。 正の整数を入力してください。 デフォルトは 3000 ミリ秒です。
詳細プロパティ	Salesforce Data Cloud 接続で設定できる追加の接続プロパティ（再試行ステータスコード、接続タイムアウト、読み取りタイムアウト、書き込みタイムアウトなど）。 各プロパティを key=value の形式で、アンパサンドとコロンの組み合わせ(&:)で区切って入力してください。タイムアウト値は正の整数でなければなりません デフォルトは okhttp.retryStatusCodes=429,500,502,503,504&: okhttp.connectTimeout=30&:okhttp.readTimeout=30&:okhttp.writeTimeout=30 です。

第 189 章

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。
シークレットコンテナの使用	組織に対して設定されている Secrets Manager にこの接続の機密資格情報を保存します。このプロパティは、組織に Secrets Manager が設定されている場合にのみ表示されます。このプロパティは、データ取り込みおよびレプリケーションとデータアクセス管理サービスではサポートされていません。 接続でシークレットコンテナを有効にすると、Secure Agent が Secrets Manager からどの資格情報を取得するかを選択できます。このオプションを無効にした場合、資格情報は組織の設定方法に応じてリポジトリまたはローカル Secure Agent に保存されます。 注: この接続を使用してプッシュダウンまたはプロキシサービスを介してデータアクセスポリシーを適用する場合、シークレットコンテナ設定オプションを使用することはできません。 Secrets Manager を設定および使用する方法については、Administrator のヘルプにある「Secrets Manager の設定」を参照してください。
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。 セキュアエージェント、ホステッドエージェント、サーバーレスランタイム環境、またはエラスティックランタイム環境を選択します。 アプリケーション取り込みとレプリケーションタスクで、セキュアエージェントを選択するか、初期ロードジョブの場合に限り、サーバーレスランタイム環境を選択できます。ホステッドエージェントまたはエラスティックランタイム環境は使用できません。 ランタイム環境の設定および使用方法の詳細については、Administrator のヘルプにある「ランタイム環境」を参照してください。

プロパティ	説明
Salesforce Marketing Cloud の URL	<p>エージェントが Salesforce Marketing Cloud WSDL への接続に使用する URL。</p> <p>次に、OAuth 1.0 URL の URL の例を示します。</p> <p><code>https://webservice.s7.exacttarget.com/etframework.wsdl</code></p> <p>次に、OAuth 2.0 URL の URL の例を示します。</p> <p><code>https://<SUBDOMAIN>.soap.marketingcloudapis.com/etframework.wsdl</code></p> <p>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。</p>
ユーザー名	<p>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。</p> <p>注: このプロパティは、アプリケーション取り込みとレプリケーションタスク用に設定された接続には適用されません。</p>
パスワード	<p>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。</p> <p>注: このプロパティは、アプリケーション取り込みとレプリケーションタスク用に設定された接続には適用されません。</p>
クライアント ID	<p>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。</p>
クライアント シークレット	<p>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。</p>
プロキシサーバーを使用	<p>プロキシを経由して Salesforce Marketing Cloud に接続します。</p> <p>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。</p> <p>注: このプロパティは、アプリケーション取り込みとレプリケーションタスク用に設定された接続には適用されません。</p>
ロギングの有効化	<p>タスクのロギングを有効にします。</p> <p>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。</p> <p>注: このプロパティは、アプリケーション取り込みとレプリケーションタスク用に設定された接続には適用されません。</p>
UTC オフセット	<p>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。</p> <p>注: このプロパティは、アプリケーション取り込みとレプリケーションタスク用に設定された接続には適用されません。</p>
バッチサイズ	<p>エージェントがバッチでターゲットに書き込む行数。</p> <p>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。</p> <p>注: このプロパティは、アプリケーション取り込みとレプリケーションタスク用に設定された接続には適用されません。</p>
複数の BU の有効化	<p>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。</p> <p>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。</p> <p>注: このプロパティは、アプリケーション取り込みとレプリケーションタスク用に設定された接続には適用されません。</p>

第 190 章

Salesforce Mass Ingestion 接続のプロパティ

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

Salesforce Mass Ingestion の接続は、接続されたアプリケーションを使用して Salesforce データにアクセスします。接続を設定する前に、Salesforce の接続アプリケーションを設定して、接続が Salesforce データにアクセスできるようにする必要があります。

注: 接続アプリケーションの設定の詳細については、ナレッジベース記事「[000172095](#)」を参照してください。

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

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

OAuth 2.0 ユーザー名パスワードフロー認証の接続プロパティ

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

接続プロパティ	説明
接続名	接続の名前。この名前は、組織内で一意にする必要があります。接続名には、英数字、スペース、および次のような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。
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。 アプリケーション取り込みとレプリケーションタスクでは、Secure Agent またはサーバーレスランタイム環境を選択できます。ホステッドエージェントは使用できません。
ユーザー名	Salesforce アカウントのユーザー名。

接続プロパティ	説明
パスワード	Salesforce アカウントのパスワード。
セキュリティトークン	<p>Salesforce アカウントに関連付けられたセキュリティトークン。</p> <p>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。</p> <p>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。</p>
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	<p>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。</p> <p>デフォルトは 51.0 です。</p> <p>注: 51.0 より古いバージョンは使用できません。</p>
OAuth トークン URL	<p>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。</p> <p>デフォルト値は次のとおりです。</p> <p><code>https://login.salesforce.com/services/oauth2/token</code></p> <p>このデフォルト URL は、すべての Salesforce インスタンスに使用されます。</p> <p>または、インスタンス固有の URL を入力できます。</p> <p><code>https://<instance domain URL>/services/oauth2/token</code></p> <p>インスタンス固有の URL を使用すると、Salesforce ホストサーバーへのより直接的で高速な接続を確立できます。共通のデフォルトエンドポイントの負荷が高く、共通のデフォルトエンドポイントの使用時に取り込みジョブが認証エラーで失敗する場合は、代わりにこの代替 URL を使用してください。</p>

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

OAuth 2.0 JWT ベアラーフロー認証の接続プロパティ

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

接続プロパティ	説明
接続名	<p>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、および次のような特殊文字を含めることができます: <code>_ . + -</code></p> <p>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。</p>
説明	接続の説明（オプション）。最大長は 255 文字です。

接続プロパティ	説明
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。 アプリケーション取り込みとレプリケーションタスクでは、Secure Agent またはサーバーレスランタイム環境を選択できます。ホステッドエージェントは使用できません。
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。
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。 <code>https://login.salesforce.com/services/oauth2/token</code> このデフォルト URL は、すべての Salesforce インスタンスに使用されます。 または、インスタンス固有の URL を入力できます。 <code>https://<instance domain URL>/services/oauth2/token</code> インスタンス固有の URL を使用すると、Salesforce ホストサーバーへのより直接的で高速な接続を確立できます。共通のデフォルトエンドポイントの負荷が高く、共通のデフォルトエンドポイントの使用時に取り込みジョブが認証エラーで失敗する場合は、代わりにこの代替 URL を使用してください。 タスクで Bulk API 1.0 を使用して Salesforce ソースからデータを取り込む予定の場合は、インスタンス固有の URL を指定する必要があります。

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。

第 191 章

Salesforce Pardot 接続のプロパティ

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

次の表に、Salesforce Pardot 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。
シークレットコンテナの使用	組織に対して設定されている Secrets Manager にこの接続の機密資格情報を保存します。 このプロパティは、組織に Secrets Manager が設定されている場合にのみ表示されます。 このプロパティは、データ取り込みおよびレプリケーションとデータアクセス管理サービスではサポートされていません。 接続でシークレットコンテナを有効にすると、Secure Agent が Secrets Manager からどの資格情報を取得するかを選択できます。このオプションを無効にした場合、資格情報は組織の設定方法に応じてリポジトリまたはローカル Secure Agent に保存されます。 注: この接続を使用してプッシュダウンまたはプロキシサービスを介してデータアクセスポリシーを適用する場合、シークレットコンテナ設定オプションを使用することはできません。 Secrets Manager を設定および使用する方法については、Administrator のヘルプにある「Secrets Manager の設定」を参照してください。
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。 Secure Agent、ホステッドエージェント、またはエラスティックランタイム環境を指定します。 ランタイム環境の設定および使用方法の詳細については、Administrator のヘルプにある「ランタイム環境」を参照してください。

プロパティ	説明
認証	Salesforce Pardot オブジェクトにアクセスするための認証方法。
認証 URL	<p>ユーザー要求を認証して認証コードを取得するために使用される Salesforce Pardot サーバーエンドポイント。</p> <p>認証 URL は、https://login.salesforce.com/services/oauth2/authorize です。</p>
アクセストークン URL	<p>認証コードをアクセストークンに交換するために使用される Salesforce Pardot アクセストークンエンドポイント。</p> <p>アクセストークン URL は、https://login.salesforce.com/services/oauth2/token です。</p>
クライアント ID	登録プロセス中に作成される Salesforce Pardot 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	登録プロセス中に作成される Salesforce Pardot 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	アクセストークンに付与されたアクセスのスコープ。
アクセストークン	データにアクセスするために Salesforce Pardot によって生成されたアクセストークン。
更新トークン	新しいアクセストークンを取得するための更新トークン。
Pardot ビジネスユニット ID	データの読み取り元となる Salesforce Pardot ビジネスユニットの ID。
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。
認証コードパラメータ	認証 URL で使用する追加パラメータ。

第 192 章

SAP 接続プロパティ

SAP 接続を作成して、Intermediate Document (IDoc) または BAPI/RFC インタフェースを介して SAP からデータにアクセスします。

タイプとして **[SAP]** を選択した場合は、**[SAP 接続タイプ]** リストから次の接続を設定できます。

- IDoc Reader
- IDoc Writer
- SAP RFC/BAPI インタフェース

前提条件

SAP 接続を使用する前に、SAP 管理者は前提条件のタスクを実行して Secure Agent マシンと SAP システムを設定する必要があります。

IDoc および SAP BAPI/RFC 機能进行处理するには、必要なライセンスが SAP システムで有効になっているかどうかを確認する必要があります。

SAP ライブラリのダウンロードと設定

中間ドキュメント (IDocs) または BAPI/RFC インタフェースを介して SAP データにアクセスするには、Secure Agent マシンで SAP NetWeaver RFC SDK ライブラリと SAP JCo ライブラリをダウンロードして設定する必要があります。ライブラリのダウンロードで問題が発生した場合は、SAP カスタマサポートにお問い合わせください。

1. [SAP Support Portal](#) に移動し、**[ソフトウェアのダウンロード]** をクリックします。
注: [SAP Support Portal](#) から **[ソフトウェアのダウンロード]** にアクセスするには、SAP 資格情報が必要です。
2. Secure Agent をホストするオペレーティングシステムに固有の最新バージョンの SAP NetWeaver RFC SDK 7.50 ライブラリをダウンロードします。

次の表に、各オペレーティングシステムに対応するライブラリを示します。

オペレーティングシステム	SAP NetWeaver RFC SDK ライブラリ
Linux 64	<ul style="list-style-type: none"> - libicudata.so.50 - libicui18n.so.50 - libicuuc.so.50 - libsapnwrfc.so - libsapucum.so
Windows 64	<ul style="list-style-type: none"> - icudt50.dll - icuin50.dll - icuuc50.dll - libsapucum.dll - sapnwrfc.dll

3. SAP NetWeaver RFC SDK 7.50 ライブラリを次のディレクトリにコピーします。
<Informatica Secure Agent installation directory>\apps\Data_Integration_Server\ext\deploy_to_main\bin\rdtm
存在しない場合は、deploy_to_main\bin\rdtm ディレクトリを作成します。
4. SAP NetWeaver RFC SDK ライブラリごとに以下の権限を設定します。
 - 現在のユーザーに読み取り、書き込みおよび実行権限。
 - 他のすべてのユーザーに読み取りおよび実行権限。
5. Secure Agent を実行しているマシンのオペレーティングシステムに基づいて、[SAP Support Portal](#) から最新バージョンの 64 ビット SAP JCo ライブラリをダウンロードします。

Secure Agent システム	SAP JCo ライブラリ
Windows	sapjco3.jar sapjco3.dll
Linux	sapjco3.jar libsapjco3.so

6. 次のディレクトリに JCo ライブラリをコピーします。
<Informatica Secure Agent installation directory>\apps\Data_Integration_Server\ext\deploy_to_main\bin\rdtm-extra\tpl\sap
存在しない場合は、deploy_to_main\bin\rdtm-extra\tpl\sap ディレクトリを作成します。
7. Informatica Intelligent Cloud Services にログインし、Secure Agent の JAVA_LIBS プロパティを設定します。
 - a. **[Administrator]** > **[ランタイム環境]** の順に選択します。
 - b. **[ランタイム環境]** をクリックして、**[ランタイム環境]** ページにアクセスします。
 - c. エージェント名の左側で、**[Secure Agent の編集]** をクリックします。
 - d. **[サービス]** リストから、**[データ統合サーバー]** を選択します。
 - e. **[タイプ]** リストから、**[Tomcat JRE]** を選択します。

- f. Secure Agent を実行しているマシンのオペレーティングシステムに基づいて、JAVA_LIBS 値を入力します。

オペレーティングシステム	値
Windows	../bin/rdtm-extra/tpl/sap/sapjco3.jar;../bin/rdtm/javaliib/sap/sap-adapter-common.jar
Linux	../bin/rdtm-extra/tpl/sap/sapjco3.jar../bin/rdtm/javaliib/sap/sap-adapter-common.jar

警告: テーブルから値を直接コピーすると、値のハイフン (-) が誤ってコピーされることがあります。値をテキストエディタにコピーし、コピーした値が破損していないことを確認します。

System Configuration Details Reset All

Service: Data Integration Server ▼

Type: Tomcat JRE ▼

Type	Name	Value
Tomcat JRE	JAVA_LIBS	../bin/rdtm-extra/tpl/sap/sapjco3.jar;../bin/rdtm/javaliib/sap/sap-adc

- g. **【保存】** をクリックします。
- h. Secure Agent をインストールしたすべてのマシンで手順 2 - 7 を繰り返します。
8. Secure Agent を再起動します。

SAP ユーザー権限の設定

SAP システムで SAP ユーザーアカウントを設定して、中間ドキュメント (IDocs) および BAPI/RFC インタフェースを介したデータの交換を有効にします。

実行時に SAP とデータのやり取りをする場合に役立つ IDoc と SAP BAPI/RFC 機能进行处理するには、SAP に権限オブジェクトを追加する必要があります。また、処理するトランザクションの特定の IDoc および SAP BAPI/RFC 関数にアクセスする必要もあります。

次の表に、IDoc および SAP BAPI/RFC 関数进行处理するために必要な権限を示します。

関数	オブジェクト名	認証
SAP BAPI/RFC	S_RFC	SYST、SDTX、SDIFRUNTIME、RFC_METADATA、RFC1、RFC2、ABAP4_COMMIT_WORK、BAPI_TRANSACTION_COMMIT
IDoc	S_RFC	SYST、SDTX、SDIFRUNTIME、RFC1、RFC2、EDIMEXT

SAP システムで SAP ユーザー認証を設定する方法の詳細については、「[SAP user authorizations](#)」を参照してください。

sapnwrfc.ini ファイルの設定

SAP は、RFC (Remote Function Call) という通信プロトコルを使用して外部のシステムとデータのやり取りを行います。

SAP IDoc または SAP BAPI/RFC インタフェースを介して SAP に対する読み取りまたは書き込みを行う場合は、SAP IDoc または SAP BAPI/RFC 関数进行处理してデータの転送を容易にする sapnwrfc.ini ファイルが必要です。

sapnwrfc.ini ファイルを作成し、SAP 接続タイプに必要な接続情報と RFC 固有のパラメータを含めます。DOS エディタまたはワードパッドを使用して sapnwrfc.ini ファイルを作成すると、メモ帳で頻繁に発生するエラーを回避できます。さまざまな接続タイプに使用できる sapnwrfc.ini ファイルのサンプルの詳細については、「[「接続タイプのサンプル sapnwrfc.ini ファイル」 \(ページ 708\)](#)」を参照してください。

sapnwrfc.ini ファイルを作成した後に、エージェントディレクトリに sapnwrfc.ini ファイルを配置する必要があります。エージェントは sapnwrfc.ini ファイルを検証し、設定された接続にそのファイルを使用します。

エージェントディレクトリへの sapnwrfc.ini ファイルの配置

次のように、Secure Agent またはサーバーレスランタイム環境を使用して、RFC クライアントとして SAP システムに接続できます。

- Secure Agent を使用するには、sapnwrfc.ini ファイルを次の場所に配置します。
<Informatica Secure Agent installation directory>\apps\Data_Integration_Server\ext\deploy_to_main\bin\rdtm\
- サーバーレスランタイム環境を使用するには、sapnwrfc.ini ファイルを次の場所に配置します。
\\data2\home\cldagnt\SystemAgent\apps\Data_Integration_Server\ext\deploy_to_main\bin\rdtm\

注: deploy_to_main\bin\rdtm ディレクトリが存在することを確認します。ディレクトリが存在しない場合は、ディレクトリを作成してからファイルを配置します。

必要なディレクトリにファイルを配置した後に、エージェントを再起動します。

以前のバージョンからのアップグレード

以前のバージョンからアップグレードする場合は、sapnwrfc.ini ファイルを作成する必要はありません。Secure Agent は、sapnwrfc.ini ファイルを deploy_to_main\bin\rdtm ディレクトリにコピーします。

sapnwrfc.ini ファイルの確認

ユーザーが接続を作成すると、Secure Agent は最初に、sapnwrfc.ini ファイルがディレクトリ内に存在するかどうかを確認します。sapnwrfc.ini ファイルが存在する場合、Secure Agent は sapnwrfc.ini ファイルを使用します。存在しない場合は、例外が発生します。

接続タイプのサンプル sapnwrfc.ini ファイル

sapnwrfc.ini ファイルを使用して、次のタイプの接続を設定できます。

SAP アプリケーションサーバーへの接続

この接続を作成し、RFC クライアントと SAP システムの間の通信を有効にします。それぞれの接続エントリは、1 つのアプリケーションサーバーと 1 つの SAP システムを指定します。

以下の例に、sapnwrfc.ini ファイルの特定の SAP アプリケーションサーバーの接続エントリを示します。

```
DEST=sapr3  
ASHOST=sapr3  
SYSNR=00
```

SAP 負荷分散のための接続

この接続を作成し、SAP が実行時の負荷が最も低いアプリケーションサーバーへの RFC 接続を作成できるようにします。SAP 負荷分散を使用する場合は、この接続を使用します。

以下の例に、sapnwrfc.ini ファイルの SAP 負荷分散の接続エントリを示します。

```
DEST=sapr3  
R3NAME=ABV  
MSHOST=infamessageserver.informatica.com  
GROUP=INFADDEV
```

SAP ゲートウェイで登録されている RFC サーバプログラムへの接続

この接続を作成して、受信する送信 IDoc のソースとなる SAP システムに接続します。

以下の例に、sapnwrfc.ini ファイルの SAP ゲートウェイで登録されている RFC サーバープログラムの接続エントリを示します。

```
DEST=sapr346CLSQA
PROGRAM_ID=PID_LSRECEIVE
GWHOST=sapr346c
GWSERV=sapgw00
```

さまざまな接続タイプに対して、sapnwrfc.ini ファイルで次のようなパラメータを設定できます。

sapnwrfc.ini のパラメータ	説明	適用できる接続タイプ
DEST	接続用の SAP システムの論理名。 すべての DEST エントリは一意にする必要があります。SAP システムごとに DEST エントリを 1 つだけ設定する必要があります。 バージョン 4.6C 以降の SAP の場合は、最大文字数が 32 文字です。バージョン 4.6C より前のバージョンの場合は、最大文字数は 8 文字です。	このパラメータは、以下のタイプの接続に使用します。 - 特定の SAP アプリケーションサーバーへの接続 - 負荷分散を使用する接続 - SAP ゲートウェイで登録されている RFC サーバープログラムへの接続
ASHOST	SAP アプリケーションのホスト名または IP アドレス。Secure Agent はこのエントリを使用して、アプリケーションサーバーに接続します。	このパラメータを使用して、特定の SAP アプリケーションサーバーへの接続を作成します。
SYSNR	SAP システム番号。	このパラメータを使用して、特定の SAP アプリケーションサーバーへの接続を作成します。
R3NAME	SAP システムの名称。	このパラメータを使用して、SAP 負荷分散を使用する接続を作成します。
MSHOST	SAP メッセージサーバーのホスト名。	このパラメータを使用して、SAP 負荷分散を使用する接続を作成します。
GROUP	SAP アプリケーションサーバーのグループ名。	このパラメータを使用して、SAP 負荷分散を使用する接続を作成します。
PROGRAM_ID	プログラム ID。プログラム ID は、IDoc を送受信するために SAP システムで定義した論理システムのプログラム ID と同一であることが必要です。	このパラメータを使用して、SAP ゲートウェイで登録されている RFC サーバープログラムへの接続を作成します。
GWHOST	SAP ゲートウェイのホスト名。	このパラメータを使用して、SAP ゲートウェイで登録されている RFC サーバープログラムへの接続を作成します。

sapnwrfc.ini のパラメータ	説明	適用できる接続タイプ
GWSERV	SAP ゲートウェイのサーバー名。	このパラメータを使用して、SAP ゲートウェイで登録されている RFC サーバープログラムへの接続を作成します。
TRACE	RFC 接続関連の問題をデバッグします。トレースに求める詳細レベルに基づいて、以下のいずれかの値を設定します。 - 0. オフ - 1. Brief - 2. Verbose - 3. フル	このパラメータは、以下のタイプの接続に使用します。 - 特定の SAP アプリケーションサーバーへの接続 - 負荷分散を使用する接続 - SAP ゲートウェイで登録されている RFC サーバープログラムへの接続

次のスニペットは、sapnwrfc.ini ファイルの例を示しています。

```

/*=====*/
/* Connection to an RFC server program registered at an SAP gateway */
/*=====*/
DEST=<destination in RfcRegisterServer>
PROGRAM_ID=<program-ID, optional; default: destination>
GWHOST=<host name of the SAP gateway>
GWSERV=<service name of the SAP gateway>
/*=====*/
/* Connection to a specific SAP application server */
/*=====*/
DEST=<destination in RfcOpenConnection>
ASHOST=<Host name of the application server.>
SYSNR=<The back-end system number.>
/*=====*/
/* Connection to use SAP load balancing */
/* The application server will be determined at run time. */
/*=====*/
DEST=<destination in RfcOpenConnection>
R3NAME=<name of SAP system, optional; default: destination>
MSHOST=<host name of the message server>
GROUP=<group name of the application servers, optional; default: PUBLIC>

```

SAP の論理システムとしての SAP コネクタの定義

SAP との間で IDoc を送受信するには、SAP コネクタを SAP の外部論理システムとして定義する必要があります。

SAP コネクタを外部論理システムとして定義するには、SAP コネクタとの IDoc ALE 統合のために SAP で単一の論理システムを作成し、SAP コネクタと通信するための SAP システム内の tRFC ポートで設定された RFC 接続先を作成します。

外部論理システムを識別するには、作成した論理システムのパートナープロファイルを作成する必要もあります。

SAP コネクタを論理システムとして定義すると、SAP は、SAP から送信 IDoc を受け取り、SAP に受信 IDoc を送信する外部システムとして SAP コネクタを承認します。

注: これらの手順は、SAP バージョン 4.6C に適用されます。別のバージョンを使用する場合は、手順が異なる場合があります。SAP で論理システムを作成する方法の詳細については、SAP のマニュアルを参照してください。

SAP コネクタの論理システムの作成

SAP コネクタをネットワーク内のクライアントとして一意に識別するには、SAP コネクタを SAP の外部論理システムとして定義する必要があります。

1. SAP にログインし、SALE トランザクションに移動します。
2. **[IMG の表示]** ウィンドウでツリーを展開し、**[アプリケーションリンクの有効化]** > **[送信および受信システム]** > **[論理システム]** > **[論理システムの定義]** 操作に移動します。
3. **[IMG - Activity]** アイコンをクリックして、**[論理システムの定義]** 操作を実行します。
情報ダイアログボックスが表示されます。
4. **[Enter]** をクリックします。
[Change View Logical Systems] ウィンドウが表示されます。
5. **[New Entries]** をクリックします。
6. **[新しいエントリ]** ウィンドウで、SAP コネクタの論理システムエントリの名前と説明を入力します。

RFC 宛先の作成

論理システムを作成した後に、SAP システムで SAP コネクタの RFC 接続先とプログラム ID を作成する必要があります。

1. トランザクション SM59 に進みます。
2. **[RFC 接続先の表示と管理]** ウィンドウで、**[作成]** をクリックします。
[RFC 宛先] ウィンドウが表示されます。
3. RFC 宛先として、作成した論理システムの名前を入力します。
4. TCP/IP 接続を作成するには、接続タイプとして「T」を入力します。
5. RFC 宛先の説明を入力します。
6. **[保存]** をクリックします。
7. 起動タイプについては、**[登録]** をクリックします。
8. プログラム ID については、RFC 宛先名と同じ名前を入力します。
saprfc.ini ファイルの PROGRAM_ID パラメータの値として、このプログラム ID を使用します。

RFC 接続先に対する tRFC ポートの作成

SAP コネクタの RFC 接続先とプログラム ID を作成した後に、SAP で定義した RFC 接続先の tRFC ポートを作成する必要があります。SAP では、tRFC ポートを使用して SAP コネクタと通信します。

1. トランザクション WE21 に進みます。
2. **[ポート]** > **[トランザクション RFC]** をクリックします。
3. **[登録]** をクリックします。
[Ports in IDoc Processing] ダイアログボックスが表示されます。
4. **[ポート名の生成]** または **[Own Port Name]** をクリックして、名前を入力します。
5. **[Enter]** をクリックします。
6. ポートの説明を入力します。
7. IDoc レコードのバージョンタイプを選択します。
8. 作成した RFC 宛先の名前を入力します。

SAP コネクタのパートナープロファイルの作成

SAP コネクタ用に定義した論理システムのパートナープロファイルを作成します。SAP は、外部システムと通信する際に、パートナープロファイルを使用して外部システムを特定します。

1. トランザクション WE20 に進みます。
2. **【登録】** をクリックします。
3. 以下のプロパティを入力します。

パートナープロファイルプロパティ	説明
パートナ番号	SAP コネクタに対して作成した論理システムの名前。
パートナタイプ	パートナープロファイルタイプ。ALE 分散システム用の論理システムの場合は、「LS」と入力します。

4. **【後処理】** タブで、次のプロパティを入力します。

パートナープロファイルプロパティ	説明
タイプ	ユーザータイプ。ユーザの場合は US を入力します。
エージェント	SAP ユーザーのログイン名。
言語	SAP 言語に対応する言語コード。日本語の場合は JA を入力します。

5. **【分類】** タブで、次のプロパティを入力します。

パートナープロファイルプロパティ	説明
パートナクラス	ALE を入力します。
パートナステータス	パートナとの通信の状態を示します。パートナと通信するには、「A」を入力してアクティブにします。

パートナープロファイルへの受信パラメータおよび送信パラメータの作成

SAP コネクタにパートナープロファイルを定義した後に、パートナープロファイルに送信パラメータと受信パラメータを作成する必要があります。

送信パラメータでは、IDoc のメッセージタイプ、IDoc の基本タイプ、および送信 IDoc 用のポート番号を定義します。受信パラメータでは、受信 IDoc の IDoc メッセージタイプを定義します。

SAP は、IDoc を SAP コネクタに送信するときに、送信パラメータを使用します。SAP が SAP コネクタに送信する IDoc のメッセージタイプごとに送信パラメータを作成します。SAP は SAP コネクタから IDoc を受け取る際に、受信パラメータを使用します。SAP が SAP コネクタから受け取る IDoc のメッセージタイプごとに受信パラメータを作成します。

1. **【パートナープロファイル】** ウィンドウから、**【送信パラメータの登録】** をクリックします。

2. **【パートナープロファイル: 送信パラメータ】** ウィンドウで、次のプロパティを入力します。

送信パラメータのプロパティ	説明
メッセージタイプ	SAP システムが SAP コネクタに送信する IDoc メッセージタイプ。
受信ポート	定義した tRFC ポート番号。
IDoc タイプ	SAP システムが SAP コネクタに送信する IDoc の基本タイプ。

3. **【保存】** をクリックします。
【パケットサイズ】 プロパティが表示されます。
4. パケットサイズとして、10 から 200 までの IDoc の値を入力します。
パケットサイズによって、SAP が 1 つのパケットで SAP コネクタに送信する IDoc の数が決まります。
5. **【Enter】** をクリックします。
6. 手順 1 から 5 までを繰り返して、SAP が SAP コネクタに送信する IDoc メッセージタイプごとに送信パラメータを作成します。
7. **【受信パラメータの登録】** をクリックします。
8. **【パートナープロファイル: 受信パラメータ】** ウィンドウで、次のプロパティを入力します。

受信パラメータのプロパティ	説明
メッセージタイプ	SAP システムが SAP コネクタから受け取る IDoc メッセージタイプ。
プロセスコード	プロセスコード。SAP システムはプロセスコードを使用して、SAP システムが受け取る IDoc を処理するための関数モジュールを呼び出します。

9. **【Enter】** をクリックします。
10. 手順 7 から 9 までを繰り返して、SAP システムが SAP コネクタから受け取る IDoc メッセージタイプごとに受信パラメータを作成します。

SAP 接続

中間ドキュメント (IDocs) または BAPI/RFC インタフェースを介して SAP に接続するように SAP 接続プロパティを設定してみましょう。

始める前に

開始する前に、Secure Agent マシンと SAP システムを設定して SAP 接続を確立する必要があります。

これらのタスクの詳細については、「[「前提条件」 \(ページ 705\)](#)」を参照してください。

接続の詳細

次の表に、基本接続プロパティを示します。

財産	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。
シークレットコンテナの使用	組織に対して設定されている Secrets Manager にこの接続の機密資格情報を保存します。 このプロパティは、組織に Secrets Manager が設定されている場合にのみ表示されます。 このプロパティは、データ取り込みおよびレプリケーションとデータアクセス管理サービスではサポートされていません。 接続でシークレットコンテナを有効にすると、Secure Agent が Secrets Manager からどの資格情報を取得するかを選択できます。このオプションを無効にした場合、資格情報は組織の設定方法に応じてリポジトリまたはローカル Secure Agent に保存されます。 注: この接続を使用してプッシュダウンまたはプロキシサービスを介してデータアクセスポリシーを適用する場合、シークレットコンテナ設定オプションを使用することはできません。 Secrets Manager を設定および使用する方法については、Administrator のヘルプにある「Secrets Manager の設定」を参照してください。
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。 Secure Agent、またはサーバーレスランタイム環境を選択します。 サーバーレス環境の設定の詳細については、 「サーバーレスランタイム環境の使用」 (ページ 716) を参照してください。

SAP 接続タイプ

IDoc Reader、IDoc Writer、および SAP RFC/BAPI インタフェースの接続タイプを設定して、中間ドキュメント (IDocs) および BAPI/RFC インタフェースを介して SAP のデータにアクセスできます。
必要な SAP 接続タイプを選択し、接続固有のパラメータを設定します。

SAP IDoc Reader 接続

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、IDoc Reader 接続の基本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	sapnwrfc.ini ファイルで指定された SAP アプリケーションサーバーの DEST エントリ。 この接続先エントリのプログラム ID と、IDoc を受信するために SAP システムで定義した論理システムのプログラム ID が同じであることを確認してください。 sapnwrfc.ini ファイルの詳細については、「 sapnwrfc.ini ファイルの設定 」(ページ 707)を参照してください。
コードページ	IDoc インタフェースを介して SAP データの読み取りを行うときに接続で定義される SAP アプリケーションサーバーのコードページ。 リストから次のいずれかのコードページを選択します。 <ul style="list-style-type: none"> - 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

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、IDoc Writer 接続の基本接続プロパティを示します。

プロパティ	説明
ユーザー名	SAP アカウントに接続するための適切なユーザー権限を持つユーザー名。
パスワード	SAP アカウントに接続するためのパスワード。
宛先エントリ	sapnwrfc.ini ファイルで指定された SAP アプリケーションサーバーの DEST エントリ。 sapnwrfc.ini ファイルの詳細については、「 sapnwrfc.ini ファイルの設定 」(ページ 707)を参照してください。
コードページ	IDoc インタフェースを介して SAP データの書き込みを行うときに接続で定義される SAP アプリケーションサーバーのコードページ。 リストから次のいずれかのコードページを選択します。 <ul style="list-style-type: none"> - 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。

プロパティ	説明
言語コード	SAP 言語に対応する言語コード。 接続先の SAP システムから必要な言語コードを取得します。
クライアントコード	SAP アプリケーションサーバーのクライアント番号。 接続先の SAP システムから必要なクライアント番号を取得します。

SAP RFC/BAPI インタフェース接続

SAP RFC/BAPI インタフェースを介して SAP データの読み取りまたは書き込みを行うには、**[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の基本接続プロパティを示します。

プロパティ	説明
ユーザー名	SAP アカウントに接続するための適切なユーザー権限を持つユーザー名。
パスワード	SAP アカウントに接続するためのパスワード。
宛先エントリ	sapnwrfc.ini ファイルで指定された SAP アプリケーションサーバーの DEST エントリ。 sapnwrfc.ini ファイルの詳細については、 「sapnwrfc.ini ファイルの設定」 (ページ 707) を参照してください。
コードページ	SAP RFC/BAPI インタフェースを介して SAP データの読み取りまたは書き込みを行うときに接続で定義される SAP アプリケーションサーバーのコードページ。 リストから次のいずれかのコードページを選択します。 <ul style="list-style-type: none"> - 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	SAP 言語に対応する言語コード。 接続先の SAP システムから必要な言語コードを取得します。
クライアントコード	SAP サーバーのクライアント番号。 接続先の SAP システムから必要なクライアント番号を取得します。

サーバーレスランタイム環境の使用

Linux で SAP 接続の設定時に、AWS または Azure でホストされているサーバーレスランタイム環境を使用して SAP システムに接続できます。

SAP Secure Network Communication (SNC) プロトコルを使用する場合、サーバーレスランタイム環境を使用することはできません。

サーバーレスランタイム環境を使用して SAP 接続を設定する前に、次のタスクを実行してください。

- AWS または Azure アカウントの Amazon S3 バケットあるいは Azure コンテナに SAP ライブラリを追加します。
- .yaml サーバーレス構成ファイルを設定する。
- Linux 上のサーバーレスランタイム環境の JAVA_LIBS プロパティを設定します。

AWS または Azure アカウントの Amazon S3 バケットあるいは Azure コンテナに SAP ライブラリを追加します

サーバーレスランタイム環境で SAP 接続を設定するには、次の手順を実行します。

1. AWS または Azure のサーバーレスエージェント設定用に次の構造を作成します: <補足ファイルの場所>/serverless_agent_config
2. AWS アカウントまたは Azure アカウントの次の場所にある Amazon S3 バケットあるいは Azure コンテナに SAP ライブラリを追加します: <補足ファイルの場所>/serverless_agent_config/sap

.yaml サーバーレス構成ファイルを設定する

次の手順を実行して、サーバーレスランタイム環境で.yaml サーバーレス構成ファイルを設定し、SAP ライブラリをサーバーレスエージェントディレクトリにコピーします。

1. 次のコードスニペットをテキストエディタにコピーします。

```
version: 1
agent:
  dataIntegrationServer:
    autoDeploy:
      sap:
        nwrfdc:
          - fileCopy:
              sourcePath: sap/nwrfdc/<rfc_library_filename>
          - fileCopy:
              sourcePath: sap/nwrfdc/<sapnwrfdc_filename>
```

ここで、ソースパスは AWS または Azure のライブラリファイルのディレクトリパスです。

2. 構文とインデントが有効であることを確認してから、ファイルを serverlessUserAgentConfig.yaml として次の AWS または Azure の場所に保存します: <補足ファイルの場所>/serverless_agent_config.yaml ファイルの実行時に、ライブラリが AWS または Azure の場所からサーバーレスエージェントディレクトリにコピーされます。

サーバーレスランタイム環境の JAVA_LIBS プロパティを設定する

Administrator で次の手順を実行して、Linux 上のサーバーレスランタイム環境に JAVA_LIBS プロパティを設定します。

1. Informatica Intelligent Cloud Services にログインします。
2. **[Administrator]** > **[サーバーレス環境]** の順に選択します。
3. **[サーバーレス環境]** タブで、必要なサーバーレスランタイム環境の **[アクション]** メニューを展開し、**[編集]** を選択します。
4. **[ランタイム設定のプロパティ]** タブで、サービスに **[データ統合サーバー]** を選択し、タイプに **[Tomcat_JRE]** を選択します。
5. **[プロパティの追加]** をクリックします。
6. **[名前]** フィールドに JAVA_LIBS と入力し、次の値を設定します。
../bin/rdtm-extra/tpl/sap/sapjco3.jar:../bin/rdtm/javajlib/sap/sap-adapter-common.jar
7. **[保存]** をクリックします。

サーバーレス環境の設定および使用方法の詳細については、Administrator のヘルプにある「ランタイム環境」の「サーバーレスランタイム環境のセットアップ」を参照してください。

第 193 章

SAP ADSO Writer 接続のプロパティ

[SAP ADSO Writer] 接続のセットアップ時に、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。

プロパティ	説明
接続名	接続の名称。 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。
シークレットコンテナの使用	組織に対して設定されている Secrets Manager にこの接続の機密資格情報を保存します。 このプロパティは、組織に Secrets Manager が設定されている場合にのみ表示されます。 このプロパティは、データ取り込みおよびレプリケーションとデータアクセス管理サービスではサポートされていません。 接続でシークレットコンテナを有効にすると、Secure Agent が Secrets Manager からどの資格情報を取得するかを選択できます。このオプションを無効にした場合、資格情報は組織の設定方法に応じてリポジトリまたはローカル Secure Agent に保存されます。 注: この接続を使用してプッシュダウンまたはプロキシサービスを介してデータアクセスポリシーを適用する場合、シークレットコンテナ設定オプションを使用することはできません。 Secrets Manager を設定および使用する方法については、Administrator のヘルプにある「Secrets Manager の設定」を参照してください。

プロパティ	説明
ランタイム環境	<p>タスクを実行するランタイム環境の名前。</p> <p>Secure Agent、サーバーレスランタイム環境、またはエラスティックランタイム環境を選択します。</p> <p>ランタイム環境の設定および使用方法の詳細については、Administrator のヘルプにある「ランタイム環境」を参照してください。</p>
SAP サーバー接続タイプ	<p>使用する SAP サーバー接続タイプ。</p> <p>次のオプションから選択します。</p> <ul style="list-style-type: none"> - 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: <ul style="list-style-type: none"> - 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。 <p>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。</p>

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	<p>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。</p> <pre>jco.client.trace="1"; jco.client.cpic_trace="3";</pre> <p>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</p>

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が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	<p>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。</p> <pre>jco.client.trace="1"; jco.client.cpic_trace="3";</pre> <p>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</p>

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。 <ul style="list-style-type: none"> - 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、 <i>[3 - プライバシー保護（整合性と認証）を適用]</i> 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	<p>X509 証明書ファイルへのパス。</p> <p>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。</p> <p>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。</p>
追加パラメータ	<p>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。</p> <pre>jco.client.trace="1"; jco.client.cpic_trace="3";</pre> <p>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。</p> <p><Informatica Secure Agent installation directory>\apps\Data_Integration_Server\<DIS version>\ICS\main\bin\rdtm</p> <p>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。</p> <p><Informatica Secure Agent installation directory>\apps\Data_Integration_Server\<DIS version>tomcat.out</p>

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	<p>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。</p> <p>デフォルトの長さは 256 です。</p>
SNC パートナー名	<p>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。</p> <p>デフォルトの長さは 256 です。</p>
SNC 保護品質 (QoP)	<p>SAP PSE または証明書名を指定します。</p> <p>以下のオプションから選択できます。</p> <ul style="list-style-type: none"> - 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。 <p>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。</p>

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

第 194 章

SAP BAPI 接続のプロパティ

SAP BAPI 関数を使用して SAP からデータにアクセスするための SAP BAPI 接続を作成します。

前提条件

SAP BAPI 接続を使用する前に、SAP 管理者は特定の前提条件のタスクを実行して Secure Agent マシンと SAP システムを設定する必要があります。

また、SAP BAPI 機能を処理するには、必要なライセンスが SAP システムで有効になっているかどうかを確認する必要があります。

SAP ライブラリのダウンロードと設定

SAP BAPI 関数を使用して SAP データにアクセスするには、Secure Agent マシンに SAP JCo ライブラリをダウンロードして設定を行う必要があります。ライブラリのダウンロードで問題が発生した場合は、SAP カスタマサポートにお問い合わせください。

1. [SAP Support Portal](#) に移動し、[ソフトウェアのダウンロード] をクリックします。
注: [SAP Support Portal](#) から [ソフトウェアのダウンロード] にアクセスするには、SAP 資格情報が必要です。
2. Secure Agent を実行しているマシンのオペレーティングシステムに基づいて、最新バージョンの 64 ビット SAP JCo ライブラリをダウンロードします。

オペレーティングシステム	SAP JCo ライブラリ
Windows	- sapjco3.jar - sapjco3.dll
Linux	- sapjco3.jar - libsapjco3.so

3. 次のディレクトリに JCo ライブラリをコピーします。
<Informatica Secure Agent installation directory>\apps\Data_Integration_Server\ext\deploy_to_main\bin\rdtm-extra\tpl\sap
存在しない場合は、deploy_to_main\bin\rdtm-extra\tpl\sap ディレクトリを作成します。

4. Informatica Intelligent Cloud Services にログインし、Secure Agent の JAVA_LIBS プロパティを設定します。
 - a. **[Administrator]** > **[ランタイム環境]** の順に選択します。
 - b. **[ランタイム環境]** をクリックして、**[ランタイム環境]** ページにアクセスします。
 - c. エージェント名の左側で、**[Secure Agent の編集]** をクリックします。
 - d. **[サービス]** リストから、**[データ統合サーバー]** を選択します。
 - e. **[タイプ]** リストから、**[Tomcat JRE]** を選択します。
 - f. Secure Agent を実行しているマシンのオペレーティングシステムに基づいて、JAVA_LIBS 値を入力します。

オペレーティングシステム	値
Windows	..\bin\rdtm-extra\tpl\sap\sapjco3.jar;..\bin\rdtm\javalib\sap\sap-adapter-common.jar
Linux	../bin/rdtm-extra/tpl/sap/sapjco3.jar../bin/rdtm/javalib/sap/sap-adapter-common.jar

警告: テーブルから値を直接コピーすると、値のハイフン (-) が誤ってコピーされることがあります。値をテキストエディタにコピーし、コピーした値が破損していないことを確認します。

System Configuration Details Reset All

Service: Data Integration Server ▼

Type: Tomcat JRE ▼

Type	Name	Value
Tomcat JRE	JAVA_LIBS	../bin/rdtm-extra/tpl/sap/sapjco3.jar../bin/rdtm/javalib/sap/sap-adapter-common.jar

- g. **[保存]** をクリックします。
 - h. Secure Agent をインストールしたすべてのマシンで手順 2 - 4 を繰り返します。
5. Secure Agent を再起動します。

SAP ユーザー権限の設定

SAP BAPI 関数を使用したデータ交換を有効にするには、SAP システムで SAP ユーザーアカウントを設定します。

次の表に、SAP BAPI 関数を使用してデータにアクセスし、データを処理するためのユーザー権限を設定するために必要なオブジェクトと権限を示します。

読み取りオブジェクト名	認証
S_RFC	SYST、SDTX、SDIFRUNTIME、RFC1、RFC2

これらの権限とその使用方法の詳細については、「[SAP user authorizations](#)」を参照してください。

SAP BAPI への接続

SAP に接続して SAP BAPI 関数を使用してデータを処理するように SAP BAPI 接続プロパティを設定してみましょう。

始める前に

開始する前に、SAP BAPI 接続を確立するように Secure Agent マシンと SAP システムを設定する必要があります。

これらのタスクの詳細については、「[「前提条件」 \(ページ 724\)](#)」を参照してください。

接続の詳細

次の表に、基本接続プロパティを示します。

財産	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。
シークレットコンテナの使用	組織に対して設定されている Secrets Manager にこの接続の機密資格情報を保存します。 このプロパティは、組織に Secrets Manager が設定されている場合にのみ表示されます。 このプロパティは、データ取り込みおよびレプリケーションとデータアクセス管理サービスではサポートされていません。 接続でシークレットコンテナを有効にすると、Secure Agent が Secrets Manager からどの資格情報を取得するかを選択できます。このオプションを無効にした場合、資格情報は組織の設定方法に応じてリポジトリまたはローカル Secure Agent に保存されます。 注: この接続を使用してプッシュダウンまたはプロキシサービスを介してデータアクセスポリシーを適用する場合、シークレットコンテナ設定オプションを使用することはできません。 Secrets Manager を設定および使用する方法については、Administrator のヘルプにある「Secrets Manager の設定」を参照してください。
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。 Secure Agent、サーバーレスランタイム環境、またはエラスティックランタイム環境を選択します。 サーバーレス環境の設定の詳細については、「 「サーバーレスランタイム環境の設定」 (ページ 728) 」を参照してください。 エラスティック環境の設定の詳細については、「 「エラスティックランタイム環境の設定」 (ページ 729) 」を参照してください。
認証	SAP システムにアクセスし、SAP BAPI 関数を使用してデータを処理するための認証タイプ。 [BAPI 接続] 認証タイプを選択し、認証固有のパラメータを設定します。
ユーザー名	SAP アカウントに接続するための適切なユーザー権限を持つユーザー名。
パスワード	SAP アカウントに接続するためのパスワード。

財産	説明
ホスト名	接続する SAP サーバーのホスト名または IP アドレス。
クライアント	SAP サーバーのクライアント番号。 接続先の SAP システムから必要なクライアント番号を取得します。
言語	SAP 言語に対応する言語コード。 接続先の SAP システムから必要な言語コードを取得します。
システム番号	SAP サーバーのシステム番号。 接続先の SAP システムから必要なシステム番号を取得します。

詳細設定

次の表に、詳細接続のプロパティを示します。

プロパティ	説明
SAP の追加パラメータ	<p>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 プロパティ。</p> <p>このフィールドを使用して接続の追加パラメータを設定する次の例を参照してください。</p> <ul style="list-style-type: none"> - 負荷分散接続を作成するには、次のサンプルに一覧表示されている追加の引数を定義します。 GROUP=interfaces MSHOST=<Message server hostname> R3NAME=<System ID or name of SAP system> SAP は、ユーザーが指定したパラメータを基に接続タイプを推測します。例えば、ユーザーが GROUP、MSHOST、および R3NAME パラメータを定義すると、SAP は接続タイプがロードバランシング接続であると推測します。GROUP パラメータは SAP アプリケーションサーバーのグループ名を定義し、MSHOST パラメータは SAP メッセージサーバーのホスト名を定義します。R3NAME パラメータは、SAP システムのシステム ID または名前を定義します。 - 各 BAPI/RFC 呼び出しで SAP システムにデータをコミットするには、DOCOMMIT=true パラメータを定義します。 - セキュアネットワークコミュニケーション（SNC）プロトコルを使用して接続を作成するには、必要な追加パラメータを定義します。 <p>詳細については、Informatica How-To ライブラリの記事 「How to configure the SAP Secure Network Communication protocol」 を参照してください。</p> <p>専用の接続フィールドと 【SAP の追加パラメータ】 フィールドの両方でプロパティを指定した場合、【SAP の追加パラメータ】 フィールドで指定した値が優先されます。</p> <p>SAP パラメータの詳細については、SAP のマニュアルを参照してください。</p>
Jco トレース	<p>SAP システムによる JCo 呼び出しを追跡するかどうかを決定します。</p> <p>デフォルトは [無効] です。デフォルトでは、SAP 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ません。</p> <p>JCo トレースを有効にすると、次のディレクトリから JCo トレースファイルにアクセスできます。</p> <pre><Informatica Secure Agent のインストールディレクトリ>\apps\Data_Integration_Server \<latest_version>\ICS\main\bin\rdtm</pre>

ビジネスサービスとしての SAP BAPI コネクタの設定

マッピングまたはマッピングタスクの Web サービストランスフォーメーションで SAP BAPI 接続を使用し、SAP BAPI コネクタをビジネスサービスとして使用します。

詳細については、Informatica How-To ライブラリの記事

「[How to configure SAP BAPI Connector as a business service](#)」を参照してください。

サーバーレスランタイム環境の設定

Linux で SAP BAPI 接続を設定するときに、AWS または Azure でホストされているサーバーレスランタイム環境を使用して SAP システムに接続できます。

SAP Secure Network Communication (SNC) プロトコルを使用する予定がある場合、サーバーレスランタイム環境を使用することはできません。

サーバーレスランタイム環境を使用して SAP BAPI 接続を設定する前に、次のタスクを実行してください。

- AWS または Azure アカウントの Amazon S3 バケットあるいは Azure コンテナに SAP ライブラリを追加します。
- .yaml サーバーレス構成ファイルを設定する。
- Linux 上のサーバーレスランタイム環境の JAVA_LIBS プロパティを設定します。

AWS または Azure アカウントの Amazon S3 バケットあるいは Azure コンテナに SAP ライブラリを追加します

サーバーレスランタイム環境で SAP BAPI 接続を設定するには、次の手順を実行します。

1. AWS または Azure のサーバーレスエージェント設定用に次の構造を作成します: <補足ファイルの場所>/serverless_agent_config
2. AWS アカウントまたは Azure アカウントの次の場所にある Amazon S3 バケットあるいは Azure コンテナに SAP ライブラリを追加します: <補足ファイルの場所>/serverless_agent_config/sap

.yaml サーバーレス構成ファイルを設定する

次の手順を実行して、サーバーレスランタイム環境で.yaml サーバーレス構成ファイルを設定し、SAP ライブラリをサーバーレスエージェントディレクトリにコピーします。

1. 次のコードスニペットをテキストエディタにコピーします。

```
version: 1
agent:
  dataIntegrationServer:
    autoDeploy:
      sap:
        jco:
          - fileCopy:
              sourcePath: sap/jco/<sapjco_library_filename>
          - fileCopy:
              sourcePath: sap/jco/<sapjco_library_filename>
```

ここで、ソースパスは AWS または Azure のライブラリファイルのディレクトリパスです。

2. 構文とインデントが有効であることを確認してから、ファイルを serverlessUserAgentConfig.yaml として次の AWS または Azure の場所に保存します: <補足ファイルの場所>/serverless_agent_config.yaml ファイルの実行時に、SAP ライブラリが AWS または Azure の場所からサーバーレスエージェントディレクトリにコピーされます。

サーバーレスランタイム環境の JAVA_LIBS プロパティを設定する

Administrator で次の手順を実行して、Linux 上のサーバーレスランタイム環境の JAVA_LIBS プロパティと JVMClassPath プロパティを設定します。

1. Informatica Intelligent Cloud Services にログインします。
2. **[Administrator]** > **[サーバーレス環境]** の順に選択します。
3. **[サーバーレス環境]** タブで、必要なサーバーレスランタイム環境の **[アクション]** メニューを展開し、**[編集]** を選択します。
4. **[ランタイム設定のプロパティ]** タブで、サービスに **[データ統合サーバー]** を選択し、タイプに **[Tomcat_JRE]** を選択します。
5. **[プロパティの追加]** をクリックします。
6. **[名前]** フィールドに JAVA_LIBS と入力し、次の値を設定します。
../bin/rdtm-extra/tpl/sap/sapjco3.jar:../bin/rdtm/javajlib/sap/sap-adapter-common.jar
7. **[保存]** をクリックします。

サーバーレスランタイム環境の設定および使用方法の詳細については、Administrator のヘルプにある「サーバーレスランタイム環境」を参照してください。

エラスティックランタイム環境の設定

マッピング実行中にエラスティックランタイム環境がカスタムバイナリファイルにアクセスして実行できるよう、ランタイム環境でこれらのファイルを設定することができます。

カスタムバイナリファイルを設定する前に、Informatica Intelligent Cloud Services 内でデータを処理できる Kubernetes クラスタを作成できるエラスティックランタイム環境を必ず AWS にデプロイしてください。

エラスティックランタイム環境のデプロイの詳細については、「[Deploy an elastic runtime environment](#)」を参照してください。

エラスティックランタイム環境をデプロイした後、マウントされたディスクにカスタムバイナリファイルを配置し、使用するバイナリファイルの正確なパスを POST 要求内にコピーします。

カスタムバイナリファイルを管理するには、Informatica Intelligent Cloud Services for Elastic Runtime Environment 内で以下の手順を実行します。

1. 組織にログインし、セッション ID とランタイム環境 ID を取得します。
2. REST API への POST 呼び出しを、セッション ID、ランタイム環境 ID、および、マウントされたディスクから以前にコピーしたバイナリファイルのパスを渡して行います。
POST 呼び出しの詳細については、『REST API リファレンス』ガイド内の「[Supplementary files](#)」を参照してください。

POST 要求の例を以下に示します。

```
POST <base URL>/api/v3/RuntimeEnvironment/<runtime environment ID>/ElasticConfig
Content-Type: application/json
Accept: application/json
INFA-SESSION-ID: <SessionId>
{
  "rteId": "rte-12345",
  "specification": {
    "agent": {
      "dataIntegrationServer": {
        "sap": {
          "jcos": [{"sourcePath": "/<path to binaries>/jco1"}],
```

```
"nwrfs": [{"sourcePath": "<path to binaries>/nwrfs1"}],  
"hanas": [{"sourcePath": "<path to binaries>/hana1"}]  
}
```

この POST 呼び出しにより、データ統合サーバーの再起動がトリガーされます。

3. Administrator でデータ統合サーバーの状態を確認することで、エラスティックランタイム環境が起動されて稼働していることを確認します。
4. 接続をテストするかマッピングを実行することで、エラスティックランタイム環境がカスタムバイナリファイルにアクセスして使用できることを確認します。

第 195 章

SAP BW コネクタ接続プロパティ

SAP BW および SAP BW/4HANA アプリケーションの SAP BW オブジェクトからデータを安全に読み取るための SAP BW コネクタ接続を作成します。

前提条件

SAP BW 接続を使用する前に、SAP 管理者は特定の前提条件のタスクを実行して Secure Agent マシンと SAP システムを設定する必要があります。

また、SAP BW データを処理するには、必要なライセンスが SAP システムで有効になっているかどうかを確認する必要があります。

SAP ライブラリのダウンロードと設定

SAP BW オブジェクトからデータの読み取りを行うには、Secure Agent マシンに SAP JCo ライブラリをダウンロードして設定する必要があります。ライブラリのダウンロードで問題が発生した場合は、SAP カスタマサポートにお問い合わせください。

1. [SAP Support Portal](#) に移動し、[ソフトウェアのダウンロード] をクリックします。

注: [SAP Support Portal](#) から [ソフトウェアのダウンロード] にアクセスするには、SAP 資格情報が必要です。

2. Secure Agent を実行しているマシンのオペレーティングシステムに基づいて、最新バージョンの 64 ビット SAP JCo ライブラリをダウンロードします。

オペレーティングシステム	SAP JCo ライブラリ
Windows	- sapjco3.jar - sapjco3.dll
Linux	- sapjco3.jar - libsapjco3.so

3. 次のディレクトリに JCo ライブラリをコピーします。

```
<Informatica Secure Agent installation directory>\apps\Data_Integration_Server\ext\deploy_to_main\bin  
\rdtm-extra\tpl\sap
```

存在しない場合は、deploy_to_main\bin\rdtm-extra\tpl\sap ディレクトリを作成します。

4. Informatica Intelligent Cloud Services にログインし、Secure Agent の JAVA_LIBS プロパティを設定します。
 - a. **[Administrator]** > **[ランタイム環境]** の順に選択します。
 - b. **[ランタイム環境]** をクリックして、**[ランタイム環境]** ページにアクセスします。
 - c. エージェント名の左側で、**[Secure Agent の編集]** をクリックします。
 - d. **[サービス]** リストから、**[データ統合サーバー]** を選択します。
 - e. **[タイプ]** リストから、**[Tomcat JRE]** を選択します。
 - f. Secure Agent を実行しているマシンのオペレーティングシステムに基づいて、JAVA_LIBS 値を入力します。

オペレーティングシステム	値
Windows	..\bin\rdtm-extra\tpl\sap\sapjco3.jar;..\bin\rdtm\javalib\sap\sap-adapter-common.jar
Linux	../bin/rdtm-extra/tpl/sap/sapjco3.jar../bin/rdtm/javalib/sap/sap-adapter-common.jar

警告: テーブルから値を直接コピーすると、値のハイフン (-) が誤ってコピーされることがあります。値をテキストエディタにコピーし、コピーした値が破損していないことを確認します。

System Configuration Details Reset All

Service: Data Integration Server ▼

Type: Tomcat JRE ▼

Type	Name	Value
Tomcat JRE	JAVA_LIBS	..\bin\rdtm-extra\tpl\sap\sapjco3.jar;..\bin\rdtm\javalib\sap\sap-adc

- g. **[保存]** をクリックします。
5. JAVA_LIBS 値を保存した後に、Secure Agent の JVMClassPath プロパティを設定します。
 - a. **[サービス]** リストから、**[データ統合サーバー]** を選択します。
 - b. **[タイプ]** リストで、**[DTM]** を選択します。
 - c. Secure Agent を実行しているマシンのオペレーティングシステムに基づいて、JVMClassPath 値を入力します。

オペレーティングシステム	値
Windows	pmserver sdk.jar;..\bin\rdtm-extra\tpl\sap\sapjco3.jar;..\bin\rdtm\javalib\sap\sap-adapter-common.jar
Linux	pmserver sdk.jar../bin/rdtm-extra/tpl/sap/sapjco3.jar../bin/rdtm/javalib/sap/sap-adapter-common.jar

警告: テーブルから値を直接コピーすると、値のハイフン (-) が誤ってコピーされることがあります。値をテキストエディタにコピーし、コピーした値が破損していないことを確認します。

System Configuration Details
Reset All

Service:
Data Integration Server

Type:
DTM

Type	Name	Value
DTM	JVMClassPath	pmserversdk.jar:../bin/rdtm-extra/tpl/sap/sapjco3.jar:../bin/rdtm/

- d. **【保存】** をクリックします。
 - e. Secure Agent をインストールしたすべてのマシンで手順 2 - 5 を繰り返します。
6. Secure Agent を再起動します。

SAP ユーザー権限の設定

SAP システムで SAP ユーザー権限を設定し、InfoCubes、InfoSets、MultiProviders、および DataStore オブジェクトなどの SAP BW オブジェクトにアクセスし、読み取りを行います。

次の表に、SAP BW にアクセスしてデータの読み取りを行うためのユーザー権限の設定に必要な権限オブジェクト、フィールド、および値を示します。

権限オブジェクト	フィールド	値
S_RFC	RFC_TYPE	FUNC、FUGR
	RFC_NAME	/INFADI/BWRDR、/INFADI/ZTEST_COMMUNICATION、BAPI_CUBE_GETLIST、DDIF_FIELDINFO_GET、BAPI_IOBJ_GETDETAIL、RFCPING、RFC_GET_FUNCTION_INTERFACE、RSAB、SYST
	ACTVT	16
S_BTCH_JOB	JOBACTION	RELE
	JOBGROUP	*
S_RS_ADMWB	RSADMWBOBJ	データの読み取りを行う Administrator Workbench オブジェクト名を指定します。 Administrator Workbench オブジェクトの詳細については、SAP のドキュメントを参照してください。
	ACTVT	3
S_RS_ICUBE	RSINFOAREA	アクセスするインフォエリア名を入力します。 インフォエリアの詳細については、SAP のドキュメントを参照してください。
	RSINFOCUBE	アクセスするインフォキューブオブジェクト名を指定します。 インフォキューブの詳細については、SAP のドキュメントを参照してください。

権限オブジェクト	フィールド	値
	RSIRSICUBE OBJ	DEFINITION、DATA、UPDATERULE
	ACTVT	3

また、次の権限オブジェクトを追加して、SAP BW にアクセスしてデータの読み取りを行うためのユーザー権限を設定することもできます。

- BAPI_ODSO_GETLIST および BAPI_ISET_GETLIST オプションの RFC オブジェクトを持つ S_RFC 権限オブジェクト。
- アクティビティ値 ACTVT=3 を持つ S_RS_ISET および S_RS_ODSO 権限オブジェクト。

これらのオブジェクトとその使用方法の詳細については、「[SAP user authorizations](#)」を参照してください。

SAP BW へのトランスポートファイルのインストール

SAP BW や SAP BW/4HANA などの Unicode SAP システムの SAP BW オブジェクトからデータを読み取るには、SAP BW トランスポートファイルを Secure Agent ディレクトリから SAP システムにインストールします。

トランスポートファイルをインストールするための前提条件

SAP BW トランスポートをインストールする前に、次の前提条件のタスクを必ず実行してください。

- SAP マシンにインストールしたトランスポートファイルが最新のものであることを確認します。次のディレクトリから最新のトランスポートファイルを取得します:
 <Informatica Secure Agent installation directory>\downloads\package-bwreader.<Latest version>\package\rdtm\sap-transport\SAPBWReader
- 本番システムにトランスポートをインストールする前に、開発システムにトランスポートをインストールしてテストしてください。

以下の表に、アクセスする SAP BW ソースタイプに基づいてインストールする必要があるトランスポートを一覧で示します。

データおよび Co ファイル名	トランスポート要求	機能
RUN_BWRDR_R900723.g00 RUN_BWRDR_K900723.g00	g00K900723	SAP BW アプリケーションの SAP ADSO InfoCube、InfoSets、または MultiProviders オブジェクトからデータを読み込むには、RUN_BWRDR トランスポートをインストールします。 SAP NetWeaver BW バージョン 7.x の RUN_BWRDR トランスポートを使用します。
BW4HANA_R900164.B42 BW4HANA_K900164.B42	B42K900164	SAP BW/4HANA アプリケーションの SAP ADSO または CompositeProviders オブジェクトからデータを読み込むには、BW4HANA トランスポートをインストールします。

トランスポートファイルのインストール

SAP BW トランスポートファイルをインストールするには、次のタスクを実行します。

1. トランスポートファイルは、Secure Agent マシンの次のディレクトリにあります:
 <Informatica Secure Agent installation directory>\downloads\package-bwreader.<Latest version>\package\rdtm\sap-transport\SAPBWReader

2. アクセスする各 SAP マシンの SAP トランスポート管理ディレクトリにある Cofile ディレクトリに、cofile トランスポートファイルをコピーします。
cofile トランスポートファイルでは、RUN_BWRDR_K<number>.g00 命名規則を使用します。
3. ファイル名から「RUN_BWRDR_」を削除して、cofile の名前を変更します。例えば、RUN_BWRDR_K900723.g00 という名前の cofile トランスポートファイルの場合、ファイル名を K900723.g00 に変更します。
4. アクセスする各 SAP マシンの SAP トランスポート管理ディレクトリにある Data ディレクトリにデータトランスポートファイルをコピーします。
データトランスポートファイルでは、RUN_BWRDR_R<number>.g00 命名規則を使用します。
5. ファイル名から「RUN_BWRDR_」を削除して、ファイルの名前を変更します。
例えば、RUN_BWRDR_R900723.g00 という名前のデータトランスポートファイルの場合、ファイル名を R900723.g00 に変更します。
6. STMS でトランスポートを SAP にインポートするには、**[補足]** > **[その他の依頼]** > **[追加]** をクリックし、トランスポート要求をシステムキューに追加します。
7. **[インポートキューに移送依頼追加]** ダイアログボックスに、cofile トランスポートの要求番号を入力します。
要求番号は、名前変更された cofile の順番を g00K<number>のように反転させたものです
例えば、K900723.g00 と名前変更された cofile トランスポートファイルの場合、要求番号として「g00K900723」と入力します。
8. インポートキューの要求領域で、追加したトランスポート要求番号を選択し、**[インポート]** をクリックします。

SAP BW への接続

SAP BW および SAP BW/4HANA アプリケーションに接続して SAP BW オブジェクトからデータを読み取るように、SAP BW 接続プロパティを設定しましょう。

始める前に

開始する前に、Secure Agent マシンと SAP システムを設定して SAP BW 接続を確立する必要があります。

これらのタスクの詳細については、「[「前提条件」 \(ページ 731\)](#)」を参照してください。

接続の詳細

次の表に、基本接続プロパティを示します。

財産	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。

財産	説明
シークレットコンテナの使用	<p>組織に対して設定されている Secrets Manager にこの接続の機密資格情報を保存します。このプロパティは、組織に Secrets Manager が設定されている場合にのみ表示されます。このプロパティは、データ取り込みおよびレプリケーションとデータアクセス管理サービスではサポートされていません。</p> <p>接続でシークレットコンテナを有効にすると、Secure Agent が Secrets Manager からどの資格情報を取得するかを選択できます。このオプションを無効にした場合、資格情報は組織の設定方法に応じてリポジトリまたはローカル Secure Agent に保存されます。</p> <p>注: この接続を使用してプッシュダウンまたはプロキシサービスを介してデータアクセスポリシーを適用する場合、シークレットコンテナ設定オプションを使用することはできません。</p> <p>Secrets Manager を設定および使用する方法については、Administrator のヘルプにある「Secrets Manager の設定」を参照してください。</p>
ランタイム環境	<p>タスクを実行するランタイム環境の名前。</p> <p>Secure Agent を選択します。</p>
ユーザー名	SAP BW アカウントに接続するための適切なユーザー権限を持つユーザー名。
パスワード	SAP BW アカウントに接続するためのパスワード。

接続タイプ

SAP BW および SAP BW/4HANA アプリケーションへの接続タイプとしてアプリケーションおよび負荷分散を設定できます。

必要な接続タイプを選択し、接続固有のパラメータを設定します。

アプリケーション接続

アプリケーション接続は、SAP アカウント名、パスワード、クライアント番号、ホスト名、システム番号、および言語コードが必要なデフォルトのタイプです。

次の表に、アプリケーション接続の基本的な接続プロパティとその説明を示します。

接続プロパティ	説明
ホスト名	接続する 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	<p>SAP BW サーバーのシステム番号。</p> <p>接続先の SAP システムから必要なシステム番号を取得します。</p>
クライアント	<p>SAP BW サーバーのクライアント番号。</p> <p>接続先の SAP システムから必要なクライアント番号を取得します。</p>
言語	<p>SAP 言語に対応する言語コード。</p> <p>接続先の SAP システムから必要な言語コードを取得します。</p>

詳細設定

次の表に、アプリケーション接続の詳細接続プロパティとその説明を示します。

プロパティ	説明
トレース	<p>SAP システムによる JCo 呼び出しを追跡するかどうかを決定します。</p> <p>0 から 8 までのいずれかの値を入力します。</p> <p>デフォルトでは、SAP 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ません。デフォルトは 0 です。</p> <p>トレースレベル値の追加情報については、「Setting up an SAP Java Connector (SAP JCo) and Related Traces」を参照してください。</p> <p>トレースファイルは以下のディレクトリからアクセスできます。</p> <ul style="list-style-type: none"> - 設計時の情報: <Informatica Secure Agent のインストールディレクトリ>\apps\Data_Integration_Server\<最新のバージョン>\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	<p>SAP BW データの読み取りを行うときに使用できる追加の JCo 接続パラメータ。</p> <p>複数の JCo 接続パラメータをセミコロンで区切って、次の形式で入力できます。</p> <p><parameter name1>=<value1>;<parameter name2>=<value2>;<parameter name3>=<value3>....</p> <p>例えば、SAP SNC 接続を作成する場合は、次の追加パラメータを入力します。</p> <p>SNC_MODE=1;SNC_QOP=3;SNC_MYNAME=p:CN=<Common name>, OU=<Organizational unit>, O=<Organization>, C=<Country>;SNC_PARTNERNAME=p:CN=<Common name>, OU=<Organizational unit>, O=<Organization>, C=<Country>;SNC_LIB=C:\SNC_11\sapcrypto.dll;TRACE=1</p>
ポート範囲	<p>HTTP ポート範囲。SAP BW 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 BW テーブルに接続します。デフォルトの範囲は 10000-65535 です。</p> <p>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。</p>
HTTPS の使用	<p>HTTPS プロトコルを使用して SAP に接続します。</p> <p>HTTPS 経由で SAP に接続するには、管理者が Secure Agent マシンと SAP システムに HTTPS を設定していることを確認してください。</p> <p>HTTPS 経由で SAP に接続する方法の詳細については、「SAP に接続するための HTTPS の設定」(ページ 740)を参照してください。</p>
キーストア の場所	<p>SAP に接続するキーストアファイルのパスとファイル名。</p> <p>パスとファイル名を次の形式で入力します。</p> <p><ディレクトリ>/<キーストアファイル名>.jks</p>
キーストア のパスワード	<p>キーストアファイルにアクセスするためのパスワード。</p>

プロパティ	説明
プライベートキーのパスワード	.P12 ファイルにアクセスするためのエクスポートパスワード。
SAP の追加パラメータ	<p>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 プロパティ。</p> <p>Secure Agent が SAP に接続できるようにするために必要な RFC 固有のパラメータと接続情報を指定します。</p> <p>例えば、SNC 接続パラメータを、次のサンプルに示す追加の引数として指定できます。</p> <pre>MSHOST= <Message server hostname> GROUP=PUBLIC R3NAME=SLT SNC_MODE=1 SNC_QOP=3 SNC_MYNAME=p:CN=<Common name>, OU=<Organizational unit>, O=<Organization>, C=<Country> This is the SNC name of the Secure Agent machine. SNC_PARTNERNAME=p:CN=<Common name>, OU=<Organizational unit>, OU=SAP Web AS, O=<Organization>, C=<Country>. This is the SNC name of the SAP system. SNC_LIB =<Secure Agent installation directory>/apps/Data_Integration_Server/ext/deploy_to_main/bin/<libsapcrypto.so for Linux/sapcrypto.dll for Windows> X509CERT=<X509 certificate></pre> <p>SNC パラメータの詳細については、Informatica How-To ライブラリの記事「How to configure the SAP Secure Network Communication protocol」を参照してください。</p> <p>RFC 固有のパラメータの詳細については、SAP のマニュアルを参照してください。</p> <p>注: [SAP の追加パラメータ] フィールドと [追加パラメータ] フィールドの両方でパラメータを指定した場合、[SAP の追加パラメータ] フィールドで指定した値が優先されます。</p>

負荷分散接続

実行時の負荷が最も低い SAP BW サーバーに接続する場合、負荷分散接続を作成します。

負荷分散接続の作成時には、[接続の詳細] セクションにリストされているすべてのプロパティに加えて、[詳細設定] セクションにメッセージホスト名、R3 名/SysID、およびグループ値を入力する必要があります。

次の表に、負荷分散接続の基本的な接続プロパティとその説明を示します。

接続プロパティ	説明
ホスト名	接続する 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 BW サーバーのシステム番号。 接続先の SAP システムから必要なシステム番号を取得します。
クライアント	SAP BW サーバーのクライアント番号。 接続先の SAP システムから必要なクライアント番号を取得します。
言語	SAP 言語に対応する言語コード。 接続先の SAP システムから必要な言語コードを取得します。

詳細設定

次の表に、負荷分散接続の詳細接続プロパティとその説明を示します。

プロパティ	説明
メッセージ ホスト名	必須。負荷分散接続を使用する場合に接続する SAP メッセージサーバーのホスト名。
R3 名/SysID	必須。負荷分散接続を使用する場合に接続する SAP メッセージサーバーのシステム ID。
グループ	必須。負荷分散接続を使用する場合に接続に使用する SAP ログオングループの名前。
トレース	<p>SAP システムによる JCo 呼び出しを追跡するかどうかを決定します。</p> <p>0 から 8 までのいずれかの値を入力します。</p> <p>デフォルトでは、SAP 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ません。</p> <p>デフォルトは 0 です。</p> <p>トレースレベル値の追加情報については、 「Setting up an SAP Java Connector (SAP JCo) and Related Traces」 を参照してください。</p> <p>トレースファイルは以下のディレクトリからアクセスできます。</p> <ul style="list-style-type: none"> - 設計時の情報: <Informatica Secure Agent のインストールディレクトリ>\apps \<Data_Integration_Server>\<最新のバージョン>\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	<p>SAP BW データの読み取りを行うときに使用できる追加の JCo 接続パラメータ。</p> <p>複数の JCo 接続パラメータをセミコロンで区切って、次の形式で入力できます。</p> <p><parameter name1>=<value1>;<parameter name2>=<value2>;<parameter name3>=<value3>....</p> <p>例えば、SAP SNC 接続を作成する場合は、次の追加パラメータを入力します。</p> <p>SNC_MODE=1;SNC_QOP=3;SNC_MYNAME=p:CN=<Common name>, OU=<Organizational unit>, O=<Organization>, C=<Country>;SNC_PARTNERNAME=p:CN=<Common name>, OU=<Organizational unit>, O=<Organization>, C=<Country>;SNC_LIB=C:\SNC_11\sapcrypto.dll;TRACE=1</p>
ポート範囲	<p>HTTP ポート範囲。SAP BW 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 BW テーブルに接続します。デフォルトの範囲は 10000-65535 です。</p> <p>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。</p>
HTTPS の 使用	<p>HTTPS プロトコルを使用して SAP に接続します。</p> <p>HTTPS 経由で SAP に接続するには、管理者が Secure Agent マシンと SAP システムに HTTPS を設定していることを確認してください。</p> <p>HTTPS 経由で SAP に接続する方法の詳細については、「SAP に接続するための HTTPS の設定」 (ページ 740) を参照してください。</p>
キーストア の場所	<p>SAP に接続するキーストアファイルのパスとファイル名。</p> <p>パスとファイル名を次の形式で入力します。</p> <p><ディレクトリ>/<キーストアファイル名>.jks</p>
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。

プロパティ	説明
プライベートキーのパスワード	.P12 ファイルにアクセスするためのエクスポートパスワード。
SAP の追加パラメータ	<p>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 プロパティ。</p> <p>Secure Agent が SAP に接続できるようにするために必要な RFC 固有のパラメータと接続情報を指定します。</p> <p>例えば、SNC 接続パラメータを、次のサンプルに示す追加の引数として指定できます。</p> <pre>MSHOST= <Message server hostname> GROUP=PUBLIC R3NAME=SLT SNC_MODE=1 SNC_QOP=3 SNC_MYNAME=p:CN=<Common name>, OU=<Organizational unit>, O=<Organization>, C=<Country> This is the SNC name of the Secure Agent machine. SNC_PARTNERNAME=p:CN=<Common name>, OU=<Organizational unit>, OU=SAP Web AS, O=<Organization>, C=<Country>. This is the SNC name of the SAP system. SNC_LIB =<Secure Agent installation directory>/apps/Data_Integration_Server/ext/deploy_to_main/bin/<libsapcrypto.so for Linux/sapcrypto.dll for Windows> X509CERT=<X509 certificate></pre> <p>SNC パラメータの詳細については、Informatica How-To ライブラリの記事「How to configure the SAP Secure Network Communication protocol」を参照してください。</p> <p>RFC 固有のパラメータの詳細については、SAP のマニュアルを参照してください。</p> <p>注: [SAP の追加パラメータ] フィールドと [追加パラメータ] フィールドの両方でパラメータを指定した場合、[SAP の追加パラメータ] フィールドで指定した値が優先されます。</p>

SAP に接続するための HTTPS の設定

HTTPS 経由で SAP に接続し、SAP BW ソースから読み取りを行うには、Secure Agent マシンと SAP システムの両方で OpenSSL 証明書が使用可能であることを確認してください。

Secure Agent マシンで OpenSSL 証明書を作成します。次に、作成した証明書を PSE 形式で SAP システムトラストストアにインポートします。

さらに、SAP BW 接続で HTTPS を有効にするには、SAP BW 接続プロパティと SAP システムの両方で、キーストアファイルの生成キーストアパスワードとプライベートキーパスワードを指定する必要があります。

OpenSSL 証明書の作成

OpenSSL 証明書を作成する前に、前提条件のタスクを実行する必要があります。

- Secure Agent マシンに OpenSSL をダウンロードしてインストールします。
- Secure Agent と SAP システムをホストするマシンのオペレーティングシステムに基づき、SAPGENPSE 暗号化ツールの最新パッチを SAP Service Marketplace からダウンロードします。
デフォルトでは、SAPGENPSE ファイルは nt-x86_64 ディレクトリに抽出されます。
- SAP パラメータ icm/server_port、ssl/ssl_lib、sec/libsapsecu、ssf/ssfapi_lib、ssf/name、icm/HTTPS/verify_client、ssl/client_pse、wdisp/ssl_encrypt を設定します。
詳細については、SAP のマニュアルを参照してください。

OpenSSL を使用して自己署名証明書を作成するには、次のタスクを実行します。

1. コマンドラインから、OPENSSL_CONF 変数に openssl.cfg ファイルへの絶対パスを設定します。
例えば、コマンド `set OPENSSL_CONF= C:\OpenSSL-Win64\bin\openssl.cfg` を実行します。
2. <openssl installation directory>\bin ディレクトリに移動します。
3. 2048 ビットの RSA プライベートキーを生成するには、次のコマンドを実行します:
`openssl.exe req -new -newkey rsa:2048 -sha1 -keyout <RSAkey File_Name>.key -out <RSAkey File_Name>.csr`
4. プロンプトが表示されたら、次の値を入力します。
 - プライベートキーのパスワード (PEM パスフレーズ)。秘密鍵の暗号化に使用するフレーズを入力します。確認のためにパスワードを再入力します。
重要: この PEM パスワードを書き留めます。自己署名キーと PKCS#12 証明書の作成時に、このパスワードを指定する必要があります。
 - 国名の 2 文字のコード。
 - 都道府県または州の名前。
 - 市区町村名。
 - 組織名。
 - 組織単位名。
 - 共通名 (CN)。必須。
重要: Secure Agent をホストするマシンの完全修飾ホスト名を入力します。
 - 電子メールアドレス。
5. 必要に応じて、証明書要求とともに渡す次の属性を入力します。
 - チャレンジパスワード。
 - 会社名 (省略可能)。

2048 ビットの RSA プライベートキーが作成されます。指定したディレクトリに<RSAkey File_Name>.key および<RSAkey File_Name>.csr ファイルが生成されます。
6. RSA プライベートキーを使用して自己署名キーを生成するには、次のコマンドを実行します:
`openssl x509 -req -days 11499 -in <RSAkey File_Name>.csr -signkey <RSAkey File_Name>.key -out <Certificate File_Name>.crt`
7. プロンプトが表示されたら、RSA プライベートキーの PEM パスフレーズを入力します。
指定したディレクトリに<Certificate File_Name>.crt ファイルが生成されます。
8. <Certificate File_Name>.crt ファイルと<RSAkey File_Name>.key ファイルの内容を .pem ファイルに連結するには、次のタスクを実行します。
 - a. テキストエディタで<Certificate File_Name>.crt ファイルと<RSAkey File_Name>.key ファイルを開きます。
 - b. ファイルを作成して<PEM File_Name>.pem という名前で保存します。
 - c. <Certificate File_Name>.crt ファイルのコンテンツをコピーし、.pem ファイルに貼り付けます。
 - d. <RSAkey_Name>.key ファイルのコンテンツをコピーし、.pem ファイルの既存のコンテンツに追加します。
 - e. <PEM file name>.pem ファイルを保存します。
9. PKCS#12 証明書を作成するには、コマンドラインから次のコマンドを実行します:
`openssl pkcs12 -export -in <PEM File_Name>.pem -out <P12 File_Name>.p12 -name "domain name"`
10. プロンプトが表示されたら、次の詳細を入力します。
 - .pem ファイルの PEM パスフレーズ。

- P12 ファイルのエクスポートパスワード。確認のためにパスワードを再入力します。

重要: P12 ファイルのこのエクスポートパスワードを書き留めます。HTTPS 経由で SAP に接続するための Java キーストアファイルの作成時に、このパスワードを指定する必要があります。

指定した場所に<P12 File_Name>.p12 ファイルが生成されます。

11. Java キーストアファイルを作成するには、次のコマンドを入力します。

```
keytool -v -importkeystore -srckeystore <P12 File_Name>.p12 -srcstoretype PKCS12 -destkeystore <JKS File_Name>.jks -deststoretype JKS -srcalias "source alias" -destalias "destination alias"
```

12. プロンプトが表示されたら、次の詳細を入力します。

- ターゲットキーストアである JKS ファイルのパスワード。

重要: このパスワードを書き留めます。SAP BW 接続の作成時に、このパスワードを指定する必要があります。

- ソースキーストアである P12 ファイルのパスワード。P12 ファイルのエクスポートパスワードを入力します。

指定したディレクトリに<JKS File_Name>.jks ファイルが生成されます。

SAP BW 接続で HTTPS を有効にするときに、このキーストアファイルの名前と場所を指定します。また、SAP BW 接続プロパティおよび SAP システムで、[キーストアのパスワード] としてターゲットキーストアパスワードを指定し、[プライベートキーのパスワード] としてソースキーストアパスワードを指定する必要があります。

OpenSSL 証明書から PSE 形式への変換

OpenSSL 証明書を作成した後に、SAPGENPSE ツールを使用して OpenSSL 証明書を PSE 形式に変換する必要があります。

1. コマンドラインから、<SAPGENPSE 抽出ディレクトリ>ディレクトリに移動します。

2. PSE ファイルを生成するには、次のコマンドを実行します:

```
sapgenpse import_p12 -p <PSE_Directory>\<PSE File_Name>.pse <P12 Certificate_Directory>\<P12 File_Name>.p12
```

3. プロンプトが表示されたら、次の詳細を入力します。

- P12 ファイルのパスワード。P12 ファイルのエクスポートパスワードを入力します。
- PSE ファイルを保護するための個人識別番号 (PIN)。確認のために PIN を再入力します。

指定したディレクトリに<PSE File_Name>.pse ファイルが生成されます。

4. PSE 形式に基づいて証明書を生成するには、次のコマンドを実行します:

```
sapgenpse export_own_cert -p <PSE File_Directory>\<PSE File_Name>.pse -o <Certificate_Name>.crt
```

5. プロンプトが表示されたら、PSE PIN 番号を入力します。

指定した場所に<Certificate_Name>.crt ファイルが生成されます。この証明書ファイルを SAP システムのトラストストアにインポートします。

SAP システムでの HTTPS サービスの有効化

SAP システムに接続するように HTTPS を設定するには、SAP システムのトランザクションコード SAP ICM モニタ (SMICM) から HTTPS サービスを有効にする必要があります。

SAP システムで HTTPS サービスを有効にする方法の詳細については、SAP のマニュアルを参照してください。

SAP システムのトラストストアへの証明書のインポート

HTTPS 経由で SAP に接続するには、証明書を PSE 形式で SAP システムのトラストストアにインポートする必要があります。

1. SAP にログインし、STRUST トランザクションに移動します。
2. [SSL クライアント (標準)] を選択し、パスワードを指定します。
3. **【証明書のインポート】** ダイアログで、証明書ファイル形式として Base64 形式を選択します。
4. **【インポート】** アイコンをクリックし、PSE 形式の<Certificate_Name>.crt を選択します。

注: ユーザーが別の SAP ネットワークに存在する場合は、SAP アプリケーションサーバー上のエージェントホストの DNS エントリを追加する必要があります。

5. **【証明書リストに追加】** をクリックします。
6. インターネット通信マネージャを再起動します。

第 196 章

SAP BW BEx クエリ接続のプロパティ

SAP BW から SAP BW BEx クエリを安全に読み取るには、SAP BW BEx クエリ接続を作成します。

前提条件

SAP BW BEx クエリ接続を使用する前に、SAP 管理者は特定の前提条件のタスクを実行して Secure Agent マシンと SAP システムを設定する必要があります。

また、SAP BW BEx クエリデータを処理するには、必要なライセンスが SAP システムで有効になっているかどうかを確認する必要があります。

SAP ライブラリのダウンロードと設定

SAP BW BEx クエリからデータを読み取るには、Secure Agent マシンに SAP JCo ライブラリをダウンロードして設定する必要があります。ライブラリのダウンロードで問題が発生した場合は、SAP カスタマサポートにお問い合わせください。

1. [SAP Support Portal](#) に移動し、[ソフトウェアのダウンロード] をクリックします。
注: [SAP Support Portal](#) から [ソフトウェアのダウンロード] にアクセスするには、SAP 資格情報が必要です。
2. Secure Agent を実行しているマシンのオペレーティングシステムに基づいて、最新バージョンの 64 ビット SAP JCo ライブラリをダウンロードします。

オペレーティングシステム	SAP JCo ライブラリ
Windows	- sapjco3.jar - sapjco3.dll
Linux	- sapjco3.jar - libsapjco3.so

3. 次のディレクトリに JCo ライブラリをコピーします。
<Informatica Secure Agent installation directory>\apps\Data_Integration_Server\ext\deploy_to_main\bin\rdtm-extra\tpl\sap
存在しない場合は、deploy_to_main\bin\rdtm-extra\tpl\sap ディレクトリを作成します。

4. Informatica Intelligent Cloud Services にログインし、Secure Agent の JAVA_LIBS プロパティを設定します。
 - a. **[Administrator]** > **[ランタイム環境]** の順に選択します。
 - b. **[ランタイム環境]** をクリックして、**[ランタイム環境]** ページにアクセスします。
 - c. エージェント名の左側で、**[Secure Agent の編集]** をクリックします。
 - d. **[サービス]** リストから、**[データ統合サーバー]** を選択します。
 - e. **[タイプ]** リストから、**[Tomcat JRE]** を選択します。
 - f. Secure Agent を実行しているマシンのオペレーティングシステムに基づいて、JAVA_LIBS 値を入力します。

オペレーティングシステム	値
Windows	..\bin\rdtm-extra\tpl\sap\sapjco3.jar;..\bin\rdtm\javalib\sap\sap-adapter-common.jar
Linux	../bin/rdtm-extra/tpl/sap/sapjco3.jar../bin/rdtm/javalib/sap/sap-adapter-common.jar

警告: テーブルから値を直接コピーすると、値のハイフン (-) が誤ってコピーされることがあります。値をテキストエディタにコピーし、コピーした値が破損していないことを確認します。

System Configuration Details Reset All

Service: Data Integration Server ▼

Type: Tomcat JRE ▼

Type	Name	Value
Tomcat JRE	JAVA_LIBS	../bin/rdtm-extra/tpl/sap/sapjco3.jar../bin/rdtm/javalib/sap/sap-ada

- g. **[保存]** をクリックします。
 - h. Secure Agent をインストールしたすべてのマシンで手順 2 - 4 を繰り返します。
5. Secure Agent を再起動します。

SAP ユーザー権限の設定

SAP BW BEx クエリデータを処理するために、SAP システムで SAP ユーザーアカウントを設定します。

次の表に、SAP BW BEx クエリにアクセスしてデータの読み取りを行うためのユーザー権限の設定に必要なオブジェクトと権限を示します。

読み取りオブジェクト名	認証
S_RFC	RFC1、RFC_METADATA、RFC_METADATA_GET、RSAB、RSOB、RS_UNIFICATION、SDTX、SUGU、SU_USER、SYST
S_RS_COMP	ACTVT=3 (DISPLAY)
S_RS_COMP1	ACTVT=3 (DISPLAY)
S_RS_ICUBE	ACTVT=3 (DISPLAY)

これらのオブジェクトとその使用方法の詳細については、「[SAP user authorizations](#)」を参照してください。

SAP BW BEx クエリへの接続

SAP BW に接続して SAP BW BEx クエリからデータを読み取るように SAP BW BEx クエリ接続プロパティを設定してみましょう。

始める前に

開始する前に、SAP BW BEx クエリ接続を確立するように Secure Agent マシンと SAP システムを設定する必要があります。

これらのタスクの詳細については、「[「前提条件」 \(ページ 744\)](#)」を参照してください。

接続の詳細

次の表に、基本接続プロパティを示します。

財産	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。
シークレットコンテナの使用	組織に対して設定されている Secrets Manager にこの接続の機密資格情報を保存します。 このプロパティは、組織に Secrets Manager が設定されている場合にのみ表示されます。 このプロパティは、データ取り込みおよびレプリケーションとデータアクセス管理サービスではサポートされていません。 接続でシークレットコンテナを有効にすると、Secure Agent が Secrets Manager からどの資格情報を取得するかを選択できます。このオプションを無効にした場合、資格情報は組織の設定方法に応じてリポジトリまたはローカル Secure Agent に保存されます。 注: この接続を使用してプッシュダウンまたはプロキシサービスを介してデータアクセスポリシーを適用する場合、シークレットコンテナ設定オプションを使用することはできません。 Secrets Manager を設定および使用方法については、Administrator のヘルプにある「Secrets Manager の設定」を参照してください。
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。 Secure Agent、サーバーレスランタイム環境、またはエラスティックランタイム環境を選択します。 サーバーレス環境の設定の詳細については、「 「サーバーレスランタイム環境の使用」 (ページ 750) 」を参照してください。 ランタイム環境の設定および使用方法の詳細については、Administrator のヘルプにある「ランタイム環境」を参照してください。
認証	SAP BW にアクセスして SAP BW BEx クエリを読み取るための認証タイプ。 [SAP] 認証タイプを選択し、認証固有のパラメータを設定します。
ユーザー名	SAP BW アカウントに接続するための適切なユーザー権限を持つユーザー名。
パスワード	SAP BW アカウントに接続するためのパスワード。

接続タイプ

アプリケーションと負荷分散の接続タイプを設定して、SAP BW に接続し、SAP BW BEx クエリからデータの読み取りを行うことができます。

必要な接続タイプを選択し、接続固有のパラメータを設定します。

アプリケーション接続

アプリケーション接続は、SAP アカウント名、パスワード、クライアント番号、ホスト名、システム番号、および言語コードが必要なデフォルトのタイプです。

次の表に、アプリケーション接続の基本的な接続プロパティとその説明を示します。

接続プロパティ	説明
ホスト名	接続する 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 BW サーバーのシステム番号。 接続先の SAP システムから必要なシステム番号を取得します。
クライアント	SAP BW サーバーのクライアント番号。 接続先の SAP システムから必要なクライアント番号を取得します。
言語	SAP 言語に対応する言語コード。 接続先の SAP システムから必要な言語コードを取得します。

詳細設定

次の表に、アプリケーション接続の詳細接続プロパティとその説明を示します。

プロパティ	説明
トレース	<p>SAP システムによる JCo 呼び出しを追跡するかどうかを決定します。</p> <p>0 から 8 までのいずれかの値を入力します。</p> <p>デフォルトでは、SAP 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ません。</p> <p>デフォルトは 0 です。</p> <p>トレースレベル値の追加情報については、 「Setting up an SAP Java Connector (SAP JCo) and Related Traces」を参照してください。</p> <p>トレースファイルは以下のディレクトリからアクセスできます。</p> <ul style="list-style-type: none">- 設計時の情報: <Informatica Secure Agent のインストールディレクトリ>\apps \Data_Integration_Server\<最新のバージョン>\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	<p>SAP BW から SAP BW BEx クエリを読み取るときに使用できる追加の JCo 接続パラメータ。</p> <p>複数の JCo 接続パラメータをセミコロンで区切って、次の形式で入力できます。</p> <p><parameter name1>=<value1>;<parameter name2>=<value2>;<parameter name3>=<value3>....</p> <p>例えば、SAP SNC 接続を作成する場合は、次の追加パラメータを入力します。</p> <p>SNC_MODE=1;SNC_QOP=3;SNC_MYNAME=p:CN=<Common name>, OU=<Organizational unit>, O=<Organization>, C=<Country>;SNC_PARTNERNAME=p:CN=<Common name>, OU=<Organizational unit>, O=<Organization>, C=<Country>;SNC_LIB=C:\SNC_11\sapcrypto.dll;TRACE=1</p>
SAP の追加パラメータ	<p>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 プロパティ。</p> <p>Secure Agent が SAP に接続できるようにするために必要な RFC 固有のパラメータと接続情報を指定します。</p> <p>例えば、次のサンプルに一覧表示されている追加の引数として、SNC 接続パラメータを指定できます。</p> <p>GROUP=interfaces ASHOST=<Application server hostname> SYSNR=20 SNC_MODE=1 SNC_PARTNERNAME=p:CN=<Common name>, OU=<Organizational unit>, O=<Organization> SNC_MYNAME=p:CN=<Common name>, OU=<Organizational unit>, O=<Organization> SNC_LIB=<Secure Agent installation directory>/apps/server/bin/<libsapcrypto.so for Linux/ sapcrypto.dll for Windows> X509CERT=<X509 certificate> TRACE=2</p> <p>RFC 固有のパラメータの詳細については、SAP のマニュアルを参照してください。</p> <p>注: [SAP の追加パラメータ] フィールドと [追加パラメータ] フィールドの両方でパラメータを指定した場合、[SAP の追加パラメータ] フィールドで指定した値が優先されます。</p>

負荷分散接続

実行時の負荷が最も低い SAP BW サーバーに接続する場合、負荷分散接続を作成します。

負荷分散接続の作成時には、**【接続の詳細】** セクションにリストされているすべてのプロパティに加えて、**【詳細設定】** セクションにメッセージホスト名、R3 名/SysID、およびグループ値を入力する必要もあります。

次の表に、負荷分散接続の基本的な接続プロパティとその説明を示します。

接続プロパティ	説明
ユーザー名	SAP BW アカウントに接続するための適切なユーザー権限を持つユーザー名。
パスワード	SAP BW アカウントに接続するためのパスワード。
ホスト名	接続する 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 BW サーバーのシステム番号。 接続先の SAP システムから必要なシステム番号を取得します。
クライアント	SAP BW サーバーのクライアント番号。 接続先の SAP システムから必要なクライアント番号を取得します。
言語	SAP 言語に対応する言語コード。 接続先の SAP システムから必要な言語コードを取得します。

詳細設定

次の表に、負荷分散接続の詳細接続プロパティとその説明を示します。

プロパティ	説明
メッセージホスト名	必須。負荷分散接続を使用する場合に接続する SAP メッセージサーバーのホスト名。
R3 名/ SysID	必須。負荷分散接続を使用する場合に接続する SAP メッセージサーバーのシステム ID。
グループ	必須。負荷分散接続を使用する場合に接続に使用する SAP ログオングループの名前。
トレース	<p>SAP システムによる JCo 呼び出しを追跡するかどうかを決定します。 0 から 8 までのいずれかの値を入力します。 デフォルトでは、SAP 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ません。 デフォルトは 0 です。</p> <p>トレースレベル値の追加情報については、 「Setting up an SAP Java Connector (SAP JCo) and Related Traces」 を参照してください。</p> <p>トレースファイルは以下のディレクトリからアクセスできます。</p> <ul style="list-style-type: none"> - 設計時の情報: <Informatica Secure Agent のインストールディレクトリ>\apps \<Data_Integration_Server>\<最新のバージョン>\ICS\main\tomcat - 実行時の情報: <Informatica Secure Agent installation directory>\apps\Data_Integration_Server \<Latest version>\ICS\main\bin\rdtm

プロパティ	説明
追加パラメータ	<p>SAP BW から SAP BW BEx クエリを読み取る際に使用できる追加の JCo 接続パラメータ。複数の JCo 接続パラメータをセミコロンで区切って、次の形式で入力できます。</p> <pre><parameter name1>=<value1>;<parameter name2>=<value2>;<parameter name3>=<value3>....</pre> <p>例えば、SAP SNC 接続を作成する場合は、次の追加パラメータを入力します。</p> <pre>SNC_MODE=1;SNC_QOP=3;SNC_MYNAME=p:CN=<Common name>, OU=<Organizational unit>, 0=<Organization>, C=<Country>;SNC_PARTNERNAME=p:CN=<Common name>, OU=<Organizational unit>, 0=<Organization>, C=<Country>;SNC_LIB=C:\SNC_11\sapcrypto.dll;TRACE=1</pre>
SAP の追加パラメータ	<p>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 プロパティ。</p> <p>Secure Agent が SAP に接続できるようにするために必要な RFC 固有のパラメータと接続情報を指定します。</p> <p>例えば、次のサンプルに一覧表示されている追加の引数として、SNC 接続パラメータを指定できます。</p> <pre>GROUP=interfaces ASHOST=<Application server hostname> SYSNR=20 SNC_MODE=1 SNC_PARTNERNAME=p:CN=<Common name>, OU=<Organizational unit>, 0=<Organization> SNC_MYNAME=p:CN=<Common name>, OU=<Organizational unit>, 0=<Organization> SNC_LIB=<Secure Agent installation directory>/apps/server/bin/<libsapcrypto.so for Linux/ sapcrypto.dll for Windows> X509CERT=<X509 certificate> TRACE=2</pre> <p>RFC 固有のパラメータの詳細については、SAP のマニュアルを参照してください。</p> <p>注: [SAP の追加パラメータ] フィールドと [追加パラメータ] フィールドの両方でパラメータを指定した場合、[SAP の追加パラメータ] フィールドで指定した値が優先されます。</p>

サーバーレスランタイム環境の使用

Linux での SAP BW BEx クエリ接続の設定時に、Azure でホストされているサーバーレスランタイム環境を使用して SAP システムに接続できます。

SAP Secure Network Communication (SNC) プロトコルを使用する場合、サーバーレスランタイム環境を使用することはできません。

サーバーレスランタイム環境を使用して SAP BW BEx クエリ接続を設定する前に、次のタスクを実行してください。

- Azure アカウントの Azure コンテナに SAP ライブラリを追加します。
- .yml サーバーレス構成ファイルを設定する。
- Linux 上のサーバーレスランタイム環境の JAVA_LIBS プロパティを設定します。

Azure アカウントの Azure コンテナに SAP ライブラリを追加します

サーバーレスランタイム環境で SAP BW BEx クエリ接続を設定するには、次の手順を実行します。

1. Azure のサーバーレスエージェント設定用に次の構造を作成します: <補足ファイルの場所>/serverless_agent_config

2. Azure アカウントの次の場所にある Azure コンテナに SAP ライブラリを追加します: <補足ファイルの場所>/serverless_agent_config/sap

.yaml サーバーレス構成ファイルを設定する

次の手順を実行して、サーバーレスランタイム環境で.yaml サーバーレス構成ファイルを設定し、SAP ライブラリをサーバーレスエージェントディレクトリにコピーします。

1. 次のコードスニペットをテキストエディタにコピーします。

```
version: 1
agent:
  dataIntegrationServer:
    autoDeploy:
      sap:
        nwrfdc:
          - fileCopy:
              sourcePath: sap/nwrfdc/<rfdc_library_filename>
          - fileCopy:
              sourcePath: sap/nwrfdc/<sapnwrfdc_filename>
```

ここで、ソースパスは Azure の SAP ライブラリファイルのディレクトリパスです。

2. 構文とインデントが有効であることを確認してから、ファイルを serverlessUserAgentConfig.yaml として次の Azure の場所に保存します: <補足ファイルの場所>/serverless_agent_config.yaml ファイルの実行時に、SAP ライブラリが Azure の場所からサーバーレスエージェントディレクトリにコピーされます。

サーバーレスランタイム環境の JAVA_LIBS プロパティを設定する

Administrator で次の手順を実行して、Linux 上のサーバーレスランタイム環境に JAVA_LIBS プロパティを設定します。

1. Informatica Intelligent Cloud Services にログインします。
2. **[Administrator]** > **[サーバーレス環境]** の順に選択します。
3. **[サーバーレス環境]** タブで、必要なサーバーレスランタイム環境の **[アクション]** メニューを展開し、**[編集]** を選択します。
4. **[ランタイム設定のプロパティ]** タブで、サービスに **[データ統合サーバー]** を選択し、タイプに **[Tomcat_JRE]** を選択します。
5. **[プロパティの追加]** をクリックします。
6. **[名前]** フィールドに JAVA_LIBS と入力し、次の値を設定します。
../bin/rdtm-extra/tpl/sap/sapjco3.jar:../bin/rdtm/javajlib/sap/sap-adapter-common.jar
7. **[保存]** をクリックします。

サーバーレス環境の設定および使用方法の詳細については、Administrator のヘルプにある「ランタイム環境」の「サーバーレスランタイム環境のセットアップ」を参照してください。

第 197 章

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	<p>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。_ . + -</p> <p>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。</p> <p>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。</p>
説明	<p>SAP HANA CDC 接続の説明。最大長は 4000 文字です。</p>
ランタイム環境	<p>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。</p>
リスナの場所	<p>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gger（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。 <i>host_name</i> は、ホスト名または IP アドレスにできます。</p> <p><i>host_name:port_number</i></p> <p>以下に例を示します。</p> <p>HANADB1:1467</p>
ユーザー名	<p>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。</p>
パスワード	<p>[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。</p>
コレクション名	<p>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。</p>

プロパティ	説明
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gger (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	<p>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。</p> <ul style="list-style-type: none"> - 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。 <p>デフォルトは [なし] です。</p>
ページングサイズ	<p>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。</p> <p>デフォルトである最小値は 0 です。</p>
ページング単位	<p>[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。</p> <p>[行] または [キロバイト] のいずれかを選択します。</p>
マップの場所	<p>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。</p> <p>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gger (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。</p> <p>次の形式で値を入力します。<i>host_name</i> は、ホスト名または IP アドレスにできます。</p> <p><i>host_name:port_number</i></p> <p>以下に例を示します。</p> <p>SAPHANA2B:25100</p> <p>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。</p>
マップの場所のユーザー	<p>[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。</p>

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 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	<p>カスタムプロパティまたは接続プロパティのオーバーライド。カスタムプロパティとは、PowerExchange のデフォルトの設定よりも優先するために指定できるプロパティです。セミコロン (;) を区切り文字として使用して複数のプロパティを入力するか、パラメータファイルを使用して接続プロパティの上書きを指定するパラメータを指定することができます。</p> <p>例:</p> <pre><property>=<value>;<property>=<value></pre> <p>多くの場合、Informatica グローバルカスタマサポートからの指示を受けたいうで、カスタムプロパティの設定を行います。</p> <p>注: これらのプロパティは、PowerCenter の PowerExchange Client for PowerCenter (PWXPC) CDC 接続の 【PWX オーバーライド】 オプションと同じです。</p> <p>パラメータファイルを使用して接続プロパティのオーバーライドを指定するには、\$<ParameterName>の形式でパラメータを設定し、ユーザー定義パラメータ名の前にドル記号 (\$) を付けます。次に、【ランタイムオプション】 タブの 【パラメータファイル名】 フィールドにパラメータファイル名を指定することで、ユーザー定義パラメータ定義を含むパラメータファイルを使用するようにマッピングのマッピングタスクを設定します。</p> <p>注:</p> <ul style="list-style-type: none"> - マッピングおよび接続に同じパラメータを入力した場合は、接続カスタムプロパティが優先されます。 - パラメータファイルがある場合、このフィールドで指定するパラメータ名は、パラメータファイルで定義されたエントリと一致している必要があります。 <p>詳細については、「接続オーバーライドのリファレンス」の章を参照してください。</p>

第 198 章

SAP HANA 接続のプロパティ

SAP HANA 接続を作成して、SAP HANA と SAP Datasphere に接続します。

前提条件

SAP HANA データベースに対して読み取りまたは書き込みを行うための SAP HANA 接続を作成する前に、SAP HANA 管理者は、Secure Agent マシンと SAP システムを設定するための特定の前提条件タスクを実行する必要があります。

1. 64 ビットの SAP HANA ODBC ドライバをインストールします。
2. オペレーティングシステムに基づいて ODBC データソースを作成します。
 - Windows 上で、ODBC データソースアドミニストレータを使用して、SAP HANA ODBC ドライバのデータソースを作成および設定します。
 - Linux 上で、データソースエントリをシステムの \$ODBCHOME ディレクトリ内の odbc.ini ファイルに追加します。
3. ngdbc.jar ファイルをダウンロードして設定します。

クラウド内の SAP HANA データベースに接続する方法の詳細については、SAP のマニュアルの「[Connecting to the SAP HANA database in SAP HANA Cloud](#)」を参照してください。

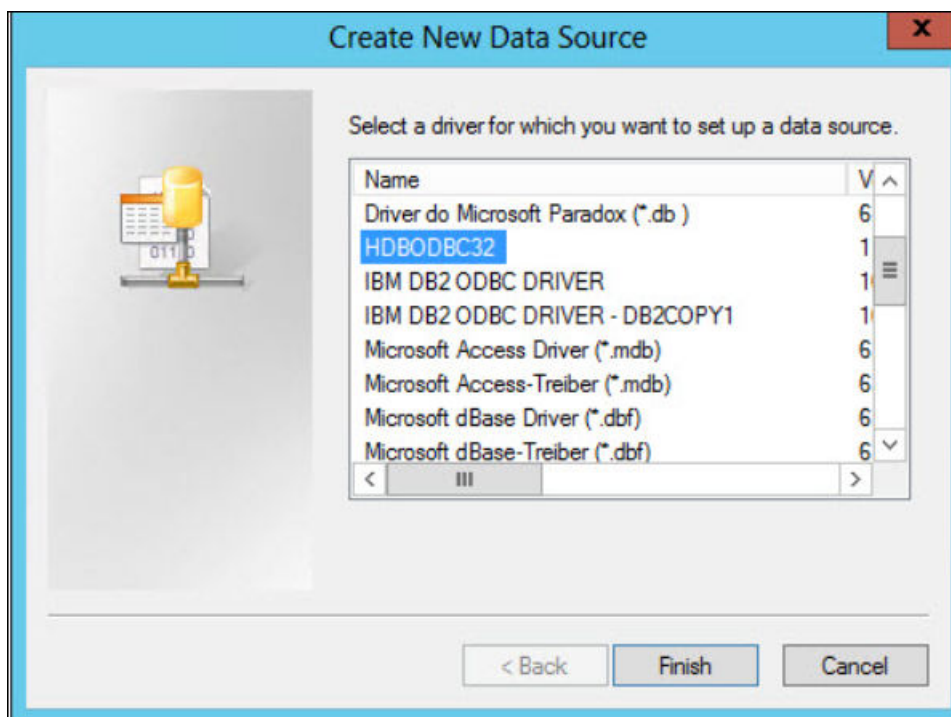
管理者が設定を完了したら、マッピングおよびマッピングタスクで SAP HANA 接続を設定して使用できます。

Windows 上での HANA ODBC データソースの作成

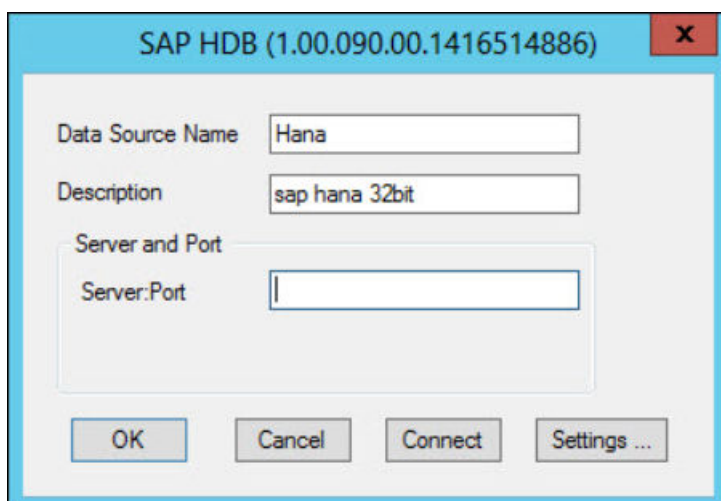
Windows に SAP HANA ODBC ドライバをインストールした後に、ODBC データソースアドミニストレータを使用して SAP HANA ODBC データソースを作成します。

1. **【スタート】 > 【管理ツール】 > 【ODBC データソース】** を選択します。
[ODBC データソースアドミニストレータ] ダイアログボックスが表示されます。
2. **【システム DSN】** タブをクリックし、**【追加】** をクリックします。
[データソースの新規作成] ダイアログボックスが表示されます。

3. 64 ビット Windows の場合は HANA ODBC ドライバ HDBODBC を、32 ビット Windows の場合はドライバ HDBCODBC32 を選択して SAP HANA データソースを設定します。



4. **【完了】** をクリックします。
[SAP HDB] ダイアログボックスが開きます。
5. SAP HANA にアクセスするために必要なデータソース名、説明、およびサーバーとポートのフィールドに入力します。
- さらに、**【接続】** をクリックして、ODBC 接続が SAP HANA サーバーに正常に接続されるかどうかをテストします。



6. **【OK】** をクリックしてドライバの設定を完了します。

Linux オペレーティングシステムでのエントリの追加

Linux に SAP HANA ODBC ドライバをインストールした後に、SAP HANA ODBC データソースを設定します。Informatica のプロセスを実行するオペレーティングシステムユーザーには、SAP HANA ODBC ドライバファイルに対する読み取り権限と実行権限が割り当てられている必要があります。

1. 次のような環境変数を設定します。

ODBCHOME

この変数を、ODBC のインストールディレクトリに設定します。

例: `setenv ODBCHOME /export/home/Informatica Cloud Secure Agent/drivers/misc/latest/bin`

ODBCINI

odbc.ini ファイルが格納されているディレクトリを示す変数を設定します。

例: `setenv ODBCINI /export/home/Informatica Cloud Secure Agent/odbc.ini`

ODBCINST

odbcinst.ini ファイルが格納されているディレクトリを示す変数を設定します。

例: `setenv ODBCINST /export/home/Informatica Cloud Secure Agent/odbcinst.ini`

LD_LIBRARY_PATH、LIBPATH、または SHLIB_PATH

共有ライブラリの環境変数を、SAP HANA ODBC ドライバがインストールされているディレクトリに設定します。

たとえば、`setenv LD_LIBRARY_PATH ".:${PM_HOME}:${JAVA_HOME}/lib:${ORACLE_HOME}/lib:/usr/sap/hdbclient:"`と設定します。

2. Secure Agent インストールディレクトリにある `odbcinst.ini` ファイルに SAP HANA ドライバの詳細を追加します。
例えば、SAP HANA データベースに接続するには、`odbcinst.ini` ファイルに次の SAP HANA ドライバの詳細を追加します。

```
[HDBODBC]
Driver=/usr/sap/hdbclient/libodbcHDB.so
Description=HANA Driver
Setup=/usr/sap/hdbclient/libodbcHDB.so
CPOutput=0
```

注: この例では、次のパスはドライバのインストール場所です。 `/usr/sap/hdbclient/`

3. システムの `$ODBCHOME` ディレクトリにある `odbc.ini` ファイルに SAP HANA データソースエントリを追加します。
例えば、次の SAP HANA データソースエントリを `odbc.ini` ファイルに追加します。

```
[SAP HANA source]
Driver=/usr/sap/hdbclient/libodbcHDB.so
DriverUnicodeType=1
ServerNode=<server_node>:<port>
encrypt=0
User=<Hana User>
Password=<Hana Password>
```

`odbc.ini` ファイルと `odbcinst.ini` ファイルは同じ場所にある必要があります。

ライブラリのダウンロードと設定

SAP HANA コネクタは、JDBC を使用してメタデータをインポートします。したがって、SAP HANA データベースからデータを読み取るには、ngdbc.jar ファイルをダウンロードして、Secure Agent マシン上で設定します。ファイルのダウンロードで問題が発生した場合は、SAP カスタマサポートにお問い合わせください。

1. 次の SAP Service Marketplace に移動します。 <http://service.sap.com/connectors>
注: Service Marketplace にアクセスするには、SAP 資格情報が必要です。
2. Secure Agent が実行されている Linux または Windows マシンに ngdbc.jar ファイルをダウンロードします。
ダウンロードするファイルが最新バージョンであることを確認します。
3. 次のディレクトリに ngdbc.jar ファイルをコピーします。
`C:\Program Files\Informatica Cloud Secure Agent\apps\Data_Integration_Server\ext\deploy_to_main\bin\rdtm-extra\HANA`
`deploy_to_main\bin\rdtm-extra\HANA` ディレクトリが存在しない場合は、作成します。
4. Secure Agent を再起動します。

SAP HANA への接続

SAP HANA および SAP Datasphere に接続するように SAP HANA の接続プロパティを設定してみましょう。

始める前に

接続を設定する前に、SAP HANA ライブラリをダウンロードして設定し、64 ビットの SAP HANA ODBC ドライバとデータソースを Secure Agent マシンにインストールして設定してください。

これらのタスクの詳細については、「[「前提条件」 \(ページ 755\)](#)」を参照してください。

接続の詳細

次の表に、基本接続プロパティを示します。

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

プロパティ	説明
シークレットコンテナの使用	<p>組織に対して設定されている Secrets Manager にこの接続の機密資格情報を保存します。このプロパティは、組織に Secrets Manager が設定されている場合にのみ表示されます。このプロパティは、データ取り込みおよびレプリケーションとデータアクセス管理サービスではサポートされていません。</p> <p>接続でシークレットコンテナを有効にすると、Secure Agent が Secrets Manager からどの資格情報を取得するかを選択できます。このオプションを無効にした場合、資格情報は組織の設定方法に応じてリポジトリまたはローカル Secure Agent に保存されます。</p> <p>注: この接続を使用してプッシュダウンまたはプロキシサービスを介してデータアクセスポリシーを適用する場合、シークレットコンテナ設定オプションを使用することはできません。</p> <p>Secrets Manager を設定および使用方法については、Administrator のヘルプにある「Secrets Manager の設定」を参照してください。</p>
ランタイム環境	<p>タスクを実行するランタイム環境の名前。</p> <p>Secure Agent、サーバーレスランタイム環境、またはエラスティックランタイム環境を選択します。</p> <p>サーバーレス環境の設定の詳細については、「サーバーレスランタイム環境の設定」(ページ 760)を参照してください。</p> <p>エラスティックランタイム環境の設定の詳細については、「エラスティックランタイム環境の設定」(ページ 761)を参照してください。</p>
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	<p>SAP HANA データベースのスキーマ名。</p> <p>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。</p>
コードページ	<p>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。</p> <p>UTF-8 コードページを選択します。</p>
ユーザー名	SAP HANA アカウントのユーザー名。
パスワード	<p>SAP HANA アカウントのパスワード。</p> <p>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: ~ ` ! @ # \$ % ^ & * () _ - + = [] : ; ' < , > . ? /</p>

詳細設定

次の表に、詳細接続のプロパティを示します。

プロパティ	説明
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。 <code>connectTimeout=180000</code> 詳細については、「 「ライブラリのダウンロードと設定」 (ページ 758) 」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。 <code>charset=sjis;readtimeout=180</code> 詳細については、「 「Linux オペレーティングシステムでのエントリの追加」 (ページ 757) 」を参照してください。

サーバーレスランタイム環境の設定

データ統合で SAP HANA 接続を設定するときに、サーバーレスランタイム環境を使用して SAP システムに接続できます。

サーバーレスランタイム環境を使用する SAP HANA 接続を設定する前に、特定の前提条件を実行する必要があります。

1. AWS または Azure のサーバーレスエージェント設定用に次の構造を作成します:
<Supplementary file location>/serverless_agent_config
2. AWS アカウントまたは Azure アカウントの次のディレクトリにある Amazon S3 バケットあるいは Azure コンテナにライブラリを追加します: <補足ファイルの場所>/serverless_agent_config/hana
3. 次のコードスニペットをテキストエディタにコピーします。

```
version: 1
agent:
  dataIntegrationServer:
    autoDeploy:
      sap:
        hanas:
          - fileCopy:
              sourcePath: sap/jco/ngdbc.jar
        odbInst:
          drivers:
            - fileCopy:
                sourcePath: ODBC/libodbcHDB.so
          dsns:
            - name: "HDBODBC"
              entries:
                - key: Driver
                  value: libodbcHDB.so
                - key: Description
                  value: "HANA Driver"
                - key: CTimeout
```

value: 0

ここで、ソースパスは AWS または Azure のライブラリファイルのディレクトリパスです。

4. 構文とインデントが有効であることを確認してから、ファイルを `serverlessUserAgentConfig.yml` として次の AWS または Azure のディレクトリに保存します:

<Supplementary file location>/serverless_agent_config

.yml ファイルの実行時に、ライブラリが AWS または Azure のディレクトリからサーバーレスエージェントディレクトリにコピーされます。

サーバーレスランタイム環境の設定および使用方法の詳細については、Administrator のヘルプにある「サーバーレスランタイム環境」を参照してください。

エラスティックランタイム環境の設定

マッピング実行中にエラスティックランタイム環境がカスタムバイナリファイルにアクセスして実行できるよう、ランタイム環境でこれらのファイルを設定することができます。

カスタムバイナリファイルを設定する前に、Informatica Intelligent Cloud Services 内でデータを処理できる Kubernetes クラスタを作成できるエラスティックランタイム環境を必ず AWS にデプロイしてください。

エラスティックランタイム環境のデプロイの詳細については、「[Deploy an elastic runtime environment](#)」を参照してください。

エラスティックランタイム環境をデプロイした後、マウントされたディスクにカスタムバイナリファイルを配置し、使用するバイナリファイルの正確なパスを POST 要求内にコピーします。

カスタムバイナリファイルを管理するには、Informatica Intelligent Cloud Services for Elastic Runtime Environment 内で以下の手順を実行します。

1. 組織にログインし、セッション ID とランタイム環境 ID を取得します。
2. REST API への POST 呼び出しを、セッション ID、ランタイム環境 ID、および、マウントされたディスクから以前にコピーしたバイナリファイルのパスを渡して行います。
POST 呼び出しの詳細については、『REST API リファレンス』ガイド内の「[Supplementary files](#)」を参照してください。

POST 要求の例を以下に示します。

```
POST <base URL>/api/v3/RuntimeEnvironment/<runtime environment ID>/ElasticConfig
Content-Type: application/json
Accept: application/json
INFA-SESSION-ID: <SessionId>
{
  "rteId": "rte-12345",
  "specification": {
    "agent": {
      "dataIntegrationServer": {
        "sap": {
          "jcos": [{"sourcePath": "/<path to binaries>/jco1"}],
          "nwrfs": [{"sourcePath": "/<path to binaries>/nwrfs1"}],
          "hanas": [{"sourcePath": "/<path to binaries>/hana1"}]
        }
      }
    }
  }
}
```

この POST 呼び出しにより、データ統合サーバーの再起動がトリガーされます。

3. Administrator でデータ統合サーバーの状態を確認することで、エラスティックランタイム環境が起動されて稼働していることを確認します。
4. 接続をテストするかマッピングを実行することで、エラスティックランタイム環境がカスタムバイナリファイルにアクセスして使用できることを確認します。

Secure Socket Layer プロトコルの設定

Secure Socket Layer (SSL) プロトコルを用いた SAP HANA 接続を使用して、SAP HANA に対する安全な読み取りまたは書き込みを行うことができます。

このセキュアな接続は、SAP Datasphere に対する読み取りまたは書き込みを行う場合にも使用できます。

SAP HANA SSL 接続を設定する手順の詳細については、Informatica How-To ライブラリの記事「[Configure a secure SAP HANA connection](#)」を参照してください。

第 199 章

SAP HANA Database Ingestion 接続のプロパティ

SAP HANA データベース取り込み接続を定義するには、接続プロパティを設定します。この接続タイプは、データ取り込みおよびレプリケーションで設定したデータベース取り込みとレプリケーションタスクのソースに使用することができます。

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。
ランタイム環境	データベース取り込みとレプリケーション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。 ローカルの Secure Agent インストールまたはサーバーレスランタイム環境のいずれかを使用できます。初期ロードに限り、クラウドソースタイプに対してサーバーレスランタイム環境を使用できます。ホステッドエージェントまたはエラスティックランタイム環境で、データベース取り込みとレプリケーションタスクを実行することはできません。
ユーザー名	SAP HANA インスタンスに接続するためのユーザー名。SAP HANA で指定されているデータベースユーザー名と同じ大文字と小文字を使用してユーザー名を入力します。
パスワード	SAP HANA インスタンスに接続するためのパスワード。
ホスト	SAP HANA データベースサーバーをホストするマシンの名前。
ポート	接続先の SAP HANA サーバーのポート番号。デフォルトは 30015 です。
データベース名	SAP HANA ソースデータベース名。

接続プロパティ	説明
詳細接続プロパティ	SAP HANA ソースへの接続に使用される SAP HANA JDBC ドライバのオプションの詳細プロパティ。 <i>property=value</i> 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: <code>encrypt=true</code> 。
キャプチャタイプ	次のいずれかのオプションを選択して、データベース取り込み増分ロードジョブが SAP HANA データベースから変更データをキャプチャするために使用するキャプチャメソッドを指定します。 <ul style="list-style-type: none"> - トリガベース。AFTER DELETE、AFTER INSERT、AFTER UPDATE トリガを使用して、スキーマ内の SAP HANA ソーステーブルから変更データをキャプチャします。トリガは、各ソーステーブルの DML 変更の操作前イメージと操作後イメージを取得し、変更のエントリを PKLOG テーブルとシャドー_CDC テーブルに書き込みます。 - ログベース。SAP HANA データベースログから変更データをキャプチャします。 デフォルトは [トリガベース] です。
ログのクリア	増分ロードの場合は必須です。キャプチャタイプに応じて、このプロパティを次のように設定します。 <ul style="list-style-type: none"> - [トリガベース] 変更キャプチャの場合、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) を入力します。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. - [ログベース] 変更キャプチャの場合、HANA または Oracle データベースキャッシュに格納されているデータレコードが圧縮されるまでの日数を入力します。この時間間隔に達すると、レコードが圧縮されますが、削除はされません。デフォルトは 14 です。値 0 は、圧縮が発生しないことを表します。実質的には、最大値はありません。
トリガプレフィックス	[トリガベース] キャプチャタイプの場合、DML 変更の操作前と操作後のイメージを取得するために CDC スクリプトが各ソーステーブルに対して生成する AFTER DELETE、AFTER INSERT、および AFTER UPDATE トリガの名前にプレフィックスを追加できます。最大 16 文字のプレフィックス値を入力します。トリガ名のプレフィックスの後にアンダースコア (_) が続きます (例: TX_SAP_DEMO_TABLE_DBMI_USER_t_d)。プレフィックスを使用して、サイトのトリガ命名規則に準拠できます。
キャッシュタイプ	[ログベース] キャプチャタイプの場合、キャッシュタイプとして [HANA] または [Oracle] を選択します。セキュアエージェントは、変更レコードをターゲットに書き込む準備が整うまで、変更データをキャッシュに保存します。
キャッシュホスト	[ログベース] キャプチャタイプの場合は、キャッシュデータベースをホストするマシンのホスト名を入力します。
キャッシュポート	[ログベース] キャプチャタイプの場合は、キャッシュデータベースサーバーのポート番号を入力します。

接続プロパティ	説明
キャッシュユーザー名	【ログベース】 キャブチャタイプの場合は、キャッシュデータベースへの接続に使用するユーザー名を入力します。
キャッシュパスワード	【ログベース】 キャブチャタイプの場合は、キャッシュデータベースへの接続に使用するパスワードを入力します。
キャッシュデータベース/サービス名	【ログベース】 キャブチャタイプの場合は、選択したキャッシュタイプに応じて、HANA キャッシュデータベース名または Oracle キャッシュサービス名を入力します。
キャッシュ追加接続プロパティ	<p>【ログベース】 キャブチャタイプの場合は、オプションのキャッシュ接続プロパティのリストを入力できます。HANA キャッシュを使用する場合は、アンパサンド (&) 区切り記号を使用します。Oracle キャッシュを使用する場合は、セミコロン (;) 区切り記号を使用します。</p> <p>例:</p> <p>HANA: latency=0&communicationtimeout=0</p> <p>Oracle: EncryptionMethod=SSL;CryptoProtocolVersion=TLSv1.1</p>
キャッシュセキュリティ接続プロパティ	<p>【ログベース】 キャブチャタイプの場合は、キャッシュ接続のオプションのセキュリティプロパティのリストを入力できます。HANA キャッシュを使用する場合は、アンパサンド (&) 区切り記号を使用します。Oracle キャッシュを使用する場合は、セミコロン (;) 区切り記号を使用します。</p> <p>例:</p> <p>HANA: encrypt=true&validateCertificate=false</p> <p>Oracle: KeyStorePassword=xyz;TrustStorePassword=xy</p>
サーバーログのパス	【ログベース】 キャブチャタイプの場合は、SAP HANA データベースサーバーのログパスを入力します。
クライアントログのパス	【ログベース】 キャブチャタイプの場合は、ソースデータベースのログの場所へのセキュアエージェントマシンのマウントパスのマッピングを入力します。
クライアントアーカイブログのパス	【ログベース】 キャブチャタイプの場合は、ソースデータベースのアーカイブログの場所へのセキュアエージェントマシンのマウントパスのマッピングを入力します。

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

第 200 章

SAP IQ 接続のプロパティ

SAP IQ 接続を作成して、SAP IQ に安全なデータの書き込みを行います。

前提条件

SAP IQ に書き込みを行うための SAP IQ 接続を作成する前に、前提条件を必ず満たすようにしてください。

SAP IQ JDBC ドライバと Sybase クライアントのインストール

SAP IQ データベースにデータの書き込みを行うには、Secure Agent マシンに SAP IQ JDBC ドライバと Sybase クライアントをインストールする必要があります。

- SAP IQ JDBC ドライバを Secure Agent マシンにインストールします。
ドライバをインストールするには、次の手順を実行します。
 1. [SAP Support Portal](#) から、jconn4.jar SAP IQ JDBC ドライバをダウンロードします。
 2. Secure Agent マシンが Windows マシンであるか Linux マシンであるかに基づいて、次のディレクトリに informatica.sapiq フォルダを手動で作成します：

Secure Agent マシン	ディレクトリ
Linux	<Secure Agent のインストールディレクトリ>/ext/connectors/thirdparty
Windows	<Secure Agent のインストールディレクトリ>\ext\connectors\thirdparty

3. SAP IQ JDBC ドライバを informatica.sapiq フォルダにコピーします。
- Sybase クライアントを Secure Agent マシンにインストールします。
Sybase クライアントをインストールするには、次の手順を実行します。
 1. SAP Web サイトから Sybase クライアントをダウンロードし、Secure Agent マシンにインストールします。
 2. Linux では、次の環境変数を追加で設定します：
 - setenv SYBASE <Sybase クライアントディレクトリ>/sybase
 - setenv SYBROOT <Sybase クライアントディレクトリ>/sybase

- setenv IQDIR16 <Sybase client directory>/sybase/IQ-16_1
- setenv LD_LIBRARY_PATH <Sybase クライアントディレクトリ>/sybase/IQ-16_1/lib64
- setenv PATH <Sybase クライアントディレクトリ>/sybase/IQ-16_1/bin64

SAP IQ JDBC ドライバをインストールし、環境変数を設定した後に、Secure Agent を再起動する必要があります。

SAP IQ への接続

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

始める前に

開始する前に、SAP IQ JDBC ドライバと Sybase クライアントを Secure Agent マシンにインストールして、SAP IQ 接続を確立する必要があります。

設定の前提条件の詳細については、「[「前提条件」 \(ページ 766\)](#)」を参照してください。

接続の詳細

次の表に、基本接続プロパティを示します。

財産	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。
シークレットコンテナの使用	組織に対して設定されている Secrets Manager にこの接続の機密資格情報を保存します。 このプロパティは、組織に Secrets Manager が設定されている場合にのみ表示されます。 このプロパティは、データ取り込みおよびレプリケーションとデータアクセス管理サービスではサポートされていません。 接続でシークレットコンテナを有効にすると、Secure Agent が Secrets Manager からどの資格情報を取得するかを選択できます。このオプションを無効にした場合、資格情報は組織の設定方法に応じてリポジトリまたはローカル Secure Agent に保存されます。 注: この接続を使用してプッシュダウンまたはプロキシサービスを介してデータアクセスポリシーを適用する場合、シークレットコンテナ設定オプションを使用することはできません。 Secrets Manager を設定および使用する方法については、Administrator のヘルプにある「Secrets Manager の設定」を参照してください。
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。 Secure Agent を選択します。
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。

財産	説明
ポート	SAP IQ データベースサーバーに接続するためのポート番号。 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 アカウントに接続するためのユーザー名。
パスワード	SAP IQ アカウントに接続するためのパスワード。
データファイルディレクトリ	実行時にデータファイルが格納される 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: \root\mydirectory\inputfile.out ディレクトリが UNIX システム上にある場合は、パスにスラッシュ (/) を使用します。 例: /root/mydirectory/inputfile.out

詳細設定

次の表に、詳細接続のプロパティを示します。

プロパティ	説明
チェックポイント	テーブルへのデータのロードに成功した後に、SAP IQ データベースがチェックポイントを発行できるようにします。 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 外部ローダーが外部ローダーログにステータスメッセージの書き込みを行う前にロードする行数。 デフォルトは 1000 です。
外部ローダー実行可能	外部ローダー実行可能ファイルのファイル名とパス。 外部ローダー実行可能ファイルの名前は、デフォルトで [dbisql] に設定されています。 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。 外部ローダーの実行可能ファイル名が abc.exe で、パスが /root/<フォルダ名>である場合は、パスおよびファイル名を次の形式で入力します： /root/<folder name>/abc.exe
ステージング済み	データのロード方法 SAP IQ データベースにデータをロードする前に、ステージングの場所にデータの書き込みを行うことができます。 デフォルトでは有効になっています。

第 201 章

SAP Mass Ingestion 接続のプロパティ

SAP Mass Ingestion 接続を設定するには、接続プロパティを設定する必要があります。

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

接続プロパティ	説明
接続名	接続の名前。この名前は、組織内で一意にする必要があります。接続名には、英数字、スペース、および次のような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。
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: ホステッドエージェントまたはサーバーレスランタイム環境でアプリケーション取り込みとレプリケーションタスクを実行することはできません。
ユーザー名	SAP インスタンスのユーザー名。
パスワード	SAP インスタンスのパスワード。
言語コード	SAP 言語に対応する言語コード。
システム番号	SAP サーバーのシステム番号。
クライアント番号	SAP サーバーのクライアント番号。
ポート範囲	Netty サーバーを実行する HTTP ポート範囲。
接続タイプ	ABAP アプリケーションサーバーにアクセスするための接続タイプ。次のオプションがあります。 <ul style="list-style-type: none">- 直接接続: サーバーホストを使用して単一の ABAP アプリケーションサーバーにアクセスします。- 負荷分散接続: メッセージサーバーを介して ABAP アプリケーションサーバーのグループにアクセスします。

接続プロパティ	説明
アプリケーションサーバー	SAP アプリケーションサーバーホストの名前。 注: このフィールドは、 【直接接続】 タイプの場合にのみ表示されます。
メッセージサーバー	SAP メッセージサーバーの IP アドレスまたは名前。 注: このフィールドは、 【負荷分散接続】 タイプの場合にのみ表示されます。
SAP ログオングループ	アクセスする SAP システムに属するサーバーのグループ名。 注: このフィールドは、 【負荷分散接続】 タイプの場合にのみ表示されます。
SAP システム ID	アクセスする SAP システムの ID。 注: このフィールドは、 【負荷分散接続】 タイプの場合にのみ表示されます。
メッセージサーバーポート	SAP メッセージサーバーがリスンしているポート番号。 注: このフィールドは、 【負荷分散接続】 タイプの場合にのみ表示されます。
データベース	基盤データベースの名前。 次のいずれかのオプションを選択します。 - Oracle - SAP HANA (S/4 トリガベース)
Oracle データベースの場合	
ユーザー名	データベースインスタンスのユーザー名。
パスワード	データベースインスタンスのパスワード。
ホスト	データベースサーバーのホスト名。
ポート	データベースサーバーに接続するときに使用するネットワークポート番号。デフォルトは 1521 です。
サービス名	Oracle データベースを一意に識別するサービス名またはシステム ID (SID)。Oracle データベースに接続するための SID を次の形式で指定します。SID:<ORACLE_SID>
コードページ	データベースサーバーのコードページ。アプリケーション取り込みとレプリケーションタスクは、UTF-8 コードページを使用します。デフォルトは UTF-8 です。
暗号化方法	初期ロードジョブの場合、Secure Agent と Oracle データベースサーバーとの間で交換するデータを暗号化するかどうかを決定します。 次のいずれかのオプションを選択します。 - SSL。データ暗号化に SSL を使用してセキュアな接続を確立します。Oracle データベースサーバーが SSL を設定できない場合、接続は失敗します。 - 暗号化なし 。SSL を使用せずに接続を確立します。データは暗号化されません。 デフォルトは 【暗号化なし】 です。

接続プロパティ	説明
暗号プロトコルバージョン	<p>暗号化方法として SSL を選択した場合、暗号化された接続を使用するためにサーバーでサポートされている暗号プロトコルを 1 つ指定するか、複数のリストで指定する必要があります。を参照してください。</p> <p>次のいずれかのオプションを選択します。</p> <ul style="list-style-type: none"> - SSLv2 - SSLv3 - TLSv1.2 <p>デフォルトは [TLSv1.2] です。</p>
サーバー証明書の検証	<p>暗号化方法として SSL を選択した場合、このオプションは、Secure Agent が Oracle データベースサーバーから送信されたサーバー証明書を検証するかどうかを制御します。</p> <p>次のいずれかのオプションを選択します。</p> <ul style="list-style-type: none"> - 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。 <p>デフォルトは False です。</p> <p>[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。</p>
トラストストア	暗号化方法として SSL を選択し、サーバー証明書の検証を有効にした場合は、クライアントが SSL 認証で信頼する認証局(CA)のリストが含まれているトラストストアファイルのパスと名前を指定します。
トラストストアパスワード	暗号化方法として SSL を選択し、サーバー証明書の検証を有効にした場合は、トラストストアファイルの内容にアクセスするためのパスワードを指定します。
証明書内のホスト名	暗号化方法として SSL を選択し、サーバー証明書の検証を有効にした場合は、セキュリティを強化するために、Oracle データベースをホストするマシンのホスト名を指定します。Secure Agent は、SSL 証明書のホスト名との接続に含まれるホスト名を検証します。
キーストア	暗号化方法として SSL を選択し、Oracle データベースサーバーでクライアント認証が有効になっている場合は、キーストアファイルのパスと名前を指定します。キーストアファイルには、クライアントが、Oracle サーバーの証明書要求に応答して送信する証明書が含まれます。
キーストアのパスワード	暗号化方法として SSL を選択し、Oracle データベースサーバーでクライアント認証が有効になっている場合は、キーストアファイルのパスワードを指定します。
キーパスワード	暗号化方法として SSL を選択し、Oracle データベースサーバーでクライアント認証が有効になっている場合は、キーストアファイルのキーのパスワードを指定します。このプロパティは、キーのパスワードがキーストアファイルとは異なる場合に使用してください。
データベース接続文字列	アプリケーション取り込みとレプリケーションタスクが 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。

接続プロパティ	説明
TDE ウォレットディレクトリ	<p>Oracle 透過的データ暗号化 (TDE) に使用される Oracle ウォレットファイルを含むディレクトリへのパス。このプロパティ値は、TDE 暗号化テーブルスペースから変更データをキャプチャする場合、かつ、次のいずれかの条件が当てはまる場合にのみ指定してください。</p> <ul style="list-style-type: none"> - 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でないか、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	<p>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。</p>
代替ディレクトリ	<p>Oracle サーバー上の REDO ログのサーバーパスプレフィックスを置き換えるローカルパスプレフィックス。ログリーダーが Oracle サーバー以外のシステムで実行され、別のマッピングを使用して REDO ログファイルにアクセスする場合、置き換え先のローカルパスは必須です。</p> <p>このプロパティは次の状況で使用します。</p> <ul style="list-style-type: none"> - 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。 <p>注: Oracle Automatic Storage Management (ASM) を使用して REDO ログを管理する場合は、このプロパティを使用しないでください。</p> <p>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。</p> <pre>server_path_prefix, local_path_prefix; server_path_prefix, local_path_prefix; ...</pre>
アクティブログマスク	<p>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。</p>
アーカイブターゲット 1	<p>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_<i>n</i> 初期化パラメータの <i>n</i> 値に対応する数値を入力します。ここで <i>n</i> は、1~10 の値です。</p> <p>[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。</p>
アーカイブターゲット 2	<p>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_<i>n</i> 初期化パラメータの <i>n</i> 値に対応する数値を入力します。ここで <i>n</i> は、1~10 の値です。この値は通常、1 より大きい数値です。</p>

接続プロパティ	説明
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する、TNS で定義された Oracle 接続文字列です。
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する、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。
ASM パスワード	Oracle ASM 環境で、[リーダー ASM ユーザー名] プロパティに指定されているユーザーのクリアテキストのパスワード。ログリーダーは、このパスワードと ASM ユーザー名を使用して、ソースデータベースのアクティブ REDO ログとアーカイブ REDO ログのストレージを管理する ASM インスタンスに接続します。
SYSASM として ASM 接続	Oracle 11g 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。
モード	<p>ログリーダーが読み取る Oracle REDO ログのソースとタイプを示します。</p> <p>次のいずれかのオプションを選択します。</p> <ul style="list-style-type: none"> - 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。 <ul style="list-style-type: none"> - 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。 <p>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。</p> <p>デフォルトは ACTIVE です。</p>

接続プロパティ	説明
スタンバイログマスク	<p>Oracle 物理スタンバイデータベースで REDO ログの多重化を使用しているときに、ログリーダーがデータベースの REDO ログを選択するために使用するマスク。ログリーダーは、REDO ロググループ内のメンバ名とマスクを比較して、読み取るログを決定します。マスクでは、アスタリスク (*) ワイルドカードを使用して、0 個以上の文字を表すことができます。</p> <p>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。</p>
スタンバイ接続文字列	データベースが読み取り専用アクセスで開かれていない場合の変更のキャプチャ用に、ログリーダーが Oracle 物理スタンバイデータベースへ接続するために使用する、TNS で定義された Oracle 接続文字列。
スタンバイユーザー名	変更のキャプチャ用に、ログリーダーが Oracle 物理スタンバイデータベースへ接続するために使用するユーザー ID。このユーザー ID には SYSDBA 権限が必要です。
スタンバイパスワード	変更のキャプチャ用に、ログリーダーが Oracle 物理スタンバイデータベースへ接続するために使用するパスワード。
RAC メンバ	<p>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。</p> <p>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。</p>
BFILE アクセス	<p>次の状況では、このチェックボックスをオンにします。</p> <ul style="list-style-type: none"> - BFILE アクセスを使用して、ローカル Oracle サーバ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。 <p>デフォルトでは、このチェックボックスはオフです。</p>
SAP HANA (S/4 トリガベース) データベースの場合	
ユーザー名	SAP HANA インスタンスへの接続に使用するユーザー名。
パスワード	SAP HANA インスタンスに接続するためのパスワード。
ホスト	SAP HANA データベースサーバーをホストするマシンの名前。
ポート	接続先の SAP HANA サーバーのポート番号。デフォルトは 30015 です。
データベース名	SAP HANA ソースデータベース名。

接続プロパティ	説明
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。 <i>property=value</i> エントリを複数指定する場合は、アンパサンド (&) で区切ります。このフィールドに入力できる JDBC 接続プロパティについては、SAP の JDBC Connection Properties のドキュメントを参照してください。例: encrypt=true。
ログのクリア	<p>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。</p> <p>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。</p> <p>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。</p> <p>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。</p> <p>LogClear contains a non numeric number. Caused by: LogClear contains a non numeric number.</p>
トリガプレフィックス	<p>トリガベースのキャプチャメソッドを使用する場合、DML 変更の操作前と操作後のイメージを取得するために CDC スクリプトが各ソーステーブルに対して生成する AFTER DELETE、AFTER INSERT、および AFTER UPDATE トリガの名前にプレフィックスを追加できます。最大 16 文字の任意のプレフィックス値を入力します。トリガ名のプレフィックスの後にアンダースコア (_) が続きます (例: TX_SAP_DEMO_TABLE_DBMI_USER_t_d)。プレフィックスを使用して、サイトのトリガ命名規則に準拠できます。</p>

第 202 章

SAP OData V2 接続のプロパティ

SAP OData V2 接続を作成して、クラウドまたはオンプレミスにデプロイされた SAP の OData V2 準拠アプリケーションから安全な読み取りまたは書き込みを行います。

前提条件

SAP OData V2 サービスに接続するには、SAP 管理者が SAP システムで SAP ユーザーアカウントを設定する必要があります。

さらに、接続プロパティを設定するときに、認証の前提条件を完了する必要があります。

SAP ユーザーアカウントの設定

SAP 管理者は、ユーザーが SAP システム内の OData V2 準拠アプリケーションにアクセスできるように、S_SERVICE 認証オブジェクトを設定します。

次の表に、S_SERVICE 認証オブジェクトが SAP でユーザー権限を設定するために必要なフィールドと値を示します。

フィールド	値
SRV_NAME	接続先の SAP サービス名を指定します。
SRV_TYPE	リストから [TADIR オブジェクトのハッシュ値] オプションを選択します。

認証オブジェクトとその使用方法の詳細については、「[SAP user authorizations](#)」を参照してください。

認証の準備

基本認証、API キー認証、認証コードの認証、およびクライアント資格情報認証のタイプを設定して、SAP の OData V2 準拠アプリケーションにアクセスできます。データ取り込みおよびレプリケーションでは基本認証のみ適用されます。

接続プロパティを設定する前に、使用する認証のタイプに基づいて認証の詳細を用意しておく必要があります。

基本

基本認証を使用して SAP OData V2 サービスに接続するには、SAP アカウントのユーザー名とパスワードが必要です。

接続先の SAP アプリケーションから必要な詳細を取得します。

SAP の基本認証の詳細については、SAP のマニュアルの「[Basic authentication](#)」を参照してください。

API キー

API キー認証を使用して SAP OData V2 サービスに接続するには、SAP OData エンドポイントに対して実行される API 呼び出しを SAP OData V2 コネクタが認証するために使用する一意の API キーが必要です。

接続先の SAP アプリケーションから API キーを取得します。

API キーの生成方法と使用方法の詳細については、SAP のマニュアルの「[Add API keys to an environment](#)」を参照してください。

承認コード

OAuth 2.0 認証コードを使用して SAP OData V2 サービスに接続するには、SAP クライアント ID、クライアントシークレット、認証トークン URL、アクセストークン URL、およびアクセストークンが必要です。

OAuth 2.0 認証コードの認証を使用する前に、次のタスクを完了してください。

- SAP で認証統合を作成し、Informatica リダイレクト URL を SAP Integration Suite に登録します。
SAP Integration Suite は、OAuth をサポートするクライアントがユーザーを認証ページにリダイレクトし、SAP にアクセスするためのアクセストークン、および必要に応じて更新トークンを生成できるようにする、サービスとしての統合プラットフォームです。

次の Informatica リダイレクト URL を SAP Integration Suite に登録します。

`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 401 エラーコードが返された場合に、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。

認証統合を作成し、認証の詳細を取得する方法の詳細については、SAP のマニュアルの「[OAuth 2.0 authorization code](#)」を参照してください。

- Secure Agent インストール内の次の 1 つ以上の場所にある jdk ディレクトリにある cacerts ファイルに .cer 証明書をインポートします。
 - <Secure Agent インストールディレクトリ>/jdk/jre/lib/security
 - <Secure Agent インストールディレクトリ>/jdk/lib/security
 - <Secure Agent インストールディレクトリ>/jdk8/jre/lib/security使用可能なすべてのディレクトリに証明書を追加してください。
- <Secure Agent インストールディレクトリ>\apps フォルダ内に jdk ディレクトリがある場合は、次のディレクトリに移動し、Secure Agent インストール内の次の 1 つ以上の場所にある jdk ディレクトリにある cacerts ファイルに .cer 証明書をインポートします。
 - <Secure Agent インストールディレクトリ>\apps\jdk\zulu8<latest_version>\jre\lib\security
 - <Secure Agent インストールディレクトリ>\apps\jdk\zulu17<latest_version>\lib\security

.cer 証明書を cacerts ファイルにインポートした後に、Secure Agent を再起動する必要があります。

クライアント資格情報

OAuth 2.0 クライアント資格情報を使用して SAP OData V2 サービスに接続するには、SAP クライアント ID、クライアントシークレット、アクセストークン URL、およびアクセストークンが必要です。

OAuth 2.0 クライアント資格情報認証を使用する前に、次のタスクを完了してください。

- クライアント資格情報付与タイプを使用して OAuth エンドポイントを設定し、次に認証統合を作成して SAP システムで認証の詳細を取得します。
認証統合を作成し、認証の詳細を取得する方法の詳細については、SAP のマニュアルの「[OAuth 2.0 client credentials](#)」を参照してください。
 - Secure Agent インストール内の次の 1 つ以上の場所にある jdk ディレクトリにある cacerts ファイルに .cer 証明書をインポートします。
 - <Secure Agent インストールディレクトリ>/jdk/jre/lib/security
 - <Secure Agent インストールディレクトリ>/jdk/lib/security
 - <Secure Agent インストールディレクトリ>/jdk8/jre/lib/security使用可能なすべてのディレクトリに証明書を追加してください。
 - <Secure Agent インストールディレクトリ>\apps フォルダ内に jdk ディレクトリがある場合は、次のディレクトリに移動し、Secure Agent インストール内の次の 1 つ以上の場所にある jdk ディレクトリにある cacerts ファイルに .cer 証明書をインポートします。
 - <Secure Agent インストールディレクトリ>\apps\jdk\zulu8<latest_version>\jre\lib\security
 - <Secure Agent インストールディレクトリ>\apps\jdk\zulu17<latest_version>\lib\security
- .cer 証明書を cacerts ファイルにインポートした後に、Secure Agent を再起動する必要があります。

SAP OData V2 への接続

SAP OData V2 サービスに接続し、SAP で OData V2 準拠アプリケーションの読み取りまたは書き込みを行うように、SAP OData V2 接続プロパティを設定してみましょう。

始める前に

開始する前に、設定する認証タイプに基づいて SAP システムを設定し、SAP アカウントから関連する設定情報を取得する必要があります。

設定の前提条件の詳細については、「[「前提条件」 \(ページ 776\)](#)」を参照してください。

接続の詳細

次の表に、基本接続プロパティを示します。

財産	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。

財産	説明
シークレットコンテナの使用	<p>組織に対して設定されている Secrets Manager にこの接続の機密資格情報を保存します。</p> <p>このプロパティは、組織に Secrets Manager が設定されている場合にのみ表示されます。</p> <p>このプロパティは、データ取り込みおよびレプリケーションとデータアクセス管理サービスではサポートされていません。</p> <p>接続でシークレットコンテナを有効にすると、Secure Agent が Secrets Manager からどの資格情報を取得するかを選択できます。このオプションを無効にした場合、資格情報は組織の設定方法に応じてリポジトリまたはローカル Secure Agent に保存されます。</p> <p>注: この接続を使用してプッシュダウンまたはプロキシサービスを介してデータアクセスポリシーを適用する場合、シークレットコンテナ設定オプションを使用することはできません。</p> <p>Secrets Manager を設定および使用方法については、Administrator のヘルプにある「Secrets Manager の設定」を参照してください。</p>
ランタイム環境	<p>タスクを実行するランタイム環境の名前。</p> <p>Secure Agent またはエラスティックランタイム環境を選択します。</p> <p>アプリケーション取り込みとレプリケーションの増分ロードジョブと組み合わせロードジョブでは Secure Agent を選択する必要がありますが、初期ロードジョブでは、Secure Agent またはサーバーレスランタイム環境のいずれかを選択できます。ホステッドエージェントまたはエラスティックランタイム環境は使用できません。</p> <p>ランタイム環境の設定および使用方法の詳細については、Administrator のヘルプにある「ランタイム環境」を参照してください。</p>
サービスタイプ	<p>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。</p> <p>リストから次のいずれかのサービスタイプを選択します。</p> <ul style="list-style-type: none"> - デフォルト。特定の SAP サービスに接続します。 - SAP ゲートウェイカタログ。SAP ゲートウェイで使用可能なすべてのサービスのリストを提供する SAP カタログサービスに接続します。 <p>デフォルト値は [デフォルト] です。</p>
サービス URL	<p>選択したサービスタイプのサービス URL。</p> <p>【デフォルト】 サービスタイプを選択した場合は、次の形式でサービスのルート URL を入力します。</p> <p>http://<SAP サーバーのホスト名>:<ポート番号>/sap/opu/odata/sap/<サービス名>/</p> <p>例えば、ホスト名が http://invs15con01.informatica.com でポート番号が 8081 のときに SAP の ZALL_DATATYPE_SRV サービスに接続する場合は、次のサービス URL を入力します。</p> <p>http://<SAP サーバーのホスト名>:<ポート番号>/sap/opu/odata/sap/ZALL_DATATYPE_SRV/</p> <p>注: アプリケーション取り込みおよびレプリケーションタスクに接続を使用する場合は、デフォルトのサービスタイプの URL の末尾に「/」を追加しないでください。タスクがソースからスキーマを取得できなくなります。</p> <p>【SAP ゲートウェイカタログ】 サービスタイプを選択した場合は、次の形式でサービス URL を入力します。</p> <p>http://<SAP サーバーのホスト名>:<ポート番号>/sap/opu/odata/IWFND/<カタログサービス名></p> <p>例えば、ホスト名が abcd01con02.example.com でポート番号が 8081 のときに SAP の CATALOGSERVICE;v=2 カタログサービスに接続する場合は、次のサービス URL を入力します。</p> <p>http://abcd01con02.example.com:8081/sap/opu/odata/IWFND/CATALOGSERVICE;v=2</p>

認証タイプ

基本認証、API キー認証、認証コードの認証、およびクライアント資格情報認証のタイプを設定して、SAP の OData V2 準拠アプリケーションにアクセスできます。データ取り込みおよびレプリケーションでは基本認証のみ適用されます。

必要な認証方法を選択し、認証固有のパラメータを設定します。

基本認証

基本認証は、少なくとも SAP アカウント名とパスワードが必要なデフォルトのタイプです。

次の表に、基本認証の基本的な接続プロパティとその説明を示します。

プロパティ	説明
ユーザー名	SAP OData V2 サービスに接続するためのユーザー名。
パスワード	SAP OData V2 サービスに接続するためのパスワード。

詳細設定

次の表に、基本認証の詳細接続プロパティとその説明を示します。

プロパティ	説明
SAP カスタムクエリオプション	<p>SAP OData V2 サービスへの接続時に使用できる追加のカスタムクエリ。</p> <p>複数の SAP カスタムクエリをアンパサンド (&) で区切って、次の形式で入力できます。</p> <pre><Custom query1>=<value>&<Custom query2>=<value>&<Custom query3>=<value>....</pre> <p>例えば、SAP OData V2 サービスへの接続時に SAP クライアント番号と言語コードを渡す場合は、次のカスタムクエリを入力します。</p> <pre>sap-client=400&sap-language=DE</pre> <p>クエリを追加する場合は、等号 (=) の前後にスペースを加えないようにしてください。</p> <p>設定できる SAP カスタムクエリのリストの詳細については、SAP のマニュアルの「SAP URL parameters」を参照してください。</p> <p>このプロパティは、データ取り込みおよびレプリケーションには適用されません。</p>

API キー認証

API キー認証には、SAP アプリケーションからの少なくとも 1 つの一意の API キーが必要です。

次の表に、共有キー認証の基本接続プロパティとその説明を示します。

プロパティ	説明
API キー	SAP OData V2 コネクタが SAP OData エンドポイントに対して実行される API 呼び出しを認証するために使用する一意の API キー。

詳細設定

次の表に、共有キー認証の詳細接続プロパティとその説明を示します。

プロパティ	説明
SAP カスタムクエリオプション	<p>SAP OData V2 サービスへの接続時に使用できる追加のカスタムクエリ。</p> <p>複数の SAP カスタムクエリをアンパサンド (&) で区切って、次の形式で入力できます。</p> <pre><Custom query1>=<value>&<Custom query2>=<value>&<Custom query3>=<value>...</pre> <p>例えば、SAP OData V2 サービスへの接続時に SAP クライアント番号と言語コードを渡す場合は、次のカスタムクエリを入力します。</p> <pre>sap-client=400&sap-language=DE</pre> <p>クエリを追加する場合は、等号 (=) の前後にスペースを加えないようにしてください。</p> <p>設定できる SAP カスタムクエリのリストの詳細については、SAP のマニュアルの「SAP URL parameters」を参照してください。</p>

認証コードの認証

OAuth 2.0 認証コードの認証には、少なくとも SAP クライアント ID、クライアントシークレット、認証トークン URL、アクセストークン URL、およびアクセストークンが必要です。

次の表に、OAuth 2.0 認証コードの認証の基本的な接続プロパティに関する説明を示します。

プロパティ	説明
認証トークン URL	<p>ユーザー要求の承認に使用される OAuth 2.0 認証サーバーの SAP 認証トークンエンドポイント。</p> <p>認証トークン URL は次の形式で入力します。</p> <pre>https://<サーバーのホスト名>:<ポート番号>/sap/bc/sec/oauth2/authorize?sap-client=<SAP クライアント番号></pre> <p>例えば、ホスト名が <code>abcd01con02.example.com</code>、ポート番号が <code>44301</code>、SAP クライアント番号が <code>800</code> の場合は、次の認証トークン URL を入力します。</p> <pre>https://abcd01con02.example.com:44301/sap/bc/sec/oauth2/authorize?sap-client=800</pre>
アクセストークン URL	<p>OAuth 2.0 認証サーバーの SAP アクセストークンエンドポイントで、認証コードを交換してアクセストークンを取得するために使用されます。</p> <p>アクセストークン URL は次の形式で入力します。</p> <pre>https://<サーバーのホスト名>:<ポート番号>/sap/bc/sec/oauth2/token?sap-client=<SAP クライアント番号></pre> <p>例えば、ホスト名が <code>abcd01con02.example.com</code>、ポート番号が <code>44301</code>、SAP クライアント番号が <code>800</code> の場合は、次のアクセストークン URL を入力します。</p> <pre>https://abcd01con02.example.com:44301/sap/bc/sec/oauth2/token?sap-client=800</pre>

プロパティ	説明
クライアント ID	アプリケーションを OAuth 用に設定したときに生成されるアプリケーションのクライアント識別子。
クライアントシークレット	クライアント ID に生成されたクライアントシークレット。
アクセストークン	<p>認証サーバーによって付与された、SAP データにアクセスするためのアクセストークン。</p> <p>OAuth エンドポイントから取得して取り込んだアクセストークン値を入力するか、[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値を入力します。</p>

詳細設定

次の表に、OAuth 2.0 認証コードの認証の詳細接続プロパティに関する説明を示します。

プロパティ	説明
スコープ	<p>SAP OData V2 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。</p> <p>複数のスコープ属性をそれぞれスペースで区切って、次の形式で入力できます。</p> <pre><Scope attribute1> <Scope attribute2> <Scope attribute3>....</pre> <p>例えば、次のスコープ属性を入力します。</p> <pre>ZGWSAMPLE_BASIC_0001 /IWFND/SG_MED_CATALOG_0002 ZAPI_CHARTOFACCOUNTS_SRV_0001</pre>
アクセストークンパラメータ	<p>アクセストークン URL で使用する追加パラメータ。</p> <p>アクセストークンのパラメータを次の JSON 形式で定義します：</p> <pre>[{"Name": "<パラメータ名>", "Value": "<パラメータ値>"}]</pre> <p>定義できるアクセストークンのパラメータの詳細については、SAP のマニュアルを参照してください。</p>
認証コードパラメータ	<p>認証トークン URL で使用する追加パラメータ。</p> <p>複数のパラメータをカンマで区切って、次の JSON 形式で定義します。</p> <pre>[{"Name": "<パラメータ名>", "Value": "<パラメータ値>"}, {"Name": "<パラメータ名>", "Value": "<パラメータ値>"}]</pre> <p>例えば、SAP OData V2 サービスへの接続時に、次の最大経過時間と状態のパラメータを使用できます。</p> <pre>[{"Name": "max_age", "Value": 60}, {"Name": "state", "Value": "test"}]</pre> <p>定義できる認証コードのパラメータの詳細については、SAP のマニュアルを参照してください。</p>

プロパティ	説明
クライアント認証	<p>SAP OData V2 サービスに接続するための認証のために、クライアント認証の詳細を送信する方法。</p> <p>リストから次のいずれかのクライアント認証を選択します。</p> <ul style="list-style-type: none"> - 本文でクライアント資格情報を送信する。認証用のクライアント ID とクライアントシークレットを要求の本文で送信します。 - 基本認証ヘッダー。認証用のクライアント ID とクライアントシークレットを要求のヘッダーで送信します。 <p>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。</p>
更新トークン	<p>更新トークンの値。</p> <p>OAuth エンドポイントから取得して取り込んだ更新トークン値を入力するか、【アクセストークンの生成】をクリックして更新トークン値を入力します。アクセストークンが有効ではない場合または有効期限が切れている場合、Secure Agent は、更新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。</p> <p>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、【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します。</p>
SAP カスタムクエリオプション	<p>SAP OData V2 サービスへの接続時に使用できる追加のカスタムクエリ。</p> <p>複数の SAP カスタムクエリをアンパサンド (&) で区切って、次の形式で入力できます。</p> <p><Custom query1>=<value>&<Custom query2>=<value>&<Custom query3>=<value>....</p> <p>例えば、SAP OData V2 サービスへの接続時に SAP クライアント番号と言語コードを渡す場合は、次のカスタムクエリを入力します。</p> <p>sap-client=400&sap-language=DE</p> <p>クエリを追加する場合は、等号 (=) の前後にスペースを加えないようにしてください。</p> <p>設定できる SAP カスタムクエリのリストの詳細については、SAP のマニュアルの「SAP URL parameters」を参照してください。</p>

クライアント資格情報の認証

OAuth 2.0 クライアント資格情報の認証には、少なくとも SAP クライアント ID、クライアントシークレット、アクセストークン URL、およびアクセストークンが必要です。

次の表に、OAuth 2.0 クライアント資格情報の認証の基本的な接続プロパティとその説明を示します。

プロパティ	説明
アクセストークン URL	<p>OAuth 2.0 認証サーバーの SAP アクセストークンエンドポイントで、認証コードを交換してアクセストークンを取得するために使用されます。</p> <p>アクセストークン URL は次の形式で入力します。</p> <p><code>https://<サーバーのホスト名>:<ポート番号>/sap/bc/sec/oauth2/token?sap-client=<SAP クライアント番号></code></p> <p>例えば、ホスト名が <code>abcd01con02.example.com</code>、ポート番号が <code>44301</code>、SAP クライアント番号が <code>800</code> の場合は、次のアクセストークン URL を入力します。</p> <p><code>https://abcd01con02.example.com:44301/sap/bc/sec/oauth2/token?sap-client=800</code></p>
クライアント ID	アプリケーションを OAuth 用に設定したときに生成されるアプリケーションのクライアント識別子。
クライアントシークレット	クライアント ID に生成されたクライアントシークレット。
アクセストークン	<p>認証サーバーによって付与された、SAP データにアクセスするためのアクセストークン。</p> <p>OAuth エンドポイントから取得して取り込んだアクセストークン値を入力するか、[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値を入力します。</p>

詳細設定

次の表に、OAuth 2.0 クライアント資格情報の認証の詳細接続プロパティに関する説明を示します。

プロパティ	説明
スコープ	<p>SAP OData V2 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。</p> <p>複数のスコープ属性をそれぞれスペースで区切って、次の形式で入力できます。</p> <p><code><Scope attribute1> <Scope attribute2> <Scope attribute3>....</code></p> <p>例えば、次のスコープ属性を入力します。</p> <p><code>ZGWSAMPLE_BASIC_0001 /IWFND/SG_MED_CATALOG_0002 ZAPI_CHARTOFACCOUNTS_SRV_0001</code></p>
アクセストークンパラメータ	<p>アクセストークン URL で使用する追加パラメータ。</p> <p>アクセストークンのパラメータを次の JSON 形式で定義します：</p> <p><code>[{"Name": "<パラメータ名>", "Value": "<パラメータ値>"}]</code></p> <p>定義できるアクセストークンのパラメータの詳細については、SAP のマニュアルを参照してください。</p>

プロパティ	説明
クライアント認証	<p>SAP OData V2 サービスに接続するための認証のために、クライアント認証の詳細を送信する方法。</p> <p>リストから次のいずれかのクライアント認証を選択します。</p> <ul style="list-style-type: none"> - 本文でクライアント資格情報を送信する。認証用のクライアント ID とクライアントシークレットを要求の本文で送信します。 - 基本認証ヘッダー。認証用のクライアント ID とクライアントシークレットを要求のヘッダーで送信します。 <p>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。</p>
SAP カスタムクエリオプション	<p>SAP OData V2 サービスへの接続時に使用できる追加のカスタムクエリ。</p> <p>複数の SAP カスタムクエリをアンパサンド (&) で区切って、次の形式で入力できます。</p> <pre><Custom query1>=<value>&<Custom query2>=<value>&<Custom query3>=<value>....</pre> <p>例えば、SAP OData V2 サービスへの接続時に SAP クライアント番号と言語コードを渡す場合は、次のカスタムクエリを入力します。</p> <pre>sap-client=400&sap-language=DE</pre> <p>クエリを追加する場合は、等号 (=) の前後にスペースを加えないようにしてください。</p> <p>設定できる SAP カスタムクエリのリストの詳細については、SAP のマニュアルの「SAP URL parameters」を参照してください。</p>

負荷分散接続の設定

SAP OData V2 接続で基本認証タイプを使用して、SAP サーバーに接続するときに負荷分散接続を作成できます。

負荷分散用の接続を設定すると、実行時に最も負荷が少ない SAP サーバーに接続できます。この機能は、データ取り込みおよびレプリケーションには適用されません。

負荷分散接続に基本認証タイプを使用する SAP OData V2 接続を設定する前に、前提条件のタスクを実行する必要があります。

- Secure Agent インストール内の次の 1 つ以上の場所にある jdk ディレクトリにある cacerts ファイルに .cer 証明書をインポートします。
 - <Secure Agent インストールディレクトリ>/jdk/jre/lib/security
 - <Secure Agent インストールディレクトリ>/jdk/lib/security
 - <Secure Agent インストールディレクトリ>/jdk8/jre/lib/security

使用可能なすべてのディレクトリに証明書を追加してください。

2. <Secure Agent インストールディレクトリ>\apps フォルダ内に jdk ディレクトリがある場合は、次のディレクトリに移動し、Secure Agent インストール内の次の 1 つ以上の場所にある jdk ディレクトリにある cacerts ファイルに .cer 証明書をインポートします。
 - <Secure Agent インストールディレクトリ>\apps\jdk\zulu8<latest_version>\jre\lib\security
 - <Secure Agent インストールディレクトリ>\apps\jdk\zulu17<latest_version>\lib\security
3. Secure Agent を再起動します。

プロキシサーバーの設定

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

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

プロキシ設定は、マッピングおよび詳細モードのマッピングで使用される接続に適用されます。プロキシ設定は、データ取り込みおよびレプリケーションには適用されません。

Secure Agent のプロキシの設定を行うには、次のタスクを実行します。

- Windows の場合は Secure Agent Manager を使用し、Linux の場合はシェルコマンドを使用して Secure Agent を設定します。
手順については、データ統合のヘルプの『または「Windows でのプロキシ設定」または「Linux でのプロキシ設定」を参照してください。
- Secure Agent のプロパティで、DTM の JVM オプションを設定します。手順については、ナレッジベースの記事「[Proxy server settings](#)」を参照してください。
- proxy.ini ファイルでプロキシサーバーのプロパティを設定します。

第 203 章

SAP OData V4 接続のプロパティ

SAP OData V4 接続を作成して、SAP Datasphere および SAP S/4HANA アプリケーションなどの OData V4 準拠アプリケーションに対する安全な読み書きを行います。

認証の準備

「基本」認証タイプと「認証コード」認証タイプは、それぞれ、SAP S/4HANA と SAP Datasphere に接続するように設定することができます。

接続プロパティを設定する前に、使用する認証のタイプに基づいて認証の詳細を用意しておく必要があります。

基本

基本認証を使用すると、SAP S/4HANA アプリケーションに接続できます。基本認証を設定するには、SAP アカウントのユーザー名とパスワードが必要です。

接続先の SAP S/4HANA アプリケーションから必要な詳細を取得します。

SAP の基本認証の詳細については、SAP のマニュアルの「[Basic authentication](#)」を参照してください。

承認コード

「OAuth 2.0 認証コード」認証を使用すると、SAP Datasphere アプリケーションに接続できます。「OAuth 2.0 認証コード」認証を設定するには、SAP クライアント ID、クライアントシークレット、承認トークン URL、アクセストークン URL、およびアクセストークンが必要です。

認証の詳細を取得するには、SAP で認証統合を作成し、Informatica リダイレクト URL を SAP Integration Suite に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 401 エラーコードが返された場合に、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。

認証統合を作成し、認証の詳細を取得する方法の詳細については、SAP のマニュアルの「[OAuth 2.0 authorization code](#)」を参照してください。

SAP OData V4 への接続

SAP Datasphere または SAP S/4HANA アプリケーションに接続するように SAP OData V4 接続プロパティを設定しましょう。

始める前に

開始する前に、設定する認証タイプに基づいて、関連する設定の詳細を SAP アカウントから取得する必要があります。

認証の前提条件の詳細については、「[認証の準備](#)」 ([ページ 787](#))を参照してください。

接続の詳細

次の表に、基本接続プロパティを示します。

財産	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。
シークレットコンテナの使用	組織に対して設定されている Secrets Manager にこの接続の機密資格情報を保存します。 このプロパティは、組織に Secrets Manager が設定されている場合にのみ表示されます。 このプロパティは、データ取り込みおよびレプリケーションとデータアクセス管理サービスではサポートされていません。 接続でシークレットコンテナを有効にすると、Secure Agent が Secrets Manager からどの資格情報を取得するかを選択できます。このオプションを無効にした場合、資格情報は組織の設定方法に応じてリポジトリまたはローカル Secure Agent に保存されます。 注: この接続を使用してプッシュダウンまたはプロキシサービスを介してデータアクセスポリシーを適用する場合、シークレットコンテナ設定オプションを使用することはできません。 Secrets Manager を設定および使用する方法については、Administrator のヘルプにある「Secrets Manager の設定」を参照してください。
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。 Secure Agent 環境またはエラスティックランタイム環境を選択します。 ランタイム環境の設定および使用方法の詳細については、Administrator のヘルプにある「ランタイム環境」を参照してください。
SAP アプリケーションタイプ	SAP OData V4 サービスエンドポイントの SAP アプリケーションタイプ。 リストから次のいずれかのアプリケーションタイプを選択します。 - SAP Datasphere。SAP Datasphere アプリケーションに接続します。SAP Datasphere にアクセスするように、「OAuth 2.0 認証コード」認証タイプを設定します。 - SAP S/4HANA。SAP S/4HANA アプリケーションに接続します。SAP S/4HANA にアクセスするように「基本」認証タイプを設定します。 デフォルトは SAP Datasphere です。

財産	説明
サービス タイプ	<p>接続する SAP OData V4 サービスエンドポイントのサービスタイプ。 リストから次のいずれかのサービスタイプを選択します。</p> <ul style="list-style-type: none"> - デフォルト。特定の SAP サービスに接続します。 - SAP ゲートウェイカタログ。SAP ゲートウェイで使用可能なすべてのサービスのリストを提供する SAP カatalogサービスに接続します。 <p>デフォルト値は [デフォルト] です。</p>
サービス URL	<p>選択したアプリケーションタイプとサービスタイプに対するサービス URL。 選択したアプリケーションタイプとサービスタイプに応じて、次の形式でサービス URL を入力します。</p> <ul style="list-style-type: none"> - SAP Datasphere アプリケーションタイプとデフォルトサービスタイプの場合: https://<SAP サーバーのホスト名>/api/v1/dwc/consumption/relational/<SAP Datasphere のスペース名>/<SAP Datasphere のアセット名>/ - SAP Datasphere アプリケーションタイプと SAP ゲートウェイカタログサービスタイプの場合: https://<SAP サーバーのホスト名>/api/v1/dwc/<SAP Datasphere のカタログサービス名>/ - SAP S/4HANA アプリケーションタイプとデフォルトサービスタイプの場合: http://<SAP サーバーのホスト名>:<ポート番号>/sap/opu/odata4/sap/<サービス名>/<サービスのパス>/<バージョン番号>/ - SAP S/4HANA アプリケーションタイプと SAP ゲートウェイカタログサービスタイプの場合: http://<SAP サーバーのホスト名>:<ポート番号>/sap/opu/odata4/iwfnd/config/default/iwfnd/<SAP S/4HANA のカタログサービス名>/<バージョン番号>/

認証タイプ

「基本」認証タイプと「認証コード」認証タイプは、それぞれ、SAP S/4HANA と SAP Datasphere に接続するように設定することができます。

必要な認証タイプを選択し、認証固有のパラメータを設定します。

基本認証

基本認証に最低限必要なものは、SAP アカウントのユーザー名とパスワードです。「基本」認証タイプを使用すると、SAP S/4HANA アプリケーションに接続できます。

次の表に、標準認証の基本的な接続プロパティとその説明を示します。

プロパティ	説明
ユーザー名	SAP S/4HANA アプリケーションへの接続に使用するユーザー名。
パスワード	SAP S/4HANA アプリケーションに接続するために必要な、ユーザー名に対するパスワード。

認証コードの認証

「OAuth 2.0 認証コード」認証はデフォルトの認証タイプです。「OAuth 2.0 認証コード」認証に最低限必要なものは、SAP クライアント ID、クライアントシークレット、承認トークン URL、アクセストークン URL、およびアクセストークンです。

「OAuth 2.0 認証コード」認証タイプを使用すると、SAP Datasphere アプリケーションに接続できます。
次の表に、OAuth 2.0 認証コードの認証の基本的な接続プロパティに関する説明を示します。

プロパティ	説明
認証トークン URL	ユーザー要求の認証に使用される SAP OAuth 2.0 認証サーバー。 認証トークン URL は次の形式で入力します。 <code>https://<サーバーのホスト名>/oauth/authorize</code> 例えば、ホスト名が <code>example.authentication.us01.hana.ondemand.com</code> の場合は、次の認証トークン URL を入力します。 <code>https://example.authentication.us01.hana.ondemand.com/oauth/authorize</code>
アクセストークン URL	認証コードを交換することでアクセストークンを取得するために使用される SAP OAuth 2.0 認証サーバー。 アクセストークン URL は次の形式で入力します。 <code>https://<サーバーのホスト名>/oauth/token</code> 例えば、ホスト名が <code>example.authentication.us01.hana.ondemand.com</code> の場合は、次のアクセストークン URL を入力します。 <code>https://example.authentication.us01.hana.ondemand.com/oauth/token</code>
クライアント ID	アプリケーションを OAuth 用に設定したときに生成されるアプリケーションのクライアント識別子。
クライアントシークレット	クライアント ID に生成されたクライアントシークレット。
アクセストークン	認証サーバーによって付与された、SAP データにアクセスするためのアクセストークン。 OAuth エンドポイントから取得して取り込んだアクセストークン値を入力するか、 【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値を入力します。

プロキシサーバーの設定

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

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

プロキシ設定は、マッピングおよび詳細モードのマッピングで使用される接続に適用されます。

Secure Agent のプロキシの設定を行うには、次のタスクを実行します。

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

手順については、データ統合のヘルプの『または「Windows でのプロキシ設定」または「Linux でのプロキシ設定」を参照してください。

- Secure Agent のプロパティで、DTM の JVM オプションを設定します。手順については、ナレッジベースの記事「[Proxy server settings](#)」を参照してください。
- proxy.ini ファイルでプロキシサーバーのプロパティを設定します。

第 204 章

SAP ODP Extractor 接続のプロパティ

SAP ODP オブジェクトからデータを安全に読み取るには、SAP ODP Extractor 接続を作成します。

SAP ODP Extractor 接続を使用して、次のアプリケーションからデータを読み取ることができます。

- SAP S/4HANA
- ECC
- オペレーショナルデータプロビジョニング（ODP）対応アプリケーション
- オペレーショナルデルタキュー（ODQ）対応アプリケーション

前提条件

SAP ODP Extractor 接続を使用する前に、SAP 管理者は特定の前提条件のタスクを実行して Secure Agent マシンと SAP システムを設定する必要があります。

また、SAP ODP データを処理するには、必要なライセンスが SAP システムで有効になっているかどうかを確認する必要があります。

SAP サーバーに必要な SAP Notes の確認

SAP ODP オブジェクトからデータの読み取りを行うには、必要な SAP Notes が SAP サーバーで使用可能であることを確認する必要があります。

- 1931427 - ODP Data Replication API 2.0
- 2232584 - ODP レプリケーション用の SAP エクストラクタのリリース（ODP SAPI）

SAP ODP Extractor コネクタは、SAP ODP オブジェクトからデータの読み取りを行うときに ODP Replication APIs バージョン 2.0 を使用します。

SAP ライブラリのダウンロードと設定

SAP ODP オブジェクトからデータの読み取りを行うには、Secure Agent マシンに SAP JCo ライブラリをダウンロードして設定する必要があります。ライブラリのダウンロードで問題が発生した場合は、SAP カスタマサポートにお問い合わせください。

1. [SAP Support Portal](#) に移動し、[ソフトウェアのダウンロード] をクリックします。

注: [SAP Support Portal](#) から [ソフトウェアのダウンロード] にアクセスするには、SAP 資格情報が必要です。

2. Secure Agent を実行するオペレーティングシステムに基づいて、64 ビットの SAP JCo ライブラリの最新のバージョンをダウンロードします。

オペレーティングシステム	SAP JCo ライブラリ
Windows	- sapjco3.jar - sapjco3.dll
Linux	- sapjco3.jar - libsapjco3.so

3. 次のディレクトリに JCo ライブラリをコピーします。

<Informatica Secure Agent installation directory>\apps\Data_Integration_Server\ext\deploy_to_main\bin\rdtm-extra\tpl\sap

存在しない場合は、deploy_to_main\bin\rdtm-extra\tpl\sap ディレクトリを作成します。

4. Informatica Intelligent Cloud Services にログインし、Secure Agent の JAVA_LIBS プロパティを設定します。
 - a. [Administrator] > [ランタイム環境] の順に選択します。
 - b. [ランタイム環境] をクリックして、[ランタイム環境] ページにアクセスします。
 - c. エージェント名の左側で、[Secure Agent の編集] をクリックします。
 - d. [サービス] リストから、[データ統合サーバー] を選択します。
 - e. [タイプ] リストから、[Tomcat JRE] を選択します。
 - f. Secure Agent が実行されるオペレーティングシステムに基づいて JAVA_LIBS 値を入力します。

オペレーティングシステム	値
Windows	..\bin\rdtm-extra\tpl\sap\sapjco3.jar;..\bin\rdtm\javalib\sap\sap-adapter-common.jar
Linux	../bin/rdtm-extra/tpl/sap/sapjco3.jar:../bin/rdtm/javalib/sap/sap-adapter-common.jar

警告: テーブルから値を直接コピーすると、値のハイフン (-) が誤ってコピーされることがあります。値をテキストエディタにコピーし、コピーした値が破損していないことを確認します。

System Configuration Details Reset All

Service:

Data Integration Server

Type:

Tomcat JRE

Type	Name	Value
Tomcat JRE	JAVA_LIBS	../bin/rdtm-extra/tpl/sap/sapjco3.jar:../bin/rdtm/javalib/sap/sap-ada

- g. **【保存】** をクリックします。
5. JAVA_LIBS 値を保存した後に、Secure Agent の JVMClassPath プロパティを設定します。
 - a. **【サービス】** リストから、**【データ統合サーバー】** を選択します。
 - b. **【タイプ】** リストで、**【DTM】** を選択します。
 - c. Secure Agent が実行されているオペレーティングシステムに基づいて、JVMClassPath 値を入力します。

オペレーティングシステム	値
Windows	pmserverjdk.jar;..\bin\rdtm-extra\tpl\sap\sapjco3.jar;..\bin\rdtm\javalib\sap\sap-adapter-common.jar
Linux	pmserverjdk.jar;../bin/rdtm-extra/tpl/sap/sapjco3.jar;../bin/rdtm/javalib/sap/sap-adapter-common.jar

警告: テーブルから値を直接コピーすると、値のハイフン (-) が誤ってコピーされることがあります。値をテキストエディタにコピーし、コピーした値が破損していないことを確認します。

System Configuration Details

Service:

Type:

Type	Name	Value
DTM	JVMClassPath	pmserverjdk.jar;../bin/rdtm-extra/tpl/sap/sapjco3.jar;../bin/rdtm/

- d. **【保存】** をクリックします。
- e. Secure Agent をインストールしたすべてのマシンで手順 2 - 5 を繰り返します。
6. Secure Agent を再起動します。

SAP ユーザー権限の設定

SAP システムで SAP ユーザーアカウントを設定し、SAP ODP データを処理します。

SAP システムで SAP ユーザー認証を設定する方法の詳細については、「[SAP user authorizations](#)」を参照してください。

次の表に、SAP ODP オブジェクトから読み取りを行うために必要な権限を示します。

読み取りオブジェクト名	権限値	値	アクティビティ	設計時間/実行時間
S_RFC	RFC_TYPE - 関数グループ (FUGR)	SYST	16	前後方向
	RFC_TYPE - 関数モジュール (FUGR)	RFC1	16	前後方向
	RFC_TYPE - 関数モジュール (FUNC)	RFCPING	16	前後方向
	RFC_TYPE - 関数グループ (FUGR)	RFC_METADATA	16	前後方向

読み取りオブジェクト名	権限値	値	アクティビティ	設計時間/実行時間
	RFC_TYPE - 関数モジュール (FUNC)	RFC_METADATA_GET	16	前後方向
	RFC_TYPE - 関数モジュール (FUNC)	RFC_GET_FUNCTION_INTERFACE	16	前後方向
	RFC_TYPE - 関数モジュール (FUNC)	RODPS_REPL_CONTEXT_GET_LIST	16	前後方向
	RFC_TYPE - 関数モジュール (FUNC)	RODPS_REPL_ODP_GET_DETAIL	16	前後方向
	RFC_TYPE - 関数モジュール (FUNC)	RODPS_REPL_ODP_GET_LIST	16	前後方向
	RFC_TYPE - 関数モジュール (FUNC)	RODPS_REPL_ODP_OPEN	16	前後方向
	RFC_TYPE - 関数モジュール (FUNC)	RODPS_REPL_ODP_CLOSE	16	前後方向
	RFC_TYPE - 関数モジュール (FUNC)	/INFADI/ODP_FETCH_XML	16	ランタイム
	RFC_TYPE - 関数モジュール (FUNC)	RODPS_REPL_ODP_FETCH	16	ランタイム
	RFC_TYPE - 関数モジュール (FUNC)	RODPS_REPL_ODP_FETCH_XML	16	ランタイム
	RFC_TYPE - 関数モジュール (FUNC)	DDIF_FIELDINFO_GET	16	前後方向
S_BTCH_ADM	フィールド名 - BTCADMIN	Y	該当なし	前後方向
S_BTCH_JOB	フィールド名 - JOBACTION	RELE	RELE (リリースジョブ)	前後方向
	フィールド名 - JOBGROUP	' '	該当なし	前後方向
S_RS_ODP_H	フィールド名 - RSODPHNAME	*	3	前後方向
	フィールド名 - RSODPHPKG	*	3	前後方向
S_RO_OSOA	フィールド名 - OLTPSOURCE	*	3	前後方向

読み取りオブジェクト名	権限値	値	アクティビティ	設計時間/実行時間
	フィールド名 - OSOAAPCO	*	3	前後方向
	フィールド名 - OSOAPART	データ定義	3	前後方向
S_RS_HYBR	フィールド名 - RSHYBRPROV	'*'	3	前後方向
	フィールド名 - RSHYBRPROJ	定義	3	前後方向
S_RS_ICUBE	フィールド名 - OLTPSOURCE	*	3	前後方向
	フィールド名 - OSOAAPCO	*	3	前後方向
	フィールド名 - OSOAPART	データ、定義	3	前後方向
S_RS_IOMAD	フィールド名 - RSINFOAREA	*	3	前後方向
	フィールド名 - RSAPPLNM	*	3	前後方向
	フィールド名 - RSIOBJNM	*	3	前後方向
S_RS_MPRO	フィールド名 - RSINFOAREA	*	3	前後方向
	フィールド名 - RSMPRO	*	3	前後方向
	フィールド名 - RSMPROOBJ	データ	3	前後方向
S_RS_ODSO	フィールド名 - RSINFOAREA	*	3	前後方向
	フィールド名 - RSODSOBJ	*	3	前後方向
	フィールド名 - RSODSPART	データ	3	前後方向
S_ADMI_FCD	フィールド名 - S_ADMI_FCD	PADM	該当なし	前後方向

セキュアなネットワーク通信プロトコルの設定

セキュアなネットワーク通信（SNC）プロトコルで SAP ODP Extractor 接続を使用するには、SAP サーバーおよび Secure Agent マシンで SNC プロトコルを設定する必要があります。
SNC プロトコルを使用した接続を作成するには、アプリケーションサーバー SNC 接続と負荷分散サーバー SNC 接続を使用します。

SAP SNC 接続を設定するための前提条件と手順の詳細については、Informatica How-To ライブラリの記事「[Configure the SAP Secure Network Communication protocol](#)」を参照してください。

SAP ODP への接続

SAP ODP オブジェクトに接続するように SAP ODP Extractor の接続プロパティを設定してみましょう。

始める前に

開始する前に、Secure Agent マシンと SAP システムを設定して SAP ODP Extractor 接続を確立する必要があります。
これらのタスクの詳細については、「[前提条件](#)」（ページ 792）」を参照してください。

接続の詳細

次の表に、基本接続プロパティを示します。

財産	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。

財産	説明
シークレットコンテナの使用	<p>組織に対して設定されている Secrets Manager にこの接続の機密資格情報を保存します。このプロパティは、組織に Secrets Manager が設定されている場合にのみ表示されます。このプロパティは、データ取り込みおよびレプリケーションとデータアクセス管理サービスではサポートされていません。</p> <p>接続でシークレットコンテナを有効にすると、Secure Agent が Secrets Manager からどの資格情報を取得するかを選択できます。このオプションを無効にした場合、資格情報は組織の設定方法に応じてリポジトリまたはローカル Secure Agent に保存されます。</p> <p>注: この接続を使用してプッシュダウンまたはプロキシサービスを介してデータアクセスポリシーを適用する場合、シークレットコンテナ設定オプションを使用することはできません。</p> <p>Secrets Manager を設定および使用する方法については、Administrator のヘルプにある「Secrets Manager の設定」を参照してください。</p>
ランタイム環境	<p>SAP S/4HANA または SAP ECC にアクセスするためのタスクを実行するランタイム環境の名前。Secure Agent、サーバーレスランタイム環境、またはエラスティックランタイム環境を選択します。</p> <p>アプリケーション取り込みとレプリケーションタスクでは、ホステッドエージェント、サーバーレスランタイム環境、またはエラスティックランタイム環境を使用することはできません。</p> <p>サーバーレス環境の設定の詳細については、「サーバーレスランタイム環境の使用」 (ページ 804) を参照してください。</p> <p>ランタイム環境の設定および使用方法の詳細については、Administrator のヘルプにある「ランタイム環境」を参照してください。</p>

SAP サーバー接続タイプ

アプリケーションサーバー、アプリケーションサーバー SNC、負荷分散サーバー、および負荷分散サーバー SNC 接続タイプを設定して、SAP ODP にアクセスできます。
必要な接続タイプを選択し、接続固有のパラメータを設定します。

アプリケーションサーバー接続

アプリケーションサーバー接続は、SAP クライアントの詳細を必要とするデフォルトのタイプです。

次の表に、アプリケーションサーバー接続の基本的な接続プロパティとその説明を示します。

接続プロパティ	説明
SAP クライアント番号	SAP アプリケーションサーバーのクライアント番号。 接続先の SAP システムから必要なクライアント番号を取得します。
SAP 言語	SAP 言語に対応する言語コード 接続先の SAP システムから必要な言語コードを取得します。
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 アプリケーションサーバーのシステム番号。 接続先の SAP システムから必要なシステム番号を取得します。
SAP ユーザー名	SAP アカウントに接続するための適切なユーザー権限を持つユーザー名。

接続プロパティ	説明
SAP パスワード	SAP アカウントに接続するためのパスワード。
サブスクリバ名	Secure Agent を SAP システムの一意のサブスクリ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オペレーショナルデルタキュー（ODQ）を定義します。

アプリケーションサーバー SNC 接続

アプリケーションサーバー SNC 接続には、Secure Agent の PSE 証明書名、SAP サーバーの PSE 証明書名、X509 証明書ファイルへのパス、および SAP クライアントの詳細が必要です。

次の表に、アプリケーションサーバー SNC 接続の基本的な接続プロパティとその説明を示します。

接続プロパティ	説明
SAP クライアント番号	SAP アプリケーションサーバーのクライアント番号。 接続先の SAP システムから必要なクライアント番号を取得します。
SAP 言語	SAP 言語に対応する言語コード 接続先の SAP システムから必要な言語コードを取得します。
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 アプリケーションサーバーのシステム番号。 接続先の SAP システムから必要なシステム番号を取得します。
SNC マイネーム	Secure Agent 用に生成されたエージェ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	SAP サーバーで生成されたサーバー 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 SNC 接続の作成時に通信パスに適用される保護のレベル。 リストから次のいずれかのオプションを選択します。 <ul style="list-style-type: none"> - 1 - 認証のみを適用 - 2 - 認証と整合性保護を適用 - 3 - 認証、整合性、プライバシー保護（暗号化）を適用 - 8 - グローバルデフォルト保護を適用（通常は 3） - 9 - 最大限の保護を適用 デフォルトは、[3 - 認証、整合性、プライバシー保護（暗号化）を適用] です。
X509 証明書を使用	ログイン方法。 X.509 証明書を使用する SNC 暗号化でログインするには、[X509 証明書を使用] を選択します。 このオプションを選択しない場合は、[X509 証明書のパスまたは SAP ユーザー名] プロパティに SAP ユーザー名を入力する必要があります。 デフォルトでは無効になっています。

接続プロパティ	説明
X509 証明書のパスまたは SAP ユーザー名	<p>X509 証明書ファイルのパスおよびファイル名。</p> <p>X509 証明書のファイル名が abc.crt で、パスが \root\<フォルダ名>である場合は、パスおよびファイル名を次の形式で入力します。</p> <p>\root\<folder name>\abc.crt</p> <p>X509 証明書を使用する場合、SAP ユーザー名を入力する必要はありません。</p> <p>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 ユーザー名を入力します。</p>
サブスクライバ名	<p>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。</p> <p>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オペレーショナルデルタキュー（ODQ）を定義します。</p>

次の表に、アプリケーションサーバー SNC 接続の詳細接続プロパティとその説明を示します。

プロパティ	説明
SAP 暗号ライブラリパス	<p>SAP 暗号化ライブラリのパスとファイル名。</p> <p>パスおよびファイル名を、Secure Agent を実行するオペレーティングシステムに基づいた次の形式で入力します。</p> <ul style="list-style-type: none"> - Windows の場合: \root\<フォルダ名>\sapcrypto.dll - Linux の場合: /root/<フォルダ名>/libsapcrypto.so

負荷分散サーバー接続

実行時に最も負荷の少ない SAP システムに接続する場合は、負荷分散サーバー接続を作成します。

負荷分散サーバー接続には、SAP クライアントの詳細とメッセージサーバーグループ名が必要です。

次の表に、負荷分散サーバー接続の基本的な接続プロパティとその説明を示します。

接続プロパティ	説明
SAP クライアント番号	<p>SAP メッセージサーバーのクライアント番号。</p> <p>接続先の SAP システムから必要なクライアント番号を取得します。</p>
SAP 言語	<p>SAP 言語に対応する言語コード</p> <p>接続先の SAP システムから必要な言語コードを取得します。</p>
SAP メッセージサーバー	SAP メッセージサーバーのホスト名。
SAP システム ID	<p>SAP メッセージサーバーのシステム ID。</p> <p>接続先の SAP システムから必要なシステム ID を取得します。</p>
SAP グループ	<p>接続に使用する SAP ログオングループの名前。</p> <p>例: PUBLIC。</p>
SAP ユーザー名	SAP アカウントに接続するための適切なユーザー権限を持つユーザー名。

接続プロパティ	説明
SAP パスワード	SAP アカウントに接続するためのパスワード。
サブスクライバ名	Secure Agent を SAP システムの一意のサブスクライバとして定義する名前。 SAP は、ユーザーが ODP からデルタデータの読み取りを行った場合に、この名前を使用して一意のオペレーショナルデルタキュー（ODQ）を定義します。

負荷分散サーバー SNC 接続

実行時に負荷が最も少ない（SNC）プロトコルを使用して SAP システムに接続する場合は、負荷分散サーバー SNC 接続を作成します。

負荷分散サーバー SNC 接続には、Secure Agent の PSE 証明書名、SAP サーバーの PSE 証明書名、X509 証明書ファイルへのパス、SAP クライアントの詳細、およびメッセージサーバーグループ名が必要です。

次の表に、負荷分散サーバー SNC 接続の基本的な接続プロパティとその説明を示します。

接続プロパティ	説明
SAP クライアント番号	SAP メッセージサーバーのクライアント番号。 接続先の SAP システムから必要なクライアント番号を取得します。
SAP 言語	SAP 言語に対応する言語コード 接続先の SAP システムから必要な言語コードを取得します。
SAP メッセージサーバー	SAP メッセージサーバーのホスト名。
SAP システム ID	SAP メッセージサーバーのシステム ID。 接続先の SAP システムから必要なシステム ID を取得します。
SAP グループ	接続に使用する SAP ログオングループの名前。 例: PUBLIC。
SNC マイネーム	Secure Agent 用に生成されたエージェント 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サーバー 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 SNC 接続の作成時に通信パスに適用される保護のレベル。 リストから次のいずれかのオプションを選択します。 <ul style="list-style-type: none"> - 1 - 認証のみを適用 - 2 - 認証と整合性保護を適用 - 3 - 認証、整合性、プライバシー保護（暗号化）を適用 - 8 - グローバルデフォルト保護を適用（通常は 3） - 9 - 最大限の保護を適用 デフォルトは、[3 - 認証、整合性、プライバシー保護（暗号化）を適用] です。

接続プロパティ	説明
X509 証明書を使用	<p>ログイン方法。</p> <p>X509 証明書を使用する SNC 暗号化でログインするには、[X509 証明書を使用] を選択します。</p> <p>このオプションを選択しない場合は、[X509 証明書のパスまたは SAP ユーザー名] プロパティに SAP ユーザー名を入力する必要があります。</p> <p>デフォルトでは無効になっています。</p>
X509 証明書のパスまたは SAP ユーザー名	<p>X509 証明書ファイルのパスおよびファイル名。</p> <p>X509 証明書のファイル名が abc.crt で、パスが \root\<フォルダ名>である場合は、パスおよびファイル名を次の形式で入力します。</p> <p>\root\<folder name>\abc.crt</p> <p>X509 証明書を使用する場合、SAP ユーザー名を入力する必要はありません。</p> <p>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 ユーザー名を入力します。</p>
サブスクライバ名	<p>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。</p> <p>SAP は、ユーザーが ODP からデルタデータの読み取りを行った場合に、この名前を使用して一意のオペレーショナルデルタキュー (ODQ) を定義します。</p>

次の表に、負荷分散サーバー SNC 接続の詳細接続プロパティとその説明を示します。

プロパティ	説明
SAP 暗号ライブラリパス	<p>SAP 暗号化ライブラリのパスとファイル名。</p> <p>パスおよびファイル名を、Secure Agent を実行するオペレーティングシステムに基づいた次の形式で入力します。</p> <ul style="list-style-type: none"> - Windows の場合: \root\<フォルダ名>\sapcrypto.dll - Linux の場合: /root/<フォルダ名>/libsapcrypto.so

詳細設定

次の表に、詳細接続のプロパティを示します。

プロパティ	説明
追加パラメータ	<p>SAP システムへの接続時に使用できる追加の SAP パラメータ。</p> <p>複数の追加パラメータをセミコロンで区切って、次の形式で入力することができます。</p> <pre><parameter name1>=<value1>;<parameter name2>=<value2>;<parameter name3>=<value3>...</pre> <p>例えば、SAP JCo および SAP CPIC トレースファイルを生成するには、次の追加パラメータを入力します。</p> <pre>jco.client.trace="1";jco.client.cpic_trace="3";</pre> <p>実行時に、次の場所に SAP JCo および SAP CPIC トレースファイルが生成されます。</p> <pre><Informatica Secure Agent installation directory>\apps\Data_Integration_Server\<DIS version>\ICS\main\bin\rdtm</pre> <p>設計時に、次の場所にある tomcat.out ファイルに SAP CCPIC トレースが生成されます。</p> <pre><Informatica Secure Agent installation directory>\apps\Data_Integration_Server\<DIS version>tomcat.out</pre>
差分フィールドを表示	<p>ODP ソース上のデータ変更の原因となった操作モードをマッピングに表示するかどうかを指定します。</p> <p>有効にすると、マッピングによって、オペレーショナルデルタキュー（ODQ）で有効になっている ODP ソースの【フィールド】タブに ODQ_CHANGEMODE および ODQ_ENTITYCNTR フィールドが生成されます。</p> <p>デフォルトでは無効になっています。</p>

SAP ODP オブジェクトからの階層データ抽出

SAP ODP Extractor 接続を使用して Unicode SAP システム内の SAP ODP オブジェクトから階層データを抽出する前に、Secure Agent ディレクトリから取得した SAP ODP Extractor トランスポートファイルを SAP システムにインストールする必要があります。

トランスポートファイルをインストールするための前提条件

SAP ODP Extractor トランスポートをインストールする前に、次の前提条件のタスクを必ず実行してください。

- SAP マシンにインストールしたトランスポートファイルが最新のものであることを確認します。次のディレクトリから最新のトランスポートファイルを取得します：

```
<Informatica Secure Agent installation directory>\downloads\package-SAPODP.<Latest version>\package\sapodp\sap-transport
```
- トランスポートファイルが SAP バージョン ERP 6.0 EHP7 システム以降に対応していることを確認します。
- 本番システムにトランスポートをインストールする前に、開発システムにトランスポートをインストールしてテストしてください。

次の表に、SAP ODP オブジェクトからデータの読み取りを行うためにインストールする必要があるトランスポートを示します。

データおよび Co ファイル名	トランスポート要求	機能
- K900861.N75 - R900861.N75	N75K900861	階層をサポートする SAP ODP から読み取る場合にのみ、トランスポートをインストールします。 階層データを含まない SAP ODP オブジェクトの場合は、SAP ODP Extractor トランスポートファイルをインストールせずに SAP ODP Extractor コネクタを使用することができます。

トランスポートファイルのインストール

SAP ODP Extractor トランスポートファイルをインストールするには、次の手順を実行します。

1. トランスポートファイルは、Secure Agent マシンの次のディレクトリにあります：
<Informatica Secure Agent installation directory>\downloads\package-SAPODP.<Latest version>\package\sapodp\sap-transport
2. アクセスする各 SAP マシンの SAP トランスポート管理ディレクトリにある Cofile ディレクトリに、cofile トランスポートファイルをコピーします。
cofile トランスポートファイルでは、次の命名規則を使用します: <number>.<sap system>
3. アクセスする各 SAP マシンの SAP トランスポート管理ディレクトリにある Data ディレクトリにデータトランスポートファイルをコピーします。
データトランスポートファイルでは、次の命名規則を使用します: <number>.<sap-system>
4. STMS でトランスポートを SAP にインポートするには、**[補足]** > **[その他の依頼]** > **[追加]** をクリックし、トランスポート要求をシステムキューに追加します。
5. **[インポートキューに移送依頼追加]** ダイアログボックスに、cofile トランスポートの要求番号を入力します。
要求番号は、名前を変更した cofile を次のような順序に置き替えたものです: <sap-system><number>
6. インポートキューの要求領域で、追加したトランスポート要求番号を選択し、**[インポート]** をクリックします。
7. Informatica Transports の以前のバージョンからアップグレードする場合は、**[オリジナルを上書き]** オプションを選択します。

サーバーレスランタイム環境の使用

Linux での SAP ODP Extractor 接続の設定時に、AWS または Azure でホストされているサーバーレスランタイム環境を使用して SAP システムに接続できます。

SAP Secure Network Communication (SNC) プロトコルを使用する場合、サーバーレスランタイム環境を使用することはできません。

サーバーレスランタイム環境を使用して SAP ODP Extractor 接続を設定する前に、次のタスクを実行してください。

- AWS または Azure アカウントの Amazon S3 バケットあるいは Azure コンテナに SAP ライブラリを追加します。
- .yaml サーバーレス構成ファイルを設定する。

- Linux 上のサーバーレスランタイム環境の JAVA_LIBS プロパティと JVMClassPath プロパティを設定します。

AWS または Azure アカウントの Amazon S3 バケットあるいは Azure コンテナに SAP ライブラリを追加します

サーバーレスランタイム環境で SAP ODP Extractor 接続を設定するには、次の手順を実行します。

1. AWS または Azure のサーバーレスエージェント設定用に次の構造を作成します: <補足ファイルの場所>/serverless_agent_config
2. AWS アカウントまたは Azure アカウントの次の場所にある Amazon S3 バケットあるいは Azure コンテナにライブラリを追加します: <補足ファイルの場所>/serverless_agent_config/sap

.yaml サーバーレス構成ファイルを設定する

次の手順を実行して、サーバーレスランタイム環境で.yaml サーバーレス構成ファイルを設定し、SAP ライブラリをサーバーレスエージェントディレクトリにコピーします。

1. 次のコードスニペットをテキストエディタにコピーします。

```
version: 1
agent:
  dataIntegrationServer:
    autoDeploy:
      sap:
        jcos:
          - fileCopy:
              sourcePath: sap/jco/<sapjco_library_filename>
          - fileCopy:
              sourcePath: sap/jco/<sapjco_library_filename>
```

ここで、ソースパスは AWS または Azure の SAP ライブラリファイルのディレクトリパスです。

2. 構文とインデントが有効であることを確認してから、ファイルを serverlessUserAgentConfig.yaml として次の AWS または Azure の場所に保存します: <補足ファイルの場所>/serverless_agent_config.yaml ファイルの実行時に、SAP ライブラリが AWS または Azure の場所からサーバーレスエージェントディレクトリにコピーされます。

サーバーレスランタイム環境の JAVA_LIBS プロパティと JVMClassPath プロパティを設定します。

Administrator で次の手順を実行して、Linux 上のサーバーレスランタイム環境の JAVA_LIBS プロパティと JVMClassPath プロパティを設定します。

1. Informatica Intelligent Cloud Services にログインします。
2. **[Administrator]** > **[サーバーレス環境]** の順に選択します。
3. **[サーバーレス環境]** タブで、必要なサーバーレスランタイム環境の **[アクション]** メニューを展開し、**[編集]** を選択します。
4. **[ランタイム設定のプロパティ]** タブで、**[データ統合サーバー]** をサービスとして選択します。
5. 次の **[タイプ]** と **[名前]** を選択し、JAVA_LIBS と JVMClassPath の値を入力します。

タイプ	名前	値
Tomcat_JRE	JAVA_LIBS	../bin/rdtm-extra/tpl/sap/sapjco3.jar:../bin/rdtm/javalib/sap/sap-adapter-common.jar
PMRDTM_CFG	JVMClassPath	pmserversdk.jar:../bin/rdtm-extra/tpl/sap/sapjco3.jar:../bin/rdtm/javalib/sap/sap-adapter-common.jar

6. **[保存]** をクリックします。

サーバーレス環境の設定および使用方法の詳細については、Administrator のヘルプにある「ランタイム環境」の「サーバーレスランタイム環境のセットアップ」を参照してください。

SAP Table Connector connection properties

Create an SAP Table Connector connection to access data directly from SAP tables and SAP ADSO objects.

You can use the SAP Table connection to read data from the following objects:

- Transparent tables
- Cluster tables
- Pool tables
- Data dictionary-based and entity-based ABAP CDS views
- SAP views
- SAP ADSO

You can also use the SAP Table connection to write data to custom transparent tables.

前提条件

SAP テーブル接続を使用する前に、SAP 管理者は特定の前提条件のタスクを実行して Secure Agent マシンと SAP システムを設定する必要があります。

また、SAP テーブルデータを処理し、SAP BW/4HANA ADSO オブジェクトからデータの読み取りを行うには、必要なライセンスが SAP システムに対して有効になっているかどうかを確認する必要があります。

SAP ライブラリのダウンロードと設定

SAP テーブルに対するデータの読み取りまたは書き込みを行うには、Secure Agent マシンに SAP NetWeaver RFC SDK ライブラリと SAP JCo ライブラリをダウンロードして設定する必要があります。ライブラリのダウンロードで問題が発生した場合は、SAP カスタマサポートにお問い合わせください。

1. [SAP Support Portal](#) に移動し、[ソフトウェアのダウンロード] をクリックします。

注: [SAP Support Portal](#) から [ソフトウェアのダウンロード] にアクセスするには、SAP 資格情報が必要です。

- Secure Agent プロセスをホストするオペレーティングシステムに固有の、SAP NetWeaver RFC SDK 7.50 ライブラリの最新バージョンをダウンロードします。

オペレーティングシステム	SAP NetWeaver RFC SDK ライブラリ
Linux 64	<ul style="list-style-type: none"> - libicudata.so.50 - libicui18n.so.50 - libicuuc.so.50 - libsapnwrfc.so - libsapucum.so
Windows 64	<ul style="list-style-type: none"> - icudt50.dll - icuin50.dll - icuuc50.dll - libsapucum.dll - sapnwrfc.dll

- SAP NetWeaver RFC SDK 7.50 ライブラリを次のディレクトリにコピーします。
<Informatica Secure Agent installation directory>\apps\Data_Integration_Server\ext\deploy_to_main\bin\rdtm
存在しない場合は、deploy_to_main\bin\rdtm ディレクトリを作成します。
- NetWeaver RFC SDK ライブラリごとに以下の権限を設定します。
 - 現在のユーザーに読み取り、書き込みおよび実行権限。
 - 他のすべてのユーザーに読み取りおよび実行権限。
- Secure Agent を実行しているマシンのオペレーティングシステムに基づいて、[SAP Support Portal](#) から最新バージョンの 64 ビット SAP JCo ライブラリをダウンロードします。

オペレーティングシステム	SAP JCo ライブラリ
Windows	sapjco3.jar sapjco3.dll
Linux	sapjco3.jar libsapjco3.so

- 次のディレクトリに JCo ライブラリをコピーします。
<Informatica Secure Agent installation directory>\apps\Data_Integration_Server\ext\deploy_to_main\bin\rdtm-extra\tpl\sap
存在しない場合は、deploy_to_main\bin\rdtm-extra\tpl\sap ディレクトリを作成します。
- Informatica Intelligent Cloud Services にログインし、Secure Agent の JAVA_LIBS プロパティを設定します。
 - [Administrator]** > **[ランタイム環境]** の順に選択します。
 - [ランタイム環境]** をクリックして、**[ランタイム環境]** ページにアクセスします。
 - エージェント名の左側で、**[Secure Agent の編集]** をクリックします。
 - [サービス]** リストから、**[データ統合サーバー]** を選択します。
 - [タイプ]** リストから、**[Tomcat JRE]** を選択します。

- f. Secure Agent が実行されるオペレーティングシステムに基づいて JAVA_LIBS 値を入力します。

オペレーティングシステム	値
Windows	../bin/rdtm-extra/tpl/sap/sapjco3.jar;../bin/rdtm/javaliib/sap/sap-adapter-common.jar
Linux	../bin/rdtm-extra/tpl/sap/sapjco3.jar;../bin/rdtm/javaliib/sap/sap-adapter-common.jar

警告: テーブルから値を直接コピーすると、値のハイフン (-) が誤ってコピーされることがあります。値をテキストエディタにコピーし、コピーした値が破損していないことを確認します。

System Configuration Details Reset All

Service: Data Integration Server ▼

Type: Tomcat JRE ▼

Type	Name	Value
Tomcat JRE	JAVA_LIBS	../bin/rdtm-extra/tpl/sap/sapjco3.jar;../bin/rdtm/javaliib/sap/sap-adapter-common.jar

- g. **【保存】** をクリックします。
- h. Secure Agent をインストールしたすべてのマシンで手順 2 - 7 を繰り返します。
8. Secure Agent を再起動します。

SAP ユーザー権限の設定

SAP テーブルデータを処理するために、SAP システムで SAP ユーザーアカウントを設定します。

次の表に、SAP テーブルにアクセスしてデータの読み取りを行うためのユーザー権限の設定に必要なオブジェクトと権限を示します。

読み取りオブジェクト名	認証
S_BTCH_JOB	DELE、LIST、PLAN、SHOW Job Operation を RELE に設定します。
S_PROGRAM	BTCSUBMIT、SUBMIT
S_RFC	SYST、SDTX、SDIFRUNTIME、/INFADI/TBLRDR、RFC1
S_TABU_DIS/ S_TABU_NUM	データを読み取る SAP テーブル名を指定します。

次の表に、SAP テーブルにアクセスしてデータの書き込みを行うためのユーザー権限の設定に必要なオブジェクトと権限を示します。

書き込みオブジェクト名	認証
S_RFC	/INFADI/GET_TRANSPORT_VERSION、/INFADI/ZPMW、 DDIF_FIELDINFO_GET、RFC1、RFCPING、RFC_READ_TABLE
S_TABU_DIS / S_TABU_NUM	データを書き込む SAP テーブル名を指定します。

注: SAP システムのバージョンに基づいて、S_TABU_DIS または S_TABU_NUM を追加する必要があります。S_TABU_DIS または S_TABU_NUM の詳細については、SAP のマニュアルを参照してください。

これらのオブジェクトとその使用方法の詳細については、「[SAP user authorizations](#)」を参照してください。

SAP テーブルから読み取るトランスポートファイルのインストール

Unicode SAP システムからの SAP テーブルからデータを読み取るには、SAP Table Reader トランスポートファイルを Secure Agent ディレクトリから SAP システムにインストールします。トランスポートファイルは、SAP バージョン ECC 6.0 以降に対応しています。

トランスポートファイルをインストールするための前提条件

SAP Table Reader トランスポートをインストールする前に、次の前提条件のタスクを必ず実行してください。

- SAP マシンにインストールしたトランスポートファイルが最新のものであることを確認します。次のディレクトリから最新のトランスポートファイルを取得します:
<Informatica Secure Agent インストールディレクトリ>\downloads\package-SAPConnector.<最新のバージョン>\package\rdtm\sap-transport\SAPTableReader
- TABLE_READER_Addon トランスポートファイルをインストールする前に、SAP で RSODPABAPCDSVIEW テーブルが使用可能であることを確認してください。RSODPABAPCDSVIEW テーブルが使用できない場合、TABLE_READER_Addon トランスポートのインストールは失敗します。
- 本番システムにトランスポートをインストールする前に、開発システムにトランスポートをインストールしてテストしてください。

以下の表に、アクセスする SAP ソースタイプに基づいてインストールする必要があるトランスポートを一覧で示します。

データおよび Co ファイル名	トランスポート要求	機能
TABLE_READER_R900176.ER6 TABLE_READER_K900176.ER6	ER6K900176	SAP 透過テーブル、クラスタテーブル、およびブールテーブルからデータを読み取るには、TABLE_READER トランスポートのみをインストールします。
TABLE_READER_Addon_R900085.S4N TABLE_READER_Addon_K900085.S4N	S4NK900085	ABAP CDS ビューからデータを読み取るには、TABLE_READER および TABLE_READER_Addon トランスポートをインストールします。 SAP NetWeaver 7.50 SP4 バージョン以降の TABLE_READER_Addon トランスポートを使用します。 TABLE_READER トランスポートをインストールするときは常に、TABLE_READER_Addon トランスポートバージョンに変更がない場合でも、TABLE_READER_Addon トランスポートを再インストールする必要があります。 注: 最初に TABLE_READER トランスポートをインストールしてから、TABLE_READER_Addon トランスポートをインストールしてください。

トランスポートファイルのインストール

SAP Table Reader トランスポートファイルをインストールするには、次の手順を実行します。

1. トランスポートファイルは、Secure Agent マシンの次のディレクトリにあります：
<Informatica Secure Agent インストールディレクトリ>\downloads\package-SAPConnector。<最新のバージョン>
\package\rdtm\sap-transport\SAPTableReader
2. アクセスする各 SAP マシンの SAP トランスポート管理ディレクトリにある Cofile ディレクトリに、cofile トランスポートファイルをコピーします。
cofile トランスポートファイルでは、次の命名規則を使用します: TABLE_READER_K<番号>.ER6
3. ファイル名から「TABLE_READER_」を削除して cofile の名前を変更します。
例えば、TABLE_READER_K900176.ER6 という名前の cofile トランスポートファイルの場合は、ファイル名を K900176.ER6 に変更します。
4. アクセスする各 SAP マシンの SAP トランスポート管理ディレクトリにある Data ディレクトリにデータトランスポートファイルをコピーします。
データトランスポートファイルでは、次の命名規則が使用されます: TABLE_READER_R<番号>.ER6。
5. ファイル名から「TABLE_READER_」を削除してファイルの名前を変更します。
6. STMS でトランスポートを SAP にインポートするには、**[補足]** > **[その他の依頼]** > **[追加]** をクリックし、トランスポート要求をシステムキューに追加します。
7. **[インポートキューに移送依頼追加]** ダイアログボックスに、cofile トランスポートの要求番号を入力します。
要求番号は、名前を変更した cofile を次のような順序に置き替えたものです: ER6K<番号>。
例えば、名前を変更した K900176.ER6 という cofile トランスポートファイルについては、要求番号に ER6K900176 と入力します。
8. インポートキューの要求領域で、追加したトランスポート要求番号を選択し、**[インポート]** をクリックします。
9. Informatica Transports の以前のバージョンからアップグレードする場合は、**[オリジナルを上書き]** オプションを選択します。

SAP テーブルに書き込むトランスポートファイルのインストール

顧客の名前空間で作成された SAP カスタムテーブルにデータを書き込むには、SAP Table Writer トランスポートファイルをインストールします。

最新の SAP Table Writer トランスポートファイルを取得してインストールするには、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。

SAP テーブルへの接続

SAP テーブルと SAP BW/4HANA ADSO オブジェクトに接続するように、SAP テーブルコネクタの接続プロパティを設定してみましょう。

始める前に

開始する前に、SAP テーブル接続を確立するように Secure Agent マシンと SAP システムを設定する必要があります。

これらのタスクの詳細については、「[「前提条件」 \(ページ 806\)](#)」を参照してください。

接続の詳細

次の表に、基本接続プロパティを示します。

財産	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。
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選択します。 サーバーレス環境の設定の詳細については、「 サーバーレスランタイム環境の使用 」(ページ 820)を参照してください。
シークレットコンテナの使用	組織に対して設定されている Secrets Manager にこの接続の機密資格情報を保存します。 このプロパティは、組織に Secrets Manager が設定されている場合にのみ表示されます。 このプロパティは、データ取り込みおよびレプリケーションとデータアクセス管理サービスではサポートされていません。 接続でシークレットコンテナを有効にすると、Secure Agent が Secrets Manager からどの資格情報を取得するかを選択できます。このオプションを無効にした場合、資格情報は組織の設定方法に応じてリポジトリまたはローカル Secure Agent に保存されます。 注: この接続を使用してプッシュダウンまたはプロキシサービスを介してデータアクセスポリシーを適用する場合、シークレットコンテナ設定オプションを使用することはできません。 Secrets Manager を設定および使用する方法については、Administrator のヘルプにある「Secrets Manager の設定」を参照してください。
ユーザー名	SAP アカウントに接続するための適切なユーザー権限を持つユーザー名。
パスワード	SAP アカウントに接続するためのパスワード。
クライアント	SAP アプリケーションサーバーのクライアント番号。 接続先の SAP システムから必要なクライアント番号を取得します。
アプリケーションサーバー	SAP テーブルから読み取りを行う場合の SAP アプリケーションサーバーのホスト名または IP アドレス。 SAP テーブルから読み取りを行うためにこのフィールドに SAP アプリケーションサーバーのホスト名または IP アドレスを入力した場合は、[Saprfc.ini パス] フィールドへの sapnwrfc.ini ファイルのディレクトリの入力、および [宛先] フィールドへの DEST エントリの入力を行わないようにしてください。 注: このプロパティは、SAP テーブルに書き込みを行う接続を作成する場合には適用されません。

財産	説明
システム番号	SAP テーブルから読み取りを行う場合の SAP アプリケーションサーバーのシステム番号。 SAP テーブルから読み取りを行うためにこのフィールドに SAP アプリケーションサーバーのシステム番号を入力した場合は、[Saprfc.ini パス] フィールドへの sapnwrfc.ini ファイルのディレクトリの入力、および [宛先] フィールドへの DEST エントリの入力を行わないようにしてください。 注: このプロパティは、SAP テーブルに書き込みを行う接続を作成する場合には適用されません。
言語	SAP 言語に対応する言語コード。 接続先の SAP システムから必要な言語コードを取得します。

詳細設定

次の表に、詳細接続のプロパティを示します。

プロパティ	説明
Saprfc.ini パス	パスとファイル名、または sapnwrfc.ini ファイルへのパス。 このプロパティは、SAP テーブルに書き込みを行う接続を使用する場合に必要です。 sapnwrfc.ini ファイルが使用可能な次のディレクトリを入力します: <Informatica Secure Agent installation directory>/apps/Data_Integration_Server/ext/deploy_to_main/bin/rdtm サーバーレスランタイム環境の場合、sapnwrfc.ini ファイルは AWS の場所から次のサーバーレスエージェントディレクトリにコピーされます。 /data2/home/cldagnt/SystemAgent/apps/Data_Integration_Server/ext/deploy_to_main/bin/rdtm sapnwrfc.ini ファイルの作成方法の詳細については、 「sapnwrfc.ini ファイルの設定」 (ページ 813) を参照してください。 このフィールドに sapnwrfc.ini ファイルのディレクトリを入力した場合は、[アプリケーションサーバー] フィールドと [システム番号] フィールドへの SAP アプリケーションサーバーのホスト名または IP アドレスとシステム番号の入力を行わないでください。
宛先	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。 宛先にはすべて大文字を使用してください。 このプロパティは、SAP テーブルに書き込みを行う接続を作成する場合に必要です。 このフィールドに DEST エントリを入力した場合は、[アプリケーションサーバー] フィールドと [システム番号] フィールドへの SAP アプリケーションサーバーのホスト名または IP アドレスとシステム番号の入力を行わないでください。
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。デフォルトの範囲は 10000-65535 です。 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、RFC プロトコルを使用して接続をテストします。
HTTPS 接続	HTTPS プロトコルを使用して SAP に接続します。 HTTPS 経由で SAP に正常に接続するには、管理者が Secure Agent マシンと SAP システムの HTTPS 用の設定を完了していることを確認してください。 HTTPS 経由で SAP に接続する方法の詳細については、 「SAP に接続するための HTTPS の設定」 (ページ 816) を参照してください。

プロパティ	説明
キーストアの場所	SAP に接続するキーストアファイルの絶対パスとファイル名。 パスとファイル名を次の形式で指定します。 <ディレクトリ>/<キーストアファイル名>.jks
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宛先パスワード。
プライベートキーのパスワード	.P12 ファイルにアクセスするためのエクスポートパスワード。
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 プロパティ。 Secure Agent が SAP に接続できるようにするために必要な RFC 固有のパラメータと接続情報を指定します。 例えば、次のサンプルに示すように、ロードバランシングパラメータを指定できます： MSHOST=<Host name of the message server> R3NAME=<Name of the SAP system> group=<Group name of the application server> 他の接続プロパティフィールドでパラメータを設定した場合は、 [SAP 追加プロパティ] フィールドに同じパラメータ値を入力しないでください。 RFC 固有のパラメータの詳細については、SAP のマニュアルを参照してください。

sapnwrfc.ini ファイルの設定

SAP は、RFC（Remote Function Call）という通信プロトコルを使用して外部のシステムとデータのやり取りを行います。

SAP テーブルにデータの書き込みを行うには、sapnwrfc.ini ファイルが必要です。

sapnwrfc.ini ファイルを作成し、SAP 接続タイプに必要な接続情報と RFC 固有のパラメータを含めます。DOS エディタまたはワードパッドを使用して sapnwrfc.ini ファイルを作成すると、メモ帳で頻繁に発生するエラーを回避できます。さまざまな接続タイプに使用できる sapnwrfc.ini ファイルのサンプルの詳細については、「[「接続タイプのサンプル sapnwrfc.ini ファイル」 \(ページ 814\)](#)」を参照してください。

sapnwrfc.ini ファイルを作成した後に、エージェントディレクトリに sapnwrfc.ini ファイルを配置します。エージェントは sapnwrfc.ini ファイルを検証し、設定された接続にそのファイルを使用します。

エージェントディレクトリへの sapnwrfc.ini ファイルの配置

次のように、Secure Agent またはサーバーレスランタイム環境を使用して、RFC クライアントとして SAP システムに接続できます。

- Secure Agent を使用するには、sapnwrfc.ini ファイルを次の場所に配置します。
<Informatica Secure Agent installation directory>\apps\Data_Integration_Server\ext\deploy_to_main\bin\rdtm\
- サーバーレスランタイム環境を使用するには、sapnwrfc.ini ファイルを次の場所に配置します。
\data2\home\cldagnt\SystemAgent\apps\Data_Integration_Server\ext\deploy_to_main\bin\rdtm\

注: deploy_to_main\bin\rdtm ディレクトリが存在することを確認します。ディレクトリが存在しない場合は、ディレクトリを作成してからファイルを配置します。

必要なディレクトリにファイルを配置した後に、エージェントを再起動します。

以前のバージョンからのアップグレード

以前のバージョンからアップグレードする場合は、sapnwrfc.ini ファイルを作成する必要はありません。Secure Agent は、sapnwrfc.ini ファイルを deploy_to_main\bin\rdtm ディレクトリにコピーします。

sapnwrfc.ini ファイルの確認

SAP テーブル接続で sapnwrfc.ini ファイルのパスとファイル名の両方を指定した場合、Secure Agent は sapnwrfc.ini ファイルを使用します。ただし、接続で sapnwrfc.ini ファイルのパスのみを定義した場合、Secure Agent は、指定したパスに sapnwrfc.ini ファイルが存在するかどうかを最初に確認します。sapnwrfc.ini ファイルが存在する場合、Secure Agent は sapnwrfc.ini ファイルを使用します。存在しない場合は、例外が発生します。

接続タイプのサンプル sapnwrfc.ini ファイル

sapnwrfc.ini ファイルを使用して、次のタイプの接続を設定できます。

SAP アプリケーションサーバーへの接続

この接続を作成し、RFC クライアントと SAP システムの間の通信を有効にします。それぞれの接続エントリは、1 つのアプリケーションサーバーと 1 つの SAP システムを指定します。

以下の例に、sapnwrfc.ini ファイルの特定の SAP アプリケーションサーバーの接続エントリを示します。

```
DEST=sapr3  
ASHOST=sapr3  
SYSNR=00
```

SAP 負荷分散のための接続

この接続を作成し、SAP が実行時の負荷が最も低いアプリケーションサーバーへの RFC 接続を作成できるようにします。SAP 負荷分散を使用する場合は、この接続を使用します。

以下の例に、sapnwrfc.ini ファイルの SAP 負荷分散の接続エントリを示します。

```
DEST=sapr3  
R3NAME=ABV  
MSHOST=infamessageserver.informatica.com  
GROUP=INFADDEV
```

SAP ゲートウェイで登録されている RFC サーバープログラムへの接続

この接続を作成して、受信する送信 IDoc のソースとなる SAP システムに接続します。

以下の例に、sapnwrfc.ini ファイルの SAP ゲートウェイで登録されている RFC サーバープログラムの接続エントリを示します。

```
DEST=sapr346CLSQA  
PROGRAM_ID=PID_LSRECEIVE  
GWHOST=sapr346c  
GWSERV=sapgw00
```

さまざまな接続タイプに対して、sapnwrfc.ini ファイルで次のようなパラメータを設定できます。

sapnwrfc.ini のパラメータ	説明	適用できる接続タイプ
DEST	接続用の SAP システムの論理名。 すべての DEST エントリは一意にする必要があります。SAP システムごとに DEST エントリを 1 つだけ設定する必要があります。 SAP バージョン ECC 6.0 以降の場合は、最大 32 文字を使用できます。	このパラメータは、以下のタイプの接続に使用します。 - 特定の SAP アプリケーションサーバーへの接続 - 負荷分散を使用する接続 - SAP ゲートウェイで登録されている RFC サーバープログラムへの接続
ASHOST	SAP アプリケーションのホスト名または IP アドレス。Secure Agent はこのエントリを使用して、アプリケーションサーバーに接続します。	このパラメータを使用して、特定の SAP アプリケーションサーバーへの接続を作成します。
SYSNR	SAP システム番号。	このパラメータを使用して、特定の SAP アプリケーションサーバーへの接続を作成します。
R3NAME	SAP システムの名称。	このパラメータを使用して、SAP 負荷分散を使用する接続を作成します。
MSHOST	SAP メッセージサーバーのホスト名。	このパラメータを使用して、SAP 負荷分散を使用する接続を作成します。
GROUP	SAP アプリケーションサーバーのグループ名。	このパラメータを使用して、SAP 負荷分散を使用する接続を作成します。
PROGRAM_ID	プログラム ID。プログラム ID は、IDoc を送受信するために SAP システムで定義した論理システムのプログラム ID と同一であることが必要です。	このパラメータを使用して、SAP ゲートウェイで登録されている RFC サーバープログラムへの接続を作成します。
GWHOST	SAP ゲートウェイのホスト名。	このパラメータを使用して、SAP ゲートウェイで登録されている RFC サーバープログラムへの接続を作成します。
GWSERV	SAP ゲートウェイのサーバー名。	このパラメータを使用して、SAP ゲートウェイで登録されている RFC サーバープログラムへの接続を作成します。
TRACE	RFC 接続関連の問題をデバッグします。 トレースに求める詳細レベルに基づいて、以下のいずれかの値を設定します。 - 0. オフ - 1. Brief - 2. Verbose - 3. フル	このパラメータは、以下のタイプの接続に使用します。 - 特定の SAP アプリケーションサーバーへの接続 - 負荷分散を使用する接続 - SAP ゲートウェイで登録されている RFC サーバープログラムへの接続

次のスニペットは、sapnwrfc.ini ファイルの例を示しています。

```
/*=====*/
/* Connection to an RFC server program registered at an SAP gateway */
/*=====*/
DEST=<destination in RfcRegisterServer>
PROGRAM_ID=<program-ID, optional; default: destination>
GWHOST=<host name of the SAP gateway>
GWSERV=<service name of the SAP gateway>
/*=====*/
```

```

/* Connection to a specific SAP application server */
/*=====*/
DEST=<destination in RfcOpenConnection>
ASHOST=<Host name of the application server.>
SYSNR=<The back-end system number.>
/*=====*/
/* Connection to use SAP load balancing */
/* The application server will be determined at run time. */
/*=====*/
DEST=<destination in RfcOpenConnection>
R3NAME=<name of SAP system, optional; default: destination>
MSHOST=<host name of the message server>
GROUP=<group name of the application servers, optional; default: PUBLIC>

```

SAP に接続するための HTTPS の設定

HTTPS 経由で SAP に接続し、SAP テーブルソースの読み取りを行うには、Secure Agent マシンおよび SAP システムで OpenSSL 証明書が使用可能であることを確認してください。

Secure Agent マシンで OpenSSL 証明書を作成します。次に、作成した証明書を PSE 形式で SAP システムトラストストアにインポートします。

さらに、SAP テーブル接続で HTTPS を有効にするには、SAP テーブル接続プロパティおよび SAP システムでキーストアファイルの生成キーストアパスワードとプライベートキーパスワードを指定する必要があります。

OpenSSL 証明書の作成

OpenSSL 証明書を作成する前に、前提条件のタスクを実行する必要があります。

- Secure Agent マシンに OpenSSL をダウンロードしてインストールします。
- Secure Agent と SAP システムをホストするマシンのオペレーティングシステムに基づき、SAPGENPSE 暗号化ツールの最新パッチを SAP Service Marketplace からダウンロードします。
デフォルトでは、SAPGENPSE ファイルは nt-x86_64 ディレクトリに抽出されます。
- SAP パラメータ `icm/server_port`、`ssl/ssl_lib`、`sec/libsapsecu`、`ssf/ssfapi_lib`、`ssf/name`、`icm/HTTPS/verify_client`、`ssl/client_pse`、`wdisp/ssl_encrypt` を設定します。
詳細については、SAP のマニュアルを参照してください。

OpenSSL を使用して自己署名証明書を作成するには、次のタスクを実行します。

1. コマンドラインから、`OPENSSL_CONF` 変数に `openssl.cfg` ファイルへの絶対パスを設定します。
例えば、コマンド `set OPENSSL_CONF= C:\OpenSSL-Win64\bin\openssl.cfg` を実行します。
2. `<openssl installation directory>\bin` ディレクトリに移動します。
3. 2048 ビットの RSA プライベートキーを生成するには、次のコマンドを実行します：
`openssl.exe req -new -newkey rsa:2048 -sha1 -keyout <RSAkey File_Name>.key -out <RSAkey File_Name>.csr`
4. プロンプトが表示されたら、次の値を入力します。
 - プライベートキーのパスワード（PEM パスフレーズ）。秘密鍵の暗号化に使用するフレーズを入力します。確認のためにパスワードを再入力します。
重要: この PEM パスワードを書き留めます。自己署名キーと PKCS#12 証明書の作成時に、このパスワードを指定する必要があります。
 - 国名の 2 文字のコード。
 - 都道府県または州の名前。

- 市区町村名。
- 組織名。
- 組織単位名。
- 共通名 (CN)。必須。

重要: Secure Agent をホストするマシンの完全修飾ホスト名を入力します。

- 電子メールアドレス。

5. 必要に応じて、証明書要求とともに渡す次の属性を入力します。

- チャレンジパスワード。
- 会社名 (省略可能)。

2048 ビットの RSA プライベートキーが作成されます。指定したディレクトリに<RSAkey File_Name>.key および<RSAkey File_Name>.csr ファイルが生成されます。

6. RSA プライベートキーを使用して自己署名キーを生成するには、次のコマンドを実行します:

```
openssl x509 -req -days 11499 -in <RSAkey File_Name>.csr -signkey <RSAkey File_Name>.key -out <Certificate File_Name>.crt
```

7. プロンプトが表示されたら、RSA プライベートキーの PEM パスフレーズを入力します。

指定したディレクトリに<Certificate File_Name>.crt ファイルが生成されます。

8. <Certificate File_Name>.crt ファイルと<RSAkey File_Name>.key ファイルの内容を .pem ファイルに連結するには、次のタスクを実行します。

- テキストエディタで<Certificate File_Name>.crt ファイルと<RSAkey File_Name>.key ファイルを開きます。
- ファイルを作成して<PEM File_Name>.pem という名前で保存します。
- <Certificate File_Name>.crt ファイルのコンテンツをコピーし、.pem ファイルに貼り付けます。
- <RSAkey File_Name>.key ファイルのコンテンツをコピーし、.pem ファイルの既存のコンテンツに追加します。
- <PEM file name>.pem ファイルを保存します。

9. PKCS#12 証明書を作成するには、コマンドラインから次のコマンドを実行します:

```
openssl pkcs12 -export -in <PEM File_Name>.pem -out <P12 File_Name>.p12 -name "domain name"
```

10. プロンプトが表示されたら、次の詳細を入力します。

- .pem ファイルの PEM パスフレーズ。
- P12 ファイルのエクスポートパスワード。確認のためにパスワードを再入力します。

重要: P12 ファイルのこのエクスポートパスワードを書き留めます。HTTPS 経由で SAP に接続するための Java キーストアファイルの作成時に、このパスワードを指定する必要があります。

指定した場所に<P12 File_Name>.p12 ファイルが生成されます。

11. Java キーストアファイルを作成するには、次のコマンドを入力します。

```
keytool -v -importkeystore -srckeystore <P12 File_Name>.p12 -srcstoretype PKCS12 -destkeystore <JKS File_Name>.jks -deststoretype JKS -srcalias "source alias" -destalias "destination alias"
```

12. プロンプトが表示されたら、次の詳細を入力します。

- ターゲットキーストアである JKS ファイルのパスワード。

重要: このパスワードを書き留めます。SAP テーブル接続の作成時に、このパスワードを指定する必要があります。

- ソースキーストアである P12 ファイルのパスワード。P12 ファイルのエクスポートパスワードを入力します。

指定したディレクトリに<JKS File_Name>.jks ファイルが生成されます。

SAP テーブル接続で HTTPS を有効にするときに、このキーストアファイルの名前と場所を指定します。また、SAP テーブル接続プロパティおよび SAP システムで、[キーストアのパスワード] としてターゲットキーストアパスワードを指定し、[プライベートキーのパスワード] としてソースキーストアパスワードを指定する必要があります。

OpenSSL 証明書から PSE 形式への変換

OpenSSL 証明書を作成した後に、SAPGENPSE ツールを使用して OpenSSL 証明書を PSE 形式に変換する必要があります。

1. コマンドラインから、<SAPGENPSE 抽出ディレクトリ>ディレクトリに移動します。
2. PSE ファイルを生成するには、次のコマンドを実行します:

```
sapgenpse import_p12 -p <PSE_Directory>\<PSE File_Name>.pse <P12 Certificate_Directory>\<P12 File_Name>.p12
```
3. プロンプトが表示されたら、次の詳細を入力します。
 - P12 ファイルのパスワード。P12 ファイルのエクスポートパスワードを入力します。
 - PSE ファイルを保護するための個人識別番号 (PIN)。確認のために PIN を再入力します。指定したディレクトリに<PSE File_Name>.pse ファイルが生成されます。
4. PSE 形式に基づいて証明書を生成するには、次のコマンドを実行します:

```
sapgenpse export_own_cert -p <PSE File_Directory>\<PSE File_Name>.pse -o <Certificate_Name>.crt
```
5. プロンプトが表示されたら、PSE PIN 番号を入力します。
指定した場所に<Certificate_Name>.crt ファイルが生成されます。この証明書ファイルを SAP システムのトラストストアにインポートします。

SAP システムで HTTPS サービスを有効にします。

SAP システムに接続するように HTTPS を設定するには、SAP システムのトランザクションコード SAP ICM モニタ (SMICM) から HTTPS サービスを有効にする必要があります。

SAP システムで HTTPS サービスを有効にする方法の詳細については、SAP のマニュアルを参照してください。

SAP システムのトラストストアへの証明書のインポート

HTTPS 経由で SAP に接続するには、証明書を PSE 形式で SAP システムのトラストストアにインポートする必要があります。

1. SAP にログインし、STRUST トランザクションに移動します。
2. [SSL クライアント (標準)] を選択し、パスワードを指定します。
[証明書のインポート] ダイアログで、証明書ファイル形式として Base64 形式を選択する必要があります。
3. [インポート] アイコンをクリックし、PSE 形式の<Certificate_Name>.crt を選択します。
注: ユーザーが別の SAP ネットワークに存在する場合は、SAP アプリケーションサーバー上のエージェントホストの DNS エントリを追加する必要があります。
4. [証明書リストに追加] をクリックします。
5. インターネット通信マネージャを再起動します。

セキュアなネットワーク通信プロトコルの設定

SAP テーブルコネクタ接続とセキュアネットワークコミュニケーションプロトコルを使用すると、SAP に対して安全な読み取りまたは書き込みを行うことができます。

SAP SNC 接続を設定する手順の詳細については、Informatica How-To ライブラリの記事「[Configure the SAP Secure Network Communication protocol](#)」を参照してください。

Secure Agent が SAP でホワイトリストに登録されたホストとして動作するようにする（オプション）

SAP テーブルデータを読み取るときに、Secure Agent がホワイトリストに登録されたホストとして動作できるようにすることができます。Secure Agent をホワイトリストに登録されたホストとして動作するように設定する前に、最新のトランスポートファイルがインストールされていることを確認します。

- Administrator で **JVMOption** プロパティを設定して、SAP システムの HTTP_Whitelist テーブルに追加できるホストとして Secure Agent を定義するには、次の手順を実行します。
 - [Administrator]** > **[ランタイム環境]** の順に選択します。
 - [ランタイム環境]** ページで、マッピングを実行する Secure Agent マシンを選択します。
 - [編集]** をクリックします。
 - [システム構成の詳細]** セクションの **[サービス]** リストから、**[データ統合サーバー]** を選択します。
 - JVMOption** フィールドを編集して、次の値を追加します。
-Dsap_whitelist_check=1
 - [保存]** をクリックします。
 - SAP のホストとして定義するすべての Secure Agent について、手順 b~f を繰り返します。
- トランザクション SE16 を使用して、SAP HTTP_Whitelist テーブルに Secure Agent にエントリを作成します。Secure Agent にエントリを作成するには、SAP システムで次の手順を実行します。
 - トランザクション SE16 に進みます。
 - Secure Agent を SAP のホストとして定義するようにプロパティを設定します。
次の表に、設定する必要があるプロパティを示します。

プロパティ	説明
MANDT	必須。SAP クライアント番号。
ENTRY TYPE	必須。このエントリと比較する URL のタイプ。 URL が CSS テーマの URL であることを示すには、01 を入力します。
SORT KEY	必須。プライマリキーとして使用される一意の値。 数字とアルファベットを入力できます。

プロパティ	説明
PROTOCOL	SAP が検証する必要があるプロトコル。 HTTP または HTTPS を入力します。 値を入力しない場合、SAP はプロトコルを検証しません。
HOST	SAP が検証する必要があるホストマシン。 Secure Agent をホストするマシンの IP アドレスを入力します。
PORT	SAP が検証する必要があるポート番号。 【ポート】 フィールドを空白のままにして、SAP ではポートを検証する必要がないことを示します。
URL	SAP が検証する必要がある URL。 SAP が URL を検証する必要がないことを示すには、*を入力します。

注: 手順 2 を実行しない場合、SAP で実行されるマッピングとタスクが失敗します。

3. SAP のホワイトリストに登録されているホストとして設定するすべての Secure Agent について、手順 1 と 2 を繰り返します。

サーバーレスランタイム環境の使用

Linux での SAP テーブルコネクタ接続の設定時に、AWS でホストされているサーバーレスランタイム環境を使用して SAP システムに接続できます。

SAP Secure Network Communication (SNC) プロトコルを使用する予定がある場合、サーバーレスランタイム環境を使用することはできません。

サーバーレスランタイム環境を使用して SAP テーブルコネクタ接続を設定する前に、次のタスクを実行してください。

- AWS アカウントの Amazon S3 バケットに SAP ライブラリを追加します。
- .yml サーバーレス構成ファイルを設定する。
- Linux 上のサーバーレスランタイム環境の JAVA_LIBS プロパティを設定します。

AWS アカウントの Amazon S3 バケットに SAP ライブラリを追加します

サーバーレスランタイム環境で SAP テーブルコネクタ接続を設定するには、次の手順を実行します。

1. AWS のサーバーレスエージェント設定用に次の構造を作成します: <補足ファイルの場所>/serverless_agent_config
2. AWS アカウントの次の場所にある Amazon S3 バケットに SAP ライブラリを追加します: <補足ファイルの場所>/serverless_agent_config/sap

.yml サーバーレス構成ファイルを設定する

次の手順を実行して、サーバーレスランタイム環境で.yml サーバーレス構成ファイルを設定し、SAP ライブラリをサーバーレスエージェントディレクトリにコピーします。

1. 次のコードスニペットをテキストエディタにコピーします。

```
version: 1
agent:
  dataIntegrationServer:
    autoDeploy:
      sap:
        jcos:
          - fileCopy:
              sourcePath: sap/jco/<sapjco_library_filename>
          - fileCopy:
              sourcePath: sap/jco/<sapjco_library_filename>
        nwrfdc:
          - fileCopy:
              sourcePath: sap/nwrfdc/<rfdc_library_filename>
          - fileCopy:
              sourcePath: sap/nwrfdc/<sapnwrfdc_filename>
```

ここで、ソースパスは AWS の SAP ライブラリファイルのディレクトリパスです。

2. 構文とインデントが有効であることを確認してから、ファイルを `serverlessUserAgentConfig.yml` として次の AWS の場所に保存します: <Supplementary file location>/serverless_agent_config.yml ファイルの実行時に、SAP ライブラリが AWS の場所からサーバーレスエージェントディレクトリにコピーされます。

サーバーレスランタイム環境の JAVA_LIBS プロパティを設定する

Administrator で次の手順を実行して、Linux 上のサーバーレスランタイム環境に JAVA_LIBS プロパティを設定します。

1. Informatica Intelligent Cloud Services にログインします。
2. **[Administrator]** > **[サーバーレス環境]** の順に選択します。
3. **[サーバーレス環境]** タブで、必要なサーバーレスランタイム環境の **[アクション]** メニューを展開し、**[編集]** を選択します。
4. **[ランタイム設定のプロパティ]** タブで、サービスに **[データ統合サーバー]** を選択し、タイプに **[Tomcat_JRE]** を選択します。
5. **[プロパティの追加]** をクリックします。
6. **[名前]** フィールドに `JAVA_LIBS` と入力し、次の値を設定します。
`../bin/rdtm-extra/tpl/sap/sapjco3.jar:../bin/rdtm/java/lib/sap/sap-adapter-common.jar`
7. **[保存]** をクリックします。

サーバーレス環境の設定および使用方法の詳細については、Administrator のヘルプにある「ランタイム環境」の「サーバーレスランタイム環境のセットアップ」を参照してください。

SAP テーブル接続のトラブルシューティング

SAP テーブル接続をテストすると、次のエラーが表示されます。

Test Connection Failed for <connection name>/sap/conn/jco/JCoException

sapjco3.jar が次のディレクトリに保存されていることを確認します:

<Informatica Secure Agent installation directory>\apps\Data_Integration_Server\ext\deploy_to_main\bin\rdtm-extra\tpl\sap

sapjco3.jar をコピーした後に、Secure Agent を再開します。

SAP テーブル接続をテストするか、SAP テーブル接続をタスクで使用すると、次のエラーが表示されます。

Test Connection Failed for <connection name>. Error getting the version of the native layer:
java.lang.UnsatisfiedLinkError: no sapjco3 in java.library.path.

sapjco3.dll ファイルの場所が、Secure Agent マシンの PATH 変数に含まれていることを確認します。

SAP テーブル接続をテストするか、タスクで接続を使用すると、次のエラーが表示されます。

Test Connection Failed for <connection name>. Error getting the version of the native layer:
java.lang.UnsatisfiedLinkError: no sapjco3 in java.library.path.

sapjco3.dll の場所を PATH 変数に追加して、Secure Agent を再開します。

SAP テーブルから読み取りを行うタスクが、次のエラーで失敗します。

Error occurred processing data from SAP : Unable to establish Http Communication between SAP server and agent!
Shutting down reader.

HTTP ポートが開いていないか、受信要求が Windows ファイアウォールによってブロックされています。この問題を解決するには、Windows ファイアウォールで詳細設定を使用して新しい受信ルールを作成します。ルールを TCP およびすべてのポートに適用して、HTTP プロトコルを選択します。

第 206 章

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
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。
シークレットコンテナの使用	組織に対して設定されている Secrets Manager にこの接続の機密資格情報を保存します。 このプロパティは、組織に Secrets Manager が設定されている場合にのみ表示されます。 このプロパティは、データ取り込みおよびレプリケーションとデータアクセス管理サービスではサポートされていません。 接続でシークレットコンテナを有効にすると、Secure Agent が Secrets Manager からどの資格情報を取得するかを選択できます。このオプションを無効にした場合、資格情報は組織の設定方法に応じてリポジトリまたはローカル Secure Agent に保存されます。 注: この接続を使用してプッシュダウンまたはプロキシサービスを介してデータアクセスポリシーを適用する場合、シークレットコンテナ設定オプションを使用することはできません。 Secrets Manager を設定および使用方法については、Administrator のヘルプにある「Secrets Manager の設定」を参照してください。
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。 Secure Agent ランタイム環境を指定します。 ランタイム環境の設定および使用方法の詳細については、Administrator のヘルプにある「ランタイム環境」を参照してください。
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。

第 207 章

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	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。
シークレットコンテンツの使用	組織に対して設定されている Secrets Manager にこの接続の機密資格情報を保存します。 このプロパティは、組織に Secrets Manager が設定されている場合にのみ表示されます。 このプロパティは、データ取り込みおよびレプリケーションとデータアクセス管理サービスではサポートされていません。 接続でシークレットコンテンツを有効にすると、Secure Agent が Secrets Manager からどの資格情報を取得するかを選択できます。このオプションを無効にした場合、資格情報は組織の設定方法に応じてリポジトリまたはローカル Secure Agent に保存されます。 注: この接続を使用してプッシュダウンまたはプロキシサービスを介してデータアクセスポリシーを適用する場合、シークレットコンテンツ設定オプションを使用することはできません。 Secrets Manager を設定および使用する方法については、Administrator のヘルプにある「Secrets Manager の設定」を参照してください。
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。 ランタイム環境の設定および使用方法の詳細については、Administrator のヘルプにある「ランタイム環境」を参照してください。
Satmetrix URL	Secure Agent が Satmetrix API に接続するために使用する URL。 URL の形式: <i>http://<会社名>.satmetrix.com</i>
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。

第 208 章

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。
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。 <i>host_name</i> は、ホスト名または IP アドレスにできます。 <i>host_name:port_number</i> 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。

プロパティ	説明
オフロード処理	<p>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。</p> <ul style="list-style-type: none"> - 自動。オフロード処理を使用するかどうかは 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。 <p>デフォルトは「いいえ」です。</p>
オフロードスレッド	<p>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。</p> <p>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。</p> <p>有効な値は 1～64 です。</p> <p>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。</p> <p>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。</p>
配列サイズ	<p>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するストレージ配列のサイズ（単位はレコード数）。</p> <p>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。</p> <p>有効な値は 1～5000 です。デフォルトは 25 です。</p> <p>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。</p>
低値をスペースに置き換える	<p>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。</p>
接続リトライ期限	<p>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。</p>

プロパティ	説明
カスタムプロパティ	<p>カスタムプロパティまたは接続プロパティのオーバーライド。カスタムプロパティとは、PowerExchange のデフォルトの設定よりも優先するために指定できるプロパティです。セミコロンの (;) 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。</p> <p>例:</p> <pre><property>=<value>;<property>=<value></pre> <p>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。</p> <p>注: これらのプロパティは、PowerCenter の PowerExchange Client for PWX NRDB Batch 接続の 【PWX オーバーライド】 オプションと同じです。</p> <p>また、このフィールドまたはパラメータファイルを使用して、接続プロパティのオーバーライドを指定することもできます。パラメータファイルを使用して接続プロパティのオーバーライドを指定するには、\$<ParameterName>の形式でパラメータを設定し、ユーザー定義パラメータ名の前にドル記号 (\$) を付けます。次に、【ランタイムオプション】 タブの 【パラメータファイル名】 フィールドにパラメータファイル名を指定することで、ユーザー定義パラメータ定義を含むパラメータファイルを使用するようにマッピングのマッピングタスクを設定します。</p> <p>注:</p> <ul style="list-style-type: none"> - マッピングおよび接続に同じパラメータを入力した場合は、接続カスタムプロパティが優先されます。 - パラメータファイルがある場合、このフィールドで指定するパラメータ名は、パラメータファイルで定義されたエントリと一致している必要があります。 <p>詳細については、「接続オーバーライドのリファレンス」の章を参照してください。</p>
書き込みプロパティ	<p>書き込みモード。次のオプションがあります。</p> <ul style="list-style-type: none"> - 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。

第 209 章

ServiceNow 接続のプロパティ

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

ServiceNow への接続

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

始める前に

接続プロパティを設定する前に、ServiceNow アカウントからユーザー名、パスワード、およびサービス URL を取得する必要があります。

次のビデオは、必要な情報を取得する方法を示しています。



接続の詳細

次の表に、基本接続プロパティを示します。

財産	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。

財産	説明
シークレットコンテナの使用	<p>組織に対して設定されている Secrets Manager にこの接続の機密資格情報を保存します。このプロパティは、組織に Secrets Manager が設定されている場合にのみ表示されます。このプロパティは、データ取り込みおよびレプリケーションとデータアクセス管理サービスではサポートされていません。</p> <p>接続でシークレットコンテナを有効にすると、Secure Agent が Secrets Manager からどの資格情報を取得するかを選択できます。このオプションを無効にした場合、資格情報は組織の設定方法に応じてリポジトリまたはローカル Secure Agent に保存されます。</p> <p>注: この接続を使用してプッシュダウンまたはプロキシサービスを介してデータアクセスポリシーを適用する場合、シークレットコンテナ設定オプションを使用することはできません。</p> <p>Secrets Manager を設定および使用方法については、Administrator のヘルプにある「Secrets Manager の設定」を参照してください。</p>
ランタイム環境	<p>タスクを実行するランタイム環境の名前。</p> <p>Secure Agent、ホステッドエージェント、サーバーレスランタイム環境、またはエラスティックランタイム環境を選択します。</p> <p>詳細モードのマッピングで接続を使用する場合は、ホステッドエージェントを使用しないでください。</p> <p>ランタイム環境の設定および使用方法の詳細については、Administrator のヘルプにある「ランタイム環境」を参照してください。</p>
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。

詳細設定

次の表に、詳細接続のプロパティを示します。

プロパティ	説明
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。

ファイアウォール設定

組織で保護ファイアウォールを使用している場合は、承認された IP アドレスのリストに Secure Agent の IP アドレス範囲を含めて、ファイアウォールを介して Secure Agent が必要なすべてのタスクを実行できるようにします。

Secure Agent では、次の IP アドレス範囲が使用されます。

- 209.34.91.0-255
- 206.80.52.0-255

- 206.80.61.0-255
- 209.34.80.0-255

プロキシサーバーの設定

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

Windows および Linux でプロキシサーバーを使用するように Secure Agent を設定できます。認証されていないプロキシサーバーのみを使用できます。マッピングおよび詳細モードのマッピングでプロキシを設定できます。

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

- Windows の場合は Secure Agent Manager を使用し、Linux の場合はシェルコマンドを使用して Secure Agent を設定します。
手順については、データ統合のヘルプの『または「Windows でのプロキシ設定」または「Linux でのプロキシ設定」を参照してください。
- proxy.ini ファイルでプロキシサーバーのプロパティを設定します。

サーバーレスランタイム環境を使用している場合、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。

正しいプロキシ設定については、ネットワーク管理者にお問い合わせください。

proxy.ini ファイルを介したプロキシサーバーの設定

プロキシサーバーを有効にするには、proxy.ini ファイルを使用して Secure Agent を設定します。

1. Secure Agent マシン上の次のディレクトリに移動します: <Secure Agent のインストールディレクトリ>\Informatica Cloud Secure Agent\apps\agentcore\conf\proxy.ini
2. プロキシサーバーのホストとポート番号を proxy.ini ファイルに追加します。
InfaAgent.ProxyHost=<Proxy server hostname>
InfaAgent.ProxyPort=<Proxy server port number>
3. Secure Agent を再起動します。

ServiceNow 接続のテスト

ServiceNow に接続できるかどうかを確認するには、REST または SOAP クライアントを開いて接続をテストします。

次の [SOAP URL](#) を使用して、REST、JSON、JSONv2、または SOAP エンドポイントをテストすることをお勧めします。

SynQ_User_Role またはロールに指定した名前を持つユーザー資格情報を使用する必要があります。

接続ステータスの確認

接続ステータスを確認するには、任意の REST クライアントから REST API を呼び出します。

API を呼び出す前に、ユーザー、グループ、およびロールが設定されていることを確認してください。

Purpose : Testing Connection with ServiceNow
URL :https://<instance>.service-now.com/api/now/table/sys_user
Authentication: Basic

適切なロールを設定すると、次の図のような応答が返されます。

GET https://ven01218.service-now.com/api/now/table/sys_db_object

Authorization: Basic Auth

Username: admin

Password: *****

Status: 200 OK Time: 15046 ms

```
{
  "result": [
    {
      "create_access": "false",
      "alter_access": "false",
      "sys_replace_on_upgrade": "false",
      "access": "",
      "live_feed_enabled": "false",
      "sys_updated_on": "2017-10-17 12:12:56",
      "sys_class_name": "sys_db_object",
    }
  ]
}
```

適切な結果が得られない場合は、ユーザーの資格情報と ServiceNow ACL を確認してください。

資格情報の確認

ACL とユーザー設定が正しいかどうかを確認するには、REST クライアントから REST API を呼び出します。

次の図に、REST クライアントからの GET 要求の検証の例を示します。

GET https://ven01218.service-now.com/api/now/table/sys_user

Authorization: Basic YWRtaW46TW9uc2FzeXMxMjMh

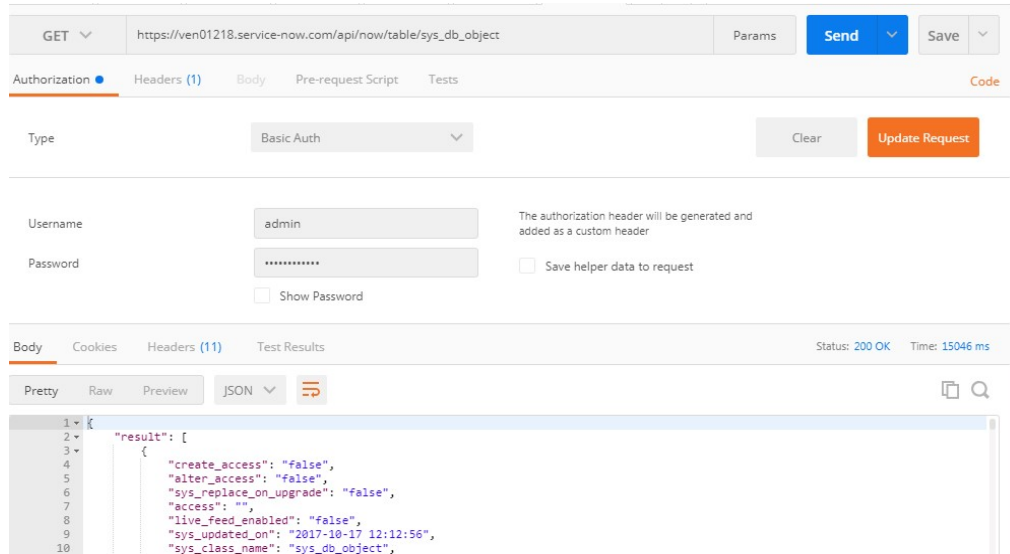
Status: 200 OK Time: 8295 ms

```
{
  "result": [
    {
      "calendar_integration": "1",
      "country": "",
      "last_position_update": "",
      "user_password": "",
      "last_login_time": "",
      "source": "",
      "sys_updated_on": "2016-03-19 06:36:42",
      "building": "",
      "web_service_access_only": "false",
      "notification": "2",
      "sys_updated_by": "system",
      "sys_created_on": "2012-02-18 03:04:49",
      "agent_status": "",
      "sys_domain": {
        "link": "https://ven01218.service-now.com/api/now/table/sys_user_group/global",
        "value": "global"
      }
    }
  ]
}
```

データ統合との接続を正常に作成するには、次の API を使用して資格情報と ACL を確認します。

API URL :https://<instance>.service-now.com/api/now/table/sys_db_object
Authentication:Basic

次の図に、REST クライアントからの GET 要求の検証の例を示します。



API のテスト

ServiceNow からのデータの読み取りまたは ServiceNow へのデータの書き込みにアクセスできる場合は、API でメタデータ情報をテストします。

- メタデータにアクセスできる場合は、次の API をテストします。
 - https://<instance>.service-now.com/api/now/table/sys_db_view.do
 - https://<instance>.service-now.com/api/now/table/sys_db_object.do
 - https://<instance>.service-now.com/api/now/table/<table_name>.do?SCHEMA
- ServiceNow テーブルまたはビューから読み取りを行う SOAP および REST API をテストします。
- REST クライアントを使用して、ACL とユーザーロールのセットアップをテストできます。REST クライアントを使用してテストするには、有効な REST API URL、適切なメソッド、有効なパラメータ、および認証が必要です。例えば、REST API を呼び出して ServiceNow テーブルからデータを取得します。REST 呼び出しを行うには、次の詳細を使用します。

Authentication : Basic (Requires username /password of user who is having SynQ_User_Role)
Method : Get
URL : valid api url

REST API の URL とパラメータの詳細については、ServiceNow のマニュアルの「[Getting Started](#)」を参照してください:

第 210 章

ServiceNow Mass Ingestion 接続のプロパティ

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

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

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

OAuth 2.0 認証の接続プロパティ

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

接続プロパティ	説明
接続名	接続の名前。この名前は、組織内で一意にする必要があります。接続名には、英数字、スペース、および次のような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。
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。 アプリケーション取り込みとレプリケーションタスクでは、Secure Agent またはサーバーレスランタイム環境を選択できます。ホステッドエージェントは使用できません。
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。

接続プロパティ	説明
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。 <code>https://{your_servicenow_instance}.service-now.com/</code>
OAuth トークン URL	ServiceNow インスタンスの OAuth トークンエンドポイント。接続に関連付けられた API クライアントは、アクセストークン要求をこのエンドポイントに送信します。

基本認証の接続プロパティ

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

接続プロパティ	説明
接続名	接続の名前。この名前は、組織内で一意にする必要があります。接続名には、英数字、スペース、および次のような特殊文字を含めることができます: <code>_ . + -</code> 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。
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。 アプリケーション取り込みとレプリケーションタスクでは、Secure Agent またはサーバーレスランタイム環境を選択できます。ホステッドエージェントは使用できません。
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。 <code>https://{your_servicenow_instance}.service-now.com/</code>

第 211 章

Shopify 接続のプロパティ

Shopify からデータの読み取りを行うための Shopify 接続を作成します。

Shopify への接続

Shopify からデータを読み取るように Shopify 接続を設定してみましょう。

始める前に

接続プロパティを設定をする前に、Shopify アカウントからショップ名と Shopify アクセストークンを取得する必要があります。

次のビデオは、必要な情報を取得する方法を示しています。



接続の詳細

次の表に、基本接続プロパティを示します。

財産	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。

財産	説明
シークレット コンテナの使用	<p>組織に対して設定されている Secrets Manager にこの接続の機密資格情報を保存します。このプロパティは、組織に Secrets Manager が設定されている場合にのみ表示されます。このプロパティは、データ取り込みおよびレプリケーションとデータアクセス管理サービスではサポートされていません。</p> <p>接続でシークレットコンテナを有効にすると、Secure Agent が Secrets Manager からどの資格情報を取得するかを選択できます。このオプションを無効にした場合、資格情報は組織の設定方法に応じてリポジトリまたはローカル Secure Agent に保存されます。</p> <p>注: この接続を使用してプッシュダウンまたはプロキシサービスを介してデータアクセスポリシーを適用する場合、シークレットコンテナ設定オプションを使用することはできません。</p> <p>Secrets Manager を設定および使用する方法については、Administrator のヘルプにある「Secrets Manager の設定」を参照してください。</p>
ランタイム環境	<p>タスクを実行するランタイム環境の名前。</p> <p>Secure Agent またはホステッドエージェントを指定します。</p> <p>データ取り込みおよびレプリケーションの場合は、Secure Agent を使用できます。</p> <p>ランタイム環境の設定および使用方法の詳細については、Administrator のヘルプにある「ランタイム環境」を参照してください。</p>
ショップ名	<p>Shopify アカウントを作成するときに指定するストア名。</p> <p>例えば、Shopify の URL が <code>https://Example.myshopify.com</code> である場合は、Example がショップ名です。</p>
Shopify アクセ ストークン	<p>アクセスを認証し、Shopify API への要求を行うためのアクセストークン。</p>

第 212 章

Slack の接続プロパティ

Slack に対してデータの安全な読み取りまたは書き込みを行うための Slack 接続を作成します。

認証の準備

ベアラートークンおよび OAuth 2.0 認証タイプを設定して、Slack にアクセスすることができます。

接続プロパティを設定する前に、使用する認証のタイプに基づいて認証の詳細を用意しておく必要があります。

OAuth 2.0 認証

OAuth 2.0 認証では、Slack に接続するために Slack 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、およびアクセストークンが必要です。

OAuth 2.0 認証を使用するには、次の前提条件を満たす必要があります。

- Slack アプリケーションを作成して、Slack のワークスペースまたはエンタープライズ組織にインストールします。
組織の管理者は、エンタープライズ組織に Slack アプリケーションをインストールします。
ユーザーまたはボット用の Slack アプリケーションを作成できます。
Slack アプリケーションの作成方法の詳細については、「[Creating an application](#)」を参照してください。
- 管理操作を使用するには、エンタープライズ組織用の Slack アプリケーションを作成してインストールし、アプリケーションで公開配布オプションが有効になっていることを確認してください。
- Slack アプリケーションの公開配布を有効にする場合は、アプリケーションのリダイレクト URL を追加して、データ統合から Slack へのアクセスの認証を行います。
例えば、次のようなりダイレクト URL を使用できます。
`https://iics-icinq1.informaticacloud.com/ma/proxy/oauthcallback`
- 必要なスコープを Slack アプリケーションに追加して、アプリケーションが Slack ワークスペース内で実行できる操作を決定します。
例えば、chat:write スコープを追加して、アプリケーションがワークスペースにメッセージを投稿稿できるようにします。
Slack で操作を実行するために必要なスコープの詳細については、「[Slack のスコープ](#)」 (ページ 840) を参照してください。
アプリケーションにスコープを追加する方法の詳細については、「[Adding scopes](#)」を参照してください。
- Slack 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取得します。クライアント ID とクライアントシークレットは、Slack アプリケーションの【基本情報】タブで確認できます。

ベアラートークン認証

ベアラートークン認証では、Slack に接続するために Slack アプリケーションのトークンが必要です。

ベアラートークン認証を使用するには、次の前提条件を満たす必要があります。

- Slack アプリケーションを作成して、Slack のワークスペースまたはエンタープライズ組織全体にインストールします。
組織の管理者は、エンタープライズ組織に Slack アプリケーションをインストールします。
ユーザーまたはボット用の Slack アプリケーションを作成できます。
Slack アプリケーションの作成方法の詳細については、「[Creating an application](#)」を参照してください。
- 管理操作を使用するには、エンタープライズ組織のアプリケーションをインストールします。
- 必要なスコープを Slack アプリケーションに追加して、アプリケーションが Slack ワークスペース内で実行できる操作を決定します。
例えば、chat:write スコープを追加して、アプリケーションがワークスペースにメッセージを投稿稿できるようにします。
アプリケーションにスコープを追加する方法の詳細については、「[Adding scopes](#)」を参照してください。
Slack で操作を実行するために必要なスコープの詳細については、「[Slack のスコープ](#)」(ページ 840)」を参照してください。
- Slack アプリケーションのトークンを取得します。トークンは、Slack アプリケーションの [OAuth と権限] ページの [ワークスペースの OAuth トークン] に表示されます。

Slack への接続

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

始める前に

開始する前に、ユーザーは Slack アカウントから情報を取得する必要があります。

認証の前提条件の詳細については、「[認証の準備](#)」(ページ 837)を参照してください。

接続の詳細

次の表に、基本接続プロパティを示します。

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

プロパティ	説明
シークレットコンテナの使用	<p>組織に対して設定されている Secrets Manager にこの接続の機密資格情報を保存します。このプロパティは、組織に Secrets Manager が設定されている場合にのみ表示されます。このプロパティは、データ取り込みおよびレプリケーションとデータアクセス管理サービスではサポートされていません。</p> <p>接続でシークレットコンテナを有効にすると、Secure Agent が Secrets Manager からどの資格情報を取得するかを選択できます。このオプションを無効にした場合、資格情報は組織の設定方法に応じてリポジトリまたはローカル Secure Agent に保存されます。</p> <p>注: この接続を使用してプッシュダウンまたはプロキシサービスを介してデータアクセスポリシーを適用する場合、シークレットコンテナ設定オプションを使用することはできません。</p> <p>Secrets Manager を設定および使用する方法については、Administrator のヘルプにある「Secrets Manager の設定」を参照してください。</p>
ランタイム環境	<p>タスクを実行するランタイム環境の名前。</p> <p>Secure Agent またはホステッドエージェントを指定することができます。</p> <p>ランタイム環境の設定および使用方法の詳細については、Administrator のヘルプにある「ランタイム環境」を参照してください。</p>
ベース URL	<p>Slack API に接続するためのベース URL。</p> <p>例: <code>https://slack.com/api/</code></p>

認証タイプ

ベアートークンおよび OAuth 2.0 認証タイプを設定して、Slack にアクセスすることができます。

必要な認証方法を選択し、認証固有のパラメータを設定します。

OAuth 2.0 認証

OAuth 2.0 認証では、Slack に接続するために Slack 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、およびアクセストークンが必要です。

次の表に、OAuth 2.0 認証の基本接続プロパティとその説明を示します。

プロパティ	説明
クライアント ID	Slack 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	Slack 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	<p>Slack アプリケーションが Slack ワークスペースで操作を実行するための権限。</p> <p>複数の値はカンマで区切ります。値の間にはスペースを追加しないようにしてください。</p> <p>chat:write または files:write スコープが必要な操作の場合は、ユーザーまたはボットのアプリケーションを作成したかどうかに基づいて、chat:write:user、chat:write:bot、または files:write:user を使用していることを確認してください。</p>

プロパティ	説明
アクセストークン	Slack アプリケーションのアクセストークン。 アプリケーションを作成したユーザーまたはボットのアクセストークンを生成します。 アクセストークンの生成時に、ワークスペース名を次の形式で指定します。 your-workspace.slack.com 管理操作を使用するには、エンタープライズ組織の URL を入力します。 例: your-workspace.enterprise.slack.com
アクセストークンパラメータ	アクセストークンを取得するためにアクセストークン URL に含める追加のパラメータ。 JSON 形式のキーと値のペアでパラメータを定義します。複数のキーと値のペアはカンマで区切ります。 例: client_id=1234567890,client_secret=abcd1234
認証コードパラメータ	認証コードを取得するために認証コード URL に含める追加のパラメータ。 JSON 形式のキーと値のペアでパラメータを定義します。複数のキーと値のペアはカンマで区切ります。 例: client_id=1234567890,scope=channels:read+groups:read+im:read+mpim:read,redirect_uri=https://iics-icinq1.informaticacloud.com/ma/proxy/oauthcallback

ベアラートークン認証

ベアラートークン認証では、Slack に接続するために Slack アプリケーションのトークンが必要です。次の表に、ベアラートークン認証の基本的な接続プロパティとその説明を示します。

プロパティ	説明
トークン	Slack アプリケーションのトークン。 Slack アプリケーションを作成したユーザーまたはボットのトークンを指定します。

Slack のスコープ

スコープは、Slack アプリケーションがワークスペースで操作を実行するための権限です。次の表に、ワークスペースで操作を実行するために Slack アプリケーションに必要なスコープとその説明を示します。

操作	ユーザーのスコープ	ボットのスコープ
Add_Reminder	reminders:write	適用できません
Add_User	admin.users:write	適用できません
Approve_Invite_Requests	admin.invites:write	適用できません
Archive_Channel	channels:write、groups:write、im:write、mpim:write	channels:manage、groups:write、im:write、mpim:write

操作	ユーザーのスコープ	ボットのスコープ
Channel_Information	channels:read、groups:read、 im:read、mpim:read	channels:read、groups:read、 im:read、mpim:read
Conversation_History	channels:history、 groups:history、im:history、 mpim:history	channels:history、groups:history、 im:history、mpim:history
Create_Channel	channels:write、groups:write、 im:write、mpim:write	channels:manage、groups:write、 im:write、mpim:write
Create_Workspace	admin.teams:write	適用できません
Delete_Channel	admin.conversations:write	適用できません
Delete_Files	files:write、files:write:user	files:write
Delete_Message	chat:write、chat:write:user、 chat:write:bot	chat:write
Delete_Reminder	reminders:write	適用できません
Invite_user_to_channel	channels:write.invites、 groups:write.invites、 mpim:write.invites、 channels:write、groups:write、 im:write、mpim:write	channels:write.invites、 groups:write.invites、 mpim:write.invites、 channels:manage、groups:write、 im:write、mpim:write
List_Channels	channels:read、groups:read、 im:read、mpim:read	channels:read、groups:read、 im:read、mpim:read
List_Channel_Members	channels:read、groups:read、 im:read、mpim:read	channels:read、groups:read、 im:read、mpim:read
List_Reminders	reminders:read	適用できません
List_User_Invites	admin.invites:read	適用できません
List_Users	users:read	users:read
List_Users_As_an_Admin	admin.users:read	適用できません
List_Workspaces	admin.teams:read	適用できません
Remove_User_From_Channel	channels:write、groups:write、 im:write、mpim:write	channels:manage、groups:write、 im:write、mpim:write
Remove_User_From_Workspace	admin.users:write	適用できません
Rename_Channel	channels:write、groups:write、 im:write、mpim:write	channels:manage、groups:write、 im:write、mpim:write
検索	search:read	適用できません
Send_Ephemeral_Message	chat:write、chat:write:user、 chat:write:bot	chat:write

操作	ユーザーのスコープ	ボットのスコープ
Send_Message	chat:write、chat:write:user、 chat:write:bot	chat:write
Set_User_Profiles	users.profile:write	適用できません
Test_Authentication	スコープは必要ありません	スコープは必要ありません
Unarchive_Channel	channels:write、groups:write、 im:write、mpim:write	channels:manage、groups:write、 im:write、mpim:write
Update_Chat	chat:write、chat:write:bot、 chat:write:user	chat:write
User_Information	users:read	users:read

第 213 章

Snowflake 接続プロパティ

Snowflake Cloud Data Warehouse 接続の設定時に、接続プロパティを設定する必要があります。

重要: Snowflake Cloud Data Warehouse コネクタは非推奨となり、メンテナンスモードに移行されました。Informatica は将来のリリースでサポートを廃止する予定です。Snowflake Data Cloud Connector を使用して Snowflake にアクセスすることをお勧めします。

次の表に、Snowflake 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	Snowflake アカウントに接続するためのユーザー名。
パスワード	Snowflake アカウントに接続するためのパスワード。
アカウント	Snowflake アカウントの名前。Snowflake URL では、アカウント名がドメイン内の最初のセグメントになります。たとえば、123abc は https://123abc.snowflakecomputing.com のアカウント名です。
ウェアハウス	Snowflake ウェアハウス名。ウェアハウス名は必ず指定する必要があります。
ロール	ユーザーに割り当てられた Snowflake ロール。

接続プロパティ	説明
追加の JDBC URL パラメータ	<p>追加の接続パラメータ。次の形式で 1 つまたは複数のパラメータを指定できます。</p> <pre><param1>=<value>&<param2>=<value>&<param3>=<value>...</pre> <p>以下に例を示します。</p> <pre>user=jon&warehouse=mywh&db=mydb&schema=public</pre> <p>Snowflake で一時テーブルを作成するために使用されるデータベースとスキーマ名をオーバーライドするには、次の形式でデータベースとスキーマ名を入力します。</p> <pre>ProcessConnDB=<DB name>&ProcessConnSchema=<schema_name></pre> <p>Okta SSO 認証を介して Snowflake にアクセスするには、次の形式で SAML 2.0 プロトコルを実装する Web ベースの IdP を入力します。</p> <pre>authenticator=https://<Your_Okta_Account_Name>.okta.com</pre> <p>注: Microsoft ADFS はサポートされていません。</p> <p>Okta 認証の設定の詳細については、次の Web サイトを参照してください: https://docs.snowflake.net/manuals/user-guide/admin-security-fed-auth-configure-snowflake.html#configuring-snowflake-to-use-federated-authentication</p>
データベース/スキーマ	<p>Snowflake データベースとスキーマ名。パラメータは以下の形式で指定します。</p> <pre><database name>/<schema name></pre> <p>注: データベース名とスキーマ名の両方を指定する必要があります。データベース名のみを指定すると、ソースオブジェクトが [ソースオブジェクトの選択] ウィンドウに表示されません。スキーマ名のみを指定すると、データの読み取り時に Invalid Schema 例外が発生します。</p>

第 214 章

Snowflake Data Cloud 接続のプロパティ

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

認証の準備

Snowflake にアクセスするための認証タイプ（標準、認証コード、キーペア、およびクライアント資格情報）を設定できます。Snowflake により安全に接続するために、認証コード、キーペア、またはクライアント資格情報認証の使用を検討してください。

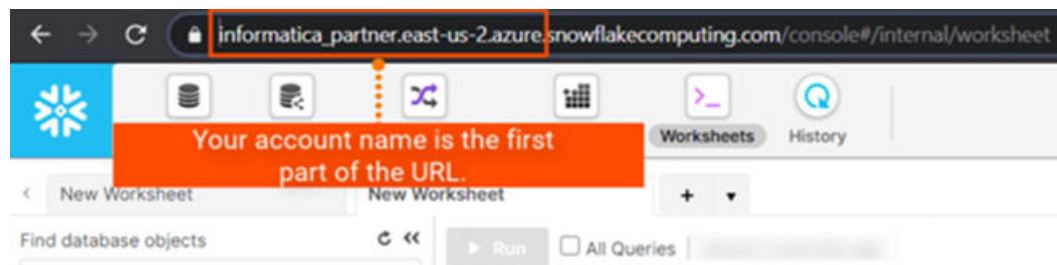
接続プロパティを設定する前に、使用する認証のタイプに基づいて認証の詳細を用意しておく必要があります。

標準

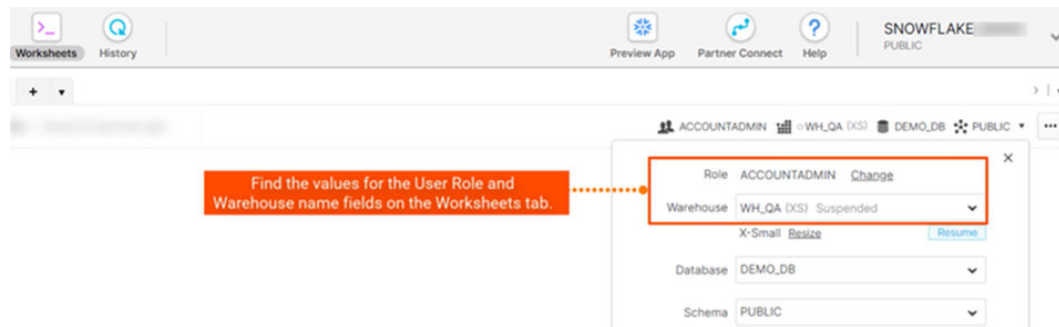
標準認証を使用して Snowflake に接続するには、Snowflake アカウント名、ウェアハウス名、ユーザー名、およびアカウントパスワードまたはプログラムによるアクセストークン（PAT）のいずれかが必要です。

Snowflake アカウント名、ウェアハウス、ロールの詳細などの必要な詳細を Snowflake アカウントから取得してみましょう。

次の画像は、Snowflake アカウントの名前がどこに表示されるかを示しています。



次の画像は、Snowflake アカウントのウェアハウスの名前とロールの詳細を確認できる場所を示しています。



プログラムによるアクセストークンの生成

標準認証を使用して Snowflake に接続するには、アカウントパスワードの代わりに、Snowflake で生成されたプログラムによるアクセストークン（PAT）を使用できます。

環境にデプロイされた Secure Agent、サーバーレスランタイム環境、またはエラスティックランタイム環境を使用する場合は、その IP アドレスの範囲から PAT を使用して Snowflake に接続できるようにする必要があります。

Snowflake で IP アドレスの範囲を許可するには、次のタスクを実行します。

1. 許可する IP アドレスに対するネットワークルールを作成します。
ネットワークルールの作成の詳細については、Snowflake ドキュメントの「[Working with network rules](#)」を参照してください。
2. 作成したネットワークルールのネットワークポリシーを作成します。
ネットワークポリシーの作成の詳細については、Snowflake ドキュメントの「[Working with network policies](#)」を参照してください。

PAT を生成する詳細な手順については、Snowflake ドキュメントの「[Generating a programmatic access token](#)」を参照してください。

承認コード

OAuth 2.0 認証コードを使用して Snowflake に接続するには、Snowflake クライアント ID、認証 URL、アクセストークン URL、およびアクセストークンが必要です。

認証の詳細を取得するには、Snowflake で認証統合を作成し、Informatica リダイレクト URL をセキュリティ統合に登録する必要があります。セキュリティ統合とは、OAuth をサポートするクライアントがユーザーを認証ページにリダイレクトし、Snowflake にアクセスするためのアクセストークン、および必要に応じて更新トークンを生成できるようにする統合の一種です。

次の Informatica リダイレクト URL をセキュリティ統合に登録します：

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

アクセストークンが期限切れになると、顧客のファイアウォール外にある Informatica リダイレクト URL は、エンドポイントへの接続と新しいアクセストークンの取得を試みます。

セキュリティ統合を作成し、認証の詳細を取得する方法の詳細については、Snowflake のマニュアルの「[Create security integration](#)」を参照してください。

注： 詳細モードで設定されたマッピングでは、認証コード認証で設定された接続を使用することはできません。

キーペア

キーペア認証を使用して Snowflake に接続するには、Snowflake アカウントのユーザー名とともに、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のパスワードが必要です。

OpenSSL を使用してパブリックキーとプライベートキーのペアを生成します。キーペア認証方法には 2048 ビットの RSA キーペアが必要です。Snowflake にアクセスするには、接続プロパティでプライベートキーファイルへのパスおよびパスワードを指定します。

パブリックキーとプライベートキーの生成

キーペア認証用のパブリックキーとプライベートキーを生成するには、Snowflake でセキュリティ管理以上のロールが必要です。

1. Open SSL コマンドラインから、プライベートキーを生成します。

- 復号化されたプライベートキーを生成するには、次のコマンドを実行し、表示されたプロンプトに従ってパスフレーズを入力します。

```
$ openssl genrsa 2048 | openssl pkcs8 -topk8 -<cryptographic algorithm> -inform PEM -out rsa_key.p8 -nocrypt
```

- 暗号化されているプライベートキーを生成するには、次のコマンドを実行し、表示されたプロンプトに従ってパスフレーズを入力します。

```
$ openssl genrsa 2048 | openssl pkcs8 -topk8 -<cryptographic algorithm> -inform PEM -out rsa_key.p8
```

注: Snowflake のマニュアルを参照して、コマンドで推奨される暗号化アルゴリズムを使用してプライベートキーを生成します。

パスフレーズは、Snowflake への接続中に、プライベートキーファイルを暗号化するために使用されます。

2. パブリックキーを生成します。次のコマンドを実行し、ファイルにある rsa_key.p8 などの暗号化されたプライベートキーを指定します:

```
openssl rsa -in rsa_key.p8 -pubout -out rsa_key.pub
```

3. Secure Agent がアクセスできるディレクトリにパブリックおよびプライベートキーファイルをコピーします。

例: C:\Program Files\Informatica Cloud Secure Agent\apps\Data_Integration_Server\data\snowflake\rsa_key.p8

Snowflake 接続を設定するときにパスの詳細が必要になります。

4. Snowflake で、ALTER USER コマンドを使用してパブリックキーを Snowflake ユーザーに割り当てます。

```
alter user <user> set rsa_public_key='<content of the public key after removing the header and footer lines>';
```

例えば、alter user jsmith set rsa_public_key='MIIXBIjABCdef...';

Snowflake 用のキーペア認証の設定の詳細については、Snowflake のマニュアルを参照してください。

詳細クラスタでのプライベートキーの設定

OpenSSL を使用してパブリックキーとプライベートキーのペアを生成した後に、詳細モードのマッピングで接続が機能するように特定のタスクを追加で実行する必要があります。

詳細クラスタで設定した接続を使用してマッピングを実行する前に、マッピングタスクでクラスタアプリケーションのプロパティを設定します。

次のリストに、マッピングタスクの詳細セッションプロパティで設定する必要があるプロパティを示します。
Spark.NeedUserCredentialFileForAdapter=true

Spark.UserCredentialDirOnDIS に指定した場所のプライベートキーの内容を、Secure Agent マシンから Spark ドライブおよびエグゼキュータにコピーします。資格情報ファイルを含むフォルダには、1MB の制限はありません。クラスタアプリケーションにコピーするシークレットキーコンテンツの資格情報ファイ

ルは、1MB を超えないようにする必要があります。値を true に設定する必要があります。デフォルトは false です。

このフラグを設定していない場合、またはこのフラグを false に設定した場合、プライベートキーファイルはクラスタアプリケーションにコピーされず、マッピングは失敗します。

Spark.UserCredentialDirOnDIS=<プライベートキーファイルディレクトリ>

プライベートキーコンテンツをクラスタアプリケーションにコピーするために指定したディレクトリで、プライベートキーを含むデフォルトの Secure Agent ディレクトリをオーバーライドします。デフォルトのディレクトリは /infra/user/credentials です。ディレクトリにプライベートキーのファイル名が含まれていないことを確認します。

このフラグを設定しない場合は、デフォルトの場所が使用されます。デフォルトの場所を使用するには、/infra/user/credentials ディレクトリを Secure Agent マシンに作成し、そこにプライベートキーファイルをコピーします。

マッピングタスクの詳細セッションプロパティで指定した場所をオーバーライドするフラグを設定する場合、Spark.UserCredentialDirOnDIS に指定したオーバーライドの場所にプライベートキーファイルが含まれていることを確認します。オーバーライドの場所とプライベートキーファイルに書き込み権限があることを確認します。

次の画像に、マッピングタスクで設定された詳細カスタムプロパティを示します。

Advanced Session Properties	
Session Property Name	Session Property Value
advanced.custom.property	Spark.NeedUserCredentialFileForAdapter=true&Spark.UserCredentialDirOnDIS=/cdagent/privKey

クライアント資格情報

OAuth 2.0 クライアント資格情報を使用して Snowflake に接続するには、Snowflake クライアント ID、アクセストークン URL、クライアントシークレット、スコープ、およびアクセストークンが必要です。

クライアント資格情報付与タイプを使用して OAuth エンドポイントを設定し、次にセキュリティ統合を作成して認証の詳細を取得します。

クライアント資格情報認証を使用して Snowflake に接続する前に、組織の管理者は前提条件のタスクを実行する必要があります。

1. Snowflake で使用する OAuth と互換性のあるクライアントアプリケーションを作成します。
2. クライアント資格情報付与タイプを使用して認証サーバーを設定します。
3. Snowflake で OAuth タイプのセキュリティ統合を作成します。
セキュリティ統合を作成し、認証の詳細を取得する方法の詳細については、Snowflake のマニュアルの「[Create security integration for external OAuth](#)」を参照してください。

注: 詳細モードで設定されたマッピングでは、クライアント資格情報認証で設定された接続を使用することはできません。

Snowflake への接続

Snowflake に接続するための Snowflake Data Cloud 接続プロパティを設定してみましょう。

始める前に

開始する前に、設定する認証タイプに基づいて Snowflake アカウントから情報を取得する必要があります。

認証の前提条件の詳細については、「[「認証の準備」 \(ページ 845\)](#)」を参照してください。

接続の詳細

次の表に、基本接続プロパティを示します。

財産	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。
シークレットコンテナの使用	組織に対して設定されている Secrets Manager にこの接続の機密資格情報を保存します。 このプロパティは、組織に Secrets Manager が設定されている場合にのみ表示されます。 このプロパティは、データ取り込みおよびレプリケーションとデータアクセス管理サービスではサポートされていません。 接続でシークレットコンテナを有効にすると、Secure Agent が Secrets Manager からどの資格情報を取得するかを選択できます。このオプションを無効にした場合、資格情報は組織の設定方法に応じてリポジトリまたはローカル Secure Agent に保存されます。 注: この接続を使用してプッシュダウンまたはプロキシサービスを介してデータアクセスポリシーを適用する場合、シークレットコンテナ設定オプションを使用することはできません。 Secrets Manager を設定および使用する方法については、Administrator のヘルプにある「Secrets Manager の設定」を参照してください。
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。 Secure Agent、ホステッドエージェント、サーバーレスランタイム環境、またはエラスティックランタイム環境を選択します。 キーペア認証を使用してサーバーレス環境を設定する方法の詳細については、 「キーペア認証でのサーバーレスランタイム環境の使用」 (ページ 859) を参照してください。 詳細モードのマッピングで接続を使用する場合、または Snowflake に接続するためにキーペア認証を設定する場合は、ホステッドエージェントを使用しないでください。 アプリケーション取り込みとレプリケーションタスクとデータベース取り込みとレプリケーションタスクでは、Secure Agent またはサーバーレスランタイム環境を使用できます。ホステッドエージェントまたはエラスティックランタイム環境で、アプリケーション取り込みとレプリケーションタスク、データベース取り込みとレプリケーションタスク、またはストリーミング取り込みとレプリケーションタスクを実行することはできません。 ランタイム環境の設定および使用方法の詳細については、Administrator のヘルプにある「ランタイム環境」を参照してください。

認証タイプ

Snowflake にアクセスするための認証タイプ（標準、認証コード、キーペア、およびクライアント資格情報）を設定できます。

必要な認証方法を選択し、認証固有のパラメータを設定します。

標準認証

標準認証はデフォルトのタイプであり、標準認証の最小要件は、Snowflake アカウント名、ウェアハウス名、ユーザー名、およびアカウントパスワードまたはプログラムによるアクセストークン（PAT）のいずれかです。

次の表に、標準認証の基本的な接続プロパティに関する説明を示します。

プロパティ	説明
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/PAT	Snowflake アカウントに接続するためのパスワードまたはプログラムによるアクセストークン (PAT)。 Snowflake アカウントのパスワードまたは Snowflake によって付与された PAT を入力します。 注: データ取り込みおよびレプリケーションで PAT を使用することはできません。
アカウント	Snowflake アカウントの名前。 例えば、Snowflake の URL が https://<123abc>.us-east-2.aws.snowflakecomputing.com/console/login#/ の場合、アカウント名は URL の最初のセグメント (snowflakecomputing.com より前) です。ここでは、123abc.us-east-2.aws がアカウント名です。 Snowsight の URL を使用する場合、例えば https://app.snowflake.com/us-east-2.aws/<123abc>/dashboard では、アカウント名は 123abc.us-east-2.aws です。 注: アカウント名にアンダースコアが含まれていないことを確認します。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する必要があります。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。

詳細設定

次の表に、標準認証の詳細な接続プロパティに関する説明を示します。

プロパティ	説明
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。 複数の JDBC 接続パラメータをアンパサンド (&) で区切って、次の形式で指定できます。 <code><param1>=<value>&<param2>=<value>&<param3>=<value>...</code> 例えば、Snowflake に接続するときに次のデータベースとスキーマの値を渡すことができます。 <code>db=mydb&schema=public</code> パラメータを追加するときは、等号 (=) の前後にスペースを加えないようにしてください。 設定可能な追加の JDBC パラメータのリストについては、「 「JDBC URL パラメータ」 (ページ 856) 」を参照してください。

認証コードの認証

OAuth 2.0 認証では、Snowflake に接続するために、認証コード付与タイプを備えた OAuth 2.0 プロトコルが必要です。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することなく、Snowflake への認証されたアクセスが可能になります。

次の表に、OAuth 2.0 認証コードの認証の基本的な接続プロパティに関する説明を示します。

プロパティ	説明
アカウント	<p>Snowflake アカウントの名前。</p> <p>例えば、Snowflake の URL が <code>https://<123abc>.us-east-2.aws.snowflakecomputing.com/console/login#</code>/ の場合、アカウント名は URL の最初のセグメント (<code>snowflakecomputing.com</code> より前) です。ここでは、<code>123abc.us-east-2.aws</code> がアカウント名です。</p> <p>Snowsight の URL を使用する場合、例えば <code>https://app.snowflake.com/us-east-2.aws/<123abc>/dashboard</code> では、アカウント名は <code>123abc.us-east-2.aws</code> です。</p> <p>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。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する必要があります。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。</p>
ウェアハウス	<p>Snowflake ウェアハウス名。</p>
認証 URL	<p>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。</p> <p>認証 URL は、<code>https://<アカウント名>.snowflakecomputing.com/oauth/authorize</code> です。この <code><アカウント名></code> 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。</p> <p>例: <code>https://<abc>.snowflakecomputing.com/oauth/authorize</code></p> <p>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。</p> <p>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。</p>
アクセストークン URL	<p>認証コードを交換するために使用され、アクセストークンを取得する、Snowflake アクセストークンのエンドポイント。</p> <p>アクセストークンの URL は、<code>https://<アカウント名>.snowflakecomputing.com/oauth/token-request</code> です。この <code><アカウント名></code> 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。</p> <p>例: <code>https://<abc>.snowflakecomputing.com/oauth/token-request</code></p> <p>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。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する必要があります。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。</p>
クライアント ID	<p>Snowflake で OAuth タイプのセキュリティ統合を作成するときに生成されるアプリケーションのクライアント ID。</p>

プロパティ	説明
クライアントシークレット	クライアント ID に対して生成されたクライアントシークレット。
アクセストークン	アクセストークンの値。 OAuth エンドポイントから取得して取り込んだアクセストークン値を入力するか、 [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値を入力します。

詳細設定

次の表に、OAuth 2.0 認証コードの認証の詳細接続プロパティに関する説明を示します。

プロパティ	説明
追加の JDBC URL パラメータ	<p>追加の JDBC 接続パラメータ。 複数の JDBC 接続パラメータをアンパサンド (&) で区切って、次の形式で指定できます。</p> <pre><param1>=<value>&<param2>=<value>&<param3>=<value>...</pre> <p>例えば、Snowflake に接続するときに次のデータベースとスキーマの値を渡すことができます。</p> <pre>db=mydb&schema=public</pre> <p>パラメータを追加するときは、等号 (=) の前後にスペースを加えないようにしてください。 設定可能な追加の JDBC パラメータのリストについては、「JDBC URL パラメータ」 (ページ 856) を参照してください。</p>
スコープ	<p>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。</p> <p>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、<code>session:role:CQA_GCP</code> 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。</p> <p>複数のスコープ属性を入力するには、それぞれのスコープ属性をスペースで区切って指定します。</p>
アクセストークンパラメータ	<p>アクセストークン URL で使用する追加パラメータ。 アクセストークンのパラメータを次の JSON 形式で定義します:</p> <pre>[{"Name": "<パラメータ名>", "Value": "<パラメータ値>"}]</pre> <p>例えば、Snowflake に接続するときに次の <code>code_verifier</code> パラメータを使用できます:</p> <pre>[{"Name": "code_verifier", "Value": "5PMddu6Zcg6Tc4sbg"}]</pre> <p>定義できるアクセストークンパラメータの詳細については、Snowflake のマニュアルの 「Introduction to OAuth」 を参照してください。</p>

プロパティ	説明
認証コードパラメータ	<p>認証トークン URL で使用する追加パラメータ。 複数のパラメータをコンマで区切って、次の JSON 形式で定義します:</p> <pre>[{"Name": "<パラメータ名>", "Value": "<パラメータ値>"}, {"Name": "<パラメータ名>", "Value": "<パラメータ値>"}]</pre> <p>例えば、Snowflake に接続するときに、次の code_challenge および code_challenge_method パラメータを使用できます:</p> <pre>[{"Name": "code_challenge", "Value": "Ikr-vv52th0UeVRi4"}, {"Name": "code_challenge_method", "Value": "S256"}]</pre>
更新トークン	<p>更新トークンの値。 OAuth エンドポイントから取得して取り込んだ更新トークン値を入力するか、【アクセストークンの生成】をクリックして更新トークン値を入力します。アクセストークンが有効ではない場合または有効期限が切れている場合、Secure Agent は、更新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、有効なり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します。</p>

キーペア認証

キーペア認証には、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のパスワード、および Snowflake に接続するための Snowflake アカウントのユーザー名が必要です。

Snowflake に接続するようにキーペア認証を設定する場合は、ランタイム環境としてホステッドエージェントを使用しないでください。

次の表に、キーペア認証の基本的な接続プロパティに関する説明を示します。

プロパティ	説明
ユーザー名	Snowflake アカウントに接続するためのユーザー名。
アカウント	<p>Snowflake アカウントの名前。 例えば、Snowflake の URL が https://<123abc>.us-east-2.aws.snowflakecomputing.com/console/login#/ の場合、アカウント名は URL の最初のセグメント (snowflakecomputing.com より前) です。ここでは、123abc.us-east-2.aws がアカウント名です。 Snowsight の URL を使用する場合、例えば https://app.snowflake.com/us-east-2.aws/<123abc>/dashboard では、アカウント名は 123abc.us-east-2.aws です。 注: アカウント名にアンダースコアが含まれていないことを確認します。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する必要があります。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。</p>

プロパティ	説明
ウェアハウス	Snowflake ウェアハウス名。
プライベートキーファイル	<p>プライベートキーファイル名を含む、Secure Agent が Snowflake にアクセスするために使用するプライベートキーファイルへのパス。</p> <p>例えば、Secure Agent マシンで次のパスとキーファイル名を指定します:</p> <ul style="list-style-type: none"> - Windows の場合: C:\Users\path_to_key_file\rsa_key.p8 - Linux の場合: /export/home/user/path_to_key_file/rsa_key.p8 <p>サーバーレスランタイム環境を使用するには、サーバーレスエージェントディレクトリで次のパスとキーファイル名を指定します:</p> <p>/home/cldagnt/SystemAgent/serverless/configurations/ssl_store/<Private key file name></p> <p>サーバーレス環境の使用方法の詳細については、「キーペア認証でのサーバーレスランタイム環境の使用」(ページ 859)を参照してください。</p> <p>注: キーストアが FIPS 認証されていることを確認します。</p>

詳細設定

次の表に、キーペア認証の詳細な接続プロパティに関する説明を示します。

プロパティ	説明
追加の JDBC URL パラメータ	<p>追加の JDBC 接続パラメータ。</p> <p>複数の JDBC 接続パラメータをアンパサンド (&) で区切って、次の形式で指定できます。</p> <pre><param1>=<value>&<param2>=<value>&<param3>=<value>....</pre> <p>例えば、Snowflake に接続するときに次のデータベースとスキーマの値を渡すことができます。</p> <pre>db=mydb&schema=public</pre> <p>パラメータを追加するときは、等号 (=) の前後にスペースを加えないようにしてください。</p> <p>設定可能な追加の JDBC パラメータのリストについては、「「JDBC URL パラメータ」 (ページ 856)」を参照してください。</p>
プライベートキーファイルのパスワード	プライベートキーファイルのパスワード。

クライアント資格情報認証

OAuth 2.0 クライアント資格情報認証には、少なくともクライアント ID、アクセストークン URL、クライアントシークレット、スコープ、およびアクセストークンが必要です。

次の表に、OAuth 2.0 クライアント資格情報認証の基本的な接続プロパティに関する説明を示します。

プロパティ	説明
アカウント	<p>Snowflake アカウントの名前。</p> <p>例えば、Snowflake の URL が <code>https://<123abc>.us-east-2.aws.snowflakecomputing.com/console/login#</code> / である場合、URL の最初のセグメント (<code>snowflakecomputing.com</code> より前) がアカウント名です。ここでは、<code>123abc.us-east-2.aws</code> がアカウント名です。</p> <p>Snowsight の URL を使用する場合、例えば <code>https://app.snowflake.com/us-east-2.aws/<123abc>/dashboard</code> では、アカウント名は <code>123abc.us-east-2.aws</code> です。</p> <p>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。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する必要があります。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。</p>
ウェアハウス	Snowflake ウェアハウス名。
アクセストークン URL	<p>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。</p> <p>OAuth エンドポイントから取得したアクセストークン URL を指定します。</p>
クライアント ID	アプリケーションを OAuth 用に設定したときに生成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	クライアント ID に対して生成されたクライアントシークレット。
スコープ	<p>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。</p> <p>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、<code>session:role:CQA_GCP</code> 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。</p> <p>複数のスコープ属性を入力するには、それぞれのスコープ属性をスペースで区切って指定します。</p>
アクセストークン	<p>アクセストークンの値。</p> <p>OAuth エンドポイントから取得して取り込んだアクセストークン値を入力するか、[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値を入力します。</p>

詳細設定

次の表に、OAuth 2.0 クライアント資格情報認証の詳細接続プロパティに関する説明を示します。

プロパティ	説明
追加の JDBC URL パラメータ	<p>追加の JDBC 接続パラメータ。 複数の JDBC 接続パラメータをアンパサンド (&) で区切って、次の形式で指定できます。</p> <pre><param1>=<value>&<param2>=<value>&<param3>=<value>...</pre> <p>例えば、Snowflake に接続するときに次のデータベースとスキーマの値を渡すことができます。</p> <pre>db=mydb&schema=public</pre> <p>パラメータを追加するときは、等号 (=) の前後にスペースを加えないようにしてください。 設定可能な追加の JDBC パラメータのリストについては、「JDBC URL パラメータ」(ページ 856)を参照してください。</p>
アクセストークンパラメータ	<p>アクセストークン URL で使用する追加パラメータ。 アクセストークンのパラメータを次の JSON 形式で定義します:</p> <pre>[{"Name": "<パラメータ名>", "Value": "<パラメータ値>"}]</pre> <p>例えば、Snowflake に接続するときに次の code_verifier パラメータを使用できます:</p> <pre>[{"Name": "code_verifier", "Value": "5PMddu6Zcg6Tc4sbg"}]</pre> <p>定義できるアクセストークンパラメータの詳細については、Snowflake のマニュアルの「Introduction to OAuth」を参照してください。</p>

JDBC URL パラメータ

Snowflake Data Cloud 接続の追加の JDBC URL パラメータフィールドを使用して、Snowflake に接続するときに追加パラメータをカスタマイズおよび設定できます。

Snowflake ウェアハウス、データベース、スキーマ、テーブル、およびストレージ統合の名前では、大文字と小文字が区別されます。追加の JDBC パラメータフィールドでプロパティを定義する場合は、この点を必ず考慮してください。

Snowflake Data Cloud 接続の追加の JDBC URL パラメータでは、次のようなプロパティを設定できます。

- Snowflake で一時テーブルを作成するために使用されるデータベースとスキーマ名をオーバーライドするには、次の形式でデータベース名とスキーマ名を入力します。

```
ProcessConnDB=<DB name>&ProcessConnSchema=<Schema name>
```
- Snowflake テーブルのインポート中に指定したデータベースおよびスキーマのみを表示するには、次の形式でデータベースおよびスキーマ名を入力します。

```
db=<Database name>&schema=<Schema name>
```
- Snowflake から UDF 文字列と数値データを読み取るには、Snowflake で UDF が作成されたデータベースとスキーマを次の形式で入力します。

```
db=<Database name>&schema=<Schema name>
```

- Okta SSO 認証を介して Snowflake にアクセスするには、次の形式で SAML 2.0 プロトコルを実装する Web ベースの IdP を入力します。

authenticator=https://<Your Okta account name>.okta.com

注: Microsoft ADFS は使用できません。

Okta 認証の設定の詳細については、「[Configuring Snowflake to use federated authentication](#)」を参照してください。

- SQL ELT の最適化のために Amazon S3、Google Cloud Storage、または Microsoft Azure Data Lake Storage Gen2 から Snowflake にデータをロードするには、Snowflake の Amazon S3、Google Cloud Storage、または Microsoft Azure Data Lake Storage Gen2 アカウント用に作成されたクラウドストレージ統合名を次の形式で入力します。

storage_integration=<Storage Integration name>

ストレージ統合の名前は大文字と小文字が区別されます。例えば、Snowflake で Amazon S3、Google Cloud Storage、または Microsoft Azure Data Lake Storage Gen2 用に作成したストレージ統合の名前が *STORAGE_INT* である場合は、次のように同じ統合名を指定する必要があります。

storage_integration=STORAGE_INT

注: また、ストレージ統合を使用せずに、Amazon S3 から Snowflake にデータをロードして、SQL ELT を最適化することもできます。

- プロキシサーバーを使用して Snowflake に接続するには、次のパラメータを入力します。

```
useProxy=true&
proxyHost=<Proxy host IP address>&
proxyPort=<Proxy server port number>&
proxyUser=<Proxy server user name>&
proxyPassword=<Proxy server password>
```

- テーブル内の二重引用符を無視し、大文字と小文字を区別しないものとしてすべてのテーブルを処理するには、次のパラメータを入力します。

QUOTED_IDENTIFIERS_IGNORE_CASE=true

接続のこのプロパティを true に設定すると、Snowflake はテーブル内の二重引用符を無視し、大文字と小文字を区別しないものとしてすべてのテーブルを処理します。

このプロパティを true に設定した場合、大文字と小文字が区別されるテーブルに同じ接続でアクセスすることはできません。大文字と小文字が区別される既存のテーブルを取得するには、新しい接続を作成する必要があります。

- Snowflake ウェブインタフェースの Snowflake ジョブで実行されるクエリをフィルタリングするには、タグ名を次の形式で入力します:

query_tag=<Tag name>

マッピングタスクの実行時に、Snowflake 接続で定義されている query_tag パラメータをオーバーライドするというオプションがあります。

query_tag パラメータをオーバーライドするには、マッピングタスクの **【ランタイムオプション】** タブをクリックします。**【詳細セッションプロパティ】** セクションで、**【セッションプロパティ名】** リストから **【カスタムプロパティ】** を選択し、次の値を入力します:

snowflake_query_tag=<Tag name>

注: 詳細モードでは、query_tag パラメータをオーバーライドすることはできません。

- Secure Agent が、書き込み操作に対する *INFA_DTM_STAGING_ENABLED_CONNECTORS* ステージングプロパティを使用して設定されている場合、Snowflake ターゲットにマイクロ秒またはナノ秒の精度で TIMESTAMPNTZ データ型のデータを書き込むには、次のパラメータとそれに対応する値を入力します。

- マイクロ秒の精度の場合は、次の値を入力します。

DTM_STAGING_TIMESTAMPNTZ_FORMAT=YYYY-MM-DD HH24:MI:SS.US

- ナノ秒の精度の場合は、次の値を入力します。

DTM_STAGING_TIMESTAMPNTZ_FORMAT=YYYY-MM-DD HH24:MI:SS.NS

このパラメータは、詳細モードのマッピングには適用されません。

- 精度の最大値が 104,857,600 である VARCHAR データ型のデータの読み取りまたは書き込みを行うには、次のパラメータを入力します。

VARCHAR_MAX_PRECISION=true

精度の最大値を 104,857,600 に増やすと、場合によっては Java ヒープ領域メモリを増やす必要があります。

Java ヒープ領域メモリを増やす方法の詳細については、ナレッジベースの記事

「[Increase Java heap size](#)」を参照してください。

リストされているパラメータに加えて、このフィールドでは、要件に基づいて他の Snowflake パラメータを柔軟に設定することができます。

外部 OAuth 認証用の Microsoft Azure Active Directory

Microsoft Azure Active Directory を外部 OAuth 認証サーバーとして使用して、Snowflake を認証できます。

Microsoft Azure Active Directory を外部 OAuth 認証サーバーとして使用するには、**【認証コード】** を接続プロパティの認証タイプとして設定します。Microsoft Azure Active Directory OAuth 認証サーバーから、アカウント名、ウェアハウス、認証 URL、アクセストークン URL、クライアント ID、クライアントシークレット、アクセストークン、およびスコープの詳細を指定します。

Microsoft Azure Active Directory OAuth 認証サーバーを設定する場合は、Snowflake のマニュアルの

「[Configure Microsoft Entra ID for external OAuth](#)」を参照してください。

プロキシサーバーの設定

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

Windows および Linux でプロキシサーバーを使用するように Secure Agent を設定できます。認証されていないプロキシサーバーまたは認証されたプロキシサーバーを使用できます。マッピングおよび詳細モードのマッピングで使用される接続に対してプロキシを設定できます。

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

- Windows の場合は Secure Agent Manager を使用し、Linux の場合はシェルコマンドを使用して Secure Agent を設定します。
手順については、データ統合のヘルプの『または「Windows でのプロキシ設定」または「Linux でのプロキシ設定」を参照してください。
- Secure Agent のプロパティで、DTM の JVM オプションを設定します。手順については、ナレッジベースの記事「[Proxy server settings](#)」を参照してください。
- Snowflake 接続の追加の JDBC URL パラメータで、プロキシサーバーのプロパティを設定します。詳細については、「[Set JDBC URL Parameters](#)」を参照してください。

サーバーレスランタイム環境のプロキシの設定を行う方法については、Administrator ヘルプの「[「プロキシサーバーの使用」](#)を参照してください。

Snowflake にアクセスするためのプライベートリンク

AWS または Azure プライベートリンクエンドポイントを使用して Snowflake にアクセスできます。

Snowflake Data Cloud 接続の作成時に、接続プロパティの【**アカウント**】フィールドに Snowflake プライベートリンクアカウント名を指定します。

AWS または Azure プライベートリンクの設定によって、Snowflake への接続が AWS または Azure 内部ネットワークを使用して確立され、パブリックインターネットを介した接続が行われなくなります。

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

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

キーペア認証でのサーバーレスランタイム環境の使用

AWS または Azure でホストされているサーバーレスランタイム環境を使用して、キーペア認証を使用して Snowflake に接続できます。

注: データ取り込みとレプリケーションでは、サーバーレス環境を使用することはできません。

サーバーレスランタイム環境を使用して Snowflake 接続を設定する前に、次のタスクを実行します。

- AWS または Azure アカウントの Amazon S3 バケットあるいは Azure コンテナにプライベートキーファイルのパスとファイル名を追加します。
- .yaml サーバーレス構成ファイルを設定する。
- Snowflake に接続するための接続プロパティを設定します。

AWS アカウントまたは Azure アカウントの Amazon S3 バケットあるいは Azure コンテナにプライベートキーファイルのパスとファイル名を追加します

サーバーレスランタイム環境で Snowflake 接続を設定するには、次の手順を実行します。

1. AWS または Azure のサーバーレスエージェント設定用に次の構造を作成します: <補足ファイルの場所>/serverless_agent_config
2. AWS アカウントまたは Azure アカウントの次の場所にある Amazon S3 バケットあるいは Azure コンテナに、プライベートキーファイル名を含むプライベートキーファイルへのパスを追加します: <補足ファイルの場所>/serverless_agent_config/SSL

.yaml サーバーレス構成ファイルを設定する

サーバーレスランタイム環境で.yaml サーバーレス構成ファイルを設定し、プライベートキーファイルのパスとファイル名のエントリをサーバーレスエージェントディレクトリにコピーするには、次のステップを実行します。

1. 次のコードスニペットをテキストエディタにコピーします。

```
version: 1
agent:
  agentAutoApply:
    general:
      sslStore:
        - fileCopy:
            sourcePath: SSL/<Private key file name>
```

ここで、ソースパスは、AWS または Azure のプライベートキーファイルのディレクトリパスです。

2. 構文とインデントが有効であることを確認してから、ファイルを `serverlessUserAgentConfig.yaml` として次の AWS または Azure の場所に保存します: <補足ファイルの場所>/`serverless_agent_config.yaml` ファイルの実行時に、プライベートキーファイルが AWS または Azure の場所からサーバーレスエージェントディレクトリにコピーされます。

Snowflake に接続するための接続プロパティの設定

Snowflake Data Cloud 接続の **【プライベートキーファイル】** フィールドに、プライベートキーファイル名を含むプライベートキーファイルへのパスを指定します。

例: `/home/cldagnt/SystemAgent/serverless/configurations/ssl_store/<プライベートキーファイル名>`

サーバーレス環境の設定および使用方法の詳細については、Administrator のヘルプにある「ランタイム環境」の「サーバーレスランタイム環境のセットアップ」を参照してください。

第 215 章

Strategy Cloud 接続のプロパティ

Strategy 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。

Strategy Cloud への接続

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

始める前に

接続を設定する前に、Strategy Cloud アカウントからユーザー名、パスワード、ベース URL を取得する必要があります。

接続の詳細

次の表に、Strategy Cloud 接続のプロパティを示します。

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

プロパティ	説明
Use Secret Use Secret VaultMCC_STRATEGYCLOUD_CONN- USE_SECRET_VAULT を使用します	<p>組織に対して設定されている Secrets Manager にこの接続の機密資格情報を保存します。</p> <p>このプロパティは、組織に Secrets Manager が設定されている場合にのみ表示されます。</p> <p>このプロパティは、データ取り込みおよびレプリケーションとデータアクセス管理サービスではサポートされていません。</p> <p>接続でシークレットコンテナを有効にすると、Secure Agent が Secrets Manager からどの資格情報を取得するかを選択できます。このオプションを無効にした場合、資格情報は組織の設定方法に応じてリポジトリまたはローカル Secure Agent に保存されます。</p> <p>注: この接続を使用してプッシュダウンまたはプロキシサービスを介してデータアクセスポリシーを適用する場合、シークレットコンテナ設定オプションを使用することはできません。</p> <p>Secrets Manager を設定および使用する方法については、Administrator のヘルプにある「Secrets Manager の設定」を参照してください。</p>
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選択します。
ベース URL	<p>Strategy Cloud インスタンスのベース URL。</p> <p>Strategy Cloud インスタンスが mycompany.cloud.microstrategy.com でホストされている場合のベース URL の例: https://mycompany.cloud.microstrategy.com/MicroStrategyLibrary</p>
ユーザー名	Strategy Cloud アカウントのユーザー名。
パスワード	Strategy Cloud アカウントのパスワード。

第 216 章

Stripe 接続のプロパティ

Stripe からデータの読み取りを行うための Stripe 接続を作成します。

Stripe への接続

Stripe からデータを読み取るように Stripe 接続を設定してみましょう。

始める前に

接続プロパティを設定する前に、Stripe アカウントからアカウント ID とシークレットキーを取得する必要があります。

次のビデオは、必要な情報を取得する方法を示しています。



接続の詳細

次の表に、基本接続プロパティを示します。

財産	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。

財産	説明
シークレットコンテナの使用	<p>組織に対して設定されている Secrets Manager にこの接続の機密資格情報を保存します。このプロパティは、組織に Secrets Manager が設定されている場合にのみ表示されます。このプロパティは、データ取り込みおよびレプリケーションとデータアクセス管理サービスではサポートされていません。</p> <p>接続でシークレットコンテナを有効にすると、Secure Agent が Secrets Manager からどの資格情報を取得するかを選択できます。このオプションを無効にした場合、資格情報は組織の設定方法に応じてリポジトリまたはローカル Secure Agent に保存されます。</p> <p>注: この接続を使用してプッシュダウンまたはプロキシサービスを介してデータアクセスポリシーを適用する場合、シークレットコンテナ設定オプションを使用することはできません。</p> <p>Secrets Manager を設定および使用方法については、Administrator のヘルプにある「Secrets Manager の設定」を参照してください。</p>
ランタイム環境	<p>タスクを実行するランタイム環境の名前。</p> <p>Secure Agent またはホステッドエージェントを指定します。</p> <p>ランタイム環境の設定および使用方法の詳細については、Administrator のヘルプにある「ランタイム環境」を参照してください。</p>
アカウント ID	Stripe アカウントの ID。
秘密鍵	アクセスを認証し、Stripe サーバーで API への要求を行うためのシークレットキー。

第 217 章

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。 <code>https://<rooturl>/learning/odatav4/<webservicename>/v1/</code> 例えば、ルート URL が <code>partner0370.scdemo.successfactors.com:443</code> で、Web サービス名が <code>curriculum</code> の場合、次のように URL を入力します。 <code>https://partner0370.scdemo.successfactors.com:443/learning/odatav4/curriculum/v1/</code> Web サービス名については、 <i>SuccessFactors Learning Web Services OData API リファレンスガイド</i> 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。

プロパティ	説明
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	<p>Web サービスを実行するユーザーアカウントのタイプ。</p> <p>次のいずれかの値を選択します。</p> <ul style="list-style-type: none"> - 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。

第 218 章

SuccessFactors ODATA 接続プロパティ

SuccessFactors ODATA 接続を作成して SuccessFactors に接続すると、Secure Agent が SuccessFactors に対してデータの読み取りおよび書き込みを実行できるようになります。SuccessFactors ODATA 接続を使用して、マッピング、同期タスク、またはマッピングタスクのソースとターゲットを指定できます。

SuccessFactors への接続

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

始める前に

接続プロパティを設定する前に、SAP SuccessFactors アカウントの企業 ID、ユーザー名、およびサービス URL が必要になります。

HTTP 基本認証を使用するには、SuccessFactors のユーザー名とパスワードが必要です。

OAuth 2 認証を使用するには、OData API へのアクセスが許可されている OAuth 2.0 クライアントアプリケーションを登録し、クライアントアプリケーションおよびプライベートキーに関連付けられている API を取得する必要があります。

次のビデオでは、SAP SuccessFactors アカウントから企業 ID、ユーザー名、およびサービス URL を取得する方法を紹介しています。



接続の詳細

次の表に、基本接続プロパティを示します。

プロパティ	説明
接続名	接続の名前。 各接続名は組織内で一意である必要があります。接続名には、英数字、スペース、および次の特殊文字を含めることができます。_ . + - , 最大長は 255 文字です。
説明	接続の説明。最大長は 4000 文字です。
シークレットコンテナの使用	組織に対して設定されている Secrets Manager にこの接続の機密資格情報を保存します。 このプロパティは、組織に Secrets Manager が設定されている場合にのみ表示されます。 このプロパティは、データ取り込みおよびレプリケーションとデータアクセス管理サービスではサポートされていません。 接続でシークレットコンテナを有効にすると、Secure Agent が Secrets Manager からどの資格情報を取得するかを選択できます。このオプションを無効にした場合、資格情報は組織の設定方法に応じてリポジトリまたはローカル Secure Agent に保存されます。 注: この接続を使用してプッシュダウンまたはプロキシサービスを介してデータアクセスポリシーを適用する場合、シークレットコンテナ設定オプションを使用することはできません。 Secrets Manager を設定および使用方法については、Administrator のヘルプにある「Secrets Manager の設定」を参照してください。
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。 Secure Agent、サーバーレスランタイム環境、またはエラスティックランタイム環境を選択します。 ランタイム環境の設定および使用方法の詳細については、Administrator のヘルプにある「ランタイム環境」を参照してください。
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。 ユーザー名では、SuccessFactors OData アカウントの企業 ID とユーザー名の組み合わせを次の形式で使します: ユーザー名@企業 ID
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。

詳細設定

次の表に、詳細接続のプロパティを示します。

プロパティ	説明
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。
トラスト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	SuccessFactors ODATA アカウントへのアクセスを認証する方法 次のいずれかの認証タイプを選択します。 <ul style="list-style-type: none">- 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。OData API へのアクセスが許可されている OAuth 2.0 クライアントアプリケーションと、クライアントアプリケーションに関連付けられている有効な OAuth トークンを登録する必要があります。
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 キーの取得方法の詳細については、SuccessFactors のドキュメント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取得方法の詳細については、SuccessFactors のドキュメントを参照してください。
会社 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。

プロキシサーバーの設定

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

Windows および Linux でプロキシサーバーを使用するように Secure Agent を設定できます。認証されていないプロキシサーバーのみを使用できます。プロキシ設定は、マッピングおよび詳細モードのマッピングで使用される接続に適用されます。

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

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

手順については、データ統合のヘルプの『または「Windows でのプロキシ設定」または「Linux でのプロキシ設定」を参照してください。

- Secure Agent のプロパティで、DTM の JVM オプションを設定します。手順については、ナレッジベースの記事「[Proxy server settings](#)」を参照してください。

サーバーレスランタイム環境のプロキシの設定を行う方法については、Administrator ヘルプの「「プロキシサーバーの使用」を参照してください。

第 219 章

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。

重要: SuccessFactors SOAP コネクタは非推奨となり、メンテナンスモードに移行されました。Informatica は将来のリリースでサポートを廃止する予定です。SuccessFactors ODATA コネクタを使用して SuccessFactors にアクセスすることをお勧めします。

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、ホステッドエージェント、サーバーレスランタイム環境、またはエラスティックランタイム環境を選択します。 ランタイム環境の設定および使用方法の詳細については、Administrator のヘルプにある「ランタイム環境」を参照してください。
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。

第 220 章

SurveyMonkey 接続のプロパティ

SurveyMonkey 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、SurveyMonkey 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。
シークレットコンテナの使用	組織に対して設定されている Secrets Manager にこの接続の機密資格情報を保存します。 このプロパティは、組織に Secrets Manager が設定されている場合にのみ表示されます。 このプロパティは、データ取り込みおよびレプリケーションとデータアクセス管理サービスではサポートされていません。 接続でシークレットコンテナを有効にすると、Secure Agent が Secrets Manager からどの資格情報を取得するかを選択できます。このオプションを無効にした場合、資格情報は組織の設定方法に応じてリポジトリまたはローカル Secure Agent に保存されます。 注: この接続を使用してプッシュダウンまたはプロキシサービスを介してデータアクセスポリシーを適用する場合、シークレットコンテナ設定オプションを使用することはできません。 Secrets Manager を設定および使用する方法については、Administrator のヘルプにある「Secrets Manager の設定」を参照してください。
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。 Secure Agent、ホステッドエージェント、またはエラスティックランタイム環境を選択します。 ランタイム環境の設定および使用方法の詳細については、Administrator のヘルプにある「ランタイム環境」を参照してください。
認証	SurveyMonkey コネクタが SurveyMonkey へのログインに使用する必要のある認証方法。 デフォルトは AuthorizationCode です。
認証 URL	認証コードを取得する認証サーバーエンドポイント。 認証 URL は https://api.surveymonkey.com/oauth/authorize です。
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される SurveyMonkey のアクセストークン URL。 アクセストークン URL は https://api.surveymonkey.com/oauth/token です。

接続プロパティ	説明
クライアント ID	アプリケーション登録プロセス中にクライアント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クライアントに発行されるクライアントシークレットキー。
スコープ	アクセス要求のスコープ。
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。
認証コードパラメータ	認証 URL で使用する追加パラメータ。
アクセストークン	<p>データにアクセスするための、SurveyMonkey によって付与されるアクセストークン。取り込まれたアクセストークンを入力するか、[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取り込みます。</p> <p>注: SurveyMonkey によって付与されたアクセストークンには有効期限がありません。アクセストークンの詳細については、SurveyMonkey のマニュアルを参照してください。</p>
更新トークン	該当なし。

第 221 章

Tableau V2 接続のプロパティ

Tableau 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、Tableau 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。
シークレットコンテナの使用	組織に対して設定されている Secrets Manager にこの接続の機密資格情報を保存します。 このプロパティは、組織に Secrets Manager が設定されている場合にのみ表示されます。 このプロパティは、データ取り込みおよびレプリケーションとデータアクセス管理サービスではサポートされていません。 接続でシークレットコンテナを有効にすると、Secure Agent が Secrets Manager からどの資格情報を取得するかを選択できます。このオプションを無効にした場合、資格情報は組織の設定方法に応じてリポジトリまたはローカル Secure Agent に保存されます。 注: この接続を使用してプッシュダウンまたはプロキシサービスを介してデータアクセスポリシーを適用する場合、シークレットコンテナ設定オプションを使用することはできません。 Secrets Manager を設定および使用する方法については、Administrator のヘルプにある「Secrets Manager の設定」を参照してください。
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。 Secure Agent 環境またはエラスティックランタイム環境を選択します。 ランタイム環境の設定および使用方法の詳細については、Administrator のヘルプにある「ランタイム環境」を参照してください。
Tableau 製品	接続する Tableau 製品の名前。 TDE 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 TDE ファイルを作成します。作成した TDE ファイルを Tableau デスクトップに手動でインポートできます。 - Tableau サーバー。生成した TDE 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 TDE ファイルを Tableau Online にパブリッシュします。

接続プロパティ	説明
接続 URL	TDE ファイルをパブリッシュする 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>
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。
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。
コンテンツ URL	TDE ファイルをパブリッシュする Tableau サーバーまたは Tableau Online 上のサイトの名前。 サイト名を入力するには Tableau 管理者にお問い合わせください。
テンプレートファイルのパス	Secure Agent による Tableau メタデータのインポート元のサンプル TDE ファイルへのパス。 テンプレート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。 <ul style="list-style-type: none"> - TDE ファイルへの絶対パス。 - TDE ファイルのディレクトリパス。 - 空のディレクトリパス。 テンプレートファイル用に指定するパスは、ターゲット TDE ファイルのデフォルトパスになります。 注: 【Tableau 製品】 接続プロパティの値として 【Tableau Desktop】 を選択する場合は、テンプレートファイルパスに少なくとも 1 つの .tde ファイルがあることを確認してください。 ファイルパスを指定しない場合、Secure Agent は、ターゲット TDE ファイルの次のデフォルトファイルパスを使用します: <Secure Agent インストールディレクトリ>/apps/Data_Integration_Server/<最新バージョン>/bin/rtdm。

第 222 章

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
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。
シークレットコンテナの使用	組織に対して設定されている Secrets Manager にこの接続の機密資格情報を保存します。 このプロパティは、組織に Secrets Manager が設定されている場合にのみ表示されます。 このプロパティは、データ取り込みおよびレプリケーションとデータアクセス管理サービスではサポートされていません。 接続でシークレットコンテナを有効にすると、Secure Agent が Secrets Manager からどの資格情報を取得するかを選択できます。このオプションを無効にした場合、資格情報は組織の設定方法に応じてリポジトリまたはローカル Secure Agent に保存されます。 注: この接続を使用してプッシュダウンまたはプロキシサービスを介してデータアクセスポリシーを適用する場合、シークレットコンテナ設定オプションを使用することはできません。 Secrets Manager を設定および使用する方法については、Administrator のヘルプにある「Secrets Manager の設定」を参照してください。
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。 Secure Agent 環境またはエラスティックランタイム環境を選択します。 ランタイム環境の設定および使用方法の詳細については、Administrator のヘルプにある「ランタイム環境」を参照してください。

接続プロパティ	説明
Tableau 製品	<p>接続する Tableau 製品の名前。</p> <p>.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。</p> <p>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。</p> <p>Tableau Server。</p> <p>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。</p> <p>Tableau Online。</p> <p>生成した .hyper ファイルを Tableau Cloud にパブリッシュします。</p>
認証方法	<p>Tableau Server または Tableau Cloud に接続するための認証方法。</p> <p>次のいずれかの方法を選択します。</p> <ul style="list-style-type: none"> - ユーザー名とパスワード。 Tableau アカウントのユーザー名とパスワードを使用して Tableau Server または Tableau Cloud に接続します。 - パーソナルアクセストークン。 Tableau アカウントのパーソナルアクセストークンとトークンシークレットを使用して、Tableau Server または Tableau Cloud に接続します。
接続 URL	<p>データ抽出ファイルをパブリッシュする Tableau Server または Tableau Cloud の URL。</p> <p>URL の形式は次のとおりです。</p> <p><code>http://<Host name of Tableau Server or Tableau Cloud>:<port></code></p>
ユーザー名	Tableau Server または Tableau Cloud アカウントのユーザー名。
パスワード	Tableau Server または Tableau Cloud アカウントのパスワード。
パーソナルアクセストークン名	Tableau Server または Tableau Cloud アカウントに接続するためのパーソナルアクセストークン。
トークンシークレット	Tableau Server または Tableau Cloud アカウントに接続するためのパーソナルアクセストークンに関連付けられたトークンシークレット。

接続プロパティ	説明
サイト ID	<p>データ抽出ファイルをパブリッシュする Tableau Server または Tableau Cloud の特定サイトを指すサイト名。</p> <p>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。</p>
スキーマファイルのパス	<p>Tableau メタデータのインポートに必要なデータ抽出ファイルのパス。</p> <p>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。</p> <ul style="list-style-type: none"> - .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。 <p>Tableau スキーマファイルのパスを指定すると、Secure Agent は、指定されたターゲットディレクトリのデータ表現に基づいて、ソースオブジェクトから .hyper ファイルを生成します。</p> <p>.hyper ファイルを Tableau Server または Tableau Cloud にパブリッシュする場合は、空のディレクトリのみを指定できます。</p> <p>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のターゲットオブジェクトの選択時に、Secure Agent には Tableau Server または Tableau Cloud にあるプロジェクトとデータソースが表示されます。</p> <p>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。</p> <p><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</p>

第 223 章

Teradata 接続のプロパティ

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

前提条件

Teradata コネクタを使用する前に、前提条件タスクを満たしていることを確認してください。

以下の前提条件タスクを実行します。

1. Teradata Parallel Transporter ユーティリティをインストールし、環境変数を設定します。
2. 成功ファイルおよびエラーファイルが含まれている Secure Agent ディレクトリにアクセスできることを確認します。このディレクトリパスは、各 Secure Agent マシンのランタイム環境で同じである必要があります。Teradata JDBC ドライバは、Secure Agent とともにパッケージ化されています。Secure Agent をインストールすると、JDBC ドライバがインストールされ、JDBC の jar が Secure Agent マシンにコピーされます。
3. Teradata データベースに接続するための認証の前提条件を設定します。ネイティブ認証、LDAP 認証、または KRB5 認証を設定できます。使用する認証タイプに基づいて、認証の詳細を手元に用意してください。
データ取り込みおよびレプリケーションでは、ネイティブ認証のみを使用できます。

Teradata Parallel Transporter Utilities

Teradata コネクタを使用する前に、Secure Agent マシンに Teradata Parallel Transporter ユーティリティをインストールしてください。

次の Teradata Parallel Transporter ユーティリティをインストールする必要があります。

- Teradata Parallel Transporter Base
- Teradata Parallel Transporter Stream Operator
- Teradata CLIV2
- Teradata Generic Security Services
- Teradata 用共有 ICU ライブラリ

Kerberos 認証の準備

必要な構成ファイルを Secure Agent マシンに配置することで、Kerberos 認証を使用して Teradata データベースに接続できます。

Teradata に接続できるように Kerberos 認証を設定する場合は、次のガイドラインを考慮してください。

- ホステッドエージェントまたはサーバーレスランタイム環境は使用できません。
- 使用する Secure Agent とデータベースサーバーが KDC サーバーに登録されていることを確認してください。
- krb5.conf ファイルに複数の KDC を追加することはできません。
- 資格情報キャッシュファイルを生成するには、以下のガイドラインを考慮してください。
 - Linux では、接続内の複数の Kerberos プリンシパルユーザーに対して資格情報キャッシュファイルを生成できます。ただし、マッピング内で使用できる Kerberos プリンシパルユーザーは 1 人だけです。
 - Windows では、接続内の複数の Kerberos プリンシパルユーザーに対して資格情報キャッシュファイルを生成できません。

Kerberos 認証の設定

Kerberos 認証を使用して Linux または Windows 上の Teradata に接続する前に、組織の管理者は前提条件のタスクを実行する必要があります。

1. Java Authentication and Authorization Service 構成ファイル（JAAS）を設定するには、次のタスクを実行します。

- a. Secure Agent マシン上に JAAS 構成ファイルを作成します。
- b. 以下のエントリを JAAS 構成ファイルに追加します。

```
JDBC_DRIVER_01 {  
    com.sun.security.auth.module.Krb5LoginModule required  
    useTicketCache=true;  
};
```

注: キーと値の各ペアは独立した行に指定してください。

2. krb5.conf ファイルを設定するには、次の手順を実行します。
 - a. Secure Agent マシン上に krb5.conf ファイルを作成します。
 - b. Key Distribution Center（KDC）と管理サーバーの詳細を、次の形式で krb5.conf ファイルに追加します。

```
[libdefaults]  
default_realm = <Realm name>  
forwardable = true  
ticket_lifetime = 24h  
  
[realms]  
<REALM NAME> = {  
    kdc = <Location where KDC is installed>  
    admin_server = <Location where KDC is installed>  
}  
[domain_realm]  
<domain name or host name> = <Domain name or host name of Kerberos>  
<domain name or host name> = <Domain name or host name of Kerberos>
```

3. Secure Agent マシンで環境変数を設定するには、次の手順を実行します。

- setenv KRB5CCNAME <資格情報キャッシュファイルの絶対パスとファイル名>
- setenv KRB5_CONFIG <Kerberos 構成ファイルの絶対パス>\krb5.conf
- setenv JAASCONFIG <JAAS 構成ファイルの絶対パス>\<ファイル名>.conf

4. Secure Agent を再起動します。

5. Secure Agent マシン上で資格情報キャッシュファイルを生成し、Kerberos 認証を使用して Teradata に接続するには、次の手順を実行します。
 - a. Secure Agent マシンで次のコマンドを実行し、Teradata のユーザー名とレルム名を指定します。
`Kinit <user name>@<realm_name>`
 - b. オプションで、Linux 上の Teradata データベースに接続する際に、Secure Agent マシン上に指定されたディレクトリとファイル名を使用して資格情報キャッシュファイルを生成するには、次のコマンドを実行します。
`Kinit -c <Directory and file name where you want to create the credential cache> <user name>@<realm_name>`
 - c. 要求されたら、Kerberos プリンシパルユーザーのパスワードを入力します。
6. `KRB5_CONFIG`、`KRB5CCNAME`、および `JAASCONFIG` プロパティを Teradata 接続の **【Kerberos アーティファクトディレクトリ】** フィールドに追加します。
 例えば、次の形式でプロパティを追加します。
`KRB5_CONFIG=<Absolute path of the Kerberos configuration file>\krb5.conf,KRB5CCNAME=<Absolute path of the credential cache file>/<File name>,JAASCONFIG=<Absolute path of the JAAS config file>\<File name>.conf`
注: キーと値のペア同士の間をカンマで区切ってください。

環境変数の設定

Teradata コネクタを使用する前に、Java および Teradata の環境変数を設定しておく必要があります。

次の表に、UNIX で設定する必要がある環境変数を示します。

環境変数	値
THREADONOFF	UNIX および Linux では、Teradata プロセスのマルチスレッド処理を有効にするために THREADONOFF 環境変数を 1 に設定します。
NLSPATH	NLSPATH 変数を opermsgs.cat ファイルの場所に設定します。 例: /opt/teradata/client/15.10/msg/%N

また、オペレーティングシステムに基づいて、共有ライブラリの環境変数も設定します。

以下の表に、オペレーティングシステムごとの共有ライブラリ変数のリストを示します。

オペレーティングシステム	値
Windows	PATH
Linux	LD_LIBRARY_PATH

例えば、Linux では次の構文を使用します。

- Bourne シェルを使用している場合は次のように入力します。
`export LD_LIBRARY_PATH="/opt/teradata/client/15.10/lib64:${LD_LIBRARY_PATH}"`
- C シェルを使用している場合は次のように入力します。
`LD_LIBRARY_PATH="/opt/teradata/client/15.10/lib64:${LD_LIBRARY_PATH}"`

環境変数を設定したら、Secure Agent を再起動します。

Teradata への接続

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

始める前に

開始する前に、前提条件を必ず満たすようにしてください。

認証の前提条件と実行する必要があるタスクの詳細については、「[「前提条件」 \(ページ 879\)](#)」を参照してください。

接続の詳細

次の表に、基本接続プロパティを示します。

プロパティ	説明
接続名	接続の名前。 各接続名は組織内で一意である必要があります。接続名には、英数字、スペース、および次の特殊文字を含めることができます。_ . + , 最大長は 255 文字です。
説明	接続の説明。最大長は 4000 文字です。
シークレットコンテナの使用	組織に対して設定されている Secrets Manager にこの接続の機密資格情報を保存します。 このプロパティは、組織に Secrets Manager が設定されている場合にのみ表示されます。 このプロパティは、データ取り込みおよびレプリケーションとデータアクセス管理サービスではサポートされていません。 接続でシークレットコンテナを有効にすると、Secure Agent が Secrets Manager からどの資格情報を取得するかを選択できます。このオプションを無効にした場合、資格情報は組織の設定方法に応じてリポジトリまたはローカル Secure Agent に保存されます。 注: この接続を使用してプッシュダウンまたはプロキシサービスを介してデータアクセスポリシーを適用する場合、シークレットコンテナ設定オプションを使用することはできません。 Secrets Manager を設定および使用する方法については、Administrator のヘルプにある「Secrets Manager の設定」を参照してください。
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。 Secure Agent を指定します。 ランタイム環境の設定および使用方法の詳細については、Administrator のヘルプにある「ランタイム環境」を参照してください。
TDPID	Teradata データベースマシンの名前、または IP アドレス。 Teradata データベースに接続するように KRB5 認証を設定する場合は、Teradata データベースマシンの完全修飾ホスト名を指定します。

プロパティ	説明
データベース名	Teradata データベース名。 データベース名を入力しない場合、Teradata PT API はデフォルトのログインデータベース名を使用します。
コードページ	Teradata データベースに関連付けられているコードページ。 次のいずれかのコードページを選択します。 - MS Windows Latin 1。ISO 8859-1 Western European データの場合に選択します。 - UTF-8。Unicode および Unicode 以外のデータの場合に選択します。 Teradata ソースからデータの抽出を行うタスクを実行する場合、Teradata PT API 接続のコードページはその Teradata ソースのコードページと同じである必要があります。

認証タイプ

ネイティブ認証タイプ、LDAP 認証タイプ、または KRB5 認証タイプを設定して、Teradata データベースに接続できます。

注: データ取り込みおよびレプリケーションでは、ネイティブ認証を使用する必要があります。KRB5 認証タイプまたは LDAP 認証タイプは使用しないでください。

必要な認証タイプを選択し、認証固有のパラメータを設定します。

ネイティブ認証

ネイティブ認証を設定するには、Teradata アカウントのユーザー名とパスワードが必要です。

次の表に、ネイティブ認証の基本接続プロパティを示します。

プロパティ	説明
ユーザー名	Teradata データベースへのアクセスに必要なデータベースの読み取りおよび書き込み権限を持つユーザー名。
パスワード	上記データベースユーザー名のパスワード。

LDAP 認証

LDAP 認証を設定するには、外部 LDAP ディレクトリサービスに対してユーザー資格情報を認証する必要があります。

注: データ取り込みおよびレプリケーションは、LDAP 認証タイプをサポートしていません。

次の表に、LDAP 認証の基本接続プロパティを示します。

プロパティ	説明
ユーザー名	LDAP データベースへのアクセスに必要なデータベースの読み取りおよび書き込み権限を持つユーザー名。
パスワード	LDAP データベースユーザー名のパスワード。

KRB5 認証

KRB5 認証を設定するには、Linux マシンでホストされる Secure Agent を設定し、Kerberos アーティファクトディレクトリに Kerberos 構成ファイルが含まれていることを確認する必要があります。

注: データ取り込みおよびレプリケーションは、KRB5 認証タイプをサポートしていません。

次の表に、KRB5 認証の基本接続プロパティを示します。

プロパティ	説明
ユーザー名	Teradata データベースに対して認証を行う Kerberos サービスプリンシパル名。
パスワード	データベース名のパスワード。 パスワードを PmKerberosPassword に設定します。

次の表に、KRB5 認証の詳細接続プロパティを示します。

プロパティ	説明
Kerberos アーティファクトディレクトリ	Kerberos 認証に必要なプロパティ。 KRB5_CONFIG、KRB5CCNAME、および JAASCONFIG プロパティを次の形式で追加します。 KRB5_CONFIG=<Absolute path of the Kerberos configuration file> \krb5.conf,KRB5CCNAME=<Absolute path of the credential cache file>/<File name>,JAASCONFIG=<Absolute path of the JAAS config file>\<File name>.conf 注: キーと値のペア同士の間をカンマで区切ってください。

詳細設定

次の表に、詳細接続のプロパティを示します。

プロパティ	説明
Tenacity	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 が継続してログインを再試行する時間（時間単位）。 正の整数を指定してください。 デフォルト値は 4 です。
最大セッション数	Teradata データベースとの接続を確立するために Teradata PT API に許可され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 フィールドに指定した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 がログインを再試行する前に待機する時間（分単位）。 ゼロ以外の正の整数を指定します。 デフォルト値は 6 です。

プロパティ	説明
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	<p>Teradata PT API が Export 演算子を使用して Teradata ソースから読み取りを行う各データブロックのサイズ（バイト単位）。</p> <p>Teradata データベースバージョン 16.20 以降の場合、最大値は 16775168 バイトです。</p> <p>Teradata データベースのバージョンが 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。</p> <p>ブロックサイズの詳細については、Teradata ログを参照し、同じバージョンの Teradata のマニュアルを確認してください。</p>
メタデータの 詳細接続 プロパティ	<p>JDBC ドライバが Teradata からメタデータを取得するためのオプションのプロパティ。</p> <p>複数のプロパティを追加する場合は、各プロパティをカンマで区切ってください。</p> <p>例えば、「tmode=ANSI,JAASCONFIG=<path to JAASCONFIG>/TeraJDBC.config」のようにします。</p> <p>次のスニペットは、必須の属性を持つ JAASCONFIG の例です。</p> <pre>Client { com.sun.security.auth.module.Krb5LoginModule required doNotPrompt=true useKeyTab=true useTicketCache=false principal="username@REALM.COM" keyTab="<Path to keyTab>/IICSTPT.keytab" };</pre>
メタデータの 資格の有 効化	<p>Teradata 接続が、テーブル名またはカラム名で使用される予約語を Teradata データベースから読み取るかどうかを決定します。</p> <p>【メタデータの資格の有効化】 チェックボックスをオンにして、Secure Agent が Teradata から予約語を読み取るようにします。</p>

データベース特権

Teradata コネクタを使用する前に、特定のデータディクショナリテーブルに対する特権を選択していることを確認してください。

次のデータベース特権を持っていることを確認します。

- DBC.Tables、DBC.Columns、DBC.UDTInfo、および DBC.Databases に対する特権を選択します。特権の選択の詳細については、Teradata JDBC ドライバのマニュアルを参照してください。

第 224 章

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
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。
シークレットコンテナの使用	組織に対して設定されている Secrets Manager にこの接続の機密資格情報を保存します。 このプロパティは、組織に Secrets Manager が設定されている場合にのみ表示されます。 このプロパティは、データ取り込みおよびレプリケーションとデータアクセス管理サービスではサポートされていません。 接続でシークレットコンテナを有効にすると、Secure Agent が Secrets Manager からどの資格情報を取得するかを選択できます。このオプションを無効にした場合、資格情報は組織の設定方法に応じてリポジトリまたはローカル Secure Agent に保存されます。 注: この接続を使用してプッシュダウンまたはプロキシサービスを介してデータアクセスポリシーを適用する場合、シークレットコンテナ設定オプションを使用することはできません。 Secrets Manager を設定および使用する方法については、Administrator のヘルプにある「Secrets Manager の設定」を参照してください。
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。 ランタイム環境の設定および使用方法の詳細については、Administrator のヘルプにある「ランタイム環境」を参照してください。
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。 <ul style="list-style-type: none">- 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	<p>UKGPro サービスアカウントのパスワード。</p> <p>次のいずれかのパスワードを指定します。</p> <ul style="list-style-type: none"> - 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	<p>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。</p> <p>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。</p> <p>サービスホスト名を次の形式で指定します：</p> <p>service\$.ultipro.com。</p> <p>ここで、\$は数値です。</p> <p>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。</p>
ユーザー API キー	<p>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。</p> <p>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] グラフィックタイトルの順に移動します。</p> <p>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。</p>
顧客 API キー	<p>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。</p> <p>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] グラフィックタイトル > [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。</p>
アプリケーションモジュール	<p>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。</p> <p>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。</p> <p>HR、給与、人材、および福利厚生</p> <p>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。</p> <p>統合イベント</p> <p>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。</p> <p>その他</p> <p>時間管理オブジェクトにアクセスします。</p>

第 225 章

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
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。
シークレットコンテナの使用	組織に対して設定されている Secrets Manager にこの接続の機密資格情報を保存します。 このプロパティは、組織に Secrets Manager が設定されている場合にのみ表示されます。 このプロパティは、データ取り込みおよびレプリケーションとデータアクセス管理サービスではサポートされていません。 接続でシークレットコンテナを有効にすると、Secure Agent が Secrets Manager からどの資格情報を取得するかを選択できます。このオプションを無効にした場合、資格情報は組織の設定方法に応じてリポジトリまたはローカル Secure Agent に保存されます。 注: この接続を使用してプッシュダウンまたはプロキシサービスを介してデータアクセスポリシーを適用する場合、シークレットコンテナ設定オプションを使用することはできません。 Secrets Manager を設定および使用する方法については、Administrator のヘルプにある「Secrets Manager の設定」を参照してください。
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。 ランタイム環境の設定および使用方法の詳細については、Administrator のヘルプにある「ランタイム環境」を参照してください。
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。 <ul style="list-style-type: none">- 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。 <ul style="list-style-type: none">- 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。

プロパティ	説明
サービス ホスト名	<p>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。</p> <p>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。</p> <p>サービスホスト名を次の形式で指定します： service\$.ultipro.com。</p> <p>ここで、\$は数値です。</p> <p>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。</p>
顧客 API キー	<p>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。</p> <p>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。</p>
ユーザー API キー	<p>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。</p> <p>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。</p> <p>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。</p>
アプリケー ション モジュール	<p>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。</p> <p>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。</p> <p>HR、給与、人材、および福利厚生</p> <p>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。</p> <p>統合イベント</p> <p>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。</p> <p>その他</p> <p>時間管理オブジェクトにアクセスします。</p>

第 226 章

Veeva Vault 接続のプロパティ

Veeva Vault オブジェクトにおけるデータの安全な読み取りや書き込みを行うための Veeva Vault 接続を作成します。

認証の準備

Veeva Vault にアクセスするために、「基本」認証タイプと「認証コード」認証タイプを設定できます。
接続プロパティを設定する前に、使用する認証のタイプに基づいて認証の詳細を用意しておく必要があります。

基本

基本認証を使用して Veeva Vault に接続するには、Veeva Vault の DNS 名、API バージョン、アカウントユーザ名、およびパスワードが必要です。

接続先の Veeva Vault CRM アプリケーションから必要な詳細を取得します。

Veeva Vault の基本認証の詳細については、Veeva Vault のマニュアルの「[User name and password](#)」を参照してください。

承認コード

OAuth 2.0 承認コードを使用して Veeva Vault に接続するには、Veeva Vault の DNS 名、API バージョン、認証 URL、アクセストークン URL、クライアント ID、スコープ、OAuth プロファイル ID、およびアクセストークンが必要です。

認証の詳細を取得するには、Veeva Vault で認証統合を作成し、OAuth 2.0 / OpenID Connect プロファイルを使用して Veeva Vault 統合に次の 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 401 エラーコードが返された場合に、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。

認証統合を作成し、認証の詳細を取得する方法の詳細については、Veeva Vault のマニュアルの「[Configuring OAuth 2.0 / OpenID Connect Profiles](#)」を参照してください。

Veewa Vault への接続

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

始める前に

開始する前に、設定する認証タイプに基づいて、関連する設定の詳細を Veewa Vault アカウントから取得する必要があります。

認証の前提条件の詳細については、「[「認証の準備」 \(ページ 890\)](#)」を参照してください。

接続の詳細

次の表に、基本接続プロパティを示します。

財産	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。
シークレットコンテナの使用	組織に対して設定されている Secrets Manager にこの接続の機密資格情報を保存します。 このプロパティは、組織に Secrets Manager が設定されている場合にのみ表示されます。 このプロパティは、データ取り込みおよびレプリケーションとデータアクセス管理サービスではサポートされていません。 接続でシークレットコンテナを有効にすると、Secure Agent が Secrets Manager からどの資格情報を取得するかを選択できます。このオプションを無効にした場合、資格情報は組織の設定方法に応じてリポジトリまたはローカル Secure Agent に保存されます。 注: この接続を使用してプッシュダウンまたはプロキシサービスを介してデータアクセスポリシーを適用する場合、シークレットコンテナ設定オプションを使用することはできません。 Secrets Manager を設定および使用する方法については、Administrator のヘルプにある「Secrets Manager の設定」を参照してください。
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。 Secure Agent 環境またはエラスティックランタイム環境を選択します。 ランタイム環境の設定および使用方法の詳細については、Administrator のヘルプにある「ランタイム環境」を参照してください。

認証タイプ

Veewa Vault にアクセスするために、「基本」認証タイプと「認証コード」認証タイプを設定できます。

必要な認証方法を選択し、認証固有のパラメータを設定します。

基本認証

基本認証はデフォルトの認証タイプです。基本認証に最低限必要なものは、Veewa Vault の DNS 名、API バージョン、アカウントユーザー名、およびパスワードです。

次の表に、基本認証の基本的な接続プロパティとその説明を示します。

プロパティ	説明
Vault DNS	Veeva Vault エンドポイントの DNS 名。 DNS 名は以下の形式で入力します。 <code>https://<Domain address>.veevavault.com</code> 例えば、ドメインアドレスが<MyDomain>である場合は、次の DNS 名を入力します。 <code>https://<MyDomains>.veevavault.com</code>
API バージョン	接続する Veeva Vault API のバージョン。 Veeva Vault API のバージョンを入力します。 例えば、Veeva Vault API のバージョンが 24.3 である場合は、次の値を入力します。 v24.3
ユーザー名	Veeva Vault アカウントに接続するためのユーザー名。
パスワード	Veeva Vault アカウントに接続するためのパスワード。

詳細設定

次の表に、基本認証の詳細接続プロパティとその説明を示します。

プロパティ	説明
再試行回数	Veeva Vault エンドポイントからの応答の受信を再試行する際の最大試行回数。
再試行間隔	Veeva Vault 接続が応答の受信を再試行するまでに待機する時間(ミリ秒)。
追加プロパティ	Veeva Vault に接続する際に設定できる追加のパラメータ。 複数の追加パラメータは、アンパサンドとコロン (&:) で区切った次のような形式で入力できます。 <parameter name1>=<value1>&:<parameter name2>=<value2>&:<parameter name3>=<value3>... デフォルトはです。 okhttp.retryStatusCodes=429,500,502,503,504&:okhttp.connectTimeout=30&:okhttp.readTimeout=30&:okhttp.writeTimeout=30 。

認証コードの認証

認証コードの認証に最低限必要なものは、Veeva Vault の DNS 名、API バージョン、認証 URL、アクセストークン URL、クライアント ID、スコープ、OAuth プロファイル ID、およびアクセストークンです。

次の表に、認証コードの認証の基本接続プロパティとその説明を示します。

プロパティ	説明
Vault DNS	<p>Veeva Vault エンドポイントの DNS 名。 DNS 名は以下の形式で入力します。 <code>https://<Domain address>.veevavault.com</code> 例えば、ドメインアドレスが<MyDomain>である場合は、次の DNS 名を入力します。 <code>https://<MyDomains>.veevavault.com</code></p>
API バージョン	<p>接続する Veeva Vault API のバージョン。 Veeva Vault API のバージョンを入力します。 例えば、Veeva Vault API のバージョンが 24.3 である場合は、次の値を入力します。 v24.3</p>
認証 URL	<p>ユーザー要求の認証に使用される Veeva Vault OAuth 2.0 認証サーバー。 認証 URL は次の形式で入力します。 <code>https://<認証サーバーのホスト名>/oauth2/v2.0/authorize</code></p>
アクセストークン URL	<p>認証コードを交換することでアクセストークンを取得するために使用される Veeva Vault OAuth 2.0 認証サーバー。 アクセストークン URL は次の形式で入力します。 <code>https://<認証サーバーのホスト名>/oauth2/v2.0/token</code></p>
クライアント ID	<p>アプリケーションを OAuth 用に設定したときに生成されるアプリケーションのクライアント識別子。</p>
スコープ	<p>Veeva Vault 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。 複数のスコープ属性をそれぞれスペースで区切って、次の形式で入力できます。 <code><Scope attribute1> <Scope attribute2> <Scope attribute3>...</code></p>
OAuth プロファイル ID	<p>Veeva Vault で OAuth プロファイルに割り当てられた一意の識別子。</p>
アクセストークン	<p>認証サーバーによって付与された、Veeva Vault データにアクセスするためのアクセストークン。 OAuth エンドポイントから取得して取り込んだアクセストークン値を入力するか、[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値を入力します。</p>

詳細設定

次の表に、認証コードの認証の詳細接続プロパティとその説明を示します。

プロパティ	説明
再試行回数	Veeva Vault エンドポイントからの応答の受信を再試行する際の最大試行回数。
再試行間隔	Veeva Vault 接続が応答の受信を再試行するまでに待機する時間(ミリ秒)。
追加プロパティ	<p>Veeva Vault に接続する際に設定できる追加のパラメータ。</p> <p>複数の追加パラメータは、アンパサンドとコロン（&:）で区切った次のような形式で入力できます。</p> <p><parameter name1>=<value1>&:<parameter name2>=<value2>&:<parameter name3>=<value3>...</p> <p>デフォルトはです。</p> <p>okhttp.retryStatusCodes=429,500,502,503,504&:okhttp.connectTimeout=30&:okhttp.readTimeout=30&:okhttp.writeTimeout=30。</p>

第 227 章

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。
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gger（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。 <i>host_name</i> は、ホスト名または IP アドレスにできます。 <i>host_name:port_number</i> 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。

プロパティ	説明
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gger (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	<p>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。</p> <ul style="list-style-type: none"> - 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。 <p>デフォルトは [なし] です。</p>
ペーシングサイズ	<p>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。</p> <p>デフォルトである最小値は 0 です。</p>
ペーシング単位	<p>[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。</p> <p>[行] または [キロバイト] のいずれかを選択します。</p>
マップの場所	<p>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。</p> <p>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gger (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。</p> <p>次の形式で値を入力します。 <i>host_name</i> は、ホスト名または IP アドレスにできます。</p> <p><i>host_name:port_number</i></p> <p>以下に例を示します。</p> <p>CDC01:25100</p> <p>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。</p>
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。

プロパティ	説明
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	<p>カスタムプロパティまたは接続プロパティのオーバーライド。カスタムプロパティとは、PowerExchange のデフォルトの設定よりも優先するために指定できるプロパティです。セミコロン (;) を区切り文字として使用して複数のプロパティを入力するか、パラメータファイルを使用して接続プロパティの上書きを指定するパラメータを指定することができます。</p> <p>例:</p> <pre><property>=<value>;<property>=<value></pre> <p>多くの場合、Informatica グローバルカスタマサポートからの指示を受けたうえで、カスタムプロパティの設定を行います。</p> <p>注: これらのプロパティは、PowerCenter の PowerExchange Client for PowerCenter (PWXPC) CDC 接続の 【PWX オーバーライド】 オプションと同じです。</p> <p>パラメータファイルを使用して接続プロパティのオーバーライドを指定するには、\$<ParameterName>の形式でパラメータを設定し、ユーザー定義パラメータ名の前にドル記号 (\$) を付けます。次に、【ランタイムオプション】 タブの 【パラメータファイル名】 フィールドにパラメータファイル名を指定することで、ユーザー定義パラメータ定義を含むパラメータファイルを使用するようにマッピングのマッピングタスクを設定します。</p> <p>注:</p> <ul style="list-style-type: none"> - マッピングおよび接続に同じパラメータを入力した場合は、接続カスタムプロパティが優先されます。 - パラメータファイルがある場合、このフィールドで指定するパラメータ名は、パラメータファイルで定義されたエントリと一致している必要があります。 <p>詳細については、「接続オーバーライドのリファレンス」の章を参照してください。</p>

第 228 章

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。
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。 <i>host_name</i> は、ホスト名または IP アドレスにできます。 <i>host_name:port_number</i> 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。

プロパティ	説明
オフロード処理	<p>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。</p> <ul style="list-style-type: none"> - 自動。オフロード処理を使用するかどうかは 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。 <p>デフォルトは [いいえ] です。</p>
オフロードスレッド	<p>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。</p> <p>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。</p> <p>有効な値は 1~64 です。</p> <p>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。</p> <p>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。</p>
配列サイズ	<p>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）。</p> <p>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。</p> <p>有効な値は 1~5000 です。デフォルトは 25 です。</p> <p>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。</p>
低値をスペースに置き換える	<p>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。</p>
接続リトライ期限	<p>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。</p>

プロパティ	説明
カスタムプロパティ	<p>カスタムプロパティまたは接続プロパティのオーバーライド。カスタムプロパティとは、PowerExchange のデフォルトの設定よりも優先するために指定できるプロパティです。セミコロンの (;) 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。</p> <p>例:</p> <pre><property>=<value>;<property>=<value></pre> <p>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。</p> <p>注: これらのプロパティは、PowerCenter の PowerExchange Client for PWX NRDB Batch 接続の [PWX オーバーライド] オプションと同じです。</p> <p>また、このフィールドまたはパラメータファイルを使用して、接続プロパティのオーバーライドを指定することもできます。パラメータファイルを使用して接続プロパティのオーバーライドを指定するには、<code>\$<ParameterName></code> の形式でパラメータを設定し、ユーザー定義パラメータ名の前にドル記号 (\$) を付けます。次に、[ランタイムオプション] タブの [パラメータファイル名] フィールドにパラメータファイル名を指定することで、ユーザー定義パラメータ定義を含むパラメータファイルを使用するようにマッピングのマッピングタスクを設定します。</p> <p>注:</p> <ul style="list-style-type: none"> - マッピングおよび接続に同じパラメータを入力した場合は、接続カスタムプロパティが優先されます。 - パラメータファイルがある場合、このフィールドで指定するパラメータ名は、パラメータファイルで定義されたエントリと一致している必要があります。 <p>詳細については、「接続オーバーライドのリファレンス」の章を参照してください。</p>
書き込みプロパティ	<p>書き込みモード。次のオプションがあります。</p> <ul style="list-style-type: none"> - 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。

第 229 章

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。
シークレットコンテナの使用	組織に対して設定されている Secrets Manager にこの接続の機密資格情報を保存します。 このプロパティは、組織に Secrets Manager が設定されている場合にのみ表示されます。 このプロパティは、データ取り込みおよびレプリケーションとデータアクセス管理サービスではサポートされていません。 接続でシークレットコンテナを有効にすると、Secure Agent が Secrets Manager からどの資格情報を取得するかを選択できます。このオプションを無効にした場合、資格情報は組織の設定方法に応じてリポジトリまたはローカル Secure Agent に保存されます。 注: この接続を使用してプッシュダウンまたはプロキシサービスを介してデータアクセスポリシーを適用する場合、シークレットコンテナ設定オプションを使用することはできません。 Secrets Manager を設定および使用する方法については、Administrator のヘルプにある「Secrets Manager の設定」を参照してください。
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。 Secure Agent、ホステッドエージェント、サーバーレスランタイム環境、またはエラスティックランタイム環境を選択します。 ランタイム環境の設定および使用方法の詳細については、Administrator のヘルプにある「ランタイム環境」を参照してください。

プロパティ	説明
認証	<p>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。</p> <p>ユーザー名トークン</p> <p>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。</p> <p>その他の認証</p> <p>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。</p> <p>NTLM 認証</p> <p>NTLM V2 認証を使用して、Web サービスを認証します。</p>
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。

第 230 章

Web サービス V2 接続のプロパティ

Web サービス 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。

重要: WebServices V2 コネクタは非推奨となり、メンテナンスモードに移行されました。Informatica は将来のリリースでサポートを廃止する予定です。Web サービスコンシューマコネクタを使用して Web サービスアプリケーションにアクセスすることをお勧めします。

次の表に、Web サービス 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 [Web サービス] を選択します。
Secure Agent	一覧から該当する Secure Agent を選択します。
WSDL URL	WSDL URI または URL を入力します。 注: [接続] タブの WSDL URL フィールドの長さは 500 文字まで増加しています。
ヘッダー CSV パス	header* CSV ファイルが作成される Secure Agent サーバーパスを入力します。
ボディ CSV パス	body* CSV ファイルが作成される Secure Agent サーバーパスを入力します。
エンドポイント URL	要求が出される場所である、Web サービスのエンドポイント URL を入力します。 注: [接続] タブのエンドポイント URL フィールドの長さは 500 文字まで増加しています。

接続プロパティ	説明
認証タイプ	<p>使用可能な認証の一覧から認証のタイプを選択します。</p> <p>なし</p> <p>認証は必要ありません。</p> <p>基本認証</p> <p>基本認証が必要です。</p> <p>WSSE ユーザートークン認証</p> <p>ユーザートークン認証が必要です。</p> <p>WSSE デジタル署名認証</p> <p>SSL 証明書に基づく認証が必要です。</p>
ユーザー名	認証に必要な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ます。
証明書パス	証明書パスは WSSE デジタル署名認証を使用する場合のみに入力します。
自動 CSV ファイル作成	「ボディ/ヘッダー CSV ファイルの自動作成」（ファイルの自動作成）または「ボディ/ヘッダー CSV ファイルの手動作成」（CSV ファイルを手動で作成）を選択します。
添付ファイルのダウンロードパス	すべてのファイルがダウンロードされる先のローカルディレクトリパスを入力します。
添付ファイルのアップロードパス	すべてのファイルがアップロードされる元のローカルディレクトリパスを入力します。
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。
空タグの許可	選択すると SOAP 要求で空タグを許可します。

第 231 章

Workday 接続のプロパティ

Workday 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。

重要: Workday コネクタは非推奨となり、メンテナンスモードに移行されました。Informatica は将来のリリースでサポートを廃止する予定です。Workday V2 コネクタを使用して Workday にアクセスすることをお勧めします。

次の表に、Workday 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	Username@Tenant 形式のユーザー名。ここで、「Tenant」は【テナント名】フィールドの値を表します。
パスワード	関連するパスワード。
ドメイン名	Workday ドメインの名前。例: impl-cc.workday.com
テナント名	Workday テナントの名前。例: informatica_gms1
モジュール名	接続先のモジュール。
ログインの有効化	ログインの有効化。 ログインを有効化するチェックボックスを選択します。

第 232 章

Workday Mass Ingestion 接続のプロパティ

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

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

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

基本認証の接続プロパティ

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

接続プロパティ	説明
接続名	接続の名前。この名前は、組織内で一意にする必要があります。接続名には、英数字、スペース、および次のような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。
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。 アプリケーション取り込みとレプリケーションタスクでは、Secure Agent またはサーバーレスランタイム環境を選択できます。ホステッドエージェントは使用できません。
ドメイン名	アクセスするリソースを含む Workday ドメインの名前。
テナント名	アクセスする Workday テナントの識別子。
バージョン	オプション。接続が Workday データを取得するために使用する必要があるエンドポイントの Web サービス記述言語（WSDL）バージョン。Web サービスでサポートされる操作のリストは、このフィールドで指定した WSDL バージョンによって異なります。 注: Workday Mass Ingestion 接続は、WSDL v37.0 に含まれていないサービスからデータを読み取らない可能性があるため、WSDL v37.0 を使用することをお勧めします。 WSDL バージョンの詳細については、「 Workday Web Services (WWS) documentation 」を参照してください。

接続プロパティ	説明
ユーザー名	Workday アカウントのユーザー名。
パスワード	Workday アカウントのパスワード。

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

OAuth 2.0 更新トークンフロー認証の接続プロパティ

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

接続プロパティ	説明
接続名	接続の名前。この名前は、組織内で一意にする必要があります。接続名には、英数字、スペース、および次のような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。
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。 アプリケーション取り込みとレプリケーションタスクでは、Secure Agent またはサーバーレスランタイム環境を選択できます。ホステッドエージェントは使用できません。
ドメイン名	アクセスするリソースを含む Workday ドメインの名前。
テナント名	アクセスする Workday テナントの識別子。
バージョン	オプション。接続が Workday データを取得するために使用する必要があるエンドポイントの Web サービス記述言語（WSDL）バージョン。Web サービスでサポートされる操作のリストは、このフィールドで指定した WSDL バージョンによって異なります。 注: Workday Mass Ingestion 接続は、WSDL v37.0 に含まれていないサービスからデータを読み取らない可能性があるため、WSDL v37.0 を使用することをお勧めします。 WSDL バージョンの詳細については、「 Workday Web Services (WWS) documentation 」を参照してください。
ユーザー名	オプション。Workday アカウントのユーザー名。
クライアント ID	Workday に登録されているアプリケーションのクライアント ID。
クライアントシークレット	Workday に登録されているアプリケーションのプライベートキー。
更新トークン	Workday が登録済みアプリケーション用に生成するトークン文字列を更新します。
トークンエンドポイント	Workday インスタンスの OAuth トークンエンドポイント。登録されているアプリケーションは、このエンドポイントにアクセストークン要求を送信します。

第 233 章

Workday V2 接続のプロパティ

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

Workday への接続

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

接続の詳細

次の表に、基本接続プロパティを示します。

プロパティ	説明
接続名	接続の名前。 各接続名は組織内で一意である必要があります。接続名には、英数字、スペース、および次の特殊文字を含めることができます。_ . + - , 最大長は 255 文字です。
説明	接続の説明。最大長は 4000 文字です。
シークレットコンテナの使用	組織に対して設定されている Secrets Manager にこの接続の機密資格情報を保存します。 このプロパティは、組織に Secrets Manager が設定されている場合にのみ表示されます。 このプロパティは、データ取り込みおよびレプリケーションとデータアクセス管理サービスではサポートされていません。 接続でシークレットコンテナを有効にすると、Secure Agent が Secrets Manager からどの資格情報を取得するかを選択できます。このオプションを無効にした場合、資格情報は組織の設定方法に応じてリポジトリまたはローカル Secure Agent に保存されます。 注: この接続を使用してプッシュダウンまたはプロキシサービスを介してデータアクセスポリシーを適用する場合、シークレットコンテナ設定オプションを使用することはできません。 Secrets Manager を設定および使用する方法については、Administrator のヘルプにある「Secrets Manager の設定」を参照してください。
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。 Secure Agent、ホステッドエージェント、サーバーレスランタイム環境、またはエラスティックランタイム環境を選択します。 ランタイム環境の設定および使用方法の詳細については、Administrator のヘルプにある「ランタイム環境」を参照してください。

プロパティ	説明
認証	Workday モジュールにアクセスするための Workday サービスによる認証。 [Workday] を選択します。
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。 ユーザー名とテナント名は次の形式で入力できます。 <ユーザー名>@<テナント名> 例: jjoe@informatica_pt1 テナント名を指定しない場合、Secure Agent によって指定したユーザー名にテナント名が追加されます。
パスワード	Workday サービスにログインするためのパスワード。
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。 Web サービスで使用可能なモジュールの詳細については、次のリンクを参照してください: Modules for the web services 。
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。 サポートされているバージョンの詳細については、次のリンクを参照してください: Supported WSDL versions 。

詳細設定

次の表に、詳細接続のプロパティを示します。

プロパティ	説明
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場合に選択します。Workdaystandard オブジェクトフィールドを取得する場合は選択を解除します。 デフォルトでは無効になっています。

第 234 章

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。

重要: Xactly コネクタは非推奨となり、メンテナンスモードに移行されました。Informatica は将来のリリースでサポートを廃止する予定です。

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。
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、ホステッドエージェント、サーバーレスランタイム環境、またはエラスティックランタイム環境を選択します。 ランタイム環境の設定および使用方法の詳細については、Administrator のヘルプにある「ランタイム環境」を参照してください。
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。
ログギングの有効化	タスクのログ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。

第 235 章

Xero 接続のプロパティ

Xero 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、Xero 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。
シークレットコンテナの使用	組織に対して設定されている Secrets Manager にこの接続の機密資格情報を保存します。 このプロパティは、組織に Secrets Manager が設定されている場合にのみ表示されます。 このプロパティは、データ取り込みおよびレプリケーションとデータアクセス管理サービスではサポートされていません。 接続でシークレットコンテナを有効にすると、Secure Agent が Secrets Manager からどの資格情報を取得するかを選択できます。このオプションを無効にした場合、資格情報は組織の設定方法に応じてリポジトリまたはローカル Secure Agent に保存されます。 注: この接続を使用してプッシュダウンまたはプロキシサービスを介してデータアクセスポリシーを適用する場合、シークレットコンテナ設定オプションを使用することはできません。 Secrets Manager を設定および使用する方法については、Administrator のヘルプにある「Secrets Manager の設定」を参照してください。
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。 Secure Agent、ホステッドエージェント、またはエラスティックランタイム環境を指定します。 ランタイム環境の設定および使用方法の詳細については、Administrator のヘルプにある「ランタイム環境」を参照してください。
認証	Xero コネクタが Xero へのログインに使用する必要のある認証方法。 デフォルトは AuthorizationCode です。
認証 URL	認証コードを取得する認証サーバーエンドポイント。 認証 URL は https://login.xero.com/identity/connect/authorize です。
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必要な Xero のアクセストークン URL。 アクセストークン URL は https://identity.xero.com/connect/token です。

接続プロパティ	説明
クライアント ID	アプリケーション登録プロセス中にクライアント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クライアントに発行されるクライアントシークレットキー。
スコープ	アクセス要求のスコープ。
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。
認証コードパラメータ	認証 URL で使用する追加パラメータ。
アクセストークン	<p>データにアクセスするための、Xero によって付与されるアクセストークン。</p> <p>【トークンの生成】 をクリックして、アクセストークンを取り込みます。</p> <p>注: アクセストークンを手動で入力しないでください。アクセストークンを手動で入力すると、アクセストークンの有効期限が切れた場合に接続が失敗します。</p>
更新トークン	<p>新しいアクセストークンを取得するための更新トークン。</p> <p>【トークンの生成】 をクリックして、更新トークンを取り込みます。</p> <p>アクセストークンが有効期限切れの場合、エージェントは、更新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。</p>
Xero テナント ID	<p>Xero のテナント ID。</p> <p>テナント ID は Xero 管理者から取得できます。</p>

第 236 章

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。

重要: XML ソースコネクタは非推奨となり、メンテナンスモードに移行されました。Informatica は将来のリリースでサポートを廃止する予定です。

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。

第 237 章

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。

重要: XML ターゲットコネクタは非推奨となり、メンテナンスモードに移行されました。Informatica は将来のリリースでサポートを廃止する予定です。

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。

第 238 章

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。 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。
シークレットコンテナの使用	組織に対して設定されている Secrets Manager にこの接続の機密資格情報を保存します。 このプロパティは、組織に Secrets Manager が設定されている場合にのみ表示されます。 このプロパティは、データ取り込みおよびレプリケーションとデータアクセス管理サービスではサポートされていません。 接続でシークレットコンテナを有効にすると、Secure Agent が Secrets Manager からどの資格情報を取得するかを選択できます。このオプションを無効にした場合、資格情報は組織の設定方法に応じてリポジトリまたはローカル Secure Agent に保存されます。 注: この接続を使用してプッシュダウンまたはプロキシサービスを介してデータアクセスポリシーを適用する場合、シークレットコンテナ設定オプションを使用することはできません。 Secrets Manager を設定および使用する方法については、Administrator のヘルプにある「Secrets Manager の設定」を参照してください。
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。 ランタイム環境の設定および使用方法の詳細については、Administrator のヘルプにある「ランタイム環境」を参照してください。
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。

接続プロパティ	説明
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。
スキーマポリシー	<p>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。</p> <ul style="list-style-type: none"> - 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	<p>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。</p> <p>FILENAME:PASSWORD</p> <p>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。</p> <p>Windows: %APPDATA%\postgresql\root.crt</p> <p>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。</p>
セキュアな、無効化されたトラスト	<p>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。</p> <p>デフォルトは false です。</p>

第 239 章

Zendesk 接続のプロパティ

Zendesk 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。

重要: Zendesk コネクタは非推奨となり、メンテナンスモードに移行されました。Informatica は将来のリリースでサポートを廃止する予定です。Zendesk V2 コネクタを使用して Zendesk にアクセスすることをお勧めします。

次の表に、Zendesk 接続のプロパティを示します。

接続プロパティ	説明
Secure Agent	タスクを実行する Secure Agent。
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。
カスタムフィールド	<p>Zendesk オブジェクトのカスタムフィールドを指定します。</p> <p>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 のカスタムフィールドキーの値です。</p> <p><オブジェクト 1>=<フィールドキー 1>,<データ型>,<サイズ>,<フィルタ可能性>,<プライマリキー>;<フィールドキー 2>,<データ型>,<サイズ>,<フィルタ可能性>,<プライマリキー></p> <p><オブジェクト 2>=<フィールドキー 1>,<データ型>,<サイズ>,<フィルタ可能性>,<プライマリキー>;<フィールド ID2>,<データ型>,<サイズ>,<フィルタ可能性>,<プライマリキー></p> <p>以下に例を示します。</p> <p>Organizations="support_description,String,255,true,false";</p> <p>Users="fixes,String,255,true,false";age,Double,255,true,false";"required,Boolean,255,true,false";"select,String,255,true,false";"support_description,String,255,true,false";"reg_ex,String,255,true,false"</p> <p>注: Tickets オブジェクトに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次の形式で指定する必要があります。Tickets="CF_<フィールドキー 1>,<データ型>,<サイズ>,<フィルタ可能性>,<プライマリキー>;"CF_<フィールド ID2>,<データ型>,<サイズ>,<フィルタ可能性>,<プライマリキー>"</p> <p>以下に例を示します。</p> <p>Tickets="CF_360003199614,String,255,true,false;"CF_360003373654,String,255,true,false"</p>

第 240 章

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 には基本認証方式を使用して接続できます。基本認証では、Zendesk アカウントに関連付けられたログイン資格情報とサブドメインを使用します。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。

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。

注: OAuth 2.0 認証は適用されません。 [Zendesk's updated security protocols](#) に準拠するために、このサポートは廃止されました。

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

接続プロパティ	説明
接続名	接続の名前。この名前は、組織内で一意にする必要があります。接続名には、英数字、スペース、および次のような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。
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。 アプリケーション取り込みとレプリケーションタスクでは、Secure Agent またはサーバーレスランタイム環境を選択できます。ホステッドエージェントは使用できません。
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。

第 241 章

Zendesk V2 接続のプロパティ

Zendesk に対してデータの安全な読み取りおよび書き込みを行うための Zendesk V2 接続を作成します。

認証の準備

Zendesk にアクセスするように基本認証、API トークン認証、OAuth 2.0 クライアント資格情報の認証のタイプを設定することができます。

接続プロパティを設定する前に、使用する認証のタイプに基づいて認証の詳細を用意しておく必要があります。

基本認証

基本認証を使用して Zendesk に接続するには、Zendesk アカウントのユーザー名とパスワードが必要です。

接続先の Zendesk アカウントから必要な詳細を取得します。

API トークン認証

API トークン認証を使用して Zendesk に接続するには、Zendesk アカウントのユーザー名と API トークンが必要です。

Zendesk で API トークンを生成するには、アカウントで API トークンへのアクセスが有効になっている管理者である必要があります。

1. Zendesk アカウントにログインします。
2. **管理センター**に移動します。【**アプリと統合**】をクリックし、【**API**】>【**API トークン**】の順に選択します。
3. 【**API トークンの追加**】をクリックします。
4. API トークンの名前を入力します。
5. 【**保存**】をクリックしてトークンを生成します。
6. 【**コピー**】をクリックします。

Zendesk での API トークン認証の詳細については、Zendesk のマニュアルの「[Managing API tokens](#)」を参照してください。

OAuth 2.0 クライアント資格情報認証

OAuth 2.0 クライアント資格情報認証を使用して Zendesk に接続するには、Zendesk のクライアント ID とクライアントシークレットが必要です。

クライアント資格情報付与タイプを使用して OAuth エンドポイントを設定し、次に認証統合を作成して認証の詳細を取得します。

OAuth 2.0 クライアント資格情報認証を使用して Zendesk 接続を設定する場合は、Zendesk アプリケーション内の識別子の値を **クライアント ID** として、また、シークレット値を **クライアントシークレット** として使用してください。

認証統合を作成し、認証の詳細を取得する方法の詳細については、Zendesk のマニュアルの「[OAuth authentication with your application](#)」を参照してください。

Zendesk への接続

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

始める前に

開始する前に、Zendesk で、管理者権限を持つユーザーアカウントが作成されていることを確認します。設定する認証タイプに応じて、Zendesk アカウントから関連する設定の詳細を取得します。

認証の前提条件の詳細については、「[「認証の準備」 \(ページ 919\)](#)」を参照してください。

接続の詳細

次の表に、基本接続プロパティを示します。

財産	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。
シークレットコンテナの使用	組織に対して設定されている Secrets Manager にこの接続の機密資格情報を保存します。 このプロパティは、組織に Secrets Manager が設定されている場合にのみ表示されます。 このプロパティは、データ取り込みおよびレプリケーションとデータアクセス管理サービスではサポートされていません。 接続でシークレットコンテナを有効にすると、Secure Agent が Secrets Manager からどの資格情報を取得するかを選択できます。このオプションを無効にした場合、資格情報は組織の設定方法に応じてリポジトリまたはローカル Secure Agent に保存されます。 注: この接続を使用してプッシュダウンまたはプロキシサービスを介してデータアクセスポリシーを適用する場合、シークレットコンテナ設定オプションを使用することはできません。 Secrets Manager を設定および使用する方法については、Administrator のヘルプにある「Secrets Manager の設定」を参照してください。

財産	説明
ランタイム環境	<p>タスクを実行するランタイム環境の名前。</p> <p>Secure Agent、ホステッドエージェント、サーバーレスランタイム環境、またはエラスティックランタイム環境を指定します。</p> <p>ランタイム環境の設定および使用方法の詳細については、Administrator のヘルプにある「ランタイム環境」を参照してください。</p>
URL	<p>Zendesk アカウントの URL。</p> <p>完全な URL を指定します。</p> <p>例えば、https://informaticabusinesssolution13.zendesk.com/api/v2 です。</p>

認証タイプ

Zendesk にアクセスするように基本認証、API トークン認証、OAuth 2.0 クライアント資格情報の認証のタイプを設定することができます。

必要な認証タイプを選択し、その認証に固有のパラメータを設定します。

基本認証

基本認証では、Zendesk アカウントのユーザー名とパスワードを使用して Zendesk に接続する必要があります。基本認証が、デフォルトの認証タイプです。

次の表に、基本認証の基本的な接続プロパティとその説明を示します。

プロパティ	説明
ユーザー名	Zendesk アカウントに接続するためのユーザー名。
パスワード	Zendesk アカウントに接続するためのパスワード。

詳細設定

次の表に、基本認証の詳細接続プロパティとその説明を示します。

プロパティ	説明
カスタムフィールド	<p>Zendesk オブジェクトのカスタムフィールド。</p> <p>カスタムフィールドの設定に関する詳細については、「「Zendesk のカスタムフィールド」 (ページ 923)」を参照してください。</p>
プロキシの使用	<p>プロキシサーバー経由で Zendesk に接続します。</p> <p>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。</p> <p>プロキシサーバーへの接続の詳細については、「「プロキシサーバーの設定」 (ページ 924)」を参照してください。</p>
ロギングの有効化	<p>コネクタのログ記録を有効にします。</p> <p>このチェックボックスをオンにすると、接続の作成時にログ記録が有効になり、その接続を使用してメタデータのインポートやタスクの実行を行います。</p>

API トークン認証

API トークン認証では、Zendesk に接続するために、Zendesk アカウントのユーザー名と API トークンが必要です。

次の表に、API トークン認証の基本的な接続プロパティとその説明を示します。

プロパティ	説明
ユーザー名	Zendesk アカウントに接続するためのユーザー名。
API トークン	Zendesk エンドポイントに対して行われた API 要求を認証するために Zendesk アプリケーションから生成された API トークン。

詳細設定

次の表に、API トークン認証の詳細接続プロパティとその説明を示します。

プロパティ	説明
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。 カスタムフィールドの設定に関する詳細については、「 「Zendesk のカスタムフィールド」 (ページ 923) 」を参照してください。
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。 プロキシサーバーへの接続の詳細については、「 「プロキシサーバーの設定」 (ページ 924) 」を参照してください。
ロギングの有効化	コネクタのログ記録を有効にします。 このチェックボックスをオンにすると、接続の作成時にログ記録が有効になり、その接続を使用してメタデータのインポートやタスクの実行を行います。

クライアント資格情報認証

クライアント資格情報認証では、Zendesk に接続するために Zendesk のクライアント ID とクライアントシークレットが必要です。

次の表に、OAuth 2.0 クライアント資格情報認証の基本的な接続プロパティに関する説明を示します。

プロパティ	説明
クライアント ID	アプリケーションを OAuth 用に設定したときに生成されるアプリケーションのクライアント識別子。
クライアントシークレット	クライアント ID に生成されたクライアントシークレット。

詳細設定

次の表に、OAuth 2.0 クライアント資格情報認証の詳細接続プロパティに関する説明を示します。

プロパティ	説明
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。 カスタムフィールドの設定に関する詳細については、「 「Zendesk のカスタムフィールド」 (ページ 923) 」を参照してください。
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。 プロキシサーバーへの接続の詳細については、「 「プロキシサーバーの設定」 (ページ 924) 」を参照してください。
ロギングの有効化	コネクタのログ記録を有効にします。 このチェックボックスをオンにすると、接続の作成時にログ記録が有効になり、その接続を使用してメタデータのインポートやタスクの実行を行います。
クライアント資格情報スコープ	Zendesk 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おけるアクセス要求のスコープ。 複数のスコープをカンマで区切って入力することができます。 デフォルトは読み書きです。 スコープの指定の詳細については、Zendesk マニュアルの「 Scopes 」を参照してください。
クライアント資格情報の有効期限	生成されたアクセストークンの有効期限が切れるまでの時間(秒単位)。 デフォルトは 3600 です。

Zendesk のカスタムフィールド

次の Zendesk オブジェクトに存在するカスタムフィールドからデータの読み取りを行うには、Zendesk V2 コネクタを使用します。

- 組織
- チケット
- ユーザー

Zendesk のカスタムフィールドからデータの読み取りを行うには、Zendesk V2 接続を作成するときに【**カスタムフィールド**】プロパティを設定する必要があります。

次の表に、Zendesk V2 コネクタでサポートされるさまざまなカスタムフィールドとデータ型の一覧を示します。

Zendesk のカスタムフィールド型	データ型
チェックボックス	BOOLEAN
日付	STRING

Zendesk のカスタムフィールド型	データ型
小数	DOUBLE
複数行のテキスト	STRING
数値	INTEGER
テキスト	STRING

Zendesk のカスタムフィールドの設定の詳細については、Zendesk ドキュメントにある「[Custom fields and custom field types](#)」を参照してください。

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 アプリケーションの【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"
```

例:

```
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。

プロキシサーバーの設定

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

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

プロキシ設定は、マッピングおよび詳細モードのマッピングで使用される接続に適用されます。

Secure Agent のプロキシの設定を行うには、次のタスクを実行します。

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

手順については、データ統合のヘルプの『または「Windows でのプロキシ設定」または「Linux でのプロキシ設定」を参照してください。

- proxy.ini ファイルでプロキシサーバーのプロパティを設定します。

サーバーレスランタイム環境のプロキシの設定を行う方法については、Administrator ヘルプの「ランタイム環境」にある「プロキシサーバーの使用」を参照してください。

第 242 章

Zuora AQuA の接続プロパティ

Zuora 接続を作成して、Zuora から安全なデータの読み取りを行います。Zuora AQuA 接続は **【接続】** ページで作成することができます。

同期タスクまたはマッピングタスクを作成するときに Zuora AQuA 接続を使用します。

Zuora への接続

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

始める前に

接続プロパティを設定する前に、Zuora アカウントから情報を取得する必要があります。次のビデオは、Zuora アカウントから情報を取得する方法を示しています。



接続の詳細

次の表に、基本接続プロパティを示します。

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

プロパティ	説明
シークレットコンテナの使用	<p>組織に対して設定されている Secrets Manager にこの接続の機密資格情報を保存します。</p> <p>このプロパティは、組織に Secrets Manager が設定されている場合にのみ表示されます。</p> <p>このプロパティは、データ取り込みおよびレプリケーションとデータアクセス管理サービスではサポートされていません。</p> <p>接続でシークレットコンテナを有効にすると、Secure Agent が Secrets Manager からどの資格情報を取得するかを選択できます。このオプションを無効にした場合、資格情報は組織の設定方法に応じてリポジトリまたはローカル Secure Agent に保存されます。</p> <p>注: この接続を使用してプッシュダウンまたはプロキシサービスを介してデータアクセスポリシーを適用する場合、シークレットコンテナ設定オプションを使用することはできません。</p> <p>Secrets Manager を設定および使用方法については、Administrator のヘルプにある「Secrets Manager の設定」を参照してください。</p>
ランタイム環境	<p>タスクを実行するランタイム環境の名前。</p> <p>Secure Agent 環境またはエラスティックランタイム環境を選択します。</p> <p>ランタイム環境の設定および使用方法の詳細については、Administrator のヘルプにある「ランタイム環境」を参照してください。</p>
エンドポイント URL	<p>Zuora サーバーの URL。</p> <p>例えば、URL を「https://www.zuora.com/apps/api/」のように指定できます。</p>
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。
WSDL バージョン	Zuora WSDL のバージョン番号。

詳細設定

次の表に、詳細接続のプロパティを示します。

プロパティ	説明
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。
削除した行の取得	<p>オプション。増分モードで、削除した行を取得します。</p> <p>デフォルトは false です。</p>
UTC オフセット	<p>特定の場所と日付での協定世界時（UTC）との時差。</p> <p>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。</p>

第 243 章

Zuora 接続のプロパティ

Zuora 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。

重要: Zuora コネクタは非推奨となり、メンテナンスモードに移行されました。Informatica は将来のリリースでサポートを廃止する予定です。REST V2 コネクタを使用して Zuora にアクセスすることをお勧めします。

次の表に、Zuora 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。 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。 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。

第 244 章

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。

重要: Zuora REST V2 コネクタは非推奨となり、メンテナンスモードに移行されました。Informatica は将来のリリースでサポートを廃止する予定です。REST V2 コネクタを使用して Zuora にアクセスすることをお勧めします。

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ください。 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できます。 <ul style="list-style-type: none">- 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。

プロパティ	説明
エンティティ ID	<p>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。</p> <p>要求メッセージエディタ内でエンティティ ID を指定することもできます。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。</p> <p>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。</p>
Zuora API バージョン	<p>Zuora REST V2 接続に使用する Swagger ファイル。</p> <p>Zuora Swagger API V1_2017_09_06 または Zuora Swagger API V1_2018_08_23 swagger ファイルを選択できます。</p>
カスタムフィールド設定	<p>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。</p> <p>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できます。</p> <ul style="list-style-type: none"> - 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 <p>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。</p> <p>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 を参照してください。</p>

索引

A

ActiveCampaign
 接続プロパティ [39](#)
Adabas
 接続プロパティ [43](#)
Adabas CDC
 接続プロパティ [40](#)
Adaptive Insights
 接続プロパティ [46](#)
Adobe Analytics
 接続プロパティ [47](#)
Adobe Analytics Mass Ingestion 接続
 接続プロパティ [49](#)
Adobe Experience Platform
 接続プロパティ [51](#)
Advanced FTP V2 接続
 プロパティ [54](#)
Advanced FTPS V2 接続
 プロパティ [58](#)
Advanced SFTP V2 接続
 プロパティ [62](#)
Amazon Aurora
 接続プロパティ [72](#)
Amazon DynamoDB
 接続プロパティ [74](#)
Amazon DynamoDB V2
 接続プロパティ [75](#)
Amazon Kinesis 接続
 概要 [77](#)
Amazon Redshift
 接続プロパティ [81](#)
Amazon Redshift V2
 接続プロパティ [94](#)
Amazon Redshift V2 接続
 概要 [83](#)
Amazon S3
 接続プロパティ [110](#)
Amplitude
 接続プロパティ [145](#)
Anaplan V2
 接続プロパティ [148](#)
Ariba V2
 接続プロパティ [151](#)
AS2
 プロパティ [153](#)

B

BigMachines
 接続プロパティ [160](#)
Birst Cloud 接続
 接続プロパティ [162](#)
Business 360
 接続プロパティ [168](#)

Business 360 FEP
 接続プロパティ [170](#)

C

CallidusCloud Commissions
 接続プロパティ [171](#)
CallidusCloud File Processor
 接続プロパティ [173](#)
Cassandra V2 接続
 プロパティ [175](#)
Chatter
 接続プロパティ [177](#)
Cloud アプリケーション統合コミュニティ
 URL [30](#)
Cloud 開発者コミュニティ
 URL [30](#)
Cloud 統合ハブ接続
 接続プロパティ [178](#)
Concur
 接続プロパティ [180](#)
Concur V2
 接続プロパティ [182](#)
Couchbase 接続
 プロパティ [184](#)
Coupa
 接続プロパティ [186](#)

D

Datacom
 接続プロパティ [218](#)
Datacom CDC
 接続プロパティ [215](#)
Db2 for i
 接続プロパティ [227](#)
Db2 for i CDC
 接続プロパティ [224](#)
Db2 for i Database Ingestion 接続
 接続プロパティ [229](#)
Db2 for LUW CDC
 接続プロパティ [231](#)
Db2 for LUW Database Ingestion 接続
 接続プロパティ [234](#)
DB2 for z/OS
 接続プロパティ [240](#)
DB2 for z/OS CDC
 接続プロパティ [237](#)
Db2 for z/OS アンロードファイル
 接続プロパティ [247](#)
Db2 for z/OS イメージコピー
 接続プロパティ [245](#)
Db2 for z/OS バルクロード
 接続プロパティ [235](#)

Db2 for zOS Database Ingestion 接続

接続プロパティ [243](#)

Db2 Warehouse on Cloud

接続プロパティ [255](#)

DB2 ローダー

接続プロパティ [251](#)

Domo 接続

プロパティ [259](#)

Dropbox

接続プロパティ [260](#)

E

Elasticsearch 接続

プロパティ [262](#)

Eloqua REST

接続プロパティ [275](#)

F

FHIR

接続プロパティ [277](#)

File List

接続プロパティ [282](#)

File Processor

接続プロパティ [284](#)

FileIO

接続プロパティ [286](#)

FTP/SFTP

接続プロパティ [293](#)

FTP/SFTP 接続

リモートディレクトリ [293](#)

ルールおよびガイドライン [295](#)

ローカルディレクトリ [293](#)

概要 [293](#)

G

Google Ads

接続プロパティ [296](#)

Google Analytics

接続プロパティ [299](#)

Google Analytics Mass Ingestion 接続

接続プロパティ [302](#)

Google BigQuery

接続プロパティ [303](#)

Google Bigtable

接続プロパティ [318](#)

Google Cloud Storage

接続プロパティ [319](#)

Google Drive

接続プロパティ [324](#)

Google PubSub

接続プロパティ [326-328](#)

Google Sheets

接続プロパティ [329](#)

Google スプレッドシート V2

接続プロパティ [331](#)

Greenplum

接続プロパティ [336](#)

H

Hadoop

接続プロパティ [340](#)

Hadoop Files V2

接続プロパティ [345](#)

Hadoop コネクタ

JDBC URL [341](#)

Hadoop コネクタ:

JDBC ドライバクラス [342](#)

Hadoop ファイル

接続プロパティ [343](#)

Hive

接続プロパティ [348](#)

HubSpot

接続プロパティ [351](#)

I

IBM MQ

接続プロパティ [352](#)

IMS

接続プロパティ [358](#)

IMS CDC

接続プロパティ [355](#)

Informatica Intelligent Cloud Services

Web サイト [30](#)

Informatica グローバルカスタマサポート

連絡先情報 [31](#)

J

JD Edwards EnterpriseOne

接続プロパティ [361](#)

JDBC

接続プロパティ [363, 758](#)

JDBC V2

接続プロパティ [366](#)

JIRA

接続プロパティ [375](#)

JIRA Cloud 接続 [371](#)

JSON Target 接続

プロパティ [377](#)

K

Kerberos 認証

Microsoft SQL Server [494](#)

Oracle [589](#)

Klaviyo

接続プロパティ [382](#)

L

LDAP

接続プロパティ [386](#)

M

Magento V1

接続プロパティ [388](#)

Mailchimp

接続プロパティ [389](#)

Microsoft Access
 接続プロパティ [393](#)
Microsoft Azure Blob Storage V2
 接続プロパティ [398](#)
Microsoft Azure Blob Storage V3
 接続プロパティ [401](#)
Microsoft Azure Data Lake Storage Gen2
 接続プロパティ [408](#)
Microsoft Azure SQL Data Warehouse
 接続プロパティ [417](#)
Microsoft Azure SQL Data Warehouse - データベース取り込み接続
 接続プロパティ [415](#)
Microsoft Azure SQL Data Warehouse V2
 接続プロパティ [419](#)
Microsoft Azure Synapse Analytics Database Ingestion 接続
 接続プロパティ [424](#)
Microsoft Azure Synapse SQL
 接続プロパティ [430](#)
Microsoft CDM Folders V2
 接続プロパティ [437](#)
Microsoft Dynamics 365 for Sales 接続
 概要 [444](#)
Microsoft Dynamics 365 Mass Ingestion 接続
 接続プロパティ [453](#)
Microsoft Dynamics CRM 接続
 接続プロパティ [457](#)
Microsoft Dynamics NAV
 接続プロパティ [459](#)
Microsoft Excel
 接続プロパティ [460](#)
Microsoft SharePoint
 接続プロパティ [479](#)
Microsoft SQL Server
 接続プロパティ [495](#)
Microsoft SQL Server CDC
 接続プロパティ [490](#)
Microsoft SQL Server コネクタ
 管理 [503](#)
Mixpanel
 接続プロパティ [505](#)
MLLP
 接続プロパティ [506](#)
MongoDB Mass Ingestion
 接続プロパティ [508](#)
MongoDB V2 接続
 プロパティ [513](#)
 概要 [512](#)
MongoDB 接続
 プロパティ [510](#)
MRI Software
 接続プロパティ [521](#)
MySQL
 接続プロパティ [525](#)
MySQL CDC
 接続プロパティ [522](#)

N

Netezza
 接続プロパティ [531](#)
NetSuite
 接続プロパティ [543](#)
NetSuite Mass Ingestion 接続
 接続プロパティ [541](#)
NICE Satmetrix
 接続プロパティ [545](#)

O

OAuth アクセストークン
 生成 [166](#)
OData V2 Protocol Reader
 接続プロパティ [552](#)
OData V2 アプリケーション
 接続プロパティ [557](#)
ODBC
 接続プロパティ [567](#)
OpenAir
 接続プロパティ [576](#)
Oracle
 接続プロパティ [590](#)
Oracle CDC
 接続プロパティ [604](#)
Oracle Cloud Object Storage 接続
 プロパティ [609](#)
Oracle CRM Cloud V1
 接続プロパティ [612](#)
Oracle CRM On Demand
 接続プロパティ [614](#)
Oracle Database Ingestion 接続
 接続プロパティ [615](#)
Oracle Financials Cloud V1
 接続プロパティ [626](#)
Oracle Fusion Cloud Mass Ingestion 接続
 接続プロパティ [631](#)
Oracle HCM Cloud V1
 接続プロパティ [633](#)

P

PostgreSQL
 接続プロパティ [649](#)
PostgreSQL CDC
 接続プロパティ [644](#)

Q

QuickBooks V2
 接続プロパティ [655](#)

R

Redis 接続
 プロパティ [657](#)
REST API
 接続プロパティ [659](#)
REST V2
 接続プロパティ [660](#)
REST V3
 接続プロパティ [678](#)
 認証
 標準 [678](#)

S

Salesforce
 接続プロパティ [690](#)
Salesforce Analytics
 接続プロパティ [686](#)
Salesforce Commerce Cloud
 接続プロパティ [688](#)

Salesforce Data Cloud
 接続プロパティ [695](#)
Salesforce Marketing Cloud
 接続プロパティ [698](#)
Salesforce Mass Ingestion 接続
 接続プロパティ [700](#)
Salesforce Pardot
 接続プロパティ [703](#)
SAP ADSO Writer
 接続プロパティ [718](#)
SAP BAPI
 接続プロパティ [726](#)
SAP BAPI コネクタ
 管理 [729](#)
SAP BW
 接続プロパティ [735](#)
SAP BW BEx クエリ接続
 プロパティ [746](#)
SAP HANA CDC
 接続プロパティ [752](#)
SAP HANA Database Ingestion 接続
 接続プロパティ [763](#)
SAP HANA コネクタ
 管理 [760](#), [761](#)
SAP IDoc Reader
 接続プロパティ [714](#)
SAP IDoc Writer
 接続プロパティ [715](#)
SAP IQ
 接続プロパティ [767](#)
SAP Mass Ingestion 接続
 接続プロパティ [769](#)
SAP OData V2 接続 [778](#)
SAP OData V4 接続
 接続 [787](#)
SAP RFC/BAPI インタフェース
 接続プロパティ [716](#)
SAP テーブル
 接続プロパティ [810](#)
SAP 接続
 IDoc および BAPI/RFC [713](#)
SAS 接続
 プロパティ [823](#)
Satmetrix
 接続プロパティ [824](#)
Secure Agent [413](#)
ServiceNow Mass Ingestion 接続
 接続プロパティ [833](#)
SFTP 接続
 キー交換アルゴリズム [294](#)
Snowflake
 接続プロパティ [843](#)
Stripe
 接続プロパティ [863](#)
SuccessFactors LMS 接続
 プロパティ [865](#)
SuccessFactors ODATA コネクタ
 接続プロパティ [867](#)
SuccessFactors コネクタ
 接続プロパティ [871](#)
SuccessFactors 接続
 概要 [867](#)
SurveyMonkey
 接続プロパティ [872](#)

T

Tableau V2
 接続プロパティ [874](#)
Tableau V3
 接続プロパティ [876](#)
Teradata
 接続プロパティ [882](#)

U

UKGPro V2
 接続プロパティ [886](#)
UltiPro
 接続プロパティ [888](#)

V

Veeva Vault 接続 [891](#)
VSAM
 接続プロパティ [898](#)
VSAM CDC
 接続プロパティ [895](#)

W

Web サービス V2
 接続プロパティ [903](#)
Web サービスコンシューマ
 接続プロパティ [901](#)
Web サイト [30](#)
Workday
 接続プロパティ [905](#)
Workday Mass Ingestion 接続
 接続プロパティ [906](#)

X

Xactly
 接続プロパティ [910](#)
Xero
 接続プロパティ [911](#)
XML ソース
 接続プロパティ [913](#)
XML ターゲット
 接続プロパティ [914](#)

Y

Yellowbrick
 接続プロパティ [915](#)

Z

Zendesk
 接続プロパティ [917](#)
Zendesk Mass Ingestion 接続
 接続プロパティ [918](#)
Zendesk V2 接続 [920](#)
Zuora
 接続プロパティ [928](#)

Zuora REST V2
接続プロパティ [929](#)

あ

アクティビティまたはカスタムフィールド
設定 [266](#)
アップグレード通知 [31](#)
アドオンコネクタ
インストール [32](#)
構築 [32](#)
目的 [32](#)

お

オープンテーブル
接続プロパティ [581](#)

き

キー [413](#)
キーストア証明書
作成 [588](#)
キー交換アルゴリズム
SFTP 接続 [294](#)

し

シーケンシャルファイル
接続プロパティ [825](#)
システムステータス [31](#)

す

スキーマ [413](#)
ステータス
Informatica Intelligent Cloud Services [31](#)

と

トラストストア証明書
作成 [587](#)

ふ

プライマリキーとセカンダリキー [413](#)
フラットファイル
接続プロパティ [288](#)

め

メンテナンスの停止 [31](#)

も

モックコネクタ [37](#)

ら

ランタイム環境 [413](#)